DESEMPEÑO DE REDES DE MÚLTIPLE SALTO ANTE ATAQUE DE DENEGACIÓN DE SERVICIO Y ALIVIO DE SU IMPACTO

TESIS DE MAESTRIA PRESENTADA POR:

ING. CESAR ANDRES RAMIREZ SARMIENTO

ASESOR:

NESTOR MISAEL PEÑA TRASLAVIÑA, Ph.D

UNIVERSIDAD DE LOS ANDES
DEPARTAMENTO DE INGENIERIA ELECTRICA Y ELECTRONICA
MAESTRIA EN INGENIERIA ELECTRONICA
BOGOTA, JULIO 2006

AGRADECIMIENTOS

A mi papá Julio César y mi mamá Josefita por el ánimo, la confianza y el apoyo que me brindaron en todo momento.

A mi hermano Diego y en especial a mi hermana Sandra por la compañía y las palabras de aliento.

A mi familia, tías, primos, amigos, Norita y todos los que me brindaron su apoyo. A mi tío Gabriel, Marlene, Mauricio, Lina y Tito porque me abrieron sus puertas en los momentos difíciles.

Al profesor Néstor Peña por su comprensión y paciencia.

Finalmente esta tesis va dedicada a dos personas muy especiales a mi Nonita y a Luisa Fernanda que se fueron durante este año y me dieron fuerza e iluminaron desde el cielo.

TABLA DE CONTENIDO

LISTA DE FIGURAS Y TABLAS

1. INTRODUCCIÓN

Una red inalámbrica Ad Hoc o de múltiple salto consiste en un conjunto de nodos móviles, los cuales tienen la capacidad de comunicarse entre sí, sin la ayuda de una infraestructura fija a través del espacio libre, formando una topología de red arbitraria y distribuida. En éste nuevo entorno, los nodos participan en la toma de decisiones, realizando las funciones propias del mantenimiento de la red y tomando parte en los algoritmos enrutamiento. Esto hace que la topología de la red pueda cambiar rápidamente y de una forma no predecible [1].

El uso de medios inalámbricos hace por naturaleza a las redes Ad Hoc más vulnerables a ataques. En redes alambradas, el atacante necesita ganar el acceso al medio físico pasando a través de "*firewalls" y "gateways"* [2]. En redes inalámbricas el escenario es distinto, no existen "*firewalls" y "gateways"* (a menos de que exista un punto de acceso conectado a una red física) entonces, pueden sufrir ataques de toda dirección, por tanto, cada nodo en una red Ad Hoc debe estar preparado para encontrase con su adversario y por tanto con las consecuencias que el ataque le pueda acarrear [3]. Debido a la falta de una infraestructura de seguridad centralizada, la comunicación está más expuesta a ataques de seguridad y los nodos pueden ser fácilmente comprometidos.

Cuando un ataque ocurre, técnicas de prevención y defensa como encriptamiento y autenticación, son usualmente las primeras líneas de defensa [4]. 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 los errores de programación y de diseño, o a la fragilidad y poca compatibilidad de los protocolos y estándares existentes [4]. O es posible que debido a la espontaneidad e imprevisibilidad con que se establece una red Ad Hoc no sea posible instalar estas técnicas de defensa.

En las redes inalámbricas los ataques de denegación de servicio (DoS), pueden ser clasificados principalmente en dos tipos, aquellos en la capa de enrutamiento y aquellos en la capa de acceso al medio MAC [5]. Ninguno de los dos ha sido

ampliamente estudiado ni se han buscado formas claras de evitarlos. Esta tesis se enfocó en los ataques de denegación de servicio basados en tráfico sobre las redes de múltiple salto, más específicamente, la investigación se hizo acerca de éste tipo de ataques sobre la capa de acceso al medio del protocolo IEEE 802.11 DCF [6], actualmente usado 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 colisión, tal y como lo proponen [7] - [9] o ajustando el límite mínimo de la ventana de contención mediante una relación lineal de acuerdo al número de nodos activos en la red como en [10] - [11].

Aunque el protocolo 802.11b DCF es actualmente usado para construir redes Ad Hoc, fue originalmente diseñado para redes de área local inalámbricas no para redes de múltiple salto [5], lo que revela problemas en el comportamiento del protocolo y de la capa MAC. Estos problemas son tratados en [12] donde se proponen mejoras en el protocolo TCP y en la capa MAC, en [13] - [14] donde estudian la verdadera efectividad del intercambio de paquetes de control ante problemas como el del nodo escondido, en [15] donde se estudia el comportamiento de TCP sobre la capa MAC de 802.11 y se propone el aumento del límite de retransmisión para mejorar su desempeño, en [16] donde basados en otros artículos, realizan un estudio detallado de los problemas de desempeño de IEEE 802.11 en redes Ad Hoc, y en [17] donde los autores exponen los problemas de capacidad de éste tipo de redes.

En los artículos antes descritos, se trabaja con redes bajo condiciones de tráfico homogéneas o al menos similares, no frente a un comportamiento de ataque. En [18] proponen el método de *Back-Pressure* que consiste en que la fuente de tráfico tenga memoria del tamaño de las colas de los nodos en la ruta hacia su destino, como mejora en el número de paquetes entregados TCP en presencia de tráficos UDP. Acerca de los ataques de denegación de servicio sobre la capa MAC en redes de múltiple salto están los siguientes trabajos: [4] en donde analizan varias topologías de ataque de denegación de servicio sobre una red de múltiple salto

explotando la capa de acceso al medio y propone un protocolo al cual llama FAIRMAC para mejorar el caudal de la red, y en [19] donde resumen vulnerabilidades del protocolo y listan una serie de soluciones basados en estas vulnerabilidades sin estudiarlas (solo las proponen), entre ellas una modificación al algoritmo de *Backoff* de 802.11 DCF, que es lo que finalmente se plantea en esta tesis como solución para fortalecer la capa de acceso al medio ante los ataques de denegación de servicio y aliviar su efecto sobre la red de múltiple salto.

Éste documento se desarrolla de la siguiente manera: en el capítulo 2, se explica brevemente el protocolo MAC IEEE 802.11 y se dan algunos antecedentes de artículos relacionados al tema, en el capítulo 3 se presentan algunos problemas que presenta la capa de acceso al medio del protocolo respecto al desempeño, en el capítulo 4 se describen los ataques de denegación de servicio basados en tráfico y el efecto que estos tienen sobre una red de múltiple salto. El capítulo 5 propone una solución para disminuir los efectos del ataque sobre la red de múltiple salto en cuanto a cantidad de paquetes entregados y caudal de la red. Finalmente el capítulo 6, plantea conclusiones encontradas a través del desarrollo de esta tesis. La herramienta usada en esta investigación es el software de simulación de redes Qualnet®[20].

2. ANTECEDENTES

La detección de anomalías y actividad de denegación de servicio (en inglés *Denial of Service, DoS*) son temas ampliamente tratados en la actualidad en especial, para el caso de Internet sobre redes tradicionales o del tipo alambrado, debido a su amplia cobertura y por tanto, al fácil acceso a los servicios ofrecidos por estas redes de un gran número de usuarios a nivel mundial [21] - [24].

Existen dos tipos de eventos que a menudo producen sobrecargas en lo sitios de la *"web"* (redes alambradas o tradicionales) hasta llegar al punto, que los servicios que estos proveen son notablemente disminuidos o totalmente interrumpidos: "*Flash Events"* y los ataques de denegación de servicio [23].

Los eventos "*flash"* o *"Flash Events"* (FE) son causados por un aumento en el número de solicitudes legítimas (aumento de tráfico) a un sito *"web"* en particular, causando un incremento dramático en la carga del servidor, lo cual resulta en un incremento considerable en la pérdida de paquetes y congestión. Estos eventos pueden ser predecibles cuando el sitio está conciente de la posibilidad de que ocurran, sin embargo hasta en éste caso, los sitios *"web"* no siempre cuentan con los recursos necesarios y suficientes para manejar el FE a tiempo [23].

Los ataques de denegación de servicio (DoS), contienen solicitudes maliciosas cuyo objetivo es evitar la operación normal de un sitio evitando que los usuarios legítimos accedan. Los DoS, son causados por el incremento en el número de clientes o debido a que un cliente particular envía un número de solicitudes a una tasa muy alta creando congestión sobre un servicio. Otros ataques DoS se deben a un número pequeño de clientes que emiten una tasa alta de solicitudes, y otros debido a un número muy grande de clientes generando una tasa de solicitud baja, pero en ambos casos las solicitudes por cliente son estables durante el ataque, con tráfico ampliamente desviado al comportamiento normal [23].

Regularmente los ataques DoS provienen desde clientes que acceden por primera vez al servicio, es decir que nunca han sido vistos en la red a la cual quieren

acceder, sin embargo ataques voluntarios o involuntarios provenientes de clientes regulares de la red no pueden ser descartados [24].

En las redes con infraestructura, se han desarrollado esquemas avanzados de encriptación de la información, así como la presencia de dispositivos especializados de seguridad, tales como *"firewalls" y "gateways"* que buscan evitar la entrada de los ataques a las redes, sin embargo es muy difícil eliminar totalmente los ataques de denegación de servicio y siempre un ataque tendrá repercusiones sobre la red [23]. En general las consecuencias de los Eventos *"Flash"* o de los ataques de Denegación del Servicio son los mismos: una disminución notable en el desempeño de la red y en el porcentaje de información (paquetes entregados) recibida, debido al alto volumen de tráfico que sobre un nodo los dos fenómenos presentan [23].

La conveniencia de las redes de acceso inalámbricas basadas en 802.11 ha llevado a que éstas tengan un amplio despliegue en los sectores industrial, militar y personal, en base a la suposición implícita de disponibilidad y confidencialidad. Sin embargo, ha sido ampliamente sugerido que 802.11 es altamente susceptible a ataques DoS contra sus protocolos de manejo y de acceso al medio, como se muestra en [5], donde por medio de una red física (*testbed*), evidencia las vulnerabilidades de una red de área local inalámbrica sobre el protocolo 802.11 ante un ataque de denegación de servicio dentro de la red.

La combinación de espectro libre, codificación eficiente de canal y *hardware* de interfase barato, han hecho bastante popular el acceso a redes basadas en 802.11. Sin embargo, éste mismo despliegue hace a las redes basadas en 802.11 un blanco atractivo para atacantes potenciales. Las amenazas de ataques DoS sobre el protocolo MAC de 802.11, son un problema latente en todas las redes especialmente en las redes inalámbricas. Sin infraestructura física, un atacante posee cierta flexibilidad para decidir donde y cuando atacar, permaneciendo en el anonimato, debido a la dificultad de localizar la fuente individual de trasmisiones inalámbricas [5]. Por éste motivo es necesario conocer el funcionamiento del protocolo y así hacer un mejor análisis de sus defectos frente a un ataque.

2.1 Protocolo MAC IEEE 802.11 [6]

El método fundamental de acceso de la MAC IEEE 802.11 es una función de coordinación distribuida (DCF) conocida como CSMA/CA (en inglés, *Carrier Sense Multiple Access with Collision Avoidance*), la cual permite que se comparta el medio automáticamente entre capas físicas compatibles y permite un tiempo aleatorio de retroceso (algoritmo de *Backoff*) seguido a la condición de que el medio esté ocupado.

La función de coordinación distribuida está basada en el intercambio de paquetes de control e información, llamado por muchos autores comunicación de 4 vías. El nodo que desea transmitir sensa el canal y verifica que los nodos dentro de su vecindad no estén transmitiendo ninguna clase de paquetes, es decir que el canal esté desocupado. Una vez el nodo comprueba esto, envía un paquete de control de solicitud de envío (RTS, *Request To Send*) al nodo con el cual desea comunicarse. El nodo destino al recibir éste paquete, inmediatamente responde con el paquete de control listo para enviar (CTS, *Clear To Send*), indicando que es posible empezar la transmisión. Éste intercambio de paquetes de control es conocido como el apretón de manos RTS/CTS (en inglés, *handshake* RTS/CTS). Posteriormente el cliente envía sus paquetes de información y una vez recibidos por el nodo destino o servidor, éste envía un acuse de recibo al cliente (*ACK*) indicando que la transmisión fue satisfactoria.

Existe un intervalo de tiempo entre *"frames"* (paquetes) llamado espacio entre paquetes (en inglés, *Interframe space*, IFS). Cuatro diferentes tipos de IFS son definidos por el estándar para proveer niveles de prioridad para acceder al medio inalámbrico, aunque para el modo DCF solo se usan 3, los cuales son especificados por la capa física:

- SIFS (*Short Interframe Space*): Es un espacio de tiempo usado entre los paquetes de la comunicación 4 vías. SIFS = 10µs.

- DIFS (*DCF Interframe Space*): Éste espacio de tiempo es usado antes de iniciar el proceso de transmisión o antes de iniciar el proceso de *backoff*. Esta ventana debe ser lo suficientemente grande para que el nodo se

cerciore del estado del canal (ocupado o desocupado). DIFS = SIFS + 2 x (*SlotTime*) = 50µs.

- EIFS (*Extended Interframe Space*): Es un espacio de tiempo usado cuando la capa física le indica a la capa MAC que una transmisión de paquetes previa no resultó en una recepción correcta del paquete. EIFS = SIFS + $\frac{ACKframesize}{basicrate}$ + DIFS, donde $ACKframesize$ es el tamaño en bits del acuse de recibo y $bascirate$ es la tasa básica de envío (1Mbps).

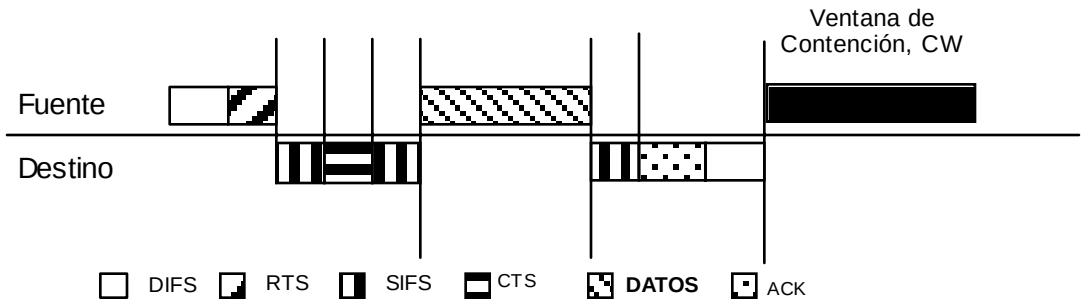

Figura 1.Proceso de comunicación entre nodos en la capa MAC.

La Figura 1 muestra la comunicación de 4 vías entre dos nodos y sus respectivos tiempos entre paquetes.

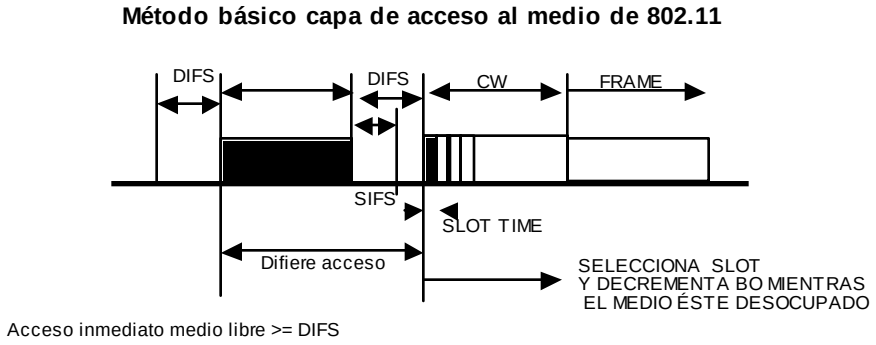

Figura 2. Método básico de acceso MAC 802.11 DCF.

El método básico de acceso de la capa MAC se muestra en la Figura 2. Si el medio está libre por un tiempo mayor o igual a una ventana DIFS, el nodo puede iniciar su transmisión, de lo contrario si el canal está ocupado el nodo difiere su acceso hasta que el canal esté desocupado, espera una DIFS, asigna la ventana de contención y entra en el proceso de retroceso mediante el algoritmo de Backoff. Una vez termina éste proceso el nodo puede enviar su paquete.

El algoritmo de *Backoff*, cuyo diagrama de flujo se muestra en la Figura 3, es llamado por cada nodo cada vez que desea transmitir, ha sensado el canal y lo ha encontrado libre por un tiempo mayor a un tiempo DIFS. También conocido como BEB (en inglés, *Binary Exponential Backoff algorithm*) funciona de la siguiente manera:

1. El nodo sensa el canal mediante la capa física y capa de acceso al medio.

2. Si el canal está libre por un tiempo mayor o igual a una ventana DIFS se le asigna al nodo el valor de la ventana de contención, si es el primer paquete a enviar se le asigna el valor mínimo *aCWmin* = 31. Si por el contrario, el canal está ocupado el tiempo de *Backoff* se detiene en el valor actual y el nodo debe esperar a que el canal se desocupe.

3. En base al valor de la ventana de contención escogido, se calcula el tiempo de *Backoff* usando la fórmula: *Backoff Time = Random() x aSlotTime*, donde: *Random()*: Entero Pseudo aleatorio sobre el intervalo [0,CW] donde $aCWmin \leq CW \leq aCWmax$. Para 802.11b *aCWmin* = 31 y *aCWmax* = 1023 y *aSlotTime*: Valor definido por la capa física, para 802.11b, *aSlotTime* = 20µs.

4. Calculado el tiempo de *Backoff* el algoritmo empieza a retroceder de 1 *time slot* hasta que el tiempo de *Backoff* sea cero, al ocurrir esto el nodo puede transmitir su paquete.

5. Si la transmisión fue exitosa, se asigna el valor mínimo de la ventana de contención al nodo, es decir 31. Si no fue exitosa el valor de la ventana de congestión se dobla y le suma 1, y reinicia el retroceso del algoritmo. Si continua sin lograrse la transmisión la ventana de contención continua

doblándose hasta alcanzar el valor máximo de ésta (*aCWmax* = 1023) y posteriormente se reinicia.

Cabe resaltar que éste proceso de retroceso sólo es llevado a cabo cuando el canal es sensado como libre. Más detalles e información acerca del protocolo 802.11 y de su capa MAC pueden encontrarse en [6] y [25].

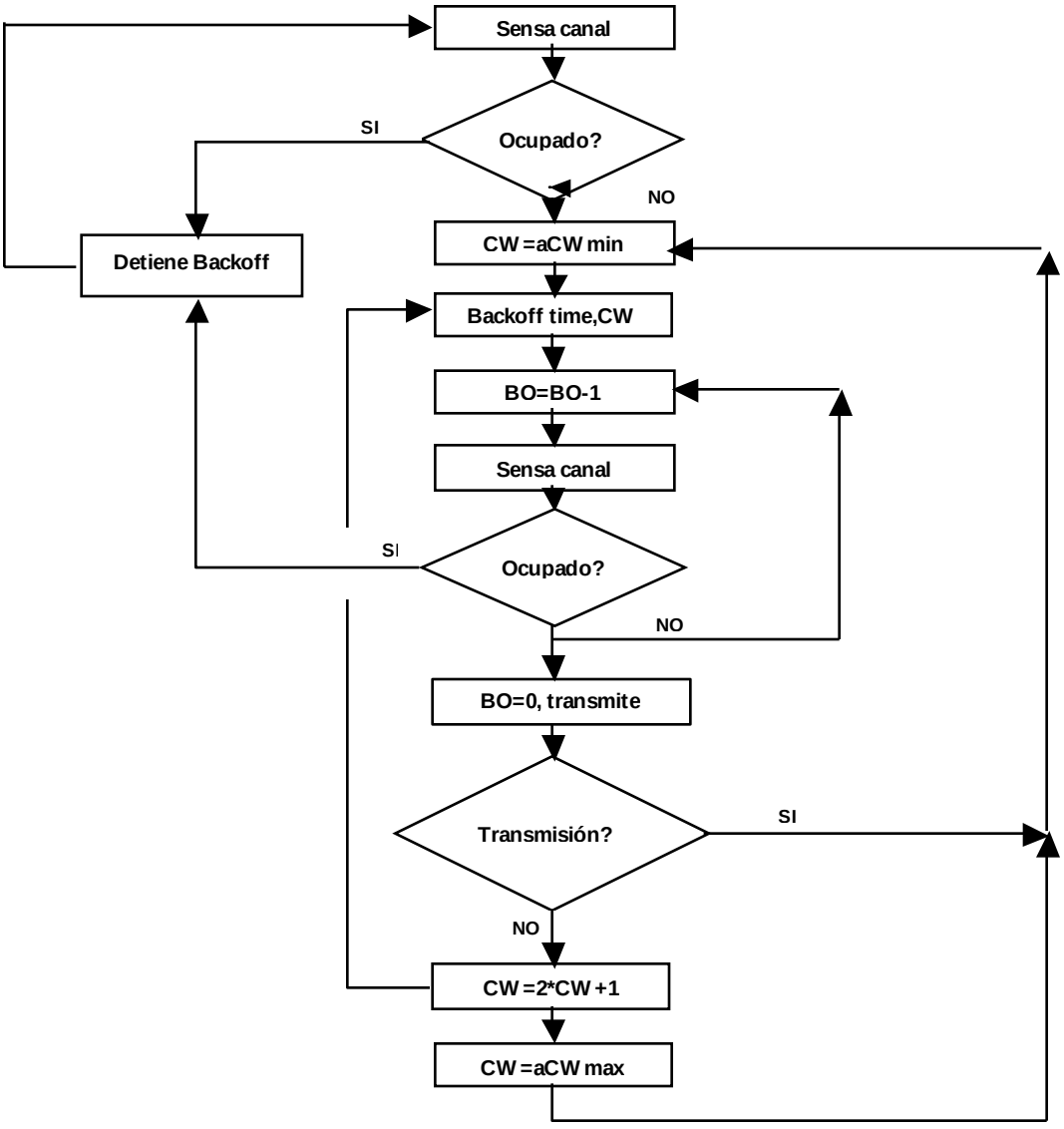

Figura 3. Algoritmo de Backoff para 802.11 DCF según [6].

2.2 Mejoras al algoritmo de Backoff del protocolo MAC 802.11 DCF

Recientemente, se ha estado estudiando la forma de mejorar el desempeño en términos de caudal del protocolo MAC 802.11 DCF en redes de 1 solo alto, redes similares a las redes de área local inalámbricas con la diferencia de que no tienen un punto de acceso a una red física. Aunque las redes Ad Hoc de 1 sólo salto son diferentes a las *WLAN*, las mejoras que se hacen a los dos tipos de redes suelen compararse entre sí. Modelos analíticos del desempeño de 802.11 en redes Ad Hoc de 1 salto son descritos en [7] y [26].

Una de las primeras mejoras propuestas sobre un algoritmo de Backoff es llamada MACAW [27] (el cual data a 1994, mientras que la primera versión del estándar 802.11 salió en 1997). Aunque esta mejora no fue propuesta sobre el protocolo MAC 802.11 en sí, es decir con el fin de mejorar el esquema CSMA/CA, sino sobre un protocolo anterior llamado MACA (de características similares) [27], sirve como base a las propuestas más recientes, que también buscan suavizar la manera como el algoritmo de *Backoff* decrementa después de una transmisión exitosa.

2.2.1 Algoritmos basados en el decremento de la Ventana de Contención

Entre los artículos que proponen una mejora al algoritmo de Backoff BEB [6] en redes de 1 salto están: el algoritmo DIDD (*Double Increment Double Decrement)* especificado en [7], el algoritmo MIMD (*Multiplicative Increase Multiplicative Decrease*) [8], y el EIED (*Exponential Increase exponential Decrease*) [9] elaborado por el Instituto Nacional de Estándares (NIST). La mejora consiste, en modificar el procedimiento en como el algoritmo BEB decrementa (selección del valor de la ventana de contención, CW) en un nodo, después de que ha logrado transmitir. La variación hecha en cada uno de los algoritmos se resume a continuación, en la Figura 4.

$$BEB:\begin{cases} CW \leftarrow \min(2\cdot CW, CW_{\max}) & \textit{incremento cuando ocurre una colisión} \\ CW \leftarrow CW_{\min} & \textit{decremento después de tranmisión} \end{cases}$$

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

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

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

Figura 4. Mejoras al algoritmo BEB

Estos algoritmos buscan suavizar el decremento del algoritmo de *Backoff*, es decir, darle más pasos entre el valor actual que tenga la ventana de contención según las veces que haya tenido que doblarse y el valor mínimo de la ventana de contención, con el fin de mejorar el caudal total en la red.

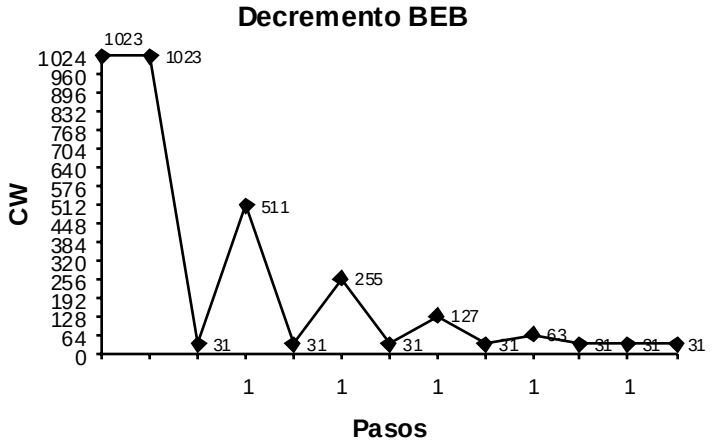

Figura 5. Método de decremento algoritmo de *Backoff* estándar después de una transmisión exitosa.

La Figura 5 muestra como el algoritmo de *Backoff* decrementa la ventana de contención después de que el nodo ha logrado transmitir, siempre hacia su valor mínimo, realizando solo un paso desde su valor actual hasta *CWmin*.

La desventaja de estos algoritmos, es que no buscan hacer más equitativo o más justo el tráfico de todos los nodos que simultáneamente usen la red. Un ejemplo de

cómo estos algoritmos decrementan la ventana de contención de un nodo, después de una transmisión exitosa se muestra en la Figura 6 para el algoritmo EIED, donde a CW se le asigna el valor de acuerdo a la ecuación de la Figura 4., lo que resulta en un mayor numero de pasos de decremento

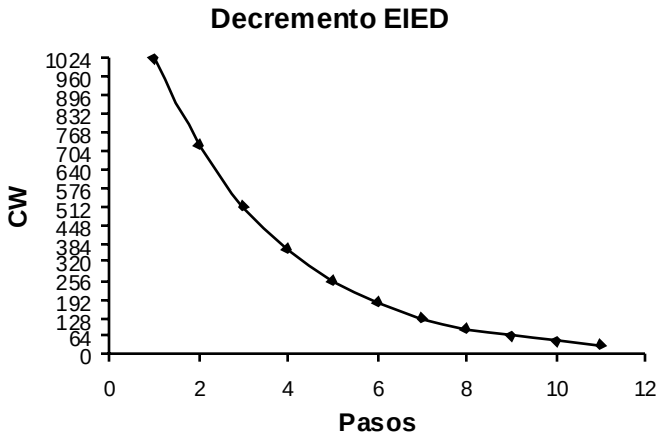

Figura 6. Decremento de algoritmo de *Backoff* EIED después de transmisión.

2.2.2 Algoritmo NBA

Optimizar la ventana de contención es otra forma de mejorar el desempeño de una red de 1 salto. Esto es tratado en [10], donde definen el algoritmo NBA (*Neighbourhood Backoff Algorithm*) basado en el número de nodos activos de la red.

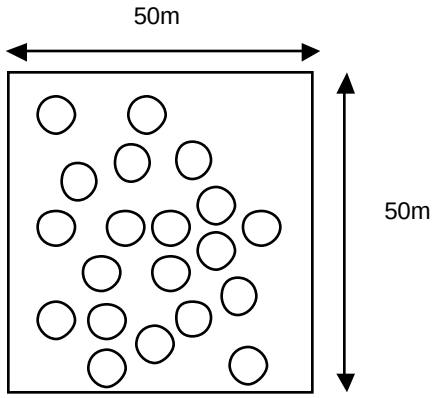

Figura 7. Escenario simulación de 20 nodos, algoritmo NBA

Por éste motivo, inicialmente se establece en Qualnet® [20], redes de 1 salto de diferente número de nodos (4, 5, 6, 11, 15, 20, 25 y 30 nodos, un ejemplo se muestra en la Figura 7), donde todos los nodos están ubicados aleatoriamente dentro del mismo rango de transmisión en un área de 50m X 50m, todos

transmitiendo simultáneamente entre ellos a tres diferentes tasas: con carga menor a la capacidad del canal (5.5Mbps), carga igual a la capacidad del canal (11Mbps) y carga superior a la capacidad del canal (16.5Mbps). En éste 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* es muy alto, se desperdicien recursos o si es muy bajo, el número de colisiones aumente. El parámetro M802_11b_CW_MIN, en el archivo mac_802_11.h de Qualnet®[20], define el límite mínimo de la ventana de contención. Normalmente a medida que el número de nodos de la red crece, el caudal total en la red va disminuyendo.

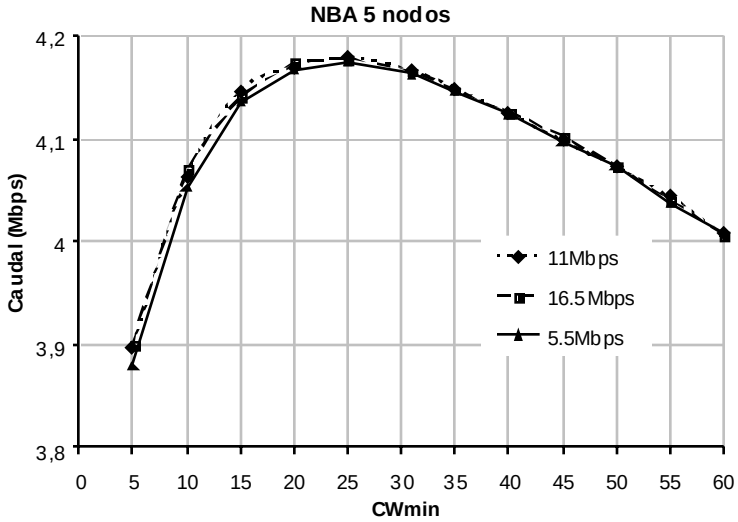

Figura 8. Optimización de la ventana de contención para red de 5 nodos, algoritmo NBA.

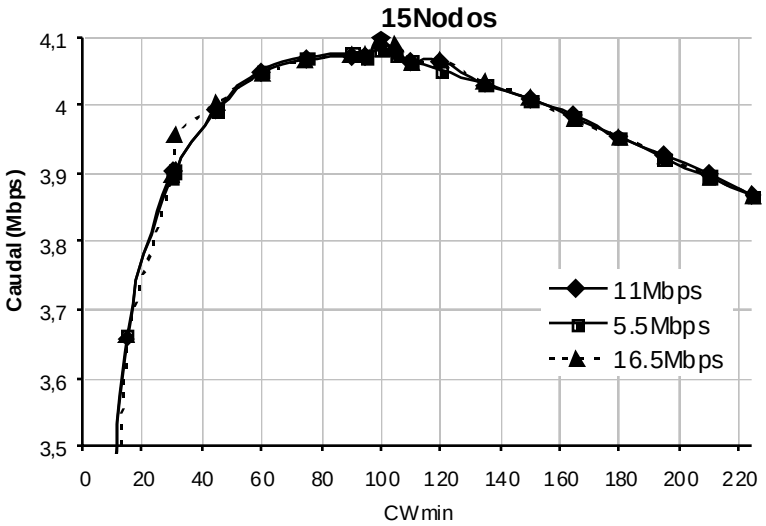

Figura 9. Optimización de la ventana de contención para red de 15 nodos, algoritmo NBA

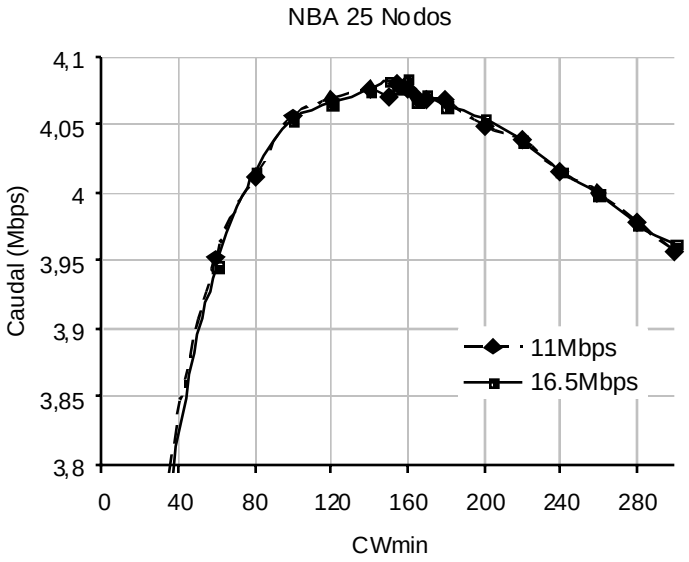

Figura 10. Optimización de la ventana de contención para red de 25 nodos, algoritmo NBA.

Tomando los valores de *CWmin* que optimizan el caudal es decir, donde mejora el desempeño de cada una de las redes, por ejemplo para una red de 5 nodos *CWmin* = 25 como lo muestra la Figura 8, para la red de 15 nodos *CWmin* = 100 como se muestra en la Figura 9 y para una red de 25 nodos *CWmin* =155 como en la Figura 10 (a diferencia del estándar MAC 802.11 DCF, donde *CWmin* = 31 para cualquier tamaño de red). Aproximando estos valores a una relación lineal, se encuentra que el valor óptimo del límite mínimo de la ventana de contención, *CWmin* = 6N – 4 (Figura 11), siendo N el número de nodos en la red.

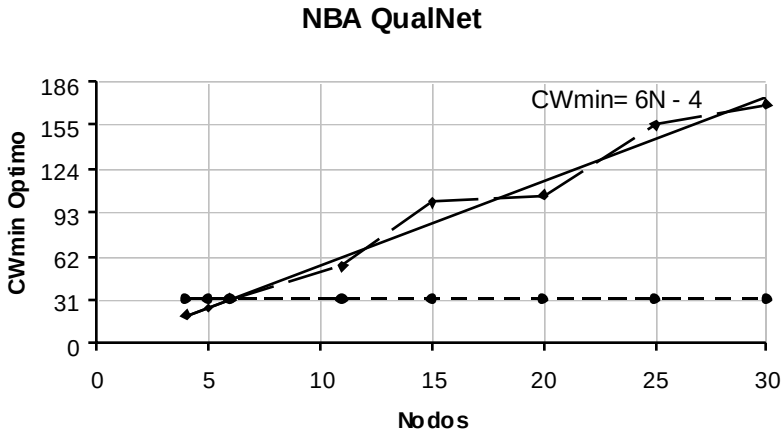

Figura 11. Relación entre el número de nodos y el límite mínimo de la ventana de contención.

En el artículo original [10], encuentran que el valor óptimo de *CWmin* = 8.5N – 5, sin embargo éste fue originado usando el software de simulación *OPNET Modeller* [28].

Probando con diferentes topologías aleatorias de red (12 semillas para un nivel de confianza del 95% con una variación del 1% con respecto al valor medio del caudal), se comprueba una tendencia clara al optimizar *CWmin*, en el aumento del caudal, a medida que la red es más grande. En la 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 [10], mientras que usando el estándar original a medida que aumenta el número de nodos el caudal cae notablemente (Figura 12).

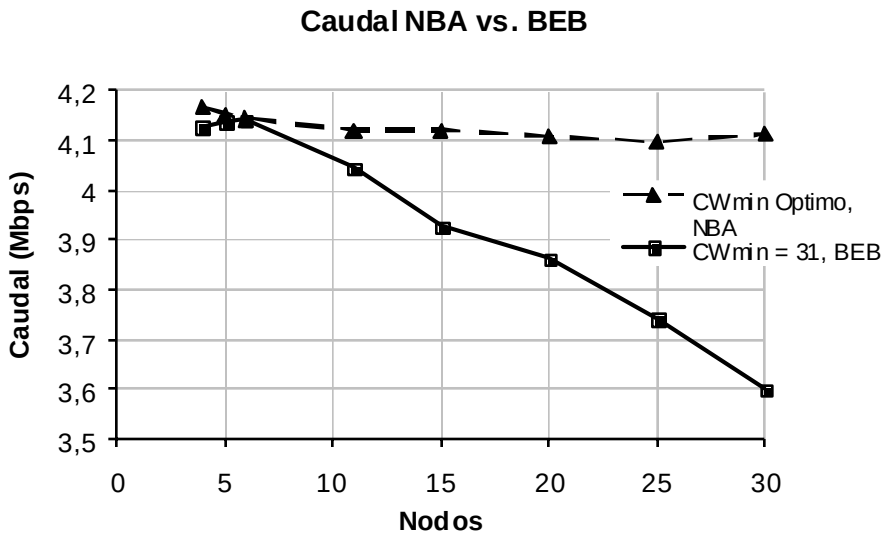

Figura 12. Mejora del desempeño con el algoritmo NBA.

Existen otros trabajos como [11], donde para redes de área local inalámbricas encuentran que la relación entre el número de nodos y el límite mínimo de la ventana de contención, para mejorar el desempeño de la red es CWmin = 5.1N, algoritmo al cual llaman LMILD.

Implementando en Qualnet®[20] los algoritmos de mejora de desempeño de redes de 1 salto y comparándolos en las mismas topologías de red usadas para el algoritmo NBA[10], encontramos que el que muestra mejor desempeño en cuanto aumento del caudal total es el algoritmo NBA [10], en las diferentes topologías de

red de diferente número de nodos. Como se muestra en las Figuras 13 y 14, tanto MIMD, EIED como NBA, muestran una mejoría sobre el algoritmo BEB y el algoritmo NBA presenta el mejor desempeño.

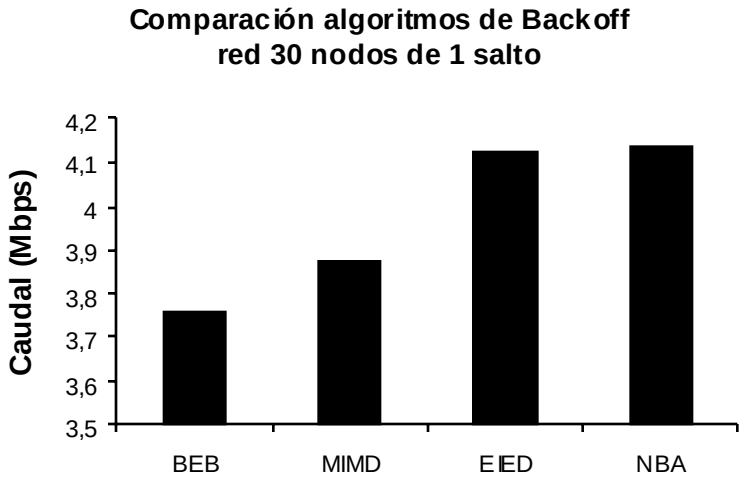

Figura 13. Comparación en red de 30 nodos de 1 salto de varios algoritmos de *Backoff*.

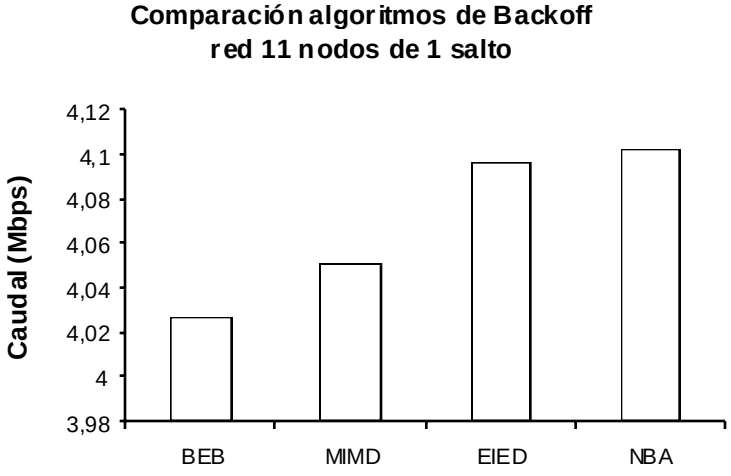

Figura 14. Comparación en red de 11 nodos de 1 salto de varios algoritmos de *Backoff*.

3. LA CAPA MAC 802.11 EN MÚLTIPLE SALTO

Las redes Ad Hoc son construidas usando el protocolo MAC 802.11b DCF. Vulnerabilidades aparecen pues éste protocolo, MAC 802.11, no trabaja bien en redes Ad Hoc bajo condiciones de transmisión en múltiples saltos, debido a que originalmente fue diseñado para trabajar en redes inalámbricas de área local o de un sólo salto y entonces los parámetros y características especificados en el estándar [6] no son los mejores para una red Ad Hoc.

Trabajos como [5] y [12] concluyen que la versión actual del protocolo de redes de área local inalámbricas no funciona bien en redes de múltiple salto, sobre todo en las capas de transporte, física y de acceso al medio donde se presentan problemas de inequidad o desigualdad en el envío de paquetes por interferencia entre nodos e inestabilidad del tráfico TCP. Para esto proponen medidas tales como disminuir la ventana de congestión *(snd_cwnd*) de TCP y ajustar el tamaño del paquete enviado.

3.1 Problemas relevantes de la capa MAC

Específicamente, cuando es usado en una red de múltiple salto, debido a su diseño, el actual protocolo MAC IEEE 802.11 presenta los siguientes problemas.

3.1.1 Rango de interferencia

El rango de transmisión de un nodo dentro de una red Ad Hoc, debe cubrir la distancia de separación entre los nodos. Éste rango de transmisión genera un rango de interferencia, el cual hace que los nodos dentro de éste rango, no puedan transmitir al mismo tiempo, pues interfieren con la posible transmisión de otros nodos dentro del mismo rango, los cuales deben diferir su transmisión por un tiempo aleatorio (algoritmo de *Backoff*). En [13] y [14] se calcula analíticamente el rango de interferencia usando otro modelo de recepción de paquetes en la capa física, según la fórmula $I_R = 1.78 \cdot d_{TR}$ donde I_R es el rango de interferencia y d_{TR} es la distancia entre los nodos de transmisión y recepción, sin embargo éste rango de interferencia es muy difícil calcularlo, ya que no es un valor fijo y depende de factores tales como

la potencia de transmisión, sensibilidad de recepción, altura de la antena, separación entre los nodos, etc.. Qualnet®, no especifica como toma éste rango de interferencia, sin embargo por experimentos posteriores plasmados en éste capítulo, se puede intuir que es superior a dos veces el rango de transmisión configurado.

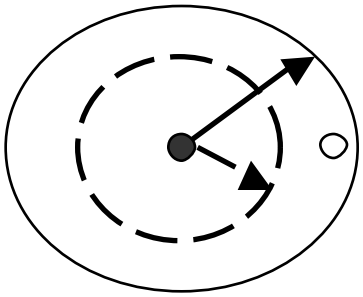

Figura 15. Rango de interferencia.

En la Figura 15, la flecha y el círculo en líneas representan el rango de transmisión del nodo, mientras que la flecha y círculo continuos representan el rango de interferencia. La sección entre el rango de interferencia, menos el rango de transmisión es conocida como Área de Interferencia ($AI = ¶ * r_{continuo}^2 - ¶ * r_{lineas}^2$).

3.1.2 Nodo escondido

El problema del nodo escondido todavía existe en las redes de múltiple salto a pesar de que el estándar ha puesto mucha atención a éste problema. Éste se presenta cuando un nodo está en el rango de transmisión de dos de sus nodos vecinos y estos desean iniciar una transmisión hacia éste al mismo tiempo. En éste caso, los nodos vecinos están escondidos entre sí, ya que están fuera de su rango de transmisión, pero dentro de su rango de interferencia tal y como se muestra en la Figura 16, de ahí el nombre de problema del nodo escondido [29].

Aunque el *handshake* RTS/CTS fue diseñado para evitar éste problema en redes *WLAN* (en opinión del autor de éste documento, tal vez innecesario ya que todos los nodos están a 1 solo salto del punto de acceso y en el mismo rango de transmisión lo que les permite sentir las transmisiones de los otros), en redes de múltiple salto se intensifica el problema, ya que al no estar los nodos que pretenden transmitir en el rango de transferencia del otro, no pueden sentir la presencia de paquetes y de paquetes de control, lo que los lleva a transmisión y a causar colisiones [29]. De

manera más sencilla éste problema ocurre cuando un nodo cree que el medio está libre cuando en realidad no lo está, pues está siendo utilizado por otro nodo al cual no oye.

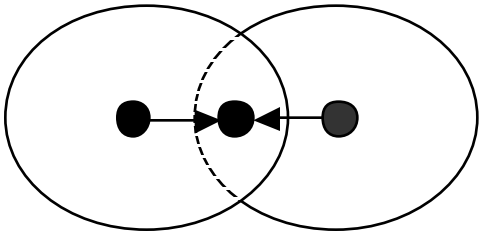

Figura 16. Problema del nodo escondido [29].

3.1.3 Nodo expuesto

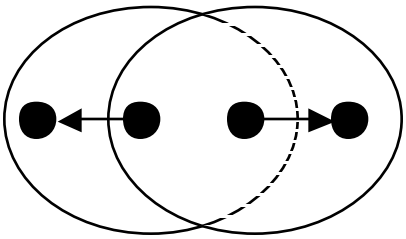

Figura 17. Problema del nodo expuesto [29].

No existe algún esquema en el estándar para tratar el problema del nodo expuesto, el cual es aún más dañoso en redes de múltiple salto [29]. Éste problema ocurre como en la Figura 17, cuando dos nodos que quieren transmitir a sus respectivos vecinos, están en el rango de transmisión entre sí, lo que impide que estos dos nodos transmitan simultáneamente, ya que al sensar su vecindad, el medio siempre va a parecerles ocupado. Es decir, cuando un nodo recibe señal que su vecino está transmitiendo éste retrocede con el fin de evitar una colisión, pero en realidad el medio esta desocupado [29]. Éste problema ocurre cuando un nodo cree que el medio está ocupado, cuando en realidad el nodo que supuestamente ocupa el medio no interfiere en su transmisión a otro destino.

3.1.4 Descenso del caudal

La disminución en el desempeño de la red (Caudal) a medida que aumenta el número de saltos, es otro problema que presenta el protocolo MAC 802.11 DCF sobre las redes Ad Hoc.

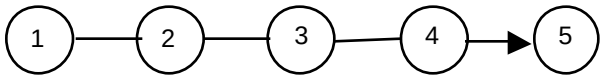

Figura 18.Topología de nodos en cadena.

Si se tiene una cadena de nodos como la indicada en la Figura 18, donde los paquetes se originan en el primer nodo y son reenviados hasta el último nodo, separados cada 350m con un rango de transmisión de 376m, emulando los múltiples saltos de una red Ad Hoc, 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 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. El amplio rango de interferencia hace que sólo cada 5 nodos puede haber transmisiones simultáneas, lo que lleva a una caída notable en el desempeño de la red. En éste caso se esperaría que la caída del caudal sea 1/4 [17], sin embargo ésta es todavía mucho más dramática como se muestra en la Figura 19 para un tráfico CBR (el máximo caudal se alcanza en una sesión CBR con el tamaño máximo posible del paquete, 2020bytes) de distintos tamaño de paquetes y en la Figura 20, para tráfico FTP.

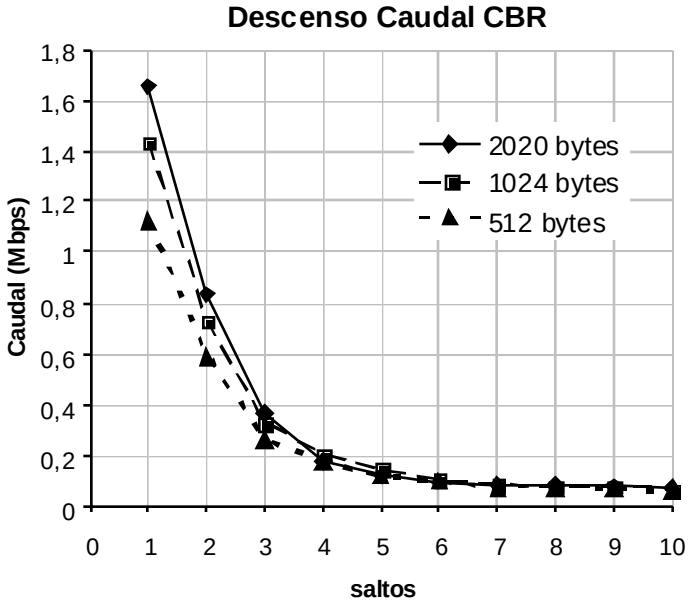

Figura 19. Descenso del caudal en red de múltiples saltos sesión CBR con tasa de envío 2Mbps.

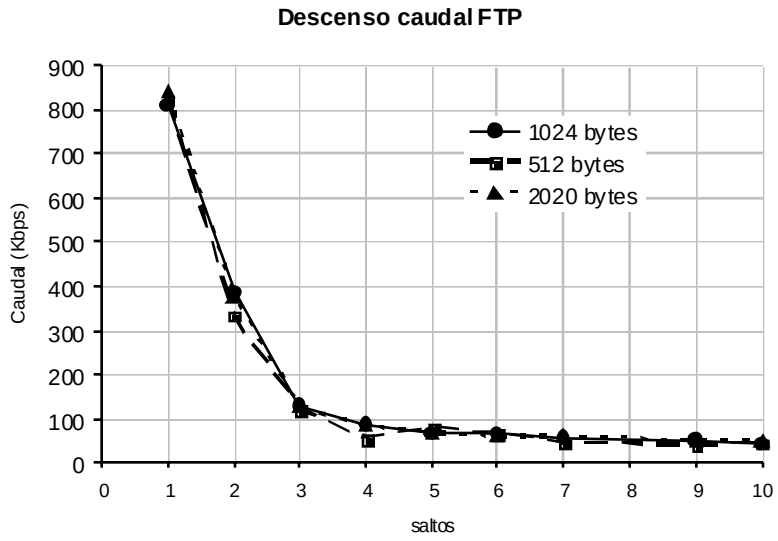

Figura 20. Descenso del caudal en red de múltiples saltos sesión FTP al enviar 1000 paquetes a 1Mbps.

Por éste motivo el caudal en las redes de menor tamaño es mucho mayor que en las redes con mayor número de saltos para cada uno de sus sesiones de tráfico.

3.2 Comportamiento injusto e inequitativo

La combinación de los problemas descritos en el numeral 3.1, lleva a un comportamiento injusto e inequitativo. A medida que dos nodos vecinos se acercan o se alejan, hace que a ciertas distancias, el tráfico sea suprimido en su totalidad, es decir cuando existe una segunda transmisión bloqueando la transmisión inicial. Sin embargo, esto no quiere decir que una suceda primero que la otra, son simultáneas.

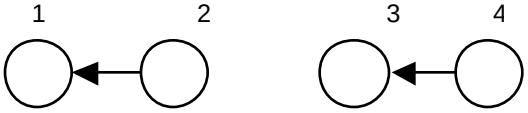

Figura 21 Topología que muéstrale comportamiento inequitativo en redes de múltiple salto.

A medida que se cambia la distancia entre los nodos 2 y 3 en la Figura 21, 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 21, sino en las otras tres combinaciones posibles de sentido del tráfico entre cada par de nodos [19]. 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. Para éste caso el rango de transmisión entre los nodos 1 y 2 es de 75m y entre 3 y 4 es de 150m.

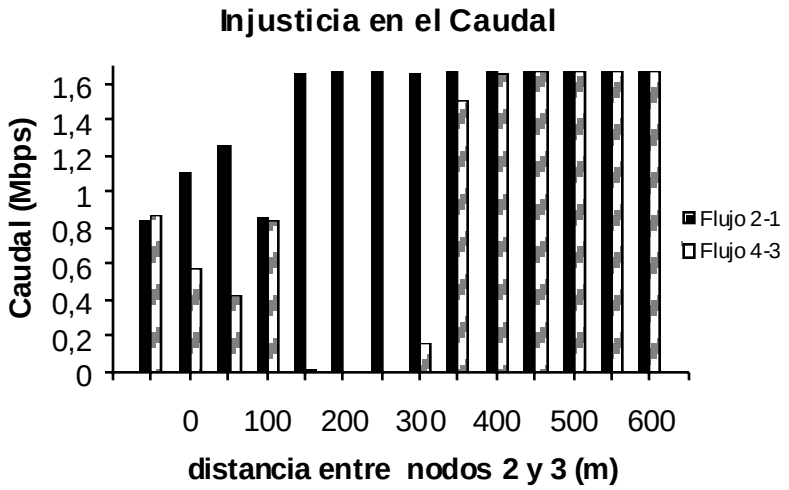

Figura 22. Injusticia en el caudal de dos tráficos con la misma dirección.

Como se ve en la Figura 22, el flujo del nodo 2 al nodo 1 suprime el otro flujo totalmente cuando dos y tres están separados entre 150m y 300m, lugares críticos de interferencia. En las siguientes Figuras (23-25) se observa la injusticia cuando pares de nodos con la misma separación de la Figura 21, tienen otras direcciones de tráfico o de flujo entre sí.

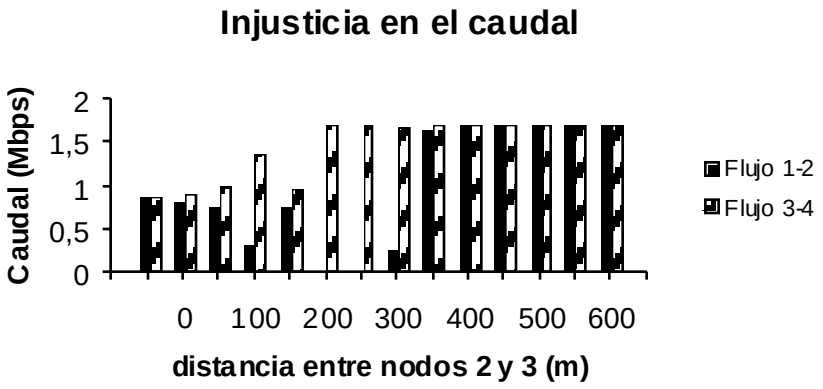

Figura 23. Injusticia en el caudal de dos tráficos con la misma dirección.

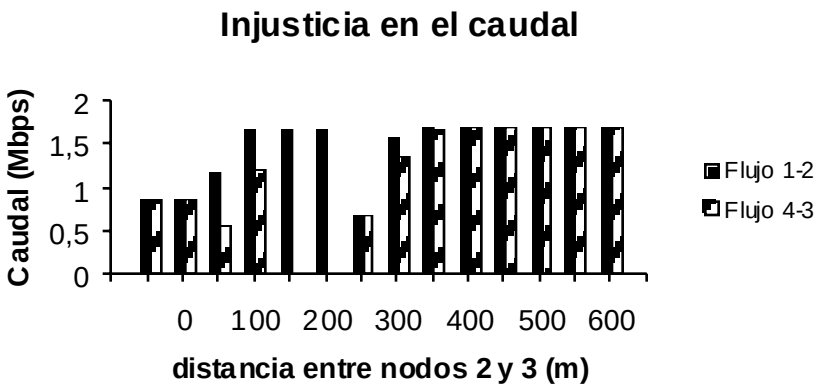

Figura 24. Injusticia en el caudal de dos tráficos con diferente dirección.

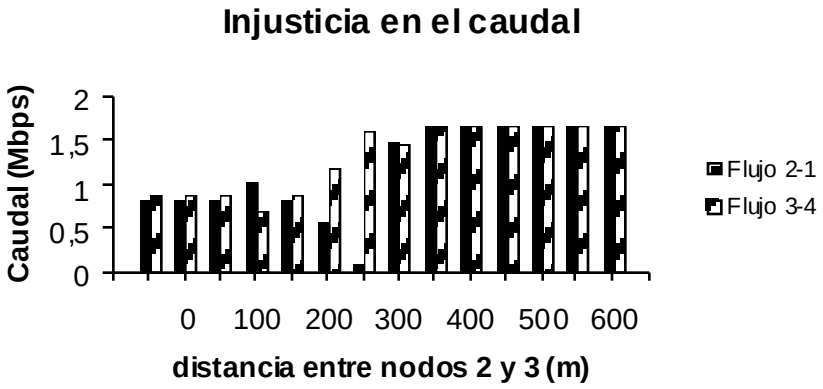

Figura 25. Injusticia en el caudal de dos tráficos con diferente dirección.

4. DENEGACIÓN DE SERVICIO EN LA CAPA MAC

4.1 Efecto Captura

Los problemas anteriormente planteados llevan a que las redes Ad Hoc, más específicamente la capa MAC de IEEE 802.11 presente vulnerabilidades ante la presencia de tráficos heterogéneos. Estos inconvenientes llevan a un problema más grave llamado: *Efecto captura* [4] y [18], el cual 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 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 la 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 (incluso por encima del hecho de que se inicie después) que llevan a que el efecto captura se produzca son [12]:

1. El número de saltos, es decir entre menor número de saltos tenga una transmisión mayor es la posibilidad de suprimir el tráfico ganando el acceso al medio.

2. El segundo es 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 en una red de múltiple salto, más específicamente en la capa MAC, se puedan presentar y sean muy fácil de lanzar y lograr.

Cuando un nodo lanza una transmisión a una tasa muy alta es decir, ataca otro nodo (sea éste cómplice o no), en la vecindad (entre más cerca más fuerte) de un tercero, el tráfico que envía o recibe éste tercero 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 26 y sus efectos se ven en las Figuras 28 y 29.

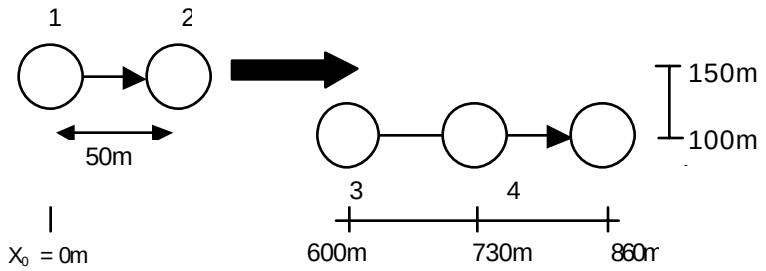

Figura 26. Ataque de denegación de servicio sobre cadena de dos saltos.

En la Figura 26., 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. Las dimensiones de escenario de simulación son 1700 m de largo por 200m de altura. El flujo del nodo 1 a 2 es del total del ancho de banda del canal, 2Mbps, con paquetes de 2020 bytes de tipo CBR y la tasa de envío del nodo 3 hacia el nodo 5 es también 2Mbps, con el mismo tamaño y tipo de paquetes que envía el nodo 1. La potencia de transmisión establecida es 4.092 dBm. Las posiciones de los nodos son las siguientes: inicialmente el nodo 1 (X_0, 150m) y nodo 2 (X_0 + 50m, 150m), nodo 3 (600m, 100m), nodo 4 (730m, 100m) y nodo 5 (860m, 100m). 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 27) permanezca en el área de interferencia del tráfico normal (flecha negra delgada, Figura 27) suprime totalmente el tráfico de 3 a 5, similar a lo que indica de la Figura 26.

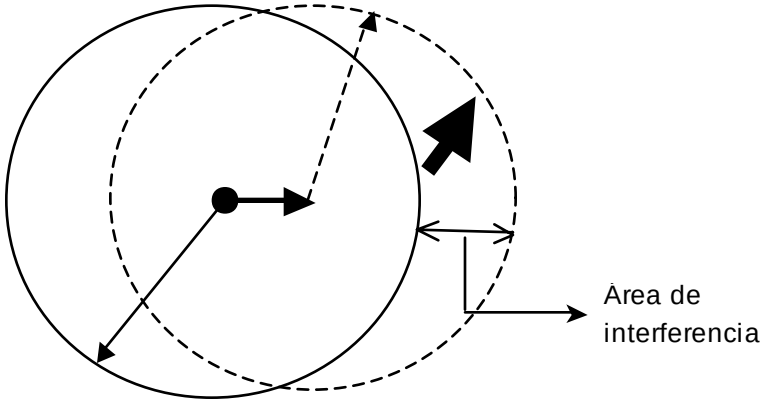

Figura 27. Área de interferencia, zona de ataque.

El ataque tiene efecto y suprime totalmente caudal 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 (aprox. entre 900 y 1300m) como se muestra en la Figura 28 y en la Figura 29 normalizando el caudal.

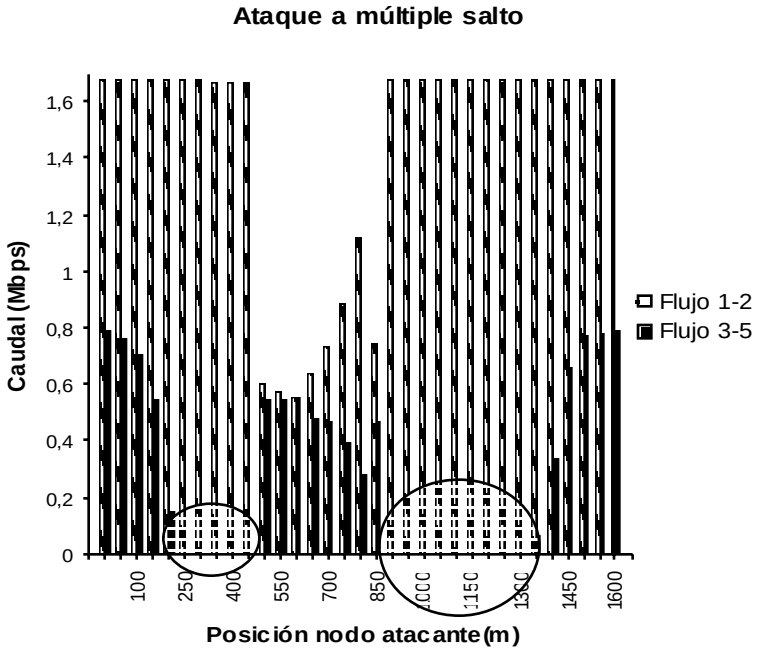

Figura 28. Caída del caudal ante denegación de servicio sobre cadena de dos saltos.

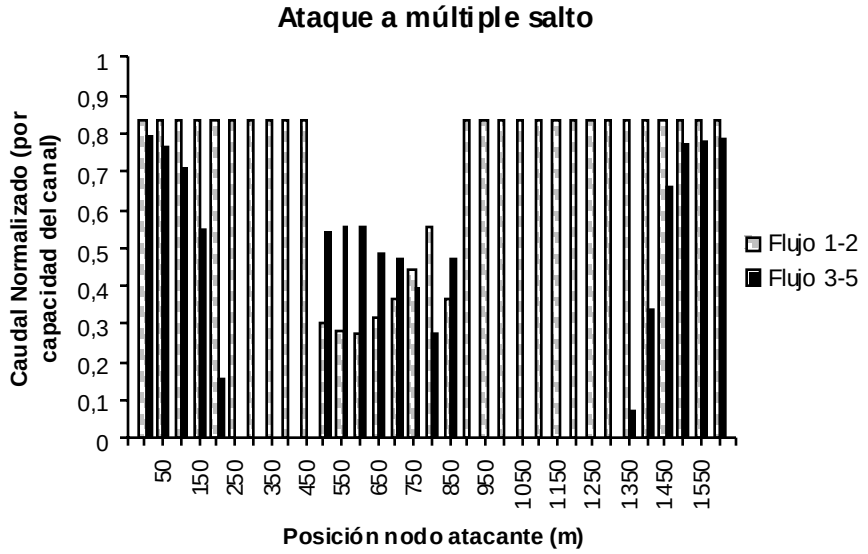

Figura 29. Caída del caudal normalizado por el número de saltos ante DoS sobre cadena de dos saltos.

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 forma de malla como el escenario usado en [4], de diferente número de nodos (25, 36, 49, 64, 81, 100, 121, 144 y 169). El área de simulación varía de acuerdo al número de nodos de la red (ej. para 13 X 13 = 169 nodos, 13 X 350m = 4550m). El escenario fue escogido debido a su simplicidad y efectividad en mostrar el impacto de la inequidad e injusticia de la capa MAC sobre TCP debido al ataque [4].

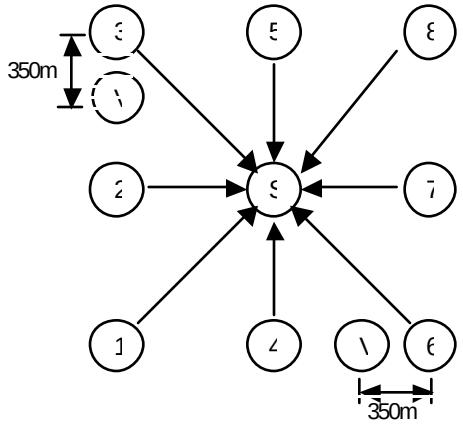

Figura 30. Escenario de simulación.

Cada nodo está separado de los otros 350m y se ajustó la potencia de transmisión a 16.78 dBm, para que el rango de transmisión cubra esta distancia hasta 376m, 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 30) son enviados 1000 paquetes de 512 bytes de tipo TCP en 8 diferentes sesiones hacia el nodo central de la red (nodo S, Figura 30) durante 900s de simulación (1000 X 512 X 8 = 4096000 bytes), los cuales representan el tráfico normal de la red. La aplicación usada para el tráfico normal es FTP/GENERIC, la cual permite configurar el tiempo de la sesión de trafico, el tamaño del paquete y el número total de paquetes a enviar pero, el tiempo en el cual se envía cada paquete es definido aleatoriamente por Qualnet® (luego las tasas de envío varían desde aprox. 8kbps hasta 30kbps). El ataque es simulado por una sesión de tráfico CBR a una tasa muy alta (la escogida fue 2Mbps). 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 y que trae el software de simulación usado, Qualnet ® por defecto.

La topología de simulación fue escogida de tal manera de que los nodos siempre estuviesen en el rango de transmisión de sus vecinos con el fin de que se respetara la condición de múltiple salto. Los nodos son estáticos ya que de esta manera la distancia de transmisión es constante y así, es posible estudiar el rango de transmisión y por tanto de interferencia, característica importante para la presencia

de un ataque por congestión dentro de la red, descartándose pérdida de paquetes por rompimiento del enlace [4]. Adicionalmente, el ataque sobre un nodo estático es peor que sobre un nodo en movimiento, ya que éste puede mantenerse por todo el tiempo deseado, y era necesario estudiar los ataques sobre la red en condiciones extremas.

Los tráficos FTP van desde su nodo cliente hasta el nodo servidor ubicado en el centro de la red buscando una mejor observación de las vulnerabilidades de la capa MAC ante el ataque de denegación de servicio: disminución del caudal a mayor número de saltos, inequidad o injusticia, interferencia en las transmisiones y efecto captura, sobre un escenario sencillo.

Dejando un tiempo en el que un ataque es efectivo sobre la red, 900s de simulación, en la red de mayor número de nodos usada, se varió cada 100 el número de paquetes enviados desde 100 a 3000. Se encontró que en éste tiempo de simulación hasta 1600 paquetes, eran entregados por cada una de las sesiones al nodo servidor en la red sin ataque, pues era necesario que la relación de entrega de paquetes fuera 1, para verificar la pérdida de paquetes por el ataque. Se decidió el envío de 1000 paquetes ya que con éste, la red alcanzó el mayor caudal y así podrían observarse los efectos del ataque sobre esta medida con mayor facilidad.

La relación de paquetes entregados esta definido por la ecuación: $RPE = \frac{\text{Total paquetes recibidos}}{\text{Total paquetes enviados}}, [0-1]$ y el caudal en el nodo servidor se define mediante: $Caudal = \frac{\text{Total de bits recibidos}}{\text{Fin Sesión - Inicio Sesión}}, [bps]$.

La sesión de ataque tiene el mismo tiempo de duración y es simultánea a las 8 sesiones de tráfico FTP enviadas desde los clientes. Si el ataque cesa, el tráfico normal continúa y el desempeño de la red mejora si se deja por un mayor tiempo.

La tasa de ataque usada en todos los casos fue de 2Mbps es decir, el total del ancho de banda del canal, sin embargo desde tasas de ataque cercanas a 1Mbps se obtienen resultados similares.

El protocolo de enrutamiento usado fue AODV. Inicialmente se usó el protocolo de enrutamiento DSR, otro protocolo de enrutamiento muy común en redes de múltiple salto. Sin embargo, éste no funciona bien en redes de un tamaño considerable (en redes de más de 81 nodos para la tesis) ya que el tamaño de cada paquete enviado aumenta debido al crecimiento del encabezado del paquete a causa del protocolo enrutamiento, donde va guardando el tamaño de la ruta actual (a mayor número de nodos y de saltos mayor tamaño de la ruta), lo que lleva a que sobrepase el tamaño máximo de paquete permitido por el estándar. AODV, enruta sin ningún problema sobre todos los tamaños de red usados.

Tres topologías de ataque fueron lanzadas siguiendo el escenario de simulación anteriormente descrito, basadas en las descritas en [4]: ataque a un salto del servidor o en la vecindad del nodo receptor, ataque a un salto del cliente o en la vecindad del nodo fuente y ataque de múltiple salto, sin embargo aunque las tres fueron estudiadas y se hacen comentarios acerca de las otras, ésta tesis está enfocada y plantea la posible solución en la primera topología de ataque, ya que es la que trae mayores problemas a la red de múltiples saltos como se mencionó previamente. Las simulaciones de los ataques y de la solución fueron hechas con 10 semillas y un intervalo de confianza del 95% [30].

4.3 Ataque a un salto del servidor

El objetivo de éste experimento en mostrar que un servicio es vulnerable ante un ataque lanzado por cualquiera de sus vecinos [4]. Para esto se lanzó una sesión CBR a la tasa máxima del canal es decir 2Mbps, desde un nodo a un salto del nodo del servidor hacia uno de sus vecinos, Figura 31, en cada una de las redes de diferente número de nodos según el escenario de simulación descrito en el numeral 4.2 y la Figura 30. Un ejemplo del archivo de configuración usado en Qualnet® (.config) para el escenario de 169 nodos y las sesiones de tráfico (.app) utilizadas en éste escenario, se muestran en el Anexo.

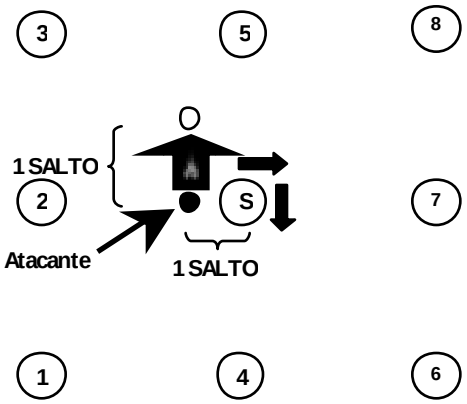

Figura 31. Ejemplo de ataques a un salto del servidor.

Cabe resaltar que si el ataque se mueve a otros nodos en la vecindad a un salto del servidor (dos ejemplos se muestran con las flechas negras más delgadas de la Figura 31), el efecto que tiene sobre los demás tráficos de la red es similar. Sin embargo los resultados son los correspondientes al ataque como lo muestra la flecha negra gruesa de la Figura 31. A medida que la tasa de ataque aumenta la disminución del tráfico normal o TCP de la red es mayor sin importar el tamaño del paquete enviado tal y como se muestra para algunos tamaños de red en la Figura 32.

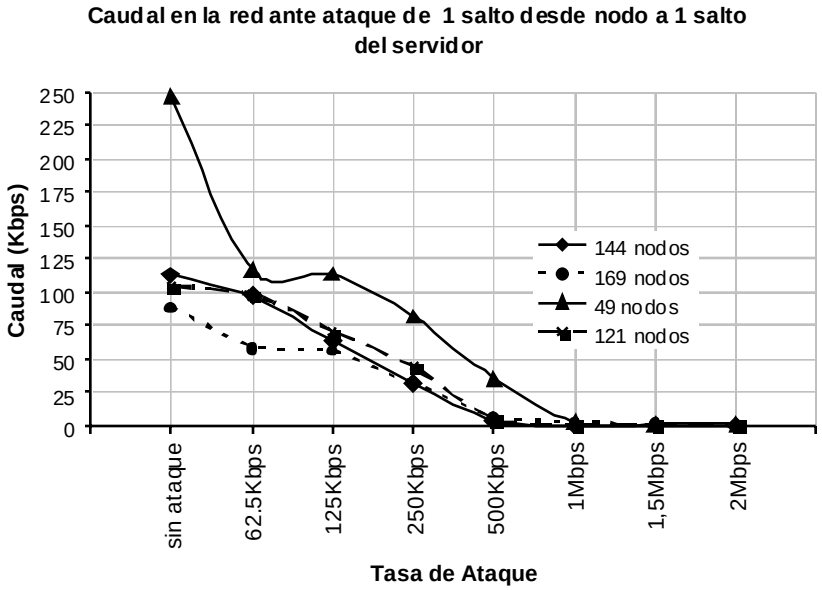

Figura 32. Caudal total en varias redes vs. Tasa de ataque.

Como lo indica la tabla 1, el descenso en el caudal recibido por el servidor en el tiempo de simulación establecido, es dramático y lleva 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.

Total de nodos	Con ataque (2Mbps)	Sin ataque	Porcentaje
25	5529	663091	0,83
36	1234	387414	0,31
49	1709	246492	0,69
64	1193	210797	0,56
81	440	147954	0,29
100	941	106803	0,88
121	467	104491	0,44
144	573	112738	0,50
169	239	88476	0,27

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

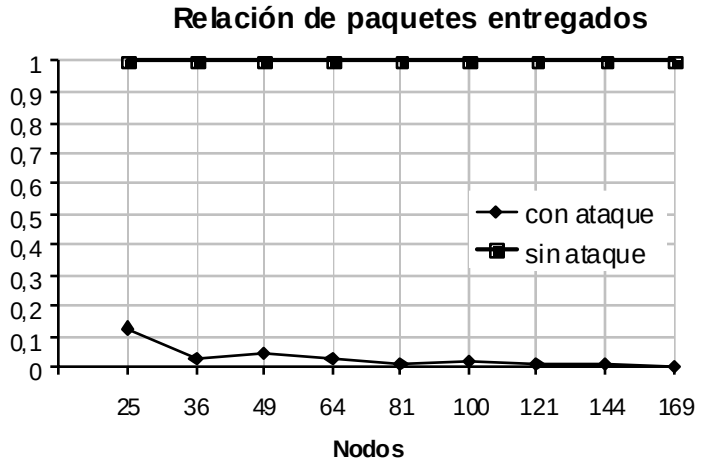

Figura 33. Relación de entrega de paquetes red sin ataque vs. red con ataque.

Al realizar el ataque a la tasa de 2Mbps, muchos de los paquetes se pierden como lo muestra la Figura 33, 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 de control enviados (RTS/CTS) en las redes con ataque en general es mayor, que en la red sin ataque, como lo muestra la Figura 34, buscando lograr

establecer la comunicación o el acceso el medio, sin éxito por la presencia del ataque. Sin embargo, cuando existe un ataque, la mayoría de paquetes de control RTS son enviados por el nodo atacante y la mayoría de los paquetes CTS son enviados por el nodo que recibe el ataque (mas del 90%).

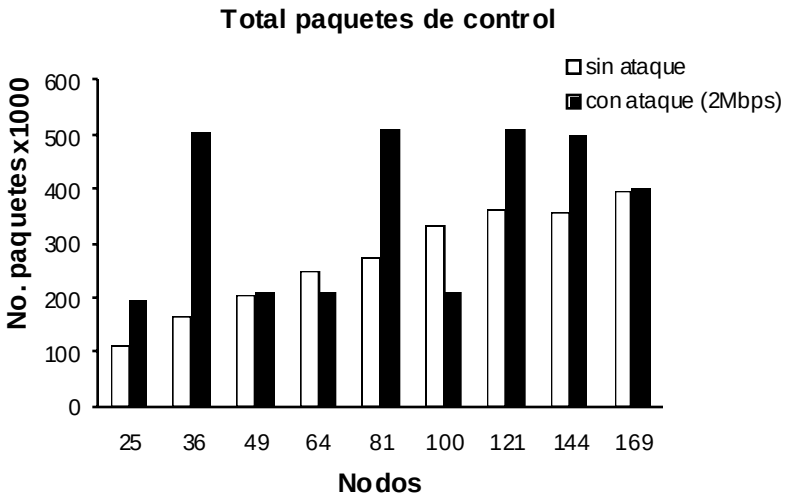

Figura 34. Número de paquetes de control red sin ataque vs. red con ataque.

El ataque lleva al 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 y al estar en el área de interferencia de los tráficos que tratan de llegar desde sus fuentes, los demás nodos retroceden entrando 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 Figura 35 muestra éste escenario, donde el círculo negro representa el nodo atacante, la flecha la dirección del ataque y el círculo vacío el receptor del tráfico de ataque. Para el caso de la Figura 35 el ataque es hecho sobre el nodo 3.

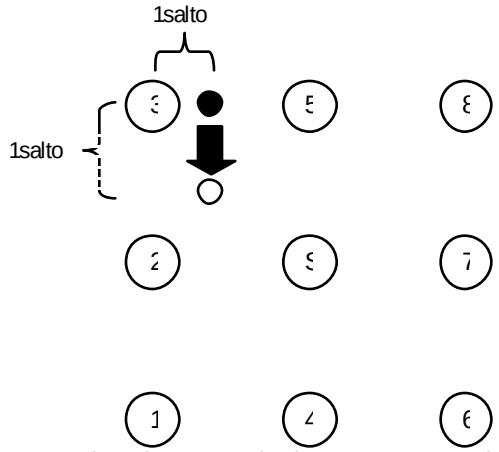

Figura 35. Ejemplo escenario de ataque a un salto del cliente.

La disminución en el caudal y en 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 [4] y se da únicamente para el nodo que esta haciendo atacado, ya que el ataque busca estar en la zona de interferencia de la fuente escogida y no afecta radicalmente el normal funcionamiento de los demás tráficos. Si las fuentes de tráfico y sus trayectorias están suficientemente separados el ataque no debe afectar el normal desempeño de la red, ya que están ubicadas fuera del rango de transmisión y de interferencia del ataque, por éste motivo en las redes más pequeñas donde los clientes están separadas por menos saltos, éste ataque podría disminuir el caudal de fuentes cercanas, sin embargo como el nodo servidor también esta a menos saltos la disminución en el caudal no es tan grave y la relación de entrega de paquetes permanece alta.

Un ataque de múltiple salto es muy 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 los otros nodos que están en la trayectoria del tráfico como enrutadores [4]. 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 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 lleva a una congestión localizada si la red es suficientemente grande ya que si la red es pequeña, la partición podría ser posible.

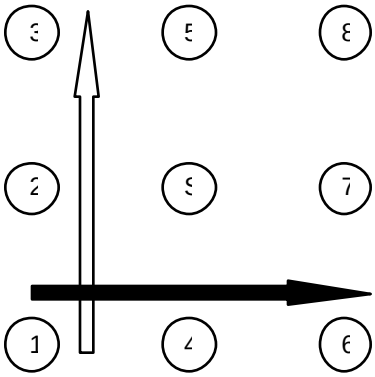

Figura 36. Ataques de múltiple salto, partición de la red.

La Figura 36 muestra con las flechas dos casos posibles de cómo se el atacante podría buscar partir la red. El escenario de simulación tiene las mismas condiciones físicas y de tráfico del numeral 4.2 y la Figura 30, más el ataque. Por ejemplo, lanzando un ataque desde un vecino de 1 hasta un vecino de 3, a una tasa de 2Mbps, buscando partir la red y suprimir los servicios de los nodos 1, 2 y 3, se obtienen los resultados de la tabla 2.

	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

Tabla 2. Resultados ataque de múltiple salto, dirección vertical.

La Tabla 2 muestra que aunque si hay un descenso en el caudal de los 3 clientes ubicados en la partición (1, 2 y 3), los peores resultados se obtienen para el nodo 1, ya que el nodo atacante está en su vecindad y la red se comporta como si el ataque estuviese a un salto del cliente, reduciendo notablemente su caudal a cerca del 2% y el número de paquetes entregados en los 900s de simulación, al 3%. El nodo 2 alcanza a entregar todos sus paquetes pero su caudal se ve disminuido a cerca del 30%. El nodo 3 también logra entregar todos los paquetes al servidor, luego su relación de entrega de paquetes es 1 y su caudal diminuye a cerca del 45%. Los efectos sobre el nodo 3 son menores ya que está más alejado de la fuente del ataque y por lo tanto la intensidad de su tráfico ha disminuido por el mayor número de saltos.

	Con ataque		**Sin ataque**	
cliente	Caudal (bps)	kbytes entregados	Caudal (bps)	kbytes entregados
1	1244	134	6151	512
2	6358	512	19164	512
3	7352	512	12407	512
4	7136	512	13576	512
5	7832	512	8505	512
6	5066	512	6899	512
7	7832	512	11198	512
8	8660	512	10576	512

Tabla 3. Resultados ataque de múltiple salto 2, dirección horizontal.

En opinión del autor de esta tesis, aunque hay una reducción del caudal, esto no es tan importante ya que toda la información, es decir todos los paquetes están siendo entregados en forma satisfactoria durante el tiempo de simulación establecido (900s) y la pérdida de paquete es una consecuencia más grave. Resultados del ataque desde un vecino del nodo 1 hasta un vecino del nodo 6, buscando partir la red y separar los nodos 1, 4 y 6 de la red (ataque horizontal) se muestran a continuación en la Tabla 3, con comportamientos similares.

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

Como se mencionó en el capítulo 4, 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 reiniciar más veces su ventana de contención y su tiempo de *Backoff* es más bajo, impidiendo que las transmisiones de los otros nodos lleguen al servidor pues siempre gana el acceso al medio. El esquema BEB favorece el último ganador entre los nodos contendientes por el canal.

Los ataques de denegación de servicio en redes Ad Hoc son un tema sobre el cual se ha hecho poca investigación y aún menos cuando estos son dirigidos a explotar los problemas que la capa de acceso al medio del protocolo 802.11 presenta cuando funciona en redes de múltiple salto. Estos problemas tienen como base, que el diseño del protocolo no fue hecho para éste tipo de redes y sumándole un ataque de denegación de servicio basado en congestión los problemas de la red se hacen aún mayores llegando a reducir hasta en su totalidad el tráfico normal que puede circular por la red.

Análisis sobre la prevención de los ataques de denegación de servicio se han hecho anteriormente pero pocas soluciones se han creado al respecto. En [19] se 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 de los DoS sobre cadenas de nodos. Los autores proponen soluciones como: disminuir la distancia entre el nodo fuente y destino, 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 realizan ni muestran resultados de estas soluciones, solo las plantean.

Una solución concreta para disminuir el efecto en la red Ad Hoc del ataque es planteada en [4], aunque no explica con profundidad como se hizo, consiste en aumentar la justicia y equidad en el comportamiento de la capa MAC para ayudar a evitar la disminución del caudal. Los autores del artículo llaman a esta solución

FAIRMAC, que es un protocolo basado en TDMA el cual usa *"time slots"* fijos y logra mejoras de hasta el 50% bajo condiciones de ataque, trabajando exclusivamente en una red de topología en malla (12X12) de 144 nodos.

Buscando fortalecer la capa MAC con el fin de que el atacante al interior de la red evite éste comportamiento exitoso se estudiaron los parámetros configurables de la capa MAC, las ventanas de tiempo entre paquetes y el algoritmo de *Backoff*, los cuales se tratan a continuación.

5.1 Límites de retransmisión

Una retransmisión es definida como un nuevo intento de enviar un paquete de información o un paquete de control desde la capa de acceso al medio, separados por intervalos de SIFS, cuando estos no son recibidos exitosamente por su destino debido al tráfico en la red, una colisión o una falla en el enlace. Cada nodo o estación que pertenezcan a una red que use el protocolo 802.11b debe mantener un límite de retransmisión corto (SSRC) y un límite de retransmisión largo (SLRC), los cuales toman inicialmente un valor de cero.

El límite de retransmisión corto (SSRC), es el número máximo de retransmisiones 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 (SLRC), es el valor máximo de retransmisiones esperadas para que una estación reciba un paquete ACK, en otras palabras el número máximo de veces que una estación puede retransmitir un paquete de datos. El estándar de 802.11 [6] 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 [31] asignan por defecto un valor 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 máximo para los límites de retransmisión para 802.11b, sólo define los valores por defecto antes nombrados. Para 802.11a el estándar define que el rango de los límites de retransmisión es de 1 a 255.

El estándar 802.11 [6], fue diseñado originalmente (no se ha modificado y sigue siendo usado) para redes de área local inalámbricas, por lo tanto los parámetros de configuración de la capa MAC están establecidos para el desempeño de estas redes de un sólo salto, sin tenerse en consideración la topología de múltiple salto y otras características que se puedan presentar, llevando a que no sean los más adecuados para las redes de múltiple salto. Entre estos parámetros se encuentran los límites de retransmisión.

Los ataques de denegación de servicio (DoS), reducen considerablemente el tráfico y el rendimiento en las redes. Al aumentar los límites de retransmisión se reduciría la probabilidad de que los paquetes se pierdan rápidamente debido a colisiones por congestión y al efecto captura, haciendo la capa MAC más insistente en buscar que el envío y recepción de los paquetes sea satisfactorio, ya que como se mencionó anteriormente los valores por defecto funcionan bien en redes *WLAN* donde la posibilidad de congestión y de rompimiento del enlace son más bajas y la comunicación se hace directamente con los puntos de acceso (AP). No obstante, un aumento considerable en estos valores podría ser no 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 [15], 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 de 7 a 14 y el límite de retransmisión de paquetes de datos de 4 a 10. El artículo registra que para redes con mayor número de saltos se logran incrementos en el caudal y en 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 [18], se propone que con un aumento mayor en los límites de retransmisión, de 7 a 21 para el límite de retransmisión corto y de 4 a 12 para el límite de retransmisión largo en una red más compleja con 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 éste experimento en condiciones de red similares a los usados en esta tesis y en el artículo, no se

encontró que la mejora del desempeño llegara al valor reportado, solo se encontró una mejora de aproximadamente 2% en el caudal total de la red.

Con la topología del escenario de simulación planteado y lanzando el ataque de denegación de servicio basado en congestión en el vecindario del nodo servidor a una tasa igual al total del ancho de banda del canal inalámbrico (2Mbps), con los límites de retransmisión por defecto (7 y 4), el ataque hace que el caudal total de la red disminuya hasta 0.5% y el número de bytes recibidos al 1.4% con respecto a la red sin ataque, para la red de 144 nodos y en menos del 1% del caudal y a menos del 1.5% de bytes recibidos en las redes de mayor número de nodos, como se mostró en la Tabla 1 y en la Figura 33, en el numeral 4.3.

Para mejorar el efecto que el ataque tiene sobre el tráfico normal de la red, se variaron los límites de retransmisión de dos maneras: primero, variando el límite de retransmisión de paquetes cortos y dejando el límite de retransmisión de paquetes largos fijo, para encontrar el valor del límite de retransmisión de paquetes cortos con el cual se obtiene el mayor caudal. Una vez encontrado éste valor se dejó fijo y se varió el límite de retransmisión largo hasta encontrar, el valor con el cual el caudal es mayor, y segundo realizando un procedimiento similar, variando el límite de retransmisión largo y dejando fijo el límite de retransmisión de paquetes corto, para encontrar el valor del límite de retransmisión de paquetes largos con el cual se obtiene el mayor caudal y con éste valor encontrado fijo, se varió el límite de retransmisión corto hasta encontrar el valor con el cual el caudal era mayor. Los límites de retransmisión, son valores configurables (archivo .config) en los escenarios de Qualnet®.

Lo que se busca es 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 para que algunos paquetes puedan llegar a su destino, y el rendimiento de la red aumente.

Aunque aumentar los límites de retransmisión no muestra una tendencia clara en el aumento del caudal total de la red, aumentar los dos límites de retransmisión 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) (léase límite de retransmisión de

paquetes cortos, SRL),y límite de retransmisión de paquetes largos, LRL) el desempeño en el caudal total de la red en presencia del ataque de denegación de servicio mejora desde aproximadamente un 10% hasta aproximadamente el 25% tal y como se muestra en la Figura 37, ya que más paquetes son entregados al servidor o a su destino. Esta medida fortalece la capa MAC ante la presencia del ataque, pero esta mejora no es considerada como definitiva y el caudal de la red y el número de paquetes recibidos permanecen bajos.

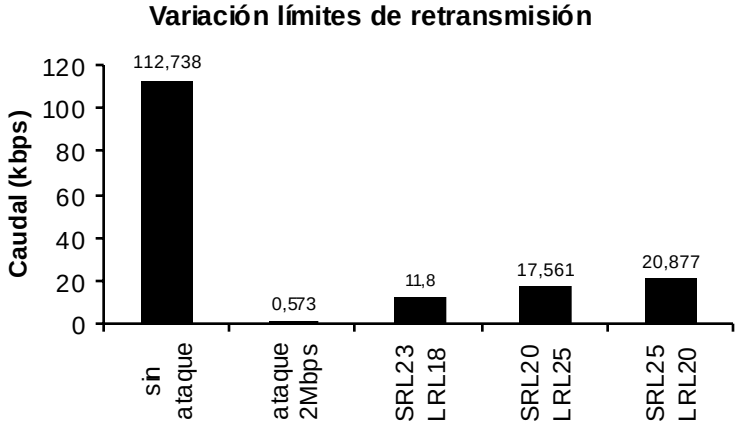

Figura 37. Mejora del caudal total en la red ante ataque de denegación de servicio de 2Mbps mediante la variación de los límites de retransmisión en red 144 nodos

5.2 Mejora algoritmo de Backoff ante denegación de servicio

Como se ha mencionado a lo largo de éste documento, el problema principal es el efecto captura que hace que el ataque de denegación de servicio, con menor número de saltos y mayor cantidad de tráfico tenga privilegio de acceso al medio ya que el retroceso del algoritmo de *Backoff* siempre lo favorece, pues siempre que un nodo reinicia su ventana de contención, el tiempo de *Backoff* calculado es el menor, venciendo a los demás nodos por el acceso al canal. Esto ocurre cuando el ataque se encuentra en el área de interferencia lo que hace que los otros tráficos sean suprimidos y el caudal de la red sea casi cero.

Los algoritmos de mejora del desempeño anteriormente tratados (numeral 2.2), no funcionan para fortalecer la capa de acceso al medio en redes de múltiple salto, debido a que estos algoritmos continúan dando prioridad al transmitir al nodo con más tráfico es decir al nodo que logra la última transmisión exitosa, el ataque para

éste caso. No obstante, estos sirven como base para encontrar la mejora de desempeño de una red de múltiple salto cuando en su interior hay un ataque de denegación de servicio.

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 fue aumentando el valor del límite mínimo de la ventana de contención para todos los escenarios de simulación, buscando hacer más equitativa la oportunidad de todos los nodos para transmitir. A partir de esto se encontró que el caudal aumentaba al igual que el número de paquetes entregados a medida que *CWmin* era mayor, sobretodo cuando la red tiene un mayor número de nodos y de saltos, para los tráficos normales. Algunos de los resultados obtenidos, usando el escenario de simulación descrito en el numeral 4.3 y la Figura 31, para 3 tamaños de red se muestran en las Figuras 38-40.

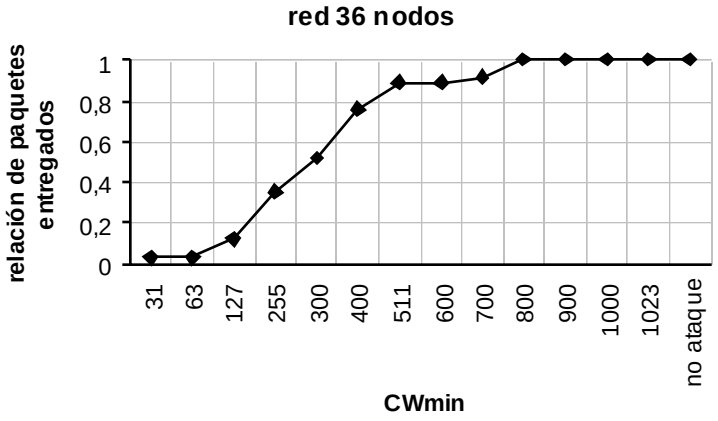

Figura 38. Relación de paquetes entregados red 36 nodos bajo ataque aumentando CWmin.

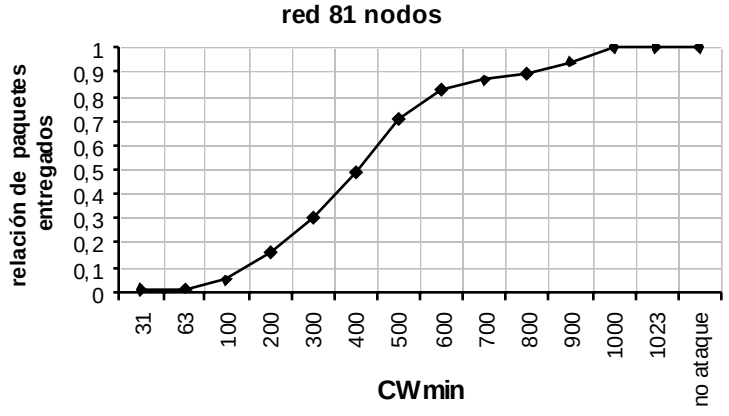

Figura 39. Relación de paquetes entregados red de 81 nodos bajo ataque aumentando CWmin.

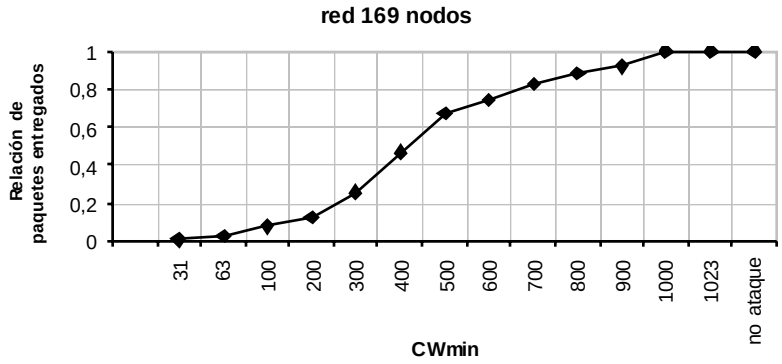

Figura 40. Relación de paquetes entregados red de 169 nodos bajo ataque aumentando CWmin.

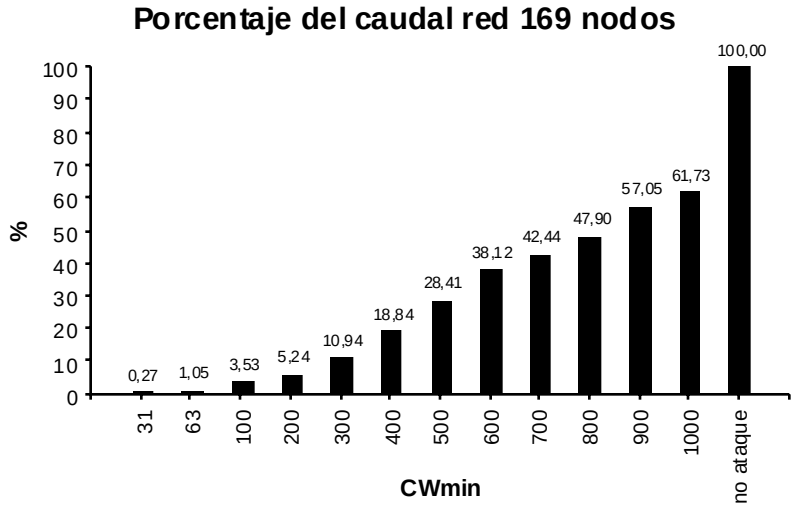

Figura 41. Aumento en el caudal en red de 169 nodos bajo ataque.

La relación de entrega de paquetes en los 3 tamaños de red va aumentando hasta alcanzar 1 (100%). El caudal en la red bajo ataque aumenta considerablemente llegando hasta un valor del 60% en la red de 169 nodos como lo muestra la Figura 41.

Debido a éste 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. Éste mismo comportamiento puede notarse en todos los tamaños de red y se muestra a continuación en la Figura 42, para la red de 144 nodos.

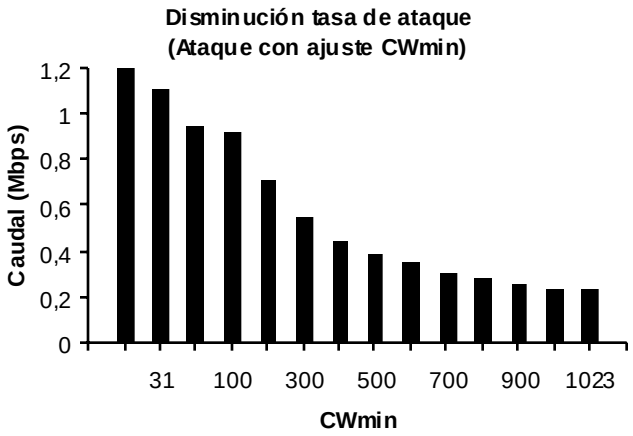

Figura 42. Disminución tasa de ataque con ajuste de CWmin red 144 nodos.

Teniendo en cuenta todo lo anteriormente descrito, referente a la disminución del efecto del ataque al aumentar *CWmin*, se propone una mejora al algoritmo que no es tan agresiva en la forma con que retrocede y que es suave para que no aumente 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 descritas en el numeral 2.2, de tal forma que no hubiese necesidad de dejar fijo el límite mínimo de la ventana de contención. Por éste motivo 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:

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

Figura 43. Modificación al algoritmo BEB para reducir el impacto de DoS.

Cuando hay una colisión, al igual que en el esquema BEB, la ventana de contención se dobla hasta alcanzar su límite máximo (1023). Después de una transmisión exitosa en lugar de reiniciar 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 las misma o mayor oportunidad de transmitir ya que su tiempo de

Backoff puede ser menor que el del atacante y el tráfico del ataque disminuye como se mostró en la Figura 42.

Modificando el algoritmo BEB en la función Mac802_11ResetCW del archivo mac_802_11.cpp de Qualnet®, con el nuevo algoritmo hay una mejora notable en el caudal y en su relación de entrega de paquetes de las redes, cuando ocurre un ataque en su interior. En las redes de mayor tamaño, la mejora del caudal es mayor alcanzando hasta el 60%, como se muestra en la Tabla 4 y la relación de entrega de paquetes alcanza valores desde el 80% hasta el 100%, como se muestra en la Figura 44, teniendo en cuenta que en las redes de menor tamaño sin condición de ataque, el caudal alcanzado por los cada uno de los clientes es mayor.

Porcentaje caudal bajo ataque		
Nodos	**BEB**	**Algoritmo modificado**
25	0,83	11,01
36	0,31	30,92
49	0,69	16,83
64	0,56	18,17
81	0,29	48,33
100	0,88	33,07
121	0,44	53,23
144	0,50	55,81
169	0,27	62,75

Tabla 4. Porcentajes del caudal en redes bajo ataque.

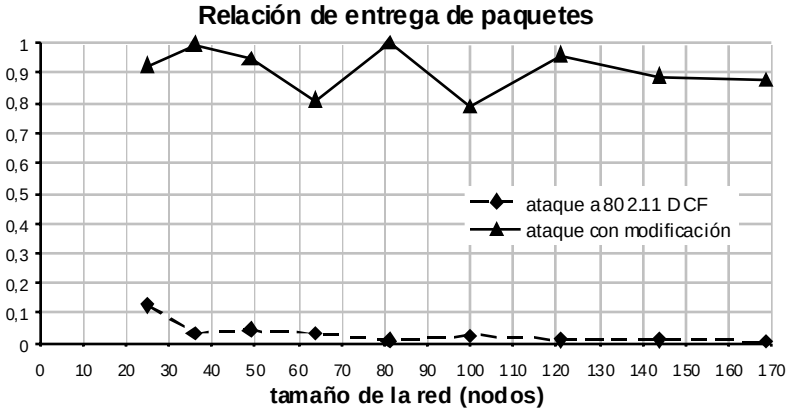

Figura 44. Mejora relación entrega de paquetes.

El grado de retroceso del algoritmo de *Backoff* (-1) fue escogido debido a que brinda un mejor desempeño sobre otros también considerados bajos y lineales,(-2, -16 ,-32, - 64) que se muestran en la Figura 45. En las Figuras 45 y 46, 2CW-16 significa que se dobla la ventana de contención cuando hay colisión y se disminuye linealmente en 16 cuando ocurre una transmisión exitosa, para cualquier tamaño de red. Como ejemplo las Figuras 45 y 46 muestran el comportamiento en una red de 144 nodos.

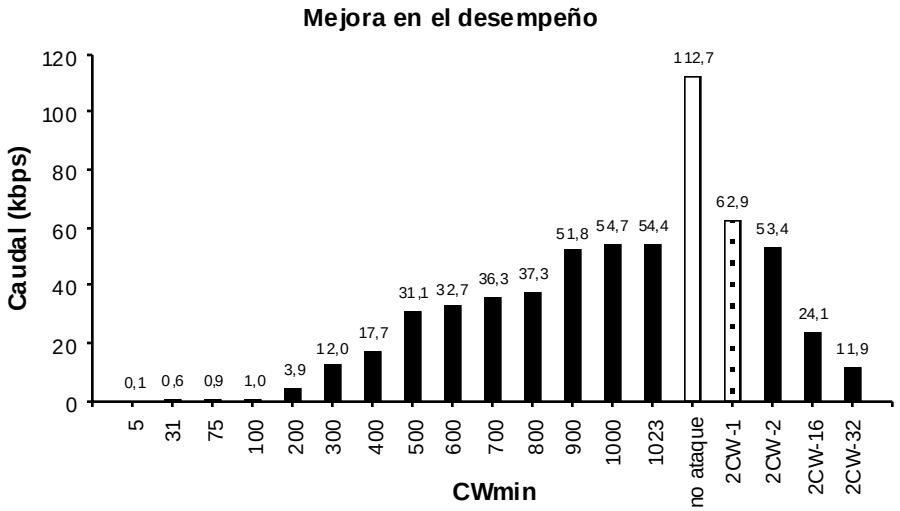

Figura 45. Comparación del caudal entre mejoras al BEB en red 144 nodos, bajo ataque de 2Mbps.

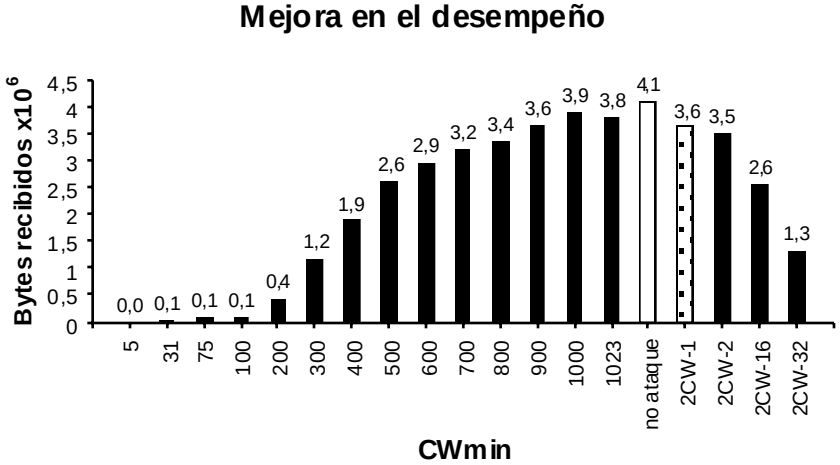

Figura 46. Comparación bytes recibidos entre mejoras al BEB en red 144 nodos bajo ataque de 2Mbps.

Siendo esta mejora al algoritmo una medida de prevención y fortalecimiento del protocolo, 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 en esas redes, como se muestra en la Figura 47.

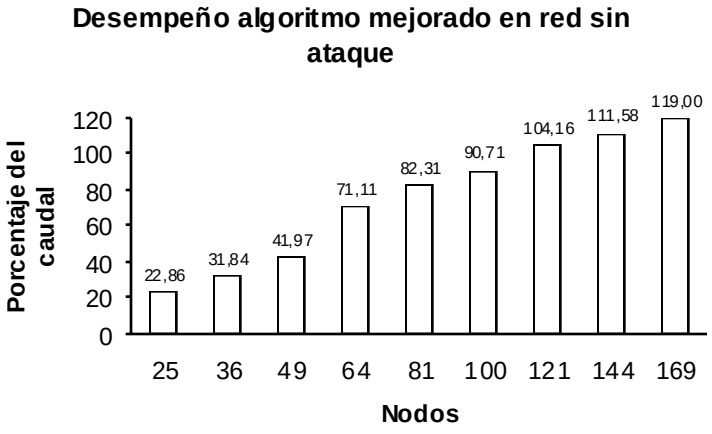

Figura 47. Porcentaje del caudal en redes sin ataque con algoritmo mejorado.

La relación de entrega de paquetes siempre permanece alta, todos los paquetes son recibidos por el servidor, tanto con el BEB como con el algoritmo mejorado, luego no hay disminución en esta métrica y el algoritmo mejorado funciona correctamente como se muestra en la Figura 48.

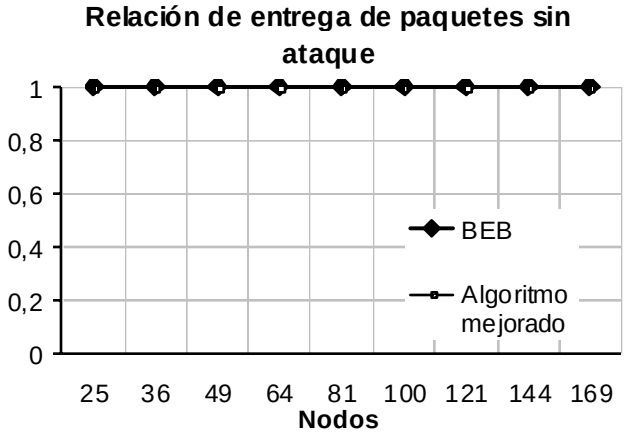

Figura 48. Relación de entrega de paquetes BEB vs. Algoritmo mejorado para DoS.

El tiempo promedio de envío de paquetes es mucho mayor para una red bajo ataque que para una red sin ataque. En la red sin ataque, el tiempo de transmisión (tiempo que le toma al servidor en recibir todos los paquetes de una fuente determinada) crece a medida que la red es de mayor tamaño, debido al mayor número de saltos que deben atravesar los paquetes. Los nodos de la red expuestos a un ataque, agotan sus reintentos y sus ventanas de contención alcanzan su máximo, llevando a que la mayoría de paquetes se pierdan. Con el algoritmo modificado, el tiempo de envío de paquetes crece comparado con el de la red funcionando con el estándar, por el aumento del tamaño de las ventanas de contención de los nodos sin embargo, al realizarse más transmisiones exitosas con la modificación del algoritmo, menos paquetes se pierden luego el tiempo total de transmisión es menor que el de la red bajo ataque, como lo muestra la Figura 49.

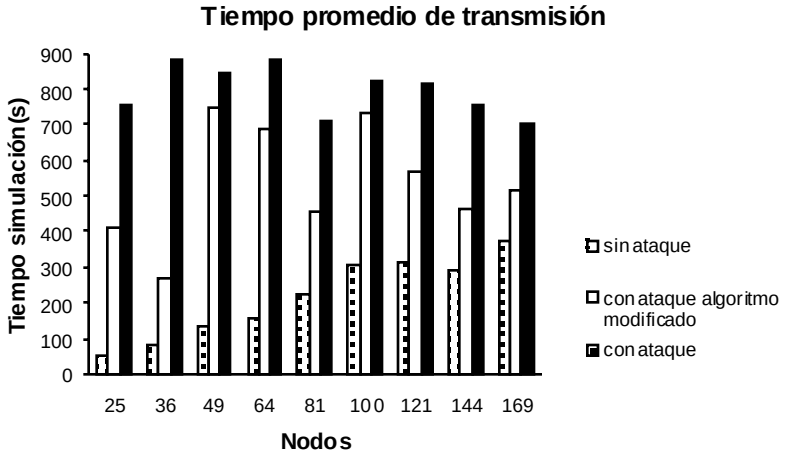

Figura 49. Comparación tiempo promedio de transmisión.

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 a la red de múltiple salto, la mejora ante el ataque es evidente y se muestra en la Figura 50. La relación de paquetes entregados crece al 100% para todas las redes, Figura 50 y el caudal incluso sobrepasa el desempeño sin ataque en las redes de mayor número de nodos, en la Figura 51.

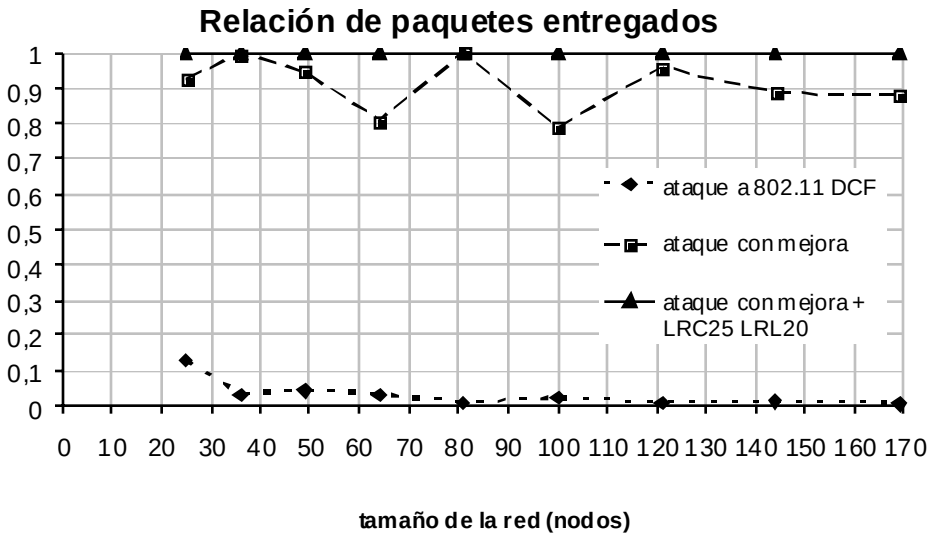

Figura 50. Relación de entrega de paquetes algoritmo mejorado para DoS.

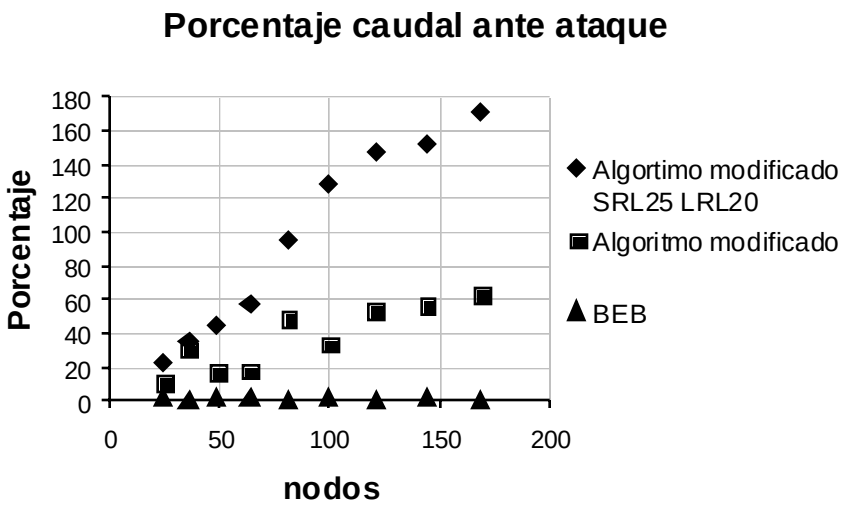

Figura 51. Porcentaje del caudal algoritmo mejorado para DoS.

6. CONCLUSIONES

Esta investigación se enfocó en los ataques de denegación de servicio basados en tráfico sobre la capa de acceso al medio del protocolo IEEE 802.11, actualmente usada para la construcción de las redes Ad Hoc. Un ataque de denegación de servicio basado en tráfico puede ser lanzado de manera muy sencilla en una red Ad Hoc, sólo aumentando la tasa de envío de paquetes por parte de un nodo (de manera involuntaria o voluntaria) muy por encima de los otros tráficos, lo que trae consecuencias a la red como la disminución en el número total de paquetes recibidos y por tanto una caída notable en el caudal de la red.

Se verificó que la localización y número de saltos del ataque de denegación de servicio son cruciales en cuanto a ubicar que estaciones el atacante quiere dejen de transmitir, así como el tamaño de la red en cuanto a la distancia o al número de saltos entre el cliente y el servidor. Los ataque de múltiple salto son poco factibles y las consecuencias se dan solo en la vecindad de la fuente de ataque.

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 éste 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 éste trabajo, sin embargo existen pocos o ningún mecanismo que mitiguen el impacto del ataque sobre de la red.

En éste trabajo se estudiaron algunos algoritmos para mejorar el desempeño de redes de un solo salto y se comprobó que estos 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, aumentado 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 en esta investigación.

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 entregan el 100% de los paquetes enviados.

7. REFERENCIAS

[1] García Carlos, Moreno José, Soto Ignacio y Vidal Iván, “Servicios de Valor Añadido en Redes Móviles Ad-hoc”, Departamento de Ingeniería Telemática, Universidad Carlos III de Madrid, *XIII Jornada Telecom I+D*, 2003.

[2] Arun Kumar Bayya, Siddhartha Gupte, Yogesh Kumar Shukla, Anil Garikapati, Security in Ad-hoc Networks”, Computer Science Department, University of Kentucky”, Recuperado de: http://www.cs.uky.edu/~singhal/term-papers/Fourth-paper.doc.

[3] Foong Heng Wai, Yin Nwe Aye, Ng Hian James, “Intrusion Detection in Wireless Ad-Hoc Networks”, Recuperado de: http://www.comp.nus.edu.sg/~cs4274/termpapers/0304-I/group4/paper.pdf.

[4] Vikram Gupta, Michalis Faloutsos, Srikanth Krishnamurthy, “Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks”, National Science Foundation under Grant No. 9985195, DARPA award N660001-00-18936, *MilCom Anaheim*, 2002.

[5] 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.

[6] *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.*

[7] 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.

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

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

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

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

[16] 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.

[17] Jinyang Li, Charles Blake, Douglas S.J. De Couto, Hu Imm Lee, and Robert Morris, “Capacity of Ad Hoc 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.

[18] 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.

[19] 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.

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

[21] David Moore, Stefen Savage, Geoffrey M.Voelker, “Quantitative Network Security Analysis”, CAIDA/SDSC and CSE Department University of California, San Diego. 2002.

[22] V. Yegneswaran, P. Barford, J. Ullrich, “Internet Intrusions: Global Characteristics and Prevalence”, *In Proceedings of the International Conference on Measurements and Modeling of Computer Systems*, SIGMETRICS 2003.

[23] Jaeyeon Jung, Balachander Krishnamurthy, Michael Rabinovich,” Flash Crowds and Denial of Service Attacks: Characterization and Implications for CDNs and Web Sites”, *WWW2002*, Mayo 7-11, 2002, Honolulu Hawaii USA.

[24] David Moore, Stefen Savage, Geoffrey M Voelker, “Inferring Internet Denial of Service Activity”, *In Proceedings of the USENIX Annual Technical Conference*. 2001.

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

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

[27] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang, “MACAW: A Media Access Protocol for Wireless LAN’s”, *In Proc. ACM SIGCOMM.94*, London, England, 1994, pp. 212–225.

[28] *OPNET® Modeller,.* www.opnet.com.

[29] 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.

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

[31] *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Linux. Chapter 5 Advanced Configuration, OL-1376-02,* Disponible en: http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_installation_and_configuration_guide_book09186a008007f93c.html.

ANEXO. ARCHIVOS DE CONFIGURACIÓN Y TRÁFICO

A continuación se incluye el archivo de configuración (.config) de la red de 169 nodos y posteriormente la configuración de las sesiones de tráfico para la misma red bajo ataque.

```
# ***** QualNet Configuration File *****

# ************* General ***********

VERSION 3.8
EXPERIMENT-NAME Qualnet
SIMULATION-TIME 901S
SEED 1

# ************* Parallel Settings ***********

PARTITION-SCHEME AUTO

# ************* Terrain ***********

COORDINATE-SYSTEM CARTESIAN
TERRAIN-DIMENSIONS ( 4550, 4550 )
DUMMY-ALTITUDES ( 1500, 1500 )
TERRAIN-DATA-BOUNDARY-CHECK YES

# ************* Nodes ***********

DUMMY-NUMBER-OF-NODES 169
NODE-PLACEMENT FILE
NODE-POSITION-FILE C:\qualnet\3.8\bin\cwmin169ftpgen\cwmin169ftpgen\cwmin169ftpgen.nodes

# ************* Mobility ***********

MOBILITY NONE
MOBILITY-POSITION-GRANULARITY 1.0
MOBILITY-GROUND-NODE NO

# ************* Wireless Settings ***********
# ************* Channel ***********

PROPAGATION-CHANNEL-FREQUENCY 2400000000
PROPAGATION-MODEL STATISTICAL
PROPAGATION-LIMIT -111.0
PROPAGATION-PATHLOSS-MODEL TWO-RAY
PROPAGATION-SHADOWING-MODEL CONSTANT
PROPAGATION-SHADOWING-MEAN 4.0
PROPAGATION-FADING-MODEL NONE

# ************* Radio/Physical Layer ***********

PHY-MODEL PHY802.11b
PHY802.11-AUTO-RATE-FALLBACK NO
PHY802.11-DATA-RATE 2000000
```

```
PHY802.11b-TX-POWER--1MBPS 15.0
PHY802.11b-TX-POWER--2MBPS 16.78305
PHY802.11b-TX-POWER--6MBPS 15.0
PHY802.11b-TX-POWER-11MBPS 15.0
PHY802.11b-RX-SENSITIVITY--1MBPS -93.0
PHY802.11b-RX-SENSITIVITY--2MBPS -89.0
PHY802.11b-RX-SENSITIVITY--6MBPS -87.0
PHY802.11b-RX-SENSITIVITY-11MBPS -83.0
PHY802.11-ESTIMATED-DIRECTIONAL-ANTENNA-GAIN 15.0
PHY-RX-MODEL PHY802.11b
PHY-LISTENABLE-CHANNEL-MASK 1
PHY-LISTENING-CHANNEL-MASK 1
PHY-TEMPERATURE 290.0
PHY-NOISE-FACTOR 10.0
ANTENNA-MODEL OMNIDIRECTIONAL
ANTENNA-GAIN 0.0
ANTENNA-HEIGHT 1.5
ANTENNA-EFFICIENCY 0.8
ANTENNA-MISMATCH-LOSS 0.3
ANTENNA-CABLE-LOSS 0.0
ANTENNA-CONNECTION-LOSS 0.2

# ************* MAC Protocol ***********

MAC-PROTOCOL MAC802.11
MAC-802.11-DIRECTIONAL-ANTENNA-MODE NO
MAC-802.11-SHORT-PACKET-TRANSMIT-LIMIT 25
MAC-802.11-LONG-PACKET-TRANSMIT-LIMIT 20
MAC-802.11-RTS-THRESHOLD 0
MAC-802.11-PCF-STATISTICS NO
MAC-PROPAGATION-DELAY 1US
PROMISCUOUS-MODE YES

# ************* Adaptation Layer ***********

ADAPTATION-LAYER-STATISTICS NO
ATM-STATIC-ROUTE NO

# ************* ARP Enabled ***********

ARP-ENABLED NO

# ************* ARP Specs ***********

ARP-TIMEOUT-INTERVAL 20M

# ************* Network Protocols ***********

# ************* Network Protocol ***********

NETWORK-PROTOCOL IP
IP-ENABLE-LOOPBACK YES
IP-LOOPBACK-ADDRESS 127.0.0.1
IP-FRAGMENTATION-UNIT 2048
IP-QUEUE-NUM-PRIORITIES 3
IP-QUEUE-PRIORITY-INPUT-QUEUE-SIZE 50000
DUMMY-PRIORITY-QUEUE-SIZE NO
IP-QUEUE-PRIORITY-QUEUE-SIZE 50000
DUMMY-PRIORITY-WISE-IP-QUEUE-TYPE NO
IP-QUEUE-TYPE FIFO
```

```
IP-QUEUE-SCHEDULER STRICT-PRIORITY
ROUTER-BACKPLANE-THROUGHPUT 0

# ************* Routing Protocol ***********

DUMMY-ROUTING DYNAMIC
ROUTING-PROTOCOL AODV
AODV-NET-DIAMETER 35
AODV-NODE-TRAVERSAL-TIME 40MS
AODV-ACTIVE-ROUTE-TIMEOUT 3S
AODV-MY-ROUTE-TIMEOUT 6S
AODV-HELLO_INTERVAL
AODV-HELLO-INTERVAL 1S
AODV-HELLO_INTERVAL
AODV-ALLOWED-HELLO-LOSS 2
AODV-RREQ-RETRIES 2
AODV-ROUTE-DELETION-CONSTANT 5
AODV-PROCESS-HELLO NO
AODV-LOCAL-REPAIR NO
AODV-SEARCH-BETTER-ROUTE NO
AODV-BUFFER-MAX-PACKET 100
AODV-BUFFER-MAX-BYTE 0
AODV-OPEN-BI-DIRECTIONAL-CONNECTION YES
AODV-TTL-START 1
AODV-TTL-INCREMENT 2
AODV-TTL-THRESHOLD 7
HSRP-PROTOCOL NO
STATIC-ROUTE NO

DEFAULT-ROUTE YES
DEFAULT-ROUTE-FILE C:\qualnet\3.8\bin\cwmin169ftpgen\cwmin169ftpgen\cwmin169ftpgen.routes-
default

# ************* MPLS configuration ***********

MPLS-PROTOCOL NO

# ************* Transport Layer ***********
TCP LITE
TCP-USE-RFC1323 NO
TCP-DELAY-ACKS YES
TCP-DELAY-SHORT-PACKETS-ACKS NO
TCP-USE-NAGLE-ALGORITHM YES
TCP-USE-KEEPALIVE-PROBES YES
TCP-USE-PUSH YES
TCP-MSS 512
TCP-SEND-BUFFER 16384
TCP-RECEIVE-BUFFER 16384

# ************* ATM Layer2 ***********

# ************* ATM Layer2 ***********

ATM-RED-MIN-THRESHOLD 5
ATM-RED-MAX-THRESHOLD 15
ATM-RED-MAX-PROBABILITY 0.02
ATM-RED-SMALL-PACKET-TRANSMISSION-TIME 10MS
ATM-QUEUE-SIZE 15000
ATM-SCHEDULER-STATISTICS NO
ATM-LAYER2-STATISTICS NO
```

```
ATM-QUEUE-STATISTICS NO

# ************* Traffic and Status ***********

# ************* Application Layer ***********

APP-CONFIG-FILE C:\qualnet\3.8\bin\cwmin169ftpgen\cwmin169ftpgen\cwmin169ftpgen.app

# ************* Tracing ***********

PACKET-TRACE NO
ACCESS-LIST-TRACE NO

# ************* Statistics ***********

APPLICATION-STATISTICS YES
TCP-STATISTICS YES
UDP-STATISTICS YES
ROUTING-STATISTICS YES
ICMP-STATISTICS NO
IGMP-STATISTICS NO
EXTERIOR-GATEWAY-PROTOCOL-STATISTICS YES
NETWORK-LAYER-STATISTICS YES
QUEUE-STATISTICS YES
SCHEDULER-STATISTICS YES
MAC-LAYER-STATISTICS YES
PHY-LAYER-STATISTICS YES
MOBILITY-STATISTICS NO
MPLS-STATISTICS NO
MPLS-LDP-STATISTICS NO
RSVP-STATISTICS NO
SRM-STATISTICS NO
DIFFSERV-EDGE-ROUTER-STATISTICS NO
QOSPF-STATISTICS NO
ACCESS-LIST-STATISTICS NO
POLICY-ROUTING-STATISTICS NO
ROUTE-REDISTRIBUTION-STATISTICS NO
SIGNALLING-STATISTICS NO
MOBILE-IP-STATISTICS NO

# ************* Device properties ***********

USE-NODE-ICON YES
NODE-ICON C:\qualnet\3.8\bin\cwmin169ftpgen\cwmin169ftpgen\DEFAULT.GIF

# ************* Node Orientation ***********

AZIMUTH 0
ELEVATION 0

# ************* Parallel Properties ***********
PARTITION 0

#----------------Default Subnet ----------------
SUBNET N8-192.0.0.0 { 1 thru 169 } Default

IP-FORWARDING NO
[ 1 thru 169 ] IP-FORWARDING YES
```

COMPONENT 0 {1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59
COMPONENT 0 {60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111
COMPONENT 0 {112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153
COMPONENT 0 {154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169} 169 2275.0 2275.0 0.0 4550.0 4550.0 3000.0

La aplicación de tráfico FTP/GENERIC se configura de la siguiente manera: FTP/GENERIC nodo fuente nodo destino Paquetes a enviar Tamaño del paquete en bytes Inicio de transmisión Fin de la sesión Prioridad

La aplicación de tráfico CBR se configura: CBR nodo fuente nodo destino Paquetes a enviar Tamaño del paquete en bytes Tiempo entre paquetes Inicio de transmisión Fin de la sesión Prioridad

FTP/GENERIC 1 85 1000 512 1S 921S PRECEDENCE 0
FTP/GENERIC 7 85 1000 512 1S 921S PRECEDENCE 0
FTP/GENERIC 13 85 1000 512 1S 921S PRECEDENCE 0
FTP/GENERIC 79 85 1000 512 1S 921S PRECEDENCE 0
FTP/GENERIC 91 85 1000 512 1S 921S PRECEDENCE 0
FTP/GENERIC 157 85 1000 512 1S 921S PRECEDENCE 0
FTP/GENERIC 163 85 1000 512 1S 921S PRECEDENCE 0
FTP/GENERIC 169 85 1000 512 1S 921S PRECEDENCE 0
CBR 84 97 0 512 2.048MS 1S 921S PRECEDENCE 0

Para una mayor explicación se puede referir al manual de usuario de Qualnet® o a los archivos default.app y default.config.