Implementación de Técnicas de Reputación en Redes MANET Cooperativas

Alberto Rodriguez-Mayol y Javier Gozálvez

Uwicore, *Ubiquitous Wireless Communications Research Laboratory* http://www.uwicore.umh.es
Universidad Miguel Hernández de Elche. Avda de la Universidad, s/n, 03202 Elche, España.
f.rodriguez@umh.es , j.gozalvez@umh.es

***Abstract* — Some trends in the research of future 4G mobile networks explore the issue of different radio access technologies running in the same network and available for the user in a transparent manner. MCN-MR (Multi-hop-Cellular Networks – Mobile Relay) networks seem to be a winner technology in flexibility, availability and low deployment and management cost. Nevertheless, individual users' cooperation is needed to retransmit the packets of other nodes, and consequently some techniques to persuade the nodes not to behave selfishly will be needed. This work focuses on the study of two cooperation system proposals in realistic scenarios and emphasizes the importance of some determining factors like the use of realistic channel propagation models, the size of the simulation field, transmission power and selfishness detection capability that have been ignored in the literature so far.**

I. Introducción

Mientras los dispositivos de comunicaciones inalámbricas comerciales actuales ya disponen de acceso a distintos sistemas de comunicaciones (WiFi, GSM, GPRS-EDGE, UMTS, etc.), a través de sus correspondientes interfaces radio, en el ámbito de la investigación se camina ya hacia la cuarta generación de comunicaciones móviles. Si bien todavía no hay un consenso absoluto en el concepto de la futura tecnología *Beyond 3G*, sí es cierto que incluirá y perfeccionará esta hibridación de tecnologías de acceso radio. El concepto de redes MCN (*Multi-hop-Cellular Networks*) nace a partir de esta filosofía, con el propósito de aunar las características complementarias de Wifi, muy popular y con altas velocidades de transmisión de datos, pero de corto rango, con las de las redes celulares, que ofrecen un despliegue universal. En este tipo de redes, el uso de múltiples saltos en la transmisión reduce la distancia de comunicación de cada salto, y por tanto las pérdidas de propagación, permitiendo proveer de altas tasas de transmisión a los nodos más alejados de las estaciones base, que son los más perjudicados en los sistemas celulares tradicionales. Dentro de las redes MCN, se han identificado dos variantes: los sistemas MCN-FR (*Multi-hop Cellular Network Fixed Relay*) y MCN-MR (*Multi-hop Cellular Network Mobile Relay*). MCN-FR emplea estaciones fijas para las transmisiones multi-hop, mientras que MCN-MR utiliza como retransmisores los propios terminales del usuario. Los sistemas fijos tienen como ventaja un bajo coste de diseño, dado que la funcionalidad de las estaciones estaría limitada a la recepción, regeneración y retransmisión de la señal. Sin embargo, el despliegue de nuevas estaciones supone un coste elevado, además de la polémica existente respecto a los efectos sobre la salud de la radiación electromagnética. Por su parte, los sistemas móviles destacan por su flexibilidad, su gran disponibilidad y bajo coste. Sin embargo, dado que MCN-MR utiliza el terminal móvil del usuario como retransmisor, plantea la cuestión de qué sistema emplear para incentivarle a prestar sus propios recursos, tales como la batería del terminal, para el beneficio del conjunto de toda la red. En la literatura sobre redes MANET se han propuesto distintos sistemas para combatir los efectos negativos del egoísmo de los nodos. En esta línea, este trabajo analiza distintas técnicas de incentivo a cooperación propuestas, teniendo en cuenta todos los factores que pueden afectar tanto a la conectividad como a la capacidad de detección de nodos egoístas, factores que no han sido suficientemente estudiados anteriormente [3]. Se han realizado lotes de simulaciones que comparan el comportamiento de dos de estos sistemas de cooperación, TEAM y WD, frente al comportamiento de la red sin ningún tipo de sistema de prevención de egoísmo (SPP *Selfishness Prevention Protocol*).

II. Egoísmo en redes MCN-MR

Tradicionalmente, los sistemas de incentivo a la cooperación han sido aplicados a redes MANET, donde las principales funciones de creación, gestión y mantenimiento de la red, deben ser desempeñadas de manera distribuida por los nodos móviles que la componen. Ante la ausencia en estas redes de una autoridad central confiable, se hace necesario implementar mecanismos de seguridad que permitan mantener a raya a posibles nodos maliciosos que puedan amenazar el funcionamiento correcto de la red [4]. Parte de la investigación sobre SPP realizada en torno a redes MANET puede extenderse a redes MCN-MR. La estructura de este tipo de redes puede dividirse en dos partes que funcionan coordinadamente: por un lado, la parte celular cuya gestión centralizada recae sobre las estaciones base celulares y el núcleo de la red, y por otro lado la parte *multi-hop*, en donde ciertas tareas tales como la búsqueda, selección y mantenimiento de nodos vecinos y de rutas se deben realizar de manera distribuida, y donde la vigilancia de la seguridad cobra gran importancia, ya que la conectividad *multi-hop* puede verse seriamente afectada por el comportamiento egoísta o malicioso de los nodos. Uno los ataques más comunes en redes MCN-MR, en las que cada nodo debe buscar una ruta *multi-hop* hacia la estación base, es el denominado "*packet dropping*". En este ataque los nodos participan en los procesos de establecimiento y mantenimiento de rutas, para poder enrutar sus propios paquetes en caso necesario, pero llegado el momento se niegan a retransmitir los paquetes de los demás nodos, bien para ahorrar el preciado recurso de la batería del terminal o bien por la desconfianza de cara al usuario que puede generar esta tecnología inicialmente [1]. Aunque existen otros posibles ataques, el presente trabajo se centra exclusivamente en el de "*packet dropping*", ya que los

usuarios pueden percibir que existe una motivación importante en la preservación de la batería que no se da en otro tipo de ataques más sofisticados, los cuales sólo pueden ser realizados por usuarios expertos.

Los SPP se pueden clasificar en tres grandes categorías [3]: sistemas de reputación, de crédito y basados en teoría de juegos. Por un lado, los esquemas basados en crédito consisten en el comercio de derechos y obligaciones de retransmisión de paquetes y colaboración empleando cierta divisa, que puede ser real o virtual. Este tipo de sistemas están limitados por la necesidad de disponer de una entidad central de administración, así como de un sistema a prueba de falsificaciones y de una aplicación universal en todos los nodos de la red. Por otro lado, los estudios basados en teoría de juegos tratan de analizar las estrategias de los usuarios, a partir de modelos de redes muy simplificados. A pesar de que dichos modelos permiten extraer conclusiones interesantes, se basan en asunciones que no se ajustan suficientemente a la realidad. Por las razones anteriores este trabajo se centra en los SPP basados en reputación, en los que cada nodo observa el comportamiento de sus nodos vecinos en cuanto a su colaboración en las tareas de enrutamiento y retransmisión de paquetes, y utiliza esta información para excluir a aquellos que hayan exhibido un mal comportamiento en el proceso de búsqueda de ruta. La mayoría de estos sistemas se basan en la técnica *watchdog* de observación promiscua de paquetes introducida por primera vez en [1], ya que su implementación es totalmente distribuida y sólo necesita que el terminal disponga de la capacidad de escucha en modo promiscuo. De entre los sistemas de reputación propuestos, en este trabajo se han seleccionado dos: en primer lugar, el sistema WD [1] por ser la primera y más sencilla de las aportaciones, con el propósito de comparar su funcionamiento respecto a otra técnica más sofisticada denominada TEAM [2]. También se comparará el rendimiento de estas dos técnicas con el de la red funcionando sin ningún SPP, y una técnica idealista, denominada PD (*Perfect Detection*), implementada como límite superior de rendimiento a modo comparativo. PD asume que en todo momento la información sobre la identidad de los nodos y su egoísmo está disponible para cualquier nodo, en otras palabras, que el sistema de detección de egoístas es perfecto.

III. TÉCNICAS IMPLEMENTADAS

El primero de los sistemas implementados, denominado en este trabajo como WD, fue presentado por primera vez en [1]. Consiste en dos extensiones que se ejecutan por encima del protocolo de enrutamiento DSR: *watchdog* y *pathrater*. *Watchdog* es una técnica de vigilancia promiscua que comprueba la correcta retransmisión de los paquetes por parte de los nodos vecinos. Supongamos que cierto paquete debe atravesar la secuencia de nodos S, B, C y D para llegar del origen S al destino D. El nodo S, sabiendo que B debe retransmitirlo hacia C, almacenará el paquete en el buffer local al mismo tiempo que lo retransmite a B. De esta manera, quedará a la espera de escuchar la retransmisión del paquete desde B a C dentro de un cierto tiempo límite. Si pasado ese tiempo, no se ha escuchado la retransmisión por parte de B, entonces el nodo S anota una falta al nodo B. Cada nodo lleva un registro de las faltas observadas de aquellos nodos con los que ha interaccionado. Cuando la cuenta del número de faltas supera cierto umbral, dicho nodo es tachado como egoísta y será evitado en todo establecimiento de ruta posterior durante un cierto tiempo, tras el cual podrá ser reintegrado. Además, se notifica mediante un mensaje al nodo origen sobre la rotura del enlace y el mal comportamiento del nodo. Por otro lado, la extensión *pathrater* puede ser ejecutada en paralelo al *watchdog* y utiliza la información facilitada por éste para mantener una tabla de reputación de todos los nodos vecinos con los que se establece algún contacto. En dicha tabla se asigna una puntuación de reputación a cada nodo en función de su participación en el enrutamiento de los paquetes del nodo con unas sencillas reglas. Para seleccionar una ruta entre varias alternativas, se escogerá aquella que obtenga un mayor promedio, o sea, la que a priori sea la más confiable por haberse detectado menos comportamientos anómalos [1].

Si bien WD consigue evitar en un alto porcentaje de casos aquellas rutas que tienen egoístas, tiene una serie de inconvenientes. En primer lugar, su política no castiga al nodo egoísta para incentivarlo a colaborar, sino que sólo lo evita en sus rutas, lo cual resulta incluso beneficioso para el egoísta, que evita tener que transmitir paquetes para los demás. Además, existen algunos problemas [1] que afectan negativamente al funcionamiento correcto de *watchdog*, tales como colisiones en el nodo origen, colisiones del paquete en el nodo destino, falsas acusaciones, etc. Estos problemas han motivado un proceso de perfeccionamiento del protocolo WD a través de la literatura hasta hoy, en distintas adaptaciones de sistemas de reputación [3]. En este trabajo se ha implementado el sistema TEAM propuesto en [2], que emplea como técnica de vigilancia básica el *watchdog* pero establece una serie de mejoras tales como la reducción del excesivo *overhead* causado por los mensajes de acusación en WD y una detección más rápida de los egoístas, mediante la inclusión de tres tipos de reputación: reputación directa, reputación observada, y reputación recomendada. El nodo no vigila únicamente que los demás nodos retransmitan correctamente los paquetes de los cuales es origen (reputación directa), sino que vigila que cada nodo de su entorno retransmita todos los paquetes que le llegan, independientemente del origen del paquete (reputación indirecta). Por otro lado, el sistema de reputación recomendada consiste en analizar la secuencia de nodos que ha atravesado el paquete correspondiente desde el origen y en función de ciertas reglas, asignar a cada uno de los nodos de la ruta del paquete cierto incremento en su reputación recomendada. Este sistema está basado en la asunción de que si un nodo retransmite un paquete procedente de otro nodo es porque confía en que dicho nodo no es egoísta, y por tanto, está recomendando implícitamente dicho nodo al aceptar retransmitir sus datos. TEAM utiliza los tres tipos de valores de reputación del nodo (directa, observada y recomendada) para obtener la confianza en dicho nodo, mediante una fórmula de ponderación que atribuye más importancia a la reputación directa y menos a la indirecta y la recomendada [2]. La información de la confianza en un nodo es empleada por TEAM para tomar decisiones sobre distintas funciones de enrutamiento tales como aceptar o no un paquete de búsqueda de ruta y retransmitir o no los paquetes de otro nodo.

IV. ESCENARIOS DE SIMULACIÓN Y MODELOS DE CANAL

El presente estudio ha sido desarrollado empleando la plataforma de simulación ns2 (*Network Simulator* v.2). Sobre un escenario tipo Manhattan con un número variable de dimensiones (900x900m^2, 1350x1350m^2 y 1800x1800m^2, con número de nodos 114, 238 y 406 respectivamente). En este escenario, los nodos se desplazan siguiendo un modelo de movilidad '*Random Walk Obstacle*'. La densidad espacial es de un nodo cada 80 metros, aproximadamente. La existencia de edificios no sólo restringirá el movimiento de los nodos a determinadas direcciones, sino que además, influirá notablemente en el desempeño del sistema cuando se empleen modelos de canal que tengan en cuenta las condiciones de visibilidad reales y su efecto en la propagación de la señal. La tecnología de acceso radio empleada por los nodos es 802.11a a 5.8GHz, con una potencia de transmisión de 17dBm y 20dBm, utilizando una tasa de transmisión de 12Mbps. El modelo de tráfico sigue un patrón a ráfagas, consistente en sesiones de 150 segundos. Cada sesión se compone de periodos de actividad (ON) de duración 0.5 segundos y periodos de inactividad (OFF) de 29.5 segundos. Dado que el efecto de negativo de la congestión sobre la técnica de detección *watchdog*, señalado en [1], es motivo de controversia en [7], se han realizado dos tipos de simulaciones en cuanto al tráfico para estudiar el efecto de la congestión por separado. En el primero se evita el efecto de la congestión provocando que cada nodo inicie su sesión cuando el anterior haya terminado la suya, en sesiones no simultáneas. En el segundo tipo de tráfico, con sesiones simultáneas, diferentes nodos pueden iniciar sus sesiones aunque otros nodos tengan sesiones en curso.

Uno de los aspectos más importantes que cabe mencionar es el del protocolo de enrutamiento utilizado. Como ya se ha comentado, la práctica totalidad de los SPP basados en reputación necesitan ser implementados sobre un protocolo de enrutamiento en origen tipo DSR (*Dynamic Source Routing*). Estos protocolos tienen dos características que los hacen adecuados para el empleo de sistemas de reputación: primero, los paquetes de búsqueda y establecimiento de ruta (RREQ *Route Request* y RREP *Route Reply* respectivamente) contienen toda la secuencia de nodos que atraviesa el paquete, de manera que el nodo vigilante puede saber si el paquete debe ser retransmitido o no por el siguiente nodo; segundo, todos los nodos registran en su tabla local de enrutamiento varias rutas hacia un mismo destino pero es exclusivamente el nodo origen el que escoge finalmente la ruta. Por contra, en los protocolos tipo AODV, la selección de ruta se hace nodo a nodo, es decir, en cada nodo se registra únicamente una ruta, y se descartan el resto de paquetes de enrutamiento procedentes de rutas alternativas. Además, no es necesario registrar toda la secuencia de nodos de la ruta en la tabla de rutas, bastando con anotar el destino y el siguiente nodo. A pesar de que tradicionalmente se ha empleado DSR en los sistemas de reputación, hemos considerado más conveniente emplear una versión modificada de AODV. La razón es que, en el estándar de redes inalámbricas *mesh* 802.11s se especifica como protocolo de enrutamiento obligatorio el HWMP (*Hybrid Wireless Mesh Protocol*), el cual está inspirado en una combinación de un protocolo proactivo y un protocolo reactivo tipo AODV. De esta manera, en este trabajo se ha empleado una adaptación del protocolo AODV implementado en ns-2 en la extensión del Monarch Project [8] para que pueda ser utilizado con los sistemas WD y TEAM. Esta adaptación ha consistido en incluir la identidad de los nodos de la ruta en los paquetes de enrutamiento, tal y como se hace en el protocolo DYMO [9], que es una evolución del protocolo AODV. Además, se permite el procesamiento de varios mensajes de enrutamiento, con el objetivo de que existan varias alternativas entre las que seleccionar la ruta, lo cual es otra de las modificaciones ya incluidas en el protocolo HWMP.

Se emplean tres modelos distintos de canal. El modelo más simple es el de 2 rayos, que predice las mismas pérdidas que el modelo de espacio libre hasta cierta distancia crítica, a partir de la cual, las pérdidas tienen una dependencia de orden cuatro con la distancia (d^4). Frente a este modelo que no tiene en cuenta las condiciones reales de visibilidad entre emisor y receptor, este trabajo incluye otro más realista extraído del modelo urbano micro-celular desarrollado en el proyecto europeo WINNER [5]. Este modelo es uno de los más completos para entornos urbanos, y en el que se considera una menor altura de la antena de la BS, y que sí tiene en cuenta la diferencia entre condiciones de visión directa (LOS – *Line-of-Sight*) o NLOS (*Non Line-of-Sight*) y por ello lo denominaremos LOS-NLOS. El tercero de los modelos, extraído de [6], es similar al LOS-NLOS pero además tiene en cuenta los siguientes efectos del canal radio: la correlación espacial del desvanecimiento lento y las perturbaciones provocadas por la componente de multi-trayecto sobre el nivel de potencia recibida. Este tercer modelo se denominará en lo sucesivo modelo Realista. La principal diferencia entre los dos últimos y el primero, además de tener un menor alcance, es que aquéllos consideran las condiciones de visibilidad entre emisor y receptor, lo cual conlleva a que las distancias recorridas por los paquetes sean en promedio mayores, y por tanto, las rutas estén compuestas por un número mayor de saltos, factor que degrada considerablemente el funcionamiento de la red en presencia de nodos egoístas, como se verá.

V. RESULTADOS

El diagrama de la figura 1 sintetiza los principales resultados obtenidos en este trabajo, que serán discutidos en esta sección. En la parte izquierda de la figura se muestran diferentes parámetros con repercusión sobre la conectividad de la red: el porcentaje de nodos egoístas, el protocolo de prevención de egoísmo, la potencia de transmisión, el modelo de propagación y el tamaño del escenario y el efecto de la congestión. Se resume además la influencia de estos parámetros de entrada sobre algunos importantes factores del rendimiento de la red, como la conectividad, el porcentaje de detecciones falsas del SPP, la consideración de valores específicos para los parámetros de propagación en condiciones de no visibilidad por parte del modelo de canal, la distancia de salto, la distancia total entre emisor y receptor y el número de saltos por transmisión, utilizando para ello los signos "+" y "-". Por ejemplo, si se incrementa el porcentaje de nodos egoístas, habrá más detecciones pero también menos conectividad, o si se aumenta la potencia de transmisión, aumentará la distancia de salto, como se muestra en los resultados.

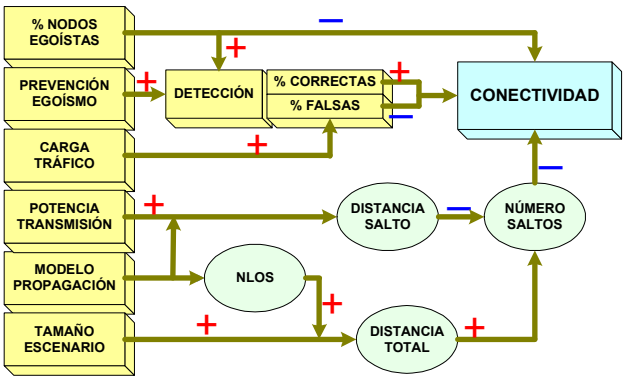

Figura 1: Factores conectividad en redes MCN-MR

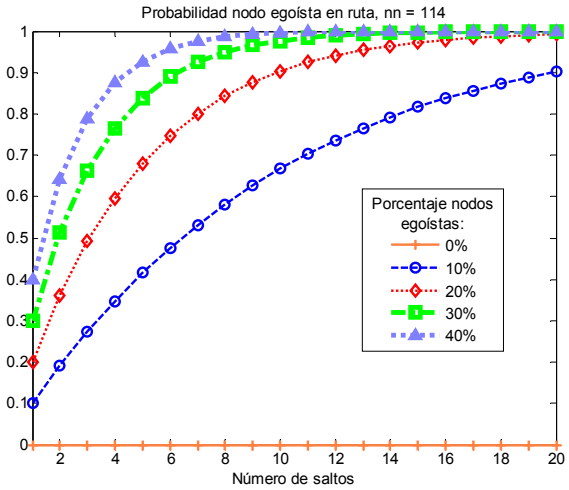

Figura 2: Factores conectividad en redes MCN-MR

Cabe destacar en la figura 1 el hecho de que la existencia de nodos egoístas en la red afecta considerablemente a la conectividad. Por un lado, la mayor ventaja de la tecnología multi-hop consiste precisamente en la posibilidad de realizar transmisiones en *multi-hop* para evitar el bajo rendimiento de recorrer largas distancias con un solo salto. Por otro lado, la conectividad de un enlace *multi-hop* depende de la estabilidad de cada uno de los enlaces, y por tanto la presencia de nodos egoístas puede ser muy negativa, ya que la existencia de un único nodo egoísta en una ruta la convierte en inservible. Para apreciar esto se muestran en la figura 2 varias curvas que relacionan el número de saltos de la ruta con la probabilidad de encontrar un nodo egoísta en la misma, para distintos porcentajes de nodos egoístas. Incluso para un número de saltos bajo como 2 o 3 y un porcentaje de nodos egoístas de sólo el 20%, la probabilidad de encontrar una ruta sin nodos egoístas se reduce considerablemente. La figura 2 se ha elaborado a partir de la ecuación (1), en la que P representa la probabilidad de encontrar una ruta con algún nodo egoísta, ns es el número de saltos, nn el número de nodos y $pns1$ es el porcentaje de nodos egoístas. Se asume que no se considera ningún SPP en el proceso de selección de ruta, es decir, todas las rutas tienen la misma probabilidad de ser seleccionadas, independientemente del número de nodos egoístas que contenga.

$$P = 1 - \prod_{i=1\ldots ns} \frac{\lfloor nn(1-pns1)\rfloor - i + 1}{nn - i + 1} \qquad (1)$$

A continuación se explora la influencia de los diferentes factores mencionados en la figura 1. En primer lugar, examinaremos los efectos de considerar modelos realistas de propagación frente al modelo comúnmente utilizado de 2 Rayos. Se considera un escenario de referencia de tamaño 1350x1350m^2 y potencia de transmisión de 17dBm, en el que se empleará el protocolo AODV sin aplicación de ningún SPP. La tabla I muestra el incremento de un 25% en la distancia total recorrida por los paquetes recibidos correctamente, sin nodos egoístas, empleando el modelo LOS-NLOS o el modelo Realista. También se muestra el efecto de aumentar el porcentaje de nodos egoístas (20% y 40%), que disminuye la conectividad por la pérdida de los paquetes procedentes de nodos alejados. En el modelo realista, el descenso en la distancia total es de un 33% (de 705m para 0% de egoístas a 470m para 40%). Por otro lado, la distancia total también depende del tamaño del escenario. Tomando como referencia el escenario realista de 1350m de lado, la distancia desciende un 31% si se reduce el lado a 900m, mientras que aumenta un 29% en el escenario de 1800m. Aunque este resultado es obvio, nos permite justificar el descenso en el rendimiento para los nodos más alejados en el escenario grande con alta tasa de egoístas.

TABLA I: DISTANCIA TOTAL TRANSMISIÓN (M)

Lado (m)	Modelo canal	% nodos egoístas		
		0	20	40
1350	2 Rayos	**555.21m**	**526.27m**	**489.95m**
	LOS-NLOS	689.64m (+24.2%)	559.01m (+6.2%)	446.53m (-8.9%)
	Realista	705.41m (+27.1%)	600.57m (+14.1%)	470.94m (-3.9%)
900	Realista	482.57m (-31.6%)	420.74m (-30.0%)	369.85m (-21.5 %)
1800	Realista	913.63m	706.78m	512.32 m

TABLA II: DISTANCIA SALTO (M)

Distancia salto (m)	Potencia (dBm)	Modelo canal		
		2 Rayos	LOS-NLOS	Realista
Promedio	17	**301.38**	**166.75** (-44-6%)	**171.89** (-43.0%)
	20	400.90 (+33,0%)[b]	189.89 (+13.8%)	198.12 (+15.3%)
Percentil 95	17	**403.70**	**260.87** (-35.4%)	**300.27** (-25.6%)
	20	546.46 (+35.4%)[b]	295.11 (+13.1%)	352.09 (+17.3%)

Tal y como era esperable, los modelos de canal realistas también reducen la distancia de salto. El valor medio de la distancia de salto para los paquetes recibidos correctamente, se reduce en un 44%, así como también la distancia de salto correspondiente al percentil 95, en un 35% y 25% para LOS-NLOS y Realista, como se muestra en la tabla II, tomando como referencia el modelo de 2 Rayos. Por otro lado, un incremento de 3dB en la potencia aumenta la distancia de salto en un 33% para el modelo de 2 Rayos mientras que en el resto el aumento es más moderado (en torno a un 14%). Un incremento similar se puede apreciar en la tabla II para el percentil 95. La combinación de una distancia total a recorrer por los paquetes mayor y una distancia de salto menor en los modelos realistas, da como resultado un aumento considerable en el número de saltos promedio de las rutas establecidas y el número de saltos promedio por paquete recibido correctamente. En el caso de no aplicar ningún SPP y sin nodos egoístas, el aumento es de 2.27 a 4.97 y 4.81, como se muestra en la tabla III. El aumento relativo es similar para el sistema WD y también para el sistema PD. Otro efecto derivado del incremento del porcentaje de nodos egoístas, desde 0% hasta 40%, es el descenso en el número de saltos promedio de los paquetes recibidos correctamente. Esto se debe a que en las rutas largas hay más probabilidad de encontrar un nodo egoísta, y por tanto la ruta o bien será descartada en caso de que se aplique algún SPP o bien los paquetes serán descartados por el nodo egoísta y no contabilizados en caso contrario. En el modelo 2 Rayos este descenso no es relativamente muy notable, de 2.05 saltos a 1.80, lo que supone un -12.2%, mientras que en el modelo Realista esta caída es mucho más acusada, de 4.61 a 2.75 saltos, un -40.35%.

TABLA III: NÚMERO DE SALTOS PROMEDIO DE RUTA ESTABLECIDA Y POR PAQUETE RECIBIDO

SPP	Modelo canal	Número promedio de saltos por ruta establecida	Número promedio de saltos por paquete		
			0%	20%	40%
sin SPP	2 Rayos	**2.27**	2.05	1.93	1.80
	LOS-NLOS	4.97 (+118.94%)	4.47	3.43	2.64
	Realista	4.81(+111.89%)	4.61	3.62	2.75
WD	2 Rayos	**2.33**	2.03	1.99	1.99
	LOS-NLOS	4.98(+113.84%)	4.48	4.06	3.60
	Realista	5.06(+117.09%)	4.61	4.22	3.89

Una vez que se ha examinado la influencia de los parámetros de dimensionamiento en el número de salto de las rutas y la conectividad, a continuación se discutirá la capacidad de detección de los sistemas TEAM y WD. Según la figura 1, los porcentajes de detecciones correctas y erróneas son dos importantes parámetros del rendimiento del sistema de detección y prevención de egoísmo, que influyen directamente en la conectividad sin estar relacionados directamente con el número de saltos de las transmisiones. En este trabajo definimos dos parámetros que caracterizan la capacidad de discriminación de nodos egoístas: tasa de sensibilidad positiva, y tasa de error positiva. Aplicado a la técnica *watchdog* de escucha promiscua de retransmisiones de paquetes, tenemos las siguientes definiciones, plasmadas en la ecuación (2): la sensibilidad positiva S_+ es el porcentaje de detecciones verdaderas de paquetes descartados (*RDD Real forwarding Denials Detections*) frente al número de veces que un nodo egoísta ha sido requerido para retransmitir paquetes (*RSN Requests for Selfish Nodes*); mientras que la tasa de error positiva E_+ es el porcentaje de ocasiones en que una verdadera retransmisión se interpretó como un falso descarte de paquetes (*FDD False Denials Detections*) frente al número de ocasiones que se solicitó una retransmisión a un nodo no egoísta (*RNSN*). Análogamente, podrían definirse una sensibilidad negativa S_- (capacidad de detección de nodos no egoístas) y una tasa de error negativa E_- (porcentaje de error en la detección de nodos egoístas). Sin embargo, por restricciones de espacio y dado que son parámetros complementarios en el sentido de que $S_+ + E_- = 1$ y $S_- + E_+ = 1$, sólo nos ocuparemos de las dos primeras. Además se puede definir un parámetro de eficacia de detección D que resuma la capacidad de detección básica del protocolo en un escenario determinado, como la razón logarítmica entre la capacidad de detección de egoístas y el error en la detección.

$$S_+ = RDD/RSN \quad E_+ = FDD/RNSN \qquad (2) \qquad D = 10 * \log\left(S_+/E_+\right) \qquad (3)$$

Estos parámetros se han comparado en los siguientes escenarios, en la tabla IV: el primero, 238 nodos, potencia 17dBm, con sesiones no simultáneas y modelo de canal 2 rayos, el escenario 2 es idéntico pero con sesiones no simultáneas y canal Realista, el escenario 3 con sesiones simultáneas y canal Realista, el escenario 4 reduce las dimensiones a 114 nodos, y el escenario 5 donde se aumenta la potencia a 20dBm, para los dos algoritmos WD y TEAM examinados (ya que sobre los protocolos AODV o PD no es posible definir estos parámetros, bien porque no realizan detecciones como en AODV o bien porque no las necesitan, al conocerse ya de antemano la identidad de los egoístas como en PD). Ambos protocolos tienen una buena S_+ en el primer

escenario, cercana al 100%. Además, TEAM mantiene esta buena S_+ en todos los escenarios. Esto quiere decir que casi todas retransmisiones que no han sido realizadas por nodos egoístas han sido detectadas por la técnica *watchdog*. Por otro lado, en el primer escenario, WD obtiene una tasa de error E_+ del 4.85%, mientras que TEAM sufre un error E_+ casi nueve veces superior. Esto reduce el parámetro D, con un valor de 30.12 en WD y 8.72 en TEAM. La alta E_+ en TEAM, que se da en todos los escenarios, se traduce en que en un gran número de ocasiones en las que un nodo no egoísta realiza correctamente la retransmisión, esto no es detectado por el sistema. Sin embargo, se ha podido constatar en los resultados, que la mayoría de estos errores se deben a la consideración de reputación indirecta en TEAM, la cual es más inexacta debido a que la vigilancia en la retransmisión de los paquetes puede en ocasiones realizarse sobre nodos que no están en el rango del nodo vigilante, y por tanto no será posible contabilizar la correcta retransmisión. Además, el impacto real de esta inexactitud sobre la tasa de acusaciones erróneas no es tan alto como podría esperarse, debido a que la reputación indirecta debe estar ponderada según TEAM por debajo de la reputación directa [2] (ver sección III). Comparando el segundo escenario con el primero, vemos que la elección de un canal realista reduce el rendimiento no sólo debido a los factores antes mencionados, que aumentan el número de saltos, o a factores ajenos a la problemática de nodos egoístas, sino que también afecta directamente a la capacidad de detección de los protocolos. En concreto, en WD, S_+ desciende un 5% y E_- aumenta un 6%. Por su parte, en TEAM S_+ sigue siendo muy buena pero el error aumenta más de un 20%, reduciendo drásticamente el parámetro D. Esto quiere decir que hay más nodos que son tachados como egoístas injustamente, debido a la mayor variabilidad de los canales realistas y a la obstaculización de los edificios. El tercer escenario introduce el efecto de la congestión, reduciendo la S_+ en WD en un 4%. Sin embargo, a través de pruebas realizadas con un porcentaje de carga aún mayor, se puede comprobar que existe una mayor correlación, aunque no se muestran los resultados por falta de espacio. Finalmente que la capacidad de detección es constante frente a la variación de factores como las dimensiones físicas (escenario 4) o por un aumento de la potencia de transmisión (escenario 5).

TABLA IV: CAPACIDAD DE DETECCIÓN DE *WATCHDOG*

SPP	Parámetro	Escenario				
		1	2	3	4	5
WD	S_+ (%)	98.59	93.87	89.76	90.55	91.14
	E_+ (%)	4.85	10.79	10.80	9.31	10.10
	D	30.12	21.63	21.18	22.75	22.00
TEAM	S_+ (%)	99.98	99.30	98.70	98.86	98.97
	E_+ (%)	41.79	65.52	65.86	59.52	64.24
	D	8.72	4.16	4.05	5.08	4.32

Finalmente presentamos una serie de diagramas de barras en las figuras 3 a 6 que reflejan el rendimiento final de la red en distintos escenarios. Cada barra apilada corresponde a un parámetro que describe el destino de los paquetes: porcentaje de paquetes correctamente recibidos (*PDR Packet Delivery Ratio*), porcentaje de paquetes descartados por la indisponibilidad de rutas o por caídas de enlaces, porcentaje de paquetes descartados por nodos egoístas y porcentaje de paquetes descartados por su procedencia sospechosa (nodo origen egoísta o presencia de nodos intermedios egoístas en la ruta). Cada grupo de cinco barras representa un SPP diferente (AODV sin SPP, WD, TEAM y PD) en las figuras 3 a 5, mientras que cada barra corresponde a un porcentaje de nodos egoístas, creciente de 0% a 40%. Las figuras 3 y 4 corresponden a los modelos de 2 Rayos, y Realista respectivamente, con sesiones no simultáneas, mientras que en la 5 se emplea el modelo Realista y sesiones simultáneas. Se ha considerado el escenario de 238 nodos con una potencia de transmisión de 17dBm en las figuras 3 a 5. Comparando la figura 3 y la 4 se puede apreciar el efecto de emplear un canal realista: un descenso notable del PDR debido sobre todo a un porcentaje mayor de paquetes descartados por los nodos egoístas, salvo en el protocolo PD, donde los paquetes no son enrutados por el resto de nodos dado que proceden de nodos egoístas. Además, ningún nodo egoísta tiene ocasión de descartar un paquetes, porque su identidad es conocida por todos los nodos. El descenso del PDR está justificado por los tres factores mostrados anteriormente: primero, el empleo de un modelo realista disminuye el PDR *per se*; además, el incremento del número de saltos promedio de las transmisiones disminuye las probabilidades de encontrar una ruta libre de egoístas; por último, la capacidad de detección de nodos egoístas de la técnica *watchdog* también es menor. En el escenario con carga alta de la figura 5, además, se observa que el descenso en PDR está causado también por un aumento en el número de paquetes sin ruta, debido a la congestión en la red, y en menor medida, también por la peor capacidad de detección de *watchdog* en estas condiciones. Finalmente, la figura 6 refleja la influencia de los factores que modifican el número de saltos, usando el sistema TEAM. El primer grupo de columnas corresponde al escenario estándar de 238 nodos y potencia 17dBm, mientras que en el segundo se aumenta la potencia a 20dBm, en el tercero se disminuye el tamaño del escenario y en el último se aumenta. Los resultados confirman que el porcentaje de paquetes descartados disminuye siempre que en el escenario hay un promedio de saltos menor, como al aumentar la potencia o disminuir el tamaño, mientras que aumenta considerablemente al aumentar el tamaño del escenario.

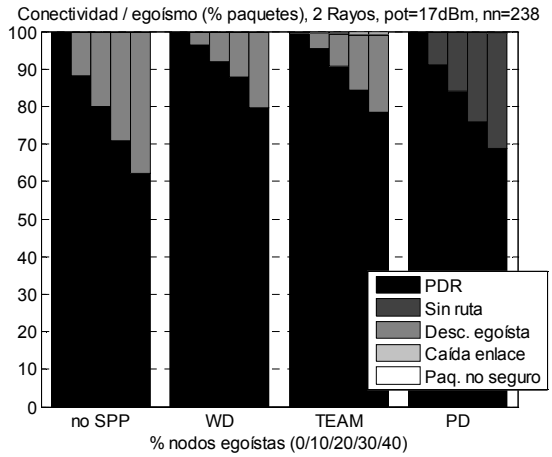

Figura 3: PDR y paquetes descartados con modelo 2 Rayos

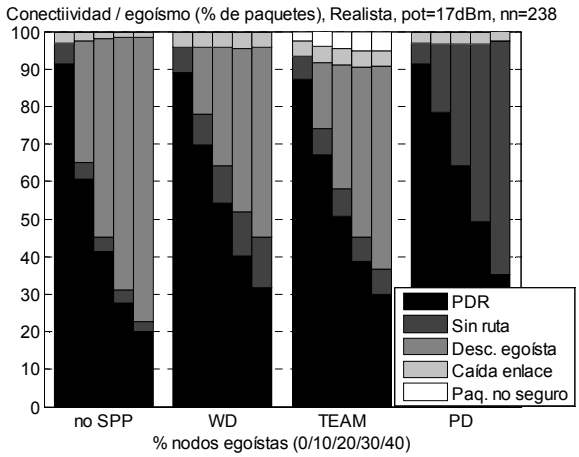

Figura 4: PDR y paquetes descartados con modelo Realista

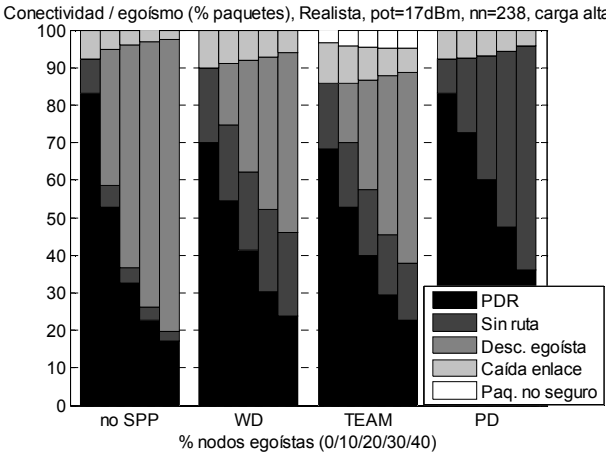

Figura 5: PDR y paquetes descartados, Realista y carga alta

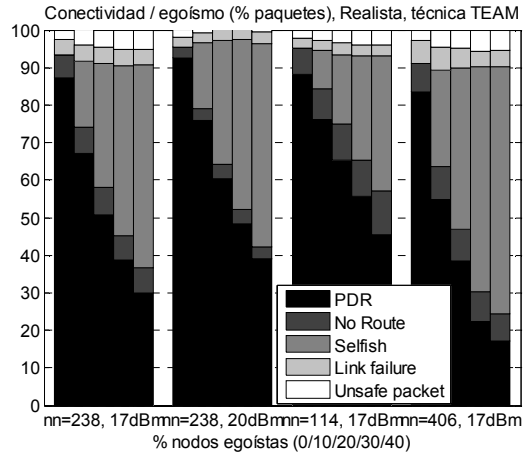

Figura 6: PDR y paquetes descartados para distintos escenarios

VII. Conclusión

Se ha analizado la influencia de ciertos parámetros de simulación y dimensionado sobre la eficiencia de distintos sistemas de reputación para el incentivo a la cooperación en redes MCN-MR. Los factores claves del rendimiento de estos sistemas en presencia de nodos egoístas son la capacidad de detección de la técnica *watchdog* y el número de saltos promedio de las transmisiones, elementos que hasta ahora no habían sido estudiados suficientemente. Se ha demostrado la conveniencia de emplear un modelo de canal realista para un correcto estudio de ambos parámetros, así como la necesidad de incentivar a los nodos egoístas a cambiar su estrategia, puesto que un porcentaje elevado de los mismos afecta muy negativamente al rendimiento final de la red, independientemente de la capacidad de detección del sistema de prevención que se aplique.

Agradecimientos

Este trabajo ha sido financiado por el Ministerio de Ciencia e Innovación bajo el proyecto TEC2008-06728, por el Ministerio de Industria, Turismo y Comercio bajo el proyecto TSI-020400-2008-113, por el Ministerio de Fomento de España a través del proyecto T39/2006, y por la Generalitat Valenciana a través de la beca con ref. BFPI/2007/269.

Referencias

[1] S. Marti et al., “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” *Libro de Actas ACM MobiCom 2000*, pgs. 255–265.
[2] Balakrishnan, V.; Varadharajan, V.; Tupakula, U.; Lues, P., "TEAM: Trust Enhanced Security Architecture for Mobile Ad-hoc Networks," *Libro de Actas 15th IEEE International Conference on Networks, 2007, ICON 2007*, pgs.182-187, 19 - 21 Noviembre 2007.
[3] Younghwan Yoo et al., “Why does it pay to be selfish in a MANET?,” *Wireless Communications*, vol. 13, pgs. 87-97, Diciembre 2006.
[4] R. Molva, P. Michiardi, “Security in Ad hoc Networks,” *Libro de Actas Personal Wireless Communications*, 2003.
[5] WINNER, “D1.1.1. WINNER II interim channel models”, *Public Deliverable,* http://www.ist-winner.org/index.html
[6] M. Sepulcre, J. Gozalvez, “On the Importance of Radio Channel Modeling for the Dimensioning of Wireless Vehicular Communication Systems”, *Libro de Actas del 7th International Conference on ITS Telecommunications, ITST '07*, 6-8 de Junio de 2007
[7] S. Buchegger, C. Tissieres, J.Y.Le Boudec, “A test-bed for misbehavior detection in mobile ad-hoc networks,” *Proc. IEEE Workshop on Mobile Computing Systems and Applications WMCSA*, 2-3 Diciembre 2004, pp.102 - 111.
[8] Rice Monarch Project “Wireless and mobility extensions to ns-2,” http://www.monarch.cs.rice.edu/cmu-ns.html
[9] I. D. Chakeres, Ch.E. Perkins, “Dynamic MANET on-demand (DYMO) Routing,” draft-ietf-manet-dymo-05, Internet Draft, Junio 2006.