# Desempeño de redes de múltiple salto ante ataque de denegación de servicio basado en tráfico

César Andrés Ramírez Sarmiento
*andres.cesarandres@gmail.com.*

Néstor Misael Peña T.
*npena@uniandes.edu.co*

Fecha de recepción: 19-10-2007 Fecha de selección: 18-04-2008 Fecha de aceptación: 14-01-2008

**ABSTRACT**

The Multi-hop wireless networks or ad hoc networks are build on MAC IEEE 802.11 DCF protocol, which was originally designed for wireless LAN. This adaptation have revealed problems and vulnerabilities that a based on traffic DoS attack might take advantage, avoiding normal clients to access or provide its services. In wired networks, hardware devices and preventive measures like encryption and authentication are used to the defense against the attacks, but sometimes due of ad hoc networks physical conditions, this measures could not be applied, then the network performance falls. For the simulations of based on traffic DoS consequences on MAC layer protocol, Qualnet® simulation tool was used. To improve the performance of the multi-hop network in presence of a based on traffic DoS, we propose as a preventive measure to increase and setup the default retry limits of MAC layer and a modification of BEB algorithm. These changes, reduce the effects of the DoS and improve the network perfomance in terms of throughput and packet delivery ratio.

**KEY WORDS**

Backoff algorithm, Denial of Service (DoS, Banwidth, MAC, DCF, Contention Window.

**RESUMEN**

Las redes de múltiple salto o redes ad hoc están construidas sobre el protocolo MAC IEEE 802.11 DCF el cual fue originalmente diseñado para redes de área local. Esta adaptación revela problemas y vulnerabilidades que pueden ser explotadas por un ataque de denegación de servicio basado en tráfico evitando que los clientes puedan acceder o proveer sus servicios. En este trabajo se describen comportamientos que se presentan sobre la implementación del estándar de la capa MAC en una red ad hoc ante un ataque de denegación de servicio basado en tráfico, usando la herramienta de simulación Qualnet®. Con el propósito de aliviar el impacto de un ataque de denegación de servicio basado en tráfico sobre la red se propone un ajuste en los límites de retransmisión y se modifica el algoritmo de Backoff en la capa de acceso al medio para lograr disminuir los efectos del ataque sobre la red, aumentando el caudal total y la relación de paquetes entregados.

**PALABRAS CLAVE**

Algoritmo de Backoff, Denegación de Servicio (DoS), Caudal, MAC 802.11 DCF, Ventana de Contención (CW).

**Clasificación Colciencias: Tipo 1**

## 1. INTRODUCCIÓN

Mientras que los ataques DoS han sido ampliamente estudiados en las redes tradicionales, se ha hecho poca investigación para analizar y prevenir estos ataques en las redes móviles ad hoc y pocos trabajos se encuentran al respecto. Cuando un ataque ocurre, técnicas de prevención y contramedidas como encriptamiento y autenticación, son usualmente las primeras líneas de defensa. [1] Sin embargo, estas técnicas pueden no ser suficientes a medida que los sistemas se van volviendo más complejos y siempre existen debilidades que se pueden explotar debido a errores de programación y de diseño o la fragilidad y poca compatibilidad de los protocolos y estándares existentes.[2]

En las redes inalámbricas los ataques de denegación de servicio pueden ser clasificados principalmente en dos tipos, aquellos en la capa de enrutamiento y aquellos en la capa de acceso al medio MAC.[3] Esta investigación se enfocó en los ataques de denegación de servicios basados en tráfico sobre la capa de acceso al medio del protocolo IEEE 802.11 DCF,[4] actualmente usada para la construcción de las redes ad hoc.

El mejoramiento del desempeño de las redes ad hoc es un tema de alta preocupación en la actualidad y sobre el cual se ha trabajado de manera activa. Respecto a la mejora de redes de 1 salto existe la posibilidad de modificar el algoritmo de Backoff en la forma en que decrementa tras una transmisión exitosa tal y como lo proponen [5], [6] y [7] o ajustando el límite mínimo de la ventana de contención del algoritmo mediante una relación lineal de acuerdo con el número de nodos activos en la red, como en [8] y [9].

Aunque el protocolo 802.11b DCF[4] es actualmente usado para construir redes ad hoc, fue originalmente diseñado para redes de área local inalámbricas, [3] lo que revela problemas en el comportamiento de 802.11 y de su capa MAC. Estos son tratados en [10] donde proponen mejoras en el protocolo TCP y en la capa MAC, [11] y [12] donde estudian la verdadera efectividad del intercambio de paquetes de control ante problemas como el del nodo escondido, [13] donde estudian el comportamiento de TCP sobre la capa MAC de 802.11 y proponen el aumento del límite de retransmisión para mejorar su desempeño, [14] donde basados en otros artículos, estudia y detalla los problemas de desempeño de IEEE 802.11 en redes ad hoc y [15] donde los autores exponen los problemas de capacidad en este tipo de redes.

En los artículos antes descritos se trabaja con redes en condiciones de tráfico homogéneas o al menos similares, no frente a un comportamiento de ataque o parecido. En [16] se propone el método de Back-Pressure, donde la fuente tiene memoria del tamaño de las colas de los nodos en la ruta hacia su destino, como mejora en la relación de paquetes entregados TCP en presencia de tráficos UDP. En [1] se analizan varias topologías de ataque de denegación de servicio sobre la capa de acceso al medio de una red de múltiple salto y en [17] se resumen vulnerabilidades del protocolo y se listan una serie de soluciones basadas en estas vulnerabilidades sin profundizar, entre ellas una capa MAC más justa, que es lo que finalmente se plantea en esta investigación,

como solución para fortalecer la capa de acceso al medio ante los ataques de denegación de servicio en redes de múltiple salto.

Este artículo se desarrolla de la siguiente forma: en la sección II se describen, reproducen y comparan algunas de las mejoras que se han hecho para aumentar el desempeño de las redes ad hoc, en la sección III se resumen algunos problemas y vulnerabilidades que se han identificado en el protocolo MAC 802.11, en la sección IV se hace referencia al efecto captura principal causa de estos ataques y cómo ocurre la denegación de servicio en la capa MAC. Finalmente en la sección V se plantea el fortalecimiento de la capa MAC como posible solución ante este tipo de ataque sobre la red. La herramienta usada en esta investigación es el software de simulación de redes Qualnet®[18]. Más detalles e información acerca del protocolo 802.11, de su capa MAC y de su algoritmo de Backoff (BEB) pueden encontrarse en [4] y [19].

## 2. MEJORAS AL ALGORITMO DE BACKOFF DEL PROTOCOLO MAC IEEE 802.11 DCF BEB

Recientemente se ha estudiado la forma de mejorar el desempeño, en términos de caudal, del protocolo MAC 802.11 DCF en redes de 1 salto, es decir, redes similares a las redes de área local inalámbricas sin un punto de acceso a una red física. Modelos analíticos del desempeño de 802.11 en redes ad hoc de 1 salto son descritos en [5] y [20].

### 2.1. Algoritmos basados en el decremento de la ventana de contención

Entre los artículos que proponen una mejora al algoritmo de Backoff BEB en redes de 1 salto están: el algoritmo DIDD (*Double Increment Double Decrement*) propuesto en [5], el algoritmo MIMD (*Multiplicative Increase Multiplicative Decrease*) [6], y el EIED (*Exponential Increase exponential Decrease*) [7] elaborado por el Instituto Nacional de Estándares (NIST). La mejora consiste en modificar el procedimiento como el algoritmo BEB decrementa (selección del valor de la ventana de contención, CW) en un nodo, después de que ha logrado una transmisión exitosa. La variación hecha en cada uno de los algoritmos se resume a continuación:

$$BEB: \begin{cases} CW \leftarrow \min(2 \cdot CW, CW_{max}) & \text{incremento tras una colisión} \\ CW \leftarrow CW_{min} & \text{decremento después de transmisión} \end{cases}$$

$$DIDD = MIMD: \begin{cases} CW \leftarrow \min(2 \cdot CW, CW_{max}) & \text{después de colisión} \\ CW \leftarrow \max(CW/2, CW_{min}) & \text{después de transmisión} \end{cases}$$

$$EIED: \begin{cases} CW \leftarrow \min(2 \cdot CW, CW_{max}) & \text{después de colisión} \\ CW \leftarrow \max(CW/\sqrt{2}, CW_{min}) & \text{después de transmisión} \end{cases}$$

Estos algoritmos buscan mejorar el caudal total en la red haciendo más suave el decremento del algoritmo de Backoff, es decir, dando más pasos entre el valor actual que tenga la ventana de contención y el valor mínimo de la misma. La desventaja de estos algoritmos es que no buscan hacer más equitativo o más justo el envío de todos los nodos que simultáneamente hacen uso de la red.

### 2.2. Algoritmo NBA

Optimizar la ventana de contención es otra forma de mejorar el desempeño de una red de 1 salto. Esto es descrito en [8] donde definen el algoritmo NBA (*Neighbourhood Backoff Algorithm*) basado en el número de nodos de la red. Para esto en Qualnet®[18], se establecen redes de 1 salto, de diferente número de nodos en un mismo rango

de transmisión y ubicados aleatoriamente sobre un área de 50m x 50m. Los nodos son estáticos ya que la movilidad dificulta el análisis [8]. Cada nodo envía paquetes simultáneamente a los otros a tres diferentes tasas, en un canal de 11Mbps por 180s.

Con este escenario se varía el límite mínimo de ventana de contención (CWmin) buscando el valor con el cual se optimiza el caudal en la red y evitar si CWmin alto, se desperdicien recursos o si es muy bajo el número de colisiones aumente.

Normalmente, a medida que el número de nodos de la red crece, el caudal total en la red va disminuyendo.

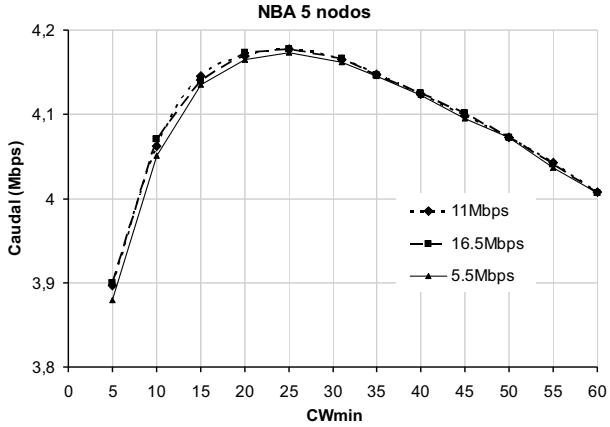


**Figura 1.** Optimización de la ventana de contención para red de 5 nodos, algoritmo NBA.

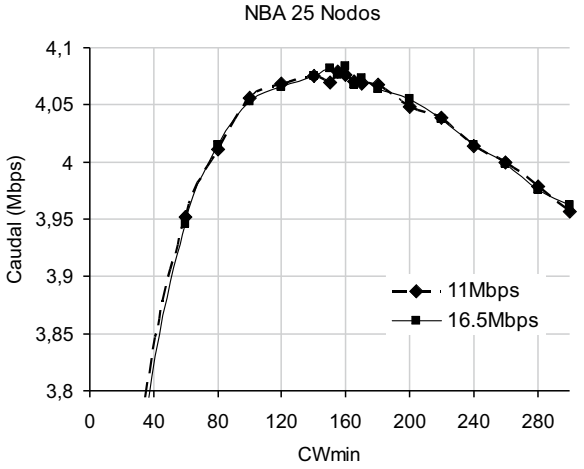


**Figura 2.** Optimización de la ventana de contención para red de 25 nodos, algoritmo NBA.

Tomando los valores de CWmin, que optimizan el caudal, donde mejora el desempeño de cada una de las redes, por ejemplo, como se observa en las Figuras 1 y 2, para una red de 5 nodos CWmin = 25 y para una red de 25 nodos CWmin =155 (a diferencia del estándar MAC 802.11 DCF donde CWmin=31) para cualquiera de las tasas de tráfico utilizadas: con carga menor a la capacidad del canal, carga igual a la capacidad del canal y carga superior a la capacidad del canal, se aproximan a una relación lineal y se encuentra que el valor óptimo de CWmin sigue la ecuación 6N – 4, donde N es el número de nodos en la red, como lo muestra la Figura 3. En el artículo original[8], encuentran que el valor óptimo de CWmin = 8.5N – 5; sin embargo, este fue originado usando el software de simulación OPNET®[21].

Con topologías aleatorias de red,[1] para un intervalo de confianza del 95%, con una variación del 1% con respecto al valor medio del caudal, al optimizar CWmin se comprueba una tendencia clara en el aumento del caudal a medida que la red crece de tamaño. Los resultados muestran en la Figura 4 que en una red de 30 nodos hay una mejora de 500Kbps, aproximadamente el 25% por encima de la red funcionando sobre el protocolo original. A pesar de que el número de nodos aumenta, el caudal permanece casi constante con el algoritmo NBA [8], mientras que usando el estándar original a medida que aumenta el número de nodos el caudal cae.

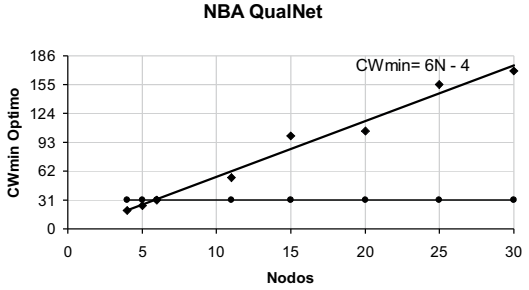


**Figura 3.** Relación entre el número de nodos y el límite mínimo de la ventana de contención.

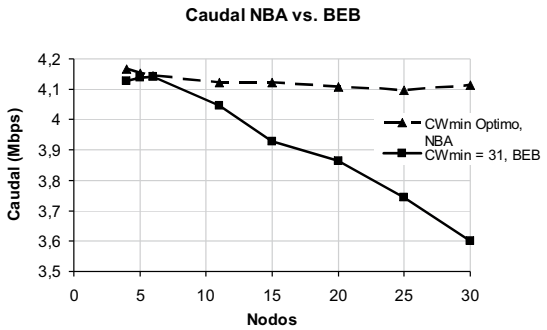


**Figura 4.** Mejora del desempeño con el algoritmo NBA.

1 Suficiente con 12 semillas, procedimiento descrito en [22].

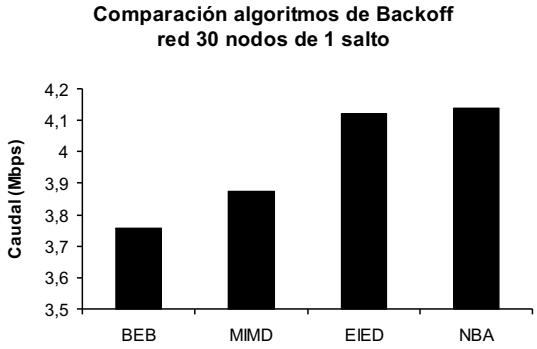


**Figura 5.** Comparación en red de 30 nodos de 1 salto de algoritmos de Backoff.

Implementando en Qualnet®[18] los algoritmos de mejora de desempeño de redes de 1 salto y comparándolos en las mismas redes usadas para el algoritmo NBA[8], encontramos que el que muestra mejor desempeño en cuanto aumento del caudal total es el algoritmo NBA [8], en las diferentes topologías de red de diferente número de nodos. Tanto MIMD, EIED como NBA, muestran una mejoría sobre el algoritmo BEB, como se observa en la Figura 5.

## 3. PROBLEMAS RELEVANTES DE LA CAPA MAC

El actual protocolo MAC IEEE 802.11 muestra varios problemas cuando es usado en una red de múltiple salto. Algunos han sido ampliamente tratados como el rango de interferencia [11] y [12], el cual aparece debido al rango de transmisión de cada nodo y hace que nodos cercanos no puedan transmitir simultáneamente y deban diferir por un tiempo aleatorio (algoritmo de Backoff). En Qualnet® el rango de interferencia es superior a 2 veces el rango de transmisión. Otros problemas comunes son el del nodo escondido y el del nodo expuesto, tratados con mayor profundidad en [11] y [23].

### 3.1. Descenso en el caudal

La disminución en el desempeño de la red a medida que aumenta el número de saltos, es otra vulnerabilidad que presenta el protocolo MAC 802.11 DCF sobre las redes ad hoc. En una cadena de nodos como en la Figura 6, separados 350m con rango de transmisión 376m, los paquetes se originan en el primer nodo y son reenviados hasta el último nodo.

El nodo 1 y el nodo 2 no pueden transmitir al mismo tiempo ya que el nodo 2 no puede recibir y enviar simultáneamente. Los nodos 1 y 3 no pueden transmitir al mismo tiempo ya que el nodo 2 no puede escuchar correctamente al nodo 1 si 3 está enviando. La transmisión del nodo 4 interfiere con los paquetes RTS enviados de 1 a 2, evitando que el nodo 2 reciba correctamente los RTS del nodo 1 o enviar los correspondientes CTS. En este caso se esperaría que la utilización máxima es 1/4 [15], sin embargo la caída es todavía mucho más dramática tanto para un tráfico CBR como para tráficos FTP (TCP) de distintos tamaños de paquete, como se muestra en la Figura 6. Por este motivo el caudal en las redes de

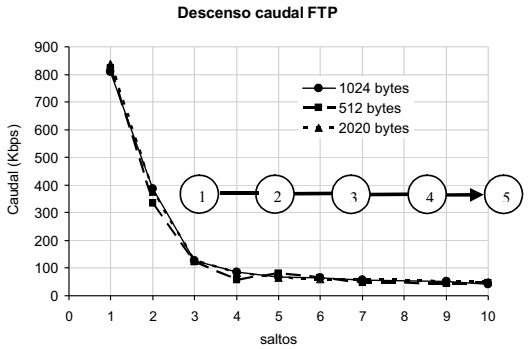


**Figura 6.** Descenso del caudal en sesión FTP de 1000 paquetes.

menor tamaño es mucho mayor que en las redes con mayor número de saltos para cada una de sus sesiones de tráfico.

### 3.2. Comportamiento injusto e inequitativo

La combinación de estos problemas lleva un comportamiento injusto e inequitativo. A medida que dos tráficos o nodos vecinos se acercan o se alejan, hace que a ciertas distancias el tráfico sea suprimido en su totalidad, cuando existe una segunda transmisión que bloquea a la transmisión inicial [17]. Al variar la distancia entre los nodos 2 y 3 en la Figura 7, aparecen zonas donde uno de los tráficos es suprimido en su totalidad. Esto no solo ocurre cuando la dirección del tráfico es como se muestra en la Figura 7, sino en las otras tres combinaciones posibles de sentido del tráfico entre cada par de nodos. Es irrelevante la distancia entre los nodos, siempre y cuando el rango de transmisión cubra esta distancia, ya que el problema real es el cruce de los rangos de interferencia que se crean.


**Figura 7.** Topología de la inequidad en redes de múltiple salto.

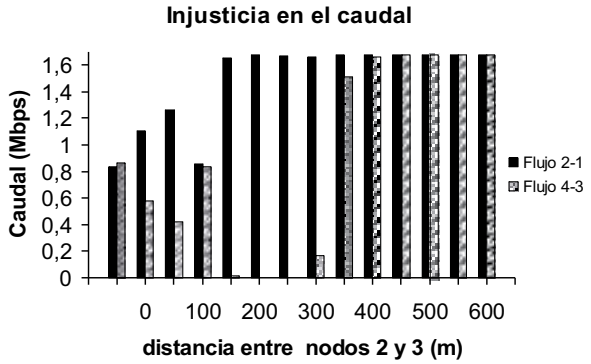


**Figura 8.** Injusticia en el caudal de dos tráficos con la misma dirección.

Para este caso el rango de transmisión entre los nodos 1 y 2 es de 75m y entre 3 y 4 es de 150m. Como se observó en la Figura 8, el flujo del nodo 2 al nodo 1 suprime el otro flujo totalmente cuando 2 y 3 están separados entre 150m y 300m, lugares críticos de interferencia.

## 4. DENEGACIÓN DE SERVICIO EN LA CAPA MAC

### 4.1. Efecto Captura

El Efecto Captura [1] y [16] sucede cuando debido a un tráfico mucho mayor, los tráficos que circulan por una red son suprimidos casi en su totalidad. Esto ocurre ya que el algoritmo de Backoff de 802.11, BEB, siempre favorece al último nodo que ganó el turno de transmitir, es decir, al nodo más activo. Cuando un nodo transmite exitosamente, la ventana de contención del algoritmo se reinicia a su límite mínimo: 31.

Mientras los otros nodos han estado retrocediendo sin lograr transmitir y sus ventanas de contención son mucho mayores, el nodo con la ventana de contención igual a 31 nuevamente gana el derecho a transmitir.

El Efecto Captura muestra sus peores consecuencias cuando la transmisión es hecha sobre nodos en la vecindad de una fuente de tráfico o de su destino, creando congestiones que evitan que el flujo normal sea enviado por su cliente o sea recibido por el nodo servidor, ya que el nodo con la tasa de envío alta siempre tiene prioridad para acceder al canal y bloquea el normal intercambio de paquetes de control, haciendo que los otros nodos siempre escuchen el canal como ocupado y se vean obligados a retroceder en su transmisión. Los dos factores en orden de importancia, que llevan a que el Efecto Captura se produzca son [10]: El número de saltos, es decir, cuanto menor número de saltos tenga una transmisión mayor es la posibilidad de suprimir el tráfico ganando el acceso al medio y la cantidad de tráfico enviado, a mayor tráfico peores las consecuencias pues los nodos con carga más pesada tienden a ganar el canal y hacen que los otros entren en su proceso de Backoff continuamente.

El Efecto Captura es la causa principal para que la presencia de ataques de denegación de servicio basados en congestión sobre la capa MAC de una red de múltiple salto, se puedan presentar y sean muy fáciles de lanzar y de lograr. Cuando un nodo realiza una transmisión a una tasa muy alta, es decir, ataca otro nodo (sea éste cómplice o no) en la vecindad de un tercero, el tráfico que envía lo recibe este tercero o puede llegar a suprimirse y el efecto es aún peor si sobre la estación convergen varios tráficos, ya sea por ser el destino final o por ser un paso necesario en la ruta a su destino. Un ejemplo sencillo del ataque sobre una cadena de nodos de dos saltos se describe en la Figura 9 y su efecto se ve en la Figura 11.

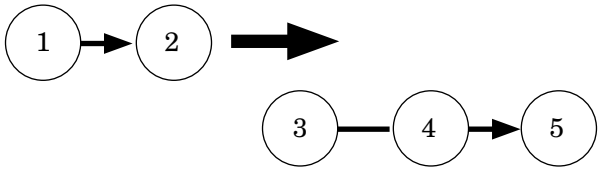


**Figura 9.** Ataque de denegación de servicio sobre cadena de dos saltos.

En la Figura 9 el nodo 1 es el nodo atacante, el nodo 2 es el receptor del ataque y éste es hecho sobre un tráfico de dos saltos que va desde el nodo 3 al nodo 5. El ataque se mueve como lo indica la flecha, de tal manera que queda en el área de interferencia primero del cliente (nodo 3) y después del servidor (nodo 5).

La distancia de separación vertical entre los nodos 2 y 3 no importa, ya que mientras el ataque (la flecha gruesa entre el área punteada y el área continua, Figura 10) permanezca en el área de interferencia del tráfico normal (flecha delgada horizontal, Figura 10) suprime totalmente el tráfico de 3 a 5, primero en el área de interferencia del cliente (entre 200m y 450m) y después en el área de interferencia del servidor, donde es mayor la supresión del caudal (entre 900 y 1.300m) como se muestra en la Figura 11.

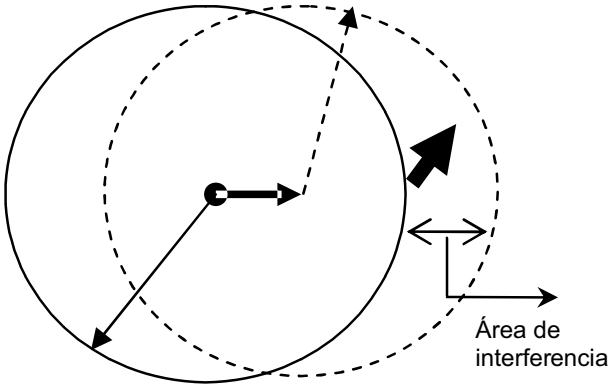


**Figura 10.** Área de interferencia, zona de ataque [17].

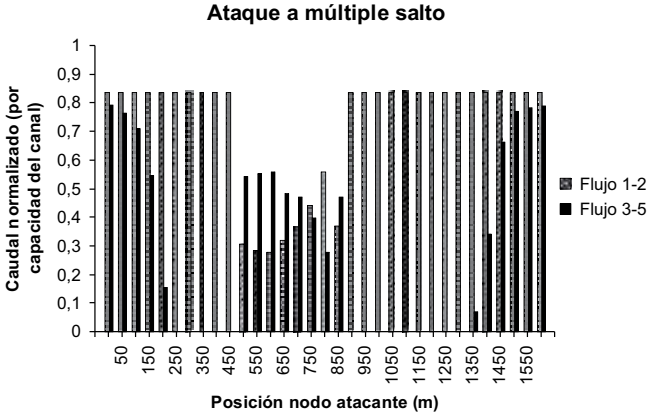


**Figura 11.** Caída del caudal ante DoS sobre cadena de 2 saltos.

Para demostrar el efecto "devastador" que puede tener un ataque de esta clase sobre el desempeño y la cantidad de información entregada, así como las posibles soluciones y la solución planteada, se configuraron una serie de experimentos los cuales se explican a continuación.

### 4.2. Escenario de simulación

Los escenarios de simulación son redes de topología en malla, similares a la red usada en [1] pero de diferente número de nodos (25, 36, 49, 64, 81, 100, 121, 144 y 169). El área de simulación varía de acuerdo con el número de nodos de la red (ej. para 169 nodos, 13 x 350m = 4.550m x 4.550m). El escenario fue escogido debido a su simplicidad en mostrar el impacto de la inequidad e injusticia de la capa MAC sobre TCP debido al ataque [1]. Los nodos están separados 350 metros y se ajustó la potencia para que el rango de transmisión cubra esta distancia hasta 376 metros, por lo tanto la transmisión es posible solo en forma horizontal y/o vertical. Desde los nodos de la esquinas y en la mitad del borde exterior de la malla (nodos 1-8, Figura 12) son enviados 1.000 paquetes de 512 bytes de tipo TCP en 8 diferentes sesiones hacia el nodo central de la red durante 900 segundos de simulación (1.000 x 512 x 8 = 4.096 kbytes), las cuales representan el tráfico normal de la red. El ataque es simulado por una sesión de tráfico CBR.

La frecuencia de operación es 2.4GHz como es sugerido para redes ad hoc, el ancho máximo del canal inalámbrico es de 2Mbps y los parámetros de la capa física y MAC son los mismos definidos en el estándar 802.11b en modo DCF que trae el software de simulación Qualnet® por defecto.

Los nodos son estáticos para mantener constante el ataque pues el ataque sobre un nodo estático es peor que sobre un nodo en movimiento y así descartar las pérdidas de paquetes por rompimiento del enlace [1]. La sesión de ataque tiene el mismo tiempo de duración y es simultánea a las 8 sesiones de tráfico FTP. Si el ataque cesa el tráfico normal continúa y el desempeño de la red mejora. La tasa de ataque usada fue de 2Mbps, sin embargo desde tasas de ataque cercanas a 1Mbps se obtienen resultados similares. El protocolo de enrutamiento usado fue AODV. Las simulaciones de los ataques y de la solución fueron hechas con 10 semillas y un intervalo de confianza del 95%.

### 4.3. Ataque a un salto del servidor

El objetivo de este experimento es mostrar que un servicio es vulnerable ante un ataque lanzado desde 1 salto por cualquiera de sus vecinos [1]. Se implementó el siguiente ataque: una sesión CBR a la tasa máxima del canal 2Mbps, desde un nodo a un salto del nodo del servidor hacia uno de sus vecinos. Cabe resaltar que si el ataque se mueve a otros nodos en la vecindad del servidor, el efecto sobre los demás tráficos de la red es similar.

Los resultados que se muestran son los correspondientes al ataque, como lo indica la flecha más gruesa en la Figura 12. A medida que la tasa de ataque aumenta la disminución del tráfico TCP de la red es mayor, sin importar el tamaño del paquete enviado, como lo muestra la Figura 13.

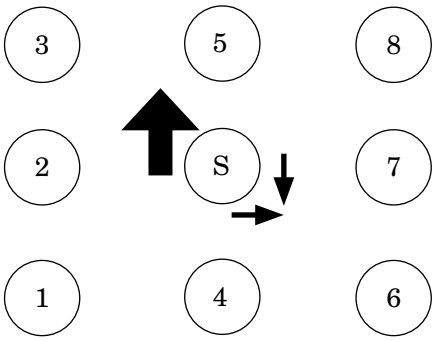


**Figura 12.** Ejemplo de ataques a un salto del servidor

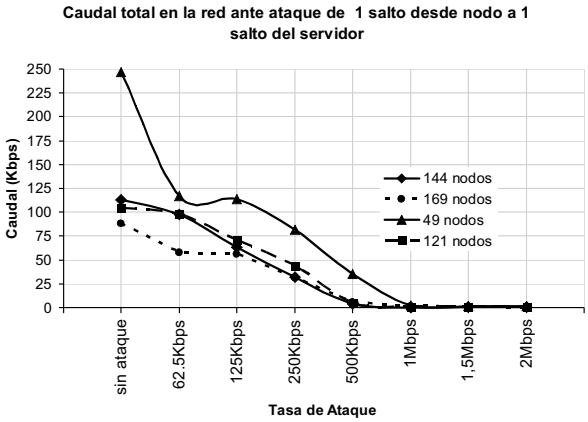


**Figura 13.** Caudal total en varias redes vs. Tasa de ataque.

**Tabla 1.** Caudal(bps) red sin ataque vs. Caudal(bps) red con ataque.

| Nodos | Con ataque | Sin ataque | Porcentaje |
|---|---|---|---|
| 25 | 5529 | 663091 | 0,83 |
| 36 | 1234 | 387414 | 0,32 |
| 49 | 1709 | 246492 | 0,69 |
| 64 | 1193 | 210797 | 0,57 |
| 81 | 440 | 147954 | 0,30 |
| 100 | 941 | 106803 | 0,88 |
| 121 | 467 | 104491 | 0,45 |
| 144 | 573 | 112738 | 0,51 |
| 169 | 239 | 88476 | 0,27 |

La Tabla 1 muestra el descenso "dramático" en el caudal en la red, a valores por debajo del 1% del desempeño normal de la red en todos los escenarios planteados. Esto se debe a la incapacidad del servidor de recibir paquetes o de transmitir el acuse de recibo de los pocos que llegan.

El ataque produce una gran pérdida de paquetes, como lo muestra la Figura 14, de casi el 100%, ya que los nodos usan todos sus intentos de retransmisión sin lograr que los paquetes lleguen a su destino. El número de paquetes RTS y CTS en las redes con ataque es mayor que en la red sin ataque buscando lograr establecer la comunicación, sin éxito, por la presencia del ataque. El ataque produce el efecto captura ya que al tener una tasa más alta y tener un solo salto de camino, gana siempre la contención y por lo tanto tiene la prioridad para transmitir mientras que los demás nodos retroceden y entran nuevamente a realizar sus respectivos Backoff.

### 4.4. Otras topologías de ataque

El ataque a un salto del cliente, desde un nodo vecino hacia otro ubicado a 1 salto del nodo atacante, quiere resaltar la forma como se puede suprimir el tráfico de una fuente de tráfico específica. La disminución en el caudal y de la relación de paquetes entregados al servidor se debe a la imposibilidad de establecerse el handshake RTS/CTS, por el bloqueo de dichos paquetes de control por parte del ataque y se da únicamente para el nodo que es atacado.

Un ataque de múltiple salto es difícil de lanzar y más difícil aún que llegue a suprimir el tráfico de un grupo de nodos o de toda la red. Primero porque si los nodos fuente y destino del ataque están aliados o no, el atacante debe violar el sistema de autenticación de la red para poder usar como enrutadores los otros nodos que están en la trayectoria del tráfico[1]. Segundo, porque a medida que crece el número de saltos el caudal del ataque también disminuye, problema general de la capa MAC de 802.11 DCF, luego un ataque de

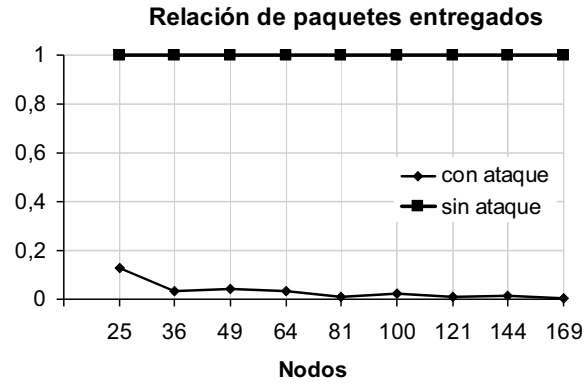


**Figura 14.** Relación de entrega de paquetes red sin ataque vs. red con ataque.

denegación de servicio basado en tráfico es más efectivo cuando el número de saltos que atraviesa es menor. Esto lleva a que si se lanza un ataque de múltiple salto buscando partir la red, es decir, impedir el normal funcionamiento de ciertos nodos de la red que se encuentren en la partición, el ataque lleve a una congestión localizada si la red es suficientemente grande.

La Figura 15 muestra con las flechas dos casos posibles de cómo el atacante podría buscar partir la red, por ejemplo lanzando un ataque desde un vecino de 1 hasta un vecino de 3 y suprimir los servicios de los nodos 1, 2 y 3.

Los resultados en la Tabla 2 muestran que aunque sí hay un descenso en el caudal de los 3 clientes en la partición (1, 2 y 3), los peores resultados los tiene el nodo 1, ya que el atacante está en su vecindad y la red se comporta como si el ataque estuviese a un salto del cliente, reduciendo su caudal y el número de paquetes entregados a cerca del 2%. El nodo 2 alcanza a entregar todos sus paquetes pero su caudal se ve disminuido a cerca del 30%. La relación de entrega de paquetes del nodo 3 es 1, su caudal disminuye a cerca del 45%.

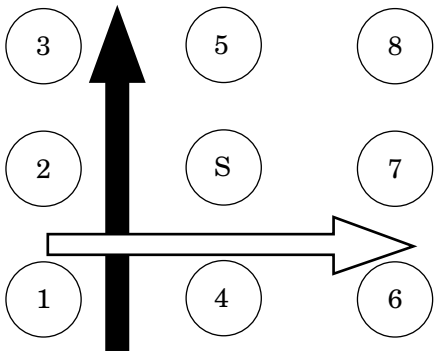


**Figura 15.** Ataques de múltiple salto, partición de la red.

**Tabla 2.** Resultados de ataque de múltiple salto en red de 169 nodos

| | Con ataque | | Sin ataque | |
|---|---|---|---|---|
| Cliente | Caudal (bps) | kbytes entregados | Caudal (bps) | kbytes entregados |
| 1 | 158 | 13.3 | 6151 | 512 |
| 2 | 6722 | 512 | 19164 | 512 |
| 3 | 4892 | 512 | 12407 | 512 |
| 4 | 10275 | 512 | 13576 | 512 |
| 5 | 8117 | 512 | 8505 | 512 |
| 6 | 5728 | 512 | 6899 | 512 |
| 7 | 7921 | 512 | 11198 | 512 |
| 8 | 11770 | 512 | 10576 | 512 |

Los efectos sobre el nodo 3 son menores, ya que está más alejado de la fuente del ataque y por lo tanto la intensidad del ataque ha disminuido por el mayor número de saltos.[1] En opinión del autor de este artículo, aunque hay una reducción del caudal, esto no es tan importante ya que toda la información, es decir, todos los paquetes son entregados en forma satisfactoria y la pérdida de paquete es una consecuencia más grave. Los resultados del ataque desde un vecino del nodo 1 hasta un vecino del nodo 6 presentan comportamientos similares.

## 5. ALIVIO DEL IMPACTO ANTE DENEGACIÓN DE SERVICIO DE LA CAPA MAC IEEE 802.11 DCF

La causa principal de estos ataques es el efecto captura. El nodo que lanza el ataque de denegación de servicio gana siempre el privilegio de transmitir ya que puede reanudar continuamente su ventana de contención y su tiempo de Backoff es menor, lo cual impide que las transmisiones de los otros nodos lleguen al servidor, pues el BEB siempre favorece el último ganador entre los nodos contendientes por el canal.

Análisis sobre la prevención de los ataques de denegación de servicio se han hecho anteriormente pero pocas soluciones se han propuesto. En [17] el autor analiza las causas de la pasividad y permisividad de la capa MAC ante el ataque de denegación de servicio y las consecuencias en el caudal sobre cadenas de nodos. Los autores proponen soluciones como disminuir la distancia entre el nodo fuente y destino de los tráficos con el fin de reducir el tamaño del área de interferencia, aumentar el nivel de seguridad de las redes y mejorar la capa MAC en cuanto a comportamiento equitativo; sin embargo no desarrollan ni muestran resultados de estas soluciones.

Una solución concreta para disminuir el efecto en la red ad hoc del ataque es planteada en [1], aunque superficial, propone aumentar la justicia y equidad en el comportamiento de la capa MAC para evitar la disminución del caudal. Los autores del artículo llaman a esta solución FAIRMAC; es un protocolo basado en TDMA que usa *time slots* fijos y logra mejoras de hasta el 55%, al trabajar exclusivamente en una red de topología de malla (12 x 12) de 144 nodos. Para mejorar la capa MAC, con el fin de evitar que un ataque en el interior de una red sea exitoso, se estudiaron los parámetros configurables de la capa MAC y el algoritmo de Backoff, los cuales se tratan a continuación.

### 5.1. Límites de retransmisión

El límite de retransmisión corto es el número límite máximo de transmisiones configurado para una estación, esperadas para recibir un paquete CTS, es decir, el número máximo de veces que es posible retransmitir un paquete RTS. El límite de retransmisión largo es el valor límite de transmisiones esperadas para que una estación reciba un paquete ACK, o el número máximo de veces que una estación puede retransmitir un paquete de datos.

El estándar de 802.11 [4] define un valor al límite de retransmisión corto de 7 intentos y al límite de retransmisión largo de 4 intentos. Tarjetas de red inalámbricas comerciales como las Cisco Aironet [24] asignan un valor variable de 16 para los límites de retransmisión largo y corto, en un rango de 1 a 128; sin embargo, el estándar no define un número máxi-

mo para los límites de retransmisión para 802.11b. Para 802.11a el estándar define que el rango de los límites de retransmisión es de 1 a 255 [4].

Al aumentar los límites de retransmisión se reduce el número de paquetes perdidos debido a colisiones por congestión y por tanto al efecto captura, haciendo la capa MAC más insistente en buscar que el envío y recepción de los paquetes sea satisfactorio. No obstante, un aumento en estos valores podría no ser recomendable para la red ya que se desperdiciarían recursos de ancho de banda y se estaría muy alejado de los valores comerciales para estos dos parámetros.

En [13], para redes inalámbricas de múltiple salto, de comportamiento estático, topología en cadena y un solo tráfico TCP a través de ellas sin necesidad de enrutamiento, se aumentó el límite de retransmisión de paquetes cortos a 14 y el límite de 9 retransmisión de paquetes de datos a 10. El artículo registra que para redes con mayor número de saltos se logra incrementar el caudal y el número de paquetes recibidos desde el 18% hasta el 39%. Cabe resaltar que las redes utilizadas no presentaban condiciones de tráfico heterogéneas y menos una simulación de un ataque de denegación de servicio sobre la red. En [16] se propone que con un aumento mayor en los límites de retransmisión, a 21 para el límite de retransmisión corto y a 12 para el límite de retransmisión largo en una red más compleja: sesiones de tráfico TCP enrutados mediante el protocolo AODV en presencia de un tráfico UDP, se logra mejorar el desempeño de la red propuesta hasta en un 33%. Al ser replicado este experimento en condiciones de red similares, no se encontró que la mejora del desempeño llegara al valor reportado, solo se observó una mejora mínima del 3% en el caudal total de la red.

En el escenario de simulación planteado y lanzando el ataque de denegación de servicio basado en congestión en el vecindario del nodo servidor (descritos en la sección IV) a una tasa igual al total del ancho de banda del canal (2Mbps), con los límites de retransmisión por defecto (7 y 4), el ataque hace que el caudal total de la red caiga hasta 0.5% y el número de bytes recibidos a 1.4% para la red de 144 nodos y en menos del 1% del caudal y a menos del 1.5% de bytes recibidos en todas las redes.

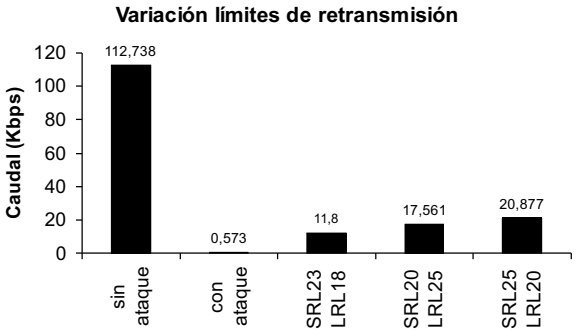


**Figura 16.** Caudal total en la red ante DoS ajustando los límites de retransmisión.[2]

2. SRL: Límite de retransmisión de paquetes cortos, LRL: Límite de retransmisión de paquetes largos

Para darle una mayor insistencia a la capa MAC al retransmitir los paquetes que se pierden debido a la presencia del ataque en la red, teniendo en cuenta el comportamiento de múltiple salto y así los paquetes puedan llegar a su destino y el rendimiento de la red mejore, se aumentaron los límites. Aunque aumentar los límites de retransmisión no muestra una tendencia clara en el aumento del caudal de la red, sí ayuda a aliviar el efecto del ataque. Con valores de los límites de retransmisión por encima de 20, por ejemplo 23 y 18, 25 y 20, 20 y 25 (límite de retransmisión de paquetes cortos y límite de retransmisión de paquetes largos) el caudal total de la red en presencia del ataque DoS mejora desde cerca de un 10% hasta aproximadamente el 25%, tal y como se muestra en la Figura 16, ya que más paquetes son entregados a su destino.

### 5.2. Mejora del algoritmo de Backoff ante denegación de servicio

El efecto captura hace que el ataque de denegación de servicio, con menor número de saltos y mayor cantidad de tráfico, tenga privilegio sobre el acceso al medio ya que el retroceso del algoritmo de Backoff lo favorece, pues cuando reanuda su ventana de contención el tiempo de Backoff siempre es el menor, venciendo a los demás nodos por el acceso al canal.

Los algoritmos de mejora del desempeño tratados en la sección II, no funcionan en disminuir el efecto captura en la capa de acceso al medio en redes de múltiple salto, debido a que estos algoritmos continúan dando prioridad al transmitir al nodo que logra la última transmisión exitosa, el ataque para este caso. Para evitar que el tiempo de Backoff del nodo atacante siempre fuera el menor y hubiese una gran diferencia con los tiempos de Backoff de los clientes, obligándolos a ceder el acceso al canal continuamente, se aumentó el valor del límite mínimo de la ventana de contención para todos los escenarios de simulación, en busca de hacer más equitativa la oportunidad de todos los nodos para transmitir. A partir de esto se encontró que el caudal y la relación de paquetes entregados aumentaban a medida que CWmin era mayor, sobre todo cuando la red tiene un mayor número de nodos y de saltos para los tráficos normales. Un ejemplo de esto se muestra en la Figura 17.

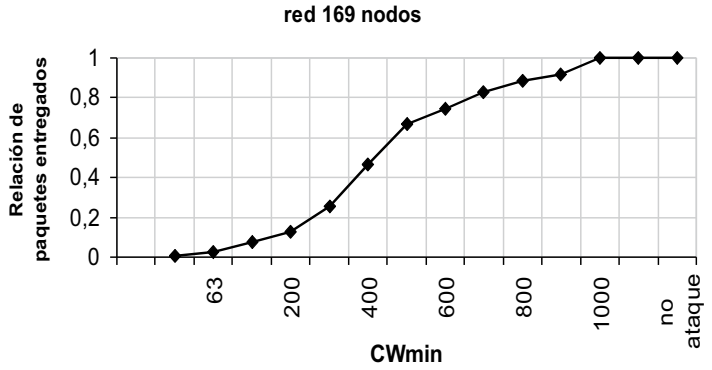


**Figura 17.** Relación de paquetes entregados en red de 169 nodos bajo ataque aumentando CWmin.

La relación de entrega de paquetes en la red de 169 nodos, Figura 17, va aumentando hasta alcanzar 1 (100%). El caudal en la red bajo ataque aumenta considerablemente y llega hasta por encima del 60%. Debido a este comportamiento más equitativo, el número de veces que transmite el nodo atacante disminuye y por tanto su tráfico, aumentando así el desempeño de los clientes. Este mismo comportamiento puede notarse en todos los tamaños de red y se muestra en la Figura 18, para la red de 144 nodos.

Teniendo en cuenta lo anteriormente descrito, se propone una modificación en el algoritmo que no es tan agresiva en la forma como retrocede y que fuese igual de suave para que no aumentara la injusticia e inequidad en las transmisiones de los clientes. También se buscó que fuera dinámica, similar a las mejoras para la red de 1 salto, de tal forma que no hubiese necesidad de dejar fijo CWmin. Por esto se realizó la siguiente modificación en el algoritmo de Backoff de 802.11 dejando los límites mínimo y máximo de la ventana de contención, tal y como los trae el estándar:

$$\begin{Bmatrix} CW \leftarrow \min(2 \cdot CW, CW_{max}) & después\ de\ colisión \\ CW \leftarrow \max(CW\text{-}1, CW_{min}) & después\ de\ transmisión \end{Bmatrix}$$

Cuando hay una colisión, al igual que en el esquema BEB, la ventana de contención se dobla hasta alcanzar su límite máximo (1.023). Después de una transmisión exitosa, en lugar de reanudar la ventana de contención a 31, escoge el máximo entre el valor mínimo de CW y el valor actual de la ventana de contención menos 1 *time slot* (en tiempo 20µs). Esto hace que los tamaños de las ventanas de contención de todos los nodos, incluido el nodo de ataque, sean similares, entonces los clientes pueden tener la misma o mayor oportunidad de transmitir ya que su tiempo de Backoff puede ser menor que el del atacante. Usando el algoritmo propuesto, en las redes de mayor tamaño, la mejora del caudal alcanza hasta el 60% y la relación de entrega de paquetes desde el 80% hasta el 100% como se muestra en la Figura 21.

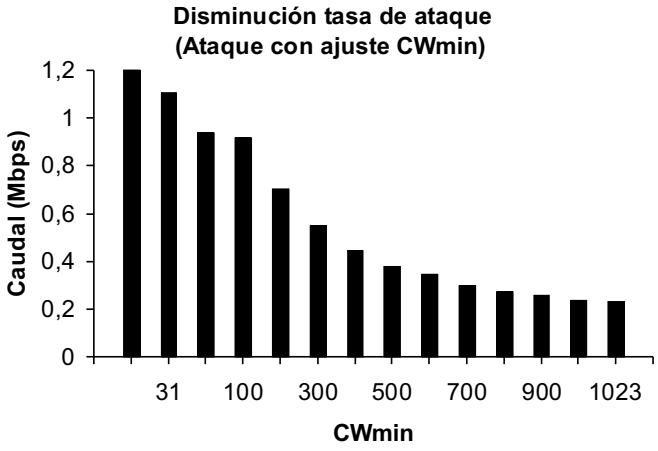


**Figura 18.** Disminución tasa de ataque con ajuste de CWmin, red 144 nodos.

El grado de retroceso del algoritmo de Backoff (- 1) fue escogido debido a que da un mejor desempeño sobre otros también considerados bajos y lineales. En las gráficas a continuación 2CW-16 significa que se dobla la ventana de contención cuando hay colisión y se disminuye 16 linealmente cuando ocurre una transmisión exitosa, para cualquier tamaño de red. Como ejemplo la Figura 19 muestra el comportamiento en una red de 144 nodos.

Siendo esta mejora al algoritmo una medida de fortalecimiento de la capa MAC, es necesario observar el comportamiento de la red sin ataque. El caudal disminuye en redes pequeñas, debido a que mayores tiempos de Backoff en tráficos de pocos saltos llevan a una mayor demora en la entrega de los paquetes. Sin embargo, en redes de mayor tamaño, con tráficos de más saltos, el algoritmo incluso mejora el caudal.

La relación de entrega de paquetes siempre permanece alta, tanto con el BEB como con el algoritmo propuesto, como se observa en la Figura 20, luego no hay disminución en esta métrica y el algoritmo propuesto funciona correctamente.

Si adicionalmente, además de modificar el algoritmo de Backoff frente al ataque de denegación de servicio, se aumenta la insistencia de envío de un paquete en la capa de acceso al medio a unos valores más acordes con la red de múltiple salto, la mejora ante el ataque es evidente y se muestra en la Figura 21. La relación de paquetes entregados crece al 100% para todas las redes y el caudal incluso sobrepasa el desempeño sin ataque en las redes de mayor número de nodos.

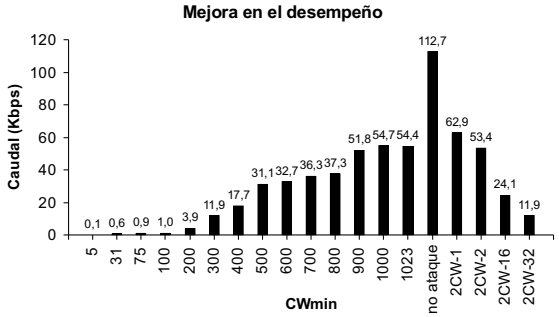


**Figura 19.** Comparación del caudal entre mejoras al BEB en red 144 nodos.

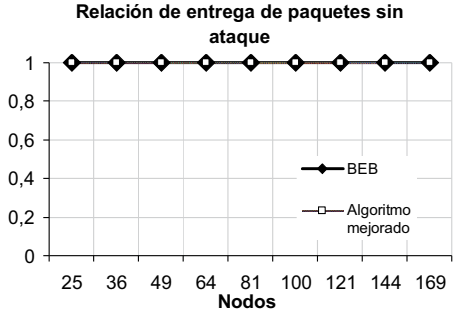


**Figura 20.** Relación de entrega de paquetes BEB vs. Algoritmo mejorado para DoS, sin ataque

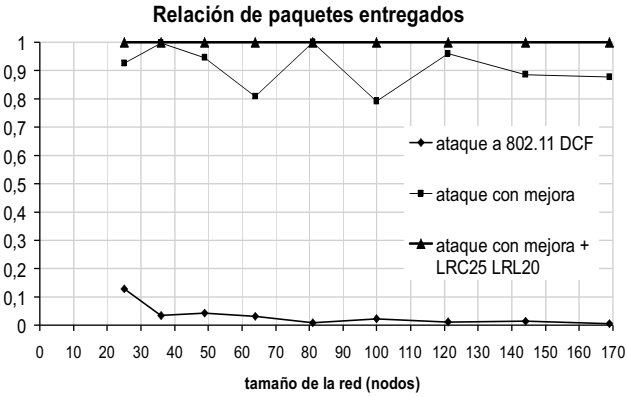


**Figura 21.** Relación de entrega de paquetes algoritmo mejorado para DoS.[3]

## 6. CONCLUSIONES

Esta investigación comprueba que la causa de la fragilidad de la red ante un ataque de denegación de servicio basado en tráfico es el efecto captura, que ocurre porque el algoritmo de Backoff de 802.11 favorece al nodo más activo de la red, es decir, al último en ganar el derecho a transmitir entre los nodos que contienden por el acceso al canal. Poco se ha estudiado acerca de este fenómeno en las redes de múltiple salto y se ha buscado adaptar métodos de las redes tradicionales como mecanismo de defensa ante estos ataques tales como encriptación y autenticación, los cuales no son tratados en este trabajo; sin embargo, existen pocos o ningún mecanismo que mitiguen el impacto del ataque sobre la red.

En este trabajo se estudiaron algoritmos para mejorar el desempeño de redes de un solo salto y se comprobó que no funcionan en redes de múltiple salto ya que continúan dándole favoritismo al nodo que ha logrado transmitir en el anterior intento. Se probaron otras mejoras planteadas para mejorar el desempeño tales como la disminución de la ventana de congestión de TCP [10], el ajuste del tamaño máximo del segmento y el ajuste del tiempo de espera tras colisión EIFS, sin ser positivas ante la presencia de un ataque de denegación de servicio en la red.

Se mostró que los límites de retransmisión, tal y como vienen definidos en el estándar, no son adecuados para las redes de múltiple salto y menos ante una red bajo ataque. Ajustando los límites a valores por encima de 20, se aumenta la insistencia de la capa MAC en el envío de paquetes, lo que hace que se pierdan menos cuando hay un ataque, aumentando el caudal y la relación de paquetes entregados. Esta medida mejora el desempeño de la capa MAC ante la presencia del ataque pero no es considerada como definitiva.

3. LRC: Límite de retransmisión corto, SLR: Límite de retransmisión largo

Una mejora adecuada del algoritmo de Backoff no solo aumenta el número de veces que pueden transmitir los nodos frente a un ataque de denegación de servicio, sino que puede servir como base para mejorar la calidad de servicio en una red *ad hoc*. La mejora propuesta y realizada aumenta el rendimiento en la red hasta un 60% y la relación de paquetes entregados hasta el 95% frente a un ataque. Al aplicar el algoritmo a la red en condiciones normales, el caudal en redes pequeñas es menor; sin embargo, la relación de entrega de paquetes permanece en 1. Si adicionalmente se realiza el ajuste de los límites de retransmisión a 25 y 20, el caudal aumenta considerablemente y se entrega el 100% de los paquetes enviados.

## BIBLIOGRAFÍA


[1] Vikram Gupta, Michalis Faloutsos, Srikanth Krishnamurthy. Denial of Service Attacks at the MAC Layer in Wireless ad hoc Networks. National Science Foundation, MilCom Anaheim, 2002.

[2] Wenke Lee Huang Yi-An, Zhang Yongguang. Intrusion Detection Techniques for Mobile Wireless Networks. Paper accepted for publication in ACM MONET Journal in 2002 and appear in this issue of ACM WINET due to editorial constraints.

[3] John Bellardo, Stefan Savage. 802.11 Denial of Service Attacks: real Vulnerabilities and Practical Solutions. Department of Computer Science and Engineering University of California at San Diego. In Proceedings of the USENIX Security Symposium, Aug 2003.

[4] ANSI/IEEE Std 802.11, 1999 Edition (Reafirmed 2003) Information technology -Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements— Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Sponsor LAN MAN Standards Committee of the IEEE Computer Society.

[5] P. Chatzimisios, A.C. Boucouvalas, V. Vitsas, A. Vafiadis, A. Economidis, P. Huang. A simple and effective backoff scheme for the IEEE 802.11 MAC protocol. Proceedings of the 2nd International Conference on Cybernetics and Information Technologies, Systems and Applications (CITSA 2005), Vol.I, pp. 48-53, Orlando, Florida, USA, 14-17 July 2005.

[6] H. Wu, S. Cheng, Y. Peng, K. Long, J. Ma. IEEE 802.11 Distributed Coordination Function (DCF): Analysis and Enhancement. Proc. IEEE ICC, New York, NY, 2002/04-05.

[7] Nah-Oak Song, Byung-Jae Kwak, Jabing Song, Leonard E. Miller. Enhancement of IEEE 802.11 Distributed Coordination Function with Exponential Increase Exponential Decrease Backoff Algorithm. Advanced Network Technologies Division National Institute of Standards and Technology NIST, MD, USA. 2003.

[8] Mahmoud Taifour, Farid Na¨t-Abdesselam and David Simplot-Ryl. Neighbourhood Backoff Algorithm for Optimizing Bandwidth in Single Hop Wireless Ad-Hoc Networks. LIFL/IRCiCA Laboratory - INRIA POPS Project. University of Sciences and Technologies of Lille, France. In Proc. 3erd. IEEE International Workshop on Mobility Management and Wireless Access (MobiWac, 2005), Maui Hawaii.

[9] J. Deng, P.K. Varshney, Z. J. Haas. A New Backoff Algorithm for the IEEE 802.11 Distributed Coordination Function. In Proc. of Communication Networks and Distributed Systems Modeling and simulations CNDS 04, San Diego CA, USA, January 18-2,2004.

[10] Shugong Xu, Tarek Saadawi. Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless ad hoc Networks. IEEE Communications Magazine, vol.39, Issue 6, June 2001.

[11] Kaixin Xu, Mario Gerla, Sang Bae. Effectiveness of RTS/CTS Handshake in IEEE 802.11 based ad hoc Networks. Ad hoc Networks, 1(1):107–123, July 2003.

[12] Kaixin Xu, Mario Gerla, Sang Bae. How effective is the IEEE 802.11 RTS/CTS handshake in .network. GLOBECOM 02. IEEE, vol 1, 17-21 Nov. 2002. pp 72-76.

[13] Rui Jiang, Chinya V. Ravishankar, Vikram Gupta. Interactions between TCP and the IEEE 802.11 MAC protocol. DISCEX, Volume I, 2003.

[14] Claude Chaudet, Dominique Dhoutaut, Isabelle Guérin Lassous. Performance Issues with 802.11 in ad hoc networking. Inria Ares team – Laboratoire Citi, Insa de Lyon. IEEE Communications Magazine, July 2005.

[15] Jinyang Li, Charles Blake, Douglas S.J. De Couto, Hu Imm Lee, and Robert Morris. Capacity of .wireless Networks. MIT. In Proceedings of the Seventh annual international conference on Mobile computing and networking (MobiCom 2001), pages 61–69, Roma, Italy, July 2001.

[16] Vikram Gupta, Michalis Faloutsos, Srikanth Krishnamurthy. Improving the performance of TCP in the presence of interacting UDP flows in ad hoc networks. IFIP Networking 2004, Athens, Greece.

[17] Yihong Zhou, Dapeng Wu, Scott M. Nettles. Analyzing and Preventing MAC-Layer Denial of Service Attacks for Stock 802.11 Systems. IEEE/ACM First International Workshop on Broadband Wireless Services and Applications, San Jose, CA, October 2004.

[18] Qualnet® Developer. Scalable Network Technologies Inc., SNT. Version 3.8. y Qualnet Community Forums. Disponible: www.qualnet.com

[19] Matthew S. Gast. 802.11® Wireless Networks: The Definitive Guide. Publisher: O'Reilly. April 2002. Pages: 464.

[20] G. Bianchi. Performance Analysis of the IEEE 802.11 Distributed Coordination Function, IEEE JSAC, vol. 18, no. 3, pp. 535 - 547, March 2000.

[21] OPNET® Modeller. www.opnet.com.

[22] Jerry Banks, John S. Carson. Discrete-Event System Simulation. Prentice Hall International series in industrial and system engineering.2001.

[23] Mari Carmen Domingo. Tesis Doctoral: Diferenciación de servicios y mejora de la supervivencia en redes ad hoc conectadas a redes fijas. Universidad Politécnica de Cataluña. 2005.

[24] Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Linux. Chapter 5 Advanced Configuration. OL-1376-02.

## CURRÍCULOS

**César Andrés Ramírez S. M.SC.** Desempeño de redes de múltiple salto ante ataque de denegación de servicio y alivio de su impacto. Tesis de grado, Magíster en Ingeniería. Area: electrónica y de computadores, línea de investigación telecomunicaciones. Universidad de los Andes.2006.

**Néstor Misael Peña T. Ph.D.** Department of Electrical and Electronic Engineering, Universidad de los Andes. (e-mail: npena@uniandes.edu.co).