# Universidad Central “Marta Abreu” de Las Villas

## Facultad de Ingeniería Eléctrica

### Departamento de Telecomunicaciones y Electrónica


# TRABAJO DE DIPLOMA


# Redes inalámbricas de múltiples saltos

# (Redes Ad-Hoc)


**Autor: Fouad Ziad Othman**

**Tutor: Dr. Pedro José Arco Rios**



**Santa Clara**

**2007**

**"Año 49 de la Revolución "**

# Universidad Central “Marta Abreu” de Las Villas

## Facultad de Ingeniería Eléctrica

### Departamento de Telecomunicaciones y Electrónica


# TRABAJO DE DIPLOMA


# Redes inalámbricas de múltiples saltos

# (Redes Ad-Hoc)


**Autor: Fouad Ziad Othman**

E-mail: fouadcuba@yahoo.com

**Tutor: Dr. Pedro José Arco Rios**

E- mail: Parco @uclv.edu.cu


**Santa Clara**

**2007**

**"Año de la 49 de la Revolución"**


Hago constar que el presente trabajo de diploma fue realizado en la Universidad Central "Marta Abreu" de Las Villas como parte de la culminación de estudios de la especialidad de Ingeniería en Telecomunicaciones y Electrónica, autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

_____

Firma del Autor

Los abajo firmantes certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

_____

Firma del Tutor

_____

Firma del Jefe de Departamento donde se defiende el trabajo

_____

Firma del Responsable de Información Científico-Técnica

*La confianza es la mitad del triunfo*

*Napoleón Bonaparte*

- *A mi familia por todo el apoyo brindado durante estos años y por confiar en mí.*
- *A mi tutor Pedro Arco Rios por dedicarle el tiempo necesario en la realización de esta tesis.*
- *A todos los profesores por enseñarme y transmitirme sus concimientos.*
- *A mis verdaderos amigos, No quisiera mencionar sus nombres, pues cometería el grave error de olvidar a alguno y eso sería imperdonable.*
- *A mis amigos el Ing. Ali Khaled, Ing.Ahmad Mezher, el Dr. Bassam Safa y Dr. Amjad Abdallah (Abo Ali) por su fidelidad como hermanos.*
- *A Roro, por estar siempre a mi lado, siempre estará en mi corazón.*
- *Al pueblo de cuba y su revolución por darme la oportunidad de estudiar aquí y hacer mi sueño realidad.*

- *A mis padres por guiarme por el largo camino de la vida (les debo todo a ellos).*
- *A mis hermanos Taha, Madona, Mohamad y Ali por todo lo que han aguantado por mí en estos 5 años.*
- *A mi tía por quererme como un hijo propio, y en especial a Dania (siempre estarán en mi corazón).*
- *A Samer Ali, por ser más que un hermano.*

*A todos muchas gracias.*

*Fouad*

# TAREA TÉCNICA

- Búsqueda de información sobre las redes inalámbricas con sistemas de múltiples saltos.
- Resumir los aspectos esenciales correspondientes a las arquitecturas empleadas en ese tipo de redes.
- Resumir los problemas técnicos esenciales correspondientes a los protocolos empleados en ese tipo de redes (TCP).
- Estudiar y resumir las estrategias técnicas que se están investigando con el objetivo de mejorar la eficiencia en la utilización de la capacidad del canal.
- Hacer un programa en el MATLAB 7.0 que puede mostrar el análisis grafico del comportamiento de los parámetros que afectan el rendimiento de este protocolo en estas redes.

**Firma del Autor** **Firma del Tutor**

# RESUMEN

En este trabajo se hizo un detallado análisis de las características, las arquitecturas y los estándares de las redes inalámbricas Ad-Hoc, las cuales son de una gran importancia hoy en día debido a las ventajas que ofrecen para los usuarios. Para esto se explica en detalle el protocolo TCP aplicado en esas redes, así como los algoritmos para el control de congestión. Además se mencionan algunos problemas que se presentan en este tipo de redes y las soluciones propuesta para cada uno.

Con el objetivo de entender el comportamiento del protocolo TCP en esas redes, se implementa un programa en el MATLAB 7.0 que demuestra el comportamiento del tamaño de la ventana con respeto a la razón de perdida de paquete usando un modelo matemático conocido como TCP-Friendly, teniendo en cuenta las importancias de cada parámetro para poder realizar correctamente el análisis. Por último se mencionan las principales causas de la degradación del tamaño de ventana.

# INTRODUCCIÓN

Desde finales de la década de los 80 la situación de las redes de computadoras ha cambiado de manera sustancial. Se han producido constantes actualizaciones de tecnología y un incremento de la variedad de formas de acceso. A las redes que usan transmisión por hilo, se han sumado las que utilizan medios inalámbricos, debido a ciertas ventajas como la flexibilidad de operación, bajo costo y la facilidad de instalación. Estas transformaciones han sido impulsadas por nuevas circunstancias comerciales, el desarrollo tecnológico y la evolución de los requerimientos y necesidades de los usuarios. Numerosos centros educacionales e industriales, cuentan con redes con un número de computadoras cada vez más creciente, repartidas por una gran cantidad de subredes, lo que provoca dificultades en la gestión y administración de la misma, además de la necesidad de estar instalando continuamente nuevas líneas de pares.

Actualmente el desarrollo de las redes de comunicaciones y las necesidades de los usuarios demandan el soporte de la movilidad y es precisamente este requerimiento el que resulta ser uno de los mayores retos para el soporte de ínterconectividad entre los usuarios de las redes de datos. El problema del soporte de movilidad se puede dividir en dos grupos: el soporte de movilidad global (macro movilidad) y el soporte de movilidad local (micro movilidad). En general, el problema de la movilidad en redes que utilizan el protocolo de red IP se deriva del hecho de que las direcciones IP se utilizan como identificador y como localizador de un nodo dentro de una subred. De esta forma, cuando un nodo cambia su punto de conexión a la red, o sea el nodo móvil se cambia a otra subred, la dirección IP asignada al nodo deja de ser válida dentro de la nueva subred. En la actualidad se han realizado diversas propuestas para el soporte de micro y macro movilidad en redes. Este tipo de redes y específicamente las redes Ad-Hoc pueden ser desarrolladas de forma muy rápida debido a que no hay que usar ninguna infraestructura,

por eso presentan un enorme potencial de uso en situaciones tales como las comunicaciones militares o los sistemas de emergencia. También presentan un tremendo potencial en computación distribuida, redes inalámbricas de sensores, y redes híbridas inalámbricas (redes que integran sistemas celulares y Ad-Hoc).

Hoy en día, a nivel del Departamento de Electrónica y Telecomunicaciones de la Facultad de Ingeniería Eléctrica de la UCLV, se han realizado pocos estudios sobre las redes de micro movilidad, de ahí la importancia de recopilar información sobre el tema, lo cual permitirá contar con una documentación actualizada y ordenada que posibilite a docentes y estudiantes introducirse en los aspectos técnicos de este tipo de redes. Para llevar a cabo nuestra investigación, se debe cumplir los siguientes objetivos.

Objetivo general:

- Caracterizar las estructuras y problemas fundamentales de las redes de transmisión de datos inalámbricos Ad-Hoc de múltiples saltos.

Objetivos específicos:

- Resumir los aspectos esenciales relacionados con las topologías, los protocolos y estándares de las redes Ad-Hoc.
- Caracterizar la aplicación del protocolo TCP en las redes Ad-Hoc y los algoritmos usados para el control de congestión.
- Analizar el comportamiento de este protocolo desde el punto de vista de la razón de transmisión y las perdidas de paquetes.

**Organización del informe**

Se utilizarán como método teórico, el análisis y crítica de diversas fuentes, tales como libros, artículos e Internet. Y el método comparativo, para comparar procesos y fenómenos a partir de programas elaborados al efecto. Para exponer los resultados de esta investigación, este documento de tesis está dividido y estructurado de la siguiente forma.

En el capitulo 1 se hace referencia a las topologías de las redes inalámbricas y específicamente las redes Ad-Hoc, así como los estándares usados en estas redes. También se habló de la capa física y la subcapa MAC debido a que el estándar usado (802.11) como todos los estándares incluidos en 802, especifica únicamente esas dos capas. Además se hizo un breve estudio de la implicación de la capa de radio, y una comparación entre los múltiples saltos y el salto único, y las ventajas de usar este tipo de redes.

En el capitulo 2 se hizo un análisis del protocolo TCP aplicado en estas redes, así como los mecanismo de control de congestión explicando cada uno de los algoritmos usados en este protocolo. Aquí se trataron los problemas fundamentales que plantean conflictos a las capacidades del protocolo TCP.

En el capitulo 3 se hace un profundo análisis del protocolo TCP-Friendly, y se implementa un programa en el MATLAB 7.0, para el análisis grafico del comportamiento de los parámetros que más afectan el rendimiento de este protocolo.

# CAPÍTULO 1: GENERALIDADES DE LAS REDES INALÁMBRICAS

## 1.1 Breve introducción a las redes inalámbricas

En general, una de las formas de clasificar las redes de telecomunicaciones puede ser como redes cableadas y redes inalámbricas; si bien las redes cableadas constituyen la parte fundamental de los sistemas de comunicaciones, las redes del tipo inalámbrico adquieren singular importancia debido a sus características y flexibilidad de operación. Si los usuarios están interconectados a una red por cableado físico, su movilidad se reduce drásticamente. Por otro lado, la ventaja más obvia de las redes inalámbricas es la de permitir la movilidad de los dispositivos de red dentro de un área de cobertura específico. De igual forma, la implementación de una red inalámbrica se facilita al no requerir de infraestructura cableada, lo que las hace muy útiles en situaciones de emergencia, también es fácil instalar este tipo de redes en edificios donde el diseño no consideró la implementación de una red de datos cableada o donde la implementación de una red cableada resulta ser muy difícil y/o costosa.

Los sistemas inalámbricos han capturado la atención y la imaginación del público, y se han convertido en el segmento de mayor y más rápido crecimiento en las telecomunicaciones, donde su principal consecuencia ha sido dotar de movilidad a los nodos de la red al liberarlos de sus conexiones físicas (cableado), dichos nodos pueden funcionar de encaminadores y de anfitriones (Host).

Los sistemas inalámbricos también están empezando a ofrecer múltiples servicios con calidad como una conversación telefónica, la transferencia de ficheros, acceso a la Web o la realización de videoconferencias, sin restricciones de lugar y de tiempo. Estos ejemplos de comunicación inalámbrica espontánea entre dispositivos o nodos podrían ser definidos de manera informal como un esquema, al que a menudo se denomina formación de redes Ad-Hoc, que permite a los dispositivos establecer la comunicación, en cualquier

momento y en cualquier lugar**.** En realidad, la formación de redes Ad-Hoc como tal no es nueva, sino que lo nuevo es la forma de configuración, de uso y de sus elementos [25].

## 1.2 Tipos de redes inalámbricas

Existen diversas clasificaciones de las redes inalámbricas, de acuerdo con su topología se pueden dividir en dos tipos: **Redes de infraestructura** y **Redes Ad-Hoc**.

### 1.2.1 Redes de infraestructura

Se caracterizan por tener un punto de acceso AP (Access Point) que se encarga de proporcionar la conexión entre los diversos nodos inalámbricos de la red. En este tipo de topologías siempre se requieren dos saltos para enrutar paquetes de un nodo hacia otro en la red inalámbrica. Lo anterior se debe a que la comunicación entre los nodos de una red de infraestructura requiere de la intervención del punto de acceso para conmutar los paquetes de una fuente hacia un destino. Evidentemente, es necesario que todos los nodos se encuentren dentro del área de cobertura del AP, de otra forma no es posible la comunicación [16] [18] [23].

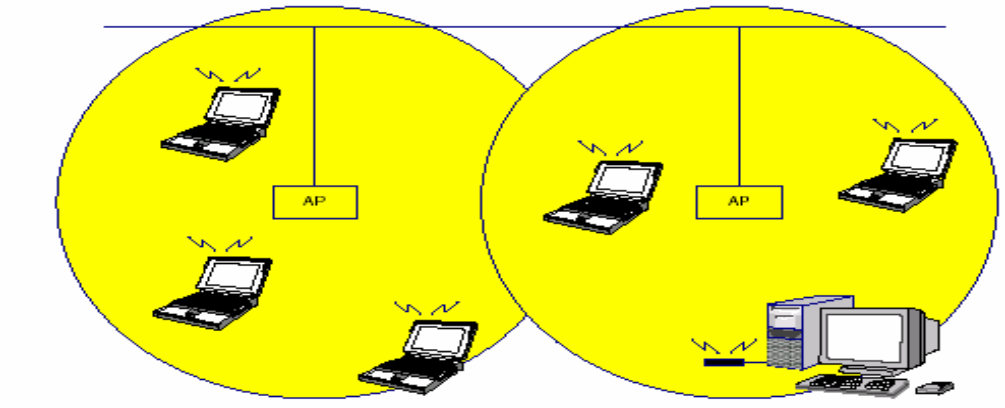


**Figura 1.1** Red de infraestructura

### 1.2.2 Redes Ad-Hoc

Las redes Ad Hoc consisten en nodos móviles (también llamado modo independiente IBSS) [3] interconectados con enlaces de comunicación inalámbricos multisaltos que a diferencia de las redes inalámbricas convencionales, las redes Ad-Hoc no tienen una infraestructura fija de red o administración central, donde la topología de estas redes cambia dinámicamente con nodos móviles entrando o saliendo de la red, y con consecuencias de que algunos enlaces de comunicación llegan a ser inválidos, por ello uno de los principales objetivos en este tipo de redes es encontrar una trayectoria que tenga suficientes recursos para satisfacer las limitaciones del retardo, ancho de banda, calidad de los datos multimedia (video, audio, etc.), enviando paquetes hacia otros nodos y ejecutar las aplicaciones del usuario, adicionalmente también todos los nodos pueden ser móviles dinámicamente, creando una red inalámbrica auto-creciente, auto-organizada y auto-administrada. Por lo tanto, las comunicaciones en estas redes se crearían únicamente por interacciones entre sus nodos móviles inalámbricos, usando esas interacciones para proporcionar el control de flujo necesario y funciones de administración, pero siendo la comunicación degradada en algunos casos por la movilidad de sus nodos. Es decir, los nodos pueden entrar y salir de áreas de mayor interferencia, o alejarse repentinamente de una zona de cobertura de otro nodo con el cual establecía una comunicación [26].

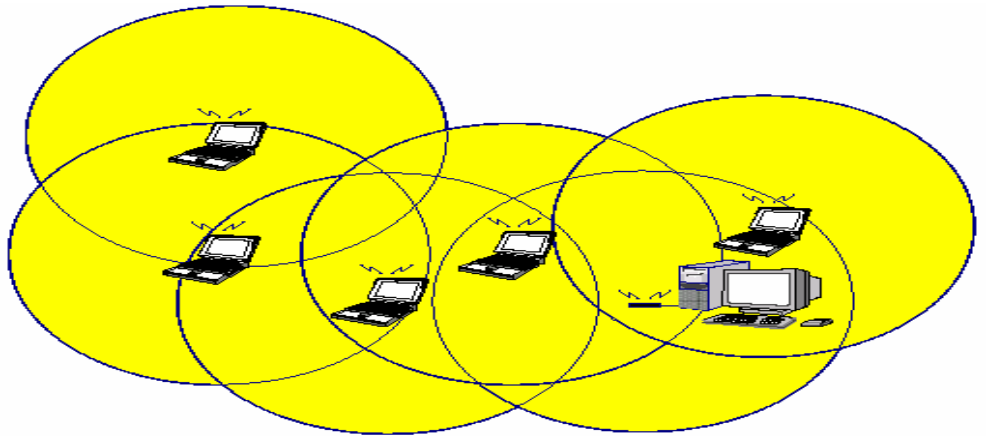

**Figura 1.2** Red Ad-Hoc

## 1.3 Características de las redes Ad-Hoc

Existen diferentes características que usualmente se asocian a una red inalámbrica del tipo Ad-Hoc. A continuación se listan algunas de las características que distinguen a este tipo de redes:

- **Inalámbrica:** Los nodos emplean para comunicarse el medio inalámbrico.
- **Basada en una estructura Ad-Hoc:** La red se forma de manera dinámica y no se restringen a una topología de red predeterminada. La topología de una red Ad-Hoc puede cambiar constantemente y de manera arbitraria de acuerdo con las necesidades de los usuarios de la red.
- **Enrutamiento Multi-salto:** Cada nodo incorpora la funcionalidad de enrutador y tienen la capacidad de conmutar paquetes para lograr la comunicación entre dos nodos diferentes.
- **Movilidad:** Los nodos tiene la libertad de moverse, de aquí la naturaleza dinámica de la red.

En resumen, las redes inalámbricas Ad-Hoc no se limitan a una infraestructura de red fija, y es posible crear redes de acuerdo con las necesidades en el momento.

## 1.4 Implicaciones de la capa de radio

### 1.4.1 ¿Porqué múltiples saltos?

Al tratar con un medio de radiodifusión inalámbrico poco fiable, se deben adoptar especiales consideraciones de radio en el sistema de comunicación de una red Ad-Hoc, para garantizar una operación fiable y eficiente. Una manera de hacer esto es emplear múltiples saltos, lo que facilita la reutilización de recursos tanto en el dominio espacial como en el temporal, siempre y cuando los nodos que participan en la red estén razonablemente bien distribuidos en el espacio. En contraste con esto, las redes de un salto simple comparten fundamentalmente los recursos del canal en el dominio del

tiempo. La figura 1.3 muestra una representación esquemática de la interferencia espacial en escenarios de salto múltiple y de salto simple. Cada caso considera una situación idéntica con respecto a la distribución de nodos, fuentes y destinos. En el escenario de salto múltiple, los paquetes son encaminados por relés intermedios. Sin embargo, la red de simple salto envía los datos directamente desde la fuente al destino. Los círculos de la figura 1.3 indican un alcance controlado en potencia de los nodos que transmiten. La figura 1.3 representa también los nodos inactivos, estos nodos no están involucrados como fuentes, como destinos, ni como relés intermedios. De esta figura sacamos la sensación de que el escenario multisalto proporciona mayor eficiencia espectral (bit/s/Hz/m**2**) [11].

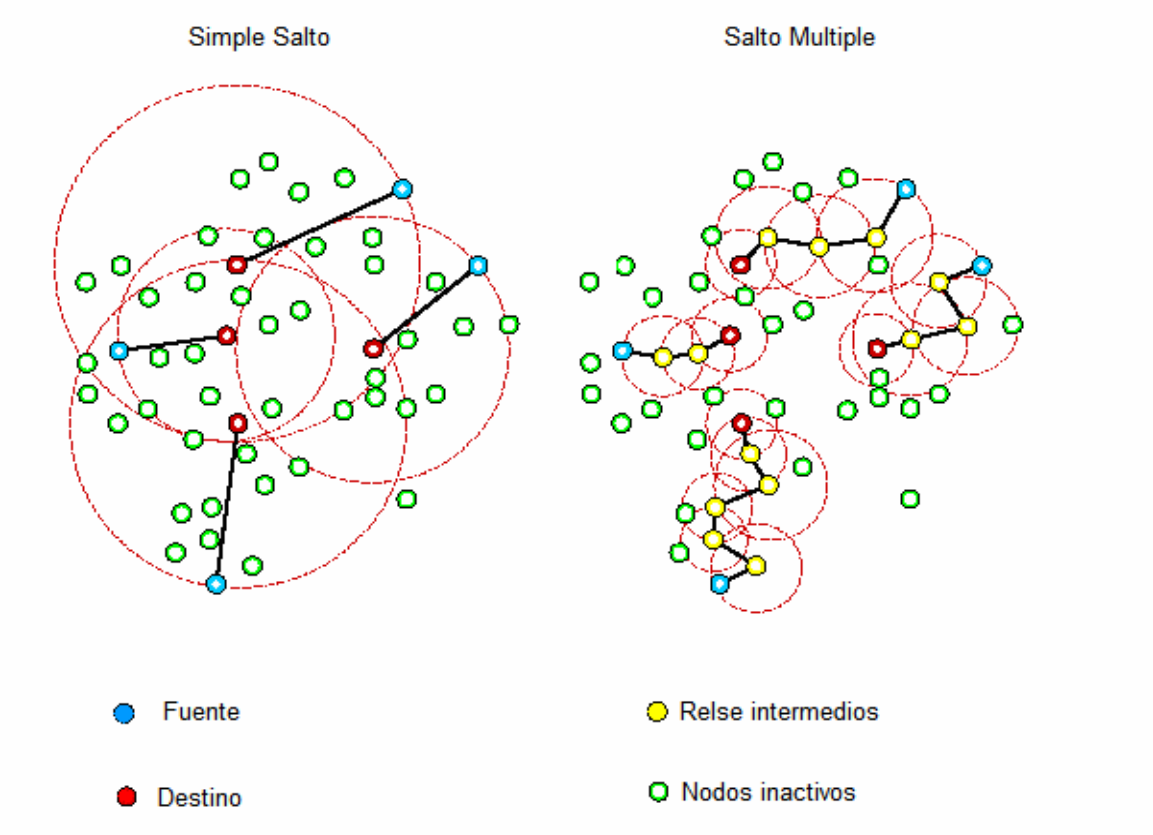


**Figura 1.3** La interferencia espacial

### 1.4.2 Comparación de saltos múltiples y saltos simples

Si el salto múltiple es necesario, adecuado o incluso posible, depende de factores tales como el número y la distribución de terminales en la red, la densidad relativa del tráfico, las características del canal de radio, las limitaciones prácticas de la comunicación, y las razones para la optimización de determinados parámetros. Bajo algunas circunstancias, una red de salto múltiple podría, en realidad, degenerar para convertirse en una de salto simple. Una razón obvia para emplear los saltos múltiples es proporcionar conectividad, ya que algunos terminales podrían estar fuera del alcance de los demás, y por lo tanto no podrían formar una red de salto simple.

## 1.5 Características del salto múltiple (reenvío)

En un escenario de salto múltiple, tiene sentido no desperdiciar más energía de la que cada salto requiere. En esencia, la clave para el ahorro de energía es controlar la potencia de transmisión, a fin de compensar las pérdidas del camino que se producen cuando se envía un mensaje entre nodos adyacentes.

### 1.5.1 Factor de reducción del consumo de energía ( $N^{\alpha-1}$ )

En un escenario de red con poco tráfico de datos, el consumo total de energía puede ser reducido en un factor aproximado de **(** $N^{\alpha-1}$ **),** donde $N$ es el número de saltos equidistantes entre la fuente y el destino, y α es la constante de propagación. En teoría, α es igual a 2 para la propagación libre en el espacio. Pero para entornos realistas, a menudo se le asigna un valor de 3 ó 4. Para derivar la relación, primero describimos la pérdida por propagación $L_{(db)}$ en términos de su relación con la distancia (D) [11] [21]:

$$L_{(db)} = K \times D^{\alpha} \qquad (1.1)$$

Para una correcta recepción a un nivel dado de ruido en el receptor, se requiere una mínima potencia de recepción $P_{(rx-\min)}$. De acuerdo con esto, la potencia de transmisión para un salto sobre una distancia D es, descrito de manera algo simplista:

$$P_{(tx-1)} = P_{(rx-\min)} \times K \times D^{\alpha} \qquad (1.2)$$

Si la distancia (D) se divide en *N* saltos, cada salto individual requiere:

$$P_{(tx-N)} = P_{(rx-MIN)} \times K \times \left(\frac{D}{N}\right)^{\alpha} \qquad (1.3)$$

Para N saltos totales:

$$P_{(tx-N-T)} = P_{(rx-\min)} \times K \times \left(\frac{D}{N}\right)^{\alpha} \times N \qquad (1.4)$$

Esto es un factor $N^{\alpha}$ menor que un salto simple. Por lo tanto, la reducción total de la potencia de transmisión de extremo a extremo es:

$$\frac{N^{\alpha}}{N} = N^{\alpha-1}$$

En este análisis, hemos excluido muchos factores perjudiciales, tales como distancias de salto desiguales, retransmisiones, y las características de los canales con desvanecimiento de la señal. Además, hemos supuesto un modelo muy simple de pérdida por propagación. No obstante, los resultados apuntan a un potencial ahorro de energía. Por ejemplo, comparado con el caso del salto simple, dados $\alpha$ = 3,5 y $N$ = 16, la energía teórica total de extremo a extremo por paquete se reduce 1.000 veces, ó 30 dB. Las malas noticias son

que en una red Ad-Hoc móvil la conectividad entre vecinos tiene que ser mantenida y la información de encaminamiento tiene que ser distribuida.

Por lo tanto, en situaciones de gran movilidad, el tráfico de control requerido en una red de salto múltiple podría consumir una notable cantidad de energía, incluso en ausencia de tráfico de datos.

Un beneficio directo de controlar la energía en las transmisiones de corto alcance es que ello puede reducir el nivel total de interferencia en una red de salto múltiple homogénea con múltiples nodos en comunicación y tráfico fijo. En una primera aproximación sin considerar la ubicación de la interferencia específica el nivel medio de interferencia se reduce en la misma cantidad que la energía de transmisión; esto es, en $N^{\alpha-1}$. Además, menos interferencia implica mayor capacidad del enlace. Dada una aplicación un poco cruda de la relación de Shannon de la capacidad de canal con ancho de banda limitado, y suponiendo que la interferencia esté bien modelada con ruido gausiano complejo, la capacidad individual del enlace aumenta para valores altos de N. Esto se muestra más abajo, donde B es el ancho de banda y $\left(\frac{S}{N}\right)$ es la relación señal - interferencia para un enlace en un sistema de salto simple de referencia que ha sido sustituido por un sistema de salto múltiple [11]:

$$C_{enlace} = B \times \lg_2\left(1 + \left(\frac{S}{N}\right) \times N^{\alpha-1}\right) \qquad (1.5)$$

El retardo de extremo a extremo depende del nivel al que se mida la latencia y del principio de reenvío aplicado. Un mensaje de tamaño razonable que se vaya a reenviar bajo la modalidad de almacenar y enviar (store and forward) experimentará un retardo que es proporcional al número de saltos. No obstante, este retardo está compensado en parte por un incremento en la tasa de datos del enlace.

La segmentación de mensajes grandes en múltiples paquetes afecta también al retardo de extremo a extremo. Mediante la segmentación del mensaje, varios paquetes pueden ser transferidos concurrentemente en saltos consecutivos. Bajo esas suposiciones, el retardo impuesto por múltiples saltos es pequeño en comparación con el retardo resultante de la

velocidad del enlace y del tamaño del mensaje. De hecho, el retardo de extremo a extremo podría en realidad beneficiarse de múltiples saltos. Debido a que el tráfico puede ser encaminado concurrentemente por múltiples enlaces en una "cadena multi salto," el reto es aliviar la interferencia asociada.

Obviamente, cuando la potencia de transmisión es limitada, podría no ser posible llegar a la estación deseada sin múltiples saltos. Por otra parte, debido a que el tamaño máximo de los mensajes es fijo, demasiados saltos aumentarán el retardo. Esto implica que un número *N* de saltos, puede proporcionar un retardo mínimo bajo restricciones de potencia de transmisión y un tamaño de mensaje dado.

En resumen, el salto múltiple es beneficioso, debido a que:

- ahorra los recursos de energía de transmisión.
- reduce la interferencia.
- aumenta el caudal total de la red.

El salto múltiple podría ser también una necesidad, para proporcionar algún tipo de conectividad entre terminales muy distantes.

### 1.6 El estándar IEEE 802.11

El estándar 802.11 del IEEE (El Instituto de Ingenieros Eléctricos y Electrónicos) es elmás usado de todos los estándares para LAN inalámbrico, debido a que supone la alternativa más viable y económica para proveer de servicio de red en ubicaciones en las que instalar el cableado para una red "convencional" es demasiado caro o difícil. Como todos los estándares incluidos en el grupo 802, especifica únicamente la capa física y la subcapa MAC, adaptada a las peculiaridades específicas del medio inalámbrico. Las interfaces ofrecidas por (802.11) a las capas superiores son los mismos que los que ofrecen los demás estándares 802.x. El objetivo de este estándar es proveer de conectividad inalámbrica a dispositivos inalámbricos, que pueden ser portables o estar instalados en vehículos móviles, y que necesiten el establecimiento rápido de conexión en red local. El estándar 802.11 también trata de guiar a las organizaciones responsables del

espectro radioeléctrico a estandarizar bandas de frecuencias para la comunicación de dispositivos en redes de área local vía radio. La capa MAC también debe ser capaz de tratar con varios tipos distintos de métodos de transmisión, como transmisión infrarroja o técnicas de espectro ensanchado.

IEEE 802.11, al contrario que otros estándares del IEEE 802, necesitó tomar en consideración el hecho de que debía soportar la movilidad de los nodos. Esto hizo que se tuviera que examinar el mantenimiento de la conexión, de los niveles de batería e incluso la provisión de seguridad. Según el estándar, las estaciones o terminales móviles (MT) tienen dos modos de operación, el modo infraestructura, donde las MT se pueden comunicar con puntos de acceso (AP) conectados a la WLAN, o el modo ad hoc, en el que los MT pueden comunicarse entre si directamente sin necesidad de AP.

### 1.6.1 Servicios ofrecidos por una red IEEE 802.11

Existen cuatro servicios, que son aportados por todos los nodos de la red, incluidos los AP:

- **Autenticación:** Este servicio es utilizado para establecer la identidad de cada estación. Es necesario debido a que solo los usuarios autenticados estarán autorizado a conectarse a la red, pero los esquemas de autenticación se basan en un intercambio de mensaje relativamente inseguro, ya que por defecto se suele usar un sistema abierto que suele desembocar en la autenticación de todas las estaciones que lo soliciten.
- **Desautenticación:** Termina una relación de autenticación, como lo define su nombre.
- **Privacidad:** En una red cableada, para acceder a la información, un atacante necesitaría obtener acceso físico al cable antes de intentar capturar tráfico. Sin embargo en una red de área local inalámbrica el acceso a la red es mucho mas fácil, ya que solo necesitaríamos usar la antena y los métodos de desmodulación correctos. Para evitar ese problema y proporcionar cierto nivel de privacidad,

802.11 proporciona un servicio basado en la encriptación de todas las comunicaciones mediante el servicio denominado WEP.

- **Reparto de datos:** Este es el servicio usado para transmitir y recibir datos, sin embargo, al igual que ethernet, no garantiza que la transmisión sea completamente fiable.

### 1.6.2 Grupos de trabajo 802.11

Para solucionar distintos aspectos de las redes de área local inalámbricas, el grupo de trabajo del IEEE encargado de éste estándar se ha dividido en varios subgrupos [9] [16], los cuales se mencionan a continuación:

- 802.11: Fue el primero de todos, y su objetivo era el desarrollo de las especificaciones de la subcapa MAC y los distintos niveles físicos necesarios para la comunicación sin cables de nodos en una red de área local, ya fueran estos fijos, móviles o portables. El primer estándar 802.11 fue publicado en 1997.
- 802.11a: Este grupo creó un estándar para WLAN en la banda de frecuencias de 5 GHz, donde es posible conseguir hasta 54 Mbps de velocidad. El estándar 802.11a fue ratificado en 1999.
- 802.11b: Este grupo de trabajo creó un estándar para redes de área local inalámbricas que funcionan en la banda de frecuencias ISM (Industrial, Científica y Médica) de 2,4 GHz, que está disponible para su uso libre en todo el mundo. Este estándar es popularmente conocido como Wi-Fi (Wireless Fidelity), y puede ofrecer hasta 11 Mbps. Este estándar fue publicado en 1999.
- 802.11c: Este grupo de trabajo desarrolla estándares para equipos que trabajan como puentes, y se utilizan en los puntos de acceso y puertas de enlace. El estándar fue publicado en 1998.
- 802.11d: El objetivo de este grupo es publicar definiciones y requerimientos de los sistemas necesarios para la operación del estándar 802.11 en países que no lo han adoptado como estándar. Fue publicado en 2001.

- 802.11e: Su objetivo es extender el estándar original para proveerlo de capacidades para la diferenciación de servicios y QoS. En Julio de 2005, el grupo 802.11e da por finalizado su trabajo en una reunión en San Francisco, California, y envía un borrador para ser aprobado y publicado al RevCom, que es el comité de revisión de estándares del IEEE (Standards Review Comitee). Aprobado en septiembre de 2005.
- 802.11f: Desarrolla especificaciones para la implementación de puntos de acceso y sistemas de distribución para evitar problemas de interoperatibilidad entre distintos fabricantes y distribuidores de equipos. Publicado en 2003.
- 802.11g: Este grupo de trabajo se encarga de ampliar el estándar 802.11b para que soporte transmisiones de alta velocidad, hasta 54 Mbps, en la misma banda de frecuencias de 802.11b y manteniendo la compatibilidad con éste. 802.11g utiliza multiplexación ortogonal con división de frecuencias (OFDM), al igual que 802.11a. Este estándar se publicó en 2003.
- 802.11h: Este estándar, publicado en 2003, fue desarrollado para hacer que la subcapa MAC cumpliera con las especificaciones en Europa para WLAN en la banda de 5 GHz, que requieren mecanismos de control de potencia transmitida y selección dinámica de frecuencias.
- 802.11i: Es un estándar para redes de área local inalámbricas que mejora la seguridad del estándar 802.11 mediante la introducción de sistemas de encriptación más potentes que el sistema WEP definido por el estándar. El nuevo sistema de encriptación se denomina TKIP. Fue ratificado en julio de 2004.
- 802.11j: Este grupo de trabajo adapta la subcapa MAC de 802.11 para que funcione en Japón en las nuevas bandas disponibles de 4.9 y 5 GHz.
- 802.11n: El objetivo de este grupo es definir las modificaciones necesarias en la capa MAC del estándar 802.11 para permitir modos de operación capaces de rendimientos (throughput) mucho mas altos, con máximos de al menos 100 Mbps mediante el uso del denominado MIMO (multiple-input multiple-output). El

trabajo de este grupo sigue en progreso en la fecha de redacción de este documento.

### 1.6.3 Capa física

IEEE 802.11 soporta tres medios distintos, uno basado en infrarrojo, y otros dos basados en transmisión radio. La capa física está conceptualmente dividida en dos partes, la subcapa dependiente del medio físico (PMD), y el protocolo de convergencia con el medio físico (PLCP). Mientras la primera de estas dos partes se encarga de la codificación, decodificación, modulación de las señales y todo lo que tenga que ver con el medio en particular usado, la segunda de estas partes abstrae la funcionalidad de la capa física que debe ofrecerse a la capa MAC. PLCP ofrece por tanto a la subcapa MAC los puntos de acceso al servicio (SAP) independientes de la tecnología de transmisión, además del sistema detector de portadora mediante CCA (Clear Channel Assesment). El SAP abstrae el canal, que podrá ofrecernos 1, 2 Mbps según el estándar original, o 11 o 54 Mbps según las normas 802.11b o 802.11a y g, respectivamente. El CCA es usado por la capa MAC para implementar el mecanismo CSMA/CA, que será explicado mas adelante. Las tres elecciones para la capa física definidas en el estándar original [4] son las siguientes:

- Espectro ensanchado por salto de frecuencias (FHSS) en la banda ISM de 2.4 GHz a 1Mbps (usando GFSK de dos niveles) y a 2 Mbps (con GFSK de 4 niveles).
- Espectro ensanchado por secuencia directa (DSSS) en la banda ISM de 2.4 GHz a 1 Mbps (usando DBPSK) y a 2 Mbps (con DQPSK).
- Infrarrojo en las longitudes de onda en el rango 850-950 nm a 1 y 2 Mbps usando un esquema de modulación por posición de pulsos (PPM, Pulse Position Modulation).

### 1.6.4 Subcapa MAC

MAC se define como subnivel inferior, provee el acceso compartido de las tarjetas de red al medio físico, es decir, define la forma en que se va a acceder al medio físico empleado en la red para el intercambio de datos. Las redes inalámbricas introducen diversos retos que se deben de superar. Entre estos se puede incluir el hecho de que los nodos inalámbricos deben de compartir el canal de radio como parte del proceso de comunicación. Por lo anterior en este tipo de medios de transmisión se tiene la desventaja de que hay una alta probabilidad de pérdida de paquetes, comparado con las redes cableadas. Además existe otro problema asociado a las redes inalámbricas como problema del nodo oculto [24]. El problema del nodo oculto se puede ejemplificar fácilmente cuando se consideran tres terminales A, B y C, donde A y C no pueden escucharse entre sí; el problema del nodo oculto se ilustra en la figura 1.4. Por otro lado, el nodo B escucha a las terminales A y C; por consiguiente si las terminales A y C tratan de transmitir al mismo tiempo hacia la terminal B se presentará una colisión de paquetes.

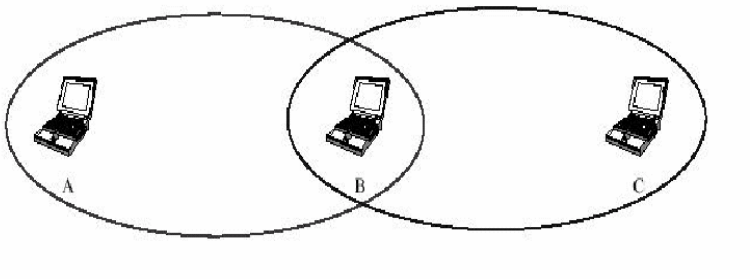


**Figura 1.4** Problema del nodo oculto

El principal método de acceso al medio en IEEE 802.11 se denomina Función de Coordinación Distribuida (DCF, Distributed Coordination Function), que es un mecanismo obligatorio según el estándar basado en una versión de CSMA/CA, que utiliza un mecanismo de intercambio de mensajes RTS-CTS (Request To Send – Clear To Send) para evitar el problema del "Terminal oculto" Hay un segundo método,

denominado Función de Punto de Coordinación (PCF, Point Coordination Function), que se usa para implementar el servicio de datos en tiempo real, en el que el AP controla el acceso al medio y evita la transmisión simultánea por parte de varios nodos. Este PCF, no puede usarse en redes ad hoc por motivos evidentes.

La subcapa DCF hace uso de un sencillo algoritmo MAC. Si una estación desea transmitir una trama MAC, escucha el medio. Si el medio se encuentra libre, la estación puede transmitir y sino debe esperar hasta que se haya completado la transmisión en curso, antes de poder transmitir. DCF no incluye una función de detección de colisión (es decir, CSMA/CD) puesto que la detección de colisión no resulta practica en redes inalámbricas. El rango dinámico de la señal en el medio es muy elevado, de manera que una estación que transmita no puede distinguir las señales débiles de entrada del ruido y de los efectos de su propia transmisión. Para asegurar el suave y correcto funcionamiento de este algoritmo, DCF hace uso de retardos conocido como espacio entre trama (IFS) [2] [7].

Haciendo uso de IFS [28], las reglas para acceso CSMA son:

- Una estación con una trama a transmitir sondea el medio. Si este esta libre, la estación espera para ver si el medio permanece libre durante un tiempo igual a IFS. Si es así, la estación puede transmitir inmediatamente.
- Si el medio esta ocupado (porque la estación encuentra inicialmente ocupado el medio o porque el medio es ocupado durante el tiempo IFS), la estación aplaza la transmisión y continua supervisando el medio hasta que la transmisión en curso haya finalizado.
- Una vez que esto ha ocurrido, la estación espera otro IFS. Si el medio permanece libre durante este periodo, la estación espera según un esquema de retroceso exponencial binario y sondea de nuevo el medio. Si el medio se encuentra aun libre la estación puede transmitir.

Como en Ethernet, la técnica de retroceso exponencial binario, proporciona un método para gestionar la red cuando tiene mucho trafico. Si una estación intenta transmitir y encuentra ocupado el medio, espera un cierto tiempo y lo intenta de nuevo. Sucesivos intentos de transmisión fallidos provocan tiempos de retroceso cada vez mayores.

El esquema se ha mejorado para que DCF proporcione un acceso basado en prioridades, simplemente mediante el uso de tres valores IFS [1] como se muestra en la figura 1.5, estos valores son:

- SIFS (IFS corto): el IFS más corto, usado para todas las acciones de respuesta inmediata.
- PIFS (función de coordinación puntual IFS): IFS de longitud intermedia, empleada por el controlador centralizado en el esquema PCF cuando realiza sondeos.
- DIFS (función de coordinación distribuida IFS): IFS mayor, utilizado como un retardo mínimo para tramas asíncronas que compiten para conseguir el acceso.

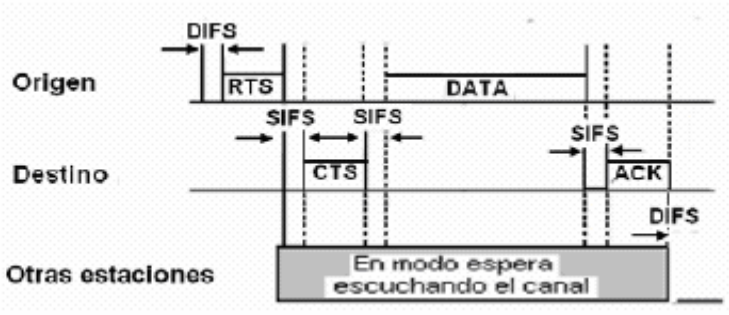


**Figura 1.5** Protocolo MAC en 802.11

### 1.6.4.1 Uso de confirmaciones

Las confirmaciones (ACK, acknowledgements) deben enviarse para asegurar el correcto reparto de paquetes en la red. Para paquetes que han sido enviados a un único destinatario (unicast), éste debe acceder al medio tras esperar un tiempo igual a SIFS y enviar el ACK. El resto de las estaciones deben esperar un tiempo igual a DIFS mas el tiempo de

retorno, reduciéndose así la probabilidad de colisión. Por tanto, los envíos de confirmaciones tras recibir un paquete de datos tendrán siempre mayor prioridad que una transmisión de un nuevo paquete de datos. Para asegurar la correcta recepción de una trama de la capa MAC, ACK usa un código de redundancia cíclica (CRC). Si no se recibe un ACK, se retransmite la información en cuestión. El número de retransmisiones posibles es limitado, y cuando dicho número alcanza su límite, se comunica el fallo a las capas superiores.

#### 1.6.4.2 RTS-CTS

La mayoría del tráfico utiliza el DCF, que utiliza el mecanismo RTS-CTS para evitar el problema del terminal oculto [8], que es uno de los principales problemas observados en redes inalámbricas. Este es un ejemplo clásico de los problemas que surgen al no tener información completa sobre la topología de la red remarcando la naturaleza no transitiva de la comunicación inalámbrica. En algunos casos, un nodo de la red puede recibir transmisiones de otros dos nodos que no pueden escucharse mutuamente entre sí. Esto implica que el receptor puede ser bombardeado por las transmisiones de los dos emisores a la vez, con la consecuente colisión y por tanto, reducción del rendimiento de la red. Los emisores, por su parte, al no poder oírse entre sí, tienen la impresión de que el receptor está listo para recibir, sin interferencias de ningún otro nodo.

Para evitar este problema, el emisor envía un mensaje de petición de envío (RTS, Request To Send) al receptor, Este mensaje incluye la dirección del receptor del siguiente paquete de datos y la duración estimada de toda la transmisión. Como este mensaje será escuchado por todos los nodos que estén en el área de cobertura del emisor, cada uno de ellos configurará un parámetro denominado NAV (Network Allocation Vector) consecuentemente. Este parámetro NAV, especifica en cada nodo el mínimo tiempo que debe esperar el nodo antes de intentar una transmisión. Tras esperar un tiempo SIFS, el receptor del RTS responde con un paquete listo para recibir (CTS, Clear To Send) si esta listo para recibir los datos. Este paquete CTS contiene un campo de duración, y todas los demás nodos de la red que reciban este CTS, reconfiguran sus NAV. Es obvio que las

estaciones que reciben el CTS pueden ser distintas al conjunto de nodos que reciben el RTS, debido a la presencia de terminales ocultos, tal y como se explicó anteriormente.

Una vez que se ha enviado el paquete RTS y que se ha recibido satisfactoriamente un mensaje CTS, se asume que todos los nodos dentro de las distancias de recepción tanto de emisor como del receptor de esta comunicación estarán advertidos de que el medio está reservado para esta comunicación ya en curso. Por tanto el emisor comenzará a enviar sus paquetes de datos tras esperar un tiempo SIFS. El receptor, tras recibir los datos, espera un nuevo tiempo SIFS y envía un ACK. Tan pronto como se termine la transmisión, el NAV de cada nodo marcará que el medio está libre y podrá repetirse el proceso de nuevo, a menos que mientras tanto se haya oído algún otro diálogo RTS/CTS.

El paquete RTS es como cualquier otro paquete, y se pueden dar colisiones sólo al principio del diálogo, cuando RTS o CTS están siendo mandados. Una vez que RTS o CTS se han enviado satisfactoriamente, como se ha explicado, el parámetro NAV evitará las colisiones. El uso del mecanismo de diálogo RTS/CTS antes del envío de datos se conoce como "detección virtual de portadora".

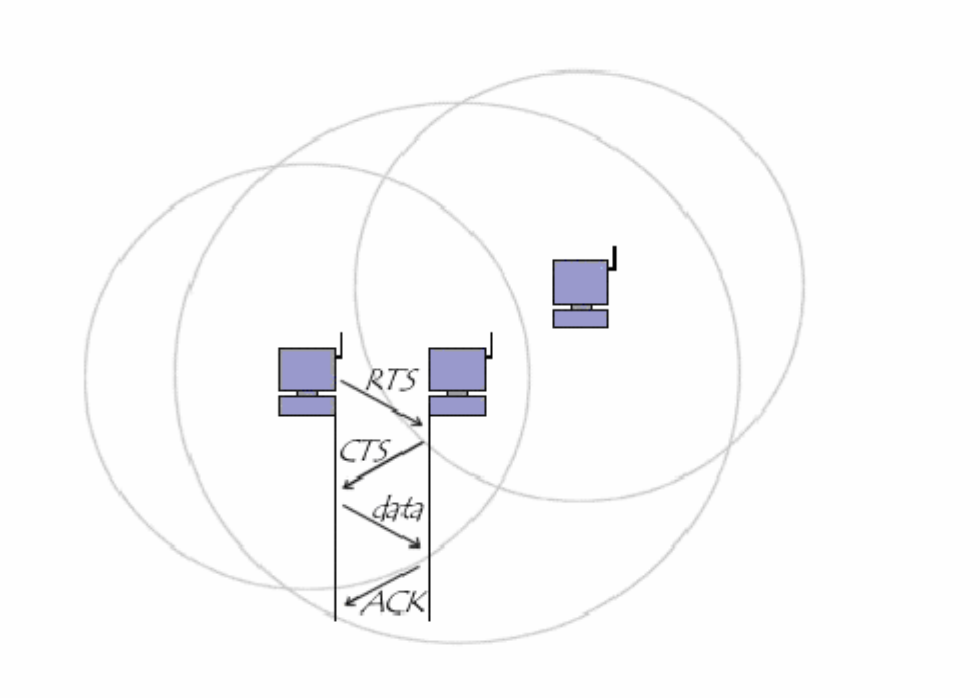


**Figura 1.6** Detección virtual de portadora

## 1.7 Conclusiones

Las redes inalámbricas introducen diversos retos que se deben de superar, pero por otro lado la tecnología inalámbrica facilita la instalación de redes de datos en diversos escenarios donde las redes cableadas no son factibles. Sin embargo, las redes inalámbricas de ningún modo pretenden reemplazar a las cableadas, ya que éstas pueden considerarse como el complemento ideal para extender los requerimientos de servicio que demandan los usuarios de hoy en día.

Debido a la movilidad de la red, los nodos pueden entrar y salir del alcance de otros nodos, por lo que la conectividad será parcial en el tiempo, o sea, la topología será dinámica y la conectividad no se garantiza siempre.

A pesar de las ventajas ofrecidas por las redes Ad-Hoc inalámbricas, su explotación comercial requiere soluciones realistas para diferentes problemas que se presentan en la práctica, como la provisión de calidad de servicio para aplicaciones en tiempo real, la tarificación de los servicios y la eficiencia de la energía.

Por ultimo, en el medio inalámbrico las tasas de error de bit son significativamente mayores que en el medio cableado. La transmisión de un nodo de una red inalámbrica se ve afectada por la transmisión simultánea de todos los nodos vecinos que se encuentran dentro del área de transmisión. Entonces, tenemos tasas de error típicas del orden de $10^{-4}$ en canales inalámbricos frente al $10^{-9}$ típico de un red de fibra óptica.

Todos estos factores implican que al ser el medio físico de redes inalámbricas peor que el cableado, el protocolo que controle el acceso al medio debería ser mucho más robusto para disipar todos estos inconvenientes.

# CAPÍTULO 2: TCP EN REDES INALÁMBRICAS

## 2.1 El protocolo TCP

TCP es un protocolo de redes de la capa de transporte, el cual ofrece un servicio estable de flujo de datos, orientado a conexiones. Es un protocolo duplex-completo, lo que significa que cada conexión de TCP le presta apoyo a un par de flujo de datos (byte streams), moviéndose en direcciones opuestas. El TCP acepta control de flujo de datos (flow control), lo que le impide al mensajero exceder la capacidad de la memoria intermedia (Buffer) del destinatario. Aún más, el TCP ejecuta control de congestiones (congestión control), lo que previene que el mensajero injecte demasiado tráfico en la red. El TCP es un protocolo de punto a punto (end-to-end). El TCP ha sido usado principalmente para redes alámbricas, así que ha sido afinado con ciertas suposiciones en mente. Por ejemplo, cuando un segmento de data se pierde, en una red alámbrica, es relativamente seguro suponer que se debe a congestión de la red (esto es, muchos segmentos están tratando de utilizar la red). Pero, si se trata de un vínculo inalámbrico o subred, la causa pudiera ser mala recepción en donde se encuentra el usuario [20].

Debemos saber que TCP sobre redes cableadas y sobre redes inalámbricas deberían trabajar en forma diferente. El primero da por supuesto que si no recibe un ACK (confirmación) por el paquete que envió, la red debe estar congestionada, y que el ruido presente en la red poco tuvo que ver con la no confirmación. Entonces en vez de reintentar a lo loco, lo que agravaría la congestión, se toma su tiempo. En cambio, sobre redes inalámbricas el ruido es la principal causa de pérdida de paquetes, por la naturaleza del canal. Al no recibir un ACK, TCP debería insistir lo antes posible. Entonces si se toma la misma filosofía que para redes cableadas, el rendimiento de la red inalámbrica se viene abajo [13].

Para obtener servicio de TCP, el emisor y el recibidor tienen que crear los puntos terminales de la conexión (los sockets). La dirección de un socket es la dirección de IP del host y un número de 16 bits que es local al host (la puerta). Se identifica una conexión

con las direcciones de socket de cada extremo; se puede usar un socket para conexiones múltiples a la vez [20].

### 2.1.1 Maquina de estado

El funcionamiento del TCP se explica mediante un modelo teórico denominado maquina de estado finito TCP [5]. En la figura 2.1, los círculos representan estados y las flechas transiciones entre los mismos, el nombre en cada transición muestra lo que recibe el TCP para generar esta transición y lo que envía como respuesta.

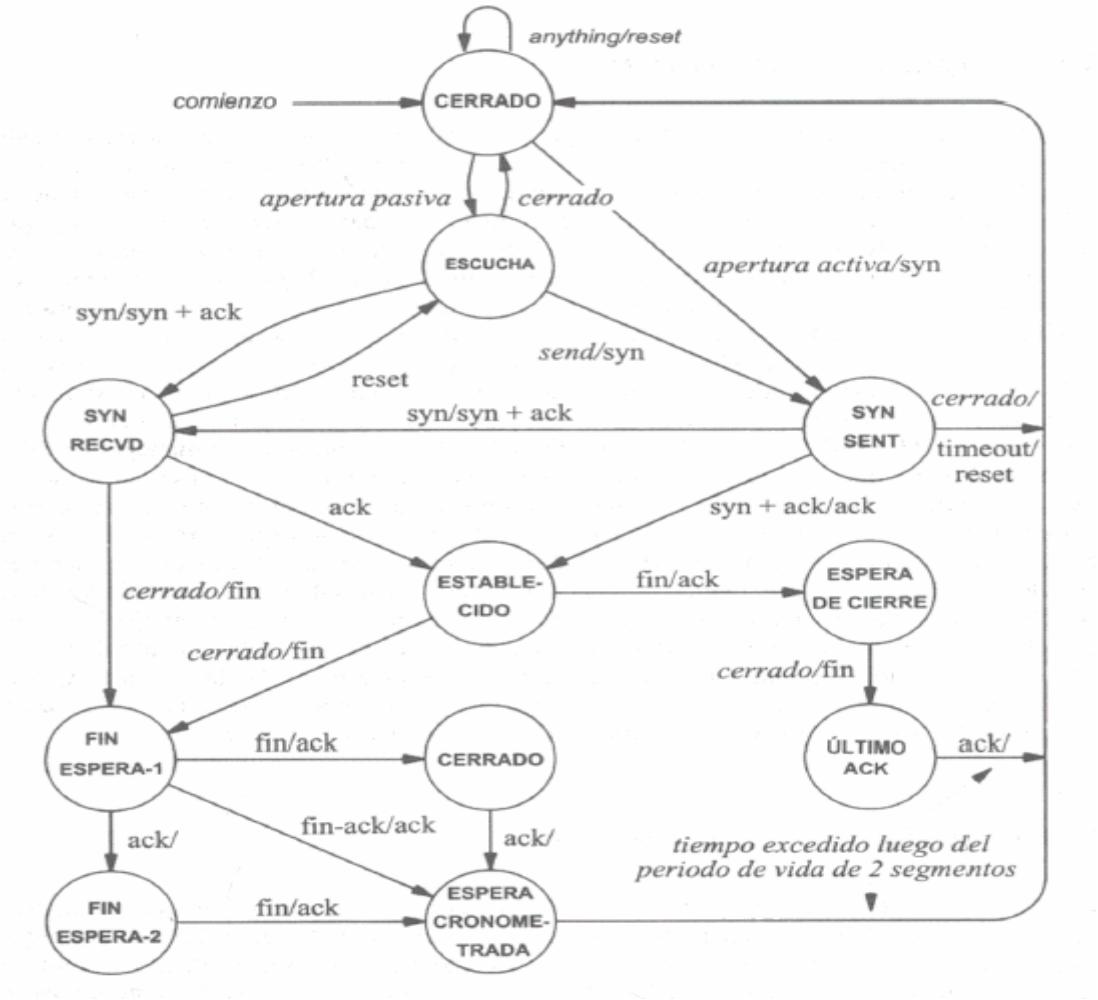


**Figura 2.1** Maquina de estado TCP.

Como habíamos dicho que el TCP es un protocolo orientado a conexión, el cual requiere que ambos puntos extremos de la conexión TCP estén de acuerdo en participar. Esto es antes de empezar una conexión, los programas de aplicación en ambos extremos deben estar de acuerdo en que desean dicha conexión. Primeramente el software TCP empieza en estado CERRADO en cada extremo, para esperar una conexión desde otra máquina se emite un comando APERTURA PASIVA contactando al sistema operativo e indicándole que aceptara una conexión entrante. El programa de aplicación del otro extremo debe contactar a su sistema operativo mediante una solicitud de APERTURA ACTIVA para establecer una conexión. El comando APERTURA ACTIVA provoca una transición del estado CERRADO al estado SYN SEND cuando TCP continúa con la transmisión emite un segmento SYN, si el otro extremo devuelve un segmento que contiene un SYN mas un ACK entonces TCP pasa al estado ESTABLECIDO y comienza la transferencia de datos.

El estado de ESPERA CRONOMETRADA revela como maneja TCP algunos de los problemas que se presentan con la entrega no confiable. TCP conserva una noción del máximo tiempo de vida del segmento, el tiempo máximo que un segmento puede mantenerse activo en la red. Para evitar la interferencia de segmentos de una conexión previa con los actuales, el TCP cambia al estado ESPERA CRONOMETRADA después de cerrar una conexión. Se mantiene en este estado dos veces el máximo tiempo de vida del segmento antes de borrar sus registros de la conexión. Si algún segmento duplicado logra llegar a la conexión durante el intervalo de exceso de tiempo, TCP lo rechazará. Sin embargo, para manejar casos cuyo último acuse de recibo fue perdido, reconocerá los segmentos válidos y reiniciará el temporizador. Dado que el temporizador permite distinguir entre conexiones anteriores y actuales, se evita que se responda con un RST (iniciación) si el otro extremo retransmite una solicitud FIN.

### 2.1.2 Características del TCP

La capa TCP incluye mecanismos para cumplir con el compromiso de fiabilidad. Éstos son:

- **Secuenciación:** el proceso emisor TCP divide los flujos en una secuencia de segmentos de datos que se transmiten como paquetes IP. A cada segmento TCP se

le asocia un número de secuencia. Proporciona el número de byte correspondiente al primer byte del segmento dentro del stream. El receptor utiliza los números de secuencia para ordenar los segmentos recibidos antes de colocarlos en el stream de entrada del proceso receptor. No puede colocarse ningún segmento en el flujo de entrada hasta que todos los segmentos con números de secuencia inferiores hayan sido recibidos y colocados en el stream, de modo que los segmentos que lleguen desordenados debe reposar en un búfer hasta que lleguen sus predecesores.

- **Control del flujo:** El emisor tiene cuidado de no saturar el receptor o a los nodos intermedio. Esto se consigue con un sistema de acuses de recibo por segmento. Siempre que el receptor envía al emisor un reconocimiento indicando el número de secuencia mayor de los recibidos junto con un tamaño de ventana. Si existe un flujo de datos inverso, los reconocimientos se incluyen en los segmentos de datos normales, en otro caso se transmiten como segmentos de reconocimiento. El campo de tamaño de ventana en el segmento de reconocimiento indica la cantidad de datos que el emisor tiene permiso para enviar antes del siguiente reconocimiento.

- **Retransmisión:** el emisor registra los números de secuencia de los segmentos que envía. Cuando recibe un reconocimiento asume que los segmentos aludidos han sido recibidos satisfactoriamente, por lo que pueden ser borrados de los búferes de salida. Cualquier segmento que no haya sido reconocido en un tiempo límite fijado, será retransmitido por el emisor.

- **Almacenamiento:** el búfer de entrada en el receptor se utiliza para equilibrar el flujo entre el emisor y el receptor. La información normalmente se extraerá del búfer antes de que éste se llene, aunque al final el búfer puede desbordarse y los segmentos entrantes serán desechados sin registrarse su llegada. Por lo tanto, su llegada no será reconocida y el emisor se verá obligado a retransmitirlos de nuevo [6].

## 2.2 Formato del segmento TCP

El segmento TCP es la unidad de transferencia entre el software TCP de dos maquinas. Estos se intercambian para establecer conexiones, transferir datos, enviar acuses de recibo, anunciar los tamaños de ventanas y para cerrar conexiones. El segmento TCP cumple con el siguiente formato:

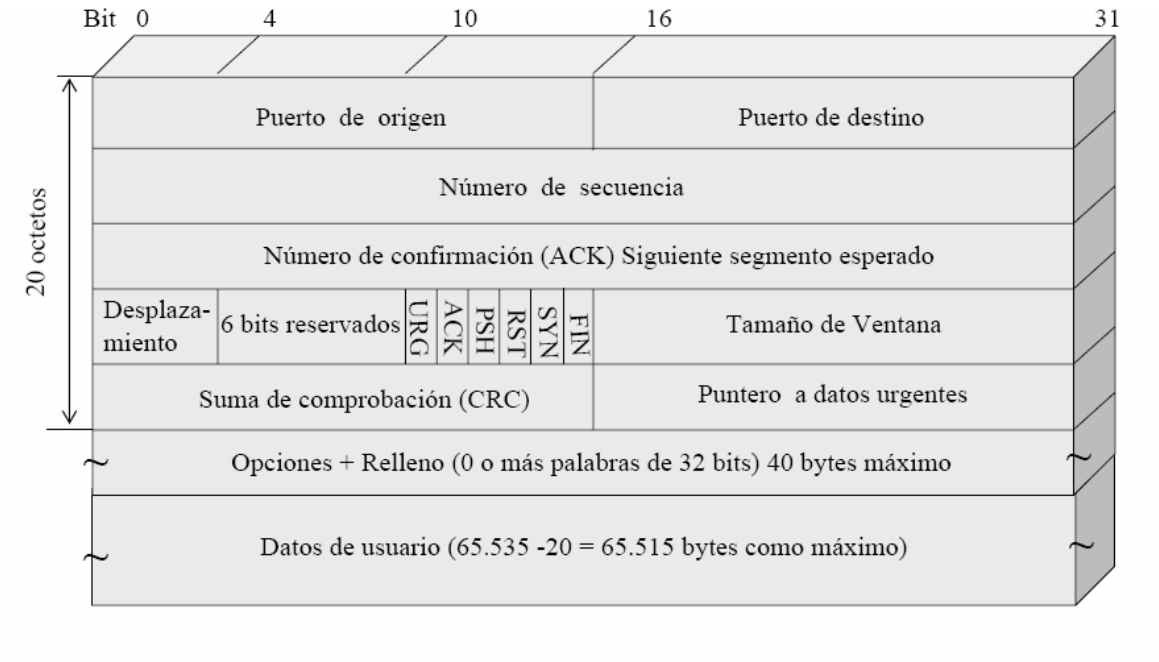


**Figura 2.2** Formato del segmento TCP.

Cada segmento TCP es un paquete de datos formado por una cabecera de 20 byte, una parte opcional de tamaño variable y datos [5]. En el encabezado se transportan la identificación y la información de control, los campos puerto de origin y puerto de destino contienen los números de puerto TCP que identifican los programas de aplicación en los extremos de la conexión. El campo número de secuencia identifica la posición de los datos del segmento en el flujo de datos del trasmisor. El campo de número de confirmación define el número de octetos que la fuente espera recibir después.

El campo desplazamiento o longitud de cabecera (4 bits) contiene un número entero que especifica la longitud del encabezado del segmento, en múltiplos de 32 bits, esto es necesario porque el campo opciones varía en su longitud dependiendo de las opciones que se hayan incluido y esto hace que el tamaño de la cabecera TCP dependa de las opciones seleccionadas. El campo de 6 bits reservado para mejorar el protocolo cuando sea necesario.

El campo code bits es un campo de 6 bits, que se usa para determinar el propósito y contenido del segmento. Estos bits indican como se debería interpretar los otros campos en el encabezado como se muestra en la siguiente tabla.

| Bit (de izquierda a derecha) | Significado si el bit esta puesto a 1 |
|---|---|
| URG | Indica el comienzo de los datos urgente |
| ACK | Indica que el numero de ACK es valido |
| PSH | Este segmento solicita una operación push |
| RST | Iniciación de la conexión |
| SYN | Para establecer conexión |
| FIN | Libera la conexión |

El campo ventana informa acerca del tamaño de la memoria intermedia (buffer), y la cantidad de byte que puede enviarse. Si la ventana tiene el valor cero quiere decir que se han recibido todos los bytes hasta número ACK-1 y el receptor no desea recibir más datos en este momento.

El campo suma de comprobación (CRC) es para lograr fiabilidad. Este es un CRC de la cabecera, los datos y la siguiente pseudo cabecera.

El campo opciones es para añadir características que no están cubiertas por la cabecera fija. Por ejemplo especificar la carga útil máxima que puede aceptar cada nodo.

## 2.3 Control de la congestión en TCP

TCP fue diseñado para trabajar con cualquier capa de enlace pero para redes inalámbricas se encuentra con bastantes problemas, uno de los problemas es el cuello de botella. TCP cuenta con cuatro algoritmos para el control de la congestión [14]: partida lenta, evasión de la congestión, retransmisión rápida y recuperación rápida.

### 2.3.1 Partida lenta y evación de congestión

La partida lenta y la evasión de la congestión son algoritmos usados para detectar el estado de la red y el control de flujo. La implementación de estos algoritmos requiere de dos parámetros de estado denominadas **cwnd** (ventana de congestión, que es utilizada para representar la mayor cantidad de datos que se pueden transmitir sin que se reciba confirmación) y **ssthresh** (umbral de partida lenta). Cuando TCP va a iniciar una transmisión en un medio desconocido lo hace de forma tal que no provoque congestión, debido a una ráfaga de datos mayor que la soportada por la red, para lograr esto cada nueva conexión TCP es iniciada con el envío de un segmento cuyo valor de **cwnd** (en bytes) es igual al valor de MSS (tamaño máximo del segmento), cada vez que se capta un acuse de recibo el valor de la ventana de congestión es incrementado en un MSS como se muestra en la figura 2.3. Esto equivale a decir que el valor de la ventana de congestión es doblado por cada RTT (viaje redondo). Una vez que el valor de **cwnd** supera al valor de **ssthresh** se pasa del mecanismo de partida lenta al de evasión de la congestión en el cual el valor de **cwnd** es incrementado aproximadamente en un segmento por cada RTT este mecanismo se sigue usando hasta que se detecte congestión.

Este algoritmo se trata de:

- Incrementar **cwnd** por cada RTT (incremento lineal)

- Dividir **cwnd** por dos cada vez que ocurre un time out (decremento multiplicativo) que será explicado mas adelante [22].

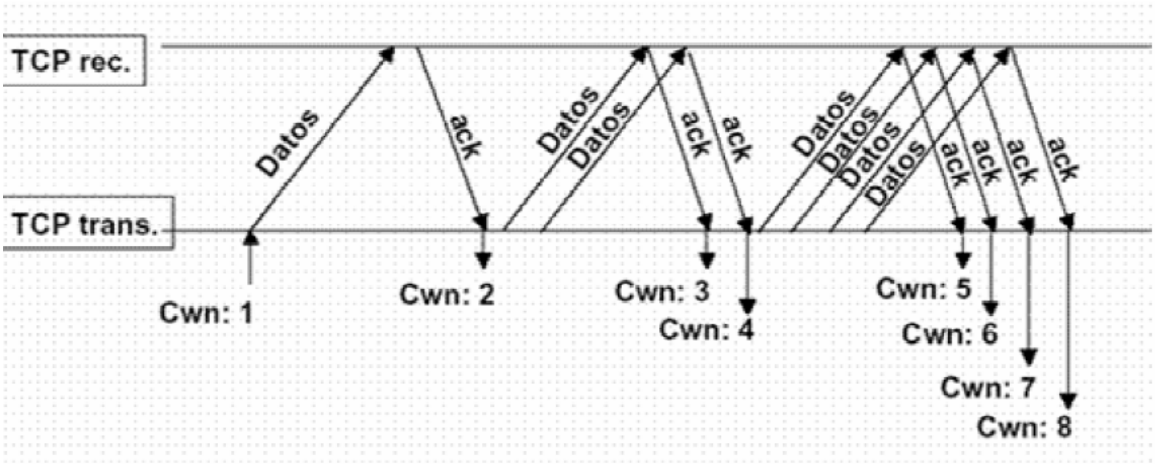


**Figura 2.3** Evolución del tamaño de ventana de congestión (CWND).

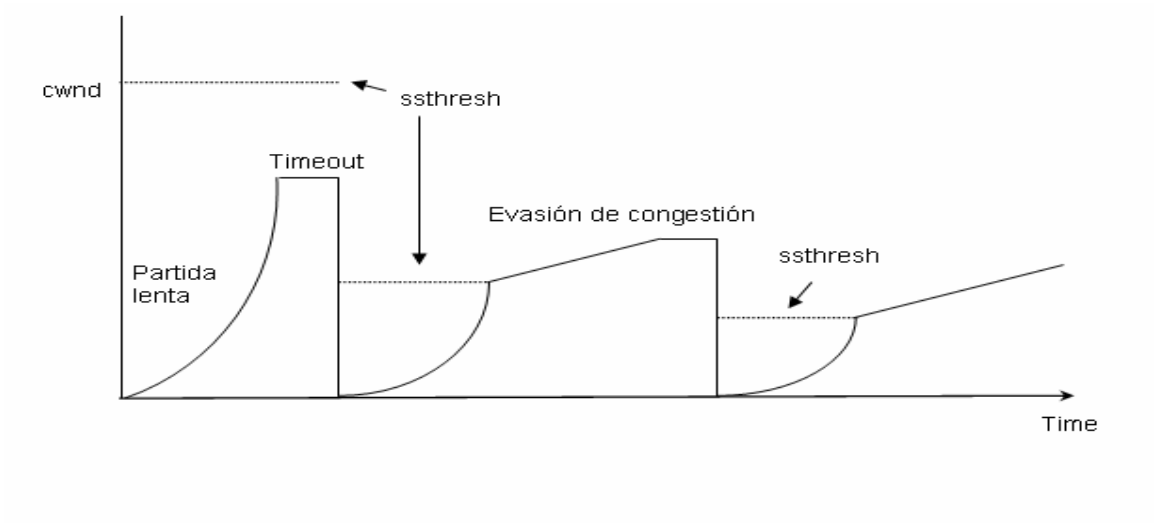


**Figura 2.4** Variación de la ventana de congestión.

En resumen:

Si **cwnd** ≤ **ssthresh** estamos en partida lenta

**cwnd** = **cwnd** + 1MSS (2.1)

Si **cwnd** > **ssthresh** estamos en evasión de congestión

$$cwnd = cwnd + \frac{(MSS)^2}{cwnd} \qquad (2.2)$$

Después de un time out

**ssthresh**= **cwnd** /2

**cwnd** =1 y se ejecuta la partida lenta.

### 2.3.2 Retransmisión rápida y recuperación rápida

La retransmisión rápida es un camino más eficiente para determinar las pérdidas antes de que termine el tiempo de vida del segmento. Está basado en el envió de **ACK** (acuses de recibo) duplicados (tres **ACK** idénticos) desde el receptor para indicar la presencia de segmentos fuera de orden. Cuando este mecanismo detecta una pérdida se utiliza la recuperación rápida para controlar la transmisión durante el tiempo que demore la recuperación de la pérdida, luego que este proceso termina, el trasmisor reduce a la mitad el valor de la ventana de congestión y reinicia el mecanismo de evasión de la congestión en lugar de pasar al de arranque lento.


**Figura 2.5** Comportamiento de CWND.

## 2.4 Redes Ad-Hoc y TCP

Todas las redes inalámbricas, tienen ciertas características como alta latencia, alta pérdida de paquetes y ancho de banda variable, que plantean conflictos a las capacidades del protocolo TCP.

### 2.4.1 Problemas en redes Ad-Hoc

Los problemas que aparecen en este tipo de red se pueden clasificar en 4 categorías:

- **Errores del canal**
- **Efectos de contención en el acceso al medio**
- **Efectos producidos por la movilidad de los nodos de conmutación**
- **Efectos producidos por rutado mutitrayecto**

**Errores del canal:**

Son causado por ruido electromagnético, interferencia, y desvanecimiento y la consecuencia de dicho problema es que los bits que componen un paquete se reciben de forma errónea.

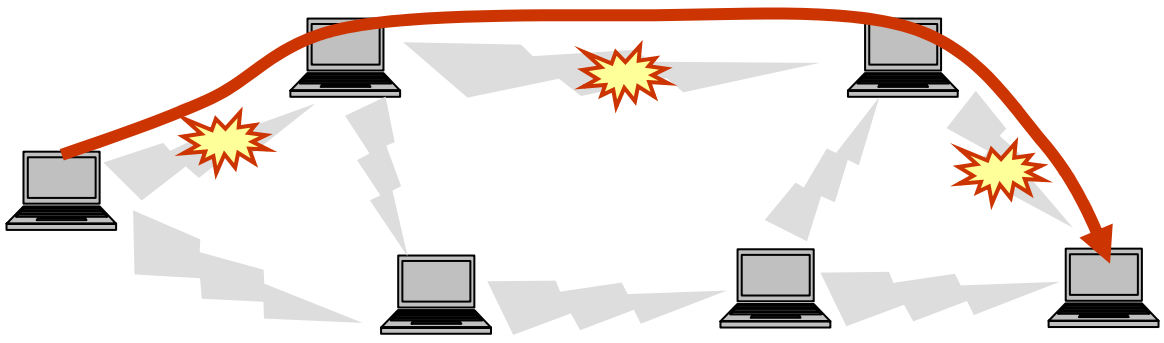

**Figura 2.6** Errores del canal.

Efectos en TCP: Los paquetes se pierden, se agotan RTOs, se activan los mecanismos de control de congestión, las prestaciones se deterioran enormemente.

**Efectos de contención en el acceso al medio:**

Como sabemos que los mecanismo de la subcapa MAC no evitan la aparición de colisión ni el reparto injusto de los recursos de transmisión, causando la perdida de los paquetes o la demora de estos en ser transmitido.

Ejemplos de este problema son el terminal oculto y terminal expuesto [24]:

Terminal oculto: es un nodo que esta en el rango de interferencia con el receptor, pero fuera del rango de sensibilidad con el emisor. Este terminal produce colisión con los paquetes del emisor.

Terminal expuesto: un nodo que está en el rango de sensibilidad del emisor, pero fuera del rango de interferencia del receptor. Este terminal no puede mandar sus paquetes aunque no molestarían a nadie.


**Figura 2.7** Problemas del Terminal oculto y Terminal expuesto.

Efectos en TCP: Los paquetes se pierden, se agotan RTOs, se activan los mecanismos de control de congestión, las prestaciones se deterioran enormemente.

**Efectos producidos por la movilidad:**

Son causadas por la movilidad de los nodos de conmutación, causando así que la ruta se rompa [12], y la necesidad de encontrar otro camino.

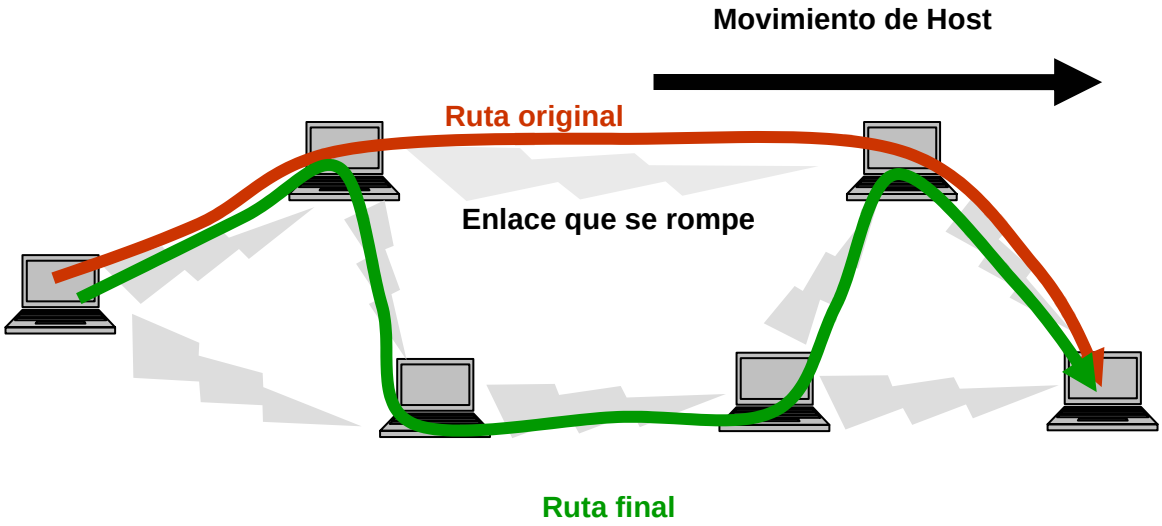


**Figura 2.8** Problemas por la movilidad.

Efectos en TCP: Mientras se encuentra una nueva ruta o se resuelve una partición de red, se agotan RTOs, se activan los mecanismos de control de congestión, las prestaciones se deterioran enormemente

**Efectos producidos por rutado multitrayecto:**

Los paquetes viajan por rutas diferentes y como consecuencia de eso los paquetes se desordenan y tienen latencia poco uniforme.

Efecto en TCP: Se reciben ACKs duplicados, se activan los mecanismos de control de congestión, las prestaciones se deterioran.

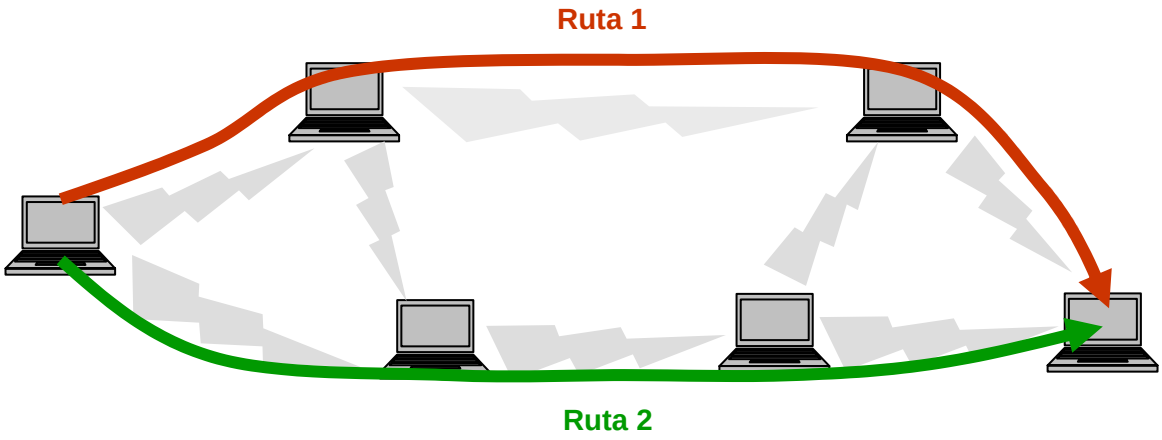


**Figura 2.9** Problemas del rutado multitrayecto.

### 2.4.2 Soluciones propuestas para estos problemas

**Soluciones basada en modificar el nivel de enlace:**

Si se pierde un paquete en el salto inalámbrico, hay que esperar un RTO completo para poder retransmitirlo. Para eso el nivel de enlace implementa un protocolo fiable. Se usan dos técnicas para ofrecer fiabilidad al protocolo de enlace, que contribuyen a evitar que la capa de enlace de datos afecte el comportamiento de TCP utilizando un tamaño de ventana de control de flujo pequeño, lo cual afectaría a la capa de transporte. Las técnicas en cuestión son:

- Solicitud automática (ARQ): cuando el receptor detecte un paquete con errores irrecuperable, envía de forma instantánea una solicitud de retransmisión de los mismos.

- Corrección de errores (FEC): consiste en añadir información redundante sobre los paquetes de forma que sea posible recuperarlos incluso cuando se hayan producido errores en la recepción de algunos bits. Cuanto más información redundante, más errores se pueden recuperar y menos retransmisiones serán necesarias y por lo tanto menor ancho de banda estará disponible. Se recomienda la utilización de códigos correctores de errores en enlace inalámbricos con el fine de mejorar la razón de error de bit en el canal para resguardar de esta forma a TCP de la falsas señales de congestión.

**Soluciones con retroalimentación:**

La retroalimentación (feedback) consiste en que la red informe a las entidades TCP sobre el estado de la red en el caso que haya una congestión o una ruptura de ruta, así las entidades de TCP podrán conocer con mayor precisión el estado de la red [10].

Ejemplos de retroalimentación:

- ECN: Este mecanismo permite que un emisor TCP detecte la presencia de congestión independientemente de que haya, o no, pérdida de paquetes y podrá detener la congestión antes de que los efectos de esta se hagan explicita (pérdida de paquete, aumento de latencia, etc.)
- ICMP: este mensaje avisa una ruptura de ruta, La desventaja de este mecanismo es que puede provocar una demora adicional antes de que TCP este listo para enviar los datos.

Protocolos que se basan en retroalimentación [27]:

- TCP-F (TCP-Feedback): cuando se detecta un fallo en una ruta, se informa de manera explícita al emisor. Este congela el estado de la conexión hasta que se reciba una notificación explícita de que la ruta restablecida.
- TCP-ELFN (TCP-Explicit Link Failure Notification): Se informa la ruptura de una ruta, pero es el emisor que se ocupa de averiguar cuando la ruta se ha establecido enviando sondas periódicas.

- ATCP (Ad hoc TCP): Utiliza mecanismos estándar de notificación: ECN, ICMP, etc. Es compatible con "TCPs normales". Sólo realiza control de congestión mediante ECN, congelando el estado si una ruta se rompe.

**Soluciones sin retroalimentación:**

Se basa en modificar el comportamiento de TCP. Las ideas básicas son:

Garantizar que el tamaño de la ventana de congestión permanezca moderado, de forma que no se fuerce a la red a entrar en congestión (producto ancho de banda retardo de propagación), y tratar de detectar cambios en la topología de enrutado a través de los paquetes que llegan fuera de orden.

Protocolos que utilizan esas ideas son [10]:

- Adaptive congestion window limit setting
- TCP- Door
- Fixed RTO

# CAPÍTULO 3: SIMULACIONES EN REDES Ad-Hoc

## 3.1 Introducción

A pesar de todos los problemas que sufre el protocolo TCP en las aplicaciones inalámbricas como ruido del canal, el efecto de la movilidad de los nodos y el efecto de contención en la capa MAC, este protocolo se clasifica como el mejor para los clientes del estándar 802.11. El problema básico de este protocolo es cuando TCP detecta congestión, reduce su ventana de congestión a la mitad. La solución para estos problemas es usar el protocolo TCP-friendly (amigable), basado en el protocolo TCP-Reno que usa los cuatro algoritmos explicados en el capitulo 2 para el control de congestión. Este protocolo usa un modelo matemático desarrollando un análisis simple de la razón de transmisión en un flujo TCP, en función de la razón de pérdidas de paquetes y la RTT (Tiempo de ida y vuelta). Este modelo se basa en capturar el comportamiento del mecanismo de la retransmisión rápida, y el efecto del mecanismo de tiempo agotado (Time out).

## 3.2 Desarrollo del modelo

El comportamiento del mecanismo de evasión de congestión está modelado en términos de ciclos. Un ciclo empieza con la transmisión de W paquetes de extremo a extremo, donde W es el tamaño de la ventana de congestión (cwnd). Una vez mandados estos paquetes, la fuente transmisora TCP deja de mandar hasta recibir la primera confirmación (ACK) de uno de estos paquetes, marcando así la terminación de este ciclo y la iniciación del próximo ciclo. En este modelo el valor de cada ciclo es igual al RTT e independiente del tamaño de la ventana. En el próximo ciclo, un grupo de paquetes W' van a ser mandados, donde W' es el tamaño de la nueva ventana.

Durante la evasión de congestión y en la ausencia de pérdida, el tamaño de la ventana aumenta linealmente con el tiempo, con una razón de 1/b, donde b es el número de paquetes confirmado con la recepción de los ACK (típicamente 2), esto es:

- si en el primer ciclo fueron mandados W paquetes y confirmados correctamente, entonces W/b ACKs van a ser recibidos.
- Puesto que cada ACK aumenta en tamaño por 1/W, el tamaño de la ventana al iniciar el segundo ciclo va a ser W'= W+ 1/b.

Hay que tener en cuenta que:

- La duración del ciclo es independiente del tamaño de la ventana.
- El tiempo necesario para mandar los paquetes es menor que la RTT.
- En caso de la pérdida de un paquete, todos los paquetes mandados en este ciclo van a ser perdidos (tail drop).

## 3.3 Indicaciones de pérdidas

Existen dos métodos para la indicación de pérdida, uno basado en la recepción de los ACKs duplicado (3 ACK idéntico) desde el receptor, y el otro es el efecto del tiempo agotado (Time out) debido a demora de los ACK.

### 3.3.1 Indicación de pérdida del tipo ACK duplicado (TD)

El periodo TD (TDP) se va a definir como el periodo entre dos indicaciones de pérdida del tipo TD. Entre las indicaciones de dos TD, estamos en evasión de congestión y la ventana aumenta con una razón de 1/b.

Para el i-ésimo TDP:

1 Yi = # de paquetes mandados en este periodo.

2 Ai = la duración del periodo.

3 Wi = tamaño de la ventana al final del periodo.

Teniendo en cuenta esos parámetros, la razón de transmisión se puede definir como [19]:

$$B = \frac{E[Y]}{E[A]} \qquad (3.1)$$

TDP empieza de inmediato después de la indicación de perdida de TD, entonces la ventana de congestión va a ser igual a W(i-1)/2, la mitad del tamaño de la ventana antes que ocurra esa indicación de pérdida. Al final de cada ciclo la ventana es incrementada por 1/b y el número de paquetes es incrementado en uno cada b ciclo.

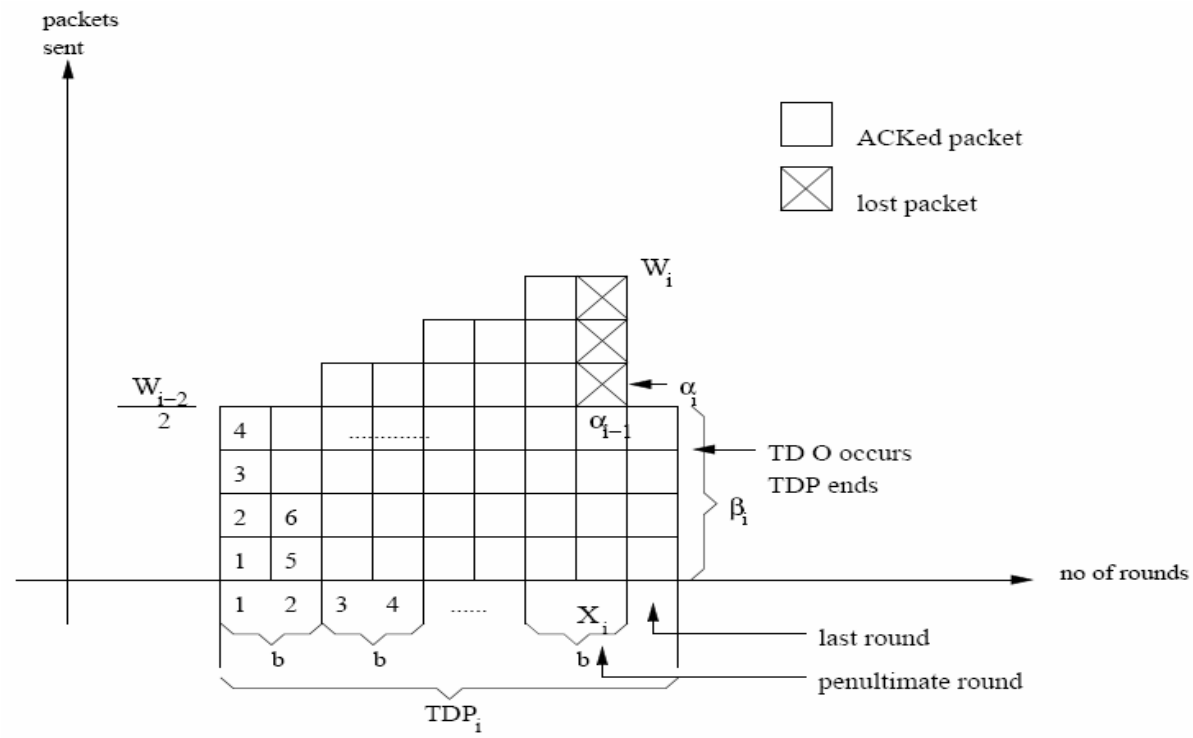


**Figura 3.1** paquetes mandados durante TDP.

Si definimos αi como el primer paquete perdido en el TDPi y Xi como el ciclo donde ocurrió esa pérdida como se muestra en la figura 3.1, después de αi, más paquetes van a ser mandados en un ciclo adicional antes que ocurra la indicación de la pérdida y se termina este TDP. Entonces tenemos un número total de Yi = αi + (Wi) – 1.

El número de paquetes se puede definir como:

$$E[Y] = E[\alpha] + E[W] - 1 \qquad (3.2)$$

Asumiendo que todos los paquetes que se pierden en un ciclo son independientes de los paquetes perdidos en el otro ciclo, y la probabilidad de que αi= K es igual a la probabilidad de que exactamente K-1 paquetes fueron confirmado entonces:

$$P[\alpha = \mathrm{K}] = (1-P)^{K-1} P, \qquad \mathrm{K}=1,2,\ldots \qquad (3.3)$$

$$E[\alpha] = \sum_{K=1}^{\infty} (1-P)^{K-1} PK = \frac{1}{P} \qquad (3.4)$$

Combinando (3.2) y (3.4) tenemos:

$$E[Y] = \frac{1-P}{P} + E[W] \qquad (3.5)$$

Ahora tenemos que derivar E[W] y E[A], para esto consideramos de nuevo un TDPi, y definimos Rij como la duración (RTT) del j-ésimo ciclo del TDPi. Considerando Rij una variable independiente del tamaño de la ventana y del número de ciclos.

La duración del TDPi [17] seria:

$$Ai = \sum_{J=1}^{Xi+1} Rij$$

$$E[A] = (E[X]+1)E[r] \qquad E[r] = RTT$$

$$E[A] = (E[X]+1)RTT \qquad (3.6)$$

Ahora si analizamos la evolución de W en función del número de ciclos como se muestra en la figura 3.1 entonces tenemos que:

$$Wi = \frac{W_{i-1}}{2} + \frac{Xi}{b} \qquad i=1,2,... \qquad (3.7)$$

$$E[W] = \frac{2}{b} E[X] \qquad (3.8)$$

Yi se define como:

$$Yi = \sum_{k=0}^{Xi/b-1} \left( \frac{W_{i-1}}{2} + K \right) b + \beta i$$

$$= \frac{Xi}{2} \left( \frac{W_{i-1}}{2} Wi - 1 \right) + \beta i \qquad (3.9)$$

Donde $\beta i$ es el número de paquetes mandados en el último ciclo.

Combinando (3.8) y (3.5) tenemos:

$$\frac{1-P}{P} + E[W] = \frac{E[X]}{2} \left( \frac{E[W]}{2} + E[W] - 1 \right) + E[\beta] \qquad (3.10)$$

Como sabemos que $\beta i$ , es el número de paquetes mandados en el último ciclo está distribuido uniformemente entre 1 y Wi entonces $E[\beta] = \frac{E[\beta]}{2}$

Combinando (3.10) y (3.8) tenemos:

$$E[W] = \frac{2+b}{3b} + \sqrt{\frac{8(1-p)}{3bp} + \left(\frac{2+b}{3b}\right)^2} \qquad (3.11)$$

Combinando (3.8) y (3.11) tendremos que:

$$E[X] = \frac{2+b}{6}\sqrt{\frac{2b(1-p)}{3p} + \left(\frac{2+b}{6}\right)^2} \qquad (3.12)$$

Combinando (3.6) y (3.12) tendremos que:

$$E[A] = RTT\left(\frac{2+b}{6} + \sqrt{\frac{2b(1-p)}{3p} + \left(\frac{2+b}{6}\right)^2} + 1\right) \qquad (3.13)$$

Ahora para hallar la relación de la razón de transmisión desde la ecuación (3.1) y (3.5)

$$B(p) = \frac{\frac{1-p}{p} + E[W]}{E[A]} \qquad (3.14)$$

Sustituyendo E[W] y E[A] tendremos que:

$$B(p) \approx \frac{1}{RTT}\sqrt{\frac{3}{2bp}} \qquad (3.15)$$

Aquí en este análisis no se tomó en cuenta el efecto del tiempo agotado (time out) que se explicará más adelante.

### 3.3.2 Indicación de pérdida incluyendo el tiempo agotado

La degradación del tamaño de la ventana se ve afectado por el efecto del tiempo agotado más que de la retransmisión rápida, entonces para un buen modelo se deben capturar las indicaciones del tiempo agotado. Esto ocurre en caso de que los paquetes de confirmación (ACKs) se pierden, y tampoco son recibidos los ACKs duplicados. El transmisor espera un tiempo denotado como T0, y luego retransmite los paquetes que no fueron confirmados. Después de un tiempo agotado, la ventana se reduce por uno, y un solo paquete está resentido en el primer ciclo después del tiempo agotado. En caso de que ocurra otro T0 antes de la retransmisión de los paquetes perdidos en el primer tiempo agotado, el periodo del tiempo agotado se dobla a un valor igual a $2T_0$, este proceso es repetido hasta que llegue a $64T_0$, después de este valor el periodo del tiempo agotado se mantiene constante.

En la figura 3.2 se nota la evolución del tamaño de la ventana incluyendo la indicación de pérdida debido al triple ACK y el efecto del tiempo agotado donde:

- $Z_i^{TD}$ denota el intervalo de tiempo dos TO consecutivo.
- $Z_i^{T0}$ denota la duración del TO.

Como sabemos que la definición del periodo TD (TDP) ocurre entre dos indicaciones de pérdidas de TD, también si incluimos el T0, este TDP empieza después la indicación de pérdida debido al TD y termina con la indicación de pérdida debido al TO.

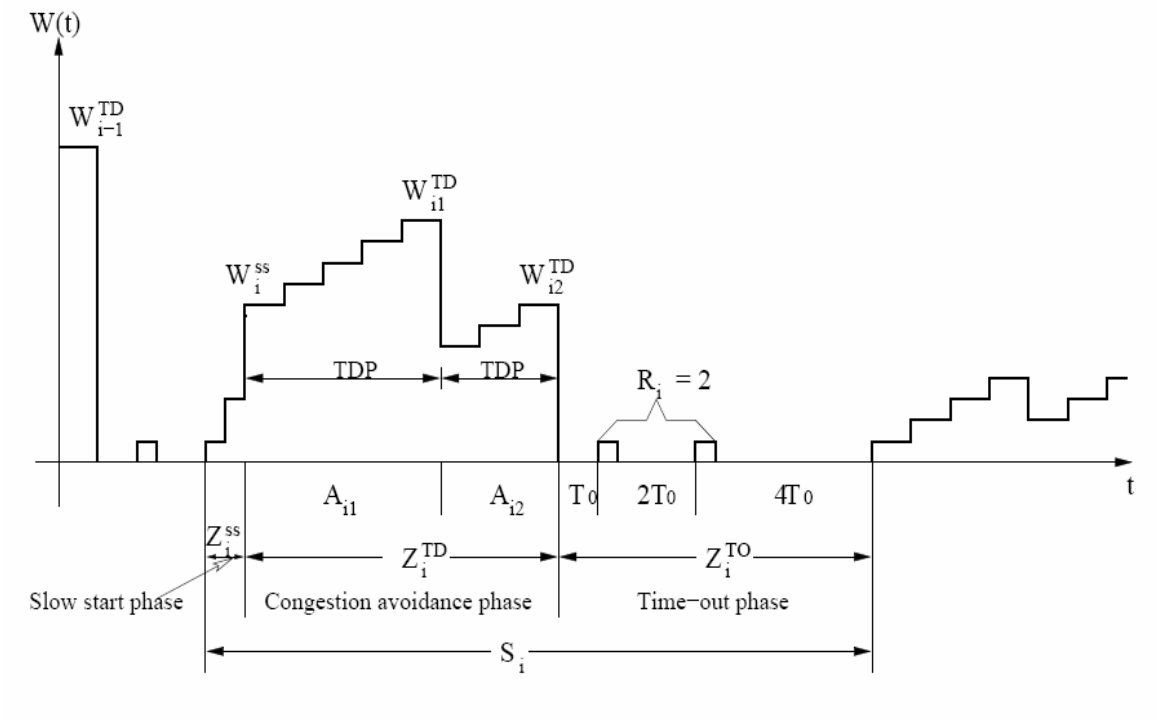


**Figura 3.2** Evolución del tamaño de la ventana incluyendo los TD y TO

Después de un análisis matemático [17] [19] se llega a la expresión final del modelo TCP-friendly para calcular la razón de transmisión:

$$B(p) \approx \frac{1}{RTT\sqrt{\frac{2bp}{3}} + T0\min\left(1{,}3\sqrt{\frac{3bp}{8}}\right)p\left(1+32p^2\right)} \qquad (3.16)$$

Donde la primera parte en el denominador $RTT\sqrt{\frac{2bp}{3}}$ representa el efecto del TD, mientras el resto del denominador representa el efecto del tiempo agotado.

### 3.4 Aplicaciones en el MATLAB

Partiendo de la ecuación (3.16) se hizo un programa en el MATLAB, llamado tcpanalisis, que nos permite analizar el comportamiento de este modelo TCP-friendly en este tipo de redes y el comportamiento de la ventana con respeto a las indicaciones de pérdidas.

#### 3.4.1 Descripción del programa

Como este programa se trata de analizar el comportamiento del tamaño de ventana contra la probabilidad de pérdida de paquetes, entonces primero tenemos que sacar una relación entre el tamaño de la ventana y la razón de transmisión. Para eso tenemos que:

W= B(p)*RTT

También definimos a K como una constante para hacer la variación de T0, donde:

T0=k*RTT y luego definimos $\alpha$=1/b, donde $\alpha$ va a ser el incremento de la ventana al final de cada ciclo.

Entonces el tamaño de la ventana sería:

$$W = \frac{1}{\sqrt{\frac{2p}{3\alpha}} + K \min\left(1{,}3\sqrt{\frac{3p}{8\alpha}}\right) p\left(1 + 32\,p^2\right)} \qquad (3.17)$$

Mediante esa función en el MATLAB, se pueden entregar los parámetros de entrada que deseamos analizar. Esos parámetros serian:

1. Pmin, Pmax, P, para saber la probabilidad mínima y la máxima que se va a analizar y por ultimo P para saber el rango entre dos probabilidades, o sea la resolución.
2. $\alpha$, K, RTT

3. C, donde C va a ser la capacidad del enlace, y wbits que va a definir el tamaño de la ventana en bits.

Entregando estos parámetros como entrada, el programa hará tres análisis, un primer análisis que analiza el comportamiento del tamaño de la ventana contra la probabilidad de pérdida de paquetes (W vs P). Un segundo análisis para ver el comportamiento de la razón de transmisión contra la probabilidad de pérdida de paquetes (B(p) vs P) y Un tercer análisis va a ser para la capacidad del enlace. Como se sabe que la razón de transmisión va a ser: $\min\left(\frac{W_{\max}}{RTT}, C\right)$, donde C representa la capacidad del enlace.

### 3.4.2 Resultado del análisis

En un primer análisis, se tomará como datos de entrada:

- La probabilidad de pérdida de paquetes varía desde 0.001 hasta 0.14 con un rango de 0.0001 entre dos probabilidades.
- b = 2 (valor típico), o sea $\alpha$ =0.5, K=1segundo, RTT= 200ms, C=1024kb/s (1Mbps), y por último, para analizar el tamaño de la ventana, hay que saber que, según la especificación de la IEEE 802.11, la MTU toma como valor máximo 2276 bytes [15] sin la necesidad de fragmentación en la capa MAC, y el umbral de fragmentación en la capa MAC es 2312 bytes. Aquí se toma la MSS = 536 bytes y W=5 segmentos, entonces la wbits=21440 bits.

A continuación se verán los resultados de este análisis:

En la figura 3.3 se muestra el comportamiento de la ventana con respeto a la probabilidad de pérdida de paquete, según (3.17) se nota la degradación de la pérdida de paquete al aumentar el tamaño de la ventana.

En la figura 3.4 se analiza el comportamiento de la razón de transmisión B(p) con respeto a la pérdida de paquete con una degradación de la misma, mientras mayor sea la razón de transmisión y dependiendo del valor de RTT.

En la figura 3.5 se analiza el comportamiento de la razón de transmisión con respeto a la capacidad del enlace, mientras $\frac{W\max}{RTT}$ sea mayor que la capacidad del enlace, se mantiene constante hasta que la probabilidad de pérdida llega a un punto p = 0.0076 que empieza a trabajar a la capacidad de la razón de transmisión.

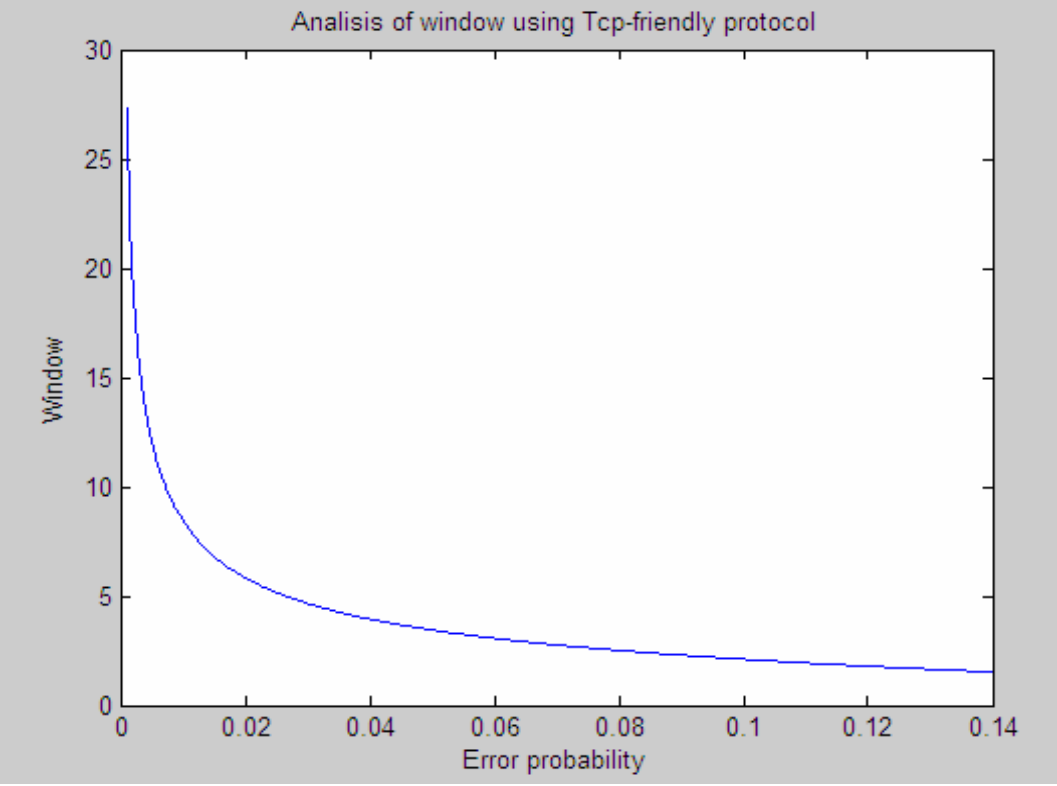


**Figura 3.3** Comportamiento de la ventana vs la probabilidad de perdida de paquete.

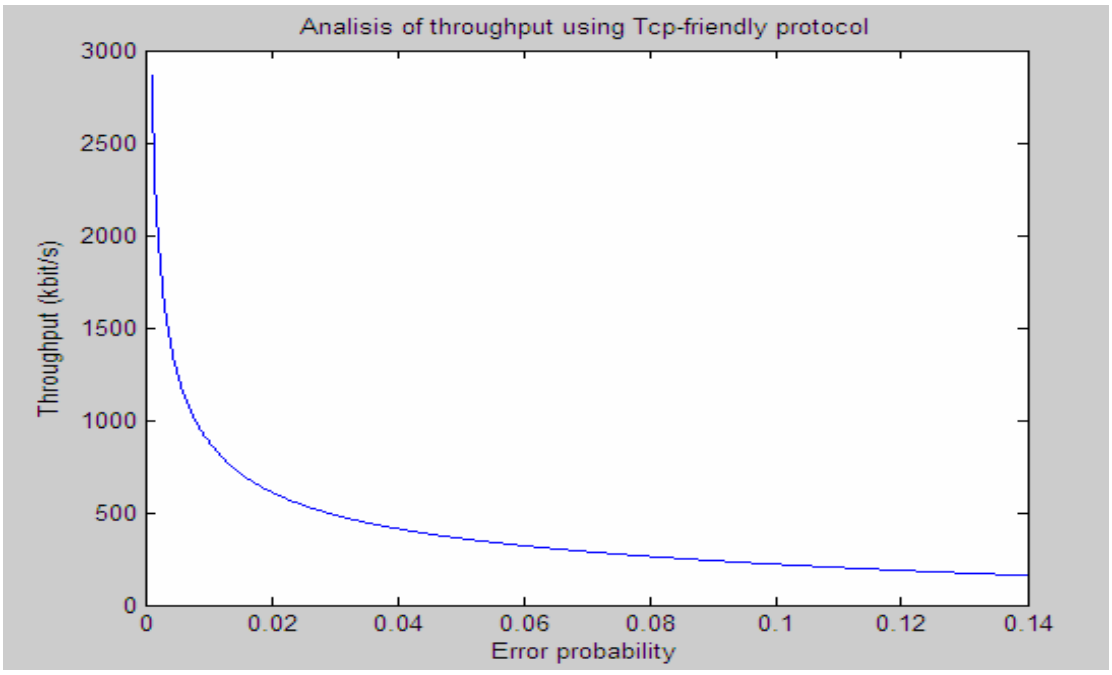


Figura 3.4 Comportamiento de la razón de transmisión B(p)

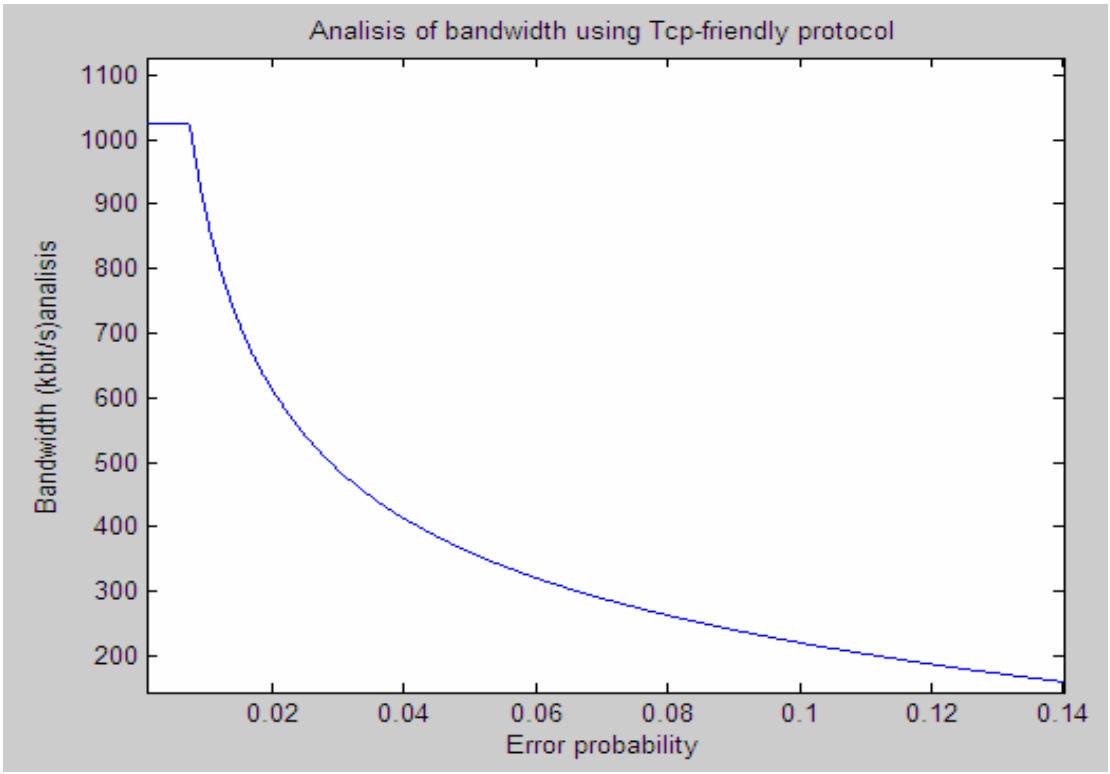


**Figura 3.5** Comportamiento de B(P) vs la capacidad del enlace

En un segundo análisis se dedicará a la indicación de pérdida del tiempo agotado (TO), para valores de K=0 (o sea sin incluir el TO), y para k=2. Con este análisis se observa que la degradación del tamaño de la ventana es más afectado por el tiempo agotado que la indicación de los ACKs.

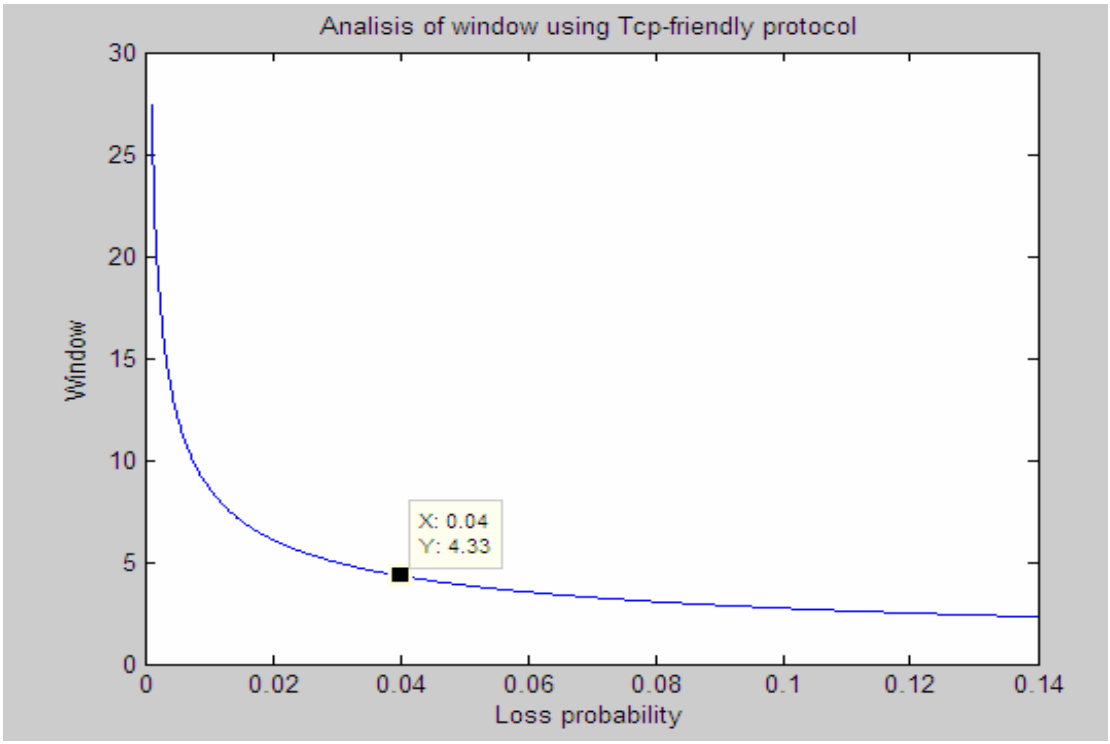


**Figura 3.6** Análisis de la ventana con k=0.

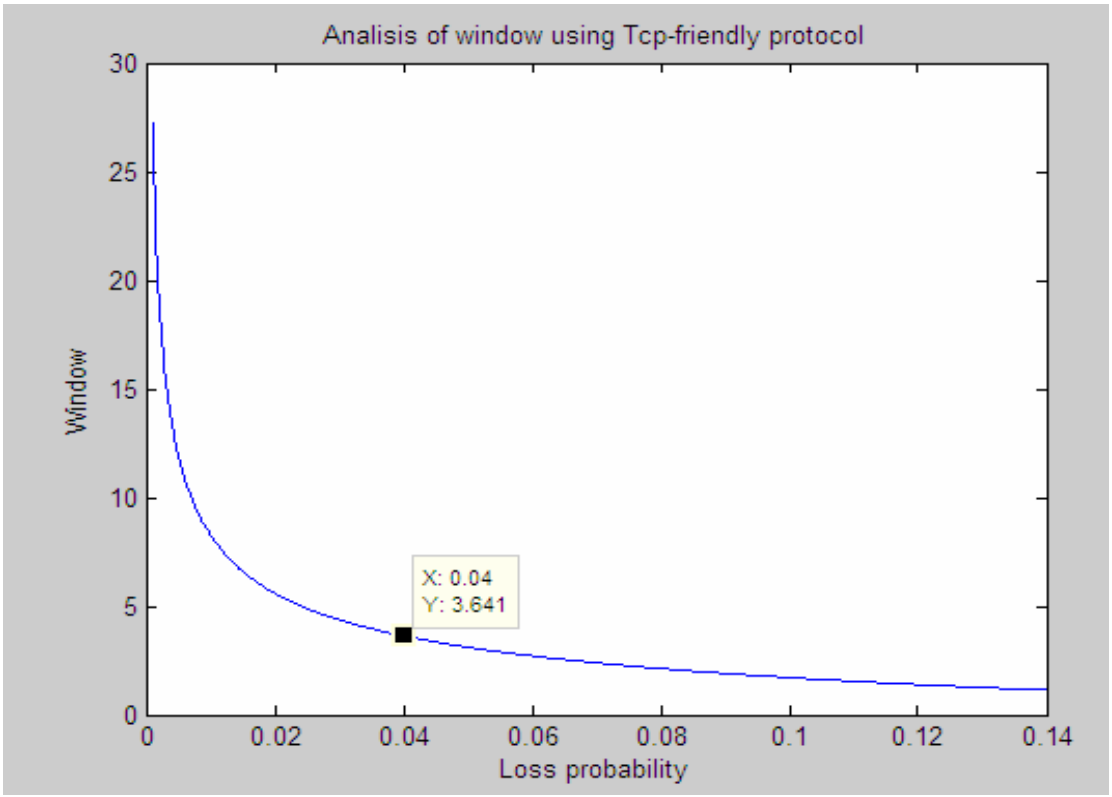


**Figura 3.7** Análisis de la ventana con K=2.

En un tercer análisis se cambiaran los valores de la ventana W de 5 segmentos hasta 20 segmentos, así wbits sería igual a 85760 bits, lo que significa que la razón de transmisión $\frac{W\max}{RTT}$, se mantendría por arriba de la capacidad del canal por mas tiempo comparado con la figura 3.5 hasta un umbral de pérdida de paquetes igual a 0.0832, que empieza a trabajar a la capacidad de la razón de transmisión como se ve en la figura 3.8.

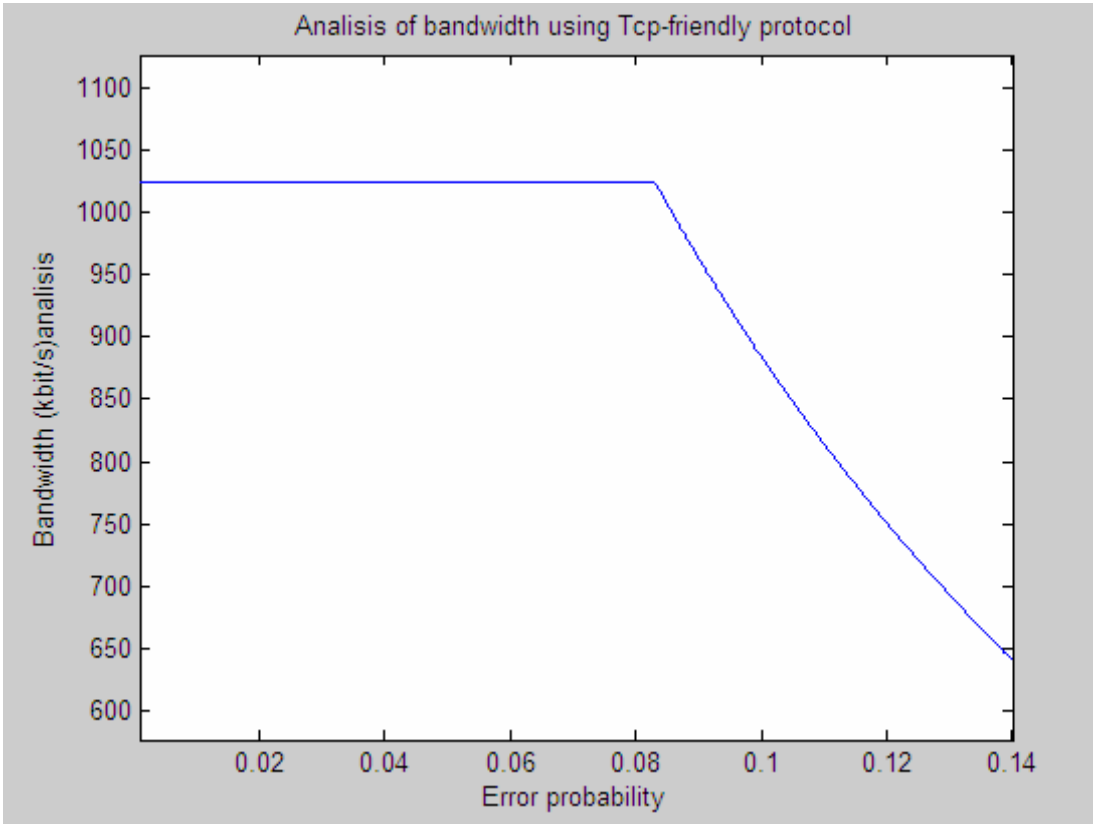


**Figura 3.8** Comportamiento de la razón de transmisión para valores mayores de W

# CONCLUSIONES Y RECOMENDACIONES

En este trabajo se realizó un detallado análisis del protocolo TCP en las redes inalámbricas Ad-Hoc, para lo cual se tuvo en cuenta la extensa bibliografía técnica disponible en Internet. Luego de analizar los resultados obtenidos en el presente trabajo se llegó a las siguientes conclusiones:

1. El protocolo TCP queda como mejor propuesta para este tipo de redes y específicamente los basados en TCP-Reno que a diferencia de otras versiones de TCP, éstos usan los algoritmos de recuperación rápida cuando reciben las indicaciones de pérdida de paquete (3 ACKs duplicado) y no se ingresa en la partida lenta sino en evasión de congestión.
2. El conocimiento de todos los parámetros de la ecuación TCP-Friendly son necesarios para entender el comportamiento de cada uno de éstos, así como realizar correctamente el análisis.
3. El programa demuestra que los efectos del tiempo agotado son las principales causas de la degradación del tamaño de ventana.

Dada la enorme importancia que pueden llegar a tener las comunicaciones inalámbricas y en especial las redes Ad-Hoc, y debido a que estas redes están en constante desarrollo, seria necesario seguir profundizando en su análisis, así como la búsqueda de información sobre este tema como:

1. Los protocolos de encaminamientos tales como: AODV, DSR, TORA.
2. Los nuevos protocolos de acceso al medio como DQCA AD HOC que fue especificado para redes en modo Ad-Hoc.

# REFERENCIAS BIBLIOGRÁFICAS

[1] Aladrén, M, Bueno, D, " DIFERENCIACIÓN DE SERVICIOS POR CLASE EN REDES INALÁMBRICAS", disponible en: http://w3.iec.csic.es/ursi/articulos_coruna_2003/actas_pdf/SESION%204/S4.%20Aula%202.5/1029-DIFERENCIACION.PDF, Última visita: abril del 2007.

[2] Bastidas, C, "Estudio de la fractalidad del tráfico en redes Ad-hoc sobre WLAN", 2006, disponible en: https://upcommons.upc.edu/pfc/bitstream/2099.1/3799/1/53936-1.pdf, Última visita: 24 de abril del 2007.

[3] Berto, R, "Como montar una red inalámbrica", 2001, disponible en: http://www.todo-linux.com/manual.todo linux.com/redes/Inalambrico%20COMO%20%20Montar%20Red%20Inalambrica.pdf, Última visita: 6 de junio del 2007.

[4] Cano, J, " Redes de Área Local", 2003, disponible en: http://www.redes.upv.es/ralfi/ficheros/presentaciones/06%20Inalambricas%20802-11.pdf, Última visita: 24 de mayo del 2007.

[5] Comer, D, "REDES GLOBAES de INFORMACION con INTERNET y TCP/IP, 1ra parte, 2005.

[6] David, I, "REDES E INTERCONEXIÓN DE REDES", 2001, disponible en: http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/REDES02.htm, Última visita: 22 de abril del 2007.

[7] Delgadillo, S, Guzmán, D, Muller, A y Grote, W, "ANALISIS EXPERIMENTAL DE UN AMBIENTE WI-FI MULTICELDA", Rev. Fac. Ing. –Univ. Tarapacá, Vol. 13, No. 3, p. 45-52, 2005.

[8] Embid, J y Peirón, J, "Estándar IEEE para redes inalámbricas", 2002, disponible en: http://webdiis.unizar.es/~chus/san/trabajos/7-802.11.PDF, Última visita: 24 de abril del 2007.

[9] Estrada, A, " Seguridad en WIFI", 2005, disponible en: http://www.redes.upv.es/ralfi/ficheros/presentaciones/06%20Inalambricas%20802-11.pdf, Última visita: 25 de mayo del 2007.

[10] Fernandez, L, "Protocolo de transporte en redes inalambricas", 2006, disponible en: http://gsyc.escet.urjc.es/moodle/file.php/26/Transparencias/TcpWireless.ppt, Última visita: 22 de abril del 2007.

[11] Frodigh, M, Johansson, P y Larsson, P, "Formación de redes inalámbricas ad hoc—El arte de la formación de redes sin red", Ericsson Review No.4, 2000.

[12] Goff, T, Abu-Ghazaleh, B y Phatak, S, "Analysis of TCP on Ad Hoc Network", disponible en: http://cs.binghamton.edu/~nael/research/papers/icpp01, Última visita: 17 de mayo del 2007.

[13] González, R, "TCP sobre redes inalámbricas", 2006, disponible en: http://www.lugmen.org.ar/pipermail/lug-novatos/2006-June/006455.html, Última visita: 24 de abril del 2007.

[14] Holland, G y Vaidya, N, "TCP Performance over Ad Hoc", 2002, disponible en: http://www.cs.ualberta.ca/~yaser/presentations/tcpadhoc.ppt nuevo, Última visita: 25 de mayo del 2007.

[15] Kawadia, V y Kumar, R, "Experimental Investigation into TCP Performance over wireless Multihop Network", journal SIGCOMM ' 05, 2005.

[16] Kreft, A, "Redes Inalambricas", 2003, disponible en: http://www.pc-news.com/detalle.asp?sid=&id=4&Ida=1270, Última visita: 26 de mayo del 2007.

[17] Lung, J, "Modeling TCP Throughput", 1999, disponible en: http://webtp.eecs.berkeley.edu/meetings/Throughput.ppt, Última visita: 25 de mayo del 2007.

[18] Ortiz, F, "El estándar IEEE 802.11 Wireless LAN", disponible en: http://greco.dit.upm.es/~david/TAR/trabajos2002/08-802.11 Francisco-Lopez-Ortiz-res.pdf, Última visita: 24 de abril del 2007.

[19] Padhye, J, Firoiu, V, Towsley, D y Krusoe, J, "Modeling TCP Throughput: Simple Model and its Empirical Validation", journal "Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication", p. 303-314, 1998, disponible en: http://www.cs.umass.edu/Dienst/Repository/2.0/Body/ncs, Última visita: 25 de mayo del 2007.

[20] Pentikousis, K, "Podrá Ser El TCP El Protocolo De Transporte Del Siglo 21?", 2000, disponible en: http://www.acm.org/crossroads/espanol/xrds7-2/tcp21.html, Última visita: 24 de abril del 2007.

[21] Reigadas, F, Fernández, A y Moran, F, "Implementación de IEEE802.11 en enlaces largos para zonas rurales aisladas", 2005, Disponible en: http://cita2006.mty.itesm.mx/ponencias/Implementacion%20de%20IEEE%20802.11%20en%20enlaces%20largos%20para%20zonas%20rurales%20aisladas.pdf, Última visita: 24 mayo del 2007.

[22] Semke, J, Mahdavi, J y Mathis, M, "The Macroscopic Behavior of the TCP Congestion Avoidance Algorithm", ACM Computer Communication Review, Volume: 27, Issue: 3, July 1997.

[23] Segarra, J, "Sistemas Distribuidos y Redes de Computadoras", Doctorado en ingenería de sistemas e informática, Universidad de Zaragoza, España, 2005.

[24] Vassis, D y Kormentzaz, G, " Performance analysis of IEE802.11 ad hoc network in the presence of hidden terminal", journal of computer network, Vol. 13, issue 9, P. 2345-2352, 20 JUNIO 2007.

[25] Velarde, L, Lujan, L, Medina, L y García, F, "Simulación y Evaluación de las prestaciones de una Red Ad Hoc Inalámbrica en un Campus Universitario con Trafico de Datos en Tiempo Real y No Real con el Modelo Swan", disponible en: http://itdelicias.edu.mx/Paginas/Sistemas/Luis/PonenciaSWAN.pdf , Última visita: 12 de abril del 2007.

[26] Vidal, I, García, C, Soto, I y Moreno, J, "Servicios de ValorAñadido en Redes Móviles Ad-hoc", disponible en: http://www.it.uc3m.es/ividal/articulos/telecom03_adhoc.pdf, Última visita: 2l de abril de 2007.

[27] Wang, F y Zhsng, Y, "Improving TCP performance over Mobile Ad-Hoc Networks with out of order Detection and Response", 2002, disponible en: http://www.cs.ucla.edu/classes/fall03/cs218/paper/mobilhoc, Última visita: 17 de mayo del 2007.

[28] Zárate, J, Ramos, I, Kartsakli, E, Verikoukis, C y Alonso,L, "Evaluación de Algoritmos Cross-Layer para la Optimización de Sistemas de Comunicaciones Inalámbricas en modo Ad Hoc", disponible en: http://www.telecomid.com/anteriores/2006/trabajosdefinitivos2006/Programa_archivos/pdf/8.pdf, Última visita: 17 de mayo del 2007.

# Anexos A: Programa en el MATLAB

**Aquí se muestra el programa hecho en el MATLAB 7.0 y cabe señalar que para buscar la ayuda en el MATLAB 7.0 que es de gran importancia para poder trabajar con el programa o sea conocer los parámetros que les entra, sólo hace falta escribir la expresión help filename y ahí sale.**

```
function [y,t,razont,B,pr]=tcpanalisis(pmin,pmax,p,alfa,k,RTT,c,wbits);
%tcpanalisis generates  vectors y,t,razont,B,and pr given the minimum
%probability and the maximum probability that u like to analize and also
%the range between the 2 probabilites and given also alfa and k and RTT and
%c and wbits where these parameters are defined down.
%FORMAT:
%[y,t,razont,B,pr]=tcpanalisis(pmin,pmax,p,alfa,k,RTT,c,wbits);
%INPUTS:
%pmin = is the minumum loss probabiliy of a packet that you like to analize.
%pmax = is the maximum loss probabiliy of a packet that you like to analize.
%p = is the range that you like to be between two probabilites.
%k= constant, where To=K*RTT
%alfa = 1/b, where b is the delayed ACK.
%RTT = Round trip time.
%c = link capacity
%wbit=  window size en bits
%OUTPUTS:
%y = returns the vector of calculating the window of all values of
%probabilites between pmin and pmax.
%t = returns the vector of all probabilites that have been analized.
%razont = throughput
%pr=  threshold for probability
%PLOTS:
%(t,y) - Representation of loss probability vs Window
%(t,razont) - Representation of loss probability vs Throughput
%(t,B) - Representation of loss probability vs Bandwidth
e=pmin:p:pmax;
y = zeros(1,length(e));
j =1;
```

```
for i =pmin:p:pmax
     w(j)=1/(sqrt(2/(3*alfa)*i)+(k*min(1,3*sqrt((3/(8*alfa))*i))*i*(1+(32*i*i))));
     j=j+1;
end;
for i =1:length(e)
    y(i)=w(i);
end
t =pmin:p:pmax;
plot(t,y)
title('Analisis of window using Tcp-friendly protocol')
xlabel('Loss probability')
ylabel('Window')
pause;
razont=((y/RTT)*wbits)/1024;
plot(t,razont)
title('Analisis of throughput using Tcp-friendly protocol')
xlabel('Loss probability')
ylabel('Throughput (kbit/s)')
B = zeros(1,length(razont));
for i =1:length(razont)
    if razont(i)>c
        B(i)=c;
    else B(i)=razont(i);

    end;
end;
razont
for i =1:length(razont)
    if razont(i)<c
        f=i
   break;
    end;
end;
pause;
plot(t,B)
title('Analisis of bandwidth using Tcp-friendly protocol')
xlabel('Loss probability')
ylabel('Bandwidth (kbit/s)')
if min(B)>0, miny=0.9*min(B); else, miny=1.1*min(B); end
if max(B)<0, maxy=0.9*max(B); else, maxy=1.1*max(B); end
axis([min(t) max(t) miny maxy])
pr=(f*pmax)/length(razont);
```

# Glosario de términos

**Ad-Hoc:** Una red Ad-Hoc consiste en un grupo de computadoras que se comunican cada una directamente con las otras a través de señales de radio (banda ISM) sin usar un punto de acceso. Las configuraciones Ad-Hoc son comunicaciones del tipo punto a punto. Las computadoras de la red inalámbrica que deben comunicarse entre ellas necesitan una tarjeta de red inalámbrica (interne o externa) del tipo PCMCIA. Para enviar las señales se usan antenas omnidireccionales y las computadoras portátiles la captan y la descifran mediante sus tarjetas PCMCIA.

**CALIDAD DE SERVICIO:** es la capacidad de cumplir con las restricciones temporales cuando se transmiten y se procesan flujos de datos multimedia en tiempo real. Las aplicaciones que transmiten datos multimedia requieren tener garantizados uno ancho de banda y unos límites de latencia en los canales que utiliza. Algunas aplicaciones varían sus demandas dinámicamente, y especifican tanto la calidad de servicios aceptable mínimo como la óptima deseada.

**CSMA:** acceso múltiple con sentido de portador. Cuando una estación tiene datos para mandar, primer examina si alguien está usando el canal. Espera hasta que el canal esté desocupado y entonces transmite un marco. Si hay un choque, espera un período aleatorio y trata otra vez.

**CWND (congestion window):** La ventana de congestión es una variable que limita la cantidad de datos que TCP puede enviar (en ningún momento TCP podrá enviar segmentos con un número de secuencia mayor que la suma del ACK con mayor número de secuencia recibido y el menor de los tamaños de las variables rwnd y cwnd). Su tamaño variará dependiendo de las condiciones de la red, si la red no descarta paquetes, el tamaño de la ventana aumentará, aumentando la velocidad de transmisión del receptor.

**Decibel (dB):** La unidad estándar utilizada para expresar ganancia o pérdida de energía.

**Desvanecimiento:** Se conoce con el nombre de desvanecimiento a toda disminución de la potencia recibida de señal con relación a su valor nominal. La diferencia entre este nvel nominal y el nivel recibido en condición de desvanecimiento se llama profundidad de desvanecimiento y se expresa en dB.

**Distancia de salto:** El numero de saltos que tiene que tomar un paquete para viajar desde la fuente hacia su destino final. Un diámetro de red es el máximo número de saltos por los que tiene que pasar un paquete de un nodo a otro.

**ICMP:** Protocolo de mensaje de control Internet, permite que los ruteadores en una red de redes reporten los errores o informaciones de control hacia otros ruteadores.

**IEEE:** El Institute of Electrical and Electronics Engineers (IEEE) también conocido como i-e-cubo, es una organización profesional técnica sin ánimo de lucro que incluye a más de 377.000 persona en 150 países. El IEEE se ha convertido en una autoridad en varias áreas técnicas, desde ingeniería informática hasta ingeniería en telecomunicaciones, pasando por otras como ingeniería biomédica o ingeniería eléctrica.

A través de su extensa red de publicaciones, conferencias y actividades destinadas al desarrollo de estándares, el IEEE produce el 30% de las publicaciones en ingeniería eléctrica e informática. Actualmente lleva a cabo anualmente 300 conferencias con reconocido prestigio internacional, y patrocina el desarrollo de más de 900 estándares.

**MAC:** El término MAC (Media Access Control) se utiliza para referirse a la dirección física de un dispositivo de red. Esta dirección debe ser única para cada dispositivo de red y es asignado en el momento de su fabricación. Una dirección MAC esta formada por 6 bytes que se representan en formato hexadecimal de esta forma: 11:22:33:44:55:66. De esos 6 bytes los 3 primeros corresponden con el identificador del fabricante, y los 3 siguiente con el identificador único de cada dispositivo. El identificado del fabricante es asignado por el IEEE para asegurar su unicidad. Es responsabilidad del fabricante asegurarse la unicidad del identificador del dispositivo para evitar repeticiones.

**MATLAB:** Es un lenguaje de alto nivel para uso computacional técnico. Se enfoca a cálculos computacionales, simulación y programación.

**Nodos expuestos:** Una estación que cree que el canal esta ocupado, pero en realidad esta libre pues el nodo que le oye no le interferiría para transmitir a otro destino.

**Nodos ocultos:** Una estación que cree que el canal esta libre, pero en realidad esta ocupado por otro nodo que no oye.

**Producto ancho de banda retardo de propagación (BDP):** Esto define la cantidad de datos que el protocolo puede tener "volando" en cada instante para la completa utilización de la capacidad del canal. El retardo usado en esta ecuación es el tiempo de ida y regreso de un paquete.

**Protocolos:** Los protocolos de comunicación son grupos de reglas que definen los procedimientos convenciones y métodos utilizados para transmitir datos entre dos o más dispositivos conectados a la red.

**Protocolo de control de transporte (TCP):** Provee una conexión confiable que permite la entrega sin errores de un flujo de bytes desde una máquina a otra en la Internet. Parte el flujo en mensajes discretos y lo monta de nuevo en el destino. Maneja el control de flujo.

**Razón de transmisión:** Es el número máximo de bits de información que pueden ser transmitido en un enlace de transmisión por unidad de tiempo. Típicamente se expresa en megabit por segundo (Mbps).

**Red de múltiple salto:** Una red en la cual un paquete debe pasar por varios nodos antes de llegar a su destino final.

**RMSS (Receiver Maximum Segment Size):** Es el mayor tamaño de segmento que el receptor puede admitir. La cantidad máxima de datos que el receptor puede recibir.

**RTO:** Tiempo de espera de la confirmación de un paquete (ACK).

**RTT:** Tiempo que transcurre desde que el segmento ha sido enviado, hasta que se recibe la confirmación de que ha sido recibido por el receptor. El RTT determina la velocidad de transmisión de TCP, ya que el emisor TCP envía cada RTT el tamaño determinado por cwnd.

**Ruido:** El termino ruido representa una señal que no contiene información, formada por una mezcla aleatoria de longitudes de onda.

**RWND (Receiver Window):** es la cantidad máxima de datos que puede recibir un

receptor de tráfico TCP.

**Segmento:** Se utiliza para designar cualquier paquete TCP, ya sea un paquete de datos o uno de reconocimiento (Ack).

**Servicio orientado a conexión:** Como el sistema telefónico. La conexión es como un tubo, y los mensajes llegan en el orden en que fueron mandados.

**Servicio sin conexión:** Como el sistema de correo. Cada mensaje trae la dirección completa del destino, y el ruteo de cada uno es independiente.

**SMSS (Sender Maximum Segment Size):** Es el mayor tamaño de un segmento que el emisor puede transmitir. La cantidad máxima de datos que el emisor puede enviar.

**SSTHRESH:** Esta variable se utiliza para determinar qué algoritmo de control de congestión se debe utilizar, partida lenta o la evasión de congestion.

**Ventana:** es el número de tramas que pueden estar pendiente de confirmar por el receptor.

# Glosario de acrónimos

| | |
|---|---|
| ACK | Acknowledgements (confirmaciones) |
| AP | Punto de Acceso |
| ARQ | Automatic repeat request |
| CCA | Clear Channel Assesment |
| CRC | Verificación de redundancia cíclica |
| CSMA/CA | Carrier sense multiple access with collision avoidance |
| CTS | Clear to send |
| DCF | Distributed Coordination Function |
| ECN | Notificación explicita de congestionamiento |
| FEC | Forward Error Correction |
| ICMP | Internet Control Message Protocol |
| IEEE | Institute of Electrical and Electronic Engineering |
| ISM | Industrial Scientific Medical band (2.4 GHz) |
| MAC | Media Access Control |
| MIMO | multiple-input multiple-output |
| MT | Terminales Móviles |
| MTU | Maximum Transfer Unit |
| NAV | Network Allocation Vector |
| PCF | Point Coordination Function |
| PCMCIA | Personal Compute Memory Card International Association |
| PLCP | Physical Layer Convergence Protocol |

| | |
|---|---|
| PMD | Physical Medium Dependent sublayer |
| QoS | Quality of Service |
| RTO | Round Trip Overtime |
| RTS | Request to send |
| RTT | Round Trip Time |
| SAP | Service Access Point |
| TCP | Transmission Control Protocol |
| TKIP | Temporal Key Integrity Protocol |
| TO | Time Out |
| WEP | Wired Equivalent Privacy |
| WiFi | Wireless Fidelity |
| WLAN | Wireless LAN |