Prevención de Egoísmo Basada en Verosimilitud en Redes MANET

Alberto Rodriguez-Mayol y Javier Gozalvez
Ingeniería de Comunicaciones
Universidad Miguel Hernández de Elche
Avda. de la Universidad s/n 03202 Elche
f.rodriguez@umh.es, j.gozalvez@umh.es

***Resumen*- En las redes ad-hoc móviles es necesario que los nodos que componen la red colaboren en la retransmisión de paquetes cuando los nodos origen y destino no se encuentran dentro del rango de transmisión. Sin embargo, algunos nodos pueden negarse a cooperar para ahorrar recursos de batería o comunicación. En la literatura se han propuesto mecanismos de prevención de egoísmo basados en reputación, en los cuales los nodos observan el comportamiento de sus vecinos para detectar y aislar a aquellos nodos egoístas que no retransmiten los paquetes. Por tanto, se necesitan mecanismos de detección exactos y rápidos para distinguir los nodos cooperativos y los egoístas. Este trabajo presenta un mecanismo de detección con un novedoso enfoque basado en verosimilitud que mejora las prestaciones de los mecanismos Bayesianos empleados tradicionalmente, y que es más robusto frente al comportamiento egoísta impredecible de los nodos.**

***Palabras Clave*- Redes MANET, redes ad-hoc móviles, prevención de egoísmo, watchdog, reputación.**

I. INTRODUCCIÓN

Para asegurar unos niveles de conectividad adecuados, las redes móviles ad-hoc (MANET *Mobile Ad-hoc Networks*) requieren la cooperación de los nodos individuales para la retransmisión de paquetes desde el nodo origen al nodo destino [1]. Dado que algunos nodos pueden negarse a cooperar, por ejemplo para ahorrar recursos de batería o computación, en los últimos años ha habido un trabajo intenso en el desarrollo de esquemas de prevención de egoísmo, que pueden clasificarse genéricamente en basados en reputación, basados en crédito y basados en teoría de juegos [2]. Las estrategias basadas en reputación detectan el comportamiento egoísta o cooperativo de los nodos observando sus retransmisiones, y registrando su nivel de cooperación en tablas. Estas tablas son posteriormente utilizadas por los protocolos de enrutamiento para seleccionar la ruta más segura y aislar y evitar a los nodos egoístas identificados.

Se han propuesto diferentes técnicas para observar a los nodos y detectar su comportamiento egoísta o cooperativo. Una de las técnicas más relevantes, debido a su nivel de aceptación, simplicidad y eficiencia, dado que el proceso de observación no introduce una sobrecarga de comunicación adicional, es la técnica *watchdog* [3]. Con *watchdog*, un nodo (el nodo precursor) que transmite un paquete hacia un nodo retransmisor, usa el modo promiscuo de la MAC para observar la retransmisión del paquete dentro del tiempo establecido. Si la retransmisión es observada correctamente, el nodo precursor registra una acción positiva del nodo retransmisor en su tabla de reputación; en otro caso, se registra una acción egoísta. Sin embargo, errores esporádicos en el canal o colisiones de paquetes pueden impedir la observación correcta de la retransmisión, lo cual provoca que se registre una acción egoísta incorrectamente [4]. Estos registros incorrectos pueden afectar negativamente al funcionamiento y al rendimiento del proceso de detección, que debe decidir si un nodo debe ser o no acusado de comportarse egoístamente a partir de la información registrada por la técnica de observación. Los estudios más avanzados en esta materia basan su proceso de detección en un enfoque Bayesiano [5]-[7], que generalmente requiere la utilización de un número elevado de observaciones para reducir la probabilidad de acusar incorrectamente a un nodo cooperativo o de no detectar a un nodo egoísta. Además, los mecanismos Bayesianos se caracterizan por la necesidad de establecer un compromiso entre la exactitud y la rapidez del proceso de detección, que puede afectar negativamente a su rendimiento y al funcionamiento global de la red. Si se reduce el mínimo número de observaciones necesarias para acusar a un nodo, se mejora la rapidez en la detección, pero en un alto porcentaje de ocasiones las acusaciones son incorrectas. Si un nodo cooperativo se ve incorrectamente acusado, será aislado, no podrá participar en la red en lo sucesivo ni como origen o destino ni retransmisor, reduciendo por tanto la conectividad de la red y siendo castigado injustamente. Por el contrario, si se eleva el número mínimo de observaciones, se reduce notablemente el error en las acusaciones, pero a su vez esto provoca que los nodos egoístas descarten un número elevado de paquetes antes de que sean finalmente identificados. En este contexto, este trabajo propone un novedoso enfoque alternativo basado en verosimilitud que supera a las técnicas Bayesianas tradicionales tanto en exactitud como en rapidez de decisión. No existen en la literatura antecedentes de técnicas de detección basadas en verosimilitud. Para demostrar sus ventajas, se aplica al mecanismo de detección *watchdog*, aunque podría ser aplicado a otras técnicas de observación.

II. TÉCNICAS DE DETECCIÓN DE EGOÍSMO BAYESIANAS

Considérese una red MANET en la cual ciertos nodos rechazan selectivamente la retransmisión de algunos de los paquetes que deben retransmitir para otros nodos, con

probabilidad p_s. p_s es una variable aleatoria, con un valor distinto para cada nodo, y con función densidad de probabilidad $f_{ps}(x)$. $f_{ps}(x)$ describe la distribución del parámetro p_s en una red determinada (es decir, qué proporción de nodos descartan paquetes con probabilidad p_s=x, para x variando entre 0 y 1). Sea p_e la probabilidad de error de la técnica de observación, es decir, la probabilidad de que una acción cooperativa sea tomada por una acción egoísta. En el caso de *watchdog*, p_e es equivalente a la probabilidad de error de recepción de paquete debido a errores en el canal y colisiones de paquetes. Sea D el proceso aleatorio que describe la observación de las retransmisiones, con dos posibles eventos a considerar: D=0 si la retransmisión es observada, D=1 en otro caso. Existen dos razones por las cuales el resultado de D puede ser la no observación de la retransmisión: bien el nodo no ha retransmitido el paquete (p_s), o bien la retransmisión no ha sido correctamente detectada, con probabilidad $(1-p_s)p_e$. Este proceso se repite con cada retransmisión de paquete, conformando un proceso de tipo Binomial D_n con probabilidad p_d:

$$\Pr(D=1) = p_s + (1-p_s)p_e = p_s + p_e - p_s p_e = p_d \qquad (1)$$

Tras n observaciones, el mecanismo de detección debe decidir si el nodo está ocasionalmente actuando de manera egoísta (p_s>0). Esta decisión debe ser exacta, es decir, debe minimizar el cociente de acusaciones incorrectas *IA* (*Incorrect Accusations*) y de no acusaciones incorrectas *INA* (*Incorrect No Accusations*), y al mismo tiempo debe ser rápida, para minimizar el número δ de paquetes descartados por un nodo egoísta antes de ser detectado. *IA* se define como el cociente entre el número de nodos cooperativos acusados incorrectamente de comportarse de manera egoísta y el número total de nodos cooperativos. *INA* se define como el cociente entre el número de nodos egoístas no detectados y el número total de nodos egoístas.

Los mecanismos de detección más avanzados propuestos en la literatura son variantes del enfoque Bayesiano propuesto en [5]. Este enfoque asume que las observaciones de retransmisión permiten al nodo precursor estimar la p_s real del nodo. Para ello se supone que la $\hat{p}_s$ estimada sigue una distribución de tipo Beta, Beta(α,β). Esta distribución depende de dos parámetros, α y β. En este enfoque, α y β se inicializan a 1, y se incrementan cada vez que se observa un comportamiento egoísta o cooperativo, respectivamente. Al comienzo, cuando todavía no se ha realizado ninguna observación, el nodo precursor no tiene ninguna certeza sobre la p_s real del nodo, y por ello la función Beta(1,1) es una distribución uniforme, indicando que la $\hat{p}_s$ estimada puede tomar cualquier valor entre 0 y 1 con la misma probabilidad. Cuanto mayor es el número de observaciones realizadas, más exacta es la aproximación de la función Beta(α,β) a la p_s real del nodo retransmisor. Cuando el número de observaciones es suficientemente grande, el nodo precursor estima el valor de la p_s real, usando para ello el valor esperado de la distribución Beta(α,β) en ese momento. Este valor esperado es utilizado por el nodo precursor como una métrica para decidir si el nodo retransmisor está actuando egoístamente. Si el valor de la métrica supera el umbral de acusación τ, que es un parámetro de configuración de entrada de cada técnica que expresa el nivel máximo de egoísmo aceptable, entonces el veredicto es que el nodo retransmisor está actuando egoístamente. Se han propuesto distintas técnicas Bayesianas basadas en este procedimiento que se exponen a continuación.

La primera de las técnicas, denominada en el presente trabajo BIW (*Bayesian with Infinite Window*) [5]-[6], define la métrica como

$$M_{BIW}(n,\alpha,l) = \left.\frac{\alpha(n)}{n}\right|_{n\geq l} \qquad (2)$$

donde $\alpha(n)$ representa el número de acciones negativas registradas en las últimas n observaciones, y l es el mínimo número de observaciones que aseguran la validez estadística de la métrica. Si el valor de dicha métrica supera el umbral de acusación τ, entonces el nodo es acusado de actuar egoístamente. La segunda métrica, denominada BFW (*Bayesian with Finite Window*), que fue empleada en [7], tiene en cuenta sólo las últimas l observaciones, como se refleja en:

$$M_{BFW}(n,\alpha,l) = \left.\frac{\alpha(n-l,n)}{l}\right|_{n\geq l} \qquad (3)$$

[5] propone una mejora de la métrica BIW, denominada aquí BDF (*Bayesian with Discount Factor*) por claridad, la cual introduce un factor de descuento:

$$u = 1 - \frac{1}{l} \qquad (4)$$

Sea s el resultado de la última observación D_i. Esto quiere decir que si s=0 entonces se ha observado una retransmisión y si s=1 se ha observado un comportamiento egoísta. Entonces, la actualización de α y β sería en este caso:

$$\begin{aligned} \alpha_{DF}(i) &:= u\alpha_{DF}(i-1) + s \\ \beta_{DF}(i) &:= u\beta_{DF}(i-1) + (1-s) \end{aligned} \qquad (5)$$

El factor de descuento u atenúa la importancia de las observaciones más antiguas frente a las más recientes, de manera que el nodo retransmisor debe cooperar continuamente a lo largo del tiempo, ya que un comportamiento positivo en el pasado no compensa comportamientos negativos recientes. La métrica de egoísmo BDF puede definirse entonces como:

$$\begin{aligned} M_{BDF}(n,\alpha,l) &= \left.\frac{\alpha_{DF}(n)}{\alpha_{DF}(n)+\beta_{DF}(n)}\right|_{n\geq l} = \\ &= \left.\frac{1-u^{\alpha(n)}}{2-u^{\alpha(n)}-u^{l-\alpha(n)}}\right|_{n\geq l} \end{aligned} \qquad (6)$$

Donde las siglas *DF* indican que $\alpha_{DF}(,n)$ se refiere, no al número de observaciones de acciones egoístas en el instante n, sino al valor de α en el instante n computado según la ecuación (5). Análogamente al caso del enfoque Bayesiano original, una métrica Bayesiana con factor de descuento BDF y con una ventana de tamaño l, BFDF (*Bayesian Finite window with Discount Factor*) puede definirse como:

$$\begin{aligned} M_{BFDF}(n,\alpha,l) &= \left.\frac{\alpha_{DF}(n-l,n)}{\alpha_{DF}(n-l,n)+\beta_{DF}(n-l,n)}\right|_{n\geq l} = \\ &= \left.\frac{1-u^{\alpha(n-l,n)}}{2-u^{\alpha(n-l,n)}-u^{l-\alpha(n-l,n)}}\right|_{n\geq l} \end{aligned} \qquad (7)$$

Para un funcionamiento correcto de las técnicas de detección Bayesianas es necesario seleccionar de manera óptima el valor de los parámetros de configuración l y τ. El objetivo de la optimización es maximizar la exactitud (o equivalentemente, minimizar el error *IA* e *INA*) y la rapidez (δ) de la detección de egoístas. En la selección óptima del valor de de estos parámetros se debe tener en cuenta la influencia de los parámetros $f_{ps}(x)$ y p_e. Mientras que el valor de p_e puede ser estimado en tiempo real, como en [8], o a través de mensajes de señalización como en [9], la estimación del valor de la función de distribución $f_{ps}(x)$ en una red MANET es una tarea difícil. Además, se necesitarían un gran número de observaciones l para obtener unos cocientes de error aceptables, lo cual por otro lado incrementaría el número promedio de paquetes descartados por nodos egoístas δ. Para entender mejor la importancia de la selección de los parámetros (τ,l), se realiza a continuación una estimación analítica de su influencia en los parámetros de resultado *IA* e *INA* para la técnica BFW. Si se considera un número suficientemente grande de experimentos, los cocientes *IA* e *INA* pueden aproximarse por la probabilidad de que un nodo cooperativo sea acusado y de que un nodo egoísta no sea detectado, respectivamente. Sea A_n el evento de que un nodo haya sido acusado en el instante n. Si se asume, para facilitar los cálculos, que la métrica de egoísmo BFW se calcula solamente cada l observaciones, entonces los eventos de acusación en instantes diferentes son independientes e idénticamente distribuidos, y la probabilidad de acusación tras n observaciones se puede calcular como:

$$\Pr(A_n) = 1 - \Pr(\overline{A}_n) \approx 1 - \Pr\left(\bigcap_{i=1}^{n/l} \overline{A}_{i\cdot l}\right) \tag{8}$$

Dado que el evento de ser acusado en un instante es independiente del de ser acusado en cualquier otro instante, se puede expresar como un producto, y después se aplica la métrica BFW de la ecuación (3):

$$\Pr(A_n) \approx 1 - \prod_{i=1}^{n/l} \Pr(\overline{A}_{i\cdot l}) = 1 - \prod_{i=1}^{n/l} \Pr\left(\alpha((i-1)l, i\cdot l)/l \le \tau\right) \tag{9}$$

Igualmente, se puede simplificar el producto de probabilidades a una potencia, dado que la probabilidad de que sea acusado en un instante o en otro es la misma, por ser el tamaño de ventana siempre idéntico.

$$\Pr(A_n) \approx 1 - \Pr\left(\alpha(1,l)/l \le \tau\right)^{n/l} \tag{10}$$

Finalmente, recuérdese de la Teoría de Probabilidad, la expresión de la función de distribución binomial. Dada una variable X que sigue una distribución binomial con probabilidad p, la función de distribución F describe precisamente la probabilidad de que, tras n pruebas, se hayan dado x éxitos

$$F(x;n,p) = \Pr(X \le x) = \sum_{i=0}^{\lfloor x \rfloor} \binom{n}{i} p^i (1-p)^{1-i} \tag{11}$$

En el caso que nos interesa, las n pruebas corresponden a las n observaciones del nodo, la probabilidad p corresponde a la p_d definida anteriormente. Con todo esto, a partir de las ecuaciones (10) y (11) se puede llegar a la expresión siguiente:

$$\Pr(A_n) \approx 1 - \Pr(\alpha(1,l) \le l\tau)^{n/l} = 1 - F(\lfloor l\tau \rfloor; l, p_d)^{n/l} \tag{12}$$

Usando la ecuación (1), los las probabilidades de *IA* e *INA* se pueden expresar como:

$$\Pr(IA) = 1 - F(\lfloor l\tau \rfloor; l, p_e)^{N/l} \tag{13}$$

$$\Pr(INA) = F(\lfloor l\tau \rfloor; l, p_e + p_s - p_s p_e)^{N/l} \tag{14}$$

La Fig. 1 subraya la dependencia de las probabilidades de *IA* e *INA* respecto al umbral de acusación τ para distintos valores de probabilidad de egoísmo del nodo (p_s) y un tamaño de ventana l fijo e igual a 12 (se observa una tendencia similar si se varía l manteniendo τ fijo). Un objetivo de diseño podría ser minimizar *IA* e *INA*; sin embargo, la Fig. (1) muestra que ambos parámetros siguen tendencias opuestas. Para valores de p_s mayores o iguales a 0.2, las probabilidades *IA* e *INA* son minimizadas simultáneamente en el punto τ=0.45. Por otro lado, si p_s es igual a 0.1, τ debería tomar un valor entre 0.35 y 0.4, pero en este caso las probabilidades *IA* e *INA* no podrían ser reducidas más allá de 0.1.

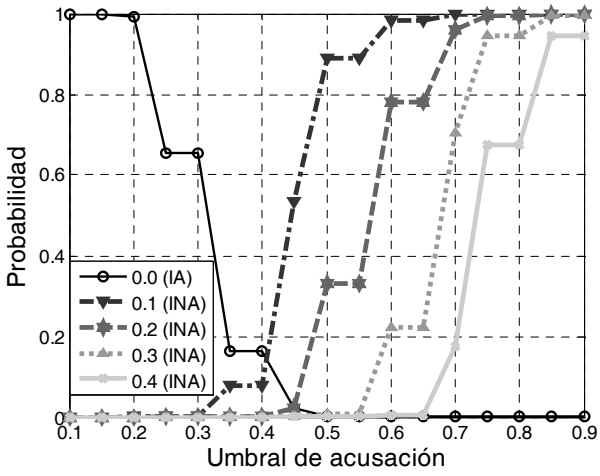

Fig. 1. Probabilidades de *IA* e *INA* en función del umbral de acusación τ. La leyenda corresponde a distnitos valores de p_s.

Con otra estrategia, la probabilidad de *IA* se puede reducir incrementando el número de observaciones l, pero sin embargo, esto conlleva a un incremento del número de paquetes descartados por nodos egoístas (δ) antes de que su comportamiento sea detectado y sean aislados. Como se ha visto, es importante subrayar que los valores óptimos de τ y l varían en función de cual sea la distribución en la red del parámetro de egoísmo p_s entre los nodos, la cual no es conocida a priori. Por ello, el rendimiento y las perspectivas de implementación de las técnicas basadas en el enfoque Bayesiano se ven considerablemente limitados.

III. Propuesta de Detección de Egoísmo Basada en Verosimilitud

Para superar las limitaciones de las técnicas de detección de egoísmo Bayesianas, este trabajo propone un nuevo enfoque basado en verosimilitud y desarrolla un nuevo mecanismo a partir de este enfoque. En el enfoque de verosimilitud se define una nueva métrica diseñada para comprobar, después de cada observación D_n, si lo más

probable es que el número de acciones egoístas observado $\alpha(n)$ corresponda exclusivamente a equivocaciones del proceso de observación, provocadas por errores en el canal radio y colisiones de paquetes, representado por la probabilidad p_e, o si por el contrario es más probable que se deba a la combinación de este efecto unido al comportamiento egoísta del nodo retransmisor, representado por la probabilidad p_s. En este contexto, se necesita una función que mida la probabilidad de que la hipótesis nula "*las acciones egoístas observadas se deben exclusivamente a la inexactitud del método de observación*" sea verdadera. Este trabajo utiliza como punto de partida para hallar dicha función de verosimilitud a la función de distribución Binomial expresada en la ecuación (11). Dada la complejidad de la expresión exacta de la función de distribución Binomial, se toma la aproximación basada en la desigualdad de Hoeffding:

$$F(x,n,p) \approx \exp\left(-2\frac{(np-x)^2}{n}\right) \tag{15}$$

A partir de dicha expresión, este trabajo propone una función de verosimilitud F_L, que tiene en cuenta el número de observaciones n, el número de observaciones de acciones egoístas $\alpha(n)$ y la probabilidad de error de observación p_e:

$$F_L(\alpha,n,p_e) \approx \exp\left(-2\frac{(\Delta_-(np_e-\alpha(n)))^2}{n}\right) \tag{16}$$

donde se define Δ_- como:

$$\Delta_-(x) = \frac{x-|x|}{2} = \begin{cases} 0 & x \geq 0 \\ x & x < 0 \end{cases} \tag{17}$$

Las métricas propuestas, denominadas métrica de verosimilitud con ventana infinita LIW (*Likelihood Infinite Window*) y métrica de verosimilitud con ventana finita LFW (*Likelihood Finite Window*), se definen como el promedio de la función de verosimilitud F_L para todas las observaciones y para las últimas l observaciones, respectivamente:

$$M_{LIW}(n,\alpha,l,p_e) = \frac{1}{n}\sum_{i=1}^{n}\exp\left(-2\frac{(\Delta_-(ip_e-\alpha(i)))^2}{i}\right)\Bigg|_{n\geq l} \tag{18}$$

$$M_{LFW}(n,\alpha,l,p_e) = \frac{1}{l}\sum_{i=n-l+1}^{n}\exp\left(-2\frac{(\Delta_-(ip_e-\alpha(i)))^2}{i}\right)\Bigg|_{n\geq l} \tag{19}$$

Al contrario de lo que sucede en las técnicas Bayesianas, la propuesta de detección basada en verosimilitud solamente acusa a un nodo de actuar egoístamente cuando el valor de la métrica de verosimilitud calculado es inferior al umbral de acusación τ. En tal caso, no se confirmaría la hipótesis nula, y opr tanto el nodo es egoísta. En este contexto, es importante señalar que τ no es una medida del valor máximo aceptable de egoísmo, sino una medida de la mínima verosimilitud de la hipótesis de que el nodo no está comportándose de manera egoísta. Por consiguiente, el parámetro τ no está aquí directamente relacionado con la distribución del parámetro p_s entre el conjunto de nodos de la red, lo cual facilita la selección de un valor adecuado del parámetro τ y mejora las perspectivas de implementación de la propuesta.

IV. Evaluación de Rendimiento

Para la evaluación del rendimiento de la técnica propuesta y su comparación con las técnicas Bayesianas tradicionales se han realizado extensos lotes de simulaciones. Cada prueba básica de simulación consiste en la valoración por parte de cada técnica de una realización concreta del proceso de detección Binomial descrito en la sección II y la determinación (usando el criterio de acusación de la técnica considerada) de si dicha realización se corresponde o no con la de un nodo egoísta. Por una realización entendemos una muestra concreta $\{\alpha(i)\}$ i=1,…,N, de observaciones de acciones egoístas, siendo N el número total de observaciones realizadas, sobre un nodo con egoísmo p_s mediante una técnica de observación con una probabilidad de error p_e. En dicha realización $\alpha(i)$ representa el número de observaciones de paquetes descartados realizadas tras i observaciones. Si tras i observaciones, con $l \leq i \leq N$, se cumple el criterio de acusación de la técnica de detección, entonces el veredicto es que el nodo está descartando paquetes. Por el contrario, si eso no ocurre para ningún valor $\alpha(i)$, con $l \leq i \leq N$, entonces el veredicto es que las observaciones de paquetes descartados en realidad corresponden a los errores de la técnica de detección de *watchdog*. El resultado de una prueba básica es por tanto, para cada técnica de detección implementada, un veredicto negativo o positivo de acusación del nodo retransmisor. La rapidez de la técnica en la detección de nodos egoístas podrá ser evaluada contando el número de observaciones k que han sido necesarias antes de la acusación, en caso de que el egoísmo del nodo en la realización concreta de la prueba fuera p_s>0. Es decir, la rapidez sería el mínimo valor de i tal que la secuencia $\{\alpha(i)\}$ i=1,…,N cumple la condición de acusación en la observación i=k. Por otro lado, la exactitud de la técnica se puede evaluar comparando el veredicto de la técnica con el egoísmo real del nodo retransmisor p_s. Una acusación es incorrecta si el egoísmo real del nodo es nulo p_s=0, y una no acusación es incorrecta si por el contrario p_s>0. A través de la realización de un gran número de pruebas en distintas condiciones, se pueden obtener promedios numéricos de los parámetros de evaluación considerados: δ, *IA* y *NIA*. A continuación se explicarán cuáles han sido las condiciones consideradas y el procedimiento para hallar los valores óptimos de los parámetros de configuración (τ,l).

Se realizaron simulaciones preliminares para seleccionar los valores óptimos de los parámetros (τ,l) para cada una de las técnicas, en escenarios con diferentes valores de p_s. Es necesario recalcar que los valores óptimos de (τ,l) no tienen porque ser iguales para todas las técnicas. En primer lugar, el parámetro τ expresa conceptos diferentes en las técnicas Bayesianas y de verosimilitud, como ya se ha comentado. Por simplicidad, se ha usado la misma notación en ambos casos, puesto que se trata de un cierto umbral que toma valores entre 0 y 1 y que es comparado con la métrica para decidir si el nodo es egoísta. Sin embargo, en las técnicas Bayesianas τ expresa un umbral de máximo egoísmo permitido, mientras que en las de verosimilitud determina la mínima certeza aceptable de que el nodo no sea egoísta. Además, el funcionamiento de cada técnica requiere unos valores específicos de (τ,l). La selección de los valores óptimos de (τ,l) variará también para cada red concreta en función de la

distribución $f_{ps}(x)$ del parámetro p_s del egoísmo de los nodos en dicha red.

Por las razones mencionadas, en el proceso de selección de los valores óptimos de (τ,l) para cada técnica, se deben tener en cuenta los distintos valores posibles del parámetro p_s de un nodo retransmisor. Sea $x_i \in \{0.0,...,1.0\}; i = 1,..., N_{ps}$ el conjunto finito y discreto de los posibles valores del parámetro p_s dentro de la distribución $f_{ps}(x)$. Entonces, los valores promedio de $IA(m,\tau,l)$, $INA(m,p_s,\tau,l)$ y $\delta(m,p_s,\tau,l)$ para cada valor de p_s, para cada técnica de detección m y para un conjunto de N nodos puede computarse usando el siguiente principio de proporcionalidad:

$$\begin{aligned} IA(m, f_{ps}, \tau, l) &= f_{ps}(0.0) IA(m, \tau, l) \\ INA(m, f_{ps}, \tau, l) &= \sum_{i=2}^{N_{ps}} f_{ps}(x_i) INA(m, x_i, \tau, l) \\ \delta(m, f_{ps}, \tau, l) &= \sum_{i=2}^{N_{ps}} f_{ps}(x_i) \delta(m, x_i, \tau, l) \end{aligned} \quad (20)$$

Dada la infinidad de posibles distribuciones $f_{ps}(x)$ del parámetro de egoísmo p_s en una red real, el paso siguiente ha sido definir un conjunto de distribuciones $\{f_{ps}(x)_i\}$ que sean representativas de las potenciales distribuciones en una red MANET real. En este trabajo, las características más influyentes de la distribución $f_{ps}(x)$ son la proporción de nodos no egoístas $f_{ps}(0)$ y la proporción de nodos egoístas con un nivel de egoísmo p_s reducido pero no nulo. A continuación se expone un ejemplo para ilustrar la primera característica. En una red con muchos nodos no egoístas será más perjudicial que la técnica de detección empleada tenga un nivel alto de *IA* que de *INA*, es decir, dado que la mayoría son no egoístas, con un nivel elevado de *IA* habrá un número considerable de acusaciones incorrectas. En cambio no sería muy perjudicial que tuviera un valor más elevado de INA, dado que hay pocos egoístas en la red. Dado que, como se ha comentado en la sección II, existe un compromiso entre los parámetros *IA* e *INA*, la selección de la pareja de parámetros (τ,l) deberá tener en cuenta la proporción de nodos no egoístas $f_{ps}(0)$. Por ello, a la hora de determinar las distribuciones $f_{ps}(x)$ a tener en cuenta, se han considerado 8 valores para la proporción de nodos no egoístas: $f_{ps}(0) \in \{0.2,0.3,...,0.9\}$.

Respecto a la segunda característica, los nodos que tienen un bajo nivel de egoísmo p_s son más difíciles de detectar que los nodos con un p_s alto, es decir, obtienen valores elevados de *INA*, dado que su comportamiento se puede enmascarar con la probabilidad de observación errónea p_e. De ahí que un nodo con un nivel de egoísmo reducido pueda confundirse más fácilmente con un nodo no egoísta, y viceversa. Esto puede apreciarse claramente además en la Figura 1, en las curvas correspondientes a la probabilidad de *INA* para distintos valores de p_s. Por ejemplo, fijando un valor de τ=0.6, la probabilidad de que un nodo con egoísmo reducido (p_s=0.1) pase desapercibido es casi completa, mientras que para un nodo con mayor nivel de egoísmo (por encima de $p_s \geq 0.4$) es nula. Por consiguiente, se han considerado 3 tipos de función para la $f_{ps}(x)$ de los nodos egoístas: uniforme, linealmente creciente (menor proporción de nodos con egoísmo difícil de detectar) y linealmente decreciente. Combinando estos 3 tipos de función, con los 8 valores mencionados de proporción de nodos no egoístas $f_{ps}(0)$, se han obtenido un conjunto de 24 distribuciones representativas $\{f_{ps}(x)_i\}$.

En el proceso de selección de los valores óptimos de los parámetros de configuración (τ,l) debe tenerse en cuenta el compromiso anteriormente comentado entre la rapidez y la exactitud en las técnicas de detección, especialmente en las técnicas Bayesianas. Por ello, se han considerado dos criterios diferentes. El criterio de exactitud consiste en seleccionar la pareja (τ,l) que minimice la suma de los promedios de los cocientes de *IA* e *INA*. Por otro lado, el criterio de rapidez tiene en cuenta tanto la suma de los promedios de *IA* e *INA* como también el número de paquetes descartados antes de que un nodo egoísta sea detectado δ. La Tabla 1 muestra los valores de (τ,l) que en promedio se ajustan mejor a los criterios de optimización de exactitud y rapidez para cada una de las técnicas de detección. El conjunto de valores de (τ,l) evaluados fueron todas las posibles combinaciones de $\tau \in \{0.1,0.15,\ldots,0.9\}$ y $l \in \{3,6,12,24,48\}$, y los resultados han sido obtenidos considerando una p_e igual a 0.1. La Tabla 1 también muestra el porcentaje de ocasiones en que el valor seleccionado de (τ,l), que mejor se ajustaba a los criterios exactitud y rapidez en promedio, resultaba asimismo ser la configuración óptima en cada una de las veinticuatro distribuciones $\{f_{ps}(x)_i\}$ consideradas individualmente (parámetro *Opt*. en Tabla 1).

En primer lugar, debe señalarse que en todas las técnicas Bayesianas el valor de l que ha resultado seleccionado es el más alto (48) de entre todos los que han sido considerados, cuando se utilizaba el criterio de exactitud. Por otro lado, si se considera el criterio de rapidez, se requiere un valor apreciablemente menor del parámetro l, para reducir su impacto sobre el número de paquetes descartados δ. Pero esto a su vez, conlleva a un reajuste del parámetro τ seleccionado a un valor mayor y por tanto más permisivo con el egoísmo, para compensar el efecto colateral negativo de reducir el número de observaciones l sobre el cociente de *IA*. El compromiso entre la rapidez y la exactitud de la detección, especialmente en las técnicas Bayesianas, queda patente en este resultado.

Por otro lado, las técnicas de verosimilitud no necesitan un valor elevado del parámetro l, incluso cuando se considera el criterio de exactitud, según muestra la Tabla 1, lo cual es de esperar que reduzca el número de paquetes descartados por egoístas δ. Los resultados mostrados también ponen de manifiesto que la configuración óptima en promedio de (τ,l) para el mecanismo LFW resultaba ser la configuración óptima para casi todas las distribuciones consideradas en el conjunto $\{f_{ps}(x)_i\}$. En concreto, resulta ser óptima en el 100% de los casos cuando se considera el criterio de exactitud y en el 66% de los casos cuando se considera el criterio de rapidez. En este aspecto las restantes técnicas resultan ser considerablemente inferiores. La configuración de la técnica BDF resulta ser óptima en el 100% de los casos para el criterio de exactitud y el 50% para el de rapidez, pero los valores de (τ,l) de ambas configuraciones son completamente diferentes, lo cual no ocurre en el caso de la técnica LFW. Esta es una ventaja de implementación muy notable de LFW respecto al resto de técnicas, ya que la distribución del parámetro de egoísmo entre los nodos de la red es desconocida y con esta única configuración para LFW se optimiza a la vez la exactitud y la rapidez para casi todas las

distribuciones consideradas del parámetro p_s. Puede concluirse por tanto a partir de la Tabla I que la elección de unos parámetros de configuración para las técnicas Bayesianas que maximicen la exactitud, disminuyen considerablemente la rapidez en la detección de egoístas, y viceversa. Este compromiso no existe en las técnicas basadas en verosimilitud, especialmente en la técnica con ventana finita LFW, dado que una misma configuración resulta ser óptima tanto en rapidez como en exactitud.

		BIW	BFW	BDF	BFDF	LIW	LFW
τ	exact.	0.20	0.30	0.45	0.35	0.30	0.10
	rapidez	0.35	0.35	0.50	0.50	0.35	0.10
l	exact.	48	48	48	48	12	3
	rapidez	6	24	3	12	3	3
Opt	exact.	58.33	66.67	100.0	62.50	66.67	100.0
	rapidez	16.67	16.67	50.00	41.67	4.17	66.67

Tabla 1: Configuración óptima de (τ,l).

La Tabla 2 muestra el promedio de los parámetros de resultados *IA*, *INA* y δ obtenidos para el conjunto $\{f_{ps}(x)_i\}$ de distribuciones y para los distintos mecanismos de detección. Los resultados mostrados en la Tabla 2 fueron obtenidos usando la configuración óptima de (τ,l) mostrada en la Tabla 1, para cada técnica y criterio de selección. Ante todo, debe señalarse que ambas propuestas de verosimilitud, y especialmente LFW, obtienen el mejor rendimiento tanto con el criterio de exactitud como con el criterio de rapidez, lo cual permite conseguir un porcentaje muy bajo de acusaciones incorrectas de nodos cooperativos y de nodos egoístas no detectados, además de lograr el menor número de paquetes descartados por los nodos egoístas antes de ser detectados. Si bien alguna de las técnicas Bayesianas puede obtener una marca mejor de rendimiento en alguno de los parámetros analizados, esto siempre está asociado a una degradación considerable de otro parámetro de rendimiento. En particular, los valores altos de l de las configuraciones que optimizan el criterio de exactitud en las técnicas Bayesianas están correlacionados con cocientes de *IA* e *INA* bajos, pero también con una gran degradación en el número de paquetes descartados por los nodos egoístas antes de ser detectados (δ). Por otro lado, también en las técnicas Bayesianas, el criterio de rapidez reduce el parámetro δ, pero esto se consigue a expensas de incrementar el error de detección, ya sea en el cociente de *IA* o de *INA*. Las diferencias entre las técnicas Bayesianas y las técnicas de verosimilitud se pueden explicar de la siguiente manera. En el enfoque Bayesiano, τ se corresponde al umbral máximo de egoísmo aceptable. Por consiguiente, al incrementar su valor para reducir el cociente de acusaciones incorrectas *IA* (de manera que se compense el efecto de reducir el parámetro l) provoca que los nodos con un egoísmo menor que el estipulado por el umbral $p_s<\tau$ no sean correctamente detectados y por tanto el cociente *INA* aumenta. Por el contrario, en las técnicas de verosimilitud, τ mide la mínima verosimilitud requerida para que la hipótesis de que el nodo no está actuando egoístamente sea aceptada. En este caso, la reducción de τ, es decir, la exigencia de un menor nivel de verosimilitud, rebaja el cociente de acusaciones incorrectas *IA*, pero no provoca que los nodos con un bajo nivel de egoísmo p_s no sean detectados, ya que τ se refiere en este caso a la verosimilitud y no directamente al nivel de egoísmo p_s del nodo. Entre las técnicas de verosimilitud, es preferible emplear LFW ya que además de lograr el mejor rendimiento promedio con la configuración óptima seleccionada, sus prestaciones son también óptimas para la mayoría de las distribuciones del parámetro f_{ps} consideradas en el conjunto $\{f_{ps}(x)_i\}$ y para los dos criterios de exactitud y de rapidez. Por tanto puede concluirse que, con la técnica LFW de verosimilitud se consigue superar el compromiso existente en las técnicas Bayesianas entre la rapidez y exactitud de la detección que impide hallar una configuración de (τ,l) que optimice a la vez los tres parámetros de rendimiento considerados de *IA*, *INA* y δ, independientemente del número de nodos egoístas que participen en la red y de su grado de egoísmo.

		BIW	BFW	BDF	BFDF	LIW	LFW
IA [%]	exact.	1.86	3.76	0.46	3.38	0.94	0.06
	rapidez	11.32	2.18	22.70	6.44	0.62	0.06
INA [%]	exact.	3.40	0.20	0.00	0.40	0.00	0.60
	rapidez	3.20	3.40	3.00	1.00	2.80	0.60
δ	exact.	12.14	13.13	17.03	13.04	4.87	2.35
	rapidez	2.04	7.33	1.51	6.04	2.78	2.35

Tabla 2: Rendimiento promedio.

V. CONCLUSIONES

En trabajos anteriores sobre redes MANET, han sido propuestos mecanismos de prevención de egoísmo basados en reputación para detectar y aislar a posibles nodos egoístas que no colaboran en la retransmisión de paquetes para otros nodos, generando problemas de conectividad. Los mecanismos de detección propuestos hasta la fecha se basan en un enfoque Bayesiano con distintas variantes que se caracteriza por un compromiso entre la exactitud y la rapidez del proceso de detección. En este contexto, este trabajo propone un novedoso enfoque para el diseño de mecanismos de detección basado en verosimilitud, que tiene en cuenta de manera explícita la probabilidad de error del método de observación del comportamiento de los nodos. Con dicho enfoque, la técnica de detección no evalúa directamente el egoísmo del nodo, sino la verosimilitud de que las observaciones realizadas correspondan al comportamiento de un nodo no egoísta. El estudio llevado a cabo demuestra que la propuesta basada en verosimilitud supera el rendimiento de las propuestas Bayesianas, tanto en términos de exactitud como de rapidez de detección. Otro resultado importante obtenido es que con el método de verosimilitud se obtiene un rendimiento óptimo con la misma configuración de los parámetros de entrada de la técnica para la gran mayoría de las distribuciones del parámetro de egoísmo de los nodos consideradas. De esta manera, no es necesario estimar a priori la distribución real en la red de este parámetro, lo cual sería además difícilmente realizable.

AGRADECIMIENTOS

Este trabajo ha sido posible por el apoyo del Ministerio de Ciencia e Innovación del Gobierno de España y de los fondos FEDER a través de los proyectos TEC2008-06728, de la Generalitat Valenciana a través de los proyectos ACOMP/2010/111 y BFPI/2007/269.

REFERENCIAS

[1] S. Buchegger, J. Mundinger y J.-Y Le Boudec, "Reputation Systems for Self-organized Networks," *IEEE Technology and Society Magazine*, vol. 27, no. 1, pp. 41–47, Marzo 2008.

[2] Y. Yoo y D.P. Agrawal, "Why Does it Pay to Be Selfish in a MANET?," *IEEE Wireless Communications Magazine*, vol. 13, no. 6, pp. 87-97, Diciembre 2006.

[3] S. Marti, T. J. Giuli, K. Lai y M. Baker, "Mitigating Routing Misbehavior in Mobile Ad-hoc Networks," *en Libro de Actas de la ACM International Conference on Mobile Computing and Networking*, pp. 255-265, 2000.

[4] A. Rodriguez-Mayol y J. Gozalvez, "On the Implementation Feasibility of Reputation Techniques for Cooperative Mobile Ad-hoc Networks," *en Libro de Actas del 16th European Wireless*, Abril 2010.

[5] S. Buchegger y J.-Y Le Boudec, "A Robust Reputation System for P2P and Mobile Ad-hoc Networks," *en Libro de Actas del 2nd Workshop on the Economics of Peer-to-Peer Systems*, Junio 2004.

[6] D. Djneouri y N. Badache, "On Eliminating Packet Droppers in MANET: a Modular Solution," *Ad hoc Networks*, vol. 7, no. 6, pp. 1243-1258, Septiembre 2009.

[7] L. Yang, J.M. Kizza, Alma-Cemerlic y F. Liu, "Fine-Grained Reputation-based Routing in Wireless Ad Hoc Networks," *en Libro de Actas del IEEE Intelligence and Security Informatics*, pp. 75-78, Junio 2007.

[8] H. Jiang, Y. Yang, J. Xu y L. Wang, "Estimation of Packet Error Rate at Wireless Link of Vanet," *Advances in Wireless Sensors and Sensor Networks, Lecture Notes in Electrical Engineering*, vol. 64, pp. 329-359, 2010.

[9] B. Han y S. Lee, "Efficient Packet Error Rate Estimation in Wireless Networks," *en Libro de Actas de la 3rd International ICST Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities*, pp. 1-9, Mayo 2007.