VNIVERSIDAD NACIONAL AVFNOMA DE MEXICO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN INGENIERÍA

FACULTAD DE INGENIERÍA

"DISEÑO, IMPLEMENTACIÓN Y EVALUACIÓN DE UN PROTOCOLO MAC CON ALTO REUSO ESPACIAL PARA REDES INALÁMBRICAS CON INFRAESTRUCTURA Y AD HOC"

T E S I S

QUE PARA OPTAR POR EL GRADO DE:

MAESTRO EN INGENIERÍA

INGENIERÍA ELÉCTRICA - TELECOMUNICACIONES

P R E S E N T A:

ING. LUIS ALONSO MÉNDEZ BARREDO

TUTOR:
DR. JAVIER GÓMEZ CASTELLANOS

2005

JURADO ASIGNADO:

Presidente: Dr. VÍCTOR RANGEL LICEA

Secretario: Dr. HÉCTOR BENÍTEZ PÉREZ

Vocal: Dr. JAVIER GÓMEZ CASTELLANOS

1er. Suplente: Dr. CARLOS RIVERA RIVERA

2do. Suplente: Dr. SALVADOR LANDEROS AYALA

Lugar donde se realizó la tesis:

FACULTAD DE INGENIERÍA, CIUDAD UNIVERSITARIA MEXICO D.F.

TUTOR DE TESIS:

DR. JAVIER GÓMEZ CASTELLANOS

_____

FIRMA

DEDICATORIAS

A mis padres:

María Guadalupe Barredo Cano y Alonso Méndez Sántiz por su apoyo incondicional para poder lograr este objetivo en mi vida y por estar siempre ahí para mi…

A mi hermano Marcos, aunque no estás físicamente conmigo, me has acompañado siempre en mi camino…

AGRADECIMIENTOS

A la Universidad Nacional Autónoma de México por darme la oportunidad de realizar mis estudios de posgrado.

A mi asesor, el Dr. Javier Gómez Castellanos por su dirección y apoyo para la realización de esta tesis.

A la Dirección General de Estudios de Posgrado y al Instituto Tecnológico de Teléfonos de México por el apoyo otorgado por medio de sus programas de becas.

A UNAM-PAPIIT proyecto IN-103803 por el apoyo otorgado para poder realizar esta tesis.

A los Doctores:

Dr. Víctor Rancel Licea
Dr. Salvador Landeros Ayala
Dr. Carlos Rivera Rivera
Dr. Héctor Benítez Pérez

Por sus comentarios y sugerencias que permitieron mejorar este trabajo.

A mis hermanos, Cuauhtémoc y Liliana Méndez Barredo por sus palabras de aliento, y por darme ánimos para seguir hacia delante.

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN.

Los protocolos MAC de acceso múltiple con resolución de colisiones han utilizado una potencia de transmisión fija y no han considerado mecanismos de control de potencia en base a la distancia entre transmisor y receptor con el propósito de mejorar el reuso espacial de canal.

En esta tesis se diseña, implementa y evalúa un protocolo MAC inalámbrico de acceso múltiple controlado por potencia dentro de la estructura de evasión de colisiones. Este protocolo generaliza el modelo de evasión de colisiones transmitir-posponer de los protocolos actuales a un modelo de supresión de colisiones mas flexible “potencia limitada variable”. Este algoritmo está diseñado para redes ad hoc y no requiere la presencia de estaciones base para administrar la potencia de transmisión (es descentralizado). La ventaja de implementar un protocolo controlado por potencia en una red ad hoc es que los pares fuente-destino pueden estar más estrechamente empacados en la red permitiendo un número más grande de transmisiones simultáneas (reuso espectral).

Los resultados de simulación muestran que el protocolo implementado en esta tesis mejora el rendimiento en comparación con el MAC IEEE 802.11 sin control de potencia cuando los pares fuente-destino se encuentran más localizados, es decir, que se encuentran a un solo salto del nodo origen. Sin embargo, una desventaja que presenta el protocolo implementado es la desigualdad de acceso al medio conforme los pares fuente-destino se encuentran más distantes como se muestra en el capítulo 5. En esta trabajo se utiliza esta desigualdad de acceso al medio para proporcionar calidad de servicio diferenciado en redes inalámbricas ad hoc como se mostrará en el capítulo 6.

CAPÍTULO I
INTRODUCCIÓN

1.1 PROTOCOLOS DE CONTROL DE ACCESO AL MEDIO INALÁMBRICO.

La capacidad de comunicarse con cualquier persona en el planeta en cualquier lugar ha sido el sueño del hombre por mucho tiempo, la comunicación inalámbrica es el único medio que puede permitir este tipo de comunicación. Con los avances recientes en VLSI y tecnologías inalámbricas ahora es posible construir sistemas inalámbricos de alta velocidad que son baratos así como fáciles de instalar y operar; sin embargo, el medio inalámbrico es un medio de *broadcast* y por consiguiente múltiples dispositivos pueden acceder al medio al mismo tiempo haciendo que múltiples transmisiones simultáneas puedan resultar en datos distorsionados, haciendo la comunicación imposible. Un protocolo de control de acceso al medio (MAC) modera el acceso al medio compartido mediante la definición de reglas que permitan a los dispositivos comunicarse entre ellos de una manera ordenada y eficiente. Los protocolos MAC por consiguiente juegan un papel crucial en hacer posible este paradigma, garantizando la distribución eficiente y justa del escaso ancho de banda inalámbrico [1].

1.1.1 Conceptos Generales de Red.

Una red inalámbrica consiste de dispositivos con adaptadores inalámbricos que se comunican entre ellos usando ondas de radio. Estos dispositivos inalámbricos son llamados nodos y/o estaciones. La señal transmitida por un nodo solo puede ser recibida dentro de una cierta distancia del transmisor, la cual es llamada el rango del nodo. Un punto de acceso (AP) es un nodo especial en la red que no es móvil y esta situado en un punto central. Las redes inalámbricas difieren en el mecanismo de duplexaje y la arquitectura de red.

1.1.1.1 Opciones de Duplexaje.

Los mecanismos de duplexaje se refieren en cómo son multiplexados los canales de transmisión y recepción de datos. Estos canales pueden ser multiplexados en diferentes ranuras de tiempo o diferentes canales de frecuencia. El duplexaje por división de tiempo (TDD) se refiere a la multiplexación de la transmisión y la recepción en diferentes periodos de tiempo en la misma banda de frecuencia. Utilizar diferentes bandas de frecuencia para el enlace de subida y bajada se llama duplexaje por división de frecuencia (FDD). En FDD es posible para el nodo transmitir y recibir datos al mismo tiempo.

1.1.1.2 Arquitectura de Red.

En base a la arquitectura de red, las redes inalámbricas pueden ser lógicamente divididas en dos clases: Distribuidas y Centralizadas.

Redes inalámbricas distribuidas, también son llamadas redes Ad hoc (figura 1.1a). Son terminales inalámbricas que se comunican entre ellas sin una infraestructura pre-existente. Una red Ad Hoc no tiene administración central, de tal manera que la red no se colapsa cuando una de sus terminales se apaga o se cambia de lugar. En una red distribuida toda la transmisión y recepción de datos tiene que ser en la misma banda de frecuencia ya que no hay nodos especiales para convertir la transmisión de una banda de frecuencia a otra. Por consiguiente todas las redes Ad hoc operan en el modo TDD.

Redes inalámbricas centralizadas también llamadas redes de último-salto (ver figura 1.1b), son extensiones de redes cableadas con terminales inalámbricas en la última parte de la red. Estas redes tienen una estación base o AP que actúa como la interfase entre las redes cableadas y las redes inalámbricas. En las redes centralizadas las transmisiones en el canal de bajada (estación base hacia nodo inalámbrico) son de tipo *broadcast* y pueden ser escuchados por todos los dispositivos en la red dentro del rango de cobertura de la estación base. El canal de subida (nodo hacia estación base) es compartido por todos los nodos y por consiguiente es un canal de acceso múltiple. La estación base puede controlar el acceso del enlace de subida de acuerdo a requerimientos de calidad de servicio (QoS). Una red centralizada puede operar ya sea en el modo TDD o FDD.

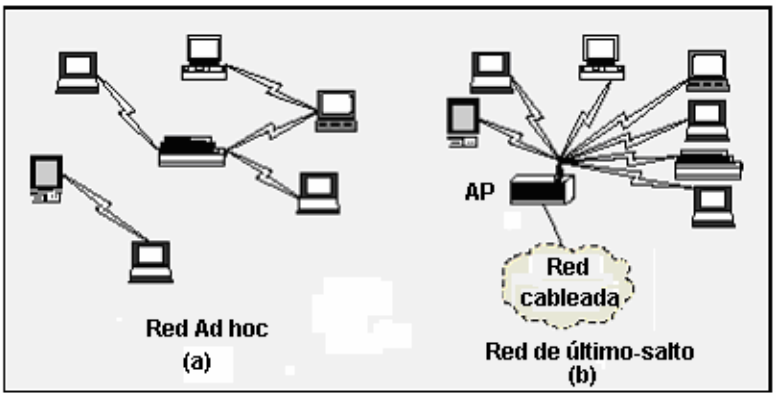

Figura 1.1 Alternativas de arquitectura del sistema.

1.1.1.3 Sistemas Ranurados.

El canal inalámbrico se dice que es ranurado si los intentos de transmisión toman lugar en instantes discretos de tiempo. Un sistema ranurado requiere una amplia sincronización de tiempo en la red, que es fácil de conseguir en redes centralizadas mediante el uso de la estación base como referencia de tiempo. Esta sincronización es difícil de lograr en las redes distribuidas. Una ranura es la unidad básica de tiempo en un sistema ranurado.

1.1.2 Propiedades del Medio Inalámbrico.

Las propiedades únicas del medio inalámbrico hacen el diseño de los protocolos MAC diferente y más desafiante al de las redes cableadas. Estas propiedades de los sistemas inalámbricos y su medio son:

- Operación Half-Duplex: En los sistemas inalámbricos es muy difícil recibir datos cuando el transmisor está enviando. Eso es debido a que cuando un nodo está transmitiendo datos, una gran fracción de la energía de la señal se filtra en la trayectoria de recepción.
- Canal variante con el tiempo. Las señales de radio se propagan de acuerdo a tres mecanismos principalmente: reflexión, difracción y dispersión. La señal recibida por un nodo es una superposición de versiones atenuadas y recorridas en el tiempo de la señal transmitida. Como resultado, la potencia de la señal recibida varia en función del tiempo y la distancia. A este fenómeno se le llama *propagación multitrayectoria*. La tasa de variación del canal está determinada por el tiempo de coherencia del canal. El tiempo de coherencia está definido como el tiempo dentro del cual la intensidad de la señal recibida cambia en 3 dB [1]. Cuando la intensidad de la señal recibida cae por debajo de un cierto umbral, se dice que el nodo se encuentra en *desvanecimiento*. La técnica de saludo inicial es una estrategia ampliamente usada para mitigar la calidad del enlace variante en el tiempo. Cuando dos nodos se desean comunicar, intercambian pequeños mensajes para verificar que el canal inalámbrico entre ellos permita una comunicación exitosa. Un saludo exitoso (intercambio de paquetes exitoso) indica un buen enlace de comunicación entre los dos nodos.
- Errores en ráfagas. Como consecuencia del canal variante con el tiempo y de la intensidad de la señal variable, los errores son más probables en las transmisiones inalámbricas. Los errores en un enlace inalámbrico ocurren en ráfagas cuando un nodo esta en desvanecimiento.

La pérdida de paquetes debido a errores en ráfagas pueden ser minimizados empleando una o más de las siguientes técnicas: paquetes más pequeños, códigos de corrección de errores, métodos de retransmisión.

- Detección de portadora dependiente de la ubicación. La detección de portadora está en función de la posición del receptor relativo al transmisor. En el medio inalámbrico, la intensidad de la señal decae dependiendo de la distancia. Solo los nodos dentro de un radio específico del transmisor pueden detectar la portadora en el canal. Esta detección de portadora dependiente de la ubicación resulta en nodos ocultos y expuestos. Un nodo oculto es aquel que está dentro del rango de cobertura del receptor deseado pero fuera del rango de cobertura del transmisor; en cambio, un nodo expuesto es aquel que está dentro del rango de cobertura del transmisor, pero fuera del rango de cobertura del receptor.

1.2 IEEE 802.11 a/b/g WLAN BASADO EN CSMA/CA.

Las redes inalámbricas de área local (WLANs) proporcionan conectividad inalámbrica de banda ancha entre PCs y otros dispositivos electrónicos así como acceso a la red central y otros equipos en ambientes empresariales, públicos y del hogar. Las WLANs también ofrecen una manera fácil para configurar redes de computadoras evitando la necesidad de instalación de cables. Otra aplicación potencial de las WLANs es como extensión de alta velocidad para redes de acceso de radio celular [2].

Actualmente la tecnología WLAN que opera en la banda ISM (Industria, Científica, Médica) de 2.4 GHz es ampliamente usada. Además de ser una tecnología propietaria, IEEE 802.11 proporciona un estándar internacionalmente aceptado para WLANs con tasas de datos de hasta 2 Mbps, utilizando tres técnicas de transmisión permitidas en la capa física Espectro disperso de saltos en frecuencia (FHSS), Espectro disperso de secuencia directa (DSSS) e Infrarrojo (IR). Una extensión en la capa física a este estándar conocida como DSSS de tasa alta (HR-DSSS) que opera con una tasa más alta, 802.11b, logra tasas de datos de hasta 11 Mbps y también opera en la banda ISM de 2.4 GHz. Sin embargo, el incremento en la demanda de tasas más altas y la necesidad de un espectro de frecuencia dedicado para aplicaciones WLAN ha conducido al desarrollo de un nuevo estándar y la asignación de nuevas frecuencias. En norte América, la comisión de comunicaciones federales (FCC) ha asignado 300 MHz de espectro a la banda UNII (Unlicensed National Information Infrastructure) en 5 GHz, y la IEEE ha desarrollado otra extensión a la capa

física 802.11 conocida como 802.11a que utiliza una técnica de multiplexaje por división de frecuencias ortogonales (OFDM). La capa física de este nuevo estándar soporta múltiples modos de transmisión, proporcionando tasas de datos crudos de hasta 54 Mbps cuando las condiciones del canal lo permitan. Además de los diferentes estándares anteriormente mencionados, en 2001, una segunda técnica de modulación OFDM fue introducida (802.11g) en la banda ISM de 2.4 GHz y en teoría puede operar a una tasa de hasta 54 Mbps.

1.2.1 Método de acceso en IEEE 802.11 a/b/g.

El acceso prioritario al medio inalámbrico es controlado a través del uso de intervalos de tiempo (IFS – Inter Frame Spacing) entre la transmisión de los paquetes. Los intervalos IFS son periodos obligatorios de tiempo inactivo en el medio de transmisión. En el estándar se especifican tres intervalos con el propósito de habilitar el acceso prioritario al canal [3]; estos son del más corto al más largo: IFS corto (SIFS), IFS de función de coordinación puntual (PIFS) y IFS de función de coordinación distribuida (DIFS), los valores de estos tiempos varían de acuerdo a la versión del estándar y se definirán con más detalla en el capítulo 2.
Para acceder al canal, un nodo debe seguir los siguientes pasos [4]:

- Cuando una estación tiene un paquete en su cola de espera listo para transmitir, primero muestrea el canal. Si el canal se detecta libre por un periodo DIFS, la estación puede comenzar la transmisión inmediatamente.
- Si inicialmente se detecta que el canal esta ocupado, o se torna ocupado durante el periodo DIFS, la estación pospone su transmisión y continúa monitoreando el medio hasta que la actual transmisión haya terminado.
- Cuando la transmisión actual ha terminado, la estación espera por otro intervalo DIFS mientras sigue monitoreando el medio. Si después del periodo DIFS el canal sigue desocupado, la estación calcula el número de ranuras de tiempo que tiene que esperar antes de transmitir mediante el algoritmo backoff exponencial binario y de nuevo monitorea el canal. Después de haber esperado el número de ranuras de tiempo determinado por el algoritmo, la estación puede comenzar la transmisión.

La parte de evasión de colisiones del protocolo se implementa a través de un procedimiento de espera aleatorio. Como se mencionó, cuando una estación monitorea el medio ocupado, espera por un periodo desocupado DIFS y calcula un tiempo aleatorio de espera que consiste de un número determinado de ranuras.

Cuando el medio se torna desocupado, la estación disminuye su temporizador hasta que llegue a cero, o el medio se torne ocupado otra vez. En el último caso, el temporizador de espera se congela hasta que el medio esté libre otra vez. Cuando los contadores de dos o más estaciones llegan a cero al mismo tiempo ocurre una colisión, en este caso, las estaciones calculan un nuevo tiempo aleatorio de espera (como se describe con más detalle en la sección 2.5.3.2).

1.2.2 Detección de la portadora en IEEE 802.11 a/b/g.

En el estándar IEEE 802.11, la detección de la portadora se realiza en la interfase aérea, referida como *detección física de portadora*, y en la subcapa MAC, referida como *detección de portadora virtual*. La detección física de portadora detecta la presencia de otros usuarios WLAN IEEE 802.11 por medio del análisis de todos los paquetes detectados, y también detecta actividad en le canal a través de la intensidad relativa de la señal de otras fuentes.

La detección virtual de portadora se logra usando campos de tiempo en los paquetes RTS, CTS y Datos, los cuales indican la duración de la transmisión actual. A este campo de tiempo se le llama Vector de asignación de red (NAV), el cual indica el tiempo que durará la transmisión actual. Todos los nodos que escuchan los mensajes RTS, CTS, Datos entrarán en backoff por una cantidad de tiempo NAV (especificada en el campo de duración del paquete) antes de muestrear el canal otra vez [3].

1.2.3 Potencia de transmisión común en IEEE 802.11 a/b/g.

Actualmente el protocolo MAC inalámbrico dominante es el estándar IEEE 802.11, que sigue el paradigma de “Acceso múltiple por detección de portadora con resolución de colisiones (CSMA/CA)” [6]. En este protocolo todos los nodos deben usar el mismo rango de transmisión común para todas las transmisiones de control y de datos y por lo tanto exhiben un pobre reuso espectral (número de transmisiones simultáneas que toman lugar en la red al mismo tiempo). Un nodo que transmite un paquete hacia otro en su proximidad debe primero adquirir el espacio físico antes de iniciar la transmisión del paquete de datos con el objetivo de evitar colisiones debido a estaciones expuestas y ocultas en la red inalámbrica de canal compartido, esto se logra mediante el intercambio de un saludo de paquetes de control entre el transmisor y el receptor. La transmisión de los paquetes de control RTS/CTS se hace con la potencia común de transmisión acordada (normalmente una potencia más alta que la mínima potencia necesaria para alcanzar al destino objetivo) para la correcta operación de la

capa MAC. Sin embargo, esta transmisión "bloqueará" un área limitada por el área de detección donde ninguna otra transmisión puede tomar lugar, por lo que este método prohíbe múltiples transmisiones concurrentes sobre la región del espacio físico obtenido. Como resultado hay un espacio físico desperdiciado en cada transmisión al mantener un método de rango común [5]. Para optimizar el reuso espacial del canal en una red de canal inalámbrico compartido, el par de nodos en comunicación deben adquirir solo la *mínima área* del espacio físico que se necesita para completar exitosamente la transmisión de datos. La figura 1.2 ilustra este escenario, donde se observa que con los protocolos MAC existentes, la transmisión de A hacia B evitaría que C enviara a D ya que C escucharía el RTS de A como se observa en las líneas sólidas que son los rangos de transmisión de A y B (suponiendo que C se encuentra a una distancia lo suficientemente cerca de A para detectar el RTS; es decir, que la potencia de recepción del paquete RTS en el nodo C sea mayor o igual a un cierto umbral de detección) por lo que tendría que posponer su transmisión. Sin embargo, si A redujera su nivel de potencia de transmisión lo suficiente para alcanzar a B, y de igual forma C transmitiera con la mínima potencia necesaria para alcanzar a D (líneas punteadas), ambas transmisiones ocurrirían simultáneamente.

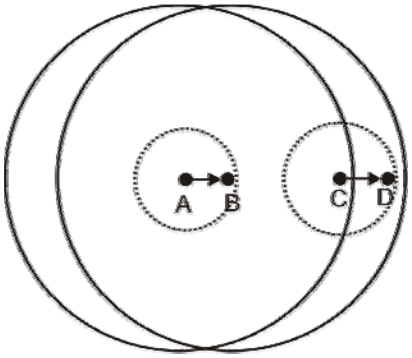

Figura 1.2 Mejoramiento de la capacidad con control de potencia de transmisión.

Para una potencia de transmisión dada, ignorando los desvanecimientos por multitrayectorias y los ensombrecimientos (considerando que son factores despreciables en ambientes de espacio abierto), la potencia de recepción está en relación inversa con la distancia entre el transmisor y receptor. Existen varios modelos de propagación para modelar estas pérdidas, que dependen principalmente en la distancia *d* entre transmisor y receptor. La potencia de recepción P_r de una señal a una distancia *d* está dado por:

$$P_r = P_t G_t G_r \frac{h_t^2 h_r^2}{d^4} \qquad (1)$$

Donde P_t representa la potencia de transmisión, G_t y G_r son las ganancias de las antenas del transmisor y receptor respectivamente, y h_t y h_r son las alturas de las antenas.

Dado el valor de P_r, cualquier receptor podrá decodificar correctamente un paquete, si la relación señal a interferencia (SIR) esta por arriba de cierto umbral (por ejemplo, en el simulador ns-2 este valor es de 10 dB). La SIR se puede definir de la siguiente manera:

$$SIR = \frac{P_r}{\sum_{n=1}^{I} P_k} = \frac{P_r}{P_i} \geq SIR\_\min \qquad (2)$$

En la ecuación 2, P_i representa la potencia interferente combinada de otras transmisiones en la vecindad.

En resumen, dado que los paquetes de control necesitan ser transmitidos con la misma potencia fija (máxima), los protocolos MAC de acceso múltiple actuales no pueden cambiar adaptivamente el espacio físico adquirido dependiendo de que tan cerca estén el transmisor del receptor, por lo que el uso de una potencia de transmisión común en la red hace a las capas subyacentes mas simples (capa MAC), sin embargo reduce la capacidad de la red y existe un desperdicio de energía de los dispositivos.

1.3 MAYOR REUSO ESPECTRAL EN IEEE 802.11.

Como se mencionó en la sección anterior, una de las principales desventajas del MAC IEEE 802.11 es que requiere que todos los nodos en la red utilicen una potencia de transmisión común para la transmisión de paquetes de control y datos. Actualmente existen varias propuestas hechas alrededor del estándar IEEE 802.11 que remueven esta limitación y proporcionan un mayor reuso espectral, nos referimos a estas propuestas de MAC como CSMA de reuso espacial (SR-CSMA).

Los dos principios principales que gobiernan el diseño de protocolos MAC SR-CSMA son:

(i) Principio de conservación de potencia, que dicta que cada fuente debe transmitir empleando la mínima potencia de transmisión necesaria para alcanzar al receptor deseado; y

(ii) Principio de cooperación, que dicta que ninguna fuente que inicie una nueva transmisión puede interrumpir transmisiones en curso mediante una transmisión demasiado “ruidosa”.

Mientras que estos protocolos MAC mejoran el desempeño de las redes simples y de múltiples saltos de medio compartido, su desempeño está aún limitado por el uso de CSMA/CA.

Uno de estos protocolos es el protocolo de acceso múltiple controlado por potencia [6] (PCMA) y descrito en el capítulo 3. PCMA permite a los nodos transmitir RTS-CTS con una potencia de transmisión que no interrumpa la operación de otros nodos en la red, de esta manera incrementando el reuso espacial en comparación con IEEE 802.11.

El protocolo PCMA utiliza dos canales de frecuencias separadas para su operación, un canal se utiliza para tráfico de datos y el otro canal es usado para señalización. El intercambio de paquetes en el canal de datos utiliza un saludo inicial petición-de-potencia-para-enviar (RPTS), potencia-aceptable-para-enviar (APTS), datos y ACK, que es similar a la secuencia RTS-CTS-Datos-ACK utilizada en IEEE 802.11. El propósito del intercambio RPTS-APTS que precede a la transmisión de datos es similar al RTS-CTS, excepto que su objetivo no es forzar a una terminal oculta a entrar en backoff, en vez de esto, es dejar que los pares fuentes-destino que desean transmitir calculen la potencia de transmisión mínima para comunicarse entre ellos (principio de conservación de potencia). En el protocolo PCMA, los receptores activos envían periódicamente un tono de ocupado en el canal de señalización para avisar a los transmisores potenciales su máxima tolerancia para admitir ruido extra (interferencia). Un nodo que intenta transmitir un paquete debe primero detectar la señal de tono de ocupado en el canal de señalización, si existe un tono de ocupado, entonces el nodo ajusta su potencia de transmisión tal que no interrumpa una transmisión en curso al comunicarse con su receptor deseado (principio de cooperación).

Otro ejemplo de SR-MACs es el protocolo MAC de ahorro de energía (Power Saving MAC) [7]; este MAC toma ventaja de técnicas de control de potencia para reducir la interferencia entre pares de transmisiones e incrementar el reuso espacial de las redes inalámbricas (WLANs). Basándose en el concepto de conjunto independiente máximo (MIS por sus siglas en inglés) este MAC permite tantos pares de transmisiones simultáneas como sean posible. El MAC enterado de interferencia (IA-MAC) [8] es otro ejemplo de SR-MACs, IA-MAC es bastante similar al protocolo PCMA excepto que IA-MAC no utiliza un canal de control adicional para señalización.

1.4 CONTROL DE POTENCIA EN LA ESTRUCTURA CSMA/CA.

En esta tesis se diseña, implementa y evalúa un protocolo de acceso múltiple controlado por potencia dentro de la estructura de evasión de colisiones. En este protocolo se generaliza el modelo de evasión de colisiones transmitir-posponer de los protocolos actuales a un modelo de supresión de colisiones más flexible “potencia limitada variable”. El algoritmo está estipulado para redes ad hoc y no requiere la presencia de estaciones base para administrar la potencia de transmisión (es descentralizado). La ventaja de implementar un protocolo controlado por potencia en redes ad-hoc es que los pares fuentes destinos pueden estar más estrechamente empacados en la red permitiendo un gran número de transmisiones simultáneas. El protocolo MAC controlado por potencia se implementó en un simulador de redes comúnmente usado, ns2, que se explica en detalle más adelante en la tesis. Para la implementación del protocolo se requirió modificar el código y parámetros de los archivos mac-802_11.cc, wirelessphy.cc, channel.cc y ns-default.tcl para que durante la simulación realizaran la función de control de potencia de acuerdo a los principios fundamentales que gobiernan el diseño de protocolos MAC SR-CSMA.

Los resultados de simulación obtenidos, muestran que el protocolo de acceso múltiple implementado mejora el desempeño de rendimiento en comparación con IEEE 802.11 sin control de potencia, como se mostrará en la sección 5.2 del capítulo 5, ya que permite un número mayor de transmisiones simultáneas que IEEE 802.11 (mayor capacidad) mediante la reducción de los niveles de potencia de transmisión a los niveles mínimos necesarios que garanticen la recepción exitosa en el destino deseado, de esta manera mejorando la utilización del canal. El beneficio de este tipo de protocolos (basados en SR-CSMA) sobre IEEE 802.11 se incrementan cuando el tráfico se vuelve más localizado (cuando los nodos se comunican con otros nodos solo en su vecindad). Sin embargo, una propiedad negativa de los protocolos SR-CSMA es que favorecen transmisiones de rangos cortos sobre las transmisiones de rangos largos bajo cargas pesadas de tráfico [6]. Se resalta esta observación porque utilizamos esta inequidad en nuestro favor para implementar calidad de servicio controlado por potencia.

Como se mencionó anteriormente, existe cierto favoritismo en los protocolos basados en SR-CSMA, esta desigualdad inherente hacia transmisiones de rangos largos no es específica del protocolo PCMA, sino que es un comportamiento común de los protocolos SR-CSMA que proporcionan un reuso espectral más alto en la red.

En esta tesis, se utiliza esta desigualdad como la base para proporcionar diferenciación de servicio en redes inalámbricas ad-hoc. La intuición es como sigue: *Si dividimos una transmisión de rango largo en transmisiones de rangos mas cortos, podemos con mayor probabilidad incrementar las oportunidades de transmisión de los enlaces de rangos más cortos, mejorando la calidad de servicio (QoS) punto-a-punto observado en un flujo particular [5]*. Este objetivo se puede lograr agregando nodos retransmisores entre pares fuente destino. Este método, sin embargo, podría ser perjudicial para otros flujos y para la capacidad total de la red para transportar tráfico. A este método le llamaremos PCQoS (calidad de servicio controlado por potencia) y discutiremos sus beneficios y desventajas con más detalle en el capítulo 6.

En este capítulo se presenta una descripción de algunos conceptos generales sobre redes así como de las propiedades del medio inalámbrico. Se aborda de manera superficial el estándar IEEE 802.11, las diferentes capas físicas que soporta, método de acceso y de detección de portadora. Se describe el funcionamiento del estándar IEEE 802.11 en base al uso de una potencia de transmisión común y se menciona como se puede lograr un mayor reuso espectral/espacial en la red mediante el uso de una potencia de transmisión variable y siguiendo dos principios fundamentales de diseño. Por último se presenta una propuesta de calidad de servicio controlado por potencia tomando ventaja de los protocolos basados en SR-CSMA.

La estructura de esta tesis está organizada de la siguiente manera: en el capítulo 2 se describe el estándar IEEE 802.11, en el capítulo 3 se describe el funcionamiento del protocolo de acceso múltiple controlado por potencia para redes inalámbricas de paquetes (PCMA), en el capítulo 4 se hace una descripción del funcionamiento del simulador ns-2 así como la implementación del protocolo de control de acceso al medio controlado por potencia; en el capítulo 5 se evalúan los parámetros más importantes del protocolo implementado en esta tesis que son rendimiento e igualdad de acceso al medio, en el capítulo 6 se desarrolla una aplicación de calidad de servicio controlado por potencia y por último se presentan las conclusiones de la tesis en el capítulo 7.

CAPÍTULO II
EL ESTÁNDAR IEEE 802.11

2.1 INTRODUCCION.

La computación inalámbrica es una tecnología que se está desarrollando muy rápido y que proporciona a los usuarios conectividad sin estar atado a una red cableada. Las redes locales inalámbricas, al igual que su contraparte cableada están siendo desarrolladas para proporcionar anchos de banda grandes a los usuarios en un área geográfica limitada. Varios estándares de comunicación inalámbrica han evolucionado, los cuales tratan de proporcionar el acceso al medio inalámbrico compartido. Los protocolos tales como el HiperLAN, IEEE 802.11, Bluetooth son ejemplos de dichos estándares. El protocolo IEEE 802.11 es el más ampliamente usado [9].

El proyecto de desarrollo del estándar IEEE 802.11 empezó en la década de los 90´s y varios diseños preliminares del estándar han sido publicados para su revisión. La meta del estándar es "desarrollar una especificación de capa Física (PHY) y de Control de Acceso al Medio (MAC) para conectividad inalámbrica de estaciones fijas, portátiles y móviles dentro de un área local". El estándar tiene dos propósitos:

- "Proporcionar conectividad inalámbrica a maquinaria automática, equipo, o estaciones que requieran un rápido desarrollo, los cuales pueden ser portátiles, manuales o que puedan estar montados en vehículos en movimiento dentro de un área local".

- "Ofrecer un estándar para usarse por cuerpos regulatorios con el fin de estandarizar el acceso a una o mas bandas de frecuencia para el propósito de comunicaciones de área local".

El estándar preliminar IEEE 802.11 describe una tasa de transmisión de datos obligatorio a 1Mb/s con soporte opcional a 2Mb/s para redes inalámbricas de área local (WLAN). También se especifica soporte obligatorio para transferencia de datos asíncrono así como soporte adicional para servicios distribuidos de tiempo limitado (DTBS). La transferencia de datos asíncronos se refiere al tráfico que es relativamente insensible a retardos de tiempo como el correo electrónico y transferencia de archivos. Por otro lado, tráfico limitado en tiempo, es tráfico que esta limitado por retardos de tiempo especificados para lograr una calidad de servicio aceptable (QoS) ejemplo de este tipo de tráfico es voz y video en paquetes [3].

El estándar IEEE 802.11 define dos capas. La primera capa es la Física (PHY), el cual especifica el esquema de modulación utilizado y las características de señalización para la transmisión a través de radio frecuencias. La segunda capa es el control de acceso al medio (MAC) la cual determina como se utiliza el medio.

De particular interés en la especificación es el soporte de dos esquemas fundamentalmente diferentes de MAC para transportar servicios asíncronos y limitados en tiempo. El primer esquema, Función de Coordinación Distribuida (DCF), es similar a las redes de paquetes tradicionales que soportan entrega de datos con mejor esfuerzo. El DCF está diseñado para transporte de datos asíncronos, donde todos los usuarios que tienen datos para transmitir tienen la misma oportunidad de acceder a la red. La Función de Coordinación Puntual (PCF) es el segundo esquema de MAC. El PCF está basado en encuestas (polling) que están controladas por un AP y está diseñado principalmente para la transmisión de tráfico sensible a retardos.

2.2 ARQUITECTURA.

El estándar IEEE 802.11 soporta tres topologías básicas para WLAN: Conjunto de servicios básicos (BSS), Conjunto de servicios básicos independientes (IBSS) y el conjunto de servicios extendidos (ESS). Las tres configuraciones son soportadas por la implementación de la capa MAC [3].

2.2.1 Conjunto de servicios básicos (BSS).

Es el bloque fundamental de la arquitectura del estándar IEEE 802.11. Un BSS está definido como un grupo de estaciones que están bajo el control directo de una función de coordinación simple (DCF o PCF) los cuales se definen más adelante. El área geográfica que cubre el BSS se le conoce como *área de servicio básico* (BSA), el cual es análogo a una celda en una red de comunicaciones celulares. Conceptualmente, todas las estaciones dentro del BSS se pueden comunicar directamente con todas las demás estaciones en el BSS. Sin embargo, las degradaciones del medio de transmisión debido a los desvanecimientos o interferencia de otros BSSs cercanos que rehúsan las mismas características de capa física (frecuencia y código de dispersión, o patrón de saltos), puede causar que algunas estaciones parezcan “ocultas” a otras estaciones.

2.2.2 IBSS / Ad Hoc.

Una red Ad-Hoc es un grupo deliberado de estaciones dentro de una BSS simple con el propósito de comunicación en red sin la ayuda de una red de infraestructura. La Figura 2.1 es una ilustración de una *BSS independiente* (IBSS), que es el nombre formal para una red Ad Hoc en el estándar IEEE 802.11. Cualquier estación puede establecer una sesión de comunicación directa con cualquier otra estación dentro del BSS, sin el requerimiento de canalizar todo el tráfico a través de un AP centralizado.

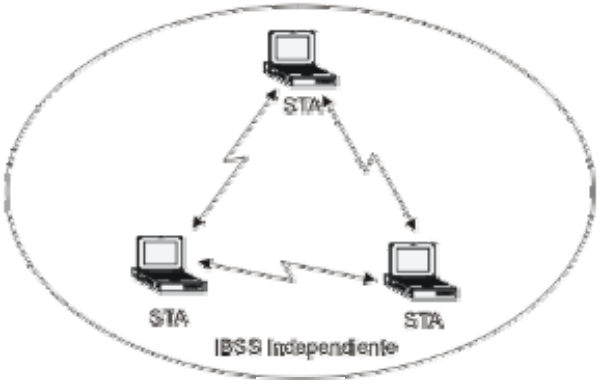

Figura 2.1 Bosquejo de una red Ad Hoc.

2.2.3. ESS / Infraestructura.

En contraste a la red Ad Hoc, las redes de infraestructura se establecen para proporcionar a los usuarios de redes inalámbricas servicios específicos y extensión de cobertura. Las redes de infraestructura en el contexto del estándar IEEE 802.11 se establecen empleando puntos de acceso. El punto de acceso es análogo a la estación base en una red de comunicaciones celulares. El punto de acceso soporta extensión de cobertura mediante la provisión de puntos de integración necesarios para la conectividad de red entre múltiples BSSs, de esta manera formando un *conjunto de servicios extendidos* (ESS). El ESS tiene la apariencia de un conjunto de servicio básico grande para la subcapa de *control de enlace lógico* (LLC) para cada estación (STA). El conjunto de servicios extendidos consiste de múltiples BSS que están integrados usando un *sistema de distribución* común (DS). El sistema de distribución puede ser pensado como la columna de la red que es responsable de transporte a nivel MAC de unidades de datos de servicio MAC (MSDU). El sistema de distribución, como se especifica en IEEE 802.11, es independiente de la implementación. Por consiguiente, el DS podría ser una LAN Ethernet cableada 802.3, una LAN 802.4 token bus,

LAN IEEE 802.5 token ring, o una red de área metropolitana de interfase de datos distribuidos por fibra óptica (FDDI), u otro medio inalámbrico IEEE 802.11. Se debe notar que mientras el DS puede ser físicamente el mismo medio de transmisión que el BSS, son lógicamente diferentes, ya que el BSS es solamente usado como la columna de transporte para transferir paquetes entre diferentes BSSs en el conjunto de servicios extendidos (ESS).

Un conjunto de servicios extendidos también puede servir como puerta de acceso para nodos inalámbricos hacia una red cableada tal como Internet. Esto se logra por medio de un dispositivo conocido como *portal*. El portal es una entidad lógica que especifica el punto de integración sobre el sistema de distribución donde la red IEEE 802.11 se integra con otra red diferente. Si la red es una IEEE 802.X, el portal incorpora funciones que son análogas a un puente; esto es, este proporciona extensión de cobertura e interpretación entre diferentes formatos de trama. La figura 2.2 ilustra un conjunto de servicios extendidos desarrollado con dos BSSs, un sistema de distribución, y un acceso portal a una LAN cableada.

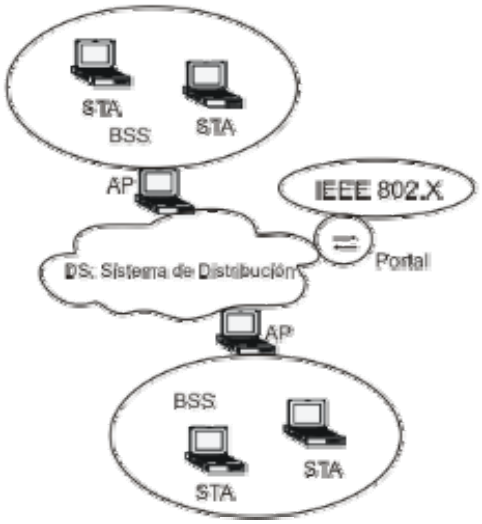

Figura 2.2 Bosquejo de una red de infraestructura.

2.3 PILA DEL PROTOCOLO 802.11.

Los protocolos usados por todas las variantes de los estándares 802, incluso Ethernet, tienen una estructura muy similar. La capa física de 802.11 corresponde bastante bien a la capa física del modelo OSI, pero la capa de enlace de datos en todos los protocolos 802 se dividen en dos o más subcapas. En el caso del estándar IEEE 802.11 la capa de enlace de datos esta dividida en dos: Subcapa de control de enlace lógico y de control de acceso al medio [10].

Un bosquejo parcial de la pila del protocolo 802.11 se puede observar en la figura 2.3 donde se muestra las diferentes capas físicas que soporta el estándar IEEE 802.11.

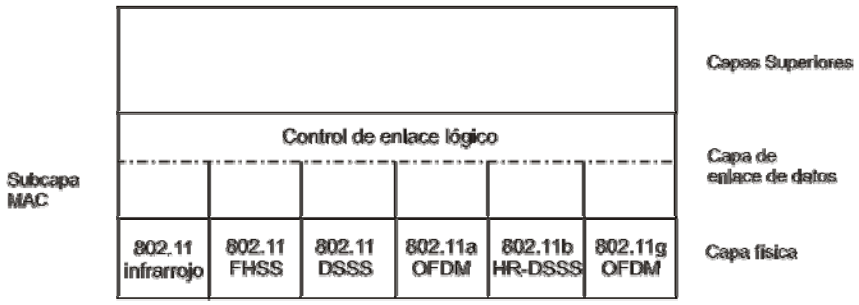

Figura 2.3. Parte de la pila del Protocolo IEEE 802.11

2.4 CAPA FISICA.

La capa física del estándar 802.11 (PHY) es la interfase entre el MAC y el medio inalámbrico donde los paquetes son transmitidos y recibidos. La capa física proporciona tres funciones. Primero, proporciona una interfase para intercambiar paquetes con la capa superior MAC para transmisión y recepción de datos. Segundo, emplea modulación de espectro disperso y de la señal portadora para transmitir paquetes de datos sobre el medio inalámbrico. Tercero, proporciona indicación de detección de portadora hacia el MAC para verificar actividad en el medio [11].

El estándar preliminar IEEE 802.11 de 1997, especifica tres técnicas de transmisión permitidas en la capa física [3]:

- Espectro disperso por salto de frecuencia (FHSS.
- Espectro disperso de secuencia directa (DSSS).
- Tecnología infrarroja (IR).

Las primeras dos técnicas operan en la banda sin licencia ISM de 2.4 GHz mientras que IR opera en banda base. Todas estas técnicas operan con tasas de datos de 1 o 2 Mbps.
En 1999, dos nuevas técnicas fueron introducidas para lograr anchos de banda más grandes:

- La primera (802.11a) opera en el rango de frecuencias de 5 GHz de la banda sin licencia UNII y define una técnica de multiplexaje por división de frecuencias ortogonales (OFDM-Orthogonal Frequency Division Multiplexing) que puede lograr tasas de datos hasta de 54 Mbps.

- La segunda (802.11b) opera en la banda ISM de 2.4GHz y define tasas de datos a 11 Mbps y 5.5 Mbps (además de las tasas de 1 y 2 Mbps) utilizando una extensión de DSSS llamado HR/DSSS (High Rate/ DSSS), también define una técnica de conmutación de tasas donde las redes de 11Mbps pueden caer a 5.5 Mbps, 2 Mbps, o 1 Mbps bajo condiciones de ruido o para operar con capas físicas 802.11 anteriores.

En 2001, una segunda técnica de modulación OFDM fue introducida (802.11g) en la banda ISM que es diferente a la banda de frecuencia UNII de 802.11a y en teoría puede operar a una tasa de hasta 54 Mbps [10].

A continuación examinaremos de forma breve cada una de las diferentes técnicas de transmisión permitidas en la capa física.

2.4.1 802.11 Infrarrojo (IR).

La especificación de la técnica IR emplea transmisión difusa en el rango de longitudes de onda de 850 a 950 nm. Utiliza Modulación por posición de pulsos (PPM- Pulse Position Modulation) para transmitir datos usando radiación IR. PPM varía la posición de un pulso con el propósito de transmitir diferentes símbolos binarios. De esta manera la técnica de IR puede ser utilizada para transmitir información ya sea a 1 o 2 Mbps. La banda IR esta diseñada solo para uso dentro de edificios y opera con transmisiones no dirigidas.

Para transmitir a 1Mbps, se utilizan 16 símbolos para transmitir 4 bits de información (16-PPM), mientras que en el caso de 2 Mbps, se utilizan 4 símbolos para transmitir 2 bits de información (4-PPM). Los símbolos de datos siguen el código Gray. Este código tiene la propiedad que un pequeño error en la sincronización del tiempo produce un solo bit en error en la salida [4].

Las transmisiones IR tienen varias desventajas, estos sistemas comparten parte del espectro que utiliza el sol, lo cual lo hace práctico solo para ambientes dentro de edificios. Las lámparas fluorescentes también emiten radiaciones en el espectro IR causando degradación de la relación señal a interferencia (SIR) en los receptores, además tienen anchos de banda bajos y alcanzan rangos que raramente exceden 20m. Estas son algunas razones que hacen a los sistemas IR una opción no popular.

2.4.2 Transmisiones de espectro disperso.

Los sistemas de espectro disperso emplean transmisiones de radio frecuencia (RF) como el medio de capa física. Dos subsistemas principales existen: Espectro disperso por saltos de frecuencia (FHSS) y Espectro disperso de secuencia directa (DSSS). DSSS es principalmente una tecnología que se emplea dentro de edificios, mientras que FHSS es principalmente una tecnología que se emplea para interconectar edificios. La técnica actual de transmisiones de espectro disperso fue desarrollada por los militares como un intento de reducir el "*jamming*" y espionaje. Las transmisiones de espectro disperso toman una señal digital y la expanden o dispersan para hacerla parecer como ruido aleatorio de fondo en vez de una transmisión de señal digital. La codificación toma lugar ya sea por medio de FSK (Frequency Shift Keying) o PSK (Phase Shift Keying), ambos métodos incrementan el tamaño de la señal de datos así como el ancho de banda. Aunque la señal parece como ruido (más ancho de banda) y más fácil de detectar, la señal no es entendible y se asemeja al ruido de fondo a menos que el receptor este sintonizado con los parámetros correctos [14].

2.4.2.1 802.11 Espectro disperso por saltos en frecuencia (FHSS).

La técnica FHSS utiliza la banda ISM de 2.4 GHz (esto es 2.4000 – 2.4835 GHz). En los Estados Unidos, se han especificado un máximo de 79 canales en el conjunto de saltos. El primer canal tiene una frecuencia central de 2.402 GHz, y todos los canales subsecuentes están espaciados 1MHz. La separación de 1 MHz es mandado por la FCC para la banda ISM de 2.4GHz. La separación de canal corresponde a 1 Mb/s de ancho de banda instantáneo. Tres conjuntos diferentes de secuencias de saltos son establecidos con 26 secuencias de saltos por conjunto. Diferentes secuencias de saltos permite a múltiples BSSs coexistir en la misma área geográfica, el cual es importante para aliviar congestión y maximizar el rendimiento (throughput) en un BSS. La razón de tener tres diferentes conjuntos es para evitar periodos de colisión prolongados entre diferentes secuencias de saltos en un conjunto. La mínima tasa de saltos permitida es 2.5 saltos/seg. La tasa de acceso básico de 1 Mb/s emplea GFSK de dos niveles, donde un 1 lógico es codificado usando la frecuencia $Fc + f$ y un 0 lógico usando la frecuencia $Fc - f$. La tasa de acceso mejorada de 2 Mb/s emplea GFSK de cuatro niveles, donde dos bits son codificados al mismo tiempo utilizando cuatro frecuencias [3].

2.4.2.2 802.11 Espectro disperso de secuencia directa (DSSS).

La técnica DSSS también utiliza la banda ISM de 2.4 GHz, donde la tasa de acceso básico de 1 Mb/s se codifica empleando DBPSK (Differential Binary Phase Shift Keying), y la tasa mejorada de 2 Mb/s emplea DQPSK (Differential Quadrature Phase Shift Keying). La dispersión se hace dividiendo el ancho de banda disponible en 11 subcanales, cada uno de 11MHz de ancho, y usando una secuencia Barker de 11 chips para dispersar cada símbolo de datos. La máxima capacidad del canal es por consiguiente (11 chips/símbolo) / (11MHz) = 1Mb/s si se emplea DBPSK. Conjuntos de servicio básico (BSSs) adyacentes y traslapados pueden ser alojados asegurando que las frecuencias centrales de cada BSS estén separadas por al menos 30 MHz. Este requerimiento rígido permite tan solo dos BSSs adyacentes o traslapados operar sin interferencia [3].

2.4.2.3 802.11b DSSS de tasa alta (HR/DSSS).

La única técnica (que no viola las regulaciones de FCC) capaz de lograr velocidades mas altas es DSSS que fue seleccionada como la técnica de capa física estándar, que soporta 1 y 2 Mbps y dos nuevas velocidades de 5.5 y 11 Mbps [14].

Para incrementar la tasa de datos en el estándar 802.11b, en 1998 Lucent Technologies y Harris Semiconductor propusieron a la IEEE un estándar llamado CCK (Complementary Code Keying). En vez de los dos códigos Barker de 11 bits, CCK usa un conjunto de 64 códigos únicos de 8 bits, de esta manera hasta 6 bits pueden ser representados por un código (en vez de 1 bit representado por un símbolo Barker). Como un conjunto estos códigos tienen propiedades matemáticas únicas que les permite ser correctamente distinguidos uno de otro por el receptor, aun en presencia de ruido e interferencia multi-trayectoria (Por ejemplo, interferencia causada por recibir múltiples reflexiones dentro de un edificio).

La tasa de datos de 5.5 Mbps usa CCK para codificar 4 bits por portadora, mientras que la tasa de 11 Mbps codifica 8 bits por portadora. Ambas velocidades emplean QPSK como la técnica de modulación y una señal de 1.375 MSps. QPSK emplean cuatro rotaciones (0, 90,180 y 270 grados) para codificar 2 bits de información en el mismo espacio mientras que BPSK codifica 1.

Para soportar ambientes muy ruidosos así mismo como un rango más amplio, las WLANs 802.11b emplean conmutación de tasas de transmisión dinámicos, permitiendo que las tasas de datos sean automáticamente ajustados para compensar la naturaleza cambiante del canal. Idealmente los usuarios se conectan a una tasa máxima de 11Mbps. Sin embargo, cuando los dispositivos se mueven mas allá del rango óptimo para operar a 11 Mbps, o se presenta alguna interferencia substancial, los dispositivos 802.11b transmitirán a velocidades más bajas, cayendo a 5.5, 2, y 1 Mbps. Así mismo, si el dispositivo regresa dentro del rango de transmisiones de alta velocidad, la conexión automáticamente mejorará [16]. Esto se debe a que los dispositivos 802.11b conforme se alejan del rango óptimo, los radios se adaptan y utilizan un mecanismo de codificación menos complejo (y más bajo) para enviar datos. Esta conmutación de tasas también implica que puede operar con 802.11 DSSS, pero no con 802.11 FHSS. La tabla 2.1 identifica las diferencias.

Tasa de Datos	Longitud del código	Modulación	Tasa de símbolos	Bits/Símbolo
1 Mbps	11(Secuencia Barker)	BPSK	1 Msps	1
2 Mbps	11(Secuencia Barker)	QPSK	1 Msps	2
5.5 Mbps	8(CCK)	QPSK	1.375 Msps	4
11 Mbps	8(CCK)	QPSK	1.375 Msps	8

Tabla 2.1. Especificaciones de tasas de datos de 802.11b.

2.4.3 Multiplexaje por Division de Frecuencias Ortogonales (OFDM):

La multiplexación por división de frecuencia (FDM) transmite múltiples señales simultáneamente sobre una simple ruta de transmisión, cada señal viaja dentro de un único rango de frecuencia (portadora), el cual es modulado por los datos. Estos datos pueden ser voz o video. La figura 2.4 (a) muestra la relación relativa de las portadoras dentro de una asignación de frecuencia dada.

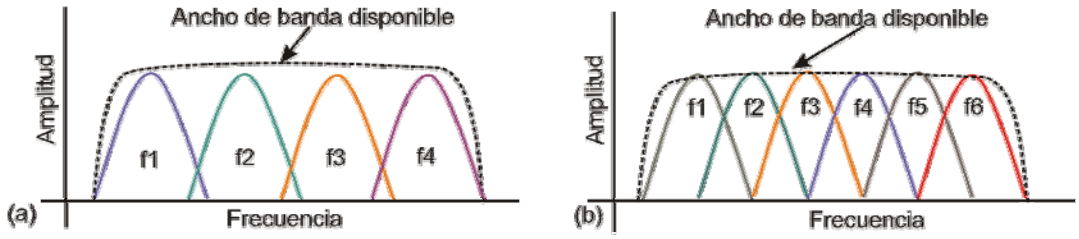

Figura 2.4. Técnicas de transmisión de la señal. (a) FDM, (b) (OFDM)

Aunque el beneficio principal de FDM es el incremento de ancho de banda, FDM también reduce la interferencia intersímbolo debido a multitrayectorias (ISI). El incremento de ancho de banda trae consigo un nivel de ineficiencia: Arriba del 50 % del espectro disponible se desperdicia en las bandas de guarda, las cuales aseguran el aislamiento entre diferentes frecuencias [15]. FDM utiliza múltiples portadoras para transmitir información. Las señales viajan dentro de un rango de frecuencia único (portadora), la cual es modulada por los datos.

La técnica de espectro disperso de multiplexación de frecuencias ortogonales (OFDM) además utiliza QAM (Quadrature Amplitude Modulation), una técnica avanzada de procesamiento digital de la señal, distribuyendo los datos sobre múltiples portadoras espaciadas en frecuencias precisas, como se muestra en la figura 2.4 (b). Los espaciamientos precisos proporcionan la ortogonalidad que evita que los demoduladores vean otras frecuencias. Debido a que cada portadora puede ser únicamente identificada, se eliminan las bandas de guarda, incrementando la eficiencia del uso del espectro de frecuencia. La figura 2.5 ilustra la ortogonalidad de las diferentes frecuencias portadoras, la frecuencia base es igual a 1/T, donde T = periodo del símbolo. Las líneas negras representan una suma de las diferentes frecuencias portadoras.

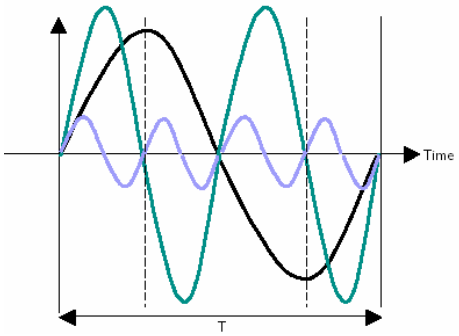

Figura 2.5. Ortogonalidad de las diferentes frecuencias portadoras.

2.4.3.1 802.11a Multiplexaje por división de frecuencias ortogonales (OFDM).

A diferencia de 802.11b, 802.11a fue diseñado para operar en la banda UNII (Unlicensed National Information Infrastructure) de 5 GHz. Distinto a la banda ISM, el cual ofrece alrededor de 83 MHz en el espectro de 2.4 GHz, IEEE 802.11a utiliza casi cuatro veces más que la banda ISM, ya que la banda UNII ofrece 300 MHz de espectro relativamente libre de interferencia. A diferencia de 802.11b, el estándar 802.11a utiliza la técnica de **multiplexaje por división de frecuencia,** que se espera sea más eficiente en ambientes dentro de

edificios. Como se mencionó previamente, la FCC ha asignado 300 MHz de espectro para la banda UNIII en el bloque de 5 GHz, 200 MHz de los cuales estan en 5,150 MHz - 5,350 MHz, con los otros 100 MHz en 5,725 MHz - 5,825 MHz. La primera ventaja de 802.11a sobre 802.11b es que este estándar opera en el espectro de 5.4 GHz, lo cual da la ventaja de funcionamiento de las altas frecuencias. Pero, la frecuencia, potencia radiada y distancia están en una relación inversa, de tal forma que moverse de 2.4 GHz a 5 GHz induce a distancias más cortas y/o requerimientos de mayor potencia. Es por esto que el estándar 802.11a incrementa el EIRP al máximo de 50 mW. El espectro de 5.4 GHz se divide en tres "dominios" de trabajo y cada dominio tiene restricciones de máxima potencia [14].

La segunda ventaja está en la técnica de codificación que utiliza 802.11a. El estándar 802.11a utiliza un esquema de codificación llamado COFDM u OFDM (coded orthogonal frequency division multiplexing). Cada subcanal en la implementación COFDM es de alrededor de 300 KHz de ancho. COFDM trabaja mediante la división de una portadora de datos de alta velocidad en varias sub-portadoras de baja velocidad, las cuales son transmitidos en paralelo. Cada portadora de alta velocidad es de 20 MHz de ancho y es dividida en 52 sub-canales, cada uno de aproximadamente 300 KHz de ancho. COFDM utiliza 48 de estos subcanales para datos, mientras que los cuatro restantes son usados para corrección de errores. COFDM envía tasas de datos más altas y un alto grado de recuperación de la señal, gracias a su esquema de codificación y corrección de errores. En 802.11a se utiliza BPSK para codificar 125 Kbps, produciendo una tasa de datos de 6 Mbps. Si se utiliza QPSK, es posible codificar hasta 250 Kbps por canal, el cual logra una tasa de datos de 12 Mbps. Además si se emplea 16-QAM codificando 4 bits por hertz, se logra una tasa de datos de 24 Mbps. El estándar define velocidades básicas de 6,12, y 24 Mbps, que deben soportar los productos compatibles con 802.11a. Las tasas de datos de 54 Mbps se logran usando 64-QAM, el cual produce 8/10 bits por ciclo, y un total de hasta 1.125 Mbps por cada canal de 300 KHz, el cual multiplicado por 48 canales de datos resulta en una tasa de datos de 54 Mbps.

2.4.3.2 802.11g Multiplexaje por división de frecuencias ortogonales (OFDM).

El estándar opera en la banda de 2.4 GHz, y emplea dos modos de operación obligatorios y dos opcionales. Los métodos de modulación/acceso obligatorios son los mismos modos, CCK (Complementary Code Keying) utilizado por 802.11b (de ahí la compatibilidad con este estándar) y OFDM (Orthogonal Frequency Division Multiplexing) utilizado por 802.11 a (pero

en este caso en la banda de frecuencia de 2.4 GHz). El modo CCK obligatorio soporta 11Mbps y el modo OFDM tiene una tasa máxima de 54 Mbps. También existen otros dos modos que utilizan diferentes métodos para alcanzar una tasa de datos de 22Mbps, PBCC-22 (Packet Binary Convolutional Coding, para 6 a 54 Mbps) y CCK-OFDM (para una tasa máxima de 33 Mbps).

La ventaja de 802.11g es que mantiene compatibilidad con 802.11b y ofrece tasas de datos más rápidas comparables con 802.11a. Sin embargo, el número de canales disponibles no se incrementa, ya que los canales son una función del ancho de banda, no de la modulación de la señal de radio, y en este punto, 802.11a tiene la ventaja de sus 8 canales, comparado con los tres canales disponibles con 802.11 b y g. Otra desventaja de 802.11g es que trabaja en la banda de 2.4 GHz y debido a la interferencia que se experimenta en esta banda, nunca será tan rápido como 802.11a [16].

2.5 SUBCAPA DE CONTROL DE ACCESO AL MEDIO IEEE 802.11, 802.11 a/b/g.

La subcapa MAC es responsable de los procedimientos de asignación de canal, direccionamiento de unidades de datos de protocolo (PDU), formato de tramas, chequeo de error, fragmentación y reagrupación. El medio de transmisión puede operar en el modo de contención exclusivamente, requiriendo que todas las estaciones contiendan (compitan) por el acceso al canal por cada paquete transmitido. El medio también puede alternar entre el modo de contención, conocido como el *periodo de contención* (CP), y el *periodo libre de contención* (CFP). Durante el CFP, el uso del medio esta controlado (o arbitrado) por el punto de acceso, por consiguiente se elimina la necesidad de las estaciones de contender por el acceso al canal [3].

2.5.1 Estructura del frame 802.11.

El estándar IEEE 802.11 soporta tres tipos diferentes de frames: administración, control, y datos. Las paquetes de administración son usadas para la asociación y disociación de la estación con el punto de acceso, temporización y sincronización, y autentificación y deautentificación. Los paquetes de control son usados para el saludo inicial durante el periodo de contención, para confirmaciones positivas durante el periodo de contención, y para terminar el periodo libre de contención.

Los paquetes de datos son usados para la transmisión de datos durante el periodo de contención y el periodo libre de contención, y pueden ser combinados con peticiones y confirmaciones durante el periodo libre de contención. El formato de paquete del estándar IEEE 802.11 se ilustra en la Figura 2.6.

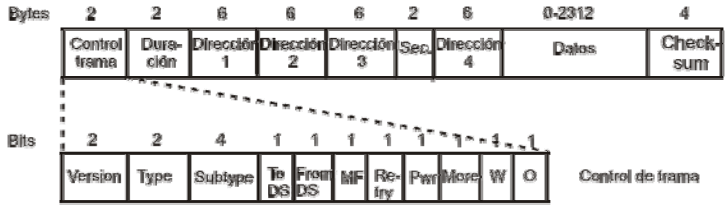

Figura 2.6. Formato de frame del estándar IEEE 802.11

Campo de control de frame contiene la siguiente información:

- Version: Permite dos versiones del protocolo operar al mismo tiempo en la misma celda.
- Type: Identifican al paquete si es de control, administración o datos.
- Subtype: Adicionalmente Identifican el tipo de paquete (RTS, CTS, etc).
- To DS: Indica si el paquete va hacia el sistema de distribución (DS).
- From DS: Indica si el paquete viene del sistema de distribución.
- MF: Este bit indica que se realizaran más fragmentaciones.
- Retry: Este bit marca una retransmisión de un paquete que ya había sido enviado.
- Pwr Mgt: Este bit es usado por la estación base (AP) para poner al receptor en estado dormido o para reactivarlo.
- More: Este bit indica que el transmisor tiene paquetes adicionales pare el receptor.
- W: Este bit especifica que los datos han sido encriptados usando el algoritmo WEP.
- O: Este bit le dice al receptor que una secuencia de paquetes con este bit activado debe ser procesado estrictamente en orden.

Campo de duración: Avisa cuanto tiempo ocuparan el canal el paquete y su confirmación (ACK), para que otras estaciones actualicen su NAV (vector de asignación de red).

Dirección: Contiene cuatro direcciones dos son para la dirección del transmisor y el receptor deseado, y otras dos para los APs fuente y destino para tráfico entre celdas.

Secuencia: Permite a los fragmentos ser numerados. De los 16 bits disponibles, 12 identifican al paquete y 4 al fragmento.

Datos: Contiene los datos útiles, de hasta 2312 bytes.

CheckSum: Chequeo de redundancia cíclica de 32 bits (CRC) se usa para detección de errores.

Los campos de administración tienen un formato similar a los paquetes de datos, excepto que sin una dirección de AP, porque los paquetes de administración están restringidos a una celda. Los paquetes de control son aún más cortos, tiene solo una o dos direcciones, no tienen campo de Datos ni de secuencia. La información clave esta en campo de subtipo, generalmente RTS, CTS o ACK.

2.5.2 Terminal oculta y terminal expuesta.

Una diferencia significativa entre una red de área local inalámbrica y una cableada es el hecho que, en general no se puede considerar una topología totalmente conectada entre los nodos de una red WLAN [4]. Este hecho da lugar a los problemas de terminal “oculta” y terminal “expuesta”. Dado que no todas las estaciones están dentro del rango de uno a otro, las transmisiones en curso en una parte de la celda pueden no ser recibidos en alguna otra parte dentro de la misma celda. El problema de la terminal oculta puede ser ejemplificado por medio de la figura 2.7 (a), donde la estación C está transmitiendo a la estación B. Si A sensa el canal, no escuchara a nadie y falsamente concluirá que puede empezar a transmitir hacia B, ocasionando una colisión. Por otro lado existe el problema inverso, de la terminal expuesta, que se ilustra en la figura 2.7 (b). En este caso B desea enviar hacia C, para poder hacer esto la estación B escucha el canal, cuando escucha una transmisión, falsamente concluye que no puede enviar hacia C aún cuando la estación A esta transmitiendo hacia la estación D. Además, la mayor parte de los radios son half-duplex, lo que significa que no pueden transmitir y escuchar al mismo tiempo en la misma frecuencia.

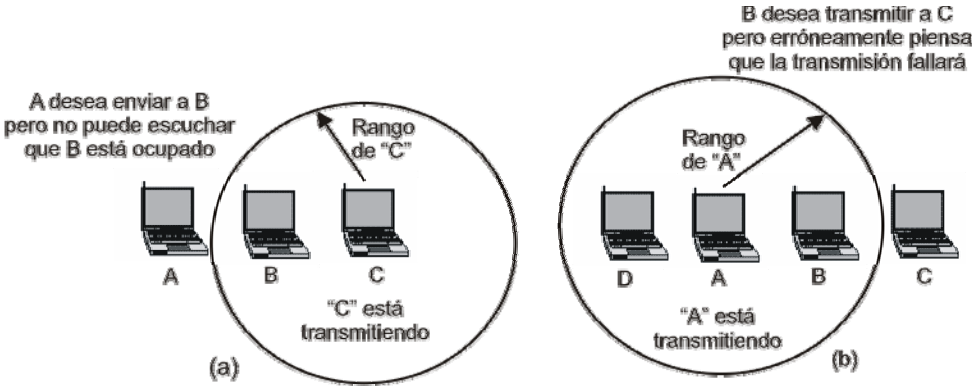

Figura 2.7. (a) Problema de terminal oculta. (b) problema de terminal expuesta.

Para tratar con este problema, 802.11 soporta dos modos de operación. El primero, llamado DCF (Distributed Coordination Function), no utiliza ningún tipo de control central (en ese aspecto, similar a Ethernet). El otro llamado PCF (Point Coordination Function), utiliza el punto de acceso para controlar toda la actividad en su celda. Todas las implementaciones deben soportar DCF pero PCF es opcional [10].

2.5.3 Función de Coordinación Distribuida (DCF).

La función de coordinación distribuida es el método de acceso fundamental usado para soportar transferencia de datos asíncronos sobre el principio básico de mejor esfuerzo. Como se identifica en la especificación, todas las estaciones deben soportar la función de coordinación distribuida. La DCF opera únicamente en la red ad hoc, y opera ya sea únicamente o coexiste con la función de coordinación puntual (PCF) en una red de infraestructura. La arquitectura del MAC esta representada en la Figura 2.8, donde se muestra que la DCF esta directamente encima de la capa física y soporta servicios de contención [3]. Los servicios de contención implican que cada estación con un MSDU en la cola de espera para transmisión debe contender por el acceso al canal y, una vez que el MSDU es transmitido, debe volver a contender para tener acceso al canal para todos los paquetes subsecuentes. Los servicios de contención promueven acceso justo al canal para todas las estaciones.

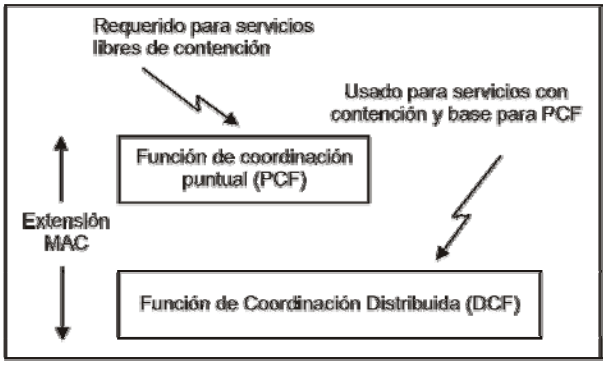

Figura 2.8. Arquitectura MAC.

La función de coordinación distribuida esta basada en acceso múltiple por detección de portadora con evasión de colisiones (CSMA/CA). El acceso múltiple por detección de portadora con detección de colisiones (CSMA/CD) no se usa porque una estación es incapaz de escuchar el canal para detectar colisiones mientras esta transmitiendo.

2.5.3.1 CSMA/CA.

En el estándar IEEE 802.11, la detección de la portadora se realiza en la interfase aérea, referida como *detección física de portadora*, y en la subcapa MAC, referida como *detección de portadora virtual*. La detección física de portadora detecta la presencia de otros usuarios WLAN IEEE 802.11 por medio del análisis de todos los paquetes detectados, y también detecta actividad en le canal a través de la intensidad relativa de la señal de otras fuentes.

Una estación fuente realiza detección de portadora virtual mediante el envío de una unidad de datos de protocolo de comunicación (MPDU-Message Protocol Data Unit) con información de duración en el encabezado de los paquetes petición para enviar (RTS), libre para enviar (CTS) y paquetes de datos. Un MPDU es una unidad de datos completa que se pasa de la subcapa MAC a la capa física. El MPDU contiene información de encabezado, datos útiles, y chequeo de redundancia cíclica de 32 bits. El campo de duración indica la cantidad de tiempo (en microsegundos) después del término del presente paquete que el canal estará ocupado para completar la transmisión exitosa del paquete de datos o de administración. Las estaciones en el conjunto de servicios básicos (BSS) usan la información en el campo de duración para ajustar su vector de asignación de red (NAV), el cual indica la cantidad de tiempo que debe transcurrir hasta que la actual transmisión este completa y el canal pueda ser muestreado otra vez como estado desocupado. El canal se indica como ocupado si los mecanismos de detección de portadora virtual o física indican que el canal esta ocupado.

El acceso prioritario al medio inalámbrico es controlado a través del uso de intervalos de tiempo (IFS – Inter Frame Spacing) entre la transmisión de los paquetes. Los intervalos IFS son periodos obligatorios de tiempo inactivo en el medio de transmisión. En el estándar se especifican tres intervalos IFS que se describen a continuación:

- Short Inter Frame Space (SIFS): El intervalo SIFS es el IFS más pequeño, seguido por PIFS y DIFS, respectivamente. Las estaciones que requieren esperar un SIFS tienen prioridad de acceso sobre aquellas estaciones que tienen que esperar un PIFS o un DIFS antes de transmitir; por consiguiente, el intervalo SIFS tiene la más alta prioridad de acceso al medio de comunicación.
- Point Coordination IFS (PIFS): Es utilizado por el Punto de acceso (AP) para ganar acceso al medio antes que cualquier otra estación al comenzar el periodo libre de contención (CFP). Dado que es más corto que un DIFS le da la capacidad al AP de bloquear trafico asíncrono para poder realizar operaciones limitadas en tiempo.

- Distributed Coordination IFS (DIFS): Es utilizado por una estación cuando opera bajo DCF, y se utiliza como el retardo mínimo para tráfico asíncrono que esta compitiendo por el acceso. Un nodo espera por la duración de un DIFS antes de transmitir cualquier paquete cuando el canal se encuentra libre.

La duración de los IFS, está definido por la duración de una ranura de tiempo y es por lo tanto dependiente de la capa física [12]. La figura 2.9 ilustra el uso de estos intervalos de tiempo y los valores de cada intervalo se muestran en la tabla 2.2.

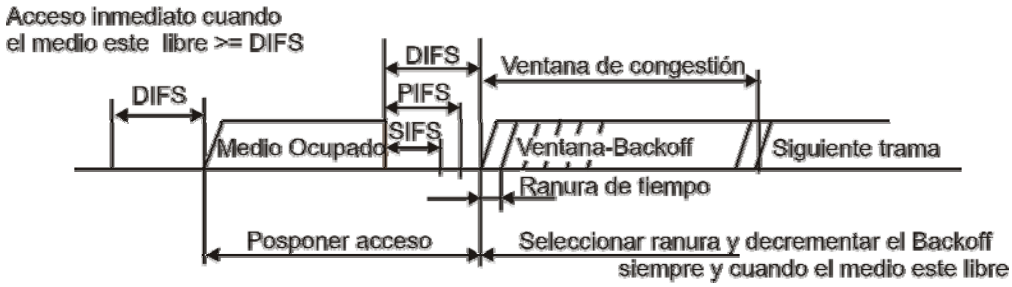

Figura 2.9. Temporización del MAC IEEE 802.11.

Versión	**SIFS**	**Slot time**
802.11	10 μs	20 μs
802.11 a	16 μs	9 μs
802.11 b	10 μs	20 μs
802.11 g	10/16 μs	20/9 μs

Tabla 2.2 valores de tiempo

Los valores de los tiempos PIFS y DIFS se calculan de acuerdo a las siguientes ecuaciones:

$$PIFS = SIFS + SlotTime$$
$$DIFS = SIFS + 2 \times SlotTime$$

En la tabla 2.2 se observa que la versión “g” del estándar utiliza 2 valores de SIFS y de *Slot time* esto es debido a que debe mantener compatibilidad con la versión “b” del estándar cuando se requiere operar en una red mixta (b y g al mismo tiempo), sin embargo, cuando opera con tasas altas similares a la versión “a” utiliza los mismos parámetros de temporización que 802.11 a.

Para el método de acceso básico, cuando una estación detecta que el canal esta libre, la estación espera un periodo DIFS y sensa el canal nuevamente, si el canal aún sigue libre transmite un MPDU. La estación receptora calcula el *checksum* y determina si el paquete fue recibido correctamente. Si la recepción fue correcta, la estación receptora espera un intervalo SIFS y transmite un paquete de confirmación positivo (ACK) de regreso a la estación fuente, indicando que la transmisión fue exitosa. La figura 2.10 es un diagrama de tiempo que ilustra la transmisión exitosa de un paquete de datos. Cuando el paquete de datos es transmitido, el campo de duración del paquete se usa para que todas las estaciones en el conjunto de servicios básicos (BSS) sepan cuanto tiempo estará ocupado el medio. Todas las estaciones que escuchan el paquete de datos ajustan su NAV basados en el valor del campo de duración, que incluye el intervalo SIFS y el ACK que sigue después del paquete de datos.

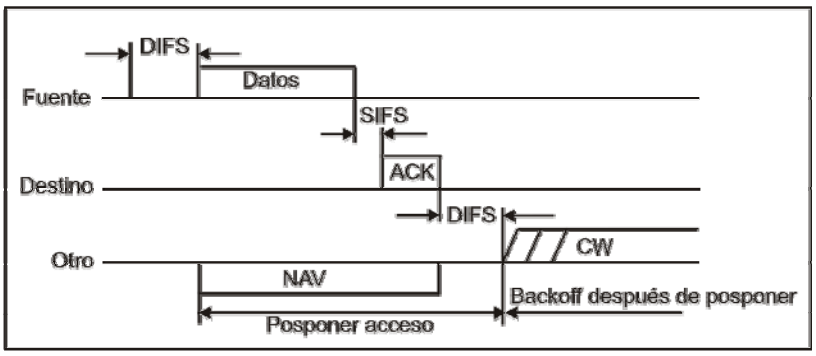

Figura 2.10. Transmisión de un MPDU sin RTS/CTS.

Dado que una estación fuente en un BSS no puede escuchar sus propias transmisiones, cuando ocurre una colisión, la fuente continúa transmitiendo el MPDU completo. Si el MPDU es grande (por ejemplo 2300 octetos), una gran cantidad de ancho de banda del canal se desperdicia debido a un MPDU con errores. Los paquetes de control RTS y CTS pueden ser usados por una estación para reservar ancho de banda del canal previo a la transmisión de un MPDU y para minimizar la cantidad de ancho de banda desperdiciada cuando ocurre una colisión. Los paquetes de control RTS y CTS son relativamente pequeños (RTS es de 20 octetos y CTS de 14 octetos) cuando se comparan al máximo tamaño de paquete de datos (2346 octetos). El paquete de control RTS se transmite primero por la estación fuente (después de una exitosa contienda por el canal) que tiene paquete de administración o datos en la cola de espera de transmisión hacia una estación destino especificado.

Todas las estaciones en el BSS, que escuchan el paquete RTS, leen el campo de duración (ver Fig. 2.6) y ajustan su NAV de acuerdo a este valor. La estación destino responde al paquete RTS con un paquete CTS después de que un periodo inactivo SIFS ha transcurrido. Las estaciones que escuchan el paquete CTS observan el campo de duración y nuevamente actualizan su NAV. Si la recepción del paquete CTS es exitosa, la estación fuente esta virtualmente asegurada que el medio es estable y reservado para la transmisión exitosa de un MPDU. Se debe notar que las estaciones son capaces de actualizar su NAV basados en el paquete RTS de la estación fuente y del CTS de la estación destino, el cual ayuda a combatir el problema de la "terminal oculta". La Figura 2.11 ilustra la transmisión de un MPDU usando el mecanismo RTS/CTS. Las estaciones pueden escoger en nunca usar RTS/CTS, usar RTS/CTS cuando el MSDU exceda el valor de RTS_Threshold (parámetro manejable), o siempre usar RTS/CTS. Si una colisión ocurre con un MPDU RTS o CTS, se desperdicia mucho menor ancho de banda en comparación con un gran MPDU de datos. Sin embargo, para un medio cargado ligeramente, un retardo adicional se impone por la información incluida en los paquetes RTS/CTS.

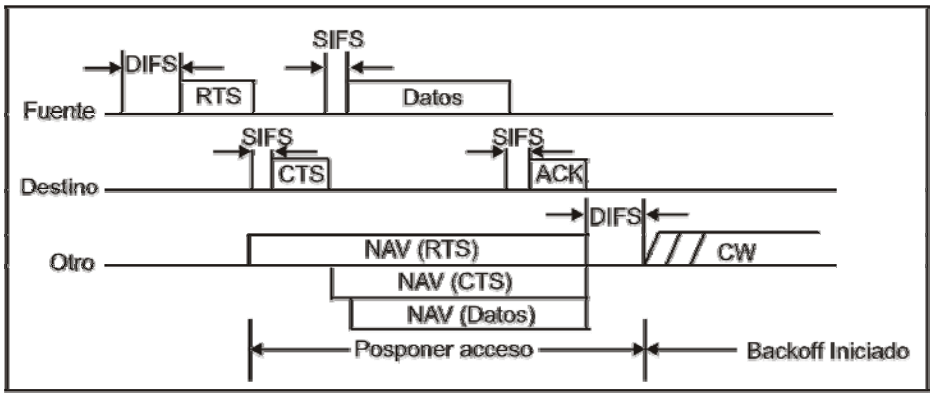

Figura 2.11. Transmisión de un MPDU usando RTS/CTS.

Los MSDUs grandes que pasan del LLC a la subcapa MAC podrían requerir fragmentación para incrementar la confiabilidad de la transmisión. Para determinar si se realiza la fragmentación, los MPDUs son comparados a un parámetro controlable que se le llama Umbral_de_Fragmentación (Fragmentation_Threshold). Si el tamaño del MPDU excede el valor de este umbral, el MSDU se divide en múltiples fragmentos. Los MPDUs resultantes son de tamaño igual al Umbral_de_Fragmentación, excepto el último MPDU, que es de tamaño variable y no excede el tamaño del umbral.

Cuando un MSDU se fragmenta, todos los fragmentos se transmiten secuencialmente (Figura 2.12).

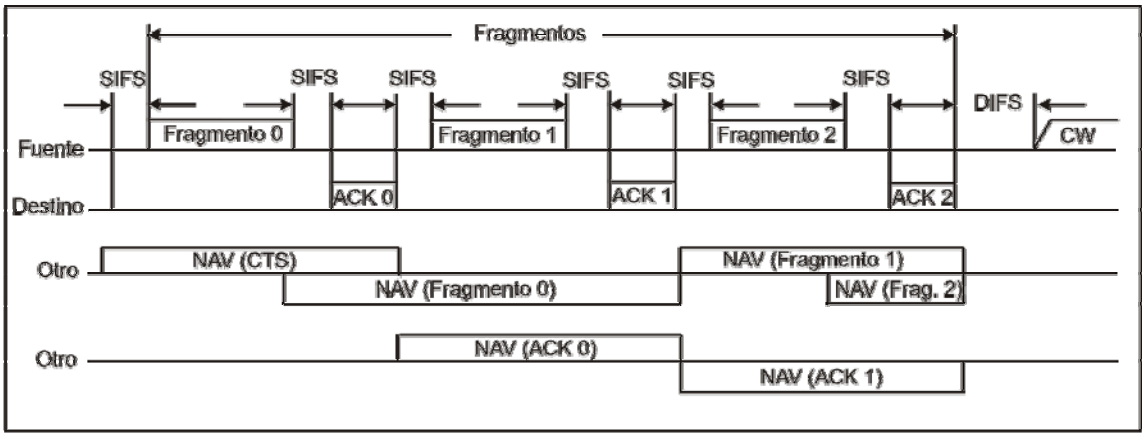

Figura 2.12. Transmisión de un MPDU fragmentado.

El canal no se libera hasta que se haya transmitido de manera exitosa el MSDU completo, o la estación fuente no reciba un reconocimiento por un fragmento transmitido. La estación destino manda un reconocimiento positivo por cada fragmento recibido exitosamente mediante el envío de un paquete DCF ACK hacia la estación fuente. La estación fuente mantiene el control del canal durante toda la transmisión del MSDU ya que solo espera un periodo SIFS después de que recibe el paquete ACK y luego transmite el siguiente fragmento. Cuando la estación fuente no recibe un ACK por un fragmento transmitido previamente, la estación fuente detiene la transmisión y vuelve a contender por el canal. Una vez que la estación fuente vuelve a ganar el canal, empieza a transmitir el último fragmento no confirmado.

Si se utilizan paquetes RTS y CTS, solo el primer fragmento se envía empleando este mecanismo de inicio de transmisión. El campo de duración de los paquetes RTS y CTS solo cuenta para la transmisión del primer fragmento hasta la transmisión de su paquete ACK (del primer fragmento). Las estaciones en el BSS en lo sucesivo mantienen actualizado su NAV mediante la extracción del campo de duración de todos los paquetes subsecuentes.

La parte de evasión de colisiones de CSMA/CA se realiza a través de un procedimiento de *backoff* aleatorio. Si una estación tiene un paquete para transmitir e inicialmente detecta que el canal esta ocupado; entonces la estación espera hasta que el canal este libre por un periodo DIFS, y luego calcula un tiempo de *backoff* aleatorio.

Para el estándar IEEE 802.11, el tiempo esta dividido en periodos que corresponden a una ranura de tiempo (Slot_Time). A diferencia de Aloha ranurado, donde la ranura de tiempo es igual al tiempo de transmisión de un paquete, la ranura de tiempo (Slot_Time) utilizado en 802.11 es mucho más pequeño que un MPDU y se usa para definir los intervalos IFS y para determinar el tiempo de *backoff* para las estaciones en el periodo de contención. El Slot_Time es diferente para cada implementación de capa física.

2.5.3.2 Algoritmo "*Exponential Backoff*".

El tiempo de backoff aleatorio es un valor entero que corresponde a un número de ranuras de tiempo. Inicialmente, la estación calcula el tiempo backoff en el rango de 0-7. Después de que el medio se torna libre después de un periodo DIFS, las estaciones decrementan su temporizador de backoff hasta que el medio se torna ocupado otra vez o el temporizador llega a cero. Si el temporizador no ha llegado a cero y el medio se torna ocupado, la estación congela su temporizador. Cuando el temporizador finalmente se ha decrementado hasta cero, la estación transmite su paquete. Si dos o mas estaciones decrementan a cero al mismo tiempo, ocurrirá una colisión, y cada estación tendrá que generar un nuevo tiempo de backoff en el rango de 0-15. Por cada intento de retransmisión, el tiempo de backoff crece $\lfloor 2^{2+i} \cdot ranf() \rfloor \cdot Slot\_Time$, donde i es el número de veces consecutivas que una estación intenta transmitir un MPDU, $ranf()$ es una variable aleatoria uniforme entre (0,1), y $\lfloor x \rfloor$ representa el entero mas grande menor que o igual a x. El periodo inactivo después de un periodo DIFS se le conoce como *ventana de contención* (CW).

La ventaja de este método de acceso al canal es que promueve igualdad entre las estaciones, pero su debilidad es que probablemente no podría soportar DTBS. La igualdad se mantiene porque cada estación debe volver a competir por el canal después de cada transmisión de un MSDU. Todas las estaciones tienen igual probabilidad de ganar el acceso al canal después de cada intervalo DIFS. Los servicios limitados en tiempo típicamente soportan aplicaciones tales como video o voz en paquetes que deben ser mantenidos con un retardo mínimo especificado. Con DCF, no hay un mecanismo que garantice un retardo mínimo a las estaciones que soportan servicios limitados en tiempo.

2.5.4 Función de Coordinación Puntual (PCF).

La función de coordinación puntual es una capacidad opcional, el cual es orientado a conexión y proporciona transferencia de tramas libres de contención (CF). El PCF depende del coordinador puntual (PC) para realizar encuestas (polling), permitiendo a las estaciones encuestadas transmitir sin necesidad de contender por el canal. La función del coordinador puntual es realizada por el punto de acceso (AP) dentro de cada conjunto de servicios básicos (BSS). Las estaciones dentro del BSS que son capaces de operar en el periodo libre de contención (CFP) son conocidos como estaciones enteradas libres de contención (CF-aware stations). El método mediante el cual se mantiene las tablas de encuestas y se determina la secuencia de las encuestas, se deja al implementador [3].

El PCF debe coexistir con el DCF y lógicamente se encuentra por encima del DCF (ver figura 2.8). El intervalo de repetición CFP (CFP_Rate) se usa para determinar la frecuencia con el cual ocurre el PCF. Dentro de un intervalo de repetición, una parte del tiempo es asignado a tráfico libre de contención, y el resto se proporciona para tráfico basado en contención. El intervalo de repetición CFP se inicia por un “beacon frame”, que es transmitido por el AP. Una de sus funciones principales es sincronización y temporización. La duración del intervalo de repetición CFP es un parámetro manejable que es siempre un número completo (integral number) de “beacon frames”. Una vez que se ha establecido el CFP_Rate, se puede determinar la duración del CFP. El tamaño máximo del CFP se determina por medio del parámetro manejable CFP_Max_Duration. El valor mínimo del parámetro CFP_Max_Duration es el tiempo requerido para transmitir dos MPDUs de tamaño máximo, incluyendo los sobre encabezados, el “beacon frame” inicial y una trama CF_End. El valor máximo de CFP_Max_Duration es el intervalo de repetición CFP menos el tiempo requerido para transmitir exitosamente un MPDU de tamaño máximo durante el periodo de contención (CP) (el cual incluye el tiempo de establecimiento de conexión RTS/CTS y el ACK). Por consiguiente, el tiempo debe ser dividido para que al menos un MPDU sea transmitido durante el periodo de contención. Le concierne al AP determinar cuanto tiempo operar el CFP durante cualquier intervalo de repetición dado. Si el tráfico es muy ligero, el AP puede reducir el CFP y proporcionar el restante del intervalo de repetición para el DCF. El CFP también podría ser reducido si el tráfico DCF del intervalo de repetición previo se prolonga (carry over) al intervalo actual. La cantidad máxima de retardo en la que se puede incurrir es el tiempo que se toma en transmitir el RTS/CTS, un MPDU máximo y el ACK.

La figura 2.13 es un bosquejo del intervalo de repetición CFP, que ilustra la coexistencia de DCF y PCF.

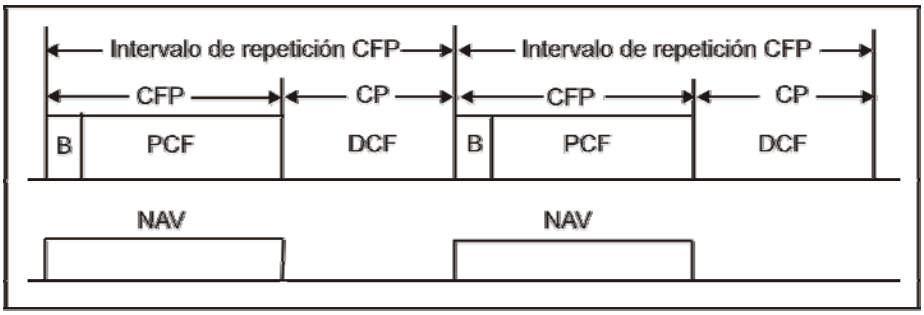

Figura 2.13. Coexistencia de DCF y PCF.

En el inicio de un intervalo de repetición CFP, todas las estaciones en el BSS actualizan su NAV a la máxima duración del CFP (i.e., CFP_Max_Duration). Durante el CFP, el único tiempo en que las estaciones están permitidas para transmitir es en respuesta a un sondeo (poll) del coordinador puntual (PC) o para transmisión de un ACK que es después de un intervalo SIFS de haber recibido un MPDU. En el inicio del CFP el coordinador puntual hace una detección del medio, si el medio permanece desocupado por un intervalo PIFS transmite un "beacon frame" (B) para iniciar el CFP. El coordinador puntual empieza la transmisión libre de contención (CF) después de un intervalo SIFS de que se ha transmitido el "beacon frame" mediante el envío de tramas CF-Poll (no datos), Datos, o Datos+CF-Poll. El coordinador puntual puede terminar inmediatamente el CFP mediante la transmisión de una trama CF-End, lo cual es común si la red está ligeramente cargada y el coordinador puntual no tiene tráfico en la cola de espera. Si una estación enterada libre de contención (CF-aware station) recibe una trama CF-poll (no datos) del coordinador puntual, la estación puede responder después de un periodo desocupado SIFS, con una trama CF-ACK (no datos) o Datos+CF-ACK. Si el coordinador puntual recibe una trama Datos+CF-ACK de una estación, el PC puede enviar una trama Datos+CF-ACK+CF-Poll a una estación diferente, donde la porción CF-ACK de la trama se usa para confirmar la recepción de la trama de datos previa. La capacidad de combinar tramas de sondeo (polling) y de confirmación con tramas de datos transmitidas entre estaciones y el coordinador puntual, fue diseñada para mejorar la eficiencia. Si el PC transmite una trama CF-Poll (no datos) y la estación destino no tiene datos para transmitir, la estación envía una trama de Función Nula (no datos) de regreso al coordinador puntual.

La figura 2.14 ilustra la transmisión de tramas entre el coordinador puntual y una estación, y viceversa. Si el PC falla al recibir un ACK de una trama de datos transmitida, el PC espera por un intervalo PIFS y continua transmitiendo a la siguiente estación en la lista de sondeo (polling list).

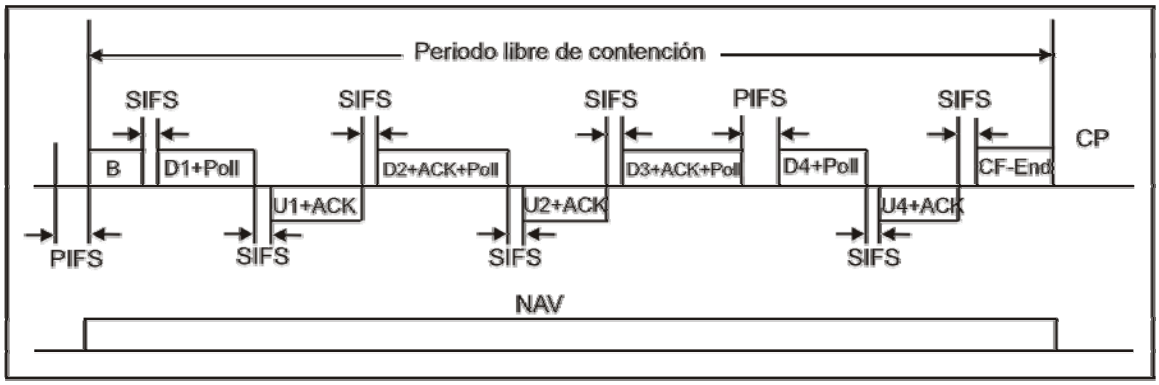

Figura 2.14. Transmisión de PC-a-estación.

Después de recibir el sondeo del PC, como se describió anteriormente, la estación puede escoger transmitir una trama a otra estación en el BSS. Cuando la estación destino recibe la trama, se envía un DCF ACK a la estación fuente y el PC espera por un intervalo PIFS después de la trama ACK para poder transmitir cualquier trama adicional. La figura 2.15 ilustra la transmisión de tramas de estación a estación durante el CFP.

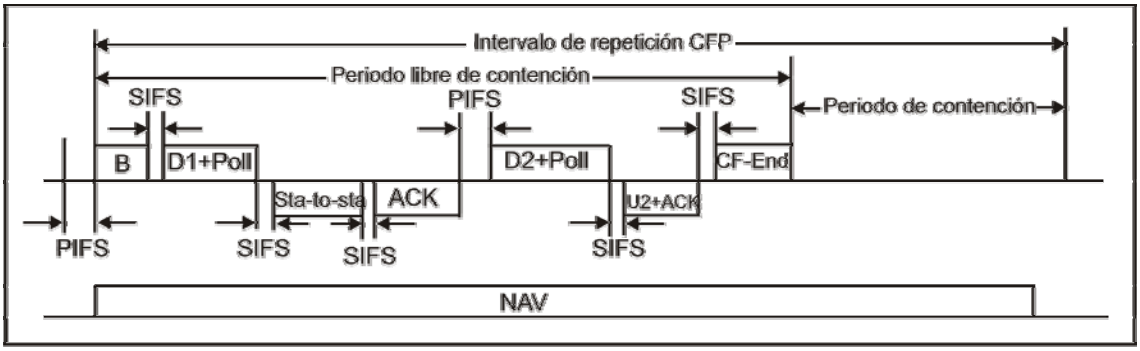

Figura 2.15.Transmisión de estación a estación.

El Coordinador puntual puede escoger transmitir una trama a una estación no-CF-aware. Una vez recibida una trama exitosa, la estación esperará un intervalo SIFS y responderá al PC con una trama ACK standard. La fragmentación y reagrupación son adecuados con el valor empleado de Umbral_de_Fragmentación (Fragmentation_Threshhold) para determinar cuales MSDUs son fragmentados previo a su transmisión. Es responsabilidad de la estación destino reagrupar los fragmentos para formar el MSDU original.

2.5.5 Subcapa Mac para 802.11 b/g.

La arquitectura básica, características y servicios de 802.11 b/g están definidos en el estándar original 802.11, con cambios hechos solamente en la capa física. Estos cambios resultan en tasas de datos más altas y una conectividad más robusta [14].

2.5.6 Subcapa Mac para 802.11a.

El estándar 802.11a utiliza las mismas funciones MAC que 802.11b, la herencia del formato del paquete de la tecnología 802.11 a 802.11a no tendrá un impacto significativo en las operaciones de red. Sin embargo, una desventaja del formato MAC 802.11 es que mientras la capa física se ha mejorado con incremento de potencia y un nuevo esquema de codificación, el formato MAC reduce el efecto de estas mejoras debido a un "overhead "significativo, causado por el objetivo y diseño de proporcionar un ambiente eficiente y libre de colisiones. Debido a la herencia de la ineficiencia del MAC 802.11b, las tasas esperadas de 802.11a están en el rango de 38 Mbps, para 54 Mbps. A diferencia de 802.11b, 802.11a no requiere encabezados para transmitir a 1 Mbps, lo cual en teoría podría incrementar la eficiencia del throughput esperado en un 15% [14].

2.6 RANGOS DE PROPAGACION DE LA SEÑAL.

Como se mencionó anteriormente, la responsabilidad del Protocolo MAC es el arbitraje de accesos a un medio compartido entre varios sistemas finales. En el estándar IEEE 802.11, esto se realiza por medio de un mecanismo estocástico y distribuido Ethernet: Acceso Múltiple por detección de portadora con evasión de colisiones (CSMA/CA). IEEE 802.11 especifica dos protocolos de control de acceso al medio, Función de Coordinación Puntual (PCF) y función de Coordinación Distribuida (DCF). DCF es un esquema totalmente distribuido, mientras que PCF es un esquema centralizado construido en la cima de DCF.

En la figura 2.16 se definen los diferentes rangos que se utilizan para este estándar: Rango de transmisión, rango de detección de portadora y rango de interferencia [13]. En la siguiente descripción consideramos a B como la fuente y A como el receptor para una transmisión en curso.

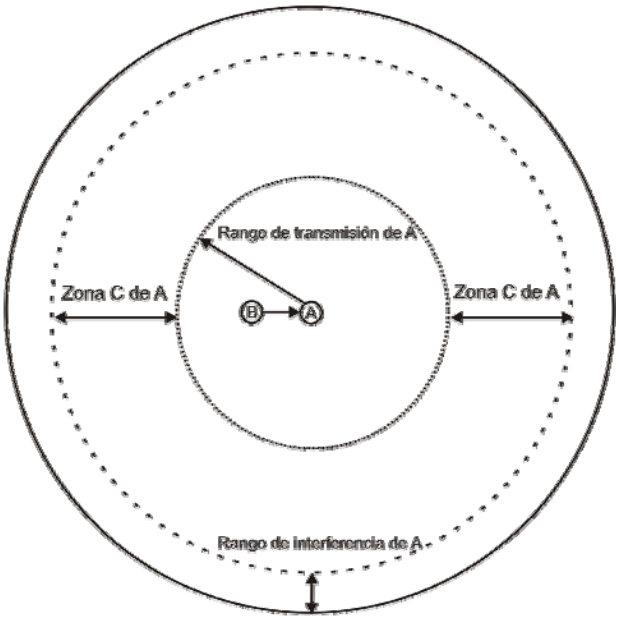

Figura 2.16. Ilustración de los rangos de transmisión, detección de portadora y de interferencia.

Rango de Transmisión: Este representa el rango dentro del cual un paquete puede ser recibido exitosamente, considerando que no hay interferencia de otros nodos.

Rango de detección de portadora: El rango dentro del cual se puede detectar una transmisión se le llama rango de detección de portadora. Este es siempre mas grande (hasta 2 veces mas grande) que el rango de transmisión. Se debe de notar que diferentes niveles de potencia resultan en diferentes tamaños para los rangos de transmisión y de detección de portadora, considerando al rango de transmisión como parte del rango de detección de portadora. Dada una potencia de transmisión; la mayor parte de las tarjetas WLAN consideran que los rangos de transmisión y detección de portadora son fijas. La *Zona de Detección de Portadora* (*Zona-C*) se define como el área donde una señal puede ser detectada, pero no puede ser decodificada.

Rango de Interferencia: Esta zona representa el rango dentro del cual un nodo en el modo de recepción puede ser interferido por otra transmisión. El rango de interferencia puede variar dependiendo de la distancia entre transmisor y receptor, del nivel de potencia con el que se transmite el paquete y también del número de transmisiones en curso en la vecindad del nodo. Por lo tanto el tamaño del rango de interferencia puede variar.

2.7 SERVICIOS.

El estándar 802.11 establece que cada red inalámbrica de área local (WLAN) debe proporcionar nueve servicios. Estos servicios están divididos en dos categorías: cinco servicios de distribución y cuatro servicios de estación. Los servicios de distribución se refieren a la administración de membresías (asociaciones) en la celda e interacción con estaciones fuera de la celda. En contraste, los servicios de estación se refieren a la actividad dentro de una simple celda.

Los cinco servicios de distribución son proporcionados por las estaciones base y tratan con la movilidad de las estaciones conforme entran y salen de la celda, conectándolos o desconectándolos de las estaciones base. Los cinco servicios son los siguientes:

Asociación. Este servicio es utilizado por estaciones móviles para conectarse a las estaciones base. Típicamente, este servicio se utiliza justo después de que una estación entra dentro del rango de una estación base. Cuando esto sucede, la estación anuncia su identidad y sus capacidades. Las capacidades incluyen tasa de datos soportada, necesidad de servicios PCF (por ejemplo: polling), y requerimientos de administración de potencia. La estación base puede aceptar o rechazar a la estación móvil. Si la estación móvil es aceptada, se debe de autenticar.

Disociación: El servicio que cancela el enlace inalámbrico entre la estación móvil y la estación base, de esta forma rompiendo la conexión. Una estación móvil debe usar este servicio antes de apagarse o de moverse a otro lugar, de la misma manera la estación base antes de apagarse para mantenimiento.

Reasociación: Una estación puede cambiar a su estación base preferida utilizando este servicio. Esta habilidad es útil para estaciones que se mueven de una celda a otra. Dos celdas (BSS) adyacentes forman una ESS si están definidas por un ESSID común, proporcionándole a una estación la capacidad de moverse de un área hacia otra.

Si la reasociación se utiliza correctamente no se perderán datos como consecuencia de la transferencia.

Distribución: Este servicio determina como enrutar tramas enviadas a la estación base. Si el destino es local a la estación base, las tramas pueden ser enviadas directamente al aire. En otro caso, las tramas tienen que ser reenviados sobre la red cableada. Este servicio se realiza a través del sistema de distribución (DS) y es usado en casos especiales en la transmisión de tramas entre estaciones base.

Integración: Si una trama necesita ser enviada a través de una red no 802.11 con un sistema de direccionamiento o formato de trama diferente, este servicio manipula la traducción del formato 802.11 al formato requerido por la red destino.

Los cuatro servicios restantes son dentro de la celda (esto es, relacionados a las acciones dentro de una simple celda). Estos servicios son usados después de que ha tomado lugar la asociación y es como sigue:

Autenticación: Debido a que las comunicaciones inalámbricas pueden ser fácilmente enviadas o recibidas por estaciones no autorizadas, una estación se debe autenticar antes de que le sea permitido enviar datos. Después de que una estación móvil ha sido asociada por la estación base (esto es, aceptada dentro de su celda), la estación base le envía un frame de pregunta para ver si la estación móvil conoce la clave secreta que le ha sido asignada. Esto prueba su conocimiento de la clave secreta mediante la encripción de la trama de pregunta y enviándola de regreso a la estación base. Si el resultado es correcto, la estación móvil esta completamente dada de alta en la celda.

Deautenticación: Cuando una estación previamente autenticada quiere dejar la red, es deautenticada. Después de la deautenticación, ya no puede usar la red.

Privacidad: Para que la información enviada sobre una red inalámbrica se mantenga confidencial, debe ser encriptada. Este servicio administra la encripción y desencripción. El algoritmo de encripción especificado es el RC4, inventado por Ronald Rivest del MIT.

Entrega de datos: El servicio principal de la capa MAC es el de proporcionar intercambio de tramas entre capas MAC. Las estaciones móviles usan el algoritmo de Acceso Múltiple por Detección de Portadora (CSMA/CA) como el esquema de acceso al medio.

CAPÍTULO III
PROTOCOLO DE ACCESO MULTIPLE CONTROLADO POR POTENCIA, PARA REDES INALAMBRICAS DE PAQUETES.

3.1 INTRODUCCION.

Un tema importante en las redes inalámbricas es el desarrollar protocolos de acceso al medio eficientes que optimicen el reuso espectral, y por lo tanto, maximicen la utilización del canal. Estudios teóricos recientes han mostrado que los protocolos de acceso al medio ideales que usan control de potencia óptimo pueden mejorar la utilización del canal por un factor de $O\left(\sqrt{\rho}\right)$, donde ρ es la densidad de nodos en la región (usando aproximaciones de modelo fluido). Esto motiva el estudio de protocolos de acceso al medio inalámbrico controlados por potencia [6], [17].

Trabajos anteriores en control de potencia han tratado principalmente con redes celulares, donde bandas de frecuencia separadas son asignadas típicamente para canales de subida y de bajada y las estaciones base proporcionan control centralizado. También se han presentado algoritmos de control de potencia distribuido, en el sentido de que estaciones base individuales controlan la potencia. Sin embargo, estas técnicas todavía requieren la configuración celular fundamental (usuarios móviles se comunican a través de estaciones base – acceso centralizado). Otro tipo de trabajos se han enfocado en protocolos MAC que controlan el nivel de potencia de transmisión para conservar el consumo de potencia.

Los protocolos MAC con evasión de colisiones basados en acceso múltiple, han utilizado potencia de transmisión fija, y no han considerado mecanismos de control de potencia basados en la distancia entre el transmisor y el receptor con el fin de mejorar el reuso espacial del canal inalámbrico.

El protocolo de acceso múltiple controlado por potencia (**PCMA**) generaliza el modelo de evasión de colisiones transmitir-posponer "*on / off*" de protocolos actuales a un modelo de supresión de colisiones más flexible "Potencia limitada variable". El algoritmo esta aprovisionado (estipulado) para redes ad hoc y no requiere la presencia de estaciones base para administrar la potencia de transmisión (es descentralizado).

La ventaja de implementar un protocolo controlado por potencia en una red ad hoc es que los pares fuente-destino pueden estar empacados más estrechamente en la red permitiendo un número mas grande de transmisiones simultáneas (reuso espectral/espacial).

3.2 EL PROBLEMA Y LA METODOLOGIA PARA LA SOLUCION.

Los protocolos MAC basados en acceso múltiple con evasión de colisiones consideran de que un par transmisor-receptor debería primero "obtener el espacio físico" antes de iniciar una transmisión de paquetes de datos. Obtener el espacio físico permite al transmisor-receptor evadir las colisiones debido a estaciones ocultas y expuestas en redes inalámbricas de canal compartido (La figura 3.1 ilustra este escenario). El mecanismo del protocolo que se usa para lograr tal evasión de colisiones típicamente involucra un saludo con un intercambio de paquetes de control RTS/CTS (request-to-send / clear-to-send) entre el transmisor y el receptor que antecede a la transmisión de paquetes de datos. Este saludo permite a cualquier estación que escuche un paquete de control o detecte una portadora ocupada, que evite una colisión mediante posponer su propia transmisión mientras la transmisión de datos este en progreso (como se muestra en la figura 3.1).

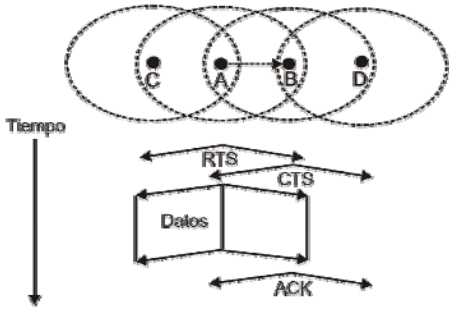

Figura 3.1. Operación general del protocolo para Acceso Múltiple con Evasión de Colisiones.

La parte de arriba de la figura 3.1 muestra cuatro nodos inalámbricos que tienen un rango de transmisión mostrados por las elipses punteadas. A es el transmisor y B es su receptor deseado, C es la estación expuesta (en el rango del transmisor, pero no del receptor) y D es la estación oculta (dentro del rango del receptor, pero no del transmisor). Se observa que para una transmisión exitosa entre A y B, D no debe transmitir. Cuando A desea enviar un paquete de datos a B, este sensa el canal para ver si está libre. Si el canal está libre A envía un paquete RTS hacia B. Si el nodo C escucha el RTS, este pospone su transmisión hasta que A pueda escuchar el CTS del nodo B. Si B está libre para recibir, envía de regreso un paquete CTS al nodo A. Cuando D escucha el CTS, este pospone su transmisión hasta que

A termine de enviar sus datos a B. Cuando C detecta una portadora ocupada este pospone su transmisión. Después de que B recibe el paquete de datos correctamente, envía un paquete ACK a la estación A. Esta es la operación ideal del protocolo.

Mediante el envío de paquetes RTS/CTS se obtiene el espacio físico para evitar colisiones debido a estaciones ocultas y expuestas que es sin duda un requerimiento fundamental para la operación eficiente del acceso al medio inalámbrico, este método prohíbe múltiples transmisiones concurrentes sobre el espacio físico obtenido. Para optimizar el reuso espacial del canal en una red de canal inalámbrico compartido, un par de nodos en comunicación deben obtener tan solo la *mínima área* del espacio físico que necesiten para completar exitosamente una transmisión de datos (La figura 3.2 ilustra este escenario).

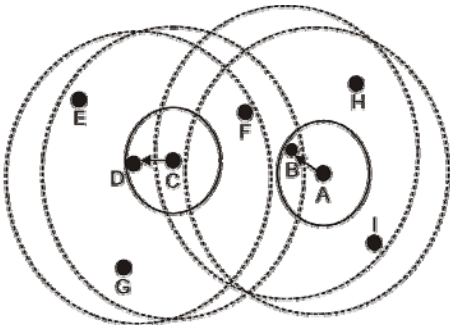

Figura 3.2. Motivación para control de potencia en Acceso al medio basado en evasión de colisiones.

Desafortunadamente, el mecanismo de evasión de colisiones considerado arriba (para 802.11) para que funcione correctamente, los paquetes de control y datos deben ser transmitidos con una *potencia fija* por la siguiente razón. Cuando A esta enviando datos a B, el CTS de B debe llegar a cada estación oculta cuya transmisión pueda causar una colisión en B. De la misma manera, el RTS de A debe llegar a cada estación expuesta con quien su transmisión de datos pueda colisionar. Esto significa que el intercambio RTS-CTS debe adquirir el canal en un rango máximo sobre el cual cualquier estación expuesta u oculta pueda causar colisiones (una función de la potencia de transmisión máxima de una estación interferente). De esta manera aún si la transmisión de datos de A se envía a una potencia más baja (para propósitos de conservación de potencia), el par A-B debe adquirir el canal considerando la potencia de transmisión del peor de los casos de todas las otras estaciones (potenciales interferentes) en su región.

Desde la perspectiva de reuso de canal, esto implica que ajustando la transmisión para datos no tiene impacto en términos de incrementar el reuso del canal, y es equivalente al protocolo MAC de "potencia fija". En resumen, debido a que los paquetes de control necesitarán ser transmitidos con la misma potencia fija (máxima), los actuales protocolos MAC de acceso múltiple que siguen el esquema anterior no pueden cambiar adaptivamente el tamaño del espacio físico obtenido dependiendo de que tan cerca estén el transmisor del receptor.

Para la colocación de nodos mostrada en la figura 3.2, en un protocolo tradicional MAC basado en evasión de colisiones, si C esta enviando a D entonces A no podría enviar a B dado que B escucharía el RTS de C y detectaría la transmisión en curso. Sin embargo, si C reduce su potencia de transmisión tal que sea suficiente para D capturar su señal entonces otros nodos en la región (por ejemplo A) también podrían proceder con su transmisión. Tal protocolo permitiría un empacamiento más ajustado de pares fuente-destino dentro del entorno de red, consecuentemente mejorando el reuso espectral.

El objetivo es cambiar el modelo de transmisión "potencia fija on / off" de los protocolos existentes, a un modelo de transmisión mas flexible "Control de potencia variable y limitado", por consiguiente cambiar el modelo de obtención de espacio físico fijo a un modelo de obtención de espacio físico adaptivo para evasión de colisiones.

El cambio fundamental que se hace en el método existente es el siguiente: A diferencia de los protocolos actuales que usan la recepción de paquetes de control (RTS/CTS) como una acción on-off para transmitir / posponer por estaciones expuestas y ocultas, este método usa la *intensidad de señal de un mensaje de control recibido, para limitar* la potencia de transmisión de estas estaciones. Este mensaje de control (se envía en un canal de frecuencia diferente a los mensajes de datos) es una "versión generalizada de CTS", el cual se describe en la sección 3.4 como un pulso de señal en un canal de "tono ocupado". Sin embargo, la recepción por una estación oculta no prohíbe la transmisión. En este caso, cada nodo oculto limita su potencia de transmisión en función de la intensidad de la señal recibida del CTS generalizado en el nodo. Dado un mecanismo que permite a los nodos avisar su tolerancia a interferencia manipulando la potencia de transmisión del CTS generalizado, se tiene la capacidad de lograr acceso múltiple controlado por potencia apegándose a dos principios claves:

1) El *principio de conservación de potencia* dicta que cada estación debe transmitir con el nivel de potencia mínimo que se requiere para ser escuchado exitosamente por el receptor deseado, bajo las condiciones de red actual (esto es ganancia de canal entre el par fuente-destino y potencia de ruido observado en el destino), y
2) El *principio de cooperación* dicta que ninguna estación que comience una nueva transmisión debe transmitir lo suficientemente fuerte que disturbe transmisiones en curso.

Implementando estos dos principios, en coordinación con el mecanismo para avisar la tolerancia a la interferencia a través de la generalización del CTS, se logra acceso múltiple controlado por potencia eficiente dentro del esquema de los protocolos de evasión de colisiones.

3.3 LOS MODELOS DE CANAL Y DE RED.

Como en IEEE 802.11 y otros protocolos de acceso múltiple, se considera un modelo de canal compartido en el cual las transmisiones simultáneas en la vecindad del receptor resultarán en una colisión en el receptor. En una capa física de espectro disperso, este modelo (acceso al canal compartido) corresponde a un grupo de nodos que accedan al medio con el mismo patrón de saltos de frecuencia en espectro disperso por saltos en frecuencia, o la misma secuencia de número pseudo aleatorio en espectro disperso de secuencia directa. En la capa MAC, no se considera un modelo celular, y no se forza a estaciones base designadas a ser transmisores o receptores de datos.

3.3.1 Modelos de Propagación del canal.

El porcentaje de reuso espacial y potencia de transmisión requerida para que un nodo envíe una señal válida a su destino dependerá de la *ganancia* entre cada fuente y destino, el cual modela la *atenuación de la potencia del transmisor sobre la distancia.* Se definen dos regiones en redes WLAN 802.11 de pérdidas por trayectoria: la región donde la ganancia cae proporcionalmente con la distancia al cuadrado (dentro de la zona de Fresnel) y se refiere al área $1/d^2$ y la región (fuera de la zona de Fresnel o mas allá de la distancia de sobre cruce (cross-over distance)) donde la ganancia es proporcional a la distancia a la cuarta potencia y se refiere al área $1/d^4$ (modelo de los dos rayos).

En el diseño del protocolo, se mide la ganancia actual G_{ij} basada en la potencia del transmisor (anunciado en el paquete) y la potencia en el receptor. Entonces se compensa para considerar las distorsiones introducidas por el desvanecimiento, por un factor de la amplitud del desvanecimiento rápido (una función del modelo del canal).

En PCMA, se considera que:

1. Los canales de datos y de tono de ocupado observan ganancias similares.
2. Se mantiene la reciprocidad del canal de tal manera que la ganancia entre dos nodos es aproximadamente la misma en ambas direcciones.
3. La ganancia del canal es estacionaria por la duración de la transmisión de los paquetes de datos y de control.

Para asegurar que la ganancia en los canales de datos y de tono de ocupado sea similar (la primera consideración), las componentes de frecuencia del tono de ocupado deben estar dentro del ancho de banda coherente del canal de datos. El ancho de banda coherente es inversamente proporcional a la dispersión de retardo multitrayectoria, el cual puede variar considerablemente dependiendo del medio ambiente. En muchos ambientes de exteriores la dispersión de retardo puede ser más grande que $1\mu s$ resultando en un ancho de banda coherente de 1MHz. Sin embargo, también hay obligaciones de mínimo espaciamiento de canal impuestas como un resultado del protocolo que requiere que el tono de ocupado sea transmitido por los receptores al mismo tiempo que recibe los datos. Por consiguiente, para evitar que los pulsos de tono de ocupado en transmisión degraden los datos, es necesario colocar el canal de tono de ocupado fuera de la banda de coherencia. Un método que permite evitar este problema es permitir que el pulso de tono de ocupado degrade los datos y se considere que los datos tienen una cantidad suficiente de redundancia para corregir los errores. Esto se simplifica por el hecho de que el receptor conoce las posiciones de los bits que podrían ser degradados por la transmisión del tono de ocupado.

Existen tres efectos del canal básicos: pérdida por trayectoria el cual esta directamente relacionado a la separación entre fuente y destino, ensombrecimientos (shadowing) el cual se debe a objetos entre la fuente y el destino que atenúan la señal, y multitrayectorias las cuales son el resultado de múltiples trayectorias (entre el transmisor y receptor) y que se combinan en el receptor.

La distancia es la misma en ambas direcciones (esto es, de fuente a destino y de destino a fuente) y los objetos que bloquean las trayectorias son los mismos en ambas direcciones. Sin embargo, la manera en que las trayectorias se refractan en los objetos y se combinan en la fuente y los receptores destino pueden diferir dependiendo de la magnitud de los efectos multitrayectoria. Por consiguiente, solo las multitrayectorias afectan la validez de la segunda consideración. Sin embargo, siempre y cuando los efectos multitrayectoria sean pequeños la consideración se mantiene. La tercera consideración garantiza que la ganancia del canal medida desde que se envía la petición inicial (paquete de control) es aún válida por la duración del paquete de datos y ACK. Las pérdidas por trayectoria y los ensombrecimientos tendrán poco efecto ya que la distancia que un nodo se mueve en la duración de una transmisión de datos y control (en el orden de pocos milisegundos) es pequeño. Con los efectos multitrayectoria la ganancia no será estacionaria por la duración de un paquete. Sin embargo, la ganancia promedio (el término corto – en el orden de unos pocos bits) medida para el RTS (o un paquete equivalente de petición por la fuente) también es válido en los paquetes de datos y ACK que siguen ya que la ganancia promedio de término corto es en primer lugar un factor de pérdidas por trayectoria y efectos de ensombrecimientos (desvanecimientos lentos). Aún en ambientes celulares los ajustes de potencia no son los suficientemente rápidos para reaccionar a los desvanecimientos rápidos (efectos multitrayectoria). Por consiguiente las degradaciones introducidas por los desvanecimientos rápidos deben ser superadas por técnicas de capa física tales como receptores RAKE, OFDMA, o codificación de canal, o ser tolerados con compensación adicional en potencia de transmisión.

3.3.2 Restricciones de Potencia.

Sean Pt_Max y Pt_Min las potencias de transmisión máxima y mínima respectivamente para un transmisor en el canal de datos. Sea RX_Thresh y CS_Thresh la mínima potencia de señal para recibir un paquete válido y para detectar una portadora, respectivamente. Sea SIR_Thresh el “umbral de captura” esto es, la relación señal a interferencia mínima para el cual un receptor pueda recibir exitosamente un paquete.

Dados los parámetros de potencia del transmisor y receptor y las características de propagación del canal, un transmisor i debe transmitir un paquete a un receptor j con la mínima potencia de transmisión Pt_i que satisfaga las siguientes restricciones de potencia:

1. La potencia de transmisión de i debe estar dentro del rango de: $Pt\_Min \le Pt_i \le Pt\_Max$
2. La potencia recibida en j debe al menos ser igual al umbral de potencia recibida mínima, $G_{ij}Pt_i \ge RX\_Thresh$.
3. La relación señal a ruido observada para la transmisión en j debe al menos ser igual al mínimo umbral relación señal a interferencia (SIR), $SIR_j = \frac{G_{ij}Pt_i}{Pn_j} \ge SIR\_Thresh$, donde Pn_j es el ruido total que el nodo j observa en el canal de datos y está definido como $Pn_j = \sum_{l \ne i} G_{lj}Pt_l + N_j$. El término N_j es la potencia del ruido térmico (la potencia observada en el receptor cuando ningún nodo esta transmitiendo) observado en el nodo j y $G_{lj}Pt_l$ es la potencia recibida en j de algún nodo interferente *l*.
4. Sea E_k la "tolerancia al ruido" de cualquier receptor k que esta recibiendo una transmisión en curso en la vecindad de i. E_k es la potencia de ruido adicional que k (actualmente recibiendo datos de algún otro nodo con potencia $\mathrm{P}_{\mathrm{r}k}$) puede tolerar antes de que su SIR caiga por debajo del SIR_Thresh, y esta definido como $E_k = \frac{\mathrm{P}_{\mathrm{r}k}}{SIR\_Thresh} - Pn_k$. Dado que la potencia de transmisión de i no debe corromper ninguna transmisión en curso $Pt_i \le \min_k \left\{ \frac{E_k}{G_{ik}} \right\} = Pt\_bound_i$.

Si las cuatro restricciones anteriores se logran, entonces i puede transmitir exitosamente a j sin corromper transmisiones en curso. Los asuntos críticos son por consiguiente:

a) El saludo entre un par transmisor-receptor para determinar la potencia de transmisión mínima que satisfaga las restricciones 2 y 3 (principio de conservación de potencia).

b) Para cada receptor, anunciar su tolerancia a ruido de tal manera que ningún transmisor potencial corrompa su recepción en curso aplicando la restricción 4 (principio de cooperación).

Para poder cumplir con las restricciones de potencia, se tuvieron que realizar modificaciones a los archivos ../ns-default.tcl y ../mac-802_11.cc. En el archivo ../ns-default.tcl se modificaron los valores de RX_Thresh, CS_Thresh y SIR_Thresh, además se cambió el valor fijo de potencia de transmisión definido en este archivo por una potencia variable que se calcula de acuerdo a la distancia entre transmisor y receptor para que esté dentro los límites de potencia mínima y máxima de acuerdo a los parámetros definidos en [6]. Este cálculo de potencia de transmisión se realizó en una rutina implementada dentro del archivo ../mac-802_11.cc cuyo algoritmo se presenta en la figura 4.9 del capítulo 4. Las restricciones 2 y 3 son condiciones que deben cumplir todos los nodos receptores para la recepción exitosa de un paquete, para estos puntos se modificaron los parámetros RX_Thresh_ y SIR_Thresh_ del archivo ../ns-default.tcl. Para la implementación de la restricción 4 se siguió el mismo algoritmo que para la restricción 1 donde un nodo que desea iniciar una nueva transmisión debe calcular la interferencia que ocasionará a todos los nodos receptores, en caso de que la SIR de algún receptor caiga por debajo del umbral establecido por SIR_Thresh_ el nodo que desea transmitir realiza la acción especificada para cada tipo de paquete como se muestra en el algoritmo 4.8.

3.4 PROTOCOLO PCMA.

El objetivo de PCMA es lograr acceso múltiple controlado por potencia dentro de la estructura de los protocolos de acceso múltiple basados en CSMA/CA. En estos protocolos, hay dos componentes principales: (a) *evasión de colisiones,* y (b) *resolución de colisiones.* La evasión de colisiones ocurre por medio de una combinación de detección de portadora por el transmisor y aplazamiento de transmisiones por estaciones ocultas y expuestas cuando escuchan paquetes RTS/CTS. La resolución de colisiones ocurre por medio del algoritmo backoff.

3.4.1 Visión general del protocolo PCMA.

En PCMA, la evasión de colisiones es generalizada a control de potencia. Los métodos de evasión de colisiones convencionales tienen un "modelo on / off", en donde un nodo puede ya sea transmitir (si éste no esta posponiendo una transmisión y no detecta una portadora ocupada) o no transmitir. Sin embargo, en la sección 3.3 se determinó que un nodo puede transmitir al receptor deseado siempre y cuando satisfaga cuatro restricciones. De esta manera, el modelo "on / off" se generaliza a un "modelo de potencia limitada". Con el propósito de lograr el modelo limitado de potencia, el componente de control de potencia en PCMA tiene dos mecanismos principales:

A. Un saludo (handshake) RPTS/APTS Petición de potencia para enviar (request-power-to-send)/ potencia aceptable para enviar (acceptable-power-to-send) entre el transmisor de datos y el receptor, el cual se usa para determinar la potencia de transmisión mínima que resultará en una recepción exitosa del paquete en el receptor. El saludo RPTS/APTS ocurre en el *canal de datos* y antecede la transmisión de datos. Después de la recepción exitosa de los datos, el receptor envía un paquete ACK para confirmar la recepción.
B. El aviso de tolerancia de ruido se usa por cada receptor activo para anunciar la máxima potencia de ruido adicional que puede tolerar (dados sus niveles recibidos actuales de la señal y niveles de potencia de ruido). El aviso de tolerancia al ruido o tono de ocupado es *pulsado* periódicamente por cada receptor en el *canal de tono ocupado*, donde la intensidad de señal del pulso indica la tolerancia a ruido adicional. Un transmisor potencial primero "detecta la portadora" escuchando el tono ocupado por un periodo de tiempo mínimo para detectar el limite superior de su potencia de transmisión para todos los paquetes de control (RPTS, APTS, ACK) y datos.

La secuencia de saludo (handshake) en el canal de datos es RPTS-APTS-DATA-ACK. Se observa que hay una cuestión en como proteger apropiadamente el ACK de colisión dado que la potencia de ruido observado en la fuente no puede ser actualizada durante la transmisión de datos. Sin embargo, este es un problema fundamental asociado con todos los métodos de control de potencia ya que la detección de la portadora mientras se transmite es extremadamente costosa. El último componente principal en PCMA es resolución de colisiones, el cual es basado en el algoritmo de *backoff*.

PCMA tiene una analogía uno-a-uno con los componentes claves del estándar de protocolos CSMA/CA. En el transmisor, monitorear el tono de ocupado es equivalente a detectar la portadora.

En el receptor, pulsar periódicamente el tono de ocupado es equivalente a enviar un CTS para evasión de colisiones. El saludo RPTS/APTS que antecede la transmisión de datos es similar al saludo RTS/CTS, excepto que el propósito no es forzar a terminales ocultas a entrar en *backoff.* De esta manera PCMA puede mejorar la eficiencia de acceso al canal sin cambiar el paradigma fundamental del MAC.

3.4.2 Pasos del Protocolo PCMA.

Los pasos del protocolo considerando algún nodo fuente *i* que envía a algún nodo destino *j* y un transmisor interferente potencial *l*, se muestra en la figura 3.3.

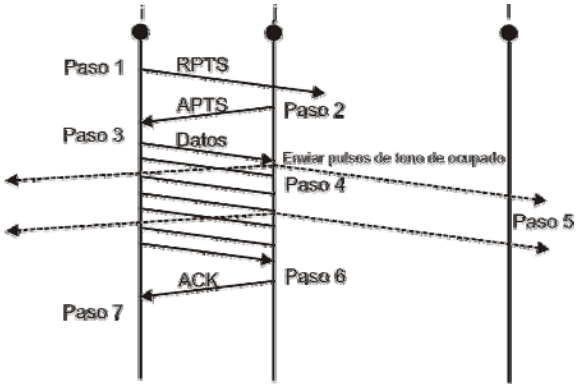

Figura 3.3. Pasos del protocolo PCMA.

Paso 1: Un nodo *i* en su estado IDLE monitorea el canal de tono ocupado para determinar su límite de potencia Pt_bound_i midiendo la máxima potencia recibida en el canal de *tono ocupado* sobre una ventana de tiempo umbral. Cuando *i* busca transmitir un paquete de datos, espera hasta que ΥPt_bound_i sea mas grande que Pt_Min, y luego entra en backoff por un intervalo aleatorio limitado por su contador backoff para permitir resolución de contención. El termino Υ es una constante (Υ=0.9 para resultados de simulación) que mantiene el nivel de potencia ligeramente debajo del umbral (Pt_bound). El nodo continúa detectando el tono de ocupado durante su backoff. Si al terminar el backoff el límite de potencia de transmisión (Pt_bound) es aún mas grande que la potencia de transmisión mínima Pt_Min, por un factor de $1/\Upsilon$, entonces *i* envía un mensaje de control petición de potencia para enviar (RPTS) con un nivel de potencia de transmisión $Pt = \Upsilon Pt\_bound$ en el canal de DATOS. El paquete RPTS contiene el nivel de potencia de transmisión (Pt) y potencia de ruido de la fuente, Pn_Si (obtenida de la interfase aérea), y colocado en el paquete.

Paso 2: Cuando el destinatario recibe el RPTS, este mide la potencia con la que se recibe ($\Pr$). La ganancia del canal G_{ij}, es la potencia de la señal recibida sobre la potencia transmitida (Potencia anunciada en el paquete RPTS). Entonces el receptor requiere que los datos sean enviados con una potencia:

$$Pt_i\_des = \max\left\{\frac{Rx\_Des}{G_{ij}}, \frac{SIR\_Des \cdot Pn\_D_j}{G_{ij}}\right\}, \qquad (1)$$

Con el propósito de satisfacer su umbral de potencia recibida y su umbral de relación señal a interferencia (SIR). En este punto, las restricciones $Rx\_Des > Rx\_Thresh$ y $SIR\_Des > SIR\_Thresh$ asegura que las restricciones de potencia de la sección 3.3.2 sean cumplidas, y $\Pr n\_Dj$ sea la potencia de ruido medida en el receptor. La potencia Pt_i_des se coloca en un paquete de control APTS de tal forma que la fuente pueda ser notificada del nivel de potencia para enviar su paquete de datos. Considerando la misma ganancia en ambas direcciones, la potencia de transmisión para el paquete APTS se calcula que sea:

$$Pt_j = \max\left\{\frac{Rx\_Des}{G_{ij}}, \frac{SIR\_Des \cdot Pn\_S_i}{G_{ij}}\right\}, \qquad (2)$$

Donde la potencia de ruido del destinatario es reemplazado por el de la fuente (extraído del paquete RPTS). Si esta potencia es menor que Pt_bound calculada en el receptor, entonces el APTS es enviado con una potencia Pt_j en el canal de DATOS.

Paso 3: Cuando la fuente recibe el paquete APTS, checa si la potencia de transmisión deseada esta por debajo de su limite de potencia actual, y transmite el paquete de DATOS con una potencia Pt_i_des en el canal de datos si este limite se satisface. Si la fuente termina su contador de tiempo antes de recibir el APTS, incrementa multiplicativamente su limite backoff y empieza de nuevo.

Paso 4: El receptor empieza a enviar pulsos de tono ocupado en el canal de *tono ocupado* después de empezar a recibir el paquete de datos. La potencia del tono de ocupado, Pt_BT_j, enviado desde el nodo j depende de la tolerancia al ruido, E_j,y se calcula de la siguiente forma:

$$Pt\_BT_j = \frac{C}{E_j}, \qquad (3)$$

El valor de $C = Pt\_Max \cdot CS\_Thresh$ es tal, que un nodo a una distancia en que agregue exactamente ruido adicional E_j cuando este transmitiendo a una potencia máxima Pt_Max reciba el tono de ocupado en exactamente el CS_Thresh. Se debe notar que los tonos de ocupado tienen que ser recibidos en el umbral de detección dado que sus potencias solo van a ser medidas y no se necesitan recibir bits de datos. Además dado que la potencia del tono de ocupado no puede ser más grande que Pt_BT_Max hay una tolerancia de ruido mínima, dado por:

$$E\_\min = \frac{C}{Pt\_BT\_Max}. \qquad (4)$$

Este valor limita la capacidad del tono ocupado para restringir a estaciones muy alejadas cuando el receptor es muy sensible a pequeños incrementos en el ruido. Si no hubiera una mínima tolerancia de ruido, la potencia del tono de ocupado podría potencialmente acercarse al infinito y obligar a los nodos infinitamente alejados a no transmitir en ningún momento. Se observa que si $E\_\min$ se sustituyera en la ecuación 3 la potencia del tono de ocupado resultante sería entonces $Pt\_BT_j = Pt\_BT\_Max$, el cual se asemeja (adapta) a las limitaciones físicas. La tolerancia al ruido resultante es:

$$E_j = \max\left\{\frac{\Pr}{SIR\_Thresh} - Pn_j, E\_\min\right\}, \qquad (5)$$

Paso 5: Cuando un nodo l recibe el tono de ocupado con una potencia de $\Pr\_BT_l = \frac{C}{E_j}G_{jl}$, este calcula su limite de potencia de transmisión impuesto por el nodo j de la siguiente manera:

$$\Pr\_bound_j = \frac{C}{\frac{C}{E_j}G_{jl}} = \frac{E_j}{G_{jl}} \qquad (6)$$

Entonces el nodo j puede recibir como máximo $\Pr_j = \frac{E_j}{G_{lj}} G_{jl}$ del nodo l ya que consideramos que $G_{lj} \cong G_{jl}$, y $\Pr_l = E_j$. Dado que pueden haber tonos de ocupado recibidos de múltiples receptores, el límite de potencia de transmisión en un nodo esta definido por el receptor más sensible (el receptor que puede tolerar la menor potencia de transmisión de este nodo)

$$Pt\_bound = \min\left\{ \min_j \left\{ \frac{E_j}{G_{jl}} \right\}, Pt\_\max \right\} . \qquad (7)$$

Los receptores envían periódicamente pulsos de tono de ocupado con el propósito de minimizar la probabilidad de interferencia destructiva (i.e. colisiones). El ancho del pulso esta basado en el intervalo de captura de la señal del receptor. Enviar pulsos separados también permite a los receptores actualizar periódicamente sus avisos de tolerancia al ruido para evitar colisiones con los nuevos transmisores. La frecuencia que se necesita para los pulsos de tono ocupado esta basado en la tasa de cambio del ruido de fondo (carga de tráfico). Hay otro problema que puede suceder (particularmente con mucha carga de tráfico): múltiples transmisores potenciales, por encima de escuchar un tono de ocupado de un receptor, pueden localmente decidir que es aceptable transmitir y comenzar la transmisión simultáneamente (dentro de un periodo del aviso de tono de ocupado), en consecuencia crear acumulativamente suficiente ruido para desestabilizar la recepción de un paquete en curso. Este problema es similar a contención, excepto que la falla de la resolución de la contención corrompe transmisiones en curso en vez de paquetes contendientes. Una solución simple para reducir tales colisiones es que un receptor inmediatamente pulse un tono de ocupado cuando sienta un cambio en su tolerancia a ruido sobre un nivel de umbral.

Paso 6: Cuando el destinatario reciba los paquetes de datos completos sin errores, envía un paquete ACK en el canal de datos con un nivel de potencia necesario para que llegue a la fuente.

Paso 7: Si la fuente recibe un paquete ACK válido resetea su máximo backoff y regresa a su estado IDLE, en otro caso incrementa el backoff máximo y empieza de nuevo.

Para la implementación de los pasos 1, 2, 3, 5 y 6 del protocolo se realizó una rutina en la que cada nodo con un paquete de control o de datos listo para enviar, tiene que cumplir con las restricciones de potencia definidas en 1 y 4 de la sección anterior que especifica que se debe calcular una potencia de transmisión que se encuentre dentro de los límites de Pt_Min y Pt_Max, y que si se transmite con esta potencia no se debe afectar a ninguna comunicación en curso, es decir que la SIR de todos los receptores activos no caiga por debajo del SIR_Thresh, como se especifíca en los algoritmos que se muestran en las figuras 4.8, 4.9 y 4.10. Si las restricciones de potencia no se cumplen, cada nodo transmisor debe realizar una acción especificada dependiendo del tipo de paquete.

En el paso 7 no se hizo ninguna modificación ya que el funcionamiento es igual al del estándar IEEE 802.11. Para la implemenatación del protocolo no se consideró un canal extra para la señalización como se especifica en el paso 4, debido a que no se consideró necesario para comprobar el funcionamiento del protocolo PCMA.

En este capítulo hemos descrito el funcionamiento del protocolo de acceso al medio controlado por potencia (PCMA), que es una de las propuestas hechas en base al protocolo MAC 802.11 dentro de la estructura de acceso múltiple con evasión de colisiones. El estudio de este protocolo servirá como base para su implementación en software para el análisis y evaluación de rendimiento e igualdad de acceso al medio, que se verá en los siguientes capítulos.

CAPÍTULO IV
DISEÑO E IMPLEMENTACION DEL PROTOCOLO DE CONTROL DE ACCESO AL MEDIO CONTROLADO POR POTENCIA (PCMAP).

4.1 GENERALIDADES DEL SIMULADOR ns-2.

Para la implementación y evaluación del protocolo PCMAP se utilizó el simulador ns-2 (*Network Simulator)* que es un simulador de redes orientado a objetos y manejado por eventos discretos, que simula una gran variedad de redes tanto alámbricas como inalámbricas; así como una gran variedad de redes IP; implementa protocolos de transporte tales como TCP, UDP, SRM; generadores de trafico como FTP, Telnet, web, cbr y real-audio, mecanismos de administración de colas de espera como Drop Tail, RED, CBQ y variantes de *Fair Queueing (FQ)* tales como FQ, SFQ (Stochastic FQ) y DRR (Deficit Round-Robin), algoritmos de enrutamiento y difusión dirigida e implementaciones de capa física (punto a punto, LANs y múltiples modelos de propagación inlámbricas) y protocolos de la capa MAC para simulaciones de redes cableadas e inalámbricas; además proporciona funciones de visualización y trazado de datos [18].

4.1.1 Dualidad C++/OTcl.

El simulador *ns* está escrito en C++ con un interprete OTcl como interfaz de usuario, soporta una clase jerárquica en C++ (también llamada jerarquía compilada), y una clase jerárquica similar dentro del intérprete OTcl (también llamado jerarquía interpretada). Las dos jerarquías están estrechamente relacionadas una con otra; desde la perspectiva del usuario, existe una correspondencia uno-a-uno entre una clase en la jerarquía interpretada y una clase en la jerarquía compilada. La raíz de esta jerarquía es la clase TclObject. Los usuarios crean nuevos objetos de simulador a través del intérprete; estos objetos son instanciados dentro del intérprete, y están estrechamente representados por un objeto correspondiente en la jerarquía compilada. La clase jerárquica interpretada está automáticamente establecida a través de funciones definidas en la clase TclClass. Los objetos instanciados por el usuario son representados a través de funciones definidas en la clase TclObject. Existen otras jerarquías en el código C++ y los scripts de Tcl; estas otras jerarquías no son reflejadas en la manera de Tcl Object.

Por razones de eficiencia, *ns* separa la implementación de la trayectoria de datos de la implementación de la trayectoria de control. Con el propósito de reducir tiempo de procesamiento de paquetes y eventos (no tiempo de simulación), el organizador de eventos y los objetos de componente de red básicos en la trayectoria de datos están escritos y compilados utilizando C++. Estos objetos compilados están disponibles para el interprete OTcl a través de una vinculación que crea un objeto OTcl correspondiente para cada uno de los objetos C++ y hace que las funciones de control y las variables configurables especificadas por el objeto C++ actúen como funciones miembro y variables miembro del objeto OTcl correspondiente. En esta manera, los controles de los objetos C++ son dados a OTcl. También es posible agregar funciones miembro y variables a un objeto C++ enlazado a un objeto OTcl. Los objetos en C++ que no necesitan ser controlados en una simulación o usados internamente por otro objeto no necesitan estar enlazados a OTcl. Así mismo, un objeto (no en la trayectoria de datos) puede ser completamente implementado en OTcl. La figura 4.1 muestra un ejemplo de jerarquía de objeto en C++ y OTcl. Una cosa que se debe de notar en la figura es que para los objetos C++ que tienen una vinculación OTcl formando una jerarquía, hay una jerarquía de objeto OTcl correspondiente muy similar a C++ [19].

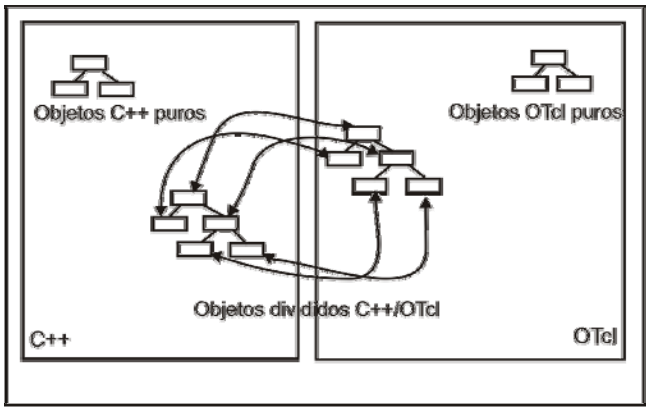

Figura 4.1. La Dualidad C++ y OTcl

4.1.2 Separación de C++ y OTcl.

Como se mencionó anteriormente, *ns* utiliza dos lenguajes (C++ y OTcl) debido a que el simulador tiene dos tipos distintos de cosas que necesita hacer. Por un lado, la simulación detallada de protocolos requiere de un lenguaje de programación de sistemas el cual pueda manejar bytes y encabezados de paquetes eficientemente e implementar algoritmos que corran sobre grandes conjuntos de datos. Para estas tareas la velocidad de tiempo de ejecución es importante y el tiempo de *turn-around* (correr una simulación, encontrar una

falla, corregir una falla, recompilar, volver a correr) es menos importante. Por otro lado, una gran parte en investigación de redes implica ligeras variaciones de parámetros o configuraciones, o explorar nuevos escenarios. En estos casos, el tiempo de iteración (cambiar el modelo y volver a correr) es más importante. Dado que la configuración corre una vez (al inicio de la simulación), el tiempo de ejecución en esta parte de la tarea es menos importante.

ns logra estas dos necesidades con dos lenguajes, C++ y OTcl. El lenguaje C++ corre más rápido pero es mas lento para cambiar, haciéndolo apropiado para la implementación detallada de protocolos. OTcl corre mucho más lento pero puede ser cambiado muy rápidamente (e interactivamente), haciéndolo ideal para la configuración de simulaciones. ns (vía tclcl) proporciona una liga para hacer que los objetos y variables aparezcan en los dos lenguajes.

El hecho de tener dos lenguajes, implica que cada uno es utilizado para un propósito específico:
OTcl para Control:

- Configuración de escenarios de simulación.
- Manipulación de objetos C++ existentes.

C++ para "datos":

- Procesamiento de paquetes o conexiones.
- Si se necesita cambiar el comportamiento de una clase C++ existente en modos que no estuvieran anticipados.

4.1.3 Perspectiva del usuario del simulador *ns-2*.

Desde la perspectiva del usuario, *ns* es un interpretador de scripts Orientados a objetos de TCL (OTcl) que tiene un organizador de eventos de simulación, objetos de componentes de red y librerías de módulos de organización de red (plumbing). En otras palabras, para usar *ns*, se programa en el lenguaje OTcl (ver Figura 4.2).

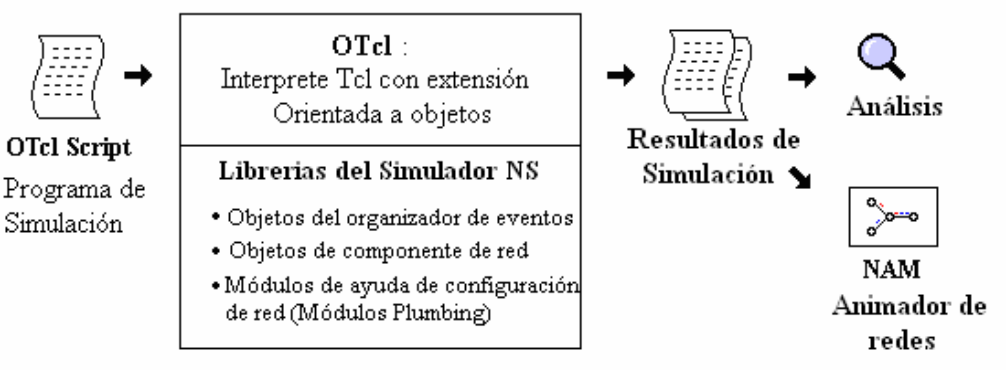

Figura 4.2. Perspectiva del usuario de ns

Para configurar y correr una red simulada, un usuario debe escribir un script en OTcl que inicia un organizador de eventos, configura la topología de red usando los objetos de red y las funciones de *plumbing* en la librería, y le dice a los generadores de tráfico cuando deben iniciar y cuando terminar de transmitir paquetes a través del organizador de eventos. El término "*plumbing*" se utiliza para la configuración de red, ya que configurar una red es conectar posibles trayectorias de datos entre objetos de red mediante la puesta del apuntador "neighbor" de un objeto a la dirección de otro objeto apropiado. Cuando un usuario desea hacer un nuevo objeto de red, puede hacerlo fácilmente ya sea escribiendo un nuevo objeto o haciendo un objeto compuesto de la librería de objetos, y conectar la trayectoria de datos a través del objeto. Esto puede sonar como un trabajo complicado, pero los módulos de conexión OTcl hacen el trabajo muy fácil. El poder de *ns* viene del "Plumbing" [19].

4.1.4 Organizador de Eventos de *ns-2*.

Otro componente importante además de los objetos de red, es el organizador de eventos. Un evento en *ns* es el ID de paquete que es único para cada paquete y tiene un tiempo de registro además de un apuntador a un objeto que maneja el evento. En *ns*, un organizador de eventos mantiene información del tiempo de simulación y despacha todos los eventos en la cola de espera programados para el tiempo actual mediante el llamado de componentes de red apropiados, estos componentes normalmente son aquellos que expidieron los eventos, y se les permite realizar una acción apropiada, asociada con el paquete apuntado por el evento. Los componentes de red se comunican entre si pasándose paquetes, sin embargo esta tarea no consume tiempo de simulación. Todos los componentes de red que necesitan gastar algún tiempo de simulación al manejar un paquete (esto es, un retardo) utilizan el organizador de eventos mediante la expedición de un evento para el paquete y esperan que este evento sea despachado por si mismo antes de realizar cualquier acción en el manejo del paquete. Otro uso del organizador de eventos es el de temporizador; los temporizadores utilizan el organizador de eventos en una manera similar que lo hacen los retardos. La única diferencia es que el temporizador mide un valor de tiempo asociado con un paquete y realiza una acción apropiada relacionada al paquete después de que cierto tiempo ha pasado, y no simula un retardo [19].

4.1.5 Arquitectura General de *ns-2*.

La figura 4.3 muestra la arquitectura general de *ns.* En esta figura un usuario general (no un desarrollador de *ns*) se puede pensar que se encuentra en la esquina inferior izquierda, diseñando y corriendo simulaciones en Tcl utilizando los objetos de simulador en la librería de OTcl. Los organizadores de eventos y la mayor parte de los componentes de red están implementados en C++ y disponibles hacia OTcl a través de una vinculación que esta implementada usando tclcl. Todo esto junto hace *ns*, el cual es un intérprete extendido Tcl orientado a objetos con librerías de simulador de redes [19].

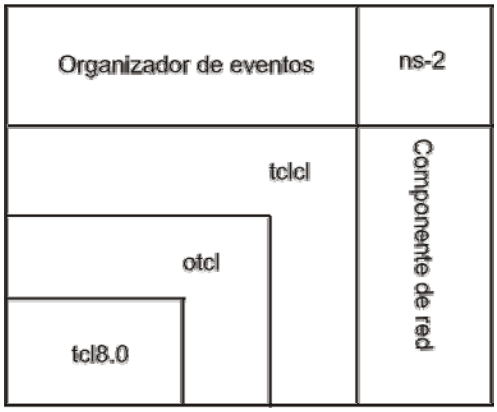

Figura 4.3. Vista de la arquitectura de ns.

Esta sección examinó brevemente la estructura general y la arquitectura de *ns*. En este punto, uno se debe de preguntar acerca de como obtener resultados de simulación en *ns*. Como se muestra en la figura 4.1, cuando termina una simulación, *ns* produce uno o más archivos de salida de texto que contienen datos detallados de simulación, si se especifica que haga esto en el script de OTcl. Los datos pueden ser para análisis de simulación o como una entrada a una herramienta de visualización de simulación gráfica llamada Animador de redes (NAM- Network Animator). NAM tiene una interfase gráfica de usuario similar a un reproductor de CD, además tiene una pantalla de control de velocidad. Adicionalmente, puede presentar información gráfica tal como rendimiento (throughput) y número de paquetes caídos en cada link, aunque la información gráfica no puede ser usada para análisis preciso de la simulación.

4.2 SISTEMA DE RED MÓVIL EN ns-2.

En esta sección, se describen las características esenciales de un nodo móvil, los mecanismos de enrutamiento y los componentes de red que son usados para construir la pila de red de un nodo móvil. Los componentes que son cubiertos brevemente son: canal, interfase de red, modelo de propagación, protocolo MAC, cola de prioridad (IFQ), capa de enlace (LL) y el protocolo de resolución de direcciones (ARP).

4.2.1 Modelo inalámbrico básico en ns-2.

El modelo inalámbrico esencialmente consiste del nodo móvil como núcleo del modelo de movilidad, con características de soporte adicionales que permite la simulación de redes ad-hoc de múltiples saltos, WLANs, redes de sensores, etc. Un nodo móvil es un objeto de un nodo básico con funcionalidades agregadas de un nodo móvil e inalámbrico tales como la capacidad de moverse dentro de una topología dada, capacidad de recibir y transmitir señales hacia y del canal inalámbrico etc. Una diferencia principal entre un nodo básico y un nodo móvil, es que un nodo móvil no esta conectado a través de *enlaces* a otros nodos básicos o móviles [18]. En esta sección describiremos las características esenciales de un nodo móvil, sus mecanismos de enrutamiento, haremos mención de protocolos de enrutamiento que utiliza, la creación de la pila de red que permite el acceso al canal de un nodo móvil, así como una breve descripción de cada componente de la pila, del soporte de trazado y de la generación de escenarios de movimiento y de tráfico para simulaciones de redes inalámbricas.

4.2.2 Simulación de redes Inalámbricas en ns-2.

El objetivo de esta sección es el de proporcionar una breve introducción a la simulación de redes inalámbricas por medio de ns-2; aunque una mejor guía se puede obtener por medio la documentación existente o de los tutoriales en línea los cuales se pueden encontrar en las referencias del final del capítulo [19],[20] y [21].

Estructura genérica del Script en OTcl:

- Definición de Variables Globales.
- Crear el organizador de eventos.
- Crear la topología.
- Activar la opción de trazado.
- Configuración del nodo móvil.
- Creación del nodo móvil.

- Movimiento del nodo móvil en caso de que se desee.
- Generador de tráfico.
- Definición del modelo de movimiento y de tráfico.
- Definición de la posición inicial en NAM y finalización de simulación.

4.2.2.1 Definición de variables.

Como se mencionó en la sección anterior un nodo móvil consiste de componentes de red como capa de enlace (LL), Cola de espera (IFQ), capa MAC, etc. En el inicio de una simulación inalámbrica, se necesita definir el tipo de cada uno de estos componentes de red. Además, se necesita definir otros parámetros como el tipo de antena, el modelo de propagación, el tipo de protocolo de enrutamiento empleado por los nodos móviles y algunos otros que a continuación se ilustran. El Script en OTcl empieza con una lista de estos diferentes parámetros que acabamos de mencionar, de la siguiente manera:

```
# ======================================================================
# Definición de  opciones
# ======================================================================

set val(chan)       Channel/WirelessChannel    ;# Tipo de canal
set val(prop)       Propagation/TwoRayGround   ;# Modelo de propagación
set val(netif)      Phy/WirelessPhy            ;# Tipo de Interfase de red
set val(mac)        Mac/802_11                 ;# Tipo de MAC
set val(ifq)        Queue/DropTail/PriQueue    ;# Tipo de cola de espera
set val(ll)         LL                         ;# Tipo de capa de enlace
set val(ant)        Antenna/OmniAntenna        ;# Tipo de antena
set val(x)              670                    ;# X dimensión de la topografía
set val(y)              670                    ;# Y dimensión de la topografía
set val(ifqlen)         50                     ;# max no. de paquetes en ifq
set val(seed)           0.0                    ;# Semilla para generar número aleatorio
set val(adhocRouting)   DSR                    ;# Protocolo de enrutamiento
set val(nn)             3                      ;# número de nodos
set val(cp)             "../mobility/scene/cbr-3-test"  ;# Archivo de escenario
set val(sc)             "../mobility/scene/scen-3-test" ;# Archivo de escenario
set val(stop)           400.0                   ;# tiempo de simulación
```

Donde val() es un arreglo que se utiliza para definir estas variables.

4.2.2.2 Organizador de evento.

Un evento es la ejecución de un procedimiento tcl programado para ocurrir en un tiempo determinado. Un simple ejemplo muestra como se crea un organizador de eventos:

- Crea un organizador de evento:
  `set ns_ [new Simulator]`
- Programación de un evento:
  ```
  $ns at <time> <event>
  <event>: cualquier comando permitido ns/tcl
  ejemplo: $ns at 5.0 “finish”
  ```
- Inicio del organizador:
  `$ns_ run` Este comando va en la última línea del programa.

Existen actualmente cuatro organizadores de eventos disponibles en el simulador, cada uno de los cuales esta implementado utilizando una estructura de datos diferente: List Scheduler, Heap Scheduler, Calendar Queue Scheduler, real Time Scheduler.

4.2.2.3 Crear la topología.

En las simulaciones de *ns* se necesita definir la topografía de los nodos móviles, los cuales se deben hacer antes de crear los nodos. Normalmente se crea una topología plana especificando el largo y el ancho de la topografía utilizando el siguiente comando.

```
set topo      [new Topography]
$topo load_flatgrid $val(x) $val(y)
```

Donde `$val(x), $val(y)` fueron definidos anteriormente como variables globales.

4.2.2.4 Activar la opción de trazado.

Si se activa la opción de trazado en el script OTcl, al terminar la simulación *ns* produce uno o más archivos de texto que contienen datos detallados de la simulación. Estos datos pueden ser para el análisis de la simulación o como una entrada a una herramienta de visualización llamada Animador de redes. Para activar esta opción se utilizan los siguientes comandos:

- Trazado ns:
```
set tracefd  [open wireless1-out.tr w]
$ns trace-all $tracefd
```
- Trazado nam:
```
set namtrace    [open wireless1-out.nam w]
$ns_ namtrace-all-wireless $namtrace $val(x) $val(y)
```

Los comandos anteriores escribirán en los archivos que se encuentran entre corchetes los cuales contienen información detallada de la simulación.

4.2.2.5 Configuración y creación del nodo móvil.

La siguiente interfase de programación de aplicación (API) configura un nodo móvil con todos los valores definidos, como protocolo de enrutamiento, pila de red (LL, MAC, IFQ), tipo de canal, topografía, modelo de propagación así como la activación o desactivación de diferentes tipos de trazado en diferentes niveles (router, mac, agent) para que pueda ser guardado en el archivo de trazado definido anteriormente.

```
$ns_ node-config -adhocRouting $val(adhocRouting) \
                 -llType $val(ll) \
                 -macType $val(mac) \
                 -ifqType $val(ifq) \
                 -ifqLen $val(ifqlen) \
                 -antType $val(ant) \
                 -propType $val(prop) \
                 -phyType $val(netif) \
                 -channelType $val(chan) \
                -topoInstance $topo \
                -agentTrace ON \
                 -routerTrace OFF \
                 -macTrace OFF
```

Después de haber configurado el nodo móvil, el siguiente paso es crearlo, esto se realiza mediante la siguiente rutina:

```
for {set i 0} {$i < $val(nn) } {incr i}
   {
     set node_($i) [$ns_ node]
     $node_($i) random-motion 0    ;# deshabilita movimiento aleatorio.
   }
```

El ciclo "*for"* se utiliza para crear la cantidad de nodos especificada por `$val(nn)`.

4.2.2.6 Movimiento del nodo.

El nodo móvil esta diseñado para moverse en una topología de 3 dimensiones; sin embargo la tercera dimensión no se utiliza (Z=0); es decir, el nodo móvil se considera que siempre se mueve en un terreno plano con el eje Z siempre igual a 0. De esta forma el nodo móvil tiene coordenadas X, Y y Z=0, los cuales se actualizan continuamente conforme el nodo se mueve. Existen dos mecanismos para inducir el movimiento de los nodos: En el primer método, la posición inicial del nodo y sus destinos futuros pueden ser puestos explícitamente. Estas directivas están incluidas en un archivo de movimiento separado.

La posición inicial y los destinos futuros para un nodo móvil pueden ser puestos utilizando los siguientes comandos:

```
$node set X_ <x1>
$node set Y_ <y1>
$node set Z_ <z1>
$node at $time setdest <x2> <y2> <speed>
```

En el tiempo `$time` el nodo se empezaría a mover de su posición inicial de (X1, Y1) hacia el destino (X2, Y2) con la velocidad especificada.

En este método las actualizaciones del movimiento del nodo son activados cuando se requiere saber la posición del nodo en un tiempo determinado. Esta actualización se puede dar por una petición de un nodo vecino que busca conocer la distancia entre ellos, o la directiva de *setdest* que se menciona a continuación que cambia la dirección y velocidad del nodo.

Los archivos de movimiento del nodo se realizan por medio del generador de escenario de CMU que se encuentra en el directorio ~ns/indep-utils/cmu-scen-gen/setdest cuya sintaxis es la siguiente:

```
./setdest [-n num_of_nodes] [-p pausetime] [-s maxspeed] [-t simtime] \
      [-x maxx] [-y maxy] > [outdir/movement-file]
```

El segundo método emplea movimiento aleatorio del nodo, los comandos que se utilizan son los siguientes:

```
$node_($i) random-motion 1
$node_($i) start
```

Lo que inicializa al nodo con una posición aleatoria y realiza actualizaciones para cambiar la dirección y velocidad del nodo; los valores de posición y velocidad son generadas de manera aleatoria.

4.2.2.7 Generador de tráfico.

Las conexiones aleatorias de tráfico TCP y CBR pueden ser configuradas entre nodos móviles utilizando un script para generar tráfico. Este script está disponible en el directorio *~ns/indep-utils/cmu-scen-gen* y se llama *cbrgen.tcl*. Este script puede ser usado para crear conexiones de tráfico CBR y TCP entre nodos móviles inalámbricos. Con el propósito de crear un archivo de conexión de tráfico, se necesita definir el tipo de conexión de tráfico (CBR o TCP), el número de nodos y el número máximo de conexiones que van a ser configurados entre ellos, una semilla aleatoria y en caso de conexiones CBR, una tasa de datos cuyo valor inverso se utiliza para calcular el intervalo de tiempo entre los paquetes CBR. La sintaxis para este comando es el siguiente:

```
ns cbrgen.tcl [-type cbr|tcp] [-nn nodes] [-seed seed] [-mc connections]

[-rate rate] > [outdir/trafic-file]
```

Los tiempos de inicio de las conexiones están generadas aleatoriamente, y distribuidos uniformemente entre 0 y 180 segundos.

4.2.2.8 Definición del modelo de movimiento y de tráfico.

Después de la creación de un nodo móvil y de la generación de los archivos de movimiento y de tráfico que se definieron previamente como val(sc) y val(cp) respectivamente, el siguiente paso es leer estos archivos de movimiento así como de conexiones de trafico (CBR o TCP) con los siguientes comandos:

- Define modelo de movimiento de los nodos
  source $val(sc)
- Define modelo de tráfico
  source $val(cp)

4.2.2.9 Definición de la posición inicial en NAM y finalización de simulación.

El siguiente comando se utiliza para definir la posición inicial de los nodos en la interfase gráfica. Donde `<size>` denota el tamaño del nodo en NAM y `$val(nn)`es el numero de nodos totales. Esta función debe ser llamada después de que se ha definido el modelo de movilidad.

```
for {set i 0} {$i < $val(nn)} {incr i} {
  $ns_ initial_node_pos $node_($i) <size>
 }
```

Ahora se necesita definir el tiempo en que el programa debe de detenerse, y decirle a los nodos que restablezcan sus componentes de red internos, esto se realiza con los siguientes comandos:

```
# Termina la simulación

for {set i 0} {$i < $val(nn) } {incr i} {
    $ns_ at <time0> "$node_($i) reset";
}
$ns_ at <time1> "stop"
$ns_ at <time2> "$ns_ halt"
proc stop {} {
    global ns_ tracefd
    close $tracefd
}
```

Donde <time0> es el tiempo especificado para terminar la simulación. Los nodos son restablecidos en ese tiempo y la función `"$ns_ halt"` se llama en `<time2>` un poco después de que los nodos se han restablecido. El procedimiento `stop{}` se llama para terminar los trazados y cerrar los archivos.

4.3 CARACTERÍSTICAS INTERNAS DE LOS NODOS MÓVILES EN ns-2.

Un nodo móvil es un objeto de un nodo básico de *ns* con funcionalidades agregadas que contiene demultiplexores, agentes de enrutamiento una pila de red que consiste de una capa de enlace (LL), un módulo ARP conectado al LL, una interfase de cola de espera (IFq), una capa mac (MAC) e interfase de red (netIF), todos estos conectados al canal inalámbrico [18]. Estos componentes de red son creados y conectados en OTcl. El esquemático de un nodo móvil se muestra en la figura 4.4:

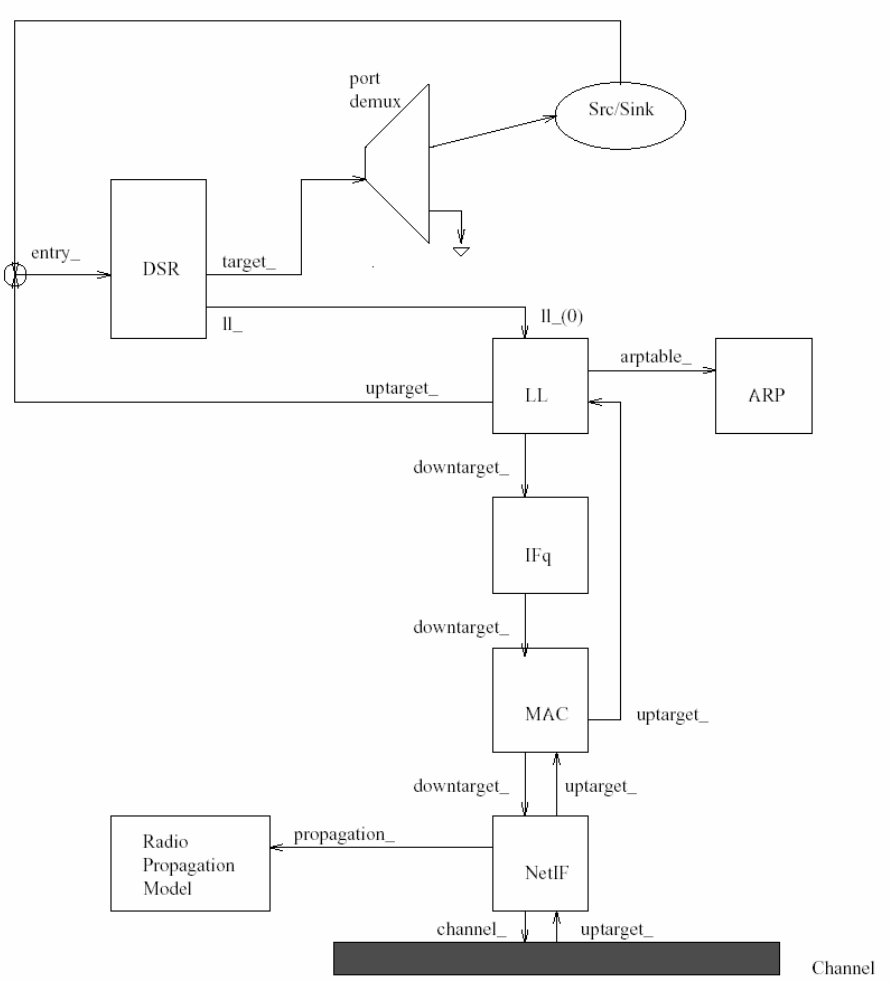

Figura 4.4. Esquemático de un nodo móvil.

4.3.1 Componentes de red de un nodo móvil.

Como se mencionó en la sección anterior, un nodo móvil tiene características agregadas diferentes a un nodo básico de *ns*, los componentes de red de un nodo móvil se describen a continuación.

Capa de enlace (LL). Esta capa es la responsable de simular los protocolos de enlace de datos y protocolos que pueden ser implementados dentro de esta capa, como fragmentación de paquetes y reensamble, así como protocolos de enlace confiable (como ARQ). Otra función importante de la capa de enlace es la de poner la dirección de destino MAC en el encabezado MAC del paquete. En la implementación actual esta tarea involucra dos cuestiones separadas: Encontrar la dirección IP del nodo en el siguiente salto (enrutamiento) y resolver esta dirección IP a la dirección MAC correcta (ARP). Para simplicidad, el mapeo por default entre dirección IP y MAC es uno a uno, lo que significa que las direcciones IP son rehusadas en la capa MAC. La capa de enlace tiene conectado un módulo ARP (Protocolo de resolución de direcciones) (ver figura 4.4), que resuelve las conversiones de dirección IP a dirección MAC (hardware). En general para todos los paquetes salientes (hacia el canal), estos son pasados a la capa de enlace por el agente de enrutamiento y la capa de enlace lo pasa hacia la cola de espera. Para todos los paquetes entrantes (que llegan al canal) al capa mac pasa los paquetes a la capa de enlace los cuales son enviados al punto de entrada de nodo. La *clase LL* esta implementada en *~ns/ll.{cc,h}* y en *~ns/tcl/lan/ns-ll.tcl.*

Protocolo de resolución de direcciones (ARP). El módulo del protocolo de resolución de direcciones recibe peticiones de la capa LL. Si el protocolo ARP tiene la dirección de hardware de destino, lo escribe dentro del encabezado mac del paquete. En otro caso difunde una petición ARP, y almacena el paquete temporalmente. Por cada dirección de hardware de destino desconocido, hay un *buffer* para un solo paquete. En caso de que paquetes adicionales al mismo destino sean enviados a ARP, el primer paquete almacenado se tira. Una vez que la dirección hardware del siguiente salto del paquete es conocido, el paquete se inserta en la cola de espera. La *clase ARPTable* esta implementada en ~ns/arp.{cc,h} y ~ns/tcl/lib/ns-mobilenode.tcl.

Interfase de cola de espera (IFq). La clase PriQueue esta implementada como una cola de espera prioritaria que da preferencia a paquetes de enrutamiento, insertándolos a la cabeza de la cola de espera. Soporta el funcionamiento de un filtro sobre todos los paquetes en la cola de espera y quita aquellos con una dirección de destino especificada. Esta clase está implementada en *~ns/priqueue.{cc,h}.*

Capa de control de acceso al medio (MAC). La función de coordinación distribuida (DCF) del protocolo MAC 802.11 fue implementado por CMU. Esta capa utiliza un formato RTS/CTS/DATOS/ACK para todos los paquetes que van dirigidos a un solo destino en la red (unicast) y simplemente envía DATOS para todos los paquetes de difusión (broadcast). La implementación utiliza detección de portadora virtual y física. La *clase Mac802_11* esta implementada en *~ns/mac-802_11.{cc,h}.*

Interfase de red (NetIf). La capa de interfase de red sirve como una interfase de hardware que es usada por los nodos móviles para acceder al canal. La interfase de comunicación compartida inalámbrica está implementada como *clase Phy/WirelessPhy*. Esta interfase sujeta a colisiones y al modelo de propagación de radio recibe paquetes transmitidos por otros nodos hacia el canal. Esta interfase marca cada paquete transmitido con los meta-datos relacionados a la interfase transmisora tales como la potencia de transmisión, longitud de onda, etc. Estos meta-datos en el encabezado del paquete son usados por el modelo de propagación en la interfase de red receptora para determinar si el paquete tiene la mínima potencia para ser recibida y/o capturada y/o detectada (detección de portadora) por el nodo receptor. El modelo se aproxima a la interfase de radio DSSS (Lucent WaveLan direct-sequence-spread-spectrum). Las implementaciones de interface de red se encuentran en ~ns/phy.{cc,h} y ~ns/wireless-phy.{cc,h}.

Modelo de propagación de radio. Este modelo utiliza atenuación en espacio libre ($1/r^2$) en distancias cercanas y una aproximación al modelo de dos rayos ($1/r^4$)para distancias lejanas. La aproximación supone reflexión de tierra plana. La implementación de estos modelos se encuentran en ~ns/tworayground.{cc,h}.

Antena. Los nodos móviles utilizan una antena omnidireccional que tiene ganancia unitaria. La implementación se encuentra en ~ns/antenna.{cc,h}.

4.4 CÓDIGO EN ns-2 DEL MAC 802.11.

El protocolo MAC 802.11 fue implementado en C++, esta capa utiliza un formato RTS/CTS/DATOS/ACK para todos los paquetes que van dirigidos a un solo destino (unicast) en la red y simplemente envía DATOS para todos los paquetes de difusión (broadcast). La *clase Mac802_11* esta implementada en *~ns/mac-802_11.{cc,h}.*

Existen cuatro rutas diferentes que el código puede seguir [22]:

- Transmisión de un paquete
- Recepción de un paquete destinado para sí mismo
- Escuchar un paquete no destinado para sí mismo
- Paquetes en colisión

4.4.1 Transmisión de un paquete.

De forma general toma la siguiente ruta (cuando no hay errores o congestión):

recv() -> send() -> sendDATA() y sendRTS() -> poner defer timer
-> deferHandler() -> check_pktRTS() -> transmit()
-> recv() -> receive timer inicializado.
-> recv_timer() -> recvCTS() -> tx_resume() -> iniciar defer timer -> rx_resume()
-> deferHandler() -> check_pktTx() -> transmit()
-> recv() -> receive timer inicializado.
-> recv_timer() -> recvACK() -> tx_resume() -> callback_ -> rx_resume() -> Listo!

Cuando el primer RTS falla:

recv() -> send() -> sendDATA() y sendRTS() -> iniciar defer timer
-> deferHandler() -> check_pktRTS() -> transmit -> iniciar send timer
-> send_timer() -> RetransmitRTS() -> tx_resume() -> backoff inicializado
backoffHandler() -> check_pktRTS() -> transmit

El resto es igual que arriba.

4.4.2 Recepción de un paquete destinado para si mismo: De forma general toma la siguiente ruta (cuando no hay errores o congestión):

recv() -> receive timer inicializado
-> recv_timer() -> recvRTS() -> sendCTS() -> tx_resume() -> iniciar defer timer -> rx_resume()
-> deferHandler() -> check_pktCTRL() -> transmit()
-> recv() -> receive timer inicializado
-> recv_timer() -> recvDATA() -> sendACK() -> tx_resume()->iniciar defer timer->uptarget_-> recv()
-> deferHandler() -> check_pktCTRL() -> transmit() -> iniciar send timer
-> send_timer() -> tx_resume() <- Listo!

4.5 PASOS DE LA IMPLEMENTACIÓN DEL PROTOCOLO PCMA.

En esta sección se presentan los pasos de la implementación del protocolo PCMA, los pasos del protocolo corresponden a la situación en que un nodo *i* desea enviar un paquete al nodo *j* y un nodo *l* potencialmente interferente desea transmitir. Los pasos hacen referencia al algoritmo de pseudocódigo que se muestran en las siguientes figuras.

Se debe notar que el protocolo no utiliza las letras i,j,l ya que el código es general para cualquier nodo y por lo tanto no tendría sentido el utilizar estas letras para referirse a un nodo en particular o a su destino. La implementación se desarrolló para que funcione de acuerdo a los principios básicos que gobiernan el diseño de protocolos MAC de reuso espacial [6], para lo cual se utilizaron tablas para guardar información de los nodos transmisores y receptores como se ilustra a continuación en la tabla 4.1.

# de nodo Tx	# de nodo RX	t1	t_2	X	Y	Z	Pt
0							
1							
2							
3							
.							
.							
.							
n							

(a)

# de nodo Rx	t1	t2	X	Y	Z	Pt	Pr	I	S/I	# de nodo Tx	Flag
0											
1											
2											
3											
.											
.											
.											
n											

(b)

Tabla 4.1 (a) Transmisores (b) Receptores

4.5.1 Función recv() modificada.

Los cambios que se realizaron a la función recv() original, son en la parte de recepción del primer bit de un paquete que proviene de la capa física, como se observa en la figura 4.5, se emplea una condición para determinar si el nodo receptor está recibiendo un solo paquete, en este caso se llena una tabla de receptores con diferentes campos de este nodo como son: Id (identificador) del receptor, el tiempo en que recibe el primer bit, el tiempo en que recibirá el último bit del paquete, la posición xyz del nodo receptor, la potencia con la que le transmitieron el paquete y la potencia con la que lo recibe, el Id del nodo que le transmitió el paquete así como la ΣI que está recibiendo el nodo receptor y su relación S/ ΣI. En caso de que sea el segundo paquete que está recibiendo este nodo, la única acción que realiza es actualizar el campo ΣI.

El algoritmo presentado en la figura 4.5 es una modificación al algoritmo original (recv()) del archivo mac-802_11.cc, en este caso se hicieron los cambios mencionados anteriormente para que cada nodo receptor guarde información necesaria cada vez que recibe un paquete, de esta forma mantener actualizada la tabla de recepción para utilizar los datos almacenados durante la implementación del protocolo, esto es, calcular distancias, verificar interferencia en un nodo, además para poder saber si un nodo receptor se encuentra activo, etc.

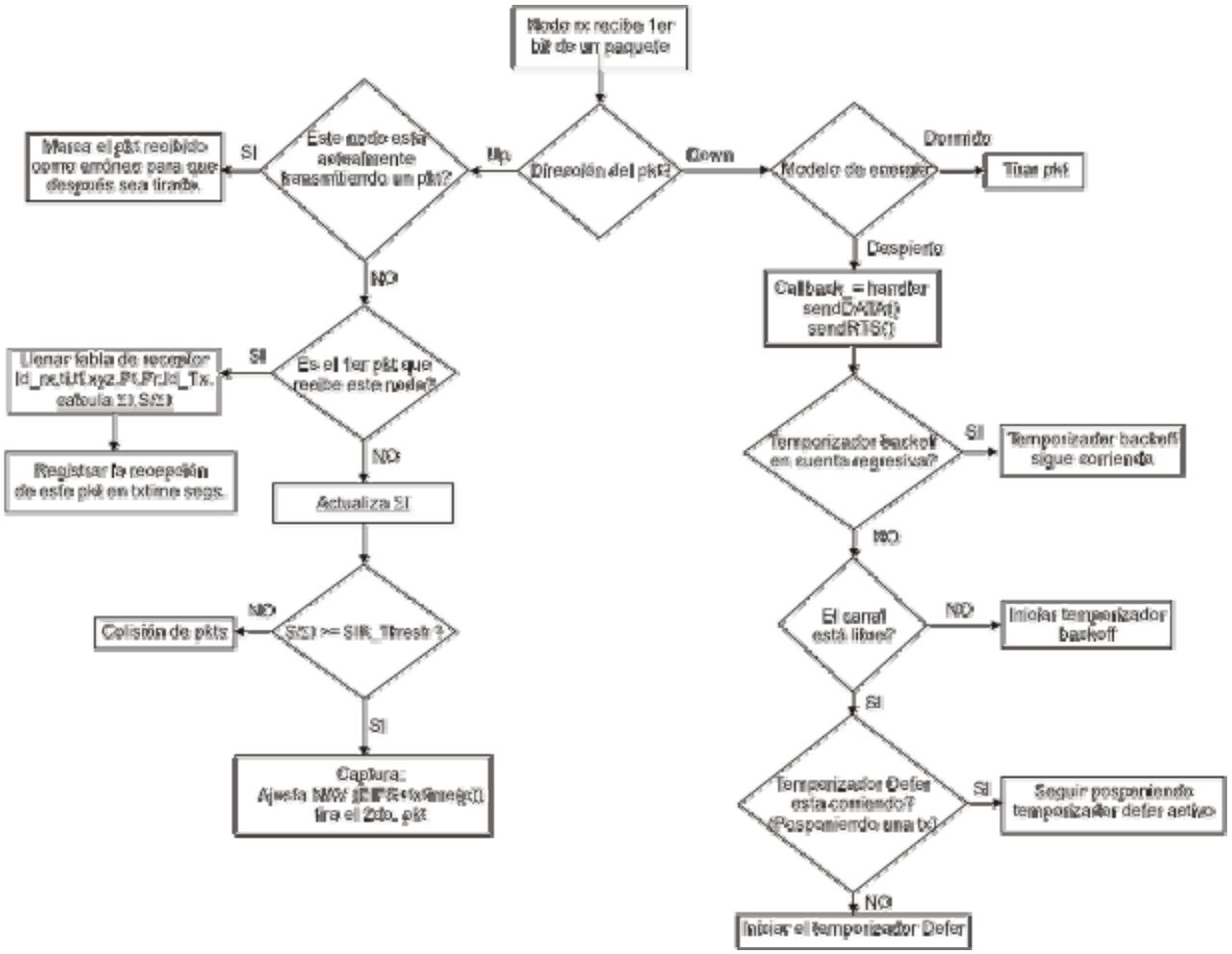

Figura 4.5. Algoritmo de la función recv() modificada.

4.5.2 Algoritmo para calcular y actualizar ΣI en un nodo receptor.

Como se mencionó en la función recv() modificada, el nodo receptor puede calcular o actualizar el campo de ΣI, esta acción se realiza mediante el algoritmo que se muestra en la figura 4.6.

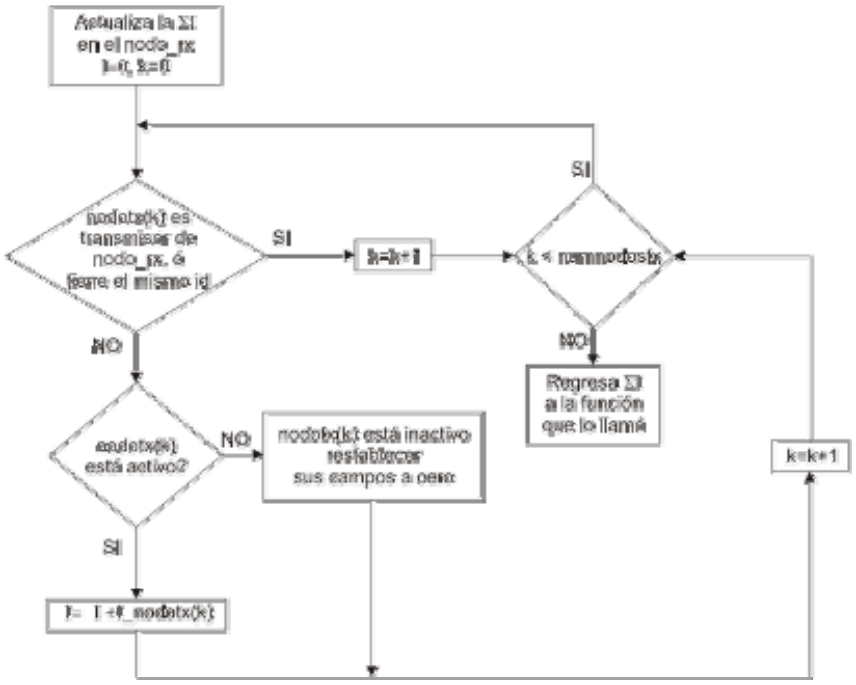

Figura 4.6. Algoritmo para calcular y actualizar ΣI en un nodo receptor.

De manera general, el receptor suma las interferencias que está recibiendo de todos los transmisores activos, excepto su propio transmisor. Esto es, primero se realiza una verificación de que el nodo transmisor en cuestión no sea el que le esta transmitiendo al nodo receptor (porque en este caso sería señal y no interferencia) y que no tenga el mismo Id del nodo receptor (ya que los nodos pueden ser tanto transmisores como receptores); si esto se cumple, se verifica que el nodo transmisor en cuestión este activo, es decir, que en el tiempo de simulación actual el nodo este transmitiendo un paquete, si esta condición se cumple se calcula (mediante la llamada del algoritmo que calcula la potencia interferente) y se suma la interferencia que esta causando este nodo transmisor y se verifica al siguiente nodo.

Si el nodo transmisor actual es el que le esta transmitiendo al nodo receptor, continúa con el siguiente nodo transmisor, siempre y cuando el contador de nodos transmisores no se haya excedido del total, que si fuera el caso simplemente regresa el valor de ΣI a la función que lo llamó. Si el nodo transmisor actual ya no esta activo restablece los campos de este nodo a cero y continúa con el siguiente nodo siempre y cuando el contador de nodos transmisores no se exceda del total.

4.5.3 Algoritmo para calcular la potencia interferente (Pr) en un nodo receptor.

Este algoritmo regresa el valor de la potencia interferente que ocasiona un nodo transmisor hacia un receptor, esto se realiza llamando a la función y pasándole como argumentos la potencia con la que se transmite y la distancia a la que se encuentra el nodo interferente. Dependiendo de la distancia, se emplea el modelo de dos rayos o el modelo de espacio libre, como se muestra en la figura 4.7.

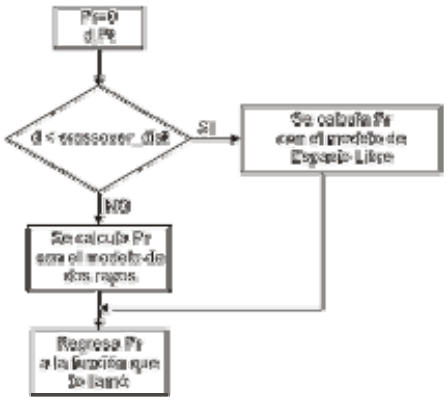

Figura 4.7. Algoritmo para calcular la potencia interferente (Pr) en un nodo receptor.

4.5.4 Funciones check_pktCTRL(), check_pktRTS() y check_pktTX() modificadas.

Estas funciones son llamadas cuando los temporizadores “defer” o “backoff” han expirado, lo que significa que un nodo ha esperado un tiempo suficiente antes de transmitir con el fin de reducir el riesgo de colisiones y ahora esta listo para transmitir un paquete, las funciones check_pktCTRL(), check_pktRTS() y check_pktTX() como se mencionó anteriormente son llamadas por las funciones backoffHandler() y deferHandler() dependiendo de que temporizador haya expirado.

Como se observa en la figura 4.8, la modificación realizada en estas funciones consiste en incluir una condición que verifica si el nodo que tiene un paquete listo para enviar satisface las condiciones de control de potencia (esto se realiza a través del algoritmo de condiciones de PCMA), si este no fuera el caso el paquete no se transmitirá y se realizará la acción especificada para cada tipo de paquete. Las condiciones de control de potencia se describen en el algoritmo que se muestra en la figura 4.9.

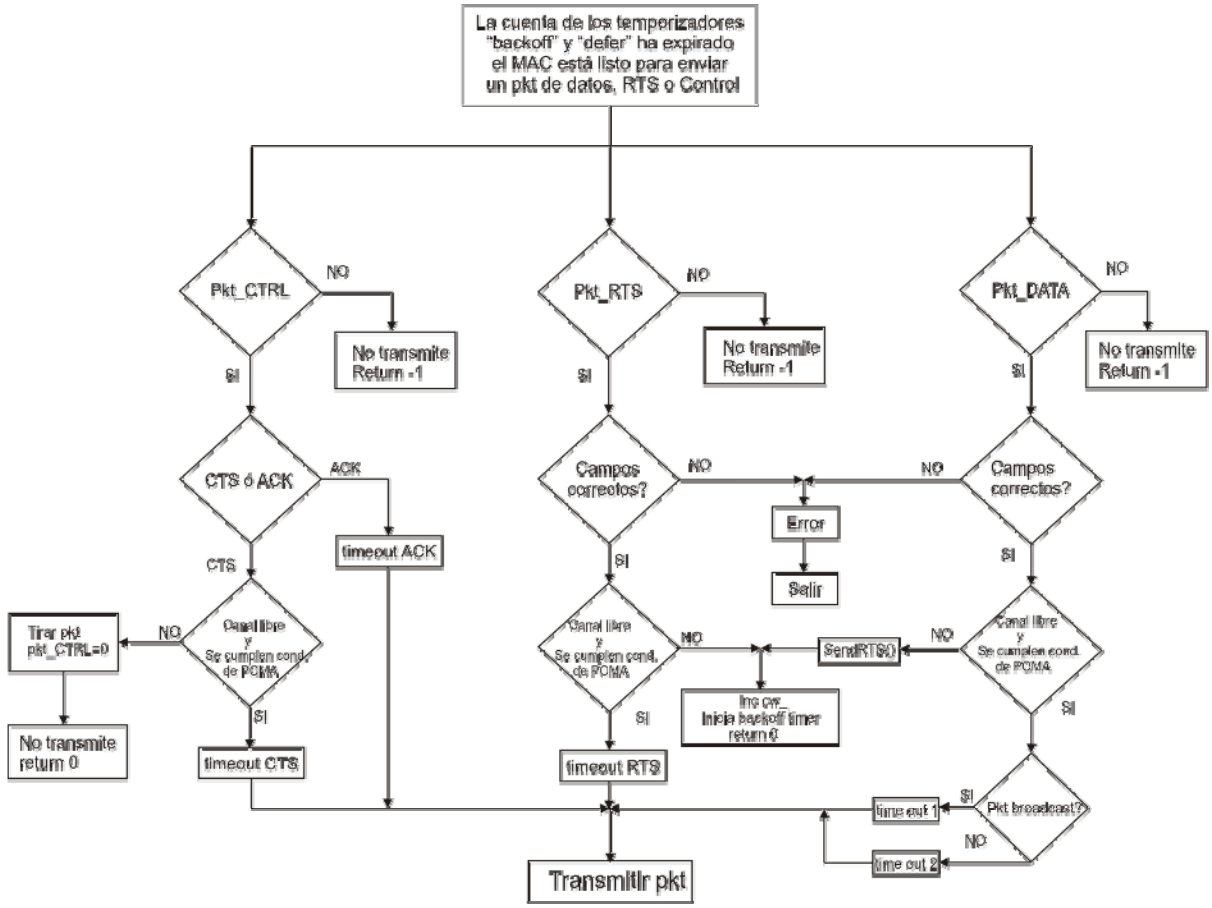

Figura 4.8. Funciones check_pktCTRL(), check_pktRTS() y check_pktTX() modificadas.

4.5.5 Algoritmo de condiciones de PCMA.

Esta función se llama cuando un nodo esta listo para enviar un paquete y realiza una ultima verificación para detectar si el canal está libre y se satisface las condiciones de control de potencia (esta última es la condición agregada a las funciones check_). Esta condición se realiza mediante el algoritmo que se muestra en la figura 4.9. La primera acción que realiza este algoritmo es calcular la interferencia (mediante el algoritmo calcular y actualizar ΣI en un

nodo receptor Figura 4.6) que en el tiempo de simulación actual el nodo receptor deseado esta recibiendo de todos los nodos transmisores interferentes, luego calcula la distancia que existe entre el posible transmisor y el receptor deseado.

Figura 4.9. Algoritmo de condiciones de PCMA.

Si el nodo receptor deseado esta recibiendo cierta cantidad de interferencia de nodos vecinos, se calcula una Prmin1 que es igual a la SIR deseada en ese nodo multiplicada por la ΣI que esta recibiendo el nodo, luego se obtiene la Prmin para el nodo receptor mediante la obtención del valor mas grande entre la Prmin1 y una Pr_deseada (que es 2% mas que Rx_Thresh), ya que Prmin1 podría resultar mas pequeña que el umbral de recepción de un paquete.

Si el nodo receptor deseado no esta recibiendo interferencia, entonces Prmin es igual a Pr_deseada en el nodo receptor. Una vez calculada Prmin y la distancia entre posible transmisor y el nodo receptor deseado, el siguiente paso es calcular la potencia mínima (Ptmin) con la que se va a transmitir el paquete, para esto se llama a la función que calcula Ptmin y se realiza una condición para verificar que este valor de Ptmin se encuentre dentro del rango de Pt_min y Pt_max para este protocolo de acuerdo con [6]. El siguiente paso es actualizar la ΣI que están recibiendo todos los nodos receptores activos, mediante el llamado del algoritmo para actualizar ΣI en TODOS los receptores, luego suponiendo que se transmite con Ptmin se hace un calculo de ΣI y $S/\Sigma I$ virtual en cada nodo receptor activo, para determinar si se afecta la recepción de un paquete en curso si se transmitiera con Ptmin. Si la $S/\Sigma I$ virtual es menor que la SIR_Thresh, significa que si se transmitiera con Ptmin, se afectará alguna comunicación en curso, por lo que la función regresa una bandera indicando que el nodo que estaba listo para transmitir no podrá hacerlo y tendrá que esperar otro tiempo antes de volver a intentarlo.

4.5.6 Algoritmo para calcular la Ptmin de un nodo que intenta transmitir.

Este algoritmo (Figura 4.10) regresa el valor de la potencia mínima que necesita un nodo que intenta transmitir hacia un nodo receptor deseado, esto se realiza llamando a la función y pasándole como argumentos la Prmin con que se desea que el nodo receptor reciba un paquete y la distancia a la que se encuentra el nodo receptor. Dependiendo de la distancia, se emplea el modelo de dos rayos o el modelo de espacio libre.

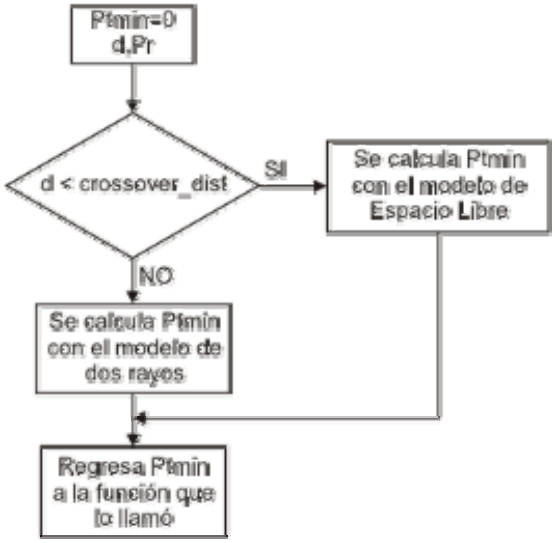

Figura 4.10. Algoritmo para calcular la Ptmin de un nodo que intenta transmitir.

4.5.7 Algoritmo para actualizar ΣI en TODOS los receptores.

Esta función se llama cuando se quiere actualizar la interferencia que están recibiendo todos los nodos receptores activos, los pasos que se realizan se muestran en la figura 4.11.

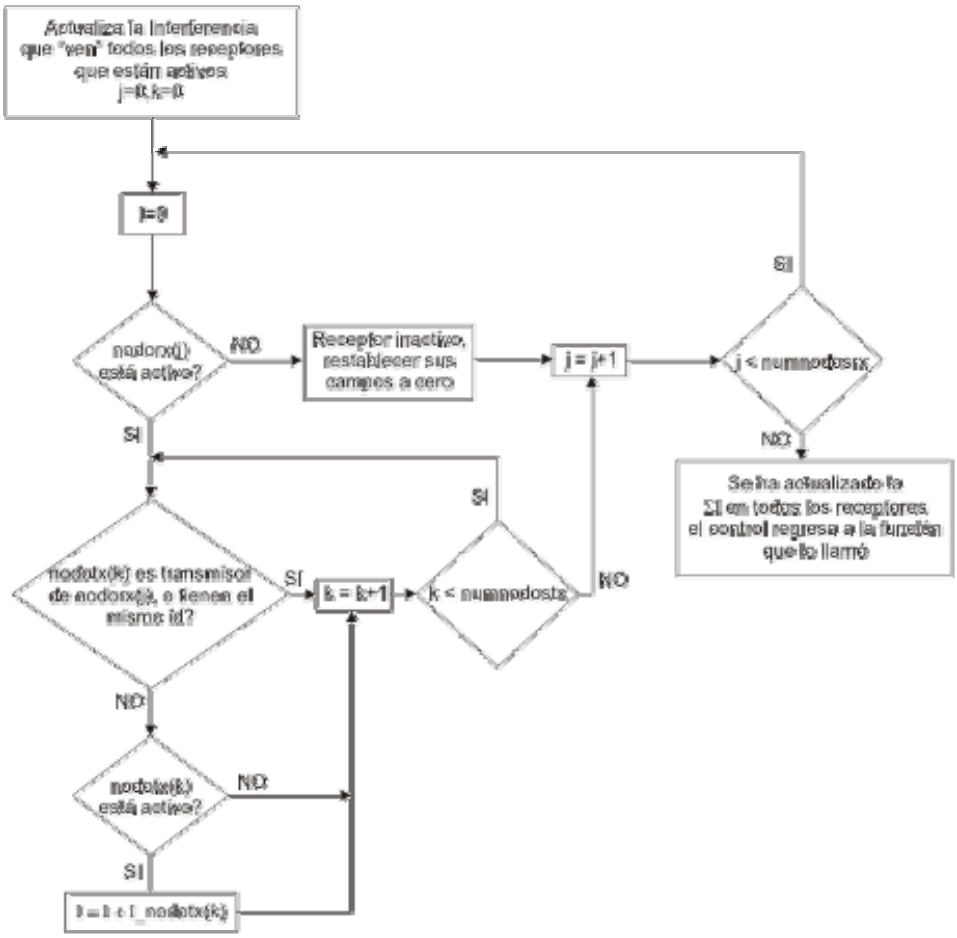

Figura 4.11. Algoritmo para actualizar ΣI en TODOS los receptores.

Primero se verifica si el nodo receptor en cuestión (nodorx(j)) está activo, es decir, que en el tiempo de simulación actual este recibiendo algún bit de un paquete, en este caso se realiza otra verificación para asegurarse que el nodo transmisor (nodotx(k)) no sea el transmisor del nodorx(j) y que no tengan el mismo id (ya que un nodo es transmisor y receptor), si esta condición se cumple se verifica que el nodotx(k) este activo en el tiempo de simulación actual, si es así, se suma la interferencia que le ocasiona al nodorx(j) y se continúa con el siguiente nodo transmisor, siempre y cuando el contador no se haya excedido del número total de nodos transmisores.

Si el nodotx(k) es transmisor del nodorx(j) o tienen el mismo id, o si el nodo nodotx(k) ya no está activo se incrementa el contador de transmisores y se continúa con el siguiente nodo transmisor. Si el contador de nodos transmisores se excede del número total, se continúa con el siguiente nodo receptor al que se desea actualizar la interferencia y el ciclo se inicia de nuevo, hasta que no haya más nodos receptores por actualizar, en este caso el control se regresa a la función que lo llamo, en este punto todos los receptores han actualizado su campo de interferencia.

4.5.8 Función transmit() modificada.

Esta función es la que se llama cuando un nodo va a transmitir un paquete, este macro se invoca en la última línea de las funciones check_ cuando todas las verificaciones han pasado y se han calculado los valores correspondientes de timeout para cada tipo de paquete. Los cambios que se realizaron en esta función fueron: agregar al encabezado común del paquete un campo de potencia (Ptmin) que fue calculado previamente en las funciones check_, llenar una tabla con los valores del nodo transmisor (id del nodo transmisor, id del nodo receptor, posición xyz del nodo transmisor, tiempo en que se envía el primer bit, tiempo en que se envía el último bit del paquete y potencia de transmisión) y restablecer los campos de ΣI de los nodos receptores y actualizarlos (Figura 4.12). El campo de Ptmin que se agregó al encabezado común del paquete se utiliza en la capa física, donde se especifica la potencia con la que será enviado el paquete.

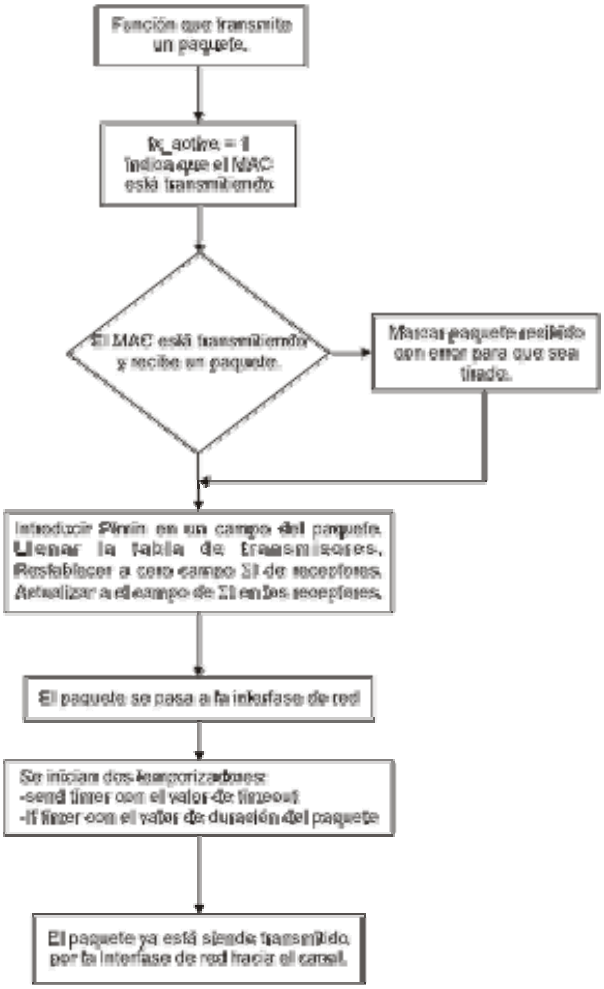

Figura 4.12. Función transmit() modificada.

Los temporizadores utilizados son los mismos, *send timer* es para indicar al MAC del posible fallo en la transmisión de un paquete, y que el MAC pueda realizar las acciones adecuadas si esto sucede; y el If timer le indica al MAC de que la capa física ha terminado de enviar el paquete.

En este capítulo se realizó una descripción general del simulador de redes *ns-2* y su utilidad en el modelado y simulación de diferentes tipos de redes, en especial redes inalámbricas ad hoc, se hizo una descripción del concepto de nodo móvil dentro del simulador así como de sus características internas; además, se presentó un breve tutorial sobre como realizar un script en tcl para la simulación de redes inalámbricas en *ns-2* y de las partes más importantes que sigue el programa mac-802_11.cc para el envio y recepción de paquetes. Por último se hace una descripción detallada por medio de algoritmos sobre las modificaciones que se hicieron a las funciones del archivo mac-802_11.cc.

Se debe observar que en el archivo original así como en el modificado se utilizan una serie de variables globales y locales que se utilizan en la mayoría de las funciones, como es el caso de los temporizadores. Estos temporizadores se utilizan para simular tiempos de espera y actividad de los nodos así como retardos, como son: tiempo que durará la transmisión de un paquete, tiempo que durará la recepción, tiempo en que se espera recibir un paquete, tiempo que un nodo debe esperar antes de iniciar la transmisión de un paquete, etc. Estos tiempos dependen del tamaño del paquete que se está enviando o recibiendo, de los tiempos IFS que se especifican de acuerdo a la capa física y son constantes de acuerdo a la versión del estándar, etc., por lo que el tamaño del paquete, los tiempos IFS y los retardos de transmisión afectan al comportamiento de los temporizadores y en consecuencia se podría presentar un menor rendimiento en la red.

CAPÍTULO V
EVALUACIÓN DEL DESEMPEÑO DEL PROTOCOLO PCMA

5.1 INTRODUCCION.

En este capítulo se investiga el desempeño del protocolo PCMA bajo diferentes condiciones de red, primero se describe el ambiente de simulación en el que fueron implementados PCMA y IEEE 802.11 luego se comparan las propiedades de rendimiento e igualdad de acceso de estos dos protocolos.

5.2 AMBIENTE DE SIMULACIÓN.

Para evaluar el desempeño del protocolo PCMA se utilizó el simulador *ns2* descrito en el capítulo anterior. Para el resultado de las simulaciones que se muestran, se quitó el overhead causado por los algoritmos de enrutamiento (ya que el objetivo de esta tesis es el de evaluar protocolos MAC y no protocolos de enrutamiento) y los destinos fueron restringidos a un salto de los nodos fuente.

Tipo de Parámetro	Valor del Parámetro
Tamaño del paquete	512 Bytes
Tasa de datos	2Mbps
Frecuencia portadora	914 MHz
RTS	20 Bytes
CTS, ACK	14 Bytes
Max. Retransmisiones MAC	7
SIR_Thresh	6 dB
SIR_Des	10 dB
CS_Thresh	-78 dBm
Rx_Thresh	-64 dBm
Rx_Des	-60 dBm
Pt_min	-7.5 dBm
Pt_max	28.5 dBm
Pt	24.5 dBm

Tabla 5.1 Parámetros de simulación

Los valores de los parámetros utilizados en la simulación se muestran en la tabla 5.1. Como se observa PCMA puede enviar a una potencia mínima de -7.5 dBm y una potencia máxima de 28.5 dBm, y 802.11 envía a una potencia fija de 24.5 dBm.

La potencia máxima de PCMA es 4 dB mayor que el de 802.11 de tal forma que un destino en el rango de transmisión máximo para 802.11 también estará en el rango de transmisión máximo de PCMA, permitiendo una compensación de potencia de transmisión de 4 dB. Esto permite que los mismos archivos de escenario (que determinan la conectividad de los nodos) sean utilizados por los dos protocolos. El modelo de tráfico es simple: los nodos fuente generan tráfico CBR y se escogen aleatoriamente del conjunto de todos los nodos, y los destinos se escogen también aleatoriamente del conjunto de todos los nodos, y están a un salto de los nodos fuente (en el rango de transmisión). Cada transmisión de datos entre fuente y destino será referida como un flujo, y cada flujo tendrá una tasa de transmisión especificada que se refiere al número de paquetes enviados por segundo. El tamaño de los paquetes de datos y RTS es de 512 y 20 bytes respectivamente mientras que el tamaño del paquete CTS y ACK es de 14 bytes.

El modelo del canal empleado en las simulaciones fue un simple modelo de pérdida por trayectoria que tiene un punto de sobre cruce fuera de la zona de Fresnel (86 m para los parámetros escogidos en estas simulaciones) de $\lambda/(4\pi d^2)$ (modelo de espacio libre) a $A/(d^4)$ (modelo de dos rayos), donde λ es la longitud de onda y A es una ganancia escalar que depende de la altura y ganancia de las antenas receptoras y transmisoras.

5.3 RENDIMIENTO.

En esta sección se evalúa el rendimiento de PCMA comparado con 802.11, el escenario utilizado en la simulación se muestra en la figura 5.1, en cada grupo se encuentran 50 nodos y se realizan 42 conexiones en cada grupo que hacen en total 84 conexiones en la red.

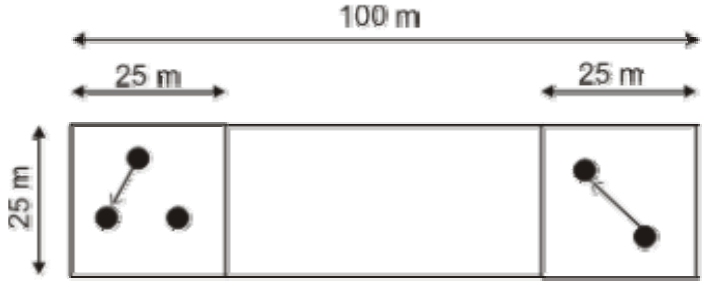

Figura 5.1 Ejemplo de 2 agrupaciones en una red de 100 por 100 m.

En la figura 5.1 se muestra un red sencilla de 2 agrupaciones de nodos, los nodos escogen un grupo (de 25 metros cuadrados cada uno y posicionados en las esquinas de una red de 100 por 25 m) de forma aleatoria y una posición aleatoria dentro del grupo.

La figura 5.2 demuestra el rendimiento para la región que contiene a las dos agrupaciones. El transmisor se escoge de manera aleatoria del conjunto de todos los nodos en la red y el destino también se escoge de manera aleatoria de los otros nodos en el grupo del transmisor. Como se observa en esta configuración, PCMA se desempeña mejor que 802.11, la mejora ocurre debido a que PCMA puede enviar paquetes simultáneamente en ambas agrupaciones mediante la reducción de su potencia de transmisión, mientras que en 802.11 cada nodo en un grupo debe competir siempre con los nodos del otro grupo (aparte de los nodos de su mismo grupo).

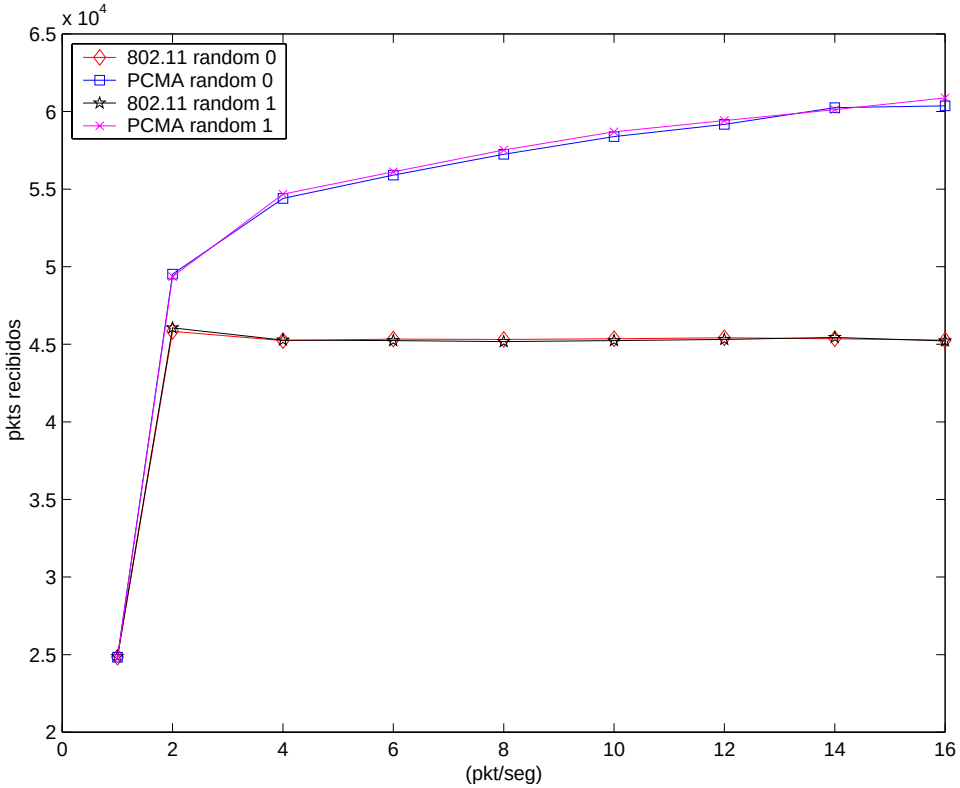

Figura 5.2 Rendimiento para una red de 100 por 100 m con nodos separados en regiones agrupadas, con 84 flujos cada uno enviando 512 bytes.

Como se muestra en la figura 5.2, conforme la red se hace mas agrupada el rendimiento se incrementa debido a que hay un mayor número de transmisiones simultáneas y la competencia entre los nodos es menor que si compitieran con los nodos del otro grupo. Este tipo de escenarios definen bien la distribución de usuarios en un ambiente típico ya que en la mayoría de los casos se espera que los usuarios se encuentren distribuidos en grupos.

5.4 IGUALDAD DE ACCESO.

En la figura anterior (figura 5.2) se observa que el desempeño del protocolo controlado por potencia sigue incrementando aún bajo cargas altas, debido a que las transmisiones de rangos grandes son bloqueadas por los límites de potencia de transmisión, permitiendo un número más grande de transmisiones de rangos cortos. Conforme la carga en la red se incrementa, la probabilidad de que un nodo requiera mas potencia que el límite de potencia de transmisión, también se incrementa. La potencia esperada para que una fuente alcance a su destino se incrementará conforme la carga en la red se incrementa debido a un incremento en el ruido de fondo. Las fuentes que requieren mayores potencias de transmisión (esto es, rangos de transmisión más grandes para un simple canal con pérdidas por trayectoria) entrarán en *backoff* con mayor probabilidad, permitiendo un número más grande de transmisiones de rangos cortos. Por consiguiente, un MAC controlado por potencia que opera en ambiente de acceso múltiple, resultará en favoritismo (injusto) hacia pares fuente-destino que envían en distancias mas cortas. Este fenómeno es particularmente evidente sobre el rango de conectividad de 250-m para PCMA, para demostrarlo se realizaron diferentes pruebas, donde la fracción de paquetes totales recibidos por nodos destinos en cinco rangos de distancias (0-50, 50-100, 100-150, 150-200, 200-250) de sus fuentes, se muestran para 100 flujos que envían, 1, 4, 16, 64 paquetes por segundo. Un protocolo perfectamente justo resultaría en un número de paquetes enviados a cada rango linealmente creciente, dado que el número de destinos dentro de cada rango se incrementa en proporción a $2\pi r$, donde r es la distancia desde el nodo fuente.

En las figuras que se muestran a continuación se observa el porcentaje de paquetes enviados a cada rango para demostrar que PCMA con cargas altas es injusto para las conexiones de rangos más grandes, en comparación con 802.11.

Los valores de los parámetros utilizados en la primera prueba se muestran en la tabla 5.2. Como se observa, el área del escenario es de 300 por 300 m donde se colocaron 400 nodos con posiciones aleatorias, de las cuales se establecieron 100 flujos aleatorios en diferentes rangos, 3 en el rango de 0-50 m, 14 en el rango de 50-100 m, 19 en el rango de 100-150 m, 28 en el rango de 150-200m y por último 36 en el rango de 200-250m, el tipo de paquetes utilizados fue CBR/UDP de 512 Bytes de tamaño y el tiempo en que se realizó la simulación fue de 300 segundos. Los valores de potencia mínima y máxima también se muestran en la tabla así como los umbrales y valores deseados de la relación señal a interferencia, de detección de portadora, y de potencia de recepción de un paquete.

Parámetros	**Valor del parámetro**
Área de escenario	300x300 m
# nodos	400
# conexiones	100
conex. Uniforme en 10 seg	NO
1,4,16,64 pkt/seg	SI
Tipo de paquete	CBR/UDP
Tamaño de paquete	512 bytes
Random	1
Nodos por Rango	3, 14, 19,28, 36
Tiempo de simulación	300 seg
Ptmin	0.1778e-3 W
Ptmax	0.707945W
SIR_Thresh	6 dB
SIR_Deseada	10 dB
CS_Thresh	1.5849E-11
Rx_Thresh	3.981E-10
Rx_Deseada	4.06062E-10

Tabla 5.2 Parámetros utilizados para la simulación del escenario de 300 por 300 m.

Otro parámetro que se consideró fue el valor de random puesto a 1, ya que se observó que al variar este valor los resultados se mantenían constantes por lo que se optó por utilizar este valor en el resto de las simulaciones.

En la figura 5.3 se muestran los resultados obtenidos de la simulación con los parámetros de la tabla 5.2. Se observa que para 1 y 4 paquetes por segundo el comportamiento de PCMA es bastante equitativo, esto se debe a que el área de simulación es relativamente pequeña y las conexiones se encuentran muy juntas haciendo que las conexiones de rangos cortos compitan entre si (como el caso del MAC 802.11 original), permitiendo conexiones de rangos más grandes, lo que hace que el acceso al canal sea más equitativo. Por otro lado, al transmitir 16 y 64 paquetes por segundo, el protocolo se vuelve más injusto ya que la mayor parte de paquetes enviados caen en el rango de 50-100 m mientras que los de rangos medios se mantienen y los de rangos más grandes disminuyen. Como se mencionó anteriormente, conforme se incrementa la carga en la red la potencia esperada por una fuente para alcanzar a su destino también se incrementa debido a un incremento en el ruido de fondo por lo que las fuentes con rangos de transmisión más grandes tienen más probabilidad de entrar en backoff.

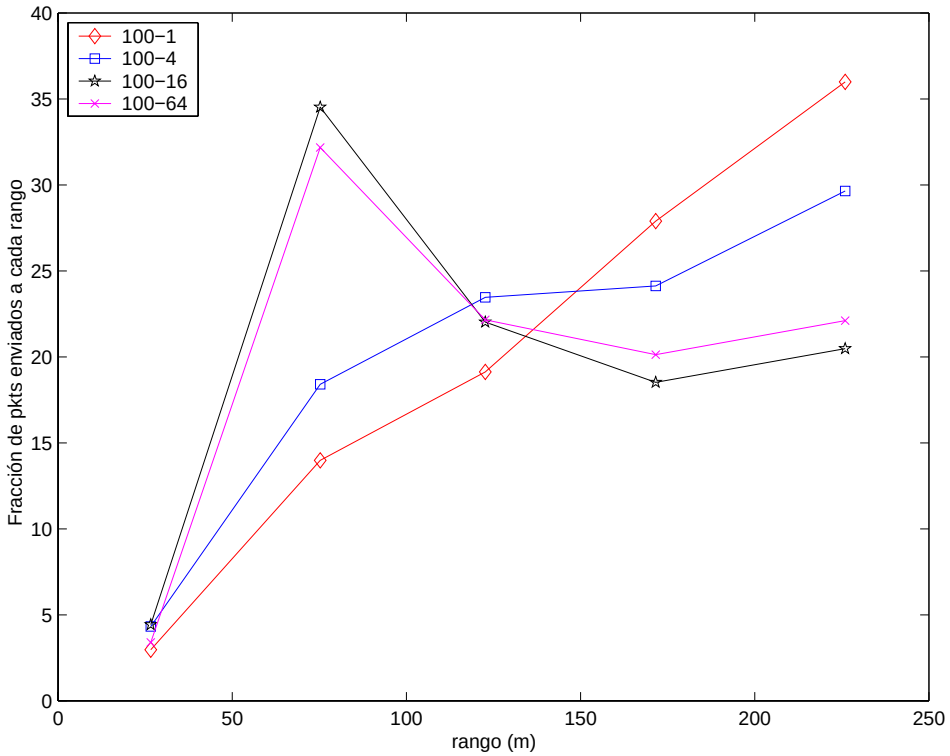

Figura 5.3 Distribución de rangos de destinos para PCMA en una red de 300 x 300 m.

La tabla 5.3 muestra los valores de los parámetros utilizados en la segunda prueba realizada, en esta prueba se cambió el área de simulación a 500 por 500 m así como la distribución de las conexiones que se realizó de manera uniforme entre 0 y 10 segundos. Los otros parámetros se mantuvieron sin cambios.

Parámetros	**Valor del parámetro**
Area de escenario	500x500 m
# nodos	400
# conexiones	100
conex. Uniforme en 10 seg	SI
1,4,16,64 pkt/seg	SI
Tipo de paquete	CBR/UDP
Tamaño de paquete	512 bytes
Random	1
Nodos por Rango	3, 14, 19,28, 36
Tiempo de simulación	300 seg
Ptmin	0.1778e-3 W
Ptmax	0.707945W
SIR_Thresh	6 dB
SIR_Deseada	10 dB
CS_Thresh	1.5849E-11
Rx_Thresh	3.981E-10
Rx_Deseada	4.06062E-10

Tabla 5.3 Parámetros utilizados para la simulación del escenario de 500 por 500 m.

La fracción de paquetes enviados a cada rango para el escenario de 500 por 500 m se muestra en la figura 5.4. En esta gráfica se puede observar más claramente lo que se mencionó al principio de la sección, de que un MAC controlado por potencia resulta en favoritismo injusto hacia las conexiones de rangos más cortos ya que las transmisiones de rangos grandes son bloqueadas por los límites de potencia de transmisión. Además se observa en la figura 5.4 que al aumentar la carga a 4, 16 y 64 paquetes por segundo, este fenómeno se vuelve más evidente ya que la potencia esperada para que un nodo fuente alcance a su destino aumenta al incrementar la carga, por lo que las fuentes que tengan rangos de transmisión más grandes tendrán mas probabilidad de entrar en backoff.

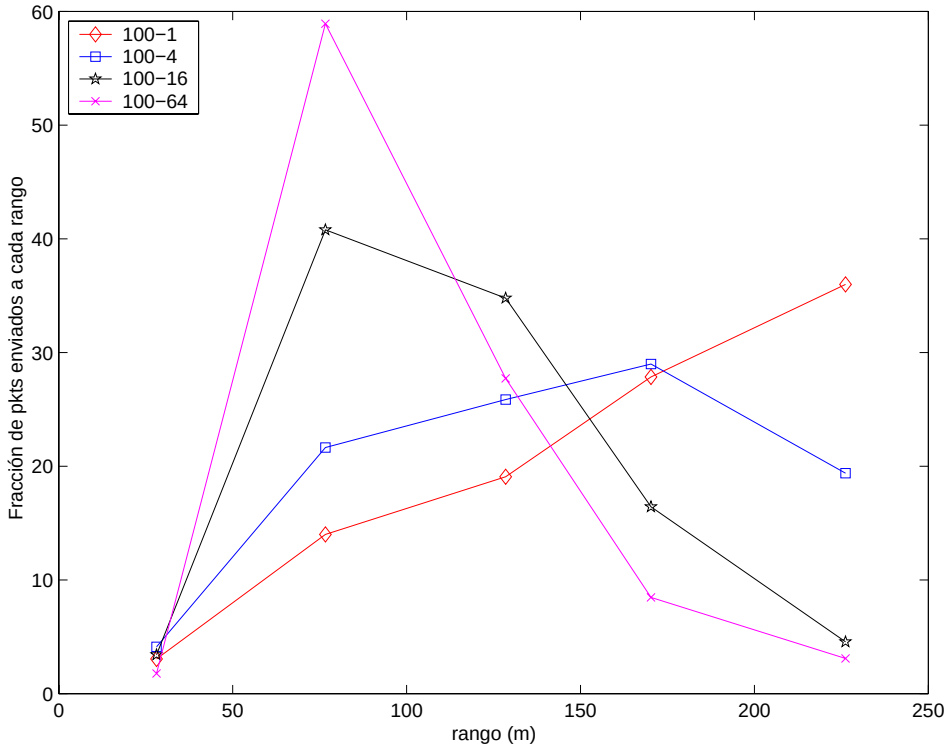

Figura 5.4 Distribución de rangos de destinos para PCMA en una red de 500 x 500 m.

Para la tercera prueba, se realizaron dos cambios, el área de simulación a 1000 por 1000 m y el número de nodos en la red a 1600 nodos (tabla 5.4), los demás parámetros se mantuvieron sin cambios.

Parámetros	**Valor del Parámetro**
Área de escenario	1000x1000
# nodos	1600
# conexiones	100
conex. Uniforme en 10 seg	SI
1,4,16,64 pkt/seg	SI
Tipo de paquete	CBR/UDP
Tamaño de paquete	512 bytes
Random	1
Nodos por Rango	3, 14, 19,28, 36
Tiempo de simulación	300 seg
Ptmin	0.1778e-3 W
Ptmax	0.707945
SIR_Thresh	6 dB
SIR_Deseada	10 dB
CS_Thresh	1.5849E-11
Rx_Thresh	3.981E-10
Rx_Deseada	4.06062E-10

Tabla 5.4 Parámetros utilizados para la simulación del escenario de 1000 por 1000 m.

En la figura 5.5 se muestran los resultados obtenidos de la simulación con los parámetros de la tabla 5.4. Se observa que para 1 y 4 paquetes por segundo el comportamiento del protocolo es equitativo, es decir, el número de paquetes enviados a cada rango se incrementa linealmente, esto se debe a que el área de simulación es relativamente grande y las conexiones se encuentran separadas unas de otras permitiendo transmisiones simultáneas entre pares fuente-destino de diferentes rangos. Sin embargo, al incrementarse la carga en la red a 16 y 64 paquetes por segundo la tasa de paquetes enviados sobre una gran distancia decrece y la mayoría de las conexiones son de rangos cortos.

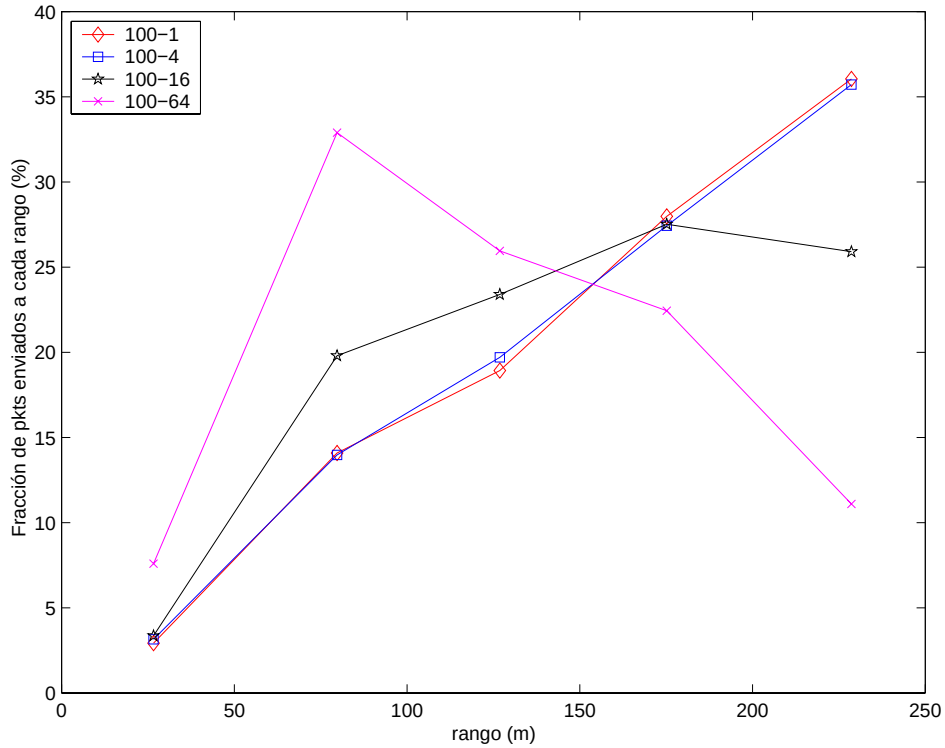

Figura 5.5 Distribución de rangos de destinos para PCMA en una red de 1000 x 1000 m.

La fracción de paquetes enviados a cada rango para 802.11 se muestra en la figura 5.6. El protocolo también se observa que es un poco injusto (envía un poco menos de paquetes en rangos más grandes y se reciben más paquetes en los rangos cortos) conforme la carga se incrementa, pero no al extremo de un protocolo controlado por potencia como PCMA. El protocolo 802.11 tiene una probabilidad igual de enviar paquetes a los destinos a cualquier distancia dado que la potencia de transmisión no se toma en cuenta mientras se compite por el canal.

Sin embargo, dado que todas las transmisiones son enviadas con niveles de potencia fijas, hay menos protección de ruido para los destinos mas alejados de sus fuentes, resultando en un número grande de paquetes perdidos con cargas de red más grandes. Además, 802.11 tiene un rango de interferencia fijo que está determinado por el rango sobre el cual otros nodos pueden “escuchar” paquetes RTS o CTS, y el rango sobre el cual otros transmisores pueden detectar la energía de algún transmisor. Sin embargo, este rango debería ser incrementado conforme la distancia entre pares fuente destino se incrementa ya que estos reciben menos potencia de la señal deseada, también debería incrementarse conforme un receptor se encuentre bastante expuesto a la energía de otros transmisores. Por consiguiente, con cargas más altas el ruido de fondo agregado causará que los receptores que obtienen menor potencia de la señal deseada de su transmisor correspondiente, tengan más paquetes erróneos. Por otro lado, PCMA tiene la misma cantidad de protección (4 dB de compensación de potencia) para los destinos en todos los rangos; sin embargo, la probabilidad de enviar un paquete a destinos más alejados se reduce al aumentar la carga en la red como se describió arriba.

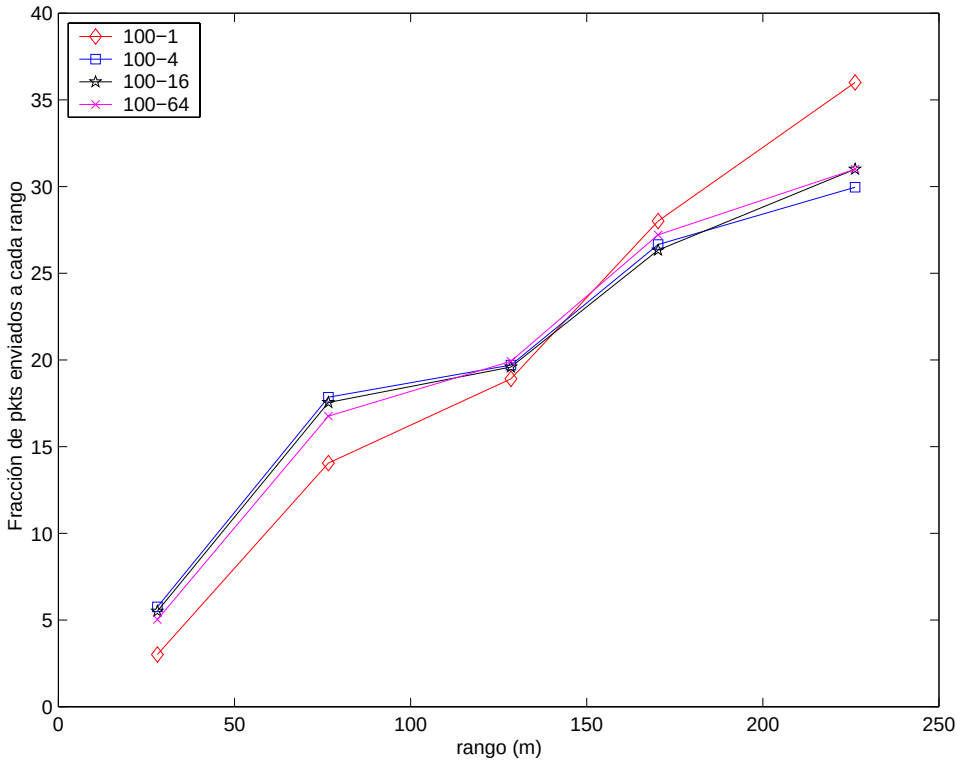

Figura 5.6 Distribución de rangos de destinos para 802.11.

En este capítulo se evaluaron los protocolos de acceso al medio controlado por potencia (PCMA) y el MAC 802.11 de acuerdo al rendimiento y la igualdad de acceso al medio. Se observó que en PCMA el rendimiento es mejor en comparación con 802.11 cuando el tráfico está localizado y los usuarios se encuentran distribuidos en grupos, como es el caso de un ambiente de trabajo típico, esto sucede debido a que PCMA puede enviar paquetes simultáneamente en ambos grupos mediante la reducción de la potencia de transmisión, lo que hace que cada nodo compita solo con los otros nodos de su grupo. Sin embargo, una desventaja observada en el protocolo PCMA en comparación con el MAC 802.11 es la desigualdad de acceso al medio, ya que en PCMA las transmisiones de rangos largos son bloqueadas por los límites de potencia de transmisión ya que en una transmisión de rango largo la potencia esperada para que una fuente alcance a su destino se incrementará conforme la carga en la red aumenta debido a un incremento en el ruido de fondo, por lo que las fuentes que requieran mayores potencias de transmisión entrarán en *backoff* con mayor probabilidad, permitiendo un número más grande de transmisiones de rangos cortos. Por otro lado, se observó que en el MAC 802.11 el acceso al medio es más equitativo ya que en este protocolo se tiene la misma probabilidad de enviar los paquetes a los destinos a cualquier distancia ya que no se toma en cuenta la potencia de transmisión mientras se compite por el canal.

En resumen, para PCMA la fase de contención favorece a los nodos que compiten con menos potencia (pares fuente-destino con rangos más cortos), pero una vez que los nodos han competido por el canal, todos reciben la misma calidad de señal, sin embargo, en 802.11 la fase de contención no favorece a algún nodo en particular, pero cuando un nodo ha competido exitosamente, los pares fuente-destino que se encuentran alejados reciben una calidad de señal mas baja [17].

CAPÍTULO VI
PCQoS: CALIDAD DE SERVICIO CONTROLADO POR POTENCIA EN REDES INALAMBRICAS AD HOC.

6.1 INTRODUCCIÓN.

Las principales ventajas y desventajas de la calidad de servicio (QoS) involucradas en una red inalámbrica Ad Hoc están relacionadas al número promedio de veces que un paquete es reenviado contra el número promedio de nodos interferentes por transmisión intentada [5]. El Incremento del rango de transmisión reduce el número de veces que un paquete necesita ser reenviado por nodos intermedios hacia su destino final, sin embargo, al incrementar el rango de transmisión también se incrementa la interferencia y por consiguiente, la competencia por el canal cada vez que un nodo intenta transmitir, de esta manera incrementándose los retardos de transmisión. Una situación inversa sucede cuando se reduce el rango de transmisión, en [23] se muestra que el reducir el rango de transmisión es una mejor solución en términos de incrementar la capacidad de transportar tráfico de redes inalámbricas Ad Hoc. El análisis presentado en [23] solo considera la capacidad física de la red y no la ineficiencia del protocolo MAC empleado para transportar datos. Desafortunadamente, los protocolos MAC utilizados en las redes inalámbricas Ad Hoc proporcionan un desempeño limitado, en particular aquellos protocolos desarrollados para operaciones de acceso a un medio compartido.

El estándar IEEE 802.11 no es el mejor protocolo MAC para redes inalámbricas Ad Hoc de múltiples saltos [26], ya que las aplicaciones experimentan retardos y bajos niveles de rendimiento. Disminuir el rango de transmisión produce un incremento en el número de saltos para alcanzar a su destino, y cada vez que el siguiente salto intenta transmitir y detecta que el medio esta ocupado, entra en backoff (con un periodo de tiempo que incrementa exponencialmente por cada intento de transmisión fallido) antes de intentar transmitir otra vez utilizando el protocolo de acceso CSMA/CA. Este problema se acentúa con el hecho de que todos los nodos deben usar el mismo rango para todas las transmisiones de paquetes de control y datos, exhibiendo un pobre reuso espectral (e.g. número de transmisiones simultáneas que toman lugar en la red al mismo tiempo).

El objetivo de este capítulo es el de estudiar la interacción entre control de potencia y calidad de servicio entregada a las aplicaciones para redes inalámbricas ad hoc. Basándonos en los resultados de este estudio se propone, diseña, implementa y evalúa el protocolo *PCQoS* (Calidad de servicio controlado por potencia) para capturar las ventajas y desventajas de la relación potencia/calidad de servicio para aplicaciones que desean mejorar el desempeño de calidad de servicio con el costo de agregar más saltos a sus trayectorias.

PCQoS representa el primer esquema de enrutamiento que integra algoritmos de control para realizar este balance de potencia/calidad de servicio en redes inalámbricas ad hoc. PCQoS puede ser usado para establecer un conjunto de clases de servicios diferenciados en redes ad hoc, por ejemplo, este tipo de redes podría ofrecer dos tipos de clases de servicios a los dispositivos/aplicaciones: 1) una clase dorada, que intenta mejorar el rendimiento y retardo que observan las aplicaciones/dispositivos; y 2) una clase de mejor esfuerzo con un rendimiento más pobre y mayor retardo. PCQoS ofrece una variedad de estrategias y políticas que hacen a las diferentes clases de servicios fáciles de implementar. Bajo este régimen, las aplicaciones que necesiten un desempeño preferencial de rendimiento o retardo, se suscribirán a las clase dorada mientras que las otras aplicaciones usarían la clase normal de mejor esfuerzo. Tal división de aplicaciones en redes inalámbricas ad hoc controladas por potencia representan una nueva dirección, ya que las redes inalámbricas ad hoc del futuro necesitarán proporcionar diferenciación de servicio para posibles clases diferentes de aplicaciones. Estas aplicaciones aún no emergen, pero con el desarrollo de este protocolo se anticipa que aplicaciones existentes tales como flujos en tiempo real y aplicaciones de transacción de datos se beneficiarán de redes inalámbricas ad hoc construidos en técnicas de calidad de servicio controlado por potencia.

6.2 MAYOR REUSO ESPECTRAL EN IEEE 802.11.

Recordando la desigualdad de acceso de los protocolos basados en SR-CSMA, se observó en la figura 5.4 que para una red con poco tráfico (por ejemplo, 1 pkt por segundo) PCMAP se comporta de manera equitativa, ya que la fracción de paquetes enviados a cada rango se incrementa linealmente. En el caso donde la red opera bajo condiciones de tráfico más pesados, la fracción de paquetes enviados en distancias más grandes disminuye debido al comportamiento desigual de SR-CSMA.

Este es el resultado de la regla número 2 (ver sección 3.4.2 del capítulo 3) de los MACs basados de SR-CSMA que dicta que ninguna fuente que inicie una nueva transmisión puede desestabilizar transmisiones en curso mediante una transmisión demasiado “ruidosa”. Para transmisiones de rangos grandes es improbable que consigan una oportunidad de transmitir en presencia de transmisiones en curso de rangos cortos en su vecindad.

Esta desigualdad de acceso se utiliza como la base para proporcionar servicios diferenciados en redes inalámbricas ad hoc. La intuición es como sigue: *Si rompemos una transmisión de rango grande en transmisiones de rangos más cortos, entonces podemos incrementar muy probablemente la oportunidad de transmisión de las conexiones resultantes de rangos más cortos, mejorando la calidad de servicio observada por un flujo en particular.* Este objetivo se puede lograr agregando nodos repetidores entre pares fuente-destino. Este método, sin embargo podría ser perjudicial hacia otros flujos y hacia la capacidad total de la red para transportar tráfico como se mostrará mas tarde en la sección 6.5. En lo que sigue, estudiaremos las ventajas y desventajas mediante “PCQoS “y se discutirá sus beneficios y desventajas con más detalle en la siguiente sección, utilizaremos el término redirector en vez de nodo repetidor para diferenciar cuando se agregan nodos intermedios en los enlaces.

6.3 PROTOCOLO PCQoS.

En la sección previa se mencionó que dividiendo un enlace de rango grande en enlaces de rangos más cortos podría impactar la calidad de servicio en la capa de aplicación tal como rendimiento y retardo. Ahora consideraremos la construcción de un mecanismo de calidad de servicio para aplicaciones específicas que desean tomar ventaja en el mejoramiento de su calidad de servicio. Esta ventaja, no ha sido discutida en la literatura y podría lograrse simplemente agregando redirectores entre pares fuentes destino, consecuentemente habilitar un cierto control en el desempeño de rendimiento y retardo que ven las aplicaciones.

La figura 6.1 muestra las ventajas y desventajas de agregar redirectores a una ruta. Los parámetros de simulación son los mismos que en la figura 5.4 excepto que aquí uno de los 36 flujos en el rango de 200-250 metros fue dividido en enlaces de rangos más cortos mediante la adición de redirectores entre la fuente y el destino. Para el caso de un redirector, el nodo repetidor se escogió para que estuviera a la mitad entre el nodo transmisor y receptor, para el caso de tres redirectores los tres nodos repetidores fueron puestos

aproximadamente a distancias iguales entre los nodos transmisor y receptor y así sucesivamente. Al agregar un redirector en la ruta, se observa en la figura 6.1 que el rendimiento se incrementa en casi 1000% comparado con cero redirectores (que es el rendimiento obtenido por este flujo en la figura 5.4), el poner tres redirectores incrementa el rendimiento en 21% comparado con un redirector. Para 5 y 7 redirectores se observa en la figura que el rendimiento empieza a empeorar. Después de observar este comportamiento podemos identificar dos zonas operacionales en la figura 6.1, la zona izquierda que le llamaremos estable donde la adición de redirectores se traduce en una mejora en el rendimiento y la zona derecha o inestable donde el agregar redirectores empeora el rendimiento.

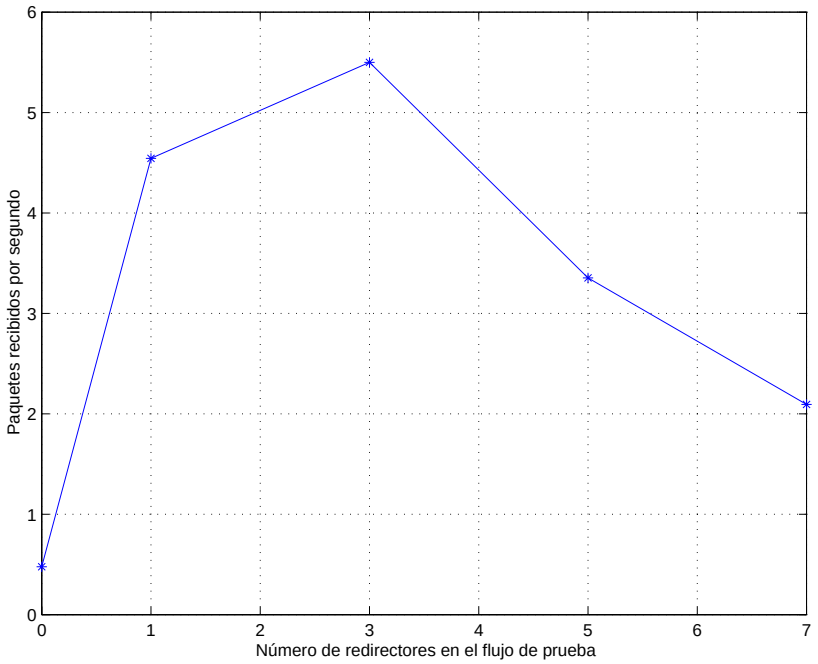

Figura 6.1. Paquetes recibidos vs número de redirectores

Cuando se habilita la adición o la sustracción de redirectores para lograr un control de calidad de servicio, necesitamos poner atención particular en cuales usuarios pueden agregar o remover redirectores con el propósito de asegurar operaciones significativas y estables para la red inalámbrica como un todo. Esto es porque el agregar un redirector a un flujo impacta el desempeño de calidad de servicio de posiblemente (en el peor caso) de todos los otros flujos en la red. Permitirle a todos los flujos agregar o remover redirectores puede resultar en una solución inestable (zona derecha de la figura 6.1) donde cada flujo intente optimizar sus propias restricciones de calidad de servicio al mismo tiempo.

A este fenómeno le llamaremos *efecto domino;* este efecto puede ser visto como el impacto global de una estrategia ambiciosa local por un nodo/aplicación/usuario. Con el propósito de que un flujo tenga cierto control sobre su calidad de servicio, es suficiente controlar el número de redirectores utilizados solo por este flujo. De manera más precisa, es necesario controlar de cierta manera el número y la posición de los redirectores en la red.

Con el propósito de controlar el impacto del efecto *domino* en la red es necesario limitar el número y la tasa de adición o remoción de redirectores en la red. La manera más simple de lograr este objetivo es limitando el número de flujos que están permitidos agregar o remover redirectores, por ejemplo, los flujos del *plan dorado* pueden tener este control para optimizar el desempeño de su aplicación mientras que los usuarios *normales* no pueden. Esta política esencialmente diferencia entre la población de nodos/usuarios/aplicaciones en la red. Tal política ayudaría a limitar el número de usuarios de servicio dorado por un proveedor de servicios de internet (ISP) con el propósito de soportar calidad de servicio diferenciado sobre los usuarios normales. PCQoS esta motivado en este modelo, como su nombre sugiere, PCQOS balancea potencia de transmisión y desempeño de calidad de servicio para flujos en redes inalámbricas ad hoc.

En PCQoS se propone que solo un subconjunto de flujos/aplicaciones tenga la capacidad de agregar o remover redirectores. Los flujos que tengan esta flexibilidad serían más sensibles que los otros flujos en términos de sus requerimientos de calidad de servicio, por ejemplo, algunas aplicaciones podían estar transmitiendo información sensible a retardo como es el caso de audio de tasa baja o mensajes de alarma importantes, mientras que otras aplicaciones podrían transmitir información insensible a retardos tales como mediciones locales de temperatura como es el caso de las redes de sensores. De manera más específica, definimos “clase dorada” para flujos (alta prioridad) que son sensibles a potencia y calidad de servicio y “clase normal” (baja prioridad) a los flujos que toleran calidad de servicio de mejor esfuerzo. La separación de flujos usando diferentes prioridades no es una limitación de PCQoS sino una propiedad común de los protocolos que intentan mejorar el desempeño promedio de cierto conjunto de flujos en deterioro de otros, como es el caso del modelo *Diffserv* abordado en IETF [24].

6.3.1 Descripción del Protocolo.

PCQOS está definido por las fases de *monitoreo* y *control*. Durante los periodos de monitoreo, los flujos de clase dorada monitorean el flujo continuo de paquetes de sus respectivas fuentes y pueden decidir tomar o no tomar acciones de control Potencia-Calidad de servicio basándose en alguna política específica del usuario o la aplicación. Durante la fase de control, los redirectores pueden ser agregados o removidos dinámicamente de las trayectorias de los flujos de clase dorada. El posicionamiento de lo redirectores no solo tiene que ver con agregarlos o removerlos de la trayectoria de red, sino también con la ubicación de los redirectores en relación con los flujos de clase dorada.

La figura 6.2 ilustra el ciclo operacional de PCQoS. En esta figura se muestra un ejemplo del comportamiento de desempeño de un parámetro (esto es, rendimiento, retardo, etc.) para un flujo hipotético con respecto al tiempo.

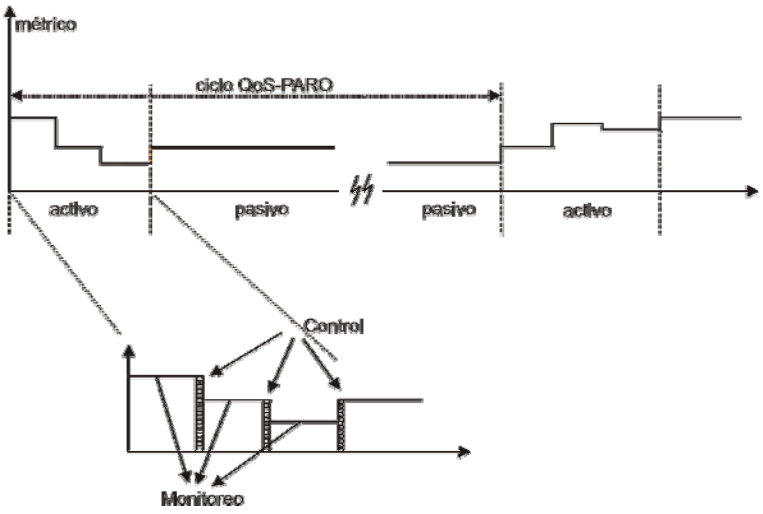

Figura 6.2 Ciclo Operacional de PCQoS.

El ciclo PCQoS tiene periodos operacionales *pasivos* y *activos*; durante los periodos activos, los flujos de clase dorada pueden agregar o remover redirectores de sus rutas con el propósito de modificar su desempeño potencia-calidad de servicio, diferentes flujos de clase dorada pueden tener diferentes objetivos en sus políticas de potencia-calidad de servicio. Sin embargo, hay varias políticas base que los flujos de clase dorada deben obedecer mientras agregan o remueven redirectores con el propósito de asegurar la operación estable de la red inalámbrica (explicaremos estas políticas base más adelante).

Definiremos como una red estable a la situación en que un usuario/flujo/aplicación puede activar la adición de un redirector más a su enlace original solo si al hacerlo el rendimiento de cierto parámetro se mejora. Después de que un flujo de clase dorada termina de agregar o remover redirectores de su trayectoria, se cambia al modo operacional pasivo por un intervalo en que no se pueden agregar o remover redirectores aún si durante en ese intervalo el desempeño de calidad de servicio observado cambia. La motivación de tener periodos activos y pasivos en PCQoS es el de hacer improbable que dos flujos de clase dorada en la misma vecindad agreguen o remuevan redirectores de sus trayectorias al mismo tiempo. La razón por la que estos periodos son importantes, es que al tener dos flujos sensibles de clase dorada modificando su número de redirectores de tal forma que interfieran con los valores de rendimiento de calidad de servicio que están siendo monitoreados por cada usuario, conduciría a mediciones inestables. Los periodos activos y pasivos tienen diferentes duraciones de tiempo que a continuación se describen.

Los intervalos activos están compuestos de varios periodos de control y monitoreo. La figura 6.2 se enfoca en un intervalo activo donde un nodo destino monitorea el desempeño de algún parámetro (retardo de un paquete de fuente a destino, rendimiento, etc.) por algún tiempo antes de que una política específica que se esté usando active la adición o remoción de redirectores. La duración de los periodos de monitoreo deberá permitir la recepción de múltiples paquetes para calcular el valor promedio del parámetro que se está midiendo o controlando. La duración de periodos activos depende de la política específica que se está usando y se puede extender sobre varios intervalos de monitoreo o control. Definiremos la duración promedio de de un periodo activo como T_{act} y al número de flujos de clase dorada en la red como N_{gold}. Calculamos la duración de intervalos pasivos T_{pas} como una variable aleatoria uniformemente distribuida entre $\left[\frac{1}{2}N_{gold}T_{act}\ ,\ 2\left(N_{gold}T_{act}\right)\right]$. La constante $N_{gold}T_{act}$ es la suma de no traslape de los periodos activos para todos los flujos de clase dorada. El factor $\frac{1}{2}N_{gold}T_{act}$ limita el intervalo mínimo entre dos periodos activos, mientras que el factor $2\left(N_{gold}T_{act}\right)$ reduce la probabilidad de que dos o más flujos de clase dorada tengan periodos activos traslapados.

6.3.2 Fase de Control-Monitoreo.

En el diseño de PCQoS consideramos los siguientes parámetros: retardo de paquete (PD), rendimiento de paquetes (PT) y potencia de transmisión (TP). Sin embargo, otros parámetros también podrían ser monitoreados dependiendo de una política o aplicación en particular. En base al monitoreo de uno o más parametros en el receptor, el receptor decide si el desempeño observado de potencia/calidad de servicio es satisfactorio basado en la política específica que el usuario está utilizando, y puede realizar alguna acción (agregar o remover redirectores) para modificar el número de redirectores en su trayectoria durante el periodo activo.

6.3.3 Políticas de usuario.

Optimizar un parámetro para lograr un cierto nivel de desempeño (esto es, minimizar PD o maximizar PT) mediante la adición o remoción de redirectores, es difícil y no es siempre realizable debido al “efecto domino” discutido anteriormente. Además, las redes inalámbricas de múltiples saltos tienen una capacidad máxima para cargar tráfico y el límite superior de esta capacidad está compartido por todas las sesiones de los flujos activos en la red. Optimizar rendimiento y retardo, al igual que la potencia de transmisión simultáneamente, es extremadamente desafiante.

Agregar redirectores afecta a la capacidad total de la red para cargar tráfico, este comportamiento aplica para IEEE 802.11 como para los protocolos SR-CSMA. Sin embargo, agregar redirectores no necesariamente degrada el desempeño de calidad de servicio observado por “todos” los flujos en la red para el tipo de MACs SR-CSMA. Durante la discusión de PCMAP se mostró que una sesión que transmite sobre un enlace de rango grande tiene menos oportunidad de transmitir bajo el tipo de MACs SR-CSMA en comparación a las sesiones que transmiten sobre enlaces de rangos más cortos. Por consiguiente, bajo ciertas condiciones, dividir un enlace de rango grande en enlaces de rangos más cortos mediante la adición de redirectores, mejora el desempeño de calidad de servicio en comparación al mismo flujo sin ningún redirector en su trayectoria.

En PCQoS, los usuarios de clase dorada no tienen restricciones en sus objetivos de desempeño, lo que si restringe PCQoS son las políticas (mecanismos de reglas) que los usuarios de clase dorada pueden usar mientras intentan alcanzar su calidad de servicio individual y sus objetivos de ahorro de energía.

Estas políticas son necesarias para limitar la degradación inherente de calidad de servicio en la red que resulta de la adición de redirectores por los usuarios de clase dorada. En PCQoS se identifican dos puntos operacionales estables o políticas que son factibles para los usuarios de clase dorada:

- *Normal:* Este es el comportamiento por default de redes basadas en IEEE 802.11 o SR-CSMA sin redirectores (los paquetes son transmitidos directamente entre pares fuente-destino). Este caso corresponde a transmitir con la potencia de transmisión común en IEEE 802.11, o con la mínima potencia de transmisión entre pares fuente destino en las redes basadas en SR-CSMA. Sin embargo, no aplicar control de potencia significa que más rutas de rangos grandes para el caso de SR-CSMA sufrirán degradación de desempeño debido a la inequidad del protocolo.
- *Punto de saturación:* Bajo esta política los usuarios de clase dorada están permitidos para agregar o remover redirectores activamente. Se define al punto de saturación, como el punto donde la acción de agregar un redirector mas a una ruta no proporcionaría alguna mejora significativa en el desempeño de algún parámetro en particular siendo controlado.

Definición: Sea M_k el valor del parámetro que está siendo controlado después de agregar el redirector k a la ruta. El redirector $k+1$ será agregado a la ruta solo si

$$M_{k+1} > M_k(1+\delta) \qquad (1)$$

Donde δ es el margen predefinido que hace meritorio la adición de un redirector más. La idea de limitar el número de redirectores es para evitar los efectos negativos potenciales de agregar más redirectores, en términos de degradación de calidad de servicio adicional observado por otros flujos (de clase dorada y de mejor esfuerzo) en la red inalámbrica.

En PCQoS, cada uno de los flujos de clase dorada seleccionados es capaz de agregar o remover redirectores con el propósito de lograr su balance de desempeño Potencia/calidad de servicio de una manera ambiciosa (cada nodo puede tener diferentes objetivos de balance potencia/calidad de servicio). Se define el desempeño objetivo de un flujo como $Metrico^{\text{objetivo}}$, este objetivo puede ser específico de una aplicación, de una clase de servicio o el default para todos los flujos de clase dorada en la red. También definimos el desempeño monitoreado de soportar N redirectores en una trayectoria como $Metrico_N^{medido}$.

Durante los periodos de monitoreo-posicionamiento, un flujo de clase dorada agregará o removerá redirectores con el propósito de llevar el desempeño observado $Metrico_N^{medido}$ lo más cerca al desempeño objetivo $Metrico^{\text{objetivo}}$. En todos los casos los flujos de clase dorada pueden agregar redirectores siempre y cuando la política del punto de saturación métrica descrita anteriormente no haya sido alcanzada, que es un requerimiento necesario para mantener la operación saludable de la red.

El desempeño de los parámetros de calidad de servicio de las aplicaciones, tales como rendimiento y retardo podrían ser mejorados mediante la adición o remoción de redirectores, dependiendo de las condiciones operacionales específicas experimentadas en la red. Bajo ciertas condiciones el desempeño de rendimiento y retardo puede mejorar mediante al adición de redirectores debido al comportamiento desigual de los MAC controlados por potencia, como se discutió anteriormente (zona izquierda de la figura 6.1). Sin embargo, en otras condiciones de red, remover redirectores podría mejorar el desempeño de rendimiento y retardo ya que toma lugar un menor reenvío de paquetes (zona derecha de la figura 6.1). Como resultado, los flujos de clase dorada necesitan determinar experimentalmente si agregar (buscar-agregar) o remover (buscar-remover) redirectores produce o no un mejor desempeño como puede ser el caso. El siguiente algoritmo (Figura 6.3) controla la adición o remoción de redirectores durante un periodo activo, determinando el punto de balance de esta operación.

```
Buscar-Agregar
{
   #Actualmente N redirectores en la trayectoria
    if (Metrico_N^medido < Metrico^objetivo)
⊙       agregar redirector
        if (Metrico_N+1^medido > Metrico^objetivo)
              parar
        elseif (Metrico_N+1^medido > Metrico_N^medido (1+δ))
              N++
               ir a ⊙
        else  remover redirector
}
Buscar-remover
{
  #Actualmente N redirectores en la ruta
   if (Metrico_N^medido < Metrico^objetivo)
⊙     remover redirector
      if (Metrico_N-1^medido > Metrico^objetivo)
            parar
      elseif (Metrico_N-1^medido > Metrico_N^medido (1+δ))
            N--
             ir a ⊙
       else agregar redirector
}
```

Figura 6.3. Operación de PCQoS.

Es importante notar que aún si un flujo es capaz de alcanzar su nivel de desempeño objetivo durante un periodo activo, PCQoS no puede garantizar que el nivel de desempeño se mantenga durante los periodos operacionales pasivos. Esto es debido a que durante estos periodos, otros flujos de clase dorada pueden intentar optimizar sus propios parámetros de desempeño, por consiguiente afectar en alguna magnitud el desempeño de calidad de servicio observado por todos los otros flujos en la red, como es el caso del efecto domino.

6.4 ADICIÓN Y REMOCIÓN DE REDIRECTORES.

Hasta ahora hemos estado mencionando las palabras agregar y remover redirectores sin explicar cómo se llevan acabo estas dos operaciones en la red inalámbrica ad hoc. En PCQoS se utiliza el protocolo PARO [25] para realizar estas operaciones. PARO es un protocolo de enrutamiento que opera arriba de la capa de enlace pero debajo de la capa de red y es capaz de agregar redirectores incrementalmente para dividir enlaces de rangos largos en varios enlaces de rangos más cortos. Originalmente se desarrollo PARO como una manera para reducir el consumo total de potencia de transmisión en las redes inalámbricas ad hoc, sin embargo, el mismo protocolo puede ser utilizado en PCQoS para dividir rutas o enlaces de rangos largos con el propósito de mejorar los desempeños de rendimiento y retardo en un flujo en particular.

6.4.1 PARO: Protocolo de Optimización de Rutas por medio de Potencia.

La operación de PARO puede no ser intuitiva, debido a que en la primera iteración de PARO el nodo fuente se comunica con el nodo destino directamente sin involucrar ninguna retransmisión de paquetes por redirectores. Cualquier nodo capaz de alcanzar a “escuchar” a los nodos fuente y destino puede calcular si la retransmisión de un paquete puede reducir la potencia de transmisión en comparación con el intercambio directo entre los nodos fuente y destino. Cuando este es el caso, un nodo intermedio puede elegir convertirse en un redirector y enviar un mensaje de redirección-de-ruta a los nodos fuente y destino para informarles acerca de la existencia de una ruta más eficiente en potencia para la comunicación entre ellos.

Definición: Sea $SIR_{\min}$ la relación señal a interferencia mínima con la cual un paquete puede aún ser recibido apropiadamente. Si $R_{i,j}$ es la potencia medida de la señal recibida en el nodo i de un paquete transmitido por el nodo j con una potencia T_j, y I_i es la interferencia local medida por el nodo i, entonces la potencia de transmisión mínima para que el nodo j se comunique con el nodo i, $T_{j,i}^{\min}$, es tal que $\frac{R_{i,j}}{I_i} \geq SIR_{\min}$.

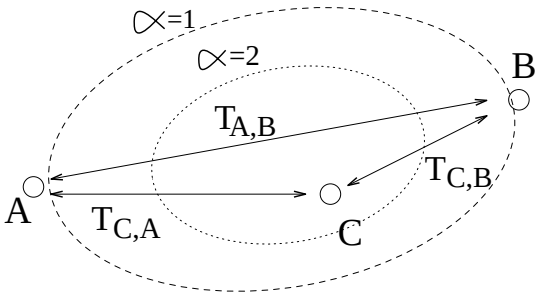

Figura 6.4 Operación de Redirección.

La figura 6.4 ilustra la operación de PARO. En este ejemplo, los nodos A, B, y C están localizados dentro del máximo rango de transmisión de cada uno, e inicialmente, el nodo A se comunica directamente con el nodo B. Debido a que el nodo C es capaz de "escuchar" paquetes de los nodos A y B, puede calcular si la nueva ruta $A \leftrightarrow C \leftrightarrow B$ tiene una potencia de transmisión más baja que la ruta original $A \leftrightarrow B$. De manera más precisa, el nodo C calcula que una optimización de ruta entre los nodos A y B es factible si:

$$T_{A,B}^{\min} > \alpha\left(T_{C,A}^{\min} + T_{C,B}^{\min}\right) \qquad (2)$$

Similarmente, definimos el porcentaje de optimización de agregar un redirector entre dos nodos en comunicación en una ruta, η, como:

$$\eta = \frac{T_{C,A}^{\min} + T_{C,B}^{\min}}{T_{A,B}^{\min}} \qquad (3)$$

El factor α en la ecuación 2 restringe el área entre dos nodos en comunicación donde se puede seleccionar un redirector potencial. En la figura 6.4, se muestra la región equivalente donde se puede localizar un redirector potencial para $\alpha = 1$ y $\alpha = 2$. El tamaño y la forma de estas regiones para encontrar redirectores potenciales, depende principalmente del parámetro de pérdidas de propagación.

En este punto hemos mostrado el caso donde un solo redirector intermedio se agrega a una ruta entre un par fuente-destino. El mismo procedimiento puede ser aplicado repetidamente para optimizar más una ruta en enlaces más pequeños como resultado de agregar más redirectores entre nodos fuente-destino.

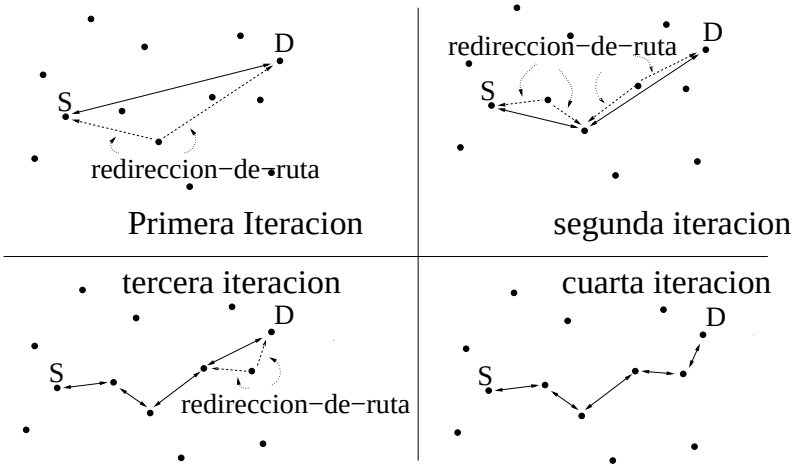

Figura 6.5 Convergencia de PARO.

La figura 6.5 ilustra un ejemplo de una ruta fuente-destino que comprende cinco segmentos con cuatro redirectores que requiere de cuatro iteraciones para la convergencia de la ruta. La figura muestra la ruta tomada por los paquetes de datos después de cada iteración y los nodos intermedios seleccionados como redirectores después de transmitir peticiones de redirección de ruta exitosamente. Esta figura (6.5) ilustra una ruta inicial con un solo salto, claramente el mismo procedimiento puede ser aplicado entre cualquier enlace, incluyendo el caso de una ruta compuesta de múltiples enlaces o saltos que es el caso de redes ad hoc de múltiples saltos.

El protocolo PARO optimiza las rutas un paso a la vez, por consiguiente, requiere de varias iteraciones para converger en una ruta “óptima”. La palabra iteración se refiere al evento en el cual un paquete de datos provoca que un nodo transmita una petición de redirección de ruta por primera vez. Como resultado, el tiempo de convergencia de PARO dependerá de la tasa de transmisión de datos (flujo medido en paquetes por segundo) transmitida por la fuente.

6.4.2 PCQoS y PARO.

Con el propósito de soportar posicionamiento de redirectores PCQoS, se realizó una modificación al protocolo original de PARO. Esta modificación requiere controlar la adición y remoción de redirectores con el fin de habilitar un tipo de control burdo sobre el desempeño de calidad de servicio y ahorros de energía basados en una cierta política de Potencia/Calidad de servicio.

El protocolo básico PARO agrega tantos redirectores en una ruta como sea posible por lo que es muy probable que para redes con densidades de nodos más grandes muchos más redirectores estén disponibles en las rutas en comparación con el ejemplo mostrado en la figura 6.5. Como resultado, para PCQoS sería necesario agregar un control sobre el número específico de redirectores introducidos en la ruta.

Debido a que más de un redirector puede ser agregado a una ruta durante una iteración, es insuficiente enviar un paquete de señalización pidiendo la adición de un redirector a la ruta actual. Esto produciría un comportamiento ambiguo porque no estaría claro cual redirector de entre todos los redirectores potenciales encontrados a lo largo de la ruta en una iteración ofrece el mejor desempeño en optimización de potencia e interferencia. En el caso de la iteración 2 (figura 6.5), el redirector que esta del lado derecho es el que debería ser seleccionado porque logra una η más alta en comparación al redirector que esta del lado izquierdo. Debido a este comportamiento ambiguo potencial, se modificó el protocolo original PARO de tal manera que todos los redirectores potenciales encontrados en una iteración primero son evaluados ya sea en la fuente o en el destino antes de tomar la decisión de cual redirector específico seleccionar.

La operación de PCQoS es diferente al protocolo PARO en las acciones tomadas después de la recepción de una petición de redirección de ruta de redirectores potenciales. La recepción de una petición de redirección de ruta por un potencial redirector en PCQoS, no provoca la inmediata redirección del flujo de paquetes, como ocurre en el protocolo PARO original, en cambio, PCQoS crea entradas de datos en una tabla de redirección de ruta y marca los estados de estas entradas como *durmientes* (inactivos). Las entradas de estado durmiente en las tablas de redirección de ruta permanecen inactivas hasta que un mensaje de señalización explícitamente cambia el estado a activo. Cuando las entradas se ponen en activo, se comportan exactamente como entradas de redirección de ruta como en el protocolo PARO original, lo que representa una mejora al protocolo.

Una vez que la fuente o el destino seleccionan un redirector específico basado en alguna política de decisión (que podría ser específico a un flujo/nodo/aplicación), se puede enviar un paquete a lo largo de la trayectoria para activar dinámicamente un redirector seleccionado. El mismo procedimiento se aplica cuando se remueve un redirector de una ruta, excepto que ahora el último redirector agregado es el primero que se remueve.

6.5 EVALUACIÓN DE PCQoS.

Para analizar la operación de PCQoS se utilizó ns2 (un simulador de redes comúnmente usado) y se utilizó el protocolo PCMAP como ejemplo de MAC de reuso espacial, como se define en [6]. Para el análisis de PCQoS se extendió la implementación previa del protocolo PARO original para implementar PCMAP y los componentes de posicionamiento y monitoreo de PCQoS. Los parámetros de simulación se muestran en la tabla 6.1.

Parámetro	Valor
Área	500x500
no. de nodos	400
no. de conexiones	100
pkts/seg	1,4,16,64
Tipo de tráfico	CBR/UDP
Tamaño de paquete	512 Bytes
Conexiones por rango	3,14,19,28,36
Tiempo de simulación	300 seg.
Ptmin	0.1778e-3 W
Ptmax	0.707945 W
SIR_Thresh	6 dB
SIR_deseada	10 dB
CS_Thresh	1.5849e-11
Rx_Thresh	3.981e-10
Rx_deseada	4.06062e-10

Tabla 6.1 Parámetros de Simulación.

La comunicación entre dos nodos en PCMAP utiliza un intercambio de paquetes de señalización RPTS-APTS antes de que se lleve a cabo la transmisión de datos. En este trabajo se reutiliza el mismo módulo para calcular la potencia de transmisión mínima utilizada en el protocolo PARO original y la potencia de transmisión mínima en PCMAP (para ver cómo el protocolo PARO calcula la potencia de transmisión mínima entre dos nodos ver [25]). En la implementación de PCMAP, si embargo, se agregó una copia local del ruido en el

encabezado de cada paquete transmitido, como se define en las especificaciones de PCMAP [6], esta adición es necesaria para PCMAP porque los niveles de ruido (o interferencia) no son despreciables como es el caso en la evaluación de PARO. Las operaciones de PCMAP que incluyen los principios de conservación y cooperación se implementaron de acuerdo a [6].

El modelo de propagación en ns-2 está basado en el modelo de espacio libre para rangos cortos y el modelo de dos rayos para rangos más largos, este modelo es apropiado para ambientes fuera de edificios donde existe una señal fuerte de línea de vista entre los nodos transmisor y el receptor, y donde las antenas son omnidireccionales. El modelo de espacio libre calcula la potencia recibida como:

$$R_{j,i} = \frac{T_{i,j} G_t G_r \lambda^2}{(4\pi d)^2 L} \tag{4}$$

Donde $R_{j,i}$, es la potencia recibida en el nodo j cuando el nodo i transmite con potencia $T_{i,j}$, d es la distancia que separa al transmisor del receptor, λ es la longitud de onda de la señal, L es un factor de ajuste y G_t, G_r son las ganancias de las antenas de los nodos transmisores y receptores respectivamente. El modelo de propagación de dos rayos considera que hay dos componentes importantes de la señal. Este modelo calcula la intensidad de la señal recibida en el nodo destino como:

$$R_{j,i} = \frac{T_{i,j} G_t G_r h_t^2 h_r^2}{d^4} \tag{5}$$

Donde h_t^2 y h_r^2 son las alturas de las antenas de los nodos transmisor y receptor respectivamente. La distancia de corte d_c donde el cálculo cambia del modelo de espacio libre al modelo de dos rayos está dado por:

$$d_c = \frac{4\pi h_t h_r}{\lambda} \tag{6}$$

En lo que sigue se presenta la evaluación de PCQoS. En la evaluación, se experimenta con diferentes aspectos operacionales de PCQoS y se muestra como los flujos/nodos/aplicaciones de clase dorada pueden agregar o remover redirectores para modificar dinámicamente su calidad de servicio observada y su desempeño en potencia. Cada punto en las gráficas presentadas son de un promedio de 10 experimentos, cada uno de ellos utiliza una semilla diferente para cada experimento.

En la evaluación de PCQoS no se consideró movilidad porque agrega otra magnitud y complejidad al problema. Las mismas ideas y soluciones presentadas en el protocolo PARO original para soportar nodos móviles tales como mantener una tasa mínima de paquetes que fluye entre pares fuente-destino e incrementar la potencia de transmisión mínima para cada transmisión son aplicables para los protocolos de acceso IEEE 802.11 y PCMAP.

6.5.1 Desempeño de PCQoS.

A continuación, se evalúan varios aspectos del desempeño y comportamiento del protocolo propuesto PCQoS.

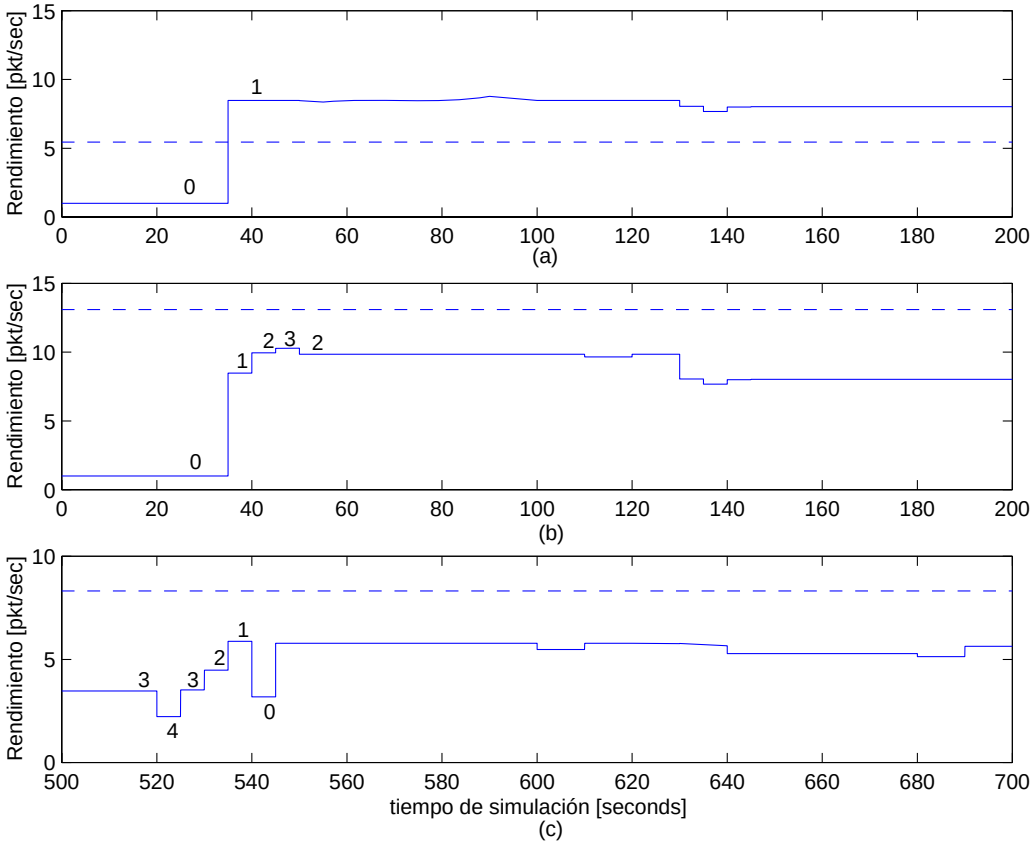

Figura 6.6 Desempeño de rendimiento de un flujo que opera PCQoS.

Comportamiento Individual de PCQoS: Las figuras 6.6 (a)(b)(c) muestran los trazados del desempeño de rendimiento de un flujo de clase dorada de prueba en el rango de 200-250 metros bajo PCQoS. La línea discontinua en la figura 6.6 (a)-(c) denota el desempeño objetivo (en este caso rendimiento). Los intervalos de monitoreo están puestos a 5 segundos y la duración de los periodos pasivos está uniformemente distribuido entre 150-800 segundos.

Las tres gráficas que se muestran en la figura 6.6 contrastan la operación de PCQoS del flujo de prueba en diferentes condiciones de red: En la figura 6.6(a) solo 10% de los flujos son de clase dorada, en la figura 6.6 (b) es igual que (a) pero con un desempeño objetivo mas alto (línea discontinua), y la figura 6.6(c) el 30% son flujos de clase dorada.

La figura 6.6 (a) muestra el comportamiento de PCQoS cuando el desempeño objetivo es más alto que el desempeño inicial. En este caso, el flujo de prueba utiliza el algoritmo de buscar-agregar (detallado en la sección 6.3.2) previendo que hay pocos flujos de rangos cortos en la vecindad, para poder mejorar su rendimiento tomando ventaja del comportamiento desigual del MAC. Agregar 1 redirector después de 30 segundos hace que se incremente el desempeño inicial por arriba del desempeño objetivo antes de que el flujo se mueva a su periodo pasivo. La prohibición a los flujos de clase dorada de agregar más redirectores después de que han alcanzado sus objetivos de desempeño, es una propiedad importante de PCQoS. Agregar mas redirectores en esta situación solo degradará el desempeño de otros flujos en la vecindad del flujo de prueba. Además del número de redirectores que se usan en la ruta, también se muestran los periodos activos y pasivos encima de la línea de trazado.

La figura 6.6 (b) muestra el comportamiento de PCQoS cuando el desempeño objetivo esta arriba del desempeño inicial sin redirectores. El flujo de prueba utiliza el algoritmo buscar-agregar previendo que hay pocos flujos de rangos cortos en la vecindad. En este ejemplo el flujo de prueba agrega primero 1 redirector, luego 2 y por último 3 redirectores a su ruta. Debido a que la mejora en el desempeño después de agregar el tercer redirector esta debajo del punto de saturación ($\delta = 10\%$ en este ejemplo), el tercer redirector es removido y solo se seleccionan dos redirectores para este periodo activo.

Hasta este punto hemos mencionado que una regla común de PCQoS es que los flujos de clase dorada no agregan redirectores si el punto de saturación se ha alcanzado para evitar interferencia innecesaria hacia otros nodos en la red inalámbrica. Se debe notar que durante el intervalo pasivo el rendimiento monitoreado cambia como resultado del efecto domino creado por otros flujos de clase dorada que agregan redirectores a sus trayectorias.

La figura 6.6 (c) muestra el comportamiento de PCQoS cuando ya hay 3 redirectores en un flujo de prueba después de 500 segundos de trazado y el desempeño está por debajo del desempeño objetivo en el inicio de un periodo activo.

El flujo de prueba utiliza otra vez el algoritmo de buscar-agregar para agregar el cuarto redirector a la trayectoria. Dado que el desempeño deseado no se logra, el flujo de prueba utiliza el algoritmo buscar-remover para dejar en la trayectoria solo un redirector que en este caso proporciona el desempeño mas alto posible en el periodo activo para el flujo de prueba.

6.5.2 Desempeño Conjunto de PCQoS.

En los experimentos previos hemos mostrado el desempeño de PCQoS para flujos individuales. Ahora analizamos el impacto conjunto en la calidad de servicio cuando un subconjunto de flujos en la red tiene permitido agregar redirectores.

Se evalúa una red de 400 nodos en un área de 500 x 500 metros con 100 flujos cada uno enviando 16 pkts/seg de 512 bytes de tamaño, los nodos fuente escogen a su destino de manera aleatoria dentro de su rango de 250 metros. Para estos experimentos seleccionamos los 5 escenarios que se muestran en la tabla 6.2. El término $N < x >$ en la tabla 6.2 significa que N flujos de clase dorada en este rango agregaron x redirectores a sus trayectorias. Se seleccionaron estos 5 escenarios ya que se consideró que muestran de una mejor manera las ventajas y desventajas de PCQoS. El escenario 1 corresponde a una red SR-CSMA sin PCQoS (esto es, no se agregaron redirectores a ninguna ruta/trayectoria). El escenario 2 corresponde al caso donde PCQoS se aplica aleatoriamente a 10 de 36 flujos en el rango de 200-250 metros, y solo hay un redirector entre los puntos finales. El escenario 3 es igual que el escenario 2 solo que ahora se posicionaron 3 redirectores entre los puntos finales. En el escenario 4, una tercera parte de los flujos en los rangos de 100-150, 150-200, 200-250 metros agregaron solo un redirector a sus trayectorias. Finalmente en el escenario 5 todos los flujos en la red agregaron tantos redirectores a sus trayectorias como fueron necesarios de tal forma que todos los enlaces resultantes estuvieron en el rango de 0-50 metros.

	0-50 3 flujos	**50-100** 14 flujos	**100-150** 19 flujos	**150-200** 28 flujos	**200-250** 36 flujos
S1	0	0	0	0	0
S2	0	0	0	0	10 <1>
S3	0	0	0	0	10 <3>
S4	0	0	6 <1>	9 <1>	12 <1>
S5	0	14 <2>	19 <3>	28 <5>	36 <7>

Tabla 6.2. Escenarios de Simulación para el Análisis de Desempeño Agregado.

La figura 6.7 muestra la fracción de los paquetes totales recibidos por los destinos en cada escenario sobre los cinco rangos de distancias (0-50, 50-100, 100-150, 150-200, 200-250 metros respectivamente) de sus fuentes. El hecho de que se tengan 3,14, 19, 28 y 36 flujos para los rangos de 0-50, 50-100, 100-150, 150-200, 200-250 metros respectivamente en la tabla 6.2, es un resultado directo de permitir a cada fuente escoger un destino de manera aleatoria dentro de su rango de 250 metros.

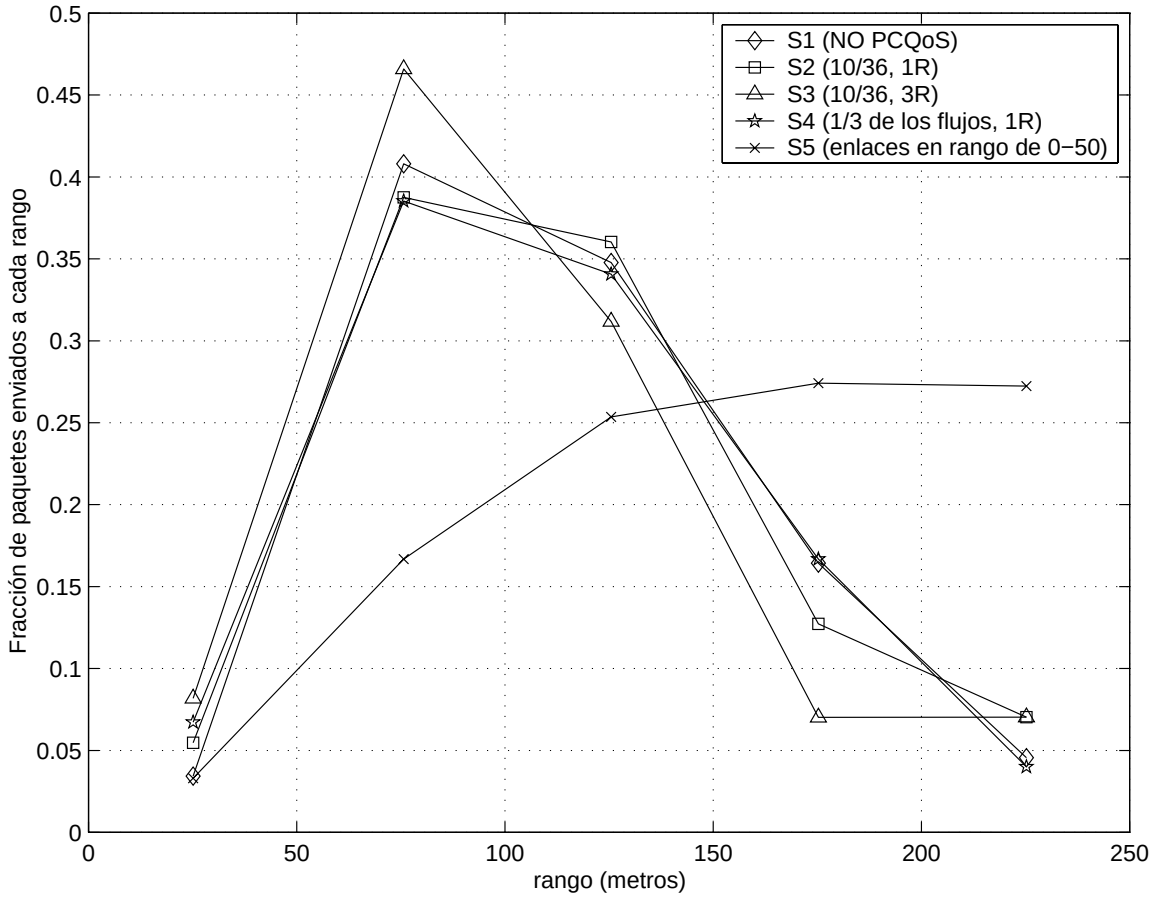

Figura 6.7 Desempeño de Rendimiento de flujos que han implementado QoS-PARO.

Primero observamos el escenario 2 donde 10 de 36 flujos en el rango de 200-250 metros agregaron solo 1 redirector a sus trayectorias y se compara su desempeño con el escenario 1 (sin PCQoS). Como se puede ver en la figura 6.7 la fracción de los paquetes totales recibidos por los destinos en el rango de 200-250 metros mejora significativamente comparado con el escenario 1. Este es un resultado directo del incremento en el rendimiento obtenido por los 10 flujos de clase dorada en este rango que han implementado PCQoS con un redirector en su trayectoria.

El efecto negativo es que ahora tenemos menos paquetes recibidos para los flujos en el rango de 150-200 metros en comparación con el escenario 1. Los flujos en el rango de 150-200 metros obtuvieron un rendimiento mas bajo en el escenario 2 debido a que ahora hay 20 “enlaces” más (debido a que los 10 flujos en el rango de 200-250 metros se dividieron en dos enlaces cada uno en el rango de 100-150 metros) que incrementa el comportamiento desigual hacia los flujos en el rango de 150-200 metros. Este es un claro ejemplo del efecto domino, donde una decisión ambiciosa local impacta el desempeño de otros flujos en la red. La figura 6.8 muestra el rendimiento actual obtenido por los 36 flujos en el rango de 200-250 metros para el escenario 2. Los primeros 10 flujos en la figura 6.8 corresponden a los flujos de clase dorada seleccionados en el escenario 2. Los resultados que se muestran en la figura 6.8 muestran claramente el incremento en el rendimiento obtenido por los flujos de clase dorada seleccionados en comparación con el resto de los flujos que no agregaron redirectores a sus trayectorias.

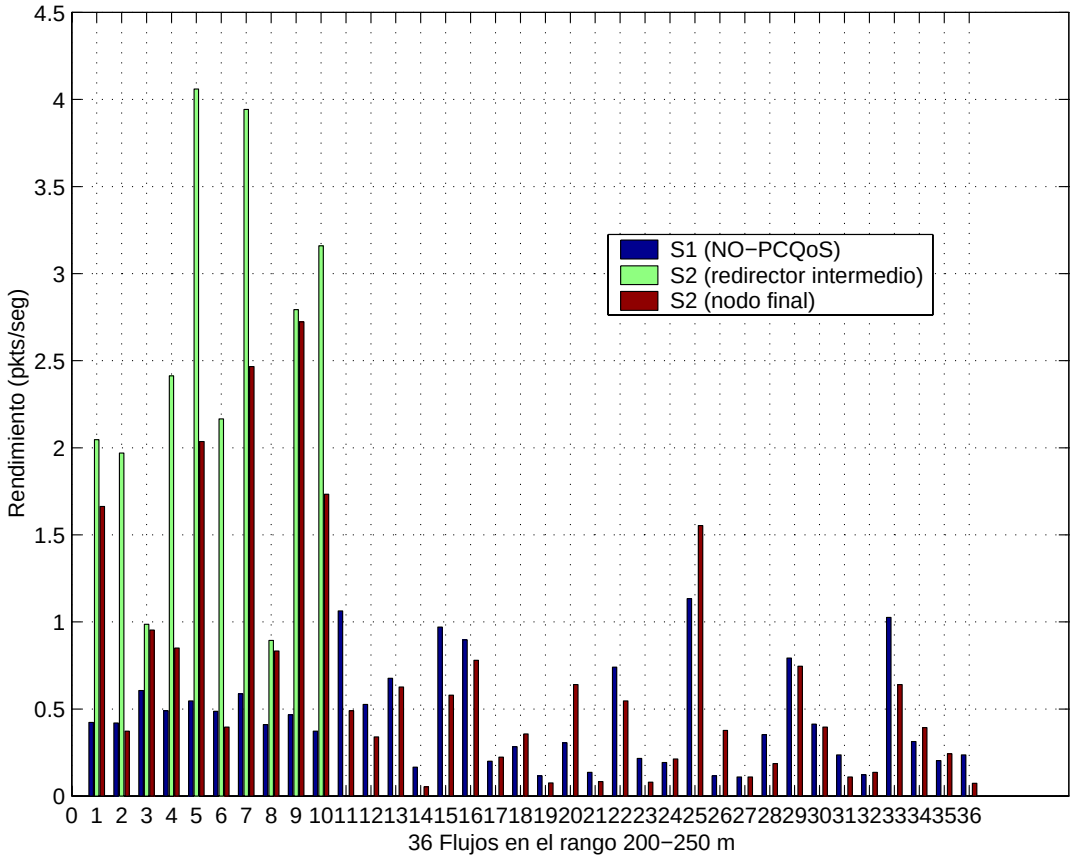

Figura 6.8 Desempeño de rendimiento de 10 flujos en el rango de 200-250 metros que agregaron 1 redirector a su trayectoria.

El escenario 3 es similar al escenario 2 solo que ahora los 10 flujos seleccionados agregaron 3 redirectores a su trayectoria en vez de un redirector como fue el caso del escenario 2. La figura 6.9 muestra el rendimiento promedio recibido por cada uno de los 10 flujos seleccionados en el escenario 3.

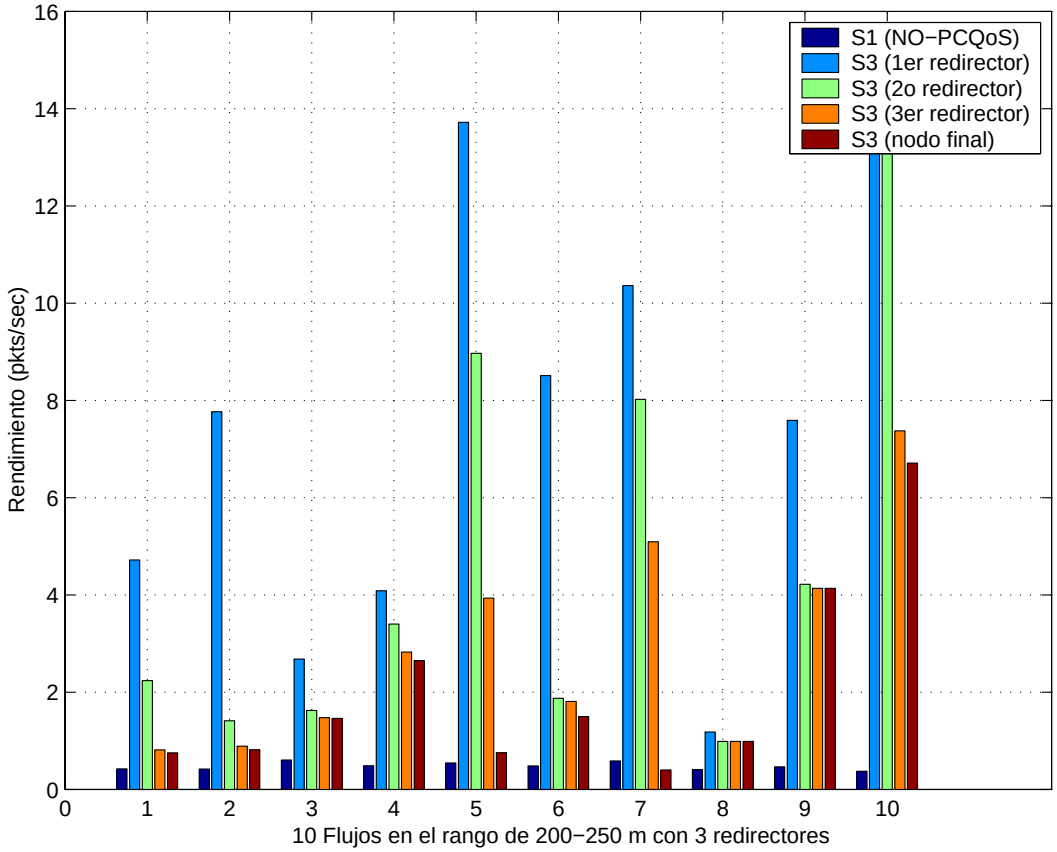

Figura 6.9 Desempeño de rendimiento de 10 flujos en el rango de 200-250 metros que agregaron 3 redirectores a su trayectoria.

Para efectos de comparación también se muestra el rendimiento obtenido en el escenario 1 cuando no se agregaron redirectores. Como podemos ver en esta figura 6.9, en la mayoría de los casos la adición de 3 redirectores se traduce en un rendimiento más alto para estos flujos en comparación con el escenario 1 (El flujo 7 es la excepción). Este es el resultado del incremento en el rendimiento obtenido por los 10 flujos de clase dorada en este rango que han implementado PCQoS con 3 redirectores en sus trayectorias. En lo que respecta a la figura 6.7, la fracción de paquetes totales recibidos por los destinos en el rango de 150 a 200 metros es más bajo en el escenario 3 en comparación con el escenario 2. Esto es por la presencia de múltiples enlaces de rangos más cortos creados por la adición de 3 redirectores a los 10 flujos seleccionados en el escenario 3.

En el escenario 4 un tercera parte de los flujos en los rangos de 100-150, 150-200, 200-250 metros agregaron un solo redirector a sus trayectorias. En la figura 6.10 (los primeros 6 flujos corresponden al rango de 100-150, del 7 al 15 al rango de 150-200 m y los últimos 12 al rango de 200-250 m) se observa que los flujos seleccionados en los rangos de 100-150 y 150 a 200 metros obtuvieron un rendimiento mucho más alto en comparación con los flujos seleccionados en el rango de 200-250 metros. Los flujos de clase dorada en el rango de 200-250 metros se beneficiaron poco al agregar un redirector en este escenario porque hay un número más alto de enlaces de rangos más cortos introducidos por los flujos seleccionados en los rangos de 100-150 y 150-200 metros quienes agregaron mayor inequidad hacia los flujos de rangos mas largos.

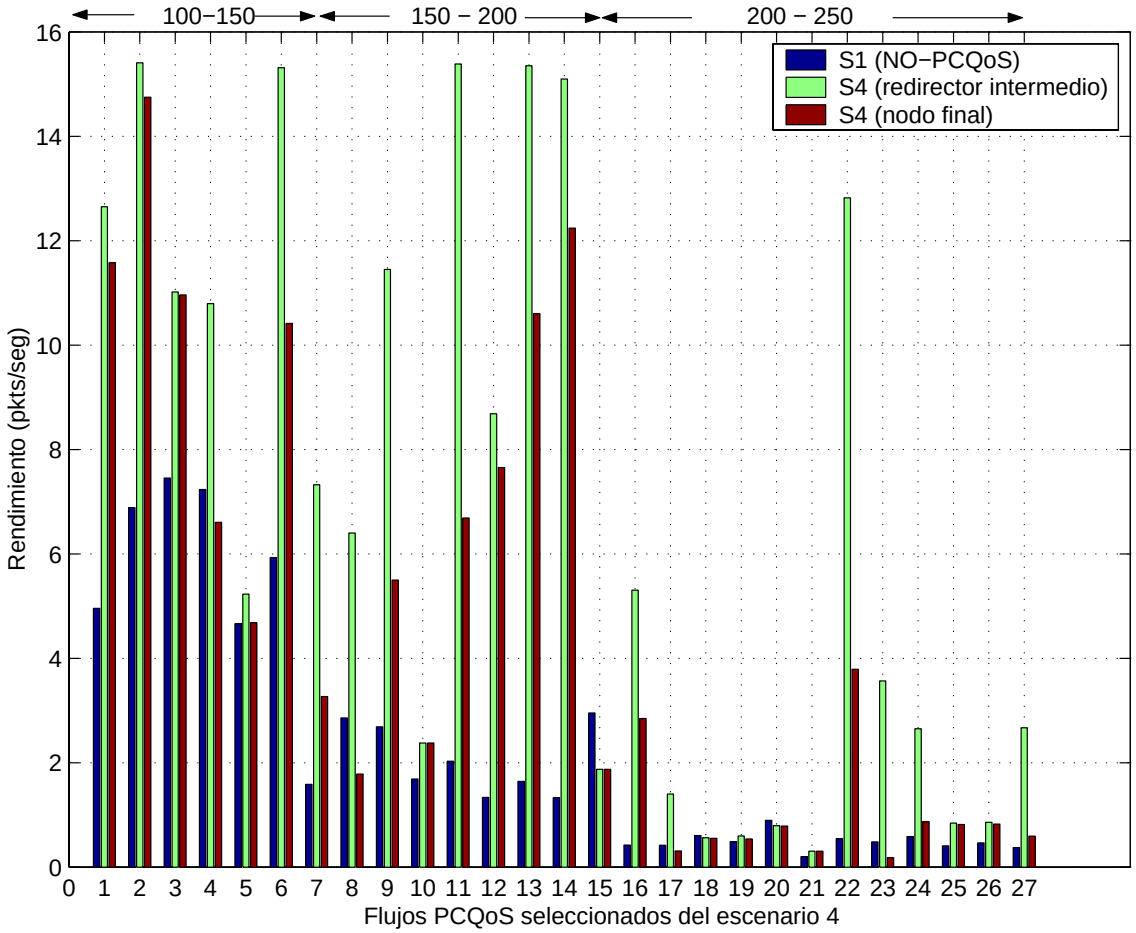

Figura 6.10 Desempeño de rendimiento de 1/3 de los flujos en los rangos de 100-150, 150-200 y 200-250 metros que agregaron un redirector a sus trayectorias.

Finalmente, en el escenario 5, los 100 flujos en la red agregaron tantos redirectores a sus trayectorias como fueron necesarios de tal forma que todos los enlaces resultantes están en el rango de 0-50 metros. Este escenario tiene cierta similitud a una red IEEE 802.11 con un rango de transmisión común de 50 metros. En este caso el rendimiento obtenido por los flujos en el rango de 200-250 metros es aún mejor que en el escenario 1, sin embargo, como veremos más adelante el rendimiento total de la red se degrada rápidamente en este escenario.

La figura 6.11 (a) muestra el rendimiento promedio conjunto entregado de los 100 flujos, medidos en los puntos finales de cada flujo para los 5 escenarios.

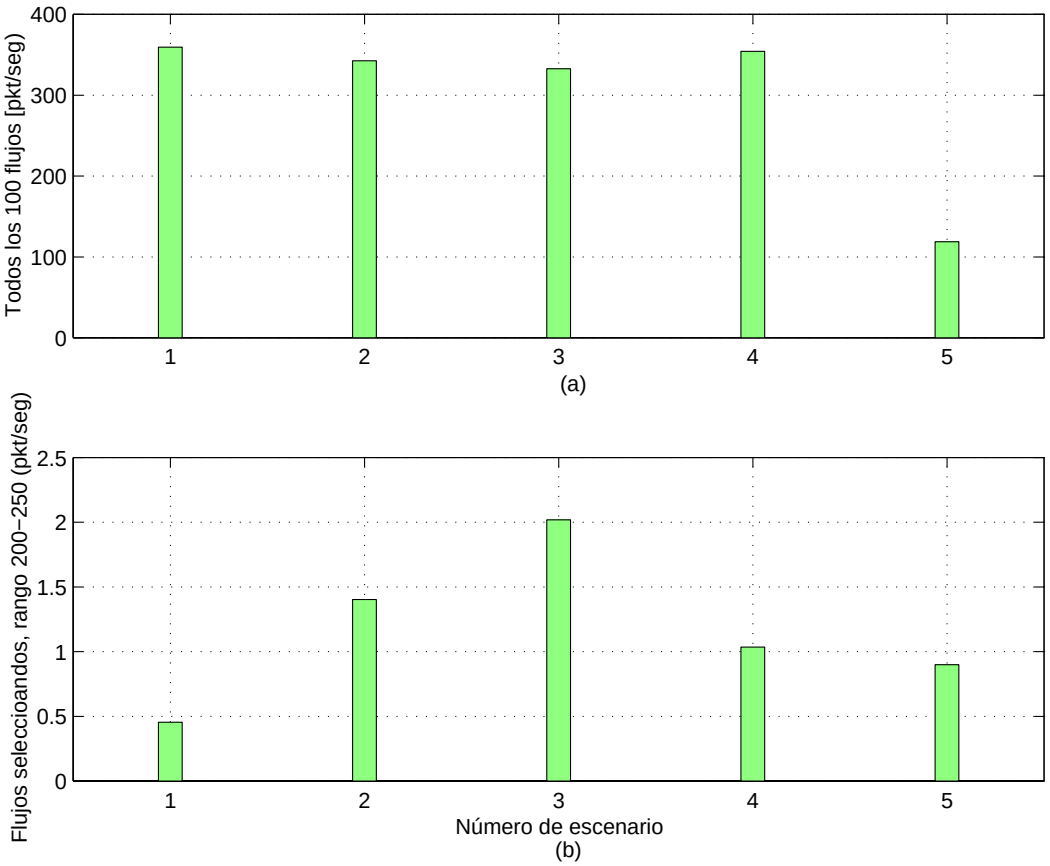

Figura 6.11 (a) y (b). Desempeño de rendimiento conjunto de PCQoS.

Los resultados más importantes de la figura 6.11 (a) son: Primero, el rendimiento máximo se obtiene en el escenario 1 (SR-MAC sin PCQoS). Esto no es sorpresivo ya que se mencionó que cualquier intento de dividir enlaces por medio de control de potencia solo degradaría el desempeño global de la red.

Segundo, el peor rendimiento se obtuvo en el escenario 5 cuando los 100 flujos agregaron tantos redirectores como fueron necesarios, de tal forma que los enlaces resultantes cayeron en el rango de 0-50 metros lo que incremento el efecto domino en la red.

La figura 6.11 (b) muestra el rendimiento promedio recibido para los flujos de clase dorada seleccionados en el rango de 200-250 metros para los escenarios 1 a 5. Como referencia, los 36 flujos en el escenario 1 obtuvieron un rendimiento promedio de 0.45 pkt/seg por flujo. En los escenarios 2 y 3 el uso de PCQoS en los flujos seleccionados incrementó el rendimiento en 309% y 445% respectivamente. El rendimiento más alto observado en el escenario 3 es el resultado de romper enlaces de rangos largos en 4 enlaces de rangos más cortos, disminuyendo el comportamiento desigual de SR-MACs. En los escenarios 4 y 5 las ganancias en rendimiento son menos impresionantes comparados con los escenarios 2 y 3, pero más altos que el escenario 1 para estos flujos. El hecho de que PCQoS logre un rendimiento más alto aún en el escenario 5 para los flujos en el rango de 200-250 metros muestra las ventajas de PCQoS como un método para incrementar el desempeño para flujos de rangos largos cuando se utilizan SR-MACs en redes inalámbricas ad hoc, aunque el desempeño conjunto total de los flujos en este escenario es bastante pobre como vimos en la figura 6.11 (a).

Las figuras 6.8 a 6.10 también muestran el rendimiento promedio recibido después de cada redirector de los flujos de clase dorada seleccionados. La tendencia común en estas figuras es que el rendimiento promedio recibido después del redirector i en la trayectoria de fuente a destino, es más alto que en el redirector $i+1$. Este es un patrón que ya ha sido reportado en la literatura [27] y es creado por fuentes de tráfico que no tienen control de la tasa de transmisión (por ej. CBR/UDP). Los tipos de fuentes semejantes a CBR intentan inyectar en la red una tasa constante de paquetes sin el conocimiento de la capacidad de ancho de banda actual de la ruta entre fuente y destino. Aún si la fuente es capaz de transmitir una cierta tasa de paquetes al primer redirector, los otros redirectores en la ruta podrían tener dificultades (congestión de tráfico) para mantener la misma tasa de paquetes hacia el destino.

CONCLUSIONES.

Los protocolos de control de acceso al medio definen reglas para acceder ordenadamente al medio compartido y juegan un papel crucial en la distribución eficiente y justa de escaso ancho de banda inalámbrico.

Una de las principales desventajas del estándar IEEE 802.11 es que utiliza un rango de transmisión común para todos los paquetes de control y datos, esto trae consigo un pobre reuso espectral (número de transmisiones simultáneas que pueden tomar lugar en la red al mismo tiempo) ya que un nodo que transmite a otro en su cercanía debe transmitir con una potencia fija (normalmente una potencia mas alta que la potencia mínima necesaria para alcanzar a su destino) para la correcta operación de la capa MAC.

Mientras que el estándar IEEE 802.11 exhibe un pobre reuso espectral en las redes inalámbricas ad hoc, se han desarrollado varias propuestas en torno a este estándar que están diseñadas para un mayor reuso espectral y por consiguiente, mejorar el rendimiento de la red. En esta tesis se diseño, implemento y evaluó un protocolo de acceso múltiple controlado por potencia con el fin de entender el comportamiento de los MAC de reuso espectral y de analizar las ventajas y desventajas con respecto al MAC IEEE 802.11. Los resultados presentados en el capítulo 5 muestran que el protocolo implementado permite una mayor cantidad de comunicaciones simultáneas (esto es, se obtiene mayor capacidad) en comparación al estándar IEEE 802.11 mediante la reducción de los rangos de transmisión a los mínimos necesarios que garanticen la recepción exitosa del destino deseado (mejorando la utilización del canal). Se observó que el beneficio de este protocolo sobre IEEE 802.11 se incrementa conforme el tráfico se vuelve más localizado, es decir, cuando los nodos se comunican con otros nodos solo en su vecindad, ya que argumentamos que las distribuciones de los nodos en un ambiente típico (en la mayoría de las situaciones) se espera que sea más agrupado, como el escenario simulado en la sección 5.2. En la figura 5.2 se mostró que conforme la red se encuentra más agrupada, se incrementa el rendimiento (throughput) ya que es posible una mayor cantidad de transmisiones simultáneas y menos nodos compiten dentro de cada grupo (cluster). Sin embargo, una propiedad negativa de este tipo de protocolos es que favorecen a las transmisiones de rangos cortos sobre los de rangos largos bajo cargas altas de tráfico (como se mostró en las gráficas de las figuras 5.3-5.5), que es el resultado de aplicar la regla número 2 de los protocolos basados en SR-CSMA que

dicta que ninguna fuente que inicie una nueva transmisión puede interrumpir transmisiones en curso mediante una comunicación demasiado “ruidosa”. Por lo tanto, las transmisiones de rangos largos tienen poca probabilidad de conseguir una oportunidad de transmitir en presencia de comunicaciones de rangos cortos en su vecindad. Estos resultados contrastan con el de la figura 5.6 en donde se observa que la igualdad de acceso en el estándar IEEE 802.11 es más justa en comparación a los MAC basados en SR-CSMA.

En esta tesis se estudió el impacto de agregar o remover redirectores en una red basada en PARO sobre los parámetros tradicionales tales como rendimiento y retardo punto a punto. Primero se estudio este impacto en las redes ad hoc inalámbricas basadas en MAC´s IEEE 802.11 y con control de potencia y se mostró las limitaciones de estos protocolos MAC para operaciones inalámbricas de un solo salto y de múltiples saltos. Se discutió el desempeño desigual de pares fuente destino de acuerdo a su ubicación en las redes inalámbricas basadas en SR-CSMA. Se mostró como este comportamiento desigual se puede utilizar como la base para tener calidad de servicio (QoS) diferenciado en las redes inalámbricas ad hoc. Se propuso PCQoS para construir mecanismos de calidad de servicio dentro del sistema base PARO para aplicaciones específicas que desean mejorar su desempeño de QoS. En PCQoS, los flujos seleccionados agregan o remueven redirectores de sus trayectorias con el propósito de modificar su desempeño observado de QoS y ahorro de energía. También se mostró que modificar el desempeño de QoS y ahorro de energía de los flujos seleccionados es a expensas de una potencial degradación de QoS observado por flujos no seleccionados (esto es, flujos/aplicaciones que no utilizan redirectores en sus trayectorias). PCQoS representa el primer protocolo de enrutamiento controlado por QoS/Potencia y está basado en control de transmisión de rango variable.

Los protocolos basados en SR-CSMA así como la aplicación desarrollada de PCQoS son protocolos cuyo diseño aún está en progreso, por lo que el trabajo futuro será enfocado a la aplicación de los protocolos SR-CSMA a las redes de sensores inalámbricos y a las redes MESH, así como a una aproximación parcial en hardware sobre el estándar IEEE 802.11. Con lo que respecta a PCQoS el trabajo futuro será enfocado a proporcionar calidad de servicio diferenciado a las redes tipo MESH.

Los resultados obtenidos de este trabajo de tesis sirvieron para escribir un artículo que se publicará en un Journal aún por definir, en el área de redes inalámbricas ad hoc y cuyo nombre es: “Power Controlled Quality of Service in Wireless Ad Hoc Networks”.

GLOSARIO.

ACK	Acknowledge - Confirmación
AP	Access Point – Punto de Acceso
API	Application Program Interface – Interfase de Programas de Aplicación
APTS	Acceptable Power to Send – Potencia para Enviar Aceptable
ARP	Address Resolution Protocol – Protocolo de Resolución de Direcciones
BSA	Basic Service Area – Area de Servicio Básico
BSS	Basic Service Set – Conjunto de Servicios Básicos
CBR	Constant Bit Rate – Tasa de Bits Constante
CCK	Complementary Code Keying
CFP	Contention Free Period – Periodo Libre de Contención
CP	Contention Period – Periodo de Contención
CRC	Ciclic Redundacy Check
CSMA/CA	Carrier Sense Múltiple Access with Collision Avoidance – Acceso Múltiple por Detección de Portadora con Resolución de Colisiones
CSMA/CD	Carrier Sense Multiple Access with Collision Detection – Acceso Múltiple por Detección de Portadora con Detección de Colisiones
CTS	Clear To Send – Libre para Enviar
CW	Congestion Window – Ventana de Congestión
DBPSK	Differential Binary Phase Shift Keying
DCF	Distributed Coordination Function – Función de Coordinación Distribuida
DIFS	Distributed Coordination Function Inter Frame Spacing – Espaciamiento entre Paquetes del Coordinador Distribuido
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution System – Sistema de Distribución
DSSS	Direct Sequence Spread Spectrum – Espectro Disperso de Secuencia Directa
DTBS	Distributed Time Bounded Service - Servicios Distribuidos Limitados en Tiempo.
EIRP	Effective isotropic radiated power - Potencia Radiada Efectiva Isotrópica
ESS	Extended Service Set – Conjunto de Servicios Extendido
ESSID	Extended service Set ID – Identificador del Conjunto de Servicio Extendido
FCC	Federal Communications Commission – Comisión de Comunicaciones Federales
FDD	Frequency Division Duplex – Duplexaje por División de Frecuencia
FDDI	Fiber Distributed Data Interface – Interface de Datos Distribuido por Fibra
FHSS	Frequency Hopping Spread Spectrum – Espectro disperse de Salto de frecuencias
FSK	Frequency Shift Keying
FTP	File Transfer Protocol – Protocolo de Transferencia de Archivos
GFSK	Gaussian Frequency Shift Keying
HR-DSSS	High Rate DSSS – DSSS de tasa alta
IBSS	Independent Basic service Set – Conjunto de Servicios Básicos Independiente
IEEE	Institute of Electrical and Electronic Engineers – Instituto de Ingenieros Eléctricos y Electrónicos

IFQ	Interface Queue – Cola de espera
IP	Internet Protocol – Protocolo de Internet
IR	Infra Red - Infrarrojo
ISI	Inter Symbol Interference – Interferencia Intersímbolo
ISM	Industrial Scientific Medical – Médico Científico Industrial
ISP	Internet Service Provider – Proveedor de Servicios de Internet
LLC	Logical Link Layer – Capa de Enlace Lógico
MAC	Medium Access Protocol – Protocolo de Acceso al medio
MPDU	Message Protocol Data Unit – Unidad de Datos del Protocolo de Mensaje
MSDU	MAC Service Data Unit – Unidad de Datos de Servicio MAC
NAM	Network Animator – Animador de redes
NAV	Network Allocation Vector – Vector de asignación de Red
OFDM	Orthogonal Frequency Division Multiplexing – Multiplexaje por División de Frecuencias Ortogonales.
OSI	Open Systems Inteconnection – Interconexión de Sistemas Abiertos
PBCC	Packet Binary Convolutional Coding
PC	Point Coordinator – Coordinador Puntual
PCF	Point Coordination Function – Función de Coordinación Puntual
PCMA	Power Controlled Multiple Access – Acceso Múltiple Controlado por Potencia
PCQoS	Power Controlled Quality of Service – Calidad de Servicio Controlado por Potencia
PDU	Packet Data Unit – Unidad de Paquete de Datos
PIFS	Point Coordination Function Inter Frame Spacing - Espaciamiento entre Paquetes del coordinador puntual.
PPM	Pulse Position Modulation – Modulación por Posición de Pulsos
PSK	Phase Shift Keying
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service – Calidad de Servicio
RPTS	Request Power to Send – Petición de Potencia para Enviar
RTS	Request To Send – Petición para Enviar
SIFS	Short Inter Frame Spacing - Espaciamiento entre Paquetes Corto
SIR	Signal to Interference Ratio – Relación Señal a Interferencia
SR-CSMA	Space Reuse CSMA – CSMA de reuso espacial.
TCP	Transmission Control Protocol – Protocolo de Control de Transmisión
TDD	Time Division Duplex - Duplexaje por División de Tiempo
UDP	User Datagram Protocol – Protocolo de Datagramas de Usuario
UNII	Unlicensed National Information Infrastructure – Infraestructura de Información Nacional sin Licencia.
VLSI	Very Large Scale of Integration – Muy alta escala de integración
WEP	Wired Equivalent Privacy – Privacidad Equivalente Cableada
WLAN	Wireless Local Area Networks – Redes de área local inalámbrica

APÉNDICE A.

FUNCIONES IMPORTANTES DEL ARCHIVO mac-802_11.cc.

recv() (DOWN): La clase Mac proviene de la clase base connector, por lo que los paquetes a ser enviados son recibidos por la función recv(). Dado que la función recv() también es llamada cuando un paquete viene del canal, recv() checa el campo de dirección en el encabezado del paquete. Si la dirección es DOWN, es decir, que el paquete viene de una capa superior (capa de enlace LL), entonces el paquete se pasa a la función send().

recv() (UP): La función recv() se llama cuando un paquete se recibe de una capa superior o inferior. Si el paquete se recibe de una capa inferior (NetIf), la primera verificación no se realiza. En este punto el medio físico ha recibido el primer bit de un paquete entrante, pero el MAC no puede hacer nada con el paquete hasta que el paquete completo sea recibido. Si el paquete se recibe mientras el MAC esta transmitiendo otro paquete, entonces el paquete recibido será ignorado, lo que significa que se pone a 1 la bandera de error en el encabezado del paquete. Si el MAC no está recibiendo algún paquete, entonces el estado rx_state_ se cambia a RECV y se llama a la función checkBackoffTimer(). Posteriormente, el paquete entrante se asigna a pktRX_ y se inicializa el *temporizador de recepción* por la duración txtime() del paquete. Si el MAC ya estaba recibiendo un paquete cuando otro paquete llega, comparará la potencia recibida del nuevo paquete con el primer paquete recibido. Si la potencia del nuevo paquete es más pequeña que la potencia del primer paquete por al menos el umbral de captura (CPThresh_= 10dB), el nuevo paquete será ignorado (capturado) y se llama a la función capture(). Si los niveles de potencia de los dos paquetes son muy parecidos, habrá una colisión y el control se transferirá a la función collision(), quien tirará el paquete entrante. El paquete original no será tirado hasta que se complete su recepción. El control regresará al MAC en cuanto el temporizador de recepción expire, llamando a la función recvHandler(), el cual llamará a la función recv_timer().

send(): La función send() primero checa el modelo de energía, tirando el paquete si el nodo se encuentra en el modo dormido (sleep). Después le asigna a la variable callback_ el valor del handler que fue pasado como parámetro a la función send(). Es de esta manera en que el handler puede ser llamado cuando la transmisión del paquete se ha completado. En el siguiente paso, send() llama a sendDATA y sendRTS los cuales construyen el encabezado MAC para el paquete de datos y el paquete RTS para que vayan con el paquete de datos, los cuales son almacenados en pktTx_ y pktRTS_ respectivamente. El encabezado MAC para el paquete de datos se le asigna un número de secuencia único (con respecto al nodo).

A continuación, el MAC checa su backoff timer, si el backoff timer no se encuentra en cuenta regresiva (counting down), entonces el nodo checa si el canal (el medio) esta desocupado, si es así, el nodo empezará a posponer su transmisión (defer). El nodo realiza esto empleando la función is_idle(). De acuerdo a las especificaciones de 802.11, el nodo pospondrá su transmisión un tiempo difs mas una cantidad de tiempo escogida aleatoriamente en el intervalo [0, cw_], donde cw_ es la ventana de congestión actual. Si el nodo ya esta esperando en su temporizador de posponer (defer timer), este continuará esperando (sin reanudar su temporizador).

Si se detecta que el medio está ocupado, entonces el nodo empieza su temporizador backoff. En este punto, la función send() ha terminado y el control continuará cuando uno de los temporizadores expire, llamando a deferHandler() o backoffHandler().

sendDATA(): Esta función construye el encabezado MAC para el paquete de datos. Esto involucra incrementar el tamaño del paquete, poniendo el tipo como *data* y el subtipo como *data*. El paquete al pasar por esta función ya debe de tener anexado un encabezado MAC completo. La función luego almacena el tiempo de duración del paquete (txtime), que es calculado por la función txtime(), que básicamente es el tamaño del paquete multiplicado por la tasa de datos. Este valor se calcula dos veces, ya que se emplean tasas de datos diferentes si el paquete es unicast o broadcast. Además, si el paquete no es un paquete broadcast, se calcula el campo de duración en el encabezado MAC. Por duración, se entiende la cantidad de tiempo que esta comunicación necesita el canal después de que el paquete de datos se ha transmitido. Para el caso de un paquete de datos, este corresponde a la cantidad de tiempo para transmitir un ACK y un SIFS. Si el paquete es broadcast este campo se pone a cero (no ACK para paquetes broadcast). En este punto, el MAC ha terminado de construir el encabezado MAC para el paquete y finalmente lo asigna a la variable interna pktTx_ para apuntar al paquete que estuvimos trabajando. Esto es esencialmente una manera de almacenar el paquete a ser transmitido en un buffer local en el MAC. Ahora, el código regresa a la función send().

sendRTS(): Esta función es la responsable de crear un paquete RTS con la dirección destino especificada en conjunto con el paquete de datos que el MAC esta tratando de enviar. La primera tarea que realiza es checar el tamaño del paquete contra la variable RTSthreshold. Si el paquete es mas pequeño (o si es broadcast) entonces no se envía RTS antes de la transmisión de datos (el mecanismo RTS/CTS no se utiliza). En este último caso, la función simplemente regresa el control a la función send(), en otro caso, se crea un nuevo paquete (esto se realiza en la primera línea de la función) y sus campos son llenados de manera apropiada (esto es, el tipo se pone como MAC). Una estructura rts_frame se usa para llenar el resto del encabezado del paquete y los valores apropiados son puestos en los campos rts, la dirección de destino se llena con la dirección pasada como parámetro a la función y el campo rf_ta se llena con la dirección MAC del nodo transmisor. El campo de duración también se calcula como el tiempo para transmitir un CTS, el paquete de datos (pktTx_) y el ACK (mas 3 tiempos SIFS). Después de que se ha construido el paquete, la variable interna pktRTS_ se asigna para apuntar al nuevo paquete RTS, posteriormente, el control se regresa a la función send().

sendCTS(): Esta función es la responsable de crear un paquete CTS y hacer que la variable interna pktCTRL_ apunte a este paquete. Todo procede de forma directa, con todos los campos llenados con los valores apropiados. El campo de duración es similar que el de RTS, menos el tiempo de duración del CTS (txtime) y un tiempo SIFS. Después de haber creado el paquete CTS el control se regresa a la función recvRTS().

sendACK(): Esta función se encarga de crear un paquete ACK que será enviado en respuesta a un paquete de datos. El paquete es creado y todos los campos se llenan con valores apropiados. El campo de duración se pone a cero lo que indica a los otros nodos que una vez que el ACK se haya completado, no necesitan posponer su comunicación.

Una vez que el paquete ha sido construido exitosamente, pktCTRL_ apunta al nuevo paquete ACK y el control se regresa a la función recvDATA().

deferHandler(): Esta función es llamada cuando el temporizador defer timer ha expirado. Cuando esto sucede, significa que el nodo ha esperado un tiempo suficiente antes de transmitir (para reducir la ocurrencia de una colisión) e intentará enviar un paquete. Por consiguiente, la primera tarea que la función realiza es asegurarse que existe un paquete de datos, control o RTS esperando ser transmitido. La función entonces llama check_pktCTRL(), y se asegura que el backoff timer no este corriendo, después, llama a check_pktRTS() y check_pktTx(). Si alguna de estas funciones check_ regresa un valor de cero, la función defer handler se detiene, lo que indica que la función check_ ha tenido éxito en la transmisión de un tipo de paquete. Por lo tanto, la transmisión de paquetes se maneja por una de estas funciones check_. En este punto, muy probablemente ha empezado la transmisión de algún tipo de paquete y el control se reiniciará con la expiración del temporizador interface timer, quien llama la función txHandler() que simplemente limpia la bandera tx_active_ para indicar que la capa física actualmente no esta transmitiendo algo. El control también se reanuda si otro paquete se recibe vía la función recv(): un paquete CTS si se envió un RTS, un paquete de datos si se envió un CTS, o un ACK si se acaba de enviar un paquete de datos. El control también se puede reanudar con la expiración del temporizador de envío, que llama la función sendHandler() y este a su vez llama send_timer().

check_pktCTRL(): Esta función es responsable de transmitir paquetes CTS y ACK, los cuales están apuntados por la variable pktCTRL_. La primera tarea que realiza la función es verificar si esta variable apunta a algo, si no, regresa -1 lo que indica que nada se transmite. La función también retornará, si el estado de transmisión (tx_state_) indica que el MAC está actualmente transmitiendo ya sea un paquete CTS o ACK. La función luego realiza una selección en base en el tipo de paquete de control que se va a enviar (CTS o ACK). Si el paquete es CTS, el MAC verificara el estado del medio usando la función is_idle(). Si el canal esta ocupado, el paquete CTS será tirado y la variable pktCTRL_ puesta a cero. Si el canal esta libre, la función pondrá el valor de tx_state_igual a MAC_CTS para indicar que el MAC está actualmente transmitiendo un CTS y luego llamará al macro checkBackoffTimer(). Después de esto, la función calcula el valor *timeout* (cuanto tiempo debería esperar el MAC antes de que decida que el paquete que envió no fue recibido correctamente). En el caso que el paquete de control sea un ACK, el MAC procede de la misma manera excepto que en este caso no se verifica el estado del medio, simplemente transmite el paquete. Finalmente, se llama la función transmit() con pktCTRL_ y el valor *timeout* calculado previamente como argumentos. En este punto, la capa física ha iniciado la transmisión del paquete de control.

Check_pktRTS(): Esta función como las otras dos funciones de verificación, es responsable de transmitir un paquete (ene este caso un paquete RTS). SI no hay un paquete RTS listo para ser enviado, esto es, que RTS sea igual a null, la función simplemente retorna con un valor de -1, indicando que no envío ningún paquete. La declaración de una sentencia *switch* se utiliza para detectar un paquete RTS construido inapropiadamente. Antes de enviar el RTS se detecta el canal, si se detecta que esta ocupado se duplica la ventana de congestión (cw_) utilizando la función en línea inc_cw() y el backoff timer se empieza otra vez, por lo tanto la función retorna sin enviar el paquete cuando el canal está ocupado.

Si el canal está libre, la función pondrá el valor de tx_state_igual a MAC_RTS y luego llamará al macro checkBackoffTimer(). Después, se calcula el valor del *timeout* para que el MAC conozca cuánto tiempo esperar la recepción del paquete CTS. Finalmente se llama el macro transmit() y se le envía como parámetros el paquete RTS y el valor de *timeout;* en este punto, la capa física ha empezado la transmisión del paquete RTS.

Check pktTX(): Esta función al igual que las otras dos funciones de verificación, es responsable de transmitir un paquete, en este caso los paquetes de datos. Si no hay paquete de datos en espera para ser enviado (pktTX_ es *null*), entonces la función retorna con un valor de -1, indicando que no se transmitió nada. De la misma manera, se utiliza una sentencia switch para detectar un paquete de datos construido inapropiadamente. Si se detecta que el canal está ocupado, se llama la función sendRTS(), esto significa que a pesar del intercambio RTS/CTS otro nodo está utilizando el canal (posiblemente debido a movilidad), o no se está utilizando RTS (si fuera este caso la función sendRTS() no haría nada). Adicionalmente, la ventana de congestión (cw_) se duplica utilizando la función en línea inc_cw() y se empieza el backoff timer de tal manera que el MAC permanecerá libre hasta que el otro nodo haya completado su transmisión. Si el canal se encuentra libre, la función pondrá el valor tx_state_ igual a MAC_SEND y se invoca el macro checkBackoffTimer(). El valor de *timeout* se calcula de dos maneras, dependiendo si el paquete de datos es o no *broadcast,* si no lo es, el valor de *timeout* es el tiempo que el MAC debería esperar antes de decidir que un ACK no fue recibido. Si el paquete es *broadcast*, el valor de *timeout* es simplemente el tiempo de transmisión del paquete ya que no se enviarán ACKs en conjunto con paquetes broadcast. Finalmente, se invoca el macro transmit() y se envían como argumentos el paquete de datos y el valor *timeout* calculado, en este punto el paquete de datos ha empezado a transmitirse.

checkBackoffTimer(): Este macro realiza dos verificaciones. Primero, si el medio esta libre y el backoff timer esta actualmente en pausa, entonces lo reactiva para que siga contando. Segundo, si el medio no esta libre y el backoff timer esta corriendo (medio ocupado y temporizador sin pausa), entonces pone el temporizador en pausa. Esto corresponde al hecho que el MAC solo realiza una cuenta regresiva del backofftimer mientras el canal este libre. Conforme a las especificaciones, el temporizador no debería estar corriendo cuando el canal está siendo usado por otro nodo.

transmit(): Este macro toma dos argumentos, un paquete y un valor de *timeout*, además pone la variable de bandera tx_active_ a uno para indicar que el MAC está actualmente transmitiendo un paquete. El macro luego realiza una verificación, ya que si se está transmitiendo un ACK es posible que el nodo pueda estar recibiendo un paquete, si es el caso ese paquete debería ser tirado. Si el MAC está actualmente recibiendo un paquete y se está transmitiendo un ACK, marca el paquete que se está recibiendo como un paquete con errores. A continuación, el paquete se pasa a la interfase de red (clase WirelessPhy) el cual es apuntado por *downtarget_* (realmente, solo una copia del paquete se envía a la capa inferior en caso de que se necesite hacer una retransmisión). Finalmente se inician dos temporizadores, *send timer* que se inicia con el valor de *timeout* quien alertará al MAC que la transmisión probablemente ha fallado. El segundo temporizador interface timer (mhIF_) se inicia con el valor de duración del paquete (txtime()), cuando este temporizador expira, el MAC sabrá que la capa física ha completado la transmisión del paquete.

send_timer(): Esta función es llamada cuando expira el TxTimer (mhSend_). Este temporizador expira después de una cantidad de tiempo calculada como *timeout* en la función check_ correspondiente. La expiración de este temporizador significa diferentes cosas dependiendo del tipo de paquete que se envió. Mediante una declaración *switch*, el MAC checa el valor de tx_state_ para darse cuenta del tipo de paquete que fue recientemente enviado y entonces manipula cada paquete de forma diferente. Si el último paquete enviado fue un RTS, la expiración de temporizador significa que no se recibió un CTS, ya sea porque el paquete RTS colisionó o porque el nodo receptor esta esperando para poder transmitir. El MAC responde mediante el intento de retransmitir el RTS llamando a la función RetransmitRTS(). Si el último paquete enviado fue un paquete CTS, la expiración del temporizador significa que no se recibió el paquete de datos. Este es un evento poco frecuente que ocurre si el paquete CTS colisionó o si el paquete de datos contenía errores. El MAC maneja esto simplemente reestableciéndose a si mismo a un estado desocupado, esto implica liberar el paquete CTS almacenado en pktCTRL_. Si el último paquete enviado fue un paquete de datos, la expiración del temporizador significa que no se recibió el paquete ACK. El MAC resuelve esta situación llamando a la función RetransmitDATA(). Finalmente, si el último paquete enviado fue un ACK, la expiración del temporizador significa que el paquete ACK se ha transmitido ya que no se espera una respuesta para paquetes de este tipo. El MAC libera el paquete ACK que es apuntado por pktCTRL_.

Después de que cada caso ha sido resuelto y posiblemente un paquete este preparado para ser retransmitido, el control es concedido a la función tx_resume(). Si un paquete va a ser retransmitido, el backoff timer ya ha sido iniciado con la ventana de congestión incrementada.

tx_resume(): Esta función es llamada cuando el MAC se esta alistando para enviar un paquete pero necesita poner algunos temporizadores. Si un paquete de control (CTS o ACK) esta esperando ser enviado, esta función simplemente empieza el temporizador de posponer por una cantidad SIFS, esto es porque se supone que un nodo debe esperar un breve periodo de tiempo antes de transmitir. Si un paquete RTS esta esperando ser enviado, entonces el MAC se asegura que el backoff timer no se encuentra actualmente ocupado, si lo esta, entonces el MAC esperará para empezar el temporizador de posponer (defer timer). Si el backoff timer no está ocupado se inicia el temporizador de posponer por un tiempo aleatorio en el intervalo [0, cw_] más un tiempo DIFS. Si lo que se va a enviar es un paquete de datos, y el MAC no esta actualmente en backoff (el temporizador de backoff esta libre), entonces se inicia el temporizador de posponer para el paquete de datos. Si no se utilizó un RTS para este paquete, entonces el temporizador de posponer se establece a una variable aleatoria en el intervalo [0, cw_] más un tiempo DIFS, en cambio si se utilizó un RTS, el MAC solo pospondrá su transmisión por un tiempo SIFS. Esto se debe a que si se utilizo un paquete RTS, entonces el canal ya ha sido reservado para este MAC y no necesita preocuparse por las colisiones.

Si no hay paquetes esperando ser enviados, pero la variable *callback_* está definida, esta variable se maneja de tal forma que corresponda a la transmisión de un paquete completada exitosamente. Finalmente la variable tx_state_ se pone a *idle* y el control retornará al MAC cuando el temporizador de posponer haya expirado (deferHandler()) o regrese a la función que lo llamo, como una de las funciones *recv* (funciones de recepción de paquetes).

capture(): Esta función se llama cuando se recibe un segundo paquete mientras el MAC ya está recibiendo otro paquete, pero el segundo paquete se recibe con una potencia suficientemente débil que la capa física pueda ignorarlo. La acción importante que realiza esta función es actualizar el NAV de tal forma que la detección de portadora sabrá que el canal estará ocupado después de que haya terminado de recibir su paquete. Esta función también elimina el paquete capturado.

collision(): El manejador de colisiones primero checa la variable rx_state_ y la pone a MAC_COLL en caso de que esta sea la primera colisión durante el paquete actual. Si un tercer paquete colisiona, rx_state_ ya estará en el estado de MAC_COLL. Luego, el MAC calcula cuanto tiempo durará el nuevo paquete y cuanto tiempo durará el paquete viejo, si el paquete nuevo dura más que el viejo, entonces el MAC hace al nuevo paquete pktRx_ y reinicia el temporizador de recepción (mhRecv_), en este caso el paquete viejo se elimina y solo se queda con el nuevo. En el caso de que el paquete viejo dure más que el paquete nuevo, el paquete nuevo simplemente se elimina y pktRX_ no cambia. Al final de esta función, el paquete colisionado que dure menos ha sido eliminado y la variable rx_state_ se pone en MAC_COLL.

recv_timer(): Esta función, es el manejador del temporizador de recepción de paquetes, llamado cuando mhREcv_ expira (aunque indirectamente a través de RecvHandler). La expiración del temporizador de recepción significa que un paquete ha sido completamente recibido y se puede realizar una acción determinada. Primero, el MAC verifica si su estado actual esta en el modo de transmisión de un paquete mediante el chequeo de la bandera tx_active_, si es así, entonces el MAC no habría escuchado este paquete entrante por lo que debe ser eliminado (sin ajustar el NAV). Después, se checa la variable rx_state_ para determinar si hubo una colisión en este paquete (esto es, rx_state_ igual a MAC_COLL), si es así, entonces pktRX_ es el paquete colisionado que duró más y ahora debe ser eliminado, además el NAV es ajustado por un tiempo EIFS, que es la cantidad de tiempo que el MAC debe esperar después de una colisión. El MAC después checa si el paquete tiene errores, y lo elimina si algún error fuera detectado (el paquete fue recibido con suficientes bits en error que el nivel actual del FEC no podría arreglar todos los problemas, esto es, después del FEC, el checksum también falló); otra vez, el NAV se ajusta a un tiempo EIFS después de que el paquete erróneo se ha terminado de recibir. Lo siguiente que realiza el MAC es verificar si el paquete está destinado para él, si no es así, el MAC receptor actualiza su NAV con el valor que lee del campo de duración del encabezado MAC del paquete recibido. Esta es la manera en que el MAC no intenta transmitir mientras otros nodos están utilizando el canal. La siguiente verificación consiste en enviar al paquete a un *tap* si es un paquete de datos (esencialmente enviar el paquete a cualquiera que desee escuchar en modo promiscuo), el siguiente chequeo involucra un algoritmo de fidelidad adaptiva y básicamente mantiene información de los nodos dentro de su rango de radio. Finalmente, la última verificación realizada es de filtrado de dirección, donde todos los paquetes que no estén destinados para este nodo son eliminados. El NAV ya habría sido actualizado, así que no hay necesidad de hacer algo más con el paquete.

En este punto, el MAC decide que hacer en base en el tipo de paquete que acaba de recibir, si el paquete es del tipo MAC_Type_Management, simplemente se tira. Si es un paquete RTS, CTS, ACK o datos, se llama la función recvRTS(), recvCTS(), recvACK() ó recvDATA() respectivamente. Después de esto, pktRX_ se pone a cero y el control se da a rx_resume()

rx_resume(): Esta función se llama después de que la función recv_timer() se ha completado. Esta función únicamente se encarga de poner a la variable rx_state_ a *idle* y luego invocar a la función checkBackoffTimer().

backoffHandler(): Esta función se llama cuando el backoff timer expira. Primero checa si hay un paquete de control (CTS o ACK) esperando ser enviado, si es así, se asegura de que el MAC este ya sea enviando el paquete o posponiendo antes de enviar el paquete. Si no hay un paquete de control llama a la función check_pktRTS() en otro caso llama check_pktTX(). Esto significa que en la expiración del backoff timer, un paquete de RTS o de datos será transmitido, si es que alguno de ellos esta en espera.

txHandler(): Es un manejador para IFtimer que simplemente limpia la bandera en el MAC para indicar que el radio ya no está activo.

Temporizadores.

Los temporizadores están definidos en los archivos ~ns/mac/mac-timers.{h,cc} mientras que los manejadores (funciones llamadas cuando los temporizadores expiran) están en ~ns/mac/mac-802_11.cc.

IFTimer: El temporizador de interfase (Interface Timer) mantiene información del tiempo que la interfase estará en el modo de transmisión. Este es el tiempo en que la interfase esta activamente transmitiendo bits al aire. El manejador para este temporizador es txHandler().

NavTimer: Se inicia con la recepción de un paquete por la duración del tiempo indicado en el campo de duración del encabezado MAC. El manejador llamado al expirar este temporizador es navHandler().

RxTimer: Se inicia cuando se recibe el primer bit de un paquete y se fija por la duración de tiempo que el paquete requerirá para ser completamente recibido. Este temporizador se necesita porque en la simulación el paquete entero esta disponible tan pronto se recibe el primer bit, pero el MAC no debe acceder al paquete hasta que no haya sido completamente recibido. En el caso de la colisión de un paquete, el temporizador de recepción se restablece para que expire al final del paquete colisionado de mayor duración. Al expirar el temporizador, indirectamente llama recv_timer() mediante la llamada primero de recvHandler().

TxTimer: Indica el tiempo en el cual un paquete ACK/CTS debería ser recibido. El TxTimer (mhSend_) se inicia cuando un paquete es transmitido por la función transmit(). Cada tipo de paquete espera una respuesta, por ejemplo, un paquete RTS espera en respuesta un CTS. Por lo tanto, el temporizador se detiene cuando se recibe un paquete CTS, datos, o ACK.

El temporizador no se inicia con la transmisión de un paquete ACK ya que un paquete ACK no necesita respuesta. Con la expiración de este temporizador, se llama indirectamente a la función send_timer() mediante la llamada primero del manejador sendHandler().

DeferTimer: Es el tiempo que un nodo debe esperar antes de iniciar la transmisión de un paquete. Si un paquete de control (CTS o ACK) esta esperando ser enviado, esta función simplemente empieza el temporizador de posponer (defer timer) por una cantidad SIFS, esto es porque se supone que un nodo debe esperar un breve periodo de tiempo antes de transmitir. Si un paquete RTS esta esperando ser enviado, entonces el MAC se asegura que el backoff timer no se encuentra actualmente ocupado, si lo esta, entonces el MAC esperará para empezar el temporizador de posponer. Si el backoff timer no está ocupado se inicia el temporizador de posponer por un tiempo aleatorio en el intervalo [0, cw_] más un tiempo DIFS. Si lo que se va a enviar es un paquete de datos, y el MAC no esta actualmente en backoff (el temporizador de backoff esta libre), entonces se inicia el temporizador de posponer para el paquete de datos. Si no se utilizó un RTS para este paquete, entonces el temporizador de posponer se establece a una variable aleatoria en el intervalo [0, cw_] más un tiempo DIFS, en cambio si se utilizó un RTS, el MAC solo pospondrá su transmisión por un tiempo SIFS. Esto se debe a que si se utilizo un paquete RTS, entonces el canal ya ha sido reservado para este MAC y no necesita preocuparse por las colisiones.

BackoffTimer: Es el tiempo que un nodo debe esperar antes de transmitir un paquete cuando encuentra que el canal esta ocupado, cuando va a retransmitir algún tipo de paquete que no fué recibido correctamente o cuando se ha recibido un ACK y se quiere transmitir de nuevo. Este temporizador está contando cuando el canal está libre y en pausa cuando el canal está ocupado.

BeaconTimer: No se utiliza.

BIBLIOGRAFIA Y REFERENCIAS.

[1] Ajay Chandra, V. Gummalla. “Wireless Medium Access Control Protocols”. IEEE Communications Surveys and Tutorials, Segundo Cuatrimestre 2000.

[2] Angela Doufexi, Simon Armour. “A Comparison of the HiperLAN/2 and IEEE 802.11a Wireless LAN standards”. IEEE Communications Magazine, Mayo 2002.

[3] Brian P. Crow , “IEEE 802.11 Wireless Local Area Networks”, IEEE Communications Magazine Septiembre 1997.

[4] P. Nicopoliditis, Wireless Networks. John Wiley, 2003

[5] Javier Gómez, Luis Méndez. “PCQoS: Power Controlled QoS in Wireless Ad Hoc Networks” White paper, Junio 2005.

[6] Jeffrey P. Monks. “A Power Controlled Multiple Access Protocol for Wireless packet Networks”. Proceedings of the IEEE INFOCOM 2001.

[7] Kuei Ping Shih. “A Power Saving MAC Protocol by Increasing Spatial Reuse for IEEE 802.11 Ad Hoc WLANs”. 19th Internatinal Conference on Advanced Information Networking and Applications (AINA 2005), Taipei Taiwan.

[8] D. Maniezzo, P. Bergamo. “How to Outperform IEEE 802.11: Interference Aware (IA) MAC”. Proceedings of MedHocNet 2003. Túnez Junio 2003.

[9] Nitin Gupta, “A Performance Analysis of the 802.11 Wireless LAN Medium Access Control”, Communications in Information and Systems, Vol. 3, No. 4, Pags. 279-304, Septiembre 2004.

[10] Andrew S. Tanenbaum, Computer Networks, 4th edition, Prentice Hall 2003.

[11] http://www.intelligraphics.com/articles/80211_article.html

[12] William Stallings, Data and Computer Communications, 5th edition Prentice Hall 1997.

[13] Hrishikesh Gossain, “A Novel Power Control MAC Protocol with Spatial Reusability for Wireless Ad Hoc Networks”, OBR Center of Distributed and Mobile Computing Department of ECECS, University of Cincinnati, 2001.

[14] Plamen Nedeltchev, “Wireless Local Area Networks and the 802.11 Standard” , Marzo 2001, http://www.cisco.com/warp/public/784/packet/jul01/pdfs/whitepaper.pdf

[15] Steve Kapp. “More Bandwidth without the Wires”. IEEE Internet Computing, Julio-Agosto 2002.

[16] http://www.tutorial-reports.com/wireless/wlanwifi/802.11b.php

[17] Jeffrey P. Monks, “Transmission Power Control for Enhancing the Performance of Wireless Packet data Networks”, Ph. D. Thesis, University of Illinois at Urbana Champaign, 2001.

[18] “The *ns* manual”, http://www.isi.edu/nsnam/ns/ns-documentation.html

[19] “Ns by example”, http://nile.wpi.edu/NS/

[20] “Marc Greis´s tutorial”, http://www.isi.edu/nsnam/ns/tutorial

[21] “The Network Simulator ns-2: workshops, tutorials, and presentations”, http://www.isi.edu/nsnam/ns/ns-tutorial/index.html

[22] “802.11 MAC code in ns-2”, http://www.ece.rice.edu/~jpr/ns/docs/802_11.html

[23] P. Gupta y P. R. Gumar. “The Capacity of Wireless Networks”, IEEE Transactions on Information Theory, Vol. IT-46, no. 2, 2000.

[24] D. Clark y J. Wroclawsky. “An Approach to Service Allocation in the Internet”.

[25] J. Gómez Castellanos y Andrew T. Campbell. “PARO: Supporting Transmisión Power Control for Routing in Wireless Ad Hoc Networks”. ACM/Kluwer Journal on Wireless Networks (WINET), 2003.
[26] Shugong Xu y Tarek Saadawi. “Does the IEEE 802.11 MAC Protocol Work Well in Multihop Ad Hoc Networks”. IEEE Communications Magazine, pp. 130-137, Junio 2001.
[27] J. Li et al. “Capacity of Ad hoc Wireless Networks”. Proceedings of ACM Mobicom, Julio de 2002.