Evaluación del Proceso de Escaneo en Redes 802.11: una perspectiva taxonómica

Laudin Molina Troconis
Núcleo Universitario Alberto Adriani
Universidad de Los Andes
El Vigía, Venezuela
Correo electrónico: laudin@ula.ve

Andrés Arcia-Moret
International Centre for Theoretical Physics (ICTP)
Trieste, Italia
Correo electrónico: aarcia_m@ictp.it

***Resumen*—La actual popularidad de las redes IEEE 802.11 permiten que usuarios nómadas mantengan conectividad a la red. Para que los dispositivos de estos usuarios establezcan conexión a la red, deben ejecutar un proceso de escaneo (o *scanning*), el cual permite reconocer las redes disponibles y sus características, con el fin de seleccionar una red para conectarse. En ciertas situaciones, es bien sabido que el proceso de descubrimiento resulta ser el responsable de la mayor parte del retardo inducido.**

Dentro de la gran cantidad de trabajos en el área, en este artículo se presentan y clasifican los trabajos del estado del arte desde dos grandes perspectivas. La primera está orientada al estudio y evaluación del procesos de escaneo. La segunda, se hace desde la perspectiva de estrategias orientadas a reducir el tiempo de escaneo, y de aumentar su efectividad para optimizar el proceso de *handoff*.

***Palabras Claves*—Redes Inalámbricas, Escaneo, IEEE 802.11, handoff.**

I. Introducción

La tecnología de acceso inalámbrico más popular hoy en día está definida en el estándar IEEE 802.11 [1], que contiene diferentes revisiones, siendo 802.11b y 802.11g las populares para redes de área local. Ambas operan en la misma frecuencia, correspondiente a los 2.4 GHz, que es una frecuencia libre, por lo que en la práctica se encuentran numerosas redes que forman despliegues espontáneos [2] e independientes, es decir, sin coordinación ni planificación central, lo que conlleva a redes con características y configuraciones variables y con los Puntos de Acceso (PA) distribuidos sin un patrón predecible, provocando que las Estaciones Móviles (EM) deban estar preparadas para operar en ambientes caóticos.

El estándar 802.11 [1] define el control de acceso al medio (MAC: *Medium Access Control*) y varias especificaciones de la capa física (PHY: *Physical Layer*) para estaciones móviles pertenecientes a una red inalámbrica de área local (WLAN: *Wireless Local Area Network*). De acuerdo con el estándar, las redes 802.11b/g dividen el espectro en 11 canales (en algunos países pueden ser 13 ó 15), desde 2412 MHz hasta 2462 MHz. En la revisión 802.11b cada canal tiene una longitud de 22 MHz y utiliza la técnica de modulación "espectro ensanchado por secuencia directa" (DSSS: *Direct Sequence Spread Spectrum*). Por su lado, la revisión 802.11g tiene una longitud del canal de 20 MHz y utiliza la técnica de modulación "multiplexación por división de frecuencias ortogonales" (OFDM: *Orthogonal Frequency Division Multiplexing*). En ambos casos las separación entre canales es de 5 MHz, por lo que los canales vecinos están solapados. Debido a las características del medio utilizado y a las pérdidas debido a la propagación, el alcance de las redes locales podría estar limitado unas pocas decenas de metros, aunque podría reducirse a unos pocos metros en presencia de obstáculos.

Una red 802.11 puede configurarse para operar en modo *ad-hoc*, en donde las EM mantienen conexión directamente, o en modo *infraestructura*, que requiere la presencia de un PA encargado de gestionar el acceso a la red y al que deben conectarse todas las EM pertenecientes a la red. En este artículo nos concentramos en las redes de tipo infraestructura.

Para que una EM forme parte de una red debe: escanear los PA disponibles en el entorno, seleccionar el PA al que estará asociado y finalmente realizar el proceso de autenticación y asociación. El descubrimiento puede realizarse utilizando escaneo pasivo o escaneo activo. En el escaneo pasivo la EM está atenta a tramas de tipo administración, denominadas *Beacons*, enviadas periódicamente por los PA, estas tramas contienen información sobre el PA y permiten realizar el proceso de asociación y mantener sincronizadas las estaciones que forman parte de la red. En el escaneo activo, la EM difunde tramas (denominadas *Probe Request*: Preq) en una lista de canales seleccionados y espera por tramas de respuesta (denominadas *Probe Response*: Presp) de los PA que recibieron su solicitud. La Fig. 1 muestra una versión simplificada del escaneo activo descrito en el estándar [1]. Su ejecución es como sigue:

Para cada canal a ser revisado:

- Esperar hasta que el temporizador *Probe Delay* haya expirado o que se reciba notificación de actividad en el canal;
- Realizar el acceso al canal;
- Transmitir un Preq en *broadcast*;
- Iniciar el temporizador *ProbeTimer*;
- Si no se ha detectado actividad en el canal antes que el temporizador alcance *MinChannelTime* (MinCT), entonces reiniciar el proceso en el siguiente canal. Por el contrario, si se ha detectado actividad en el canal, esperar hasta que el temporizador alcance *MaxChannelTime* (MaxCT) y luego procesar los Presp recibidos; que eventualmente formarán parte de la lista de los PA seleccionables.

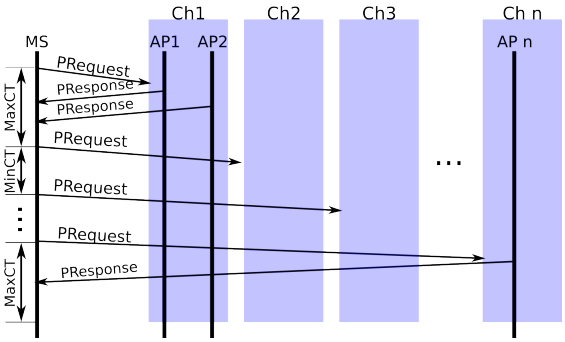

Figura 1: Escaneo activo

- Reiniciar el proceso en el siguiente canal.

El estándar indica que el valor de MaxCT debe ser mayor o igual a MinCT, a su vez MinCT debe ser mayor o igual a *Probe Delay*, permitiendo que estos tres valores sean fijados a discreción por el fabricante de la interfaz 802.11 y/o el diseñador del controlador. En el estudio presentado en [3] se muestra que un ajuste apropiado de estos valores es determinante en la duración y efectividad del proceso de escaneo, razón por la que distintos autores han conducido investigaciones [4]–[8] para determinar los valores óptimos de estos parámetros y la influencia del escaneo sobre otros procesos de red, tales como: conexión a la red y *handoff* de capa 2.

Una aproximación del tiempo empleado por el proceso de escaneo descrito en el estándar [1] corresponde a la presentada por Montavont et al. [9], donde definen MinCT como el tiempo mínimo dedicado a la revisión de cada canal y también el tiempo máximo que toma recibir la respuesta de un PA. Definen MaxCT como el tiempo máximo dedicado en cada canal durante el escaneo, permitiendo a los distintos PA del entorno competir por el acceso al medio y transmitir un Presp.

El proceso de descubrimiento en redes IEEE 802.11 ha sido estudiado desde varias perspectivas por distintos autores. Se destacan las siguientes tendencias:

(a) *Disminución de la duración del escaneo*: Independientemente de la aplicación, esta tendencia agrupa trabajos que proponen una optimización de la configuración del proceso de escaneo a través de la evaluación de las variables. Esto con el único fin de disminuir el tiempo de escaneo.
   - Estudio del proceso de escaneo, donde revisan el proceso de descubrimiento en forma detallada;
   - Caracterización de los algoritmos de escaneo activo de interfaces de red inalámbricas.

(b) *Impacto del escaneo en la asociación*: se refiere a los trabajos que optimizan el proceso de escaneo tomando en cuenta el impacto en la asociación para usuarios nómadas, o durante el *handoff* para usuarios móviles.
   - Optimización del rendimiento del proceso de descubrimiento;
   - El descubrimiento como parte esencial del proceso de *handoff*;
   - Localización de objetos móviles utilizando redes IEEE 802.11.

I-A. Caracterización del escaneo activo

Distintos estudios [10]–[12] han reportado diferencias en las estrategias de escaneo activo utilizadas por interfaces de red 802.11 distintas. Las diferencias incluyen: uso de caché para mantener información del entorno, secuencia de canales explorados, frecuencia de ejecución del proceso de escaneo, posibilidad de interrumpir el escaneo, número de tramas utilizadas durante el proceso, entre otros.

El estudio presentado por Gupta et al. [11] fue de los primeros que evaluaron y caracterizaron las interfaces 802.11 en función del escaneo activo. Es importante destacar que las pruebas presentadas en [11] se realizaron utilizando el sistema operativo Fedora Core 4, kernel Linux versión 2.6.11-1.1369. Éste utiliza el escaneo activo a fin de caracterizar interfaces de red. Para ello centra el estudio en parámetros propios del escaneo activo: canal por el que se transmite el primer Preq, el número total de Preq transmitidos en todos los canales, número de Preq transmitidos por canal y el tiempo que la interfaz permanece revisando un canal. De los resultados presentados se destaca que la revisión de los canales no siempre comienza por el canal 1, ni sigue un orden secuencial monótono (Ch1, Ch2, Ch3, . . . , Ch11), por ejemplo, indican que la combinación de canales 1, 7 y 9 son los primeros en ser revisados en el 75 % de los casos evaluados. También detectaron que, dependiendo del algoritmo de escaneo activo, uno o más Preq pueden ser transmitidos por la EM cuando se está revisando un canal particular.

También reportaron diferencias en el tiempo dedicado a la revisión de cada canal. De acuerdo con los experimentos realizados, las interfaces invierten un mayor tiempo en revisar el canal 6.

Mediante experimentos con una misma interfaz 802.11 y distintos controladores para ésta, infieren que el algoritmo de escaneo activo se encuentra implementado en el controlador, pues cambios en el controlador varían el comportamiento del escaneo activo. Sin embargo, también observaron que, en algunos casos, el uso del mismo controlador pero distintas interfaces de red también lo altera. Todo esto sugiere que el comportamiento del escaneo activo es alterado por distintos factores, entre ellos: el hardware de la interfaz 802.11 y su controlador. .

I-B. Escaneo activo en el kernel de Linux

El kernel de Linux hace uso de un "Framework MAC 80211", que implementa un conjunto de funcionalidades de la capa MAC en el software (en forma de módulos del kernel), de manera que las interfaces 802.11 y sus controladores pueden reutilizar estas funciones y hacer uso de los mismos algoritmos, además cada interfaz tiene la posibilidad de implementar un algoritmo de escaneo particular en el hardware. La implementación de las operaciones MAC en el software es conocido como *SoftMAC* y se encuentra en el módulo "`mac80211.ko`". Entre las funcionalidades implementadas en el módulo está el escaneo activo y pasivo.

El escaneo activo implementado en el kernel de Linux procede según el algoritmo mostrado en la Fig. 2, que, como se observa, varía del algoritmo descrito en la norma [1] y presentado en la Fig. 1. En el kernel se utilizan dos

```
1: for all canal i do
2:    Sintonizar canal i
3:    temporizador = 0
4:    while True do
5:       Recibir Presp
6:       if temporizador = IEEE80211_PROBE_DELAY
         then
7:          break
8:       end if
9:    end while
10:   Transmitir Preq
11:   temporizador = 0
12:   while True do
13:      Recibir Presp
14:      if temporizador = IEEE80211_CHANNEL_TIME
         then
15:         break
16:      end if
17:   end while
18: end for
```

Figura 2: Escaneo en el kernel de Linux

tiempos de espera: `IEEE80211_SCAN_PROBE_DELAY` e `IEEE80211_CHANNEL_TIME`. El primero es el tiempo que espera la EM antes de transmitir el Preq luego que la interfaz ajusta el canal de operación. El segundo es el tiempo que la interfaz permanece a la espera de Presp en cada canal luego de transmitido el Preq.

Los valores de `IEEE80211_PROBE_DELAY` e `IEEE80211_CHANNEL_TIME` dependen de la configuración del kernel y son calculados de acuerdo a Eq. 1 y Eq. 2.

$$\text{IEEE80211\_PROBE\_DELAY} = \text{HZ} / 33 \quad (1)$$

$$\text{IEEE80211\_CHANNEL\_TIME} = \text{HZ} / 33 \quad (2)$$

Donde `HZ` representa la frecuencia de operación del kernel, dado en "tics por segundo", valor establecido al momento de compilar el kernel. De manera que `IEEE80211_PROBE_DELAY` y `IEEE80211_CHANNEL_TIME` corresponden a 30,30 ms en ambos casos.

En las secciones que siguen se discuten los trabajos revisados. En la Sección II los estudios sobre la optimización del proceso de descubrimiento, en la Sección III los trabajos sobre la optimización de los temporizadores usados en el escaneo y en la Sección IV se comentan sobre el proceso de escaneo y su relación con el *handoff*. Finalmente, en la Sección V se presentan las conclusiones.

II. Sobre la optimización del proceso de descubrimiento

En [10] se presenta un estudio detallado del proceso de *handoff* de capa MAC y su duración en redes *in-door*. Dividen los retardos del *handoff* en tres: *Probe Delay*, *Authentication Delay* y *Reassociation Delay*, siendo el *Probe Delay* el correspondiente a la fase de escaneo. En el análisis del escaneo definen *Probe-Wait latency* como el tiempo que la EM espera en cada canal luego de transmitido un Preq, por lo que indican que el *Probe-Wait* debe estar comprendido entre los valores correspondientes a MinCT y MaxCT. A su vez, la duración total t, de revisar N canales deberá estar acotada por la Eq. 3.

$$N_{ch} \times MinCT <= t <= N_{ch} \times MaxCT \quad (3)$$

Los experimentos realizados por [10] consisten de tres redes 802.11b que coexisten en un edificio, una EM y un *sniffer* usado para capturar los paquetes intercambiados por la EM y la red. Realizaron distintas pruebas, cada una caracterizada por el uso de una interfaz 802.11 particular y una de las redes, en total se probaron nueve escenarios combinando tres interfaces de red en la EM (Lucent Orinoco - 7.28.1, Cisco 340 - 4.25.10 y ZoomAir prism 2.5 - 0.8.3) y tres redes. Esto permitió, a través de un estudio empírico, las siguientes conclusiones:

1. El proceso de escaneo ocupa, en las configuraciones presentadas, el 90 % de la duración total del *handoff*;
2. El hardware utilizado en la red (interfaz 802.11 del PA y las EM) afecta significativamente la duración del *handoff*, observándose duraciones que van desde 53,3 ms hasta 420,8 ms, con una diferencia máxima promedio de 367,5 ms;
3. Diferentes interfaces 802.11 presentan distintos algoritmos de escaneo, destacando las siguientes diferencias:
   - La interfaz Cisco transmite once (11) Preq, uno por cada canal, con un tiempo de espera por canal de entre 17 ms, si no se reciben Presp (MinCT) y 38 ms, en caso contrario (MaxCT);
   - La interfaz Lucent transmite solo tres Preq en los canales 1, 6 y 11. Cada uno transmitido a 1 Mbps. El tiempo de espera en cada canal no es identificado claramente, sin embargo, los resultados sugieren una espera de aproximadamente 13 ms en cada canal, independientemente de la presencia o no de Presp;
   - La interfaz ZoomAir, al igual que la Lucent, solo transmite por los canales 1, 6 y 11. En este caso observaron que los tiempos de espera por canal se agruparon alrededor de 63 ms y 73 ms.

En [4] indican que el tiempo de respuesta de los PA depende de la carga de la red y del número de estaciones, razón por la que este tiempo no está acotado, pues el número de PA y la congestión de la red puede aumentar. Así mismo, en [13], se revisa la Eq. 4, que fue introducida por Montavont et. al en [9]. Esta ecuación estima la duración del escaneo completo (S), donde los autores desprecian el valor del temporizador *Probe Delay* presente en el algoritmo descrito en la norma [1], pues lo consideran como un componente pasivo de escaneo activo.

$$S = Ch_o \times T_o + Ch_v \times T_v \quad (4)$$

S es el tiempo que ocupa revisar todos los canales, es decir, la duración del escaneo completo o *full scanning*;

Ch_o se refiere a la cantidad de canales con actividad, es decir, ocupados;

T_o es el tiempo que ocupa revisar un canal con actividad;

Ch_v representa la cantidad de canales sin actividad, es decir, desocupados;

T_v es el tiempo que ocupa revisar un canal sin actividad.

Asumiendo que $T_v = MinCT$ y $T_o = MaxCT$, analizan la influencia del escaneo activo en la duración del *handoff* y mencionan tres intervalos de tiempo que consideran improductivos:

1. Cuando una EM detecta actividad en un canal pero sin obtener Presp se desperdicia $MinCT$;
2. Cuando la EM revisa un canal vacío se desperdicia $Probe\,Delay + MinCT$;
3. Por último el tiempo que transcurre desde que se recibe el último Presp hasta que se cumple MaxCT. En este caso se desperdicia un intervalo dependiente de cada situación.

En [3] los autores estudian el impacto de MinCT y MaxCT sobre la efectividad y duración del escaneo activo. Definen dos métricas para describir el escaneo activo: falla total de escaneo (*full scanning failure*) y retardo total de escaneo (*full scanning latency*). La primera se refiere a la imposibilidad para descubrir algún PA luego de revisar todos los canales del espectro, la segunda indica el tiempo que ocupa realizar la revisión de todos los canales disponibles. El retardo total de escaneo se expresa en la Eq. 5, que relaciona MinCT, MaxCT y la probabilidad $P(ch)$ de actividad en el canal ch.

$$L = \sum_{ch=1}^{n} (1 - P(ch)) \times MinCT + P(ch) \times (MinCT + MaxCT) \quad (5)$$

En [13] los autores realizan simulaciones del escaneo activo, variando los valores de MinCT y MaxCT y en distintas condiciones del entorno (número, canal de operación y disposición de los PA). Concluyeron que no es posible tener un par de valores, para MinCT y MaxCT, que sean óptimos para todo escenario, esto es debido a que modificaciones en el despliegue de la red provocan cambios impredecibles en los tiempos de respuesta de los PA. Los resultados son confirmados en [3], donde realizaron pruebas experimentales con distintas configuraciones de despliegues de PA para simular condiciones reales, tales como: la interferencia, solapamiento de canales y la presencia de tráfico en la red. Como resultado de los experimentos determinaron los siguientes intervalos para los temporizadores MinCT y MaxCT:

$$6\,ms \leq MinCT \leq 34\,ms \quad (6)$$

$$8\,ms \leq MaxCT \leq 48\,ms \quad (7)$$

que abarcan el conjunto de valores óptimos para las distintas configuraciones evaluadas. Los intervalos se estimaron en función del tiempo que toma recibir la primera y la última respuesta a un Preq.

Otro resultado presentado en [3] indica que la presencia o no de tráfico en la red altera considerablemente el tiempo de respuesta de los PA, por ejemplo, en un despliegue ideal donde solo se tiene un PA en los canales no solapados y sin tráfico en la red obtienen un Presp antes de 6 ms en el 87 % de los experimentos, mientras que al introducir tráfico en la red solo el 43 % de las respuestas es obtenida antes de 6 ms.

Tomando en cuenta los estudios presentados en esta sección y luego de la revisión de distintos trabajos, se pueden diferenciar varias estrategias para optimizar el proceso de descubrimiento de redes 802.11. De acuerdo con Eq. 3 y Eq. 5, para reducir el retardo total de escaneo se deben disminuir el número de canales a revisar y los valores tomados por MinCT y MaxCT, a riesgo de no descubrir una parte del entorno. Otras estrategias consisten en predecir la configuración del entorno o la ejecución por etapas del algoritmo de escaneo.

III. Optimización de los temporizadores del escaneo

Tal como se observa en la Eq. 3 y la Eq. 5, la duración de un escaneo activo es influenciado por los valores de MinCT y MaxCT. Varios trabajos han propuesto y evaluado estrategias de optimización en base a MinCT y MaxCT.

A continuación se presentan dos tipos de estrategias que proponen la optimización de los temporizadores que controlan el proceso de escaneo.

III-A. Estrategias estáticas

En [4] los autores estudian técnicas para reducir la duración del *handoff* en redes 802.11b. En el trabajo se divide el *handoff* en tres etapas: detección, búsqueda y ejecución. La detección consiste en el proceso que permite a la EM conocer que es necesario iniciar el proceso de *handoff*. La búsqueda permite que la EM conozca los PA disponibles en el entorno. Finalmente, durante la ejecución, la EM selecciona uno de los PA del entorno y establece un nuevo enlace con este último. La búsqueda se refiere a la ejecución del proceso de descubrimiento de los PA, que por lo general se realiza mediante el escaneo activo. Los autores proponen reducir la duración de esta fase a través de un apropiado ajuste de los valores de MinCT y MaxCT. Mediante consideraciones teóricas y simulaciones establecen valores para MinCT y MaxCT. MinCT es calculado como el tiempo máximo requerido por un PA para responder un Preq dado que el PA y el canal se encuentran desocupados. Si se desprecia el tiempo de generación de Preq y Presp, MinCT corresponde al tiempo que el PA debe esperar para acceder al medio. Éste es calculado en la Fig. 3, donde DIFS se refiere al espacio inter-tramas de la función de coordinación distribuida (*Distributed Coordination Function Inter-Frame Space*, $CWmin$ es el tamaño mínimo de la ventana de contención en número de *slots* y $SlotTime$ es la duración de cada *slot* en microsegundos [1]. Los autores de [4] concluyen que MinCT debe ser 1 TU[1].

El valor de MaxCT es el tiempo de espera máximo cuando el canal se encuentra ocupado, por lo que no es un valor constante y depende del uso del medio y de la cantidad de PA que se encuentre compitiendo. En [4] realizan simulaciones para estimar el valor de MaxCT. Sugieren que 10 TU (10,24 ms) para MaxCT es un valor razonable que prevendría obtener respuesta de los PA sobrecargados.

[1]TU: *Time Unit*, unidad usada en el estándar y correspondiente a $1024\,\mu s$

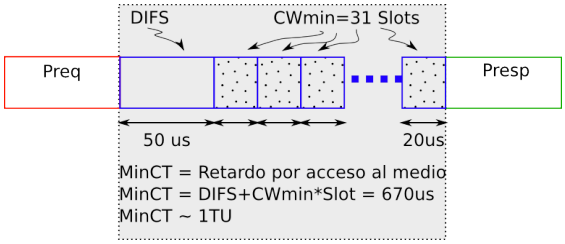

Figura 3: MinCT para redes IEEE 802.11b

Los trabajos presentados en [8] y [7] establecen valores aún menores para MaxCT, fijándolo en 5 ms el primero y 6 ms el segundo. En [8], muestran el resultado de múltiples mediciones de los tiempos de respuesta de los PA bajo distintas condiciones: sin tráfico, con tráfico TCP desde y hacia el PA y con tráfico UDP desde y hacia el PA. En promedio, el tiempo de respuesta de un PA ante un Preq es de 2 ms y el máximo observado es de 4 ms, por lo que ajustan MaxCT a 5 ms para garantizar que se reciben la mayor parte de los Presp. Estos resultados contrastan con otros estudios, particularmente los presentados en [7], que indica que alrededor del 40 % de todas las respuestas de los PA se reciben en 11 ms y el 98 % en 50 ms. La razón de la diferencia podría deberse a las condiciones en que se realizaron los experimentos, particularmente al número de PA operando, pues las pruebas experimentales reportadas en [8] se realizaron en una oficina con solo dos PA en operación, mientras que en [7] se realizaron en un campus universitario, donde se reportó la presencia de diez PA en promedio. Sin embargo, los resultados indican que los PA con buena señal, esto es, con indicador de fuerza de señal de recepción (RSSI: Received Signal Strength Indicatior) superior a -75 dBm, responden de primero con probabilidad igual a 0,487 y de estar entre las tres primeras respuestas con probabilidad igual a 0,902. En promedio, el tiempo de respuesta de los PA con buena señal es de 6,054 ms con una desviación estándar de 1,58 ms. Tomando en cuenta estos datos, [7] utiliza 6 ms para MaxCT. En [6] se realizan simulaciones y pruebas en ambientes controlados en donde estudian los valores de MinCT y MaxCT. Los autores de [6] determinaron que los valores de MinCT y MaxCT deben pertenecer a los intervalos [6 ms; 34 ms] y [8 ms; 48 ms] respectivamente. Para obtener estos valores, los autores midieron el retardo del primer y los siguientes Presp recibidos en cada canal y con diferentes configuraciones del despliegue de los PA. La principal observación de los experimentos realizados en [6] indica que el desempeño del proceso de descubrimiento es afectado por características propias del despliegue, tales como distribución de los canales y cantidad de tráfico presente.

III-B. Estrategias dinámicas

Otra posible estrategia, presentada en [3] y discutida ampliamente en [14], consiste en ajustar dinámicamente, durante el proceso de escaneo, los valores de MinCT y MaxCT. El objetivo del método presentado consiste en reducir el tiempo dedicado a la revisión de cada canal (reducir MinCT y MaxCT) a medida que se avanza en los canales y se descubren PA. De forma análoga, los valores de MinCT y MaxCT son incrementados en la medida en que no se detecten PA. La ejecución del algoritmo es como se muestra en la Fig. 4,

1: N = número de PA descubiertos en el canal i
2: Q = mayor señal de entre los PA encontrados en el canal i
3: Fijar valores iniciales para MinCT y MaxCT
4: **for all** Canal i **do**
5: Explorar canal i
6: **if** $N = 0$ **then**
7: Incrementar los valores de MinCT y MaxCT en ΔT
8: **else**
9: Decrementar los valores de MinCT y MaxCT según $R(Q, N)$
10: **end if**
11: **end for**

Figura 4: Escaneo dinámico [3]

donde los valores de MinCT y MaxCT son incrementados simultáneamente en $\Delta T = 50\,\%$ de últimos valores exitosos (valores de MinCT y MaxCT donde se detectó al menos un PA), mientras que el decremento es determinado por una función dada $R(Q, N)$ que valora las condiciones del entorno. Los autores sugieren entonces, una correlación entre el tráfico de los canales.

Los resultados mostrados indican que la falla total de escaneo se mantiene por debajo del 2 % y los valores del retardo total de escaneo varían entre 190 ms y 434 ms.

IV. El rol del escaneo en el proceso de handoff

Hasta ahora hemos discutido sobre la optimización del proceso de escaneo tomando en cuenta solamente los temporizadores que lo controlan. En esta sección, discutiremos sobre las consideraciones en el algoritmo de escaneo cuando se toma en cuenta como parte de un proceso de handoff o de asociación.

IV-A. Escaneo periódico

Como se ha mencionado, una EM que realiza un escaneo activo revisa los canales del espectro que sean indicados al momento de invocarlo; uno después del otro sin interrupciones, por lo que durante el proceso la interfaz de red no puede enviar ni recibir tramas, es decir, se interrumpe la conexión. El *escaneo periódico* consiste en agrupar los canales del espectro en subgrupos de unos pocos canales e intercalar la revisión de unos pocos canales con la transmisión/recepción de tramas de capa 2, esto evita que las interrupciones en el servicio de red sean muy largas, en su lugar se tienen múltiples interrupciones de duración menor.

En [9] discuten esquemas de escaneo con el fin de disminuir la duración del *handoff*, una de las propuestas presentadas consiste en realizar el proceso de escaneo en forma periódica, con cada fase revisando un canal durante exactamente MinCT. El objetivo de esta estrategia es encontrar los PA disponibles antes de iniciar el *handoff* y mientras la EM mantiene conexión. El escaneo anticipado permite construir una lista de los PA disponibles. En la lista se mantiene el identificador del PA (dirección MAC), el canal en el que está operando y el SSID (*Service Set Identifier*).

En el proceso descrito en [9], la EM inicia una fase del escaneo usando dos periodos distintos. Estos periodos dependen de la calidad de la señal del PA con el que mantiene la conexión actual. Si la señal es suficientemente buena ([-50 dBm; -75 dBm]), la EM elige un número aleatorio entre 1 y 2 segundos. Cuando la señal tiene un valor menor a -75 dBm y si aún no se tienen PA candidatos en la lista, el periodo toma un valor entre 200 y 300 ms, de esta manera se acelera el proceso de descubrimiento. Si la EM descubre al menos un PA durante el escaneo anticipado, el periodo se vuelve a fijar a los valores iniciales, es decir, 1 ó 2 segundos.

Cuando la EM requiere asociarse a un PA comienza consultando la lista que se obtuvo durante el escaneo anticipado, si la lista está vacía o no es posible asociarse con los PA de la lista se inicia el proceso de escaneo activo descrito en el estándar.

En Liao y Gao [15] se presenta una estrategia denominada *smooth scanning* para buscar minimizar los efectos del retardo del descubrimiento en la ejecución del *handoff*. La operación de escaneo es dividida en múltiples subfases, separadas por suficiente tiempo como para permitir la transmisión de tramas de datos entre dos subfases. Para los autores, tener múltiples subfases implica que el tiempo global para revisar el total de canales del espectro (escaneo completo) será grande, por lo que si se tiene una EM en movimiento, es posible que al finalizar todas las subfases se tenga información desactualizada. Una EM en movimiento tendría suficiente tiempo para revisar todos los canales si se mueve a una velocidad modesta, por ejemplo, si la duración del escaneo completo es de 2 s y la EM se desplaza a velocidad de peatón (unos 1,5 m/s), entonces la EM se desplazará unos 3 m, por lo que este método puede ser efectivo si los PA presentan un solapamiento de más de 3 m.

La estrategia presentada en [8], similar al *smooth scanning*, es utilizada durante el *handoff* en redes 802.11. Los autores descubren el entorno utilizando escaneo activo dividido en fases con una duración variable, intercaladas con actividad que permite tráfico en la interfaz. El intervalo de cada escaneo es adaptado de forma dinámica para evitar la sobrecarga de la red y al mismo tiempo actualizar la información del entorno oportunamente. Adicionalmente, la estrategia es mejorada gracias al uso de una lista de canales organizada por prioridad. Esta lista contiene información de todos los canales en los que existen PA y esos PA utilizan el mismo SSID que el del PA actual. De igual manera, los PA con los que la EM ha mantenido conexión también son registrados.

En [16] y [17] la duración de las subfases del *smooth scanning*, es ajustada dinámicamente a fin de mantener una calidad de servicio de forma que las interrupciones de la red no sean percibidas por el usuario. La solución presentada en [16] y [17] se aprovecha del buffer con que cuentan los distintos elementos de una red. Así, la EM realiza subfases del escaneo activo mientras las aplicaciones que hacen uso de la red mantienen datos en los buffers, una vez que las estaciones vacían el buffer el escaneo es interrumpido para permitir el uso de la red y así llenar los buffers nuevamente. En caso de que la conexión se vea interrumpida porque no se mantiene conexión con ningún PA o porque la señal del PA con el que se mantiene conexión es muy baja, entonces se ejecuta el escaneo completo.

Podemos decir entonces que todos los enfoques que hacen uso de *smooth scanning* pretenden minimizar el impacto del escaneo como una de las fases del *handoff*.

IV-B. Escaneo selectivo

Como se mencionó en las secciones anteriores, durante un escaneo activo la EM debe revisar los canales del espectro que sean especificados al momento de invocarlo, o la totalidad de los canales disponibles; comportamiento que se conoce como escaneo completo. Una forma de acelerar el escaneo activo consiste en reducir la cantidad de canales a revisar, estrategia que se denominará *escaneo selectivo*.

En [18], los autores discriminan los canales a revisar. El método sugerido utiliza una máscara que indica los canales en los que se ha detectado actividad recientemente. La máscara es construida durante el proceso de descubrimiento. En búsquedas sucesivas solo se revisan los canales indicados en la máscara. El proceso es el siguiente:

1. Cuando la interfaz es inicializada se realiza un escaneo completo, en donde se envía un Preq por cada canal y se espera por respuesta de los PA (Presp);
2. Los canales en los que se recibe al menos un Presp son marcados encendiendo el bit correspondiente en la máscara. Los bits correspondientes a los canales 1, 6 y 11 siempre se encuentran encendidos debido a que son canales no solapados y han mostrado alta probabilidad de presencia de PA;
3. Se selecciona el mejor de entre los PA encontrados. Los autores de [18] califican los PA de acuerdo al nivel de la señal recibida (nivel de RSSI);
4. El canal en el que opera el PA seleccionado se remueve de la máscara, es decir, el bit correspondiente es desactivado. Esta operación se realiza debido a que consideran que la probabilidad de encontrar PA adyacentes y operando en el mismo canal son bajas;
5. Si no es posible seleccionar un PA, la máscara es invertida a nivel lógico y repiten los pasos 2, 3 y 4;
6. Si luego de los pasos anteriores aún no es posible seleccionar un PA, ejecutar el escaneo completo, es decir, revisar todos los canales del espectro.

De acuerdo con los resultados presentados por los autores, se mejora considerablemente el impacto del escaneo en otros procesos, tales como el *handoff*, en donde se observa una reducción del retardo de 40 %, en promedio, respecto al escaneo activo definido en el estándar. La estrategia anterior es combinada con el uso de un caché con información de los PA y su entorno. De acuerdo con los autores, combinando estas dos estrategias la duración del *handoff* es de 3 ms en promedio, siempre que se haga hit en el caché en la primera búsqueda. La penalización por fallo de caché (*cache miss*) es de 6 ms, lo que implica que si se incurre en los dos fallos de caché la duración del escaneo activo es de 12 ms más el tiempo que toma ejecutar el escaneo selectivo.

La información del caché se mantiene en una tabla que utiliza la dirección MAC del PA actual (PA al que se encuentra conectada la EM) como campo clave. Luego, cada entrada en la tabla contiene una lista de las direcciones MAC de los PA adyacentes al PA actual y que fueron descubiertos durante los escaneos selectivos realizados previamente. Esta lista es

creada por la EM a medida que se desplaza por el entorno y realiza *handoff* de un PA a otro. La tabla que contiene el caché está limitada a 10 filas y 2 columnas, por lo que la EM mantendrá información sobre el entorno de los últimos 10 PA con la que estuvo conectado, y en cada caso solo los 2 PA con mejor señal serán registrados. El caché es aprovechado de la siguiente manera:

1. Cuando la EM se asocia a un PA, el PA y la información del entorno (otros PA junto con el nivel de la señal) es almacenada en la tabla;
2. Cuando se necesita realizar un escaneo, primero se revisan las entradas en el caché que corresponden con el entorno actual (entorno del PA actual);
3. Si no se logra encontrar un PA, entonces se realiza el escaneo selectivo descrito anteriormente;

Una estrategia diferente es presentada en [19], que propone utilizar la probabilidad de que un PA se encuentre operando en el canal C para determinar la secuencia en que se deben revisar los canales del espectro. En [19] el orden en que se realiza la revisión de los canales resulta crítico, pues el escaneo presentado termina cuando se encuentra un PA que provea conectividad. Bajo condiciones encontradas en la práctica, en donde los PA se distribuyen principalmente en los canales no solapados 1, 6 y 11, la estrategia presentada en [19] encuentra un PA disponible luego de revisar 3.64 canales en promedio.

IV-C. Uso de grafos de vecindario

Otra propuesta para discriminar los canales del espectro y predecir el entorno consiste en construir grafos de vecindario (GV), que contienen la información del entorno. Los GV son grafos no dirigidos, en cuyas aristas se representan los PA y en los enlaces se representa la ruta de movilidad posible entre los PA. Existen varias maneras de implementar GV en redes inalámbricas. En forma centralizada, donde existe un GV global que es almacenado en un servidor central, en esta implementación todos los eventos sobre descubrimiento son reportados y consultados al servidor GV. En forma distribuida, cada PA mantiene un GV con la información de su entorno, es decir, mantiene una lista de los PA vecinos. Las estaciones obtienen el GV local del PA actual una vez que se ha establecido el enlace. Durante un *handoff*, las EM transmiten información sobre el PA anterior al PA actual, de esta manera el PA actual es capaz de conocer la información de los PA a su alrededor y al mismo tiempo construir el GV que le corresponde. Cuando una EM establece un enlace con un PA, éste le transfiere información sobre el entorno, de esta manera la EM está preparada con información del entorno que podría serle útil en la ejecución de nuevos escaneos. El problema central de estas técnicas radica en que cada PA debe descubrir y mantener registro de las características de su entorno, lo que implica modificaciones en la funcionalidad y forma de operación de los PA. Esto puede resultar inviable, pues las redes encontradas en ciudad presentan características de despliegues espontáneos, donde la administración es realizada en forma descentralizada y sin coordinación y con los PA de modelo, hardware y software diferente [20].

En [5] utilizan un GV global que mantiene información de toda la red en la EM. Gracias al GV, la EM tiene conocimiento sobre el entorno, por lo que los canales a revisar y el tiempo de espera en cada canal puede ser optimizado aprovechando la información del GV. En el algoritmo presentado en la Fig. 5 se describe el proceso presentado en [5], que modifica el algoritmo de escaneo completo para hacer uso del GV.

```
1: for all Canal i donde existen PA en el entorno do
2:    Difundir Preq en el canal i
3:    Iniciar temporizador
4:    while True do
5:       Recibir Presp
6:       if Se recibió Presp antes de que MinCT expire then
7:          break
8:       else if Los PA del canal i respondieron then
9:          break
10:      else if MaxCT expiró then
11:         break
12:      end if
13:   end while
14: end for
```

Figura 5: Escaneo utilizando GV

En [21] se presenta una estrategia similar a la descrita en [5], pero sugiere aprovechar la información almacenada en los GV para transmitir los Preq utilizando *unicast* en lugar de *broadcast*.

Otra modificación a la estrategia de los GV, denominada *GV-Podado* y propuesta en [5], consiste en recolectar información sobre el solapamiento o no de los PA, es decir, los PA que no pueden ser alcanzados simultáneamente por una EM. Según esta estrategia, si PA_i y PA_j son no solapados y se recibe un Presp de PA_i, entonces es imposible recibir Presp de PA_j. Utilizando esta información es posible reducir el tiempo de espera en cada canal e inclusive el número de canales a revisar. Los resultados obtenidos en [5] indican mejoras respecto al algoritmo escaneo completo de 80,7 % y 83,9 % para las estrategias GV y GV-Podado respectivamente.

En [9] presentan y evalúan una estrategia denominada "PA Adyacentes". Ésta se basa en el hecho de que cada PA conoce su entorno, por lo que puede identificar los PA que le son adyacentes. Cuando las redes son desplegadas, los PA pueden ser configurados con una lista de los PA adyacentes en términos de área de cobertura. Esta información es mantenida por la lista de PA vecinos y es transmitida a las estaciones. Luego, la EM tiene información sobre el entorno y en caso de requerir cambiar de PA; durante un *handoff* por ejemplo, primero intentará asociarse con los PA de la lista de adyacentes, si la asociación fracasa con todos los PA de la lista, entonces se ejecuta el proceso de descubrimiento descrito en el estándar.

V. CONCLUSIONES

Desde los primeros pasos de las tecnologías IEEE 802.11 se documentan trabajos que buscan estudiar y optimizar el proceso de descubrimiento, algunos modelos teóricos que describen la duración y efectividad del descubrimiento han sido documentados, lo que ha permitido profundizar en estudios teóricos y empíricos. Los primeros estudios realizados presentaron valores teóricos para los temporizadores utilizados en el proceso de descubrimiento y en la duración total del

proceso, estos fijan el valor de MinCT en 1 TU debido al tiempo de respuesta mínimo de un PA, sin embargo, estudios posteriores mostraron que el tiempo de respuesta de un PA es susceptible a la ocupación del canal, la potencia de la señal y a las características del dispositivo, por lo que otros autores documentan valores en rangos que van en los intervalos [6ms, 34ms] para MinCT y [5ms, 48ms] para MaxCT. Todo esto sugiere que distintos escenarios requieren tratamientos diferentes y que no se tienen valores óptimos que sean universalmente válidos, por lo que también se ha propuesto ajustar dinámicamente los temporizadores. Otras propuestas apuntan a la reducción del número de canales a revisar e inclusive a revisar los canales de acuerdo a un orden calculado en función de experiencias previas, utilizando para ello grafos, caché y modelos probabilísticos.

Actualmente, las redes IEEE 802.11 siguen aumentando en número y popularidad entre los dispositivos móviles, por lo que nuevos usuarios demandan mayor nivel de satisfacción al tiempo que aparecen nuevas posibilidades. Así pues, son necesarios nuevos estudios que profundicen la relación entre los distintos factores presentes en las redes y el descubrimiento y que permitirán el desarrollo de nuevas y eficientes estrategias para el escaneo de redes. En trabajos futuros se espera identificar y evaluar condiciones del entorno que afecten el proceso de descubrimiento, particularmente el intercambio de tramas realizado, esto permitirá explorar algoritmos de descubrimiento que ajusten los parámetros identificados en función de las condiciones del entorno.

AGRADECIMIENTOS

Los autores desean agradecer al Consejo de Desarrollo Científico, Humanístico, Tecnológico y de las Artes (CDCH-TA) de la Universidad de Los Andes por el financiamiento a través del proyecto I-1369-13-02-B.

REFERENCIAS

[1] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, http://standards.ieee.org/about/get/802/802.11.html, IEEE Estándar 802.11, 2007.

[2] A. Akella, G. Judd, S. Seshan, y P. Steenkiste, "Self-management in chaotic wireless deployments," en *Proceedings of the 11th annual international conference on Mobile computing and networking*, ser. MobiCom '05. New York, NY, USA: ACM, 2005, pp. 185–199.

[3] G. Castignani, A. Arcia, y N. Montavont, "A study of the discovery process in 802.11 networks," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 15, pp. 25–36, March 2011.

[4] H. Velayos y G. Karlsson, "Techniques to reduce the IEEE 802.11b handoff time," *2004 IEEE International Conference on Communications IEEE Cat No04CH37577*, vol. 00, no. c, pp. 3844–3848, 2004.

[5] M. Shin, A. Mishra, y W. A. Arbaugh, "Improving the latency of 802.11 hand-offs using neighbor graphs," en *Proceedings of the 2nd international conference on Mobile systems, applications, and services*, ser. MobiSys '04. New York, NY, USA: ACM, 2004, pp. 70–83.

[6] G. Castignani, A. Arcia-Moret, y N. Montavont, "An evaluation of the resource discovery process in ieee 802.11 networks," en *Proceedings of the Second International Workshop on Mobile Opportunistic Networking*, ser. MobiOpp '10. New York, NY, USA: ACM, 2010, pp. 147–150.

[7] J. Teng, C. Xu, W. Jia, y D. Xuan, "D-scan: Enabling fast and smooth handoffs in AP-Dense 802.11 wireless networks," *IEEE INFOCOM 2009 The 28th Conference on Computer Communications*, vol. 9041350, no. 2007, pp. 2616–2620, 2009.

[8] H. Wu, K. Tan, Y. Zhang, y Q. Zhang, "Proactive scan: Fast handoff with smart triggers for 802.11 wireless LAN," *IEEE INFOCOM 2007 26th IEEE International Conference on Computer Communications*, pp. 749–757, 2007.

[9] N. Montavont, J. Montavont, y T. Noel, "Enhanced schemes for L2 handover in IEEE 802.11 networks and their evaluations," en *IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications PIMRC*, vol. 3. RSM - Dépt. Réseaux, Sécurité et Multimédia (Institut Mines-Télécom-Télécom Bretagne-UEB), LSIIT - Laboratoire des sciences de l'image, de l'informatique et de la télédétection (CNRS UMR 7005), 2005, pp. 1429 – 1434.

[10] A. Mishra, M. Shin, y W. Arbaugh, "An empirical analysis of the IEEE 802.11 MAC layer handoff process," *SIGCOMM Comput. Commun. Rev.*, vol. 33, no. 2, pp. 93–102, Abril 2003.

[11] V. Gupta, R. Beyah, y C. Corbett, "A characterization of wireless NIC active scanning algorithms," en *WCNC*. IEEE, 2007, pp. 2385–2390.

[12] T. King y M. B. Kjærgaard, "Composcan: adaptive scanning for efficient concurrent communications and positioning with 802.11," en *Proceedings of the 6th international conference on Mobile systems, applications, and services*, ser. MobiSys '08. New York, NY, USA: ACM, 2008, pp. 67–80.

[13] G. Castignani y N. Montavont, "Adaptive discovery mechanism for wireless environments," en *14th Eunice Open European Summer School*. RSM - Dépt. Réseaux, Sécurité et Multimédia (Institut Mines-Télécom-Télécom Bretagne-UEB), 2008.

[14] G. Castignani, "Exploiting network diversity," Disertación de Ph.D., Télécom Bretagne - Université Européene de Bretagne, 2012.

[15] Y. Liao y L. Gao, "Practical schemes for smooth mac layer handoff in 802.11 wireless networks," en *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*, ser. WOWMOM '06. Washington, DC, USA: IEEE Computer Society, 2006, pp. 181–190.

[16] J.-W. Nah, S.-M. Chun, S. Wang, y J.-T. Park, "Adaptive handover method with application-awareness for multimedia streaming service in wireless LAN," en *Proceedings of the 23rd international conference on Information Networking*, ser. ICOIN09. Piscataway, NJ, USA: IEEE Press, 2009, pp. 1–7.

[17] J.-T. Park, J.-W. Nah, S. Wang, y S.-M. Chun, "Context-aware mobility management with energy efficiency for multimedia streaming service in wireless LAN," en *Proceedings of the 6th IEEE Conference on Consumer Communications and Networking Conference*, ser. CCNC09. Piscataway, NJ, USA: IEEE Press, 2009, pp. 1332–1337.

[18] S. Shin, A. G. Forte, A. S. Rawat, y H. Schulzrinne, "Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs," en *Proceedings of the second international workshop on Mobility management & wireless access protocols*, ser. MobiWac '04. New York, NY, USA: ACM, 2004, pp. 19–26.

[19] J. Eriksson, H. Balakrishnan, y S. Madden, "Cabernet: vehicular content delivery using wifi," en *Proceedings of the 14th ACM international conference on Mobile computing and networking*, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 199–210.

[20] L. Molina, A. Arcia-Moret, G. Castignani, y N. Montavont, "Caracterización de despliegues espontáneos IEEE 802.11," en *Memorias del 5to Congreso Iberoamericano de Estudiantes de Ingeniería Eléctrica*, ser. Cibelec '12, 2012.

[21] S.-H. Park, H.-S. Kim, C.-S. Park, J.-W. Kim, y S.-J. Ko, "Selective channel scanning for fast handoff in wireless lan using neighbor graph," en *Personal Wireless Communications*, ser. Lecture Notes in Computer Science, I. Niemegeers y S. de Groot, Eds. Springer Berlin / Heidelberg, 2004, vol. 3260, pp. 629–629.