Revista Facultad de Ingeniería
ISSN: 0717-1072
facing@uta.cl
Universidad de Tarapacá
Chile

Delgadillo Á., Sebastián; Guzmán V., David; Müller G., Andrés; Grote H., Walter
ANÁLISIS EXPERIMENTAL DE UN AMBIENTE WI-FI MULTICELDA
Revista Facultad de Ingeniería, vol. 13, núm. 3, 2005, pp. 45-52
Universidad de Tarapacá
Arica, Chile

Disponible en: http://www.redalyc.org/articulo.oa?id=11414672017

# ANÁLISIS EXPERIMENTAL DE UN AMBIENTE WI-FI MULTICELDA

**Sebastián Delgadillo Á.[1] David Guzmán V.[1] Andrés Müller G.[1] Walter Grote H.[1]**

*Recibido el 24 de junio de 2005, aceptado el 12 de octubre de 2005*

**RESUMEN**

Las redes locales inalámbricas de banda ancha han experimentado un desarrollo explosivo con la introducción del protocolo IEEE802.11. El hecho de que éstas operen en una banda no licitada ha permitido que aparezcan numerosos "hot spots", que no siempre son instalados por personal experto. En este trabajo se analiza el problema que se presenta en un ambiente IEEE802.11b WiFi multicelda, en que no se ha tenido el cuidado de planificar la asignación de canales. Se presenta la interferencia medida experimentalmente en un escenario típico multicelda controlando los parámetros de activación del mecanismo RTS/CTS y elección de canales adyacentes.

Palabras clave: Telecomunicaciones, protocolo MAC IEEE 802.11b, interferencia electromagnética, problema terminal oculto y expuesto.

***ABSTRACT***

*Wireless Local Area Networks (WLAN) have experienced an explosive growth since the introduction of the IEEE802.11 protocol. The fact that it operates on non-licensed frequency bands has given way that a large amount of "hot spots" have been installed by operators that not always have the necessary expertise. In this publication we analyze the problem that arises in a multicell environment where no frequency planning has been carried out. Experimental measurements are performed in such an environment, by controlling parameters like activation of the RTS/CTS mechanism and frequency planning.*

*Keywords: Telecommunications, IEEE 802.11b MAC protocol, electromagnetic interference (EMI), hidden and exposed terminal problem.*

## INTRODUCCIÓN

Las Redes Inalámbricas de Área Local (WLAN's, *Wireless Local Area Network*) IEEE 802.11b proporcionan conectividad y acceso a las tradicionales redes cableadas, como si fuese una extensión de estas últimas, pero con la flexibilidad y movilidad que ofrecen las comunicaciones inalámbricas. En sectores públicos (aeropuertos, universidades y centros comerciales) suelen operar varias redes inalámbricas WiFi, usando "*hot spots*" que pretenden otorgar un servicio a los usuarios, con ninguna o escasa planificación de frecuencias. La única forma de evitar los traslapes de frecuencia es realizando una planificación de frecuencias entre los canales 1, 6 y 11, lo que da lugar a 3 frecuencias de reuso, en el mejor de los casos. Si se usan canales repetidos o canales adyacentes, se producen efectos de interferencias por traslape de las bandas de frecuencia. El efecto de este fenómeno no ha sido estudiado, según los autores del presente trabajo, motivo de análisis de la presente labor.

En caso que utilicen exactamente el mismo canal, se da el problema del terminal expuesto, que se traduce en que un terminal se inhibe de transmitir, porque escucha la transmisión de otro terminal operando en la misma frecuencia, pero que está conectado a un punto de acceso diferente. Otro problema típico que se genera en un ambiente multicelda es el problema del terminal oculto, el cual se produce cuando un terminal no es capaz de detectar la presencia de otro terminal en la red. Dado que en redes CSMA el método de acceso múltiple requiere la detección de portadora para determinar el estado ocioso u ocupado del medio, la incapacidad de realizar esta operación se traduce en un problema de desempeño.

[1] Departamento de Electrónica-UTFSM. Casilla Postal 110-V, Av. España 1680, Valparaíso, Chile, wgh@elo.utfsm.cl

Producto de estos dos fenómenos se generan muchos problemas para los usuarios como, por ejemplo, una baja en la tasa efectiva de servicio (*throughput*) y retardo excesivo en la transmisión de paquetes.

Se analizará un escenario en el cual se presenta el problema del terminal oculto y el problema del terminal expuesto cuando hay dos AP, comparando los resultados obtenidos en forma empírica con el mejor desempeño que puede esperarse desde un punto de vista teórico. Adicionalmente se analizará el fenómeno de las interferencias causadas por la utilización de canales adyacentes.

Para realizar las mediciones, se usan las referencias [6] y [2]. En [6] se propone un método empírico para obtener los parámetros de relevancia de una red WiFi mediante mediciones, escenario que se amplía y complementa en [2], donde se incluye el problema del terminal oculto.

Los resultados obtenidos de este trabajo demuestran que en un ambiente multicelda el uso del protocolo RTS/CTS mejora la utilización del canal, manteniendo una equidad en el acceso entre las estaciones clientes en un ambiente multicelda. Con respecto a la utilización de canales intermedios, se concluyó que el utilizarlos da como resultado una significativa disminución del *throughput* en las transmisiones.

El trabajo está dividido en 6 secciones. En la primera se hace una introducción al tema, mientras que en la segunda se muestra el escenario de pruebas, donde se deducen las máximas tasas efectivas teóricas que podrían esperarse. En la tercera sección se describe la infraestructura utilizada en las mediciones (HW y SW) y el procedimiento seguido en las mediciones. En la cuarta se informa de los resultados obtenidos en algunas mediciones cuando los "*hot spots*" hacen uso del mismo canal. En la quinta sección se muestra el efecto de transmitir en canales traslapados y se finaliza con las conclusiones.

## ESCENARIO DE PRUEBAS Y COTAS MÁXIMAS PARA LA TASA EFECTIVA DE SERVICIO

Previo al hecho de realizar mediciones experimentales, conviene calcular el Máximo *Throughput* (MT) que puede esperarse teóricamente en un escenario ideal en que un terminal móvil se comunica con un AP. El cálculo más sencillo es aquél en que se supone que no existe otra interferencia. Para obtenerlo, se supone: 1) que el canal está libre de errores, y 2) durante la transmisión hay sólo un AP activo, y solamente una estación cliente capaz de recibir los paquetes enviados desde la AP. El resultado de este cálculo será una cota máxima a ser esperada en un ambiente experimental.

El cálculo tiene que considerar que el intercambio de mensajes entre el AP y el terminal sigue un protocolo establecido. El protocolo básico de la Función de Coordinación Distribuida (DCF: *Distributed Coordination Function*) se traduce en que una estación que recibe un paquete para ser transmitido inalámbricamente primero establece un valor inicial para un contador de cuenta regresiva que contabiliza ranuras de contienda que detecta ociosas. Cuando alcanza la cuenta 0 transmite. Esta cuenta la realiza mientras detecta el canal ocioso después de una transmisión y un tiempo adicional DIFS (*Distributed InterFrame Space*). Si su transmisión es recibida exitosamente, el destinatario emite un reconocimiento (ACK) después de un tiempo SIFS (*Short InterFrame Space*). En caso de estar en presencia del fenómeno del terminal oculto, se precede al envío de datos de un intercambio RTS (*Request To Send*) enviado por el emisor, seguido de un CTS (*Clear To Send*) del receptor, con tiempos entre mensajes SIFS, como se ilustra en la figura 1.


Fig. 1 Protocolo RTS/CTS usado en IEEE 802.11.

El *throughput* se obtiene entonces aplicando las siguientes ecuaciones:

$$MT = \frac{L_{paquete}}{L_{paquete} / R_{datos} + T_{control}} \quad (1)$$

$$T_{control}\Big|_{sin\ RTS} = \frac{CW_{min}}{2} + 2T_{delta} + 2T_{PCLP} + \frac{ACK}{R_{datos}} \quad (2)$$

$$T_{control}\Big|_{conRTS} = \frac{CW_{min}}{2} + 4T_{delta} + 4T_{PCLP} + \frac{RTS + CTS + ACK}{R_{datos}} \quad (3)$$

Donde la definición y valores de los parámetros de la ecuaciones de la (1) a la (3) se encuentran en la tabla 1.

Tabla 1 Parámetros IEEE 802.11b [5].

| Definición | Significado | Valor |
|---|---|---|
| $L_{paquete}$ | Tamaño del paquete transmitido | 1472[bytes] |
| $R_{datos}$ | Tasa de transmisión bruta | 11[Mbps] |
| $CW_{Min}$ | Ventana de Contienda Mínima | 32 |
| *MACheader* | Agregado MAC de 28 bytes min | 28 [bytes] |
| *ACK* | Datos en una trama MAC ACK | 14 [bytes] |
| *RTS* | Datos en una trama MAC RTS | 20 [bytes] |
| *CTS* | Datos en una trama MAC CTS | 14 [bytes] |
| $T_{PCLPS}$ *(opt)* | PCLP para tasas de 2, 5.5 y 11 Mbps | 96[ms] |
| $T_{PCLPL}$ | PCLP para tasas de 1 Mbps | 192[ms] |
| $T_{DIFS}$ | Duración de un tiempo DIFS | 50[ms] |
| $T_{SIFS}$ | Duración de un tiempo SIFS | 10[ms] |
| s | Duración de intervalo de contienda | 20[ms] |
| $T_{delta}$ | Tiempo Tx/Rx y procesamiento | 1[ms] |

El tamaño del paquete de datos escogido en la tabla 1 corresponde al máximo tamaño que puede tomar un paquete IP en una red Ethernet. El valor de la ventana de contienda $CW_{min}$ corresponde a 32, ya que es el valor que viene por defecto en las componentes WiFi. Dado que el valor inicial del contador del contador de *backoff* se distribuye aleatoriamente en forma uniforme, se toma el valor promedio para este cálculo en las ecuaciones (2) y (3). La estructura de una trama MAC se muestra en la figura 2. En la figura 3, en cambio, se muestra la composición del encabezado MAC. Además, como se desprende de la tabla 1, el estándar define que el PLCP (*Physical Convergence Layer Procedure*) puede ser de dos tipos, según sea la calidad del enlace. El PLCP largo (*long*) se usa normalmente como opción por defecto, a veces sin poder sustituirlo por el PLCP corto, por lo cual tiene más sentido evaluar el *throughput* con el PLCP largo. En la figura 2 se muestra la estructura de este encabezado de la capa física, que normalmente se transmite a una tasa de 1 Mbps, como aparece en la tabla 1.

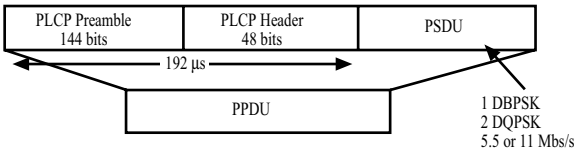


Fig. 2 Formato Long PLCP PPDU [5].

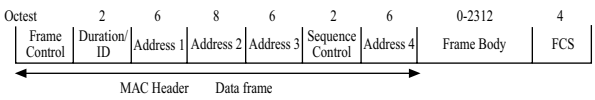


Fig. 3 Formato Trama MAC [5].

Normalmente los datos del encabezado se transmiten a la tasa nominal a la que opera el terminal de la red con condiciones de enlace más pobres. Si la tasa de transmisión bruta se fija a 11 Mbps, entonces se obtienen los valores de las ecuaciones (4) y (5) para la máxima tasa efectiva de servicio (MT) con PLCP largo, al reemplazar los valores de la tabla 1 en las ecuaciones (1) a (3):

$$MT_{conRTS} = 4,74[\,Mbps\,] \quad (4)$$

$$MT_{sin\,RTS} = 6,51[\,Mbps\,] \quad (5)$$

Se observa de estos resultados que es mucho más conveniente operar a altas tasas de transmisión bruta, sin intercambio RTS/CTS. Sin embargo, en presencia del fenómeno de terminal oculto, será más conveniente usar el mecanismo RTS/CTS, como se desprende de las pruebas experimentales que se describirán luego.

Se desea crear un entorno donde operan varias redes inalámbricas WiFi, con ninguna o escasa planificación de frecuencias, para analizar de qué manera se deteriora el *throughput* por esta mala planificación. Un caso simple a considerar es la instalación de 2 "*hot spots*" que pretenden otorgar un servicio a los usuarios que tienen terminales móviles. El escenario más difícil es aquEl en que los "*hot spots*" están ocultos entre sí, hay un terminal que está en la zona de cobertura de ambos y hay presente otro terminal que está oculto a ese terminal, pero en la zona de cobertura de sólo uno de los "*hot spots*". La situación descrita puede resumirse en términos de la figura 4. Las transmisiones se realizan entre un punto de acceso (AP: *Access Point*), el AP1 y el terminal móvil STA1 (STA: *Station*), y entre el AP2 y la STA2. En este escenario, el terminal móvil STA/2, que está en zona de traslape, "ve" a ambos APs, o sea, la STA1 está en zona de terminal expuesto. La otra estación cliente (STA/1), que se encuentra en la zona de cobertura del AP1 sólo "ve" al AP1. Ambas STAs no escuchan sus transmisiones, es decir, son ocultas entre sí.

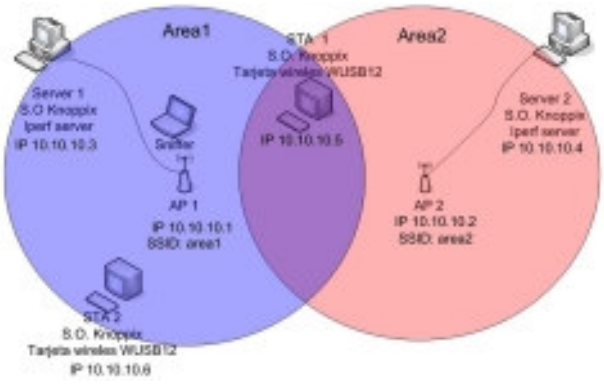


Fig. 4 Escenario de medición.

El máximo *throughput* por enlace se producirá cuando el medio esté siendo siempre ocupado sin producirse colisiones. El MT del canal va a ser el obtenido en (4) o (5), pero el MT por enlace será la mitad al obtenido anteriormente, ya que el canal es compartido en el tiempo.

De esta manera la *máxima tasa efectiva de servicio por enlace* para el escenario desarrollado usando el PLCP largo será el siguiente:

$$\begin{aligned} MT_{conRTS} &= 2{,}37\,[\,Mbps\,] \\ MT_{sin\,RTS} &= 3{,}26\,[\,Mbps\,] \end{aligned} \qquad (6)$$

Este resultado se explica por el hecho de que el medio es compartido en el tiempo.

## INFRAESTRUCTURA DE LOS EXPERIMENTOS

Para los experimentos se utilizaron 2 APs Cisco Aironet 1100, ya que permiten variar fácilmente muchos parámetros de configuración. Un parámetro importante que ofrecen estos dispositivos es el control de potencia de transmisión, la que puede ser ajustada de 1 mW a 100 mW, permitiendo de esta forma controlar el radio de cobertura de un AP. Otro parámetro importante que se puede variar en estos dispositivos es el umbral de activación RTS/CTS.

En las estaciones clientes se utilizaron tarjetas *Linksys WUSB12.* La particularidad de estas tarjetas es que se conectan al puerto USB y, más importante, pueden ser fácilmente recubiertas de material ECCOSORB VHP-4 que absorbe la señal electromagnética, introduciendo una atenuación –adicional a la de la propagación natural– de 20 dB, aproximadamente.

En un *notebook* Sony Vaio PIV de 1.5GHz, 512 MB de RAM se colocó una tarjeta Orinoco Silver, la cual permite trabajar en modo de "escucha". Además, se instaló un *sniffer AiroPeek NX* que permite analizar el intercambio de paquetes en la interfaz de aire usando el S.O Windows XP *Home Edition*. La idea de utilizar un *sniffer* en la interfaz de aire es la de poder verificar las configuraciones de *hardware* como el intercambio de tramas RTS/CTS y ocupación del canal inalámbrico que se utilizarán en las pruebas para minimizar interferencias.

Los computadores genéricos utilizados como servidores (conectados en la puerta *Ethernet* de los AP's) son Pentium III de 700Mhz, 128 MB de memoria RAM. En los servidores y clientes se utilizó como S.O. *Knoppix* versión 3.3 y 3.4 para evitar alterar la configuración original del S.O. del disco duro que tenían. Como estaciones clientes se utilizaron 2 *notebook* Dell Latitude D600 con procesador Pentium M de 1,4 GHz, 512MB de RAM.

*Iperf* es una herramienta para establecer transmisiones entre cliente y servidor, permitiendo la configuración de varios parámetros y características para paquetes TCP como UDP.

Características de *Iperf* aprovechadas en los experimentos son:

- El servidor maneja múltiples conexiones. Es posible especificar la cantidad de datos a ser transferidos, la tasa de generación y el tiempo que se desea que permanezca activa la transmisión.
- Cuando sea apropiado, las opciones pueden ser especificadas en k (kilo-) y M (mega-). De este modo, se puede especificar 128K en vez de 131072 bytes.
- *Iperf* reporta *throughput*, retardo (*delay*), *jitter* (variación del retardo) y pérdidas de datagramas en intervalos de tiempo especificados.

En las siguientes secciones se describe la validación de los instrumentos de medición (el generador de tráfico, los computadores donde se ejecuta el programa *Iperf*, el *sniffer* y el *notebook)*, verificando que ninguno de ellos sea un elemento limitante para la realización de los experimentos, salvo los que tienen relación directa con el fenómeno que se desea medir experimentalmente.

## VALIDACIÓN DE LAS ESTACIONES CLIENTES (TERMINALES)

Para asegurar que las computadoras (*notebooks*) no fueran la limitante en relación a la máxima tasa de transferencia que pueden enviar, se realizaron comparaciones entre tarjetas inalámbricas utilizando *Iperf* (en su versión para Linux). En la prueba se utilizaron las siguientes tarjetas inalámbricas:

- Orinoco Silver, adaptador PCMCIA.
- Dlink DWL-650, adaptador PCMCIA.
- Linksys WUSB12, adaptador USB.

Se utilizó el acceso básico (protocolo WiFi sin intercambio de mensajes RTS/CTS) para realizar estas mediciones. La prueba se realizó durante un minuto y consistía en enviar datos desde una sola estación al servidor utilizando *Iperf*. El *throughput* de saturación es la máxima tasa de transferencia sin pérdida de paquetes.

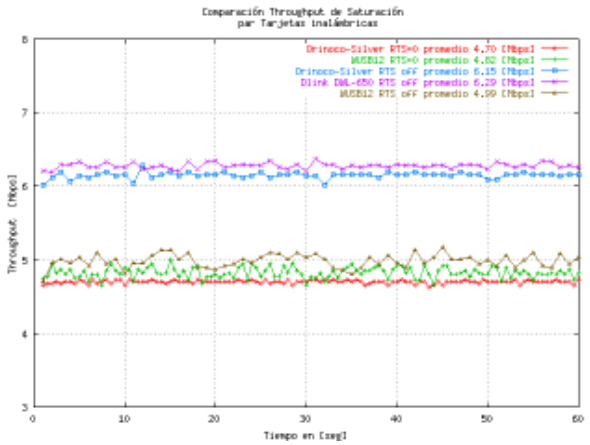


Fig. 5 Comparación Throughput de Saturación para tarjetas inalámbricas Orinoco Silver, Dlink DWL-650 y Linksys WUSB12 para el tráfico de subida.

En la figura 5 se aprecian los resultados de esta medición. El máximo *throughput* alcanzado por el adaptador Dlink DWL-650, cuyo valor promedio es de 6.29 [Mbps], confirma los resultados publicados en [6]. El adaptador Orinoco Silver, en cambio, obtuvo un *throughput* de 6.15 [Mbps]. El peor caso es el entregado por el adaptador WUSB12 con un valor promedio de 4.99 [Mbps]. Las diferencias respecto de los valores teóricos obtenidos se deben a imperfecciones de las componentes (como queda claramente de manifiesto en el WUSB12) y, en menor grado, debido a que *Iperf* mide el *throughput* UDP. En el caso en estudio, el efecto del encabezado UDP es del orden de 3,6% (eso es, el valor esperado de *throughput*, considerando el encabezado UDP como parte del paquete, es de 6.51 [Mbps] para DWL-650, lo que coincide con el valor teórico encontrado en la ecuación (5)).

Utilizando intercambio de tramas RTS/CTS se obtuvieron los siguientes resultados: al adaptador DWL-650 no se puede configurar de tal modo que el umbral de activación RTS sea 0, por lo cual se descarta para la realización de los experimentos. Ajustando el umbral de activación del mecanismo RTS en 0 para el adaptador Orinoco Silver, se alcanzó un *throughput* de 4.70 [Mbps], cercano al *throughput* alcanzado por el adaptador WUSB12.

Esta prueba resulta en que el adaptador WUSB12 es el componente de peor desempeño. Sin embargo, es la única que puede ser recubierta fácilmente de material de esponja que absorbe la radiación electromagnética, comúnmente usado en la fabricación de cámaras anecoicas. Como se describió anteriormente, se requiere este efecto para introducir las pérdidas necesarias para crear el efecto de terminal oculto en el espacio restringido de un laboratorio [3]. A lo anterior se agrega el hecho que estas componentes se introducen en envases de cartón recubiertos completamente de papel aluminio, salvo una boca, para incrementar el efecto de aislamiento electromagnético y tener control sobre el diagrama de radiación electromagnética de los dispositivos. El hecho de que este componente presente una limitante máxima a la tasa efectiva de servicio se aprecia en la figura 6, donde la tasa efectiva de servicio se incrementa cuando hay dos terminales, reflejando que: 1) el AP no tiene problemas para operar a tasas cercanas a 6.2 Mbps y superiores a las del WUSB12, y 2) se confirma que la tasa efectiva de servicio máxima del WUSB12, en recepción de paquetes es de 3.9 Mbps.

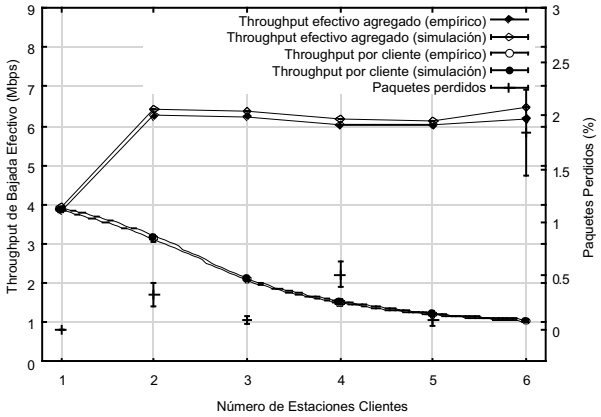


Fig. 6 Throughput de transmisiones de paquetes desde un AP a clientes equipados con WUSB12.

***Validación del sniffer***: Para establecer que el *sniffer* capture todos los paquetes emitidos, se transmite información durante 1 minuto usando el programa *Iperf* a la tasa máxima alcanzada por la tarjeta WUSB12 sin intercambio RTS (4.99 Mbps), colocando al *notebook* que corre el *sniffer* en las inmediaciones del AP. Se registra el intercambio de mensajes que se produce entre las estaciones y se verifica que no se producen pérdidas de información en el *sniffer*. Con esta medición se concluye que el *sniffer* captura todos los paquetes transmitidos.

***Validación de los generadores de tráfico.*** Para comprobar que el generador de tráfico *Iperf* no fuese un cuello de botella, se intentó transmitir a una tasa mayor a la que el sistema puede soportar. Para esto, se efectuó una transmisión durante 1 minuto a una tasa de 11[Mbps]. Esta transmisión dio como resultado un *throughput* de 4.98 [Mbps] (comprobado con lo datos entregados por el programa, y de los datos obtenidos del *sniffer*), lo cual resulta en un 45,2% de pérdida de paquetes. Así se

demuestra que el programa generador de tráfico no es una limitante en las mediciones.

***Preparativos para realizar las mediciones.*** Antes de medir el desempeño de las redes inalámbricas, es necesario realizar los siguientes pasos:

**1-** El estándar 802.11b define 11 canales de transmisión, pero sólo un conjunto de 3 de ellos no se traslapan entre sí, los cuales son el 1, 6 y el 11, como se muestra en la figura 7.

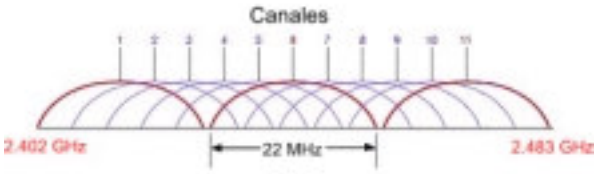


Fig. 7 Disposición de canales en el espectro del protocolo 802.11b.

Se verifica entonces cuál de los canales no traslapados (1, 6, 11) tiene menos interferencias causadas por redes WiFi que operan en las inmediaciones del laboratorio. Para esto, se utiliza el *sniffer*, y se elige el canal que registra menos actividad (en el caso de las mediciones realizadas, afortunadamente se ubicó un canal desocupado).

**2-** Para el experimento que se desea realizar, se debe comprobar que los APs están ocultos entre sí. Esto tiene por objeto simular un escenario de lo que puede ocurrir en un barrio céntrico con varios "*hot-spots".* Así se desea recrear ese escenario en un laboratorio de dimensiones no muy grandes. Para lograr esta recreación en un laboratorio, se introdujeron los AP –envueltos en material electro-magnéticamente absorbente– a cajas de cartón forradas de aluminio, con solamente una pequeña apertura. Se midió la cobertura que cada AP brindaba, reduciendo la potencia de transmisión a modo de poder confinarla a un área pequeña. Para comprobar que los APs no percibían las transmisiones entre sí, se configuró el AP 2 como repetidor, en el mismo SSID (*Service Set Identifier*) del AP1, y, desde el servidor 1 se ejecutó el comando *ping* por un tiempo considerable (app. 10 min.), hacia la dirección IP del AP2. Dado que el AP2 no respondió al *ping*, se verificó que ambos AP se encuentran ocultos, uno respecto del otro.

Se puso un WUSB12 envuelto en material electro-magnéticamente absorbente en la zona de traslape, y el otro en la zona de cobertura del AP1 (ver figura 4). Así se asegura que ambos terminales están ocultos entre sí. Se verificó que existía la comunicación deseada y que el fenómeno del terminal oculto también se presentaba entre los terminales usando un procedimiento similar al de los AP. Estas pruebas se realizaron antes y después de efectuar las mediciones, para asegurar la validez del escenario de pruebas. Esta verificación es importante para asegurar que las condiciones de enlace no se hayan modificado durante la ejecución del experimento.

**3-** Configuración de los APs y tarjetas: se les configura el SSID (area1, area2), IP, y mismo canal para ambos.

**4-** Configuración en STAs y APs el parámetro *RTSThreshold*. Se deja en valor 0 cuando se efectúan mediciones con RTS y se deja en valor 2347 (en realidad, cualquier valor mayor que la máxima trama Ethernet) cuando se efectúa mediciones sin RTS (en ambos, APs y antenas).

## PRUEBAS EXPERIMENTALES Y RESULTADOS

A continuación, se describen los resultados obtenidos cuando se tiene que los dos AP comparten el mismo canal y se tiene una situación descrita en forma esquemática por la figura 4.

Se analiza el desempeño de las transmisiones en el escenario en dos casos: sin activación del mecanismo RTS/CTS (escenario 1) y con ello (escenario 2, figura 8). En este último caso, estando los AP ocultos entre sí, se pueden producir colisiones de paquetes RTS en la STA2. De igual forma, al estar ocultos entre sí STA1 y STA2, los paquetes CTS enviados de una no serán percibidos por la otra.

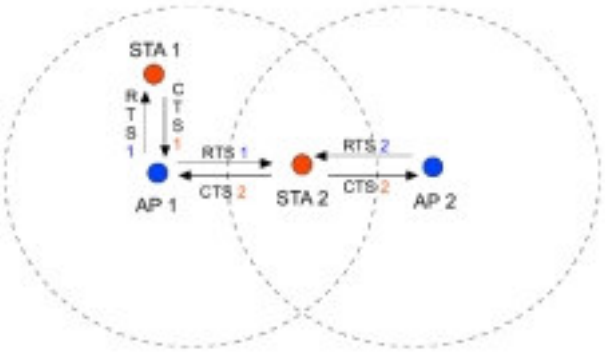


Fig. 8 Intercambio RTS/CTS en el escenario 2.

Se midió el tráfico de bajada. Se hicieron varias mediciones en las cuales se fue variando la tasa de transmisión en el cliente desde 1 [Mbps] hasta 6 [Mbps], y se vio la cantidad de errores en la transmisión en ambos servidores. Se transmitieron paquetes de 1.472 bytes, el umbral de fragmentación se fijó en 1.500 bytes (no hay fragmentación), tanto en AP's como en los terminales se

fijó el valor de la ventana de contienda en CW min de 32 bytes y CW máx de 1024 bytes. Los resultados se detallan a continuación.

De la figura 9 se desprende que cuando se transmite sin la trama RTS, a medida que se aumenta la carga, la tasa efectiva de servicio (*throughput*) para los enlaces es dispar. Esto se produce debido a que la STA2 es cubierta por los dos AP se abstiene de transmitir cada vez que escucha transmisiones propias del enlace 1 (problema del nodo expuesto). En cambio, la STA 1, al no escuchar a la STA 2 (problema nodo oculto), transmitirá como si el canal estuviera a su entera disposición, obteniendo una mayor tasa efectiva de servicio (*throughput*). A pesar de lo anterior, el efecto neto de este escenario no es preocupante, puesto que se alcanza una eficiencia del 87% de la capacidad máxima que pueden alcanzar los adaptadores WUSB12.

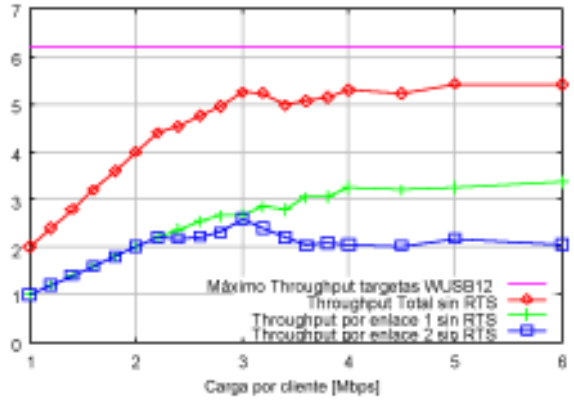


Fig. 9 Throughput promedio por canal vs. carga por cliente, sin RTS.

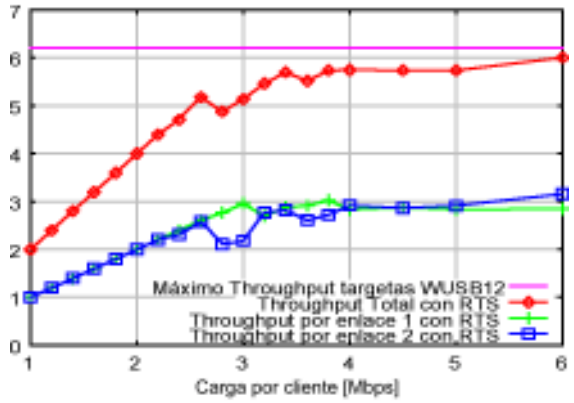


Fig. 10 Throughput promedio por canal vs. carga por cliente, con RTS.

De la figura 10 se desprende que al aumentar la carga por enlace al usar el protocolo RTS/CTS, las transmisiones se equiparan. Además la tasa efectiva total de servicio es ligeramente mayor que en el caso anterior –cerca del 94% de la capacidad máxima alcanzable con las adaptadoras WUSB12– demostrando que el mecanismo es efectivo.

Lo que es evidente de este experimento es que la tasa efectiva de servicio de cada AP queda reducida a la mitad, es decir, cada uno de los proveedores de servicio ve reducida la capacidad de atención de sus clientes en forma significativa, debido a una pobre planificación de frecuencias.

## EFECTO DE CANALES TRASLAPADOS

A continuación, se muestran los resultados que se obtuvieron en un escenario como el de la figura 4, utilizando canales cercanos en ambas celdas. Se utilizaron los mismos valores de CW y tamaño de paquetes del experimento anterior.

Se hicieron transmisiones simultáneas en ambas celdas, en el área 1 se dejó fijo el canal 6 y en el área 2 se fue variando desde el canal 1 hasta llegar al canal 6. Se transmitió a la máxima carga que el sistema pudo aceptar. Para lograr esto, se fue disminuyendo la carga en ambas transmisiones (tomando un valor inicial de 4 Mbps) hasta llegar a un porcentaje de error de paquetes menos al 1%.

Al observar la figura 11 se puede apreciar cómo decae el *throughput* en los enlaces a medida que los canales se traslapan más. Esto era de esperarse, ya que, a medida que aumenta el traslape, mayor será la interferencia de canal adyacente. También se observa que al estar trabajando los dos enlaces en el canal 6, el *throughput* aumenta con respecto al *throughput* anterior. Esto se debe a que al estar operando en el mismo canal, las estaciones pueden detectar las transmisiones existentes y evitar colisiones.

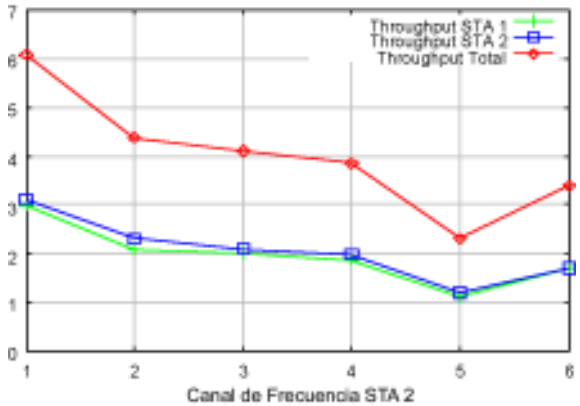


Fig. 11 Throughput promedio por canal v/s canal de frecuencia STA 2, sin RTS.

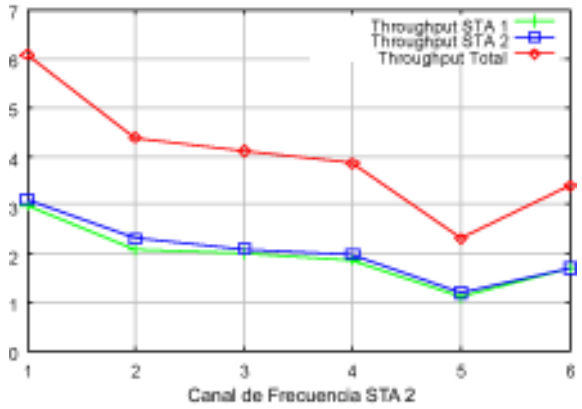


Fig. 12 Throughput promedio por canal v/s canal de frecuencia STA 2, con RTS.

La figura 12 ilustra que el uso del mecanismo RTS/CTS mejora considerablemente la tasa efectiva de servicio de las transmisiones, por la ventaja que implica el que los paquetes RTS (de tamaño mucho menor que los paquetes de datos) sean aquellos que se ven afectados por la interferencia producida por el canal adyacente y no la transmisión del paquete de datos misma.

## CONCLUSIONES

En el escenario analizado se muestran tres problemas básicos en redes inalámbricas modelados: el problema del terminal oculto, el problema del terminal expuesto y el fenómeno de captura. Éste se produce por efectos del mecanismo de *backoff* exponencial con que opera el protocolo en conjunto con el hecho de que los nodos de la red sólo tienen acceso parcial a la actividad que se registra en sus enlaces. Cuando no se utiliza intercambio RTS/CTS entre APs y STAs, en situaciones de alta carga en la red, siempre una STA captura el canal, lo cual conlleva a una mayor tasa de transmisión de esta STA, en desmedro de las otras que estén haciendo alguna transmisión, inclusive hacia otro AP cercano. La solución a este problema es utilizar el intercambio RTS/CTS, ya que en situaciones de alta carga no permite que una STA se apodere del canal, equipando así la tasa de las transmisiones.

Otra conclusión es el no utilizar los mismos canales RF en celdas cercanas, ya que, como se vio en los tres escenarios, se generan problemas de interferencias entre los canales, produciéndose así una baja en el *throughput* de los enlaces.

Con respecto a la utilización de canales traslapados, se puede concluir que es recomendable siempre usar sólo canales no traslapados, ya que si se utilizan canales cercanos, como en las mediciones hechas, se genera una baja en el desempeño de la red. Por lo anterior es recomendable siempre hacer una planificación detallada de redes inalámbricas en los lugares en donde se desee implementar esta tecnología, para obtener el máximo desempeño posible.

## AGRADECIMIENTOS

Este trabajo ha sido posible gracias a aportes parciales del proyecto FDI 01 “Difusión Multimedial Inalámbrica IP” y del proyecto UTFSM 230322 “Modelado Estadístico de Canales Inalámbricos en las Bandas de 2.4 y 3.5GHz” y del proyecto Fondef D00I1048 “Desarrollo de Comunicaciones Multimediales sobre Redes Inalámbricas”. Se agradece, además, la valiosa ayuda de Víctor Cea M. para realizar las mediciones.

## REFERENCIAS

[1] H. Araya. “Análisis de Desempeño del Protocolo IEEE 802.11b en Ambiente WLL”. Tesis para optar al grado de Magíster. Universidad Técnica Federico Santa María. Valparaíso, Chile. Febrero 2003.

[2] V. Cea. “Desarrollo de Experiencias de Laboratorio en torno al Protocolo IEEE802.11b”. Memoria para optar al título de Ingeniero Civil Electrónico. Universidad Técnica Federico Santa María. Valparaíso, Chile. Agosto 2004.

[3] Emerson & Cuming Microwave Products, http://www.eccosorb.com/

[4] D. Guzmán. “Efectos del tamaño de la ventana de colisiones en el desempeño de un sistema WiLL usando el protocolo IEEE802.11”. Memoria para optar al título de Ingeniero Civil Ectrónico. Universidad Técnica Federico Santa María. Valparaíso, Chile. Junio 2004.

[5] IEEE, Supplement to International Standard 802.11: “Wireless LAN Medium Access Control (MAC) an Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band”. IEEE, Inc. 1999.

[6] A. Vasan and U. Shankar. “An Empirical Characterization of Instantaneous Throughput in 802.11bWLANs”. Department of Computer Science. University of Maryland. 2002.