MÁSTER EN
INVESTIGACIÓN EN
INFORMÁTICA

CURSO 2007-08

CONFIGURACIÓN DHCP EN REDES MANET SUBORDINADAS

José Ignacio Ruiz Núñez

Dirigido por:

Alicia Triviño Cabrera

Departamento de Lenguajes y Ciencias de la Computación

Universidad de Málaga

Luis Javier García Villalba

Departamento de Ingeniería del Software e Inteligencia Artificial

Universidad Complutense de Madrid

DEPARTAMENTO DE INGENIERÍA DEL SOFTWARE E INTELIGENCIA ARTIFICIAL

FACULTAD DE INFORMÁTICA

UNIVERSIDAD COMPLUTENSE DE MADRID

Resumen

Las redes móviles ad hoc (MANET) permiten a diferentes dispositivos móviles comunicarse entre ellos a través de enlaces inalámbricos. Un problema a resolver es la conexión de una MANET a otras redes incluyendo Internet. Con este propósito, los dispositivos móviles deberían obtener una dirección IP topológicamente correcta. El protocolo DHCP (*Dynamic Host Configuration Protocol*) para IPv6, conocido como DHCPv6, es un mecanismo estándar para la configuración de estado completo de direcciones IPv6 que trabaja con mensajes *link-local*. Dada la naturaleza multisalto propia de las redes MANET, el protocolo no puede ser aplicado directamente en estas redes. Este trabajo propone una solución para implementar DHCPv6 en una red móvil ad hoc. Además, se incluyen varias optimizaciones para aumentar el rendimiento de la red.

Abstract

Mobile Ad-hoc NETworks (MANET) allow different mobile devices to communicate with each other through multiple wireless links. One problem to solve is the connection of MANET to other networks including the Internet. With this purpose, the mobile devices should be provided of topologically correct IP addresses. The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is a defined standard mechanism for the configuration of IPv6 addresses in a stateful manner which works with link-local messages. Due to their multihop nature, this protocol cannot be directly applicable in MANETs. This work proposes a solution to implement DHCPv6 on an ad-hoc network. Additionally, it includes several optimizations to improve the network performance.

Agradecimientos

Quiero hacer presente mi agradecimiento a la profesora Alicia Triviño Cabrera por toda la ayuda material y moral recibida. Este esfuerzo de investigación no hubiera sido posible sin su voluntad y compromiso.

Igualmente, quiero agradecer al profesor Luis Javier García Villalba por todos los consejos recibidos durante el estudio.

Lista de acrónimos

AREQ	Address REQuest
AODV	Ad hoc On-demand Distance Vector
BA	Binding Acknowledgement
BootP	Protocolo Bootstrap
BU	Binding Update
CoS	Clase de Servicio
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSDV	Destination-Sequenced Distance-Vector
DSR	Dynamic Source Routing
DSSS	Direct Sequence Spread Spectrum
DYMO	DYnamic Manet On-demand
GloMo	Global Mobile Information Systems
GSR	Global State Routing
GWADV	GateWay ADVertisement

IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGWADV	Internet Gateway Advertisement
IGWSOL	Internet Gateway Solicitation
IP	Internet Protocol
IPng	IP de nueva generación
IPsec	Internet Protocol Security
IRT	Initial Retransmission Time
LAR	Location Arded Routing
LPR	Low-cost Packet Radio
LMR	Lightweight Mobile Routing
MAC	Medium Access Control Address
MANET	Mobile Ad hoc NETwork
MRA	Modified Router Advertisements
MRC	Maximum Retransmission Count
MRD	Maximum Retransmission Duration
MRT	Maximum Retransmission Time

MTU	Maximun Transfer Unit
NIC	Número de Intentos de Configuración
NIS	Network Information Service
NDP	Neighbor Discovery Protocol
NS	Network Simulator
NTDR	Near-term Digital Radio
OFDM	Orthogonal Frecuency-Division Multiplexing
OLSR	Optimizad Link State Routing
OPNET	Optimized Network Engineering Tools
PA	Prefix Advertisement
PADD	Primary ADDress
PDA	Personal Digital Assistant
QoS	Quality of Service
RA	Router Advertisement
RFC	Request For Comments
ROAM	Routing On-demand Acyclic Multi-path
RREP	Route REPly

RREQ	Route REQuest
RERR	Route ERRor
RT	Retransmission Timeout
SURAN	Survivable Radio Networks
TBRPF	Topology Broadcast Reverse Path Forwarding
TTL	Time To Live
UDP	User Datagram Protocol
VoIP	Voz sobre IP
WG	Work Group
WRP	Wireless Routing Protocol
ZRP	Zone Routing Protocol

ÍNDICE

1. INTRODUCCIÓN

Internet se ha convertido en unos de los medios de difusión de información más importantes del mundo y las personas lo utilizan, en su vida rutinaria y profesional, como canal de comunicación, como sistema de colaboración masiva o simplemente como distracción. En los últimos años, la proliferación de dispositivos móviles cada vez más potentes (ordenadores portátiles, PDAs, móviles de última generación, etc) posibilita la integración de éstos con Internet. Sin embargo, la característica de movilidad que acompaña a este tipo de dispositivos provoca el nacimiento de nuevos retos tecnológicos.

Una red móvil ad hoc o MANET (*Mobile Ad hoc NETwork*) es un conjunto de nodos móviles que se comunican entre sí a través de enlaces inalámbricos (*wireless*). Al contrario de las redes convencionales, una red MANET no necesita la existencia de una infraestructura previa ya que cada nodo se apoya en los demás para conseguir comunicarse con otro creando la llamada comunicación multisalto.

Este tipo de redes tiene varios inconvenientes que una red convencional no presenta. La topología de este tipo de redes puede cambiar rápidamente y de una forma impredecible. Además, pueden surgir variaciones en las capacidades de los nodos y enlaces, errores frecuentes en la transmisión y falta de seguridad. Por último, se debe tener en cuenta los recursos limitados de los nodos ya que normalmente una red ad hoc estará formada por dispositivos alimentados por una batería.

El resto de este capítulo está organizado como sigue. El apartado 1.1 presenta el objeto de investigación de este trabajo. En el apartado 1.2 se analizan algunos trabajos relacionados. En último lugar, el capítulo 1.3 resume la estructura del resto del trabajo.

1.1 Objeto de la investigación

Las MANET pueden ser clasificadas en MANET subordinadas o MANET autónomas en función de si están conectadas o no a una red externa. En una MANET autónoma los nodos pueden identificarse unívocamente a través de una dirección IP con la única premisa de que esta dirección sea distinta a la de cualquier otro nodo de la red. Sin embargo, en una MANET subordinada se obliga a usar un direccionamiento IP topológico correcto y enrutable globalmente. Un ejemplo típico de MANET subordinada es una MANET que es parte de Internet (Figura 1.1).

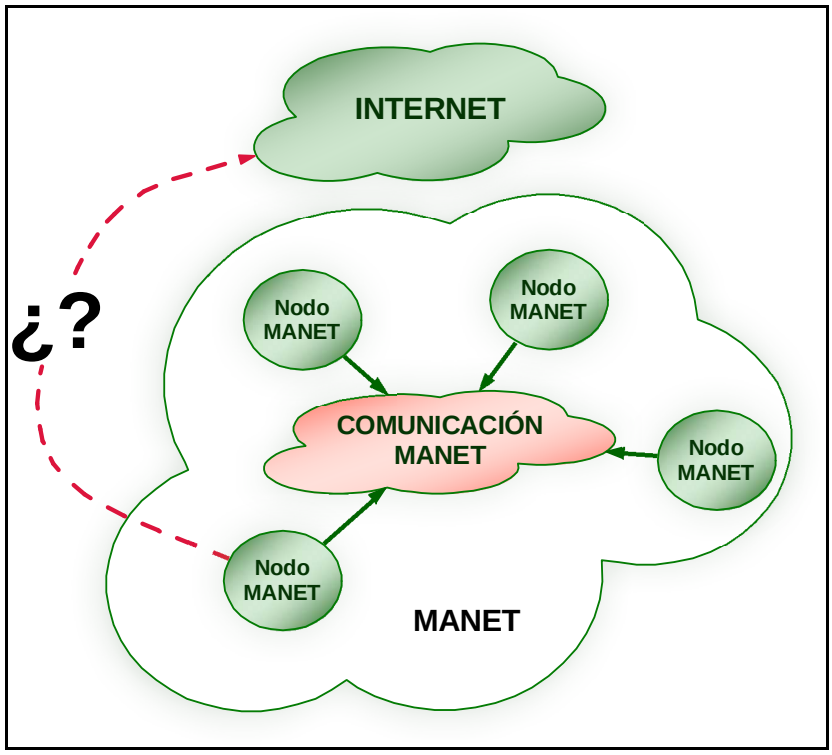

Fig. 1.1. MANET subordinada

El proceso de configuración es el conjunto de pasos a través de los cuales un nodo consigue obtener su dirección IP dentro de la red (dirección global para Internet). Existen dos mecanismos de configuración de direcciones: sin estado (*stateless*) y de estado completo (*stateful*). La configuración de direcciones sin estado propone que sea el propio nodo el encargado de generar su dirección IP. La dirección se obtiene de la concatenación de un prefijo de red conocido y un

número teóricamente único dentro de la red generado por el nodo. Este mecanismo puede exigir la inclusión de un módulo encargado de comprobar la unicidad de la dirección generada llamado Detección de Direcciones Duplicadas o DAD (*Duplicate Address Detection*).

Por otro lado, la configuración de direcciones de estado completo se basa en la utilización de servidores que controlan y asignan las direcciones a todos los nodos de la red. *Dynamic Host Configuration Protocol* (DHCP) [Droms, 2003] es un ejemplo de configuración de estado completo. Sin embargo, dada la naturaleza multisalto de las redes MANET, este protocolo no puede ser aplicado directamente.

Este trabajo propone una solución para implementar DHCP versión 6 (DHCPv6), a emplear junto con IPv6, en una MANET para que sus nodos sean capaces de obtener una dirección IP global y, por tanto, dispongan de comunicación con Internet. Además, se analizan varias optimizaciones para mejorar el rendimiento de la red.

1.2 Trabajos relacionados

Las MANET presentan características especiales que deben tenerse en cuenta a la hora de implementar un protocolo de configuración de direcciones. Existen muchas soluciones para redes convencionales (por ejemplo, RFCs 4861, 4862, 3315, etc) pero en su diseño no se tuvieron en cuenta las redes móviles ad hoc. Es necesario, pues, dar soporte multisalto, soporte a topologías dinámicas y soporte a la unión (*merging*) y partición (*partitioning*) de redes, eventos que son típicos en las redes MANET.

Hay numerosos trabajos [Bernardos, 2005] que realizan propuestas para la configuración de direcciones en una MANET utilizando tanto el mecanismo sin estado como el de estado completo. Quizás la Internet Engineering Task Force (IETF) [IETF, 2008] tenga el grupo de trabajo más conocido llamado *Dynamic*

Host Configuration Work Group (DHC WG) [DHC WG, 2008] que desarrolló DHCP para automatizar, localizar, configurar y manejar direcciones IP y otros parámetros de configuración. Actualmente este grupo trabaja con el protocolo DHCPv6 y ha elaborado diversas propuestas (*Internet Drafts*) para la aplicación de DHCP sobre MANETs.

Muchas de las propuestas que se comentan a continuación hacen uso de los siguientes términos:

- *Pasarela de Internet (gateway)*. Es el dispositivo que hace de puente entre dos redes, en nuestro caso, entre la MANET e Internet. Entiende los protocolos de ambas redes y por tanto toda comunicación entre un nodo móvil e Internet debe pasar a través de él. Entre otras funcionalidades, el *gateway* de Internet es el responsable de propagar los parámetros necesarios para la configuración de direcciones IP dentro de la MANET. Además, proporciona las funcionalidades de encaminamiento ad hoc que no se encuentran implementadas en el *Router de Acceso* común.

- *Dirección local*. Es la dirección que un nodo tiene asignada dentro de la MANET. Se trata de un identificador único pero que solamente puede ser utilizada para comunicación con otros nodos dentro de la propia MANET, no siendo válida para otros nodos de otras redes como Internet

- *Dirección global*. Es la dirección que un nodo tiene asignada para comunicarse con otros nodos que están en el exterior, como en Internet.

En la propuesta [Rufino, 2006] se supone la existencia de un *gateway* y que cada nodo cuenta con una dirección local única, llamada PADD (*Primary ADDress*). El *gateway* manda periódicamente mensajes PA (*Prefix Advertisement*)

a todos los nodos anunciándoles un prefijo global IPv6. Cuando los nodos reciben el mensaje, construyen una dirección IPv6 global que les permite acceder a Internet. Uno de los inconvenientes de este protocolo, además de la sobrecarga producida por los mensajes PA, es que no se da soporte al *merging*.

[Clausen, 2005] propone que solamente los nodos configurados participen en las labores de configuración enviando mensajes ADDR_BEACON a todos sus vecinos. Cuando un nodo desea obtener una dirección global, al recibir un mensaje ADDR_BEACON de un nodo configurado, contesta a éste último con un mensaje AREQ (*Address REQuest*). El nodo configurado responde con un mensaje Addr-Config en el que asigna una dirección local al nuevo nodo. Con esta dirección se puede establecer un intercambio de mensajes entre ambos nodos para obtener una dirección global. La forma de asignar la dirección global puede hacerse de diversas formas, por ejemplo, configurando los nodos para que actúen como *proxy* y transmita las peticiones a un servidor DHCP. Uno de los inconvenientes de este método es que al menos un nodo de la red debe ser configurado manualmente con una dirección global.

[Wakikawa, 2006] también utiliza uno o varios *gateways*. Supone la existencia de una dirección local para cada nodo antes de comenzar su ejecución. Esta dirección la obtendrán los nodos al iniciarse o al unirse a la red. Propone varios mecanismos para que los nodos descubran la presencia de los *gateways* y, con su ayuda, obtener la dirección global. Pueden ser los *gateways* los que periódicamente envíen mensajes a todos los nodos o bien que sean los propios nodos los que manden mensajes de solicitud de una dirección.

En [Cha, 2003] se propone un nuevo mecanismo para la configuración de direcciones IP globales para MANETs. Se trata de un mecanismo de configuración de estado completo basado en el intercambio de mensajes de control extendidos de los protocolos de encaminamiento utilizados en las redes ad hoc. En lugar de utilizar DHCP plantea que sea el *gateway* el que se encargue de proveer conectividad global a los nodos. El *gateway* conoce el prefijo de red y

es capaz de generar direcciones globales. Mantiene un listado de las direcciones asignadas a cada nodo y cuando le llega una nueva petición asigna una dirección que no está asignada a ningún otro nodo de la red. Este mecanismo podría presentar problemas cuando se desee descentralizar la asignación de direcciones.

[Templin, 2008], actualmente en revisión, conecta los nodos de la MANET con las llamadas *virtual ethernets*, que son enlaces compartidos imaginarios. Los nodos acceden a estos enlaces a través de una interfaz que se configura sobre las interfaces de la MANET, pudiendo así comunicarse y obtener una dirección IPv6 global usando por ejemplo DHCPv6. Realmente se trata de un mecanismo que usa IP sobre IP lo que puede presentar problemas de encapsulación de mensajes.

Por último, [Singh, 2008] realiza una implementación de DHCPv6 sobre MANET intentando minimizar la sobrecarga de mensajes de control.

1.3 Estructura del trabajo

El resto del trabajo está organizado en siete capítulos con la estructura que se comenta a continuación.

El Capítulo 2 realiza un estado del arte de las redes ad hoc incluyendo varias clasificaciones y prestando especial interés a los protocolos de encaminamiento utilizados para este tipo de redes.

El Capítulo 3 presenta la nueva tecnología de Internet, IPv6. Se enumeran las nuevas características que incorpora y algunas de las mejoras para dar soporte a las redes móviles ad hoc, como son la autoconfiguración de direcciones y la movilidad.

El Capítulo 4 repasa los aspectos fundamentales que son necesarios para la

integración a Internet de una MANET. Se mostrarán varias propuestas prestando especial atención en la utilizada durante este trabajo.

El Capítulo 5 se centra en el protocolo DHCP. Se analizaran las causas que hacen que no se pueda aplicar directamente sobre una MANET.

El Capítulo 6 presenta las propuestas para la adaptación del protocolo DHCP en redes móviles ad hoc, consiguiendo que los nodos de estas redes obtengan una dirección IP global para el acceso a Internet. Así mismo, describe la propuesta de este trabajo para la utilización de DHCPv6 sobre redes MANET subordinadas incluyendo alguna mejora al protocolo convencional.

El Capítulo 7 incluye los resultados obtenidos de las simulaciones realizadas y comparativas con otros métodos.

Por último, el Capítulo 8 muestra las principales conclusiones extraídas de este trabajo así como algunas líneas futuras de trabajo.

2. REDES MÓVILES AD HOC

Una red móvil ad hoc o MANET (*Mobile Ad hoc NETwork*) es un conjunto de nodos móviles que se comunican entre sí a través de enlaces inalámbricos (*wireless*). Al contrario de las redes convencionales, una red MANET no necesita la existencia de una infraestructura previa ya que cada nodo se apoya en los demás para conseguir comunicarse con otro creando la llamada comunicación multisalto.

El capítulo se estructura de la siguiente forma. En el apartado 2.1 se hace un repaso cronológico de la evolución de las redes ad hoc. En el apartado 2.2 se analizan las características básicas de este tipo de redes. En el apartado 2.3 se presta atención al protocolo de comunicación que actualmente se utiliza en MANET, el IEEE 802.11. El apartado 2.4 realiza una clasificación de las redes ad hoc. El apartado 2.5 repasa los protocolos de encaminamiento que se emplean en MANET. Por último, el apartado 2.6 profundiza en el protocolo de encaminamiento AODV utilizado en este trabajo.

2.1 Historia

En muy pocos años, el campo de las redes ad hoc ha tenido una rápida expansión visible en la proliferación de dispositivos inalámbricos de bajo coste como ordenadores portátiles, asistentes personales digitales, (PDAs), teléfonos móviles, etc.

A comienzos de los años 70 un trabajo pionero en radio de la Universidad de Hawai introduce el primer sistema que usa el medio de la radio para la transmisión de información. Conocido ampliamente como ALOHA [Abramson, 1970], fue desarrollado por Abramson y Kuo.

El trabajo realizado en Hawai llevó al desarrollo de una arquitectura

distribuida consistente en una red de difusión de radio con mínimo control central llamada PARNET bajo el sponsor de DARPA en 1972 [Feeney, 2001]. El proyecto ayudó a establecer el concepto de redes móviles ad hoc. PARNET permitía la comunicación directa entre usuarios móviles sobre grandes áreas geográficas, ancho de banda compartido y protección contra los efectos de múltiples caminos.

Los rápidos avances de la tecnología de la radio en los años 70 provocó la aparición de múltiples sistemas de comunicación móvil como teléfonos celulares e inalámbricos, sistemas de radio búsqueda, satélites móviles, etc.

Posteriormente DARPA desarrolló el proyecto SURAN (*Survivable Radio Networks*) en 1983 que trata las tareas de escalabilidad de la red, la seguridad, la capacidad de proceso y gestión de energía. Se dedicaron esfuerzos para desarrollar dispositivos de bajo coste y con poco gasto de energía que pudieran soportar los avanzados protocolos de encaminamiento, escalar a miles de nodos las redes y dar soporte para ataques a la seguridad. El resultado fue la aparición de la tecnología conocida como LPR (*Low-cost Packet Radio*) en 1987.

A mitad de los 90 se produce un nuevo avance con la llegada de tarjetas de radio 802.11 para ordenadores personales y portátiles. En dos artículos [Freebersyser, 2001][Jain, 2003] se propone por primera vez la idea de una colección de *hosts* móviles con una infraestructura mínima, y la IEEE (*Institute of Electrical and Electronic Engineers*) acuña el término de "redes ad hoc".

Durante el mismo tiempo, el Departamento de Defensa de Estados Unidos continuaba trabajando con proyectos como el GloMo (*Global Mobile Information Systems*) o el NTDR (*Near-term Digital Radio*). El objetivo del GloMo era permitir la conectividad multimedia de tipo *Ehernet*, en cualquier momento y en cualquier lugar, entre los dispositivos inalámbricos. NTDR son protocolos que se basan en dos componentes: agrupamiento y encaminamiento. Los algoritmos de agrupamiento organizan dinámicamente una red en líderes de grupo y

miembros de grupo. Los líderes forman la columna vertebral de la red y los miembros se comunican entre sí a través de dicha columna. NTDR inicialmente fue un prototipo para la Armada de los Estados Unidos y en la actualidad algunos países lo utilizan como base para otros protocolos.

La definición de estándares como IEEE 802.11 [IEEE, 2003] provocó el rápido crecimiento de las redes móviles en campos no sólo militares, sino también en el mundo comercial.

2.2 Características básicas

Como su propio nombre indica la característica principal de una MANET es la movilidad de los nodos, que pueden cambiar de posición rápidamente. La necesidad de crear redes de forma rápida en lugares sin infraestructura suele implicar que los nodos exploren el área y, en algunos casos, se deban unir para conseguir un objetivo. El tipo de movilidad que desarrollen los nodos puede tener una influencia a la hora de escoger el protocolo de encaminamiento que aumente el rendimiento de la red.

Otro de los aspectos importantes en la redes ad hoc es la llamada auto-organización que se estudia en profundidad en [Dressler, 2006]. La idea principal se basa en la coordinación y colaboración de todos los nodos de la red para conseguir un mismo objetivo. Se han propuesto varios métodos de auto-organización para redes en general y para redes ad hoc en particular. La auto-configuración puede desglosarse en las siguientes capacidades:

- Auto-reparación: mecanismos que permitan detectar, localizar y reparar automáticamente los fallos siendo capaces de distinguir la causa del error. Por ejemplo, sobrecarga o mal funcionamiento.

- Auto-configuración: métodos de generación de configuraciones adecuadas en función de la situación actual dependiendo de las

circunstancias ambientales. Por ejemplo, conectividad o parámetros de calidad de servicio.

- Auto-gestión: capacidad de mantener dispositivos o redes dependiendo de los parámetros actuales del sistema.

- Adaptación: adecuación a los cambios de las condiciones ambientales. Por ejemplo, cambio en el número de nodos vecinos.

A continuación se presentan el resto de características de las redes móviles ad hoc.

- *Ausencia de infraestructura*. Al contrario que las redes convencionales que cuentan con la existencia de elementos físicos, las redes móviles se forman autónomamente.

- *Topología dinámica*. Los nodos se pueden mover arbitrariamente haciendo que algunos enlaces se destruyan y otros se creen cuando un nodo se acerque a otros que antes tenía fuera de su alcance.

- *Ancho de banda limitado*. En la mayoría de las ocasiones será menor que el de una conexión cableada, afectado además por las interferencias de las señales electromagnéticas.

- *Variación en la capacidad de los enlaces y los nodos*. Los nodos pueden disponer de varias interfaces de radio que difieren entre sí en capacidad de transmisión/recepción y en la banda de frecuencia en la que trabajan. Esta característica complica el desarrollo de los protocolos de encaminamiento en gran medida.

- *Conservación de energía*. Algunos o todos los nodos de una MANET son alimentados por una batería y no tienen posibilidad de recargarla. Para

estos nodos, el criterio más importante a la hora de diseñar sistemas y protocolos será la optimización de la conservación de energía.

- *Escalabilidad*. En muchas aplicaciones las redes ad hoc pueden llegar a tener miles de nodos lo que conlleva dificultad en tareas como direccionamiento, encaminamiento, gestión de localización, gestión de configuración, interoperabilidad, seguridad, etc.

- *Falta de seguridad*. La seguridad juega un papel importante en las redes ad hoc dado el carácter vulnerable de los enlaces inalámbricos que se forman. Los protocolos de encaminamiento deben proporcionar una comunicación segura. Existen áreas de investigación en este sentido que sugieren incluir datos de sensores externos e información geográfica y topográfica en el propio algoritmo de encaminamiento.

- *Encaminamiento multisalto*. Los nodos actúan como *routers* para retransmitir los paquetes que se intercambian nodos cuyo alcance no permite una comunicación directa.

- *Entorno imprevisible*. Las redes ad hoc pueden darse en terrenos en los que las situaciones no son las más óptimas debido a condiciones peligrosas o desconocidas. Pueden darse casos donde los nodos se destruyan, se estropeen o comiencen a producir fallos.

- *Comportamiento de los terminales*. Uno de las principales claves para que una MANET tenga un funcionamiento adecuado es la confianza que cada nodo tiene que tener sobre los demás. Sin esta confianza sería imposible crear un protocolo de encaminamiento ya que la información debe transmitirse por varios nodos intermedios. Normalmente, los protocolos de encaminamiento que descubren los terminales intermedios se basan en las respuestas que dan los nodos sobre el coste de la comunicación. Existen nodos maliciosos que podrían intencionadamente

informar de forma incorrecta sobre los costes con la finalidad de recibir todos los paquetes, poder manipularlos, alterarlos o incluso eliminarlos. Algunas soluciones al respecto se encuentran en [García, 2006].

2.3 IEEE 802.11

El IEEE describe las normas a seguir por cualquier fabricante de dispositivos inalámbricos para que puedan ser compatibles entre sí. La primera propuesta de este estándar mantenía tasas de transmisión de 1 y 2 Mbps en la banda de frecuencias ISM (*Industrial Scientific and Medical*), situada en 2.4 GHz. Además, se especificaban como tecnologías en la capa física los infrarrojos y el canal radio. Con los años, se ha llegado a distintas versiones del estándar. Se citan los más importantes a continuación:

- IEEE 802.11a: hasta 54 Mbps a 5 GHz. Utiliza en la capa física la tecnología OFDM (*Orthogonal Frecuency-Division Multiplexing*).

- IEEE 802.11b: hasta 11 Mbps a 2.4 GHz. Actualmente es el más utilizado. Utiliza la tecnología DSSS (*Direct Sequence Spread Spectrum*) en la capa física.

- IEEE 802.11e: pretende proporcionar calidad de servicio QoS (*Quality of Service*) para su uso en servicios como VoIP (Voz sobre IP) y *Streaming*. Una aproximación para otorgar calidad de servicio es la de diferenciar los paquetes clasificándolos en un número pequeño de tipos de servicios y utilizar mecanismos de prioridad para proporcionar una calidad de servicio adecuada a cada tráfico.

- IEEE 802.11f: desarrolla especificaciones para la implementación de puntos de acceso y sistemas de distribución para evitar problemas de interoperabilidad entre distintos fabricantes y distribuidores de equipos.

- IEEE 802.11g: hasta 54 Mbps a 2.4 GHz. Soporta tanto OFDM como DSSS en la capa física

2.4 Clasificación

La terminología de redes ad hoc aún no está muy asentada y no existe una clasificación clara. A continuación se exponen varias clasificaciones situando el lugar en el que se encuentran las redes MANET.

Existen redes ad hoc con infraestructura donde los nodos se mueven mientras se comunican con una estación base fija. Cuando un nodo se mueve fuera del rango de una estación fija entra en el alcance de otra estación. Por otro lado se encuentran las redes ad hoc sin infraestructura donde no existen estaciones base fijas y todos los nodos de la red necesitan actuar como *routers*. Las redes MANET son redes ad hoc sin infraestructura.

Otra clasificación de las redes ad hoc incluye las redes de un solo salto y las redes multisalto. Los nodos de las redes de un solo salto se comunican únicamente con los nodos que tiene a su alcance. En las redes ad hoc multisalto, los nodos que no pueden comunicarse directamente utilizan nodos intermedios para retransmitir la información. Las redes MANET son redes ad hoc multisalto.

Por último hay una clasificación que incluye las redes MANET como un tipo independiente. Se incluyen tres tipos de redes ad hoc:

- Redes MANET.

- Redes de sensores. Formadas de dispositivos sensoriales, generalmente compuestos por un sensor tradicional y un conversor analógico-digital. La unidad de proceso está compuesta de un microprocesador y una pequeña memoria. Pueden incluir sistemas de localización y sistemas de

movilidad. En estas redes el número de nodos suele ser mucho mayor que en una MANET pero la movilidad se considera escasa o nula (solamente cambia la topología con la pérdida o desconexión de nodos). Es habitual el flujo de información desde muchos orígenes hasta un nodo llamado sumidero (*sink*) que se encarga de procesar la información y enviársela al destino. Por lo tanto, es un tipo opuesto al modelo de Internet donde las conexiones son extremo a extremo y con inteligencia en los extremos.

- Redes híbridas. También denominadas mixtas, son redes ad hoc que usan infraestructuras IP si están disponibles.

A su vez las redes MANET se pueden dividir en dos tipos en función de si están conectadas o no a otras redes:

- Redes MANET autónomas. Son redes que no están conectadas a ninguna otra red. Los nodos de la red se pueden identificar unívocamente a través de una dirección IP con la única premisa de que sea distinta a la de cualquier otro nodo de la red.

- Redes MANET subordinadas. Son redes conectadas a una o más redes externas. Se obliga a usar un direccionamiento IP topológico correcto y enrutable globalmente. Un ejemplo típico de MANET subordinada es una MANET que es parte de Internet.

2.5 Protocolos de encaminamiento

El concepto de encaminamiento básicamente comprende dos actividades. En primer lugar, determinar los caminos óptimos y, en segundo lugar, transferir los grupos de paquetes de información a través de la red. Los algoritmos utilizan varias métricas para calcular el mejor camino para que los paquetes lleguen a su destino. Estas métricas son medidas estándar como podría ser el

número de saltos que son usados por el algoritmo para determinar el camino óptimo. El proceso para determinar el camino inicializa y mantiene tablas de encaminamiento que contienen la información total de cada ruta. La información que se almacena para cada ruta varía de un algoritmo a otro.

Las redes MANET se construyen de forma dinámica cuando un conjunto de nodos crean rutas entre sí para conseguir la conectividad entre ellos. Los nodos de la MANET pueden actuar como origen o destino de una comunicación, pero también como *rourters* cuando una relación entre nodos no se puede realizar directamente por motivos de alcance. De esta forma se crean comunicaciones multisalto. Un protocolo de encaminamiento de una red móvil ad hoc necesita proveer un mecanismo que mantenga las rutas hacia los destinos frente al movimiento de los nodos que puede provocar que las rutas se destruyan, y sea necesario encontrar una ruta alternativa para mantener la comunicación entre los nodos.

El objetivo de un protocolo de encaminamiento para redes móviles es conseguir el envío de un mensaje de un nodo a otro sin existir un enlace directo. La mayoría de protocolos de encaminamiento para redes MANET provienen de adaptaciones realizadas sobre protocolos de redes fijas, siendo su principal problema la cantidad de fallos que se producen en la comunicación debido a la movilidad de los nodos.

2.5.1 Clasificación

Desde que se empezaron a estudiar las redes ad hoc se han propuesto diversas clasificaciones de los protocolos de encaminamiento que se resumen en [Jayakumar, 2007].

En función de la estructura los protocolos pueden ser clasificados en protocolos uniformes o no uniformes. En los protocolos uniformes ningún nodo de la red realiza un papel distinto al de los demás, todos ellos envían y

responden a los mensajes de control del mismo modo. Sin embargo, en los protocolos no uniformes se reduce el número de nodos que participan en las tareas de encaminamiento.

Otra clasificación propone dividir los protocolos en función de la información de estado que almacenan los nodos de la red. De esta forma existen protocolos basados en la topología y protocolos basados en el destino. En los primeros, cada nodo toma decisiones basándose en una completa información de la topología de la red. Los segundos, son protocolos que manejan vectores de distancias, en los que cada nodo intercambia con sus vecinos las distancias que conoce a otros nodos.

La clasificación más difundida propone dividir los protocolos de encaminamiento dependiendo de cómo se detectan y mantienen las rutas a los destinos, surgiendo los siguientes tipos de protocolos:

- *Protocolos proactivos*. En este tipo de encaminamiento cada nodo mantiene información de cómo llegar a cualquier otro nodo de la red e intercambia esta información con todos sus vecinos. La información de encaminamiento es normalmente almacenada en un número diferente de tablas. Periódicamente se actualizan las tablas si la topología de red cambia. La diferencia entre los protocolos de este tipo se encuentra en la forma de actualizar y detectar la información de encaminamiento y el tipo de información que se guarda en cada tabla. La ventaja que aportan estos protocolos es la baja latencia ya que las rutas están siempre disponibles. Sin embargo, esto conlleva un consumo de energía muy alto en los nodos y se puede producir una sobrecarga de mensajes en la red debido a la inundación periódica de mensajes. DSDV (*Destination-Sequenced Distance-Vector*) [Perkins, 1994], WRP (*Wireless Routing Protocol*) [Murthy, 1995], GSR (*Global State Routing*) [Chen, 1998], OLSR (*Optimizad Link State Routing*) [Clausen, 2003] o

TBRPF (*Topology Broadcast Reverse Path Forwarding*) [Bellur, 2003] son ejemplos de protocolos de encaminamiento proactivos. En general, estos protocolos tratan de evitar bucles en las rutas, consumo excesivo de memoria y reducción del tamaño de los paquetes que contienen la información de las tablas de encaminamiento

- *Protocolos reactivos*. Estos protocolos tratan de reducir la sobrecarga que producen los protocolos proactivos. Para ello proponen que los nodos de la MANET, cuando no tienen una ruta a un destino, la calculen sólo cuando es necesaria, es decir, cuando el nodo tenga que comenzar un intercambio de paquetes con el destino. El descubrimiento de una ruta normalmente se realiza por inundación de mensajes de solicitud por toda la red. Estos protocolos conllevan una latencia alta, provocada por el descubrimiento de rutas, sin embargo, la sobrecarga de mensajes por la red se reduce. AODV (*Ad hoc On-demand Distance Vector*) [Perkins, 2003], DYMO (*DYnamic Manet On-demand*) [Chakeres, 2005], DSR (*Dynamic Source Routing*) [Johnson, 2007], ROAM (*Routing On-demand Acyclic Multi-path*) [Raju, 1999], LMR (*Lightweight Mobile Routing*) [Corson, 1995] o LAR (*Location Arded Routing*) [Ko, 1998] son algunos de los protocolos de encaminamiento reactivos. La mayoría de ellos tienen el mismo coste de encaminamiento en el peor escenario posible ya que casi todos siguen la misma filosofía para el descubrimiento de rutas. El protocolo AODV ha sido el utilizado para este trabajo y será analizado en detalle en el siguiente apartado.

- *Protocolos híbridos*. Combinando los protocolos proactivos y reactivos nacen los protocolos híbridos que pretenden minimizar los inconvenientes de ambos. La idea de estos protocolos es que los nodos de la red trabajen de forma proactiva con los nodos más cercanos y de forma reactiva con el resto de nodos. La parte reactiva controla la

sobrecarga y el consumo de memoria al calcular las rutas sólo cuando son necesarias. En contraste, la parte proactiva necesita actualizar periódicamente la información almacenada y mantiene rutas que quizás nunca serán utilizadas, añadiendo una innecesaria sobrecarga. El caso más conocido de protocolo híbrido es ZRP (*Zone Routing Protocol*) [Haas, 1997].

2.6 Protocolo AODV

El protocolo de encaminamiento AODV (*Ad hoc On-demand Distance Vector*) [Perkins, 2003] es un protocolo bajo demanda basado en encaminamiento por vector distancia. De esta forma, los nodos que no tengan ninguna ruta activa tampoco guardarán información de encaminamiento ni participarán en el intercambio de tablas de encaminamiento. Por tanto, un nodo no tendrá que descubrir ni guardar información de una ruta hacia otro nodo hasta que no se comunique con él, a no ser que sea nodo intermedio de dos nodos que tengan establecida una comunicación. Cada nodo mantendrá una tabla de encaminamiento con la información que posea de las rutas y, así, no será necesario que los paquetes lleven información de la ruta a seguir, con el consecuente ahorro en ancho de banda.

La tabla de encaminamiento guarda un tiempo de vida para cada entrada, de forma que si este tiempo expira reiniciará la búsqueda de una ruta para el destino que tuviera asociado. De igual manera, las entradas de la tabla llevan asociadas un número de secuencia que sirve para evitar bucles en las rutas, además de ayudar a distinguir información antigua de información actualizada posteriormente. El correcto funcionamiento de AODV dependerá principalmente de que cada nodo mantenga actualizado su propio número de secuencia.

2.6.1 Mensajes de control

Los mensajes de control definidos en la especificación de AODV, conocidos como mensajes genéricos de AODV, se describen a continuación.

2.6.1.1 Mensajes RREQ

Los mensajes de petición de ruta o RREQ (*Route REQuest*) son utilizados por los nodos para comenzar el proceso de descubrimiento de ruta cuando desean comunicarse con otro nodo. Para ello, primero aumentan su propio número de secuencia y a continuación inundan la red con un mensaje RREQ con el formato indicado en la Figura 2.1. Durante un tiempo, el nodo guardará el identificador del mensaje y la dirección origen del mismo para evitar procesarlo si le llega de vuelta (ver Figura 2.2).

Tipo	J	R	G	D	U	Reservado	Nº de saltos
RREQ ID							
Dirección IP del destino							
Número de secuencia del destino							
Dirección IP del origen							
Número de secuencia del origen							

Fig. 2.1. Formato del mensaje RREQ de AODV

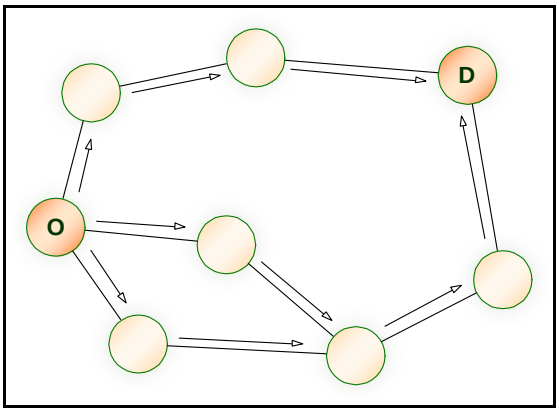

Fig. 2.2. Propagación del un mensaje RREQ en AODV

Para intentar ahorrar ancho de banda se puede usar la técnica del *expanding ring search* (aumentar anillo de búsqueda) que consiste en que el RREQ enviado tendrá un tiempo de vida o TTL (*Time To Live*) mínimo. De esta manera, sólo los

dispositivos cercanos al nodo origen reciben el RREQ. Si no se obtiene respuesta se irá aumentando el área donde se reciben los mensajes RREQ mediante el incremento del TTL, incrementando hasta llegar a un límite de TTL. Esta técnica limita la propagación de los mensajes de RREQ y, en el caso de no obtener respuesta, va aumentando el alcance de los mensajes.

Un nodo que recibe un RREQ debe crear o actualizar una ruta hacia el nodo vecino que se lo ha transmitido. Después comprueba si es un mensaje duplicado y si es así no realiza ningún proceso más. Si no es duplicado el nodo crea o actualiza una ruta inversa hacia el origen del mensaje RREQ. Si ya existía dicha ruta se tiene que actualizar su número de secuencia con el del mensaje RREQ si éste último es mayor. El "siguiente salto" (*next hop*) será el vecino del que se ha recibido el mensaje. Por esta ruta se podrá retransmitir el RREP si viene de vuelta.

Si el nodo que recibe el RREQ no está en condiciones de generar un RREP deberá retransmitir el RREQ, actualizando antes el número de secuencia para el destino del mensaje con el suyo propio si es mayor que el que lleva el mensaje.

2.6.1.2 Mensajes RREP

Los mensajes de respuesta de ruta o RREP (*Route REPly*) se envían como respuesta a la llegada de un RREQ, si el nodo es el destino o si tiene información actualizada para llegar a él. Si la información está actualizada se detectará gracias a los números de secuencia. El formato de los mensajes RREP puede verse en la Figura 2.3. Los mensajes RREP no se inundan en la red sino que se envían en unicast hacia el nodo que originó el proceso de descubrimiento de ruta por el camino inverso creado con la inundación del RREQ (Figura 2.4).

Si el nodo que genera el RREP es el destino, justo antes de enviarlo, deberá incrementar en una unidad su número de secuencia si ese fuera el valor anunciado por el RREQ. Si es un nodo intermedio el que lanza el RREP pondrá

en el mensaje el número de secuencia que posee para el destino.

Tipo	R	A	Reservado	Prefijo Sz	Nº de saltos
Dirección IP del destino					
Número de secuencia del destino					
Dirección IP del origen					
Tiempo de vida					

Fig. 2.3. Formato del mensaje RREP de AODV.

Los nodos que procesan un RREP crean o actualizan la ruta hacia el vecino que se lo ha enviado. Además, crean o actualizan la ruta directa hacia el destino (el emisor del RREP) para poder encaminar los paquetes que vaya destinados a ese nodo.

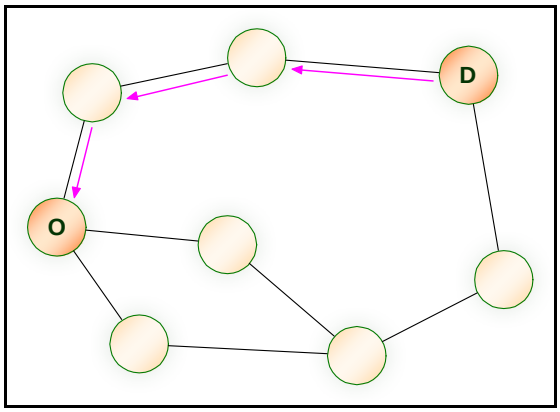

Fig. 2.4. Camino del mensaje de vuelta RREP al origen

2.6.1.3 Mensajes RERR

Los mensajes RERR (*Route ERRor*) se utilizan para notificar que no se puede alcanzar un destino determinado. El formato de un mensaje RERR puede observarse en la Figura 2.5.

Tipo	N	Reservado	Cuenta destino
Inalcanzable dirección IP del destino			
Inalcanzable número de secuencia del destino			
Inalcanzable dirección IP del destino adicional			
Inalcanzable número de secuencia del destino adicional			

Fig. 2.5. Formato del mensaje RERR de AODV.

El que un nodo no sea capaz de alcanzar un determinado destino puede

deberse a tres situaciones distintas:

- Cuando un nodo detecta la pérdida de conectividad con un vecino que es el "siguiente salto" de una ruta activa.

- Cuando un nodo tiene que enviar un paquete dirigido a un destino del que no se conoce ninguna ruta activa.

- Cuando un nodo recibe un RERR de un vecino anunciando la pérdida de conectividad con vecinos que utilizaba con "siguiente salto" en rutas activas.

2.6.1.4 Mensajes HELLO

Los nodos que forman parte de rutas activas pueden enviar información de conectividad a sus vecinos mediante mensajes HELLO. Los nodos los generarán cuando en un determinado período de tiempo no hayan transmitido ningún mensaje *broadcast*.

Los mensajes HELLO son realmente RREP con un TTL o tiempo de vida de un salto para que sólo sean recibidos por los vecinos del nodo que los envía. Su formato puede observarse en la Figura 2.3. Cuando un vecino procesa un mensaje HELLO debe crear o actualizar la entrada de la tabla de encaminamiento cuyo destino es el origen del mensaje. Si algún vecino recibe un mensaje HELLO de un nodo, y tras un período de tiempo de espera no recibe ningún otro mensaje de él, dará el enlace por perdido.

2.6.2 Descubrimiento de rutas

El descubrimiento de rutas se hace inundando la red con mensajes RREQ. Cuando un nodo recibe un RREQ crea o actualiza una entrada en su tabla de encaminamiento hacia el origen de la petición, estableciendo de esta forma un camino inverso hacia el nodo origen al presuponer que los enlaces son

simétricos. Cuando la petición llega al nodo destino genera un mensaje de respuesta RREP que transmite al nodo origen por el camino inverso establecido.

Un nodo intermedio también puede enviar un RREP si conoce un camino más reciente. Para ello, se usan números de secuencia de destino. A cada nuevo RREQ desde la fuente hacia un destino se le asigna un número mayor. De esta forma, si un nodo intermedio conoce una ruta pero tiene un número menor, no enviará el RREP. Además de para evitar utilizar rutas antiguas o rotas, los números de secuencia sirven para prevenir la formación de bucles que degraden la eficiencia de la red.

Mediante el RREP de vuelta hacia el emisor por el camino inverso, se establece la ruta entre los nodos origen y destino. A su vez, el envío de RREP se utiliza para que los nodos intermedios por los que el mensaje va pasando actualicen sus tablas de encaminamiento.

Una optimización para este procedimiento de descubrimiento de ruta es la técnica del aumento del anillo de búsqueda ya comentada anteriormente. Consiste en enviar los mensajes RREQ con un tiempo de vida (TTL) bajo para evitar su propagación por toda la red. Si tras un tiempo no se ha recibido el RREP se envía otro RREQ con un TTL mayor. Este proceso de incrementar el TTL podrá repetirse hasta que se alcance un TTL umbral. Una vez superado, se inunda la red.

2.6.3 Mantenimiento de rutas

En la tabla de encaminamiento de AODV se distinguen las entradas en función de si fueron creadas al recibir un RREQ o un RREP. Si se crearon con la llegada de un mensaje RREP son rutas hacia delante, las cuales se eliminarán si no se usan durante un intervalo de tiempo de ruta activa, es decir, si no se transmite ningún dato por esa ruta, aún cuando la ruta siga siendo válida. Si la ruta se conoció por un mensaje RREQ se dice que la ruta es hacia atrás y se

eliminará transcurrido un intervalo de tiempo, normalmente menor que el de ruta activa y suficientemente amplio como para permitir la vuelta del RREP.

Cuando el enlace al siguiente salto en una entrada de tabla se rompe, se informa a todos los vecinos activos. Un vecino de un nodo se considera activo para una entrada si envió un paquete por dicha entrada dentro del intervalo de ruta activa. Las rupturas de enlace se propagan por medio de mensajes de error de ruta, o RERR, que también actualizan los números de secuencia de destino.

Cuando un nodo no puede transmitir un paquete por fallo del siguiente enlace, incrementa su número de secuencia de destino y genera un RERR que incluye dicho número. Cuando la fuente recibe el RERR inicia un nuevo descubrimiento de ruta hacia el destino anterior, pero usando un número de secuencia al menos tan grande como el recibido. Al llegar el nuevo RREQ con el número dado al nodo destino, éste lo establece como su número de secuencia, a menos que ya tenga un número mayor que el recibido.

Los nodos vecinos pueden intercambiarse periódicamente mensajes de HELLO para detectar los fallos de enlace. La no recepción de este tipo de paquetes de un vecino activo puede interpretarse como la ruptura del enlace entre ellos.

3. TECNOLOGÍAS IPV6

IPv6 (también conocido como IPng o "IP de nueva generación") es la nueva versión del conocido protocolo de red IP, también llamado IPv4. IPv6, desarrollado por IETF, es capaz de trabajar junto a IPv4 y se desplegará de manera gradual ya que es necesario mantener todas las infraestructuras que actualmente funcionan con IPv4.

El capítulo se divide en las siguientes secciones. En la sección 3.1 se repasan los motivos por los que aparece IPv6. El apartado 3.2 comenta las características más relevantes de IPv6. En las secciones 3.3 y 3.4 se analizan las dos mejoras más significativas que incluye IPv6 para dar soporte a redes como las MANET, la autoconfiguración de direcciones y la movilidad respectivamente.

3.1 ¿Por qué IPv6?

Los creadores de IPv4 (a principios de los años 70) no se imaginaron el gran éxito que el protocolo iba a tener en muy poco tiempo. IPv4 no sólo comenzó a utilizarse en campos científicos y de educación sino en muchos otros. A comienzos de los años 90 comenzó a surgir una gran preocupación por el rápido consumo del espacio de direcciones de IPv4.

IPv4 soporta 4.294.967.296 (2^{32}) direcciones de red diferentes, un número que no permitiría dar una dirección a cada persona del planeta, y mucho menos para cada coche, teléfono, PDA, etc. Sin embargo, IPv6 soporta 340.282.366.920.938.463.463.374.607.431.768.211.456 (2^{128}) direcciones, cerca de 3,4 × 1020 (340 trillones) direcciones por cada pulgada cuadrada de la Tierra.

Por otro lado, en IPv4 el número de entradas en las tablas de rutas comenzaba a ser imposible de manejar. Con IPv6 los *routers* solamente guardan direcciones de red agregadas reduciendo así las entradas de la tabla de rutas.

IPv4, debido a la gran cantidad de aplicaciones que ha tenido, ha incorporado varias mejoras sobre el protocolo básico como permitir la Calidad de Servicio (*QoS*), seguridad con IPsec o movilidad, entre otras. El mayor problema que presentan están ampliaciones es que debido a su posterior diseño es muy difícil usar más de una a la vez.

3.2 Características de IPv6

Entre las mejoras que aporta IPv6 con respecto a IPv4 se encuentra el mayor espacio de direccionamiento que pasa de 32 bits a 128 bits, simplificación de la cabecera de IPv4 para facilitar su procesado, inclusión de IPsec, que permite autenticación y encriptación del propio protocolo base, e introduce el concepto de calidad de servicio para diferenciar diferentes flujos de tráfico.

Para el campo de las redes MANET y teniendo en cuenta el objetivo de este trabajo existen dos mejoras significativas en IPv6 como son la autoconfiguración de direcciones y la movilidad.

3.2.1 Cabecera IPv6

La cabecera en IPv4, de una longitud mínima de 20 bytes, es la mostrada en la figura 3.1. Los campos sin sombreado se corresponden con los campos que se han modificado y el resto los que desaparecen en IPv6.

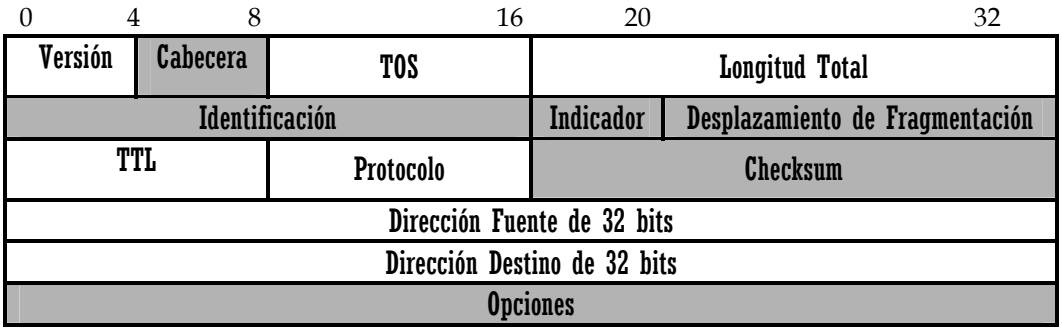

Fig. 3.1. Cabecera IPv4

En la cabecera de IPv6 (figura 3.2), con un tamaño de 40 bytes, se han eliminado varios campos para evitar la redundancia que existía en IPv4 como la

verificación de la integridad de la cabecera que otros mecanismos de encapsulado ya se encargan de realizarla como IEEE 802 MAC. Otros campos son inútiles como el campo "Desplazamiento de Fragmentación" ya que en IPv6 los encaminadores no fragmentan los paquetes.

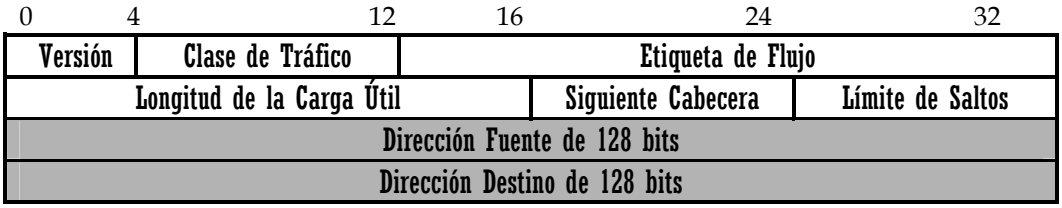

Fig. 3.2. Cabecera IPv6

La longitud fija de la cabecera hace que su procesado por parte de los encaminadores y conmutadores sea mucho más fácil.

Existen otros campos que cambian de nombre:

- "Longitud total" pasa a llamarse "Longitud de carga útil". Tiene una longitud de 2 bytes e indica la longitud de los datos.

- "Protocolo" pasa a llamarse "Siguiente cabecera". En IPv6 en lugar de usar cabeceras de longitud variable se emplean varias cabeceras encadenadas. Esto hace que desaparezca el campo de opciones. La longitud de este campo es de 1 byte.

- "Tiempo de vida" pasa a llamarse "Límite de saltos". Su longitud es de 1 byte.

Por último se añaden 2 campos nuevos que permiten a IPv6 implementar la Calidad de Servicio (*QoS*) y la Clase de Servicio (*CoS*):

- "Clase de tráfico" o "Prioridad" o "Clase". Su función es parecida al campo "TOS" de IPv4. Su longitud es de 1 byte.

- "Etiqueta de flujo". Utilizado para requisitos de tiempo real. Su

longitud es de 20 bits.

Realmente estos dos últimos campos añaden un mecanismo de control de flujo que permite la asignación de prioridades diferenciadas según los tipos de servicios.

3.2.2 Tipos de direcciones

IPv6 tiene direcciones de 128 bits contra los 32 bits de IPv4. Las direcciones se expresan con el formato *ipv6-address/prefix*, donde *prefix* es un número decimal que indica cuantos bits de la parte izquierda de la dirección pertenecen a la red. Las direcciones IPv6 permiten números hexadecimales y están compuestas por 8 grupos, de 4 números hexadecimales cada uno, separados por dos puntos cada grupo.

Las direcciones utilizadas en IPv6 están formadas por un prefijo de red y un identificador de la interfaz a la que están asignadas. Existen tres tipos distintos de direcciones IPv6: *unicast*, *anycast* y *multicast*.

Las direcciones *unicast* son identificadores para una única interfaz. El paquete que se envía a una dirección *unicast* se entrega sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4.

Las direcciones *anycast* son identificadores para un conjunto de interfaces que normalmente pertenecen a varios nodos. El paquete enviado a una dirección *anycast* será entregado en una (cualquiera) de las interfaces identificadas con dicha dirección (la más cercana).

Las direcciones *multicast* son identificadores para un conjunto de interfaces. El paquete enviado a una dirección *multicast* será entregado en todas las interfaces identificadas con dicha dirección. Permiten expresar las direcciones *broadcast* que existían en IPv4.

Las direcciones *unicast* se pueden dividir a su ver en tres tipos:

- *Link-local*. Se usan en un solo enlace para labores como configuración automática de direcciones, descubrimiento de vecinos, o situaciones en las que no hay *routers*. Un *router* no retransmitirá a otro enlace un paquete que tenga como origen o destino un dirección *link-local* (el ámbito está limitado a la red local).

- *Site-local*. Se usan para fijar direcciones a los *hosts* de una red con el fin de que puedan establecer comunicación entre ellos sin necesidad de tener un prefijo de red global. Un *router* no retransmitirá fuera de la red un paquete cuyo origen o destino sea una dirección *site-local*.

- *Global*. Son las direcciones válidas para operar en Internet y asignadas de manera jerárquica.

La conexión a Internet se realiza a través de una dirección global. El protocolo IPv6 es una extensión del protocolo IPv4 que permite obtener dichas direcciones.

3.3 Autoconfiguración de direcciones

El proceso de autoconfiguración es el conjunto de pasos a través del los cuales un *host* decide como obtener su configuración de interfaces en IPv6. El es mecanismos que permite afirmar que IPv6 es "Plug & Play".

Durante el proceso se obtiene una dirección de enlace local, se verifica que no está duplicada en el enlace y se determina la información que ha de ser configurada (direcciones y otra información).

Dentro de IPv6, las direcciones de los nodos pueden ser configuradas automáticamente, sin la ayuda de los usuarios. Para ello, se configurarán los

routers con un prefijo de red además de otros datos. Posteriormente, y de forma periódica, los *routers* se encargarán de enviar mensajes de información llamados *Router Advertisement* (RA) a toda la red. Una vez que un nodo recibe un mensaje RA obtiene su identificador de interfaz (a través de su dirección MAC u otra información) y la concatenan al final del prefijo de red que han recibido en el mensaje RA del *router*. También es posible realizar una autoconfiguración a través de un servidor DHCPv6 como se verá en este trabajo.

Por tanto en IPv6 existen dos propuestas de autoconfiguración de direcciones:

- Autoconfiguración de direcciones de estado completo (*stateful*)
- Autoconfiguración de direcciones sin estado (*stateless*)

La autoconfiguración de direcciones de estado completo se basa en la utilización de servidores como DHCPv6 que controlan y asignan las direcciones a todos los nodos de la red. Este mecanismo será visto en profundidad en los capítulos 5 y 6.

El mecanismo de autoconfiguración sin estado se suele emplear cuando no importa la dirección exacta que se asigna a un nodo sino tan sólo asegurarse que es única y correctamente enrutable. Esta solución es muy útil para redes MANET ya que no obliga a la existencia de un elemento dedicado.

La autoconfiguración de direcciones sin estado propone que sea el propio nodo el encargado de generar su dirección IP. La dirección se obtiene de la concatenación de un prefijo de red conocido y un número teóricamente único dentro de la red generado por el nodo. Este mecanismo puede exigir la inclusión de un módulo encargado de comprobar la unicidad de la dirección generada llamado Detección de Direcciones Duplicadas o DAD (*Duplicate Address Detection*).

En redes móviles ad hoc se pueden distinguir dos tipos de DAD. En uno de ellos el dispositivo comprueba la unicidad de su dirección justo de después de haberla generado. En este caso el mecanismo toma el nombre de DAD pre-servicio (*pre-service* DAD). Como alternativa existe la posibilidad de utilizar DAD en-servicio (*in-service* DAD), en el que el terminal comprueba periódicamente que su dirección sigue siendo única en la red. Este tipo de operaciones son necesarias para detectar duplicidades originadas por la unión de redes.

El mecanismo de autoconfiguración sin estado ha sido diseñado con las siguientes premisas:

- Evitar una configuración manual de los nodos. El procedimiento permite a un nodo obtener o crear direcciones únicas para cada una de sus interfaces. En el caso más simple, el identificador de interfaz consiste en la dirección de la capa de enlace de dicha interfaz.

- Para pequeñas redes no es necesaria la existencia de un servidor *stateful* o router para establecer la comunicación entre los nodos. Los nodos pueden utilizar las direcciones de enlace local que poseen un prefijo perfectamente conocido que identifica el único enlace compartido al que se conectan todos los nodos. Cada nodo, para formar su dirección, antepone el prefijo de enlace local a su identificador de interfaz.

- En el caso de redes grandes que incluyen varias subredes y *routers* tampoco es necesario el uso de servidores *stateful*. Los nodos requieren los prefijos que identifican las subredes a las que se conectan para generar sus direcciones globales o de enlace local. Estos prefijos pueden ser anunciados periódicamente por los *routers*.

- Un administrador debe tener la capacidad de especificar el mecanismo

(*stateless*, *stateful*, o ambos) que será aplicado por los nodos. Los *routers* pueden realizar esta función mediante mensajes de anunciación.

3.4 Movilidad

Dada la versatilidad que proporcionan las redes móviles ad hoc cualquier dispositivo que se encuentre en una red puede salirse de ésta y adentrarse en otra sin previo aviso en un movimiento de itinerancia o *roaming*. En estas situaciones es necesario proveer de un mecanismo que permita al nodo continuar con las comunicaciones establecidas con los nodos de la red que ha abandonado. El objetivo es que un nodo sea alcanzable mientras se mueve por Internet. Al ir cambiando de redes cambiará también su dirección IP (debido al direccionamiento jerárquico en Internet), pero hay que asegurar que reciba los paquetes dirigidos a su dirección IP original.

El protocolo IPv6, a través del llamado *Mobile IPv6*, permite que un nodo móvil se mueva desde una red móvil hasta otra cambiando su dirección pero sin dejar de recibir paquetes desde su red original. Para ello es necesario que en la red original exista un *router* o agente local (*home agent*) que recoge la nueva dirección del nodo en la nueva red y se encarga de transmitir a la nueva red los paquetes que llegan con la dirección original del nodo.

Inicialmente un nodo tendrá una dirección IP original llamada *home address* y en cada red que visita recibe otra llamada *care of address*. Cada vez que el nodo recibe una nueva *care of address* registra ésta en su *home agent*. Este proceso de asociar la *home address* con la *care-of address* se conoce como *binding*. Para realizarlo, el mobile node envía un mensaje Binding Update (BU) a su *home agent* informándole de su movimiento. Este es uno de los muchos mensajes *Mobile IPv6* que se codifican en una nueva cabecera de extensión de IPv6 llamada *mobility header*. La finalidad del BU es informarle al *home agent* de la nueva dirección del nodo móvil. Un mensaje Binding Acknowledgement (BA)

es enviado en contestación al BU.

Cuando un nodo de Internet (*correspondent node*) envía un paquete a la *home address,* éste llega a la red de origen del nodo. Si el nodo móvil se encuentra en su red origen recibe el paquete y la comunicación prosigue de forma habitual. En caso contrario, es decir, el nodo está de itinerancia en otra red, el paquete será recogido por el *home agent* y éste retransmitirá el paquete a la *care of address* del nodo móvil.

A partir de ese momento, el *home agent* funcionará como *proxy* del nodo móvil. Todo paquete que se envíe a la *home address* del nodo, primero pasará por el *home agent*. Después el *home agent* retransmitirá el paquete a la *care of address*. El sentido de este enlace entre el nodo y el *home agent* es bidireccional, es decir, cuando el nodo móvil necesita enviar un paquete al *correspondent node* lo hará también a través del *home agent* tal y como indica la figura 3.3.

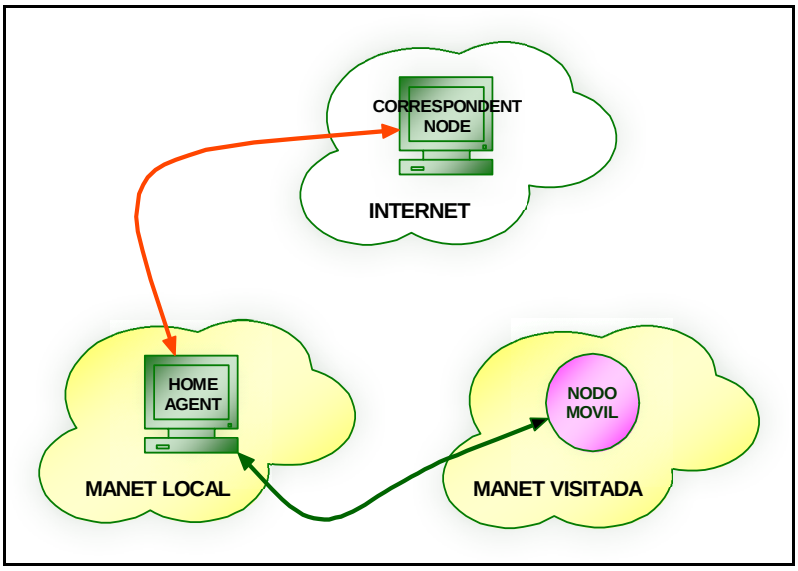

Fig. 3.3. Comunicación no optimizada

La situación anterior provoca que todo el tráfico entre el nodo móvil y el *correspondent node* deba pasar por el *home agent*, lo que supone un gran cuello de botella. En consecuencia supondría que si el *home agent* cae, todas las conexiones fallarían. Para solucionar esta situación IPv6 obliga al nodo móvil informar de

su dirección al *correspondent node* a través de un nuevo mensaje BU. A partir de este momento el *correspondent node* enviará a la *care of address* los paquetes cuyo destino sea el nodo móvil. A este proceso que se muestra en la figura 3.4 se le denomina *Route Optimization*.

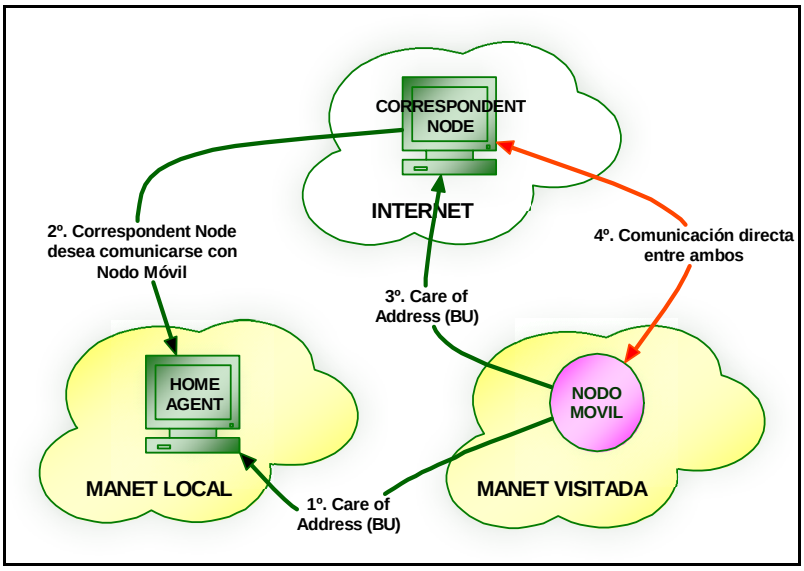

Fig. 3.4. Comunicación optimizada

La movilidad en IPv6 podría presentar cierta vulnerabilidad ante los posibles atacantes. Por ejemplo, un atacante puede enviar al *home agent* un mensaje BU diciéndole que posee una *care of address* falsa. De esta forma se crearía un túnel entre el nodo y el *home agent* incorrecto. De la misma forma un atacante puede enviar un mensaje BU en nombre de otro nodo a un *correspondent node* diciéndole que un nodo está en ubicación distinta a la real. Para evitar cualquier tipo de ataque, IPv6 obliga a utilizar asociaciones de seguridad, usando IPsec entre todos los nodos. De esta forma se protege la autenticidad e integridad de los mensajes intercambiados en el proceso.

4. INTEGRACIÓN A INTERNET DE REDES MÓVILES AD HOC

Las redes MANET juegan un papel importante en aplicaciones militares o marítimas, son de gran utilidad en conferencias y congresos, ayudan a equipos de rescate o resuelven muchos problemas en otras situaciones en las que varios dispositivos móviles necesitan compartir información.

En cualquiera de los casos anteriores el acceso a Internet es uno de los servicios más demandados en la actualidad y el gran avance de los dispositivos móviles requiere el desarrollo de esta característica. Sin embargo, las tecnologías actuales aún no están preparadas para dar soporte a este tipo de redes y necesitan solventar ciertos problemas. Estos problemas se originan principalmente por la topología altamente dinámica de las redes MANET así como de la comunicación multisalto. En una red sin infraestructura fija como es una red MANET no existen estaciones base a las cuales los nodos móviles se conectan para poder transmitir y tampoco existen *routers* especializados. En este tipo de redes los nodos son móviles y pueden ser dinámicamente conectados de maneras arbitrarias. De hecho, los nodos trabajan como *routers* ya que se encargan de descubrir y mantener rutas con el resto de nodos de la red.

El resto del capítulo se organiza de la siguiente manera. El apartado 4.1 repasa los aspectos fundamentales que son necesarios para que una MANET consiga el acceso a Internet. En el apartado 4.2 se presentan varias propuestas para conseguir la integración a Internet de las redes móviles ad hoc. En último lugar, el apartado 4.3 profundiza en el método utilizado en este trabajo para conseguir que los nodos de una MANET tengan acceso a Internet.

4.1 Introducción

Para la conexión a Internet debe existir un *router* de acceso que sea el encargado de conectar la red MANET con Internet. Los nodos de la red que se

encuentren en el área de cobertura del *router* de acceso no tendrán problemas para conectarse con otros *hosts* externos. Los *routers* actuales no cuentan con el soporte necesario para funcionar con una red MANET ya que su información se restringe a su área de cobertura. Existen varias propuestas (en forma de *IETF Internet Drafts*) encaminadas a dar soporte a las restricciones que presentan los *routers* de acceso convencionales y que se pueden dividir en 2 grupos:

- Inclusión de un *gateway*. Conectado al *router* de acceso, ya sea a través de una conexión cableada o inalámbrica, aparece un nuevo elemento llamado *gateway* que servirá de puente entre el r*outer* de acceso y la red MANET. El *gateway* proporcionará al r*outer* de acceso las funcionalidades de encaminamiento ad hoc. En este caso se trata de *gateways* **dedicados** que incorporan dos interfaces, una para conectarse con el *router* de acceso y otra para comunicarse con la red ad hoc. Algunas propuestas incluso sugieren modificar el r*outer* de acceso para que incluya las funcionalidades del *gateway*.

- Añadir funcionalidad a los nodos de la red MANET creando los llamados *gateways* **oportunistas**. Los nodos tendrán la función de *gateway* de tal forma que la conexión a Internet sea responsabilidad de la red MANET y no del r*outer* de acceso.

El *gateway*, pues, complementa al *router* de acceso. Por un lado, un *gateway* posibilita que los paquetes procedentes de Internet puedan viajar a través de múltiples saltos en la red proporcionando así las funcionalidades de encaminamiento ad hoc. Por otro lado, envía mensajes específicos a todos los nodos para que conozcan la dirección a la que deben enviar los paquetes cuyo destino es un *host* exterior y a la vez ayuda a la autoconfiguración de direcciones de los nodos de la MANET. Retransmiten la información del *router* de acceso.

Las tecnologías actuales presentan las siguientes limitaciones para garantizar

la integración de redes MANET con redes externas:

- Incapacidad de operar en entornos multisalto
- Incapacidad de operar con topologías altamente dinámicas
- Incapacidad de abordar la unión de redes
- Incapacidad de ofrecer soporte al particionado de redes

4.2 Propuestas de Integración a Internet de redes móviles ad hoc

Las funcionalidades junto con las características del *gateway* distinguen las propuestas para la integración de redes MANET con redes externas. A continuación se describen las más significativas.

4.2.1 Conectividad global

En esta estrategia existe un *gateway* dedicado conectado al *router* de acceso de forma inalámbrica o cableada. En ciertas ocasiones el *gateway* puede estar implementado en el propio *router* de acceso [Wakikawa, 2006].

El *gateway* puede funcionar con tres políticas diferentes:

- Reactiva. Un nodo que necesite información del *gateway* manda un mensaje IGWSOL (*Internet Gateway Solicitation*) que llega a todos los nodos de la MANET, incluido el *gateway*. Cuando éste último recibe el mensaje contesta al nodo con un mensaje IGWADV (*Internet Gateway Advertisement*). El nodo utilizará el mensaje de respuesta para configurar su dirección IP o para actualizar la dirección de su *gateway*.
- Proactiva. En este caso el *gateway* envía periódicamente mensajes de difusión IGWADV a todos los nodos de la MANET.

- Híbrida. Se trata de una combinación de las técnicas anteriores. El *gateway* se comporta de manera proactiva para los nodos que tiene cerca y el resto de nodos que no reciben los mensajes del *gateway* se comportan de forma reactiva.

En este trabajo se ha utilizado la implementación de [Hamidian, 2003] modificando los mensajes de control del protocolo de encaminamiento AODV para conseguir la conectividad a Internet. Será analizado en profundidad en el apartado 4.3.

4.2.2 Continuidad de prefijo

Este mecanismo trata de reducir la sobrecarga en la red haciendo que el *gateway* emita mensajes de información GW_INFO a sólo aquellos nodos que se encuentren a un salto. El mensaje incluye el prefijo de red adecuado para la conexión a Internet. Cada nodo que reciba el mensaje, lo reenviará a sus nodos vecinos. Si un nodo recibe varios mensajes de información de diferentes *gateways* solamente retransmitirá el del *gateway* que tenga establecido.

4.2.3 Configuración automática de múltiples *gateways*

Aplicable cuando existe más de un *gateway* que envía mensajes a los nodos de la red ad hoc. A diferencia de otros métodos en los que los nodos solamente guardan información del *gateway* que tienen establecido, este mecanismo permite guardar la información de todos los *gateways*. De esta forma la conmutación de un *gateway* a otro es inmediata.

4.2.4 Mecanismo de múltiples *gateways* móviles

Esta técnica está basada en el uso de *gateways* oportunistas. Cualquier nodo de la red ad hoc puede realizar las funciones de *gateway* sin limitar su capacidad de movimiento por la red.

4.3 AODV para la integración a Internet

En la implementación realizada por [Hamidian, 2003], sobre el protocolo de encaminamiento AODV, extiende los mensajes RREQ y RREP para poder llevar a cabo la conectividad con Internet, con los mensajes RREQ_I y RREP_I.

También añade un nuevo mensaje, GWADV, con formato similar al mensaje RREP. Para el descubrimiento proactivo de *gateway* el mensaje GWADV se extiende, añadiendo un campo identificador de RREQ denominado RREQ ID, para evitar la inundación de la red con mensajes de anuncio de *gateway* duplicados.

4.3.1 Mensajes extendidos

A continuación se enumeran los mensajes extendidos de AODV para conseguir la conectividad con Internet.

4.3.1.1 Mensajes RREQ_I

Los mensajes RREQ_I se diferencian de los mensajes RREQ explicados anteriormente en que incorporan un nuevo *flag* denominado *Flag* de Resolución de Dirección Global-Internet y es referido como *flag* I. Este *flag* se usa en la resolución de la dirección global e indica que un nodo origen solicita conectividad global.

Tipo	J	R	G	I	Reservado	Nº de saltos
RREQ ID						
Dirección IP del destino						
Número de secuencia del destino						
Dirección IP del origen						
Número de secuencia del origen						

Fig. 4.1. Formato del mensaje extendido RREQ_I de AODV

El mensaje RREQ_I es una extensión del mensaje de solicitud de *router* del protocolo NDP (*Neighbor Discovery Protocol*) [Narten, 1998] para el descubrimiento de nodos vecinos. A diferencia de los mensajes del protocolo

NDP, estos mensajes se pueden propagar por la red por múltiples saltos. En el apartado 4.3.2.1 se describirá cómo se utiliza en el descubrimiento de *gateway* de forma reactiva. En la Figura 4.1 puede verse cómo queda el formato del mensaje RREQ_I.

4.3.1.2 Mensajes RREP_I

Los mensajes RREP_I contienen los mismos campos que los mensajes RREP explicados anteriormente, con la única diferencia de que incorporan un *flag* denominado *flag* I. Este *flag* es el mismo que se utiliza para extender el mensaje RREQ al mensaje RREQ_I. En la Figura 4.2 puede observarse cómo queda el formato del mensaje RREP_I.

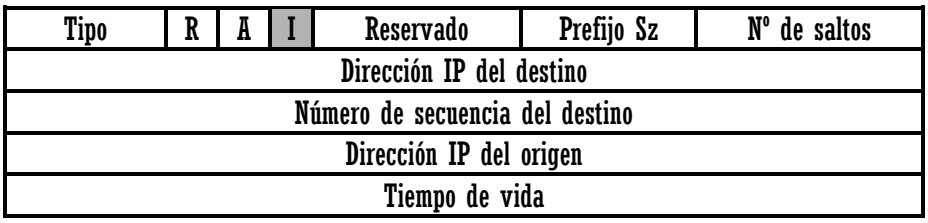

Fig. 4.2. Formato del mensaje extendido RREP_I de AODV

El *flag* I se utiliza para la resolución de la dirección global y si está indica que dicho paquete RREP contiene información sobre un *gateway*. El mensaje RREP_I es una extensión del mensaje de anuncio de *router* del protocolo NDP. De igual manera a los RREQ_I, se pueden propagar por la red por múltiples saltos en la misma. En el apartado 4.3.2.2 se describe cómo los mensajes RREP_I pueden ser usados por un *gateway* para anunciar información sobre él mismo de forma proactiva a los nodos que se encuentren situados cerca. A diferencia de los RREP convencionales de AODV, los RREP_I pueden ser:

- *Unicast* cuando son enviados como respuesta a un mensaje RREQ_I.

- *Multicast* cuando los envía el *gateway* de forma proactiva a los nodos cercanos para dar información sobre él mismo. Suelen enviarse periódicamente. Para solucionar el problema de los mensajes de anuncio duplicados, incorporan un nuevo campo y se denominan

mensajes GWADV.

4.3.1.3 Mensajes GWADV

Estos mensajes se incorporan para solucionar el problema de los mensajes de anuncio duplicados. Los mensajes RREQ tienen un campo RREQ ID, y cuando un nodo recibe un RREQ comprueba, antes de procesarlo, no haber recibido anteriormente algún RREQ con la misma dirección de origen y el mismo RREQ ID. Si ya lo había recibido, lo descarta. Así se detectan los duplicados de los mensajes RREQ. Los mensajes de anuncio son similares a los RREP, los cuales no contienen ningún campo parecido al RREQ ID con el que poder hacer la comprobación.

Por ello, se crea este nuevo mensaje para AODV, los mensajes de anuncio de *gateway* o GWADV (*GateWay ADVertisement*). Este nuevo tipo de mensajes, cuyo formato puede verse en la Figura 4.3, es básicamente un mensaje RREP extendido con un campo del mensaje RREQ, el campo RREQ ID.

Tipo	Reservado	Prefijo Sz	Nº de saltos
RREQ ID			
Dirección IP del destino			
Número de secuencia del destino			
Dirección IP del origen			
Tiempo de vida			

Fig. 4.3. Formato del mensaje GWADV de AODV

Cuando un nodo móvil recibe un GWADV primero comprueba si ha recibido alguno con la misma dirección IP origen y el mismo RREQ ID en un período definido por la variable BCAST_ID_SAVE (valor por defecto 6 segundos). Si el mensaje no había sido recibido en ese tiempo, se vuelve a reenviar en modo *broadcast* por difusión al resto de nodos, en otro caso, se descarta. De esta forma se consigue no reenviar mensajes de anuncio de *gateway* que estén llegando duplicados y evitar, así, provocar más congestión en la red.

La desventaja de utilizar esta solución para evitar los mensajes de anuncio

duplicados es que requiere modificar AODV para introducir este nuevo tipo de mensajes.

4.3.2 Descubrimiento de *gateway*

Hay tres tipos de mecanismos de descubriendo de *gateway* (reactivo, proactivo o híbrido) como ya se comentó en el apartado 4.2.1 y se diferencian en si este procedimiento lo inicia el nodo móvil, el *gateway* o ambos. A continuación, se explica cómo se implementa cada uno de ellos cuando el protocolo de encaminamiento utilizado es AODV.

4.3.2.1 Descubrimiento reactivo de *gateway*

El descubrimiento reactivo de *gateway* se inicia por un nodo móvil cuando requiere por primera vez información sobre un *gateway* o quiere actualizar la que ya posee. El nodo móvil enviará en modo *broadcast* por difusión un mensaje RREQ_I (ver Figura 4.1) hacia la dirección IP *multicast* definida para el grupo de todos los *gateways* de la MANET. A través de esa dirección de *multicast* el destino del mensaje RREQ_I sólo serán los *gateways* presentes en la red ad hoc, y sólo éstos procesarán el mensaje. Los nodos intermedios que reciban el mensaje sólo se encargarán de volver a enviarlo en modo *broadcast* por difusión. Al igual que los mensajes RREQ, los mensajes RREQ_I tienen un campo identificador de RREQ, con el cual se pueden detectar los mensajes duplicados y, por consiguiente, descartarlos. Cuando un *gateway* reciba el RREQ_I, enviará en modo *unicast* un mensaje RREP_I de vuelta que, entre otra información, contiene la dirección IP del *gateway*.

La ventaja del descubrimiento reactivo de *gateway* es que los mensajes RREQ_I se envían sólo cuando un nodo móvil necesita información sobre *gateways* para su alcance. Así, al no producirse la inundación de la red con mensajes de información de los *gateways* de forma periódica se ahorra el correspondiente ancho de banda. La principal desventaja de esta aproximación es que, generalmente, aumenta la carga en los nodos, por el reenvío de estos

mensajes, especialmente en los que se encuentran situados cerca de los *gateways*. Otra desventaja es que aumenta la latencia de la comunicación si el nodo está esperando la información del *gateway* para poder iniciarla.

4.3.2.2 Descubrimiento proactivo de *gateway*

El descubrimiento proactivo de *gateway* se inicia por el propio *gateway* inundando periódicamente la MANET con mensajes de anuncio de *gateway* (GWADV) que se transmiten en cada intervalo de TMRA, con un valor típico de 2 a 60 segundos. TMRA es la variable que indica la periodicidad con la que serán enviados los mensajes de anuncio de *gateway*, o MRA, a la MANET. Es importante señalar que el valor de este parámetro afecta a las prestaciones de la red, por lo que se han propuesto algoritmos para ajustarlo a las condiciones de la red [Triviño, 2007].

El proceso de recepción de mensajes es el siguiente: los nodos móviles que se encuentren en el rango de transmisión del *gateway* recibirán el mensaje de anuncio y los que no tuvieran ya una ruta hacia el *gateway* la crearán con una entrada nueva en su tabla de encaminamiento. Los nodos que ya tuvieran una ruta hacia el *gateway* actualizarán la entrada correspondiente de su tabla. A continuación, los nodos reenviarán el mensaje de anuncio de *gateway* a los nodos que se encuentren dentro de la zona de su rango de transmisión y así sucesivamente con el resto de nodos que reciban el mensaje de anuncio de *gateway*. Para asegurar que todos los nodos móviles de la MANET reciben el mensaje de anuncio, el número de retransmisiones lo determinará el protocolo AODV en el parámetro que especifica el diámetro de red o número de saltos máximo de los mensajes de anuncio de *gateway*, DRED, que suele tener un valor por defecto de 30 saltos. Sin embargo, esto puede conducir a que se vayan recibiendo en los nodos muchos mensajes duplicados del mensaje de anuncio de *gateway*.

El principal inconveniente de esta aproximación es común a todas las

aproximaciones proactivas y reside en el hecho de que el envío de los mensajes de anuncio de forma periódica inundando la red consume muchos recursos, ya sea en ancho de banda, operación en los nodos o baterías, característica no deseable en este tipo de redes para que su autonomía sea más duradera.

4.3.2.3 Descubrimiento híbrido de *gateway*

El descubrimiento híbrido de *gateway* surge para tratar de minimizar las desventajas de los dos anteriores combinando las dos estrategias presentadas. Según el descubrimiento híbrido, los nodos móviles que se encuentran en un cierto rango alrededor del *gateway* usará el método de descubrimiento proactivo de *gateway*, mientras que para los nodos que estén más alejados utilizará la aproximación reactiva para que los nodos de la MANET obtengan información sobre el *gateway*.

Así pues, el *gateway* enviará periódicamente mensajes RREP_I (ver Figura 4.2) en modo *broadcast* por difusión. El mensaje RREP_I se enviará en cada intervalo de TMRA, con un valor típico de 2 a 60 segundos. Todos los nodos que se encuentren en el rango de transmisión del *gateway* recibirán el RREP_I, tras lo cual, los que no tuvieran una ruta hacia el *gateway* la crearán en una entrada en su tabla de encaminamiento. Los nodos que ya tuvieran una ruta hacia el *gateway* actualizarán dicha entrada en su tabla. Después de esto, los nodos móviles que habían recibido el RREP_I lo reenviarán a los nodos que haya en su rango de transmisión y, así sucesivamente lo irán retransmitiendo los nodos que lo vayan recibiendo. El máximo número de saltos que un mensaje RREP_I puede dar a través de la MANET vendrá especificado por el parámetro TTLMRA con un valor típico de 3 saltos. Este valor define el rango donde será usado el descubrimiento de *gateway* proactivo.

Cuando un nodo móvil quede fuera del rango donde el descubrimiento de *gateway* se hace de forma proactiva, el nodo mandará en modo *broadcast* por difusión un RREQ_I a la dirección IP *multicast* de los *gateways* de la MANET.

Los nodos móviles que reciban ese mensaje sólo lo volverán a enviar en modo *broadcast* por difusión, sin procesarlo. Cuando el mensaje RREQ_I llega al *gateway*, éste envía de vuelta hacia el nodo un mensaje RREP_I en modo *unicast*.

5. DHCP

DHCP (*Dynamic Host Configuration Protocol*) es un protocolo de direccionamiento IP que permite asignar de forma automática direcciones IP a los nodos de una red.

Sin DHCP todos los nodos de una red deberían configurar manualmente su dirección IP y en caso de que muevan, volver a configurarla. DHCP permite a un administrador controlar la asignación de direcciones de forma automática.

El capítulo se divide en los siguientes apartados. En el apartado 5.1 se realiza una introducción al protocolo DHCP realizando una breve comparación entre DHCPv4 y DHCPv6. El apartado 5.2 analiza los aspectos fundamentales del protocolo DHCPv6. Por último, en el apartado 5.3 se detalla el proceso de configuración con DHCPv6.

5.1 Introducción

Un servidor DHCP (DHCP *Server*) es un equipo que ejecuta un servicio DHCP. Dicho servicio se encuentra a la escucha de peticiones DHCP y cuando una de estas peticiones es oída, el servidor responde con la información solicitada. La respuesta puede incluir una dirección IP libre pero también se puede tratar de otro tipo de información como dirección del servidor DNS, nombre DNS, puerta de enlace (*gateway*) de la dirección IP, dirección de publicación masiva, máscara de subred, MTU (*Maximun Transfer Unit*) para la interfaz, servidores NIS (*Network Information Service*), dominios NIS, servidores NIS, etc.

DHCP proviene del protocolo Bootstrap (BootP). BootP fue de los primeros métodos para asignar de forma dinámica direcciones IP a otros equipos (ordenadores, impresoras, etc.). Al crecer las redes, BootP ya no era tan

adecuado y DHCP fue creado para cubrir las nuevas demandas.

DHCP surgió como un protocolo estándar en Octubre de 1993, definido por la IETF (*Internet Engineering Task Force*) en el RFC 1531 (*Dynamic Host Configuration Protocol*) [Droms, 1993]. La última revisión se produjo en 1997 y se encuentra en el RFC 2131 [Droms, 1997] conocido hoy como DHCPv4. Con la aparición de IPv6 surgió DHCPv6 definido en Julio de 2003 en el RFC 3315 (*Dynamic Host Configuration Protocol for IPv6* (DHCPv6)) [Droms, 2003].

Existen dos diferencias principales entre DHCPv4 y DHCPv6. Una de ellas es el modelo de administración ya que mientras que en DHCPv4 el administrador activa DHCP para cada interfaz, realizando una administración por interfaz lógica, en DHCPv6 no es necesaria una configuración explícita, activándose el protocolo en una interfaz física determinada. La otra diferencia se encuentra en la forma de proporcionar la máscara de subred, mientras que en DHCPv4 se proporciona en cada dirección, en DHCPv6 la proporcionan los anuncios de encaminador, no el servidor DHCP.

5.2 DHCPv6

DHCP para IPv6 es un protocolo UDP cliente/servidor que ha sido diseñado para reducir el coste de gestión de los nodos IPv6 en lugares donde un administrador necesita un control en la asignación de los recursos de la red, mayor al que proporciona el mecanismo de configuración sin estado (*stateless*).

DHCPv6 se centra en la gestión de recursos de red como direcciones IP, información de encaminado, instalación de Sistemas Operativos, información de servicios de directorios. Para ello utiliza uno o varios servidores DHCP en lugar de mantener la información en ficheros de configuración.

DHCPv6 automatiza la asignación de direcciones IP, máscaras de subred, *gateway* por defecto, y otros parámetros IP. Cuando un cliente que ha sido

configurado para DHCP (puede ser un ordenador u otro tipo de dispositivo) se conecta a la red y manda una consulta a toda la red (*multicast*) solicitando información al servidor DHCP. El servidor DHCP puede manejar una lista de direcciones IP, información acerca de la configuración de cada cliente como el *gateway* por defecto, el nombre de dominio, los servidores DNS, etc. Una vez que el servidor recibe una petición validada asigna al cliente una dirección IP y el resto de parámetros necesarios.

El protocolo ha sido diseñado para que pueda extenderse de forma fácil con nuevos parámetros de configuración a través de las denominadas extensiones. Por otro lado, es compatible con un mecanismo de autoconfiguración sin estado.

5.2.1 Modos de asignación de direcciones

DHCP dispone de tres modos para asignar las direcciones IP: manual, automática o dinámica. Las características de estos modos son:

- Asignación manual: un administrador configura manualmente las direcciones IP de cada cliente en el servidor DHCP y cuando éste recibe una petición, comprueba la dirección MAC del cliente y le asigna la que configuró el administrador. Este mecanismo se suele utilizar cuando se quiere evitar la conexión de clientes no identificados.

- Asignación automática: el cliente que solicita una dirección obtiene una dirección aleatoria la primera vez que se comunica con el servidor DHCP. Esta dirección permanece asociada al cliente hasta que éste la libera. Este método es aconsejable cuando el número de cliente no varía demasiado.

- Asignación dinámica: el servidor DHCP asigna una dirección IP a un cliente de forma temporal. Cuando este tiempo expira, la IP es

revocada y el cliente ya no puede funcionar en la red hasta que no pida otra dirección. Este método facilita la instalación de nuevas máquinas clientes a la red.

5.2.2 *Relay Agents* DHCP

En el protocolo DHCP un cliente que desee obtener una dirección o parámetros de configuración debe establecer una comunicación con el servidor. En algunas redes, un cliente puede moverse libremente y puede darse el caso de que cliente y servidor DHCP no se encuentren en la misma subred y tengan problemas de comunicación ya que el cliente solamente podría comunicarse con servidores que estén en su misma subred.

Para solventar este problema surgen los *Relay Agents* (Agente de Relevo) DHCP. Un *Relay Agent* DHCP permite retransmitir mensajes DHCP enviados entre clientes y servidores DHCP. El *Relay Agent* actúa como el retransmisor que permite a los clientes DHCP obtener direcciones IP de un servidor DHCP que está en una subred remota.

5.3 Proceso de configuración en DHCPv6

Al igual que en DHCP para IPv4, DHCPv6 utiliza mensajes de Protocolo de datagramas de usuario (UDP). Los clientes DHCPv6 escuchan mensajes DHCP en el puerto 546 de UDP. Los agentes de retransmisión y los servidores DHCPv6 escuchan mensajes en el puerto 547 de UDP. La estructura de mensajes DHCPv6 es mucho más sencilla que la de DHCP para IPv4, que tuvo sus orígenes en el protocolo BOOTP para ofrecer compatibilidad con estaciones de trabajo sin disco.

Los servidores DHCP reciben mensajes de clientes utilizando un enlace reservado de direcciones *multicast*. Un cliente DHCP transmite la mayoría de los mensajes a esta dirección *multicast* reservada, por lo que el cliente no tiene

que ser configurado con la dirección o direcciones de servidores DHCP.

Un cliente puede utilizar su enlace de la dirección local y una conocida dirección *multicast* para descubrir y comunicarse con servidores DHCP o *Relay Agents*.

En los siguientes subapartados se repasan los mensajes del protocolo DHCPv6, algunas direcciones utilizadas durante el proceso de configuración y los intercambios de mensajes que se producen entre un cliente y servidor DHCP.

5.3.1 Tipos de mensajes

A continuación se lista el conjunto de mensajes utilizados en el protocolo DHCPv6 tal y como se indica en [Droms, 2003]. Entre paréntesis se muestra el código numérico de cada uno de ellos.

- SOLICIT (1): un cliente envía un mensaje para localizar servidores.

- ADVERTISE (2): un servidor envía un mensaje de notificación para indicar que está disponible como servicio DHCP, en respuesta a un mensaje SOLICIT recibido desde un cliente.

- REQUEST (3): un cliente envía un mensaje para pedir los parámetros de configuración, incluyendo dirección IP, a un determinado servidor.

- CONFIRM (4): un cliente envía un mensaje de confirmación a cualquier servidor disponible para comprobar si la dirección que le fue asignada es correcta para el enlace en el que el cliente está conectado.

- RENEW (5): un cliente envía un mensaje de renovación a un servidor que le proporcionó la dirección y los parámetros de configuración

para alargar su tiempo de vida o actualizar parámetros de configuración.

- REBIND (6): un cliente envía este mensaje después de no recibir respuesta de un mensaje RENEW para conseguir los mismos objetivos.

- REPLY (7): un servidor envía un mensaje de respuesta que contiene las direcciones asignadas y los parámetros de configuración en respuesta a un mensaje SOLICIT, REQUEST, RENEW o REBIND recibido de un cliente.

- RELEASE (8): un cliente envía un mensaje de liberación a un servidor que le proporcionó una dirección para indicar que ya no va a usar más esa dirección.

- DECLINE (9): un cliente envía un mensaje de disconformidad a un servidor que le proporcionó una dirección para comunicar que la dirección ya está en uso en la red a la que está conectado.

- RECONFIGURE (10): un servidor envía un mensaje a un cliente para informar que el servidor tiene nuevos parámetros de configuración y que el cliente puede solicitarlos.

- INFORMATION-REQUEST (11): un cliente envía un mensaje a un servidor para solicitar parámetros de configuración sin la asignación de dirección IP.

- RELAY-FORW (12): un *Relay Agent* envía un mensaje al servidor cuando recibe un mensaje de un cliente o de otro *Relay Agent* que desea comunicarse con el servidor.

- RELAY-REPL (13): un servidor envía un mensaje a un *Relay Agent* que está haciendo de puente entre él y un cliente.

5.3.2 Direcciones *multicast*

Tal y como se comentó en el Capítulo 3, las direcciones *multicast* son identificadores asignados a un conjunto de interfaces en múltiples *hosts*. Los paquetes que se envían a una de estas direcciones se hacen llegar a todos los interfaces que tienen asignada esta dirección. No hay direcciones de *broadcast* en IPv6, ya que su funcionalidad queda asumida por las direcciones *multicast*. Algunas direcciones de propósito específico son:

- *All_DHCP_Servers*: una dirección *multicast* (FF05::1:3) para comunicar con todos los servidores DHCP dentro de un mismo ámbito privado.

- *All_DHCP_Relay_Agents_and_Servers*: una dirección *multicast* (FF02:1:2) utilizada por un cliente para comunicarse con los vecinos (es decir, en enlace) *Relay Agent* y servidores. Todos los servidores y *Relay Agent* son miembros de este grupo *multicast*.

No existen direcciones de difusión definidas para IPv6. Por lo tanto, el uso de la dirección de difusión limitada para algunos mensajes DHCPv4 se ha reemplazado por el uso de la dirección *All_DHCP_Relay_Agents_and_Servers* de FF02::1:2 para DHCPv6. Por ejemplo, un cliente DHCPv6 que intenta descubrir la ubicación del servidor DHCPv6 en la red envía un mensaje de petición desde su dirección local de vínculos a FF02::1:2. Si existe un servidor DHCPv6 en la subred del *host*, recibe el mensaje de petición y envía una respuesta apropiada. Más comúnmente, un agente de retransmisión DHCPv6 en la subred del *host* recibe el mensaje de petición y lo reenvía a un servidor DHCPv6.

5.3.3 Flujo de mensajes

A continuación se detallará el intercambio de mensajes que ocurre entre un

cliente y servidor DHCP cuando el primero desea obtener una dirección. Para reducir la complejidad del protocolo, algunos mensajes dedicados a la confirmación de una dirección, a la renovación de una dirección o a la reconfiguración serán omitidos, prestando atención a los principales intercambios de mensajes que ocurren entre cliente y servidor. Por tanto, la implementación DHCP realizada en este trabajo se centrará solamente en los tipos de mensaje SOLICIT, ADVERTISE, REQUEST, REPLY, RELAY-FORW y RELAY-REPL.

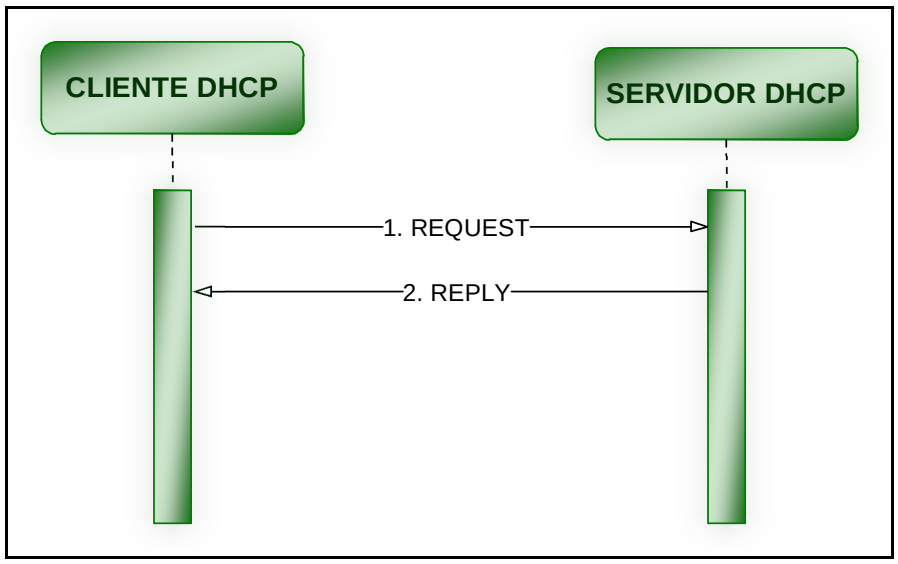

Fig. 5.1. Intercambio de mensajes DHCP para obtener información de configuración

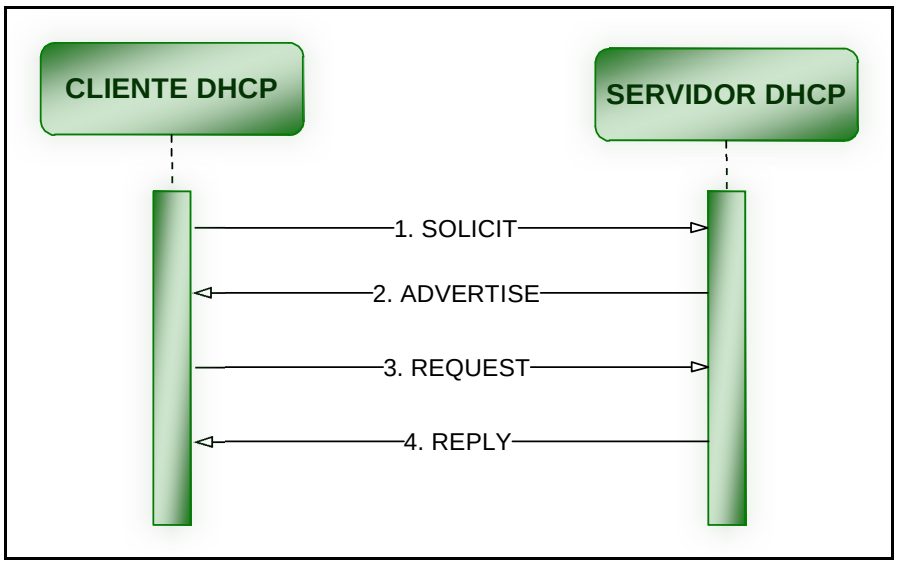

Fig. 5.2. Intercambio de mensajes DHCP para obtener una dirección

DHCPv6 puede ser aplicado con dos propósitos. En primer lugar, el servidor DHCP puede asignar direcciones IPv6 a los clientes. Un protocolo de cuatro mensajes es utilizado en este caso. Por otro lado, los clientes podrían demandar alguna otra información de configuración al servidor DHCP. Para esta situación, un protocolo de dos mensajes es iniciado por el cliente. Las figuras 5.1 y 5.2 muestran los intercambios de mensajes entre clientes y servidores en ambos casos.

Para solicitar la cesión de una o más direcciones IPv6, un cliente primero localiza un servidor DHCP y, a continuación, solicita la asignación de direcciones y otra información de configuración del servidor. El cliente envía un mensaje SOLICIT a la dirección *All_DHCP_Relay_Agents_and_Servers* para encontrar los servidores DHCP disponibles. Cualquier servidor que puede satisfacer las necesidades del cliente responde con un mensaje ADVERTISE. El cliente entonces elige uno de los servidores y envía un mensaje REQUEST al servidor pidiendo la asignación de direcciones y otra información de configuración. El servidor responde con un mensaje de respuesta REPLY que contiene la confirmación de direcciones y la configuración.

5.3.4 Retransmisión

Los clientes DHCP son los responsables de comenzar el intercambio de mensajes. Si un cliente DHCP no recibe la respuesta esperada de un servidor debe retransmitir su mensaje. En esta sección se describe la estrategia de retransmisión que los clientes DHCP usan.

El cliente DHCP comienza el intercambio de mensajes transmitiendo un mensaje al servidor. El intercambio de mensajes termina cuando el cliente recibe la apropiada respuesta desde el servidor o cuando el intercambio de mensajes se considera que ha fallado de acuerdo al mecanismo de retransmisión descrito más abajo.

Cada vez que el cliente envía o reenvía un mensaje SOLICIT calcula la variable RT (*Retransmission Timeout*). Si RT expira antes de que termine el intercambio de mensajes, el cliente recalcula RT y retransmite el mensaje.

Para el primer mensaje SOLICIT, RT se calcula como sigue:

$$RT = IRT + RAND * IRT \qquad \textit{(Ec. 5.1)}$$

donde IRT (*Initial Retransmission Time*) indica el tiempo inicial de retransmisión y RAND es un factor aleatorio escogido dentro de una distribución uniforme entre -0.1 y 0.1. Por defecto toma el valor de 1 segundo.

Los siguientes valores de RT dependerán del valor previo de RT tal y como se expresa a continuación:

$$RT = 2 * RTprevio + RAND * RTprevio \qquad \textit{(Ec. 5.2)}$$

Existe la variable MRT (*Maximum Retransmission Time*) que establece el límite superior al que puede llegar la variable RT. Por defecto toma el valor de 120 segundos. Si MRT toma el valor 0, la variable RT podrá crecer sin límite alguno. En otro caso, cuando RT alcance el valor de MRT, es decir, (MR > MRT) entonces se recalculará RT como sigue:

$$RT = MRT + RAND * MRT \qquad \textit{(Ec. 5.3)}$$

Por otro lado, la variable MRC (*Maximum Retransmission Count*) indica el número máximo de veces que un cliente puede retransmitir un mensaje antes de dar por fallida la configuración.

La variable MRD (*Maximum Retransmission Duration*) indica el máximo periodo de tiempo que un cliente puede tardar para la transmisión de un mensaje.

En caso de que MRC y MRD sean distintos de cero, el intercambio de mensajes fallará cuando cualquiera de sus valores sea superado. En caso de que MRC y MRD sean cero, el cliente DHCP continuará retransmitiendo el mensaje hasta encontrar una respuesta correcta.

6. DHCP EN UNA MANET

Con el esquema descrito en el Capítulo 5, el protocolo DHCP permite que los clientes y servidores intercambien mensajes utilizando direcciones *link-local*. Dada la naturaleza multisalto de una MANET, no es posible retransmitir este tipo de mensajes.

El capítulo se organiza de la siguiente manera. El apartado 6.1 repasa varias propuestas para la adaptación de DHCP a una red móvil ad hoc. En el apartado 6.2 se detalla el proceso seguido en este trabajo para la implementación de DHCPv6 en una MANET. Para finalizar, el apartado 6.3 propone una mejora al funcionamiento convencional de DHCPv6 que optimiza las prestaciones que ofrece en redes MANET.

6.1 Introducción

En el capítulo de introducción se describieron varias propuestas para la configuración de direcciones IP globales en una MANET. Algunas de ellas utilizaban una configuración de estado completo a través de servidores pero no seguían el estándar DHCP. Por este motivo, este trabajo se basa en la propuesta de [Singh, 2008].

[Singh, 2008] propone que debido a que los mensajes utilizados en el protocolo convencional de DHCP, con direcciones de tipo *link-local*, no pueden ser retransmitidos por los terminales de una red móvil ad hoc, los *Relay Agents* pueden colaborar en la retransmisión de los mensajes de los clientes DHCP a través de múltiples saltos.

Por tanto, [Singh, 2008] realiza una propuesta para la utilización de *Relay Agents* en una MANET. Específicamente, propone que los nodos de la MANET se configuren y actúen como *Relay Agents*. Los *Relay Agents* construyen

mensajes RELAY FORWARD cuando reciben mensajes de un cliente o mensajes RELAY FORWARD de otros *Relay Agents*. Para estos casos, el nuevo mensaje tendrá en el campo de opciones el mensaje original e incluirá una nueva cabecera que contendrá la información necesaria para llegar al siguiente salto de la red MANET. De esta forma, conforme el mensaje va circulando por la red se incluye todo el camino seguido. Al final, cuando el mensaje es recibido por un servidor DHCP éste construye un mensaje RELAY REPLY de acuerdo al mensaje recibido en el que el camino al cliente está definido explícitamente. El proceso se puede observar en la Figura 6.1.

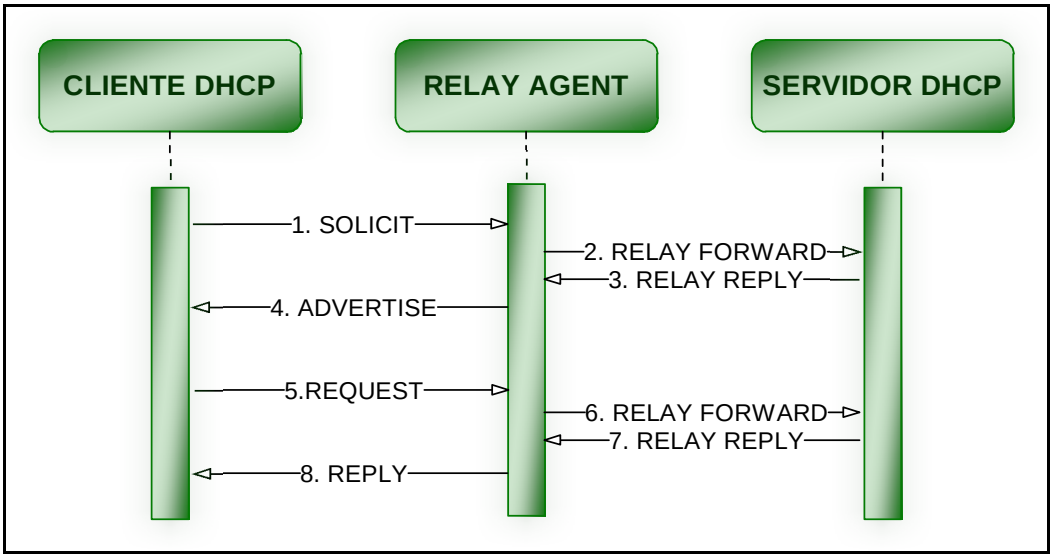

Fig. 6.1. Intercambio de mensajes DHCP para obtener una dirección con Relay Agents

6.2 Implementación

El mecanismo implementado ha sido el comentado en el apartado anterior, que utiliza el intercambio de mensajes SOLICIT, ADVERTISE, REQUEST, REPLY, RELAY-FORW y RELAY-REPL, entre clientes y servidores DHCP. Este mecanismo permitía la comunicación entre clientes y servidores con múltiples saltos, haciendo que los nodos intermedios actuarán como *Relay Agents*.

Todos los mensajes DHCP enviados entre clientes y servidores comparten un formato de cabecera idéntico y un área con un formato variable para las

opciones. Las opciones son concatenadas sin ningún tipo de separación, siguiendo una alineación en bytes. La Figura 6.2 ilustra el formato de los mensajes DHCP entre clientes y servidores.

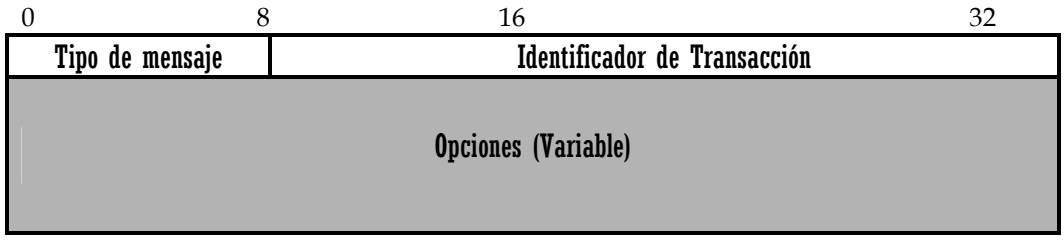

Fig. 6.2. Formato de los mensajes DHCP

El campo "Tipo de mensaje" identifica el tipo de mensaje DHCP. Los tipos posibles para este trabajo son:

- SOLICIT (1)
- ADVERTISE (2)
- REQUEST (3)
- REPLY (7)
- RELAY-FORW (12)
- RELAY-REPL (13)

El campo "Identificador de transacción" contiene un valor único que se utiliza para distinguir unívocamente un intercambio de mensajes.

En el campo "Opciones" se incluyen los identificadores de clientes y servidores y los valores de configuración que son intercambiados (dirección IPv6 global para el acceso a Internet).

Para la cesión de una dirección IPv6, el nodo de la MANET primero necesita localizar un servidor DCHP. Para ello se ha utilizado una implementación

[Hamidian, 2003] del protocolo de Conectividad Global para el descubrimiento de *gateways*. El *gateway* será el dispositivo que permita la comunicación con el servidor DHCP o, dicho de otra manera, actuará como último *Relay Agent* en el proceso de configuración.

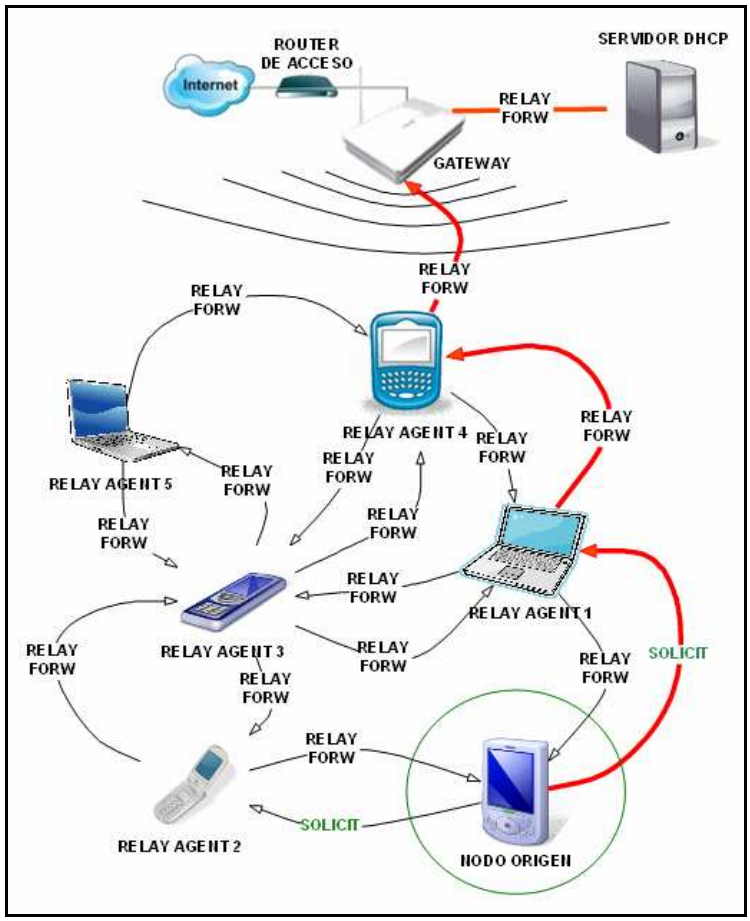

Fig. 6.3. Envío del mensaje SOLICIT desde el cliente DHCP

El intercambio de mensajes se inicia por el cliente enviando un mensaje SOLICIT a la dirección *multicast All_DHCP_Relay_Agents_and_Servers*. En una MANET este mensaje será recibido por todos los nodos que estén en el alcance del nodo origen. Los nodos que reciben el mensaje actuarán como *Relay Agents* retransmitiendo un mensaje *multicast* RELAY-FORW (como se puede ver en la Figura 6.3). A su vez, los nodos que reciben los mensajes RELAY-FORW vuelven a retransmitirlo hasta que sea recibido por el *gateway*, que actuando también como *Relay Agent*, retransmitirá la solicitud al servidor DHCP. El campo "Identificador de Transacción" se utiliza en este paso de la configuración

para evitar el múltiple procesamiento del mismo mensaje, es decir, cuando un nodo recibe un mensaje comprueba el valor de este campo y, si ya ha sido procesado, lo descarta. En la Figura 6.3 se puede observar la inundación de mensajes que se produce en la red cuando solo hubieran sido necesarios los envíos pintados en rojo.

Cuando el servidor recibe el mensaje SOLICIT (en forma de RELAY-FORW), lee del campo opciones la dirección del nodo origen que solicita la dirección y responde con un mensaje *unicast* ADVERTISE. Este mensaje, antes de llegar al destino, deberá pasar por cada uno de los *Relay Agents* que retransmitieron la solicitud (como se indica en la figura 6.4). De esta forma es encapsulado en mensajes RELAY-REPL hasta llegar al destino.

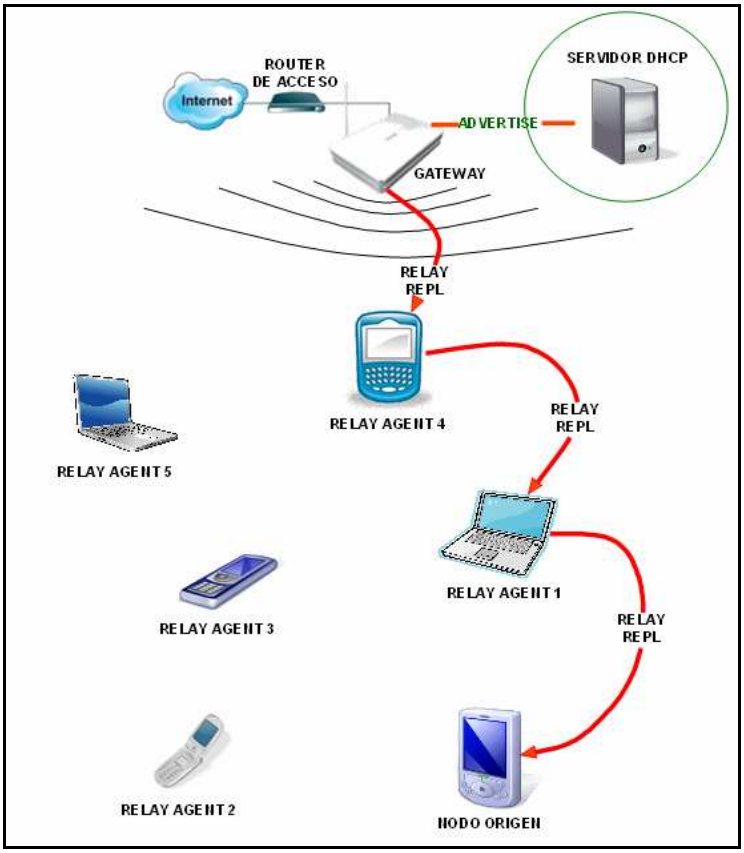

Fig. 6.4. Envío del mensaje ADVERTISE desde el servidor DHCP

El cliente entonces envía un mensaje *unicast* REQUEST al servidor pidiendo la asignación de direcciones y otra información de configuración. Este mensaje

volverá a ser retransmitido a través de mensajes RELAL-FORW por los *Relay Agents* tal y como sucedió con el mensaje SOLICIT pero, en este caso, no se utilizarán direcciones *multicast*, sino que cada *Relay Agent* conoce el camino a seguir y lo envía solamente al siguiente *Relay Agent*..

El servidor responde con un mensaje *unicast* de respuesta REPLY que contiene la confirmación de direcciones y la configuración. Este mensaje volverá a ser retransmitido a través de mensajes RELAL-REPL por los *Relay Agents* tal y como sucedió con el mensaje ADVERTISE, hasta que llega al nodo origen.

6.3 Mejora introducida

La configuración de todos los nodos de la MANET como *Relay Agent* conlleva una sobrecarga de mensajes en el proceso DHCP ya que todos los nodos retransmitirán los mensajes DHCP SOLICIT generados por el cliente (véase Figura 6.3).

Para evitarlo [Singh, 2008] propone una optimización que consiste en que un nodo cuando recibe un mensaje REQUEST de otro nodo (considerando un protocolo simplificado de 2 mensajes REQUEST-REPLY), tendrá una cierta probabilidad de actuar como Relay Agent para él y por tanto de retransmitir el mensaje. Esta probabilidad, llamada *Rp* se calcula dinámicamente cada vez que un nodo recibe un mensaje REPLY o retransmite un mensaje REQUEST. Su valor es igual al cociente entre el número de mensajes REPLY dividido por el número de mensajes REQUEST (Ec. 6.1). Cuanto mayor sea este valor, mayor probabilidad de que un nodo actúe como Relay Agent.

$$Rp = Mensajes\_REPLY\_recibidos / Mensajes\_REQUEST\_recibidos \qquad (Ec.\ 6.1)$$

[Singh, 2008] propone optimizar el proceso mediante la asignación de una probabilidad de retransmisión de los *Relay Agent*. En primer lugar, solamente los nodos que ya hayan sido configurados podrán actuar como *Relay Agents*.

Según la métrica propuesta, aquellos nodos que hayan actuado como *Relay Agent* anteriormente, tendrán más probabilidad de actuar de nuevo como tales en el siguiente proceso DHCP. Desde otro punto de vista, aquellos *Relay Agents* que no actúen como tales en el primer intento del nodo por configurar una dirección IP, decrementarán su probabilidad de servir como *Relay Agent* en los sucesivos intentos. Este comportamiento podría ocasionar que algunos nodos necesitasen muchos intentos antes de configurar una dirección IP. Con el propósito de reducir este inconveniente, en este trabajo se propone una mejora que también reduce significativamente el número de mensajes. A continuación se detalla el mecanismo implementado.

DHCPv6, como se indicó en el apartado 5.3.4, dispone de un parámetro llamado MRC (*Maximum Retransmission Count*) que establece el número máximo de veces que un nodo puede retransmitir un mensaje SOLICIT para lograr su configuración DHCP. Si su valor es igual a cero se indica que no tiene límite. La optimización consiste en la utilización de este parámetro para conseguir una reducción en el número de mensajes retransmitidos. Para ello, cada nodo que reciba un mensaje SOLICIT de otro nodo, aumentará en su memoria interna el número de intentos que lleva realizados éste último y calculará una probabilidad *P*, que será igual al número de intentos del nodo entre el valor MRC (Ec. 6.2). A mayor valor de *P* mayor probabilidad de que el nodo trabaje como *Relay Agent*. Con este mecanismo cuando un nodo envía el primer mensaje SOLICIT, serán muy pocos nodos los que trabajen como *Relay Agent* y, por tanto, retransmitan su solicitud, pero quizás suficientes para que el intercambio de mensajes entre cliente y servidor DHCP tenga éxito. A medida que un nodo realice más intentos de configuración contará con más nodos aliados.

$$P = Número\_intentos\_configuración / MRC \qquad \text{(Ec. 6.2)}$$

Además, como en [Singh, 2008], solamente los nodos que previamente hayan sido configurados con una dirección IP global podrán actuar como *Relay Agents*.

Estos nodos ya conocen el camino a seguir para comunicarse con el servidor DHCP y por tanto no necesitan enviar mensajes *multicast* a todos sus vecinos sino que enviarán un mensaje *unicast* al servidor DHCP. De esta forma también se reduce considerablemente el número de paquetes que circulan por la MANET.

7. SIMULACIONES Y RESULTADOS

Las tareas de investigación se han centrado en el acceso a Internet para una MANET. Para que un nodo de una MANET consiga la conexión con Internet necesita una dirección IP global. Para tal efecto, se ha implementado y adaptado DHCPv6 sobre MANET, que consiste en un protocolo de autoconfiguración de direcciones IP de estado completo.

Para la implementación y ejecución de las simulaciones que se han llevado a cabo en este proyecto, se ha utilizado la herramienta de simulación NS-2 [NS-2, 2008]. El simulador de redes NS-2 es uno de los simuladores de mayor difusión dentro del sector de las telecomunicaciones. En la actualidad, existen otros muchos simuladores de redes como OPNET (*Optimized Network Engineering Tools*), OMNET ++, Network Simulator, Glomosim, NCTUns, etc. No obstante, el NS-2 se ha convertido en un estándar debido a su amplia utilización, permitiendo a la hora de realizar un estudio poder comparar los resultados obtenidos con otros trabajos anteriores.

El trabajo parte de varias premisas:

- *Protocolo de encaminamiento*. Como se ha ido comentando a lo largo del texto, las redes móviles ad hoc necesitan utilizar un tipo especial de protocolo de encaminamiento que permita transmitir los paquetes en varios saltos. El simulador NS-2 dispone de varios protocolos de encaminamiento para redes ad hoc. En concreto, para las simulaciones, se ha utilizado AODV, descrito en capítulos anteriores.

- *Descubrimiento de gateways*. Para establecer esta interconexión entre las dos redes (MANET e Internet) es necesaria la ayuda de uno o varios *gateways*. Un *gateway* es el dispositivo que entiende los protocolos de ambas redes, proporciona las funcionalidades de encaminamiento ad hoc

y, a su vez, mantiene la comunicación necesaria con el *router* de acceso. Respecto a la configuración de los nodos, el *gateway* anuncia el tipo de mecanismo que los nodos de la MANET deben seguir para obtener una dirección IP. Para la integración de la MANET con Internet, en este proyecto se ha utilizado el mecanismo de Conectividad Global. En [Wakikawa, 2006] se describe como proveer acceso a Internet a redes ad hoc y explica el protocolo de Conectividad Global para el descubrimiento de *gateways*. Posteriormente [Hamidian, 2003] implementa sobre el simulador NS-2 este mecanismo. El trabajo realizado parte de esta mejora.

Una vez que se disponía de la posibilidad de encontrar *gateways*, el trabajo se centró en 2 tareas principales (descritas en el Capítulo 6):

- Implementación de DHCPv6 para la asignación de direcciones IPv6 globales a los nodos de una MANET.

- Implementación de un mecanismo que mejore el rendimiento de DHCPv6 en una MANET.

Para realizar estas dos tareas ha sido necesario en primer lugar entender la estructura del simulador. Posteriormente, se ha modificado el núcleo de NS-2 para añadir las funcionalidades de DHCP en MANET. Con estos cambios, es posible simular este protocolo en el NS-2. Sin embargo, para extraer parámetros cuantitativos sobre el comportamiento de la red hay que programar un *script* que calcule a partir de un fichero de trazas las prestaciones de la red. La inclusión de nuevas trazas en el simulador junto con la programación del *script* también ha sido parte del trabajo de este proyecto.

El resto del capítulo se estructura en los siguientes apartados. En el apartado 7.1, se indica el escenario de simulación utilizado. En el apartado 7.2 se exponen los resultados obtenidos de las simulaciones.

7.1 Escenario de simulación

La tabla 7.1 resume los parámetros principales utilizados durante las simulaciones. Las simulaciones han sido realizadas con el simulador NS-2 en redes de 25, 50, 75 y 100 nodos. Para cada número de nodos se han efectuado simulaciones en redes cuyo tamaño varía entre 100m x 100m y 1000m x 1000m. Se han seleccionado estos parámetros para comparar las prestaciones de la mejora propuesta con respecto a la implementación de [Singh, 2008]. Para cada combinación de número de nodos y tamaño de red se han lanzado 5 simulaciones obteniendo los resultados medios de todas ellas. En cada simulación se han configurado todos los nodos de la red con una dirección IP que deben obtener a través de un servidor DHCP. Se ha dejado un tiempo de 50 segundos antes de comenzar cualquier configuración para estabilizar la red. Pasado este tiempo los nodos comenzaban su configuración de forma aleatoria entre los segundos 50 y 150 de la simulación.

Parámetro	Valor
Área de simulación	De 100m x 100m hasta 1000m x 1000m
Número de nodos móviles	25, 50, 75 o 100
Número de terminales fijos	2
Número de *routers* de acceso	1
Patrón de movilidad	*Random Waypoint (setdest).* $V_{min} = 1$ *m/s.* $V_{max} = 2$ *m/s*
Tiempo de simulación	Hasta conseguir la configuración de todos los nodos
Protocolo de encaminamiento	AODV (con la mejora para conectividad global [Hamidian, 2003])
Mecanismo de descubrimiento de *gateways*	Reactivo
Cobertura de nodo	250 metros
MRC (*Maximum Retransmission Count*)	10

Tabla. 7.1. Parámetros de las simulaciones

En cada simulación el *gateway* se ha situado en el centro del escenario rodeado por todos los nodos móviles. En nuestro trabajo se trata del último *Relay Agent* que permite a los nodos comunicarse con el servidor DHCP. Para omitir los efectos de la red cableada, el *gateway* hará las funciones de servidor

DHCP.

El área de alcance radio de cada nodo queda fijado al valor por defecto de 250 metros. El parámetro MRC, utilizado en la mejora propuesta en este trabajo, se ha establecido a 10.

El movimiento que se les imprimirá a los nodos móviles está determinado por el modelo comúnmente empleado en este tipo de experimentos: *Random WayPoint*. La pauta de movimiento se describe de la siguiente manera. Cada nodo inicialmente seleccionará un punto aleatorio dentro del área de simulación y se dirigirá a él en línea recta. En el momento en que lo alcance, se detendrá durante un tiempo equivalente al tiempo de pausa y de nuevo se seleccionará de forma aleatoria un nuevo destino y así sucesivamente, hasta finalizar el período de simulación. Los movimientos de los nodos son independientes entre sí. Por otro lado, la velocidad que se le imprimirá a los nodos estará limitada por unos márgenes con cota mínima de 1 m/s, y cota máxima de 2 m/s. Se ha seleccionado una velocidad mínima no nula tal y como se recomienda en [Yoon, 2003].

7.2 Prestaciones de la Red

Para evaluar las prestaciones del protocolo propuesto, se han medido los siguientes parámetros:

- *Número de mensajes DHCP*. Como se ha comentado en capítulos anteriores, una configuración DHCP para obtener una dirección IP supone un intercambio de mensajes de tipo SOLICIT, ADVERTISE, REQUEST, REPLY, RELAY-FORW y RELAY-REPL. Este parámetro indica la cantidad de mensajes DHCP que se utilizan desde que un nodo comienza su configuración hasta que consigue su dirección IP global. Es el mejor indicador para comprobar una posible saturación de mensajes en la red. Cuánto menor sea su valor mayores serán las

prestaciones de la red.

- *Tiempo de configuración*. Tiempo consumido durante todo el proceso de configuración desde que un terminal solicita una dirección IP global al servidor DHCP hasta que la consigue. Es deseable que la configuración se realice rápidamente por lo que cuánto menor sea su valor mayores serán las prestaciones de la red.

7.3 Resultados

Para cada número de nodos se ha realizado una comparativa entre el funcionamiento convencional del protocolo DHCPv6 donde todos los nodos de la MANET actúan como *Relay Agent*, la mejora introducida en [Singh, 2008] denominada Singh-Bhatia y la mejora propuesta en este trabajo, conocida como DHCP basado en el Número de Intentos de Configuración (DHCP NIC).

La Figura 7.1 presenta gráficamente la media de mensajes consumidos por un nodo durante su configuración. Se presentan 4 gráficas correspondientes a las simulaciones con redes de 25, 50, 75 y 100 nodos. El eje de abscisas representa la dimensión de la red en metros y el eje de ordenadas la media de mensajes.

Como era de esperar, La inundación de mensajes que produce el envío del mensaje SOLICIT al comienzo de las configuraciones de los nodos (véase Figura 6.3), hace que el número de mensajes en el modelo convencional de DHCP sea elevado. Sin embargo las mejoras introducidas reducen significativamente el número de mensajes.

La mejora propuesta en este trabajo obtiene mejores resultados que la mejora de Singh-Bathia en redes de pequeñas dimensiones. Esto es debido a que en estas redes los nodos, dada su cercanía, tienen muchos aspirantes a ser *Relay Agent*, y por tanto, en un primer intento, consigan la configuración. En estas

circunstancias, Singh-Bathia puede colapsar ciertos nodos, mientras que DHCP NIC reparte más equitativamente el trabajo.

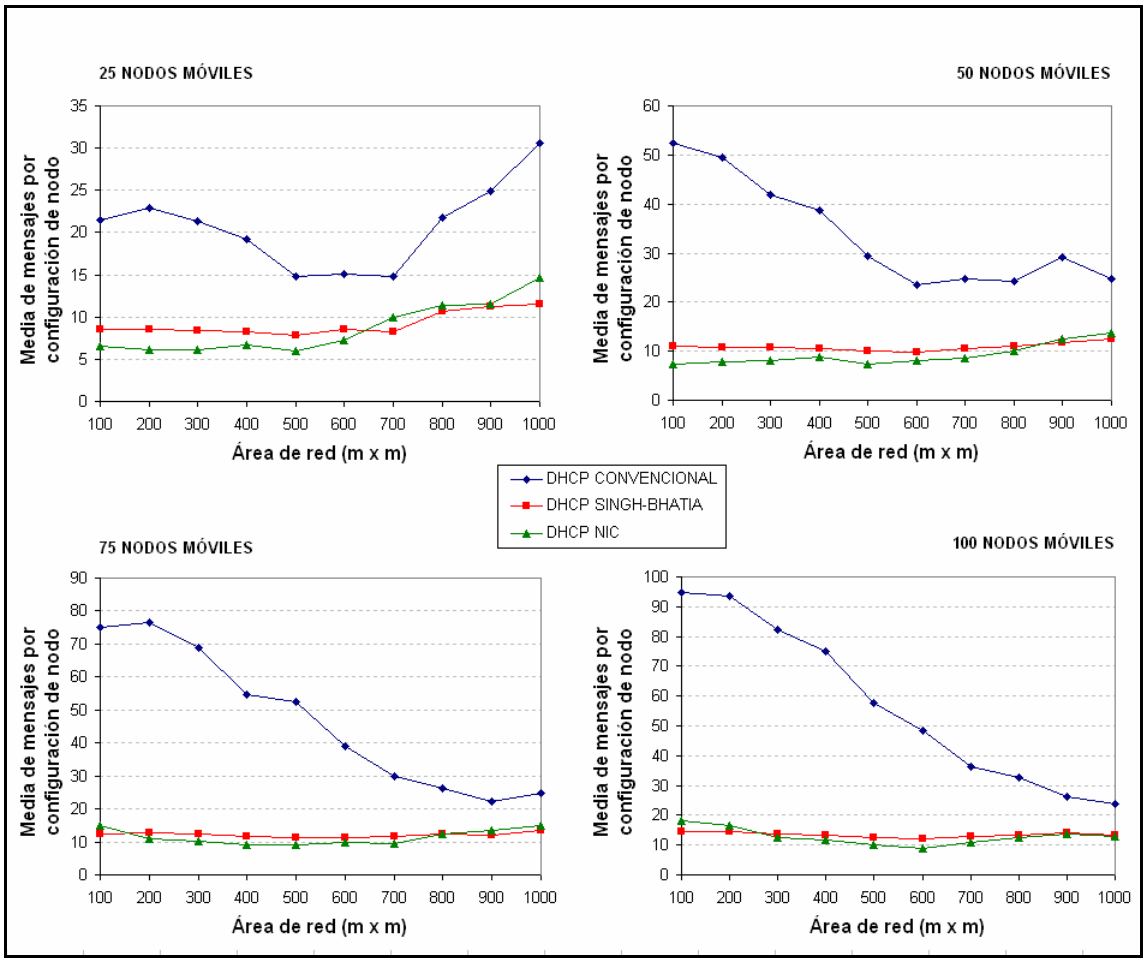

Fig. 7.1. Media de mensajes por configuración de nodo

La Figura 7.2 presenta gráficamente el tiempo medio consumido por un nodo durante su configuración. Se presentan 4 gráficas correspondientes a las simulaciones con redes de 25, 50, 75 y 100 nodos. El eje de abscisas representa la dimensión de la red en metros y el eje de ordenadas la media de tiempo.

La tendencia de los tres funcionamientos de DHCP es parecida. Cada caso tiene su propia explicación como se comenta a continuación.

DHCP en modo convencional reduce el tiempo de configuración en un primer momento debido a que se reduce la sobrecarga de mensajes que existe

en redes de pequeña dimensión y con muchos nodos (lo que puede provocar la pérdida de muchos mensajes y el fracaso de una configuración). A medida que disminuye la densidad de nodos, desaparece la sobrecarga en la red pero, sin embargo, se necesitan más intentos para lograr el objetivo, lo que aumenta el tiempo de configuración.

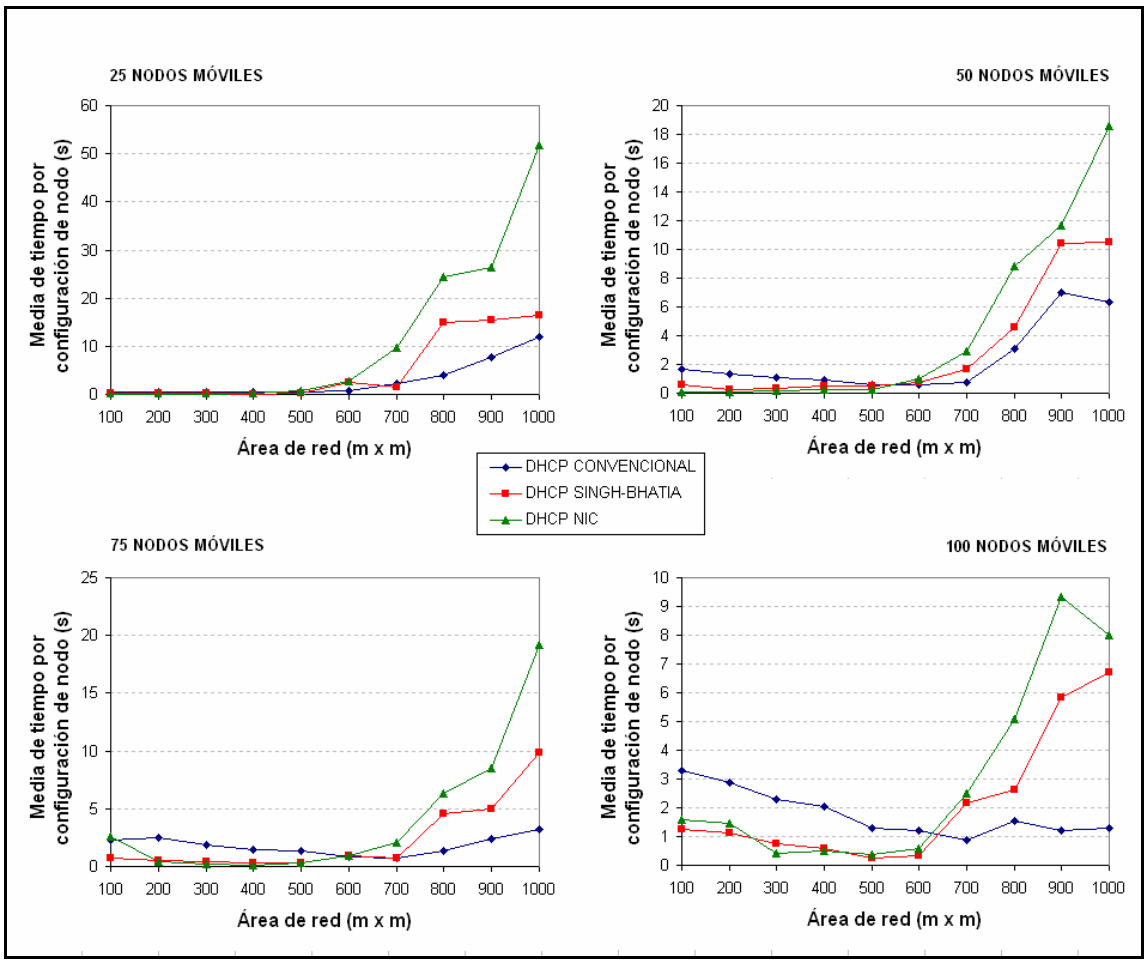

Fig. 7.2. Media de tiempo por configuración de nodo

Los modos de funcionamiento de Singh-Bathia y el de este trabajo también siguen una tendencia alcista en cuanto al tiempo medio de configuración de los nodos, conforme aumenta la dimensión de la red, aumenta también el tiempo. En estos casos, es debido a la reducción de posibilidades que se aplican sobre los nodos para que actúen como *Relay Agents*. En redes de pequeña dimensión el funcionamiento es ideal porque se evita la sobrecarga en la red, sin embargo, en redes mayores, las oportunidades se reducen y, más aún, al aplicar un

método probabilístico. Al final, los mecanismos necesitan más intentos de configuración con el consiguiente aumento del tiempo.

8. CONCLUSIONES

El objetivo de la presente investigación era proveer de conexión a Internet a los nodos de una red móvil ad hoc. Se han comentado las características especiales de este tipo de redes, que provocan que los protocolos de las redes convencionales no se puedan aplicar directamente.

En este trabajo se ha adaptado e implementado el protocolo DHCPv6 en una MANET para permitir que los nodos puedan configurar una dirección IP global y tengan, de esta forma, opción para comunicarse con otros nodos de Internet.

Sin la necesidad de añadir nuevos mensajes al estándar DHCPv6, se ha conseguido que una red ad hoc multisalto configure todos sus terminales. Esto permite que las MANET puedan integrarse con otras redes, incluso con redes convencionales con infraestructura. La adaptación consiste en configurar los nodos de la red como *Relay Agent*, que no son más que nodos que retransmiten los mensajes DHCP entre el cliente y el servidor. Al operar todos los nodos como retransmisores, se ha comprobado que el funcionamiento convencional de DHCPv6 en una MANET produce una excesiva sobrecarga de mensajes en la red. Este hecho provoca la congestión de los enlaces junto con la pérdida de mensajes de configuración DHCP y, por lo tanto, que muchos intentos terminen en fracaso.

Para reducir este inconveniente, en este trabajo se ha propuesto una optimización de la adaptación del protocolo DHCPv6 en MANET reduciéndose la sobrecarga de mensajes generados durante el proceso. La mejora introducida, basado en un sistema probabilístico, obtiene resultados positivos para redes de alta densidad de nodos. Para ello, el parámetro MRC (*Maximum Retransmission Count*) del protocolo DHCP juega un papel muy importante. Este parámetro controla el número máximo de veces que un terminal puede intentar su configuración de direcciones. Los nodos de la red conocen el valor de MRC y en

función de las solicitudes que han recibido del nodo origen también conocen los intentos que lleva realizados dicho nodo. En función de estas dos variables, la mejora propuesta aumenta la probabilidad de que un nodo actúe como *Relay Agent* de forma proporcional al número de intentos que se llevan realizados.

8.1 Trabajo futuro

El valor del parámetro MRC, que controla el número de intentos de configuración de los nodos, puede afectar en las prestaciones que ofrece el mecanismo propuesto. Cuanto mayor sea el valor de esta variable, la probabilidad de que un nodo actúe como *Relay Agent* será menor en los primeros intentos de configuración de un nodo y el número de mensajes que circulan por la red se podría reducir. Sin embargo, un valor muy alto de MRC podría implicar demasiado retardo en la configuración o incluso que ésta no se produjese. Como se comentó en el capítulo de resultados, MRC se ha establecido a 10 en todas las simulaciones. Es previsible que este parámetro dependa en gran medida de los parámetros de la red como número de nodos, densidad de la red, tráfico, etc. Como futura línea de investigación se podría analizar el valor apropiado de este parámetro en distintas configuraciones de red.

Una vez realizadas las pruebas en entornos simulados, habría que acometer su implementación para dispositivos móviles actuales y comprobar su funcionamiento en un escenario real.

El trabajo se ha centrado en el protocolo DHCPv6 por ser uno de los mecanismos de configuración de direcciones en MANET más estudiado en la actualidad. Prueba de ello son los esfuerzos que está realizando uno de los principales grupos de trabajo del IETF. Sin embargo, como se comentó en el primer capítulo existen otros protocolos, con buenos resultados en redes convencionales, y que podrían ser adaptados para una red móvil ad hoc.

REFERENCIAS

[Abramson, 1970] N. Abramson, The ALOHA system-another alternative for computer communications, in: Proc. of the Fall 1970 AFIPS Computer Conference, 1970, pp. 281-285.

[Bellur, 2003] B. Bellur, R.G. Ogier, F.L Templin, "Topology broadcast based on reverse-path forwarding routing protocol (tbrpf)", Internet Draft, draft-ietf-manet-tbrpf-06.txt, (trabajo en progreso), 2003.

[Bernardos, 2008] Carlos J. Bernardos and Maria Calderon, "Survey of IP address Autoconfiguration mechanisms for MANETs", draft-bernardos-manet-autoconf-survey-03, Internet Engineering Task Force, 2008.

[Cha, 2003] Cha, H., Park, J., and H. Kim, "Extended Support for Global Connectivity for IPv6 Mobile Ad Hoc Networks", draft-cha-manet-extended-support-globalv6-00 (trabajo en progreso), Octubre 2003.

[Chakeres, 2005] I. Chakeres, E. Belding, y C. Perkins, "Dynamic MANET On-demand (DYMO) Routing", IETF Internet Draft (trabajo en progreso), Octubre, 2005.

[Chen, 1998] T.-W. Chen, M. Gerla, "Global state routing: a new routing scheme for ad-hoc wireless networks", IEEE ICC, 1998.

[Clausen, 2003] T. Clausen y P. Jacques, "Optimized Link State Routing Protocol (OLSR)", IETF RFC 3626, Octubre, 2003.

[Clausen, 2005] Clausen, T. and E. Baccelli, "Simple MANET Address Autoconfiguration", draft-clausen-manet-address-autoconf-00 (trabajo en progreso), Febrero2005.

[Corson, 1995] M.S. Corson, A. Ephremides, "A distributed routing algorithm for mobile wireless networks", ACM/Baltzer Wireless Networks 1 (1) (1995) 61–81.

[DHC WG, 2008] Dynamic Host Configuration Work Group (DHC WG), http://www.ietf.org/html.charters/dhc-charter.html.

[Dressler, 2006] Falko Dressler, "Self-Organization in Ad Hoc Networks: Overview and Classification, Autonomic Networking Group, University of Erlangen, Febrero 2006.

[Droms, 1993] R. Droms, "Dynamic Host Configuration Protocol", RFC 1531, Octubre 1993.

[Droms, 1997] R. Droms, "Dynamic Host Configuration Protocol", RFC 2131, Marzo 1997.

[Droms, 2003] R. Droms (ed.), J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, Julio 2003.

[Feeney, 2001] L. M. Feeney, "An Energy Consumption Model for Performance Análisis of Routing Protocols for Mobile Ad Hoc Networks", Journal of Mobile Networks and Application, Kluwer Academia Publisher, 2001.

[Freebersyser, 2001] James A. Freebersyser, Barry Leiner, "A DoD perspectiva on mobile ad hoc networks", Addison Wesley, Reading, MA, pp. 29-51, 2001.

[García, 2006] L. J. García Villalba, R. Puttini, M. Hanashiro, F. Miziara, R. Sousa, C. Barenco, "On the Anomaly Intrusion-Detection in Mobile Ad Hoc Network Environments", Lecture Notes in Computer Science, Springer-Verlag, LNCS 4217, pp. 182-193, 2006.

[Haas, 1997] Haas, J., "A new routing protocol for the reconfigurable wireless networks", Proc. of IEEE 6th International Conference on Universal Personal Communications 97, pp. 562-566, 1997.

[Hamidian, 2003] Alex Ali Hamidian, "A Study of Internet Connectivity for Mobile Ad Hoc Networks in NS 2", Universidad de Lund, 2003.

[IEEE, 2003] IEEE 802.11-1999, "IEEE Standard for Local and Metropolitan Area Networks – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Standard Association, The Working Group for Wireless LAN. Edición de 1999, ratificada en Junio 2003.

[IETF, 2008] Internet Engineering Task Force (IETF), http://www.ietf.org/.

[Jain, 2003] Sushant Jain, "Energy Aware Communication in Ad – Hoc Networks", Technical Report, University of Washington, Seattle, Junio 2003.

[Jayakumar, 2007] Geetha Jayakumar, G. Gopinath, "Ad Hoc Mobile Wireless Networks Routing Protocols – A Review", Bharathidasan University, Journal of Computer Science 3, 2007.

[Johnson, 2007] D. Johnson, Y. Hu y D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", IETF RFC 4728, Febrero, 2007.

[Ko, 1998] Y.-B. Ko, N.H. Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks", Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom_98), Dallas, TX, 1998.

[Kuo, 1995] Kuo, Franklin F (1995). "The ALOHA system". ACM Computer Communication Review 25, 1995.

[Murthy, 1995] S. Murthy J.J. Garcia-Luna-Aceves, "A routing protocol for packet radio networks", First Annual ACM International Conference on Mobile Computing and Networking, Berkeley, CA, 1995, pp. 86–95.

[Narten, 1998] T. Narten, E. Nordmark y W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", IETF RFC 2461, Diciembre, 1998.

[NS-2, 2008] The Network Simulator ns2, http://www.isi.edu/nsnam/ns.

[Park, 1997] Vincent D. Park, M. Scott Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks", IEEE Conference on Computer Communications, INFOCOM'97, Abril 1997.

[Perkins, 1994] C. Perkins, P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", en Actas del ACM SIGCOMM'94 Conference on Communications Arquitectures, Protocols and Applications, Londres (Reino Unido), Agosto 1994.

[Perkins, 2003] C. Perkins E. Belding-Royer, Das, S.,"Ad hoc On-Demand Distance Vector (AODV) Routing", IETF RFC 3561, Julio 2003.

[Raju, 1999] J. Raju, J. Garcia-Luna-Aceves, "A new approach to ondemand loop-free multipath routing", 8th Annual IEEE International Conference on Computer Communications and Networks (ICCCN), Boston, MA, Octubre 1999, pp. 522–527.

[Ruffino, 2006] Ruffino, S. and P. Stupar, "Automatic configuration of IPv6 addresses for MANET with multiple gateways (AMG)", draft-ruffino-manet-autoconf-multigw-03 (trabajo en progreso), Junio 2006.

[Singh, 2008] Shubhranshu Singh, Ashutosh Bhatia, "A DHCPv6 Based IPv6 AutoConfiguration Mechanism for Subordinate MANET", Aceptado en IEEE Asia-Pacific Service Computing Conference 2008.

[Templin, 2008] Templin, F., Russert, S., and S. Yi, "MANET Autoconfiguration using Virtual Enterprise Traversal (VET)", draft-templin-autoconf-dhcp-16 (trabajo en progreso), Agosto 2008.

[Triviño, 2007] A. Triviño, B. Ruiz y E. Casilari, "Adaptive Gateway Discovery in Hybrid MANETs", en Actas del VII International Workshop on Applications and Services in Wireless Networks ASWN'2007, Santander (España), 2007.

[Wakikawa, 2006] Wakikawa, R., "Global connectivity for IPv6 Mobile Ad Hoc Networks", draft-wakikawa-manet-globalv6-05 (trabajo en progreso), Marzo 2006.

[Yoon, 2003] J. Yoon, M. Liu, B. Noble, “Random waypoint considered harmful”, Proceedings of the IEEE Twenty-Second Annual JointConference of the IEEE Computer and Communications Societies (INFOCOM 2003), vol. 2, pp. 1312- 1321, 2003.