Universidad Carlos III de Madrid
www.uc3m.es

TESIS DOCTORAL

Conectando los vehículos a Internet en el sistema de transporte inteligente estandarizado por el ETSI

Autor:

Víctor Sandonís Consuegra

Director/es:

María Calderón Pastor

Ignacio Soto Campos

DEPARTAMENTO DE INGENIERÍA TELEMÁTICA

Leganés, julio 2014

Universidad Carlos III de Madrid
www.uc3m.es

TESIS DOCTORAL

Conectando los vehículos a Internet en el sistema de transporte inteligente estandarizado por el ETSI

Autor: *Víctor Sandonís Consuegra*

Director/es: María Calderón Pastor e Ignacio Soto Campos

Firma del Tribunal Calificador:

Firma

Presidente:

Vocal:

Secretario:

Calificación:

Leganés/Getafe, de de

A mis padres Julio y África,
a mi hermana Afri
y a mi mujer Rocío.
Por todo lo que me han dado sin pedir nada a cambio.

"¿Y si un chico soñara con convertirse en algo distinto
de lo que la sociedad tenía previsto para él?
¿y si un chico aspirara a algo más?"
Película *Man of Steel*

"¿Puedes poner una cita mía?"
Rocío

Agradecimientos

Me gustaría en primer lugar agradecer a mis padres Julio y África, a mi hermana Afri y a mi mujer Rocío su apoyo incondicional en todos los aspectos de mi vida. Las palabras se quedan cortas para agradecer todo lo que han hecho por mí. Gracias también al resto de mi familia por querer lo mejor para mí.

Gracias María e Ignacio por vuestro tiempo y los conocimientos y aptitudes que me habéis transmitido. Ha sido un placer poder trabajar con vosotros durante el tiempo que he estado en la Universidad. Se echa de menos el buen ambiente de trabajo y esos "maratones" tan enriquecedores. Gracias también por vuestra paciencia en ayudarme a dar el "último empujón".

Quiero extender el agradecimiento al departamento de Ingeniería Telemática, en especial a los compañeros del despacho/laboratorio y a todas las personas que directamente o indirectamente me han ayudado a realizar este trabajo.

Gracias también a mis amigos por estar a mi lado y ayudarme a pensar en otras cosas.

Resumen

Las redes vehiculares o *Vehicular Ad hoc NETworks* (VANETs) están consideradas como la tecnología más apropiada para proporcionar a los vehículos capacidades de comunicación que se pueden aplicar a la mejora de la seguridad vial. Además, las VANETs también abren la puerta del mercado a aplicaciones no relacionadas con la seguridad vial entre las que destaca la conectividad a Internet. El acceso a Internet desde las VANETs se puede proporcionar a través de puertas de enlace situadas al borde de la carretera de manera que los vehículos cambian su punto de conexión a Internet al moverse. Esto permite a los conductores y pasajeros utilizar servicios comunes de Internet y nuevas aplicaciones que estén especialmente orientadas para ellos, como por ejemplo las aplicaciones para mejorar la eficiencia del tráfico en carreteras y áreas urbanas. Estos servicios servirán como reclamo para los usuarios, lo que acelerará la penetración de la tecnología en el mercado.

El *European Telecommunications Standards Institute Technical Committee Intelligent Transport System* (ETSI TC ITS) ha estandarizado la arquitectura y los protocolos de comunicaciones para un sistema de transporte inteligente considerando tanto aplicaciones relacionadas con la seguridad vial como la conectividad de los vehículos a Internet. El protocolo de *GeoNetworking* (GN) ha sido diseñado para el encaminamiento de los paquetes en la VANET tomando los requisitos de seguridad vial como punto principal y dejando en un segundo plano los aspectos relacionados con la conectividad a Internet.

En la presente Tesis Doctoral se afronta la problemática de la provisión de conectividad a Internet en el sistema de transporte inteligente estandarizado por el ETSI considerando escenarios de autovía/autopista. Una de las principales contribuciones es el análisis detallado del protocolo de GN que estudia la influencia de los diferentes mecanismos del protocolo, identificando sus puntos débiles y limitaciones. Además, se propone y evalúa la aplicación de diferentes mecanismos de optimización que subsanan las deficiencias encontradas y producen una mejora significativa de las prestaciones. Otra contribución importante de la Tesis Doctoral es la propuesta de una solución que permite integrar el protocolo *Proxy Mobile* IPv6 (PMIPv6) con la arquitectura del sistema de transporte inteligente del ETSI y su protocolo de GN. Se proponen un conjunto de procedimientos que adaptan PMIPv6 a la arquitectura multisalto del ITS. La solución permite a los vehículos mantener sus comunicaciones activas a pesar de los cambios de punto de conexión a Internet, sin que tengan que verse involucrados en los procedimientos de gestión de la movilidad.

El análisis del protocolo de GN, la evaluación de los mecanismos de optimización y la validación de la solución de movilidad se ha llevado a cabo a través de extensas simulaciones utilizando trazas de tráfico sintéticas y trazas de tráfico reales de una importante autopista de circunvalación de Madrid.

Palabras clave: VANET, ETSI ITS, *GeoNetworking*, PMIPv6.

Abstract

Vehicular Ad hoc NETworks (VANETs) are considered as the most suitable technology to provide vehicles with communication capabilities as a mean to improve road safety. Additionally, VANETs also open the door to non-safety applications where Internet connectivity is the main focus. Internet access from VANETs can be provided with the support of gateways located at the side of the roads, such that vehicles change their point of attachment to the Internet while they move. This allows drivers and passengers not only to use common Internet services but also new applications specifically tailored to them such as traffic efficiency applications. This Internet access from the VANET is expected to attract users' attention speeding-up market penetration of the technology.

The European Telecommunications Standards Institute Technical Committee Intelligent Transport System (ETSI TC ITS) has standardized the architecture and the communication protocols for an Intelligent Transport System (ITS) considering both safety applications and the connectivity of vehicles to the Internet. The GeoNetworking protocol (GN) has been designed to forward packets in the VANET taking safety requirements as the main concern, leaving Internet connectivity as a secondary consideration.

In this PhD thesis we tackle the problem of providing Internet access using the standardized ETSI ITS protocols/architecture in highway scenarios. One of the main contributions is a detailed analysis of the GN protocol that studies the influence of the different mechanisms of the protocol, identifying its weak points and limitations. Besides, several optimization mechanisms are applied and evaluated to tackle these limitations and that produce a significant enhancement of the performance. Another main contribution of this PhD thesis is the proposal of a solution to integrate the Proxy Mobile IPv6 (PMIPv6) protocol with the ETSI ITS architecture and its GN protocol. A set of procedures are proposed to adapt PMIPv6 to the multi-hop ETSI ITS architecture. The solution allows vehicles to keep their ongoing communications despite the change of point of attachment to the Internet without their involvement in mobility management procedures.

The analysis of the GN protocol, the evaluation of the optimization mechanisms and the validation of the mobility solution are conducted by means of extensive simulations using synthetic and real traffic traces of an important orbital highway of Madrid.

Keywords: VANET, ETSI ITS, GeoNetworking, PMIPv6.

Índice

Índice de figuras

Capítulo 1

Introducción

Una red vehicular o *Vehicular Ad hoc NETwork* (VANET) es una red *ad hoc* formada por vehículos equipados con interfaces inalámbricas que pueden comunicarse entre sí de manera descentralizada de forma que los vehículos reciben y reenvían los paquetes de datos procedentes de otros nodos de la red. Las VANETs permiten a los vehículos el establecimiento de comunicaciones para el intercambio de información donde se puede diferenciar entre comunicaciones *Vehicle-to-Vehicle* (V2V) y comunicaciones *Vehicle-to-Infrastructure* (V2I). Estas comunicaciones posibilitan el despliegue de aplicaciones con grandes expectativas de futuro que se pueden clasificar en tres grandes grupos: aplicaciones destinadas a la mejora de la seguridad vial, aplicaciones orientadas a la eficiencia del tráfico y aplicaciones de entretenimiento y servicios de información.

Las aplicaciones orientadas a la mejora de la seguridad vial han recibido el interés de la comunidad investigadora e industrial en los últimos años dado que su despliegue posibilitaría la reducción del número de víctimas en accidentes de tráfico. Según los datos de siniestralidad de la Dirección General de Tráfico (DGT), durante el año 2012 se produjeron en España 117.793 víctimas en accidentes de tráfico, de las cuales 1.903 fallecieron [1]. La aplicación de las VANETs al ámbito de la seguridad vial podría reducir estas estadísticas drásticamente, lo que tendría una gran repercusión desde el punto de vista social.

El impacto que las redes vehiculares pueden tener en la sociedad ha motivado la aparición de iniciativas en diferentes instituciones y organismos de estandarización para trabajar en este terreno. El comité técnico del sistema de transporte inteligente del ETSI, *European Telecommunications Standards Institute Technical Committee Intelligent Transport System* (ETSI TC ITS), ha estado trabajando en los últimos años en la definición de la arquitectura y los protocolos de comunicaciones para un sistema de transporte inteligente (ITS) estandarizado. El foco principal de sus especificaciones ha estado dirigido a las aplicaciones vinculadas a la mejora de la seguridad vial, dejando en un segundo plano los requisitos relacionados con las aplicaciones de mejora de la eficiencia del tráfico o de provisión de información/entretenimiento.

El acceso a Internet se está convirtiendo en un aspecto cotidiano en nuestras vidas, tanto es así que la provisión de servicios de información a los conductores y pasajeros mediante la conexión de los vehículos a Internet es otro de los aspectos de interés de las redes vehiculares. Según el Instituto Nacional de Estadística (INE), un 69,8 % de los hogares españoles cuenta con acceso a Internet. De las personas entre 16 y 74 años, el 53,8 % se conecta a Internet a diario y 7 de cada 10 personas que acceden a Internet lo han hecho utilizando un dispositivo móvil. Además, la demanda de acceso a Internet de las personas sigue una tendencia creciente [2]. La conexión de los vehículos a Internet permitiría a los conductores y pasajeros el acceso a multitud de servicios de información y utilizar cualquiera de los servicios comunes de las redes IP como la navegación web, correo electrónico, etc. Asimismo, podría propiciar la apertura de un nuevo mercado de aplicaciones de Internet que estuvieran especialmente destinadas a los conductores y pasajeros de los vehículos. Además, estos servicios servirían como reclamo para los usuarios, lo que impulsaría la penetración en el mercado de esta tecnología, permitiendo contrarrestar uno de los aspectos más críticos en el despliegue de redes vehiculares: se precisa de una cierta penetración en el mercado antes de que las comunicaciones en la VANET puedan ser viables [3]. Esto provocaría de manera indirecta que las aplicaciones destinadas a la seguridad vial fueran más efectivas (más vehículos dispondrían del equipamiento necesario para su correcto funcionamiento).

Tomando como referencia el sistema de transporte inteligente estandarizado por el ETSI, el principal objetivo del trabajo realizado en esta Tesis Doctoral se centra en el estudio de la problemática de la conexión de los vehículos a Internet en escenarios de autovía/autopista. El sistema de transporte inteligente del ETSI plantea la conexión de los vehículos a Internet a través del despliegue de múltiples dispositivos situados al borde de la carretera. Uno de los requisitos críticos para que las comunicaciones de los vehículos con nodos en Internet puedan funcionar correctamente es que el protocolo de encaminamiento que se utiliza en la VANET ofrezca unas prestaciones adecuadas cuando se encaminan los paquetes entre los vehículos y los dispositivos situados al borde de la carretera que ofrecen conectividad a Internet. Las VANETs poseen ciertas características especiales como la inestabilidad de los enlaces entre nodos, provocada por la movilidad y la variabilidad de la densidad de nodos de la red, que hacen que el correcto desempeño del protocolo de encaminamiento sea crítico para el buen funcionamiento de las comunicaciones. Por ello, una de las principales contribuciones del trabajo realizado en esta Tesis Doctoral consiste en el análisis en profundidad del protocolo de encaminamiento utilizado en la VANET del sistema de transporte inteligente definido por el ETSI, el denominado protocolo de *GeoNetworking* (GN). El estudio del protocolo de GN se ha llevado a cabo mediante una evaluación de prestaciones basada en simulación considerando diferentes circunstancias. Este análisis sistemático del comportamiento del protocolo de GN ha permitido estudiar la influencia de los diferentes mecanismos presentes en el protocolo, identificando sus limitaciones y puntos débiles. En base a este análisis pormenorizado, se propone la utilización de diversos mecanismos de optimización con los que se consigue subsanar las deficiencias y conseguir un aumento de las prestaciones.

Por otro lado, se necesita de un mecanismo de asignación y configuración de direcciones en

la VANET para que los vehículos puedan establecer comunicaciones con otros nodos de Internet. Además, es necesario un protocolo que gestione la conexión de los vehículos a los dispositivos que sirven de puerta de enlace hacia Internet. Debido al movimiento de los vehículos, su punto de conexión a Internet cambia continuamente, por lo que se precisa de un protocolo que gestione la movilidad y que permita mantener las comunicaciones de los vehículos activas aunque cambie el punto de acceso a Internet. Otra de las contribuciones del trabajo realizado en esta Tesis Doctoral consiste en la propuesta de una solución para la integración del protocolo de gestión de movilidad PMIPv6 con la arquitectura del sistema de transporte inteligente estandarizada por el ETSI y su protocolo de GN, adaptándolo al entorno multisalto de la VANET. La utilización de PMIPv6 como protocolo de gestión de movilidad permite una mayor eficiencia en los *hand-overs* que los vehículos realizan entre puntos de acceso a Internet. Además, PMIPv6 permite evitar configuraciones de seguridad complejas relacionadas con la movilidad en los vehículos puesto que las funciones de gestión de movilidad IP se realizan desde nodos situados en la red. Asimismo, la progresiva adopción por parte de los operadores de PMIPv6 como protocolo para soportar la movilidad, ofrece la oportunidad de integrar la solución de movilidad de la VANET con la presente en otras regiones de sus redes que utilizan otras tecnologías de acceso, como por ejemplo 3G/4G, y donde se puede proporcionar movilidad por medio de PMIPv6.

De esta forma, la VANET podría verse como una red de acceso *non*-3GPP integrada en la arquitectura 4G. Los vehículos podrían conectarse a Internet a través de diferentes tecnologías de acceso sin cambiar su dirección IP, eligiendo la más apropiada a cada situación, y manteniendo sus comunicaciones activas. Por ejemplo, los vehículos podrían utilizar la red 3G/4G para sus comunicaciones con Internet y moverlas a la VANET cuando sea necesario descargar tráfico de la red móvil celular del operador. Esta aproximación encaja con el modelo perseguido por los operadores: la utilización de redes acceso heterogéneas para minimizar costes y proporcionar mejores prestaciones a los usuarios. De hecho, los operadores están apostando por soluciones basadas *offloading* [4] que les permite transferir comunicaciones a otras redes de acceso para reducir el tráfico de datos en sus redes móviles celulares.

La solución propuesta se valida experimentalmente a través de simulación utilizando trazas de tráfico reales de una importante autopista de circunvalación de Madrid, lo que ayuda a que los resultados obtenidos sean más próximos a una situación real.

La Tesis Doctoral se encuentra dividida en cuatro partes. La Parte I presenta el estado del arte de las redes vehiculares, su conexión a Internet y el sistema de transporte inteligente estandarizado por el ETSI. En el Capítulo 2 se exponen los principales conceptos de las redes vehiculares, se presentan sus motivaciones y se revisan los principales aspectos que hay que considerar para su despliegue considerando sus principales casos de uso. Además, se presentan las diferentes familias de protocolos de encaminamiento comúnmente utilizados en redes vehiculares: protocolos de encaminamiento proactivos, protocolos de encaminamiento reactivos y protocolos basados en encaminamiento geográfico. El Capítulo 3 se centra en los aspectos que hay que solucionar cuando

se conectan las redes vehiculares a Internet y se revisan las soluciones existentes en la literatura. Además, se revisan los protocolos de gestión de movilidad más importantes. En el Capítulo 4 se describe la arquitectura del sistema de transporte inteligente que ha sido estandarizado recientemente por el ETSI y el protocolo de GN que se utiliza para el encaminamiento de los paquetes en la VANET.

Las contribuciones del trabajo realizado en esta Tesis Doctoral se presentan en la Parte II. El Capítulo 5 presenta un análisis detallado del funcionamiento de la arquitectura del sistema de transporte inteligente que ha definido el ETSI y en concreto, del protocolo de GN cuando se utiliza para conectar los vehículos a Internet en escenarios de autovía/autopista. Este estudio se basa en la evaluación de las prestaciones del protocolo a través de simulación, lo que permite detectar sus puntos débiles y limitaciones. Se estudia la influencia de cada uno de los mecanismos del protocolo y se estudian diversas optimizaciones que permiten mejorar las prestaciones de las comunicaciones entre los vehículos y las puertas de enlace hacia Internet.

El Capítulo 6 se centra en la gestión de movilidad necesaria para que los vehículos puedan cambiar su punto de conexión a Internet manteniendo sus comunicaciones activas mientras que se encuentran en movimiento. Se propone una solución en la que a través de una serie de procedimientos se consigue integrar el protocolo de movilidad PMIPv6 con la arquitectura del sistema de transporte inteligente del ETSI y su protocolo de GN considerando el entorno multisalto de la VANET. La solución se valida a través de simulación utilizando trazas de tráfico reales para obtener resultados más próximos a un escenario real.

La Parte III incluye, en el Capítulo 7, las conclusiones obtenidas del trabajo realizado en la presente Tesis Doctoral y, en el Capítulo 8, los trabajos futuros sobre aquellos aspectos que resultaría interesante estudiar.

El Apéndice A incluido en la Parte IV presenta una descripción de las cabeceras de los mensajes del protocolo de GN definido por el ETSI.

Los resultados obtenidos del análisis del protocolo de GN, la identificación de las limitaciones del protocolo y las diferentes optimizaciones que mejoran las prestaciones del mismo, han sido enviados para que se considere su publicación en [5]. Por su parte, la solución de integración del protocolo de gestión de movilidad PMIPv6 con la arquitectura del sistema de transporte inteligente estandarizada por el ETSI y su protocolo de GN ha sido publicada en [6].

Parte I

Estado del Arte

Capítulo 2

Redes vehiculares

En este capítulo se introducen las redes vehiculares o VANETs (*Vehicular Ad hoc NETworks*), sus motivaciones y los principales aspectos que hay que considerar para su despliegue. Además, se exponen algunos ejemplos de sus principales casos de uso. Por otro lado, se describen las diferentes familias de protocolos de encaminamiento utilizados en redes vehiculares, explicando algunos ejemplos de los protocolos más representativos de cada familia.

2.1. Introducción

Para poder definir lo que es una red vehicular o VANET es necesario introducir previamente las redes *ad hoc*. Una red *ad hoc* es una red en la que los nodos que la componen son capaces de comunicarse a través de una interfaz inalámbrica de manera descentralizada, sin necesidad de ninguna infraestructura. En una red *ad hoc* los nodos están preparados para actuar como un *router*, es decir, cada nodo es capaz de recibir y reenviar paquetes de datos a los demás nodos de la red de manera que la decisión sobre qué nodos de la red reenvían los paquetes de datos se toma de forma dinámica en función de la conectividad de la red. De esta manera, un nodo puede comunicarse con otro que se encuentre fuera de su rango de cobertura por medio de una comunicación multisalto, en la que diferentes nodos intermedios forman un camino para reenviar los paquetes de datos salto a salto desde el nodo emisor hasta el receptor.

Una red vehicular o VANET es una red *ad hoc* en la que los nodos de la red son vehículos y por lo tanto, se encuentran en movimiento. De esta manera, las VANETs son un caso particular de las denominadas redes *ad hoc* móviles o MANETs (*Mobile Ad hoc NETworks*). Lo que diferencia a las VANETs de otro tipo de redes *ad hoc* móviles es que sus nodos pueden moverse a una gran velocidad, y por lo general, siguiendo un patrón restringido. Es decir, los vehículos se mueven sobre carreteras con una determinada topología y respetando unas normas de circulación. Una característica muy importante de las redes vehiculares es que la elevada movilidad de los vehículos hace que los enlaces entre ellos sean muy inestables para las comunicaciones. Además, los

vehículos pueden contar con grandes capacidades de memoria y procesamiento. En cambio, en otros tipos de MANETs, los nodos pueden seguir un patrón de movilidad arbitrario y la capacidad de memoria y computación pueden estar limitadas.

Las VANETs permiten el intercambio de información entre vehículos por medio de las denominadas comunicaciones vehiculares. Dentro de las comunicaciones vehiculares podemos diferenciar dos escenarios que presentan características diferentes: las comunicaciones *Vehicle-to-Vehicle* (V2V) y las comunicaciones *Vehicle-to-Infrastructure* (V2I). Las comunicaciones V2V son aquellas que utilizan la VANET para el intercambio de información entre vehículos, es decir, el origen y el destino de las comunicaciones son vehículos pertenecientes a la VANET. En cambio, el término comunicaciones V2I se refiere a las comunicaciones que se pueden establecer entre los vehículos de la VANET y otros nodos en la infraestructura o Internet.

La principal motivación de las redes vehiculares, y por ende de las comunicaciones vehiculares, es que abren un gran abanico de posibles aplicaciones para mejorar la seguridad al volante, aumentar la eficiencia del tráfico y proporcionar información útil a los ocupantes de los vehículos. La mejora de la seguridad vial es una de las aplicaciones de las redes vehiculares con mayor repercusión desde el punto de vista social. Únicamente en España en el año 2012, según los datos de siniestralidad de la Dirección General de Tráfico (DGT), se produjeron 117.793 víctimas en accidentes de tráfico, de las cuales 1.903 fallecieron [1]. Las redes vehiculares podrían ayudar a reducir de forma significativa el número de víctimas en accidentes de tráfico. La idea es que los vehículos puedan enviar mensajes de alerta y que compartan entre sí información sobre su posición, velocidad y dirección. Esta información puede ser utilizada para informar con antelación a los conductores sobre zonas peligrosas en la carretera (por ejemplo hielo en un tramo de vía), frenazos bruscos o atascos repentinos, evitando accidentes y colisiones entre vehículos.

Los atascos son una de las grandes preocupaciones de los conductores que diariamente ven como pierden gran cantidad de tiempo y dinero en combustible. Además, los atascos contribuyen a la contaminación atmosférica por el CO_2 expulsado por los vehículos y a la contaminación acústica por el sonido de los cláxones. Las redes vehiculares pueden ayudar a solucionar estos problemas mejorando la eficiencia del tráfico. Como los vehículos comunican su posición geográfica, se puede utilizar esta información en sistemas que calculen las condiciones de tráfico y proporcionen las mejores rutas a seguir por los conductores en tiempo real.

La provisión de servicios de información a los ocupantes de los vehículos es otra de las aplicaciones de las redes vehiculares. Conectando las redes vehiculares a una infraestructura por medio de equipos situados al borde de las carreteras, se hace posible la conexión de los vehículos a Internet. De esta forma, los conductores y los pasajeros pueden acceder a cualquier información de su interés o utilizar cualquiera de los servicios comunes de las redes IP como la navegación web, correo electrónico, etc.

Las comunicaciones vehiculares abren un mercado con grandes expectativas de futuro, pero el despliegue de un sistema de comunicaciones vehiculares no está exento de problemas. Uno de los

aspectos más críticos es que debido a que las comunicaciones se realizan de forma cooperativa entre diferentes vehículos, se precisa de una cierta penetración de la tecnología en el mercado antes de que las comunicaciones vehiculares puedan operar correctamente. Incluso en el mejor de los casos en el que todos los vehículos que salen de las fábricas estuvieran equipados de serie con un sistema de comunicaciones vehiculares, se tardaría año y medio en llegar a una penetración del 10 % y más de 6 años en llegar al 50 % [3]. El hecho de que el usuario no perciba de inmediato los beneficios del sistema de comunicaciones vehiculares (hasta que una cantidad de vehículos suficiente no tengan instalados los equipos, el sistema no puede funcionar correctamente), supone un impedimento a que los usuarios decidan instalar el equipamiento necesario en sus vehículos.

Aunque los requisitos específicos dependen de la aplicación concreta que se quiera desplegar en la VANET, en general, se desea que la operación de las redes vehiculares sea fiable, robusta y que se garantice un retardo máximo en las comunicaciones, sobre todo si se trata de aplicaciones relacionadas con la seguridad vial. Para ello, son necesarios protocolos de comunicaciones que garanticen que las comunicaciones sean fiables (que no se pueda enviar información malintencionadamente) y que diferencien entre el tratamiento de las comunicaciones críticas (aplicaciones que tratan con temas de seguridad vial) y el tratamiento de otros tipos de comunicaciones no críticas (por ejemplo, navegación web).

Por otro lado, los protocolos de comunicaciones deben ser diseñados teniendo en cuenta las características de las VANETs. Los vehículos pueden moverse a una velocidad elevada que provoca que los enlaces entre los nodos de la red sean muy inestables. Además, la escalabilidad es otro factor muy importante. Los protocolos tienen que operar correctamente con diferentes densidades de vehículos. Deben ser capaces de trabajar adecuadamente en el caso en el que la densidad de vehículos es baja y el rango de cobertura de las antenas de los vehículos dificulta la comunicación entre ellos, como por ejemplo en un entorno rural. Del mismo modo, se debe considerar el caso en el que el tráfico es muy intenso, como puede ser en un atasco en una gran ciudad, donde la multitud de mensajes enviados puede comprometer el ancho de banda disponible en el canal inalámbrico.

2.2. Aplicaciones de las redes vehiculares

Las VANETs permiten el despliegue de diferentes aplicaciones que se pueden clasificar en tres grandes grupos: aplicaciones de seguridad vial, aplicaciones orientadas a la eficiencia del tráfico y aplicaciones de entretenimiento y servicios de información. A continuación se explica cada grupo de aplicaciones y se proporcionan algunos casos de uso como ejemplo [3].

2.2.1. Aplicaciones orientadas a la mejora de la seguridad vial

Las aplicaciones orientadas a la seguridad vial tienen como finalidad ayudar a mejorar la seguridad de los conductores. Las comunicaciones vehiculares permiten que los vehículos puedan

intercambiar entre sí información sobre su posición, velocidad y dirección, de manera que esta se pueda utilizar para evitar colisiones por frenazos bruscos o atascos repentinos informando con antelación al conductor cuando se detecta que existe la posibilidad de colisionar con otro vehículo. Si en el peor de los casos se detecta que la colisión entre vehículos es inevitable, se podrían tomar las medidas oportunas para minimizar los daños de los ocupantes de los vehículos mediante mecanismos de frenado automático o la activación de los *airbags* antes del impacto.

Otro ejemplo de caso de uso es la utilización de las comunicaciones vehiculares para difundir mensajes de alerta en la VANET para informar a los conductores sobre puntos conflictivos o zonas peligrosas en la carretera con suficiente antelación. Por ejemplo, si un vehículo dispone de un sensor que detecta que la carretera está resbaladiza por una mancha de aceite en una curva, se puede generar un mensaje de alerta que se hace llegar al resto de conductores. De esta forma, si un motorista recibe el mensaje de alerta, puede estar atento y evitar una posible caída.

Estos son solo algunos ejemplos de los numerosos casos de uso de las redes vehiculares en el ámbito de la seguridad vial.

2.2.2. Aplicaciones orientadas a la mejora de la eficiencia del tráfico

Dentro de este grupo se encuentran todas las aplicaciones orientadas a mejorar la fluidez del tráfico que se traduce en un menor consumo de tiempo y combustible para los conductores y un mejor aprovechamiento de las infraestructuras viales. Además, de manera indirecta se reduce el impacto medioambiental de la contaminación producida por los vehículos.

Las VANETs permiten a los vehículos difundir mensajes con información sobre su posición geográfica que pueden ser recopilados para calcular el estado del tráfico en diferentes zonas geográficas. De esta manera, se puede desarrollar un sistema que se encargue de recopilar esta información en un centro de control de tráfico y calcule el estado del tráfico en las carreteras en tiempo real (por ejemplo, obteniendo parámetros de densidad, flujo de vehículos y velocidades medias [7]). Del mismo modo, este sistema puede difundir mensajes en la VANET que señalen a los conductores las mejores rutas a seguir para evitar zonas congestionadas en función de las condiciones de tráfico actuales.

Otro ejemplo de caso de uso es aquel en el que se facilita a los vehículos la incorporación a una autovía o autopista. Para ello, teniendo en cuenta las condiciones de circulación de la vía, se informa a los conductores sobre la velocidad deben llevar para realizar una incorporación adecuada sin interrumpir la fluidez del tráfico.

Siguiendo la misma idea, en una intersección regulada por semáforos, se puede difundir mensajes con información del estado y temporización de los mismos. Así, los vehículos que se aproximan a la intersección pueden utilizar esta información para indicar al conductor la velocidad adecuada que debe llevar para evitar parar en la intersección innecesariamente, ahorrando combustible y reduciendo la contaminación.

2.2.3. Aplicaciones de entretenimiento y servicios de información

Las aplicaciones que no están orientadas a mejorar la seguridad vial o la fluidez del tráfico se pueden englobar dentro de este grupo.

Un caso de uso sería un servicio de notificaciones de puntos de interés mediante la difusión de mensajes en la VANET. Por ejemplo, una gasolinera difunde información en la VANET sobre sus precios, que puede ser de interés para aquellos conductores que circulan en su cercanía. Del mismo modo, se puede proporcionar información a los conductores de la ubicación de los parkings más cercanos a su posición, su estado de ocupación, precios, etc.

El acceso a Internet desde los vehículos a través de equipos situados al borde de las carreteras es uno de los casos de uso más relevantes de las redes vehiculares. Esto permite por un lado, que los conductores y los pasajeros puedan utilizar cualquiera de los servicios comunes de las redes IP como la navegación web, correo electrónico, etc., y por otro lado, hace posible la aparición de nuevas aplicaciones de Internet que estén especialmente orientadas para ellos.

2.3. Protocolos de encaminamiento para redes vehiculares

Como se ha mencionado anteriormente, las VANETs presentan ciertas características especiales como la rápida movilidad de sus nodos, que provoca que los enlaces entre nodos sean muy inestables y que las comunicaciones entre ellos se interrumpan continuamente, o que los vehículos se mueven por carreteras siguiendo un cierto patrón y unas reglas de tráfico. Además, la densidad de nodos de la red puede ser muy variable, desde un entorno rural donde la comunicación entre nodos se hace difícil por la falta de conectividad hasta un entorno urbano con una densidad elevada (por ejemplo, un atasco), donde el ancho de banda del canal inalámbrico se puede ver comprometido.

Debido a estas propiedades, los protocolos de encaminamiento son críticos para un buen funcionamiento de las comunicaciones en la VANET y deben ser diseñados teniendo en cuenta sus características. Podemos clasificar los protocolos de encaminamiento para redes *ad hoc* en tres grandes familias: protocolos de encaminamiento proactivo, protocolos de encaminamiento reactivo[1] y protocolos basados en encaminamiento geográfico. A continuación se describen las características de cada uno de los grupos y se explican algunos de sus protocolos más representativos que sirven como ejemplo de su modo de operación. Cabe mencionar que aunque nuestro interés está centrado en los protocolos que permiten el encaminamiento de paquetes para la conexión de los vehículos a Internet donde el tráfico datos es *unicast*, también existen protocolos orientados a la distribución de mensajes *broadcast* en la VANET útiles para aplicaciones vinculadas a la seguridad vial.

[1]Existen también los denominados protocolos de encaminamiento híbridos que combinan las características de los protocolos de encaminamiento reactivo y los protocolos de encaminamiento proactivo.

2.3.1. Protocolos de encaminamiento proactivo

Los protocolos de encaminamiento proactivo se caracterizan porque los nodos comparten entre sí información sobre la topología de la red periódicamente para construir las tablas de encaminamiento o tablas de rutas, asumiendo que las rutas serán útiles en algún momento. En escenarios en los que la movilidad de los nodos es elevada, como es el caso de las redes vehiculares, la topología de la red cambia continuamente. Por ello, el intercambio de información de encaminamiento entre nodos debe ser muy frecuente, ya que de lo contrario, las tablas de encaminamiento se quedarían obsoletas rápidamente.

La ventaja de los protocolos proactivos es que los nodos disponen de una ruta hacia un destino en cualquier momento, fruto del intercambio periódico de información de encaminamiento, sin tener que esperar a su descubrimiento. Sin embargo, la desventaja es que los nodos tienen que compartir información de encaminamiento entre ellos para la construcción de las tablas de rutas incluso cuando están en estado inactivo y no hay tráfico que cursar, lo que desperdicia recursos en el medio inalámbrico.

Optimized Link State Routing Protocol (OLSR) [8], *Destination-Sequenced Distance Vector Routing* (DSDV) [9] y *Topology Broadcast Based on Reverse-Path Forwarding Routing Protocol* (TBRPF) [10] son algunos de los protocolos de encaminamiento proactivo más famosos.

2.3.1.1. *Optimized Link State Routing Protocol* (OLSR)

OLSR es uno de los protocolos de encaminamiento proactivo para MANETs más representativos. De hecho, ha sido estandarizado por el MANET *Working Group* (WG) [11] del *Internet Engineering Task Force* (IETF), se ha probado su funcionamiento en diferentes escenarios de redes *ad hoc* y hay diferentes implementaciones disponibles [12] [13] [14]. A continuación se explica su funcionamiento como ejemplo de protocolo de encaminamiento proactivo.

OLSR es un protocolo de encaminamiento de estado de enlace en el que los nodos intercambian paquetes con sus vecinos periódicamente para construir la tabla de rutas basándose en la topología de la red. La distribución de la información de la topología de la red se realiza mediante la utilización de tres tipos de paquetes: *HELLO*, *Topology Control* (TC) y *Host and Network Association* (HNA).

En OLSR, los nodos conocen qué vecinos están a su alrededor mediante el intercambio periódico de mensajes *HELLO*. Cuando un nodo envía un paquete *HELLO*, incluye en el mensaje una lista de sus vecinos directos, es decir, los nodos que se encuentran a un salto dentro del radio de cobertura. Por lo tanto, mediante el procesamiento de los mensajes *HELLO* recibidos, los nodos obtienen información sobre cuáles son sus vecinos directos (los que se encuentran a un salto) y los nodos que se encuentran a dos saltos. Además, los paquetes *HELLO* sirven para comprobar el estado del enlace con todos los vecinos directos y comprobar si los enlaces inalámbricos son

unidireccionales o bidireccionales (un nodo puede comprobar si se encuentra en la lista de vecinos directos del paquete *HELLO* enviado por otro nodo).

Los paquetes TC se utilizan para distribuir la información de la topología obtenida del procesamiento de los paquetes *HELLO* por toda la red *ad hoc*. Los paquetes TC se distribuyen a todos los nodos para que puedan conocer la topología completa de la red. De esta manera, todos los nodos pueden obtener un árbol de distancia mínima de la red (aplicando por ejemplo el algoritmo de *Dijkstra* [15]) y pueden incluir una entrada en su tabla de rutas hacia cualquier destino de la red *ad hoc*.

La manera más sencilla de distribuir un mensaje a todos los nodos de la red es mediante inundación simple. El modo de operación de la inundación simple puede resumirse en que se reenvía el paquete por toda la red independientemente de qué nodo sea el destinatario. Cuando un nodo recibe un paquete, lo retransmite en *broadcast* a todos los nodos vecinos que se encuentran dentro de su radio de alcance. Antes de retransmitir un paquete, los nodos controlan que no lo han retransmitido anteriormente para que la inundación cese en algún momento. Esta técnica es robusta ya que se garantiza que el paquete se entrega al destino siempre que sea posible. Sin embargo, es muy poco eficiente debido al gran número de retransmisiones redundantes innecesarias, que incrementan el tráfico ofrecido en la red, consumen ancho de banda del medio inalámbrico y provocan colisiones [16].

Dado que la distribución de los mensajes TC mediante inundación simple sería muy costosa para el canal inalámbrico, OLSR utiliza el algoritmo *Multipoint Relay* (MPR). Este algoritmo permite reducir la sobrecarga de señalización en la red *ad hoc* haciendo que solo un subconjunto de nodos, llamados nodos MPR, realicen la distribución de los paquetes TC. Los nodos MPR son aquellos nodos que son seleccionados por el resto de nodos como vecinos bidireccionales, es decir, son vecinos que proporcionan conectividad bidireccional con todos los nodos situados a dos saltos. De esta manera, solamente es necesario que los nodos MPR reenvíen los paquetes TC para conseguir su distribución por toda la red *ad hoc*.

Por último, los mensajes HNA se utilizan cuando algún nodo se quiere anunciar como puerta de enlace hacia otra red. De esta manera, cuando los nodos reciben un paquete HNA, crean una entrada en su tabla de rutas hacia la red destino que se anuncia en el mensaje. Por lo tanto, los nodos que proporcionan conexión a Internet informan al resto de nodos de la red *ad hoc* de su disposición a cursar tráfico hacia Internet difundiendo un mensaje HNA.

2.3.1.2. *Hierarchical Optimized Link State Routing Protocol* (HOLSR)

OLSR presenta problemas de escalabilidad cuando el número de nodos en la red es elevado y los nodos se mueven con alta velocidad [17], características que coinciden con las propias de un escenario de redes vehiculares. *Hierarchical Optimized Link State Routing Protocol* (HOLSR) [18] trata de solucionar estos problemas en MANETs heterogéneas sacando provecho

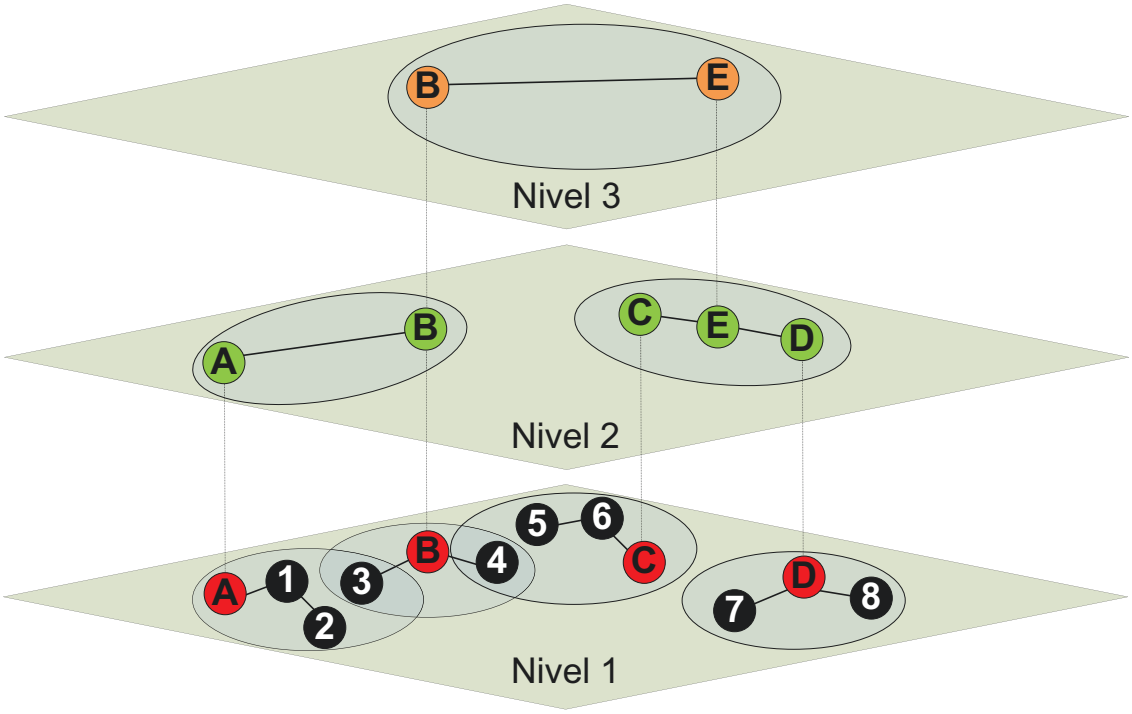


Figura 2.1: Separación en diferentes grupos y niveles jerárquicos en HOLSR

de las diferentes capacidades de comunicación y procesamiento que pueden tener los nodos de la red. Para ello, se ordenan los nodos de la red en diferentes grupos que pertenecen a distintos niveles de jerarquía en función de sus capacidades de comunicación y procesamiento. Gracias a esta separación de los nodos en diferentes niveles de jerarquía, HOLSR consigue reducir la sobrecarga producida por el tráfico de control o señalización.

En la Figura 2.1 se presenta un ejemplo de la organización de los nodos de una MANET en diferentes grupos, a distintos niveles jerárquicos en función de sus capacidades de comunicación y procesamiento. Los nodos que pertenecen al nivel 1 de la jerarquía son aquellos que tienen las menores capacidades de comunicación y cuentan solo con una interfaz inalámbrica para comunicarse con otros nodos dentro de este nivel. El nivel 2 está formado por aquellos nodos que cuentan con hasta dos interfaces inalámbricas de comunicación: una de ellas se utiliza para las comunicaciones que tienen lugar con otros nodos del nivel 1 y la otra, se usa para comunicaciones con otros nodos pertenecientes al nivel 2. De esta forma, el nivel 2 está formado por nodos que tienen mayores capacidades de comunicación y procesamiento que los nodos del nivel 1. Finalmente el nivel 3 está formado por nodos con gran capacidad de procesamiento y comunicación. Los nodos del nivel 3 pueden comunicarse con nodos de los niveles 1 y 2 si cuentan con las interfaces de comunicación adecuadas.

Por otro lado, los nodos se separan en grupos. Un grupo está formado por todos aquellos nodos que han elegido a un mismo nodo padre. Para que se formen los diferentes grupos de nodos, los nodos padre difunden periódicamente mensajes *Cluster ID Announcement* (CIA) para

invitar a otros nodos a unirse a su grupo. Cuando un nodo recibe un paquete CIA, se une al grupo y retransmite el paquete para invitar a otros nodos a unirse al grupo. En el caso de que un nodo reciba mensajes CIA procedentes de diferentes nodos padre (de diferentes grupos), el nodo se unirá al grupo del nodo padre que se encuentre más cerca en número de saltos. De esta forma, los nodos de la red se dividen en grupos en todos los niveles de jerarquía.

Debido a su movimiento, los nodos pueden cambiar de grupo por la recepción de paquetes CIA de nodos padre que se encuentren a un menor número de saltos. Además, la pertenencia a un grupo se asocia a un temporizador que se refresca con la llegada nuevos paquetes CIA del nodo padre. De esta manera, se controla que los nodos de un grupo no se queden huérfanos ante un posible fallo del nodo padre.

Dentro de cada grupo, se utiliza OLSR como protocolo de encaminamiento, con la restricción de que los paquetes *HELLO* y TC solo se intercambian entre los nodos dentro del mismo grupo. De esta forma, HOLSR consigue reducir la cantidad de información topológica que se distribuye por la red *ad hoc*, ya que solo es necesario distribuir los paquetes TC dentro de cada grupo de nodos. Para que los nodos de un grupo puedan comunicarse con nodos de otros grupos, los nodos padre intercambian información de la topología de la red en todos los niveles jerárquicos. Para ello, se utilizan los mensajes *Hierarchical TC* (HTC) que se distribuyen mediante el algoritmo MPR en cada grupo. Con esto, un nodo padre informa al resto de nodos padre de su nivel de jerarquía y de niveles superiores de los nodos que pertenecen a su grupo. De esta manera, cuanto más alto se encuentre situado un nodo en la jerarquía, más conocimiento posee sobre la topología de la red. Los nodos que pertenecen al nivel más alto, conocen la topología de toda la red *ad hoc*.

El encaminamiento de los paquetes de datos se realiza de la siguiente manera. Cuando un nodo envía un paquete de datos a un nodo destino que pertenece a su mismo grupo, existirá una entrada en su tabla de rutas (OLSR se utiliza dentro del grupo) y el nodo usará esta ruta para enviar el paquete hacia el destino. En el caso de que el destino pertenezca a otro grupo, el nodo origen enviará el paquete al nodo padre de su grupo que actúa como puerta de enlace hacia otros grupos. De esta manera el paquete sube en la jerarquía y el procedimiento se repite hasta que el paquete es recibido por un nodo padre que sabe cómo llegar al nodo destino, es decir, que sabe cuál es el nodo padre del grupo al que pertenece el destino. Entonces, el paquete puede ser encaminado hacia el destino.

2.3.2. Protocolos de encaminamiento reactivo

En los protocolos de encaminamiento reactivo los nodos intercambian información de encaminamiento bajo demanda, es decir, solo cuando es necesario. Esto significa que cuando un nodo desea enviar un paquete a un nuevo destino, primero se tiene que proceder al descubrimiento de una ruta mediante el envío de diferentes mensajes de control entre los nodos de la red.

De esta manera, los protocolos reactivos no producen sobrecarga de señalización si no hay tráfico que cursar, al contrario que los protocolos proactivos que intercambian periódicamente

información de encaminamiento para construir la tabla de rutas. Sin embargo, la penalización que hay que pagar con los protocolos reactivos es que los nodos tienen que esperar hasta que se descubra una ruta antes de poder enviar paquetes hacia un destino. En contraste, con los protocolos proactivos, los nodos ya disponen de la ruta cuando desean enviar los paquetes y no sufren un retardo inicial de descubrimiento de ruta.

Entre los protocolos de encaminamiento reactivo más famosos se encuentran *Ad hoc On-Demand Distance Vector Routing Protocol* (AODV) [19] y el protocolo que se considera su sucesor, *Dynamic MANET On-demand Routing protocol* (DYMO) o AODVv2 [20], además de *Dynamic Source Routing Protocol* (DSR) [21]. Aunque todos son protocolos de encaminamiento reactivo, la diferencia entre AODV, DYMO y DSR es que AODV y DYMO realizan encaminamiento salto a salto mientras que DSR realiza encaminamiento en origen. Cuando se realiza encaminamiento salto a salto, cada nodo que recibe el paquete se encarga de encaminar el paquete hacia el siguiente salto en función de su tabla de rutas. En cambio, cuando el encaminamiento se realiza en el origen, el nodo emisor es el que decide la ruta que debe seguir el paquete. Esta ruta se almacena en el paquete de manera que los nodos intermedios saben a qué vecino tienen que reenviar el paquete para llegar al destino.

A continuación se explica la operación del protocolo AODV como ejemplo de protocolo de encaminamiento reactivo.

2.3.2.1. *Ad hoc On-Demand Distance Vector Routing Protocol* (AODV)

AODV es un protocolo de encaminamiento reactivo de vector de distancias para MANETs que ha sido estandarizado por el IETF y del que se disponen múltiples implementaciones [22] [23].

En AODV cuando un nodo desea enviar un paquete a un nuevo destino, primero se debe proceder al descubrimiento de una ruta mediante el envío de un mensaje *Route Request* (RREQ). El mensaje RREQ se difunde mediante inundación por la red hasta que 1) el mensaje es recibido por el nodo destino o 2) el mensaje es recibido por un nodo que no es el destino, pero que tiene una ruta válida hacia el destino. Además, a la vez que el mensaje RREQ se va reenviando por la red, los nodos que lo reciben guardan de donde viene el mensaje RREQ de forma que se establecen diferentes caminos de vuelta hasta el origen, que coindicen con la trayectorias seguidas por los mensajes RREQ (AODV asume que los enlaces entre nodos son bidireccionales).

Cuando el nodo destino o un nodo que tiene una ruta válida hacia el destino recibe el mensaje RREQ, se genera un mensaje de respuesta *Route Reply* (RREP). El mensaje RREP se envía de manera *unicast* (en lugar de en *broadcast* como el mensaje RREQ) hacia el nodo origen siguiendo el mismo camino que el mensaje RREQ, pero a la inversa. Nótese que esto se puede hacer gracias a que los nodos han ido almacenando los caminos de vuelta hacia el origen. Además, con la propagación del mensaje RREP hasta el origen, los nodos intermedios guardan la ruta hacia el destino para su uso posterior para el envío de los paquetes de datos.

De esta forma, el nodo origen de la solicitud RREQ recibirá tantos mensajes RREP como rutas disponibles haya hasta el destino[2]. El nodo origen elegirá aquella ruta con menor número de saltos hasta el destino para el envío de los paquetes de datos. Además, los mensajes incluyen números de secuencia para mantener las rutas actualizadas y evitar bucles.

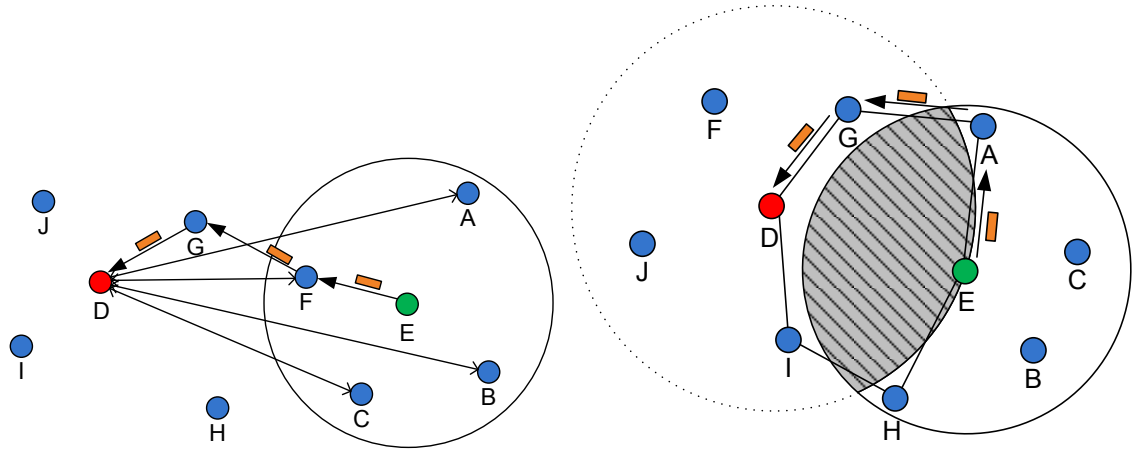
Para el mantenimiento de las rutas se establece un tiempo de caducidad de manera que los nodos mantienen las rutas en sus tablas mientras que estén en uso (mientras que haya paquetes de datos que las utilicen) y si no, tras la expiración del tiempo de caducidad, son eliminadas. Por otro lado, se utilizan mensajes *HELLO* para comprobar el estado de los enlaces con los vecinos directos. Cuando un nodo detecta que un enlace con un vecino falla, enviará un mensaje de error *Route Error* (RERR) hacia aquellos vecinos que están utilizando una ruta que se ve afectada por la caída del enlace. El mensaje RERR se reenvía de vecino en vecino hasta que llega a todos los nodos origen que tienen rutas afectadas por la caída del enlace. De esta forma, los nodos origen pueden iniciar el descubrimiento de una nueva ruta.

2.3.3. Protocolos basados en encaminamiento geográfico

Como se ha descrito anteriormente, los protocolos de encaminamiento proactivo y reactivo encaminan los paquetes en función de la topología de la red. En un escenario de red vehicular en el que la topología de la red está en continuo cambio, estos protocolos necesitan intercambiar constantemente paquetes de control para mantener las tablas de rutas actualizadas, generando una gran sobrecarga en la red. En cambio, en los protocolos basados en encaminamiento geográfico los nodos guardan información sobre la posición geográfica de los nodos vecinos y la utilizan para encaminar los paquetes. Para ello, asumen que los nodos de la red pueden obtener su posición geográfica mediante algún mecanismo de localización, como por ejemplo un GPS (*Global Positioning System*), y la existencia de un servicio de localización que permite obtener la posición geográfica del destino de los paquetes.

Geo-cast se define como la entrega de información a los nodos que se encuentran en una determinada posición geográfica. Existen tres tipos de entregas de paquetes: *geo-unicast*, *geo-broadcast* y *geo-anycast*. Un paquete *geo-unicast* va dirigido a un único destino que se encuentra en una posición geográfica determinada. En *geo-broadcast*, el paquete se entrega a todos los nodos que se encuentran dentro de una zona geográfica concreta. En *geo-anycast*, el destinatario del paquete es un nodo arbitrario entre aquellos que se encuentran dentro de un área geográfica específica. De esta manera, dentro de los protocolos basados en encaminamiento geográfico se puede diferenciar entre aquellos protocolos que están orientados a la entrega de paquetes *geo-broadcast*, *geo-anycast* o *geo-unicast* [24]. En cualquiera de los tipos de entrega (*geo-unicast*, *geo-broadcast* y *geo-anycast*), los paquetes se encaminan hacia la posición geográfica del destino en función de la localización de los nodos de la red.

[2]Se supone que el nodo destino es el que contesta a los mensajes RREQ y que no existe ningún nodo intermedio con una ruta válida hacia el destino.



(a) Elección de siguiente vecino GPSR (b) Operación de *perimeter forwarding*

Figura 2.2: Ejemplos de funcionamiento de GPSR

Greedy Perimeter Stateless Routing (GPSR) [25] y *Distance Routing Effect Algorithm for Mobility* (DREAM) [26] son algunos de los protocolos basados en encaminamiento geográfico más famosos. A continuación se describe el funcionamiento del protocolo GPSR que es el protocolo de encaminamiento geográfico más representativo.

2.3.3.1. *Greedy Perimeter Stateless Routing* (GPSR)

GPSR es un protocolo de encaminamiento geográfico que se basa en dos algoritmos para el reenvío de los paquetes por la red: *greedy forwarding*, que se utiliza siempre que es posible, y *perimeter forwarding* que se utiliza en los casos en los que no se puede hacer uso de *greedy forwarding*.

Greedy forwarding se basa en la idea de que si un nodo conoce la posición geográfica de sus nodos vecinos (aquellos que están en contacto directo dentro de su radio de cobertura), este puede determinar el mejor vecino al que enviar el paquete, que será aquel que se encuentre más cerca de la posición geográfica del destino. De este modo, el paquete puede ser reenviado de vecino en vecino de forma que en cada salto se encuentre más cerca del destino, hasta que finalmente se pueda entregar al destinatario.

En la Figura 2.2(a) se muestra un ejemplo donde el nodo E se dispone a enviar un paquete con destino el nodo D. Como el nodo F es el nodo más cercano al destino D entre los vecinos que se encuentran dentro de su radio de alcance, el nodo E envía el paquete de datos al nodo F. Los nodos cuando reciben un paquete de datos repiten la misma operación, cada nodo retransmite el paquete al vecino más cercano al destino, hasta que el paquete llegue al destino D. De esta forma, el nodo F reenvía el paquete al nodo G, que finalmente entrega el paquete al destino D.

Para que los nodos tengan conciencia de la posición geográfica de sus vecinos se utiliza un algoritmo de balizas o *beacons*. Cada nodo transmite periódicamente en *broadcast* un mensaje

beacon que contiene su identificador y posición, de forma que es recibido por sus vecinos directos, es decir, los nodos que están dentro de su radio de cobertura. Cuando un nodo recibe un mensaje *beacon*, este almacena la información que contiene para posibles usos futuros en una tabla de localización, de manera que cada vecino tiene una entrada asociada en la tabla.

El envío de mensajes *beacon* es periódico porque debido a la movilidad de los nodos es necesario refrescar las entradas de la tabla de localización para evitar tener información de posición geográfica obsoleta. Además, los vecinos pueden dejar de ser alcanzables porque debido a su movimiento salen fuera del radio de cobertura, por lo que las entradas de la tabla de localización tienen un tiempo de caducidad. Cuando el tiempo de caducidad de la entrada de un vecino expira, significa que durante un tiempo no se han recibido mensajes *beacon* del vecino que refresquen su posición geográfica en la tabla de localización. Por ello, se considera que el vecino es inalcanzable y se elimina su entrada de la tabla.

Para minimizar la sobrecarga de tráfico provocada por el envío periódico de mensajes *beacon* se utiliza *piggybacking*. De esta forma, cuando un nodo transmite un paquete de datos, incluye en el paquete su posición geográfica, que será recibida por todos los nodos que se encuentren dentro del radio de cobertura (si se reciben paquetes en modo promiscuo). Además, se puede minimizar aún más la sobrecarga debida al envío periódico de *beacons* utilizando mensajes de petición, de manera que un nodo solo solicitará información geográfica a sus vecinos cuando necesite encaminar algún paquete de datos.

Sin embargo, *greedy forwarding* tiene problemas en el encaminamiento de los paquetes cuando un nodo no puede encontrar ningún vecino dentro de su radio de alcance que se encuentre más cerca del destino que él mismo. En estas situaciones se prescinde temporalmente de *greedy forwarding* y se envía el paquete hacia otro nodo situado más lejos del destino mediante el uso del mecanismo de *perimeter forwarding*.

El mecanismo de *perimeter forwarding* se utiliza cuando falla *greedy forwarding* y se basa en la utilización del concepto de la regla de la mano derecha. De forma resumida, la regla de la mano derecha dice que una persona encerrada en un laberinto solo tiene que caminar con su mano derecha pegada a la pared para recorrer todos los muros del mismo y que, por consiguiente, en algún momento encuentra la salida. En lugar de un laberinto, modelando una red como un grafo planar, lo que tenemos es un conjunto de vértices que representan los nodos de la red y un conjunto de aristas que representan la conectividad directa entre nodos. En este caso, la regla de la mano derecha se puede utilizar para recorrer el perímetro de la zona sin vecinos que ocasiona problemas al mecanismo de *greedy forwarding*, hasta llegar a un nodo que se encuentre más cerca del destino que el nodo inicial donde falló *greedy forwarding*.

La Figura 2.2(b) presenta un ejemplo donde *greedy forwarding* falla en el nodo E porque no puede encontrar ningún vecino dentro de su radio de cobertura que se encuentre más cerca del destino D que él mismo (los nodos A y H están situados más lejos del destino). En estas circunstancias, se utiliza *perimeter forwarding* para recorrer el perímetro de la zona sombreada

sin vecinos, hasta que el paquete llega al nodo G, que está más cerca del destino que el nodo E. Finalmente, G puede entregar el paquete al destino, el nodo D.

Resumiendo, GPSR utiliza siempre que es posible *greedy forwarding* salvo en aquellos casos mencionados anteriormente en los que es necesario aplicar *perimeter forwarding*. Sin embargo, puede darse el caso de que el destino no sea alcanzable por particiones entre zonas de la red *ad hoc* o porque el destino no se encuentre dentro del radio de cobertura de ningún nodo. En ese caso, el paquete sería descartado.

En la literatura existen múltiples trabajos que comparan las prestaciones de los protocolos de encaminamiento proactivo y reactivo tanto en MANETs como en VANETs [27–32]. De manera general se puede decir que en escenarios con baja densidad de nodos y baja movilidad, los protocolos proactivos ofrecen mejores prestaciones que los protocolos reactivos. Sin embargo, los protocolos reactivos se comportan mejor que los protocolos proactivos cuando la densidad de nodos y la movilidad de los mismos aumentan. Esto se debe principalmente a la sobrecarga que se produce en la red por el intercambio de información de control para que los protocolos proactivos puedan mantener actualizadas las tablas de rutas ante la movilidad de los nodos. La elevada movilidad de los nodos hace que los protocolos proactivos utilicen rutas obsoletas, mientras que los protocolos reactivos tienen mayor capacidad de reacción ante cambios en la topología. Sin embargo, el procedimiento de descubrimiento de ruta introduce un mayor retardo en la entrega de paquetes en los protocolos reactivos frente a los protocolos proactivos. Un aspecto que se puede extraer de los diferentes análisis realizados en estos trabajos es el impacto que tiene el entorno de simulación y los patrones de movilidad de los nodos sobre la estimación de las prestaciones de los protocolos de encaminamiento [33].

Por otro lado, los protocolos de encaminamiento geográfico obtienen mejores prestaciones cuando la densidad y la movilidad de los nodos es elevada [25, 34, 35], como ocurre en un escenario de redes vehiculares. Esto se pone de manifiesto en el hecho de que un organismo de estandarización como el ETSI haya decidido utilizar un protocolo de encaminamiento geográfico en la VANET de su sistema de transporte inteligente [36].

Capítulo 3

Conexión de las redes vehiculares a Internet

En este capítulo se presentan los problemas que hay que afrontar en la conexión a Internet de las redes vehiculares y se hace una revisión de las soluciones existentes en la literatura. Además, se exponen algunas de las soluciones de gestión de movilidad más importantes.

3.1. Introducción

En los últimos años, las redes vehiculares han recibido la atención de la comunidad investigadora e industrial dado que su aplicación en la mejora de la seguridad vial puede ayudar a reducir el número de víctimas en accidentes de tráfico. Sin embargo, la mejora de la seguridad vial no es la única aplicación de las redes vehiculares que despierta interés. Como se ha comentado en la introducción, las estadísticas de acceso a Internet siguen una tendencia creciente, lo que refleja una gran demanda por parte de los usuarios. La conexión a Internet de los vehículos permitiría que sus ocupantes pudieran acceder a multitud de servicios de información y utilizar cualquiera de los servicios comunes de las redes IP como la navegación web, correo electrónico, etc. Además, podría aparecer un nuevo mercado de aplicaciones de Internet que tuviera a los conductores y pasajeros como foco de interés. La conexión de las VANETs a la infraestructura permitiría el desarrollo de aplicaciones relacionadas con la mejora de la eficiencia del tráfico que se basan en la recopilación de información sobre el estado de la circulación en un centro de control de tráfico para aconsejar a los conductores rutas alternativas sin retenciones.

La conexión de los vehículos a Internet se puede realizar a través de diferentes tecnologías de acceso [37]. Por un lado, se pueden conectar las VANETs a la infraestructura a través de equipos situados al borde de las carreteras, denominados *Road Side Units* (RSUs), que actúan como puertas de enlace y que pueden proporcionar conexión a Internet porque están conectados

a la infraestructura de red de algún operador. En este caso, las comunicaciones se llevan a cabo utilizando tecnologías inalámbricas de corto alcance o *Dedicated Short-Range Communications* (DSRC). DSRC engloba un conjunto de tecnologías de comunicaciones de corto alcance entre las que destacan las tecnologías Wi-Fi IEEE 802.11 [38], y especialmente IEEE 802.11p [39], que es una adaptación del estándar IEEE 802.11 para mejorar las prestaciones de las comunicaciones en escenarios de redes vehiculares.

Por otro lado, se puede proporcionar a los vehículos conexión a Internet mediante tecnologías de comunicaciones móviles celulares (GPRS, UMTS, LTE). En [40], los autores plantean el uso de redes celulares no solo para comunicaciones V2I, sino también para comunicaciones V2V aprovechando que las redes ya se encuentran desplegadas y que los operadores están continuamente mejorándolas. Sin embargo, la conexión a Internet de los vehículos mediante tecnologías 3G y 4G tiene como principal inconveniente que la conexión de una gran cantidad de vehículos incrementaría en gran medida el volumen de tráfico en las redes móviles de los operadores, lo que se sumaría a los problemas que estos están experimentando en sus redes para poder soportar la creciente demanda de tráfico de datos debido a la proliferación de los *smartphones*. De hecho, los operadores están apostando por soluciones basadas en *offloading* [4] que les permite transferir comunicaciones a otras redes de acceso, como por ejemplo redes Wi-Fi, para reducir el tráfico de datos en sus redes móviles celulares. Para poder hacer frente a este volumen de tráfico, los operadores tendrían que realizar una fuerte inversión en el despliegue de nuevos equipos para incrementar la capacidad de sus redes, lo que supondría un alto coste.

Por ello, el escenario que resulta más interesante, y cuyo despliegue parece más probable, es aquel que busca una solución híbrida donde los vehículos se encuentran equipados con múltiples tecnologías de comunicaciones y utilizan la más adecuada para cada situación. Por ejemplo, los vehículos podrían estar equipados con una interfaz 3G/LTE y una interfaz IEEE 802.11 de manera que la VANET fuera una red de acceso *non*-3GPP integrada en la arquitectura 4G. Este modelo sigue la tendencia que los operadores están impulsando que se basa en la utilización de redes acceso heterogéneas para minimizar costes y proporcionar mejores prestaciones a los usuarios.

La conexión de los vehículos a Internet por medio de RSUs, presenta una serie de requisitos que hay que resolver:

- Dado el gran número de vehículos que puede pertenecer a una VANET y las limitaciones de cobertura, se precisa del despliegue de múltiples RSUs que actúen como puertas de enlace hacia Internet. Será necesario emplazar adecuadamente los equipos y realizar cálculos de dimensionamiento para distribuir el tráfico de la VANET entre las diferentes RSUs. Además, hay que decidir si los vehículos se pueden conectar a las RSUs por medio de una comunicación multisalto a través de diferentes nodos de la VANET o, por el contrario, únicamente se permite la comunicación directa entre los vehículos y las RSUs (a un salto). La comunicación directa entre los vehículos y las RSUs tiene la ventaja de que los vehículos se pueden comunicar a una tasa mayor. Sin embargo, solo se puede ofrecer conectividad a

aquellos vehículos que se encuentran situados dentro del radio de cobertura de la RSU, por lo que habría que aumentar el número de RSUs necesarias para poder dar cobertura a toda la VANET. En cambio, si se utilizan comunicaciones multisalto, se puede incrementar la conectividad proporcionando acceso a Internet a vehículos que se encuentran a más de un salto de la RSU, pero a expensas de reducir la capacidad disponible [41, 42].

En cualquier caso, es necesario un protocolo que gestione la conexión de los vehículos a las puertas de enlace hacia Internet o RSUs. Debe existir un mecanismo por el que los vehículos puedan descubrir las RSUs disponibles, seleccionar la mejor RSU entre las posibles alternativas para sus comunicaciones con Internet y gestionar el cambio de conexión a nuevas RSUs cuando, debido al movimiento, se pierda conectividad con la antigua RSU que se estaba utilizando.

- Como se discutió anteriormente, es necesario un protocolo de encaminamiento para establecer las rutas entre los nodos que forman la VANET y encaminar los paquetes entre los vehículos y las RSUs conectadas a Internet. Las VANETs tienen ciertas características especiales como la inestabilidad de los enlaces entre nodos provocada por la alta movilidad, y la variabilidad de la densidad de nodos en la red, que hacen que el correcto desempeño del protocolo de encaminamiento sea crítico para el buen funcionamiento de las comunicaciones.

- Para que los vehículos puedan establecer una comunicación con cualquier otro nodo de Internet, en primer lugar, es necesario que configuren una dirección IP. Se debe asegurar que todos los vehículos configuran una dirección IP que es única dentro de la VANET, es decir, no puede haber direcciones duplicadas en la VANET, y que además, sean topológicamente válidas para que los vehículos puedan ser alcanzables desde Internet a través de las RSUs. De esta manera, se necesita un mecanismo de asignación y configuración de direcciones IP en la VANET.

- Debido a su movimiento, los vehículos cambian su punto de acceso a Internet continuamente conectándose a diferentes RSUs. Por ello, es necesario un protocolo que gestione la movilidad y que mantenga las comunicaciones de los vehículos activas a pesar del *hand-over* entre puntos de acceso.

Centrándonos en la gestión de la movilidad, esta se puede llevar a cabo en diferentes capas de la torre de protocolos, pero posiblemente la gestión de la movilidad a nivel IP sea lo más conveniente. Por ejemplo, las redes móviles celulares realizan la gestión de movilidad de los usuarios entre diferentes celdas a nivel de enlace. Otro ejemplo de tecnología donde la gestión de la movilidad se puede realizar a nivel de enlace es IEEE 802.11, que cuenta con mecanismos para realizar un *hand-over* entre diferentes puntos de acceso [43]. Sin embargo, la gestión de la movilidad a nivel de enlace está limitada a una única tecnología de comunicaciones. En el caso de que se

disponga de más de una interfaz de comunicaciones de diferentes tecnologías, como en el mencionado escenario híbrido (cuyo despliegue parece más probable) donde los vehículos podrían estar equipados con una interfaz IEEE 802.11 y una interfaz 3G/LTE, sería conveniente poder gestionar la movilidad entre redes heterogéneas, es decir, poder realizar lo que se conoce como *hand-over* vertical entre diferentes tecnologías de acceso. Para ello, son necesarias soluciones que gestionen la movilidad por encima del nivel de enlace.

Existen varias alternativas para gestionar la movilidad por encima del nivel de enlace entre sub-redes IP o entre redes heterogéneas [44], lo que generalmente implica un cambio de dirección IP del nodo móvil. El problema de la movilidad en este caso reside en que las redes TCP/IP fueron diseñadas para nodos fijos y las direcciones IP tienen dos cometidos: localizador e identificador. Por un lado, la dirección IP actúa como localizador de manera que los paquetes se puedan encaminar por la red y ser entregados al destino. Por otro lado, la dirección IP tiene el papel de identificador y es utilizada para identificar las comunicaciones entre dos extremos. El conflicto aparece cuando un nodo móvil realiza un *hand-over* entre sub-redes IP diferentes. El nodo móvil tiene que cambiar su dirección IP por una nueva que sea topológicamente válida en la nueva localización, de manera que pueda ser alcanzable desde Internet. Sin embargo, el nodo móvil desearía mantener la dirección IP que identifica a las comunicaciones que tiene activas con otros equipos.

Por otro lado, existen diferentes soluciones para gestionar la movilidad a nivel de transporte [45–47], sin embargo, son soluciones válidas para un único protocolo de transporte. De esta manera, cada protocolo de transporte tendría que implementar sus propios mecanismos de movilidad. Lo mismo ocurre a nivel de aplicación, por ejemplo, SIP soporta movilidad [48] que puede aplicarse en entornos IMS (*IP Multimedia Subsystem*) [49, 50] o IPTV [51], pero cada aplicación tiene que estar preparada para soportar el cambio de dirección IP. También existen soluciones que proponen introducir una nueva capa en la torre de protocolos como *Host Identity Protocol* (HIP) [52] o *Multiple Address Service for Transport* (MAST) [53]. Sin embargo, la propia introducción de cambios en la torre de protocolos TCP/IP tradicional es la gran desventaja de estas alternativas.

Por ello, parece que lo más adecuado es gestionar la movilidad a nivel IP, ya que es la capa común de la pila de protocolos. En la siguiente sección se presentan las soluciones de gestión de movilidad a nivel IP más importantes.

3.2. Gestión de la movilidad IP

Dentro de los protocolos de gestión de la movilidad IP podemos diferenciar dos grandes filosofías: *client-based* y *network-based*. Los protocolos que siguen el enfoque *client-based* implementan las diferentes funcionalidades necesarias para la gestión de la movilidad tanto en entidades situadas en la red como en el terminal móvil, por lo que el terminal móvil tiene que soportar y participar en los diferentes mecanismos de gestión de la movilidad. Por el contrario, los protocolos

que siguen una aproximación *network-based* tratan de mover todas las funcionalidades de movilidad necesarias a entidades en la red, de forma que la movilidad pueda ser gestionada desde la red sin que el terminal móvil tenga que verse involucrado en ningún procedimiento para gestionar su movilidad. La ventaja de esta aproximación es que se puede proporcionar movilidad a terminales estándar (sin capacidades de movilidad), dado que la red se encarga de ejecutar los mecanismos necesarios en su lugar.

Por otro lado, se puede diferenciar entre gestión de movilidad global y localizada. Si la gestión de la movilidad es global, los terminales móviles pueden moverse entre redes cualesquiera manteniendo sus comunicaciones activas. Por el contrario, si la movilidad es localizada, los terminales móviles únicamente pueden conservar sus comunicaciones activas cuando se mueven entre redes de un mismo dominio de acceso donde se soporta la movilidad.

A continuación se describen brevemente las soluciones de movilidad IP más importantes que han sido publicadas por el IETF.

3.2.1. *Mobile* IP

El IETF ha estudiado la movilidad tanto en IPv4 como en IPv6, llegando a especificar *Mobile* IPv4 (MIPv4) [54] y *Mobile* IPv6 (MIPv6) [55]. Aunque MIPv6 se basa en MIPv4 y comparten muchos de los conceptos, en MIPv6 se explotan ciertas características de IPv6 como son los mecanismos de auto-configuración de direcciones [56,57], la amplia disponibilidad de direcciones y la posibilidad de incluir cabeceras de extensión. Estas características de IPv6, junto con el problema de la escasez de direcciones IPv4 y la gran cantidad de nodos que se conectarían a Internet en un sistema de transporte inteligente, ha motivado que organismos de estandarización como el C2C-CC y el ETSI ITS adopten la utilización de IPv6 en sus sistemas [58]. Por ello, nos centramos en la descripción de MIPv6.

MIPv6 es el protocolo de movilidad de IPv6 que permite a terminales móviles, denominados nodos móviles (*Mobile Nodes*, MNs), cambiar su punto de conexión a Internet entre diferentes subredes manteniendo sus comunicaciones activas. Los MNs tienen asignadas dos direcciones IPv6, la *Home Address* (HoA) y la *Care of Address* (CoA). La HoA es la dirección permanente del MN que es topológicamente válida en su red hogar. La CoA es la dirección temporal que obtiene el MN cuando se conecta a una red visitada. De esta manera, la HoA se utiliza como identificador en las comunicaciones que establece el MN y la CoA tiene el papel de localizador en el encaminamiento de los paquetes.

MIPv6 define el *Home Agent* (HA). El HA es un *router* con funcionalidad especial situado en la red hogar del MN que se encarga de interceptar los paquetes que van dirigidos a la HoA del MN. Como el MN mantiene informado al HA sobre su localización, es decir, su CoA, el HA puede redirigir los paquetes al MN en su nueva red. Para ello, se establece un túnel bidireccional IP sobre IP entre el HA y el MN.

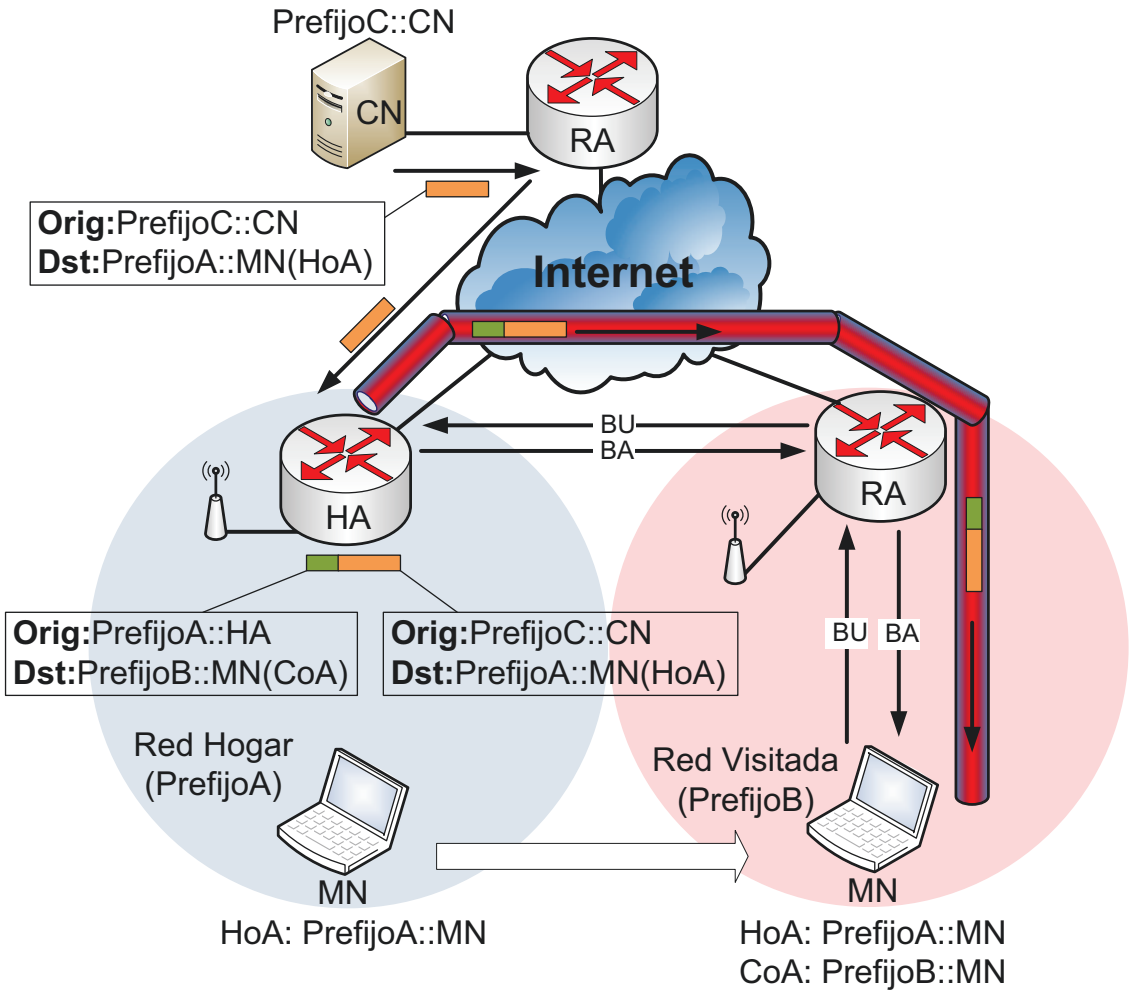


Figura 3.1: Esquema de operación de MIPv6

En la Figura 3.1 se representa el modo de operación de MIPv6. El MN pertenece a su red hogar donde tiene asignada una dirección IPv6 del prefijo A, la HoA. La HoA es topológicamente válida en la red hogar y tiene el papel tanto de identificador como de localizador mientras que el MN se encuentra conectado a su red hogar. Mientras el MN se encuentra conectado a su red hogar, las comunicaciones se establecen según los procedimientos estándar de IPv6 y no es necesario ningún comportamiento especial.

Cuando el MN se mueve y se conecta a una red visitada, obtiene una dirección IPv6 en la nueva red que es la que se denomina CoA. Es necesario que el MN obtenga una nueva dirección IPv6 que sea topológicamente válida en la red visitada para poder ser alcanzable en su nueva localización. Además, el MN utilizará la CoA como dirección origen en los paquetes que envíe en la red visitada para evitar que el *Router* de Acceso (RA) los descarte[1]. Una vez que el MN

[1]Los *routers* pueden realizar *ingress filtering* como mecanismo para evitar ataques de suplantación de direcciones

ha configurado la CoA (que en el ejemplo de la Figura 3.1 tiene el prefijo B), envía un mensaje *Binding Update* (BU) al HA para informarle de la CoA que ha configurado en la red visitada. Así, el HA es consciente de que el MN se ha movido a una red visitada y que es alcanzable por medio de su CoA. Como confirmación, el HA responde al MN con un mensaje *Binding Acknowledgment* (BA) indicando que se ha actualizado su CoA. Además, se establece un túnel bidireccional IP sobre IP entre el HA y MN para el envío de los paquetes entre la red hogar y el MN conectado a la red visitada. Esta operación se repite cada vez que el MN cambia su conexión a una nueva red visitada de manera que se actualiza en el HA la localización del MN, es decir, la CoA obtenida en cada red visitada.

Cuando el MN se comunica con otro nodo de Internet, denominado *Correspondent Node* (CN), el CN desconoce que el MN está situado en una red visitada (el MN utiliza la HoA como identificador de sus conexiones, por lo que el CN no es consciente de la CoA). Los paquetes enviados por el CN tienen como dirección IPv6 destino la HoA del MN por lo que serán encaminados hasta la red hogar. Allí, el HA los recibe en nombre del MN y se encarga de encapsularlos colocando otra cabecera IPv6 para enviarlos por el túnel entre el HA y el MN. Esta cabecera IPv6 tendrá como dirección IPv6 origen la dirección IPv6 del HA y como dirección IPv6 destino la CoA del MN, de manera que los paquetes se encaminan por el túnel hasta el MN conectado a la red visitada. Una vez que los paquetes llegan al MN, se elimina la cabecera del túnel y se entregan a las capas superiores de la torre de protocolos, que al igual que el CN, solo son conscientes de la HoA. Aunque en la figura solo se muestra el encaminamiento de los paquetes enviados por el CN hasta el MN, en el sentido contrario se procede del mismo modo: los paquetes generados por el MN son encapsulados y encaminados por el túnel hasta el HA situado en la red hogar que, tras eliminar la cabecera IPv6 del túnel, reenvía los paquetes hasta el CN.

Uno de los principales inconvenientes que presenta MIPv6 es el hecho de que los paquetes tengan que pasar por el HA situado en la red hogar aunque el MN y el CN se encuentren próximos entre sí, lo que incrementa el retardo sufrido por los paquetes. Además, el hecho de incluir la cabecera IPv6 extra para el túnel entre el HA y el MN reduce la eficiencia al aumentar el tamaño del paquete. Existe una solución de optimización de rutas que soluciona estos problemas a expensas de que el CN soporte ciertas funcionalidades de movilidad. La idea es informar al CN sobre la CoA del MN mediante el intercambio de mensajes BU y BA para que el encaminamiento de los paquetes sea directo entre el MN y CN, sin que sea necesario que los paquetes viajen por el HA en la red hogar.

Por otro lado, existen diferentes soluciones de optimización para MIPv6 como *Fast Mobile IPv6* (FMIPv6) [59] y *Hierarchical Mobile IPv6* (HMIPv6) [60] que minimizan el tiempo de interrupción durante el *hand-over* entre redes visitadas y mejoran la eficiencia de la señalización (importante en el segmento radio de las comunicaciones).

(se comprueba que la dirección origen de los paquetes es topológicamente válida en la red a la que dan servicio).

3.2.2. *Proxy Mobile* IPv6

En los últimos años ha surgido una nueva tendencia en la gestión de la movilidad a nivel IP que propone controlar la movilidad de los nodos móviles dentro de un dominio localizado sin que estos tengan que intervenir en el propio soporte de la movilidad IP. Esto se consigue haciendo que todas las funcionalidades de movilidad IP necesarias se realicen en nodos de la red. A esta tendencia se la conoce como *Network-based Localized Mobility Management* (NetLMM). Este tipo de soluciones han sido impulsadas por los operadores, ya que les permite tener más control sobre la gestión de la movilidad en sus redes. Además, como todas las funcionalidades de soporte de movilidad IP recaen en nodos de la red se simplifica en cierto modo su despliegue, ya que se evita la necesidad de *software* especial o configuraciones específicas en los nodos móviles. En contraste, otras soluciones de movilidad *client-based*, como por ejemplo MIPv6, precisan que el MN tenga una configuración de seguridad y soporte señalización específica para la movilidad.

PMIPv6 [61] es un protocolo de gestión de movilidad IP que sigue esta filosofía. PMIPv6 reutiliza algunos de los conceptos de MIPv6 [55], pero reubicando las funcionalidades de movilidad del MN en nodos situados en la red. De esta forma, una de las principales ventajas de PMIPv6 es que el MN no participa en la señalización de movilidad IP, por lo que no se precisa el MN implemente su soporte. Un MN puede moverse dentro de una zona localizada, denominada dominio de movilidad localizado (*Localized Mobility Domain*, LMD), donde los *hand-overs* son más eficientes, manteniendo su dirección IPv6 y sin participar en ningún procedimiento que implique el intercambio de señalización de movilidad IP. En otras palabras, un MN puede moverse dentro del LMD sin cambiar su dirección IPv6 y sin tener que informar sobre su localización porque la red se encarga de controlar su movimiento. Para conseguir esta funcionalidad, PMIPv6 introduce nuevas entidades y reutiliza algunos de los conceptos ya introducidos en MIPv6:

Nodo Móvil (*Mobile Node*, MN): se trata de un nodo móvil IPv6 que puede comunicarse a través de interfaces de red (probablemente inalámbricas). En PMIPv6, el MN no participa en ningún intercambio de señalización de movilidad IP.

***Mobile Access Gateway* (MAG):** es una entidad de red que tiene como misión la gestión de la movilidad de los MNs que se encuentran conectados a ella. Se encarga de informar al LMA sobre la conexión de los MNs para mantenerlos localizados dentro del LMD. La MAG es normalmente el *router* de acceso de estos MNs.

***Local Mobility Anchor* (LMA):** es la versión local del *Home Agent* (HA) de MIPv6, pero con funcionalidades extendidas. El LMA es el punto de anclaje de los prefijos asignados a los MNs dentro del LMD, denominados *Home Network Prefix* (HNP). De esta forma, todos los paquetes procedentes de Internet y que van dirigidos a prefijos del dominio PMIPv6 serán encaminados hacia el LMA. Además, el LMA mantiene rutas hacia todos los MNs del LMD por medio de túneles entre el LMA y las MAGs donde los MNs se encuentran conectados.

A continuación se explica de forma resumida la operación de PMIPv6 utilizando como referencia la Figura 3.2. Cuando un MN aparece en el LMD, este se conecta a una MAG. En la

ID	Prefijo	*Proxy*-CoA
MN A	PrefijoA::/64	MAG 1
MN B	PrefijoB::/64	~~MAG1~~ MAG2

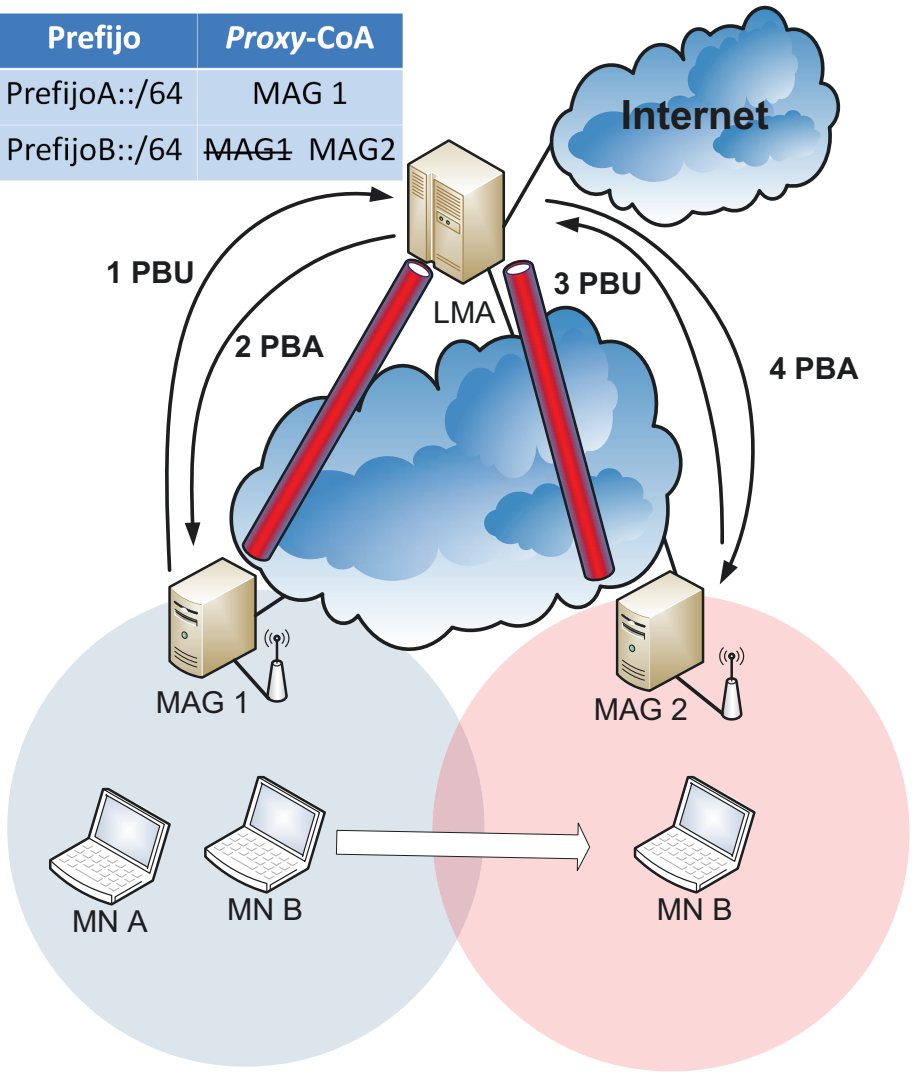


Figura 3.2: Esquema de operación de PMIPv6

figura, el MN B se conecta inicialmente a la MAG 1. La MAG 1 detectará la conexión del MN B por medio de algún evento como por ejemplo, un evento de nivel 2 o la recepción de un mensaje *Router Solicitation* (RS) enviado por el MN B. Tras comprobar que el MN B está autorizado a utilizar el servicio de movilidad, la MAG 1 envía un mensaje *Proxy Binding Update* (PBU) al LMA para informar de que el MN B está bajo su supervisión. El LMA, ante la recepción del mensaje PBU, selecciona uno de sus prefijos disponibles y se lo asigna al MN, en este ejemplo se trata del prefijo B::/64. A este prefijo se le denomina HNP y es el que se utiliza para configurar las direcciones IPv6 del enlace entre el MN y la MAG. El LMA incluye el HNP asignado en el mensaje *Proxy Binding Acknowledgment* (PBA) que envía a la MAG. De esta forma, la MAG 1 envía un mensaje *Router Advertisement* (RA) para que el MN B pueda configurar una dirección IPv6 utilizando el prefijo asignado por el LMA mediante los mecanismos de auto-configuración

de direcciones *stateless* de IPv6 [56, 57][2]). Además, durante este procedimiento se establece un túnel bidireccional IP sobre IP entre el LMA y la MAG donde el MN se encuentra conectado, utilizando la *Proxy*-CoA (*Proxy Care-of-Address*) de la MAG como punto final del túnel. Este túnel se utiliza para el encaminamiento de los paquetes de datos con origen/destino el MN B.

Mientras que el MN se mueve dentro del LMD, el MN puede desconectarse de su MAG y conectarse a una nueva MAG. Cuando el MN B se desconecta de la MAG 1 y se conecta a la MAG 2, el intercambio de mensajes de señalización PBU/PBA se repite para mantener informado al LMA de la nueva localización del MN: el LMA actualiza el túnel apuntando a la *Proxy*-CoA de la MAG 2. Además, el prefijo incluido en el mensaje PBA es el mismo que el LMA había asignado al MN B, es decir, el prefijo B::/64. De esta forma se consigue que la movilidad IP sea transparente para el MN, ya que la nueva MAG envía mensajes RA al MN anunciando el mismo prefijo que le había sido asignado por el LMA anteriormente. El MN puede mantener su dirección IPv6 mientras realiza *hand-overs* entre diferentes MAGs dentro del LMD. Así, se consigue que desde el punto de vista de los MNs, el LMD sea como un único enlace, lo que se denomina emulación de red hogar (*home network emulation*).

El encaminamiento del tráfico de datos se realiza de la siguiente manera. Los paquetes procedentes de Internet que van dirigidos a un MN del LMD, son recibidos por el LMA ya que es el punto de anclaje de los prefijos asignados a los MNs. Como en todo momento el LMA conoce a qué MAG se encuentran conectados los MNs, el LMA puede encaminar los paquetes a través del túnel bidireccional que le conecta con la MAG donde se encuentra conectado el destino. La dirección destino de la cabecera externa del túnel será la *Proxy*-CoA de la MAG donde se encuentra conectado el MN. Finalmente, la MAG elimina la cabecera externa del túnel y entrega los paquetes al MN. En el otro sentido, cuando el MN es el origen del tráfico, los paquetes se entregan a la MAG en un primer momento. Posteriormente, la MAG encamina los paquetes hacia el LMA a través del túnel bidireccional. Finalmente, el LMA elimina la cabecera externa del túnel y encamina los paquetes hacia su destino: si el destino es otro MN que se encuentra dentro del LMD, los paquetes se dirigen a la MAG donde el destino se encuentra conectado (por el túnel correspondiente). En caso contrario, los paquetes son encaminados a través de Internet hacia su destino.

Al igual que ocurre con MIPv6 [55], existen soluciones de optimización que persiguen reducir el tiempo de interrupción y la pérdida de paquetes durante el *hand-over* entre MAGs, como por ejemplo *Fast Hand-overs for Proxy Mobile IPv6* (FPMIPv6) [62]. FPMIPv6 extiende el uso de FMIPv6 [59] para el caso de PMIPv6 de manera que, estableciendo un túnel bidireccional entre la antigua MAG y la nueva MAG, se mejoran las prestaciones durante el *hand-over*.

[2]La configuración de direcciones *stateful* también está soportada, sin embargo es necesario coordinar la infraestructura DHCPv6 con la infraestructura de movilidad. Las MAGs tienen que implementar el servicio DHCPv6 *relay*.

3.2.3. Network Mobility (NEMO)

Mientras que MIPv6 [55] y PMIPv6 [61] son soluciones que gestionan la movilidad de terminales, *Network Mobility Basic Support* (NEMO) [63] surgió de la necesidad de gestionar la movilidad de redes que cambian su punto de conexión a Internet, es decir, de redes móviles. NEMO es una extensión de MIPv6 [55] en la que un *router* móvil (*Mobile Router*, MR) se encarga de gestionar la movilidad de forma transparente para los nodos que pertenecen a la red móvil (*Mobile Network Nodes*, MNNs). De esta manera, no es necesario que los MNNs implementen funcionalidades para gestionar su movilidad, ya que el MR se encarga de ello haciendo posible que puedan mantener todas sus comunicaciones activas independientemente de que la red móvil cambie su punto de conexión a Internet. A este tipo de nodos se les denomina nodos locales fijos (*Local Fixed Nodes*, LFNs). Asimismo, el estándar contempla otros tipos de MNNs como los nodos locales móviles (*Local Mobile Nodes*, LMNs). Los LMNs son nodos que tienen a la red móvil como su red hogar y pueden gestionar su movilidad a otras redes porque implementan MIP. Además, también se definen los nodos móviles visitantes (*Visiting Mobile Nodes*, VMNs) que también pueden gestionar su movilidad porque implementan MIP, pero se encuentran conectados a la red móvil de visita ya que pertenecen a otra red hogar distinta.

Como se puede ver en la Figura 3.3, cuando la red móvil no se encuentra en movimiento, esta pertenece a una red hogar (*Home Network*) donde los MNNs tienen configurada una dirección derivada de un conjunto de prefijos denominados *Mobile Network Prefixes* (MNPs). Los MNPs forman un bloque que es topológicamente válido en la red hogar. Cuando la red móvil se mueve a una red visitada, el MR obtiene una dirección IPv6 que es topológicamente válida en la red visitada, la denominada *Care of Address* (CoA). Para que la red móvil sea localizable en su nuevo punto de conexión, el MR envía un mensaje *Binding Update* (BU) al *Home Agent* (HA) situado en la red hogar. Mediante este BU, el MR informa al HA sobre la CoA que ha configurado en la red visitada. El HA confirma la recepción del BU respondiendo con un mensaje *Binding Acknowledgment* (BA) al MR. Tras este intercambio de mensajes, se establece un túnel bidireccional IP sobre IP entre el HA y la CoA del MR por el que viajarán los paquetes con origen/destino los nodos de la red móvil[3].

Como los MNPs son topológicamente válidos en la red hogar, los paquetes dirigidos a los nodos de la red móvil, como por ejemplo es el caso del MNN A en la figura, son encaminados hasta la red hogar, donde son recibidos por el HA. Como el HA conoce la localización actual de la red móvil, añade la cabecera IP externa y encamina los paquetes a través del túnel bidireccional hasta el MR (la dirección IP destino de la cabecera externa es la CoA del MR). Finalmente, el MR desencapsula los paquetes eliminando la cabecera externa del túnel y los entrega al destino. En el sentido contrario del tráfico, cuando el MNN A manda un paquete con destino al CN, este

[3]El HA puede saber los MNPs que pertenecen a la red móvil de diferentes formas: 1) por configuración estática, 2) porque el MR incluye los MNPs de la red móvil en el mensaje BU o 3) porque se ejecuta un protocolo de encaminamiento entre el MR y el HA a través del túnel bidireccional.

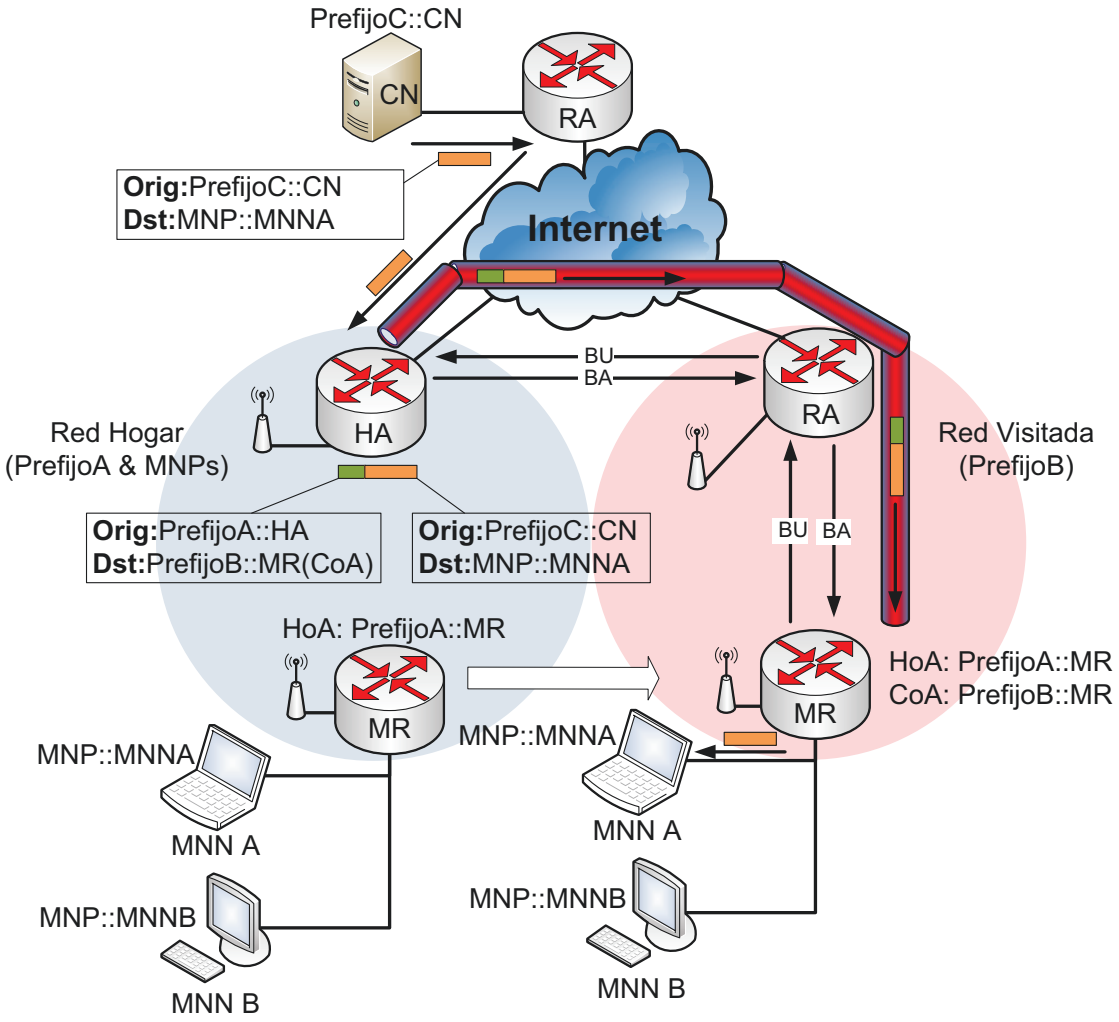


Figura 3.3: Esquema de operación de NEMO

se envía a la puerta de enlace de la red móvil, es decir al MR. De esta manera, el MR añade la cabecera externa y encamina el paquete por el túnel bidireccional hasta el HA. Finalmente, el HA elimina la cabecera externa del túnel y encamina el paquete hacia el CN a través de Internet.

Al igual que en MIPv6, uno de los inconvenientes que tiene NEMO es el encaminamiento triangular, es decir, los paquetes viajan por el HA situado en la red hogar a pesar de que el CN y la red móvil puedan estar próximos entre sí, lo que incrementa el retardo sufrido por los paquetes. Además, el túnel IP sobre IP entre el HA y el MR reduce la eficiencia al aumentar el tamaño del paquete con la cabecera IPv6 externa. Por este motivo existen soluciones de optimización de rutas que alivian estos problemas [64].

3.3. Soluciones de conexión a Internet para VANETs

El problema de la conexión a Internet de las MANETs ha sido el centro de atención de numerosos trabajos de investigación en los últimos años [65]. Sin embargo, las soluciones existentes para MANETs puede que no sean directamente aplicables en VANETs debido a sus características particulares, en especial la alta velocidad con la que se mueven sus nodos que hace que los enlaces entre ellos sean muy inestables. Por lo tanto, a continuación nos centramos en introducir brevemente algunas de las soluciones que se pueden encontrar en la literatura específicas para la conexión a Internet de redes vehiculares.

[66] presenta un protocolo de encaminamiento para VANETs que se centra en la conexión de los vehículos a Internet. Se propone un mecanismo de descubrimiento de puertas de enlace hacia Internet que reduce la sobrecarga de señalización restringiendo la cantidad de vehículos que reenvían los mensajes que envían las puertas de enlace para anunciarse. Además, los vehículos mantienen rutas hacia diferentes puertas de enlace de manera que basándose en la predicción del movimiento del resto de los vehículos, seleccionan la ruta más duradera que les conecta a Internet. Además, los vehículos se pueden anticipar al cambio de ruta hacia otra puerta de enlace cuando detectan que la ruta actual va a dejar de funcionar. En comparación con AODV+ [67] (una versión de AODV para conectar redes *ad hoc* a la infraestructura) o GPSR, se consigue aumentar la tasa de entrega de paquetes y se reduce el retardo que sufren. El artículo se centra en el protocolo de encaminamiento en la VANET, dejando algunos aspectos abiertos como la configuración/asignación de direcciones en la VANET o la gestión de movilidad global, necesarias para poder establecer comunicaciones con cualquier nodo en Internet.

En [68] se expone un estudio experimental del rendimiento de la conectividad a Internet que se puede proporcionar a los vehículos mediante puntos de acceso Wi-Fi residenciales. Los autores describen los resultados de diferentes medidas experimentales donde una flota de coches recorre zonas urbanas recopilando información sobre la conectividad entre los vehículos y los puntos de acceso Wi-Fi situados en las casas. Aunque los resultados que se presentan están limitados al caso en el que la conectividad entre los vehículos y los puntos de acceso es directa (no hay comunicación multisalto), y existen intervalos de tiempo en los que no hay conectividad con ningún punto de acceso, se muestra la viabilidad de desplegar aplicaciones para VANETs en las que los vehículos se conectan a la infraestructura, sobre todo aquellas que son tolerantes a una conectividad intermitente.

Los autores de [69] presentan una arquitectura para la conectividad de vehículos a Internet basada en tecnología WLAN. La propuesta se basa en una conexión directa entre los vehículos y los puntos de acceso WLAN situados al borde de la carretera. El problema de la conectividad intermitente y la movilidad entre puntos de acceso se gestiona a nivel de aplicación introduciendo dos entidades: el cliente *Drive-Thru* y el *proxy Drive-Thru*. Estas entidades interactúan para mantener las comunicaciones a pesar del intervalo de desconexión que se produce entre puntos

de acceso a través del protocolo *Persistent Connection Management Protocol*. La principal desventaja de la arquitectura es que está limitada a la conectividad directa entre vehículos y puntos de acceso. No se consideran comunicaciones multisalto que puedan extender la cobertura de los puntos de acceso.

En [70], los autores consideran el escenario de las comunicaciones multisalto para conectar los vehículos a la infraestructura. Los vehículos pueden mantener la conectividad a Internet mientras que realizan *hand-overs* entre diferentes puntos de acceso manteniendo sus direcciones IP. El encaminamiento de los paquetes y el soporte de movilidad se gestiona a nivel de enlace mediante la utilización de una versión mejorada del protocolo BATMAN [71]. La principal desventaja es que con la gestión de la movilidad a nivel de enlace no se soporta el *hand-over* entre redes heterogéneas. Además, se asume que los puntos de acceso operan a frecuencias distintas y que los vehículos están equipados con dos interfaces inalámbricas que operan en canales diferentes. Esto introduce cierta complejidad a la hora de asignar las frecuencias en despliegues reales. Aunque la evaluación experimental es interesante, se limita a escenarios urbanos donde los vehículos se desplazan a velocidad reducida.

El correcto funcionamiento del protocolo IP es un requisito principal para poder conectar las redes vehiculares a Internet. [72] estudia la problemática del funcionamiento del protocolo IPv6 sobre la familia de estándares IEEE 1609 que definen WAVE (*Wireless Access in Vehicular Environments*) [73]. Aunque las especificaciones señalan aspectos que son necesarios para el funcionamiento de IPv6, estos no son suficientes. Los autores realizan un análisis que expone los principales problemas que no están subsanados en la especificación y que impiden la correcta operación del protocolo IPv6 sobre redes WAVE. El problema radica en que para el funcionamiento de IPv6 se asume un modelo de enlace simétrico con un esquema de direccionamiento establecido y la disponibilidad de protocolos como *Neighbor Discovery* (ND) [56] y *Stateless Address Auto-configuration* (SLAAC) [57]. Sin embargo, el entorno cambiante de las redes vehiculares hace que los enlaces en el medio inalámbrico sean asimétricos y que el conjunto de nodos que se consideran como vecinos se modifique constantemente. Esto hace que haya que replantearse asunciones como que dos vecinos con el mismo prefijo IPv6 puedan comunicarse directamente o que protocolos como ND y SLAAC puedan enviar mensajes en *multicast* a todos los nodos del enlace. El modelo de enlace que se asume en IPv6 deja de tener sentido en redes vehiculares y es necesario realizar ciertas adaptaciones para su correcto funcionamiento [58].

[74] introduce una forma eficiente de soportar IPv6 sobre VANETs con encaminamiento geográfico basado en la arquitectura propuesta por el C2C-CC [75]. Usar los mecanismos de ND y SLAAC estándares sin ninguna modificación en VANETs puede ser comprometido porque estos protocolos asumen la existencia de un enlace en el que se pueden enviar mensajes *multicast* por debajo del nivel IP. Sin embargo, como se ha mencionado anteriormente, el concepto de enlace en una VANET tal y como se entiende a nivel IP es ambiguo. Además, la difusión de mensajes *multicast* en una VANET es costoso para el medio inalámbrico [16]. Los autores solucionan

este problema definiendo dos tipos de enlaces (enlaces C2C y enlaces virtuales punto a punto) y haciendo que el nivel IPv6 utilice información geográfica obtenida por el nivel C2C (el nivel de encaminamiento geográfico) para encaminar los paquetes. De esta forma, se consigue que los mecanismos de ND y SLAAC no dependan del envío de mensajes *multicast* a nivel de enlace. Sin embargo, la introducción de modificaciones en el protocolo IPv6 puede provocar problemas de interoperabilidad con otras implementaciones IPv6 estándar. Además, la solución no considera el soporte de movilidad IP.

[76] presenta la evaluación experimental de la solución diseñada en el proyecto *GeoNet* [77] para soportar IPv6 sobre el nivel de encaminamiento geográfico definido por el C2C-CC [75]. La evaluación experimental se centra en las comunicaciones entre vehículos (V2V) y se realiza utilizando una implementación del sistema en Linux. Se toman diferentes medidas de prestaciones tanto en laboratorios interiores como en escenarios más realistas en exteriores. Los resultados demuestran la viabilidad de soportar IPv6 sobre un protocolo de encaminamiento geográfico para comunicaciones en redes vehiculares. Un trabajo similar puede encontrarse en [78], donde se describe una implementación en Linux del protocolo de encaminamiento geográfico del C2C-CC y su integración con IPv6 siguiendo las recomendaciones del proyecto *GeoNet*.

Uno de los trabajos de investigación que trata con las soluciones de movilidad IP en redes vehiculares es [79]. Los autores analizan los requisitos de los mecanismos de movilidad IP cuando se aplican al escenario de las redes vehiculares, teniendo en cuenta sus características especiales. PMIPv6 [61] se menciona como una de las posibilidades para realizar *hand-overs* entre redes de acceso heterogéneas. Los autores se centran principalmente en la comparación de diferentes soluciones de optimización para NEMO BS [63] en escenarios vehiculares.

En [80] se analizan dos alternativas para desplegar NEMO en VANETs: MANET-*centric* y NEMO-*centric* [81]. En la solución denominada MANET-*centric*, la comunicación multisalto en la red *ad hoc* la gestiona un protocolo de encaminamiento para MANETs y NEMO opera sobre él. De esta manera, la naturaleza de la red *ad hoc* es transparente para NEMO y no es necesario introducir ninguna modificación para su funcionamiento. En cambio, en la alternativa NEMO-*centric*, la conexión de los nodos a la infraestructura se realiza a través de diferentes MRs NEMO que actúan como puertas de enlace. El protocolo de encaminamiento de la MANET se utiliza entre los nodos situados bajo el mismo MR. Los autores realizan un análisis de estas dos alternativas en el escenario de las redes vehiculares considerando aspectos como rendimiento y funcionalidad. La conclusión es que la alternativa MANET-*centric* es la más apropiada para el escenario vehicular.

En [82], se propone una solución MANET-*centric* para integrar NEMO con un protocolo de encaminamiento geográfico, tomando como referencia la arquitectura propuesta por el C2C-CC [75]. El protocolo de encaminamiento geográfico situado debajo del nivel IP en la pila de protocolos esconde la naturaleza multisalto de la VANET evitando modificaciones al nivel IPv6 estándar. De esta forma, los MRs NEMO se conectan a la infraestructura a través de una comunicación multisalto. La propuesta es validada mediante pruebas de laboratorio. A diferencia de la

propuesta descrita en el Capítulo 6, que está enfocada en la integración de un protocolo *network-based* (PMIPv6) con el protocolo de encaminamiento geográfico para la gestión de movilidad en VANETs, los autores optan por la integración de un protocolo *client-based* para la gestión de la movilidad global como es NEMO.

Por otro lado, [83] propone NEMO-*enabled* PMIPv6 (N-PMIPv6) como integración del soporte de movilidad de redes móviles en dominios PMIPv6 para escenarios vehiculares. N-PMIPv6 permite a los nodos móviles cambiar su punto de conexión entre diferentes redes móviles (diferentes MRs), entre MAGs, y entre una red móvil y una MAG con conexión directa a la infraestructura, sin la necesidad de que estos tengan que gestionar su propia movilidad ya que la red se encarga de ello en su lugar. Esto se consigue gracias a que todos los prefijos de los nodos que pertenecen al dominio PMIPv6 son asignados por el LMA, incluyendo los MNPs de los nodos móviles conectados a las redes móviles. Para ello, se extienden las funcionalidades de los MRs para que actúen como MAGs (que se denominan *mobile* MAGs). Las *mobile* MAGs se encargan de comunicar al LMA la conexión de nuevos nodos móviles a su red móvil y obtener los prefijos que han sido asignados por el LMA. Sin embargo, la solución se centra en escenarios en los que existe una comunicación directa entre nodos móviles/MRs y las MAGs, sin la posibilidad de disponer de comunicaciones multisalto a través de diferentes vehículos en la VANET.

[84] y [85] introducen P-NEMO, una combinación de NEMO [63] con PMIPv6 [61] que permite a una red móvil cambiar de punto de conexión a Internet dentro de un dominio PMIPv6 sin que el MR tenga que intercambiar señalización de movilidad, ya que las entidades presentes en PMIPv6 han sido extendidas para soportar NEMO. En concreto, el LMA se encarga de asignar tanto los HNPs (*Home Network Prefixes*) para los MRs como los MNPs (*Mobile Network Prefixes*) de los MNNs de cada MR. Las MAGs comunican siempre estos mismos prefijos al MR incluyéndolos en los mensajes RA aunque el MR cambie su punto de conexión dentro del dominio PMIPv6. A su vez, [85] presenta FP-NEMO, una extensión de este mecanismo siguiendo la misma idea que FPMIPv6 [62]. Ante eventos de nivel de enlace, se detecta que una red móvil se dispone a realizar un *hand-over* y se realiza una transferencia de contexto entre la antigua MAG y la nueva MAG para preparar el *hand-over* antes de que se realice. De esta manera se reduce el retardo del *hand-over* y la pérdida de paquetes durante el mismo. Mediante un modelo analítico, se demuestra que se mejora la eficiencia porque los MRs no tienen que enviar señalización de movilidad cada vez que realizan un *hand-over* y no es necesario realizar detección de direcciones duplicadas dentro del dominio PMIPv6. Aunque la solución de movilidad propuesta está orientada a redes vehiculares, no se tiene en cuenta la posibilidad de disponer de protocolos de encaminamiento entre vehículos en la VANET. Además, se asume que los vehículos disponen de una conexión directa con las MAGs y no se considera la posibilidad de encaminamiento multisalto en la VANET que extienda la cobertura de los puntos de acceso.

Basándose en las arquitecturas para sistemas de transporte inteligentes (ITS) de los organismos ISO (*International Organization for Standardization*), CALM (*Communications Access for*

Land Mobiles) [86] y ETSI [87], en [88] se presenta una pila de protocolos que proporciona a los vehículos conectividad IPv6 y gestión de movilidad utilizando NEMO. Para conseguir la conectividad continua de los vehículos a la infraestructura, se soporta la utilización de diferentes tecnologías de acceso de manera simultánea (*multihoming*). Para ello, se aplican las extensiones de *Multiple Care of Addresses Registration* (MCoA) [89] que permite a los MRs disponer de diferentes túneles simultáneos con el HA a través de diferentes interfaces de acceso. Además, con la intención de optimizar el *hand-over* entre RSUs, se define la manera de integrar las funcionalidades necesarias del estándar IEEE 802.21 [90]. La solución se valida mediante diversas pruebas en un prototipo real. Sin embargo, la posibilidad de establecer conexiones multisalto entre los vehículos y las RSUs no se contempla.

En esta misma línea, [91] presenta la plataforma de comunicaciones para sistemas de transporte inteligentes que se ha desarrollado dentro del proyecto *Walkie-Talkie* [92] siguiendo las directrices de los estándares de la ISO [86] y del ETSI [87]. Dentro de esta plataforma se consideran tanto comunicaciones V2V como comunicaciones V2I. Para las comunicaciones V2I se contempla la posibilidad de utilizar diferentes redes de acceso gestionando la movilidad con NEMO y MCoA [89].

El trabajo realizado en [93] ha generado contribuciones interesantes en el ámbito de la conexión de redes vehiculares a Internet. En [94] se presenta una solución de gestión de movilidad global combinando *Host Identity Protocol* (HIP) [52] y PMIPv6 para proporcionar conectividad a Internet en escenarios vehiculares urbanos. La solución permite a nodos que no tienen soporte de movilidad y a nodos que implementan HIP realizar *hand-overs* entre RSUs que pertenecen al mismo dominio PMIPv6 (*hand-over* intra-dominio) o a distinto dominio PMIPv6 (*hand-over* inter-dominio). Sin embargo, es necesario que los CNs en Internet soporten el protocolo HIP o que se sitúen detrás de un *proxy* HIP.

En [95] los autores proponen un mecanismo de encaminamiento para *streaming* de vídeo en VANETs para mejorar la calidad de vídeo percibida. Para el soporte de la movilidad, el protocolo de encaminamiento se integra con una adaptación de PMIPv6 al entorno multisalto de las VANETs. Asimismo, se propone un mecanismo de predicción de *hand-over*. El método de adaptación de PMIPv6 al entorno multisalto es similar a la solución propuesta en el Capítulo 6 para integrar PMIPv6 con la arquitectura del ITS y el protocolo de encaminamiento estandarizados por el ETSI [36, 87]. Sin embargo la arquitectura de la propuesta es diferente, los autores definen una arquitectura en la que los *routers* de acceso desempeñan el papel de MAG y dan servicio a diferentes RSUs. Además, se asume la utilización de los mecanismos de ND y *Neighbor Unreachability Detection* [56], lo que es muy costoso para el medio inalámbrico ya que se produce una gran sobrecarga de señalización al distribuir los mensajes *multicast* en la VANET [16]. En la integración propuesta en el Capítulo 6, las propias RSUs son las que actúan como *routers* de acceso y MAG a la vez. Además, se evita el uso de los mecanismos de ND completamente, ya que de acuerdo con las especificaciones del ETSI, la resolución de direcciones se puede realizar de for-

ma directa y unívoca [58]. Por otro lado, en nuestro trabajo, además de la integración de PMIPv6 con el protocolo de *GeoNetworking* del ETSI [36], también se analizan en profundidad diferentes mecanismos para mejorar su rendimiento cuando se proporciona conectividad a Internet a los vehículos de la VANET.

En [96], se propone MA-PMIP (*Multi-hop Authenticated Proxy Mobile IP*) para la provisión de servicios IP en redes vehiculares asimétricas, donde los autores desarrollan la solución para adaptar PMIP al entorno multisalto presentada en [95] y unifican los roles de *router* de acceso y MAG en las RSUs. Como aspecto positivo, los autores contemplan la autenticación de la señalización de movilidad para evitar posibles ataques. Sin embargo, esto además de introducir complejidad en los nodos, impone la restricción de que cuando un vehículo aparece en la VANET, no puede configurar una dirección IP hasta que no se encuentre conectado directamente a una RSU (un salto). Además, el mecanismo de autenticación limita la comunicación de señalización de movilidad para el *hand-over* a únicamente dos saltos. Por otro lado, para la detección de enlaces asimétricos en el medio inalámbrico, se asume el uso de los mecanismos de *Neighbor Discovery* y *Neighbor Unreachability Detection* [56] que como se ha comentado anteriormente, produce una gran sobrecarga de señalización al distribuir los mensajes *multicast* en la VANET [16]. Al contrario que en el Capítulo 6 donde se utiliza el protocolo de GN del ETSI, los autores no se ajustan a la utilización de ningún protocolo estándar para el encaminamiento de los paquetes en la VANET. Asimismo, los autores proponen un mecanismo de predicción de *hand-over* que utiliza un servidor de localización central (se trata de un punto único de fallo) para obtener la posición geográfica de los vehículos y así estimar el instante en el que se establecen los túneles entre MAGs de FPMIPv6 [62] para reducir la pérdida de paquetes durante el *hand-over*.

En [97], los autores presentan un estudio de las limitaciones de los estándares 802.11p [39] y WAVE (*Wireless Access in Vehicular Environments*) [73] para conectar los vehículos a la infraestructura y proporcionar servicios IP. Para combatir estas limitaciones proponen VIP-WAVE (*Vehicular* IP *in* WAVE) que permite la configuración de direcciones IP para servicios extendidos (comprenden el cambio de los vehículos entre RSUs) y no extendidos (limitados a la zona de servicio de una RSU). La gestión de la movilidad se lleva a cabo mediante la utilización de PMIPv6 sobre WAVE, donde las RSUs actúan como MAGs. Aunque se permite la conexión multisalto con la RSU, VIP-WAVE únicamente permite esta comunicación a un máximo de dos saltos, lo que supone una limitación.

Capítulo 4

El sistema de transporte inteligente estandarizado por el ETSI

En este capítulo se describe la arquitectura del sistema de transporte inteligente que ha sido estandarizado recientemente por el ETSI (*European Telecommunications Standards Institute*) y el protocolo de *GeoNetworking* que se utiliza para las comunicaciones en la VANET.

4.1. Introducción

La importancia de las redes vehiculares y el impacto que pueden tener en la sociedad, sobre todo con su aplicación en la mejora de la seguridad vial, han sido reconocidos por diferentes organismos de estandarización que en los últimos años han estado trabajando en la definición de la arquitectura y los protocolos de comunicación para un sistema de transporte inteligente (ITS).

El IEEE 1609 *Working Group* [98] ha estado trabajando en la familia de protocolos IEEE 1609 para *Wireless Access in Vehicular Environments* (WAVE) [73]. Este conjunto de estándares define la arquitectura, las interfaces y los protocolos para comunicaciones inalámbricas entre vehículos (V2V), y entre vehículos y la infraestructura (V2I). En este entorno y utilizando este tipo de comunicaciones, se diferencia entre aplicaciones orientadas a la seguridad vial, las destinadas a mejorar la eficiencia del tráfico y aplicaciones de información/entretenimiento para los ocupantes de los vehículos. Siguiendo un modelo divido en capas, los niveles físico y de enlace se corresponden con el estándar IEEE 802.11p [39] y el estándar IEEE 1609.4 [99], que se centra en la coordinación entre los diferentes canales servicio (SCH) y el canal de control (CCH), y que utiliza técnicas de acceso al medio del estándar 802.11e *Enhanced Distributed Channel Access* (EDCA) [100] que permiten establecer prioridades de acceso al medio para diferentes tipos de tráfico. El nivel de red se corresponde con el estándar IEEE 1609.3 [101], sobre el que se soportan dos tipos de pilas de protocolos: 1) Una pila para comunicaciones basadas en TCP/IPv6

que no están vinculadas a aplicaciones de seguridad vial, cuyos paquetes se envían utilizando los canales SCH y donde la movilidad se puede gestionar con MIPv6 y NEMO. 2) Una segunda pila para comunicaciones no basadas en IP y orientadas a la seguridad vial que utiliza WSMP (*WAVE Short Message Protocol*), un protocolo especialmente diseñado para comunicaciones en redes vehiculares. Los mensajes WSMP se pueden enviar utilizando los canales SCH o CCH. Respecto a los mecanismos de seguridad, estos se especifican en el estándar IEEE 1609.2 [102].

Respecto al estándar IEEE 802.11p [39], define diferentes modificaciones al estándar 802.11 para proporcionar mejores prestaciones en entornos de redes vehiculares. Trabajando en la banda de 5,9 GHz con canales de 10 MHz, se especifican las características del enlace para las comunicaciones V2V y V2I. El homólogo europeo del estándar IEEE 802.11p es el ITS-G5 [103], estandarizado por el ETSI y que basándose en el estándar IEEE 802.11p, especifica el nivel físico y la capa de acceso al medio para su sistema de transporte inteligente.

Por su parte, la ISO [104], a través del grupo de trabajo ISO TC 204 [105], ha definido un conjunto de estándares que especifican los diferentes modos de comunicación en un sistema de transporte inteligente que ha sido denominado como CALM (*Communications Access for Land Mobiles*) [86]. CALM trata de abstraer a las aplicaciones de la infraestructura de comunicaciones de manera que proporciona servicios de comunicaciones entre vehículos (V2V), entre los vehículos y la infraestructura (V2I), y entre nodos de la infraestructura (I2I) a través de la VANET. Se especifican diferentes arquitecturas y combinaciones de protocolos de manera que se puede seleccionar una composición adecuada en función de las necesidades de las aplicaciones. Mientras que WAVE se centra en la utilización de IEEE 802.11p como tecnología de acceso, CALM contempla un escenario heterogéneo en el que se considera el uso de diferentes tecnologías de acceso con la idea es obtener la continuidad de las comunicaciones utilizando las interfaces de acceso más adecuadas en cada momento. Por otro lado, CALM incluye a nivel de red tanto una solución con IPv6 para aplicaciones no vinculadas a la seguridad vial, como un protocolo de red especialmente diseñado para su funcionamiento en redes vehiculares, CALM FAST. El uso de CALM FAST está destinado a aquellas aplicaciones relacionadas con la seguridad vial que requieren mayor fiabilidad y bajo retardo [106].

El comité técnico del sistema de transporte inteligente del ETSI, *European Telecommunications Standards Institute Technical Committee Intelligent Transport System* (ETSI TC ITS) [107] también ha trabajado en la definición la arquitectura y los protocolos de comunicaciones para un sistema de transporte inteligente estandarizado. En esta estandarización se han considerado las aportaciones provenientes de importantes fabricantes de automóviles y de la industria del automóvil en general, como por ejemplo, el trabajo realizado por el *Car 2 Car Communication Consortium* (C2C-CC) [75]. El C2C-CC es una asociación formada por los principales fabricantes de automóviles, empresas de dispositivos electrónicos y centros de investigación que tienen como objetivo la estandarización de las interfaces y protocolos de un sistema de comunicaciones entre vehículos. Por otro lado, también se han tenido en cuenta los trabajos realizados en importantes

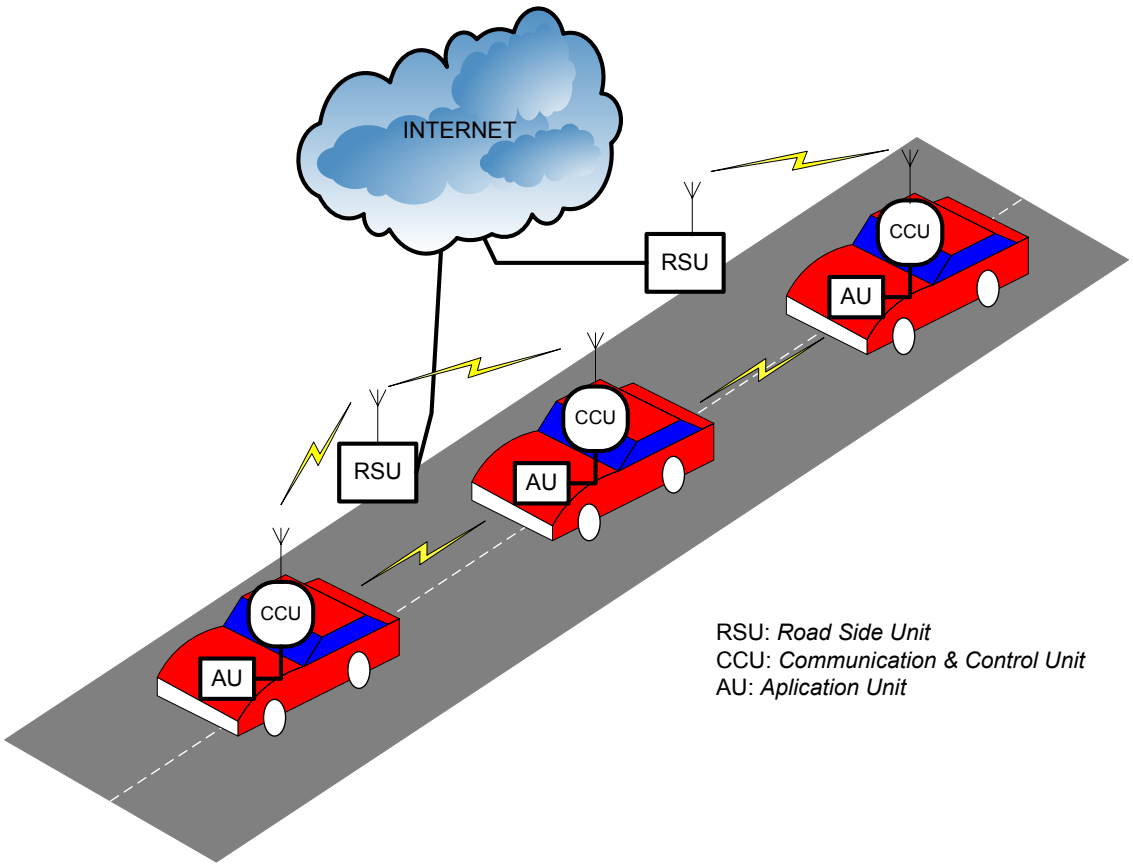


Figura 4.1: La arquitectura del sistema de transporte inteligente definida por el ETSI

proyectos de investigación sobre redes vehiculares, como el proyecto *GeoNet* [77].

Una característica común que se pone de manifiesto en las especificaciones de estos organismos de estandarización es que se presta mayor atención a los requisitos necesarios para la provisión de aplicaciones vinculadas a la mejora de la seguridad vial, dejando en un segundo plano los requisitos relacionados con las aplicaciones de mejora de la eficiencia del tráfico o de información/entretenimiento. Aunque se consideran casos de uso en los que los vehículos se conectan a Internet, el foco de atención está centrado en casos de uso para mejorar la seguridad vial en los que los vehículos distribuyen mensajes de emergencia con el objetivo de evitar accidentes de tráfico.

A continuación se entra más en detalle en la arquitectura del sistema de transporte inteligente y el protocolo de comunicación para la red vehicular que han sido estandarizados por el ETSI.

4.2. Arquitectura del sistema de transporte inteligente

La arquitectura del sistema de transporte inteligente que ha estandarizado el ETSI [87] se muestra en la Figura 4.1. En primer lugar tenemos los vehículos (*vehicle ITS stations*), que están equipados con una *Communication & Control Unit* (CCU), que implementa la pila de protocolos de comunicaciones definida por el ETSI. Las CCUs pueden verse como *routers* móviles con al menos dos interfaces de red. Una interfaz para la red interna del vehículo que sirve para comunicarse con las unidades de aplicación (*Aplication Units*, AUs). La otra interfaz, inalámbrica de corto alcance, se utiliza para las comunicaciones con otras estaciones de la VANET. Una AU es un dispositivo (como por ejemplo un ordenador situado en el salpicadero o el teléfono móvil de un pasajero) con una pila de protocolos IPv6 estándar que ejecuta una serie de aplicaciones y que se conecta a la CCU para beneficiarse de sus capacidades de comunicación. Las AUs se pueden conectar a la interfaz interna de la CCU por medio de una tecnología cableada o cualquier tecnología de comunicaciones inalámbrica (*Bluetooth*, WUSB, UWB...). De esta forma, la CCU actúa como puerta de enlace (opcionalmente puede incluir extensiones para soportar NEMO [63]) para las comunicaciones de las AUs.

Por otro lado, la red *ad hoc* del ITS está formada por las *roadside ITS stations* o *Road Side Units* (RSUs) que junto con las CCUs de los vehículos forman la VANET. Las RSUs son estaciones fijas situadas al borde de la carretera que también implementan la pila de protocolos de comunicaciones definida por el ETSI. Como las RSUs están conectadas a la red fija, además de aumentar la conectividad de la red vehicular, actúan como puertas de enlace ofreciendo conexión a Internet a los vehículos de la VANET.

Respecto a la tecnología de acceso utilizada para las comunicaciones entre las diferentes entidades del sistema, esta no se encuentra restringida al uso de una tecnología de nivel de enlace concreta. Se contempla el uso de diferentes tecnologías de acceso inalámbricas como la familia IEEE 802.11, el mencionado ITS-G5 (basado en 802.11p) o tecnologías de comunicaciones celulares como GPRS, UMTS o WiMAX.

El ETSI también ha estandarizado el protocolo de *GeoNetworking* (GN) [36] para el encaminamiento de paquetes en la VANET de su sistema de transporte inteligente. El protocolo de GN, que se sitúa entre el nivel de enlace y el nivel de red en la pila de protocolos (ver Figura 4.2), adopta el paradigma del encaminamiento geográfico. Los paquetes se encaminan por la VANET en función de la posición geográfica de los nodos y la posición del destino de los paquetes. Dada la popularidad de los dispositivos GPS, se asume que todos los nodos pueden obtener su posición geográfica y que además aprenden la posición de sus vecinos directos (aquellos que están en contacto directo con el nodo dentro de su radio de cobertura). De esta forma, los paquetes son reenviados por diferentes nodos intermedios desde el origen hasta el destino estableciendo una comunicación multisalto. En el protocolo de GN existen dos tipos de envío de paquetes principales: *geo-unicast* y *geo-broadcast*. Como se describió anteriormente cuando se introdujeron

los protocolos basados en encaminamiento geográfico, con un envío *geo-unicast* el paquete se reenvía salto a salto entre nodos hacia la posición que ocupa el destino hasta que se entrega a un nodo específico. Con un envío *geo-broadcast*, el paquete primero se dirige a una zona geográfica objetivo y posteriormente se entrega a todos los nodos que se encuentran dentro del área destino. El protocolo de GN se describe con mayor detalle más adelante.

Por otro lado, también se ha estandarizado la conexión a Internet de la red *ad hoc* del ITS, es decir, la VANET [58]. Para que los vehículos puedan comunicarse con otros nodos de Internet, se ha definido una capa de adaptación entre el nivel IPv6 y el protocolo de GN denominada *GeoNetworking to IPv6 Adaptation Sub-Layer* (GN6ASL). Esta capa implementa una serie de mecanismos que permiten la transmisión de paquetes IPv6 sobre el protocolo de GN sin que sea necesario realizar ningún cambio al protocolo IPv6 estándar. La capa GN6ASL se encarga de acoplar los niveles IPv6 y GN de manera que, desde el punto de vista de IPv6, el protocolo de GN tiene el papel de un nivel sub-IP: el protocolo de GN recibe los datagramas IPv6, los encapsula añadiendo la cabecera del nivel de GN y se encarga de encaminarlos por la VANET hasta el siguiente salto IPv6. De esta manera, dos vecinos IPv6 pueden estar separados por más de un salto de nivel de GN, pero para IPv6 esto es transparente y es como si estuvieran conectados al mismo enlace. En la Figura 4.2, el vehículo A y la RSU 1 son vecinos a nivel IPv6, pero en realidad es necesario que el nivel de GN del vehículo B retransmita los paquetes y establezca una cadena multisalto entre ellos.

Respecto a la resolución de direcciones, se realiza de forma directa. Del identificador de interfaz de una dirección IPv6 *unicast* (los últimos 64 bits de la dirección IPv6) se puede derivar de forma unívoca el identificador del nivel de GN correspondiente. Por lo tanto, se puede obtener el identificador de nivel de GN del destino a partir de la dirección IPv6 destino sin necesidad de utilizar el procedimiento ND [56]. De esta manera se evita la sobrecarga que generaría en la VANET la distribución de los paquetes *Neighbor Solicitation* y *Neighbor Advertisement* (el paquete *Neighbor Solicitation* se distribuye en *broadcast* a todos los nodos del enlace)[1] [16].

La especificación ha adoptado el mecanismo *Geographically Scoped stateless Address Configuration* (GeoSAC) [108] para la configuración automática de direcciones IPv6 y definir el concepto de enlace geográfico virtual. GeoSAC adapta los mecanismos de auto-configuración de direcciones de IPv6 SLAAC [56] [57] al direccionamiento y encaminamiento geográfico mediante la definición de un enlace geográfico virtual.

Un enlace geográfico virtual se define como la zona geográfica delimitada donde el protocolo de GN (extendiendo múltiples enlaces físicos entre nodos) entrega los paquetes *multicast* de ámbito *link-local*[2] a todos los nodos que se encuentran situados dentro del área por medio de un

[1] Aunque el estándar especifica que las direcciones IPv6 de la estaciones deben tener identificadores de interfaz de los que se pueda derivar el identificador del nivel de GN, también se puede utilizar la resolución de direcciones mediante el mecanismo de ND cuando esto no sea posible. A pesar de ello, el estándar aconseja evitarlo, y en el caso en el que sea inevitable, adaptar las constantes del protocolo para evitar un consumo excesivo de recursos en el medio inalámbrico.

[2] Por ejemplo, los paquetes con destino a la dirección *all-nodes* (FF02::1)

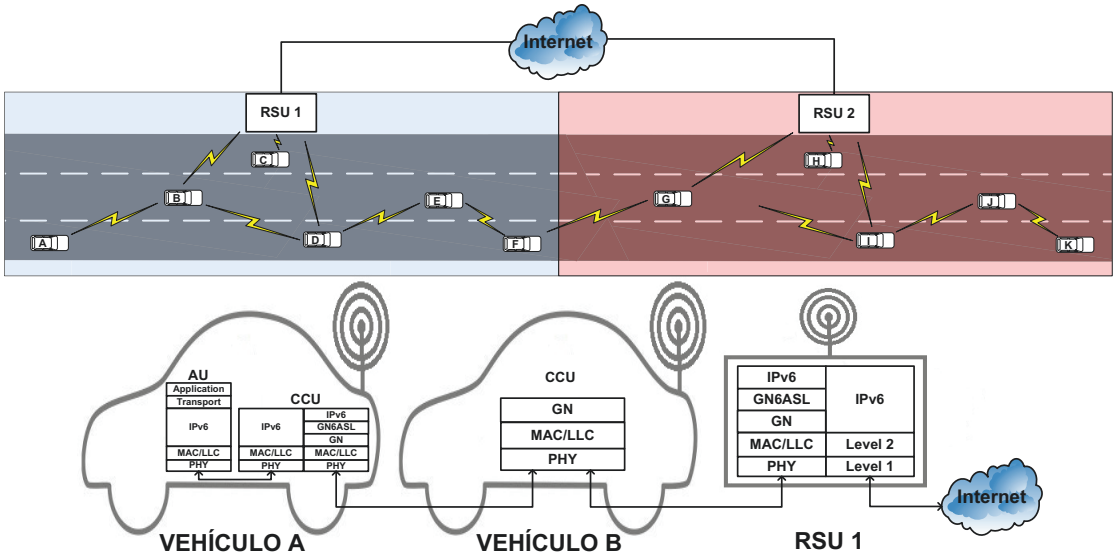


Figura 4.2: Enlaces geográficos virtuales y pila de protocolos del sistema de transporte inteligente del ETSI

envío *geo-broadcast*. De esta manera, todos los nodos que se encuentran situados dentro del área de un enlace geográfico virtual pertenecen a la misma sub-red IPv6.

De esta forma, como puede observarse en la Figura 4.2, se definen diferentes enlaces geográficos virtuales como zonas geográficas que no se solapan y que cuentan con una RSU que actúa como *router* de acceso para proporcionar conectividad a Internet a los vehículos situados dentro de cada área. Cada RSU se encarga de un área de influencia específica, es decir, de un enlace geográfico virtual. Al comportarse como un *router* de acceso, la RSU envía periódicamente paquetes *Router Advertisement* (RA) que se entregan a todos los nodos situados dentro de su área geográfica por medio de una entrega *geo-broadcast*. De esta manera, los vehículos reciben el RA y pueden configurar una dirección IPv6 global siguiendo los mecanismos de auto-configuración de direcciones de IPv6 SLAAC [56] [57].

Dado que los vehículos se encuentran en movimiento, estos cambian entre diferentes enlaces geográficos virtuales (diferentes áreas geográficas). Las CCUs de los vehículos pueden detectar el cambio de área geográfica porque los paquetes RA difundidos por las RSUs incluyen en la cabecera del protocolo de GN el ámbito del enlace geográfico virtual y la posición de la RSU que proporciona conectividad a Internet. Se han propuesto algunos mecanismos de optimización para la configuración de direcciones como [109], que permite a los vehículos conocer con anterioridad el cambio de área geográfica y reducir el tiempo que los vehículos tardan en configurar una nueva dirección IPv6 global una vez que realizan el cambio de región geográfica.

Debido a que las CCUs de los vehículos cambian de *router* de acceso (RSU) y configuran una nueva dirección IPv6 global con el cambio entre regiones geográficas, es necesario un protocolo para la gestión de la movilidad que permita mantener las comunicaciones activas a pesar del

cambio de dirección IPv6. La especificación propone *Network Mobility Basic Support* (NEMO BS) [63] como protocolo para la gestión de la movilidad entre diferentes enlaces geográficos virtuales, aunque se podrían utilizar otras soluciones de movilidad como MIPv6 [55] o PMIPv6 [61].

La Figura 4.2 sirve para explicar el encaminamiento de los paquetes en la VANET. Si una AU del vehículo A envía un paquete a un nodo en Internet, la CCU del vehículo debe enviar el paquete al *router* de acceso de su enlace geográfico virtual, es decir, a la RSU 1, que es la encargada de la zona geográfica donde está situado el vehículo. Como el vehículo A y la RSU 1 están en el mismo enlace geográfico virtual, la RSU 1 es el siguiente salto IPv6 del vehículo A, aunque pueden estar separados más de un salto a nivel del protocolo de GN. De esta forma, el paquete es retransmitido por el nivel de GN del vehículo B formando un camino multisalto entre el vehículo A y la RSU 1. Cuando la RSU 1 recibe el paquete, lo encamina hacia su destino en Internet.

En el caso en el que el destino del paquete es otro vehículo dentro de la misma región geográfica que el vehículo A, por ejemplo el vehículo F, el protocolo de GN encamina el paquete directamente hacia el vehículo destino sin pasar por el *router* de acceso (la RSU 1) ya que los vehículos A y F se encuentran en la misma sub-red IPv6 (mismo enlace geográfico virtual).

La resolución de direcciones se realiza de siguiente forma: cuando un vehículo desea mandar un paquete IPv6 a un destino con una dirección IPv6 de su mismo prefijo, se obtiene el identificador de nivel GN del destino a partir del identificador de interfaz de la dirección IPv6 destino, y se le hace llegar directamente el paquete sin necesidad de pasar por la RSU. Si la dirección IPv6 del destino tiene un prefijo distinto al del nodo origen, el paquete se envía a la RSU (*router* de acceso) para que se encargue de encaminar el paquete apropiadamente.

Cuando los paquetes proceden de Internet dirigidos al vehículo A, estos son recibidos en primer lugar por la RSU 1 y se procede de la misma manera: la RSU 1 manda los paquetes al vehículo B, que finalmente se los entrega al destino, el vehículo A.

4.3. Protocolo de *GeoNetworking* (GN)

El protocolo de *GeoNetworking* (GN) [36] estandarizado por el ETSI es un protocolo basado en encaminamiento geográfico que encamina los paquetes por la VANET en función de la posición geográfica que ocupan los nodos de la red. Se asume que los nodos pueden obtener su posición geográfica mediante algún mecanismo de localización, como por ejemplo, un GPS. Esto no supone una restricción importante dada la gran popularidad de los sistemas GPS hoy en día.

Por otro lado, todos los nodos mantienen una Tabla de Localización (TL) donde se almacena información sobre otras estaciones ITS de la VANET, incluyendo la posición de los vecinos directos, es decir, aquellos nodos que se encuentran a un salto. La posición de los vecinos se obtiene por medio de la utilización de un algoritmo de balizas o *beaconing* que funciona de la siguiente manera. Todos los nodos emiten periódicamente en *broadcast* un mensaje *beacon* anunciando su

dirección de nivel de GN y su posición geográfica, velocidad, dirección, altitud, tipo de estación ITS (vehículo o RSU), etc. que es recibido por todos los vecinos directos. Así, los nodos pueden completar su TL con la información extraída de los mensajes *beacon* recibidos. Como los mensajes *beacon* se envían periódicamente, los nodos pueden mantener su TL actualizada con la posición geográfica actual de otros nodos vecinos. Sin embargo, el algoritmo de *beaconing* genera sobrecarga de señalización en la red. Existe un compromiso entre la sobrecarga generada por el intercambio de mensajes *beacon* entre nodos y la frescura de la información almacenada en la TL, que es necesaria para una buena operación del protocolo de GN. Cuanto mayor sea la frecuencia con la que se envían los mensajes *beacon*, más precisa será la información geográfica de la que disponga el protocolo de GN, pero mayor será la sobrecarga de señalización en la red. Con el objetivo de reducir la sobrecarga de señalización generada por el algoritmo de *beaconing*, el estándar establece que se reinicialice el temporizador de *beaconing* (el temporizador que regula el intervalo entre envíos de mensajes *beacon*) cada vez que se envía cualquier otro paquete del protocolo de GN. Esto se debe a que se realiza *beacon piggybacking* cuando se envían otros paquetes. La idea es que se puede omitir el envío de un mensaje *beacon* si se envía otro paquete del protocolo de GN porque la información que va incluida en un mensaje *beacon* también se incluye en la cabecera del protocolo de GN de cualquier otro paquete[3]. Por otro lado, la TL también incluye la posición geográfica de nodos que no son vecinos directos y que por lo tanto se encuentran a más de un salto de distancia. La posición geográfica de estos nodos se descubre mediante un Servicio de Localización (SL) que se describe más adelante.

Debido a la alta movilidad de los vehículos en la VANET, la información de la TL se vuelve obsoleta rápidamente. Por ello, cada entrada en la TL tiene un tiempo de caducidad. Cuando el tiempo de caducidad de una entrada en la TL expira porque no se han recibido mensajes que la actualicen, se considera que la información no es válida y se borra la entrada de la tabla. De esta manera el tiempo de caducidad de las entradas de la TL influye en la operación del protocolo de GN, ya que regula la frescura de la información almacenada en la TL. Si el tiempo de caducidad es muy alto, el protocolo de GN puede considerar como vecinos nodos que ya no son alcanzables porque debido a su movimiento han salido fuera del radio de cobertura. Sin embargo, cuanto más bajo sea el tiempo de caducidad de las entradas en la TL, mayor tiene que ser la frecuencia de envío de *beacons*, con lo que el tráfico de señalación en la red aumenta. Además, si el tiempo de caducidad es demasiado corto, podría darse el caso de que la TL no se actualizara apropiadamente por la pérdida de paquetes *beacon* por colisiones en el canal inalámbrico.

El protocolo de GN define diferentes tipos de entrega de paquetes:

- *Geo-unicast*: el destino de un paquete *geo-unicast* es un nodo situado en una posición geográfica determinada. La posición del destino se incluye en la cabecera del protocolo de GN del paquete y es utilizada para guiar al paquete hacia el destino usando uno de

[3]Nótese que en el borrador de la última versión del estándar de GN [110] existen modificaciones en la cabecera del protocolo de GN que hacen que no se incluya la información del paquete *beacon* en todos los paquetes.

los algoritmos de encaminamiento definidos en la especificación: el algoritmo de *greedy forwarding* y el algoritmo *Contention-Based Forwarding* (CBF).

Como se describió anteriormente, *greedy forwarding* selecciona como siguiente salto de un paquete el vecino de la TL que se encuentra más cerca de las coordenadas del destino. De esta forma, el paquete se va reenviando de vecino en vecino por la VANET hasta que se entrega al destino. Con CBF, el receptor del paquete es el que decide si convertirse en el siguiente salto y reenviarlo (al contrario que con *greedy forwarding*, donde el emisor del paquete decide cual es el siguiente salto que debe reenviarlo). Con CBF, el emisor del paquete lo envía en *broadcast* a todos sus vecinos. Ante la recepción de un paquete, los nodos establecen un temporizador para enviar el paquete en función de su distancia al destino, cuya posición se encuentra incluida en la cabecera del paquete. El vecino que se encuentre más cerca del destino será el que establezca el temporizador más bajo y por lo tanto, el que reenvíe el paquete (anulando el temporizador del resto de vecinos). La operación se repite hasta que el paquete es recibido por el destino. De aquí se deduce que el algoritmo CBF no precisa de una TL con información de posición geográfica de los vecinos para su operación.

- *Geo-broadcast*: en una entrega *geo-broadcast*, el paquete va dirigido a todos los nodos que se encuentran situados dentro de una región geográfica objetivo. Los parámetros que describen el área geográfica objetivo se incluyen en la cabecera del protocolo de GN del paquete. En un primer momento, el paquete *geo-broadcast* se encamina hacia la zona geográfica destino usando el algoritmo de *greedy forwarding* tal y como si se tratara de un paquete *geo-unicast*. Una vez que el paquete llega a la región destino, se distribuye a todos los nodos dentro de la zona mediante inundación simple.

- *Geo-anycast*: la entrega *geo-anycast* es similar a la entrega *geo-broadcast*, pero con la diferencia de que el paquete solo se entrega a un único nodo entre los que se encuentran situados dentro de la región geográfica objetivo.

- *Broadcast* limitado topológicamente (*topologically scoped broadcast*): en este tipo de entrega, el paquete se hace llegar todos los nodos que se encuentran a un cierto número máximo de saltos del nodo emisor del paquete. El paquete se va retransmitiendo en *broadcast* a todos los vecinos hasta que se alcanza un número máximo de saltos determinado por el origen.

- *Broadcast* a un salto (*single hop broadcast*): el paquete únicamente se entrega a los nodos que se encuentran a un salto, es decir, aquellos nodos que están dentro del radio de cobertura del nodo emisor. Es como una entrega *broadcast* limitado topológicamente (*topologically scoped broadcast*), pero limitando el número de saltos máximo a uno.

En el apéndice A se puede encontrar el formato y los datos incluidos en la cabecera de los diferentes tipos de paquete del protocolo de GN.

En los trabajos realizados en esta Tesis Doctoral se hace uso de las entregas *geo-unicast* y *geo-broadcast*, ya que son los tipos de entrega más comunes. Respecto al envío de paquetes *geo-unicast*, se ha considerado la utilización del algoritmo de *greedy forwarding*, dejando el estudio del algoritmo CBF como trabajo futuro.

Para el descubrimiento de la posición geográfica de otras estaciones ITS que no son vecinos directos, es decir, que se encuentran a más de un salto de distancia, se utiliza el Servicio de Localización (SL). Por ejemplo, cuando se envía un paquete *geo-unicast* a un destino que no está en la TL, se utiliza el SL para averiguar la posición del destino y poderla incluir en la cabecera del paquete. El SL sigue el siguiente modo de operación: el nodo que necesita averiguar la posición geográfica de otro nodo destino envía en *broadcast* un paquete *Location Service Request* (*LS Request*) indicando la dirección de GN del nodo objetivo (aquel del que se desea obtener su posición). El paquete *LS Request* se retransmite en *broadcast* por los nodos intermedios hasta que es recibido por el nodo objetivo. Cuando esto ocurre, el nodo objetivo contesta con un mensaje *Location Service Reply* (*LS Reply*) en el que incluye su posición geográfica. El paquete *LS Reply* se encamina hasta el nodo que envió el mensaje *LS Request* tal y como si fuera un paquete *geo-unicast*. Nótese que esto es posible porque el mensaje *LS Request* incluye la posición geográfica del nodo origen. Cuando el nodo origen recibe el paquete *LS Reply* crea una entrada nueva en la TL para ese destino, que será válida hasta que su tiempo de caducidad expire. Si el nodo origen no recibe un paquete *LS Reply* de respuesta, continuará enviando peticiones *LS Request* periódicamente hasta que se reciba un paquete *LS Reply* o se alcance el número máximo de reintentos establecido.

El protocolo de GN define múltiples *buffers* para el almacenamiento de paquetes: un *buffer* del SL, un *buffer* para paquetes *geo-unicast*, un *buffer* para paquetes *geo-broadcast* y un *buffer* para el algoritmo CBF (si se encuentra habilitado). El *buffer* del SL se utiliza para almacenar los paquetes mientras que el SL resuelve la posición geográfica de un nodo destino. Los *buffers geo-unicast* y *geo-broadcast* son útiles para almacenar los paquetes *geo-unicast* y *geo-broadcast* respectivamente cuando el algoritmo de encaminamiento falla al encontrar un vecino válido como siguiente salto para enviar los paquetes hacia el destino. Los paquetes se extraen de los *buffers* cuando se incluye información sobre el destino de los paquetes en la TL y pueden ser encaminados. El almacenamiento de los paquetes en *buffers* evita su pérdida cuando, debido a la desconexión entre diferentes partes de la VANET, no hay vecinos válidos para el encaminamiento. Esto se produce con mayor probabilidad en escenarios con baja densidad de nodos. Por último, el *buffer* CBF se utiliza para almacenar los paquetes en la operación del algoritmo CBF.

Parte II

Conectando los vehículos a Internet en el sistema de transporte inteligente estandarizado por el ETSI

Capítulo 5

Optimización del protocolo de *GeoNetworking* estandarizado por el ETSI

5.1. Introducción

En el capítulo anterior se ha descrito el protocolo de *GeoNetworking* (GN) [36] que el sistema de transporte inteligente estandarizado por el ETSI utiliza para el encaminamiento de los paquetes en la VANET. El protocolo de GN actúa entre el nivel IP y el nivel de enlace de la torre de protocolos de manera que se esconde al nivel IP la topología multisalto de la VANET. El protocolo de GN permite realizar diferentes tipos de envío de paquetes entre los que destacan las entregas *geo-unicast* y *geo-broadcast*. Mientras que un paquete *geo-unicast* se entrega a un único destino situado en una posición determinada, los paquetes *geo-broadcast* se entregan a todos aquellos nodos que se encuentran situados dentro de una zona geográfica objetivo. En ambos tipos de envío, los paquetes se encaminan por la VANET en función de las coordenadas del destino, eligiendo como siguiente salto el nodo vecino que se encuentra más cerca del destino, consiguiendo el mayor avance con cada reenvío. De esta forma, los paquetes son reenviados por diferentes nodos intermedios desde el origen hasta el destino a través de una cadena multisalto.

Una de las dificultades que hay que afrontar cuando se establecen comunicaciones en redes vehiculares es el hecho de que los nodos pueden moverse a una velocidad elevada. La consecuencia de la alta y continua movilidad es que las comunicaciones sufren interrupciones continuamente debido a que los enlaces entre los nodos son muy inestables. Por otro lado, la escalabilidad es otro factor muy importante. La variabilidad de la densidad de nodos en la red es otra de las características de las redes vehiculares que dificultan las comunicaciones.

A pesar de estas dificultades, uno de los requisitos críticos para que los vehículos puedan establecer comunicaciones con nodos en Internet es que el protocolo de encaminamiento de la

VANET ofrezca un buen funcionamiento cuando se reenvían los paquetes entre los vehículos y las RSUs que brindan conexión con Internet.

El objetivo de este capítulo es analizar en profundidad el funcionamiento de la arquitectura del sistema de transporte inteligente que ha definido el ETSI y en concreto, del protocolo de GN cuando se utiliza para conectar los vehículos a Internet en escenarios de autovía/autopista. Este tipo de escenarios nos permite estudiar el protocolo de GN en condiciones en las que la velocidad de los vehículos es muy elevada, lo que dificulta las comunicaciones por la inestabilidad de los enlaces entre nodos, sobre todo con las RSUs, al tratarse de nodos fijos. Además, se considera que las comunicaciones con las RSUs son multisalto a través de diferentes vehículos, lo que permitiría reducir los costes desde el punto de vista de un despliegue real, ya que se podría dar servicio a un área mayor con la misma inversión en equipamiento. Para llevar a cabo este análisis, se realiza una evaluación basada en simulación de las prestaciones del protocolo bajo diferentes circunstancias. El análisis sistemático del comportamiento del protocolo de GN nos permite detectar sus limitaciones, puntos débiles y realizar una evaluación de la influencia de los diferentes mecanismos presentes en el protocolo. Además, se propone el uso de diversas soluciones y mejoras, estudiando su impacto sobre el protocolo, con el objetivo de subsanar las deficiencias y conseguir un aumento de las prestaciones obtenidas.

Las conclusiones que se han extraído del análisis del protocolo de GN que se presenta en este capítulo y las optimizaciones que consiguen mejorar las prestaciones del protocolo han sido recogidas y enviadas para que se considere su publicación en [5].

5.2. Escenario de simulación

A continuación se describe el escenario de simulación utilizado para evaluar las prestaciones del protocolo de GN del ETSI. Con el objetivo de conseguir resultados lo más próximos posibles a un escenario real, se ha utilizado el extensamente conocido simulador de redes OMNeT++[1]. Utilizando este simulador, hemos desarrollado nuestra propia implementación del protocolo de GN del ETSI [36] y de la capa de integración GN6ASL [58], necesaria para la transmisión de paquetes IPv6 sobre el protocolo de GN. Esta implementación se ha integrado con el *framework* INETMANET[2]. Nuestro análisis se centra en el escenario en el que una RSU proporciona conectividad a Internet a los vehículos que se encuentran dentro de su zona geográfica. La Figura 5.1 muestra un esquema del escenario de simulación. Se trata de un tramo de autovía con tres carriles y 2000 metros de longitud, donde una RSU da servicio a todos los vehículos que se encuentran dentro del segmento de carretera. Es decir, la RSU se encuentra situada en mitad del tramo de autovía y su área asignada son los 2000 metros de este segmento. Nótese que las prestaciones del

[1] *OMNeT++ Network Simulator Framework: http://www.omnetpp.org/*

[2] *INETMANET framework for OMNET/OMNeT++ 4.x (based on INET framework): https://github.com/inetmanet/inetmanet/wiki*

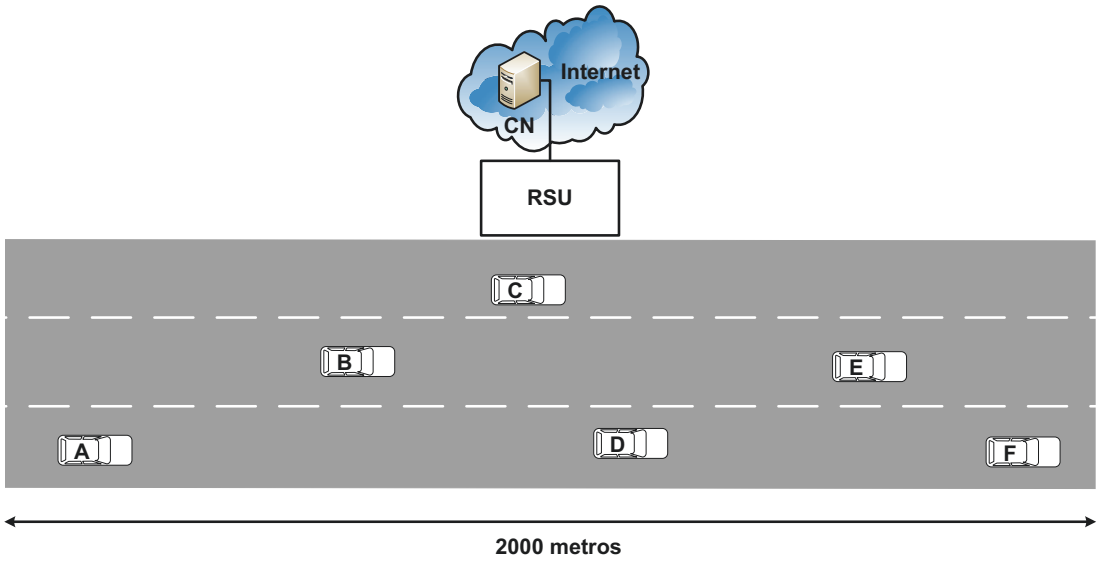


Figura 5.1: Esquema del escenario de simulación para el análisis del protocolo de GN.

protocolo de GN cuando los vehículos establecen comunicaciones con Internet pueden evaluarse utilizando un escenario de simulación que cubra únicamente una RSU (un área) dado que el protocolo de GN solo proporciona comunicaciones entre los nodos que se encuentran dentro del mismo área geográfica. El estudio de la movilidad entre diferentes zonas geográficas se realiza más adelante en el Capítulo 6.

Las trazas de vehículos que se utilizan en las simulaciones se han generado sintéticamente asumiendo una distribución exponencial para el tiempo de llegada entre vehículos [111], que puede ajustarse para obtener una determinada densidad de vehículos en el tramo de autovía (medida en vehículos por kilómetro). Mientras que no se mencione lo contrario, se asume una densidad de 45 veh/Km en los diferentes experimentos. El carril de partida de los vehículos se selecciona aleatoriamente conforme a una distribución uniforme. Respecto a la velocidad objetivo de los vehículos, esta se obtiene siguiendo una distribución Gaussiana centrada en 110 Km/h y con una desviación estándar de 10 Km/h [112]. Como existe una relación directa entre la densidad de vehículos y la velocidad de los mismos, se ha utilizado [113] para seleccionar valores realistas de velocidad y densidad. Estas trazas de vehículos se inyectan en el simulador de tráfico SUMO[3] [114], que se encuentra acoplado con el simulador de redes OMNET++ para reproducir un comportamiento realista de los conductores durante las simulaciones. Por ejemplo, los vehículos tratan de utilizar el carril derecho cuando es posible y, cuando un vehículo que viaja a su velocidad objetivo se encuentra a otro vehículo delante a una velocidad menor, reducirá su velocidad y lo adelantará cuando las circunstancias lo permitan. Por otro lado, todos los vehículos y la RSU se encuentran equipados con un nivel de enlace IEEE 802.11g operando a una tasa de 54

[3] *SUMO Simulation of Urban MObility: http://sumo.sourceforge.net/*

Mbps[4]. La potencia de transmisión se ha ajustado para proporcionar un radio de cobertura de 200 metros [116, 117].

Cuando los vehículos entran en la simulación, viajan a lo largo del área geográfica de la RSU hasta que salen del tramo de autovía. Para evitar la interacción que pueden tener los mecanismos de configuración de direcciones IPv6 sobre las prestaciones del protocolo de GN, los nodos entran en el escenario de simulación con una dirección IPv6 global pre-asignada. Sin embargo, es necesario mencionar que en las simulaciones se considera la sobrecarga de señalización necesaria para la configuración de direcciones IPv6 de GeoSAC. Es decir, la RSU distribuye periódicamente mensajes RA con el prefijo IPv6 que se utiliza en su área geográfica por medio de *geo-broadcasting*. El intervalo entre mensajes RA enviados por la RSU se selecciona uniformemente entre RA_{min} = 2.75 segundos y RA_{max} = 3.25 segundos, por lo que el intervalo medio entre mensajes RA es de 3 segundos. Tal y como se explica en el apartado 5.4.2.3, con el objetivo de evitar colisiones en el canal inalámbrico cuando la RSU distribuye los mensajes RA, en cada nodo se introduce un retardo aleatorio seleccionado uniformemente entre 0 y 5 milisegundos antes de retransmitir un paquete *geo-broadcast*. Respecto al protocolo de GN, mientras que no se mencione lo contrario, todos los parámetros han sido ajustados de acuerdo a su especificación [36].

Para evaluar el funcionamiento del protocolo de GN cuando se utiliza para proporcionar comunicaciones entre los vehículos e Internet, se establecen flujos CBR (*Constant Bit Rate*) UDP entre determinados vehículos de la VANET y un *Correspondent Node* (CN) en Internet. Con el objetivo de focalizar la evaluación del rendimiento en la VANET, el CN se encuentra directamente conectado a la RSU en las simulaciones. Cuando se selecciona un vehículo para comunicarse con el CN, se establecen dos flujos CBR UDP independientes entre el vehículo y el CN, uno en cada sentido de la comunicación. El patrón de tráfico de los flujos CBR UDP se ha seleccionado para modelar una conversación VoIP de manera que se envían paquetes de 160 bytes de datos cada 20 milisegundos (*códec* G.711). Nótese que la utilización de un patrón de tráfico CBR con un intervalo entre paquetes reducido nos permite muestrear el funcionamiento de la VANET con exactitud. Además, en la Sección 5.4.12 se evalúan las prestaciones con diferentes patrones de tráfico de datos. Los vehículos que envían y reciben tráfico de datos se seleccionan aleatoriamente siguiendo una distribución geométrica que se puede ajustar para que un determinado porcentaje de vehículos se comunique con el CN[5]. De esta manera, se han ejecutado múltiples simulaciones variando el porcentaje de vehículos que se comunican con el CN. Cada experimento se ha repetido 30 veces con diferentes semillas (se proporcionan los intervalos de confianza al 95 %).

[4]Como se ha mencionado en el estado del arte, los estándares del ETSI consideran la posibilidad de utilizar el protocolo de GN sobre diferentes tecnologías de acceso inalámbricas. Aunque el estándar IEEE 802.11p (o ITS-G5) ha sido diseñado para su utilización en redes vehiculares, en las simulaciones los nodos utilizan interfaces IEEE 802.11g ya que su uso se encuentra ampliamente extendido y se pueden encontrar tarjetas de red a un precio reducido, lo que facilitaría la penetración en el mercado. Además, su utilización en redes vehiculares resulta viable para escenarios de autovía/autopista [115].

[5]La distribución geométrica es la versión discreta de la distribución exponencial, que sirve para modelar fenómenos naturales con independencia entre sucesos (sin memoria). En nuestro escenario, el hecho de que un vehículo envíe tráfico no condiciona que los vehículos que tiene a su alrededor tengan mayor o menor probabilidad de enviar tráfico.

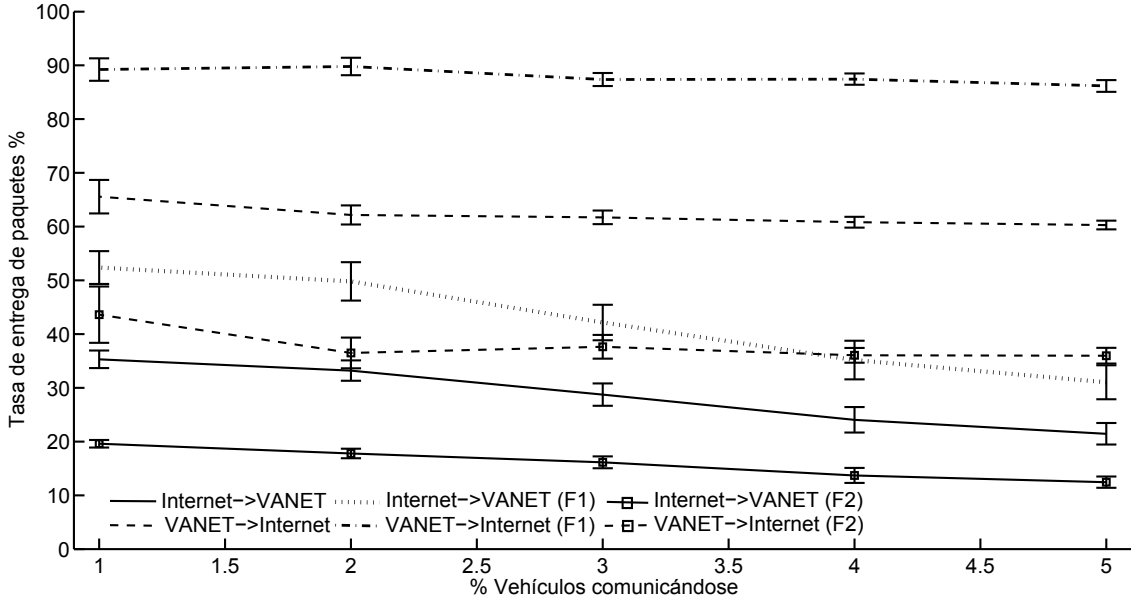


Figura 5.2: Tasa de entrega de paquetes del protocolo de GN estándar.

Las diferentes estadísticas se toman durante 200 segundos de simulación una vez que el tramo de autovía se encuentra repleto de vehículos, de manera que se recrea un escenario real en el que los vehículos tienen otros vehículos delante y detrás. Para cada vehículo, las medidas se toman desde el momento en el que este entra en el escenario de simulación hasta que sale de él tras recorrer el tramo de carretera.

5.3. Evaluación del protocolo de *GeoNetworking* estandarizado por el ETSI

Esta sección se centra en evaluar el funcionamiento del protocolo de GN estandarizado por el ETSI cuando se proporciona conectividad a Internet a los vehículos de la VANET. Para ello, se analizan los resultados de las simulaciones realizadas sobre el escenario descrito anteriormente.

La Figura 5.2 presenta los resultados de la tasa de entrega de paquetes para los flujos CBR UDP en ambas direcciones de envío (desde Internet a la VANET y vice versa) en función del porcentaje de vehículos del tramo de autovía que se comunican con el CN. Como se puede observar en la figura, la tasa de entrega de paquetes decrece conforme aumenta el porcentaje de vehículos que se comunican con el CN. Además, se puede ver que la tasa de entrega de paquetes para los flujos de Internet a la VANET es significativamente menor que la tasa de entrega de paquetes de los flujos en el otro sentido, de la VANET a Internet. Asimismo, nótese que en general, la tasa de entrega de paquetes que alcanza el protocolo de GN (menos de un 40 % en el sentido Internet-VANET y menos de un 70 % en el sentido VANET-Internet) está lejos de ser aceptable para una comunicación satisfactoria.

Un estudio pormenorizado de las trazas de las simulaciones reveló la explicación a estos comportamientos y al bajo rendimiento obtenido por el protocolo de GN. Por un lado, el descenso de la tasa de entrega de paquetes con el porcentaje de vehículos que se comunican con el CN se debe a que cuanto mayor es el tráfico de datos en la red, los recursos deben ser compartidos entre más nodos que intentan comunicarse, lo que conlleva una reducción de prestaciones. Por otro lado, se observó que el algoritmo de *greedy forwarding* selecciona vecinos inválidos como siguiente salto para el encaminamiento de los paquetes. Esto provoca que los paquetes se descarten en la capa MAC de los nodos porque no es posible entregárselos al siguiente salto cuando este no es alcanzable (por su movimiento ha salido fuera del radio de cobertura). Esto hace que las prestaciones generales sean bajas, y en particular en el sentido Internet-VANET de las comunicaciones. La selección de vecinos inválidos como siguiente salto contribuye a que la RSU se sature y que los paquetes se descarten en el nivel MAC porque su cola se llena. Hay que tener en cuenta que como la RSU actúa como *router* de acceso para todos los vehículos del tramo de carretera, esta concentra todo el tráfico entre Internet y la VANET. De esta forma, la RSU tiene que acceder al canal inalámbrico más veces que un vehículo ya que cursa mayor cantidad de tráfico. Por ello, la RSU es más vulnerable a la saturación, ya que los vehículos y la RSU tienen las mismas oportunidades de acceder al canal inalámbrico. Además, aunque con una influencia menor, hay que considerar que resulta más sencillo entregar paquetes a la RSU que a un vehículo que cambia su posición continuamente dado que los vehículos siempre conocen la posición geográfica exacta de la RSU al tratarse de un nodo fijo.

Con la intención de profundizar en estos problemas, se ha estudiado el rendimiento del protocolo de GN en función de la posición de la RSU respecto al sentido del movimiento de los vehículos de la VANET. De esta manera, las medidas sobre el escenario de simulación se han dividido en dos fases: 1) Los vehículos que se comunican con el CN viajan acercándose hacia la RSU y 2) los vehículos que se comunican con el CN se mueven alejándose de la RSU. La tasa de entrega de paquetes para los flujos en ambas direcciones, Internet-VANET y VANET-Internet, en función del porcentaje de vehículos que se comunican con el CN y diferenciando entre la fase 1 (F1) y la fase 2 (F2) también se muestra en la Figura 5.2. Como puede observarse en esta figura, existe una gran diferencia entre el rendimiento en ambas fases. En el caso en el que los vehículos que se comunican con el CN se acercan a la RSU, la RSU selecciona como siguiente salto para los paquetes que van desde Internet a la VANET al vecino más cercano al destino, que también se mueve acercándose a la RSU. Este vecino continúa siendo alcanzable hasta que se selecciona como siguiente salto otro nuevo vecino mejor posicionado que al moverse hacia la RSU se va introduciendo cada vez más en el radio de cobertura de la RSU. Por el contrario, cuando el vehículo destino se aleja de la RSU, el vecino que se selecciona como siguiente salto también se aleja de la RSU, por lo que dejará de ser alcanzable rápidamente cuando salga del radio de cobertura de la RSU. Cuando esto ocurra, los paquetes se descartarán hasta que la RSU seleccione un nuevo vecino válido para llegar al destino. Nótese que este razonamiento es igualmente válido en el otro sentido de la comunicación, cuando los vehículos intentan llegar a la RSU para enviar paquetes

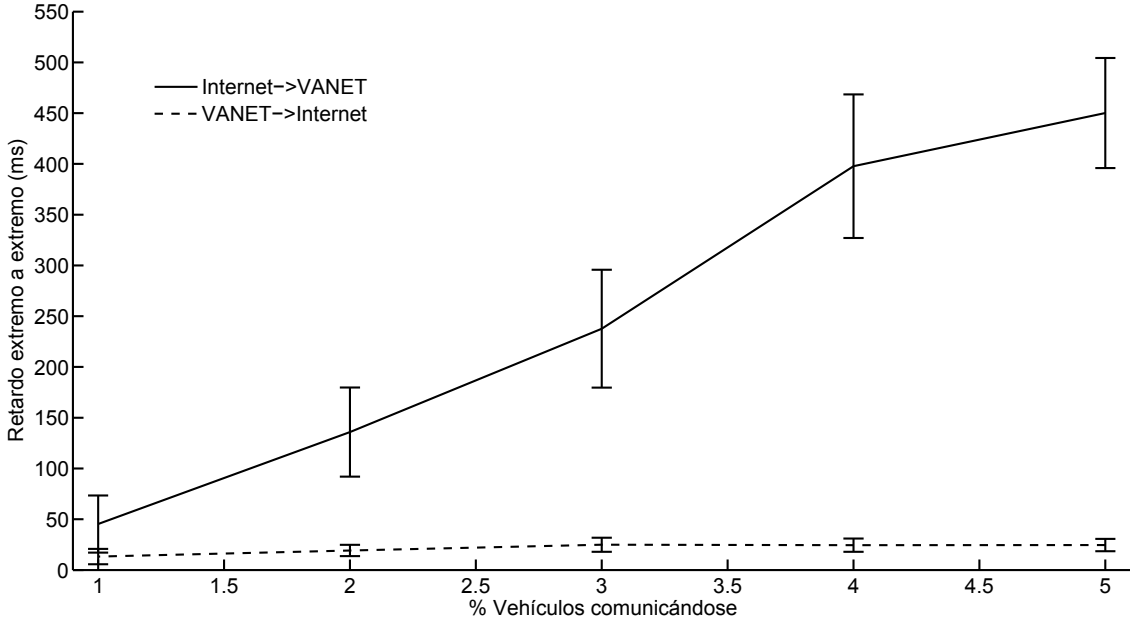


Figura 5.3: Retardo extremo a extremo del protocolo de GN estándar.

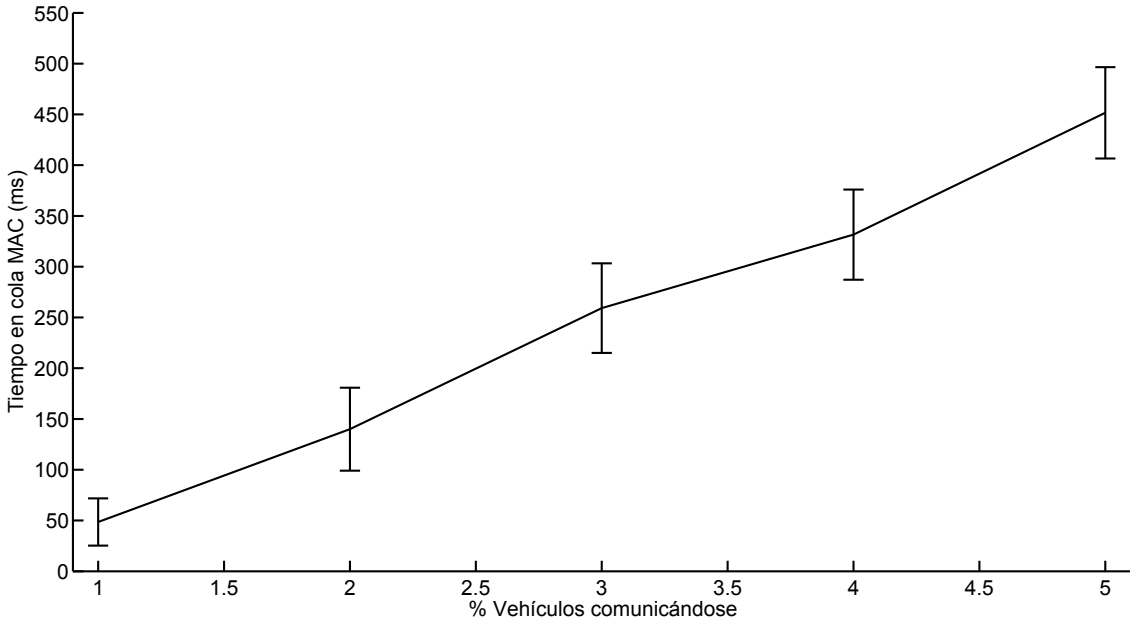


Figura 5.4: Tiempo en cola MAC en la RSU del protocolo de GN estándar.

hacia Internet. Por este motivo, la tasa de entrega de paquetes es más elevada cuando los vehículos que se comunican con el CN viajan acercándose a la RSU que cuando se alejan de ella.

Esta variación significativa de las prestaciones del protocolo de GN cuando los vehículos se acercan o se alejan de la RSU puede ser considerado cuando se diseñan protocolos de encaminamiento para redes vehiculares.

Por otro lado, también se ha estudiado el comportamiento del protocolo de GN respecto al retardo extremo a extremo que experimentan los paquetes de datos. La Figura 5.3 muestra el retardo extremo a extremo que sufren los paquetes de datos para los flujos en ambos sentidos (Internet-VANET y VANET-Internet) frente al porcentaje de vehículos que se comunican con el CN. Cuanto mayor es el porcentaje de vehículos que se comunican con el CN, mayor es el retardo extremo a extremo que experimentan los paquetes debido a que el tráfico de datos en la red aumenta y el canal inalámbrico debe ser compartido entre más nodos tratando de transmitir paquetes. Tal y como ocurría con la tasa de entrega de paquetes, existe una diferencia significativa entre el sentido Internet-VANET y el sentido VANET-Internet de las comunicaciones. Como puede apreciarse en la Figura 5.4, que muestra el tiempo que permanecen los paquetes en la cola del nivel MAC de la RSU en función del porcentaje de vehículos que se comunican con el CN, la mayor componente del retardo extremo a extremo en el sentido Internet-VANET es el tiempo que los paquetes esperan en la cola del nivel MAC de la RSU, que es mayor conforme aumenta el porcentaje de vehículos que se comunican con el CN[6]. Estos resultados muestran la saturación de la RSU, que se ve agravada por la selección de vecinos inválidos como siguiente salto por parte del algoritmo *greedy forwarding*.

A la vista de estos resultados, el rendimiento del protocolo de GN tal y como ha sido especificado por el ETSI en [36] está lejos de ser satisfactorio cuando se proporciona a los vehículos de la VANET conectividad a Internet. En la siguiente sección se realiza un análisis más detallado del protocolo de GN del ETSI para revelar cuáles son sus puntos débiles. Además se presentan y estudian diferentes mecanismos para combatirlos, consiguiendo mejorar las prestaciones del protocolo.

5.4. Análisis del protocolo de *GeoNetworking* y mecanismos de optimización

A continuación se presenta un análisis detallado de algunos aspectos del protocolo de GN que sirve para descubrir cuáles son sus puntos débiles y de esta manera saber dónde se pueden aplicar mecanismos para mejorar sus prestaciones.

5.4.1. Análisis del tiempo de caducidad de la tabla de localización

Como se mencionó anteriormente, en las simulaciones realizadas se producen pérdidas de paquetes debido a dos principales razones: 1) Se descartan paquetes en el nivel MAC de los

[6]Nótese que las medidas del retardo extremo a extremo solo consideran aquellos paquetes que llegan a alcanzar el destino. Sin embargo, en los resultados del tiempo en cola de los paquetes en el nivel MAC de la RSU se tienen en cuenta todos los paquetes de datos que envía la RSU, aunque algunos de estos paquetes se descarten antes de alcanzar al destino.

nodos porque no es posible entregar los paquetes al vecino elegido como siguiente salto porque debido a su movimiento ha salido del radio de cobertura. 2) En el sentido Internet-VANET, los paquetes se descartan en la capa MAC de la RSU debido a que su cola de paquetes se satura (la saturación de la RSU se ve agravada por la selección incorrecta de vecinos).

El problema de la selección de vecinos inválidos como siguiente salto tiene su origen en el propio funcionamiento del algoritmo de *greedy forwarding*. El algoritmo de *greedy forwarding* selecciona como siguiente salto para un paquete al vecino de la TL que está situado más cerca del destino. Cuando se descubre un vecino, se le asocia una entrada que se guarda en la TL y que se considera como válida mientras que no venza su tiempo de caducidad. Sin embargo, algunos vecinos incluidos en la TL pueden ser considerados como válidos y seleccionados como siguiente salto por el algoritmo de *greedy forwarding* aunque no sean alcanzables porque se han desplazado fuera del radio de cobertura. Se podría pensar que disminuyendo el periodo con el que se refresca la información de los vecinos en la TL (el periodo de *beacon*) se solucionaría el problema porque la información de la TL sería más reciente. En cambio, como los vecinos que se han salido del radio de cobertura no pueden actualizar su posición en la TL, esto solo incrementaría la carga de tráfico de señalización en la red, ya que el problema está producido por el largo tiempo de caducidad de las entradas de la TL (20 segundos según indica el estándar).

El problema radica en que hay vecinos que se mantienen en la TL durante un tiempo muy largo incluso cuando no son alcanzables nunca más, debido a la elevada movilidad de los nodos en la VANET. De esta manera el algoritmo de *greedy forwarding* selecciona vecinos inalcanzables como siguiente salto para encaminar los paquetes con una alta probabilidad. Esta situación no se soluciona hasta que aparece un nuevo vecino que se le considera mejor posicionado para llegar al destino o, hasta que la entrada del vecino inválido expira y se elimina de la TL. Nótese que este problema no solo hace que los paquetes se descarten mientras que se selecciona un nuevo vecino válido, sino que además contribuye a aumentar la carga de tráfico en el medio inalámbrico porque como se establece en el estándar IEEE 802.11 [38], el nivel MAC intenta entregar un paquete hasta siete veces antes de descartarlo cuando no se recibe el mensaje de confirmación ACK de nivel de enlace. Por lo tanto, como fruto de la selección incorrecta de vecino, el resto de paquetes de la cola MAC se ven retrasados hasta que se realizan los siete reintentos de transmisión. Esto provoca que el tiempo que permanecen los paquetes en la cola del nivel MAC de la RSU aumente, llegando incluso a un estado de saturación en el que los paquetes se descartan porque la cola está llena (véase la Figura 5.4). Asimismo, hay que mencionar que el algoritmo de *greedy forwarding* es especialmente propenso a esta situación, ya que su tendencia es seleccionar como siguiente salto a los vecinos que se encuentran más cerca del límite del radio de cobertura, por lo que estos normalmente salen del radio de cobertura rápidamente. Por ejemplo, como se mencionó anteriormente, cuando los vehículos destino se alejan de la RSU, la RSU selecciona como siguiente salto al vecino más lejano en la dirección del destino. Como los vehículos se mueven alejándose de la RSU, es probable que el vecino seleccionado ya haya salido fuera del radio de cobertura (la entrada en la TL es obsoleta) o, que salga fuera del radio de cobertura rápidamente

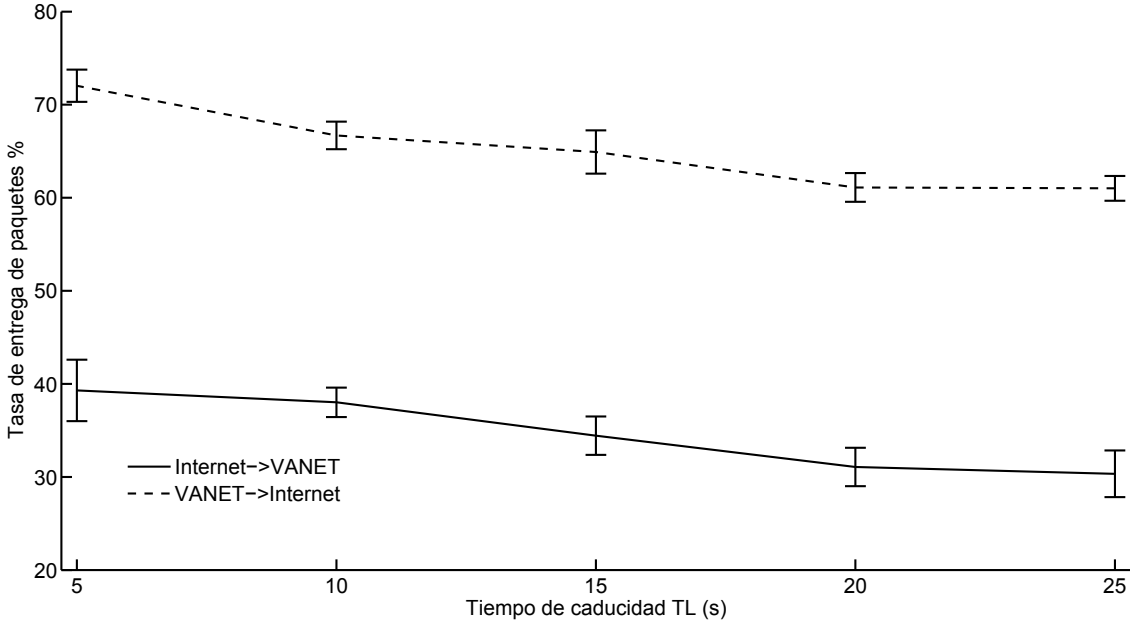


Figura 5.5: Tasa de entrega de paquetes del protocolo de GN estándar en función del tiempo de caducidad.

(la tendencia es elegir como siguiente salto a vecinos situados cerca del límite de cobertura). Esto no solo provoca que los paquetes hacia ese destino se descarten porque el vecino es inalcanzable, sino que como los reintentos de envío sin éxito a nivel de enlace contribuyen a la saturación de la RSU, se llega a una situación en la que los paquetes se descartan porque la cola del nivel MAC se llena, incluso cuando el tráfico de datos es reducido.

Para analizar este comportamiento, se ha estudiado el efecto de la variación del tiempo de caducidad de las entradas de la TL. La Figura 5.5 muestra la tasa de entrega de paquetes para los flujos CBR UDP medida en ambos sentidos de la comunicación (de Internet a la VANET y de la VANET a Internet) en función del tiempo de caducidad de las entradas de la TL en el caso en el que el 3 % de los vehículos de la VANET establecen comunicaciones con el CN. Se puede ver como la tasa de entrega de paquetes mejora cuando el tiempo de caducidad de la TL disminuye. La explicación es que si las entradas inválidas de la TL se eliminan más rápidamente, la probabilidad de que el algoritmo de *greedy forwarding* elija vecinos inalcanzables como siguiente salto disminuye. Incluso en el caso en el que se seleccione un vecino inválido como siguiente salto para los paquetes hacia un determinado destino, la situación se soluciona más rápidamente porque el tiempo de caducidad de la entrada del vecino inalcanzable expira antes. Sin embargo, como puede apreciarse, el rendimiento del protocolo de GN continúa siendo bajo incluso si el tiempo de caducidad de la TL se disminuye a 5 segundos, que es el mejor resultado de los casos simulados. Como máximo, se ha obtenido una tasa de entrega de paquetes del 72 % en el sentido VANET-Internet y del 39 % para el sentido Internet-VANET. Nótese que el tiempo de caducidad de la TL tiene que ser mayor que el periodo con el que se actualiza la información de los vecinos

(el periodo con el que se actualiza la información de los vecinos en nuestras simulaciones es de 3 segundos), por ello, el menor tiempo de caducidad que se ha considerado en las simulaciones es de 5 segundos.

Por otro lado, como la TL también se utiliza para almacenar la posición geográfica de los nodos destino averiguada por medio del Servicio de Localización (SL), el tiempo de caducidad de la TL se tiene que configurar teniendo esto en cuenta. La idea es que la posición de un destino descubierta por medio del SL tiene que ser almacenada en la TL mientras que el destino sea alcanzable por un paquete dirigido a esa posición aunque el nodo destino se haya desplazado. En otras palabras, la posición geográfica del destino tiene que ser borrada de la TL cuando el punto geográfico al que se envían los paquetes se encuentra fuera del radio de cobertura del nodo destino. Si no se dispone de una actualización de posición geográfica del destino, no tiene sentido enviar el tráfico de datos a una posición desactualizada donde el destino no puede recibirlos porque se ha movido. De hecho, esto impone un requisito más estricto que el problema de la actualización de la posición de los vecinos debido a que, un fallo eventual con la entrega de los paquetes a un vecino se puede detectar, pero el hecho de que un destino final no se encuentre en la posición donde se le envía tráfico de datos significa que los paquetes van a ser descartados. De esta forma, el tiempo de caducidad de la TL viene dado por la inecuación (5.1), donde R es el radio de cobertura de los nodos y V_{max} es la velocidad máxima de los vehículos en la carretera:

$$t_{TL} \leq \frac{R}{V_{max}} \tag{5.1}$$

En nuestro escenario, con 200 metros de radio de cobertura y considerando una velocidad máxima de 120 Km/h., de aquí en adelante, mientras que no se mencione lo contrario, se establece un tiempo de caducidad de la TL de 6 segundos. Nótese que los vehículos podrían obtener la velocidad máxima de la vía de diferentes maneras, por ejemplo: 1) Se podría incluir en los mensajes difundidos por la RSU. 2) Los vehículos podrían estimarla a partir de la información de velocidad recibida en los paquetes de GN de sus vecinos directos. 3) La velocidad máxima podría obtenerse de los mapas digitales de la base de datos del GPS instalado en el vehículo. En nuestra opinión, el tiempo de caducidad de la TL debería ser configurable en función de la tecnología de acceso utilizada (que determina el radio de transmisión, R) y la velocidad máxima de la vía (V_{max}) con el objetivo de que este valor represente realmente el tiempo durante el que se puede esperar que la entrada en la TL se pueda considerar fiable.

5.4.2. Influencia de diferentes mecanismos propuestos en el estándar de *GeoNetworking*

A continuación se estudia el efecto sobre las prestaciones de diferentes mecanismos presentes en el estándar que tienen como objetivo mejorar el funcionamiento del protocolo de GN.

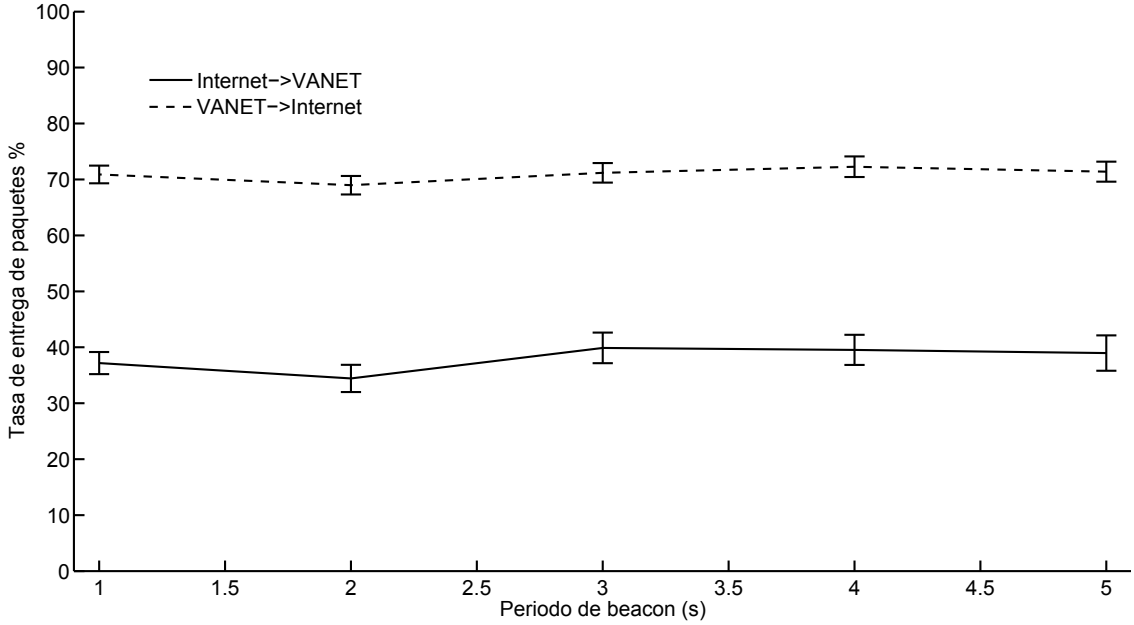


Figura 5.6: Tasa de entrega de paquetes del protocolo de GN estándar en función del periodo de *beacon*.

5.4.2.1. Algoritmo de *beaconing* y solapamiento con mensajes *Router Advertisement*

Un aspecto interesante que conviene estudiar es el algoritmo de *beaconing* y la influencia del periodo de *beacon* en las prestaciones del protocolo de GN. La Figura 5.6 presenta los resultados de la tasa de entrega de paquetes para los flujos en ambos sentidos de la comunicación, Internet-VANET y VANET-Internet, cuando se varía el periodo de *beacon* y el 3 % de los vehículos de la VANET se comunican con el CN. Como puede observarse en la figura, las prestaciones del protocolo de GN en nuestro escenario son independientes del periodo de *beacon*. La explicación a este fenómeno se debe a que existe un solapamiento entre los paquetes *beacon* y los mensajes *Router Advertisement* (RA) que distribuye la RSU, de manera que los mensajes RA juegan el papel de los mensajes *beacon* del protocolo de GN.

De acuerdo con el algoritmo de *beaconing*, los nodos periódicamente envían mensajes *beacon* en *broadcast* incluyendo su identificador, posición geográfica actual, dirección que siguen, velocidad, etc. El envío de mensajes *beacon* provoca una carga de señalización en la red que depende del periodo de *beacon* pero que, sin embargo, es necesaria para el correcto funcionamiento del protocolo. Con el objetivo de reducir la carga de señalización en la red producida por el algoritmo de *beaconing*, la especificación del protocolo de GN [36] establece que “se debería enviar un paquete *beacon* cada periodo de *beacon* a no ser que se envíe otro paquete de GN”. Es decir, los nodos envían en *broadcast* mensajes *beacon* cada periodo de *beacon* a no ser que se envíe otro mensaje de GN, en cuyo caso el temporizador que regula el envío de mensajes *beacon* se reinicializa. Esto se debe a que se realiza *beacon piggybacking* y la información del mensaje *beacon* también se incluye en la cabecera del protocolo de GN de todos los paquetes.

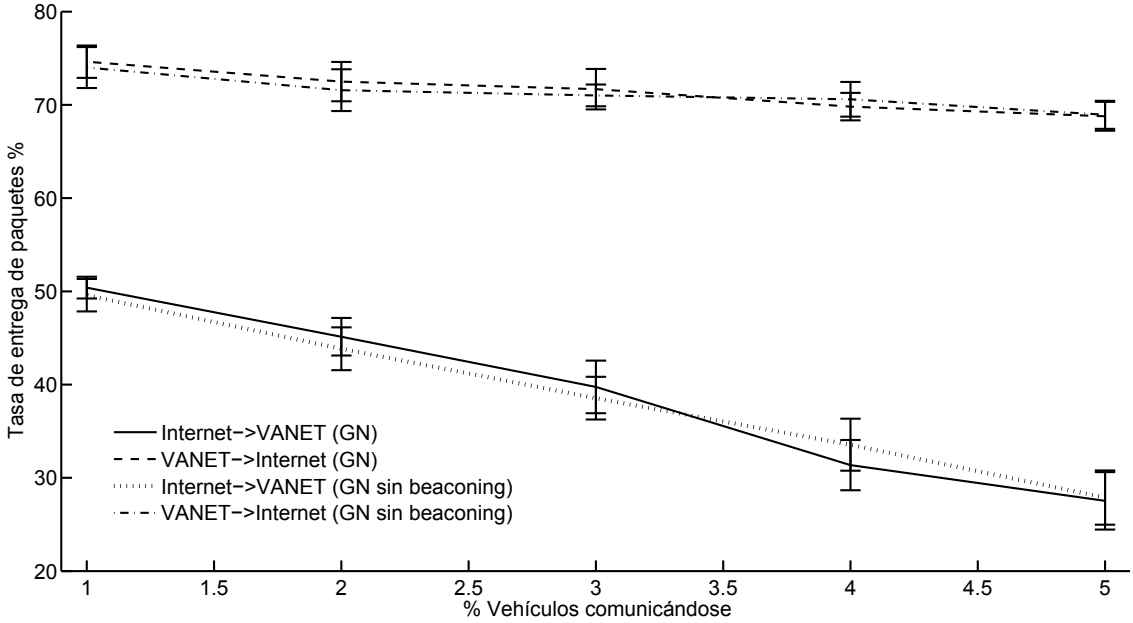


Figura 5.7: Tasa de entrega de paquetes del protocolo de GN estándar sin *beaconing*.

De esta manera, cuando los vehículos retransmiten los mensajes RA enviados por la RSU para su distribución dentro del área geográfica, estos reinicializan su temporizador de *beaconing*. Como el periodo con el que se envían los mensajes RA en nuestro escenario se solapa con el periodo del algoritmo de *beaconing*, los nodos no transmiten mensajes *beacon* a sus vecinos porque reinicializan el temporizador de *beaconing* continuamente antes de que expire. De este modo, el mecanismo de *beaconing* se ve reemplazado por la distribución de mensajes RA, ya que como la RSU envía mensajes RA periódicamente que se distribuyen a todos los vehículos del área por medio de inundación, la TL de los nodos se actualiza con información de los vecinos cada vez que la RSU envía un mensaje RA.

Para comprobar esta hipótesis y confirmar que la reinicialización de los temporizadores de *beaconing* no tiene un impacto negativo sobre las prestaciones (gracias a que los nodos pueden actualizar su TL cuando se distribuyen los mensajes RA), se obtuvieron resultados de simulaciones en las que se deshabilitaba por completo el mecanismo de *beaconing*. La Figura 5.7 muestra la comparación de la tasa de entrega de paquetes en función del porcentaje de vehículos que se comunican con el CN cuando el algoritmo de *beaconing* se encuentra activado y desactivado. Como puede observarse, la desactivación del mecanismo de *beaconing* no tiene ningún impacto sobre las prestaciones del protocolo de GN. A la vista de los resultados obtenidos, podemos concluir que el mecanismo de *beaconing* deja de actuar, sin que esto suponga una degradación de prestaciones, en escenarios donde hay paquetes que se distribuyen periódicamente utilizando inundación a todos los vehículos (con un periodo inferior o igual al del algoritmo de *beaconing*), lo que suele suceder cuando se conecta la VANET a Internet (los mensajes RA son necesarios para que los vehículos auto-configuren una dirección IPv6 global).

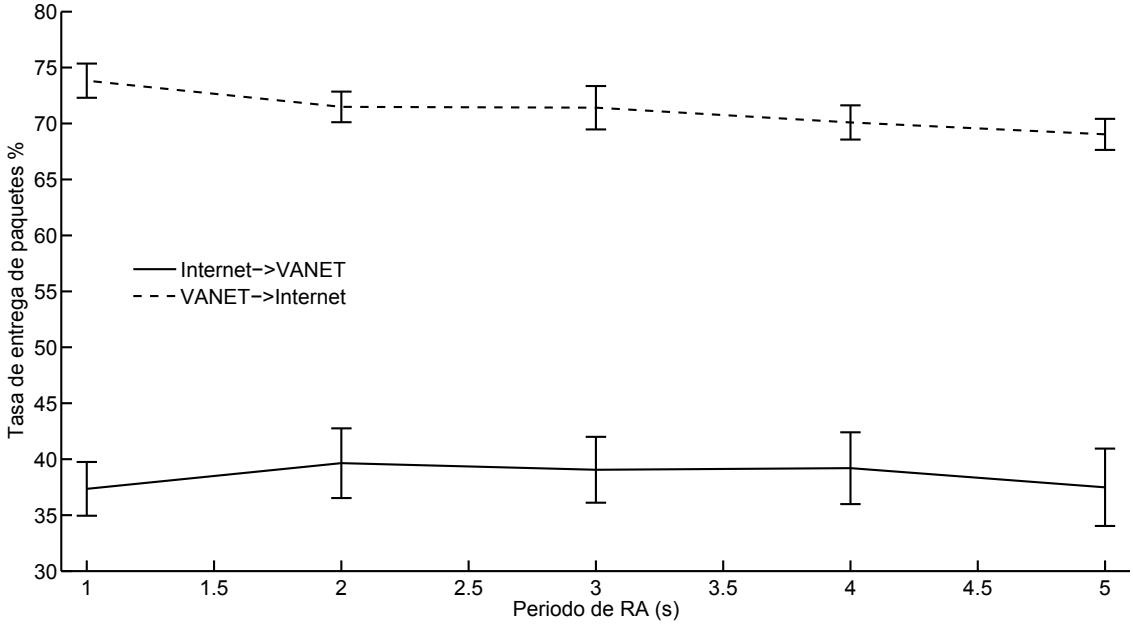


Figura 5.8: Tasa de entrega de paquetes del protocolo de GN estándar en función del periodo de RA.

Con el objetivo de observar la influencia que tiene el intervalo entre los mensajes RA que difunde la RSU en las prestaciones del protocolo de GN, se realizaron simulaciones en las que se varió el periodo entre mensajes RA y se desactivó el algoritmo de *beaconing* para evitar su interacción. La Figura 5.8 muestra la tasa de entrega de paquetes para los flujos en los sentidos Internet-VANET y VANET-Internet, cuando se varía el periodo con el que la RSU envía mensajes RA en el caso en el que el 3 % de los vehículos de la VANET establecen comunicaciones con el CN. Puede observarse cómo el periodo entre mensajes RA no tiene una influencia muy significativa. Mientras que en el sentido VANET-Internet se observa una disminución muy leve de la tasa de entrega de paquetes cuando se incrementa el intervalo entre mensajes RA, en el sentido Internet-VANET no se aprecia ninguna influencia. Este resultado, que puede parecer inesperado en un primer momento, se debe a la combinación de dos efectos: 1) El hecho de incluir la información del mensaje *beacon* en todos los paquetes hace que cada vez que se recibe un paquete de datos de un vecino, se actualice su información de posicionamiento en la TL. De esta manera, los nodos que forman parte de la cadena de encaminamiento que siguen los paquetes de datos desde la RSU hasta el vehículo destino y vice versa, actualizan muy frecuentemente la posición de los vecinos directos que pertenecen a la cadena de encaminamiento (el intervalo entre paquetes de datos es del orden de milisegundos). Es decir, cada vez que un paquete de datos viaja por la cadena de nodos entre origen y destino, se actualiza la posición de los vecinos de la cadena de encaminamiento. 2) Los vehículos tienden a mantener al mismo nodo como siguiente salto para llegar a un destino debido a que por un lado, la velocidad relativa entre vehículos es reducida (nótese que esto no aplica a la RSU al tratarse de un nodo fijo), y por otro lado, la actualización

muy frecuente de la posición de los vecinos de la cadena de encaminamiento crea una tendencia a que se sigan manteniendo a estos nodos como mejores vecinos para llegar al destino. Por lo tanto, el periodo de RA no tiene tanta influencia sobre las prestaciones como cabría esperar.

Por último, es necesario mencionar un problema que puede aparecer por la reinicialización del temporizador de *beaconing* con el envío de mensajes de GN. Cuando los vehículos se comunican con un CN, no envían mensajes *beacon* ya que se encuentran transmitiendo paquetes de datos *geo-unicast* continuamente. Sin embargo, cuando un nodo envía un paquete *geo-unicast*, el paquete solo es recibido por el nodo que ha sido seleccionado como siguiente salto y este es el único vecino que procesa la información incluida en la cabecera del protocolo de GN, que le sirve para actualizar su TL. De esta forma, otros vecinos no procesan la cabecera del protocolo de GN y como consecuencia, no actualizan su TL con la información de localización. Por lo tanto, la reinicialización del temporizador de *beaconing* puede ser inapropiada en escenarios en los que únicamente se realizan envíos de paquetes *geo-unicast* (los paquetes no se envían en *broadcast* a todos los vecinos) ya que, como los vehículos que envían los paquetes *geo-unicast* no envían paquetes *beacon*, estos no pueden ser descubiertos por sus vecinos (a excepción del nodo elegido como siguiente salto).

5.4.2.2. *Buffering*

El protocolo de GN [36] incluye un mecanismo de *buffering* de manera que cuando el algoritmo de *greedy forwarding* no consigue encontrar un vecino en la TL más cerca del destino para continuar con el encaminamiento, los paquetes se introducen en un *buffer* evitando su pérdida. Los paquetes se mantienen en el *buffer* hasta que se incluye información sobre el destino de los paquetes en la TL, de manera que puedan ser encaminados de nuevo.

Para analizar el impacto que tiene el mecanismo de *buffering* sobre las prestaciones del protocolo de GN, la Figura 5.9 muestra la tasa de entrega de paquetes para los flujos de datos de Internet a la VANET y de la VANET a Internet, frente al porcentaje de vehículos que se comunican con el CN. Se presentan los resultados cuando se habilita y se deshabilita el mecanismo de *buffering*. El almacenamiento de los paquetes en el *buffer* evita su pérdida cuando, debido a la desconexión entre diferentes partes de la VANET, no hay vecinos válidos para el encaminamiento. Por lo tanto, el mecanismo de *buffering* será útil en escenarios con baja densidad de vehículos donde existe una mayor probabilidad de que se produzcan desconexiones entre diferentes zonas de la VANET. Sin embargo, como puede observarse en la figura, la desactivación del mecanismo de *buffering* no produce ningún impacto sobre la tasa de entrega de paquetes. Esto se debe a que en nuestras simulaciones, la densidad de vehículos es suficientemente alta (45 veh/Km) como para que no se produzcan particiones en la VANET y por lo tanto, el algoritmo de *greedy forwarding* no encuentre problemas para encontrar vecinos para llegar al destino.

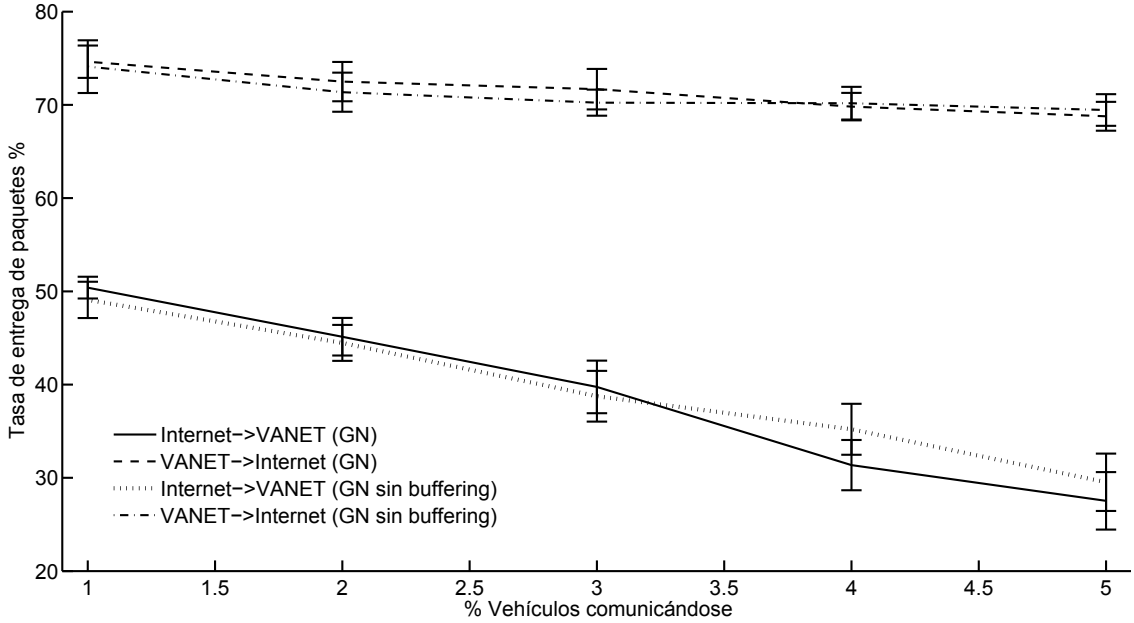


Figura 5.9: Tasa de entrega de paquetes del protocolo de GN estándar sin *buffering*.

5.4.2.3. Retardo de *broadcasting*

En el protocolo de GN, *geo-broadcasting* se realiza mediante el algoritmo *"Simple Geo-broadcast forwarding algorithm with line forwarding"*. Según este algoritmo, un paquete *geo-broadcast* se encamina hacia la zona geográfica destino usando el algoritmo de *greedy forwarding* hasta que este llega al área destino. Una vez que el paquete llega a la región destino, se hace llegar a todos los nodos que se encuentran dentro de la zona utilizando inundación simple. Sin embargo, cuando la densidad de vehículos es elevada, la distribución del paquete mediante inundación simple puede generar una tormenta de colisiones a nivel MAC. Cuando la RSU envía un mensaje RA utilizando *geo-broadcasting* dentro de su área asignada, se pueden producir colisiones porque cuando los vehículos que se encuentran dentro del radio de cobertura de la RSU reciben el mensaje RA, estos intentan retransmitir el paquete *geo-broadcast* al mismo tiempo. Lo mismo ocurre cuando, utilizando el Servicio de Localización, se envía un mensaje *LS Request* buscando a un nodo destino y que es retransmitido en *broadcast* por los nodos intermedios. Cuando los nodos tratan de retransmitir el paquete al mismo tiempo se producen colisiones en el canal inalámbrico. Aunque en la especificación del protocolo de GN no se menciona nada al respecto, para evitar este comportamiento es necesario introducir un retardo de *broadcasting* de manera que los vehículos cuando reciben un paquete y tienen que retransmitirlo en *broadcast*, esperan un tiempo aleatorio antes de hacerlo. De esta manera, se distribuye temporalmente el acceso al medio para las diferentes retransmisiones del paquete y se evitan las colisiones.

Para analizar la influencia que tiene el retardo de *broadcasting* en el funcionamiento del protocolo de GN, se realizaron simulaciones en las que se activaba o se desactivaba este mecanismo.

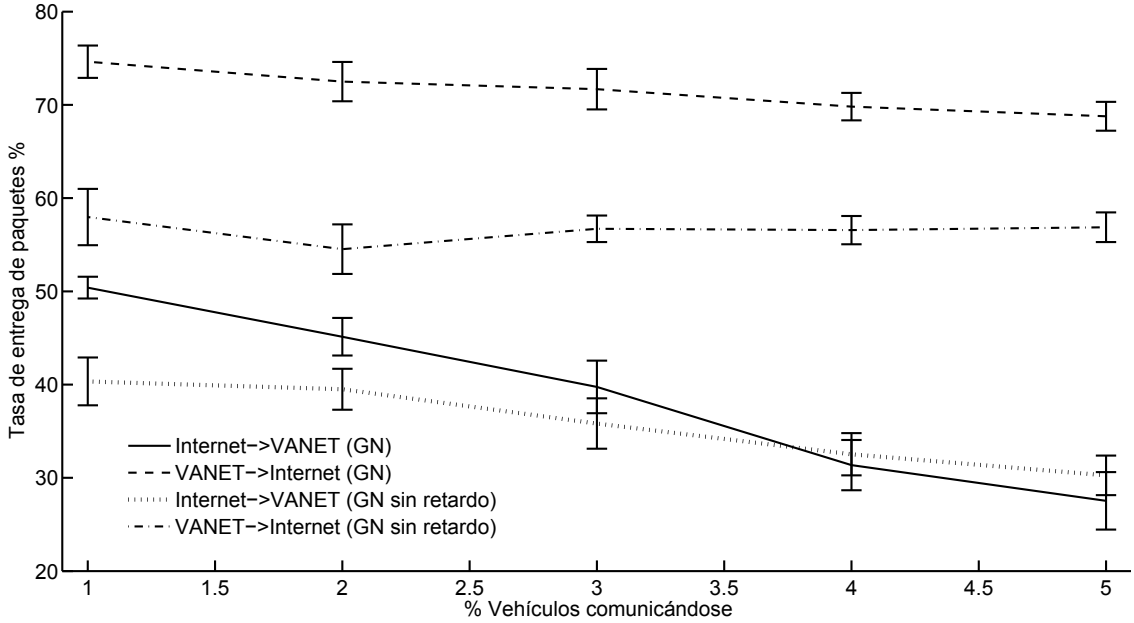


Figura 5.10: Tasa de entrega de paquetes del protocolo de GN estándar sin retardo de *broadcasting*.

La Figura 5.10 presenta los resultados de la tasa de entrega de paquetes para los flujos de datos en los sentidos Internet-VANET y VANET-Internet en función del porcentaje de vehículos que establecen comunicaciones con el CN. Cuando se desactiva el retardo de *broadcasting* se reduce la tasa de entrega de paquetes. Esta degradación tiene su origen en las colisiones producidas en el medio inalámbrico cuando todos los vehículos que se encuentran dentro del radio de cobertura de la RSU intentan retransmitir al mismo tiempo los paquetes RA que esta envía. Las colisiones provocan que los paquetes RA no puedan propagarse a más de un salto de la RSU con una alta probabilidad, de manera que los vehículos que no se encuentran en contacto directo con la RSU (se encuentran a más de un salto de la RSU) no pueden recibirlos. De esta forma, los vehículos no reciben información sobre la posición de la RSU hasta que llegan a situarse dentro de su radio de cobertura. Aunque nuestro escenario de simulación comprende una zona geográfica, gobernada por una RSU, nótese que este efecto es especialmente perjudicial cuando los vehículos cambian entre diferentes áreas gobernadas por diferentes RSUs. En ese caso, los vehículos no recibirán los mensajes RA de la RSU de la nueva zona geográfica hasta encontrase en contacto directo con ella (nótese que hasta que no se detecte la RSU de la nueva zona, el vehículo continuará utilizando como *router* de acceso a Internet la RSU de la zona antigua).

Asimismo, el hecho de que las colisiones provoquen el corte de la propagación de los mensajes RA por la VANET hace que los vehículos no puedan actualizar la información de posicionamiento de los vecinos en sus TLs. La desactualización de la información de las TLs provoca una degradación de prestaciones en el protocolo.

Además, como se mencionó anteriormente, el SL también se ve afectado. Las colisiones pro-

vocan que con una alta probabilidad, los mensajes *LS Request* no puedan propagarse más allá de un salto, haciendo que para poder obtener la posición del destino de los paquetes se realicen múltiples reintentos.

Por otro lado, puede apreciarse en la figura cómo en el sentido Internet-VANET, la diferencia de la tasa de entrega de paquetes cuando se aplica y no se aplica el retardo de *broadcasting* se reduce según aumenta el porcentaje de vehículos que se comunican con el CN (llegando a juntarse las líneas). Esto se debe a que las prestaciones del protocolo de GN con el retardo de *broadcasting* activado se van degradando conforme aumenta el porcentaje de vehículos que se comunican con el CN. En cambio, en el caso en el que se desactiva el retardo de *broadcasting*, el aumento del porcentaje de vehículos que se comunican con el CN no tiene tanta influencia porque las prestaciones son bajas de por sí para todos los porcentajes.

De estos resultados se puede desprender que la introducción del retardo de *broadcasting* es necesaria para el correcto funcionamiento del protocolo de GN, y por ello, se ha considerado su utilización en todas las simulaciones realizadas.

5.4.3. Problema de la detección de paquetes duplicados

Durante el análisis de las causas de la pérdida de paquetes en las simulaciones, se descubrió que una cantidad importante de paquetes se estaban descartando porque el mecanismo de detección de paquetes duplicados que se especifica en el estándar es demasiado simple. El mecanismo de detección de paquetes duplicados se aplica a los paquetes multisalto para evitar la formación de bucles en el encaminamiento y la posible recepción de múltiples copias del mismo paquete. El algoritmo de detección de paquetes duplicados funciona de la siguiente manera: cuando un nodo envía un paquete multisalto, se incluye un número de secuencia en el paquete que se incrementa cada vez que se envía un nuevo paquete. Por otro lado, los nodos almacenan en su TL el número de secuencia del último paquete no duplicado recibido de un nodo origen determinado. De esta manera, cuando un nodo recibe un paquete, este comprueba si se trata de un paquete duplicado comparando el número de secuencia incluido en el paquete con el valor almacenado en su TL. El paquete se considera como duplicado si el número de secuencia del paquete es menor que el almacenado en la TL (el paquete es más antiguo que el último que se ha recibido de ese nodo origen). El problema de este mecanismo tan simple es que si se reciben paquetes desordenados, estos se descartan porque se consideran duplicados cuando en realidad nunca han sido recibidos anteriormente, lo que contribuye a la degradación de la tasa de entrega de paquetes que el protocolo de GN puede alcanzar.

Aunque la especificación advierte de este problema con una nota, nuestras simulaciones revelaron que se reciben paquetes desordenados frecuentemente debido al entorno tan cambiante que presenta la VANET. Por lo tanto, se propone mejorar el mecanismo de detección de paquetes duplicados para que se mantenga no solo el número de secuencia del último paquete no duplicado

recibido de un nodo origen, sino que se almacene el número de secuencia de todos los paquetes que se han recibido recientemente. De esta manera se consigue que los paquetes sean considerados como duplicados solo si han sido recibidos con anterioridad[7].

5.4.4. Predicción de la posición geográfica de los vecinos

Diferentes trabajos en la literatura han estudiado el efecto negativo que tiene la desactualización de las rutas sobre los protocolos de encaminamiento en redes *ad hoc*, y en concreto, los errores en la información de la posición de los vecinos en protocolos de encaminamiento geográfico. En distintos trabajos [118–121] se ha analizado cómo la aplicación de mecanismos de predicción de posición ayuda a mejorar las prestaciones. Los errores en la información de posición de los vecinos están principalmente causados por la movilidad de los nodos de la red, por lo que el efecto tiene mayor relevancia cuando la movilidad de los nodos es elevada, como ocurre en el escenario de las redes vehiculares.

Cuando los nodos procesan los mensajes *beacon* o la cabecera de otros paquetes de GN, almacenan o actualizan información del nodo emisor (identificador del nodo, la posición geográfica actual, la dirección a la que se dirige, la velocidad, etc.) en la TL. Esta información se considera como válida durante un tiempo de caducidad, por lo que es posible que un nodo envíe paquetes a un vecino que, debido a la movilidad de los vehículos en la VANET, ya no sea alcanzable porque ha salido fuera del radio de cobertura. Para reducir el efecto de este problema se puede ajustar el tiempo de caducidad asociado a las entradas de la TL, tal y como se ha mencionado en la Sección 5.4.1, pero dado que no es posible ajustar un tiempo exacto para cada circunstancia, el problema seguirá existiendo.

Con la idea de evitar enviar paquetes a vecinos que debido a su movimiento han salido fuera del radio de cobertura, se introduce la utilización de un mecanismo de predicción de la posición geográfica que ocupan los vecinos [118]. Con este mecanismo, el algoritmo de *greedy forwarding* selecciona el siguiente salto teniendo en cuenta una predicción de la localización de los vecinos en lugar de la posición almacenada en la TL. La posición geográfica donde se estima que un nodo puede encontrarse se calcula con una operación muy sencilla a partir de su posición, velocidad y dirección almacenados en la TL: asumiendo que los nodos se mueven a velocidad constante, se estima la posición geográfica calculando su desplazamiento durante el tiempo que ha transcurrido desde la marca de tiempo de la entrada de la TL (instante en el que la posición, velocidad y dirección del vecino fue obtenida) hasta el momento actual [118]. De esta manera, los vecinos que se predice que se encuentran fuera del radio de cobertura no pueden ser seleccionados como siguiente salto por el algoritmo de *greedy forwarding*.

[7] Nótese que en el simulador se almacena el número de secuencia de todos los paquetes recibidos, pero esto no sería viable en la práctica. Una implementación real solamente almacenaría el número de secuencia de los paquetes que se han recibido recientemente.

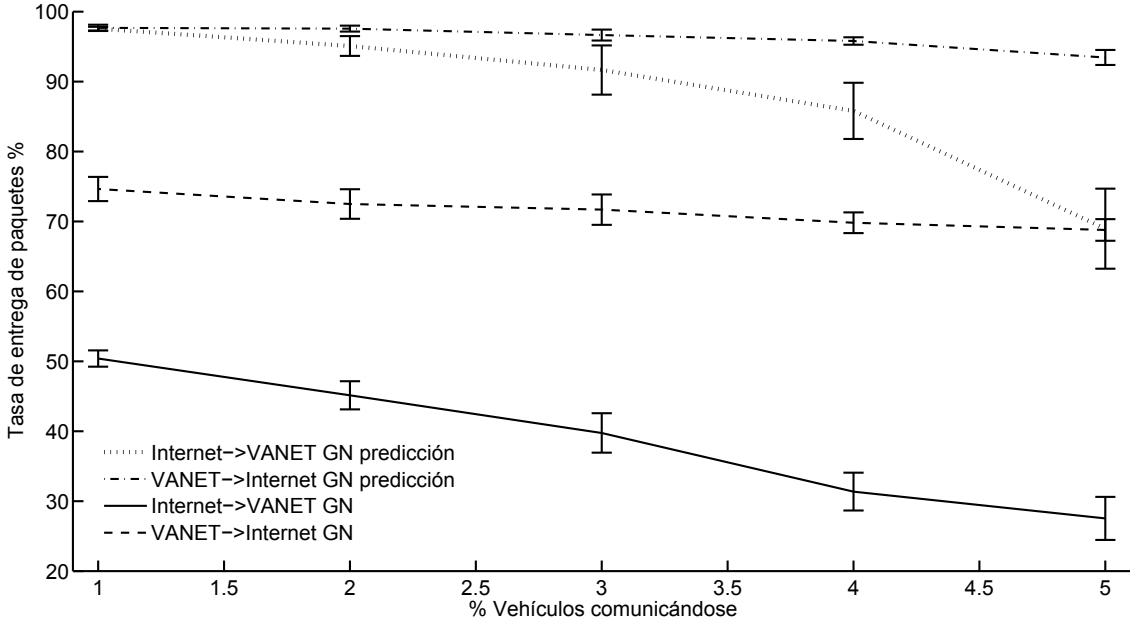


Figura 5.11: Tasa de entrega de paquetes del protocolo de GN con el mecanismo de predicción de la posición de los vecinos.

A continuación se analiza el impacto que tiene el mecanismo de predicción de la posición de los vecinos sobre el protocolo de GN. En la Figura 5.11 se muestra la tasa de entrega de paquetes para los flujos de datos, desde Internet a la VANET y desde la VANET a Internet, en función del porcentaje de vehículos que se comunican con el CN cuando se aplica el mecanismo de predicción de la posición geográfica de los vecinos. En la gráfica también se presentan los resultados del protocolo de GN estándar y como se mencionó anteriormente, el tiempo de caducidad de la TL se ha establecido a 6 segundos en ambos casos.

Comparando los resultados, se puede observar cómo la aplicación del mecanismo de predicción de la posición de los vecinos mejora en gran medida la tasa de entrega de paquetes del protocolo de GN en ambos sentidos de las comunicaciones (Internet-VANET y VANET-Internet). El mecanismo de predicción de la posición de los vecinos reduce la probabilidad de que el algoritmo de *greedy forwarding* seleccione vecinos inalcanzables. Sin embargo, la tasa de entrega de paquetes decrece conforme aumenta el porcentaje de vehículos que se comunican con el CN, sobre todo en el sentido Internet-VANET.

Este efecto viene producido en primer lugar porque al aumentar el tráfico de datos en la VANET, el medio inalámbrico tiene que ser compartido entre mayor cantidad de nodos tratando de comunicarse, lo que hace disminuir las prestaciones. Además, hay que tener en cuenta que resulta más fácil alcanzar a un nodo fijo como la RSU que a un vehículo que cambia su posición continuamente, de ahí que los flujos VANET-Internet cuenten con mayores facilidades que los flujos Internet-VANET. Por otro lado, los resultados de las simulaciones mostraron que una gran cantidad de pérdidas de paquetes en el sentido Internet-VANET se producen en la cola del nivel

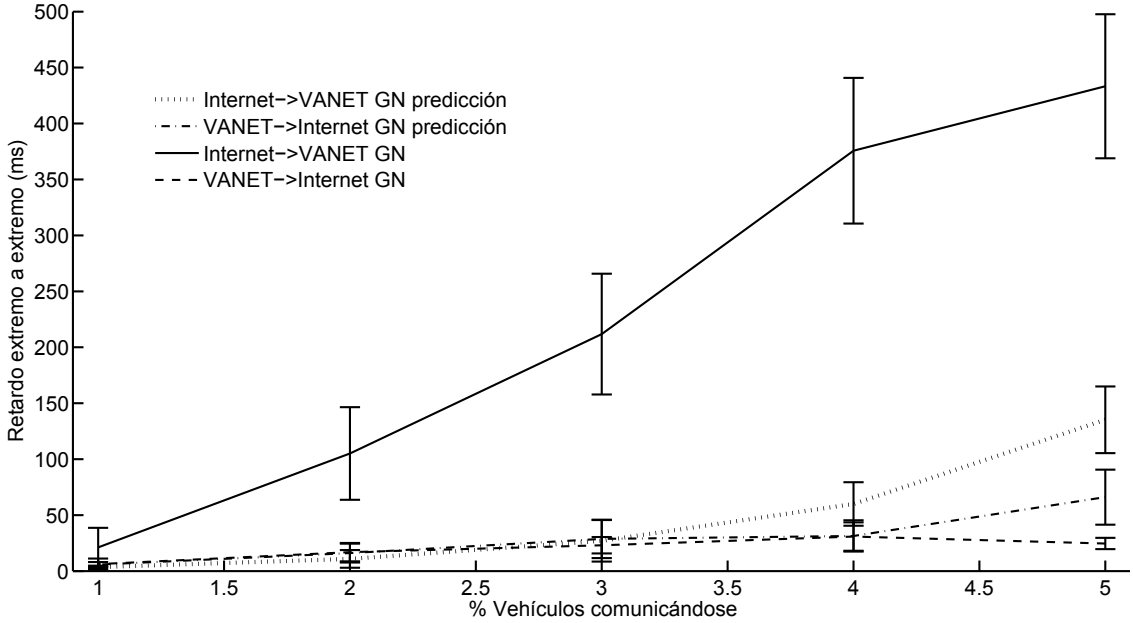


Figura 5.12: Retardo extremo a extremo del protocolo de GN con el mecanismo de predicción de la posición de los vecinos.

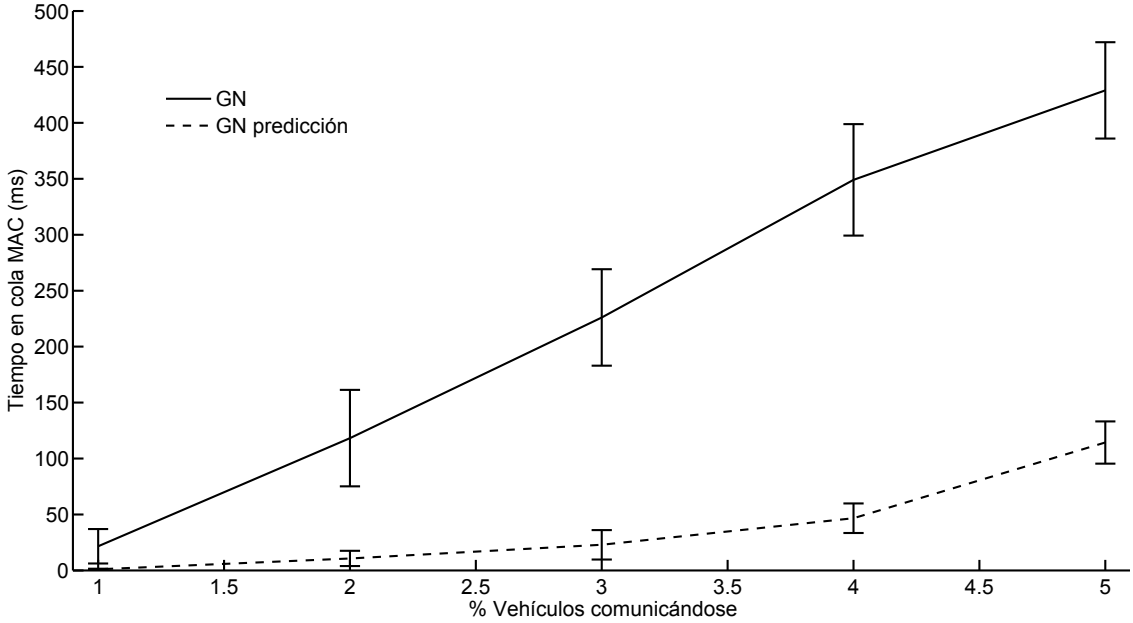


Figura 5.13: Tiempo en cola MAC en la RSU del protocolo de GN con el mecanismo de predicción de la posición de los vecinos.

MAC de la RSU. La RSU no puede reenviar todo el tráfico que recibe desde Internet y se satura según aumenta el porcentaje de vehículos que se comunican con el CN.

Las Figuras 5.12 y 5.13 muestran el retardo extremo a extremo y del tiempo que permanecen los paquetes en la cola del nivel MAC de la RSU respectivamente, en función del porcentaje de

vehículos que establecen comunicaciones con el CN. Como puede apreciarse, el mecanismo de predicción de la posición de los vecinos ayuda a disminuir el retardo extremo a extremo en el sentido Internet-VANET, que se debe en gran medida a que se reduce el tiempo que permanecen los paquetes en la cola de la capa MAC de la RSU. Centrándonos en la Figura 5.13, el tiempo que permanecen los paquetes en la cola MAC de la RSU aumenta con el porcentaje de vehículos que se comunican con el CN. Como la RSU tiene que cursar mayor cantidad de tráfico de datos, tiene que competir más veces por acceder al canal inalámbrico. Sin embargo, la RSU se encuentra en una posición de desventaja respecto a los vehículos ya que, aunque concentre el tráfico de datos de la VANET, tiene las mismas oportunidades que un vehículo de acceder al medio inalámbrico para transmitir los paquetes. De esta manera, la RSU llega a alcanzar una situación de saturación en la que los paquetes se descartan porque la cola del nivel MAC está llena. A pesar de esto, el mecanismo de predicción de la posición geográfica de los vecinos hace que la RSU pueda enviar mayor cantidad de tráfico y que las prestaciones mejoren dado que la selección de vecinos inalcanzables que contribuía a la saturación de la RSU se hace menos probable. Por otro lado, el problema de seleccionar vecinos inválidos como siguiente salto es más crítico cuando el tráfico de datos aumenta en la red: si por un error en la predicción se selecciona un vecino inválido, la capa MAC intentará enviar el paquete hasta siete veces [38] antes de descartarlo, lo que contribuye a aumentar la probabilidad de colisiones en el canal inalámbrico y el tiempo de espera de los paquetes en la cola del nivel MAC.

A la vista de estos resultados, se puede concluir que el mecanismo de predicción de la posición geográfica de los vecinos ayuda a mejorar las prestaciones del protocolo de GN de forma significativa.

5.4.5. Detección de Pérdida de Vecino

El mecanismo que se describe en esta sección, Detección de Pérdida de Vecino (DPV) sigue la misma idea que el mecanismo de predicción de la posición geográfica de los vecinos: evitar la pérdida de paquetes que se produce cuando el algoritmo de *greedy forwarding* selecciona vecinos inalcanzables como siguiente salto. Sin embargo, en vez de basarse en predicciones de posición que pueden ser erróneas en algunos casos, DPV se basa en el intercambio de información entre diferentes niveles de la pila de protocolos (*cross-layer*). Este tipo de optimizaciones en el que se intercambia información entre diferentes capas de la torre de protocolos son de gran utilidad en arquitecturas de protocolos para VANETs [122]. El funcionamiento de la DPV es el siguiente: cuando se descarta un paquete a nivel MAC porque el siguiente salto no es alcanzable (la capa MAC ha intentado enviar la trama hasta siete veces sin recibir un mensaje ACK de confirmación [38]), la capa MAC alerta al nivel de GN para que elimine al vecino inválido de la TL. De esta manera, el vecino inválido no se considera para transmisiones futuras y los paquetes pueden ser encaminados a través de otros vecinos disponibles en la TL evitando su pérdida. Además, existe una conexión de realimentación entre el nivel MAC y el nivel de GN de forma que, en vez

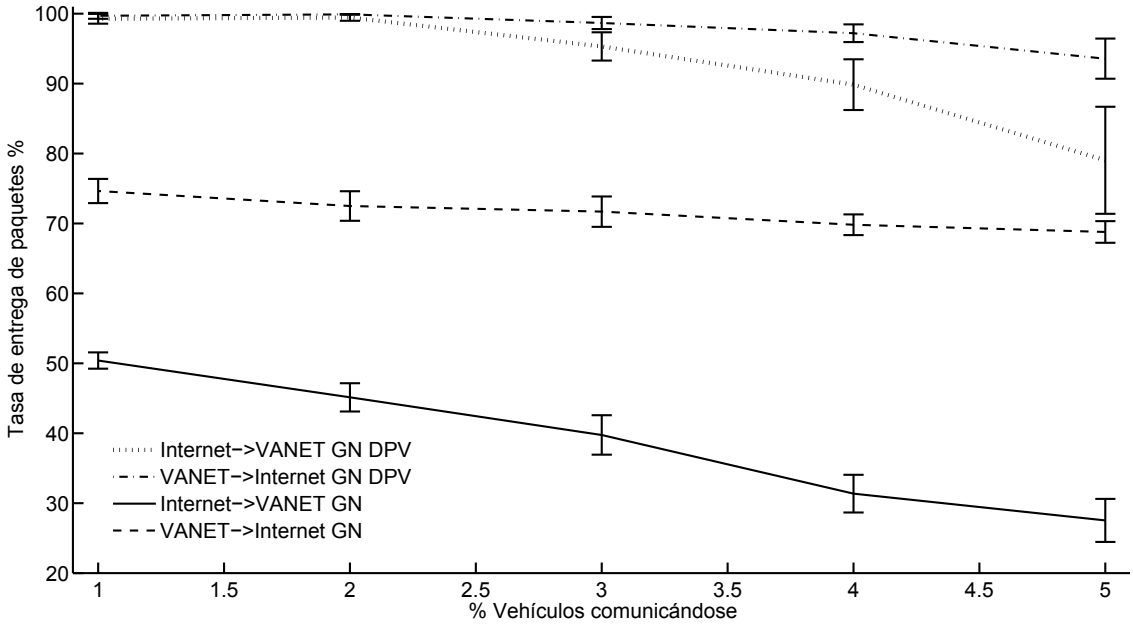


Figura 5.14: Tasa de entrega de paquetes del protocolo de GN con el mecanismo de la DPV.

de perder el paquete tras el séptimo intento de envío, este puede ser inyectado de nuevo en el nivel de GN para volver a ser encaminado.

A continuación se presentan los resultados de las simulaciones llevadas a cabo para estudiar el impacto de la DPV sobre el protocolo de GN. La Figura 5.14 presenta la tasa de entrega de paquetes para los flujos de tráfico de datos en ambos sentidos, desde Internet a la VANET y desde la VANET a Internet, frente al porcentaje de vehículos que establecen comunicaciones con el CN. Se muestran los resultados obtenidos tanto para el caso en el que se aplica el mecanismo de la DPV como para el protocolo de GN estándar. El tiempo de caducidad de la TL se ha fijado a 6 segundos en ambos casos.

Los resultados muestran cómo la DPV incrementa la tasa de entrega de paquetes significativamente. Cuando se encaminan paquetes con el mecanismo de la DPV, el nodo puede detectar a nivel de enlace si el siguiente salto no es alcanzable para eliminarlo de la TL y evitar usarlo para el encaminamiento de paquetes futuros. Sin embargo, de nuevo, la tasa de entrega de paquetes se reduce con el aumento del porcentaje de vehículos que se comunican con el CN, con mayor repercusión en el sentido Internet-VANET. Como se comentó en el análisis del mecanismo de predicción de la posición geográfica de los vecinos, esta reducción de prestaciones se produce porque el incremento de tráfico de datos en la VANET tiene como consecuencia que el canal inalámbrico tenga que ser compartido por mayor cantidad de nodos intentando comunicarse. Por otro lado, alcanzar un vehículo que se encuentra en movimiento es más problemático que entregar paquetes a un nodo fijo como la RSU, por lo que es lógico que la tasa de entrega de paquetes sea mayor en el sentido VANET-Internet que en el sentido Internet-VANET. Además, las medidas tomadas durante las simulaciones revelaron que una gran cantidad de paquetes de los flujos Internet-VANET

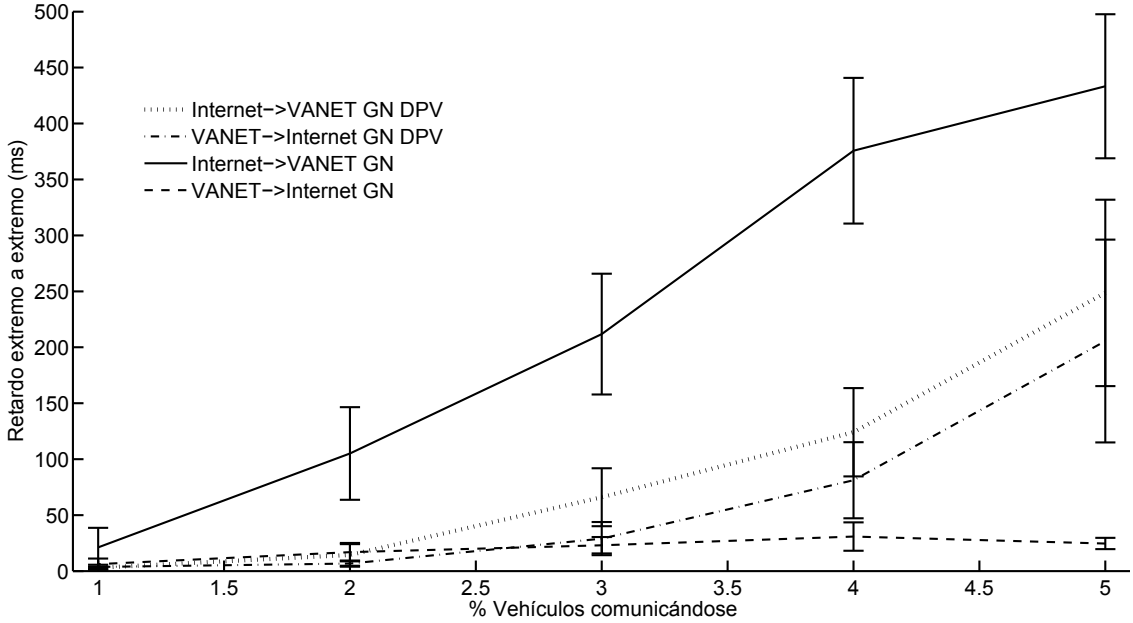


Figura 5.15: Retardo extremo a extremo del protocolo de GN con el mecanismo de la DPV.

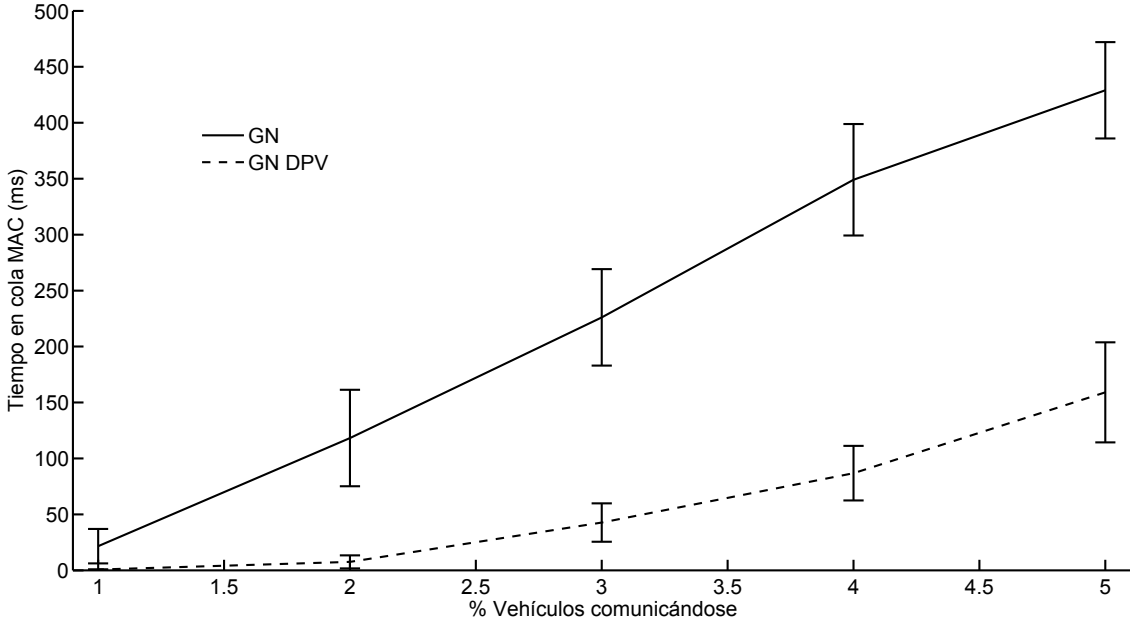


Figura 5.16: Tiempo en cola MAC de la RSU del protocolo de GN con el mecanismo de la DPV.

se descartaban en la cola del nivel MAC de la RSU. La RSU no puede cursar todo el tráfico que recibe desde Internet y se satura según aumenta el porcentaje de vehículos que se comunican con el CN.

El retardo extremo a extremo experimentado por los paquetes y el tiempo que estos permanecen en la cola de la capa MAC de la RSU en función del porcentaje de vehículos que se

comunican con el CN se presenta en las Figuras 5.15 y 5.16 respectivamente. Centrándonos en el retardo extremo a extremo, comparando el caso en el que se aplica el mecanismo de la DPV con el protocolo de GN estándar puede observarse cómo la DPV permite reducir el retardo extremo a extremo que sufren los paquetes en el sentido Internet-VANET[8]. Como se descartan los vecinos inválidos, no se realizan tantos intentos de transmisión inservibles, lo que permite a la RSU cursar mayor cantidad de tráfico. Esto se puede apreciar en la Figura 5.16, donde se observa que el tiempo que permanecen los paquetes en la cola MAC de la RSU se reduce considerablemente con la aplicación del mecanismo de la DPV. A pesar de esta mejora, el tiempo que permanecen los paquetes en cola de la RSU se incrementa con el aumento del porcentaje de vehículos que se comunican con el CN, llegando a un estado en el que la cola se llena y los paquetes se descartan. Como ya se ha comentado anteriormente, la explicación a este fenómeno se debe a que a pesar de que la RSU tiene que cursar más tráfico de datos que un vehículo (la RSU concentra el tráfico de datos de la VANET), comparte la misma probabilidad de obtener el canal inalámbrico para transmitir que los vehículos.

El mecanismo de la DPV tiene como ventaja sobre el mecanismo de predicción de la posición geográfica de los vecinos que, además de prevenir la pérdida de paquetes provocada por la selección de un vecino inalcanzable como siguiente salto, protege frente a pérdidas producidas por colisiones continuas en el canal inalámbrico. Cuando existe una carga elevada en la red, puede ocurrir que el paquete tenga que volver a retransmitirse continuamente (el nivel MAC intenta entregar el paquete hasta siete veces) y que finalmente se descarte porque, aunque el siguiente salto se encuentre dentro del radio de cobertura y sea alcanzable, las continuas colisiones hacen imposible entregárselo. Gracias a la conexión de realimentación entre el nivel MAC y el nivel de GN que introduce el mecanismo de la DPV, los paquetes pueden ser reencaminados evitando su pérdida.

Cabe mencionar que el problema de seleccionar vecinos inválidos como siguiente salto resulta más relevante cuando aumenta el tráfico de datos en la red debido a que el nivel MAC realiza hasta siete intentos de transmisión antes de detectar la pérdida del vecino e informar al protocolo de GN para que lo elimine de la TL. Bajo condiciones de saturación, el mecanismo de la DPV es un arma de doble filo. Por un lado, ayuda a mitigar el efecto de elegir vecinos inválidos y enviar constantemente paquetes a un vecino que no es alcanzable (lo que puede multiplicar la carga del canal inalámbrico por siete, ya que cada paquete se intenta entregar siete veces cuando no se consigue alcanzar al destino); y protege frente a la pérdida de paquetes producidas por colisiones continuas en el canal inalámbrico[9]. Sin embargo, por otro lado, la reinyección del paquete en el

[8]Nótese que la medida del retardo extremo a extremo puede resultar engañosa ya que el cálculo se realiza sobre aquellos paquetes que llegan a alcanzar el destino. De esta manera, puede darse el caso de que la tasa de entrega de paquetes sea muy baja y que los paquetes se entreguen en su mayoría a un salto, lo que proporcionará una medida de retardo extremo a extremo baja. Esto ocurre en la Figura 5.15, donde para porcentajes de vehículos que se comunican con el CN superiores al 3 %, el protocolo de GN estándar obtiene un retardo extremo a extremo menor que el obtenido cuando se utiliza el mecanismo de la DPV debido a que en el caso del protocolo de GN estándar, la mayoría de los paquetes se entregan a pocos saltos.

[9]Con el mecanismo de la DPV, cuando un paquete se descarta a nivel MAC debido a que se producen colisiones

nivel de GN para que vuelva a ser encaminado contribuye a aumentar todavía más el tráfico de datos en el canal inalámbrico, lo que puede provocar mayor probabilidad de colisión.

Finalmente, podemos concluir que el mecanismo de la DPV introduce grandes mejoras en el funcionamiento del protocolo de GN.

5.4.6. Combinación de los mecanismos de Detección de Pérdida de Vecino y de predicción de la posición geográfica de los vecinos

En las dos secciones anteriores se ha analizado el impacto de dos mecanismos que tienen la misma finalidad: combatir la selección como siguiente salto de vecinos inalcanzables por parte del algoritmo de *greedy forwarding* para mejorar las prestaciones del protocolo de GN. Esta sección se centra en el estudio de su interacción y se propone su combinación para optimizar el protocolo de GN.

Como los mecanismos de predicción de la posición geográfica de los vecinos y de la DPV afrontan el mismo problema siguiendo diferentes aproximaciones, se va proceder a comparar su impacto sobre el protocolo de GN tanto de forma independiente, como a estudiar su interacción cuando se combina su aplicación. En la Figura 5.17 se muestran los resultados de la tasa de entrega de paquetes de los flujos UDP CBR en ambos sentidos (de Internet a la VANET y de la VANET a Internet) en función del porcentaje de vehículos de la carretera que establecen comunicaciones con el CN. La Figura 5.18 compara los resultados del retardo extremo a extremo que experimentan los paquetes en la VANET. Se presentan los resultados de la aplicación del mecanismo de predicción de la posición geográfica de los vecinos y de la DPV de forma separada, y además, los del caso en el que se aplican conjuntamente. El tiempo de caducidad de la TL se ha establecido a 6 segundos en todos los casos.

Se puede apreciar en las gráficas que el mecanismo de la DPV consigue mejores resultados que la predicción de la posición de los vecinos en términos de la tasa de entrega de paquetes. En cambio, la situación se torna cuando se compara el retardo extremo a extremo de los paquetes: el mecanismo de predicción de la posición geográfica de los vecinos obtiene un retardo extremo a extremo menor. Esto se debe a que el mecanismo de la DPV evita descartar los paquetes cuando el siguiente salto ha salido fuera del radio de cobertura debido a su movimiento, pero el nivel MAC intenta enviar el paquete hasta siete veces antes de declarar al vecino como inalcanzable y notificar a la capa de GN para que lo elimine de la TL. De esta forma, se incrementa el retardo de encaminamiento y la carga en el canal inalámbrico, lo que hace que los resultados de retardo extremo a extremo del mecanismo de la DPV sean algo peores. Por otro lado, el mecanismo de predicción de la posición geográfica de los vecinos no introduce retardo adicional en el encaminamiento, pero puede darse el caso de que la predicción sea errónea y que se pierdan paquetes enviándolos a vecinos inalcanzables. En cambio, la conexión de realimentación del mecanismo de

continuamente, se reinyecta el paquete en el nivel de GN aumentando de esta manera el número de intentos de envío.

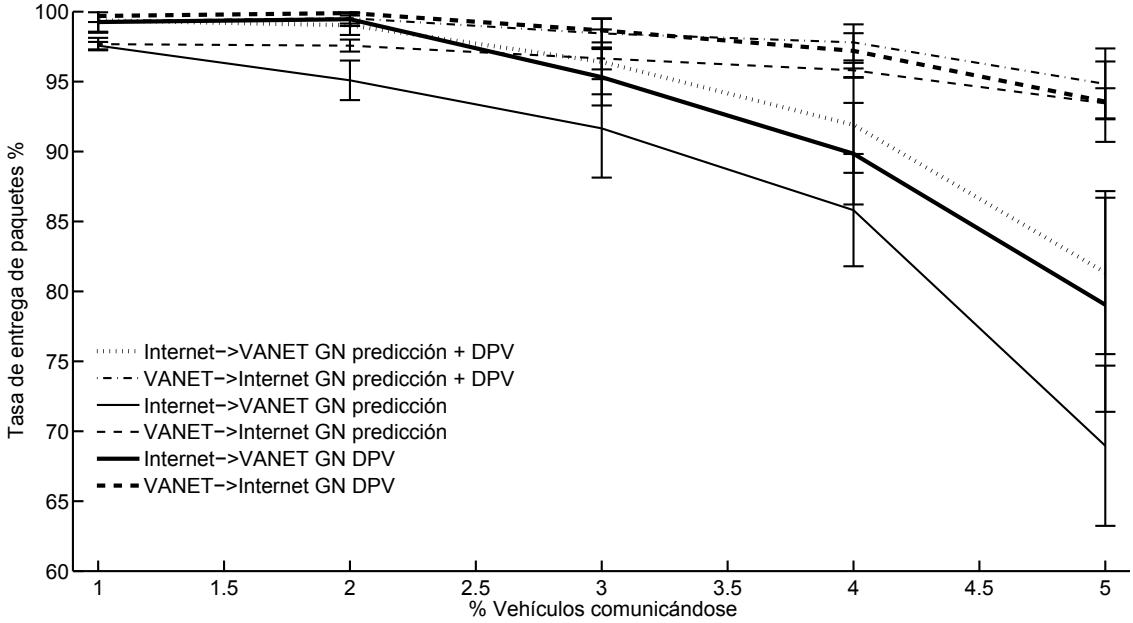


Figura 5.17: Tasa de entrega de paquetes de la combinación de los mecanismos DPV y de predicción de la posición geográfica de los vecinos.

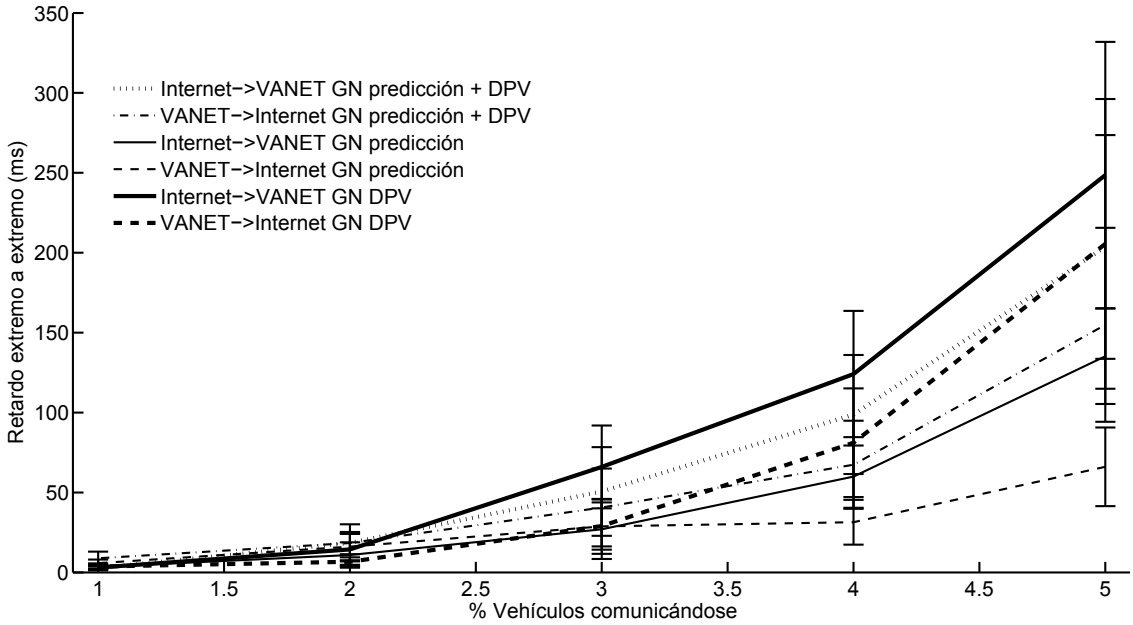


Figura 5.18: Retardo extremo a extremo de la combinación de los mecanismos DPV y de predicción de la posición geográfica de los vecinos.

la DPV permite volver a encaminar los paquetes evitando su pérdida. Por ello, la tasa de entrega de paquetes es algo mayor cuando se aplica el mecanismo de la DPV en comparación con el caso en el que se aplica el mecanismo de predicción de la posición geográfica de los vecinos.

Centrándonos en la combinación de ambos mecanismos, se puede ver que se trata del caso

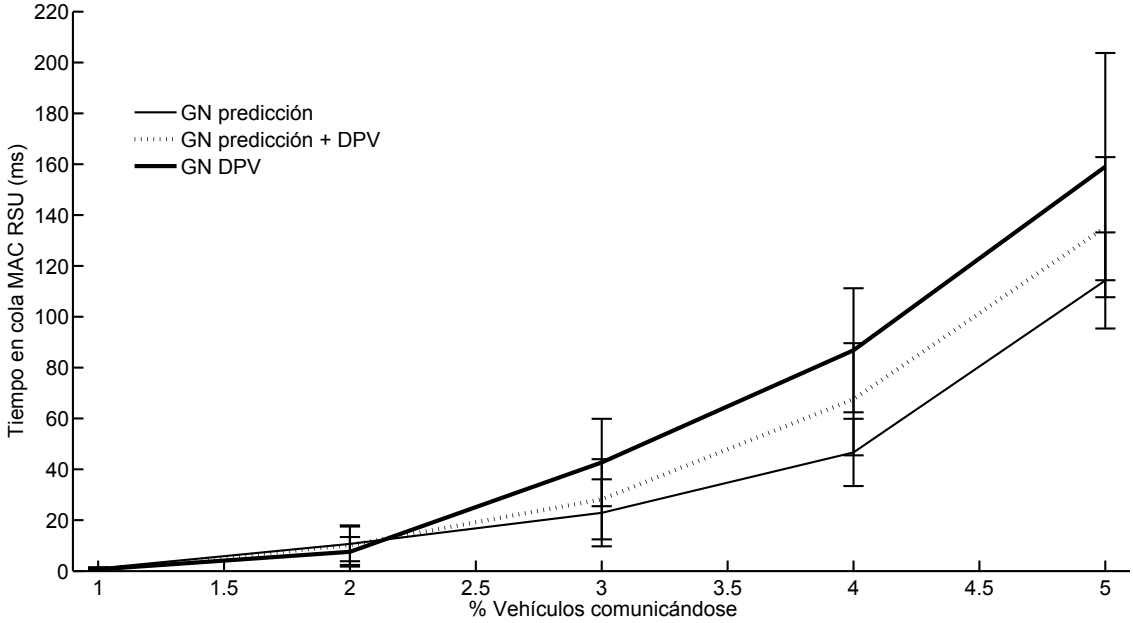


Figura 5.19: Tiempo en cola MAC en la RSU de la combinación de los mecanismos DPV y de predicción de la posición geográfica de los vecinos.

que mejor tasa de entrega de paquetes alcanza. Respecto al retardo extremo a extremo que experimentan los paquetes, los resultados de la combinación de ambos mecanismos se encuentran entre los obtenidos cuando se aplica el mecanismo de predicción de la posición geográfica de los vecinos y el caso en el que se utiliza DPV de forma separada. Esto se debe a que el mecanismo de predicción de la posición geográfica de los vecinos sirve como un primer filtro para descartar aquellos vecinos que se predice que son inalcanzables. Esto sirve para reducir el retardo de encaminamiento y la carga en el canal inalámbrico que introduce el mecanismo de la DPV cuando se selecciona un vecino inválido como siguiente salto (siete intentos de envío antes de declarar a un vecino como inválido). Por otro lado, si la predicción de la posición del vecino es errónea y se elige a un vecino inalcanzable como siguiente salto, el problema se soluciona con el mecanismo de la DPV que elimina al vecino de la TL, aunque para ello se introduzca algo de retardo adicional en el encaminamiento. Nótese que aunque los paquetes sufran más retardo, sin el mecanismo de la DPV se perderían.

Este comportamiento puede comprobarse también en la Figura 5.19 donde se representa el tiempo que permanecen los paquetes de datos en la cola del nivel MAC de la RSU. Cuando se aplica el mecanismo de la DPV, el tiempo en cola de los paquetes es mayor que en el caso del mecanismo de predicción de la posición geográfica de los vecinos. Esto se debe a que, mientras que con el mecanismo de predicción de la posición geográfica de los vecinos no se introduce ningún retardo en el encaminamiento de los paquetes, para que la DPV considere a un vecino como inalcanzable se realizan hasta siete intentos de envío a nivel MAC, lo que además de incrementar la probabilidad de colisión en el medio inalámbrico debido al aumento de carga, supone un retardo

adicional de encaminamiento para el resto de paquetes que esperan en la cola del nivel MAC. Cuando se combinan ambos mecanismos, el tiempo en cola de los paquetes obtenido se sitúa entre los dos casos anteriores. El mecanismo de predicción de la posición de los vecinos permite descartar vecinos inválidos y evita el retardo adicional que introduce la DPV. Sin embargo, cuando la predicción falla y se elige un vecino inalcanzable como siguiente salto, se evita descartar los paquetes con el mecanismo de la DPV a expensas de introducir retardo en el encaminamiento, lo que hace aumentar el tiempo que los paquetes permanecen en la cola del nivel MAC.

Cabe mencionar que como se introdujo anteriormente, el mecanismo de la DPV protege frente a las pérdidas de paquetes que pueden venir provocadas por dos causas: 1) El algoritmo de *greedy forwarding* selecciona como siguiente salto a un vecino que ha salido fuera del radio de cobertura y por lo tanto es inalcanzable. 2) Las continuas colisiones en el canal inalámbrico cuando la carga en la red es elevada que provocan que el paquete tenga que volver a retransmitirse continuamente (el nivel MAC realiza hasta siete intentos para entregar el paquete) y que finalmente se descarte porque, aunque el siguiente salto se encuentre dentro del radio de cobertura y sea alcanzable, las continuas colisiones hacen imposible entregárselo. Gracias a la conexión de realimentación que introduce el mecanismo de la DPV entre el nivel MAC y el nivel de GN los paquetes pueden ser reencaminados evitando su pérdida.

Las Figuras 5.20 y 5.21 muestran la cantidad de paquetes (en tanto por ciento respecto al número de paquetes enviados totales a nivel de aplicación) que se reinyectan en el nivel de GN para volver a ser encaminados cuando el nivel MAC determina que el siguiente salto es inalcanzable (eliminando también el vecino de la TL). Se diferencia entre las dos causas descritas previamente: el paquete se reinyecta debido a que el siguiente salto es inalcanzable (Figura 5.20) o el paquete se reinyecta debido a que tras siete intentos, el nivel MAC no ha podido entregarlo al siguiente salto por las continuas colisiones en el canal inalámbrico (Figura 5.21). Se ha considerado el caso en el que únicamente se aplica el mecanismo de la DPV y el caso en el que se combinan la DPV y el mecanismo de predicción de la posición geográfica de los vecinos.

Puede observarse que se producen muchas más reinyecciones de paquetes debido a colisiones continuas en el canal inalámbrico que a la selección de vecinos inválidos por parte del algoritmo de *greedy forwarding*. Además, la diferencia entre ambos casos se amplía rápidamente cuando se incrementa el porcentaje de vehículos que establecen comunicaciones con el CN, lo que indica la gran influencia que tiene la carga del canal inalámbrico y las colisiones para las prestaciones de la VANET.

Centrándonos en la Figura 5.20, se producen menor cantidad de reinyecciones en el caso en el que se combinan ambos mecanismos, que cuando se aplica únicamente el mecanismo de la DPV. Esto se debe a que el mecanismo de predicción de la posición geográfica de los vecinos ayuda a reducir los casos en los que se eligen vecinos inalcanzables como siguiente salto. Sin embargo, existen casos en los que la predicción falla y los paquetes terminan reinyectándose para encaminarlos nuevamente. Por otro lado, la cantidad de paquetes que se reinyectan se incrementa

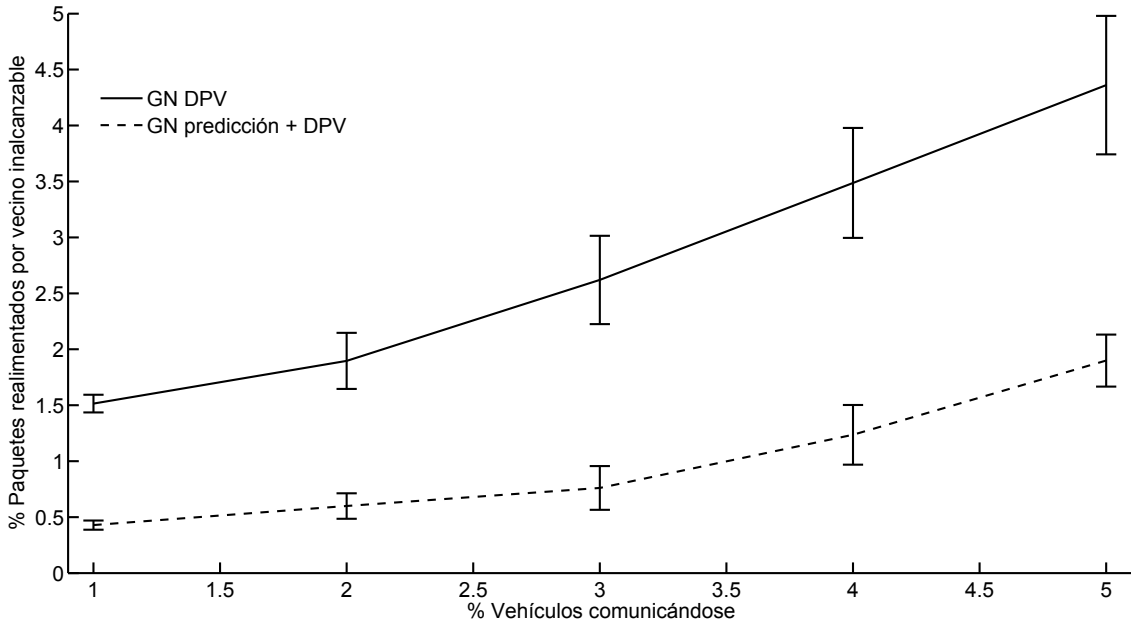


Figura 5.20: Paquetes realimentados por vecino inalcanzable.

cuando aumenta el porcentaje de vehículos que se comunican con el CN. La explicación a este efecto radica en que según aumenta el tráfico en la red, aumenta la probabilidad de colisión. Esto hace que haya nodos que no puedan actualizar correctamente la posición de sus vecinos porque los paquetes de señalización no pueden ser recibidos por todos los nodos. En otras palabras, las colisiones provocan una degradación en el refresco de la posición de los vecinos en las TLs, lo que a su vez provoca más fallos en la predicción.

Si se observa la Figura 5.21, la cantidad de reinyecciones producidas por colisiones continuas aumenta con el porcentaje de vehículos que se comunican con el CN. Al aumentar el tráfico de datos en la red, se incrementa la carga del canal inalámbrico y la probabilidad de colisión es mayor. De hecho se llegan a valores cercanos al 100 %, lo que significa que, debido a las colisiones continuas que se producen en el canal inalámbrico, es difícil entregar un paquete al destino sin que tenga que ser reinyectado por el mecanismo de la DPV en alguno de los nodos que forman la cadena de encaminamiento desde el origen hasta el destino (puede darse el caso en el que un paquete tenga que ser realimentado múltiples veces en el mismo nodo). Esto pone de manifiesto la gran influencia que tiene la carga del canal inalámbrico sobre la degradación de las prestaciones. Por otro lado, mencionar que los resultados relativos a la combinación de los mecanismos se sitúan ligeramente por debajo de los obtenidos en el caso en el que únicamente se aplica el mecanismo de la DPV, lo que indica que la probabilidad de colisión es algo inferior. Este comportamiento se debe a que, gracias al mecanismo de predicción de la posición geográfica de los vecinos, se reducen los casos en los que se elegiría un vecino inalcanzable, lo que provocaría mayor sobrecarga en el medio inalámbrico porque el nivel MAC retransmitiría estos paquetes hasta siete veces antes de que el mecanismo de la DPV eliminara el vecino de la TL y reinyectara

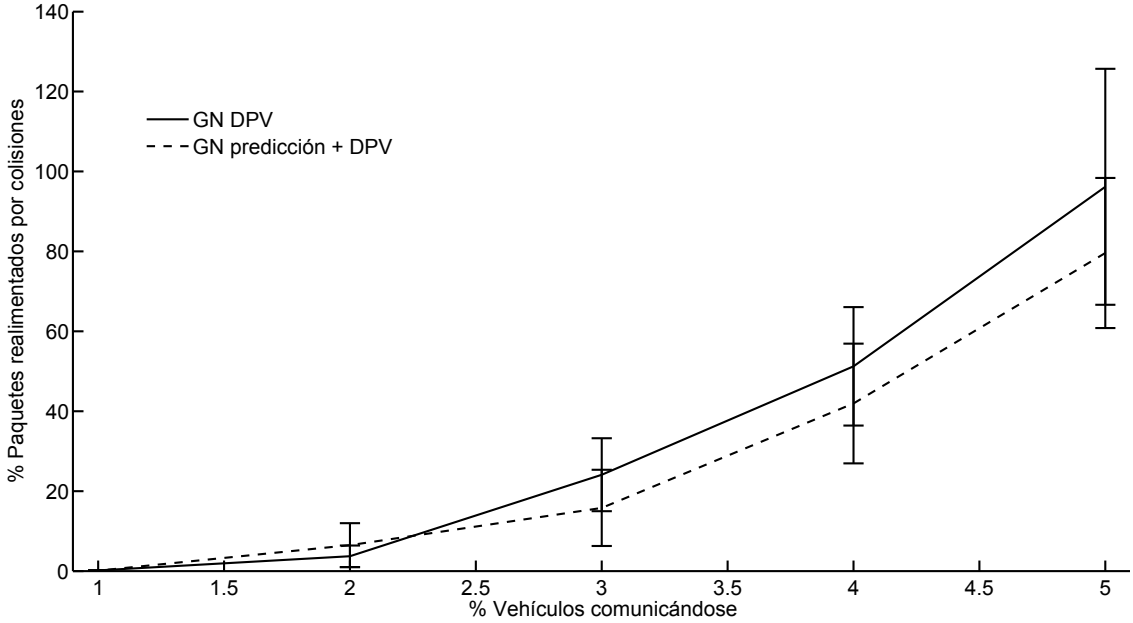


Figura 5.21: Paquetes realimentados por colisiones continuas.

el paquete en el nivel de GN. Cabe mencionar que además se produce un círculo vicioso en el que cuanto mayor es la probabilidad de colisión, más se degrada la información de la TL de los nodos (los nodos no pueden actualizar correctamente la posición de sus vecinos porque los paquetes de señalización colisionan y se pierden). A su vez, esto produce más fallos en la predicción, lo que hace que se incremente más la probabilidad de colisión porque el nivel MAC intentará enviar el paquete hasta siete veces antes de que el mecanismo de la DPV lo reinyecte en el nivel GN y elimine al vecino de la TL.

Como se ha comentado, el mecanismo de predicción de la posición geográfica de los vecinos ayuda a reducir los casos en los que se elegiría un vecino inalcanzable, lo que provocaría mayor sobrecarga en el medio inalámbrico porque el nivel MAC retransmitiría estos paquetes hasta siete veces antes de que el mecanismo de la DPV eliminara el vecino de la TL y reinyectara el paquete en el nivel de GN. Se podría pensar que las prestaciones mejorarían siendo más conservadores con la predicción de la posición de los vecinos mediante la introducción de un margen de guarda, de manera que el algoritmo de *greedy forwarding* no considerara aquellos vecinos que se predice que están fuera de un radio de cobertura efectivo o radio de cobertura de predicción. Es decir, a pesar de que el radio de cobertura real sigue siendo el mismo (200 metros), el algoritmo de *greedy forwarding* no considera aquellos vecinos que se predice que están fuera del radio de cobertura de predicción. Por lo tanto, cuanto menor sea el radio de predicción, menor será la probabilidad de que se elija un vecino inalcanzable como siguiente salto. Sin embargo, los resultados de la Figura 5.22 muestran un efecto que merece la pena mencionar. En esta figura se presenta la tasa de entrega de paquetes cuando se combinan los mecanismos de la DPV y de la predicción de la posición geográfica de los vecinos, en los sentidos Internet-VANET y VANET-Internet. Se

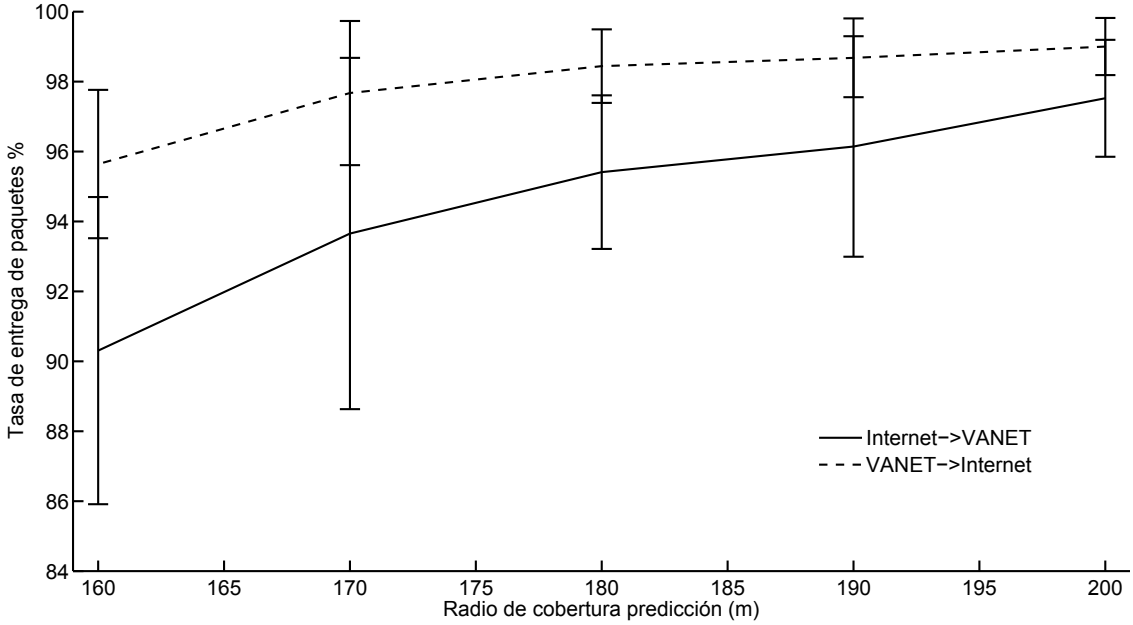


Figura 5.22: Tasa de entrega de paquetes en función del radio de cobertura del mecanismo de predicción de la posición geográfica de los vecinos.

ha considerado el caso en el que el 3 % de los vehículos se comunican con el CN y se varía el radio de cobertura efectivo considerado por el mecanismo de predicción de la posición geográfica de los vecinos. Como se puede apreciar, la tasa de entrega de paquetes decrece sensiblemente cuando el radio de cobertura de predicción se reduce. Por un lado, un radio de cobertura de predicción más pequeño reduce la probabilidad de realizar una predicción errónea, lo que ayuda a evitar la sobrecarga en el medio inalámbrico cuando se selecciona un vecino inalcanzable y el nivel MAC retransmite el paquete siete veces antes de que el mecanismo de la DPV actúe. Sin embargo, existe otro efecto con mayor peso. Si se reduce el radio de cobertura efectivo, los paquetes tienen que realizar más saltos para llegar al destino, lo que finalmente provoca que el número de transmisiones en el medio inalámbrico aumente y que por lo tanto, la probabilidad de colisión sea mayor. Esto se traduce en la degradación de prestaciones observada en la figura.

5.4.7. Protocolo de *GeoNetworking* mejorado o protocolo *Enhanced GeoNetworking*

En las secciones anteriores se han descrito y analizado diferentes mecanismos que pueden aplicarse en el protocolo de GN para mejorar sus prestaciones. De aquí en adelante, se hace referencia a la aplicación de estos mecanismos sobre el protocolo de GN como el protocolo *Enhanced* GN (EGN) o protocolo de GN mejorado. El protocolo EGN incluye la aplicación de los mecanismos de predicción de la posición geográfica de los vecinos combinada con el mecanismo de la DPV y la mejora del mecanismo de detección de paquetes duplicados. A continuación se realiza

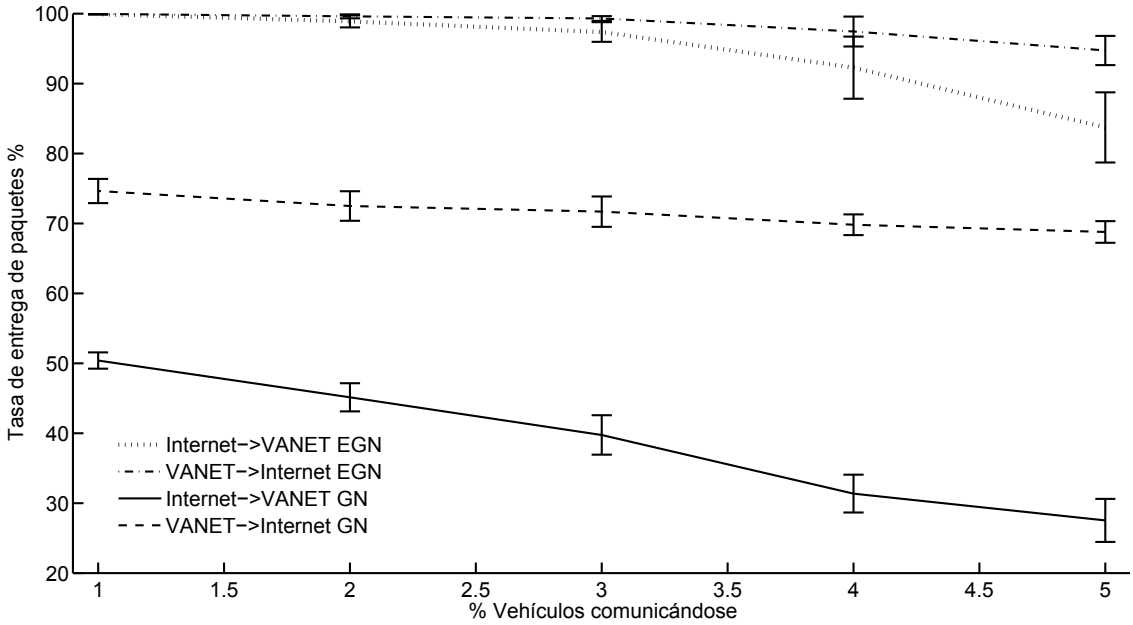


Figura 5.23: Tasa de entrega de paquetes EGN versus GN.

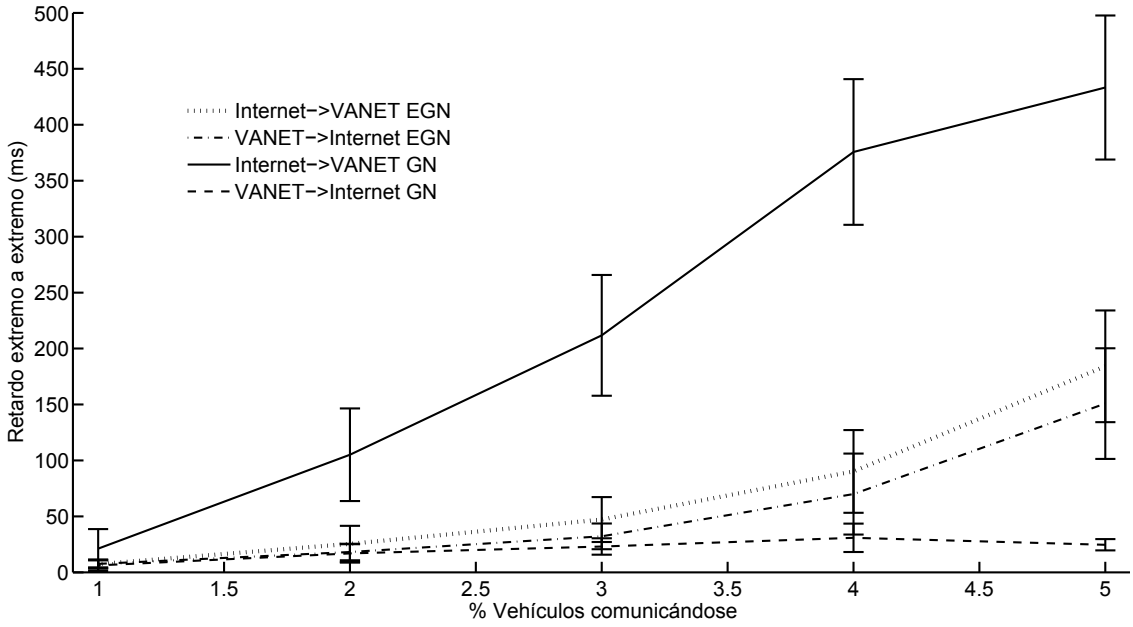


Figura 5.24: Retardo extremo a extremo EGN versus GN.

una comparación entre las prestaciones del protocolo EGN y el protocolo de GN estándar.

Las Figuras 5.23 y 5.24 muestran la comparación entre la tasa de entrega de paquetes y el retardo extremo a extremo de los paquetes alcanzados por los protocolos EGN y GN estándar en función del porcentaje de vehículos del tramo de carretera que establecen comunicaciones con el CN. El tiempo de caducidad de la TL se ha establecido a 6 segundos en ambos casos. Puede

apreciarse cómo el protocolo EGN mejora las prestaciones del protocolo de GN, alcanzando valores de tasa de entrega de paquetes cercanos al 100 % para ambos sentidos de la comunicación, Internet-VANET y VANET-Internet, cuando el porcentaje de vehículos que se comunican con el CN es bajo. Sin embargo, cuando el porcentaje de vehículos que se comunican con el CN se incrementa por encima del 3 %, se produce una degradación tanto en la tasa de entrega de paquetes como en el retardo extremo a extremo, que sobre todo se aprecia en el sentido Internet-VANET[10]. Esta degradación se produce por diferentes razones: 1) La saturación de la RSU. El tiempo que permanecen los paquetes en la cola de la capa MAC de la RSU se incrementa con el porcentaje de vehículos que se comunican con el CN (véase la Figura 5.19) porque cuanto mayor es la cantidad de tráfico que la RSU tiene que cursar, más veces tiene que competir por el medio inalámbrico para poder transmitir. Sin embargo, aunque la RSU concentra el tráfico de datos de la VANET, tiene la misma probabilidad de acceder al canal inalámbrico que cualquier vehículo. Esto provoca que la RSU alcance un estado de saturación en el que los paquetes se descartan porque la cola del nivel MAC se llena. Sin embargo, como se puede ver en la figura, la RSU puede cursar mayor cantidad de tráfico con el protocolo EGN porque la combinación del mecanismo de la DPV y el mecanismo de predicción de la posición geográfica de los vecinos reduce el severo efecto que produce seleccionar vecinos inalcanzables como siguiente salto (la selección de vecinos inválidos contribuye a la saturación de la cola del nivel MAC). 2) El problema de seleccionar vecinos inalcanzables como siguiente salto es más crítico cuando se incrementa el tráfico de datos en la red porque el nivel MAC intenta enviar un paquete hasta siete veces antes de ejecutar el mecanismo de la DPV. En una situación de saturación, el mecanismo de la DPV es un arma de doble filo. Por un lado, reduce el impacto de seleccionar vecinos inválidos y enviar constantemente paquetes a un vecino que no es alcanzable (lo que puede multiplicar la carga del canal inalámbrico por siete, ya que cada paquete se intenta entregar siete veces cuando no se consigue alcanzar al destino); y protege frente a la pérdida de paquetes producidas por colisiones continuas en el canal inalámbrico[11]. Sin embargo, por otro lado, la reinyección del paquete en el nivel de GN para que vuelva a ser encaminado contribuye a aumentar todavía más la carga del canal inalámbrico, lo que puede provocar mayor probabilidad de colisión.

Por último mencionar que con relación al análisis de las prestaciones del protocolo EGN en función de la posición de la RSU respecto al sentido del movimiento de los vehículos de la VANET, las simulaciones realizadas mostraron que la tasa de entrega de paquetes es similar en ambas fases (cuando los vehículos que se comunican con el CN viajan acercándose hacia la

[10]Nótese que la medida del retardo extremo a extremo puede resultar engañosa ya que el cálculo se realiza sobre aquellos paquetes que consiguen alcanzar el destino. De esta manera, puede darse el caso de que la tasa de entrega de paquetes sea muy baja y que los paquetes se entreguen en su mayoría a un salto, lo que proporcionará una medida de retardo extremo a extremo baja. Esto ocurre en la Figura 5.24, donde para porcentajes de vehículos que se comunican con el CN superiores al 3 %, el protocolo de GN estándar obtiene un retardo extremo a extremo menor que el protocolo EGN debido a que en el caso del protocolo de GN, la mayoría de los paquetes que consiguen entregarse realizan pocos saltos (véase la Figura 5.23).

[11]Con el mecanismo de la DPV, cuando un paquete se descarta a nivel MAC debido a que se producen colisiones continuamente, se reinyecta el paquete en el nivel de GN aumentando de esta manera el número de intentos de envío.

RSU y cuando los vehículos que se comunican con el CN se mueven alejándose de la RSU). La aplicación de los mecanismos de predicción de la posición geográfica de los vecinos y DPV evitan que el algoritmo de *greedy forwarding* seleccione como siguiente salto a vecinos que salen fuera del radio de cobertura, lo que se produce en mayor medida en la fase en la que los vehículos se alejan de la RSU. Por ello, la aplicación de estos mecanismos hace que las prestaciones de ambas fases se igualen.

5.4.8. Borrador de la nueva versión del estándar de *GeoNetworking*

Recientemente el comité técnico del sistema de transporte inteligente del ETSI, *European Telecommunications Standards Institute Technical Committee Intelligent Transport System* (ETSI TC ITS) [107] ha publicado un borrador de la nueva versión del estándar del protocolo *GeoNetworking* (GN) [110]. Este borrador introduce diferentes modificaciones que están principalmente orientadas a mejorar el funcionamiento del protocolo en aplicaciones destinadas a la seguridad vial, en las que es común la distribución de mensajes utilizando *geo-broadcasting*. Nuestro objetivo en esta sección es evaluar el impacto que tienen las modificaciones introducidas en el borrador en los escenarios en los que se proporciona a los vehículos conectividad a Internet.

A continuación se resume brevemente las variaciones más relevantes que se han introducido en el borrador de la nueva versión del estándar:

- **Nuevo algoritmo de *geo-broadcasting*:** aunque en la primera versión del estándar aparecía una primera aproximación a diferentes alternativas para protocolos de *geo-broadcasting* avanzados, por defecto el algoritmo utilizado era el ya mencionado "*Simple Geo-broadcast forwarding algorithm with line forwarding*". En el borrador de la nueva versión del estándar, se especifica más en detalle un algoritmo avanzado de *geo-broadcasting* que es el que se utiliza por defecto. Este algoritmo avanzado de *geo-broadcasting* combina mecanismos utilizados en CBF (para reducir la pérdida de paquetes debido al movimiento de los vehículos) y *greedy forwarding* (que complementa a CBF para minimizar el retardo de encaminamiento). Además, se mejora la eficiencia eligiendo a los nodos que retransmiten los paquetes dentro de un sector circular (se discriminan ciertos nodos por lo que se reduce el número de retransmisiones) y se aumenta la fiabilidad de la entrega de los paquetes mediante un proceso de retransmisiones controlado.
- **Prevención de ataques de denegación de servicio:** se define un mecanismo que tiene como objetivo evitar ataques de denegación de servicio mediante inundación de la red. Este mecanismo controla la tasa máxima de paquetes que puede enviar un nodo de manera que, si un nodo supera este límite, sus paquetes no son reenviados por los vecinos. Así, se evita que un nodo fraudulento pueda congestionar la red mediante el envío incontrolado de mensajes, aunque la congestión provocada a los vecinos directos no puede evitarse. Además, se

define un área máxima para los paquetes *geo-broadcast* de forma que los paquetes no son reenviados si su zona objetivo es demasiado grande. Cabe mencionar que estos parámetros deberían ser dimensionados correctamente ya que, en escenarios en los que se conecta la VANET a Internet por medio de RSUs, las RSUs concentran el tráfico y pueden llegar a enviar una gran cantidad de paquetes. Un mal dimensionamiento de los parámetros de este mecanismo podría limitar la conectividad de las RSUs.

- **Cambio en las cabeceras del protocolo:** uno de los cambios más importantes y que puede tener más impacto en las prestaciones del protocolo es la eliminación de la información de posicionamiento del último nodo que transmite el paquete de la cabecera de los mensajes. De esta forma, los nodos dejan de poder actualizar su TL con la información de posición de sus vecinos cuando reciben cualquier tipo de paquete de GN y únicamente pueden hacerlo cuando reciben un paquete *beacon* o *single hop broadcast*. Así, la reinicialización del temporizador de *beaconing* cuando se envían otros paquetes de GN (véase la Sección 5.4.2.1) deja de tener sentido, excepto cuando se transmiten paquetes *single hop broadcast*. Además, se han reordenado algunos de los campos de la cabecera del protocolo. En el Apéndice A se puede comprobar los cambios realizados en las cabeceras del protocolo de GN en el borrador de la nueva versión del estándar.

- **Nuevo algoritmo de detección de paquetes duplicados:** se ha modificado el algoritmo de detección de paquetes duplicados para, además de realizar un control sobre el último número de secuencia recibido de un determinado nodo origen, supervisar la marca de tiempo incluida en el paquete. El objetivo de este cambio es evitar errores que se han detectado en pruebas de campo con prototipos: cuando una CCU se reiniciaba debido a un error de *software*, se producían cambios en el número de secuencia que provocaba que algunos paquetes no fueran detectados como duplicados cuando en realidad sí que lo eran. Este comportamiento se evita mediante el análisis de la marca de tiempo de los paquetes. Sin embargo, el borrador de la nueva versión del estándar sigue manteniendo el problema mencionado en la Sección 5.4.3, los paquetes que se reciben desordenados se consideran duplicados.

Para evaluar el impacto de los cambios introducidos en el borrador de la nueva versión del estándar que pueden afectar a escenarios en los que se proporciona conectividad a Internet a los vehículos, se modificó la implementación del protocolo de GN de nuestro simulador para incluir aquellos cambios que pueden tener más impacto sobre el envío de paquetes *geo-unicast*: principalmente los cambios en la cabecera del protocolo y el nuevo algoritmo de detección de paquetes duplicados entre otros pequeños cambios, como la modificación de algunas constantes del protocolo.

Las Figuras 5.25 y 5.26 presentan la comparación de la tasa de entrega de paquetes y del retardo extremo a extremo experimentado por los paquetes entre las versiones del protocolo de GN estándar V1.1.1 y la del borrador, la versión V1.2.1. Se muestran los resultados para los

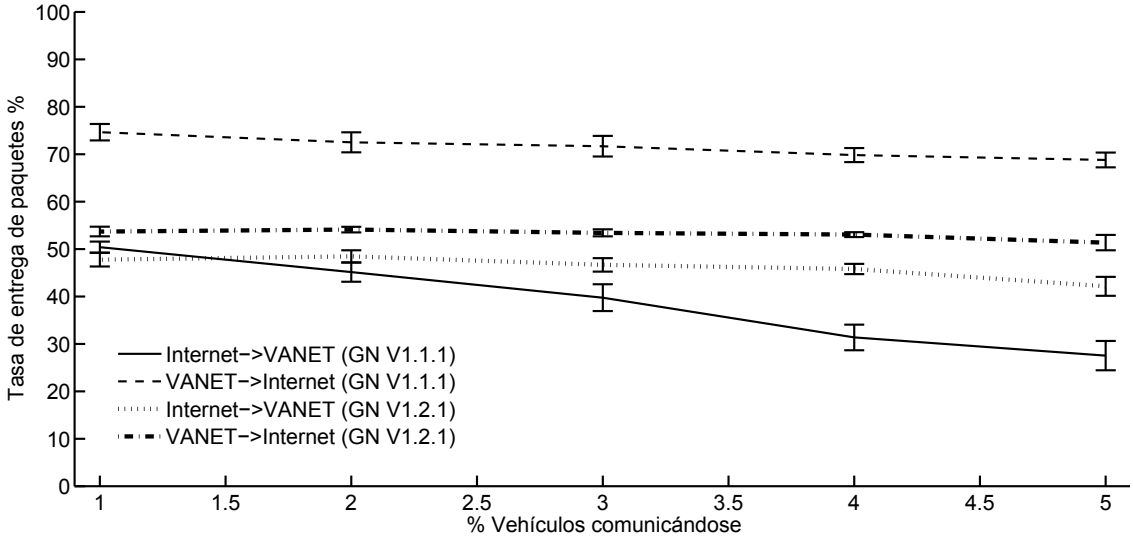


Figura 5.25: Tasa de entrega de paquetes del protocolo de GN estándar V1.1.1 versus borrador V1.2.1

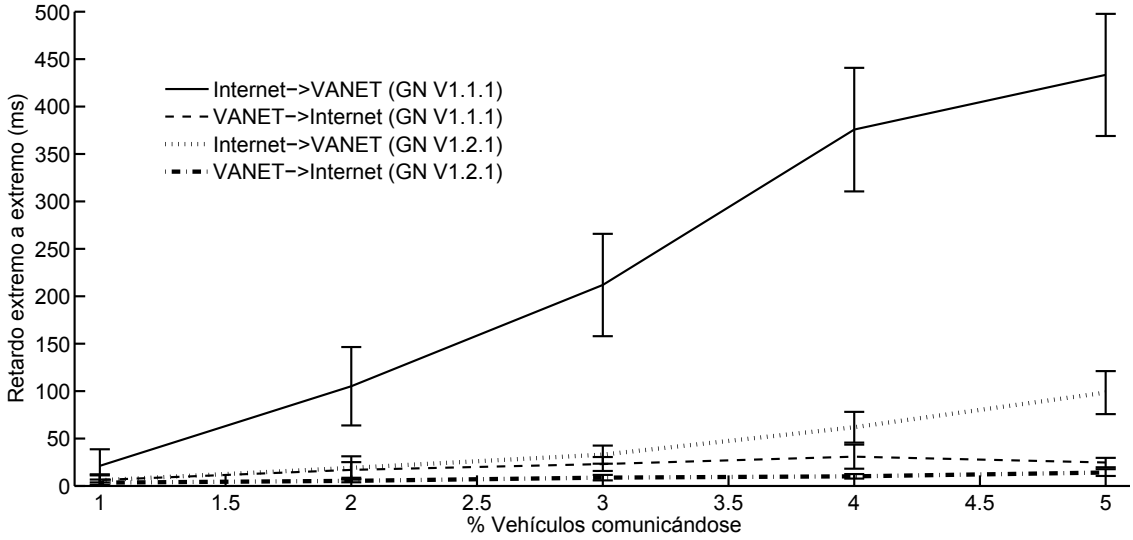


Figura 5.26: Retardo extremo a extremo del protocolo de GN estándar V1.1.1 versus borrador V1.2.1

flujos de datos de Internet a la VANET y vice versa, cuando se varía el porcentaje de vehículos que establecen comunicaciones con el CN. El tiempo de caducidad de la TL se ha establecido a 6 segundos en ambos casos, tal como se mencionó en la Sección 5.4.1. Como puede apreciarse en las figuras, en el sentido Internet-VANET, las modificaciones introducidas en el borrador de la nueva versión del estándar hacen mejorar las prestaciones: mejora la tasa de entrega de paquetes y disminuye considerablemente el retardo extremo a extremo. Sin embargo, en el sentido contrario, de la VANET a Internet, se concluye lo contrario, las nuevas modificaciones degradan la tasa de entrega de paquetes significativamente. La explicación a este comportamiento surgió tras un

profundo análisis de los resultados de las simulaciones. Los cambios en la cabecera del protocolo de GN en el borrador de la nueva versión hacen que los nodos únicamente puedan actualizar su TL con el procesamiento de los mensajes *beacon* recibidos. En cambio, en la versión V1.1.1, existen más fuentes de información para actualizar la TL, ya que cualquier paquete de GN recibido contiene información de posicionamiento del nodo que lo ha retransmitido. Esto ocurre sobre todo con los paquetes datos, que hacen que se actualice muy frecuentemente la posición de los vecinos de los que se recibe tráfico, lo que provoca una tendencia a que se mantengan los mismos nodos como mejores vecinos para llegar al destino. La reducción de posibilidades de actualizar la TL con los cambios del borrador de la nueva versión provoca que la tasa de entrega de paquetes en el sentido VANET-Internet disminuya haciendo que los paquetes se descarten antes de llegar a vecinos próximos a la RSU. Como consecuencia, el canal inalámbrico en las inmediaciones de la RSU se encuentra menos congestionado por lo que la probabilidad de colisión es menor y la RSU puede cursar mayor cantidad de tráfico en el sentido Internet-VANET. Es decir, el tiempo que los paquetes permanecen en la cola del nivel MAC de la RSU es menor, lo que hace que la RSU se congestione menos y se descarten menos paquetes. Esto explica que la tasa de entrega de paquetes y el retardo extremo a extremo mejoren en el sentido Internet-VANET.

Respecto a la modificación del algoritmo de detección de paquetes duplicados, mencionar que los cambios introducidos no han tenido ninguna repercusión sobre los resultados de las simulaciones. Como se mencionó anteriormente, los paquetes que llegan desordenados se siguen considerando como paquetes duplicados y por lo tanto, se descartan.

Un aspecto que cabe mencionar del funcionamiento del borrador de la nueva versión del estándar en función de la posición de la RSU respecto al sentido de movimiento de los vehículos de la VANET, es que las simulaciones realizadas mostraron que las prestaciones se desploman cuando los vehículos que se comunican con el CN se alejan de la RSU. La restricción de que los vehículos únicamente puedan actualizar su TL ante la recepción de mensajes *beacon* de los vecinos tiene un gran impacto cuando los vehículos que se comunican con el CN se alejan de la RSU, lo que hace que el protocolo llegue a ser inoperativo.

Por otro lado, las Figuras 5.27 y 5.28 muestran la tasa de entrega de paquetes y el retardo extremo a extremo considerando el protocolo EGN y el protocolo EGN cuando se le aplican las modificaciones introducidas en el borrador de la nueva versión del estándar, la versión V1.2.1. Las gráficas presentan los resultados para ambos sentidos de la comunicación, de Internet a la VANET y de la VANET a Internet, en función del porcentaje de vehículos que se comunican con el CN. De acuerdo con la Sección 5.4.1, el tiempo de caducidad de la TL se ha fijado a 6 segundos en ambos casos. Como se puede extraer de las figuras, la limitación de que los nodos únicamente puedan actualizar su TL ante la recepción de mensajes *beacon* degrada las prestaciones del protocolo EGN.

Como conclusión, las modificaciones introducidas en el borrador de la nueva versión del estándar, al estar especialmente orientadas a mejorar el funcionamiento del protocolo en aplica-

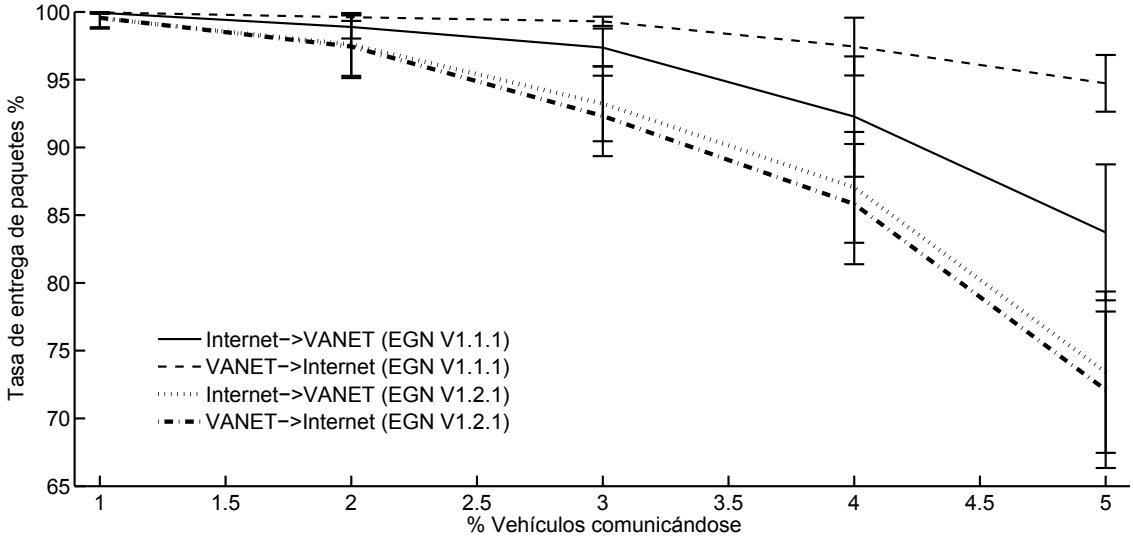


Figura 5.27: Tasa de entrega de paquetes EGN V1.1.1 versus borrador V1.2.1

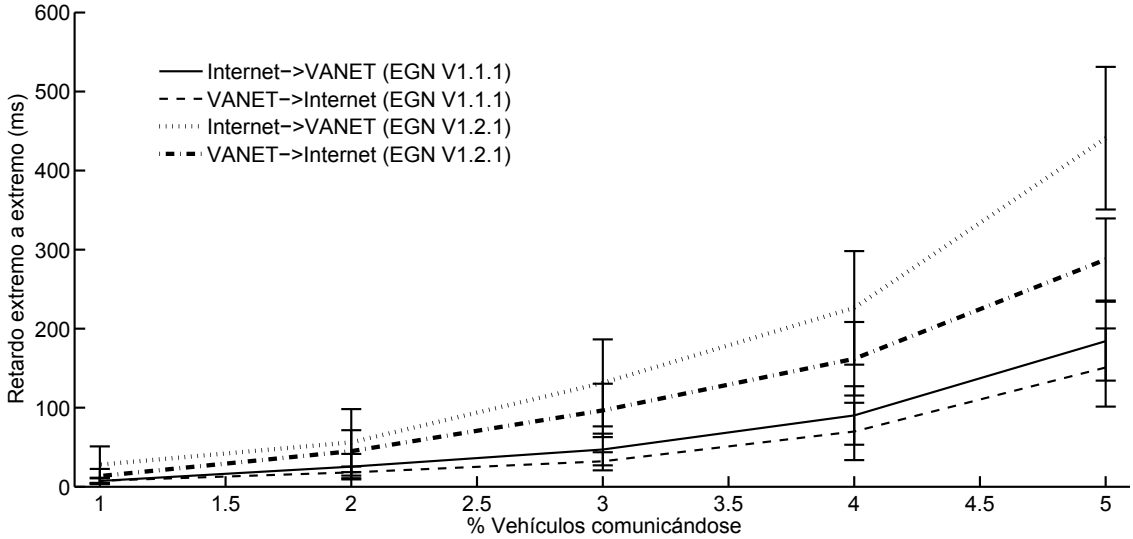


Figura 5.28: Retardo extremo a extremo EGN V1.1.1 versus borrador V1.2.1

ciones destinadas a la seguridad vial (donde es común utilizar *geo-broadcasting*), y en particular la eliminación de la información de posicionamiento del último nodo que transmite el paquete de la cabecera de los mensajes, tienen un impacto negativo sobre las prestaciones del protocolo cuando se utiliza para comunicaciones entre los vehículos e Internet (donde se utiliza *geo-unicast* para el envío de paquetes). Los nodos ya no pueden obtener información de posición de sus vecinos cuando reciben otros paquetes de GN, lo que limita las fuentes de información con las que se puede actualizar la TL a la recepción de mensajes *beacon* o paquetes *single hop broadcast*. Además, los nodos ya no pueden reinicializar el temporizador de *beaconing* cuando se envían otros paquetes de GN (excepto para paquetes *single hop broadcast*). En nuestra opinión, las ca-

beceras del protocolo de GN deberían incluir la información del mensaje *beacon* en todos los paquetes porque por un lado, posibilita que los nodos obtengan información de posicionamiento más precisa de sus vecinos y, por otro lado, mediante la reinicialización del temporizador de *beaconing* cuando se envían otros paquetes de GN, se reduce la carga de señalización en la red. De hecho, como se observó en la Sección 5.4.2.1, en nuestro escenario el mecanismo de *beaconing* deja de actuar (e introducir sobrecarga de señalización) por su solapamiento con la distribución de los mensajes RA.

De aquí en adelante, estas modificaciones se dejan a un lado ya que por el momento se trata de un borrador que todavía está bajo revisión y los resultados de las simulaciones muestran que las prestaciones empeoran.

5.4.9. Tráfico de datos unidireccional

Se ha estudiado también el comportamiento de los protocolos de GN estándar y EGN cuando únicamente existen comunicaciones unidireccionales desde la VANET a Internet o vice versa. La Figura 5.29 presenta la tasa de entrega de paquetes cuando el tráfico de datos es unidireccional desde los vehículos de la VANET hacia Internet, sin que exista ningún flujo de datos desde Internet a la VANET durante las simulaciones. El caso complementario donde únicamente se tiene tráfico de datos desde Internet a la VANET, se encuentra también representado en la Figura 5.29. Se ha medido la tasa de entrega de paquetes en función del porcentaje de vehículos de la VANET que se comunican con el CN considerando el uso del protocolo de GN estándar y del protocolo EGN.

En el caso en el que el tráfico se dirige únicamente desde la VANET a Internet, la tasa de entrega de paquetes alcanzada por los protocolos de GN estándar y EGN se puede considerar lógica teniendo en cuenta el análisis realizado previamente cuando el tráfico de datos era bidireccional. Sin embargo, nótese que hay que ser precavido cuando se comparan los resultados obtenidos en simulaciones en las que se tiene tráfico de datos unidireccional y simulaciones en las que el tráfico es bidireccional ya que las condiciones de carga de tráfico del canal inalámbrico son diferentes. De hecho, la tasa de entrega de paquetes aumenta ligeramente en el caso unidireccional respecto al caso bidireccional porque la cantidad de tráfico de datos en la red es menor (el tráfico de datos es la mitad que en el caso bidireccional). El protocolo EGN alcanza una tasa de entrega de paquetes cercana al 100 % mientras que el protocolo de GN estándar obtiene una tasa de entrega de paquetes alrededor del 76 %.

Se puede decir lo mismo cuando los paquetes se dirigen de forma unidireccional desde Internet a la VANET (sin tráfico de datos desde la VANET a Internet). El protocolo EGN obtiene una tasa de entrega de paquetes cercana al 100 % mientras que el protocolo de GN estándar alcanza una tasa de entrega de paquetes alrededor del 47 % en el mejor caso simulado.

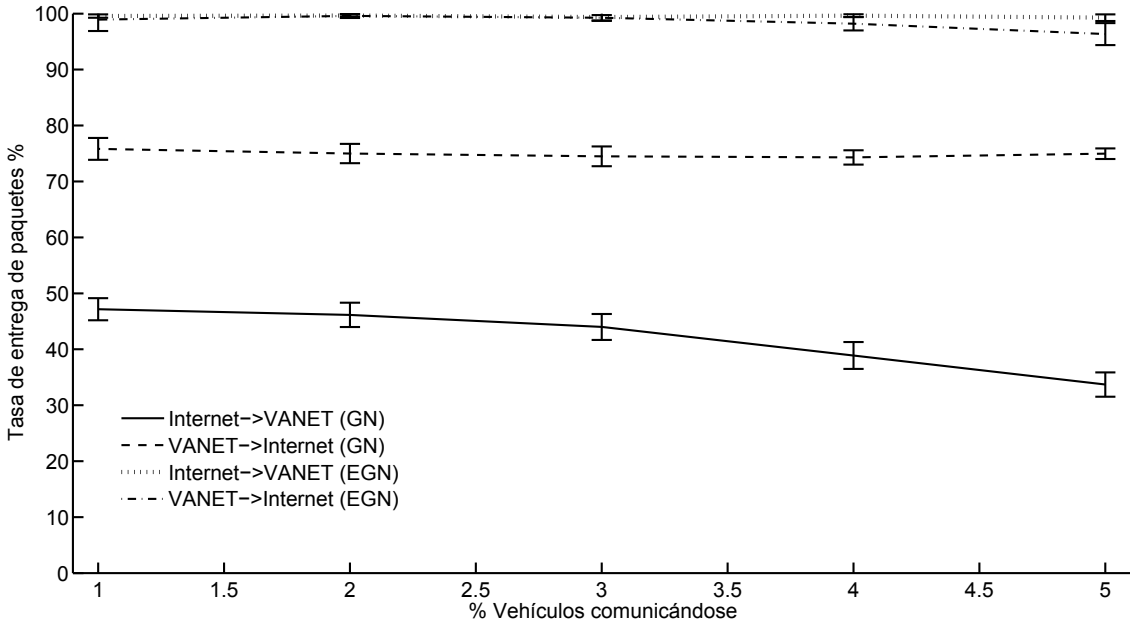


Figura 5.29: Tasa de entrega de paquetes tráfico unidireccional (Tiempo de caducidad TL = 6 segundos).

5.4.10. Mecanismo de *keep-alive* para el Servicio de Localización

Durante el análisis del protocolo de GN con tráfico unidireccional se descubrió un aspecto que resulta interesante mencionar: en el caso en el que el tráfico es unidireccional desde Internet a la VANET, el Servicio de Localización (SL) produce una sobrecarga de señalización en la red considerable porque la RSU necesita descubrir la posición geográfica del destino de cada flujo continuamente. La RSU utiliza la posición geográfica del destino de los paquetes que se encuentra almacenada en la TL hasta que el tiempo de caducidad de su entrada en la TL expira. De esta manera, una vez que la entrada de un destino ha expirado, el siguiente paquete que llega del CN dirigido a este destino, provocará el lanzamiento del SL (ya no se dispone de información en la TL). Como consecuencia, la RSU lanza el SL cada vez que se elimina la entrada del destino de cada uno de los flujos de la TL porque su tiempo de caducidad expira. Nótese que cuando el tráfico es bidireccional, el SL no se lanza periódicamente porque el tráfico de datos en el sentido VANET-Internet mantiene actualizada la posición del vehículo en la TL de la RSU, por lo que la RSU siempre conoce con precisión dónde se encuentran los vehículos que establecen comunicaciones con Internet.

Por lo tanto, cuando tenemos tráfico unidireccional desde Internet a la VANET, cuanto más corto sea el tiempo de caducidad de las entradas de la TL, mayor será la sobrecarga en la red que produce la difusión de los mensajes *LS Request* en busca de los vehículos destino. Además, si el tiempo de caducidad de las entradas de la TL se reduce, el algoritmo de *beaconing* (o los mensajes RA que se envían en *geo-broadcast*) debería enviar paquetes de control más frecuentemente para

actualizar la TL de los nodos, lo que incrementaría aún más la sobrecarga de señalización en la red.

En cambio, si el tiempo de caducidad es alto, la sobrecarga de señalización será menor, pero es posible que la RSU encamine los paquetes a una posición geográfica desactualizada donde el destino no sea alcanzable porque se ha movido. Esto provocaría la pérdida de los paquetes hasta que la entrada del destino en la TL de la RSU expirase y el SL se lanzara de nuevo para descubrir la posición actual del destino.

Nótese que los problemas que se mencionan arriba solamente ocurren en el escenario en el que el tráfico de datos es unidireccional desde Internet a la VANET. En el caso complementario, cuando el tráfico se envía desde la VANET a Internet, estos problemas no aparecen porque la RSU es un nodo fijo y los vehículos, que mandan los paquetes de datos a la RSU para llegar a Internet, siempre conocen su posición geográfica. Además, los vehículos refrescan la entrada de la RSU en su TL ante la recepción de los mensajes RA que distribuye la RSU periódicamente utilizando *geo-broadcast*. De esta manera, una vez que los vehículos descubren la localización de la RSU, no utilizan el SL para obtener su posición geográfica.

Con el objetivo de solucionar estos problemas, proponemos un mecanismo de *keep-alive* para el Servicio de Localización que resulta útil en escenarios en los que el tráfico de datos es unidireccional desde Internet a la VANET para 1) mitigar la sobrecarga de señalización en la red producida por el SL y 2) evitar la pérdida de paquetes por errores de encaminamiento cuando se utiliza información obsoleta sobre la posición geográfica del destino de los paquetes.

El mecanismo de *keep-alive* para el Servicio de Localización se basa en refrescar en la RSU la información de posicionamiento de los vehículos destino de los flujos de datos. Esto se consigue mediante el envío de unos mensajes *keep-alive* que actualizan en la RSU las entradas de la TL de aquellos vehículos que se comunican con un CN. El protocolo de GN del ETSI especifica un tipo de mensaje que encaja perfectamente con este propósito: el mensaje *LS Reply*, que incluye la posición geográfica del nodo origen del mensaje y que se envía mediante *geo-unicast* al destino (el mensaje *LS Request* se envía mediante *broadcast*/inundación, lo que consume más recursos del canal inalámbrico). El mecanismo de *keep-alive* para el Servicio de Localización funciona de la siguiente manera. Cuando un vehículo recibe un paquete de datos de la RSU, se establece un temporizador de *keep-alive* que controla el envío de mensajes *LS Reply* dirigidos a la RSU. El vehículo envía un mensaje *LS Reply* cada periodo de *keep-alive* para actualizar su entrada en la TL de la RSU (en las simulaciones el periodo de *keep-alive* se ha establecido a 3 segundos). De esta forma, la RSU puede enviar los paquetes de datos a la posición actualizada del vehículo. Además, con la intención de evitar una sobrecarga innecesaria en la red, si el vehículo envía un paquete de datos a la RSU, el temporizador de *keep-alive* se reinicializa porque este paquete actualiza la entrada del vehículo en la TL de la RSU. Si el vehículo deja de recibir paquetes de datos de la RSU, se cesa el envío de mensajes *LS Reply*.

Para comparar la sobrecarga de señalización introducida por el mecanismo de *keep-alive* para

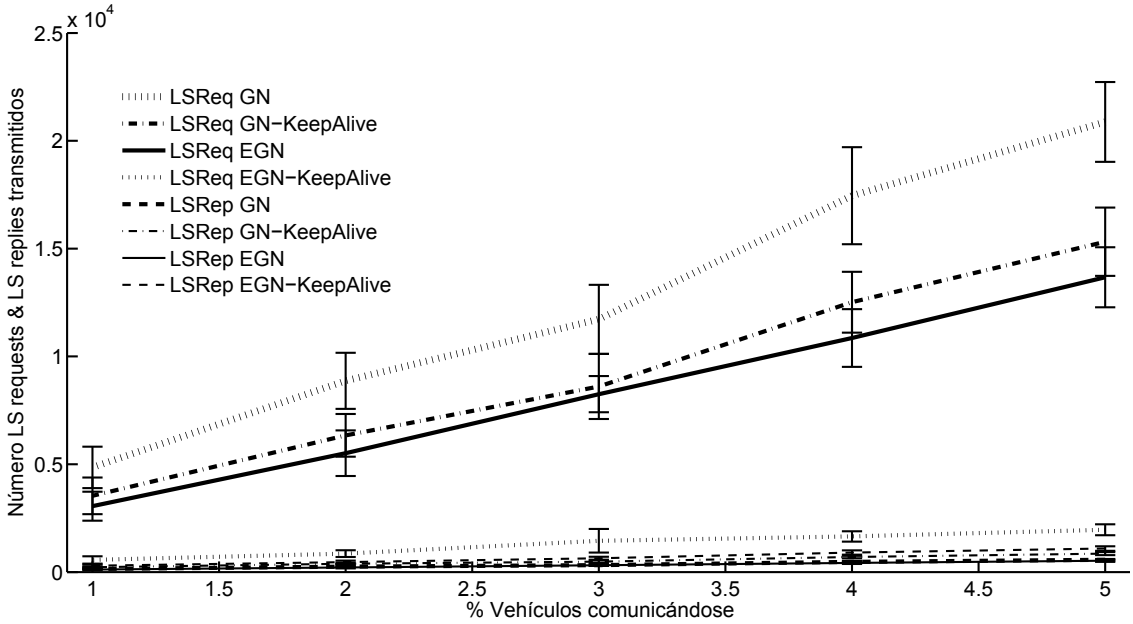


Figura 5.30: Transmisiones de mensajes *LS Request* y *LS Reply* para flujos de datos unidireccionales Internet-VANET (Tiempo de caducidad TL= 6 segundos)

el Servicio de Localización, se han ejecutado simulaciones donde el tráfico de datos solo se envía desde Internet a la VANET. La Figura 5.30 presenta el número de transmisiones de paquetes *LS Request* y *LS Reply* considerando el uso del protocolo de GN estándar y el protocolo EGN. Se muestran los resultados obtenidos cuando se aplica y no se aplica el mecanismo de *keep-alive* para el SL.

Como se puede apreciar en la figura, tanto para el protocolo de GN estándar como para el protocolo EGN, la aplicación del mecanismo de *keep-alive* para el SL reduce la sobrecarga de señalización en la red que produce el envío de mensajes *LS Request* cada vez que la entrada de un destino de la VANET expira y se elimina de la TL de la RSU. Por otro lado, la sobrecarga de señalización producida por el envío de los mensajes *LS Reply* se incrementa cuando se aplica el mecanismo de *keep-alive* para el SL. Sin embargo, nótese que los mensajes *LS Request* se distribuyen mediante *broadcast*/inundación lo que es costoso para el canal inalámbrico, mientras que los mensajes *LS Reply* se envían utilizando *geo-unicast*.

En lugar de utilizar el mecanismo de *keep-alive* para el SL, se podría intentar reducir la sobrecarga producida por el envío de mensajes *LS Request* aumentado el tiempo de caducidad de la TL. Sin embargo, esto provocaría la pérdida de paquetes porque la RSU enviaría los paquetes a una posición geográfica desactualizada, donde el destino no puede ser alcanzado porque se ha movido (recuérdese lo mencionado en la Sección 5.4.1). Este efecto se puede observar en la Figura 5.31, que muestra la tasa de entrega de paquetes para flujos de datos unidireccionales de Internet a la VANET en función del tiempo de caducidad de la TL. Los resultados para el protocolo de GN estándar y el protocolo EGN se han obtenido cuando el 3 % de los vehículos recibe tráfico desde

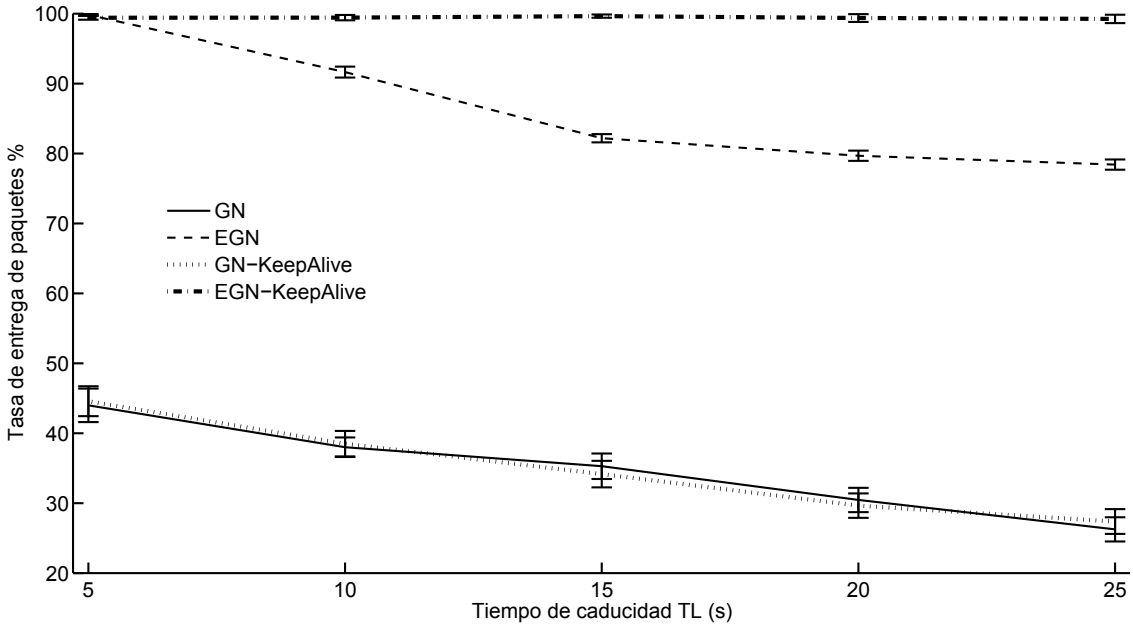


Figura 5.31: Tasa de entrega de paquetes para tráfico unidireccional Internet-VANET en función del tiempo de caducidad.

el CN. Cuando no se aplica el mecanismo de *keep-alive* para el SL, el protocolo EGN sufre una degradación de prestaciones conforme aumenta el tiempo de caducidad de la TL porque la posición geográfica de los destinos en la TL de la RSU se encuentra cada vez más desactualizada. Respecto a la tasa de entrega de paquetes del protocolo de GN estándar, el efecto producido por el mecanismo de *keep-alive* para el SL es imperceptible porque, como se ha mencionado anteriormente, una gran cantidad de paquetes se pierden porque la cola del nivel MAC de la RSU se satura (debido a que se eligen vecinos inalcanzables como siguiente salto).

El mecanismo de *keep-alive* para el SL ayuda a reducir la sobrecarga de señalización en la red, lo que es un aspecto crítico en las VANETs para poder obtener unas prestaciones adecuadas, especialmente cuando una gran cantidad de vehículos trata de comunicarse poniendo en peligro la capacidad de la VANET. Además, el mecanismo de *keep-alive* para el SL debería aplicarse en escenarios en los que los flujos de datos son unidireccionales de Internet a la VANET para evitar que la RSU envíe paquetes a posiciones geográficas desactualizadas. De aquí en adelante, se aplica el mecanismo de *keep-alive* para el SL en el protocolo EGN.

5.4.11. Análisis del impacto de la densidad de vehículos

Uno de los parámetros que tienen una influencia importante sobre las prestaciones de los protocolos de encaminamiento para redes vehiculares es la densidad de vehículos que circulan por la carretera. En escenarios en los que la densidad de vehículos es muy baja, las prestaciones decrecen debido a desconexiones entre diferentes zonas de la red vehicular. En cambio, cuando la

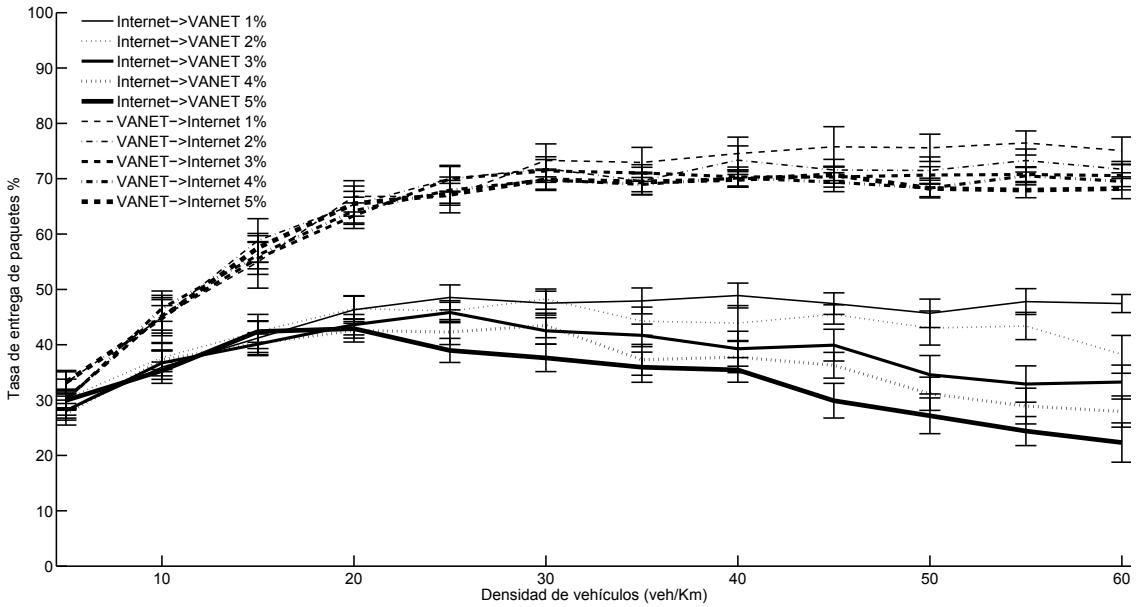


Figura 5.32: Tasa de entrega de paquetes del protocolo de GN en función de la densidad de vehículos.

densidad de vehículos es demasiado alta, se puede producir una caída de las prestaciones debido a las colisiones que se producen en el canal inalámbrico cuando una gran cantidad de vehículos tratan de transmitir paquetes de manera simultánea. Las Figuras 5.32 y 5.33 muestran la tasa de entrega de paquetes para flujos de datos bidireccionales (Internet-VANET y VANET-Internet) en función de la densidad de vehículos en la carretera. Se han obtenido resultados para diferentes porcentajes de vehículos que se comunican con el CN considerando el uso del protocolo de GN estándar (Figura 5.32) y el protocolo EGN (Figura 5.33). El tiempo de caducidad de la TL se encuentra establecido a 6 segundos para ambos casos.

Respecto al comportamiento del protocolo de GN estándar con la densidad de vehículos, se puede observar que la tasa de entrega de paquetes guarda alguna dependencia con la densidad de vehículos. La variación global de la tasa de entrega de paquetes es más significativa en el sentido VANET-Internet que en el sentido Internet-VANET. Como se explicó anteriormente, una cantidad importante de paquetes en el sentido Internet-VANET se pierden en el nivel de enlace de la RSU. Como estos paquetes están siendo descartados en el primer salto, no se produce un impacto significativo con la variación de la densidad de vehículos. En cambio, el impacto de la variación de la densidad de vehículos en la tasa de entrega de paquetes es más apreciable en el sentido VANET-Internet. Cuanto más decrece la densidad de vehículos, más baja es la tasa de entrega de paquetes. Si la densidad es baja, las desconexiones entre diferentes regiones de la VANET hacen imposible la formación de un camino multisalto desde el vehículo emisor de paquetes hasta la RSU. Cuanta más alta es la densidad de vehículos, mayor es la probabilidad de formar un camino multisalto entre el origen y el destino de los paquetes. Por lo tanto, la tasa de entrega de paquetes continúa aumentando con la densidad de vehículos hasta alcanzar un límite en el que la conectividad entre

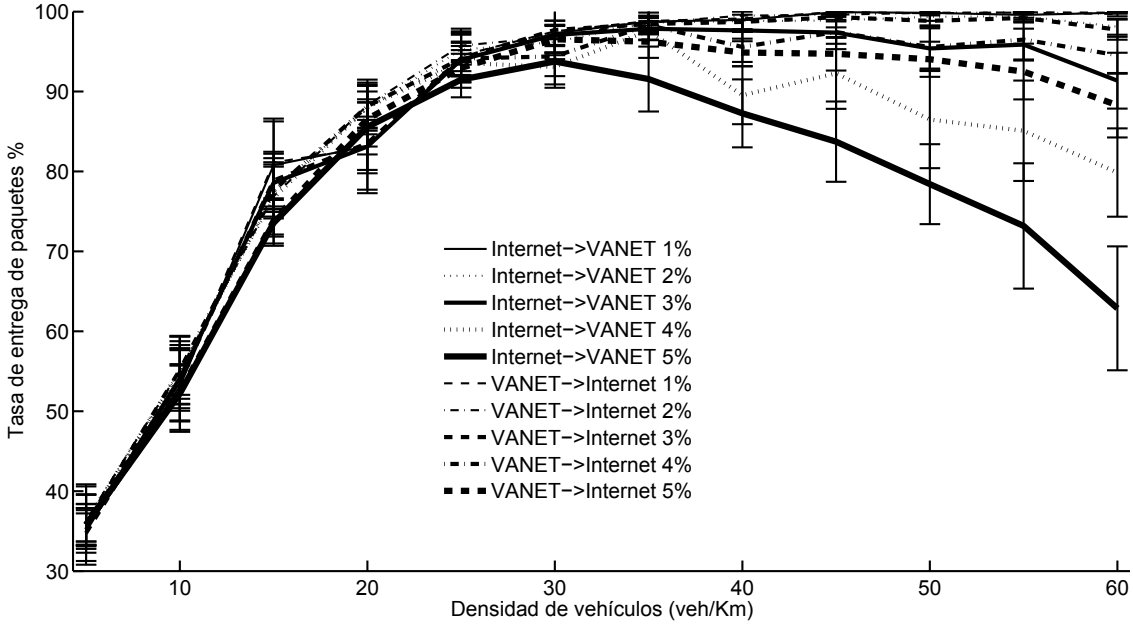


Figura 5.33: Tasa de entrega de paquetes del protocolo EGN en función de la densidad de vehículos.

el origen y el destino por medio de una cadena multisalto está garantizada independientemente de que la densidad de vehículos siga aumentando. De hecho, a partir de ese punto, para porcentajes de vehículos comunicándose con el CN por encima del 3 %, la tasa de entrega de paquetes decae con la densidad de vehículos debido al hecho de que el canal inalámbrico tiene que ser compartido por más vehículos que intentan comunicarse (la probabilidad de colisión aumenta). Por esta misma razón, cuanto mayor es el porcentaje de vehículos que se comunican con el CN, menor es la tasa de entrega de paquetes.

En el caso del protocolo EGN, la tasa de entrega de paquetes en ambos sentidos, Internet-VANET y VANET-Internet, varía con la densidad de vehículos. La probabilidad de formar una cadena multisalto entre el origen y el destino de los paquetes se incrementa con la densidad de vehículos. Por lo tanto, cuando la densidad de vehículos aumenta, la tasa de entrega de paquetes crece. Sin embargo, como ocurría en el caso del protocolo de GN estándar, cuanto mayor es el porcentaje de vehículos que se comunican con el CN, menor es la tasa de entrega de paquetes. Centrándonos en los casos de 3 %, 4 % y 5 % de vehículos comunicándose con el CN, la tasa de entrega de paquetes en el sentido Internet-VANET decrece cuando la densidad de vehículos aumenta por encima de un umbral. Esto es lógico porque cuanto mayor es la densidad de vehículos y una vez que es suficiente para tener conectividad multisalto con la RSU, mayor es la carga en la red porque mayor es el número de vehículos que se comunican con el CN. Esto provoca que la probabilidad de colisión en el medio inalámbrico se incremente, degradando las prestaciones, sobre todo en el sentido Internet-VANET por la congestión de la RSU. Sin embargo, conviene recalcar que esto es un problema de la capacidad disponible en la VANET y no del protocolo de

encaminamiento.

5.4.12. Análisis del impacto del patrón del tráfico de datos

Esta sección analiza la influencia del patrón del tráfico de datos en las prestaciones del protocolo EGN[12]. Se ha considerado el uso de los protocolos de transporte UDP y TCP, y se han obtenido resultados para los casos en los que la longitud del tramo de carretera al que da servicio la RSU es de 1000 metros y 2000 metros.

5.4.12.1. Tráfico UDP

Con el objetivo de estudiar la influencia del patrón del tráfico UDP sobre las prestaciones del protocolo EGN, se ha variado el tamaño del paquete UDP y el intervalo de tiempo entre paquetes, manteniendo la misma tasa de tráfico. Se han considerado tres patrones de tráfico UDP *Constant Bit Rate* (CBR) bidireccional: 1) paquetes de tamaño 160 bytes enviados cada 20 milisegundos, 2) paquetes de tamaño 320 bytes enviados cada 40 milisegundos y 3) paquetes de tamaño 480 bytes enviados cada 60 milisegundos. Las Figuras 5.34 y 5.35 muestran la tasa de entrega de paquetes en los sentidos Internet-VANET y VANET-Internet frente al porcentaje de vehículos que establecen comunicaciones con el CN. La Figura 5.34 se corresponde con el caso en el que el tramo de carretera tiene una longitud de 2000 metros, mientras que la Figura 5.35 muestra los resultados cuando la longitud del segmento de carretera es de 1000 metros.

Centrándonos en el caso en el que el tramo de carretera tiene una longitud de 2000 metros, se puede observar que cuanto menor es el intervalo entre paquetes, más baja es la tasa de entrega de paquetes. Un tiempo entre paquetes más pequeño implica un mayor número de transmisiones en el canal inalámbrico, lo que hace que la probabilidad de colisión entre paquetes aumente. Aunque un tamaño de paquete mayor también implica un aumento de la probabilidad de colisión, se puede ver en la figura cómo es el intervalo de tiempo entre paquetes el que tiene un mayor impacto. Por otro lado, la tasa de entrega de paquetes decrece con el porcentaje de vehículos que se comunican con el CN. Según aumenta la carga de tráfico en la red, la probabilidad de colisión aumenta, lo que hace empeorar las prestaciones. Las colisiones no solo implican la pérdida de paquetes de datos, sino que además pueden provocar una actualización incorrecta de la información de los vecinos en la TL debido a la pérdida de paquetes de control, lo que contribuye también a la degradación de las prestaciones. En el peor caso simulado, la tasa de entrega de paquetes en el sentido Internet-VANET es de solo un 10 %. La carga de tráfico en la red es extremadamente alta y las colisiones hacen la comunicación imposible. Los paquetes se descartan porque las colas del nivel MAC de los nodos se saturan. Sin embargo, este es un problema de la capacidad disponible en la VANET, y no del protocolo de encaminamiento.

[12]Para este análisis, se considera únicamente el protocolo EGN porque claramente supera en prestaciones al protocolo de GN estándar.

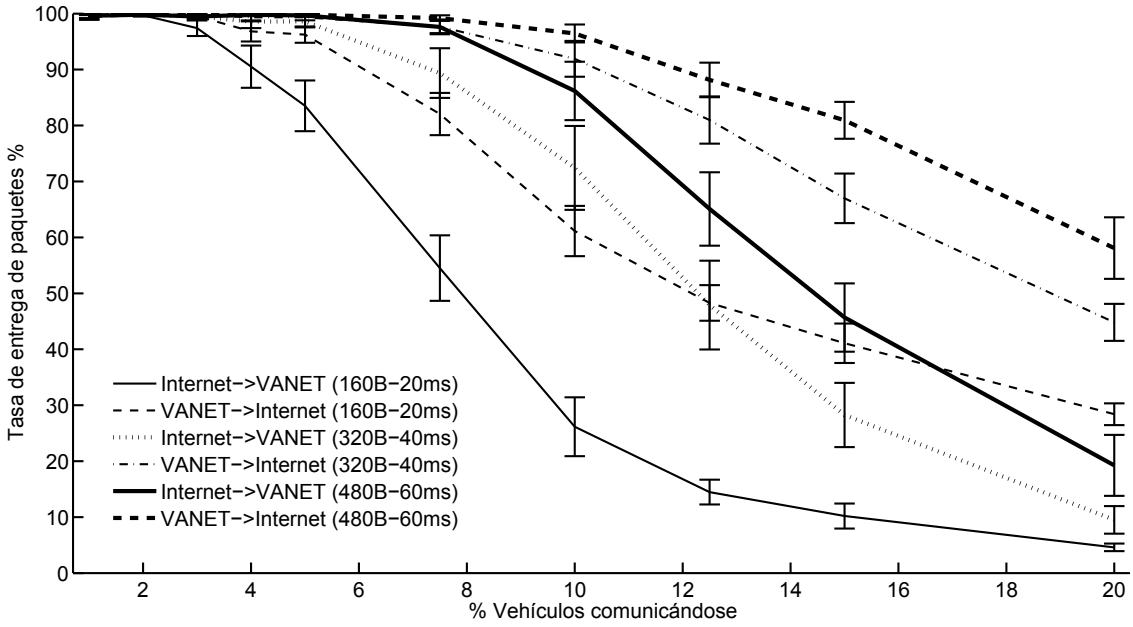


Figura 5.34: Tasa de entrega de paquetes en función del patrón de tráfico UDP (2000 metros)

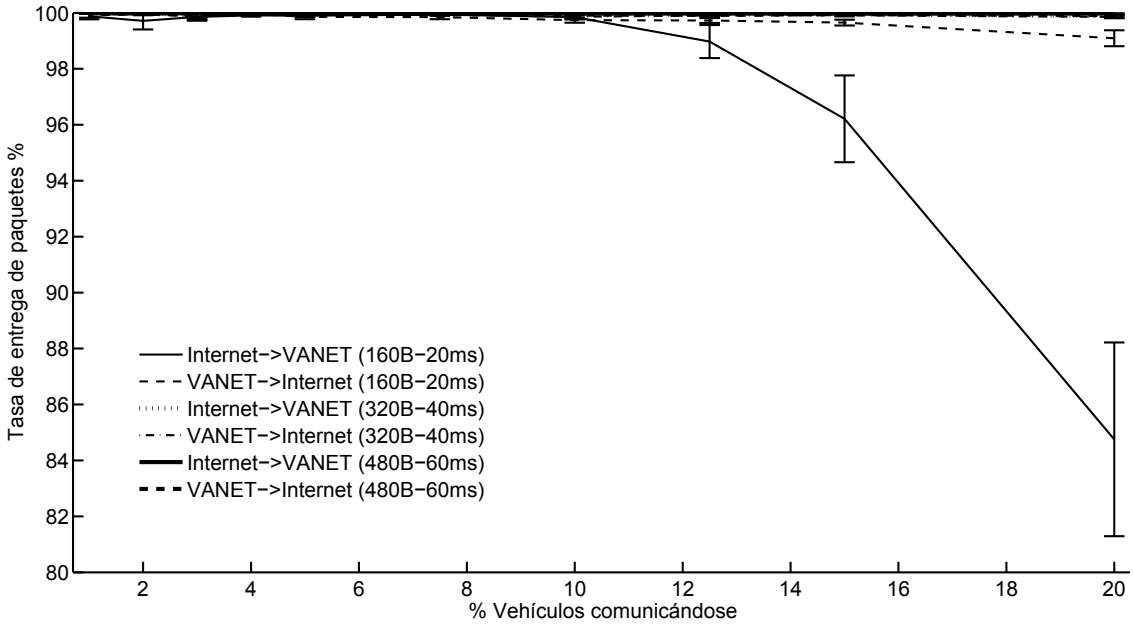


Figura 5.35: Tasa de entrega de paquetes en función del patrón de tráfico UDP (1000 metros)

Cuando la RSU cubre un tramo de carretera de 1000 metros, el número de saltos entre los vehículos y la RSU es menor. Además, la RSU presta servicio a un menor número de vehículos y por lo tanto, esto conlleva una menor congestión del canal inalámbrico. Se puede observar en la Figura 5.35, que el protocolo EGN alcanza una tasa de entrega de paquetes cercana al 100 %, excepto cuando los paquetes tienen un tamaño de 160 bytes y se envían cada 20 ms. En ese caso, se produce una caída de prestaciones en el sentido Internet-VANET debido a la congestión de

la cola de transmisión de la RSU. Aunque no es un problema del protocolo de encaminamiento, podemos concluir que la capacidad de la VANET es una limitación importante para el correcto funcionamiento de las comunicaciones entre los vehículos y la RSU. Esto resalta la necesidad de incrementar la capacidad del canal inalámbrico (mejoras en la tecnología de acceso que aumente su capacidad) o de distribuir la capacidad disponible de una manera adecuada para mejorar las comunicaciones por medio de mecanismos de control de congestión como los trabajos que se están llevando a cabo en el ETSI [123, 124]. Como trabajo futuro, sería interesante estudiar el impacto que tienen estos mecanismos de control de congestión en la capacidad de la red vehicular.

5.4.12.2. Tráfico TCP

Para el análisis del comportamiento del protocolo EGN con tráfico TCP, se ha recreado un escenario en el que los ocupantes de los vehículos navegan por páginas web. El 100 % de los vehículos que entran en la simulación realizan una transacción HTTP contra un servidor web de Internet en un momento determinado. El instante en el que cada vehículo comienza esta transacción HTTP se distribuye uniformemente entre el momento en el que el vehículo entra en la simulación hasta que sale del tramo de carretera. El tamaño del mensaje HTTP GET sigue una distribución normal de media 350 bytes y desviación estándar de 20 bytes (la distribución se ha truncado para ofrecer valores no negativos). El tamaño de la página web que se descarga sigue una distribución exponencial cuya media se puede variar. Cuando se trata con tráfico TCP no tiene sentido hablar de tasa de entrega de paquetes porque se trata de un protocolo fiable que realiza retransmisión de segmentos cuando los datos no llegan al destino final. Por ello, se realizan medidas del tiempo de descarga. El tiempo de descarga comprende desde el momento en el que el vehículo envía el mensaje HTTP GET hacia el servidor, hasta que el vehículo recibe la página web completamente (HTTP 200 OK)[13]. La Figura 5.36 presenta el tiempo de descarga en función del tamaño de la página web (media de la distribución exponencial) para los casos en los que la RSU da servicio a tramos de carretera de 1000 o 2000 metros.

Los resultados muestran que el tiempo de descarga aumenta con el tamaño de la página web. Este es un resultado lógico porque un tamaño de página web más grande implica mayor carga en la red, lo que provoca mayor retardo en la transmisión de los paquetes. Además, el tiempo de descarga es mayor cuando el tramo de carretera que cubre la RSU es más largo (2000 metros). Esto se debe a que el número de saltos entre los vehículos y la RSU es mayor, por lo que se realizan más retransmisiones de los paquetes haciendo que la carga de tráfico en la red aumente. Con una mayor carga de tráfico en la red los nodos tienen más dificultades para transmitir paquetes en el medio inalámbrico por posibles colisiones. Este fenómeno es más significativo para la RSU debido a que concentra todo el tráfico de datos del tramo de carretera. Las RSUs deberían tener más prioridad

[13]Nótese que un navegador suele enviar diferentes peticiones HTTP GET a diferentes servidores web. Para simplificar el escenario de simulación sin afectar al objetivo del análisis, lo vehículos envían un único mensaje HTTP GET.

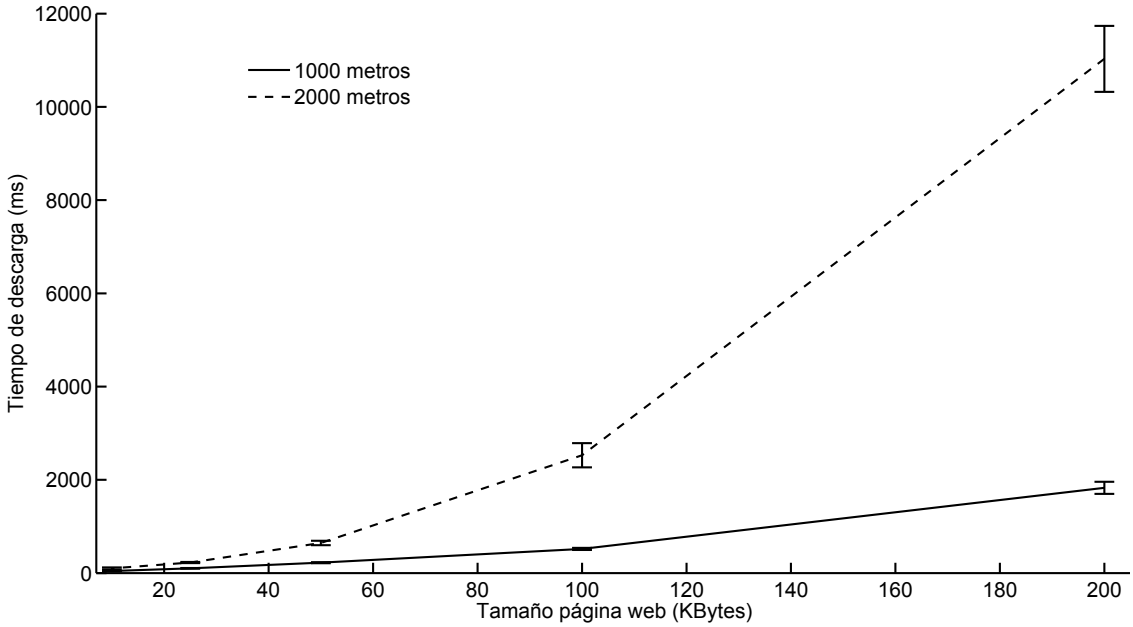


Figura 5.36: Tiempo de descarga

para acceder al canal inalámbrico que los vehículos porque tienen que cursar mayor cantidad de tráfico. Por otro lado, mencionar que se han obtenido unos tiempos de descarga que en muchos casos no podrían ofrecer una experiencia de usuario adecuada. Como se mencionó anteriormente, se precisa de ciertos mecanismos que mejoren o controlen la capacidad disponible en la VANET de manera que se pueda proporcionar una mejor comunicación entre los vehículos y la RSU.

5.5. Conclusiones

Se ha analizado en profundidad por medio de simulación las prestaciones de la arquitectura definida por el ETSI para un sistema de transporte inteligente y, concretamente, el funcionamiento del protocolo de GN cuando se proporciona conectividad a Internet a los vehículos de la VANET. Durante este estudio, se han identificado diferentes puntos débiles en el protocolo de GN. Además, se han descrito diferentes mecanismos que se pueden aplicar para mejorar sus prestaciones y se ha estudiado el impacto de estos mecanismos a través de simulación. Las principales conclusiones que se pueden extraer del análisis realizado son:

- Cuando se conecta la VANET a Internet, el mecanismo de *beaconing* deja de actuar sin producir ningún impacto sobre las prestaciones debido a su solapamiento con la distribución de los mensajes RA, necesaria para que los vehículos auto-configuren una dirección IPv6 global. Las RSUs envían periódicamente mensajes *Router Advertisement (RA)* por medio de *geo-broadcasting* que actualizan la información de los vecinos en las Tablas de Locali-

zación (TLs) de los nodos de la VANET. De esta forma, los mensajes RA asumen el papel de los mensajes *beacon*.

- Cuando se utiliza el protocolo de GN del ETSI para proporcionar conectividad a Internet a los vehículos de la VANET se obtienen prestaciones insatisfactorias. Por lo tanto, se deberían introducir algunos mecanismos para mejorar su funcionamiento.

- La mayoría de las pérdidas de paquetes tienen como causa que el protocolo de GN selecciona como siguiente salto a vecinos que se encuentran fuera del radio de cobertura debido al elevado tiempo de caducidad de las entradas de la TL (los vecinos se mantienen en la TL durante mucho tiempo, incluso si no son alcanzables nunca más).

- El tiempo de caducidad de la TL debería ser configurable en función del radio de cobertura de los nodos, determinado por la tecnología de acceso, y la velocidad máxima con la que se mueven los vehículos. De esta manera, se podría ajustar el tiempo de caducidad de la TL para evitar enviar tráfico a una posición geográfica desactualizada donde el destino final no se puede recibirlo porque se ha movido.

- Las simulaciones revelaron que frecuentemente se reciben paquetes desordenados debido al entorno altamente cambiante de las VANETs. El mecanismo de detección de paquetes duplicados del protocolo de GN debería ser modificado para evitar descartar paquetes que no son duplicados, pero que se reciben de forma desordenada.

- Resulta necesario que los vehículos esperen un tiempo aleatorio (al que hacemos referencia como retardo de *broadcasting*) antes de retransmitir los paquetes *broadcast* en la VANET, con el objetivo de distribuir temporalmente el acceso al canal inalámbrico y disminuir la pérdida de los paquetes por colisiones.

- La aplicación del mecanismo de Detección de Pérdida de Vecino (DPV) y del mecanismo de predicción de la posición de los vecinos de forma combinada mejora en gran medida las prestaciones del protocolo de GN.

- La RSU es propensa a la saturación cuando el porcentaje de vehículos que establecen comunicaciones con un *Correspondent Node* (CN) en Internet aumenta, lo que produce la degradación de las prestaciones, especialmente para los flujos de datos en el sentido Internet-VANET de la comunicación. La RSU se encuentra en desventaja respecto al resto de vehículos. Aunque la RSU cursa mayor cantidad de tráfico porque concentra todo el tráfico de datos hacia/desde Internet, tiene las mismas oportunidades de acceder al canal inalámbrico para transmitir que un vehículo. En la literatura existen diferentes propuestas que tratan de solucionar este problema en redes WLAN en modo infraestructura [125, 126]. La idea que persiguen es la de dotar a los puntos de acceso de mayores facilidades para

transmitir en el canal inalámbrico con respecto al resto de estaciones, para que de esta manera, puedan cursar mayor cantidad de tráfico. Estas soluciones se podrían adaptar para su aplicación a nuestro escenario.

- En general, los protocolos de encaminamiento geográfico para VANETs ofrecen una diferencia importante de prestaciones cuando se comparan las siguientes situaciones: 1) los vehículos que se comunican con un CN se mueven hacia la RSU y 2) los vehículos que se comunican con un CN se alejan de la RSU. Se obtienen mejores prestaciones cuando los vehículos que se comunican viajan hacia la RSU que cuando se alejan de ella por la probabilidad de seleccionar un vecino inalcanzable como siguiente salto. Puede ser interesante tener este comportamiento en cuenta cuando se diseñan protocolos de encaminamiento para VANETs.

- Las modificaciones introducidas en el borrador de la nueva versión del estándar del protocolo de GN [110] y en concreto, la eliminación de la información de posicionamiento del último nodo que transmite el paquete de la cabecera de los mensajes, tienen un impacto negativo sobre las prestaciones del protocolo cuando se utiliza para comunicaciones entre los vehículos e Internet. Realizar *beacon piggybacking* posibilita que los nodos obtengan información de posicionamiento más precisa de sus vecinos y que se reduzca la carga de señalización en la red mediante la reinicialización del temporizador de *beaconing* cuando se envían otros paquetes de GN.

- En escenarios en los que el tráfico de datos es unidireccional en el sentido Internet-VANET, el Servicio de Localización (SL) produce una sobrecarga de señalización considerable en la red porque la RSU necesita descubrir la posición geográfica del destino de cada flujo de datos cada vez que su entrada en la TL expira. Además, las prestaciones pueden verse degradadas porque la RSU continúa enviando paquetes de datos a una posición geográfica desactualizada aunque el nodo destino se haya movido. Por ello, se ha propuesto un mecanismo de *keep-alive* para el Servicio de Localización que soluciona estos problemas y mejora notablemente la tasa de entrega de paquetes para los flujos de datos unidireccionales con sentido Internet-VANET. Este mecanismo ha sido diseñado para minimizar la sobrecarga de señalización introducida.

- El análisis de prestaciones en función de la densidad de vehículos confirma que cuando la densidad de vehículos es reducida, la tasa de entrega de paquetes es baja debido a que las desconexiones entre las diferentes partes de la VANET hacen imposible formar una cadena multisalto entre origen y destino. Sin embargo, si la densidad de vehículos es muy alta, las prestaciones decrecen debido a la cantidad de vehículos que intenta comunicarse y la falta de capacidad en la VANET.

- El estudio de la influencia el patrón del tráfico de datos sobre las prestaciones señala que la capacidad en la VANET puede limitar el uso efectivo de la comunicación de la VANET con

Internet. Existe una necesidad de introducir mecanismos que incrementen la capacidad del canal inalámbrico o que distribuyan la capacidad disponible adecuadamente para mejorar las comunicaciones en la VANET.

Capítulo 6

Solución de gestión de la movilidad basada en PMIPv6 para el sistema de transporte inteligente del ETSI

6.1. Introducción

El sistema de transporte inteligente que ha estandarizado el ESTI [87] considera la conexión de los vehículos a Internet a través del despliegue de múltiples RSUs. Cuando los vehículos se encuentran dentro del ámbito de una RSU configuran una dirección IPv6 que les permite conectarse a Internet y establecer comunicaciones con otros nodos utilizando la RSU como puerta de enlace. Debido al movimiento de los vehículos, estos pueden cambiar su punto de acceso a Internet entre diferentes RSUs por lo que se precisa de un protocolo que gestione la movilidad y que mantenga las comunicaciones de los vehículos activas a pesar del cambio de conexión entre RSUs.

Mientras que el Capítulo 5 se centró en el análisis del funcionamiento del protocolo de encaminamiento utilizado en la VANET del sistema de transporte inteligente del ETSI con el objetivo de que las prestaciones fueran adecuadas para el encaminamiento de los paquetes entre los vehículos y las RSUs, este capítulo se centra en los aspectos relacionados con la gestión de la movilidad proponiendo una solución para la integración de PMIPv6 con la arquitectura del sistema de transporte inteligente del ETSI y su protocolo de *GeoNetworking* (GN) [36].

Como se introdujo en el estado del arte en el Capítulo 3 existen diferentes soluciones para la gestión de la movilidad cuando las VANETs se conectan a Internet. El sistema de transporte inteligente del ETSI contempla la utilización del protocolo NEMO [63] para que los vehículos, considerados como redes móviles, puedan cambiar su punto de conexión a Internet sin que sus comunicaciones activas tengan que ser restablecidas debido al cambio de dirección IP que se produce con el *hand-over* entre RSUs. Sin embargo, la utilización de NEMO como protocolo para la

gestión de la movilidad conlleva cierta ineficiencia en la VANET, ya que el tráfico entre las RSUs y la CCU de los vehículos (que implementa la funcionalidad del MR de NEMO) se encapsula en un túnel IP sobre IP que introduce sobrecarga por la cabecera IP adicional de los paquetes que se transmiten en la VANET. Además, NEMO presenta la problemática del encaminamiento triangular, aunque existen diferentes propuestas de optimización de rutas [64] que evitan que el tráfico de datos viaje por el HA.

La solución que se propone en este capítulo se basa en la utilización de PMIPv6 como protocolo para la gestión de la movilidad. La utilización de PMIPv6 como protocolo de gestión de la movilidad permite una mayor eficiencia en los *hand-overs* que los vehículos realizan entre RSUs si el LMA se encuentra cerca de ellas. Además, al tratarse de una solución de movilidad *network-based*, PMIPv6 evita configuraciones de seguridad complejas relacionadas con la movilidad en los vehículos ya que las funciones de gestión de movilidad IP se realizan desde nodos situados en la red. Además, la progresiva adopción por parte de los operadores de PMIPv6 como protocolo para soportar la movilidad ofrece la oportunidad de integrar la solución de movilidad de la VANET con la presente en otras regiones de sus redes que utilizan otras tecnologías de acceso, como por ejemplo LTE-EPS, y donde se puede proporcionar movilidad por medio de PMIPv6. De esta forma, los vehículos podrían conectarse a Internet a través de diferentes tecnologías de acceso y realizar *hand-overs* entre ellas sin cambiar su dirección IP y manteniendo sus comunicaciones activas, siempre que se mantengan dentro del dominio localizado. Este modelo encaja también con la visión de la VANET como una red de acceso más *non*-3GPP integrada en la arquitectura 4G y que puede ser utilizada por los operadores para descargar de tráfico sus redes celulares siempre que sea posible.

A continuación se proponen una serie de procedimientos que permiten integrar PMIPv6 con la arquitectura del sistema de transporte inteligente del ETSI. Además, se presenta un mecanismo de *bicasting* que está orientado a mejorar las prestaciones cuando los vehículos realizan el *hand-over*. Finalmente, se realiza una evaluación experimental a través de simulación que sirve para validar la viabilidad de la solución y analizar el impacto del mecanismo de *bicasting*. El escenario de simulación que se utiliza para esta validación se ha mejorado a través de la utilización de trazas de tráfico reales de una importante autopista de circunvalación de Madrid, lo que ayuda a que los resultados obtenidos sean más próximos a una situación real.

La solución que se presenta en este capítulo para la integración de PMIPv6 con la arquitectura del sistema de transporte inteligente estandarizada por el ETSI y su protocolo de GN ha sido publicada en [6].

6.2. Integración de PMIPv6 con la arquitectura del sistema de transporte inteligente del ETSI y el protocolo de *GeoNetworking*

En esta sección se presenta la solución propuesta para proporcionar a la VANET conectividad a Internet basada en la combinación de PMIPv6 [61] con la arquitectura del sistema de transporte inteligente estandarizada por el ETSI [87] y su protocolo de GN [36]. Como se ha mencionado anteriormente, la adopción de PMIPv6 como protocolo de gestión de movilidad tiene la ventaja de que permite realizar *hand-overs* eficientes, evita configuraciones de seguridad complejas en los vehículos y proporciona la posibilidad de soportar la movilidad entre diferentes tecnologías de acceso mediante la integración de la solución propuesta con la gestión de movilidad del operador, lo que justifica la elección de PMIPv6 como protocolo para gestionar la movilidad.

Sin embargo, la aplicación de PMIPv6 al entorno de las redes vehiculares no se puede realizar de forma directa ya que PMIPv6 ha sido diseñado para escenarios en los que el MN está directamente conectado con la MAG para entre otros aspectos, que la MAG pueda detectar la conexión/desconexión de los MNs mediante, por ejemplo, eventos de nivel de enlace. Por este motivo, es necesario un mecanismo que permita adaptar PMIPv6 al entorno de las VANETs multisalto, para de esta manera, poder integrarlo con la arquitectura del sistema de transporte inteligente del ETSI y el protocolo de GN.

La Figura 6.1 muestra de forma esquemática la operación de la solución propuesta para integrar PMIPv6 con la arquitectura del sistema de transporte inteligente del ETSI y adaptarlo al entorno de las VANETs multisalto. En primer lugar, las RSUs además de estar situadas al borde de la carretera con el objetivo de ampliar el rango de cobertura de la VANET y proporcionar conectividad a Internet a los vehículos, han sido extendidas para soportar las funcionalidades de las MAGs de PMIPv6. Además, se dispone de un LMA que es el punto de anclaje de todo el direccionamiento IPv6 que utilizan los vehículos de la VANET. Como las RSU/MAGs actúan como *routers* de acceso de los vehículos que están situados dentro de su zona geográfica asignada, estas distribuyen periódicamente mensajes *Router Advertisement* (RA) mediante *geo-broadcasting* dentro de su área geográfica asignada. Estos mensajes RA, que no incluyen información sobre ningún prefijo, son recibidos por todos los vehículos que están situados dentro la zona geográfica gobernada por cada RSU/MAG. Como los mensajes *geo-broadcast* de RA incluyen información sobre la posición geográfica de la RSU/MAG y su área geográfica asociada, los vehículos pueden detectar cuándo cambian de área geográfica y pueden aprender la localización de nuevas RSU/MAGs. De esta forma, los vehículos pueden descubrir las RSUs que les proporcionan conectividad con Internet.

Se toma como referencia el escenario representado en la Figura 6.1 para explicar la adaptación de PMIPv6 a las redes vehiculares multisalto, asumiendo que el vehículo A no se encontraba conectado previamente a la VANET. Cuando el vehículo A se conecta a la VANET, en primer lugar debe configurar una dirección IPv6 global para poder establecer comunicaciones con otros

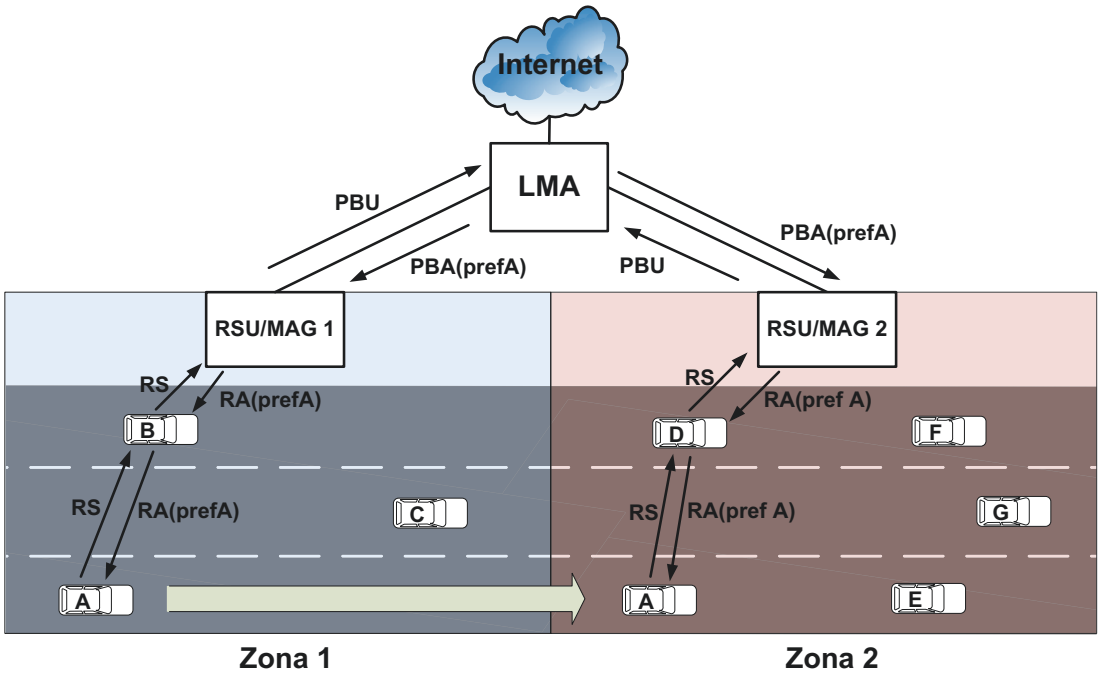


Figura 6.1: Adaptación de PMIPv6 para VANETs

nodos en Internet. La recepción de un mensaje RA *geo-broadcast* le permite aprender la posición geográfica de la RSU/MAG 1 y los parámetros de su zona geográfica asignada. De esta forma, el vehículo A descubre la RSU que debe utilizar para establecer comunicaciones con Internet. Para que la RSU/MAG 1 pueda detectar la llegada del vehículo A a su área geográfica, el vehículo A envía a la RSU/MAG 1 un mensaje *Router Solicitation* (RS) utilizando un envío *geo-unicast*. Nótese que el vehículo A conoce la posición geográfica de la RSU/MAG 1 gracias a que esta se incluye en los mensajes RA. El mensaje RS es encaminado por el protocolo de GN hasta la RSU/MAG 1 a través de una cadena multisalto formada por diferentes vehículos. De esta forma, la RSU/MAG 1 se percata de la llega del vehículo A a su área geográfica y comienza el intercambio de mensajes de señalización de movilidad con el LMA enviando un mensaje PBU para notificar la presencia del vehículo A y solicitar un prefijo para el mismo. Ante la recepción de este mensaje PBU, el LMA reserva un prefijo para el vehículo A (no existía ningún prefijo asignado previamente) y lo incluye en el mensaje PBA que se devuelve a la RSU/MAG 1. Después del procesamiento del mensaje PBA, la RSU/MAG 1 envía al vehículo A el prefijo asignado por medio de un mensaje RA utilizando un envío *geo-unicast* que se entrega a través de una cadena multisalto de vehículos (nótese que la RSU/MAG 1 obtuvo la posición geográfica del vehículo A cuando recibió el mensaje RS *geo-unicast*). De esta forma, el vehículo A puede configurar una dirección IPv6 global utilizando el prefijo asignado por el LMA mediante los mecanismos de auto-configuración de direcciones *stateless* de IPv6 [56, 57][1]. Además, se establece un túnel

[1]Nótese que cuando un nodo configura una dirección IPv6 global utilizando los mecanismos SLAAC [56, 57] no es necesario comprobar si la dirección es única en la VANET mediante el mecanismo de detección de direcciones

bidireccional IP sobre IP entre el LMA y la RSU/MAG 1 por el que se envían los paquetes de datos de las comunicaciones que establece el vehículo A con otros nodos de Internet. Con el objetivo de garantizar el éxito de este procedimiento, el vehículo A continúa enviando mensajes RS *geo-unicast* a la RSU/MAG 1 periódicamente hasta que recibe el mensaje RA *geo-unicast* con el prefijo que le ha sido asignado por el LMA.

Una vez que se completa el intercambio de señalización y el vehículo ha configurado una dirección IPv6 global, el encaminamiento de los paquetes de datos se realiza de la siguiente manera. Cuando un vehículo envía un paquete de datos, este lo envía a su RSU/MAG que actúa como puerta de enlace del área geográfica. Cuando la RSU/MAG recibe el paquete de la VANET, lo reenvía a través del túnel IP sobre IP bidireccional hasta el LMA. Finalmente, el LMA encamina el paquete hacia el destino: si el destino pertenece al LMD, el paquete se envía por el túnel que conecta con la RSU/MAG donde se encuentra vinculado el destino; en caso contrario, el paquete se encamina hacia su destino a través de Internet. En el sentido contrario, cuando los paquetes proceden de Internet y llegan al LMA, el LMA los envía a través del túnel a la RSU/MAG donde el vehículo destino se encuentra conectado. Finalmente, la RSU/MAG encamina los paquetes hasta el destino utilizando el protocolo de GN.

Debido a la movilidad de los vehículos en la VANET, estos pueden cambiar de área geográfica. El procedimiento de *hand-over* entre RSU/MAGs también se representa en la Figura 6.1. Cuando el vehículo A entra en la zona geográfica 2, detecta el cambio de área y de RSU que actúa de *router* de acceso, mediante la recepción de un mensaje RA *geo-broadcast* procedente de la RSU/MAG 2. Para notificar su presencia en la nueva zona geográfica, el vehículo A envía un mensaje RS *geo-unicast* a la RSU/MAG 2. De esta forma, la RSU/MAG 2 descubre que el vehículo A ha entrado en su zona geográfica y envía un mensaje PBU al LMA para informar de la llegada de este. El LMA comprueba que el vehículo ya tiene un prefijo asignado y, por lo tanto, devuelve a la RSU/MAG 2 un mensaje PBA con el prefijo que fue asignado previamente al vehículo A y actualiza el extremo del túnel bidireccional que se utiliza para el tráfico de datos del vehículo A, que ahora apunta a la nueva RSU/MAG 2. Mediante este intercambio de señalización de movilidad, el LMA mantiene localizado al vehículo dentro del LMD. Finalmente, como la RSU/MAG 2 envía al vehículo A el mismo prefijo que fue asignado por el LMA, este puede conservar su dirección IPv6 independientemente del cambio de punto de conexión a Internet, lo que le permite mantener sus comunicaciones activas.

Durante el procedimiento de *hand-over* entre RSU/MAGs, el vehículo A puede continuar recibiendo tráfico en el sentido Internet-VANET que procede de la antigua RSU/MAG (la RSU/MAG

duplicadas de IPv6 (*Duplicate Address Detection*, DAD). Esto se debe a que por un lado, el LMA proporciona prefijos diferentes a cada vehículo, de manera que se garantiza que la dirección IPv6 global será única en la VANET. Por otro lado, el identificador de interfaz de la dirección IPv6 se deriva de forma unívoca del identificador del protocolo de GN del nodo. Suponiendo que los identificadores del protocolo de GN son únicos en la VANET (el protocolo de GN especifica un mecanismo simple de comprobación de duplicidad de direcciones) no existen problemas con la duplicidad de direcciones ni con su resolución para la obtención del identificador de encaminamiento geográfico de un destino a partir de su dirección IPv6. De esta manera se puede evitar la inundación de mensajes *Neighbor Discovery* que es tan costoso en las VANETs [16].

1) aunque se encuentre situado dentro la nueva zona geográfica (e incluso posteriormente cuando el *hand-over* se haya completado). Esto permite evitar la pérdida de paquetes durante el *hand-over*, ya que el LMA solo comenzará a enviar tráfico al vehículo a través de la RSU/MAG 2 una vez que se haya completado el establecimiento del túnel correctamente. En el sentido VANET-Internet, el vehículo podría comenzar a enviar tráfico hacia Internet a través de la RSU/MAG 2 tan pronto como la descubra tras la recepción de un mensaje RA *geo-broadcast*. Sin embargo, es posible que el procedimiento de *hand-over* y el establecimiento del túnel no se hayan completado, lo que produciría la pérdida de los paquetes. Por ello, lo más conveniente es que el vehículo solo comience a enviar el tráfico a través de la RSU/MAG 2 una vez que el procedimiento de *hand-over* se haya completado, es decir, cuando reciba el mensaje RA *geo-unicast* procedente de la RSU/MAG 2 con el prefijo que le fue asignado por el LMA previamente. Dado que las comunicaciones pueden continuar mientras que el procedimiento de *hand-over* finaliza, se trata de un *hand-over make-before-break*.

Por último, mencionar que aunque PMIPv6 no soporta movilidad de redes sino de terminales, [127] define extensiones para el protocolo que permitirían a las CCUs obtener prefijos adicionales del LMA para que los dispositivos de la red interior de los vehículos puedan configurar una dirección IPv6 global con un prefijo que pertenece al LMD. De esta manera, la movilidad se gestiona desde la red registrando los movimientos de las CCUs y de sus prefijos asociados, tal que se controla la movilidad de la red móvil como un conjunto de nodos y no de forma individual para cada nodo. Estas extensiones se podrían aplicar directamente sobre la solución para la integración de PMIPv6 con la arquitectura del sistema de transporte inteligente estandarizada por el ETSI y su protocolo de GN.

6.2.1. Mecanismo de *bicasting*

A pesar de que las comunicaciones pueden continuar a la vez que se realiza el procedimiento de *hand-over* (es un *hand-over make-before-break*), se podrían perder paquetes o introducir retardos en el encaminamiento entre las RSU/MAGs y los vehículos que deteriorarían las comunicaciones. Con la intención de eludir este posible problema y mejorar las prestaciones de la solución para la integración de PMIPv6 con la arquitectura del sistema de transporte inteligente del ETSI, se propone un mecanismo de *bicasting*. A continuación se describe este mecanismo que permite detectar cuándo un vehículo va a realizar el *hand-over* entre diferentes RSUs de manera que se consiga minimizar el tiempo de *hand-over* y las posibles pérdidas durante el mismo por medio del envío de los paquetes en *bicasting*.

Como se mencionó en el Capítulo 3 del estado del arte, en [95] los autores utilizan un mecanismo de predicción de *hand-over* con el mismo objetivo que el mecanismo que aquí se propone, pero que se basa en los mecanismos de *Neighbor Discovery* y *Neighbor Unreachability Detection* que son costosos para la VANET porque producen sobrecarga de señalización y consumen

recursos del canal inalámbrico [16]. En cambio, el mecanismo que aquí se propone se basa en la detección del momento en el que se va a realizar el *hand-over* (no se realizan predicciones que pueden ser erróneas) mediante el análisis de la cabecera del protocolo de GN de los paquetes de datos, en lugar de los mensajes de *Neighbor Discovery*. Como las RSU/MAGs son las puertas de enlace hacia Internet de los vehículos que están situados dentro de su área geográfica asignada, cuando un vehículo se comunica con otro nodo de Internet, la RSU/MAG recibe los paquetes de datos enviados por el vehículo. Por lo tanto, la RSU/MAG puede extraer de la cabecera del protocolo de GN la posición geográfica que ocupa actualmente el vehículo. De esta manera, la RSU/MAG puede detectar cuando el vehículo se mueve a una zona geográfica distinta. Nótese que esta detección se puede llevar a cabo porque mientras que el vehículo no reciba un mensaje RA de la RSU/MAG del nuevo área, no iniciará el procedimiento de *hand-over* y por lo tanto, continuará utilizando la RSU/MAG actual como puerta de enlace hacia Internet.

Con el objetivo de minimizar el tiempo y la pérdida de paquetes que puede producirse durante el *hand-over*, si la RSU/MAG detecta que un vehículo ha entrado en una zona geográfica nueva, enviará un mensaje de notificación al LMA para informarle de que se va a producir el *hand-over* del vehículo de forma inminente. En ese instante, se establece un túnel bidireccional IP sobre IP entre el LMA y la nueva RSU/MAG, de manera que el LMA comienza a realizar *bicasting* de los paquetes de datos que vienen desde Internet y que van dirigidos al mencionado vehículo: el LMA envía una copia del mensaje a la RSU/MAG de la zona de la que el vehículo está saliendo y otra copia del paquete a la RSU/MAG encargada del nuevo área geográfica a la que el vehículo entra. Por consiguiente, se reduce la probabilidad de que se produzcan pérdidas de paquetes durante el *hand-over* entre las RSU/MAGs. Además, el establecimiento del túnel bidireccional IP sobre IP entre el LMA y la nueva RSU/MAG se realiza con antelación a que el vehículo se vincule con la nueva RSU/MAG, lo que ayudará a reducir el tiempo que tarda en completarse el procedimiento de *hand-over*[2]. Finalmente, el LMA cesa de enviar paquetes de datos en *bicasting* cuando recibe el mensaje PBU procedente de la RSU/MAG del nuevo área, lo que significa que el vehículo ha realizado el procedimiento de *hand-over*.

6.3. Evaluación experimental de la solución

A continuación se presentan los resultados obtenidos de la evaluación experimental de la solución para la integración de PMIPv6 en la arquitectura del sistema de transporte inteligente del ETSI que está basada en simulación. Esta evaluación experimental tiene principalmente dos objetivos: 1) validar la viabilidad de la solución y 2) analizar el impacto del mecanismo de *bicasting* sobre las prestaciones.

Tras la introducción del escenario sobre el que se han llevado a cabo las simulaciones, se

[2]Nótese que esta ventaja no aplica si se usan túneles pre-configurados, entre el LMA y las RSU/MAGs, que son compartidos por el tráfico de distintos vehículos.

procede con la presentación de los resultados obtenidos y su análisis. La evaluación experimental se ha divido en dos fases. En primer lugar se considera el escenario en el que un único vehículo establece comunicaciones con Internet utilizando un patrón de tráfico de datos que nos permite centrar el análisis en el procedimiento de *hand-over* y la fase de configuración de la dirección IPv6 global cuando el vehículo aparece en la VANET. Bajo estas circunstancias se analiza el impacto del mecanismo de *bicasting*. Finalmente, se evalúa la solución en un escenario más realista considerando diferentes patrones de tráfico CBR UDP y permitiendo que un determinado porcentaje de vehículos establezcan comunicaciones con Internet.

6.3.1. Escenario de simulación

A continuación se presenta el escenario de simulación sobre el que se ha llevado a cabo la evaluación experimental de la solución propuesta. Las simulaciones se han ejecutado sobre nuestras propias implementaciones del protocolo EGN[3], de la capa de integración GN6ASL [58] necesaria para la transmisión de paquetes IPv6 sobre el protocolo EGN, y del protocolo PMIPv6 [61]. La implementación ha sido integrada con el *framework* INETMANET[4] del ampliamente conocido simulador de redes OMNeT++[5]. La implementación de PMIPv6 está basada en xMIPv6[6].

El escenario de simulación, que se encuentra representado en la Figura 6.2, es un tramo de autopista de *L* metros de longitud y que cuenta con tres carriles para la circulación de los vehículos. Se han desplegado dos RSU/MAGs separadas una distancia de *D=L/2* metros entre ellas. Cada una de las RSU/MAGs se encarga de proveer servicio a los vehículos que se encuentran situados dentro de su zona geográfica asignada, de longitud *D* metros (véase la Figura 6.2).

Con el objetivo de conseguir resultados lo más próximos posibles a un escenario real, los vehículos de la simulación se generan a partir de trazas de tráfico reales de una importante autopista de circunvalación de Madrid, la autopista M-40. Estas trazas de tráfico han sido recogidas por la Dirección General de Tráfico de España [128] en el punto kilométrico 12,7 de la autopista M-40 entre las 8:30 y las 9:00 de la mañana. La densidad media de vehículos de la traza es de 54 veh/Km y la velocidad media es de 95 Km/h. Para obtener un comportamiento realista del movimiento de los vehículos durante la simulación, se ha utilizado el simulador de tráfico SUMO[7] [114], que se encuentra acoplado con el simulador de redes OMNET++. De esta manera se consigue reproducir un comportamiento realista de los conductores durante las simulaciones. Por ejemplo, los vehículos tratan de utilizar el carril derecho cuando es posible y, cuando un vehículo

[3] Se establece la configuración de parámetros y se aplican los mecanismos que, como se concluyó en el Capítulo 5, mejoraban las prestaciones del protocolo de GN, lo que se denominó *Enhanced* GN (EGN).

[4] *INETMANET framework for OMNET/OMNeT++ 4.x (based on INET framework): https://github.com/inetmanet/inetmanet/wiki*

[5] *OMNeT++ Network Simulator Framework: http://www.omnetpp.org/*

[6] *Extensible Mobile IPv6 (xMIPv6) Simulation Model for OMNeT++: http://www.kn.e-technik.tu-dortmund.de/obs/content/view/232/lang de/*

[7] SUMO *Simulation of Urban MObility*: http://sumo.sourceforge.net/

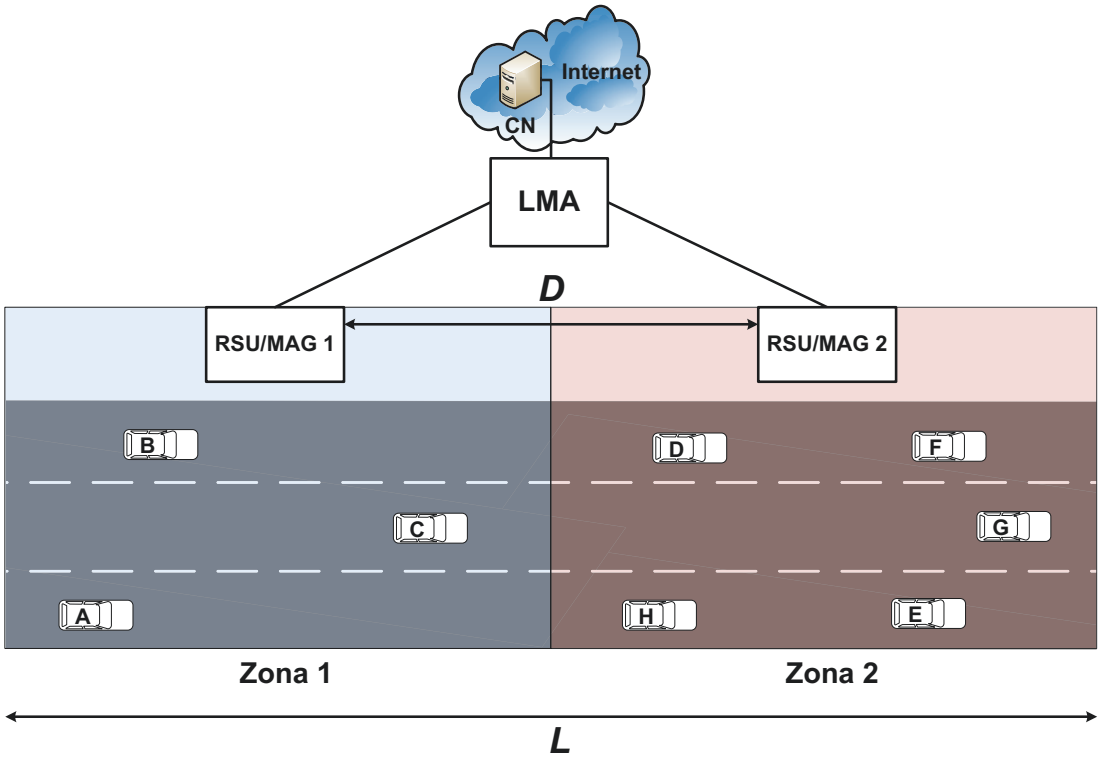


Figura 6.2: Esquema del escenario de simulación para la evaluación de la solución de movilidad.

que viaja a su velocidad objetivo se encuentra a otro vehículo delante a una velocidad menor, reducirá su velocidad y lo adelantará cuando las circunstancias lo permitan.

Siguiendo esta aproximación, los vehículos entran en el tramo de autopista en un determinado carril, instante de tiempo y velocidad indicados por las trazas de tráfico reales, viajan a través de la autopista realizando el *hand-over* entre las RSU/MAGs cuando cambian del área geográfica 1 a la zona geográfica 2, y finalmente salen del segmento de autopista. Por otro lado, todos los vehículos y la RSU se encuentran equipados con un nivel de enlace IEEE 802.11g operando a una tasa de 54 Mbps. La potencia de transmisión se ha ajustado para proporcionar un radio de cobertura de 200 metros [116, 117].

Las RSU/MAGs distribuyen periódicamente mensajes RA utilizando un tiempo entre envíos que se distribuye uniformemente entre $RA_{periodo} \pm 0.25$ segundos, de manera que el parámetro $RA_{periodo}$ es variable. Con el objetivo de evitar colisiones en el canal inalámbrico cuando las RSU/MAGs difunden los mensajes RA se aplica el mecanismo de retardo de *broadcasting* descrito en la Sección 5.4.2.3: en cada nodo se introduce un retardo aleatorio seleccionado uniformemente entre 0 y 5 milisegundos antes de retransmitir un paquete en *broadcast*.

Respecto al protocolo EGN, incluye la aplicación de los mecanismos de predicción de la posición geográfica de los vecinos combinada con el mecanismo de la DPV, la mejora del mecanismo de detección de paquetes duplicados y el mecanismo de *keep-alive* para el Servicio de

Localización. Respecto al tiempo de caducidad de la Tabla de Localización se ha establecido a 6 segundos, dado que aunque la velocidad máxima de la vía está limitada a 100 Km/h, algunos de los vehículos de la traza la sobrepasan y se proporciona un margen de guarda temporal (véase la Sección 5.4.1).

Para evaluar experimentalmente el funcionamiento de la solución propuesta y el impacto del mecanismo de *bicasting* es importante elegir un patrón de tráfico de datos adecuado. Para un primer análisis centrado en el procedimiento de *hand-over* y la fase de configuración de la dirección IPv6 global cuando los vehículos entran en la VANET, se establecen flujos CBR (*Constant Bit Rate*) UDP bidireccionales (sentido Internet-VANET y VANET-Internet) entre un vehículo de la VANET y un *Correspondent Node* (CN) en Internet. Con el objetivo de focalizar la evaluación del rendimiento en la VANET, el CN se encuentra directamente conectado a las RSU/MAGs. El patrón de tráfico de los flujos CBR UDP es de paquetes de tamaño 20 bytes enviados cada 10 milisegundos. Este patrón de tráfico (paquetes pequeños y frecuentes) permite muestrear el funcionamiento de la solución con precisión. El vehículo que envía y recibe tráfico de datos se selecciona aleatoriamente una vez que el tramo de autopista se encuentra repleto de vehículos de manera que se recrea el escenario real en el que los vehículos tienen otros vehículos delante y detrás.

Una vez que se realiza el análisis utilizando este patrón de tráfico que permite muestrear el comportamiento de la solución con mayor precisión, se evalúa el comportamiento general de la propuesta utilizando diferentes patrones de tráfico CBR UDP en el caso en el que múltiples vehículos establecen comunicaciones con el CN. Cuando se selecciona un vehículo para comunicarse con el CN, se establecen dos flujos CBR UDP independientes entre el vehículo y el CN, uno en cada sentido de la comunicación. Los vehículos que envían y reciben tráfico de datos se seleccionan aleatoriamente siguiendo una distribución geométrica que se puede ajustar para que un determinado porcentaje de vehículos de la VANET establezcan comunicaciones. Esto nos permite analizar la influencia del patrón del tráfico de datos en las prestaciones.

Por otro lado, se consideran dos configuraciones de despliegue de RSU/MAGs: *i)* tramo de carretera con una longitud L = 2000 metros donde las RSU/MAGs se encuentran separadas una distancia D = 1000 metros y *ii)* tramo de carretera con una longitud L = 4000 metros donde las RSU/MAGs se encuentran separadas una distancia D = 2000 metros.

Cada experimento se ha repetido 30 veces con diferentes semillas (se proporcionan los intervalos de confianza al 95 %). Las diferentes estadísticas se toman durante 400 segundos de simulación una vez que el tramo de autopista se encuentra repleto de vehículos. Para cada vehículo, las medidas se toman desde el momento en el que este entra en el escenario de simulación hasta que sale de él tras recorrer el segmento de carretera.

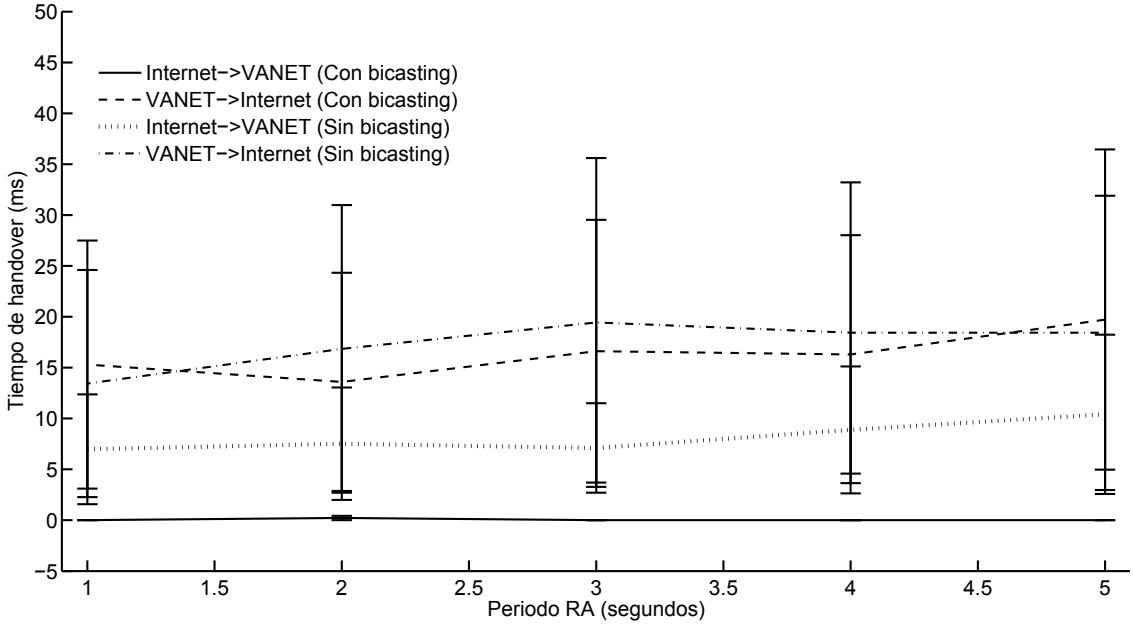


Figura 6.3: Tiempo de *hand-over* (1000 metros).

6.3.2. Análisis del procedimiento de *hand-over* y configuración de direcciones

Esta sección se centra en la evaluación del procedimiento de *hand-over* de la solución y del impacto del mecanismo de *bicasting*. Además, se presentan resultados del procedimiento de configuración de direcciones realizado por los vehículos cuando aparecen en la VANET. El análisis se lleva a cabo a partir los resultados de las simulaciones ejecutadas sobre el escenario descrito en la sección anterior.

En primer lugar se muestran los resultados relativos al tiempo de *hand-over*. El tiempo de *hand-over* se ha definido como el tiempo que transcurre desde la recepción en el destino del último paquete de datos que circula a través de la RSU/MAG 1 y la llegada del primer paquete de datos que viaja por la RSU/MAG 2. Esta medida se realiza en ambos sentidos de la comunicación (Internet-VANET y VANET-Internet). Nótese que las medidas del tiempo de *hand-over* se realizan en el destino final del tráfico. De esta manera, se consigue contabilizar el efecto que puede producirse por la pérdida de paquetes o los retardos introducidos en el encaminamiento de los paquetes en la VANET cuando los vehículos cambian de zona geográfica.

Las Figuras 6.3 y 6.4 muestran el tiempo de *hand-over* en función del intervalo de tiempo medio entre envío de mensajes RA para los escenarios en los que las RSU/MAGs se encuentran separadas una distancia de 1000 metros y para el caso en el que la distancia que las separa es de 2000 metros respectivamente. Además, se diferencian los resultados obtenidos cuando el mecanismo de *bicasting* se encuentra activado o desactivado para evaluar su influencia sobre el procedimiento de *hand-over*. Como se puede apreciar en las figuras, tanto cuando la separación entre RSU/MAGs es de 1000 metros, como cuando la distancia entre RSU/MAGs es de 2000

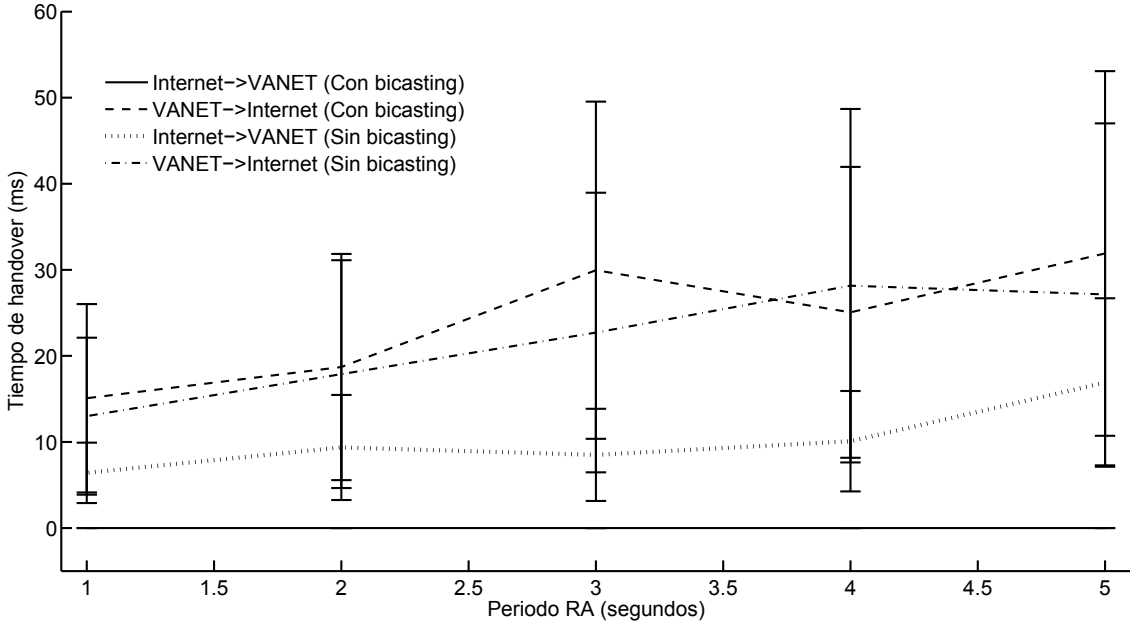


Figura 6.4: Tiempo de *hand-over* (2000 metros).

metros, el tiempo de *hand-over* se sitúa por debajo de los 30 milisegundos en ambos sentidos de la comunicación (Internet-VANET y VANET-Internet). Nótese que como el tiempo entre paquetes del patrón de tráfico utilizado para las medidas es de 10 milisegundos, tenemos un error de precisión en la media.

Por otro lado, el tiempo de *hand-over* es ligeramente mayor cuando las RSU/MAGs se encuentran separadas una distancia de 2000 metros que cuando la separación es de 1000 metros. Esto se debe a que cuanto mayor sea la distancia entre el límite del área geográfica y la RSU/MAG, más saltos deberán realizar los paquetes entre el vehículo y la RSU/MAG, por lo que más probable será que aparezca alguna inestabilidad en el encaminamiento de los paquetes en el momento en el que se realiza el cambio a la nueva zona geográfica. Esto también está relacionado con la ligera tendencia creciente con el periodo de envío de mensajes RA que se puede observar sobre todo en el escenario en el que la separación entre RSU/MAGs es de 2000 metros. Cuanto mayor es el periodo entre mensajes RA no solo más tarde se comenzará el procedimiento de *hand-over* una vez que el vehículo entra en la zona geográfica de la RSU/MAG 2, sino que también menor será el refresco de la información de la TL de los nodos (recuérdese que como se mencionó en la Sección 5.4.2.1, los mensajes RA que distribuye la RSU/MAG dentro de su área geográfica sirven para actualizar la información de la posición de los vecinos en la TL de los nodos), lo que puede provocar errores en el encaminamiento de los paquetes que se reflejen en la medida del tiempo de *hand-over*. Nótese que el procedimiento de *hand-over* se realiza cuando el vehículo se encuentra en la zona más lejana de la RSU/MAG donde es más probable que se produzcan errores en el encaminamiento de los paquetes.

También puede observarse que la medida del tiempo de *hand-over* en el sentido Internet-

VANET es inferior que en el sentido VANET-Internet. Esto se debe a que el retardo sufrido en la VANET por los paquetes procedentes de la RSU/MAG 1 es mayor que el que experimentan los paquetes que provienen de la RSU/MAG 2. Es decir, el paquete que circula por la RSU/MAG 1 se retrasa y provoca que la diferencia de tiempo entre este y el paquete recibido a través de la RSU/MAG 2 se reduzca. De hecho, se ha comprobado en las simulaciones que en ocasiones, el vehículo recibe los paquetes desordenados porque el paquete que circula por la RSU/MAG 2 llega antes que el paquete que viaja a través de la RSU/MAG 1. Además, esto ocurre con mayor frecuencia en el sentido Internet-VANET que en el sentido VANET-Internet, lo que hace que el tiempo de *hand-over* obtenido en el sentido Internet-VANET sea menor que en el sentido VANET-Internet. El motivo por el que esto sucede más en el sentido Internet-VANET es porque alcanzar un vehículo en movimiento puede ocasionar más problemas de encaminamiento que llegar a un nodo fijo como la RSU/MAG (y más cuando el vehículo se encuentra en el punto más lejano de la RSU/MAG, en el límite del área geográfica).

Respecto al mecanismo de *bicasting*, se puede observar en las figuras que su influencia es nula en el sentido VANET-Internet de la comunicación mientras que en el sentido Internet-VANET hace que el tiempo de *hand-over* se reduzca a cero. Este resultado es lógico ya que el mecanismo de *bicasting* únicamente afecta al flujo de datos en el sentido Internet-VANET. Cuando se detecta que el vehículo ha entrado en el área geográfica de la RSU/MAG 2, el LMA comienza a realizar *bicasting* de los paquetes de datos en el sentido Internet-VANET. Como consecuencia, el vehículo recibe los paquetes duplicados procedentes de ambas RSU/MAGs. Como el vehículo comienza a recibir paquetes desde la RSU/MAG 2 incluso antes de comenzar el procedimiento de *hand-over*, el tiempo de *hand-over* se reduce a cero. Sin embargo, hay que tener en cuenta que cuando el mecanismo de *bicasting* no se aplica, el tiempo de *hand-over* obtenido en el sentido Internet-VANET es menor de 10 ms gracias a que el *hand-over* es *make-before-break* (nótese que el intervalo entre paquetes de datos es de 10 ms). De esto se deduce que el mecanismo de *bicasting* no introduce grandes mejoras de prestaciones.

Las medidas sobre el número de paquetes perdidos durante el procedimiento de *hand-over* se encuentran representadas en las Figuras 6.5 y 6.6. Al igual que el tiempo de *hand-over*, las medidas de paquetes perdidos durante el *hand-over* se realizan en el destino final del tráfico para contabilizar el efecto que puede tener el encaminamiento de los paquetes en la VANET cuando los vehículos cambian de área geográfica. La Figura 6.5 se corresponde con el escenario en el que las RSU/MAGs se encuentran separadas 1000 metros, mientras la Figura 6.6 muestra los resultados cuando la distancia entre RSU/MAGs es de 2000 metros. Se puede observar cómo independientemente de la activación o desactivación del mecanismo de *bicasting*, no se producen pérdidas durante el *hand-over*. Esto se debe a que tal y como se ha diseñado el procedimiento de *hand-over*, no es necesario que los vehículos pierdan la conectividad con la RSU/MAG anterior antes de obtener conectividad a través de la nueva RSU/MAG. De esta manera, aunque el vehículo se mueva a otra zona geográfica y se conecte a una nueva RSU/MAG, puede continuar recibiendo paquetes pendientes de la antigua RSU/MAG. Se trata de un *hand-over make-before-break*.

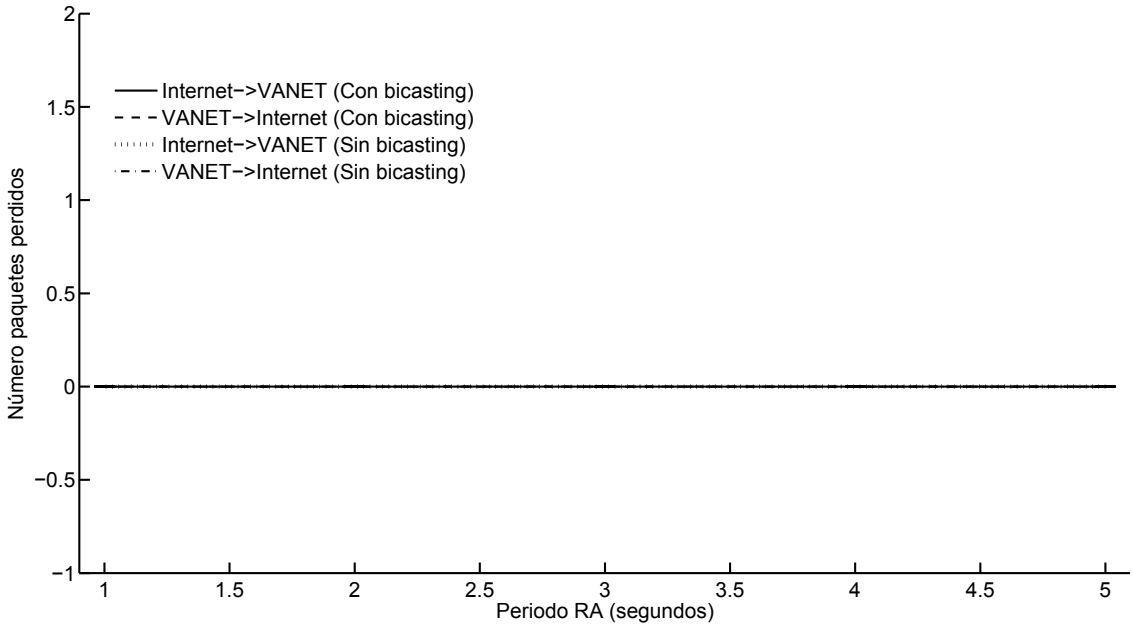


Figura 6.5: Paquetes perdidos durante el *hand-over* (1000 metros).

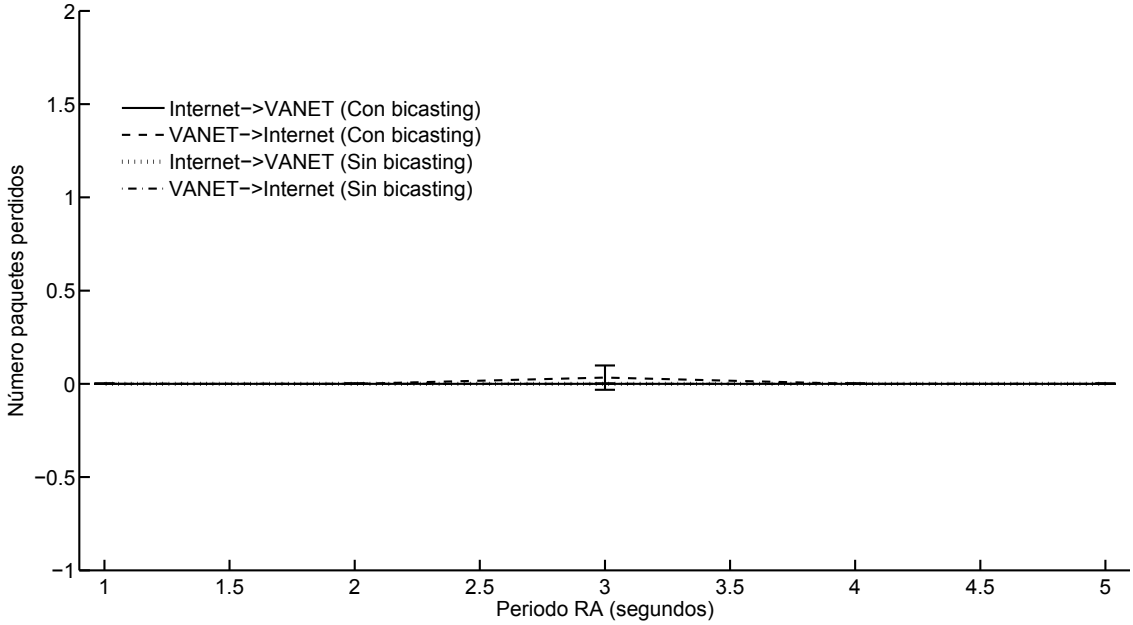


Figura 6.6: Paquetes perdidos durante el *hand-over* (2000 metros).

A la vista de estos resultados se puede concluir que no resulta conveniente la aplicación del mecanismo de *bicasting* en un escenario como el nuestro en el que el *hand-over* es *make-before-break*, ya que el impacto que produce no resulta productivo y el coste del *bicasting* es la introducción de mayor sobrecarga en la VANET. Como se resaltó en el Capítulo 5 es fundamental evitar la introducción de sobrecarga en la red que reduzca la capacidad de la VANET ya que se puede limitar el correcto funcionamiento de las comunicaciones.

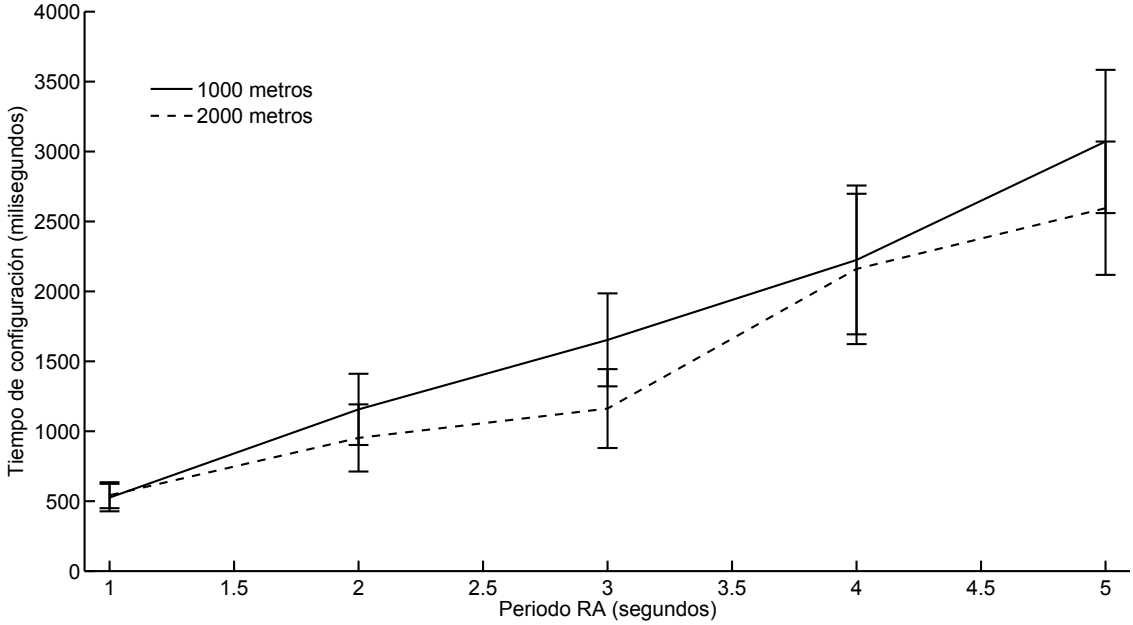


Figura 6.7: Tiempo de configuración de la solución.

Como consecuencia, a partir de aquí en adelante se considera que el mecanismo de *bicasting* se encuentra deshabilitado.

Por otro lado, se ha estudiado el tiempo de configuración, que se ha definido como el tiempo que transcurre desde que el vehículo entra en el escenario de simulación en el área geográfica 1, hasta que recibe el mensaje RA *geo-unicast* de la RSU/MAG 1 con el prefijo asignado por el LMA y puede configurar una dirección IPv6 global. La Figura 6.7 muestra el tiempo de configuración para los dos despliegues de RSU/MAGs que se han considerado (separación de 1000 metros y 2000 metros). En la gráfica se observa cómo el tiempo configuración es directamente proporcional al periodo de envío de mensajes RA. Cuanto mayor es el intervalo entre mensajes RA distribuidos por las RSU/MAGs, mayor es el tiempo medio que un nuevo vehículo que aparece en la VANET tarda en recibir el mensaje RA procedente de la RSU/MAG 1 que da comienzo al procedimiento de obtención de una dirección IPv6 global. Comparando el resultado de ambos escenarios en los que la separación entre RSU/MAGs es de 1000 y 2000 metros, los tiempos de configuración son estadísticamente semejantes ya que si se desprecia el tiempo de distribución en el área de los mensajes RA, el tiempo de configuración es independiente de la distancia entre RSU/MAGs.

Como se mencionó anteriormente, no se produce pérdidas de paquetes durante el procedimiento de *hand-over*, por lo que la tasa de entrega de paquetes no se verá afectada por el mismo. En cambio, durante el tiempo de configuración inicial al entrar al dominio localizado, los vehículos no pueden enviar ni recibir paquetes de datos porque no disponen de una dirección IPv6. A continuación se muestran los resultados de la tasa de entrega de paquetes medida desde el momento en el que el vehículo entra en el escenario de simulación hasta que sale del tramo de carretera, por lo que dentro de esta medida se recoge el tiempo que el vehículo tarda en configurar

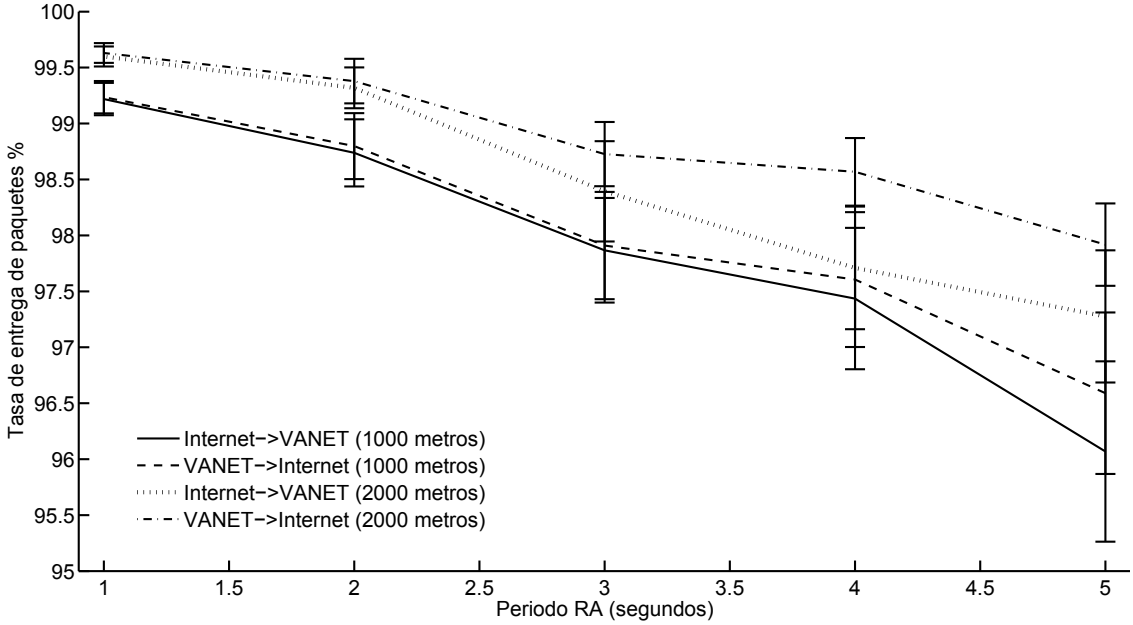


Figura 6.8: Tasa de entrega de paquetes de la solución.

una dirección IPv6 global cuando entra en el escenario de simulación. La Figura 6.8 muestra los resultados de ambos flujos CBR (Internet-VANET y VANET-Internet) en función del intervalo de tiempo medio entre envío de mensajes RA configurado en las RSUs. Se diferencian los resultados obtenidos en el caso en el que la separación entre RSU/MAGs es de 1000 metros del caso en el que la separación entre RSU/MAGs es de 2000 metros. De forma general se puede apreciar cómo la tasa de entrega de paquetes decrece conforme aumenta el intervalo de tiempo entre la distribución de mensajes RA. Esto se debe a que cuanto mayor sea el intervalo de tiempo entre mensajes RA, mayor será el tiempo que un nodo tarda en configurar una dirección IPv6 cuando entra en el escenario de simulación, lo que provocará que la tasa de entrega de paquetes disminuya. Como cuando un vehículo entra en la simulación no dispone de una dirección IPv6 global con la que poder establecer comunicaciones, los paquetes de aplicación enviados durante el tiempo de configuración se descartan.

Por otro lado, se puede observar cómo la tasa de entrega de paquetes en el sentido Internet-VANET es ligeramente inferior a la del sentido VANET-Internet debido a que entregar un paquete a un nodo fijo como la RSU es más sencillo que entregárselo a un nodo en movimiento. Los vehículos siempre conocen la posición geográfica exacta de la RSU al tratarse de un nodo fijo, mientras que si el destino es un vehículo en movimiento, los nodos que reenvían el paquete necesitan conocer de manera lo más precisa posible la posición del destino ya que de otra forma la entrega del paquete puede fallar.

Un resultado que puede llamar la atención es el hecho de que cuando las RSU/MAGs se encuentran separadas 1000 metros, la tasa de entrega de paquetes es inferior que en el caso en el que la separación es de 2000 metros, a pesar de que el número de saltos experimentados por

los paquetes es menor y por lo tanto la probabilidad de perder paquetes en la cadena de reenvío se reduce. Este efecto se debe a que el descarte de paquetes durante el tiempo de configuración (cuando es la única fuente de pérdida de paquetes) tiene un impacto mayor en el caso en el que las RSU/MAGs se encuentran separadas 1000 metros que cuando la separación es de 2000 metros. Si el tiempo que el vehículo tarda en recorrer el escenario de simulación es menor, el número total de paquetes enviados en la simulación es menor y por lo tanto, el peso de los paquetes descartados durante el tiempo de configuración es mayor.

En cualquier caso, la tasa de entrega de paquetes obtenida para los casos simulados en los dos escenarios de separación entre RSU/MAGs (1000 metros y 2000 metros) en ambos sentidos de la comunicación es superior al 95 % incluso incluyendo los paquetes descartados durante el tiempo de configuración. Además, nótese que aunque se ha analizado en detalle, la pérdida de paquetes durante el tiempo de configuración inicial de una dirección IPv6 tiene una importancia relativa, ya que se corresponde con un momento de arranque en el que generalmente las aplicaciones no habrán comenzado a intercambiar tráfico y se produce una única vez, cuando el vehículo aparece en la VANET.

A la vista de estos resultados se puede concluir que la solución propuesta resulta viable, ya que el procedimiento de configuración de direcciones IP funciona correctamente y, como no se pierden paquetes en el *hand-over* ni se introduce un retardo significativo a la comunicación, tenemos un *hand-over* sin interrupción por tratarse de un *hand-over make-before-break*. Sin embargo, hasta el momento se ha considerado que únicamente un vehículo establece comunicaciones con un patrón de tráfico de datos que no es común en la realidad. Por ello, en la siguiente sección se analiza el comportamiento general de la solución considerando el envío de diferentes patrones de tráfico CBR UDP en el caso en el que múltiples vehículos establecen comunicaciones con el CN.

6.3.3. Análisis general de la solución con diferentes patrones de tráfico de datos

Una vez que se ha estudiado y validado el procedimiento de *hand-over* descartándose la aplicación del mecanismo de *bicasting* (su efecto no resulta relevante para el coste de sobrecarga que se introduce) y se han analizado los resultados relativos al procedimiento de configuración de direcciones IPv6, se procede con un análisis general de la solución. Para este análisis general se ha considerado la posibilidad de que múltiples vehículos puedan establecer comunicaciones con el CN utilizando diferentes patrones de tráfico CBR UDP, obteniendo resultados en los escenarios en los que las RSU/MAGs se encuentran separadas entre sí 1000 y 2000 metros. Los diferentes patrones de tráfico CBR cuentan con la misma tasa de tráfico, pero se diferencian en el tamaño del paquete UDP y el intervalo de tiempo entre paquetes: 1) paquetes de tamaño 160 bytes enviados cada 20 milisegundos, 2) paquetes de tamaño 320 bytes enviados cada 40 milisegundos y 3) paquetes de tamaño 480 bytes enviados cada 60 milisegundos.

La tasa de entrega de paquetes y el retardo extremo a extremo experimentado por lo paquetes en los sentidos Internet-VANET y VANET-Internet frente al porcentaje de vehículos que estable-

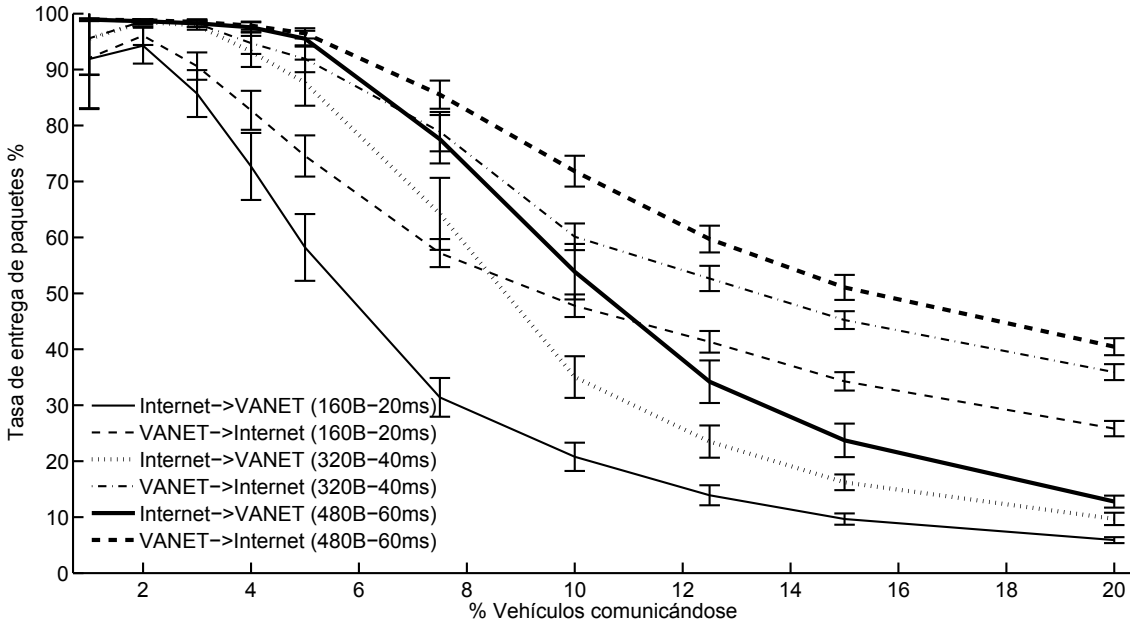


Figura 6.9: Tasa de entrega de paquetes en función del patrón de tráfico UDP (2000 metros)

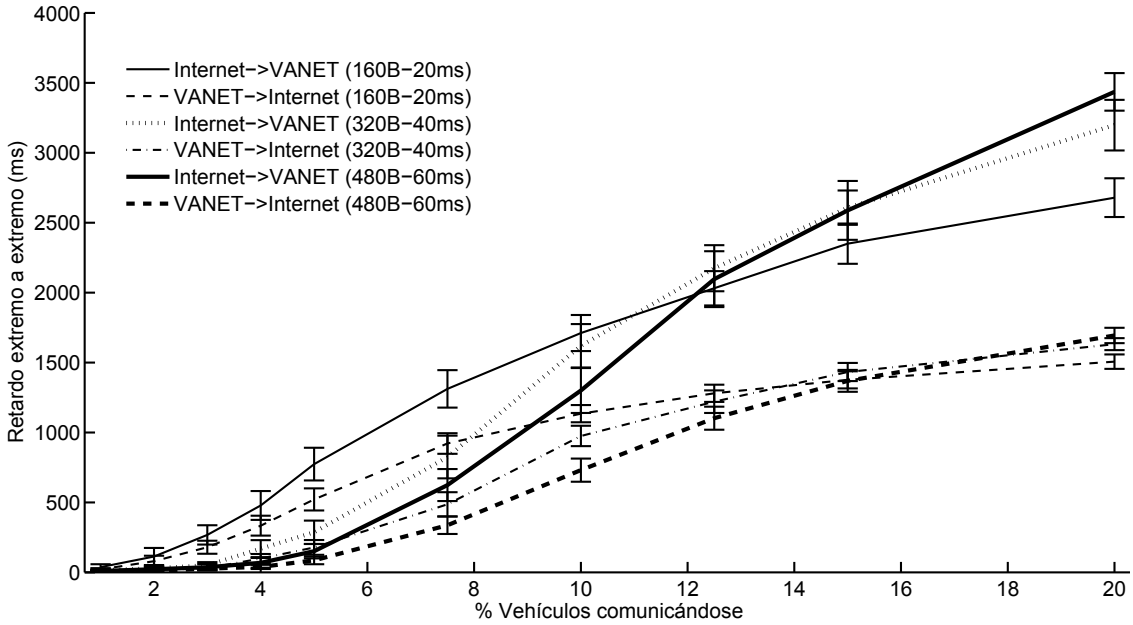


Figura 6.10: Retardo extremo a extremo en función del patrón de tráfico UDP (2000 metros)

cen comunicaciones con el CN se representa en las Figuras 6.9 y 6.10 para el escenario en el que las RSU/MAGs se encuentran separadas una distancia de 2000 metros. Los resultados para el caso en el que la distancia entre las RSU/MAGs es de 1000 metros se muestran en las Figuras 6.11 y 6.12, donde la Figura 6.11 presenta las medidas de la tasa de entrega de paquetes y la Figura 6.12 el retardo extremo a extremo que sufren los paquetes de datos.

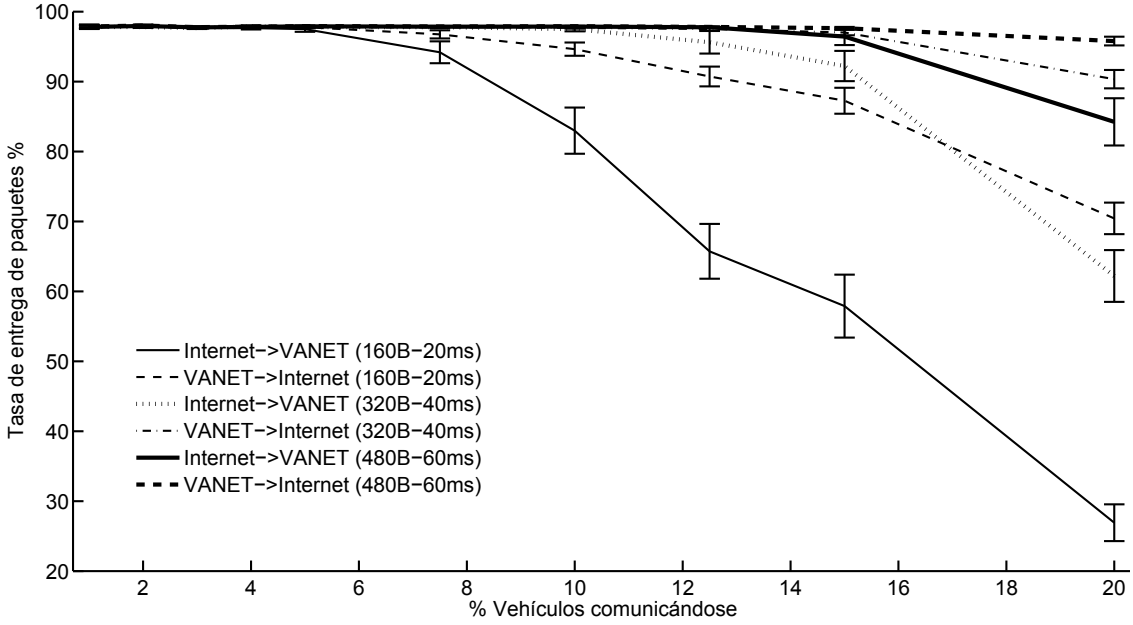


Figura 6.11: Tasa de entrega de paquetes en función del patrón de tráfico UDP (1000 metros)

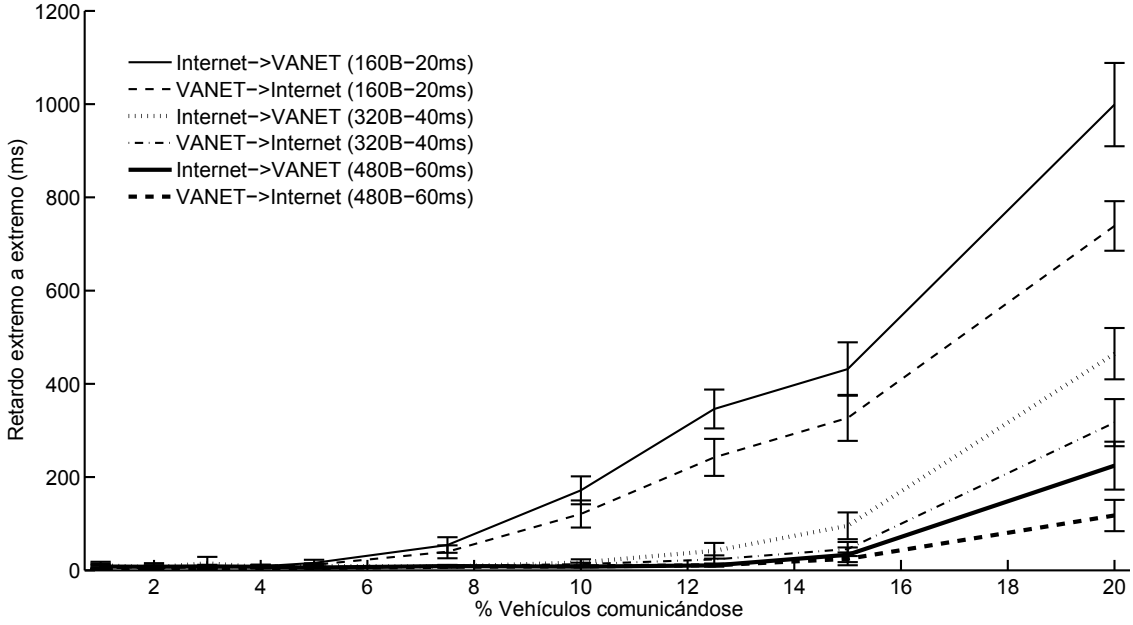


Figura 6.12: Retardo extremo a extremo en función del patrón de tráfico UDP (1000 metros)

De forma general, a la vista de estos resultados se pueden extraer conclusiones análogas a las obtenidas en la Sección 5.4.12 donde se estudió la influencia del patrón del tráfico de datos en las prestaciones del protocolo EGN considerando una única zona geográfica[8]. Se puede observar

[8]Si se realiza una comparación directa entre los resultados obtenidos considerando dos áreas geográficas y los resultados correspondientes a una única zona geográfica, se puede observar que las prestaciones cuando se consideran dos áreas geográficas son inferiores. Esto se debe a dos motivos: 1) En las medidas correspondientes a dos áreas

que las prestaciones decrecen de manera pronunciada cuando se reduce el intervalo de tiempo entre paquetes: la tasa de entrega de paquetes se degrada y el retardo extremo a extremo aumenta. Conforme el tiempo entre paquetes se reduce, el número de transmisiones en el canal inalámbrico se incrementa, produciendo un aumento de la probabilidad de colisión en el medio. Las colisiones en el medio inalámbrico provocan que los paquetes tengan que ser retransmitidos múltiples veces para conseguir que el siguiente salto los reciba correctamente, lo que hace que los paquetes se acumulen en la cola del nivel MAC. Si el nodo no puede transmitir en el medio los paquetes con suficiente rapidez se producen pérdidas de paquetes porque la cola de nivel MAC se satura. Aunque la probabilidad de colisión también aumenta con el tamaño del paquete que se transmite, de las figuras se desprende que el intervalo de tiempo entre paquetes tiene una influencia mayor[9].

Asimismo, cuanto mayor es el porcentaje de vehículos que establecen comunicaciones con el CN, mayor es la carga de tráfico que se genera en la red, lo que produce un aumento de la probabilidad de colisión en el medio inalámbrico que se traduce es una degradación de la tasa de entrega de paquetes y en un aumento del retardo extremo a extremo. Nótese que las colisiones en el medio inalámbrico también pueden producir la pérdida de paquetes de control como los mensajes RA distribuidos por las RSU/MAGs, lo que tiene como consecuencia que la actualización de la información de los vecinos en las TLs de los nodos no sea adecuada.

Todo esto contribuye a una degradación de prestaciones mayor ya que el mecanismo de Detección de Pérdida de Vecino (DPV) actúa cuando no se consigue entregar el paquete al siguiente salto (ya sea por la selección errónea del siguiente salto o por colisiones continuas) introduciendo incluso más carga de tráfico en el canal inalámbrico.

Al igual que se ha mencionado anteriormente al analizar otros resultados, existe una diferencia de prestaciones que depende del sentido de la comunicación: las prestaciones en el sentido Internet-VANET son inferiores que en el sentido VANET-Internet. La explicación a este comportamiento es que por un lado la entrega de paquetes a un nodo fijo como la RSU conlleva menos problemas que entregárselo a un vehículo que se encuentra en movimiento constante. Además, como las RSU/MAGs concentran el tráfico destinado/con origen los vehículos que se encuentran dentro de su área geográfica asignada, estas se encuentran en una posición de desventaja frente al resto de vehículos. Las RSU/MAGs cursan mayor cantidad de tráfico, pero poseen las mismas oportunidades de obtener el canal inalámbrico para transmitir que cualquier otro vehículo. Esto provoca que cuando la carga de tráfico en la red es elevada, las RSU/MAGs no puedan reenviar todo el tráfico que reciben desde Internet y los paquetes en el sentido Internet-VANET se descarten porque la cola del nivel MAC se satura. Como se ha mencionado anteriormente, existen diferentes soluciones para afrontar este problema en redes WLAN en modo infraestructura [125, 126]

geográficas se incluye el tiempo de configuración en las medidas. 2) Tal y como está diseñado el modelo de enlace radio en OMNET++, un escenario de simulación más grande con mayor cantidad de nodos transmitiendo en el canal inalámbrico conlleva un aumento de interferencias, lo que implica más errores en la recepción de los paquetes.

[9] A la hora de analizar los resultados del retardo extremo a extremo hay que tener en cuenta que las medidas solo consideran aquellos paquetes que llegan a alcanzar el destino.

que podrían adaptarse para su aplicación a nuestro escenario, y que se basan en la idea de que los puntos de acceso tengan más ventaja para transmitir en el medio inalámbrico que el resto de estaciones.

Comparando los resultados obtenidos cuando la distancia entre RSU/MAGs es de 2000 metros y cuando la separación es de 1000 metros, se puede observar que las prestaciones son mejores cuando las RSU/MAGs se encuentran separadas a una distancia menor. Cuando las RSU/MAGs se sitúan a una distancia menor entre sí, el tramo de carretera que cubren es más corto por lo que prestan servicio a una menor cantidad de vehículos. Además, la distancia en número de saltos entre los vehículos y las RSU/MAGs se reduce por lo que los paquetes tienen que ser retransmitidos menos veces. Todo esto tiene como consecuencia que la congestión del canal inalámbrico sea menor y que las prestaciones mejoren.

Sin embargo, en cuanto el porcentaje de vehículos que se comunican con el CN aumenta, las prestaciones se degradan bruscamente en ambos escenarios (separación entre RSU/MAGs de 1000 y 2000 metros). La carga de tráfico en la red provoca colisiones que hacen que las comunicaciones no se puedan mantener. Los paquetes se descartan porque las colas del nivel MAC de los nodos se saturan.

Como se comentó en el Capítulo 5, aunque esta degradación de prestaciones no es un problema del protocolo de encaminamiento ni en este caso de la solución de gestión de movilidad propuesta, se pone de manifiesto que la escasez de capacidad en la VANET limita la correcta operación de las comunicaciones entre los vehículos y las RSU/MAGs. De aquí se deprende la necesidad de aumentar la capacidad del canal inalámbrico (mejoras en la tecnología de acceso que aumente su capacidad) o de distribuir la capacidad disponible de una manera adecuada para mejorar las comunicaciones por medio de mecanismos de control de congestión como los trabajos que se están llevando a cabo en el ETSI [123, 124].

Por último, mencionar que la solución que hemos propuesto para integrar PMIPv6 en la arquitectura del sistema de transporte inteligente del ETSI permite a los nodos configurar una dirección IPv6 global correctamente y mantener la continuidad de sus comunicaciones cuando realizan un *hand-over* entre RSU/MAGs, evitando la pérdida de paquetes sin introducir retardos de *hand-over* significativos. La combinación de esta solución con el protocolo EGN no ha introducido ninguna degradación de prestaciones y por lo tanto, no tiene ningún efecto sobre los resultados obtenidos durante su análisis en el Capítulo 5.

6.4. Conclusiones

Este capítulo se ha centrado en la presentación de una solución para proporcionar a la VANET conectividad a Internet basada en la combinación de PMIPv6 [61] con la arquitectura del sistema de transporte inteligente estandarizada por el ETSI [87] y su protocolo de *GeoNetworking* [36].

Esta solución proporciona por un lado, los procedimientos necesarios para que los vehículos puedan obtener una dirección IPv6 global con la que poder comunicarse con otros nodos de Internet, y por otro lado, gestiona la movilidad de los vehículos para que puedan mantener sus comunicaciones activas cuando modifican su punto de conexión a Internet entre RSUs. La utilización de PMIPv6 como protocolo de gestión de movilidad tiene la ventaja de que permite una mayor eficiencia en los *hand-overs* si el LMA se sitúa cerca de la VANET. Además, como la movilidad se gestiona desde la red, no son necesarias configuraciones de seguridad complejas para la movilidad en los vehículos. Asimismo, si se integra la solución de movilidad de la VANET con otras partes de la red de los operadores donde se utiliza PMIPv6, los vehículos podrían conectarse a Internet a través de diferentes tecnologías de acceso sin cambiar su dirección IP, lo que les permitiría mantener sus comunicaciones activas cuando las mueven entre diferentes redes de acceso.

PMIPv6 fue diseñado inicialmente para escenarios en los que el MN se encuentra directamente conectado con la MAG. Por ello, se han propuesto una serie de procedimientos que permiten adaptar PMIPv6 al entorno de las VANETs multisalto y de esta manera poder realizar la integración con la arquitectura del sistema de transporte inteligente del ETSI y su protocolo de GN, o nuestra versión mejorada, EGN. Mediante la utilización de estos procedimientos, los vehículos pueden configurar una dirección IPv6 global con la que establecer comunicaciones con Internet. Además, el *hand-over* entre RSU/MAGs es eficiente, permite mantener la continuidad de las comunicaciones, y no requiere de soluciones adicionales como *bicasting* de tráfico.

La evaluación de la viabilidad de la solución y el análisis del impacto del mecanismo de *bicasting* se ha realizado a través de simulación utilizando trazas de tráfico reales de una importante autopista de circunvalación de Madrid. En un primer análisis centrado en el procedimiento de *hand-over*, se concluyó que el *hand-over make-before-break* entre RSU/MAGs resulta eficiente, no introduce retardos significativos ni pérdida de paquetes, y no requiere de soluciones adicionales como *bicasting* de tráfico. Aunque con la aplicación del mecanismo de *bicasting* se reduce el tiempo de *hand-over* a cero en el sentido Internet-VANET de la comunicación, el impacto que produce no resulta productivo porque independientemente de la activación o desactivación del mecanismo, no se producen pérdidas de paquetes ni retardos relevantes durante el *hand-over*. Además, como el mecanismo envía los paquetes en *bicasting* desde las RSUs cuando se detecta que un vehículo va a realizar un *hand-over*, su aplicación implica la introducción de mayor sobrecarga de tráfico, que reduce la capacidad de la VANET. Por lo tanto, la mejor opción es la de deshabilitar el mecanismo de *bicasting*.

Por otro lado, los resultados obtenidos revelan que la tasa de entrega de paquetes no se ve afectada por el procedimiento de *hand-over*, debido a que tal y como se ha diseñado, aunque un vehículo se vincule a una nueva RSU en una nueva zona geográfica, puede continuar recibiendo paquetes procedentes de la RSU del antiguo área. En cambio, el análisis del procedimiento de configuración de dirección IP reveló que la tasa de entrega de paquetes sí que se ve afectada por el tiempo de configuración de los vehículos (el tiempo de configuración es directamente proporcio-

nal al intervalo de tiempo entre mensajes RA distribuidos por las RSUs) ya que estos no pueden enviar ni recibir paquetes de datos porque no disponen de una dirección IPv6 cuando aparecen en la VANET. En cualquier caso, los resultados de la tasa de entrega de paquetes obtenidos durante las simulaciones, sin problemas de capacidad en la VANET, son cercanos al 100 %. Además, hay que tener en cuenta que el tiempo de configuración inicial de una dirección IP tiene una importancia relativa, ya que únicamente se realiza una vez cuando el vehículo aparece en la VANET, y por lo general, las aplicaciones no se verán afectadas porque todavía no habrán comenzado a intercambiar tráfico cuando arranca el sistema.

Como conclusión de este primer análisis se desprende que los resultados de las simulaciones validan la viabilidad de la solución propuesta y aconsejan las desactivación del mecanismo de *bicasting*.

En una segunda fase de la evaluación se analizó el comportamiento general de la solución conjuntamente con el protocolo EGN utilizando diferentes patrones de tráfico CBR UDP en el caso en el que múltiples vehículos pueden establecer comunicaciones con el CN. Los resultados obtenidos confirman la viabilidad de la solución que hemos propuesto para integrar PMIPv6 con la arquitectura del sistema de transporte inteligente del ETSI ya que, permite que los vehículos configuren direcciones IPv6 globales satisfactoriamente, se mantiene la continuidad de las comunicaciones cuando se realiza el *hand-over* entre MAG/RSUs y, no repercute en las prestaciones observadas del protocolo EGN. En otras palabras, los resultados obtenidos siguen la misma línea que los obtenidos durante el análisis del protocolo EGN en el Capítulo 5 y no se han visto alterados por la introducción de la solución de integración con PMIPv6 que se ha propuesto.

Parte III

Conclusiones y trabajos futuros

Capítulo 7

Conclusiones

En los últimos años, las redes vehiculares o *Vehicular Ad hoc NETworks* (VANETs) han recibido la atención de la comunidad investigadora e industrial ya que su aplicación al ámbito de la seguridad vial puede ayudar a reducir el número de víctimas en accidentes de tráfico. Las VANETs también despiertan interés por otro tipo de aplicaciones como aquellas orientadas a la eficiencia del tráfico o las aplicaciones de entretenimiento y servicios de información.

La conexión a Internet de los vehículos permitiría a sus ocupantes el acceso a multitud de servicios de información y utilizar cualquiera de los servicios comunes de las redes IP como la navegación web o el correo electrónico. El acceso a Internet se está convirtiendo en un hecho cotidiano en la vida de las personas que demandan cada vez más disponer de conexión a Internet desde cualquier lugar, incluyendo los vehículos particulares y los medios de transporte. Este escenario podría abrir la puerta a un mercado de aplicaciones de Internet que estuviera destinado a los conductores y pasajeros de los vehículos. Además, todo este tipo de servicios atractivos para los usuarios servirían como impulso para acelerar la penetración en el mercado de la tecnología.

El comité técnico del sistema de transporte inteligente del ETSI, *European Telecommunications Standards Institute Technical Committee Intelligent Transport System* (ETSI TC ITS), ha visto el impacto que las redes vehiculares pueden tener en la sociedad y en los últimos años ha estado trabajando en la definición de la arquitectura y los protocolos de comunicaciones para un sistema de transporte inteligente (ITS) estandarizado. El trabajo realizado en esta Tesis Doctoral ha estado centrado en el análisis de los aspectos relacionados con la conexión de los vehículos a Internet en el sistema de transporte inteligente estandarizado por el ETSI en escenarios de autovía/autopista.

Una de las principales contribuciones de esta Tesis Doctoral ha consistido en el profundo análisis del protocolo de encaminamiento utilizado en la VANET del sistema de transporte inteligente definido por el ETSI, denominado protocolo de *GeoNetworking* (GN). Uno de los aspectos críticos para que los vehículos puedan conectarse a Internet de forma satisfactoria es que el protocolo de encaminamiento que se utiliza en la VANET ofrezca unas prestaciones adecuadas que

permitan que las comunicaciones funcionen correctamente a pesar de la inestabilidad de los enlaces entre nodos, característica de las redes vehiculares. El estudio de prestaciones basado en simulación que se ha llevado a cabo ha revelado el comportamiento de los mecanismos del protocolo, resaltando sus limitaciones y puntos débiles.

De hecho, las prestaciones del protocolo de GN cuando se proporciona conectividad a Internet a los vehículos de la VANET son insatisfactorias. Por ello, otra de las contribuciones del trabajo realizado en esta Tesis Doctoral es la propuesta de la aplicación de diferentes optimizaciones que consiguen mejorar su funcionamiento:

- Con la intención de evitar enviar tráfico a una posición geográfica desactualizada donde el destino final no puede recibirlo porque se ha movido, se puede ajustar el tiempo de caducidad de la TL teniendo en cuenta el radio de cobertura de los nodos y la velocidad máxima con la que se desplazan los vehículos.
- Se precisa de la introducción de un retardo aleatorio cuando los nodos retransmiten los paquetes *broadcast* en la VANET para distribuir temporalmente el acceso al canal inalámbrico y reducir las colisiones entre paquetes.
- Se ha propuesto mejorar el mecanismo de detección de paquetes duplicados para evitar descartar paquetes cuando estos se reciben desordenados, algo que es común en redes vehiculares.
- Mediante la combinación del mecanismo de la Detección de Pérdida de Vecino (DPV) y del mecanismo de predicción de la posición geográfica de los vecinos se consigue una gran mejora de las prestaciones.
- La cabecera del protocolo de GN debería seguir manteniendo la información de posicionamiento del último nodo que transmite el paquete, a pesar de su eliminación en el borrador de la nueva versión del estándar [110]. Esto permite que las prestaciones sean mejores porque, por un lado, los nodos disponen de más fuentes de información para actualizar su TL, y por otro lado, la reinicialización del temporizador de *beaconing* cuando se envían otros paquetes de GN permite reducir la carga de señalización.
- El mecanismo de *keep-alive* para el Servicio de Localización permite minimizar la sobrecarga de señalización cuando el tráfico de datos es unidireccional el sentido Internet-VANET. Además, actualiza la posición del destino en la RSU, por lo que esta puede enviar el tráfico de datos a una posición geográfica actualizada donde el destino puede recibirlo.

El impacto y la viabilidad de las diferentes optimizaciones han sido evaluados a través de simulación concluyendo que, gracias a la aplicación de estos mecanismos, se consigue un importante aumento de prestaciones en las comunicaciones entre los vehículos y las RSUs que ofrecen conectividad a Internet.

Por otro lado, para que los vehículos puedan mantener comunicaciones con Internet se precisa de un mecanismo de asignación y configuración de direcciones IP en la VANET. Asimismo, como los vehículos cambian su punto de acceso a Internet entre RSUs con su desplazamiento, se necesita un mecanismo que gestione la movilidad y que permita mantener las comunicaciones de los vehículos activas a pesar de los continuos *hand-overs* entre RSUs. Otra de las principales contribuciones del trabajo realizado en esta Tesis Doctoral ha sido la propuesta de una solución para adaptar el protocolo de gestión de movilidad PMIPv6 al entorno multisalto y conseguir su integración con la arquitectura del sistema de transporte inteligente estandarizada por el ETSI y su protocolo de GN. La utilización de PMIPv6 como protocolo de gestión de movilidad permite una mayor eficiencia en los *hand-overs* que los vehículos realizan entre puntos de acceso a Internet. Además, PMIPv6 permite evitar configuraciones de seguridad complejas relacionadas con la movilidad en los vehículos, ya que las funciones de gestión de movilidad IP se realizan desde nodos situados en la red. Además, la progresiva adopción de PMIPv6 como protocolo para soportar la movilidad por parte de los operadores, ofrece la oportunidad de integrar la solución de movilidad de la VANET con otras regiones de sus redes que utilizan otras tecnologías de acceso (como por ejemplo LTE/EPS). De esta forma, la VANET puede verse como una red de acceso *non*-3GPP integrada en la arquitectura 4G y los vehículos pueden conectarse a Internet utilizando diferentes tecnologías de acceso sin cambiar su dirección IP mientras se mueven dentro del LMD, eligiendo la más adecuada para cada situación, y manteniendo sus comunicaciones activas.

La solución de integración de PMIPv6 con la arquitectura del sistema de transporte inteligente estandarizada por el ETSI que se ha propuesto, proporciona los procedimientos necesarios para la configuración de direcciones IPv6 y permite mantener la continuidad de las comunicaciones mediante *hand-overs make-before-break* sin interrupción, que no introducen retardos significativos ni producen pérdidas de paquetes. Esta solución ha sido validada experimentalmente a través de simulación utilizando trazas de tráfico reales de una importante autopista de circunvalación de Madrid, lo que proporciona mayor validez a los resultados obtenidos, ya que las simulaciones se aproximan más una situación real.

Además, se han realizado análisis utilizando diferentes patrones de tráfico de datos. Los resultados de estos análisis muestran que las prestaciones se ven gravemente afectadas por la carga de tráfico en la red. Un incremento de transmisiones de paquetes en el medio inalámbrico aumenta la probabilidad de que los paquetes colisionen, lo que se traduce en una degradación severa de prestaciones. Cabe mencionar que las RSUs se encuentran en una situación de desventaja respecto al resto de vehículos ya que a pesar de que tienen que cursar una mayor cantidad de tráfico (concentran el tráfico de las comunicaciones con Internet de su segmento de carretera asignado) cuentan con las mismas oportunidades de acceder al canal inalámbrico para transmitir que cualquier otro vehículo. Por ello, las RSUs son propensas a la saturación y las prestaciones de los flujos de datos en el sentido Internet-VANET se degradan cuando el tráfico procedente de Internet aumenta. Una forma de mitigar este efecto es reducir la distancia entre RSUs: la carga de las RSUs disminuye porque prestan servicio a un menor número de vehículos y los paquetes tienen

que recorrer una distancia menor, lo que hace que las prestaciones mejoren. Otra alternativa, sería la aplicación de diferentes mecanismos existentes en la literatura que tratan de solucionar este problema en redes WLAN en modo infraestructura [125, 126], adaptándolos a nuestro escenario. Asimismo, los resultados ponen de manifiesto que la capacidad en la VANET es una limitación importante para el correcto funcionamiento de las comunicaciones entre los vehículos y la RSU. Se precisa de la introducción de mecanismos que incrementen la capacidad del canal inalámbrico o que distribuyan la capacidad disponible adecuadamente para mejorar las comunicaciones en la VANET [123, 124].

Capítulo 8

Trabajos futuros

A continuación se exponen los asuntos que se ha considerado que sería interesante estudiar como extensión del trabajo realizado en esta Tesis Doctoral:

- El principal objetivo del trabajo realizado en esta Tesis Doctoral ha sido el análisis de los problemas que aparecen cuando se proporciona conectividad a Internet a los vehículos del sistema de transporte inteligente estandarizado por el ETSI. Este estudio se ha centrado en escenarios de autovía/autopista que tienen como principal dificultad la gran velocidad a la que se desplazan los vehículos. Sería interesante extender el estudio considerando escenarios urbanos donde la conexión entre los vehículos y las RSUs se realiza probablemente a un único salto porque el mobiliario y los edificios intervienen como obstáculos que dificultan las comunicaciones. Asimismo, se podrían realizar estudios no solo considerando la conexión a Internet de los vehículos donde el tráfico es mayoritariamente *unicast*, sino otro tipo de aplicaciones orientadas a la mejora de la seguridad vial o la eficiencia del tráfico que se basan en la difusión de mensajes en *broadcast*. Además, dado que probablemente se desplegarán múltiples servicios, sería interesante analizar la naturaleza de los servicios que son adecuados para las redes vehiculares (en función de sus requisitos en cuanto a retardos y fiabilidad de las comunicaciones), cómo realizar su conexión con la infraestructura en el caso de que sea necesario, y estudiar su interacción cuando operan de manera simultánea en la VANET.
- En el estudio del protocolo de GN se ha considerado la utilización del algoritmo de *greedy forwarding* para el encaminamiento de los paquetes. Se podrían analizar las prestaciones cuando se utiliza el otro algoritmo de encaminamiento que se propone en el estándar, el algoritmo de *Contention-Based Forwarding* (CBF), para comprobar sus prestaciones en la comunicación con Internet. Además, sería interesante estudiar más en profundidad el comportamiento del protocolo de encaminamiento geográfico cuando se introducen estimadores para calcular la posición actual de los nodos basándose en parámetros de velocidad, dirección, etc.

- Convendría extender la solución de movilidad basada en PMIPv6 que se ha propuesto para incluir diferentes aspectos de seguridad y autenticación con el objetivo de evitar posibles ataques.

- Como la solución de gestión de movilidad que se ha propuesto se basa en PMIPv6, los vehículos pueden realizar *hand-overs* entre diferentes tecnologías de acceso conservando sus comunicaciones activas. Sería interesante realizar estudios sobre diferentes parámetros, estimadores y heurísticos que indiquen el momento apropiado en el que resulta conveniente que los vehículos cambien de tecnología de acceso (incluyendo parámetros de congestión de la red de los operadores que propicien mover las comunicaciones de los vehículos a la VANET).

- Se ha observado cómo las comunicaciones se pueden ver afectadas por la falta de capacidad de la VANET. Sería conveniente realizar estudios sobre mecanismos que mejoraran las capacidades de comunicación en la VANET a través de mejoras en la tecnología de acceso (aumentando su capacidad) o mediante mecanismos de control de congestión que distribuyan de manera adecuada la capacidad disponible entre los nodos.

- Las comunicaciones en la VANET se pueden llevar a cabo gracias a que los usuarios cooperan entre sí encaminando el tráfico de otros usuarios y compartiendo los recursos disponibles honestamente. Sin embargo, puede ocurrir que existan usuarios malintencionados que no colaboren en las comunicaciones y que se apropien de los recursos disponibles en su propio beneficio, perjudicando de esta manera al funcionamiento global del sistema. En este sentido, sería interesante estudiar la introducción de los denominados mecanismos de incentivos (véase por ejemplo [129,130]) en redes vehiculares que promuevan que los usuarios se comporten honestamente y estén dispuestos a cooperar.

Parte IV

Apéndice

Apéndice A

Cabeceras del protocolo de *GeoNetworking*

Este apéndice presenta el formato de las cabeceras de los mensajes más importantes del protocolo de GN definido por el ETSI y que se han utilizado en las simulaciones del trabajo realizado en esta Tesis Doctoral. Recientemente el comité técnico del sistema de transporte inteligente del ETSI ha publicado un borrador de la nueva versión del estándar del protocolo de GN que introduce ciertas modificaciones en las cabeceras del protocolo. A continuación se presenta el formato especificado en la versión del protocolo de GN V1.1.1 [36] y la del borrador, la versión V1.2.1 [110], de manera que este apéndice pueda servir de referencia rápida para observar las diferencias entre ambas versiones.

A.1. Formato de las cabeceras del protocolo de *GeoNetworking* V1.1.1

A continuación se muestra el formato de las cabeceras de los mensajes más importantes del protocolo de GN definido por el ETSI en la versión del estándar V1.1.1.

A.1.1. Estructura de la cabecera de GN

La estructura de la cabecera del protocolo de GN se muestra en la Figura A.1, donde puede observarse que se encuentra divida en dos partes: 1) La cabecera común que se incluye en todos los mensajes del protocolo de GN y contiene información sobre el último nodo que retransmite el mensaje. 2) La Cabecera extendida que depende del tipo de mensaje que se envía. En las siguientes secciones se detalla más información sobre el formato de las mismas.

Cabecera común (288)	Cabecera extendida (-)

Figura A.1: Estructura de la cabecera del protocolo de GN V1.1.1

Identificador de GN (64)					
Marca de Tiempo (32)					
Latitud (32)					
Longitud (32)					
Velocidad (16)	Dirección (16)				
Altitud (16)	PMT (4)	PPos (4)	Pvel (3)	Pdir (3)	PA (2)

Figura A.2: Vector de posición extendido del protocolo de GN V1.1.1

A.1.2. Vector de posición extendido

El vector de posición extendido se incluye en la cabecera común, cabecera del mensaje *geo-unicast*, cabecera del mensaje *geo-broadcast*, cabecera del mensaje *LS Request* y la cabecera del mensaje *LS Reply*. Su formato se representa en la Figura A.2 donde los campos tienen el siguiente significado:

- **Identificador de GN:** se trata del identificador del nivel de GN utilizado por el nodo al que hace referencia el vector de posición.
- **Marca de Tiempo:** indica el instante tiempo en el que se obtuvieron los datos de posición del vector.
- **Latitud:** expresa latitud de la posición geográfica ocupada por el nodo.

- **Longitud:** se trata de la longitud de la posición geográfica ocupada por el nodo.
- **Velocidad:** indica la velocidad a la que se desplaza el nodo.
- **Dirección:** expresa la dirección con la que viaja el nodo.
- **Altitud:** se trata de la altitud a la que se encuentra el nodo.
- **PMT (Precisión de la Marca de Tiempo):** es un indicador de la precisión del valor expresado en el campo Marca de Tiempo.
- **PPos (Precisión de la Posición):** se trata de un indicador de la precisión de los valores expresados en los campos Latitud y Longitud.
- **Pvel (Precisión de la velocidad):** es un indicador de la precisión del valor expresado en el campo Velocidad.
- **Pdir (Precisión de la dirección):** se trata un indicador de la precisión del valor expresado en el campo Dirección.
- **PA (Precisión de la Altitud):** es un indicador de la precisión del valor expresado en el campo Altitud.

A.1.3. Vector de posición reducido

El vector de posición reducido se incluye en la cabecera del mensaje *geo-unicast* y la cabecera del mensaje *LS Reply*. Su formato se representa en la Figura A.3 donde los campos tienen el siguiente significado:

- **Identificador de GN:** se trata del identificador del nivel de GN utilizado por el nodo al que hace referencia el vector de posición.
- **Marca de Tiempo:** indica el instante tiempo en el que se obtuvieron los datos de posición del vector.
- **Latitud:** expresa latitud de la posición geográfica ocupada por el nodo.
- **Longitud:** se trata de la longitud de la posición geográfica ocupada por el nodo.

A.1.4. Cabecera común

La cabecera común se incluye en todos los mensajes del protocolo de GN y contiene información sobre el último nodo que retransmite el mensaje, es decir, su contenido se modifica salto a salto. Su formato se representa en la Figura A.4 donde los campos tienen el siguiente significado:

Identificador de GN (64)
Marca de Tiempo (32)
Latitud (32)
Longitud (32)

Figura A.3: Vector de posición reducido del protocolo de GN V1.1.1

Versión (4)	**SC (4)**	**TC (4)**	**STC (4)**	**Reservado (8)**	***Flags* (8)**
Longitud (16)				**CT (8)**	**LS (8)**
Vector de posición extendido del emisor (224)					

Figura A.4: Cabecera común del protocolo de GN V1.1.1

- **Versión:** indica la versión del protocolo de GN.
- **SC (Siguiente Cabecera):** señala el tipo de protocolo de la cabecera que se sitúa por encima del protocolo de GN.
- **TC (Tipo de Cabecera):** se trata de un identificador del tipo de cabecera del protocolo de GN.
- **STC (SubTipo de Cabecera):** se trata de un identificador del subtipo de cabecera del protocolo de GN.
- **Reservado:** campo de uso reservado.
- ***Flags*:** indica el tipo de estación ITS.
- **Longitud:** longitud en bytes de los datos incluidos en el mensaje.

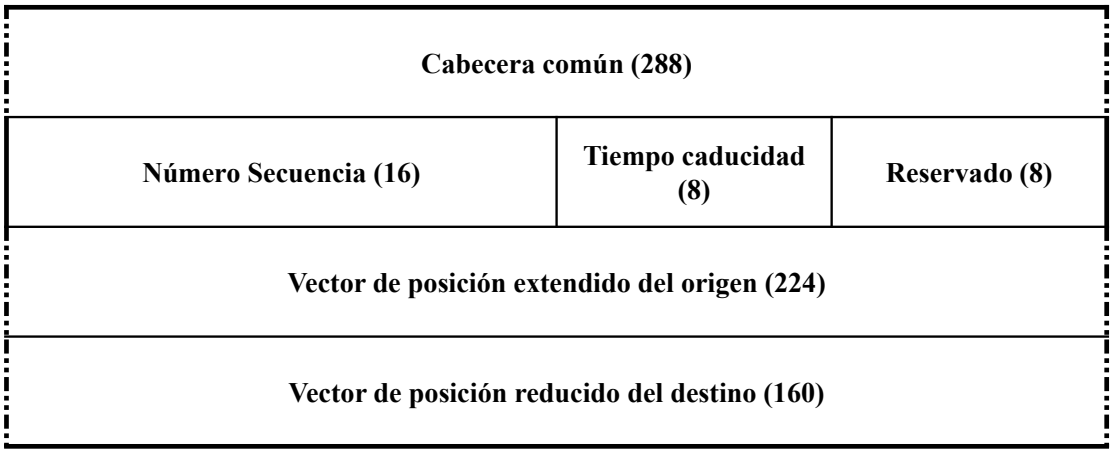


Figura A.5: Cabecera *geo-unicast* del protocolo de GN V1.1.1

- **CT (Clase de Tráfico):** señala la clase de tráfico a la que pertenece el mensaje para asuntos relacionados con la calidad de servicio.
- **LS (Límite de Saltos):** límite de saltos que se reduce en cada retransmisión de manera que el paquete se descarta si su valor llega a 0. Inicialmente se establece a un valor de 10 en el nodo origen.
- **Vector de posición extendido del emisor:** se trata del vector de posición extendido del último nodo que retrasmite el mensaje. Su formato se describe en la Sección A.1.2.

A.1.5. Cabecera *geo-unicast*

La cabecera *geo-unicast* se utiliza cuando se desea entregar el paquete a un nodo destino que se encuentra situado en una posición geográfica determinada. Su formato se muestra en la Figura A.5 donde los campos tienen el siguiente significado:

- **Cabecera común:** se trata de la cabecera común incluida en todos los paquetes del protocolo de GN. Su formato se describe en la Sección A.1.4.
- **Número de secuencia:** es un número de secuencia que se incrementa cada vez que el nodo emisor envía un paquete. El objetivo es detectar bucles en el encaminamiento de los paquetes y paquetes duplicados.
- **Tiempo de caducidad:** expresa el tiempo máximo de vida del paquete de manera que se elimina cuando este tiempo expira. Sirve para evitar que los paquetes se mantengan almacenados indefinidamente en algún *buffer*.
- **Reservado:** campo de uso reservado.

<table>
<tr><td colspan="3">Cabecera común (288)</td></tr>
<tr><td>Número Secuencia (16)</td><td>Tiempo caducidad (8)</td><td>Reservado (8)</td></tr>
<tr><td colspan="3">Vector de posición extendido del origen (224)</td></tr>
<tr><td colspan="3">Latitud zona destino (32)</td></tr>
<tr><td colspan="3">Longitud zona destino (32)</td></tr>
<tr><td>Distancia A (16)</td><td colspan="2">Distancia B (16)</td></tr>
<tr><td>Ángulo (16)</td><td colspan="2">Reservado (16)</td></tr>
</table>

Figura A.6: Cabecera *geo-broadcast* del protocolo de GN V1.1.1

- **Vector de posición extendido del origen:** se trata del vector de posición extendido del nodo origen del mensaje. Su formato se describe en la Sección A.1.2.
- **Vector de posición reducido del destino:** es el vector de posición reducido del destino. Es utilizado por el algoritmo de encaminamiento para, en función de la posición geográfica de los vecinos, elegir el siguiente salto que se encuentra más cerca del destino. Su formato se describe en la Sección A.1.3.

A.1.6. Cabecera *geo-broadcast*

La cabecera *geo-broadcast* se utiliza cuando se desea entregar el paquete a todos los nodos que se encuentran situados dentro una determinada zona geográfica objetivo. Su formato se representa en la Figura A.6 donde los campos tienen el siguiente significado:

- **Cabecera común:** se trata de la cabecera común incluida en todos los paquetes del protocolo de GN. Su formato se describe en la Sección A.1.4.
- **Número de secuencia:** es un número de secuencia que se incrementa cada vez que el

Figura A.7: Mensaje *beacon* del protocolo de GN V1.1.1

nodo emisor envía un paquete. El objetivo es detectar bucles en el encaminamiento de los paquetes y paquetes duplicados.

- **Tiempo de caducidad:** expresa el tiempo máximo de vida del paquete de manera que se elimina cuando este tiempo expira. Sirve para evitar que los paquetes se mantengan almacenados indefinidamente en algún *buffer*.
- **Reservado:** campo de uso reservado.
- **Vector de posición extendido del origen:** se trata del vector de posición extendido del nodo origen del mensaje. Su formato se describe en la Sección A.1.2.
- **Latitud zona destino:** señala la latitud de la posición geográfica del centro de la zona geográfica objetivo. El algoritmo de encaminamiento la utiliza para guiar los paquetes hacia el destino.
- **Longitud zona destino:** expresa la longitud de la posición geográfica del centro de la zona geográfica objetivo. El algoritmo de encaminamiento la utiliza para guiar los paquetes hacia el destino.
- **Distancia A:** se trata de un parámetro de distancia que permite definir la zona geográfica destino.
- **Distancia B:** se trata de un parámetro de distancia que permite definir la zona geográfica destino.
- **Ángulo:** señala la orientación de la zona geográfica destino.

A.1.7. Mensaje *beacon*

Los nodos envían periódicamente mensajes *beacon* en *broadcast* para permitir a sus vecinos conocer diversos parámetros sobre ellos. Su formato se representa en la Figura A.7 donde como puede observarse únicamente está compuesto por la cabecera común en todos los mensajes del protocolo de GN porque contiene información sobre el último emisor del paquete (que en este caso coincide con el origen). El formato de la cabecera común se describe en la Sección A.1.4.

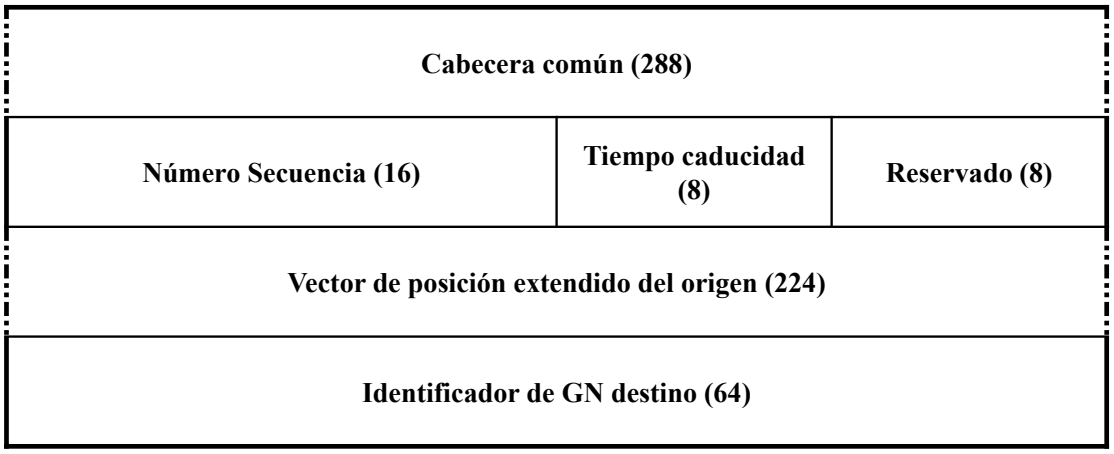


Figura A.8: Mensaje *LS Request* del protocolo de GN V1.1.1

A.1.8. Mensaje *LS Request*

El mensaje *LS Request* se utiliza en el Servicio de Localización cuando un nodo pretende obtener la posición geográfica en la que se encuentra otro nodo de la VANET. El mensaje se retransmite en *broadcast* por la red hasta que llega al nodo objetivo del que se desea obtener su posición geográfica. Su formato se representa en la Figura A.8 donde los campos tienen el siguiente significado:

- **Cabecera común:** se trata de la cabecera común incluida en todos los paquetes del protocolo de GN. Su formato se describe en la Sección A.1.4.
- **Número de secuencia:** es un número de secuencia que se incrementa cada vez que el nodo emisor envía un paquete. El objetivo es detectar bucles en el encaminamiento de los paquetes y paquetes duplicados.
- **Tiempo de caducidad:** expresa el tiempo máximo de vida del paquete de manera que se elimina cuando este tiempo expira. Sirve para evitar que los paquetes se mantengan almacenados indefinidamente en algún *buffer*.
- **Reservado:** campo de uso reservado.
- **Vector de posición extendido del origen:** se trata del vector de posición extendido del nodo origen del mensaje. Su formato se describe en la Sección A.1.2.
- **Identificador de GN destino:** se trata del identificador del nivel de GN utilizado por el nodo destino del que se desea obtener la posición geográfica que ocupa por medio del Servicio de Localización.

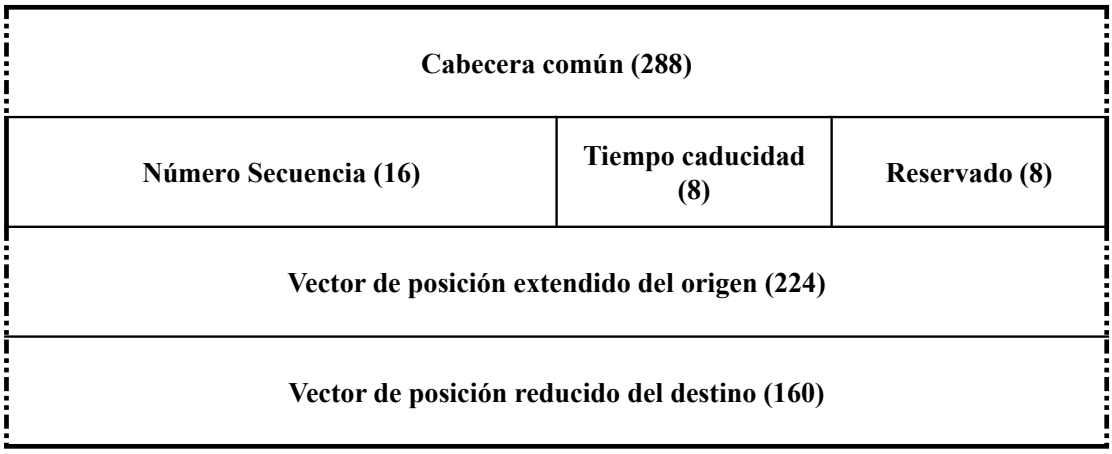


Figura A.9: Mensaje *LS Reply* del protocolo de GN V1.1.1

A.1.9. Mensaje *LS Reply*

El mensaje *LS Reply* se utiliza en el Servicio de Localización y se trata del mensaje que responde el nodo del que se desea la posición geográfica cuando recibe el mensaje *LS Request*. El paquete *LS Reply* se puede encaminar hasta el nodo que envió el mensaje *LS Request* tal y como si fuera un paquete *geo-unicast* gracias a que la posición geográfica del nodo origen se incluye en el mensaje *LS Request*. Su formato se representa en la Figura A.9 donde los campos tienen el siguiente significado:

- **Cabecera común:** se trata de la cabecera común incluida en todos los paquetes del protocolo de GN. Su formato se describe en la Sección A.1.4.
- **Número de secuencia:** es un número de secuencia que se incrementa cada vez que el nodo emisor envía un paquete. El objetivo es detectar bucles en el encaminamiento de los paquetes y paquetes duplicados.
- **Tiempo de caducidad:** expresa el tiempo máximo de vida del paquete de manera que se elimina cuando este tiempo expira. Sirve para evitar que los paquetes se mantengan almacenados indefinidamente en algún *buffer*.
- **Reservado:** campo de uso reservado.
- **Vector de posición extendido del origen:** se trata del vector de posición extendido del nodo origen del mensaje. Su formato se describe en la Sección A.1.2.
- **Vector de posición reducido del destino:** es el vector de posición reducido del destino. Es utilizado por el algoritmo de encaminamiento para, en función de la posición geográfica de los vecinos, elegir el siguiente salto que se encuentra más cerca del destino. Su formato se describe en la Sección A.1.3.

Cabecera básica (32)	Cabecera común (64)	Cabecera extendida (-)

Figura A.10: Estructura de la cabecera del protocolo de GN V1.2.1

A.2. Formato de las cabeceras del protocolo de *GeoNetworking* V1.2.1

A continuación se muestra el formato de las cabeceras de los mensajes más importantes del protocolo de GN definido por el ETSI en la versión del estándar V1.2.1.

A.2.1. Estructura de la cabecera de GN

La estructura de la cabecera del protocolo de GN se muestra en la Figura A.10, donde puede observarse que se encuentra divida en tres partes: 1) La cabecera básica que se incluye en todos los mensajes del protocolo de GN y que no se encuentra cifrada en ningún caso. 2) La cabecera común que se incluye en todos los mensajes del protocolo de GN y que se puede encontrar cifrada. 3) La cabecera extendida que depende del tipo de mensaje que se envía y que también se puede encontrar cifrada. En las siguientes secciones se detalla más información sobre el formato de las mismas.

A.2.2. Vector de posición extendido

El vector de posición extendido se incluye en la cabecera común, cabecera del mensaje *geo-unicast*, cabecera del mensaje *geo-broadcast*, cabecera del mensaje *LS Request* y la cabecera del mensaje *LS Reply*. Su formato se representa en la Figura A.11 donde los campos tienen el siguiente significado:

- **Identificador de GN:** se trata del identificador del nivel de GN utilizado por el nodo al que hace referencia el vector de posición.
- **Marca de Tiempo:** indica el instante tiempo en el que se obtuvieron los datos de posición del vector.
- **Latitud:** expresa latitud de la posición geográfica ocupada por el nodo.
- **Longitud:** se trata de la longitud de la posición geográfica ocupada por el nodo.
- **P (Precisión):** es un indicador de la precisión de los valores expresados en los campos Latitud y Longitud.

<table>
<tr><td colspan="3">Identificador de GN (64)</td></tr>
<tr><td colspan="3">Marca de Tiempo (32)</td></tr>
<tr><td colspan="3">Latitud (32)</td></tr>
<tr><td colspan="3">Longitud (32)</td></tr>
<tr><td>P
(1)</td><td>Velocidad (15)</td><td>Dirección (16)</td></tr>
</table>

Figura A.11: Vector de posición extendido del protocolo de GN V1.2.1

Versión (4)	**SC (4)**	**Reservado (8)**	**Tiempo caducidad (8)**	**LSR (8)**

Figura A.12: Cabecera básica del protocolo de GN V1.2.1

- **Velocidad:** indica la velocidad a la que se desplaza el nodo.
- **Dirección:** expresa la dirección con la que viaja el nodo.

A.2.3. Vector de posición reducido

El vector de posición reducido se incluye en la cabecera del mensaje *geo-unicast* y la cabecera del mensaje *LS Reply*. Su formato es el mismo que en la versión del protocolo de GN V1.1.1 que se describe en la Sección A.1.3.

A.2.4. Cabecera básica

La cabecera básica se incluye en todos los mensajes del protocolo de GN y no se encuentra cifrada en ningún caso. Su formato se representa en la Figura A.12 donde los campos tienen el siguiente significado:

SC (4)	Reservado (4)	TC (4)	STC (4)	Clase Tráfico (8)	*Flags* (8)
Longitud (16)				LSM (8)	Reservado (8)

Figura A.13: Cabecera común del protocolo de GN V1.2.1

- **Versión:** indica la versión del protocolo de GN.
- **SC (Siguiente Cabecera):** señala el tipo de protocolo de la cabecera que sigue a la cabecera básica (cabecera común cifrada o cabecera común sin cifrar).
- **Reservado:** campo de uso reservado.
- **Tiempo de caducidad:** expresa el tiempo máximo de vida del paquete de manera que se elimina cuando este tiempo expira. Sirve para evitar que los paquetes se mantengan almacenados indefinidamente en algún *buffer*.
- **LSR (Límite de Saltos Restantes):** límite de saltos restantes. Este valor se reduce en cada retransmisión de manera que el paquete se descarta si su valor llega a 0.

A.2.5. Cabecera común

La cabecera común se incluye en todos los mensajes del protocolo de GN y se puede encontrar cifrada. Su formato se representa en la Figura A.13 donde los campos tienen el siguiente significado:

- **SC (Siguiente Cabecera):** señala el tipo de protocolo de la cabecera que se sitúa por encima del protocolo de GN.
- **Reservado:** campo de uso reservado.
- **TC (Tipo de Cabecera):** se trata de un identificador del tipo de cabecera del protocolo de GN.
- **STC (SubTipo de Cabecera):** se trata de un identificador del subtipo de cabecera del protocolo de GN.
- **Clase Tráfico:** señala la clase de tráfico a la que pertenece el mensaje para asuntos relacionados con la calidad de servicio.
- ***Flags*:** indica el tipo de estación ITS.

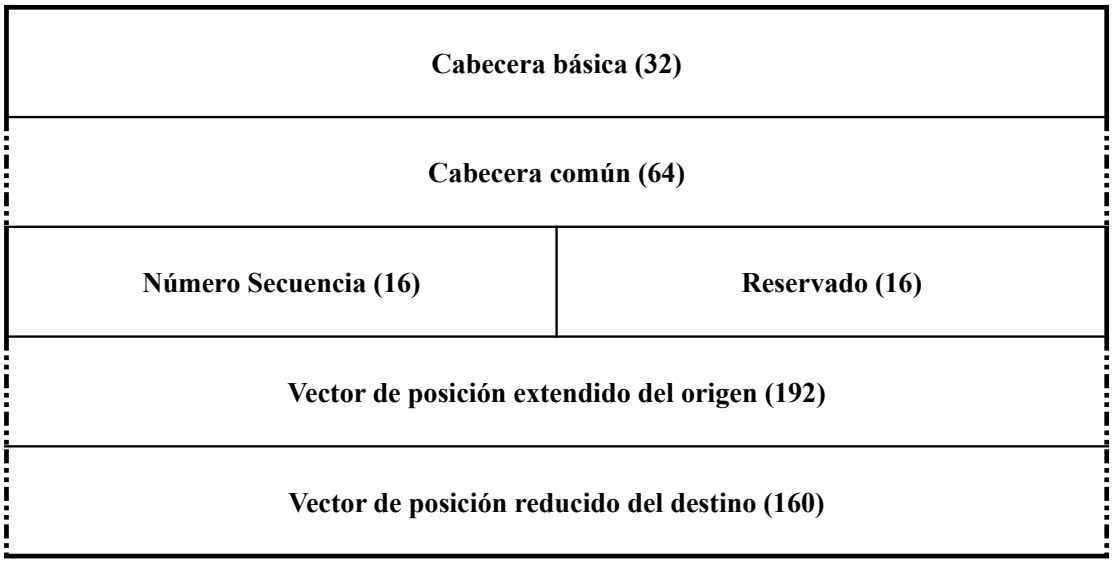


Figura A.14: Cabecera *geo-unicast* del protocolo de GN V1.2.1

- **Longitud:** longitud en bytes de los datos incluidos en el mensaje.
- **LSM (Límite de Saltos Máximo):** indica el límite de saltos máximo que puede dar el paquete. Este campo, a diferencia del campo LSR presente en la cabecera básica, no se reduce en cada retransmisión del paquete. Inicialmente se establece a un valor de 10 en el nodo origen.

A.2.6. Cabecera *geo-unicast*

La cabecera *geo-unicast* se utiliza cuando se desea entregar el paquete a un nodo destino que se encuentra situado en una posición geográfica determinada. Su formato se representa en la Figura A.14 donde los campos tienen el siguiente significado:

- **Cabecera básica:** se trata de la cabecera básica incluida en todos los paquetes del protocolo de GN. Su formato se describe en la Sección A.2.4.
- **Cabecera común:** se trata de la cabecera común incluida en todos los paquetes del protocolo de GN. Su formato se describe en la Sección A.2.5.
- **Número de secuencia:** es un número de secuencia que se incrementa cada vez que el nodo emisor envía un paquete. El objetivo es detectar bucles en el encaminamiento de los paquetes y paquetes duplicados.
- **Reservado:** campo de uso reservado.

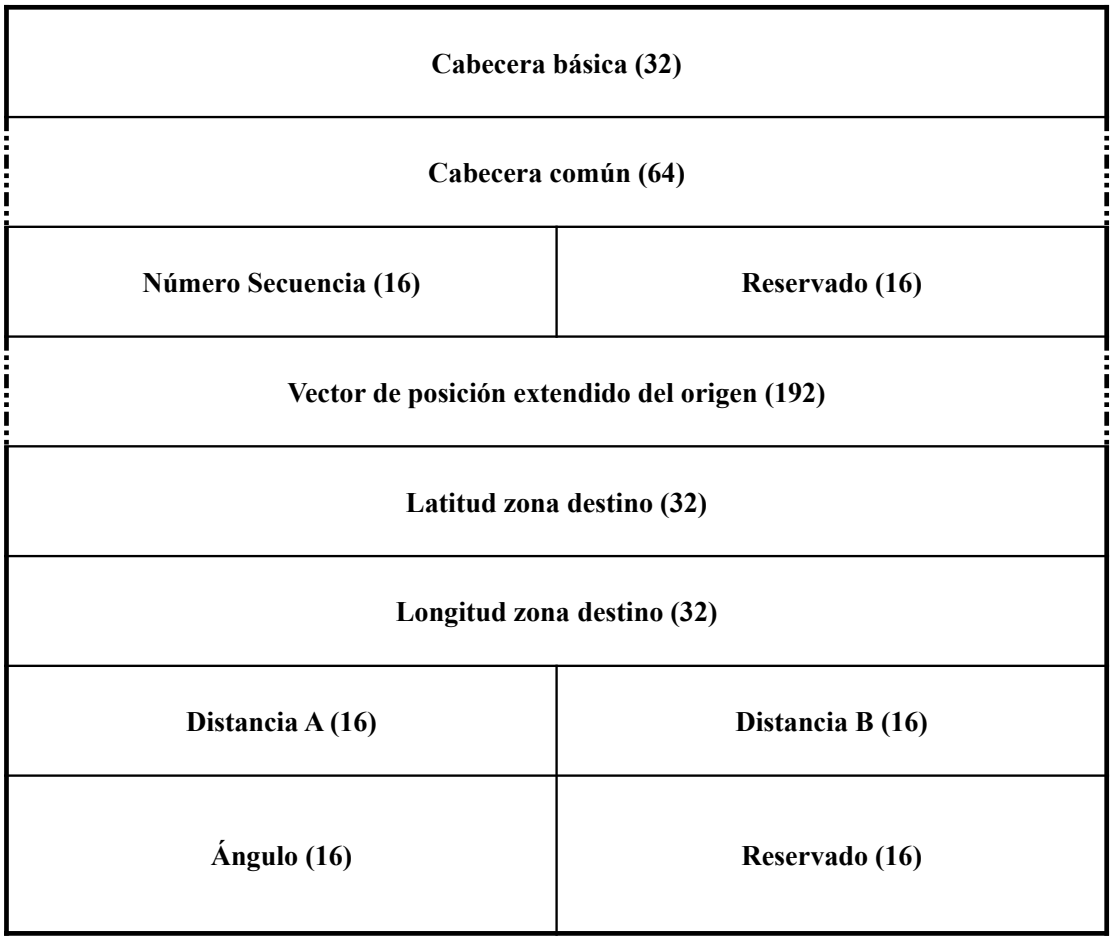


Figura A.15: Cabecera *geo-broadcast* del protocolo de GN V1.2.1

- **Vector de posición extendido del origen:** se trata del vector de posición extendido del nodo origen del mensaje. Su formato se describe en la Sección A.2.2.
- **Vector de posición reducido del destino:** es el vector de posición reducido del destino. Es utilizado por el algoritmo de encaminamiento para, en función de la posición geográfica de los vecinos, elegir el siguiente salto que se encuentra más cerca del destino. Su formato se describe en la Sección A.2.3.

A.2.7. Cabecera *geo-broadcast*

La cabecera *geo-broadcast* se utiliza cuando se desea entregar el paquete a todos los nodos que se encuentran situados dentro una determinada zona geográfica objetivo. Su formato se representa en la Figura A.15 donde los campos tienen el siguiente significado:

- **Cabecera básica:** se trata de la cabecera básica incluida en todos los paquetes del protocolo de GN. Su formato se describe en la Sección A.2.4.

- **Cabecera común:** se trata de la cabecera común incluida en todos los paquetes del protocolo de GN. Su formato se describe en la Sección A.2.5.
- **Número de secuencia:** es un número de secuencia que se incrementa cada vez que el nodo emisor envía un paquete. El objetivo es detectar bucles en el encaminamiento de los paquetes y paquetes duplicados.
- **Reservado:** campo de uso reservado.
- **Vector de posición extendido del origen:** se trata del vector de posición extendido del nodo origen del mensaje. Su formato se describe en la Sección A.2.2.
- **Latitud zona destino:** señala la latitud de la posición geográfica del centro de la zona geográfica objetivo. El algoritmo de encaminamiento la utiliza para guiar los paquetes hacia el destino.
- **Longitud zona destino:** expresa la longitud de la posición geográfica del centro de la zona geográfica objetivo. El algoritmo de encaminamiento la utiliza para guiar los paquetes hacia el destino.
- **Distancia A:** se trata de un parámetro de distancia que permite definir la zona geográfica destino.
- **Distancia B:** se trata de un parámetro de distancia que permite definir la zona geográfica destino.
- **Ángulo:** señala la orientación de la zona geográfica destino.

A.2.8. Cabecera de *beacon*

Los nodos envían periódicamente mensajes *beacon* en *broadcast* para permitir a sus vecinos conocer diversos parámetros sobre ellos. Su formato se representa en la Figura A.16 donde los campos tienen el siguiente significado:

- **Cabecera básica:** se trata de la cabecera básica incluida en todos los paquetes del protocolo de GN. Su formato se describe en la Sección A.2.4.
- **Cabecera común:** se trata de la cabecera común incluida en todos los paquetes del protocolo de GN. Su formato se describe en la Sección A.2.5.
- **Vector de posición extendido del origen:** se trata del vector de posición extendido del nodo origen del mensaje. Su formato se describe en la Sección A.2.2.

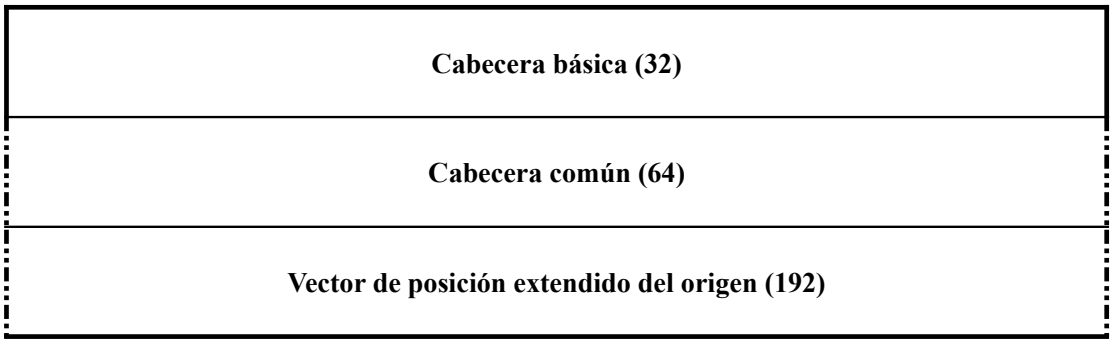


Figura A.16: Cabecera de *beacon* del protocolo de GN V1.2.1

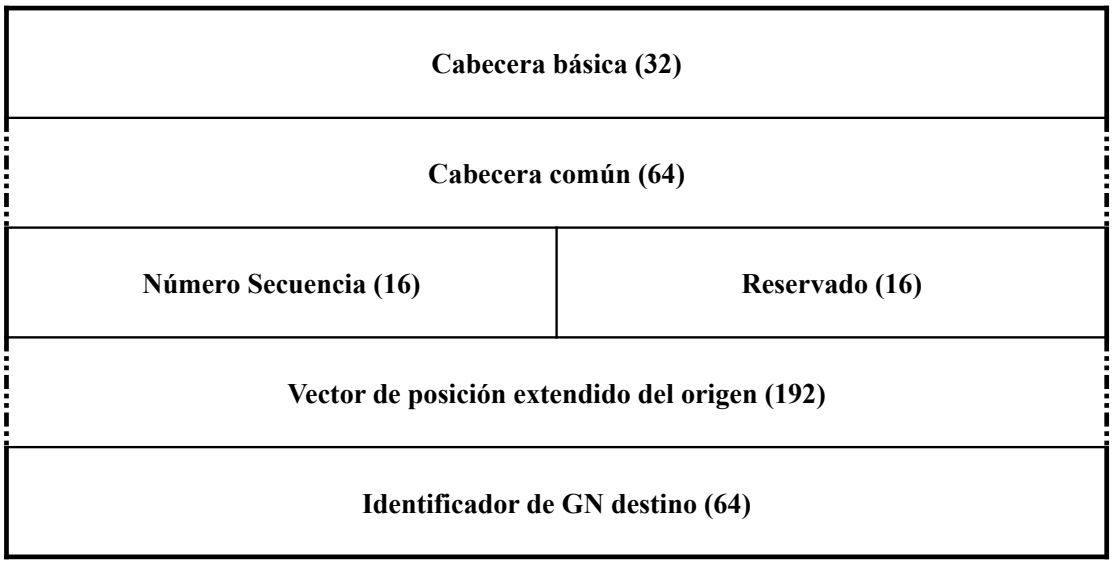


Figura A.17: Mensaje *LS Request* del protocolo de GN V1.2.1

A.2.9. Mensaje *LS Request*

El mensaje *LS Request* se utiliza en el Servicio de Localización cuando un nodo pretende obtener la posición geográfica en la que se encuentra otro nodo de la VANET. El mensaje se retransmite en *broadcast* por la red hasta que llega al nodo objetivo del que se desea obtener su posición geográfica. Su formato se representa en la Figura A.17 donde los campos tienen el siguiente significado:

- **Cabecera básica:** se trata de la cabecera básica incluida en todos los paquetes del protocolo de GN. Su formato se describe en la Sección A.2.4.
- **Cabecera común:** se trata de la cabecera común incluida en todos los paquetes del protocolo de GN. Su formato se describe en la Sección A.2.5.

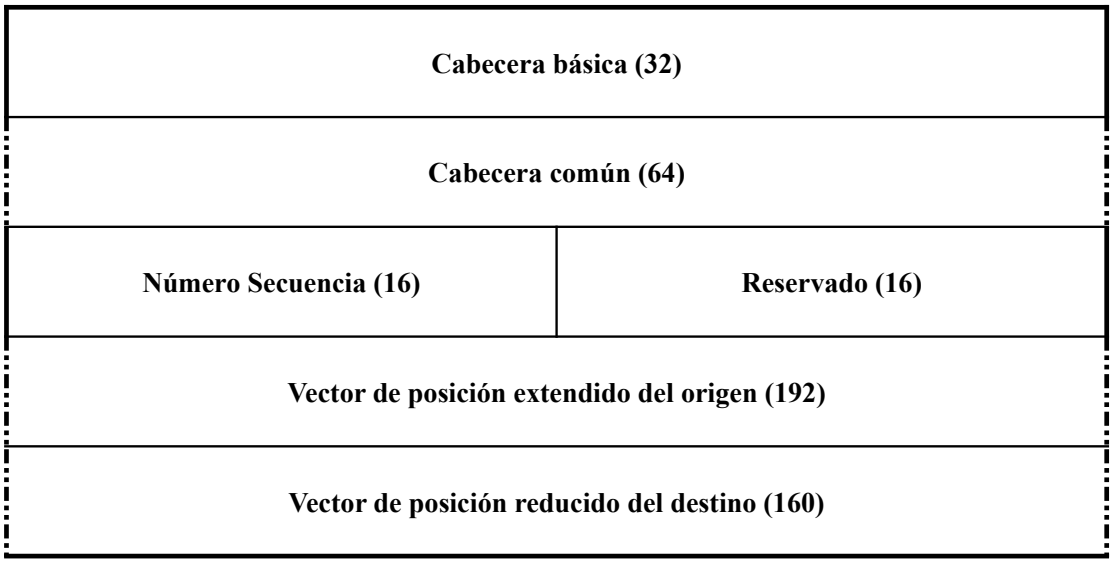


Figura A.18: Mensaje *LS Reply* del protocolo de GN V1.2.1

- **Número de secuencia:** es un número de secuencia que se incrementa cada vez que el nodo emisor envía un paquete. El objetivo es detectar bucles en el encaminamiento de los paquetes y paquetes duplicados.
- **Reservado:** campo de uso reservado.
- **Vector de posición extendido del origen:** se trata del vector de posición extendido del nodo origen del mensaje. Su formato se describe en la Sección A.2.2.
- **Identificador de GN destino:** se trata del identificador del nivel de GN utilizado por el nodo destino del que se desea obtener la posición geográfica que ocupa por medio del Servicio de Localización.

A.2.10. Mensaje *LS Reply*

El mensaje *LS Reply* se utiliza en el Servicio de Localización y se trata del mensaje que responde el nodo del que se desea la posición geográfica cuando recibe el mensaje *LS Request*. El paquete *LS Reply* se puede encaminar hasta el nodo que envió el mensaje *LS Request* tal y como si fuera un paquete *geo-unicast* gracias a que la posición geográfica del nodo origen se incluye en el mensaje *LS Request*. Su formato se representa en la Figura A.18 donde los campos tienen el siguiente significado:

- **Cabecera básica:** se trata de la cabecera básica incluida en todos los paquetes del protocolo de GN. Su formato se describe en la Sección A.2.4.

- **Cabecera común:** se trata de la cabecera común incluida en todos los paquetes del protocolo de GN. Su formato se describe en la Sección A.2.5.
- **Número de secuencia:** es un número de secuencia que se incrementa cada vez que el nodo emisor envía un paquete. El objetivo es detectar bucles en el encaminamiento de los paquetes y paquetes duplicados.
- **Reservado:** campo de uso reservado.
- **Vector de posición extendido del origen:** se trata del vector de posición extendido del nodo origen del mensaje. Su formato se describe en la Sección A.2.2.
- **Vector de posición reducido del destino:** es el vector de posición reducido del destino. Es utilizado por el algoritmo de encaminamiento para, en función de la posición geográfica de los vecinos, elegir el siguiente salto que se encuentra más cerca del destino. Su formato se describe en la Sección A.2.3.

Referencias

[1] Dirección General de Tráfico (DGT), "Las principales cifras de la Siniestralidad Vial España 2012." Disponible en: http://www.dgt.es/Galerias/seguridad-vial/estadisticas-e-indicadores/publicaciones/principales-cifras-siniestralidad/cifras_siniestralidad_2012.pdf, 2012. [Consulta junio 2014].

[2] Instituto Nacional de Estadística (INE), "Encuesta sobre Equipamiento y Uso de Tecnologías de la Información y Comunicación en los Hogares (TIC-H). Año 2013." Disponible en: http://www.ine.es/prensa/np803.pdf, octubre 2013. [Consulta junio 2014].

[3] CAR 2 CAR Communication Consortium (C2C-CC), "CAR 2 CAR Communication Consortium Manifesto. Overview of the C2C-CC System." Disponible en: http://www.car-to-car.org/index.php?eID=tx_nawsecuredl&u=0&file=fileadmin/downloads/C2C-CC_manifesto_v1.1.pdf&t=1404124442&hash=e0500662210cea662a965103c9cc472e8ce4e30c, agosto 2007. [Consulta junio 2014].

[4] 3rd Generation Partnership Project (3GPP), "IP flow mobility and seamless Wireless Local Area Network (WLAN) offload; Stage 2, TS 23.261 v11.0.0 Release 11," septiembre 2012.

[5] V. Sandonis, I. Soto, M. Calderon, and M. Urueña, "Vehicle to Internet communications using the ETSI ITS GeoNetworking protocol," *Transactions on Emerging Telecommunications Technologies*, mayo 2014. [En revisión].

[6] V. Sandonis, M. Calderon, I. Soto, and C. J. Bernardos, "Design and performance evaluation of a PMIPv6 solution for geonetworking-based VANETs," *Ad Hoc Networks. Theory, Algorithms and Applications of Wireless Networked Robotics Recent Advances in Vehicular Communications and Networking*, vol. 11, pp. 2069 – 2082, septiembre 2013.

[7] J. Barrachina, M. Fogue, P. Garrido, F. Martinez, J. Cano, C. Calafate, and P. Manzoni, "Assessing vehicular density estimation using vehicle-to-infrastructure communications,"

in *IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1–3, junio 2013.

[8] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)." Internet Engineering Task Force (IETF), RFC 3626 (Experimental), octubre 2003.

[9] C. E. Perkins and P. Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers," *SIGCOMM Comput. Commun. Rev.*, vol. 24, no. 4, pp. 234–244, 1994.

[10] R. Ogier, F. Templin, and M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)." Internet Engineering Task Force (IETF), RFC 3684 (Experimental), febrero 2004.

[11] "MANET Working Group of the Internet Engineering Task Force (IETF)." Disponible en: `http://www.ietf.org/html.charters/manet-charter.html`. [Consulta junio 2014].

[12] "OOLSR." Disponible en: `http://hipercom.inria.fr/OOLSR/`. [Consulta junio 2014].

[13] "The NRL OLSR Routing Protocol Implementation." Disponible en: `http://cs.itd.nrl.navy.mil/work/olsr/index.php`. [Consulta junio 2014].

[14] "OLSRD." Disponible en: `http://www.olsr.org/`. [Consulta junio 2014].

[15] E. Dijkstra, "A note on two problems in connexion with graphs," *Numerische Mathematik*, vol. 1, no. 1, pp. 269–271, 1959.

[16] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," in *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, MobiCom '99, pp. 151–162, ACM, 1999.

[17] E. Baccelli and J. Schiller, "Towards scalable MANETs," in *8th International Conference on ITS Telecommunications (ITST 2008)*, pp. 133 –138, 2008.

[18] L. Villasenor-Gonzalez, Y. Ge, and L. Lament, "HOLSR: a hierarchical proactive routing mechanism for mobile ad hoc networks," *IEEE Communications Magazine*, vol. 43, pp. 118 – 125, julio 2005.

[19] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing." Internet Engineering Task Force (IETF), RFC 3561 (Experimental), julio 2003.

[20] C. Perkins, S. Ratliff, and J. Dowdell, "Dynamic MANET On-demand (AODVv2) Routing." Internet Engineering Task Force (IETF) Internet-Draft, draft-ietf-manet-aodvv2-03, febrero 2014.

[21] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4." Internet Engineering Task Force (IETF), RFC 4728 (Experimental), 2007.

[22] "Kernel AODV." Disponible en: `http://w3.antd.nist.gov/wctg/aodv_kernel/`. [Consulta junio 2014].

[23] "HUT AODV for IPv6." Disponible en: `http://tcs.legacy.ics.tkk.fi/~anttit/manet/aodv/`. [Consulta junio 2014].

[24] C. Maihofer, "A survey of geocast routing protocols," *IEEE Communications Surveys Tutorials*, vol. 6, no. 2, pp. 32–42, 2004.

[25] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, MobiCom '00, pp. 243–254, ACM, 2000.

[26] S. Basagni, I. Chlamtac, V. R. Syrotiuk, and B. A. Woodward, "A distance routing effect algorithm for mobility (DREAM)," in *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*, MobiCom '98, pp. 76–84, ACM, 1998.

[27] D. Arora, E. Millman, and S. W. Neville, "Assessing the performance of AODV, DYMO, and OLSR routing protocols in the context of larger-scale denser MANETs," in *IEEE Pacific Rim Conference on Communications Computers and Signal Processing (PacRim)*, pp. 675–679, IEEE, 2011.

[28] M. Rahman, F. Anwar, J. Naeem, and M. Abedin, "A simulation based performance comparison of routing protocol on Mobile Ad-hoc Network (proactive, reactive and hybrid)," in *International Conference on Computer and Communication Engineering (ICCCE)*, pp. 1–5, mayo 2010.

[29] Y. Zhang, F. Liu, C. Liu, P. Wang, and L. Cui, "A Simulation Study of Routing Protocols for Vehicular Ad Hoc Networks Based on OPNET," in *8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)*, pp. 1–4, IEEE, 2012.

[30] S. Sagar, J. Saqib, A. Bibi, and N. Javaid, "Evaluating and comparing the performance of DYMO and OLSR in MANETs and in VANETs," in *IEEE 14th International Multitopic Conference (INMIC)*, pp. 362–366, diciembre 2011.

[31] E. Spaho, L. Barolli, G. Mino, F. Xhafa, V. Kolici, and R. Miho, "Performance Evaluation of AODV, OLSR and DYMO Protocols for Vehicular Networks Using CAVENET," in *13th International Conference on Network-Based Information Systems (NBiS)*, pp. 527–534, septiembre 2010.

[32] G. Adam, V. Kapoulas, C. Bouras, G. Kioumourtzis, A. Gkamas, and N. Tavoularis, "Performance evaluation of routing protocols for multimedia transmission over mobile ad hoc networks," in *4th Joint IFIP Wireless and Mobile Networking Conference (WMNC)*, pp. 1–6, octubre 2011.

[33] F. Maan and N. Mazhar, "MANET routing protocols vs mobility models: A performance evaluation," in *Third International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 179–184, junio 2011.

[34] A. Srivastava, D. Kumar, and S. Gupta, "Geographic and Reactive Routing Protocols for MANET," in *European Modelling Symposium (EMS)*, pp. 590–594, noviembre 2013.

[35] T. Camp, J. Boleng, B. Williams, L. Wilcox, and W. Navidi, "Performance comparison of two location based routing protocols for ad hoc networks," in *Proceedings of Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM 2002)*, vol. 3, pp. 1678–1687, 2002.

[36] European Telecommunications Standards Institute (ETSI), "ETSI TS 102 636-4-1 v1.1.1; Intelligent Transport Systems (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality," junio 2011.

[37] P. Belanovic, D. Valerio, A. Paier, T. Zemen, F. Ricciato, and C. Mecklenbrauker, "On Wireless Links for Vehicle-to-Infrastructure Communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 1, pp. 269–282, 2010.

[38] Institute of Electrical and Electronics Engineers (IEEE), "IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-1997*, pp. i–445, 1997.

[39] Institute of Electrical and Electronics Engineers (IEEE), "IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments," *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009)*, pp. 1–51, 2010.

[40] J. Santa, A. F. Gómez-Skarmeta, and M. Sánchez-Artigas, "Architecture and evaluation of a unified V2V and V2I communication system based on cellular networks," *Computer Communications*, vol. 31, no. 12, pp. 2850–2861, 2008.

[41] P. C. Ng and S.-C. Liew, "Throughput Analysis of IEEE802.11 Multi-Hop Ad Hoc Networks," *IEEE/ACM Transactions on Networking*, vol. 15, pp. 309–322, abril 2007.

[42] Z. Fu, P. Zerfos, H. Luo, S. Lu, L. Zhang, and M. Gerla, "The impact of multihop wireless channel on TCP throughput and loss," in *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM 2003)*, vol. 3, pp. 1744–1753, 2003.

[43] A. Mishra, M. Shin, and W. Arbaugh, "An empirical analysis of the IEEE 802.11 MAC layer handoff process," *SIGCOMM Comput. Commun. Rev.*, vol. 33, no. 2, pp. 93–102, 2003.

[44] D. Le, X. Fu, and D. Hogrefe, "A review of mobility support paradigms for the internet," *IEEE Communications Surveys Tutorials*, vol. 8, no. 1, pp. 38–51, 2006.

[45] D. Funato, K. Yasuda, and H. Tokuda, "TCP-R: TCP mobility support for continuous operation," in *Proceedings of the 1997 International Conference on Network Protocols (ICNP '97)*, ICNP '97, IEEE Computer Society, 1997.

[46] M. Riegel and M. Tuexen, "Mobile SCTP." Internet Engineering Task Force (IETF) Internet-Draft, draft-riegel-tuexen-mobile-sctp-09, 2007.

[47] D. Maltz and P. Bhagwat, "MSOCKS: an architecture for transport layer mobility," in *Proceedings of Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM '98)*, vol. 3, pp. 1037–1045, 1998.

[48] H. Schulzrinne and E. Wedlund, "Application-layer mobility using SIP," in *IEEE Service Portability and Virtual Customer Environments*, pp. 29–36, 2000.

[49] V. Sandonis, I. Soto, M. Calderon, I. Fernandez, and I. Vidal, "CATMISS: Context-Aware Transparent Mobility for IMS Services," *Multimedia Tools and Applications*, pp. 1–28, enero 2014.

[50] I. Vidal, I. Soto, M. Calderon, J. Garcia-Reinoso, and V. Sandonis, "Transparent network-assisted flow mobility for multimedia applications in IMS environments," *IEEE Communications Magazine*, vol. 51, pp. 97–105, julio 2013.

[51] V. Sandonis, I. Fernandez, and I. Soto, "SIP-Based Context-Aware Mobility for IPTV IMS Services," *EuroITV2012*, julio 2012.

[52] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "Host Identity Protocol." Internet Engineering Task Force (IETF), RFC 5201 (Experimental), 2008.

[53] D. Cocker, "Multiple address service for transport (MAST)," in *Proceedings of International Symposium on Applications and the Internet*, 2004.

[54] C. Perkins, "IP Mobility Support for IPv4, Revised." Internet Engineering Task Force (IETF), RFC 5944 (Proposed Standard), 2010.

[55] C. Perkins, D. Johnson, and J. Arkko, "Mobility Support in IPv6." Internet Engineering Task Force (IETF), RFC 6275 (Proposed Standard), 2011.

[56] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)." Internet Engineering Task Force (IETF), RFC 4861 (Draft Standard), 2007.

[57] S. Thomson, T. Narten, and T. Jinmei, "IPv6 Stateless Address Autoconfiguration." Internet Engineering Task Force (IETF), RFC 4862 (Draft Standard), 2007.

[58] European Telecommunications Standards Institute (ETSI), "ETSI EN 302 636-6-1 v1.2.1; Intelligent Transport Systems (ITS), Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols," mayo 2014.

[59] R. Koodli, "Mobile IPv6 Fast Handovers." Internet Engineering Task Force (IETF), RFC 5568 (Proposed Standard), 2009.

[60] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management." Internet Engineering Task Force (IETF), RFC 5380 (Proposed Standard), 2008.

[61] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6." Internet Engineering Task Force (IETF), RFC 5213 (Proposed Standard), 2008.

[62] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, "Fast Handovers for Proxy Mobile IPv6." Internet Engineering Task Force (IETF), RFC 5949 (Proposed Standard), 2010.

[63] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol." Internet Engineering Task Force (IETF), RFC 3963 (Proposed Standard), 2005.

[64] C. Ng, F. Zhao, M. Watari, and P. Thubert, "Network Mobility Route Optimization Solution Space Analysis." Internet Engineering Task Force (IETF), RFC 4889 (Informational), 2007.

[65] F. Abduljalil and S. Bodhe, "A survey of integrating IP mobility protocols and mobile ad hoc networks," *IEEE Communications Surveys Tutorials*, vol. 9, no. 1, 2007.

[66] A. Benslimane, S. Barghi, and C. Assi, "An efficient routing protocol for connecting vehicular networks to the Internet," *Pervasive and Mobile Computing*, vol. 7, no. 1, pp. 98 – 113, 2011.

[67] A. Hamidian, U. Körner, and A. Nilsson, "Performance of internet access solutions in mobile ad hoc networks," in *Wireless systems and mobility in next generation internet*, pp. 189–201, Springer, 2005.

[68] V. Bychkovsky, B. Hull, A. K. Miu, H. Balakrishnan, and S. Madden, "A Measurement Study of Vehicular Internet Access Using In Situ Wi-Fi Networks," in *12th ACM MOBICOM Conf.*, septiembre 2006.

[69] J. Ott and D. Kutscher, "The drive-thru architecture: WLAN-based Internet access on the road," in *IEEE 59th Vehicular Technology Conference (VTC 2004-Spring)*, vol. 5, pp. 2615 – 2622 Vol.5, mayo 2004.

[70] S. Annese, C. Casetti, C.-F. Chiasserini, N. Di Maio, A. Ghittino, and M. Reineri, "Seamless Connectivity and Routing in Vehicular Networks with Infrastructure," *IEEE Journal on Selected Areas in Communications*, vol. 29, marzo 2011.

[71] A. Neumann, C. Aichele, M. Lindner, and S. Wunderlich, "Better Approach To Mobile Ad-hoc Networking (B.A.T.M.A.N.)." Internet Engineering Task Force (IETF) Internet-Draft, draft-openmesh-b-a-t-m-a-n-00, abril 2008.

[72] E. Baccelli, T. Clausen, and R. Wakikawa, "IPv6 operation for WAVE - Wireless Access in Vehicular Environments," in *IEEE Vehicular Networking Conference (VNC)*, pp. 160–165, diciembre 2010.

[73] Institute of Electrical and Electronics Engineers (IEEE), "IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture," *IEEE Std 1609.0-2013*, pp. 1–78, marzo 2014.

[74] J. Choi, Y. Khaled, M. Tsukada, and T. Ernst, "IPv6 support for VANET with geographical routing," in *8th International Conference on ITS Telecommunications (ITST 2008)*, pp. 222 –227, octubre 2008.

[75] "CAR 2 CAR Communication Consortium (C2C-CC)." Disponible en: `http://www.car-to-car.org/`. [Consulta junio 2014].

[76] M. Tsukada, I. B. Jemaa, H. Menouar, W. Zhang, M. Goleva, and T. Ernst, "Experimental Evaluation for IPv6 over VANET Geographic Routing," in *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference*, IWCMC '10, pp. 736–741, ACM, 2010.

[77] "GeoNet project." Disponible en: `http://www.geonet-project.eu/`. [Consulta junio 2014].

[78] V. Sandonis, M. Calderon, and C. J. Bernardos, "Integración de IP en redes vehiculares," in *X Congreso español sobre sistemas inteligentes de transporte*, mayo 2010.

[79] S. Cespedes, X. Shen, and C. Lazo, "IP mobility management for vehicular communication networks: challenges and solutions," *IEEE Communications Magazine*, vol. 49, pp. 187 – 194, mayo 2011.

[80] R. Baldessari, A. Festag, and J. Abeille, "NEMO meets VANET: A Deployability Analysis of Network Mobility in Vehicular Communication," in *7th International Conference on ITS Telecommunications (ITST 2007)*, pp. 1–6, 2007.

[81] B. McCarthy, C. Edwards, and M. Dunmore, "The integration of ad-hoc (MANET) and mobile networking (NEMO): principles to support rescue team communication," in *Third International Conference on Mobile Computing and Ubiquitous Networking (ICMU 2006)*, 2006.

[82] R. Baldessari, W. Zhang, A. Festag, and L. Le, "A MANET-centric solution for the application of NEMO in VANET using geographic routing," in *Proceedings of the 4th International Conference on Testbeds and research infrastructures for the development of networks & communities*, TridentCom '08, ICST, 2008.

[83] I. Soto, C. J. Bernardos, M. Calderon, A. Banchs, and A. Azcorra, "NEMO-enabled localized mobility support for internet access in automotive scenarios," *IEEE Communications Magazine*, vol. 47, pp. 152–159, mayo 2009.

[84] J.-H. Lee and T. Ernst, "Lightweight NEtwork MObility Within PMIPv6 for Transportation Systems," *IEEE Systems Journal*, vol. 5, pp. 352–361, septiembre 2011.

[85] J.-H. Lee, T. Ernst, and N. Chilamkurti, "Performance Analysis of PMIPv6-Based NEtwork MObility for Intelligent Transportation Systems," *IEEE Transactions on Vehicular Technology*, vol. 61, pp. 74–85, enero 2012.

[86] International Organization for Standardization (ISO), "ISO 21217:2014 Intelligent transport systems – Communications Access for Land Mobiles (CALM) – Architecture, ISO Standard TC204 WG16," marzo 2014.

[87] European Telecommunications Standards Institute (ETSI), "ETSI EN 302 636-3 v1.1.2; Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network architecture," marzo 2014.

[88] J. Santa, F. Pereniguez-Garcia, F. Bernal, P. Fernandez, R. Marin-Lopez, and A. Skarmeta, "A Framework for Supporting Network Continuity in Vehicular IPv6 Communications," *IEEE Intelligent Transportation Systems Magazine*, vol. 6, no. 1, pp. 17–34, 2014.

[89] R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernst, and K. Nagami, "Multiple Care-of Addresses Registration." Internet Engineering Task Force (IETF), RFC 5648 (Proposed Standard), 2009.

[90] Institute of Electrical and Electronics Engineers (IEEE), "IEEE Standard for Local and metropolitan area networks - Media Independent Handover Services," *IEEE Std 802.21-2008*, enero 2009.

[91] J. Santa, F. Pereniguez-Garcia, J. Cano, A. Skarmeta, C. Calafate, and P. Manzoni, "Comprehensive Vehicular Networking Platform for V2I and V2V Communications within the Walkie-Talkie Project," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[92] "Walkie-Talkie." Disponible en: `http://www.grc.upv.es/walkietalkie/`. [Consulta junio 2014].

[93] Cespedes, S., *IP mobility support in multi-hop vehicular communications networks*. PhD thesis, University of Waterloo, 2012.

[94] S. Cespedes U. and X. Shen, "An Efficient Hybrid HIP-PMIPv6 Scheme for Seamless Internet Access in Urban Vehicular Scenarios," in *IEEE Global Telecommunications Conference (GLOBECOM 2010)*, pp. 1 –5, diciembre 2010.

[95] M. Asefi, S. Cespedes, X. Shen, and J. Mark, "A Seamless Quality-Driven Multi-Hop Data Delivery Scheme for Video Streaming in Urban VANET Scenarios," in *IEEE International Conference on Communications (ICC)*, junio 2011.

[96] S. Cespedes, S. Taha, and X. Shen, "A Multihop-Authenticated Proxy Mobile IP Scheme for Asymmetric VANETs," *IEEE Transactions on Vehicular Technology*, vol. 62, pp. 3271–3286, septiembre 2013.

[97] S. Cespedes, N. Lu, and X. Shen, "VIP-WAVE: On the Feasibility of IP Communications in 802.11p Vehicular Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, pp. 82–97, marzo 2013.

[98] "Institute of Electrical and Electronics Engineers (IEEE) 1609 WG - Dedicated Short Range Communication Working Group." `http://standards.ieee.org/develop/wg/1609_WG.html` (Abril 2014). [Consulta junio 2014].

[99] Institute of Electrical and Electronics Engineers (IEEE), "IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Multi-channel Operation," *IEEE Std 1609.4-2010 (Revision of IEEE Std 1609.4-2006)*, pp. 1–89, febrero 2011.

[100] Institute of Electrical and Electronics Engineers (IEEE), "IEEE Standard for Information technology–Local and metropolitan area networks–Specific requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements," *IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003)*, pp. 1–212, noviembre 2005.

[101] Institute of Electrical and Electronics Engineers (IEEE), "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services - Redline," *IEEE Std 1609.3-2010 (Revision of IEEE Std 1609.3-2007) - Redline*, pp. 1–212, diciembre 2010.

[102] Institute of Electrical and Electronics Engineers (IEEE), "IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages," *IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006)*, pp. 1–289, abril 2013.

[103] European Telecommunications Standards Institute (ETSI), "ETSI EN 302 663 v1.2.1; Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band," julio 2013.

[104] "ISO - International Organization for Standardization." Disponible en: `http://www.iso.org/iso/home.html`. [Consulta junio 2014].

[105] "ISO/TC 204 Intelligent transport systems." Disponible en: `http://www.iso.org/iso/iso_technical_committee?commid=54706`. [Consulta junio 2014].

[106] S. A. Mohammad, A. Rasheed, and A. Qayyum, "VANET architectures and protocol stacks: a survey," in *Communication technologies for vehicles*, pp. 95–105, Springer, 2011.

[107] "European Telecommunications Standards Institute Intelligent Transport System." Disponible en: `http://www.etsi.org/website/Technologies/IntelligentTransportSystems.aspx`. [Consulta junio 2014].

[108] R. Baldessari, C. Bernardos, and M. Calderon, "GeoSAC - Scalable address autoconfiguration for VANET using geographic networking concepts," in *IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2008)*, pp. 1 –7, septiembre 2008.

[109] M. Gramaglia, I. Soto, C. Bernardos, and M. Calderon, "Overhearing-Assisted Optimization of Address Autoconfiguration in Position-Aware VANETs," *IEEE Transactions on Vehicular Technology,*, vol. 60, pp. 3332 –3349, septiembre 2011.

[110] European Telecommunications Standards Institute (ETSI), "Draft ETSI EN 302 636-4-1 v1.2.1; Intelligent Transport Systems (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality," mayo 2014.

[111] H. Reijmers and R. Prasad, "The influence of vehicle distribution models on packet success probability on a three lane motorway," in *48th IEEE Vehicular Technology Conference (VTC 1998)*, vol. 3, pp. 1785–1789, mayo 1998.

[112] N. Wisitpongphan, F. Bai, P. Mudalige, V. Sadekar, and O. Tonguz, "Routing in sparse vehicular ad hoc wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, pp. 1538–1556, octubre 2007.

[113] Skycomp, Inc., "Major Highway Performance Ratings and bottleneck Inventory - State of Maryland - Spring 2008." Disponible en: `http://www.skycomp.com/MDSHA/resources/Spring_2008.pdf`, noviembre 2009. [Consulta junio 2014].

[114] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of SUMO - Simulation of Urban MObility," *International Journal On Advances in Systems and Measurements*, vol. 5, pp. 128–138, diciembre 2012.

[115] W. Vandenberghe, I. Moerman, and P. Demeester, "On the feasibility of utilizing smartphones for vehicular ad hoc networking," in *11th International Conference on ITS Telecommunications (ITST)*, pp. 246–251, agosto 2011.

[116] F. Martelli, M. Elena Renda, G. Resta, and P. Santi, "A measurement-based study of beaconing performance in IEEE 802.11p vehicular networks," in *Proceedings of Thirty-First Annual IEEE International Conference on Computer Communications (IEEE INFOCOM 2012)*, pp. 1503–1511, marzo 2012.

[117] F. Bai, D. D. Stancil, and H. Krishnan, "Toward Understanding Characteristics of Dedicated Short Range Communications (DSRC) from a Perspective of Vehicular Network Engineers," in *Proceedings of the Sixteenth Annual International Conference on Mobile Computing and Networking*, MobiCom '10, pp. 329–340, ACM, 2010.

[118] D. Son, A. Helmy, and B. Krishnamachari, "The effect of mobility-induced location errors on geographic routing in mobile ad hoc sensor networks: analysis and improvement using mobility prediction," *IEEE Transactions on Mobile Computing*, vol. 3, pp. 233–245, julio 2004.

[119] W. Su, S.-J. Lee, and M. Gerla, "Mobility prediction and routing in ad hoc wireless networks," *International Journal of Network Management*, vol. 11, no. 1, pp. 3–30, 2001.

[120] P. Lai, X. Wang, N. Lu, and F. Liu, "A reliable broadcast routing scheme based on mobility prediction for VANET," in *IEEE Intelligent Vehicles Symposium*, pp. 1083–1087, junio 2009.

[121] S. Shah and K. Nahrstedt, "Predictive location-based QoS routing in mobile ad hoc networks," in *IEEE International Conference on Communications (ICC 2002)*, vol. 2, pp. 1022–1027, 2002.

[122] H. Füßler, M. Torrent-moreno, M. Transier, A. Festag, and H. Hartenstein, "Thoughts on a Protocol Architecture for Vehicular Ad-hoc Networks," in *2nd Int. Workshop on Intelligent Transportation (WIT)*, 2005.

[123] European Telecommunications Standards Institute (ETSI), "ETSI TS 102 687 v1.1.1; Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part," julio 2011.

[124] R. K. Schmidt, A. Brakemeier, T. Leinmüller, B. Böddeker, and G. Schäfer, "Architecture for Decentralized Mitigation of Local Congestion in VANETs," in *10th International Conference on ITS Telecommunications (ITST)*, 2010.

[125] S. Nischal and V. Sharma, "A Joint Uplink/Downlink Opportunistic Scheduling Scheme for Infrastructure WLANs," *Computing Research Repository*, vol. abs/1310.5125, 2013.

[126] S. W. Kim, B.-S. Kim, and Y. Fang, "Downlink and uplink resource allocation in IEEE 802.11 wireless LANs," *IEEE Transactions on Vehicular Technology*, vol. 54, pp. 320–327, enero 2005.

[127] X. Zhou, J. Korhonen, C. Williams, S. Gundavelli, and C. Bernardos, "Prefix Delegation Support for Proxy Mobile IPv6." Internet Engineering Task Force (IETF), RFC 7148 (Proposed Standard), 2014.

[128] "Dirección General de Tráfico." Disponible en: `http://www.dgt.es/es/`. [Consulta junio 2014].

[129] L. Buttyán and J.-P. Hubaux, "Stimulating Cooperation in Self-organizing Mobile Ad Hoc Networks," *Mobile Networks and Applications*, vol. 8, no. 5, pp. 579–592, 2003.

[130] E. Hernández-Orallo, M. Olmos, J. Cano, C. Calafate, and P. Manzoni, "A Fast Model for Evaluating the Detection of Selfish Nodes Using a Collaborative Approach in MANETs," *Wireless Personal Communications*, vol. 74, no. 3, pp. 1099–1116, 2014.

Acrónimos

ACK *ACKnowledgment*

AODV *Ad hoc On-demand Distance Vector routing protocol*

AU *Application Unit*

BA *Binding Acknowledgment*

BU *Binding Update*

C2C-CC *Car 2 Car Communication Consortium*

CALM *Communications Access for Land Mobiles*

CBF *Contention-Based Forwarding*

CBR *Constant Bit Rate*

CCH *Control CHannel*

CCU *Communication & Control Unit*

CIA *Cluster ID Announcement*

CN *Correspondent Node*

CoA *Care of Address*

CT Clase de Tráfico

DAD *Duplicate Address Detection*

DGT Dirección General de Tráfico

DHCPv6 *Dynamic Host Configuration Protocol*

DPV Detección de Pérdida de Vecino

DREAM *Distance Routing Effect Algorithm for Mobility*

DSDV *Destination-Sequenced Distance Vector routing protocol*

DSR *Dynamic Source Routing protocol*

DSRC *Dedicated Short-Range Communications*

DYMO *DYnamic MANET On-demand routing protocol*

EDCA *Enhanced Distributed Channel Access*

EGN *Enhanced GN*

EPS *Evolved Packet System*

ETSI *European Telecommunications Standards Institute*

FMIPv6 *Fast Hand-overs for Mobile IPv6*

FPMIPv6 *Fast Proxy Mobile IPv6*

FP-NEMO *Fast P-NEMO*

GeoSAC *Geographically Scoped stateless Address Configuration*

GN *GeoNetworking*

GN6ASL *GeoNetworking to IPv6 Adaptation Sub-Layer*

GPRS *General Packet Radio Service*

GPS *Global Positioning System*

GPSR *Greedy Perimeter Stateless Routing*

HA *Home Agent*

HIP *Host Identity Protocol*

HMIPv6 *Hierarchical Mobile IPv6*

HNA *Host and Network Association*

HNP *Home Network Prefix*

HoA *Home Address*

HOLSR *Hierarchical Optimized Link State Routing protocol*

HTC *Hierarchical Topology Control*

HTTP *HyperText Transfer Protocol*

I2I *Infrastructure 2 Infrastructure*

ID *IDentifier*

IEEE *Institute of Electrical and Electronics Engineers*

IETF *Internet Engineering Task Force*

IMS *IP Multimedia Subsystem*

INE Instituto Nacional de Estadística

IP *Internet Protocol*

ISO *International Organization for Standardization*

ITS *Intelligent Transport System*

LFN *Local Fixed Node*

LMA *Local Mobility Anchor*

LMD *Localized Mobility Domain*

LMN *Local Mobile Node*

LS Límite de Saltos

LS *Location Service*

LSM Límite de Saltos Máximo

LTE *Long Term Evolution*

MAC *Media Access Control*

MAG *Mobile Access Gateway*

MANET *Mobile Ad hoc NETwork*

MA-PMIP *Multi-hop Authenticated Proxy Mobile IP*

MAST *Multiple Address Service for Transport*

MCoA *Multiple Care of Addresses Registration*

MIP *Mobile IP*

MN *Mobile Node*

MNN *Mobile Network Node*

MNP *Mobile Network Prefix*

MPR *MultiPoint Relay*

MR *Mobile Router*

ND *Neighbor Discovery*

NEMO BS *Network Mobility Basic Support*

NetLMM *Network-based Localized Mobility Management*

N-PMIPv6 *NEMO-enabled PMIPv6*

NUD *Neighbor Unreachability Detection*

OLSR *Optimized Link State Routing protocol*

OMNET *Objective Modular Network Testbed*

PA Precisión de la Altitud

PBA *Proxy Binding Acknowledgment*

PBU *Proxy Binding Update*

Pdir Precisión de la dirección

PMIP *Proxy Mobile IP*

PMIPv6 *Proxy Mobile IPv6*

PMT Precisión de la Marca de Tiempo

P-NEMO *PMIPv6-based NEMO*

PPos Precisión de la Posición

Pvel Precisión de la velocidad

RA *Router Advertisement*

RA *Router* de Acceso

RERR *Route RERRor*

RREP *Route REPly*

RREQ *Route REQuest*

RS *Router Solicitation*

RSU *Road Site Unit*

SC Siguiente Cabecera

SCH *Service Channel*

SIP *Session Initiation Protocol*

SL Servicio de Localización

SLAAC *StateLess Address Auto-configuration*

STC SubTipo de Cabecera

SUMO *Simulation of Urban MObility*

TBRPF *Topology Broadcast Based on Reverse-Path Forwarding routing protocol*

TC *Technical Committee*

TC Tipo de Cabecera

TC *Topology Control*

TCP *Transmission Control Protocol*

TL Tabla de Localización

UDP *User Datagram Protocol*

UMTS *Universal Mobile Telecommunications System*

UWB *Ultra-Wide-Band*

V2I *Vehicle 2 Infrastructure*

V2V *Vehicle 2 Vehicle*

VANET *Vehicular Ad hoc NETwork*

VIP-WAVE *Vehicular IP in WAVE*

VMN *Visiting Mobile Node*

VoIP *Voice over IP*

WAVE *Wireless Access in Vehicular Environments*

WG *Working Group*

WiMaX *Worldwide Interoperability for Microwave Access*

WLAN *Wireless Local Area Network*

WSMP *WAVE Short Message Protocol*

WUSB *Wireless Universal Serial Bus*

xMIPv6 *eXtensible Mobile IPv6*