Tesis de Máster en Ingeniería de Computadores

Departamento de Informática de Sistemas y Computadores

WATCHDOGS COLABORATIVOS PARA LA DETECCIÓN DE NODOS MALICIOSOS EN REDES MANET

Manuel David Serrat Olmos

Directores:

Dr. Enrique Hernández Orallo

Dr. Juan Carlos Cano Escribá

Valencia, junio de 2011

ÍNDICE

RESUMEN EJECUTIVO....1

CAPÍTULO 1. INTRODUCCIÓN A LAS REDES MÓVILES AD-HOC....3

1.1 Conceptos....3

1.2 Ámbitos de aplicación, ventajas y debilidades....5

1.3 Protocolos de encaminamiento para redes MANET....8

1.3.1 Dynamic Source Routing....10

1.3.2 Ad-hoc On-demand Distance Vector....13

1.3.3 Optimized Link-State Routing....15

CAPÍTULO 2. NODOS MALICIOSOS EN REDES MANET....19

2.1 Nodos maliciosos: tipos y efectos....19

2.2 Soluciones propuestas....22

2.2.1 Detección....22

2.2.2 Aislamiento....24

2.2.3 Incentivación....25

CAPÍTULO 3. WATCHDOG BAYESIANO COLABORATIVO....29

3.1 Trabajos previos....29

3.1.1 Sistemas de detección de Intrusos basados en Watchdogs....29

3.1.2 Mejorando el IDS: Watchdog Bayesiano....31

3.2 Nuestra aportación: el Watchdog Bayesiano Colaborativo....33

3.3 Estudio preliminar de resultados....36

CAPÍTULO 4. CONCLUSIONES Y FUTUROS TRABAJOS.....45
ÍNDICE DE FIGURAS.....47
ÍNDICE DE TABLAS.....49
BIBLIOGRAFÍA.....51

RESUMEN EJECUTIVO

Las redes móviles *ad hoc* (MANETs, de sus siglas en inglés, *Mobile Ad hoc NETworks*) han sido una linea de investigación que en los últimos años ha levantado mucho interés debido a la proliferación de dispositivos móviles inteligentes, como los *smartphones*, y el incremento de su potencia de cálculo y capacidades de comunicación inalámbrica. Este tipo de redes se caracterizan por carecer de infraestructura preexistente, ni tampoco de seguridad ni control centralizados, de forma que el conjunto de nodos que la forman se autoorganizan y colaboran para lograr cada cual cumplir con sus expectativas de comunicación. Al tratarse de nodos móviles, éstos cuentan con sistemas inalámbricos de comunicaciones y una batería de duración limitada. En estas redes, el número de nodos y su velocidad es variable y totalmente dinámico.

Resulta fácil vislumbrar la potencia de este enfoque para proporcionar conectividad a terminales que, de otro modo, no podrían comunicarse entre sí. Sin embargo, este mismo enfoque puede, y de hecho lo hace, generar determinados problemas relacionados con la seguridad. Algunos de estos problemas son inherentes al uso del medio aéreo. Las redes inalámbricas son propensas a presentar vulnerabilidades que favorecen ataques contra la confidencialidad de la información y disponibilidad del canal de comunicación, al ser fácilmente interferibles.

En el caso de las MANETs existen ciertos tipos de ataques que, si bien no pueden considerarse específicos al poder darse en otros tipos de redes, sí son especialmente dañinos. Al tratarse de redes que basan su funcionamiento en la colaboración entre sus nodos, cualquier comportamiento que pueda considerarse no colaborativo puede, dependiendo del número de nodos que lo presenten, poner en riesgo la existencia misma de la MANET. Y es precisamente a esos comportamientos inadecuados a los que deben hacer frente los protocolos que ofrecen funcionalidad a la red. Existen básicamente tres comportamientos inadecuados en este tipo de redes:

- el nodo malicioso, que persigue interceptar comunicaciones, falsear identidades o conseguir que la red deje de servir peticiones legítimas. dañando el servicio.

- el nodo egoísta, que hace uso de los servicios de la red pero no encamina adecuadamente los paquetes con destino a otros nodos que pasan por él, con objeto de no consumir su propia batería o sus servicios de comunicación, en el caso de estar éstos sujetos a pagos adicionales.

- el nodo averiado, cuyo comportamiento es errático debido a algún fallo en su

hardware y/o en el software que ejecuta.

En esta Tésis de Master analizaremos cómo las MANETs pueden hacer frente a los diferentes comportamientos inadecuados, especialmente aquellos nodos a los que llamaremos *black holes*, y que se caracterizan por no reenviar los paquetes que les llegan procedentes de otros nodos. No distinguiremos, en principio, con qué objetivo llevan a cabo esta actividad los *black holes*, ya que nuestro objetivo es la detección de dichas estaciones, dejando para más adelante las acciones a realizar una vez se han detectado.

Un mecanismo inicial que permita reducir este tipo de comportamientos inadecuados es la detección de los mismos, y para ello propondremos el uso de *watchdogs*, servicio activo en cada nodo de la MANET que monitorizará las comunicaciones de su vecindario para, mediante el uso de herramientas estadísticas, identificar a aquellos nodos cuyo comportamiento no se ajuste a parámetros de normalidad. Los *watchdogs* se han utilizado ampliamente en todos los sistemas de detección de intrusos (IDS, de sus siglas en inglés, *Intrusion Detection Systems*), pero en redes inalámbricas su utilización presenta una dificultad adicional debido a la naturaleza poco fiable del canal, y al ruido que éste presenta.

Uno de los trabajos en los que se basa esta Tésis de Master presenta el uso de un *watchdog* mejorado mediante un filtro bayesiano, que obtiene para cada vecino un índice de reputación que le identificará como colaborativo o no. La ventaja de usar este tipo de filtros bayesianos es que, comparado con un *watchdog* estándar, el bayesiano reduce el número de falsos positivos y falsos negativos, mejorando la exactitud de la detección. La principal actividad investigadora que hemos realizado para este trabajo ha sido la mejora del *watchdog* bayesiano, proporcionándole información adicional procedente de las reputaciones que sus nodos vecinos calculan periódicamente, conocida como “información de segunda mano”, y convirtiéndolo en un *watchdog* colaborativo. Nuestra propuesta mejora la exactitud de la implementación de partida pero, sobretodo, mejora apreciablemente la rapidez con la que se detecta al nodo malicioso.

Como trabajo futuro de investigación de cara a los estudios doctorales, nos proponemos ajustar los parámetros de funcionamiento del *watchdog* bayesiano colaborativo para conseguir una mejor tasa de detección de nodos maliciosos, así como estudiar más detalladamente el impacto que el intercambio de información de reputaciones tiene en la MANET, tanto desde el punto de vista de la productividad de la red como del consumo de baterías de los nodos que la forman. También se propondrán las medidas a llevar a cabo una vez estos nodos maliciosos han sido detectados.

CAPÍTULO 1. INTRODUCCIÓN A LAS REDES MÓVILES AD-HOC

1.1 Conceptos

Las Redes Móviles Ad hoc, conocidas también por MANETs (siglas en inglés de *Mobile Ad hoc NETworks*), son un concepto que se refiere a aquellas redes inalámbricas multi-salto, habitualmente con una **topología mallada irregular** (*mesh*), formadas únicamente por un conjunto de nodos móviles sin hacer uso de infraestructura preexistente. Al carecer de infraestructura fija previa, las redes de tipo MANET suelen carecer también de seguridad o control centralizados, de forma que para que la red sea funcional se debe asumir que los nodos que la forman son capaces de seguir un protocolo que los **autoorganice**. Igualmente, y para que los nodos puedan ver cubiertas sus necesidades de comunicación, se requiere que los todos nodos intermedios entre el nodo emisor y el nodo receptor de un mensaje, y que forman la mejor ruta emisor-receptor, reenvíen dicho mensaje al siguiente salto de esa ruta [Gior'02].

En los últimos diez años, las redes MANET han sido un aspecto de investigación muy popular en el ámbito de las Tecnologías de la Información y las Comunicaciones, con multitud de artículos y publicaciones al efecto. Aunque en la actualidad, las redes MANET podemos encontrarlas en pocos entornos de producción real, ello no es óbice para que algunas de las tecnologías que implementan las MANET se puedan encontrar también en otras clases de redes. Por ejemplo, una red de sensores inalámbricos desplegada desde medios aéreos para monitorizar el riesgo de incendios en bosques es una red *ad hoc* (aunque sus nodos no son móviles), y debe ser capaz de autoorganizarse para transmitir los datos requeridos –usualmente, temperatura y humedad– hacia uno o varios nodos sumidero, que deben a su vez transmitir hacia nodos que permitan integrar toda la información recopilada en un sistema de información adecuado. En este caso, es evidente que no se va a poder hacer un despliegue ordenado, sino que los nodos van a caer de forma aleatoria sobre el terreno a monitorizar. Aquí, la red *ad hoc* es una parte de un sistema de comunicaciones mayor, que posiblemente integre nodos con interfaces en diferentes redes con diferentes tecnologías, y posiblemente, con varias redes ad hoc desplegadas en otras ubicaciones geográficas con el mismo propósito. Pero los protocolos de descubrimiento de vecinos y rutas, topología, y encaminamiento de mensajes pueden estar basados en productos similares existentes en las MANET. En este caso concreto, la red será propiedad de una única autoridad, por lo que se asume que los nodos serán todos colaborativos.

Un tipo concreto de MANET podemos encontrarla en las llamadas redes (inter)vehiculares (VANET, *Vehicle Area Network*), que permitirán, en un futuro más o menos lejano, a nuestro automóvil comunicarse con los vehículos que nos rodean mientras circulamos, intercambiando información acerca de problemas de tráfico o para evitar colisiones. Este tipo de redes permitirán también a los nodos comunicarse con estaciones fijas ubicadas a lo largo del recorrido, para proveerse de otros servicios que proporcione dicha red. Por tanto, las VANET formarán parte de lo que se ha dado en llamar Sistemas de Transporte Inteligentes (*Intelligent Transport Systems*, o ITS), tecnologías y propuestas en plena ebullición en la actualidad, pero cuya materialización práctica aún tardará unos cuantos años.

Por tanto, una red móvil ad hoc puede caracterizarse, de forma general, por:

- estar basada en tecnologías inalámbricas de transmisión de datos, formando una estructura irregular mallada, o *mesh,* de enlaces bidireccionales.
- estar formada por nodos móviles, alimentados por baterías, y cuyas características técnicas pueden variar significativamente:
  - diferentes velocidades y patrones de movimiento.
  - diferentes alcances del radio de transmisión.
  - diferentes capacidades de proceso.
  - diferentes duraciones de baterías,...
- ser una red que no tiene necesariamente un propietario, ya que puede ser comunitaria, aunque algunos de sus servicios podrían estar sujetos a algún tipo de cargo en su caso.
- ser una red con topología dinámica, frecuentemente sin un control o seguridad centralizados, conforme a las necesidades de los nodos que la forman.
- estar basada en la colaboración por parte de todos sus nodos para funcionar y prestar servicios.

En una MANET, en un instante de tiempo, cada nodo tiene en su área de cobertura a uno o más nodos, ya que, si no los tuviera, estaría desconectado de la red. En la Figura 1 (izquierda) puede observarse que los nodos B y C son **vecinos** del nodo A, no así los nodos D y E. La parte derecha de la Figura 1 representa los enlaces posibles en ese mismo instante de tiempo. Cuando el nodo A emite, todos sus vecinos escuchan su transmisión, pero sólo tratarán el paquete si ellos son los destinatarios (finales o intermedios) del mismo. Las comunicaciones de A hacia los nodos que no son sus vecinos directos, como D y E, dependen, por tanto, de su grupo de vecinos, que harán

las veces de repetidores, encaminando los paquetes que les lleguen hacia su siguiente salto en la ruta origen-destino del paquete. Por ejemplo, para comunicarse con E, el nodo A enviará el mensaje a través de B ó C, dependiendo de cuál sea la mejor ruta según el protocolo de encaminamiento de la red, y el nodo seleccionado reenviará el mensaje hacia su destino.

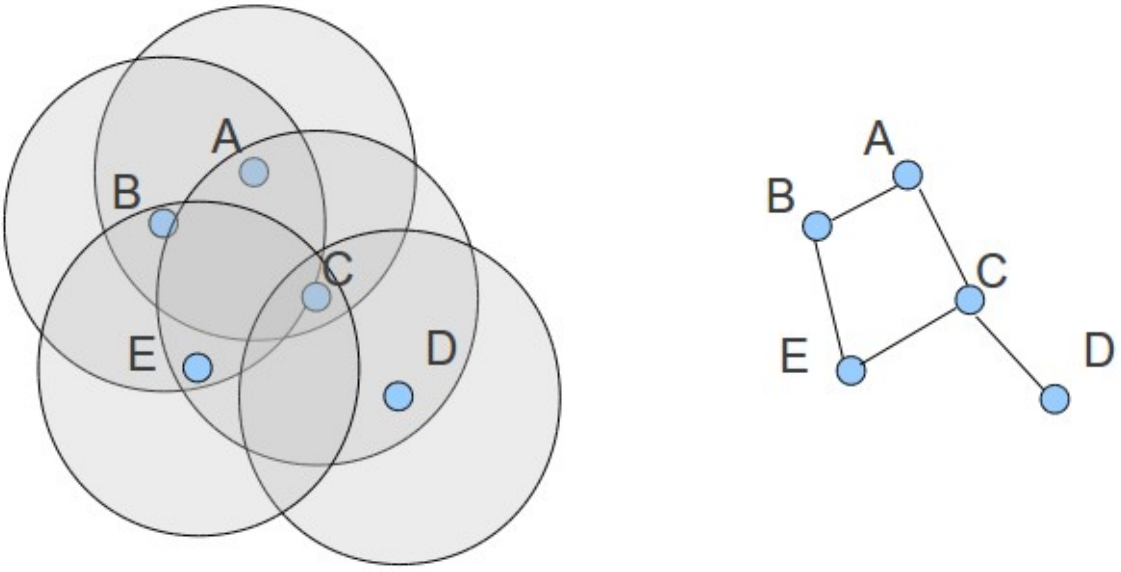

Figura 1. Red MANET de cinco nodos.

1.2 Ámbitos de aplicación, ventajas y debilidades

Los ámbitos de aplicación generales identificados para este tipo de redes se pueden resumir en las siguientes [Vaid'06]:

- redes de área personal, creando la red entre los diferentes dispositivos inalámbricos que una persona puede portar, como teléfono móvil, ordenador portátil, auriculares inalámbricos, etc.

- uso militar, creando redes entre los diferentes equipos de combate (blindados, infantería, armamento pesado,...) para mejorar el rendimiento de todos ellos mediante el intercambio ad hoc de información sobre el terreno, el clima, el enemigo, etc.

- uso civil, para el intercambio de información de todo tipo en lugares de pública concurrencia, como estadios, aeropuertos, hospitales, etc., usando dispositivos móviles inteligentes, como *smartphones* o *tablets* como nodos de la red.

- uso en emergencias, como mecanismo de distribución de información entre los

miembros de los equipos de rescate o intervención para el intercambio de información sobre riesgos, constantes vitales de los operativos, etc.

De estos cuatro ámbitos de aplicación, el más interesante desde nuestra perspectiva es el del uso civil, ya que en los demás casos existe un propietario que despliega la red y que la dota de los servicios que cree convenientes. Para nuestro trabajo, es primordial el aspecto de la inexistencia de un propietario y de un control centralizado de la red, es decir, la característica de su **construcción comunitaria y autónoma** es necesaria para nuestro análisis.

Las ventajas que presentan las redes móviles *ad hoc* surgen directamente de su forma de despliegue:

- no dependen de ninguna infraestructura concreta preexistente, por lo que se pueden desplegar en cualquier lugar en que sea necesario, en interior o exterior.

- son baratas y fáciles de desplegar. En el caso de las redes comunitarias, ni siquiera tienen un coste para nadie su despliegue (salvo el precio del terminal), y con el uso de los protocolos adecuados su despliegue consiste, básicamente, en encender los nodos y dejar que se autoorganicen. Además, suelen utilizar hardware de comunicaciones de uso masivo.

- toleran cierta cantidad de fallos, dependiendo del número de nodos, del número de rutas posibles entre cada par origen-destino, de la velocidad de cada nodo y de las trayectorias que siguen, readaptando las rutas cuando sea conveniente en función de la topología de la red en cada momento. En la Figura 2 se puede apreciar como la topología de la red que se muestra en la Figura 1 ha cambiado, por lo que la ruta entre A y D, que pasaba por C a dos saltos, ahora debe pasar también por E a tres saltos.

Sin embargo, también presentan inconvenientes o debilidades que hay que tener en cuenta [Vaid'06]:

- todos los nodos que la forman deben ejecutar los mismos protocolos para entrar a formar parte o salir de la red, buscar las mejores rutas para los destinos de paquetes, notificar su presencia a los vecinos y detectar la presencia de éstos, etc., ya que, de otro modo, no existiría la MANET, o existirían tantas como protocolos distintos estuvieran en ejecución en los nodos.

- como cualquier red inalámbrica, está afectada por determinados problemas de nivel físico y de acceso al medio compartido, como el reducido alcance, o la pérdida de paquetes por errores de transmisión o debidos a la movilidad de los nodos.

- tampoco son ajenas, por tanto, a otros problemas como el del nodo oculto y el

del nodo expuesto, típicos de las redes inalámbricas. El conocido como "problema del nodo oculto" se da cuando las transmisiones de dos nodos que no se conocen colisionan en un nodo que es vecino de ambos a la vez. En la Figura 1, los nodos A y E podrían provocar este problema en los nodos B o C. El "problema del nodo expuesto" se produce cuando dos parejas de nodos se comunican y un nodo de cada pareja está en el alcance de uno de los nodos de la otra pareja. En ese caso, las transmisiones de dichos nodos hacia sus parejas colisionan. Puede darse ese efecto en la Figura 2, si C y E trasmiten a la vez, hacia A y D respectivamente, provocando la colisión de ambas transmisiones al estar C dentro del alcance de E, y viceversa.

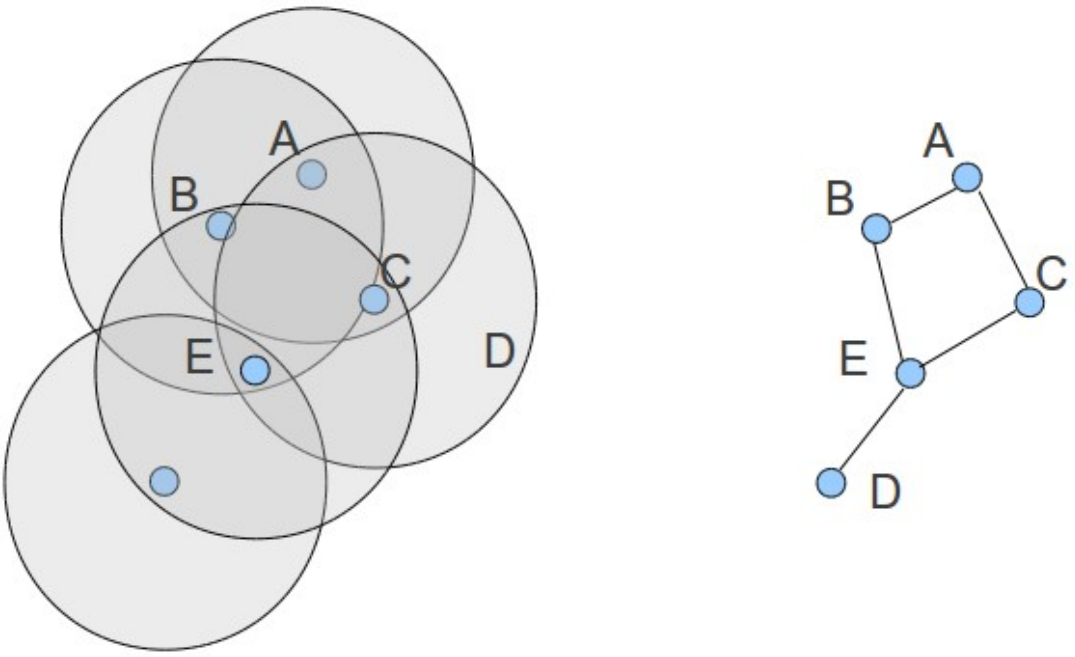

Figura 2. La red de la Figura 1, tras el movimiento del nodo D.

- el hecho de hacer uso del medio aéreo las hace vulnerables a determinadas amenazas a la seguridad, por lo que se tendrían que implementar mecanismos de protección ante dichas amenazas, como en cualquier otra red, de forma más compleja sin un control centralizado. Precisamente la parte principal de este trabajo de Tésis de Máster se centrará en estas cuestiones.

- la productividad de la red, e incluso su propia existencia, es muy dependiente de las velocidades relativas de los nodos que la forman. Si los nodos se mueven muy rápido, pronto quedan fuera del alcance de otros nodos, particionando la red o aislándose. Este problema es especialmente importante en redes VANET, dada la elevada velocidad de los vehículos que la forman.

1.3 Protocolos de encaminamiento para redes MANET

Son muchos los protocolos[1] que se han propuesto relacionados con las redes móviles ad hoc y tecnologías relacionadas. Algunos se diseñaron específicamente para ellas; otros, se adaptaron de soluciones existentes en otras redes. El principal foco de investigación en los primeros años de estas redes fueron, precisamente, los protocolos de encaminamiento que permitirían a un nodo origen hacer llegar su mensaje a un nodo destino, usando para ello la mejor ruta posible, y confiando en la colaboración del resto de nodos para su transporte mediante retransmisión.

Como en cualquier otro tipo de red, los protocolos para MANET podemos clasificarlos según varios criterios:

- dependiendo de dónde se toma la decisión de encaminamiento de cada paquete, un protocolo puede estar basado en **encaminamiento fuente**, si la decisión se toma en el nodo origen para toda la ruta del mensaje, indicando explícitamente por qué nodos ha de pasar; o **encaminamiento distribuido**, si la decisión de por qué enlace ha de encaminarse el paquete se toma en cada nodo de la ruta origen-destino. En este último caso, dependiendo de la información de encaminamiento que cada nodo almacena, podemos encontrar protocolos basados en **vector de distancia** (*distance vector*), si lo que se almacena para cada destino conocido es el siguiente salto y la distancia hasta llegar al destino, medida en número de saltos; o protocolos basado en el **estado del enlace** (*link state*), en el que cada nodo comparte con los demás el estado de sus enlaces activos, de forma que todos los nodos de la red son capaces de construir un mapa completo de la topología de la red.

- dependiendo de las posibilidades de cambiar de ruta una vez inyectado el paquete en la red, un protocolo puede ser **adaptativo**, si permite cambiar de ruta en respuesta a fallos de enlaces o congestión; o **determinista**, si no permite cambios en las rutas una vez tomada la decisión de encaminamiento inicial.

- dependiendo del mecanismo de actualización de las mejores rutas origen-destino, un protocolo puede ser **reactivo**, cuando busca la mejor ruta en el momento en que es necesario para enviar un mensaje; o **proactivo**, si está continuamente actualizando su tabla de rutas para asegurar proporcionar instantáneamente la mejor ruta para el mensaje. También pueden encontrarse soluciones **híbridas**, en las que parte de las rutas se obtengan proactivamente y se busquen otras reactivamente. Evidentemente, los criterios para tomar una decisión en este caso se basan en el tiempo necesario para obtener una nueva ruta, en los reactivos, y en la sobrecarga de red que provoca el protocolo

1 Puede encontrarse una lista detallada de estos protocolos en la URL http://en.wikipedia.org/wiki/Ad_hoc_protocol_list

proactivo al estar continuamente enviando paquetes de descubrimiento de rutas.

- dependiendo del parámetro que se use para decidir la mejor ruta, podemos encontrar protocolos:
  - que consideran la mejor ruta la que menos saltos presente, o de **camino más corto** (*shortest path*).
  - que consideran la mejor ruta la que presente una **latencia menor** entre origen y destino (*shortest time*).
  - que consideran la mejor ruta aquella en la que se busque el **camino ponderado más corto** (*shortest weighted path*), teniendo en cuenta el consumo de batería o el ancho de banda disponible en el enlace.
- dependiendo de si el protocolo utiliza o no información topológica, podemos encontrarnos con protocolos de **encaminamiento plano** o protocolos de **encaminamiento jerárquico**.

Además de estos criterios generales, podemos encontrarnos con protocolos de encaminamiento para MANET que basan sus decisiones en el uso de determinados recursos, como, por ejemplo, el nivel de batería, con el objetivo general de equilibrar el consumo medio de la misma en toda la red.

En cualquier caso, hay varias condiciones que un buen protocolo de encaminamiento para redes MANET deben cumplir:

- el grafo de dependencias de encaminamiento de todas las posibles combinaciones de nodos origen-destino no debe contener ciclos, para lo cual pueden usarse técnicas como las de *spanning tree*, en profundidad o en anchura (*Breadth-First Search* o *Depth-First Search*).
- debe operar de forma distribuida y auto-configurada, es decir, ninguna entidad debe actuar como servidor de rutas ni nada parecido, sino que cada nodo debe ser capaz de obtener una ruta a cualquier destino por sí mismo, consultando para ello al resto de nodos de la red.
- debe ser eficiente ante la naturaleza dinámica de la red, que provoca frecuentemente que aparezcan y desaparezcan nodos y enlaces.

Por supuesto, y dadas todas las consideraciones anteriores, no hay ningún protocolo que responda de forma satisfactoria a todas ellas, por lo que la elección del protocolo de encaminamiento de la MANET dependerá en buena medida del número de nodos de la misma, de su movilidad y de la cantidad de tráfico que la red haya de cursar. Cabe mencionar en este punto la existencia de un grupo de trabajo del IETF al respecto

de los protocolos de encaminamiento para redes móviles ad hoc[2].

Todos los protocolos que se utilizan en estas redes se ven obligados a trabajar en dos aspectos distintos de la comunicación: el descubrimiento o establecimiento de rutas, usando paquetes de control; y la transferencia de mensajes de datos. Cuando un nodo desea enviar un mensaje a otro nodo, debe obtener una ruta válida, y enviar el primer paquete del mensaje al primer nodo de dicha ruta. Cómo obtenga la ruta y qué haga con ella exactamente, dependerá del protocolo concreto. El primer nodo de la ruta, al recibir el paquete, repetirá el proceso conceptual de conocer la ruta hacia el destino y enviar al siguiente nodo de la misma el paquete[3], en una cadena de recepciones-retransmisiones que finalizará cuando el mensaje completo llegue a su nodo de destino.

A continuación, comentaremos algunos aspectos de tres de los protocolos para MANET más estudiados en la literatura: DSR, AODV/DYMO y OLSR. Sin embargo, podemos citar otros protocolos de encaminamiento que han sido propuestos, como ZRP, DSDV, GPSR, PAR, MDR o HSR [Abol'03].

1.3.1 Dynamic Source Routing

Dynamic Source Routing (DSR) [John'07] [Vaid'06] es un protocolo de encaminamiento para redes móviles *ad hoc* que podemos caracterizar por ser un protocolo **reactivo**, basado en **encaminamiento fuente**, en el que toda la ruta hasta el destino se escribe en la cabecera de cada paquete, y por tanto, determinista. También podemos decir que DSR es un protocolo que no hace uso de información topológica (no es jerárquico) y que selecciona la mejor ruta, entre las disponibles, en función del menor número de saltos o *hops* hasta el destino.

Periódicamente, todos los nodos emiten pequeños mensajes de HELLO para anunciar o confirmar su presencia a aquellos nodos presentes en el radio de alcance de su emisor, o sea, sus vecinos a un salto. Con esta información, cada nodo mantiene actualizada una tabla de estos vecinos a un salto, que será utilizada para el resto de actividades del protocolo.

Cuando un nodo S desea enviar un paquete a otro nodo D y no dispone en su tabla de rutas de una adecuada hacia él, se inicia el procedimiento de descubrimiento de la ruta más corta mediante el envío de un paquete ***Route Request*** (RREQ) por inundación (*flooding*). Los vecinos del nodo S, a su vez, inundarán su vecindario con el mismo paquete de RREQ, al que habrán añadido su identificador de nodo. Este proceso se va

2 Puede obtenerse más información al respecto en la URL http://www.ietf.org/html.charters/manet-charter.html

3 Algunos protocolos requieren que haya un reconocimiento explícito de la recepción del paquete en cada salto, a otros les basta con que el nodo origen reciba desde el nodo destino un reconocimiento de la llegada del paquete.

repitiendo por toda la red hasta que se alcanza el nodo destino D. Los paquetes RREQ que llegan a cualquier nodo por otras rutas después del primero se descartan. En caso de que el paquete RREQ con la lista de nodos por los que ha pasado alcance el nodo D, éste construye un paquete ***Route Reply (***RREP), incluyendo como *payload* en el mismo la información de la ruta obtenida. En la cabecera del RREP aparece dicha ruta en sentido inverso, indicando los nodos por los que debe pasar el paquete de control hasta llegar al nodo S. En el caso de que los enlaces no fueran bidireccionales, quizá hiciese falta que D iniciase un RREQ hacia S, siguiendo un proceso análogo, pero incluyendo ya como dato la ruta S→D.

Una vez el paquete RREP llega al nodo S, éste dispone ya de la ruta hacia D, por lo que comienza a enviar los paquetes de datos, insertando en la cabecera del paquete toda la ruta S→D. Cada vez que el paquete de datos llega a un nodo, éste retira de la cabecera su identificador de nodo, y lo reenvía al siguiente salto en la ruta.

Si, por el hecho de la movilidad o por cualquier otro, una paquete de S hacia el nodo D llega a un nodo intermedio I y éste no es capaz de reenviar el paquete al siguiente salto de la ruta, I generará un paquete de ***Route Error*** (RERR) para informar al nodo S de que el nodo D ya no es alcanzable siguiendo la ruta indicada. Esta situación provocará que S borre de su tabla la ruta errónea e inicie un nuevo proceso de descubrimiento de ruta hacia D. Si, pasado un determinado tiempo, a S no llega ninguna ruta válida, se considerará inalcanzable a D y se generará el correspondiente mensaje de error hacia niveles superiores del sistema.

Para mejorar el rendimiento del protocolo, éste implementa una serie de técnicas para gestionar una caché de rutas, con objeto de reducir la propagación de los RREQ y los retrasos inducidos por el descubrimiento de rutas:

- si un RREQ llega a un nodo intermedio que ya conoce la ruta desde él hasta D, la devolverá directamente a S, acelerando así el proceso de descubrimiento. Por ejemplo, si el nodo T recibe la petición de ruta S→D, con datos [S,H,K], y ya conoce la ruta [T,M,D], generará el RREP con la ruta [S,H,K,T,M,D] en el *payload* del paquete, y con [K,H,S] en la cabecera del mismo.

- cuando se aprende una ruta S→D, se aprenden también las rutas de S a todos los nodos de la ruta S→D. Por ejemplo, si la ruta S→D es [S,H,K,T,M,D], en la tabla de rutas se almacenarán las rutas [S,H,K,T,M,D], [S,H,K,T,M], [S,H,K,T] y [S,H,K] ([S,H] no se almacena porque H es vecino a un salto de S).

- cuando un nodo intermedio recibe una petición de ruta desde S, no siendo S vecino suyo a un salto, aprende la ruta inversa hacia ese nodo. Por ejemplo, el nodo T recibe una petición de ruta S→D con los datos [S,H,K], automáticamente aprende las rutas [T,K,H,S] y [T,K,H].

- igualmente, cuando un nodo intermedio recibe un RREP para que lo encamine hacia el nodo S, aprende las rutas adecuadas desde él mismo hasta D, con todos sus intermedios. Por ejemplo, si el nodo K recibe un RREP de la ruta de S→D con los datos [S,H,K,T,M,D], automáticamente aprende las rutas [K,T,M,D] y [K,T,M].

- cuando un nodo recibe un paquete de control RERR con destino a otro nodo, actualiza su tabla de encaminamiento para eliminar todas las rutas que quedan anuladas por dicho paquete de control.

- el protocolo permite también a un nodo aprender rutas escuchando (*overhearing*) los paquetes de datos que circulan por la red sin pasar por él.

Como en cualquier caché, serán necesarias ciertas tareas de gestión de la misma para eliminar rutas que ya no sean válidas debido a la movilidad de los nodos. Es posible que un nodo use varias rutas inválidas de la caché antes de encontrar una que siga siendo válida.

DSR presenta los siguientes puntos fuertes como protocolo para el encaminamiento de paquetes en redes MANET:

- la sobrecarga de paquetes de control que genera el tráfico de descubrimiento de rutas es baja, dado que sólo se requiere establecer y mantener las rutas entre nodos que se comunican de forma efectiva, no con todos los nodos presentes

- debido a las caches de los nodos intermedios, es posible que se recopilen varias rutas distintas en el nodo que solicita el descubrimiento de la ruta

Por supuesto, DSR también tiene inconvenientes:

- el primer inconveniente destacable proviene del hecho de que es un protocolo basado en encaminamiento fuente, que coloca en la cabecera del paquete la lista de nodos por los que ha de pasar hasta llegar al destino, por lo que el tamaño de la cabecera crece con el diámetro de la red y puede llegar a degradar su rendimiento

- puede producirse una “tormenta de respuestas” (*Route Reply Storm*) si muchos nodos intermedios responden a un RREQ desde sus caches de rutas, provocando un aumento de la contención en las cercanías del nodo solicitante. Para resolverlo, los nodos intermedios deben evitar generar un RREP si escuchan otro RREP cuya ruta sea más corta

- se pueden producir colisiones de RREQ en nodos vecinos, por lo que se deberán insertar retardos aleatorios en las retransmisiones para evitarlas

- potencialmente, cualquier RREQ puede llegar por inundación a todos los nodos de la red, algo que se puede evitar, por ejemplo, con el mecanismo *Location-Aided Routing* (LAR) [Ko'98], que, simplificadamente, integra la posición geográfica (GPS) del nodo origen en los RREQ y los envía sólo a una zona geográfica de la red en la que se espera que esté el nodo destino

- un nodo intermedio puede servir rutas de su caché que ya estén caducadas. Para evitarlo, se deben implementar mecanismos de limpieza de la caché, lo que aumenta el coste computacional del protocolo

1.3.2 Ad-hoc On-demand Distance Vector

Ad-hoc On-demand Distance Vector (AODV) [Perk'03] [Vaid'06] es un protocolo de encaminamiento para redes móviles *ad hoc* que podemos caracterizar por ser un protocolo **reactivo**, basado en encaminamiento distribuido cuya tabla se construye en función del **vector de distancia**, y de carácter adaptativo. Al igual que con DSR, podemos decir que AODV tampoco es un protocolo jerárquico, y que selecciona la mejor ruta, entre las disponibles, en función del menor número de saltos hasta el destino.

El objetivo planteado al diseñar AODV era mejorar a DSR, intentando evitar sus inconvenientes, y manteniendo sus ventajas o puntos fuertes. La más fácil de conseguir fue la de la reducción del tamaño de la cabecera del paquete. AODV está basado en encaminamiento distribuido, por lo que las tablas de encaminamiento se almacenan en cada nodo, de forma que los paquetes no contienen rutas, sólo los nodos origen y destino. La única limitación que impone AODV que no está presente en DSR es que requiere que el canal sea bidireccional. El funcionamiento genérico de AODV es muy similar a DSR:

- periódicamente, todos los nodos emiten pequeños mensajes de HELLO para anunciar o confirmar su presencia a aquellos nodos presentes en el alcance de su radio

- cuando un nodo S desea enviar un paquete a otro nodo D y no dispone en su tabla de encaminamiento de una ruta hacia él, se inicia el procedimiento de descubrimiento de la ruta más corta mediante el envío de un paquete *Route Request* (RREQ) por inundación (*flooding*).

- los vecinos del nodo S, a su vez, inundarán su vecindario con el mismo paquete de RREQ, al que habrán añadido su identificador de nodo formando la ruta inversa apuntando al nodo S. Este proceso se va repitiendo por toda la red hasta que se alcanza el nodo destino D, en caso de éxito, o no. Los paquetes RREQ que llegan a cualquier nodo por otras rutas después del primero se descartan.

- en caso de que el paquete RREQ con la lista de nodos por los que ha pasado alcance el nodo D, éste construye un paquete *Route Reply (*RREP), incluyendo como *payload* en el mismo la información de la ruta obtenida.

- como todos los nodos intermedios han ido almacenando en sus tablas las rutas hacia el nodo S, cuando el RREP viaja por la ruta de D a S van también recopilando la información de cómo alcanzar a D y a los nodos intermedios restantes

- la tabla de encaminamiento de cada nodo almacena, para cada destino, el nodo siguiente de la mejor ruta, la distancia hasta llegar a él y dos números de secuencia (origen y destino) para poder conocer la frescura de las rutas inversas o directas cuando lleguen al nodo RREQ y RREP posteriormente

- los cambios topológicos se aprenden de las peticiones/respuestas de descubrimiento de rutas, de mensajes de HELLO fallidos, o de paquetes *Route Error* (RERR), actualizando en consecuencia la tabla de encaminamiento del nodo

- una vez se dispone de una ruta –realmente, del primer salto y la distancia de la misma–, el nodo S envía el paquete al vecino designado en la tabla de encaminamiento

- para evitar esperar por tiempo indefinido la obtención de rutas, los paquetes RREQ tienen un TTL que empieza siendo bajo. Si un nodo recibe un RREQ con TTL a 0, lo descarta. Si S no recibe en un tiempo preestablecido un RREP, manda los RREQ con un TTL mayor

- para facilitar la limpieza de las tablas de encaminamiento, todas las rutas tienen un tiempo de vida pasado el cual son eliminadas de la tabla, y habrán de volver a ser descubiertas

En los últimos tiempos, y en el seno del grupo de trabajo de IETF sobre redes MANET (MANET WG) se ha abandonado la investigación sobre AODV, decantándose por DYMO (*Dynamic MANET On-demand Routing*), que no es más que una versión modificada de AODV. De hecho, MANET WG trabaja en la especificación de un protocolo estándar, el *Reactive MANET Protocol* (RMP) , que no es más que DYMO. Sus impulsores afirman que presenta ventajas frente a AODV en cuanto a la aceleración en el descubrimiento de rutas.

Las ventajas o puntos fuertes que podemos resaltar de AODV son los mismos que ya hemos indicado para DSR, con la adición de la ya mencionada superación del problema del tamaño de la cabecera del paquete, al usar encaminamiento distribuido. Comparado con DSR, podemos decir también que AODV es adaptativo, con lo que ello

conlleva en términos de tolerancia a fallos. Igualmente, el coste computacional de mantener limpias de rutas caducadas las tablas de encaminamiento en menor.

En cuanto a los inconvenientes, podemos citar prácticamente los mismos que hemos indicado para DSR, con la excepción ya mencionada del tamaño de la cabecera del paquete.

1.3.3 Optimized Link-State Routing

Optimized Link-State Routing (OLSR) [Clau'03] [Vaid06] es un protocolo para MANET que puede ser caracterizado como un protocolo **proactivo**, basado en encaminamiento distribuido cuya tabla se calcula en función del **estado de los enlaces**, y de carácter adaptativo. Al igual que con DSR y AODV, podemos decir que OLSR también es un protocolo no jerárquico y que selecciona la mejor ruta, entre las disponibles, en función del menor número de *hops* hasta el destino. El estado de los enlaces con los vecinos se determinan gracias a los paquetes de HELLO. Para el MANET WG, OLSR es el *Proactive MANET Protocol* (PMP) que proponen como estándar para este tipo de redes.

La característica principal de OLSR, y que merece la pena resaltar en este momento, es que, al tratarse de un protocolo proactivo, intenta reducir al máximo la sobrecarga provocada por la necesidad de inundar periódicamente la red con información topológica, ya que todos los nodos han de disponer de información completa de la topología de la misma para poder encaminar correctamente los paquetes de datos.

Para optimizar el número de retransmisiones necesarias de información topológica, OLSR maneja el concepto de ***Multipoint Relay*** (MPR). Los MPR de un determinado nodo son aquellos vecinos desde los que se alcanza a todos los vecinos a dos saltos de dicho nodo. Como en los mensajes de HELLO cada nodo transmite la lista de sus vecinos, todos los nodos conocen la lista de sus vecinos a dos saltos, actualizando por tanto la lista de sus MPR. Cuando un nodo X haya de enviar su información de estado de enlaces, lo hará a sus MPR únicamente, de ahí el hecho de que este protocolo se considere optimizado si el tamaño de su conjunto de MPR es el mínimo posible, pero de forma que siempre asegure que, a través de dichos MPR, son alcanzables todos los vecinos a dos saltos del nodo X.

El otro concepto que hay que manejar para entender cómo realiza OLSR la optimización, es el concepto de ***Multipoint Relay Selector*** (MS). El nodo X es *Multipoint Relay Selector* del nodo Y si Y ha elegido a X como MPR.

Pasemos ahora a explicar cómo calcula un nodo X su conjunto mínimo de MPRs. El algoritmo se basa en dos pasos:

- Primer Paso: seleccionar los vecinos a un salto de X ($N_1(X)$) que alcancen a aquellos vecinos a dos saltos de X ($N_2(X)$) que estén aislados, es decir, que sólo sean alcanzables por esos nodos.

- Segundo Paso: seleccionar de entre los $N_1(X)$ no seleccionados en el primer paso, aquel nodo desde el que se alcance el mayor número posible de vecinos a dos saltos, y repetir el proceso hasta que todos los $N_2(X)$ hayan sido alcanzados desde alguno de los MPR seleccionados.

Veamos un ejemplo:

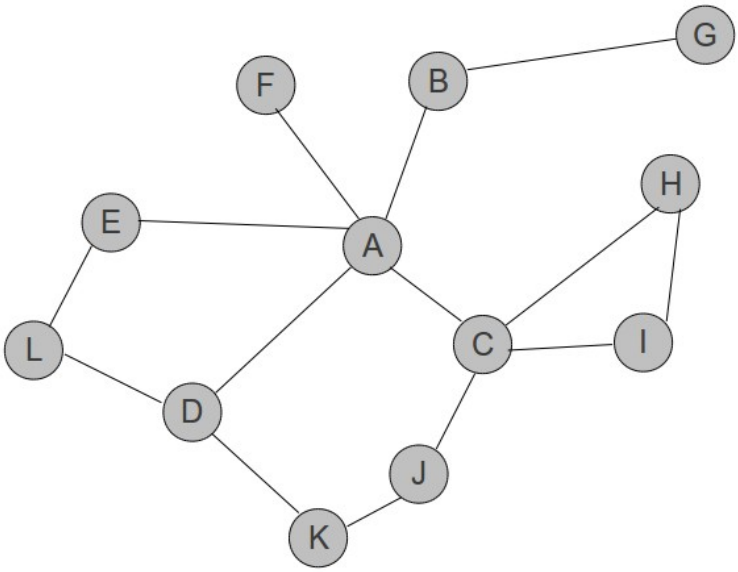

Figura 3. MANET de ejemplo.

En la Figura 3, vamos a obtener los MPR del nodo A. Para ello, sabemos que $N_1(A)$={B,C,D,E,F} y que $N_2(A)$= {G,H,I,J,K,L}. El primer paso del algoritmo de obtención de los MPR nos indicaría que es el nodo B el primer MPR seleccionado (MPR={B}), dado que es el único vecino a un salto capaz de alcanzar al vecino a dos saltos aislado G. En el segundo paso del algoritmo, del resto de vecinos a un salto elegimos aquellos que más vecinos a dos saltos alcancen, iterativamente, hasta que todos los vecinos a dos saltos estén alcanzados por algún MPR. En nuestro ejemplo, en este segundo paso seleccionaríamos al nodo C (que alcanza a tres, H,I y J) y al nodo D (que alcanza a dos, K y L). Con ello, MPR(A)={B,C,D}. A partir de la obtención del conjunto de MPR de un nodo, éste enviará dicho conjunto de MPR también en los mensajes de HELLO, de forma que los nodos referenciados inserten al nodo emisor en su *Multipoint relay selector set*, (MS). Por tanto, A estará en la lista MS de los nodos B, C y D. El cálculo de los MPR se realiza cada vez que se detecta un cambio en la topología a uno o dos saltos de cada nodo.

Cuando un nodo ha de notificar información topológica envía mensajes de control de la topología (*Topology Control*, o TC). Es importante recalcar que estos mensajes sólo se envían a aquellos nodos que se encuentran en el MS del nodo que los emite. Cuando un nodo Y vecino a un salto del nodo X, recibe de éste un mensaje TC, lo procesa, y sólo lo reenviará a sus vecinos si X está en el MS de Y. Con ésto se garantiza que se puede propagar la información de control de la topología a toda la red con el mínimo número de retransmisiones posible. Al finalizar el proceso de propagación de esta información, cada nodo tiene una lista completa de los enlaces disponibles en la red, de la cual el nodo puede obtener su tabla de encaminamiento, obtenida calculando los caminos más cortos, y que consta de cuatro entradas: el nodo de destino, el nodo por el que hay que encaminar, la distancia, y el interfaz de salida (pueden haber nodos con más de un interfaz de red inalámbrica).

¿Qué ventajas presenta OLSR sobre AODV o DSR, por ejemplo? La proactividad en la obtención de rutas es un cuestión que reviste importancia para aquellas aplicaciones de las MANET en las que el tiempo de obtención de ruta cuando se ha de enviar un paquete de datos deba ser el mínimo posible. Salvo que coincidan en el tiempo el envío del paquete de datos y el proceso de recálculo de rutas, cuando el nodo requiere enviar datos la ruta está siempre disponible, por lo que esta cuestión no introduce latencia en el envío del paquete.

Se puede aducir que en OLSR existe constantemente una sobrecarga en la red por el hecho de estar intercambiando paquetes TC entre los nodos, y que los paquetes de HELLO llevan cierto *payload*. Además, al tratarse de nodos móviles, el coste energético para las baterías de los nodos puede ser elevado. Dependiendo del tamaño de la red y de la movilidad de sus nodos, quizá los cambios topológicos no estén aún estabilizados en todos los nodos cuando ya se hayan producido otros en otro lugar. También se puede considerar que OLSR introduce cierta carga de cómputo y de almacenamiento en los nodos para la obtención de los MPR y el cálculo de rutas más cortas para cada destino.

La selección del protocolo de encaminamiento en cada MANET tiene, como se puede deducir fácilmente, muchas implicaciones posteriores. Para nuestro problema de detección de nodos maliciosos, un protocolo de encaminamiento de la red puede hacer que dicha detección sea más exacta o más rápida, pero, en principio, se debería tener como objetivo implementar mecanismos de detección que fuesen lo más independientes posible del protocolo de encaminamiento. Como en este trabajo se persigue la implementación de un *watchdog* para realizar la detección, se ha seleccionado AODV como el protocolo de encaminamiento sobre el que realizar dicha implementación, aunque podría haberse realizado sobre DSR o OLSR de forma análoga.

CAPÍTULO 2. NODOS MALICIOSOS EN REDES MANET

Ya hemos mencionado en varias ocasiones que las redes MANET basan su funcionamiento en la cooperación entre los nodos que la forman, por lo que cuanto mayor sea la red, mayores serán sus capacidades en lo que a velocidad, tolerancia a fallos y servicios prestados se refiere. Por esta razón, el despliegue de infraestructuras MANET comunitarias debe, como condición *sine qua non* [Karg'04], disponer mecanismos que protejan a la red de la presencia de nodos que, por su comportamiento inadecuado (*misbehaving nodes*), puedan ponerla en peligro.

2.1 Nodos maliciosos: tipos y efectos

Pero, ¿cuáles son los peligros que cualquier sistema MANET ha de afrontar? ¿Qué tipos de nodos cuyo comportamiento se considere inadecuado pueden aparecer en el alcance de cobertura de la red? En la literatura [Toh'10], básicamente se propone una taxonomía de nodos no cooperativos dependiendo del objetivo que el nodo persigue con su comportamiento:

- Nodo malicioso: este tipo de nodos pretende romper alguna de las propiedades de la seguridad: confidencialidad, integridad o disponibilidad. Un nodo malicioso puede intentar suplantar a nodos legítimos, para interceptar comunicaciones, atacando la confidencialidad de la información transmitida. También puede distorsionar la información que circula por la red, modificando paquetes de datos, inyectando paquetes de control falsos, o paquetes de datos en exceso para atacar la integridad de la información transmitida o la disponibilidad de la red. El abanico de técnicas que este tipo de nodos pueden utilizar para lograr su objetivo es amplísimo, ya que son comunes a casi todas las redes, con ciertas especificidades en el caso de las redes inalámbricas.

- Nodo fallido: este nodo no tiene ningún objetivo concreto, simplemente presenta averías o fallos en su hardware o software que pueden afectar a sus nodos vecinos en cualquier forma. Uno de estos nodos puede, sin ser consciente, provocar una denegación de servicio al saturar o interferir la red, transmitiendo en canales contiguos o generando un elevado volumen de tráfico.

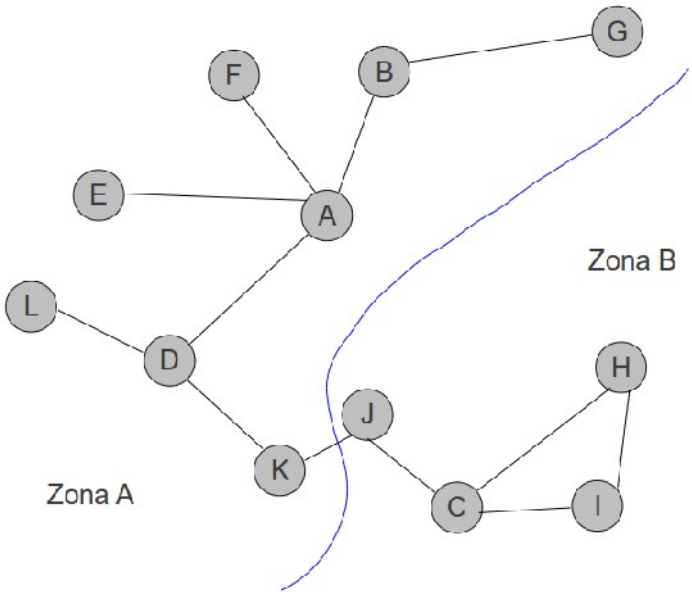

Figura 4. Particionado de la red.

- Nodo egoísta: este tipo de nodos se caracteriza por no desear la degradación o caída de la red, ya que hace uso de los servicios de la misma sin prestar ninguno a cambio, por lo que también se les conoce como nodos no colaborativos. Algunos autores [Toh'10] subclasifican estos nodos en vagos (*lazy nodes*) y constreñidos (c*onstrained nodes*). Estos nodos se aprovechan de sus vecinos para que descubran rutas y reenvíen los paquetes que ellos generan, pero no participan en el descubrimiento y/o en el reenvío de paquetes pertenecientes a los demás nodos. El motivo más habitual para que un nodo se comporte así es el ahorro de batería y/o económico, en el caso de que alguno de los interfaces del nodo esté conectado a alguna red sujeta a cargos por uso, como la red GPRS o UMTS, o simplemente al carácter egoísta de la estación o de su usuario.

Merece la pena hacer un inciso en este punto sobre las motivaciones de los nodos para comportarse egoístamente. Si lo que el nodo egoísta pretende es ahorrar batería con su comportamiento, dicho empeño es poco menos que inútil si, como suele ser habitual, los nodos están equipados con radios 802.11. Aunque algunos estudios [Cano'00] [Sund'10] dan a entender que esta motivación puede ser legítima, podemos decir que no tienen en cuenta todos los posibles estados del interfaz inalámbrico, por lo que su modelo de consumo es incompleto y, por tanto, lleva a resultados inexactos. Un interfaz inalámbrico puede estar en modo envío (*Tx*), modo recepción (*Rx*), modo inactivo (*Idle*) y modo apagado (*Off*). La mayoría de modelos analíticos sobre el consumo de nodos en redes MANET no tienen en cuenta el consumo en estado *Idle*, y que casualmente es en el que el nodo se encuentra la mayor parte del tiempo. Por ello, es evidente que teniendo en cuenta sólo *Tx* y *Rx*, si el nodo solo transmite sus paquetes ahorra batería de modo significativo. Sin embargo, teniendo en cuenta el consumo en estado *Idle* [Feen'01]

[Kim'03], que no es tan bajo como se creía, y que habitualmente no se muestra en las especificaciones de los fabricantes, el participar colaborativamente o no en la MANET produce diferencias en la duración de baterías prácticamente despreciables, ya que la mayor parte del consumo se produce cuando el nodo no está transmitiendo ni recibiendo. Y como el modo *Off*, el que realmente reduciría el consumo si pudiésemos poner el interfaz WiFi en ese estado, no es adecuado para redes MANET, en las que en cualquier momento puede recibirse un paquete para ser reenviado, **podríamos concluír que el egoísmo de un nodo es un comportamiento absolutamente improductivo** en cuanto a la duración total de su batería.

En ocasiones, quizá no sea posible dilucidar si el nodo cuyo comportamiento se considera incorrecto es malicioso, sólo es egoísta, o simplemente no funciona correctamente. Tal es el caso de los nodos conocidos como agujeros negros, o *black holes*. Considerado el tipo de ataque más habitual en redes móviles *ad hoc* [AlSh'04], un *back hole* es un nodo que aprovecha su posición en las rutas origen-destino que pasan por él para crear algún tipo de disrupción en el servicio. Si lo hacen selectivamente, se les denomina *grey holes,* aunque en lo que resta de este trabajo consideraremos que todos ellos son *black holes*, dado que el tratamiento a darles es similar[4]. Si se observa uno de estos nodos desde alguno de sus vecinos colaborativos, es muy complicado distinguir si el *black hole* es un nodo malicioso, que no reenvia paquetes de datos pero modifica paquetes de control de rutas para crear ciclos o para hacer creer que todas las mejores rutas pasan por él, o si es un nodo averiado, que simplemente no es capaz de reenviar por un problema de hardware o de versión de protocolo, o si es un nodo egoísta que no reenvía paquetes de otros para maximizar el tiempo de uso de su batería.

Si consideramos que los nodos maliciosos y los nodos averiados van a ser una inmensa minoría de los nodos cuyo comportamiento es inadecuado en una MANET [Mart'00] [Zhon'03], ello nos lleva a pensar que serán los nodos egoístas quienes con mayor frecuencia creen problemas de funcionalidad a estas redes. Los principales problemas o efectos que la proliferación de nodos egoístas pueden tener son:

- Particionado de la red: si el nodo egoísta participa en el descubrimiento de rutas pero no reenvía paquetes de datos, y todas las rutas entre dos partes de la red pasan por dicho nodo, en la práctica ambas redes quedarán separadas. En la Figura 4, el nodo J estará en todas las rutas que vayan de algún nodo de la Zona A de la red a la Zona B, o viceversa (el nodo K también está en esta situación). Pues si se diese la circunstancia desafortunada de que J fuese egoísta, las dos redes se quedarían aisladas la una de la otra hasta que por el movimiento de los nodos se pudiesen establecer nuevas rutas que no pasaran por J.

- Reducción de la productividad: los cambios de rutas necesarios para evitar a los nodos egoístas tienen un coste en tiempo, por lo que la proliferación de nodos

4 Aunque la detección de *grey holes* puede ser más difícil que la de *black holes*.

egoístas moviéndose por el alcance de la red afectará negativamente al número de paquetes de datos efectivamente transmitidos por unidad de tiempo. Igualmente, la no identificación de un nodo como egoísta y el intento de encaminar paquetes a través suyo degradará aún más el rendimiento de la red en su conjunto.

- Aumento de la latencia extremo a extremo: cuanto más se tarde en obtener una ruta, más se tarda en enviar los datos. Y si la ruta es poco fiable y hay que hacer reenvíos, la latencia extremo a extremo puede aumentar considerablemente.

2.2 Soluciones propuestas

El **problema de los nodos maliciosos o egoístas** en redes MANET, que hemos esbozado en el apartado anterior como uno de los relacionados con nodos incluidos en las denominaciones genéricas de *black hole* o *grey hole*, está presente desde hace unos años en la literatura. Los autores han definido múltiples esquemas que permiten reducir sus efectos sobre diversos protocolos de encaminamiento, proponiendo incluso ciertas modificaciones a los mismos. Para encarar el problema, es evidente que se ha de ser consciente del mismo, por lo que la **detección de nodos egoístas** sería un primer paso lógico. Qué hacer cuando se ha detectado el nodo egoísta sería el segundo paso, y en este caso la mayoría de autores se decantan por dos opciones: excluir al nodo egoísta de la MANET, o "convencerle" de los beneficios que tiene ser un nodo colaborativo mediante técnicas de incentivación o estimulación de la cooperación. En estas últimas propuestas, no es necesario el proceso de detección, ya que pretenden que el nodo, desde su inserción en la red, participe en la misma colaborativamente, gracias precisamente a los premios o recompensas que ello supone.

En lo que queda de este capítulo vamos a mostrar una visión panorámica de las diferentes propuestas realizadas hasta la fecha en cada uno de estos aspectos del problema.

2.2.1 Detección

Una vez descartada la posibilidad de transmitir en la red MANET a través de nodos en los que se confía a priori, el único camino posible para conseguir que los mensajes lleguen a nodos que están a más de un salto es que los nodos intermedios sean colaborativos. Pero cuando un nodo no lo es, es necesario detectarlo, para tomar las medidas adecuadas.

Los mecanismos de detección han de ser enfrentados a la medición de su exactitud, y para ello se pueden utilizar dos parámetros: el nivel de falsos positivos y el nivel de falsos negativos. Una detección presenta un **falso positivo** cuando deduce que un nodo es malicioso cuando en realidad no lo es. Análogamente, presenta un **falso**

negativo cuando la detección no es capaz de identificar a un nodo malicioso como tal, calificándolo de colaborador. Por tanto, un mecanismo de detección será tanto más exacto cuanto menos falsos positivos y falsos negativos presente.

Marti, Giuli y otros [Mart'00] proponen un doble mecanismo, como extensión del protocolo DSR, para mitigar los efectos negativos de la presencia de nodos egoístas. En primer lugar, proponen un ***watchdog*** para detectar qué nodos no participan en las rutas de reenvío de paquetes, y, en segundo lugar, definen un *Pathrater* (valorador de caminos, en traducción libre), que se encarga de valorar la fiabilidad de las rutas para evitar que éstas pasen por los nodos egoístas. El *watchdog*, que se encuentra en ejecución en cada nodo, y que va a ser el concepto más importante de esta Tesis, consigue realizar su tarea escuchando la red en modo promiscuo. Si el siguiente nodo de la ruta encamina el paquete, se le considera colaborativo. En caso contrario, se le considera egoísta, y entonces el mecanismo *Pathrater* evitará usarlo para el envío de mensajes en el futuro.

Este mecanismo básico del *watchdog* se convierte, pues, en pieza angular de cualquier mecanismo posterior, y la mayoría de soluciones de detección de nodos maliciosos se basan en él. Pero hay que decir que no es un mecanismo excesivamente fiable, sobretodo en redes móviles inalámbricas, principalmente, porque el medio aéreo está sujeto a ciertas carencias y problemas que lo hacen menos fiable que otros medios, y ello afecta a la exactitud de la detección del *watchdog*. La movilidad, tanto por la velocidad como por las trayectorias de los nodos, también afectan negativamente a este tipo de mecanismos de detección. Por ello, y con objeto de mejorar la exactitud de la misma, eliminando falsos positivos y falsos negativos, ha habido otras propuestas derivadas de ésta.

Buchegger y Le Boudec [Buch'05] proponen CONFIDANT que, en la línea de [Mart'00], además del *watchdog*, utilizar un mecanismo de **reputación** en sustitución del *Pathrater* para proteger a DSR. Según estos autores, un mecanismo de este tipo debería tener las siguientes funcionalidades:

- representación de la información y su clasificación, para determinar cómo se almacenan los eventos monitorizados y cómo se traducen en tasas de reputación para activar el mecanismo de respuesta

- uso de información de segunda mano, proveniente de los nodos vecinos, y que se utilizará como datos adicionales para la obtención de la reputación de un nodo, teniendo en cuenta, además, los efectos que los nodos maliciosos pueden tener en la calidad de esa información

- confianza, ligada a la reputación, ya que el establecimiento de dicha confianza será básica para tener en mayor o menor consideración la información que de otros nodos proporcionen los vecinos

- redención y respuestas secundarias, para evitar que un nodo, una vez aislado, no pueda volver a integrarse en la MANET si su comportamiento cambia

Para tratar la información recopilada por el *watchdog* y por los vecinos, CONFIDANT utiliza un *watchdog* bayesiano, en una solución similar a la que hemos implementado sobre el simulador ns-2 para esta Tesis, aunque en nuestro caso, lo hemos desarrollado para proteger al protocolo AODV. En el capítulo siguiente profundizaremos en la solución que se propone.

Kargl, Klenk y otros [Karg'04] proponen MobIDS como mecanismo de detección de nodos maliciosos. Este sistema, básicamente, se compone de varios sensores software, que se ejecutan en paralelo para obtener una valoración local de los nodos que existen alrededor del nodo en cuestión. Estas valoraciones locales se comparten posteriormente con otros nodos para obtener una valoración global del nodo al que se está evaluando. Para funcionar, MobIDS debe estar integrado en una arquitectura de seguridad llamada SAM, de los mismos autores, y utilizar información procedente del protocolo Secure DSR, prerrequisitos muy fuertes que pueden hacer que esta propuestas sea poco útil. Sin embargo, lo novedoso de esta aproximación es la cuestión referente a que no sea un único *watchdog* por nodo el que vigile el comportamiento de los vecinos, sino que sean varios especializados.

Existen otros mecanismos de detección más o menos parecidos a los citados, como CORE [Mich'02] o SORI [Qi'04], basados en cierto grado de compartición de la información de reputación, y que pueden ser consultados a través de las referencias.

2.2.2 Aislamiento

Una vez detectado el nodo malicioso, sea o no cierto que lo es, la red debe tomar alguna decisión al respecto. Evidentemente, al tratarse de una red autoconfigurable, cada nodo es el que debe tomar la decisión de forma individual. Lo más corriente es que, tras la constatación de que uno de sus vecinos es un *black hole*, el nodo afectado tome la decisión de aislarlo, es decir, de no usarlo para ninguna ruta y de no colaborar con él en las peticiones que éste realice. La propuesta de [Mart'00], sin embargo, no excluye a los nodos egoístas, sólo los evita en las rutas, aunque sigue permitiendo que éstos usen los recursos de la red.

Podría parecer que, una vez detectado el nodo malicioso y aislado, ya todo está solucionado. Independientemente de los problemas que ya hemos citado debidos a la reducción en el número de nodos colaborativos disponibles. Combinando los efectos de las redes inalámbricas, como los nodos ocultos/expuestos, con el patrón de movilidad, y con el hecho de que un nodo colaborativo deje de transmitir paquetes provenientes de un nodo que, a su modo de ver, es malicioso, podemos encontrarnos con curiosos resultados, como que el nodo legítimo sea visto como no colaborativo por un tercero con el que el nodo malicioso sí colabora.

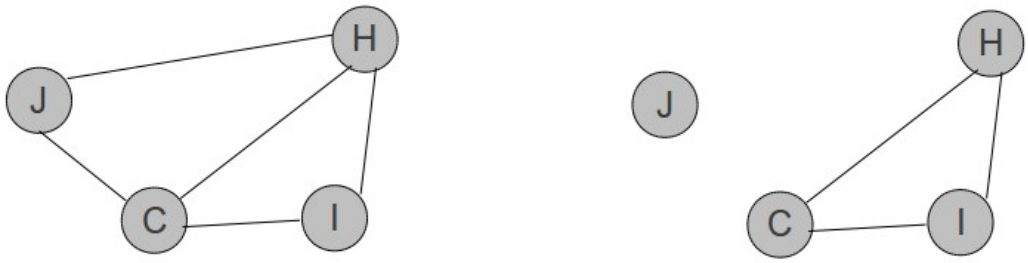

Figura 5. Efecto del aislamiento.

En la Figura 5, el nodo colaborativo J detecta que C es no colaborativo, y decide aislarlo, no reenviando paquetes de C. Pasado un tiempo, el nodo H, que no sabe que C no colabora con J, podría detectar que J no reenvía paquetes de C, e identificará a J como malicioso también, dejándolo aislado. Si J era la única ruta disponible para que este segmento de la MANET se conectara con el resto de la red, se ha producido el efecto colateral de dejar a C, H e I sin conexión a la misma, cuando lo único que J pretendía era dejar sin servicio a C por su comportamiento.

De ahí nace la necesidad de que la exactitud de la detección del *watchdog* sea la mayor posible, eliminando la mayor cantidad de falsos positivos y negativos, y de que el mecanismo de respuesta ante este tipo de nodos sea modulado en el tiempo. A mayor exactitud y cobertura del mecanismo, menores perjuicios para la red. Por resumirlo de alguna manera, la MANET no se puede permitir “condenar” a “cadena perpetua” a los nodos identificados (quizá erróneamente) como no colaborativos, sino que tendrá que implementar algún mecanismo de “reinserción” si no se quiere acabar con la existencia de la propia red a medio plazo. En este sentido, la propuesta de Buchegger y Le Boudec [Buch'05] también propone mecanismos para terminar con el aislamiento de los nodos pasado un tiempo.

2.2.3 Incentivación

Ya hemos visto que el tándem detección-aislamiento puede dar al traste con la MANET, particionándola o reduciendo muchísimo su productividad si el número de nodos egoístas es elevado. Un elevado número de propuestas en la literatura se decantan por incentivar o motivar a todos los nodos para que colaboren, algo que parece muy natural si precisamente el funcionamiento de la MANET comunitaria se debe basar en la cooperación. Son mecanismos que, muy gráficamente, podríamos ver como 'de palo y zanahoria', y no sólo de 'palo'. Aunque desde un punto de vista amplio y poco riguroso se podría percibir que la amenaza del aislamiento debería ser una motivación suficiente para los nodos, las aproximaciones detección-aislamiento no tienen en cuenta las características concretas de cada nodo, por lo que se podrían estar excluyendo nodos injustamente, por ejemplo, si éstos están dotados de poca batería o de una radio de menor alcance.

La principal limitación de estos sistemas basados en la motivación de los nodos es

que no son capaces de tratar con nodos verdaderamente maliciosos o fallidos, sólo con nodos egoístas, por lo que son soluciones específicas.

Las principales propuestas para implementar sistemas de incentivación para los nodos de una MANET se centran en dos áreas: pago virtual, y negociación. En el primer caso, cada nodo que retransmite un paquete recibe una compensación por ello, en forma de algún tipo de mecanismo de pago virtual, y que le servirá para conseguir que sus propios mensajes lleguen a su destino. En el segundo caso, cada par de nodos vecinos de la MANET negocian el grado de egoísmo de cada uno para los paquetes recibidos del otro, de forma que todos los nodos de la red conocen de antemano cuál será el comportamiento de sus vecinos, actuando en consecuencia. Por tanto, cuánto más colaborativo se muestre un nodo en fase de negociación, más obtendrá de sus vecinos en el acuerdo entre ambos.

La propuesta más conocida en cuanto a mecanismos basados en **pago virtual** es la de Buttyán y Hubaux [Butt'03], en la que definen una moneda virtual a la que llaman *nuglet*, y que va a ser usada para construir un mecanismo de reenvío de paquetes gestionado por el hardware. Las precondiciones del esquema propuesto son dos:

- cada nodo está equipado con un contador de *nuglets*, que debe estar necesariamente dentro de un módulo de seguridad a prueba de manipulaciones (*tamper-proof*, en inglés).

- cada nodo debe estar perfectamente identificado a través de un mecanismo de Infraestructura de Clave Pública (o PKI, de sus siglas en inglés), cuyo certificado también esté en el módulo de seguridad.

Estos autores proponen un mecanismo en el que, cuando un nodo desea enviar un paquete, consulta su contador de *nuglets* y si tiene suficientes como para conseguir retribuir a todos los nodos intermedios hasta el destino, lo envía al primer nodo intermedio de la ruta, y ejecutando el protocolo de sincronización de *nuglets* controlado por el módulo de seguridad. Cada nodo intermedio irá recibiendo su *nuglet* por el reenvío del paquete, hasta que éste llegue a su destino. Dichos *nuglets* son los que luego cada nodo usa para enviar sus propios paquetes siguiendo este mismo esquema.

Las principales críticas a la aproximación de Buttyán y Hubaux podemos resumirlas en:

- Las precondiciones son muy fuertes: es muy complicado montar una PKI sobre una MANET, y si se ha de recurrir a un sistema preexistente ya no estamos ante una red *ad hoc*. Por otro lado, es complicado construir hardware que sea *tamper-proof*, por lo que un usuario malicioso podría disponer de crédito ilimitado para el envío de sus paquetes y seguir negándose a reenviar los de otros sin verse penalizado por ello, si más que manipular el contador de *nuglets*.

- Los propios autores reconocen que no pueden extender el modelo para encaminamiento *multicast*, y que se pueden perder *nuglets* por el camino, por lo que el emisor no consigue que su paquete llegue a destino, y quizá algún nodo intermedio no llegue a cobrar su recompensa por reenviar el paquete de otro.

- Se pueden crear nodos con varios módulos de seguridad, por lo que la autenticidad del nodo no queda garantizada ni siquiera con una PKI.

- El uso de las técnicas criptográficas puede suponer una sobrecarga importante en nodos con escasa potencia computacional.

- Se pueden producir situaciones de cierta inanición en los nodos del borde de la MANET, que no son requeridos por ningún otro para reenvío de paquetes, pero que sí consumen rápidamente su crédito de *nuglets* para en envío de los suyos propios. Por ello, y por las pérdidas de nuglets citadas anteriormente, los autores se ven obligados a definir que, periódicamente, el sistema deba recargar el contador de *nuglets* de cada nodo con un determinado valor, lo que desvirtúa la motivación de obtener *nuglets* a cambio de reenviar paquetes de otros.

- No se tiene en cuenta el tamaño de los paquetes que se transmiten para valorar el coste del servicio. Se cobra sólo un *nuglet* por paquete reenviado.

Una propuesta alterativa a la de Buttyán y Hubaux, pero que aprovecha algunas de las conclusiones de éstos, es la de Zhong, Chen y Yang [Zhon'03], llamada SPRITE. Coincide con la propuesta anterior en que está pensada para el protocolo DSR y en la necesidad de que exista una Infraestructura de Clave Pública que provea de un certificado a cada nodo. Sin embargo, como mejora inicial no requiere de hardware especial a prueba de manipulaciones. En cambio, sí necesita de una autoridad central (*Central Clearing Service*, o CCS), ubicada fuera de la MANET, y a la que cada nodo se conecta cuando dispone de acceso a Internet. Esta CCS llevará la contabilidad de todas las operaciones de reenvío de paquetes y actualizará los saldos de los nodos en consecuencia.

El mecanismo propuesto se basa en que cada nodo intermedio de la ruta reporta, mediante un recibo al CCS, de que ha hecho *forward* del paquete recibido. El CCS sólo da por buenos recibos de un nodo en una ruta si nodos posteriores de dicha ruta reportan a su vez recibos del mismo paquete. Es el mismo CCS quien calcula para cada entrega cuánto debe pagar el emisor del paquete y cuánto reciben cada uno de los nodos intermedios por sus servicios, y la suma de éstas cantidades no necesariamente debe ser igual a lo que se carga al emisor. Para que el sistema funcione adecuadamente, por tanto, a cada nodo le ha de resultar "rentable" el reenvío del paquete. También aquí nos encontramos con que periódicamente, el CCS reparte créditos uniformemente para evitar que la red se quede sin crédito. Se cita también la posibilidad de que el CCS permita la compra de crédito de la red con dinero real.

Los autores demuestran que su sistema es infalible en entornos de reenvío de paquetes *unicast* y en el descubrimiento de rutas, pero no se demuestra que sea imposible engañar al sistema en un entorno de reenvío de paquetes *multicast*.

Los puntos débiles que identificamos en esta propuestas son:

- Como en la propuesta anterior, existe la fuerte precondición de disponer de una PKI, y que también el uso de las técnicas criptográficas puede suponer una sobrecarga importante en nodos con escasa potencia computacional. Asimismo, coinciden en el potencial problema de inanición de los nodos de borde, y, de nuevo, se decantan por el reparto de indiscriminado y periódico de crédito.

- Los autores reconocen que el espacio de almacenamiento necesario en los nodos si tardan en conectarse a Internet para reportar al CCS puede ser grande.

- Se requieren dos entidades externas para hacer funcionar correctamente la MANET, el CCS y la Autoridad Certificadora, lo cual no parece muy lógico si se está hablando de redes *ad hoc*.

De una forma alternativa a las dos estudiadas hasta el momento, Toh, Kim y otros [Toh'10] proponen SCNP (*Selfish Check Negotiation Protocol*), un mecanismo de **negociación** para modular el comportamiento egoísta de los nodos sobre AODV. En este caso no nos encontramos ante un mecanismo puramente de incentivación monetaria, sino del establecimiento de un marco en el que dos nodos vecinos saben exactamente en qué medida pueden contar con su vecino, y adaptar su propio grado de colaboración con él al nivel negociado. Este proceso se desarrolla cuando los mecanismos de detección no son concluyentes para dilucidar si un nodo es egoísta o no.

Esta negociación puede, o debe, hacerse por cada flujo, por cada aplicación o por cada usuario humano. También puede negociarse un acuerdo más amplio que cubra varios aspectos de la colaboración entre múltiples usuarios, es decir, que para poder ingresar en la MANET se exija que el nodo acepte el acuerdo preexistente negociado por los nodos circundantes.

Los autores reconocen que su propuesta es muy simple y que deja pendientes de investigación aspectos como la programabilidad del grado de egoísmo del nodo por parte del usuario humano, la relación entre egoísmo y seguridad, y la elaboración de un esquema de recompensas y penalizaciones para quienes se salgan del acuerdo.

Dado que ya establecimos en el apartado 2.1 que el egoísmo como mecanismo de ahorro baterías carece de sentido, podemos inferir asimismo que no deberían haber nodos que no reenvien paquetes debido a esta razón. Ello nos lleva a pensar que **los *black hole* que nos vamos a encontrar en las MANETs serán realmente nodos maliciosos** (o averiados), por lo que los mecanismos de incentivación no parecen una solución apropiada para este problema.

CAPÍTULO 3. *WATCHDOG* BAYESIANO COLABORATIVO

3.1 Trabajos previos

En el capítulo anterior estudiábamos las diferentes propuestas para la detección de *black holes* en redes MANET. Conocimos, sin entrar en mucha profundidad, las aproximaciones de Marti [Mart'00], Buchegger [Buch'05] y Kargl [Karg'04]. En este apartado empezaremos presentando la propuesta que el Grupo de Redes de Computadores del DISCA ha realizado con anterioridad, y a partir de la cuál se ha realizado su extensión en esta Tesis de Master.

3.1.1 Sistemas de detección de Intrusos basados en Watchdogs

El contenido de este apartado está ampliamente basado en el capítulo 5 de la Tesis Doctoral de Jorge Hortelano [Hort'11]. La solución propuesta por Hortelano, Calafate y otros [Hort'10] se basa en la detección de nodos maliciosos utilizando un ***watchdog* bayesiano** y un mecanismo de reputación. Se basaron en las asunciones siguientes:

- cada nodo dispone de un interfaz inalámbrico que permite su funcionamiento en modo promiscuo.
- cada nodo tiene una implementación del watchdog que monitoriza los paquetes enviados y recibidos en su vecindario.
- cada nodo tiene al menos tres vecinos, para garantizar una suficiente densidad para que puedan existir diferentes rutas y cada nodo pueda ser monitorizado por varios.

Para determinar si un nodo presenta un comportamiento malicioso. el *watchdog* diseñado en primer lugar cuenta los paquetes recibidos de sus vecinos usando sobreescucha, y aquellos que han de ser reenviados. Para cada nodo, se define un **nivel de confianza** como el ratio entre los paquetes que ha recibido y que debía reenviar, y los que efectivamente ha reenviado. Evidentemente, es muy complicado que un nodo tenga un índice de confianza del 100%, más, si cabe, debido a las colisiones y al ruido de la señal propios de las redes inalámbricas.

Además del ruido y de las colisiones, el otro factor que influye en la exactitud de

la detección del *watchdog* es su movimiento. A mayor velocidad, más probabilidad de pérdida de paquetes debido a efectos físicos de la señal o al alejamiento entre emisor y receptor. Por ello, el *watchdog* también se debe equipar con un umbral de tolerancia que permita un cierto grado de pérdida de paquetes sin acusar de malicioso a un nodo, reduciendo el problema de los **falsos positivos**. Dicho umbral se debe implementar en cada tipo de tráfico que el nodo maneje, para la detección de *grey holes*.

También la movilidad provoca que los la mayoría de los ataques sean temporales, es decir, sólo se manifiesten durante un determinado periodo de tiempo, no llegando a ser detectados por el *watchdog*, por lo que se pueden dar casos de **falsos negativos**. Por ello, y para reducir parte de los problemas relacionados con la movilidad de los nodos, el *watchdog* también utiliza un mecanismo de devaluación de las observaciones, de forma que las más antiguas pesen menos que las más recientes en el cómputo de la maliciosidad del nodo.

La implementación del *watchdog* inicialmente realiza las siguientes actividades principales:

1. lee paquetes de la tarjeta inalámbrica (que está en modo promiscuo).
2. genera la lista de vecinos.
3. detecta el *black hole.*
4. libera los recursos que ya no va a usar.
5. se desconecta por un tiempo aleatorio para ahorrar.

Si el *watchdog* no escucha ningún paquete de alguno de sus vecinos durante largo rato, lo elimina de su lista de vecinos, ya que se infiere que habrá salido del rango de escucha del nodo.

La implementación de este *watchdog*, por su forma de actuación, es independiente del protocolo de encaminamiento seleccionado. Sin embargo, para su evaluación se implementó sobre el simulador ns-2, eligiendo AODV como protocolo de encaminamiento de la MANET. Los resultados de las simulaciones con esta versión del *watchdog* concluyeron que:

- este *watchdog*, pese a todo, no es capaz de afrontar correctamente la movilidad de los nodos.
- la probabilidad de detección de un atacante no se basa sólo en el número de éstos, sino también en el número total de nodos.
- queda pendiente cómo afrontar el ruido de la señal y cómo inferir si un nodo está

o no en el alcance del *watchdog* cuando se está moviendo.

3.1.2 Mejorando el IDS: Watchdog Bayesiano

Por estas razones, en el grupo de investigación se planteó la conveniencia de mejorar el *watchdog*, implementando un filtro bayesiano que amortiguase los efectos del ruido causado por la movilidad de los nodos. La idea es que pueda atenuar el problema de los falsos positivos y falsos negativos usando información histórica.

Un **filtro bayesiano** estima probabilísticamente el estado de un sistema dinámico a partir de observaciones ruidosas. En un instante de tiempo t, el estado es estimado por una variable aleatoria θ, que es desconocida. Esta incertidumbre se modela asumiendo que la propia θ se representa de acuerdo a una distribución que se actualiza conforme están disponibles nuevas observaciones. Se la llama Creencia (Belief), $Bel_t(\theta)$. Para ilustrarlo, asumanos que hay una secuencia de observaciones indexadas en el tiempo z_1, z_2, ..., z_n. $Bel_t(\theta)$ se define entonces por la densidad posterior sobre la variable aleatoria θ condicionada a todos los datos observados disponibles en el instante t:

$$Bel_t(\theta) = p(\theta|z_1, z_2, ..., z_t)$$

En esta aproximación, la variable aleatoria θ está en el rango [0,1]. A continuación, usamos la distribución Beta(α, β) como distribución de la Creencia, porque es adecuada para este intervalo de valores:

$$Bel_t(\theta) = Beta(\alpha_t, \beta_t, \theta)$$

donde α y β representan el estado del sistema, y se actualizan de acuerdo a las siguientes ecuaciones:

$$\alpha_{t+1} = \alpha_t + z_t$$

$$\beta_{t+1} = \beta_t + z_t$$

La función Beta necesita dos parámetros que se actualizan en cuanto están disponibles nuevas observaciones. En nuestro enfoque, la observación z_t representa la información del *watchdog* obtenida en el intervalo [t, t + 1] sobre el porcentaje de paquetes no reenviados.

Los filtros bayesianos son una herramienta que ha sido extensivamente utilizada en determinado tipo de sistemas de información, como el tratamiento de imágenes o los filtros anti-SPAM, por ejemplo. También la solución de *watchdog* de Buchegger [Buch'05] comentada con anterioridad los utiliza.

El *watchdog* bayesiano se configura mediante tres parámetros:

- Umbral de tolerancia (γ): define el momento a partir del cual se considera que un nodo es malicioso. Un valor alto obliga a que el *watchdog* necesite muchas observaciones para hacer una detección, pero ésta es más robusta. Por contra, un valor bajo, lógicamente, generará más falsos positivos.

- Atenuación (*fading, u*): indica el peso de la información antigua obtenida, Cuanto más cerca de 1, más igualdad de influencia hay entre una observación reciente y una antigua. Valores altos dificultan la detección de cambios de comportamiento, pero mitigan los efectos del ruido.

- Tiempo de actualización: es el tiempo que ha de pasar entre dos instantes para que se calculen de nuevo los parámetros α y β, necesarios en la distribución Beta en la que se basa el filtro bayesiano. Si se actualizan α y β muy frecuentemente, y el canal es muy ruidoso, es posible que ningún paquete haya sido reenviado correctamente, por lo que el nodo investigado sería declarado malicioso. Por contra, si se actualiza poco frecuentemente, quizá el tiempo necesario para la detección sea inaceptable.

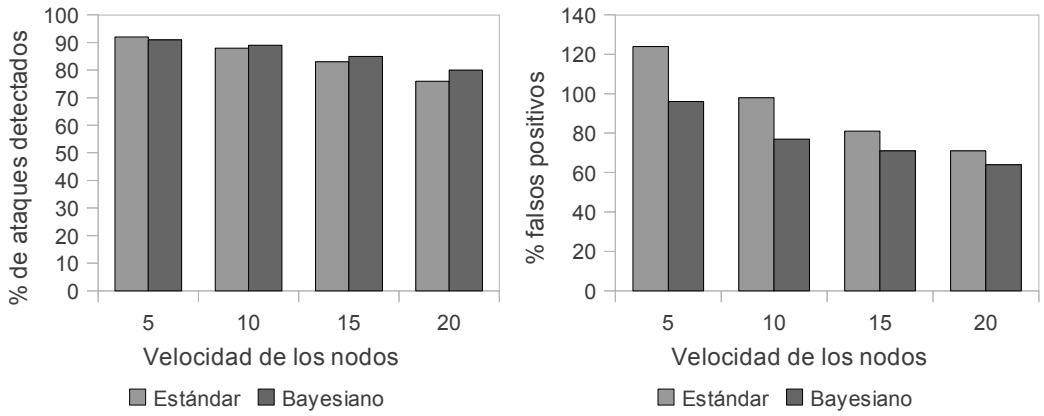

Figura 6. Comparación del watchdog bayesiano frente al estándar.

Tras su implementación como módulo de extensión del simulador Network Simulator-2 (ns-2), con AODV como protocolo de encaminamiento, el análisis de los resultados del *watchdog* bayesiano [Hort'10] ha demostrado que:

- Se ha aumentado ligeramente el porcentaje de ataques detectados, como se puede observar en la Figura 6(a), sobretodo cuánto mayor es la movilidad de los nodos, lo que supone una reducción de los falsos negativos.

- Se ha reducido un 20% de media el ratio de falsos positivos (Figura 6(b)) respecto del *watchdog* estándar, aunque esta reducción es menor cuanto mayor sea la movilidad de los nodos.

– En el 95% de los casos, el *watchdog* bayesiano ha detectado antes a los nodos maliciosos que el estándar.

3.2 Nuestra aportación: el Watchdog Bayesiano Colaborativo

Un *watchdog* bayesiano obtiene mejores resultados que un *watchdog* que no implemente esta aproximación. Pero, ¿es factible mejorarlo para que sus resultados sean aún más exactos? Tomando las ideas del *watchdog* bayesiano de Buchegger [Buch'05] sobre DSR y la implementación de Hortelano sobre AODV en el simulador ns-2, nos planteamos si la utilización de información de reputación procedente de nuestros vecinos sobre nuestros vecinos comunes mejoraría la calidad de la detección. ¿Obtendremos resultados más exactos si incorporamos información de segunda mano al *watchdog* bayesiano?

La idea central es, pues, construir un *watchdog* bayesiano, partiendo de la base del implementado por Hortelano, y que, además, sea colaborativo con sus homólogos de los nodos vecinos. La colaboración se basa en el siguiente algoritmo:

1. Cada nodo calcula los valores de α y β, necesarios para la detección basada en filtro bayesiano

2. Periódicamente, cada nodo publica la lista de sus vecinos, a los que califica publicando también los valores de α y β que ha calculado para cada uno de ellos

3. Cada nodo que recibe esta información la almacena para aquellos nodos que son vecinos suyos y del vecino del que la ha obtenido, es decir, de los vecinos comunes a ambos

4. Finalmente, para intentar la detección de nodos maliciosos, además del filtro bayesiano, el nodo promedia (de forma ponderada) a los α y β obtenidos por él mismo con la media aritmética de las reputaciones que sus vecinos le han informado sobre el nodo que está siendo investigado.

Sea i el nodo que está llevando a cabo la detección, y sea N_i el conjunto de vecinos a un salto del nodo i. Ya sabemos que este nodo calculará sus valores de $\alpha(i)_j$ y $\beta(i)_j$ para cada uno de sus vecinos j. Además, tendrá que calcular unos valores de $\alpha(i)_j^k$ y $\beta(i)_j^k$, como valores de reputación de cada uno de sus vecinos procedentes de éstos mismos[5].

5 Por $\alpha(i)_j^k$ denotamos el valor de α calculado en el nodo i como reputación agregada procedente de todos sus vecinos j, que, a su vez, la han calculado observando a sus propios vecinos k.

$$\forall_{j \in N_i} \begin{Bmatrix} \alpha(i)_j \\ \beta^i_j \end{Bmatrix} \qquad \forall_{j \in N_i} \left\{ \forall_{k \in N_j} \begin{Bmatrix} \alpha^i_{j(k)} \\ \beta^i_{j(k)} \end{Bmatrix} \right\}$$

Sea δ el peso que deseamos darle a las opiniones que nuestros vecinos publican, calculamos los valores de α' y β' que se le pasarán a la función Beta en cada instante t por cada vecino como

$$\forall_{j \in N_i} \quad \forall_{k \in N_j} \quad \alpha(i)'_j = \frac{\alpha(i)_j + \delta \cdot promedio(\alpha(i)^k_j)}{2}$$

$$\forall_{j \in N_i} \quad \forall_{k \in N_j} \quad \beta(i)'_j = \frac{\beta(i)_j + \delta \cdot promedio(\beta(i)^k_j)}{2}$$

Veamos un ejemplo numérico de la aplicación de estas expresiones basado en la MANET que se representa en la Figura 7. En este caso, las informaciones que recibiría el nodo A desde sus vecinos serían las siguientes:

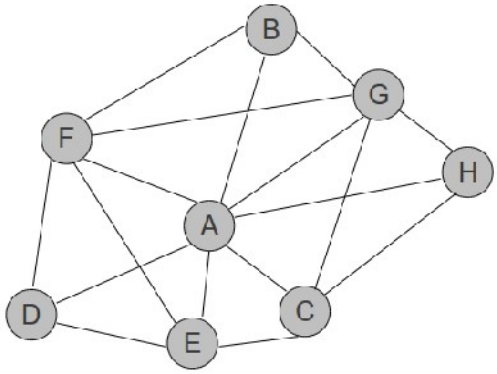

Figura 7. MANET de ejemplo para calcular α(i) y β(i).

Vecino	Reputaciones que informa[6] ($\alpha(i)_j$ y $\beta(i)_j$)
B	F: {5,1}, G:{11,1}
C	E:{1,4}, G:{18,1}, H:{1,1}
D	E:{1,2}, F:{7,1}
E	C:{34,1}, D:{1,6}, F:{15,1}
F	B:{1,1}, D:{1,4}, E:{1,3}, G:{13,1}
G	B:{1,2}, C:{52,1}, F:{27,1}, H:{1,6}

Tabla 1. Ejemplo de reputaciones emitidas por los nodos

6 También recibe la reputación sobre él mismo, pero la descarta, ya que no le es de ninguna utilidad.

Con estos datos, el nodo A obtendría las siguientes reputaciones medias de $\alpha(A)_j^k$ y $\beta(A)_j^k$ de sus vecinos en ese instante de tiempo, tanto las $\alpha(A)_j$ y $\beta(A)_j$ obtenidas por él mismo como las de "segunda mano" o indirectas:

Vecino	Reputaciones indirectas medias	Reputaciones directas	Parámetros finales[7]
B	{1, 1.5}	{1, 2}	{1, 1.75}
C	{43, 1}	{55, 1}	{49, 1}
D	{1,5}	{1, 4}	{1, 4.5}
E	{1,3}	{1, 1}	{1, 2}
F	{14,1}	{3, 1}	{8.5, 1}
G	{14,1}	{6, 1}	{10, 1}

Tabla 2. Ejemplos de $\alpha(i)_j$ y $\beta(i)_j$ obtenidos con los datos de la tabla 1

De la tabla resultado del ejemplo podemos apreciar (nodo C) que la incorporación de las reputaciones obtenidas por nuestros vecinos al cálculo de los valores de los dos parámetros de la función Beta modula los valores de dichos parámetros, de forma que suaviza el mecanismo de detección. Por ejemplo, si la trayectoria de un nodo hace que vaya paulatinamente quedando fuera del alcance del nodo desde el que se detecta, pero sigue dentro del alcance de uno de sus vecinos, sin la información de este vecino el detector pronto lo identificaría como malicioso, mientras que en este caso la información remitida por el vecino común reduciría el impacto de la evaluación hasta que el nodo desapareciese de la lista de vecinos. En la tabla anterior, basándose sólo en reputaciones directas, el nodo A hubiese considerado a C malicioso. Sin embargo, la reputación de C ante sus vecinos comunes con A no es tan mala, por lo que modula la reputación directa, lo que debería inducir una reducción de los falsos positivos.

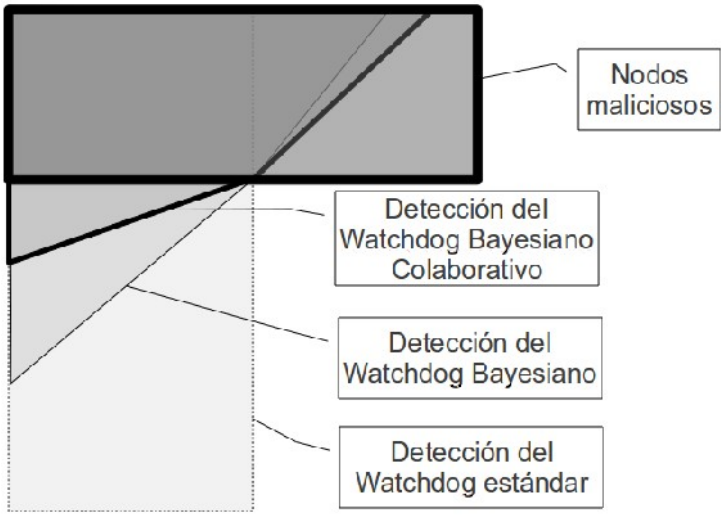

Figura 8. Hipótesis de los resultados esperados.

7 Suponemos un valor de $\delta = 1$

Por contra, si un nodo malicioso se va acercando hacia el nodo que está evaluando, y sus vecinos reportan un cierto grado de maliciosidad, la situación de partida de la evaluación del nodo es mucho más propensa a declararlo malicioso por la influencia de las reputaciones que los vecinos informan. Por tanto, también se espera que este mecanismo reduzca los falsos negativos. Se puede apreciar gráficamente el comportamiento que se espera del *watchdog* bayesiano colaborativo que proponemos en la Figura 8.

La problemática de la detección del falso negativo en las baterías de simulación es algo más compleja. Las probabilidades de su detección dependen mucho de la cantidad de nodos que haya, de la posición del nodo malicioso y del volumen de tráfico que circule por su zona, Evidentemente, si el nodo se encuentra aislado o por su zona no circula tráfico no podrá ser detectado, pero, por otro lado, su influencia negativa sobre la red también será nula. Consecuentemente, los *watchdogs* no lo detectarán, pero ello tampoco afectará al funcionamiento de la MANET.

El algoritmo de detección del *watchdog* se basa en dos bloques diferenciados, de modo que si cualquiera de ellos devuelve un resultado positivo, el nodo evaluado se considerará malicioso. La primera parte del mecanismo de detección es una función de densidad probabilística, tal y como se implementó en el *watchdog* bayesiano, ya que en esta parte no ha habido cambios. La segunda parte es la que se basa en los valores de $\alpha(i)_j$ y $\beta(i)_j$ obtenidos usando las expresiones definidas anteriormente, a partir de las reputaciones que nos han comunicado nuestros vecinos, en lugar de usar sólo las reputaciones directas. Muy simplificadamente el mecanismo de detección en el *watchdog* colaborativo, después de recopilar información sobre reputaciones directa e indirectamente, sería el siguiente:

Algoritmo 1

```
1     Para todo j vecino de este nodo
2         Si ([detección bayesiana]
3               o [detección colaborativa])
4         entonces Nodo j es malicioso
5         fSi
6     fPara
```

3.3 Estudio preliminar de resultados

Una vez planteada la propuesta y ejemplificada numéricamente, pasemos validar nuestras hipótesis sobre el mejor rendimiento del *watchdog* bayesiano colaborativo, estudiando cuáles son sus avances efectivos frente a las propuestas anteriores. Para ello, como se dijo con anterioridad, se ha implementado un módulo en C++ para el simulador ns-2 sobre el protocolo de encaminamiento AODV, y se han realizado varias baterías de simulaciones con las siguientes características:

Parámetro	**Valor**
Número de Nodos	50
Área	1000 x 1000 m.
Interfaz y Ancho de banda	802.11 con 54 Mbps
Antenas	Omnidireccionales
Velocidad de los nodos	5, 10, 15 y 20 m/s
Porcentaje de *black holes*	10%
δ	0.8
γ	0.85
fading	1
tiempo de caducidad de vecino (*neighbour time*)	1
tiempo de actualización (*observation time*)	0.2
Trafico unicast	UDP, tres flujos
Tráfico broadcast	UDP, cada 5 segundos
Tiempo de cada simulación	352 segundos

Tabla 3. Parámetros de las simulaciones.

Sobre estas premisas, se han ejecutado los escenarios de simulación simultáneamente sobre los tres tipos de *watchdog* que se desean comparar: el estándar, el bayesiano, y el bayesiano colaborativo[8]. Los resultados para cada velocidad de los nodos que se ha simulado se pueden apreciar en las Tablas 4 a 7, y los datos resumidos en la Tabla 8. En cada Tabla se evalúan siete variables:

- Exactitud: porcentaje de detecciones individuales que has sido correctas respecto de todas las que se han realizado
- Cobertura: porcentaje de *black holes* reales que han sido detectados por toda la red evaluada en su conjunto, por tanto, a mayor cobertura menos falsos negativos
- Falsos Positivos: porcentaje de *black holes* detectados, por cualquier nodo de la red, que realmente no lo eran.
- Doble detección: porcentaje de detecciones que se hubiesen obtenido

8 La comparación entre el *watchdog* estándar y el bayesiano ya se ha comentado anteriormente [Hort'10]

simultáneamente mediante el intercambio de reputaciones del *watchdog* colaborativo (condición de la línea 3 del Algoritmo 1) y mediante la parte del mecanismo de detección no modificada en este trabajo (condición de la línea 2 del Algoritmo 1). Da una idea de qué hubiese detectado nuestra propuesta sin hacer uso de la parte anteriormente implementada y, por tanto, de la mejora de la detección de nodos maliciosos.

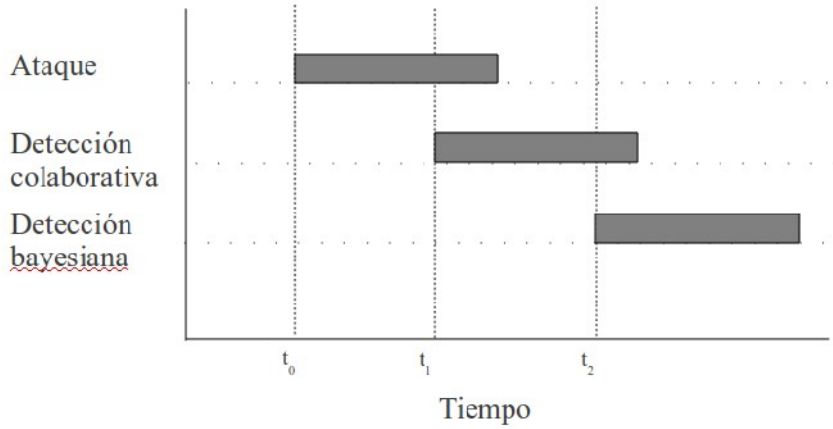

Figura 9. Linea temporal de la detección de un ataque.

- Colaborativo más rápido: porcentaje de detecciones en las que la parte colaborativa del *watchdog* (condición de la línea 3 del Algoritmo 1) ha sido la primera –o la única– en detectar el nodo malicioso. Da idea de la mejora de la detección pero, sobretodo, de la reducción de tiempo necesario para ello en el nodo en que se está ejecutando el *watchdog*. También puede verse como el tiempo durante el cual un nodo no está incurriendo en un falso negativo, como se intenta mostrar en la Figura 9. Durante el periodo $t_2 - t_1$, la detección colaborativa presenta una mejor tasa de falsos negativos frente a la bayesiana.

- Detecciones sólo por el colaborativo: cuántas detecciones han sido realizadas exclusivamente por la parte colaborativa del *watchdog*, es decir, en la que el *watchdog* bayesiano hubiese producido un falso negativo al finalizar la simulación.

- Tiempo medio de adelanto: en los casos en que ambas versiones del *watchdog* detecten un nodo malicioso. y el *watchdog* colaborativo sea el primero en indicarlo, este valor es la media de la ganancia de tiempo que el detector ha proporcionado al nodo desde el que se está midiendo, en la detección del *black hole*. Con ello, se posibilitaría actuar antes contra los nodos maliciosos. Gráficamente, es la media para toda la red del resultado de t_2-t_1 en la Figura 9.

	Standard	Bayesiano	Colaborativo	Mejoras
(A) Exactitud	61,19%	91,15%	92,23%	1,17%
(B) Cobertura	24,00%	30,00%	30,00%	0,00%
(C) Falsos Positivos	64,00%	17,00%	17,00%	0,00%
(D) Doble Detección				11,14%
(E) Colaborativo más rápido (sobre el total de detecciones)				1,04%
(F) Detecciones realizadas únicamente por colaborativo				0,78%
(G) Tiempo medio de adelanto en la detección (en segundos, para los casos (E))				5

Tabla 4. Resultados para nodos moviéndose a 5 m/s

	Standard	Bayesiano	Colaborativo	Mejoras
(A) Exactitud	57,27%	96,88%	97,39%	0,53%
(B) Cobertura	13,00%	26,00%	26,00%	0,00%
(C) Falsos Positivos	37,00%	20,00%	20,00%	0,00%
(D) Doble Detección				11,88%
(E) Colaborativo más rápido (sobre el total de detecciones)				11,88%
(F) Detecciones realizadas únicamente por colaborativo				3,77%
(G) Tiempo medio de adelanto en la detección (en segundos, para los casos (E))				5

Tabla 5. Resultados para nodos moviéndose a 10 m/s

	Standard	Bayesiano	Colaborativo	Mejoras
(A) Exactitud	55,45%	95,41%	96,06%	0,67%
(B) Cobertura	22,00%	33,00%	33,00%	0,00%
(C) Falsos Positivos	42,00%	18,00%	18,00%	0,00%
(D) Doble Detección				12,23%
(E) Colaborativo más rápido (sobre el total de detecciones)				9,66%
(F) Detecciones realizadas únicamente por colaborativo				1,78%
(G) Tiempo medio de adelanto en la detección (en segundos, para los casos (E))				5,209

Tabla 6. Resultados para nodos moviéndose a 15 m/s

	Standard	Bayesiano	Colaborativo	Mejoras
(A) Exactitud	40,45%	91,57%	92,25%	0,74%
(B) Cobertura	17,00%	37,00%	37,00%	0,00%
(C) Falsos Positivos	42,00%	29,00%	29,00%	0,00%
(D) Doble Detección				8,67%
(E) Colaborativo más rápido (sobre el total de detecciones)				5,72%
(F) Detecciones realizadas únicamente por colaborativo				0,55%
(G) Tiempo medio de adelanto en la detección (en segundos, para los casos (E))				5,001

Tabla 7. Resultados para nodos moviéndose a 20 m/s

Hay que tener en cuenta que los resultados deben verse desde dos ópticas diferentes pero complementarias: el rendimiento del *watchdog* colaborativo de forma local al nodo, y el rendimiento del *watchdog* colaborativo estudiado a nivel de toda la red. Si se estudia la exactitud de un sólo nodo detector, gracias a la mayor rapidez en la detección obtenemos, durante el periodo t_2-t_1 una detección más exacta, ya que durante ese periodo el *watchdog* bayesiano estaría produciendo un falso negativo, mientras que el colaborativo ya habrá producido un positivo, por lo que su cobertura individual es mayor. A nivel global, estas mejoras se representan en la Figura 10, y representan una mejora media del 0,78% de la exactitud.

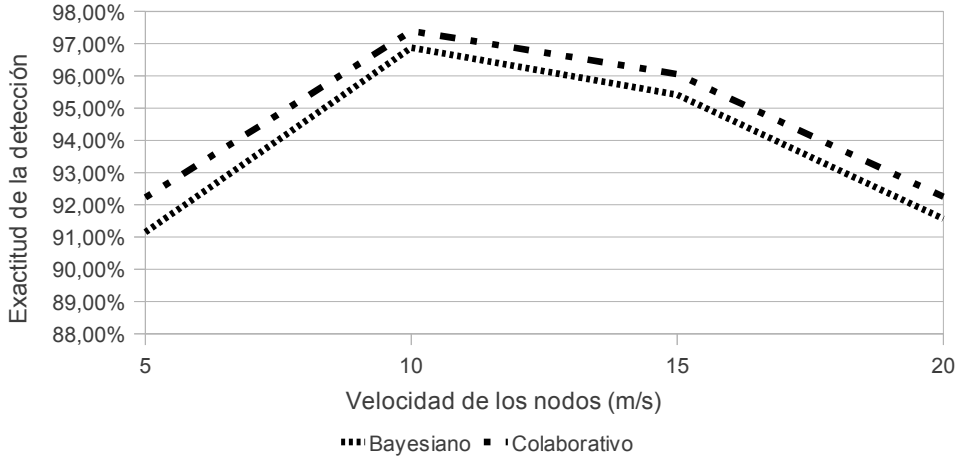

Figura 10. Comparativa de la exactitud de la detección.

De la Figura 11, nos limitaremos a observar que la tendencia respecto de la velocidad de los nodos es que, tanto la cobertura del *watchdog* como el nivel de falsos positivos encontrados, es ascendente con la velocidad. Esta conclusión es compatible con el hecho lógico, y concluido anteriormente, de que al aumentar la velocidad disminuye la exactitud global. Al disponer de menor exactitud aumentan los falsos positivos.

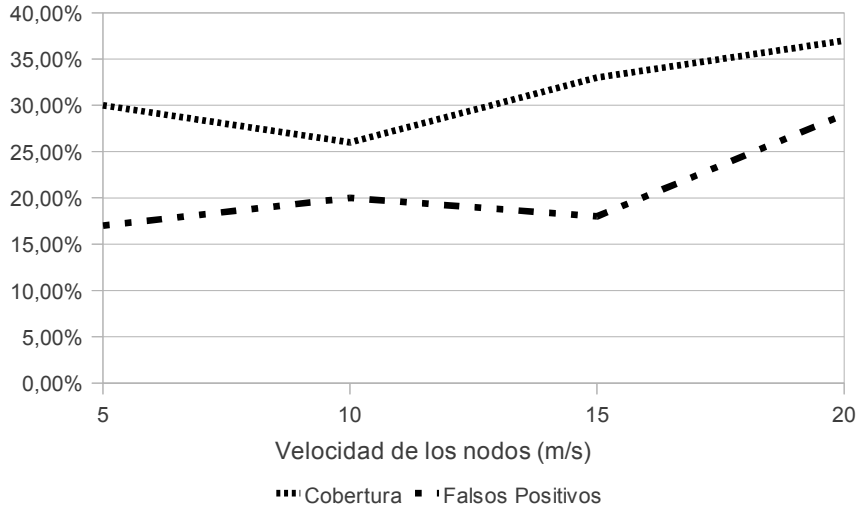

Figura 11. Coberturas y niveles de falsos positivos del watchdog colaborativo según la velocidad de los nodos.

	Mejoras
(A) Exactitud	0,78%
(B) Cobertura	0,00%
(C) Falsos Positivos	0,00%
(D) Doble Detección	10,98%
(E) Colaborativo más rápido	7,08%
(F) Detecciones realizadas únicamente por colaborativo	1,72%
(G) Tiempo medio de adelanto en la detección (en segundos, para los casos (E))	5,053 s.

Tabla 8. Comparativa de resultados del watchdog colaborativo frente al bayesiano

La Tabla 8 resume los datos comparativos más importantes obtenidos de las simulaciones realizadas. Si consideramos toda la red y no evaluamos cada instancia del *watchdog* individualmente, podemos extraer una conclusión que salta a la vista: el *watchdog* colaborativo no aumenta la cobertura de la detección (no habrá menos falsos negativos) ni reduce los falsos positivos respecto al *watchdog* bayesiano de partida. El escaso 0,78% de mejora de la exactitud se obtiene en efecto de las **mejores detecciones que cada instancia del *watchdog* colaborativo realiza individualmente**. Consecuentemente, nuestra hipótesis de que íbamos a reducir los falsos positivos y negativos se cumple sólo en el caso de los falsos negativos si se evalúan los nodos de forma separada –algo bastante lógico al tratarse la MANET de una red sin control ni seguridad centralizados y donde cada nodo debe ser lo más autosuficiente posible– pero no si se considera la red en su conjunto (Figura 12).

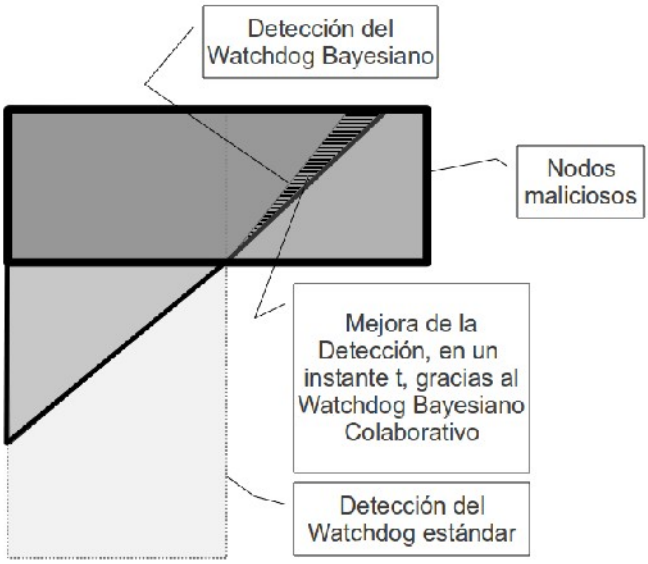

Figura 12. Representación gráfica de la mejora de la detección.

Si Bc_i es el conjunto de nodos maliciosos detectados por el nodo i usando el *watchdog* colaborativo y Bb_i es el conjunto de todos los nodos maliciosos detectados por el nodo i usando el *watchdog* bayesiano, se cumple que

$$Bc_0 \cup Bc_1 \cup ... \cup Bc_n = Bb_0 \cup Bc_1 \cup ... \cup Bb_n$$

Es decir, el conjunto formado por la unión de todos los nodos maliciosos detectados por cualquier *watchdog* colaborativo coincide con el conjunto formado por la unión de todos los nodos maliciosos detectados por cualquier *watchdog* bayesiano, aunque cada uno de los conjuntos a unir en cada caso no tienen porqué coincidir, lógicamente.

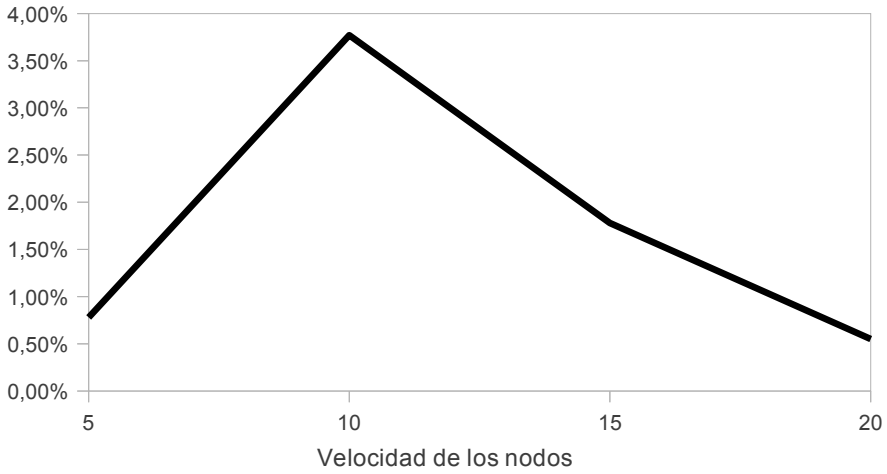

Figura 13. Detecciones exclusivas del watchdog colaborativo

La mejora real y tangible que muestran estos datos es, como ya se ha dicho, **la mayor rapidez en la detección**. Por los datos obtenidos, el *watchdog* colaborativo parece detectar los nodos maliciosos antes que el bayesiano entre un 1% y un 12% de los casos, con una media del 7,04%. En esos casos, el *watchdog* colaborativo detecta al nodo malicioso con algo más de 5 segundos de antelación, dato que es muy cercano al periodo indicado en las simulaciones para el envío de tráfico de *broadcast* por parte de los nodos.

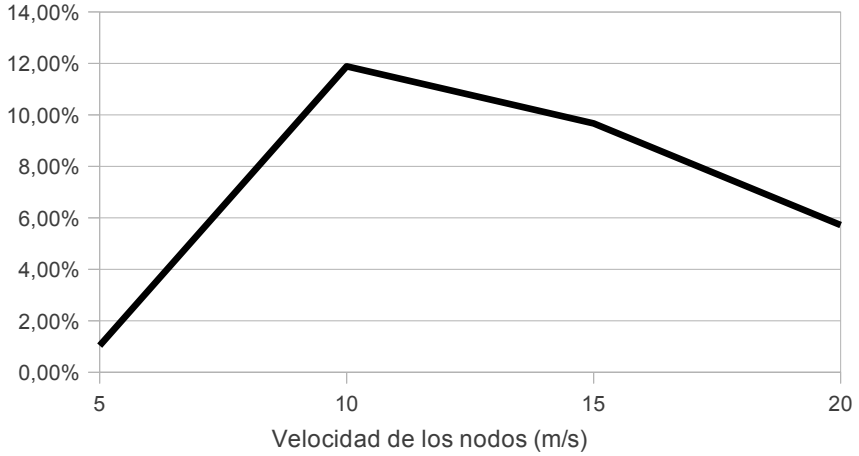

Figura 14. Mejora de la rapidez de detección (en número de casos)

Ello parece indicar que **la antelación con la que detecta nuestra propuesta está ligada a la cantidad de tráfico propio que los nodos maliciosos transmiten**. En el dato de la detección inicial también se incluyen los casos en los que el *watchdog* colaborativo de un nodo detecta un nodo malicioso y el *watchdog* bayesiano no es capaz de hacerlo (de media, un 1,72% de los casos), como se aprecia en la Figura 13. Además, como se desprende en ésta última y en la Figura 14, la mejora de dicha rapidez también decae conforme aumenta la velocidad de los nodos.

CAPÍTULO 4. CONCLUSIONES Y FUTUROS TRABAJOS

En este trabajo de Tesis de Master hemos realizado un estudio de la problemática asociada a la presencia de diferentes nodos maliciosos en las redes móviles ad hoc (MANET), llegándose a conclusiones sobre la caracterización y motivaciones del comportamiento incorrecto de dichos nodos.

La primera conclusión a la que se ha llegado con el estudio conjunto de dos temáticas ampliamente presentes en la literatura sobre este tipo de redes, el consumo de baterías y la presencia de nodos egoístas, es que **el comportamiento egoísta basado únicamente en el ahorro de baterías al no reenviar paquetes de otros nodos, es un comportamiento inútil a medio plazo**, ya que gracias a los estudios sobre el consumo de los interfaces 802.11 se puede deducir que la inmensa mayoría del consumo energético se produce en el estado Idle del interfaz [Feen'01] [Kim'03]. Por tanto, reenviar o no cierta cantidad de paquetes procedentes de otros nodos no tiene una influencia apreciable en la duración total de las baterías del nodo egoísta.

Ello nos lleva a una segunda conclusión: si no debería haber nodos egoístas en la MANET por razones energéticas porque no se obtienen ningún beneficio de ello, podemos concluir que **los nodos que presenten un comportamiento incorrecto** (*misbehaving nodes*) **deberían ser nodos averiados o nodos maliciosos**. Y frente a este tipo de nodos, los mecanismos de incentivación no tienen ningún sentido, por lo que no se consideran adecuados como solución a la problemática presentada.

Una vez establecidas estas dos conclusiones, podemos entender la necesidad de que los mecanismos de detección de nodos maliciosos sean lo más exactos posible. En trabajos anteriores [Hort'10] ya se demostró el mejor rendimiento de un *watchdog* bayesiano frente a uno estándar en la detección de nodos maliciosos. En esta Tesis de Master hemos implementado **un *watchdog* bayesiano colaborativo que ha mejorado ligeramente la exactitud de las detecciones** respecto de la implementación de partida, pero, sobretodo, **ha aumentado la rapidez de la detección de nodos maliciosos** en los nodos que ejecuten el *watchdog* propuesto. Ambas mejoras, sin embargo, pierden peso paulatinamente con el aumento de la movilidad de los nodos, y están ligadas al hecho de que el nodo malicioso trate de enviar tráfico propio.

Concretamente, en algo más de un 7% de los casos nuestro nuevo *watchdog*

colaborativo detecta los nodos maliciosos antes que el *watchdog* bayesiano, unos 5 segundos antes de media, y en un 1,72% de los casos, ha sido el único capaz de detectarlos.

Pese al trabajo realizado, aún es necesario estudiar varios aspectos de este *watchdog* bayesiano colaborativo para ajustar su funcionamiento y, a ser posible, mejorarlo:

- Evaluación de la sobrecarga que el *watchdog* colaborativo impone a la MANET por el intercambio de los mensajes de reputación, desde el punto de vista de la productividad y la latencia que implica.

- Enfoque óptimo para el envío de los mensajes de reputación, visto como compromiso entre la mejor detección y la menor sobrecarga para la red. No tiene los mismos efectos en el rendimiento de la red enviar la información de reputación dentro de los paquetes de HELLO del protocolo que implementar un protocolo específico para ello. En caso de que se opte por un protocolo específico, habría que definir el intervalo ideal de envío de estos mensajes de reputación.

- Para la adecuada ponderación del coste del *watchdog* bayesiano colaborativo, queda pendiente evaluar el impacto computacional de su implementación sobre cada nodo, ya que para su traslado a dispositivos reales éste podría ser un criterio importante si el coste computacional es demasiado elevado.

- Evaluación de la influencia del peso que se le da a las reputaciones indirectas –el parámetro δ del *watchdog* bayesiano colaborativo– en la exactitud de la detección.

- Estudio de la influencia del protocolo de encaminamiento en los resultados de la detección, para lo cual se propone evaluar el *watchdog* sobre OLSR y DSR, comparando sus resultados con los obtenidos en este trabajo para AODV.

También queda pendiente para futuros esfuerzos investigadores la implementación de esta versión del *watchdog* sobre un entorno real, como por ejemplo el *testbed* Castadiva [Hort'7] del que dispone nuestro grupo de investigación, sobre el que se podrán evaluar situaciones reales que pueden afectar a la exactitud de la detección una vez afinada ésta sobre el simulador ns-2. Para ello se partirá de la implementación real del *watchdog* bayesiano ya realizada en trabajos anteriores del grupo.

ÍNDICE DE FIGURAS

Figura 1. Red MANET de cinco nodos.....5

Figura 2. La red de la Figura 1, tras el movimiento del nodo D.....7

Figura 3. MANET de ejemplo.....16

Figura 4. Particionado de la red.....20

Figura 5. Efecto del aislamiento.....25

Figura 6. Comparación del watchdog bayesiano frente al estándar.....32

Figura 7. MANET de ejemplo para calcular $\alpha(i)$ y $\beta(i)$.....34

Figura 8. Hipótesis de los resultados esperados.....35

Figura 9. Linea temporal de la detección de un ataque.....38

Figura 10. Comparativa de la exactitud de la detección.....40

Figura 11. Coberturas y niveles de falsos positivos del watchdog colaborativo según la velocidad de los nodos.....41

Figura 12. Representación gráfica de la mejora de la detección.....42

Figura 13. Detecciones exclusivas del watchdog colaborativo.....42

Figura 14. Mejora de la rapidez de detección (en número de casos).....43

ÍNDICE DE TABLAS

Tabla 1. Ejemplo de reputaciones emitidas por los nodos.....34

Tabla 2. Ejemplos de α(i)j y β(i)j obtenidos con los datos de la tabla 1.....35

Tabla 3. Parámetros de las simulaciones.....37

Tabla 4. Resultados para nodos moviéndose a 5 m/s.....39

Tabla 5. Resultados para nodos moviéndose a 10 m/s.....39

Tabla 6. Resultados para nodos moviéndose a 15 m/s.....39

Tabla 7. Resultados para nodos moviéndose a 20 m/s.....40

Tabla 8. Comparativa de resultados del watchdog colaborativo frente al bayesiano.....41

BIBLIOGRAFÍA

[Abol'03] M. Abolhasan, T. Wysocki and E. Dutkiewicz, “A review of routing protocols for mobile ad hoc networks” in Ad-Hoc Networks, Volume 2, Issue 1, January 2004

[AlSh'04] M. Al-Shurman, S.-M. Yoo and S. Park “Black Hole Attack in Mobile Ad Hoc Networks ” in Proceedings of the 42nd annual Southeast regional conference (ACM-SE'04)

[Buch'05] S. Buchegger and J.-Y. Le Boudec, “Self-policing Mobile Ad Hoc Networks by Reputation Systems”, in IEEE Communications Magazine, July 2005

[Butt'00] L. Buttyan, J.P. Hubaux, “Enforcing Service Availability in Mobile Ad-Hoc WANs”, in IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC'2000)

[Butt'03] L. Buttyán and J.-P. Hubaux,“Stimulating Cooperation in Self-Organizing Mobile Ad hoc networks” in Mobile Networks and Applications, Volume 8, Issue 5, October 2003

[Cano'00] J. C. Cano and P. Manzoni, “A Performance Comparison of Energy Consumption for Mobile Ad Hoc Networks Routing Protocols” in Proceedings of the 8th IEEE/ACM MASCOTS 2000

[Chak'10] I. Chakeres and C. Perkins. “Dynamic MANET On-demand (DYMO) Routing”, IETF draft, 2010.

[Clau'03] T. Clausen and P. Jacquet. “Optimized Link State Routing Protocol (OLSR)” RFC 3626, 2003. http://www.ietf.org/rfc/rfc3626.txt

[Feen'01] L. Feeney and M. Nilsson, “Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment” in IEEE INFOCOM 2001

[Gior'02] Giordano, S. “Handbook of Wireless Networks and Mobile Computing”, Chapter 15: “Mobile Ad Hoc Networks”, John Wiley & Sons, Inc., New York, USA, 2002

[Hort'07] J. Hortelano, J. C. Cano, C. T. Calafate, and P. Manzoni. “Castadiva: a test-bed architecture for mobile ad hoc networks”, in The IEEE Communications

Society Symposium on Personal Indoor and Mobile Radio Communications (PIMRC'2007).

[Hort'10] J. Hortelano, C. M. T. Calafate, J. C. Cano, M. de Leoni, P. Manzoni, and M. Mecella, “Black-Hole Attacks in P2P Mobile Networks Discovered through Bayesian Filters”, in Proceedings of OTM Workshops'2010. pp.543~552

[Hort'10-2] J. Hortelano, J. C. Cano, C. T. Calafate, and P. Manzoni, “Watchdog intrusion detection systems: Are they feasible in MANETs?”, in XXI Jornadas de Paralelismo (CEDI'2010).

[Hort'11] J. Hortelano, “Design and Implementation of Architectures for the Deployment Secure Community Wireless Networks”, Doctoral Thesis, 2011, Department of Computer Engineering, Universidad Politécnica de Valencia.

[John'07] D. Johnson, D. Maltz, and Y-C. Hu, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)”, RFC 4728, 2007, http://tools.ietf.org/html/rfc4728

[Karg'04] F. Kargl, A. Klenk, S. Schlot and Michael Webber, “Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks” in Proceedings of the First European Conference on Security in Ad-Hoc and Sensor Networks (ESAS 2004)

[Kim'03] D. Kim, J.J. Garcia-Luna-Aceves, K. Obraczka, J.C. Cano, P. Manzoni, “Routing Mechanisms for Mobile Ad Hoc Networks based on the Energy Drain Rate”, in IEEE Transactions on Mobile Computing, Vol. 2, No. 2, April-June 2003, pp. 161-173.

[Ko'98] Y. Ko and N. H. Vaidya, “Location-Aided Routing (LAR) Mobile Ad Hoc Networks”, Fourth Annual International Conference on Mobile Computing and Networking (MOBICOM'98)

[Mart'00] S. Marti, T. Giuli, K. Lai and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks”, in Proceedings of the Sixth International Conference on Mobile Computing and Networking, 2000 (MobiCom'00)

[Mich'02] P. Michiardi and R. Molva, “Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks” Sixth IFIP Conference on Secure Communications and Multimedia (IFIP'02)

[Perk'03] C. Perkins, E. Belding-Royer, and S. Das., “Ad hoc On-Demand Distance Vector (AODV) Routing”, RFC 3561, 2003, http://tools.ietf.org/html/rfc3561

[Qi'04] H. Qi, W. Dapeng and P. Khosla, “SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks” in IEEE Wireless Communications and Networking Conference (WCNC, 2004)

[Sund'10] T.V.P. Sundarajan and A. Shammugam, “Modeling the Behavior of Selfish

Forwarding Nodes to Stimulate Cooperation in MANET", in International Journal of Network Security and its Applications (IJNSA), volume 2, number 2, April 2010

[Toh'10] C.K. Toh, D. Kim, S. Oh and H. Yoo, "The controversy of Selfish Nodes in Ad Hoc Networks" in Proceedings of the Twelveth international conference on Advanced communication technology (ICACT'10)

[Vaid'06] N. H. Vaidya, "Mobile Ad Hoc Networks: Routing, MAC and Transport Issues", presentation for the Twenty-fifth Annual Joint Conference of the IEEE Computer And Communications Societies (INFOCOM'06).

[Xu'06] L. Xu, Z. Lon and A. Ye, "Analysis and Countermeasures of Selfish Node problem in Mobile Ad hoc Network" in Proceeding of the Tenth International Conference on Computer Supported Cooperative Work in Design (CSCWD '06)

[Zhon'03] S. Zhong, J. Chen and Y. R. Yang, "SPRITE: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks" in Proceedings of the Twenty-second Annual Joint Conference of the IEEE Computer And Communications Societies (INFOCOM'03)