Sistemas Avanzados de Reputación para Redes Móviles Ad-hoc Cooperativas

Alberto Rodriguez-Mayol, Javier Gozalvez
Ubiquitous Wireless Communications Research Laboratory
Uwicore, http://www.uwicore.umh.es
Universidad Miguel Hernández
Avda. de la Universidad s/n, 03202, Elche (España)
f.rodriguez@umh.es, j.gozalvez@umh.es

***Resumen*- MCN-MR (*Multi-hop Cellular Network – Mobile Relay*) es una novedosa tecnología que ha sido propuesta para ser empleada en los sistemas *Beyond 3G* o *4G* por su capacidad para proporcionar homogeneidad en la calidad de servicio de toda el área de cobertura. Para ello, es necesario que los nodos cooperen en la retransmisión de los paquetes de otros usuarios, dado que el egoísmo de los nodos puede tener un efecto muy perjudicial en la conectividad *multi-hop* de las redes MCN-MR. En trabajos anteriores se han propuesto distintos tipos de protocolos basados en reputación para contrarrestar el egoísmo de los nodos en redes móviles *ad-hoc*. Sin embargo, la evaluación de su rendimiento en condiciones realistas de simulación demuestra que tienden a sobrestimar el comportamiento egoísta de los nodos. De esta forma, la disponibilidad de rutas *multi-hop* válidas se ve reducida. En este contexto, este trabajo propone y evalúa dos técnicas que corrigen el funcionamiento inexacto de la técnica *watchdog* empleada para observar el comportamiento de los nodos.**

***Palabras Clave*- Redes celulares *multi-hop*; egoísmo; técnicas basadas en reputación; *watchdog*; MANET**

I. INTRODUCCIÓN

Una de las características más distintivas y exigentes de las futuras redes *Beyond 3G* será la provisión de niveles homogéneos de Calidad de Servicio (QoS, *Quality of Service*) en toda el área de cobertura [1]. Las redes celulares convencionales han alcanzado una cobertura universal, pero son incapaces de proporcionar niveles homogéneos de QoS en toda el área de la celda y velocidades de transmisión altas en zonas alejadas de la estación base (BS, *Base Station*), debido al decrecimiento exponencial del nivel de señal con la distancia. Para superar esta limitación, los operadores pueden aumentar la densidad de BS, que a su vez incrementaría la complejidad de la planificación y el coste de despliegue y mantenimiento de la red, además del rechazo social existente en contra de la instalación de nuevos emplazamientos de antenas. Por otro lado, se ha propuesto un nuevo paradigma de redes de comunicaciones, denominadas *Multi-hop Cellular Networks* (MCN) [2], que combinan las transmisiones en modo *ad-hoc* y en modo celular, para incrementar las tasas de transmisión y proporcionar niveles de QoS homogéneos en toda la celda. En las redes MCN, las transmisiones celulares de un solo salto de larga distancia son sustituidas por una combinación de múltiples transmisiones *ad-hoc* y una última conexión celular de corta distancia con la BS. La transmisión en modo *multi-hop* celular permite extender las altas tasas de transmisión de las proximidades de la BS a las zonas del borde de la celda, además de mejorar la capacidad, la cobertura y la utilización de la energía [3].

Se han identificado dos modalidades de redes MCN. En la modalidad de retransmisión fija (MCN-FR, MCN-*Fixed Relay*), se emplean estaciones repetidoras fijas para reducir la distancia de retransmisión entre la BS y los usuarios situados en el borde de la celda. Para alcanzar el rendimiento esperado, las antenas retransmisoras deben estar situadas en emplazamientos con buenas condiciones de propagación con la BS, especialmente de visibilidad directa (LOS, *Line Of Sight*). Las redes MCN-FR tienen una complejidad de diseño relativamente baja, pero requieren la instalación de nuevas antenas con el consecuente coste económico y social [3]. Por otro lado, las redes de retransmisión móvil (MCN-MR, MCN-*Mobile Relay*) tienen una mayor flexibilidad, dado que emplean los equipos de los usuarios (UE, *User Equipment*) como estaciones retransmisoras. Sin embargo, deben superarse ciertos desafíos para conseguir los beneficios esperados de las redes MCN-MR. Uno de estos desafíos es asegurar la cooperación de los usuarios en el proceso de retransmisión de los paquetes [4]. El comportamiento egoísta de los nodos puede estar motivado por distintas causas, tales como el agotamiento de la batería del terminal, la sobrecarga en el canal, la desconfianza hacia la tecnología MCN-MR, etc. y puede provocar un importante deterioro del rendimiento de la red. En este contexto, el objetivo de los protocolos de prevención de egoísmo (SPP, *Selfishness Prevention Protocols*) es incentivar a los nodos a cooperar en las funciones de la red y evitar los ataques intencionados de nodos maliciosos.

Trabajos anteriores en el área de redes MANET (*Mobile Ad-hoc NETworks*) han abordado el problema del descarte de paquetes, en el que algunos nodos se niegan a retransmitir los paquetes originados por otros nodos, incluso después de haber accedido a retransmitirlos en la fase de búsqueda y establecimiento de rutas *multi-hop* [5]. En [5] se establecen tres grupos para categorizar las diferentes estrategias de SPP propuestas en la literatura: basadas en reputación, basadas en crédito y basadas en teoría de juegos. Las estrategias basadas en crédito utilizan una moneda real o virtual para pagar por la retransmisión de los paquetes realizada por otros nodos. El crédito se utiliza para compensar la utilización de los recursos de otros nodos en el proceso de retransmisión, y puede ser obtenido retransmitiendo los paquetes de otros nodos o simplemente se puede comprar con una moneda real. Algunas de las desventajas de los esquemas basados en crédito son la

falta de escalabilidad, la necesidad de una entidad central confiable o de un hardware de seguridad a prueba de ataques y falsificaciones [5]. Por otro lado, los modelos de teoría de juegos empleados en SPPs simulan un juego en el que cada nodo puede escoger retransmitir o no los paquetes de otros nodos en función de distintos parámetros. Permiten estudiar de manera analítica la estabilidad de los puntos de equilibrio y de las soluciones a los problemas planteados con diferentes estrategias. Sin embargo, muchas propuestas basadas en teoría de juegos no reflejan adecuadamente la influencia de algunos parámetros importantes de los sistemas reales. Alternativamente, en el presente trabajo se emplean protocolos basados en reputación, que por lo general emplean la técnica *watchdog* propuesta en [6] para observar el comportamiento de otros nodos, que será explicada más adelante. Estas observaciones se registran en una tabla de reputación que cuantifica la predisposición de cada nodo conocido a cooperar en la retransmisión. La información de la tabla de reputación se emplea en el proceso de descubrimiento y establecimiento de ruta para seleccionar una ruta sin nodos egoístas. Los esquemas de reputación son completamente distribuidos y obtienen un buen rendimiento de red [4]. Sin embargo, un estudio previo [7] mostró que la evaluación de los esquemas de reputación en condiciones de simulación simplistas puede proporcionar resultados inexactos y demasiado optimistas sobre su funcionamiento y rendimiento. En particular, [7] demostró la importancia del impacto sobre el rendimiento esperado de las técnicas SPP basadas en reputación de factores como las condiciones de propagación radio y la posible sobrecarga del canal. Tomando como punto de partida estas observaciones, en este trabajo se proponen dos nuevas estrategias para mejorar el rendimiento de esquemas basados en reputación en redes MCN-MR y se evalúa su funcionamiento en un escenario realista de simulación.

El resto del trabajo se estructura del siguiente modo. Los protocolos basados en reputación se presentan en la sección II, así como una descripción de la técnica *watchdog*. La sección III presenta las mejoras propuestas en este estudio. La sección IV introduce la plataforma de simulación implementada y la sección V discute el rendimiento conseguido con las técnicas propuestas. Finalmente, las conclusiones se presentan en la sección VI.

II. Protocolos de Prevención de Egoísmo Basados en Reputación

Los SPPs empleados para contrarrestar los ataques de descarte de paquetes tienen como objetivo detectar y aislar a los nodos egoístas para incentivarlos a cooperar. Los métodos basados en reputación se componen de dos módulos: detección y reacción. El módulo de detección de cada nodo vigila el comportamiento de otros nodos, es decir, si transmiten o no los paquetes que deben retransmitir, usando el mecanismo *watchdog* de detección explicado en la siguiente sección II.A. El módulo de reacción mantiene una tabla de reputación donde a cada nodo se le asigna un nivel de reputación basado en las observaciones del módulo de detección. La información de dicha tabla se emplea en el protocolo de enrutamiento para evitar y aislar a los nodos egoístas conocidos en futuros establecimientos de ruta. En la literatura se han propuesto otros métodos de detección de egoísmo, tales como el protocolo TWOACK [8], o el sistema propuesto en [9]. TWOACK propone que la retransmisión correcta de cada paquete sea confirmada al nodo precursor por parte del nodo sucesor mediante el envío de un paquete ACK (*ACKnowledgment*) de confirmación hacia atrás a través del nodo retransmisor (ver Figura 1). Esta estrategia introduce una sobrecarga de comunicación muy alta por la necesidad de confirmar cada paquete. Mediante otro enfoque, [9] plantea que los mensajes ACK empleados en protocolos como TCP (*Transmission Control Protocol*) para la confirmación extremo a extremo de la correcta transmisión de un paquete se utilicen para vigilar el comportamiento de los nodos. Sin embargo, dicho sistema no permite distinguir cuál es el nodo egoísta entre todos los que participan en una ruta *multi-hop* sospechosa. Por ello, en este trabajo se ha escogido como técnica de detección el sistema *watchdog*.

A. Técnica de detección watchdog

La técnica de detección *watchdog* [6] se basa en la confirmación pasiva de la retransmisión de los paquetes mediante la observación de los paquetes transmitidos por el nodo retransmisor, como se muestra en la Figura 1.

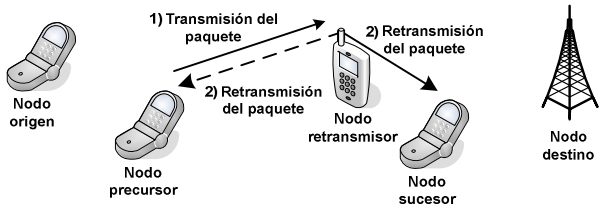

Fig. 1. Funcionamiento de la técnica de detección *watchdog*.

En la Figura 1, el nodo origen ha establecido una ruta *multi-hop* hacia el nodo destino para transmitir sus paquetes de datos. La ruta se ha establecido empleando un protocolo de enrutamiento *multi-hop* cualquiera. Los paquetes de datos se transmiten de manera consecutiva salto por salto siguiendo la secuencia *nodo origen – nodo precursor – nodo retransmisor – nodo sucesor – nodo destino*. En la figura, un paquete se transmite primero desde el nodo precursor al nodo retransmisor. En el nodo precursor, un buffer de paquetes almacena una copia temporal del paquete transmitido, que debe ser retransmitido por el nodo retransmisor. A cada paquete almacenado se le asigna un '*timeout* de paquete', que marca el tiempo máximo que puede tardar el nodo retransmisor en transmitir el paquete. En caso de que dicha transmisión se realice en el tiempo establecido y sea escuchada por el nodo precursor, se asume que el nodo retransmisor ha cooperado correctamente, lo cual se conoce como una 'detección de retransmisión'. El nodo precursor busca la copia del paquete escuchado en el buffer y la borra. En caso de que el paquete retransmitido no sea escuchado correctamente por el nodo precursor dentro del tiempo establecido, entonces se supone que el nodo retransmisor ha actuado de manera egoísta, es decir, que ha descartado el paquete. Esto se conoce como una 'detección de descarte'. Dependiendo del tipo de SPP, las detecciones de descarte y de retransmisión modifican el nivel de reputación del nodo en la tabla del nodo precursor. Un parámetro importante en el proceso de detección *watchdog* es el *timeout* de paquete, que es el tiempo máximo establecido para que el nodo retransmisor retransmita el paquete. El valor de este parámetro no está especificado en el trabajo [6]. Un valor

demasiado grande del *timeout* de paquete incrementa el tiempo necesario para detectar a los nodos egoístas, y por tanto aumenta la cantidad de paquetes que estos nodos descartan antes de ser detectados, mientras que un valor demasiado pequeño puede impedir que los nodos no egoístas tengan tiempo suficiente para llevar a cabo la retransmisión. Para ajustar correctamente este parámetro, los autores llevaron a cabo algunas simulaciones preliminares. Los resultados obtenidos mostraron que la mayoría de los paquetes eran correctamente retransmitidos 50ms después de que el nodo precursor los transmitiera. Por consiguiente, el *timeout* de paquete fue fijado en 50ms en el presente trabajo. Otro parámetro definido en la implementación de la técnica *watchdog* en este trabajo es el intervalo de comprobación de buffer, que representa el intervalo entre instantes consecutivos en los cuales se rastrea el buffer y se borran aquellos que hayan caducado durante el intervalo anterior, actualizando consecuentemente la tabla de reputación. Este parámetro se ha fijado a 25ms, de acuerdo a resultados obtenidos en simulaciones previas de optimización.

La técnica *watchdog* de detección se utiliza en la mayoría de los SPPs basados en reputación. Sin embargo, tal y como los autores demostraron en [7], los errores de propagación radio y las colisiones de paquetes debidas a la sobrecarga en el canal pueden deteriorar notablemente el rendimiento de la técnica *watchdog* y su capacidad para detectar con exactitud a los nodos egoístas. En el ejemplo de la Figura 1, las colisiones en los paquetes podrían impedir que el nodo precursor observara correctamente la retransmisión del paquete por parte del nodo retransmisor. La referencia [9] aduce que las colisiones de paquetes no afectan notablemente a la capacidad de detección de *watchdog*, incluso con una carga de tráfico muy alta. Sin embargo, esta conclusión fue extraída a partir de un *testbed* con 4 nodos, lo cual puede limitar la generalidad de esta afirmación. En caso de que el nodo precursor no escuche la retransmisión del paquete, registrará una detección de descarte incorrecta. Si persisten de manera repetida las detecciones de descartes incorrectas hacia un nodo determinado, será acusado incorrectamente de comportarse egoístamente, por lo cual será evitado en futuros establecimientos de ruta, además de ser aislado y penalizado en la retransmisión de sus propios paquetes. Las acusaciones incorrectas además reducen la disponibilidad de rutas seguras, ya que algunas de las rutas que son descartadas por contener algún nodo supuestamente egoísta son en realidad rutas válidas. Por rutas seguras se entiende aquellas rutas que se suponen válidas porque en ellas no participa ningún nodo que haya sido acusado previamente de egoísta. En este contexto, este trabajo presenta dos mejoras aplicables a cualquier SPP que emplee la técnica de detección *watchdog* con el objetivo de reducir el número de acusaciones incorrectas para mitigar sus efectos negativos.

B. Protocolo de prevención de egoísmo de Marti

El SPP implementado en este trabajo fue propuesto por Marti [6]. El protocolo de Marti se compone de dos módulos: *watchdog* y *pathrater*, que pueden asimilarse a un módulo de detección y otro de reacción, respectivamente. En el módulo *watchdog*, cada nodo precursor usa la técnica *watchdog* para observar el comportamiento de los nodos retransmisores. El módulo *watchdog* cuenta el número de veces que un nodo retransmisor ha descartado paquetes. Cuando el número de detecciones de descarte supera un cierto umbral, denominado 'umbral máximo de faltas', el nodo retransmisor es acusado de egoísta. El valor exacto del umbral de faltas no fue especificado en [6]. Mientras que un valor demasiado alto del parámetro incrementa el número de paquetes que los nodos egoístas descartan antes de ser detectados, un valor demasiado bajo incrementa el número de acusaciones incorrectas hacia nodos no egoístas que son tomados por egoístas debido a los errores de propagación o a las colisiones de paquetes. Los autores realizaron simulaciones previas para encontrar un valor de compromiso entre ambas tendencias, escogiéndose finalmente el número 5. El *pathrater* en cada nodo usa la información proveniente del *watchdog* y del protocolo de enrutamiento para seleccionar aquella ruta con más probabilidad de ser confiable, es decir, aquella cuyos nodos tengan una mayor reputación promedio. El *pathrater* mantiene la tabla de reputación a partir de la información del *watchdog* y del protocolo de enrutamiento, para todos aquellos nodos con los que interacciona. Todos los valores numéricos de lo parámetros en esta implementación han sido escogidos de acuerdo a [6], excepto aquellos cuyo valor no había sido especificado en dicho trabajo, como se menciona en el texto. Cuando el *pathrater* detecta por primera vez a un nodo, le asigna de forma automática un nivel de reputación de 0.5. El *pathrater* incrementa la reputación de todos los nodos que participan en rutas activas en 0.01 en períodos fijos de 200ms. Este período se denomina 'intervalo de incremento de reputación'. Una ruta activa es aquella a través de la cual se ha recibido o transmitido un paquete durante el último intervalo de incremento de reputación. Se establecen dos distintas categorías de nodos: neutrales y egoístas. La máxima reputación que puede alcanzar un nodo neutral, es decir, que no ha sido acusado de actuar de manera egoísta, es 0.8. Por encima de ese valor, la reputación del nodo no es incrementada aunque así se tuviera que hacer según la regla de las rutas activas. La reputación de un nodo retransmisor del cual se detecta el descarte de un paquete se reduce en 0.05. El valor mínimo de la reputación de un nodo neutral es 0, valor que se mantiene mientras el nodo no pase a ser egoísta. Como se mencionó antes, un nodo es acusado de ser egoísta cuando supera el umbral máximo de faltas. Cuando un nodo es acusado de egoísta, su reputación se fija a un valor muy negativo, -100. Este nivel negativo se mantiene por un período de tiempo, el tiempo de aislamiento, cuyo valor no fue especificado en la implementación original, pero que en este trabajo se ha fijado a 500s. Después de este período, el aislamiento del nodo se desbloquea y su reputación vuelve a un valor de 0.5, para permitir que el nodo pueda optar por cooperar. El protocolo de Marti también introduce mensajes de acusación que permiten al nodo precursor advertir al nodo origen sobre la presencia de un nodo egoísta en la ruta. No obstante, estos mensajes pueden ser falsificados y además pueden aumentar la carga de señalización. Durante los procesos de descubrimiento y establecimiento de ruta, el protocolo de enrutamiento selecciona una ruta que no contenga nodos egoístas, según la tabla de reputación. Las peticiones de retransmisión de paquetes provenientes de nodos acusados de egoístas no son aceptadas por el *pathrater*.

III. Mecanismos de Mejora de SPP Basados en Reputación

Para mitigar los efectos negativos de la inexactitud de la técnica *watchdog* causada por errores en el canal radio o por colisiones de paquetes, este trabajo propone y evalúa dos mejoras de la técnica original de Marti que pueden ser adaptadas para aplicarse en cualquier SPP que utilice la técnica *watchdog* para la vigilancia de los nodos.

A. *Warning Mode* (WM)

El modo WM (*Warning Mode*) tiene como objetivo reducir el número de acusaciones falsas causadas por errores en el canal radio o por colisiones de paquetes. WM introduce una categoría intermedia, la de nodo 'sospechoso', entre un nodo marcado como neutral y un nodo marcado como egoísta. En la implementación original de Marti, cuando el nodo retransmisor, que está siendo observado por el nodo precursor, muestra un comportamiento egoísta durante un cierto período de tiempo, es acusado de egoísta directamente, y todos los enlaces en los cuales participa el nodo en cuestión son deshechos, dado que se supone que el nodo no va a retransmitir ninguno de los paquetes. No obstante, es importante señalar que estas acusaciones pueden ser incorrectas debido a errores de transmisión radio experimentados en el nodo precursor o en el nodo retransmisor. En este contexto, en el modo WM, cuando el número de faltas excede el umbral máximo de faltas, el nodo retransmisor se marca primero como sospechoso, y sus enlaces son temporalmente deshechos. Los nodos sospechosos pueden participar en las tareas de enrutamiento otra vez, dado que podría tratarse de una acusación incorrecta. Sin embargo, se aplican restricciones adicionales sobre los nodos sospechosos para evitar un aumento de los paquetes descartados por nodos egoístas reales. Específicamente, los nodos tratarán a los nodos sospechosos como si fueran nodos neutrales, con dos excepciones. En primer lugar, el *timeout* del que dispone el nodo para retransmitir el paquete se reduce en un factor α. En este trabajo, el factor α se ha fijado a 0.5, pero podría ser optimizado. Además, el número máximo de faltas se reduce a 1, en vez de 5, para los nodos sospechosos. De esta forma, si el nodo precursor detecta una única falta más por parte de un nodo sospechoso, lo acusará definitivamente de egoísta. Por otro lado, si un nodo precursor detecta que un nodo sospechoso coopera de nuevo, entonces su reputación se incrementa para darle la oportunidad de recuperarse del nivel previo de baja reputación, que puede haber sido provocado por errores radio o colisiones de paquetes.

Los potenciales beneficios de la técnica WM provienen del hecho de que los errores en el canal radio y las colisiones de paquetes pueden producir un incremento perjudicial del número de acusaciones incorrectas en la implementación original del protocolo de Marti. Las acusaciones incorrectas tienen muchos efectos negativos. Algunos nodos cooperativos son acusados y aislados de manera injusta. El aislamiento de nodos cooperativos les obstaculizará a la hora de encontrar rutas *multi-hop* hacia la estación base. Además, dado que los nodos egoístas son evitados en las rutas *multi-hop*, el número de rutas *multi-hop* potencialmente válidas se reduce erróneamente. Esto resulta en que algunas rutas *multi-hop* válidas serán infrautilizadas, mientras que otros nodos estarán sobrecargados por las peticiones de retransmisión de paquetes. Por el contrario, con la técnica WM, los nodos sospechosos tienen una oportunidad extra para recuperarse de una injusta mala reputación. En caso de que dicho nivel de reputación fuera provocado por colisiones de paquetes o por errores de transmisión radio, la participación de los nodos sospechosos se reestablece correctamente cuando las condiciones en el canal mejoran. En cambio, si el nodo sospechoso es realmente egoísta, el número de paquetes de datos adicionales que serán descartados será mínimo, dado que será detectado y aislado rápidamente debido a las condiciones de vigilancia estrictas establecidas en WM para los nodos sospechosos.

B. *Reset Failure Mode (RFM)*

El objetivo del modo RFM es el de contrarrestar las acusaciones incorrectas que pueden estar provocadas en el momento en que un enlace entre dos nodos se deshace debido a la movilidad de los nodos, al desvanecimiento o a otros efectos del canal radio. La capa MAC (*Medium Access Control*) es responsable de detectar las caídas de los enlaces e iniciar un proceso de 'caída de enlace', para informar al protocolo de enrutamiento. Sin embargo, antes de que el proceso se inicie, algunos de los paquetes transmitidos por el nodo precursor al nodo retransmisor pueden no haber sido retransmitidos correctamente por éste. Por consiguiente, las copias de los paquetes en el buffer de paquetes del nodo precursor caducarán, y la reputación del nodo retransmisor será injustamente rebajada.

En el modo RFM, si se detecta la caída de un enlace, se trata de restablecer la reputación inicial del nodo retransmisor implicado, pues su reputación puede haberse visto afectada por detecciones de descarte incorrectas. Para ello, la reputación del nodo se reajusta a 0.5, que es la reputación inicial asignada a un nodo que interacciona por primera vez con otro. Además, el número de faltas se reinicia a 0, dado que se supone que estas faltas han sido provocadas por la caída del enlace y no por el posible comportamiento egoísta del nodo. Por último, se borran las copias de los paquetes en el buffer del nodo precursor que están pendientes de ser retransmitidas por el nodo retransmisor, dado que éste no será capaz de retransmitirlas. Debe tenerse en cuenta que sólo se aplican estas reglas en el modo RFM cuando el nodo retransmisor es todavía un nodo neutral para el nodo precursor. Si es acusado de ser egoísta antes de que se dispare el proceso de 'caída de enlace', la reputación y las faltas del nodo retransmisor no son alteradas.

Un posible inconveniente de RFM es que la restauración de la reputación por caídas de enlaces puede incrementar la reputación de nodos egoístas verdaderos, es decir, que en verdad actúan egoístamente. Esto podría ocurrir en el caso de que se detecte una caída de enlace y que el nodo retransmisor implicado sea realmente un nodo egoísta que todavía no ha sido catalogado como tal. En este caso, la reputación del nodo se vería injustamente aumentada. No obstante, es importante notar que esto ocurre sólo en transmisiones *multi-hop* con enlaces con una vida media reducida, lo cual debería ser evitado empleando protocolos de enrutamiento *multi-hop ad-hoc* eficientes. Con estos protocolos eficientes, la vida media de los enlaces es mayor que el tiempo necesario para detectar el comportamiento egoísta de un nodo, en escenarios con una movilidad baja-media, en la cual las redes MCN con retransmisión móvil son más viables.

C. Coste y complejidad

Las propuestas WM y RFM son fáciles de implementer, puesto que solo requieren ligeras modificaciones de la implementación original del SPP que se ejecuta en paralelo. Además, RFM introduce un mínimo coste computacional, debido a la utilización de funciones sencillas como la restauración del nivel de reputación, el reseteo del número de faltas y el borrado de copias de paquetes en el buffer de paquetes. Sin embargo, es importante comentar que la técnica WM incrementa el número de establecimientos de ruta en aproximadamente un 40% en comparación con el protocolo original de Marti, y también por tanto la carga de señalización asociada al proceso de descubrimiento de rutas. Se podría conseguir una importante reducción de la carga de señalización de los procesos de enrutamiento inducida por la técnica WM incrementando el tiempo de aislamiento empleado para castigar a los nodos egoístas, lo cual se investigará en futuros trabajos.

IV. Plataforma de Evaluación

A. Escenario de simulación

Se han llevado a cabo simulaciones a nivel de sistema que emulan el funcionamiento de una red inalámbrica *multi-hop* empleando la plataforma de simulación ns2 y la extensión de *Rice Monarch Project* para redes móviles [11]. El entorno de simulación consiste en un escenario tipo Manhattan de 1350x1350m^2, en el cual los nodos se mueven siguiendo el modelo de *Random Walk Obstacle* [12] y que se comunican con la BS situada en el centro del escenario a través de transmisiones *multi-hop*. Los nodos se distribuyen de manera uniforme inicialmente. La densidad de los nodos es de 1 por cada 80 metros de calle, para asegurar el establecimiento de rutas *multi-hop*. Las sesiones de tráfico consisten en transmisiones de tráfico *web* con 5 páginas en promedio por sesión, un tiempo de lectura entre descargas consecutivas de páginas de 30s, 25 objetos por página y un tiempo entre paquetes de 0.028s, tal y como especifica [13]. Con objeto de demostrar los efectos de posibles situaciones de sobrecarga en el canal, un 15% de los nodos en promedio mantiene sesiones activas de tráfico simultáneamente. El interfaz radio *ad-hoc* empleado es el del estándar 802.11a en la banda de 5.8GHz con un nivel de potencia de transmisión de 17dBm.

B. Protocolo de enrutamiento

La comunicación *multi-hop ad-hoc* entre los nodos y la BS se establece utilizando el estándar para redes *mesh* del IEEE 802.11s [14]. El protocolo HWMP (*Hybrid Wireless Mesh Protocol*) es el protocolo de enrutamiento obligatorio definido en el estándar, aunque se especifica que los proveedores pueden optar por operar también usando protocolos alternativos. HWMP combina el protocolo de enrutamiento reactivo AODV (*Ad-hoc On-demand Distance Vector*) [15] con un protocolo de enrutamiento proactivo en árbol. Para evitar una excesiva carga de señalización provocada por la utilización de un protocolo proactivo en un entorno móvil, en este trabajo se ha empleado una versión modificada del protocolo AODV que se comenta a continuación.

El protocolo de enrutamiento AODV solamente busca y establece una ruta cuando un nodo tiene datos para transmitir y no conoce la ruta hacia el nodo destino. En este caso, envía mensajes RREQ (*Route REQuest*) en modo *broadcast*, que son a su vez difundidos por sus nodos vecinos. Cuando el nodo destino recibe el mensaje RREQ, responde con un mensaje RREP (*Route REPly*) en modo *unicast* dirigido al nodo origen para confirmar el establecimiento de ruta. En el protocolo AODV original los nodos intermedios de la ruta, i.e. los nodos entre el nodo origen y el nodo destino, sólo procesan la primera de las réplicas del RREQ que reciben y descartan el resto de réplicas provenientes de rutas alternativas con una mayor latencia. Por consiguiente, la ruta *multi-hop* seleccionada entre el origen y el destino resulta ser la de menor latencia, que generalmente coincide con la que tiene menor número de saltos. En la versión implementada de AODV, los nodos intermedios pueden procesar múltiples réplicas de los mensajes de enrutamiento, para poder emplear la información de reputación en la métrica de selección de ruta. De esta manera, se procesan todos los paquetes y son aceptados aquellos que combinan una ruta libre de egoístas y con una menor latencia. Además, los mensajes de enrutamiento en la versión modificada de AODV incluyen la información de la identidad de todos los nodos participantes en la ruta, necesaria para averiguar si una ruta tiene nodos egoístas o no. Es importante señalar que estas características de la versión de AODV implementada están incluidas en el protocolo de enrutamiento DYMO (*Dynamic MANET On-demand*) [16], que es una versión mejorada del protocolo AODV.

C. Modelo de propagación radio

Para el cálculo del *pathloss* se emplea el modelo de canal para escenario urbano micro-celular propuesto en [17], que utiliza expresiones de *pahtloss* diferentes cuando existen condiciones de visibilidad (LOS *Line Of Sight*) o de no visibilidad (NLOS *Non Line Of Sight*) entre emisor y receptor. El modelo de propagación implementado modela de manera realista el canal radio, al considerar además los efectos del desvanecimiento lento y el desvanecimiento multicamino. El efecto de desvanecimiento multicamino, provocado por la recepción de múltiples réplicas de la señal transmitida en el receptor, se modela según una distribución Ricean en condiciones LOS y según distribución Rayleigh en condiciones NLOS. El desvanecimiento lento, provocado por obstáculos entre emisor y receptor, se modela con una distribución lognormal con una desviación estándar de 3dB y 4dB respectivamente para LOS y NLOS. Además, para la autocorrelación espacial característica del desvanecimiento lento se emplea el modelo de Gudmunson [18].

V. Evaluación de Resultados

Las propuestas de este trabajo tienen como fin mitigar los efectos negativos de la inexactitud del mecanismo de detección *watchdog* empleado por la mayoría de los SPPs basados en reputación, cuando se consideran condiciones realistas de simulación. Con las mejoras presentadas se disminuye el número de acusaciones incorrectas, lo cual incrementa el rendimiento general y la conectividad de la red, debido a la mayor disponibilidad de rutas *multi-hop* conocidas sin nodos egoístas.

La Figura 2 representa algunas estadísticas de rendimiento en cuanto a la recepción y al descarte de paquetes con las técnicas analizadas en este trabajo. El PDR (*Packet Delivery*

Ratio) es un parámetro del rendimiento de la red que mide el porcentaje de paquetes correctamente recibidos del total de paquetes transmitidos. Otros valores estadísticos son el porcentaje de paquetes descartados intencionadamente por nodos egoístas, el porcentaje de paquetes descartados por la inexistencia de rutas sin nodos egoístas conocidos y descartados por caídas de enlaces. Cada grupo de barras en la Figura 2 corresponde a un porcentaje diferente de nodos egoístas. Cada una de las tres barras dentro de un grupo corresponde a una técnica diferente (Marti, RFM y WM). Los números inscritos en el gráfico indican el porcentaje de incremento del PDR conseguido por las propuestas, comparado con el conseguido por la técnica original de Marti. La capacidad para distinguir con exactitud los nodos egoístas de los cooperativos con las técnicas propuestas permite obtener un incremento notable del PDR. Esto se debe al incremento del número de rutas válidas disponibles, especialmente en el caso de la propuesta WM. El incremento del número de rutas válidas disponibles con las técnicas propuestas puede apreciarse en el descenso del porcentaje de paquetes descartados debido a la inexistencia de rutas válidas conocidas ('Sin ruta' en la leyenda). El coste de esta mejora es un aumento leve de aproximadamente un 5% en el porcentaje de paquetes descartados por nodos egoístas en el modo WM. La razón de este incremento está implícita en el funcionamiento de la técnica WM. Cuando el comportamiento egoísta de un nodo retransmisor se detecta, primero se marca como un nodo sospechoso, antes de ser finalmente marcado como egoísta y aislado si continúa descartando paquetes durante el tiempo que esté marcado como sospechoso. No obstante, como se muestra en la Figura 2, el incremento en el número de paquetes descartados por los nodos egoístas, no tiene un gran impacto sobre el PDR. Además, debe señalarse que en los sistemas basados en reputación que utilizan la técnica *watchdog* para observar la retransmisión de los paquetes, la determinación del valor óptimo del umbral máximo de faltas constituye un compromiso entre la rapidez en la detección de nodos egoístas y la tasa de error de las acusaciones de egoísmo. Aunque en este trabajo el valor óptimo de dicho parámetro ha sido fijado mediante simulaciones preliminares, es inevitable que exista un cierto porcentaje de paquetes descartados, ya que la técnica de *watchdog* se basa precisamente en detectar esos descartes de paquetes. Además, un nodo egoísta que ha sido descubierto en una zona determinada del escenario de la red, puede esquivar el aislamiento aprovechándose de la movilidad de los nodos, cambiando su localización. Frente a estos inconvenientes inherentes a las redes MANET y los sistemas basados en *watchdog*, la reducción del porcentaje de paquetes descartados es un importante objetivo en el diseño de SPPs que será tenido en cuenta en futuros trabajos, a través de un mayor intercambio de información de reputación entre los distintos nodos de la red, que permita aislar a los nodos egoístas de manera efectiva.

El incremento del PDR con las técnicas propuestas se debe al descenso del número de acusaciones incorrectas y a la capacidad de seleccionar rutas *multi-hop* sin nodos egoístas. El número de acusaciones incorrectas, representado en la Figura 3(a), se refiere al número de ocasiones en las que un nodo retransmisor no egoísta fue acusado de actuar egoístamente debido a la acumulación de detecciones de descarte incorrectas provocadas por errores de propagación radio y colisiones de paquetes (ver sección II.A). El resultado más destacable es el importante descenso del número de acusaciones incorrectas conseguido con la propuesta WM (mayor del 95%), con respecto a la técnica original de Marti. Esta reducción se debe al funcionamiento de la categoría de nodo sospechoso introducida por la técnica WM, como se explicó en la sección III.A. Los nodos retransmisores que se marcan como sospechosos tienen otra oportunidad de recuperar una buena reputación antes de ser acusados finalmente de actuar de manera egoísta. Además, cabe la posibilidad de que un nodo sospechoso no vuelva a interactuar otra vez con el nodo precursor que le marcó como sospechoso. En ambos casos, no se llega a realizar finalmente la acusación. La razón del descenso del número de acusaciones incorrectas en el caso de la técnica RFM es que cuando se detecta la caída de un enlace antes de que el nodo retransmisor sea acusado de comportarse egoístamente, su reputación es restaurada. De esta forma, se reduce el efecto negativo de los niveles de reputación de las caídas de los enlaces radio.

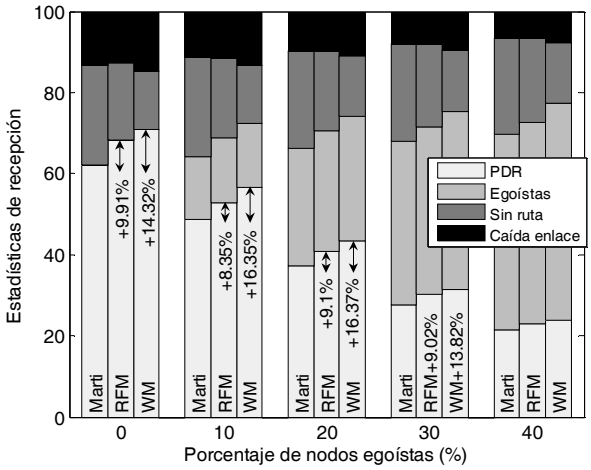

Fig. 2. Estadísticas de recepción de paquetes para las mejoras propuestas.

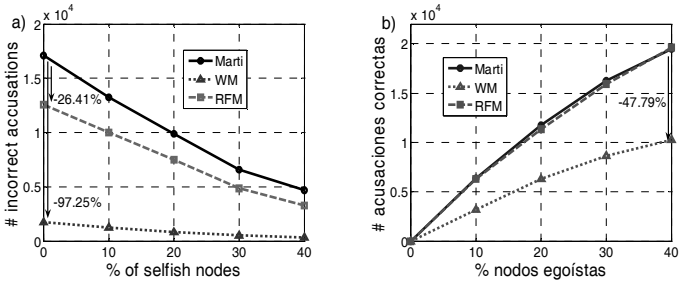

Fig. 3. Número de acusaciones incorrectas (a) y correctas (b)

El número de acusaciones correctas es un parámetro de rendimiento que refleja el número de ocasiones en que un nodo egoísta es acusado. Un mayor número de acusaciones correctas contribuye a incrementar el número de rutas *multi-hop* sin nodos egoístas. La Figura 3(b) refleja que este parámetro se mantiene constante para la técnica RFM respecto a la técnica de Marti, lo que confirma que el proceso de restauración de la reputación en la técnica RFM no beneficia a los nodos egoístas, dado que son acusados rápidamente antes de que un posible evento de caída de enlace sea iniciado. Por otro lado, en la técnica WM se detecta un descenso del número de acusaciones correctas de aproximadamente un 45%, a pesar de que los resultados mostrados en la Figura 2 se aprecia que este descenso no tiene un impacto apreciable sobre el PDR de la técnica WM. Esto

se debe a que, como se ha comentado, los nodos que son marcados como sospechosos posiblemente no vuelven a interactuar con el nodo precursor y por tanto no son finalmente acusados, pero tampoco tienen ocasión para descartar más paquetes.

La Figura 4(a) muestra el número de ocasiones en las que se estableció una ruta *multi-hop* con nodos egoístas, lo cual se conoce como establecimientos de ruta incorrectos. Por otro lado, la Figura 4(b) representa el número de establecimientos de ruta correctos, es decir, de rutas sin nodos egoístas. Se aprecia un incremento notable del número de establecimientos de ruta correctos e incorrectos con la técnica WM. Esto se debe a su propio funcionamiento. En caso de que se observe a un nodo retransmisor actuando de manera egoísta, antes de ser acusado definitivamente, se marca como sospechoso y los enlaces a través del mismo se rompen. Los nodos sospechosos pueden participar otra vez en los procesos de descubrimiento y establecimiento de rutas. Este modo de funcionamiento implica un incremento en el número de rutas establecidas, tanto correctas como incorrectas. Sin embargo, el aumento del número de rutas incorrectas no afecta al PDR apreciablemente, como se muestra en la Figura 2, debido a que los nodos sospechosos son vigilados estrictamente en la técnica WM. La técnica RFM mantiene el mismo número de rutas incorrectas establecidas respecto al protocolo de Marti, e incrementa en un 14% aproximadamente el número de rutas correctas. Esta mejora se debe al hecho de que la técnica RFM reduce el número de acusaciones incorrectas pero mantiene el número de acusaciones correctas, como se aprecia en las figuras anteriores.

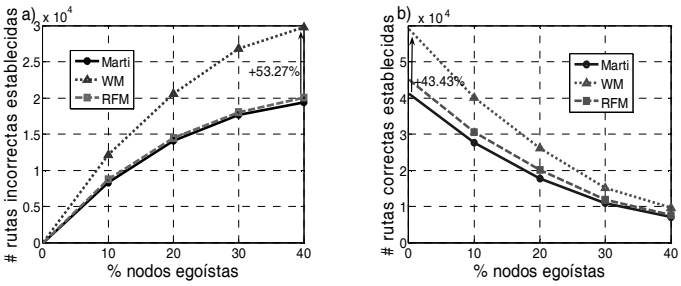

Fig. 4. Número de establecimientos de ruta incorrectos (a) y correctos (b)

En los SPPs basados en reputación, las peticiones de descubrimiento y de establecimiento de ruta son descartadas si el nodo que las recibe detecta que alguno de los nodos que participa en la ruta *multi-hop* es egoísta. El número de rutas correctas descartadas, representado en la Figura 5(a), se refiere al caso en el que realmente ningún nodo egoísta participaba en la ruta denegada. Se aprecia que tanto la técnica WM como la técnica RFM consiguen un notable descenso del número de rutas correctas descartadas, especialmente en el caso de WM. Esto conlleva a una reducción del porcentaje de paquetes descartados por la inexistencia de rutas sin nodos egoístas conocidos y al aumento del PDR que fue comentado en la Figura 2. La reducción del número de rutas correctas negadas se debe una reducción paralela del número de acusaciones incorrectas, tal como se señaló en la Figura 3. Es importante destacar que tanto WM como RFM mantienen un número de rutas incorrectas descartadas similar al del protocolo de Marti, como se muestra en la Figura 5(b). Esto significa que reducir el número de rutas correctas descartadas, lo cual incrementa la disponibilidad de rutas sin nodos egoístas, no se consigue al precio de reducir también el número de rutas incorrectas descartadas, lo cual aumentaría el porcentaje de paquetes descartados por nodos egoístas y reduciría por consiguiente el PDR.

La utilización simultánea de las técnicas WM y RFM propuestas es posible, ya que han sido implementadas de manera modular. Los resultados preliminares obtenidos al respecto indican que al ser ejecutadas simultáneamente, se obtiene un mayor incremento del número rutas correctas disponibles, con una mejora del PDR mayor que la conseguida con las técnicas empleadas por separado. Sin embargo, los resultados completos no han podido ser incluidos en la presente comunicación debido a restricciones temporales.

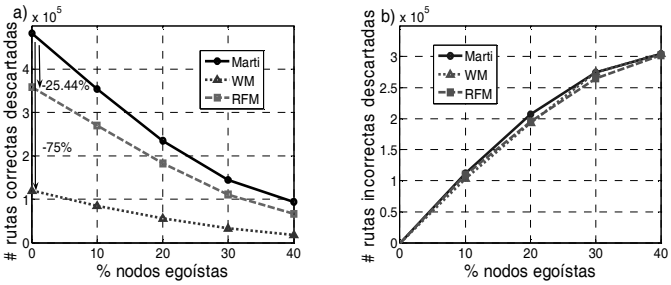

Fig. 5. Número de rutas (a) correctas e (b) incorrectas descartadas

VI. CONCLUSIONES

Este trabajo ha presentado dos técnicas de mejora del mecanismo básico de detección *watchdog* empleado en la mayoría de los protocolos de prevención de egoísmo para redes móviles cooperativas basados en reputación. Los SPPs basados en reputación tienen como objetivo detectar y aislar a los nodos egoístas que no participan en la retransmisión de los paquetes de otros nodos, pero que se benefician de la retransmisión de sus propios paquetes por parte de otros nodos. Resultados anteriores demostraban la inexactitud de la técnica *watchdog* en la detección de nodos egoístas y sus efectos negativos sobre el rendimiento de SPPs basados en reputación cuando se evaluaban en condiciones de simulación realistas. La técnica de *watchdog* sobrestima el egoísmo de los nodos al confundir las colisiones de los paquetes y los errores del canal radio con descartes intencionados de paquetes de datos. Para mitigar las consecuencias de esta inexactitud, este trabajo propone dos técnicas que mejoran la capacidad de los SPPs para detectar correctamente a los nodos egoístas y reducen el número de acusaciones incorrectas. Como se ha mostrado, las técnicas propuestas incrementan la disponibilidad de rutas *multi-hop* libres de nodos egoístas y por consiguiente aumentan también el PDR y la conectividad de las redes cooperativas *multi-hop*.

AGRADECIMIENTOS

Este trabajo ha sido financiado por el Ministerio de Ciencia e Innovación, el Ministerio de Industria y Comercio y fondos FEDER a través de los proyectos TEC2008-06728 y TSI-02400-2008-113 y por la Generalitat Valenciana a través de la ayuda con referencia BFPI/2007/269.

REFERENCIAS

[1] Recommendación ITU-R M.1645 – "Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000".

[2] Y. Lin y Y. Hsu, "Multi-hop Cellular: a new architecture for wireless communications," *Libro de Actas del IEEE Computer Communications (INFOCOM)*, pp. 1273-1282, Mar. 2000, Israel.

[3] X. J. Li, B.-C. Seet y P. H. J. Chong, "Multihop cellular networks: Technology and economics," *Computer Networks*, Elsevier, vol. 52, No. 9, pp. 1825-1837, Jun. 2008.

[4] S. Buchegger, J. Mundinger y J.-Y. Le Boudec, "Reputation systems for self-organized networks," *IEEE Technology and Society Magazine*, vol. 27, núm. 1, pp. 41-47, Primavera 2008.

[5] Y. Yoo y D.P. Agrawal, "Why does it pay to be selfish in a MANET?," *IEEE Wireless Communications Magazine*, vol. 13, núm. 6, pp. 87-97, Dic. 2006.

[6] S. Marti, T. J. Giuli, K. Lai y M. Baker, "Mitigating routing misbehavior in mobile ad-hoc networks," *Libro de Actas del International Conference on Mobile Computing And Networking ACM (MobiCOM 2000)*, pp 255-265, 2000.

[7] A. Rodriguez-Mayol y J. Gozalvez, "On the Implementation Feasibility of Reputation Techniques for Cooperative Mobile Ad-hoc Networks," *Libro de Actas del European Wireless Conference EW2010*, Abr. 2010.

[8] K. Balakrishnan, J. Deng y V.K. Varshney, "TWOACK: preventing selfishness in mobile ad hoc networks," *Libro de Actas del IEEE Wireless Communications and Networking Conference* WCNC 2005, vol. 4, pp. 2137-2142, Mar. 2005.

[9] M.T. Refaei, Y. Rong, L.A. DaSilva y H. Choi, "Detecting Node Misbehavior in Ad hoc Networks," *Libro de Actas del IEEE International Conference on Communications ICC 2007*, pp. 3425-3430, Jun. 2007.

[10] S. Buchegger, C. Tissieres y J.Y.Le Boudec, "A test-bed for misbehavior detection in mobile ad-hoc networks," *Libro de Actas del IEEE Workshop on Mobile Computing Systems and Applications WMCSA,* pp.102 – 111, Dic. 2004.

[11] Rice Monarch Project "Wireless and mobility extensions to ns-2," http://www.monarch.cs.rice.edu/cmu-ns.html

[12] K. Maeda, A. Uchiyama, T. Umedu, H. Yamaguchi, T. Higashino, "Urban pedestrian mobility for mobile wireless network simulation," *Ad Hoc Networks, Elsevier*, vol. 7, núm. 1, pp. 153–170, 2009.

[13] UMTS 30.03 v3.2.0 TR 101 112 "Selection procedures for the choice of radio transmission technologies of the UMTS," ETSI, Apr. 1998.

[14] IEEE P802.11s/D2.0, borrador de corrección del estándar IEEE 802.11: Mesh Networking, *IEEE Standard*, 2007.

[15] C. Perkins y E. Royer, "Ad hoc On-Demand Distance Vector Routing," *Libro de Actas del IEEE Workshop on Mobile Computing Systems and Applications* (WMCSA), pp. 90-100, 1999.

[16] I. D. Chakeres y C. E. Perkins, "Dynamic MANET on-demand (DYMO) Routing," draft-ietf-manet-dymo-05, Internet Draft, Jun. 2006.

[17] WINNER, "DI. 1.1. WINNER II interim channel models," *Public Deliverable*, http://www.ist-winner.org/

[18] M. Sepulcre y J. Gozalvez, "On the importance of radio channel modeling for the dimensioning of wireless vehicular communication systems," *Libro de Actas del International Conference on ITS Telecommunications 2007*, ITST '07, pp 1–5, Jun. 2007.