Evaluación de Criterios de Selección de Pasarelas en Redes MANET Híbridas

Alicia Triviño Cabrera, Gonzalo Casado Hernández, Eduardo Casilari Pérez, Francisco J. González Cañete
Dpto. Tecnología Electrónica, Universidad de Málaga
Campus de Teatinos, 29071 Málaga
Telf: 952 137191, Fax: 952131447
E-mail: atc@uma.es

Resumen

La gestión de una dirección IPv6 global y, más genéricamente, las conexiones de un nodo de una red ad hoc o MANET con Internet se ha de efectuar a través de las llamadas pasarelas o gateways. En entornos de redes móviles ad hoc con múltiples pasarelas que anuncian distintos prefijos de red, cada vez que un terminal de la red decide utilizar un gateway diferente al empleado hasta ese momento, dicho terminal debe configurar su correspondiente dirección IP para así ser capaz de retransmitir y recibir posteriormente tráfico desde el gateway seleccionado. Sin embargo, este proceso de configuración de dirección IP no es inmediato ya que generalmente en las redes ad hoc no existe una infraestructura dedicada a la gestión de las direcciones IP. Así pues, la generación de una dirección IP adecuada junto con la verificación de la unicidad de la misma constituyen las principales tareas que el nodo debe realizar al conmutar de gateway. Siguiendo esta estrategia (stateless autoconfiguration), la conmutación de gateways provoca una interrupción de las comunicaciones que generalmente repercute en un deterioro de las prestaciones que la red puede ofrecer. A su vez, el número de interrupciones depende del criterio empleado para la selección de las pasarelas. En esta ponencia, se analizará cómo influye el criterio de selección de la pasarela en el comportamiento de la MANET a través de la medida cuantitativa del porcentaje de paquetes perdidos, el retardo y la sobrecarga introducida en la red. En general, se observa que el criterio de la distancia al gateway en términos del número de saltos proporciona unas mejores prestaciones tanto en el mecanismo de integración de conectividad global como en el de continuidad de prefijo.

1. Introducción

En la actualidad existe una gran demanda de dispositivos móviles que permitan a los usuarios estar conectados en cualquier lugar y en cualquier momento. Así pues, cada vez es más habitual la utilización de puntos de acceso inalámbricos en conferencias, aeropuertos, etc. Sin embargo, en algunas ocasiones es necesario desplegar una gran cantidad de puntos de acceso para proporcionar cobertura en áreas extensas. Bajo estas circunstancias, las redes móviles ad hoc o MANET (*Mobile Ad Hoc NETwork*) constituyen una solución ideal como ampliación del área de cobertura de puntos de acceso inalámbricos.

El empleo clásico de las redes ad hoc se centra en dispositivos inalámbricos que se comunican entre sí sin la necesidad de una infraestructura centralizada encargada de gestionar los recursos radio entre dichos terminales. Sin embargo, la forma en que estos dispositivos colaboran entre sí para posibilitar la comunicación entre terminales alejados puede ser empleada para proporcionar acceso a Internet a aquellos terminales que se encuentran fuera de la región de cobertura del punto de acceso.

En general, los protocolos de encaminamiento ad hoc no son suficientes para asegurar la integración de las redes ad hoc con redes externas. Es por ello, que han surgido varios mecanismos de conexión a Internet para los terminales ad hoc. Todos ellos coinciden en la necesidad de introducir una pasarela o *gateway* en la red ad hoc que proporcione las funcionalidades de encaminamiento ad hoc así como la de propagación multisalto del prefijo de red. Los mecanismos más analizados optan por la incorporación de un dispositivo dedicado que actúe como *gateway* o bien por implantar un punto de acceso más complejo (*gateway* de acceso) [1][2][3].

Por otro lado, es posible que en ciertos escenarios coexistan múltiples *gateways* en el radio de cobertura de uno o varios nodos. En el momento en el que un nodo necesite comunicaciones con Internet, el dispositivo móvil seleccionará el *gateway* que considere más oportuno siguiendo unos criterios establecidos. Por lo tanto, el criterio seleccionado influirá en el número de conmutaciones de *gateway* que el dispositivo realizará. Cuando la conmutación implica gateways que anuncian distintos prefijos de red, el cambio lleva asociado la configuración de una dirección IP adecuada al prefijo de red del *gateway* que se va a utilizar posteriormente. En las redes ad hoc donde se carece de equipos de gestión centralizados, la configuración de direcciones IP más adecuada es la que sigue una estrategia de autosuficiencia (*stateless autoconfiguration*). Con esta metodología, un dispositivo construye su dirección IP mediante la concatenación del prefijo de red y un número que teóricamente es único (dirección MAC) o un número aleatorio. Sin embargo, bajo ciertas circunstancias la dirección IP generada podría estar duplicada. Por ejemplo, la

MAC podría estar alterada o no se desea emplear por el posible seguimiento que se podría hacer a partir de ella. Es por ello que se aconseja que el mecanismo de auto-configuración de direcciones vaya seguido de un proceso de detección de direcciones duplicadas o DAD (*Duplicate Address Detection*). La técnica clásica de DAD consiste en la búsqueda de un terminal que posea la dirección que se acaba de configurar. Esta búsqueda suele durar un cierto tiempo (típicamente 1 segundo) por lo que las comunicaciones se interrumpen durante ese intervalo [4]. En esta ponencia, se analizará el efecto que la conmutación de *gateway* posee en las prestaciones de la red.

El artículo se estructura en los siguientes puntos. En la sección 2, se detallan las características principales de los mecanismos propuestos para la integración de redes ad hoc con redes externas. Posteriormente, la sección 3 describe los criterios de selección de *gateway* considerados en este estudio. Posteriormente, en la sección 4 se explica el proceso de autoconfiguración de direcciones IP junto con la técnica de Detección de Direcciones Duplicadas. En la sección 5, se muestran los resultados de las simulaciones. Finalmente, en la sección 6 se presentan las principales conclusiones del análisis realizado.

2. Mecanismos de Conexión a Internet

La integración de las redes ad hoc con redes externas como Internet requiere la presencia de un elemento adicional denominado *gateway*. El gateway se asocia al *router* de acceso tal y como se aprecia en la Fig. 1.

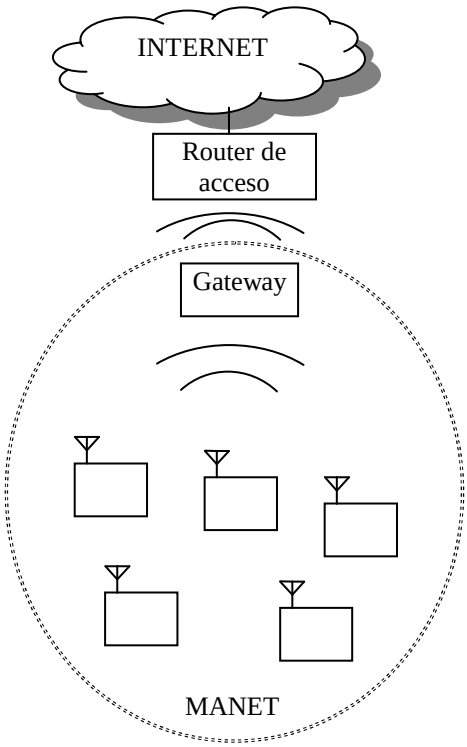

Figura 1. Esquema de una red ad hoc conectada a nternet.

Las funcionalidades del *gateway* son múltiples. Por un lado, realiza las tareas asociadas al encaminamiento dentro de la MANET mediante el empleo de un protocolo ad hoc. Por otro lado, anuncia el prefijo de red adecuado al *router* de acceso al que está vinculado mediante la propagación de mensajes MRA (*Modified Router Advertisement*) que son retransmitidos por los dispositivos móviles. Estos mensajes MRA son imprescindibles dentro de la red ya que proporcionan el prefijo de red. Esta información es necesaria para que los nodos puedan configurar su propia dirección IP y, por ende, puedan establecer conexiones con cualquier nodo en Internet.

Los mecanismos de integración en Internet difieren principalmente en las características del *gateway* así como en su comportamiento. La mayoría de las propuestas consideran un *gateway* dedicado que puede colocarse en una posición fija dentro del área de cobertura del *router* de acceso o bien integrarse directamente dentro de éste. Dentro de este esquema, el mecanismo más utilizado es el de "Conectividad global" [1]. En él, el *gateway* puede anunciarse de manera proactiva o reactiva tal y como ocurre con los protocolos de encaminamiento ad hoc. Posteriormente, también se estudió la técnica híbrida de emisión de MRAs, es decir, el anuncio proactivo en un área cercana al *gateway* y la petición reactiva procedente de los terminales ubicados fuera de esta región [5].

El mecanismo de "Continuidad de Prefijo" pretende optimizar el comportamiento del mecanismo de conectividad global en aquellos escenarios donde existan múltiples *gateways* [2]. Siguiendo las especificaciones de esta propuesta, un dispositivo que recibe múltiples MRAs (cada uno de ellos asociado a un *gateway* distinto) sólo retransmite el MRA originado en el gateway seleccionado. De esta manera, todo dispositivo para emplear el gateway seleccionado establece un camino compuesto de terminales que comparten el mismo prefijo de red y, por tanto, emplean el mismo *gateway*. La Fig. 2 muestra las diferencias principales entre ambas propuestas en el proceso de retrasmisión de MRAs. El nodo de la MANET etiquetado con A recibe dos tipos de mensajes MRA, MRA1 originado por el Gateway1 y MRA2 originado por el Gateway2. Este terminal decide utilizar el Gateway1 por lo que sólo retransmite el mensaje MRA1. El nodo B sólo puede elegir el Gateway1 para retrasmitir los paquetes a través del nodo A. El nodo B, tiene pues, un camino hacia el Gateway 1 (línea discontinua de la figura) compuesto por terminales que han seleccionado el mismo Gateway que él.

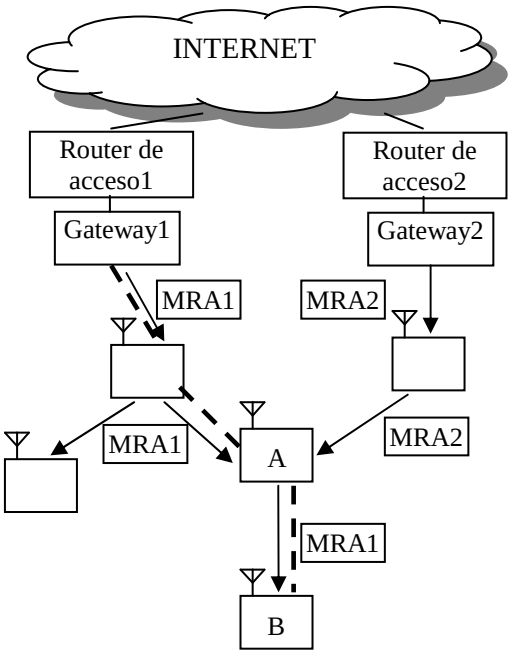

Figura 2. Reenvío de MRAs en el mecanismo de Continuidad de Prefijo

Por otro lado, ha surgido la propuesta de "Múltiples Pasarelas Móviles" que persigue que los propios terminales de la MANET se configuren dinámicamente para actuar como *gateways* [6]. Bajo este esquema, la red ad hoc consigue la flexibilidad necesaria para integrarse con redes externas en aquellos escenarios preparados para redes inalámbricas convencionales.

Debido a su amplia difusión, en esta ponencia se analizarán los efectos de la conmutación de *gateways* tanto en el mecanismo de conectividad global como en el de continuidad de prefijo.

3. Criterios de Selección de *Gateways*

En escenarios donde un terminal móvil recibe información de múltiples *gateways*, el dispositivo debe decidir cuál es el *gateway* más adecuado para sus comunicaciones siguiendo unos criterios de selección.

En este estudio, se analizarán dos de los criterios más representativos:

- Criterio de la distancia o de menor número de saltos. Ante la recepción de varios mensajes MRA con diverso origen, se opta por el *gateway* que se encuentra a un menor número de saltos del nodo. Con este criterio, se imita la selección de camino de la mayoría de los protocolos de encaminamiento clásicos y ad hoc.
- Criterio de máxima permanencia. El *gateway* seleccionado se utiliza hasta que éste deja de estar operativo o accesible para el nodo. De esta manera, se intenta reducir el número de conmutaciones de *gateways*.

4. Autoconfiguración de Direcciones IP

En el contexto de IPv6, para que los terminales estén accesibles desde el exterior deben poseer una dirección IPv6 global apropiada al contexto en el que se encuentran, es decir, con uno de los prefijos de red que anuncia el *gateway* que pretenden emplear [7].

La adquisición de la dirección IP se puede realizar a través de un proceso DHCP (*Dynamic Host Configuration Protocol*). De esta manera, un equipo centralizado sería el encargado de gestionar todas las direcciones de los equipos de la MANET. Aunque varios estudios han analizado esta estrategia [8] [9] [10], el requisito de contar con un sistema centralizado para el control de direcciones resta flexibilidad para la utilización de redes ad hoc en escenarios no acondicionados para este propósito. Es por ello, que la metodología de autoconfiguración de direcciones resulta más aconsejable.

La autoconfiguración de direcciones IP (*stateless autoconfiguration*) se fundamenta en que el propio dispositivo móvil genera su dirección IP. Para ello, concatena un número teóricamente único al prefijo de red correspondiente [11]. Este número puede extraerse de diversas fuentes. Por un lado, se podría emplear la dirección MAC. Sin embargo, algunos usuarios consideran que esta utilización permitiría el seguimiento de sus actividades por lo que optan por un número aleatorio [12]. En ambos casos, es posible que la dirección generada no sea única ya que la dirección MAC puede ser alterada [13] e incluso puede haber duplicidad en el número aleatorio si se extrae de un generador con un rango pequeño, como el empleado en el caso de los sensores. Es por ello, que se recomienda que el proceso de autoconfiguración de direcciones vaya seguido de una etapa de verificación de la unicidad de la dirección construida. Esta operación se denomina Detección de Direcciones Duplicadas o DAD (*Duplicate Address Detection*).

El proceso de DAD más extendido se denomina DAD de prueba y espera (*try and wait*). Se basa en la búsqueda de una ruta hacia un hipotético nodo que posee la misma dirección que acaba de configurar el dispositivo [4]. El nodo origen (el que está comprobando la unicidad de su dirección IP) esperará durante un intervalo de tiempo posibles respuestas del hipotético nodo. Tras ese periodo, si no se ha recibido ninguna respuesta, el nodo asume que la dirección configurada es única. Por otro lado, si el nodo origen hubiese recibido alguna respuesta, habría comprobado que existe duplicidad y, por tanto, debería generar una nueva dirección IP y debería repetir el proceso hasta obtener una dirección única. La Fig. 3 muestra el comportamiento de DAD.

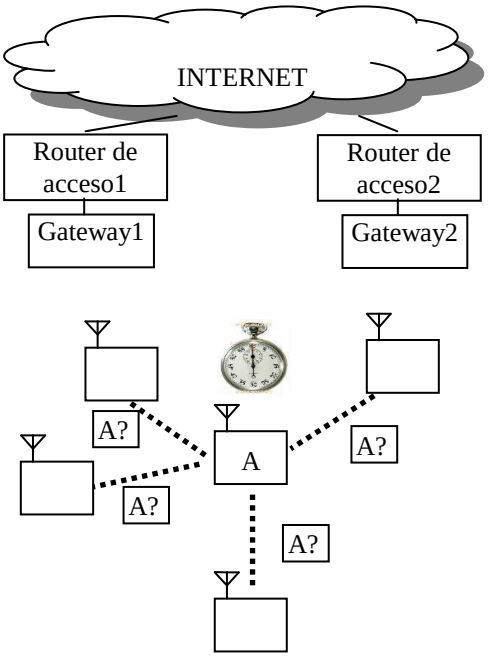

Figura 3. Proceso de DAD *try and wait*

En la Fig. 3, el nodo central configura la dirección A por lo que emite mensajes de petición de ruta o RREQ (*Route Request*) hacia un nodo con dirección A. Tras ese proceso, arranca un temporizador en espera de posibles respuestas.

En las redes móviles ad hoc, el proceso de verificación de las direcciones puede realizarse en diversos momentos distinguiéndose dos tipos principales de DAD. Por un lado, el terminal puede comprobar que su dirección IP es apropiada justo después de haberla generado. En este caso, el dispositivo estaría realizando un DAD pre-servicio (*pre-service DAD*). Por otro lado, el nodo puede comprobar periódicamente que la dirección que posee sigue siendo única. Esta operación o DAD en servicio (*in-service DAD*) es útil cuando la red ad hoc puede tener uniones con otras redes que comparten el mismo prefijo (*merging*). La utilización de DAD *in-service* resulta muy costosa desde el punto de vista de la retransmisión de paquetes ya que periódicamente se inunda la red. Por ello, los autores de esta ponencia consideran oportuno sustituir esta técnica por las propuestas de DAD pasivo que intentan distinguir la duplicidad de las direcciones mediante el análisis de los paquetes recibidos [14]. Por simplicidad, en esta ponencia se considera exclusivamente el efecto de DAD *pre-service*.

5. Simulaciones y Resultados

Debido a la dificultad de realizar pruebas con redes ad hoc reales, el análisis sobre la influencia que el criterio de selección de *gateway* presenta sobre las prestaciones de la red se realiza a través de simulaciones. Para ello, se ha escogido la herramienta de simulación más extendida dentro de los estudios de redes inalámbricas, el *Network Simulator* o *ns-2* [15]. Este simulador de eventos discretos puede ser extendido para que soporte el mecanismo de conectividad global [16]. Este módulo adicional tuvo que ser apropiadamente modificado con el propósito de definir el mecanismo de continuidad de prefijo. Conjuntamente, fue preciso implementar el mecanismo de DAD de prueba y espera dentro del ns2.

Los escenarios de simulación considerados se componen de un área de 2500x500 m^2 donde los *Gateways* se colocan en los extremos de la superficie. La red ad hoc se compone de 50 terminales móviles cuyos movimientos siguen el modelo de *Modified Random WayPoint* [17]. Bajo este patrón de movilidad, los nodos se colocan uniformemente en la región de simulación. Posteriormente, cada uno de ellos elige una velocidad comprendida entre un valor mínimo y uno máximo siguiendo una distribución uniforme. Adicionalmente, elige una posición de destino dentro del área de simulación a la que se dirige con la velocidad previamente seleccionada. Una vez que el terminal llega a su destino, puede realizar una pausa antes de repetir el proceso. Aunque la versión inicial de este modelo considera que la distribución inicial de los nodos es uniforme, en este trabajo se ha considerado que la estabilidad de los resultados se consigue si la distribución inicial de la posición de los nodos se corresponde con la distribución final que alcanza el patrón de Random WayPoint [18]. Para ello, se ha empleado el generador de movimientos incluido en la herramienta *ns*, el programa *setdest*, con los parámetros adecuados para cumplir estos requisitos.

El tráfico está asociado a 10 fuentes CBR (*Constant Bit Rate*) con una tasa de 4 paquetes por segundo. Todas las comunicaciones se establecen desde un nodo de la red ad hoc y poseen como destino un terminal fijo que debe ser accedido a través de uno de los *Routers* de Acceso.

La Tabla 1 resume el resto de los parámetros considerados en las simulaciones.

El comportamiento de la red se ha cuantificado mediante el empleo de las siguientes medidas:

- Porcentaje de Paquetes Perdidos. Se define como la proporción entre los paquetes de datos perdidos y los originados por las fuentes. Equivale al inverso del Porcentaje de Paquetes Entregados o PDR (*Packet Delivery Ratio*)
- Retardo Extremo-Extremo. Representa el tiempo medio que tarda un paquete en llegar al destino. Este tiempo incluye todas las retransmisiones a nivel MAC así como la retransmisión a través de los terminales intermedios.

TABLA 1. PARÁMETROS DE SIMULACIÓN

Área de Simulación	2500 m x 500 m
Terminales móviles	50
Gateways	2 GWs fijos en (100m, 250m) y (2400m, 250m)
Patrón de Movilidad (Random WayPoint)	Velocidad máx: [1, 10] m/s. Velocidad mín = 1 m/s Pausa : 0 segundos
Patrón de Tráfico	10 fuentes CBR De un nodo ad hoc al exterior Tasa = 4 paquetes/s Tamaño paquete= 512 B
Tiempo Simulación	2500 s
Rango Transmisión	250 m
Ejecuciones por punto	3
Protocolo ad hoc	AODV
Cola interna	64 paquetes
Intervalo MRA	10 segundos
Intervalo DAD	1 segundo

- Sobrecarga Normalizada. Equivale a la cantidad de paquetes de control que deben ser generados respecto a la cantidad de paquetes de datos recibidos. Para este cómputo, cada retransmisión de un paquete de control se considera como un nuevo paquete de control

Los datos obtenidos se representan en las Fig. 4-9. En ellas se incluye la regresión lineal de los datos con el propósito de mostrar las tendencias generales del comportamiento de los mecanismos y así, facilitar la comprensión de los mismos.

Para un primer análisis, se analizará el mecanismo de Conectividad Global. La Fig. 4 muestra el porcentaje de los paquetes perdidos cuando se emplean los dos criterios considerados en este análisis.

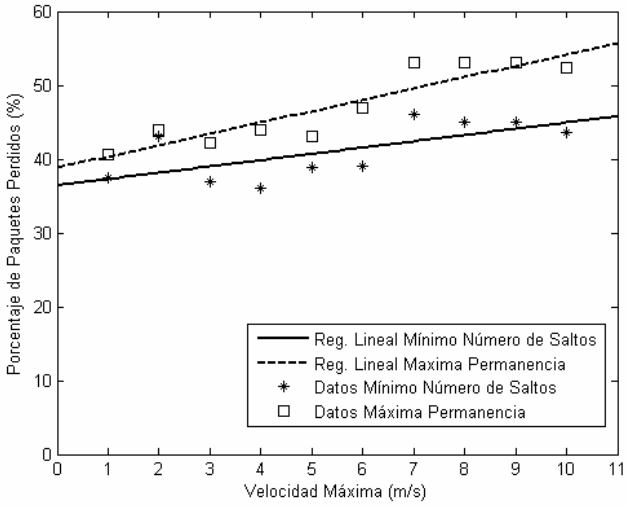

Figura 4. Porcentaje de Paquetes Perdidos en función de la velocidad Máxima de los nodos en el Mecanismo de Conectividad Global.

Tal y como puede observarse, el criterio de máxima permanencia provoca un mayor número de pérdidas. Este efecto se debe a que, en general, con este criterio los paquetes pueden ser retransmitidos por un mayor número de saltos. En cada una de las retransmisiones, el paquete puede perderse. Adicionalmente, al recorrer más saltos, los paquetes producen más interferencias en los enlaces adyacentes.

La Fig. 5 muestra el retardo Extremo-Extremo para el mecanismo de Conectividad global. Se observa un comportamiento similar al del retardo. Tal y como se comentó anteriormente, el criterio de máxima permanencia puede forzar a que los paquetes recorran más saltos en comparación con el mínimo necesario. Bajo estas circunstancias, el paquete tarda más en llegar al destino. Por otro lado, la Fig. 6 muestra la sobrecarga introducida por ambos criterios cuando se emplea el mecanismo de conectividad global.

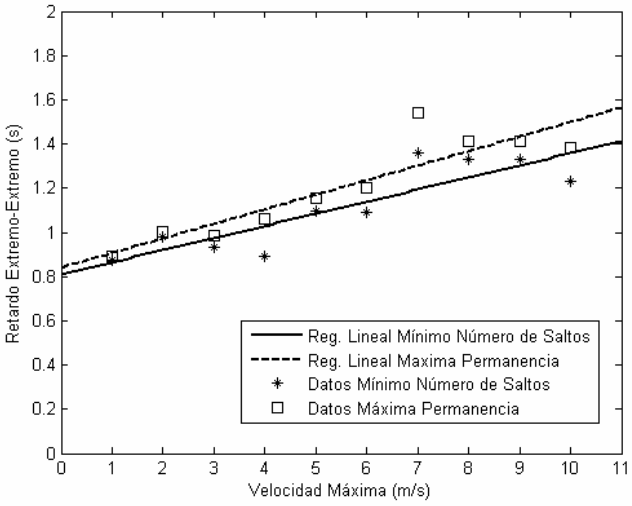

Figura 5. Retardo Extremo-Extremo en función de la velocidad Máxima de los nodos en el Mecanismo de Conectividad Global.

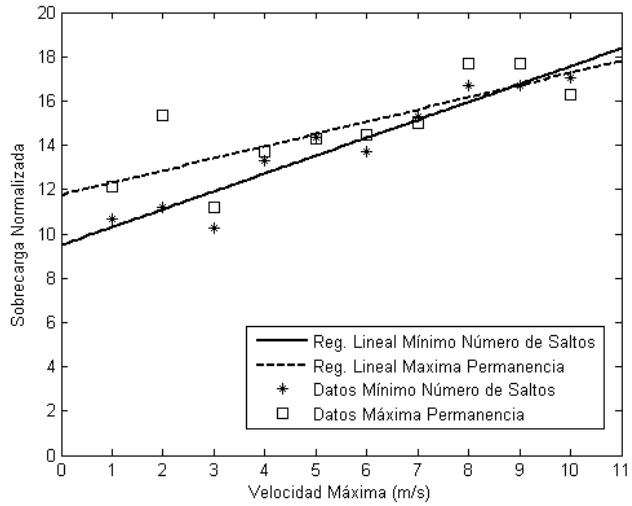

Figura 6. Sobrecarga Normalizada en función de la velocidad Máxima de los nodos en el Mecanismo de Conectividad Global.

Aunque inicialmente el criterio de Máxima Permanencia persigue reducir los procesos de DAD necesarios cada vez que se conmuta de *gateway*, este efecto se ve claramente superado por las rupturas de enlaces que ocurren dentro de la MANET. El restablecimiento de la ruta hacia el *gateway* que se pretende seguir utilizando parece más costoso que la conmutación de gateway y su posterior proceso de DAD.

Como un segundo paso del análisis efectuado, se estudió el comportamiento de la red con el mecanismo de continuidad de prefijo. Analizando los mismos parámetros que en el caso anterior, las prestaciones de la red sigue tendencias similares a los resultados obtenidos con el mecanismo de conectividad global.

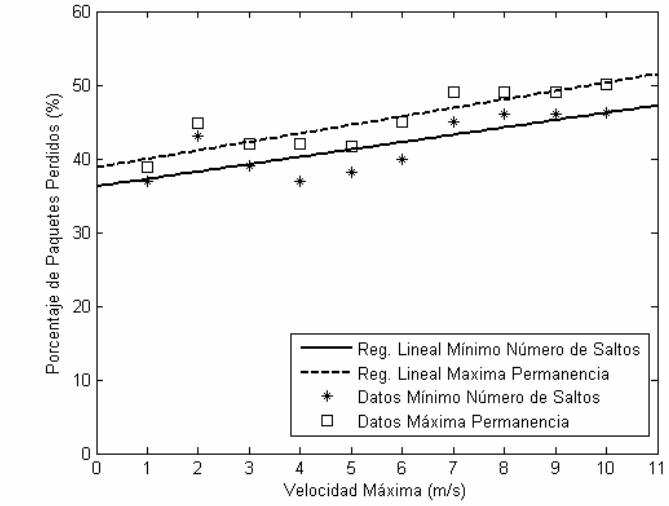

Figura 7. Porcentaje de Paquetes Perdidos en función de la velocidad Máxima de los nodos en el Mecanismo de Continuidad de Prefijo.

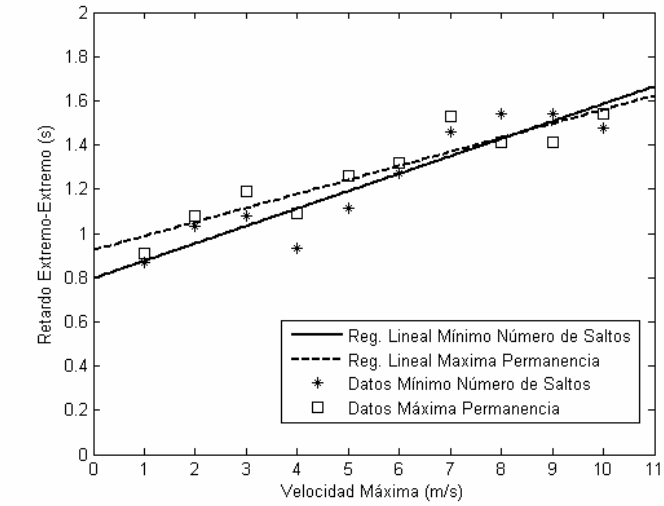

Figura 8. Retardo Extremo-Extremo en función de la velocidad Máxima de los nodos en el Mecanismo de Continuidad de Prefijo.

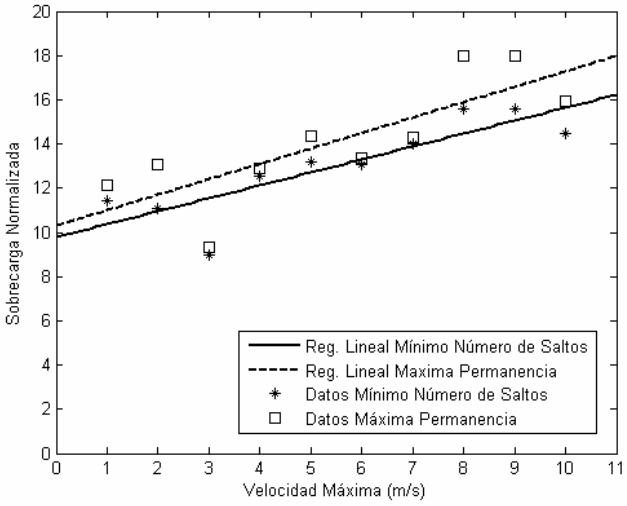

Figura 9. Sobrecarga Normalizada en función de la velocidad Máxima de los nodos en el Mecanismo de Continuidad de Prefijo.

6. Conclusiones

En esta ponencia se ha analizado las repercusiones que los criterios de selección de *gateways* generan en los mecanismos de integración de redes ad hoc con redes externas. En concreto, se han analizado dos de los criterios más representativos. Por un lado, se ha optado por estudiar el criterio de mínimo número de saltos por ser la estrategia más utilizada dentro del encaminamiento ad hoc. Por otro lado, con el propósito de reducir los procesos de DAD asociados a la conmutación de gateways, se ha analizado el criterio de máxima permanencia por el cual un terminal móvil emplea el gateway seleccionado hasta que éste deja de estar operativo.

Tanto en el mecanismo de Conectividad Global como en el de Continuidad de Prefijo se observa que las mejores prestaciones se alcanzan cuando el criterio de menor número de saltos es empleado.

Referencias

[1] Wakikawa, R., Marinen, J., Perkins, C., Nilsson, A., and Tuominen, A.J." Global Connectivity for IPv6 Mobile Ad hoc Networks", *IETF Internet Draft*, trabajo en proceso, Enero 2005.

[2] Jelger, C., Noel, T., and Frey, A.:"Gateway and address autoconfiguration for IPv6 adhoc networks", *IETF Internet Draft*, trabajo en proceso, Octubre 2003.

[3] Cha, H.W., Park, J.S, and Kim, H.J. "Extended Support for Global Connectivity for IPv6 Mobile Ad Hoc Networks", *IETF Internet Draft*, trabajo en proceso, Octubre 2003.

[4] Perkins, C., Wakikawa, R., Malinen, J., Belding-Royer, E., and Y. Suan: "IP Address Autoconfiguration for Ad Hoc Networks", *IETF Draft*, work in progress, Noviembre 2001.

[5] Ratanchandani, P., Kravets, R. : "A Hybrid Approach to Internet Connectivity for Mobile Ad Hoc Networks", en Actas de IEEE WNC 2003, Vol 3, pp.1522-1527, Nueva Orleans, Estados Unidos, Marzo 2003.

[6] Singh, S., Kim J.H., Choi,Y.G., Kang, K.L., and Roh, Y.S.: "Mobile multi-gateway support for IPv6 mobile ad hoc networks", *IETF Internet Draft*, trabajo en proceso, Junio 2004.

[7] Huitema, C.: "IPv6: the new Internet Protocol", Prentice-Hall, 1998. ISBN:0-13-850505-5.

[8] McAuley, A.,Manousakis K. : “Self-Configuring Networks” , en Actas de *21st Century Military Communications Conference* , 2000.
[9] Mohsin, M. , Prakash, R. : “IP Address Assignment in a Mobile Ad Hoc Network”, en Actas de *MILCOM 2002*, 2002.
[10] Tayal, A., Patnaik, L.: "An address assignment for the automatic configuration of mobile ad hoc networks", en Actas de *Personal Ubiquitous Computing* , 2004.
[11] Thomson, S., Narten, T.: “IPv6 Stateless Address AutoConfiguration”, IETF RFC 2462, 1998.
[12] Narten, T., Draves, R.: “Privacy Extensions for Stateless Address Autoconfiguration in IPv6”, IETF RFC 3041, Enero 2001.
[13] Vaidya, N.: “Weak Duplicate Address Detection in Mobile Ad Hoc Networks”, en Actas de MOBIHOC'02, 2002.
[14] Weniger, K. “Passive Duplicate Address Detection in Mobile Ad hoc Networks”, en Actas de IEEE Wireless Communications and Networking Conference (WCNC) 2003, Nueva Orleans, Estados Unidos, Marzo 2003.
[15] Fall, K. , Varadhan, K. : “Ns Notes and Documentation”, The VINT Project. UC Berkeley, LBN 2005.
[16] http://www.telecom.lth.se/Personal/alexh/
[17] Yoon, J., Liu, M., Noble, B.: ”Random waypoint considered harmful”, en Actas de Infocom’03, pp. 1312-1321, San Francisco. Abril 2003.
[18] Hyytia, E., Lassila, P., Nieminen, L., Virtamo, J. :“Spatial Node Distribution in the Random WayPoint Mobility Model”, IEEE Transactions on Mobile Computing, vol no. 56, pp. 680-694, Junio 2006.