Universidad de Los Andes
Facultad de Ingeniería
División de Estudios de Postgrado
Postgrado en Computación

Estudio del descubrimiento de topologías espontáneas en redes 802.11

Autor: Ing. Laudin Alessandro Molina Troconis
Tutor: Dr. Andrés Arcia Moret — Universidad de Los Andes
Cotutor: Dr. Nicolas Montavont — Telecom Bretagne

Trabajo de grado presentado ante la ilustre Universidad de Los Andes como requisito parcial para optar al grado de *Magíster Scientiae* en Computación.

Mérida, julio de 2014

Agradecimientos

Al profesor Andrés Arcia Moret, por sus revisiones y consejos, por ser guía y por fomentar mi formación profesional.

Al profesor Nicolas Montavont, por su guía y asesoría a lo largo de toda la fase experimental.

A la profesora María Gabriela Viloria, porque su apoyo me concedió tiempo de calidad para ejecutar la fase experimental.

A German Castignani, Alberto Blanc y Tanguy Kerdonkuff por sus revisiones, ideas y comentarios.

A los jurados evaluadores, la profesora María Villapol y el profesor Nelson Pérez, por tomarse el tiempo de revisar el trabajo y sugerir diferentes mejoras.

A la Universidad de Los Andes, por permitirme realizar este trabajo y co-financiar mis estudios.

A Telecom Bretagne, por recibirme y co-financiar la estadía donde se ejecutó la fase experimental.

Al CDCHTA de la Universidad de Los Andes, por su financiamiento mediante el proyecto I-1412-14-02-EM.

A Layla, porque se divirtió una mañana revisando la monografía y listando varios errores.

A Neis, por su compañía y paciencia durante la fase experimental y la recolección de datos en despliegues reales.

Resumen

Las redes bajo el estándar IEEE 802.11 son la tecnología de acceso inalámbrico más popular hoy día, con grandes despliegues en los principales centros urbanos del mundo, los cuales son realizados en forma descentralizada, resultando en topologías irregulares y con altas densidades. Esto incrementa la complejidad del proceso que permite que una estación móvil conozca las redes disponibles en un entorno, denominado descubrimiento de redes.

En este trabajo, se describe una metodología para caracterización de redes IEEE 802.11, haciendo énfasis en la medición del tiempo de respuesta de los puntos de acceso (AP: *Access Points*). El método registra, en el kernel, el intercambio de tramas *Probe Request — Probe Response*, así como los *Beacons* transmitidos por la estación móvil y los AP. Haciendo uso de este método, se presenta una descripción del despliegue encontrado en la ciudad de Rennes, Francia, que se considera espontáneo. Así mismo, también se analiza el proceso de descubrimiento en entornos desplegados de manera espontánea.

Los estudios realizados indican que es posible descubrir más de 75 redes en una localización, donde las estrategias de escaneo activo tradicionales, orientadas a escenarios de baja escala, solo son capaces de descubrir una fracción del total. Con objeto de descubrir la topología completa se necesitan los resultados parciales de múltiples y secuenciales escaneos, lo que plantea la necesidad de un sistema centralizado que asista el proceso de descubrimiento, almacenando información sobre la topología presente en las distintas zonas de un despliegue.

Palabras claves: Escaneo, redes IEEE 802.11, despliegues espontáneos.

Índice general

Capítulo 1

Introducción

Las redes inalámbricas IEEE 802.11 [1] se han convertido en la tecnología de acceso a Internet más común en la actualidad. Las estaciones de usuario de hoy en día, denominadas estaciones móviles (MS: *Mobile Stations*) en el estándar, tales como *laptops*, *tablets*, *smartphones* y consolas de juego cuentan con interfaces de red IEEE 802.11, permitiendo a un creciente número de usuarios ser parcialmente móviles. Hoy por hoy, la expansión en el dispositivos móviles se refleja en las siguientes cifras: los usuarios de teléfonos celulares a nivel mundial pasaron de pasó de 34 millones en 1993 [2] a 6.6 billones en 2014 [3]. Para 2014 se estima que más de 187 millones de *laptops* y 287 millones de *tablets* fueron despachadas en todo el mundo [4]. Para 2016 los equipos Wi-Fi y móviles generaran 54 % del tráfico IP [5]. En el 2018, el tráfico móvil será 11 veces superior al del 2013 [5]. Particularmente en Venezuela, en 2013 se tenían 30.110.565 suscriptores a telefonía móvil, lo que correspondía a 102.61 % de penetración [6].

La utilización más frecuente de las redes IEEE 802.11 se realiza en la banda del espectro correspondiente a los $2.4\,GHz$, que es una banda libre, por lo que en la práctica se encuentran numerosas redes desplegadas en forma independiente, es decir, sin coordinación ni planificación central, lo que ha ocasionado la presencia de despliegues espontáneos, con redes con características y configuraciones variables y con puntos de acceso (AP: *Acess Points*) distribuidos sin un patrón predecible, provocando que las MS deban estar preparadas para operar en despliegues caóticos.

Para acceder a la red, las MS deben estar asociadas a un AP, por lo que deben mantenerse dentro de la cobertura de la señal de radio, limitando la movilidad a un área cercana al AP. La cobertura puede ser de unas pocas

decenas de metros, dependiendo de obstáculos e interferencias. A fin de aumentar la movilidad fuera del área de cobertura de un AP, las MS deben ser capaces de descubrir, conectarse y migrar eficientemente a través de las pico-celdas formadas en los despliegues caóticos, es decir, sin coordinación ni planificación central. Este proceso es conocido como *handover* y afecta la conexión de red en varias capas del modelo sistema de interconexión de sistemas (OSI: *Open Systems Interconnection*). Se destacan dos tipos de *handover*: vertical y horizontal. El primero implica cambiar la tecnología usada para acceder a la red, por ejemplo, de IEEE 802.11 a sistema universal de telecomunicaciones móviles (UMTS: *Universal Mobile Telecommunications Systems*). El segundo está asociado a cambios de red, manteniendo la tecnología. Este trabajo se centra en el *handover* horizontal, particularmente en los procesos de la capa 2. Como se describirá en la Sección 3, las tecnologías actuales resultan en prolongadas interrupciones de red que limitan el uso de las redes móviles. Estas interrupciones se deben en gran medida a la latencia de la fase de descubrimiento de redes o escaneo [7, 8].

Por tanto, se pretende estudiar los mecanismos fundamentales involucrados en el proceso de descubrimiento y conexión a redes IEEE 802.11; en particular, el intercambio de las tramas de administración Probe Request (P_{rq}) y Probe Response (P_{resp}); esenciales para el descubrimiento, y la arquitectura de los dispositivos IEEE 802.11 que permiten enviar y recibirlas. Se busca analizar el comportamiento del proceso de descubrimiento a través de métricas obtenidas en distintos experimentos y campañas de recolección de datos, así como también, proponer un sistema que asista a las MS en el descubrimiento preciso de la topología disponible en su entorno.

1.1. Planteamiento del problema

La diversidad en las redes espontáneas [9] y las características de las redes IEEE 802.11, tales como acceso aleatorio y las propiedades de espectro de radio, provocan efectos en el escaneo que son desconocidos. Las estrategias de descubrimiento actuales no están preparadas para estos despliegues espontáneos y tampoco se ajustan a necesidades particulares de usuarios y aplicaciones, resultando en procesos de conexión y *handover* no óptimos [7,8]. Esto se debe, en parte, a que no hay una única estrategia de escaneo óptima para los distintos despliegues de red [10, 11]. Adicionalmente, las necesidades de las aplicaciones y usuarios exigen distintas características de las redes y

del escaneo. Por ejemplo, los siguientes casos de uso plantean necesidades de escaneo diferentes:

- Usuarios de baja movilidad (ver Sección 2.3) con una conexión activa, utilizando el escaneo para geolocalización. El escaneo debe ser suficientemente flexible para no afectar el trafico de red mientras mantiene una precisión apropiada [12];
- Estaciones en desplazamiento con una conexión activa, buscando una lista de AP candidatos para realizar un *handover*, donde se deben considerar las necesidades de las aplicaciones en ejecución [10]. Por ejemplo:
  - Una MS con una conexión buena, que puede permitir un escaneo largo, probablemente resultando en una lista completa de las redes disponibles.
  - Una MS con una conexión inestable, que podría estar por interrumpirse, por lo que necesita un AP candidato tan pronto como sea posible.
- MS en desplazamiento, con soporte para red tolerante a retardos (DTN: *Delay Tolerant Network*) o alguna variación. En este caso se necesita establecer una conexión rápidamente y por un periodo de tiempo posiblemente corto.
- MS con restricciones de red específicas, por ejemplo: identificador particular, calidad del enlace, entre otros.

1.2. Justificación

La posibilidad de tener conectividad a las redes, con interrupciones y bajos retardos en la red, junto con el aprovechamiento de los despliegues IEEE 802.11 encontrados en ciudades e instituciones, permitiría satisfacer requerimientos de nuevas aplicaciones e incluir nuevos usuarios, por ejemplo, a través de redes comunitarias. Para lograrlo es necesario comprender las redes desplegadas de forma espontánea, así como los procesos que permiten descubrirlas. Por tanto, es apropiado conducir un estudio que permita:

1. Detallar los procesos que intervienen en el descubrimiento de redes IEEE 802.11, especialmente los relacionados con el mecanismo de acceso al medio;

2. Conocer el estado del arte de las estrategias de descubrimiento de redes IEEE 802.11;

3. Caracterizar las redes desplegadas espontáneamente en función de los elementos que afectan la duración del proceso de descubrimiento;

4. Describir la dinámica del proceso de descubrimiento de redes.

1.3. Objetivos

1.3.1. Objetivo general

Estudiar los despliegues espontáneos de redes IEEE 802.11 y la dinámica asociada al proceso de su descubrimiento.

1.3.2. Objetivos específicos

- Comparar las estrategias de descubrimiento de redes IEEE 802.11 existentes.
- Identificar factores que afectan el proceso de descubrimiento de redes IEEE 802.11.
- Describir el proceso de descubrimiento en redes espontáneas.
- Caracterizar el tiempo de respuesta de redes IEEE 802.11 desplegadas espontáneamente ante el proceso de descubrimiento.

1.4. Metodología

Tomando en cuenta las características del trabajo, se ejecutó un trabajo mixto, realizando estudios exploratorios y descriptivos. Para ello se utilizó el método inductivo [13], estudiando experimentalmente los mecanismos de descubrimiento y de acceso al medio, y complementados con evaluaciones experimentales, mediante pruebas de laboratorio y en despliegues reales.

1.5. Aportes

Adicionalmente, las siguientes publicaciones basadas en esta investigación se presentaron a la comunidad:

- A. Arcia-Moret, **L. Molina**, N. Montavont, G. Castignani y A. Blanc, "Access Point Discovery in 802.11 Networks", Aceptado en IEEE/IFIP Wireless Days. 12 al 14 de noviembre, 2014. Río de Janeiro, Brasil [14].
- **L. Molina** y A. Arcia-Moret, "Evaluación del Proceso de Escaneo en Redes 802.11: una perspectiva taxonómica" en Memorias del 1era Conferencia Nacional de Computación, Informática y Sistemas, CONCISA, 2013. ISBN: 978-980-7602-03-7 [15].
- A. Arcia-Moret, **L. Molina**, G. Castignani y N. Montavont, "Characterizing Spontaneous IEEE 802.11 Network Deployments" en Memorias del 6th International Conference on Network Games, Control and Optimization, NetGCoop '12, 2012. ISBN: 978-1-4673-6026-5 [16].
- **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, Cibelec '12, 2012. ISBN: 978-980-7185-02-8 [17].
- **L. Molina**, A. Arcia-Moret. "Caracterización de redes 802.11", 3er Encuentro Nacional de Estudiantes de Ingeniería (3er ENEING), Margarita, Nueva Esparta, Venezuela, Marzo 2012 [18].

Capítulo 2

Redes IEEE 802.11

El acceso de una estación a una red depende del medio físico utilizado para establecer enlace con otros clientes de la red. Actualmente, el acceso inalámbrico a las redes se ha hecho muy popular, lo que ha abaratado costos, permitiendo la instalación y configuración de gran número de redes de área local (LAN: *Local Area Networks*) en universidades, bibliotecas, edificios de oficina y residenciales, parques, entre otros. Del mismo modo, cada vez son más populares las redes de área amplia (WAN: *Wide Area Networks*).

En una LAN inalámbrica las estaciones cliente son comúnmente denominadas estaciones móviles (MS: *Mobile Stations*); estas reciben y transmiten paquetes desde y hacia un punto de acceso (AP: *Access Point*), que a su vez está conectado a otra red y posiblemente a Internet. En una WAN, los paquetes son transmitidos hacia una estación base que podría estar soportada por la infraestructura de la red de telefonía móvil u otra infraestructura. Las LAN inalámbricas alcanzan coberturas de unas decenas o centenas de metros, mientras que las WAN podrían cubrir kilómetros. En ambos casos, la capacidad de la red y la cobertura está determinada por el medio utilizado y los estándares o protocolos que regulan el comportamiento de los dispositivos que intervienen en la red, siendo el estándar IEEE 802.11 [1] el más popular para las LAN inalámbricas. Este forma parte de la familia de estándares IEEE 802 para LAN y redes de área metropolitana (MAN: *Metropolitan Area Networks*). Los servicios y protocolos especificados en IEEE 802 se corresponden con las capas física y de acceso al medio del modelo sistema de interconexión de sistemas (OSI: *Open Systems Interconnection*) de 7 capas.

Salvando la ausencia de cableado, de velocidad de transmisión y las venta-

jas de mantener conectividad en dispositivos inalámbricos y/o móviles, desde el punto de vista de los usuarios finales no hay diferencia entre una conexión inalámbrica y una alámbrica, en ambos casos el uso de aplicaciones de red (navegador, chat, vídeos, terminal remoto, etc.) es igual. En general, una red alámbrica y una red inalámbrica solo se diferencian a nivel de las capas enlace de datos y física, pues son las que están relacionadas con el acceso al medio.

2.1. Componentes de una red

La arquitectura IEEE 802.11 [1] está formada por componentes que interactúan para proveer conectividad inalámbrica dentro de un área local a estaciones fijas, portátiles y móviles. La Figura 2.1 presenta los componentes de una red IEEE 802.11.

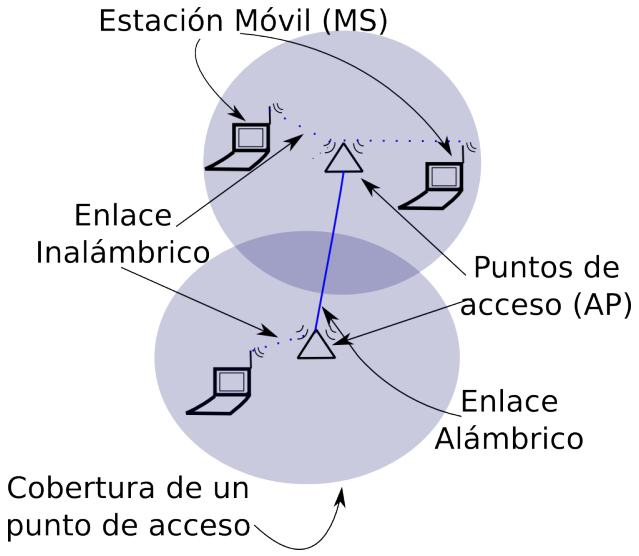


Figura 2.1: Componentes de una red IEEE 802.11

2.1.1. Estaciones Móviles

De acuerdo con [19], uno de los requerimientos del estándar IEEE 802.11 es manejar estaciones portátiles y móviles. Donde una estación portátil es una estación que puede mantener conectividad en lugares fijos, por ejemplo,

computadores de escritorio o servidores con conectividad inalámbrica. En una estación móvil la conexión se mantiene disponible mientras la estación está en movimiento.

Sin embargo, debido a las variaciones en el medio (efectos producidos por la degradación, la propagación y la dispersión de las señales), en una red IEEE 802.11 todos los clientes son tratados como MS [1].

Las MS, también conocidas como *hosts*, son los dispositivos con los que interactúan los usuarios y en los que se ejecutan las aplicaciones finales. Se puede considerar como MS los diferentes dispositivos que cuentan con una interfaz de red capaz de operar bajo el estándar IEEE 802.11, por ejemplo: computadores portátiles y de escritorio, teléfonos celulares, *tablets*, entre otros.

2.1.2. Puntos de Acceso

Los AP son parte central de una red inalámbrica de tipo infraestructura, se encargan de coordinar la comunicación en la red, todas las MS que forman parte de la red deben transmitir hacia el AP y este se encargará de enviar el tráfico hacia su destino final. También permiten la interconexión con redes operando en otros protocolos; para ello, convierte las tramas IEEE 802.11 al tipo apropiado de la otra red. Por ejemplo, en laboratorios y oficinas es común encontrar AP que permiten acceder a la Internet, por lo que deben transformar tramas IEEE 802.11 en tramas 802.3 [2, 19, 20].

2.1.3. Medio de transmisión

Los AP y las MS deben utilizar un medio que les permita mantener un enlace. Las redes IEEE 802.11 utilizan medios no guiados para mantener los enlaces entre los componentes de la red. El estándar [1] describe varios medios, cada uno con características específicas que determinan el área de cobertura de la red, las velocidades de transmisión, los niveles de interferencia, las características de la propagación, las técnicas de modulación, entre otros.

Los medios más populares utilizan distintas frecuencias del espectro electromagnético: radio, microondas, transmisiones infrarrojas y láser. El estudio presentado en este trabajo se concentra en la implementación de radio en el espectro de 2.4 GHz, que presenta los siguientes inconvenientes:

- Son propensos a la interferencia de señales provenientes de otras fuentes, incluyendo otras redes IEEE 802.11;
- Las señales son absorbidas y reflejadas por métales y fuentes de agua [21];
- La topología formada por los dispositivos es dinámica;
- Terminal oculta y terminal expuesta (ver Sección 2.5).

2.1.4. Sistema de distribución

La cobertura de una red IEEE 802.11, y por tanto la movilidad, está limitada al alcance de la señal del AP. Con el fin de aumentar la cobertura de la red y la movilidad de las MS, varios AP pueden ser interconectados a través de un sistema de distribución (DS: *Distribution System*) [1,20]. El DS es el componente lógico que permite la integración de múltiples conjunto de servicio básico (BSS: *Basic Service Set*), permitiendo que el intercambio de tramas entre MS pertenecientes a diferentes BSS. Los AP hacen uso de un enlace o *backbone* para su interconexión. La tecnología usada en el enlace no es especificada en el estándar, por lo que podría utilizarse 802.3 e inclusive IEEE 802.11.

El DS debe hacer seguimiento a la ubicación física de las MS y gestionar la entrega de las tramas a través del AP apropiado. En la Figura 2.2, la trama T, cuyo destino es $MS1$, ingresa al DS; este se encarga de direccionarla a través del *backbone* hasta $AP1$, que es el AP que sirve a $MS1$.

2.2. Tipos de red

El bloque básico de una red IEEE 802.11 es llamado conjunto de servicio básico (BSS: *Basic Service Set*), que está definido por el conjunto de MS que puede comunicarse entre sí. Se distinguen dos tipos de BSS: *Independent Basic Service Set* e *Infrastructure Basic Service Set*.

El área en la que deben permanecer las MS para mantener la comunicación y la membrecía con el BSS se conoce como área de servicio básico (BSA: *Basic Service Area*).

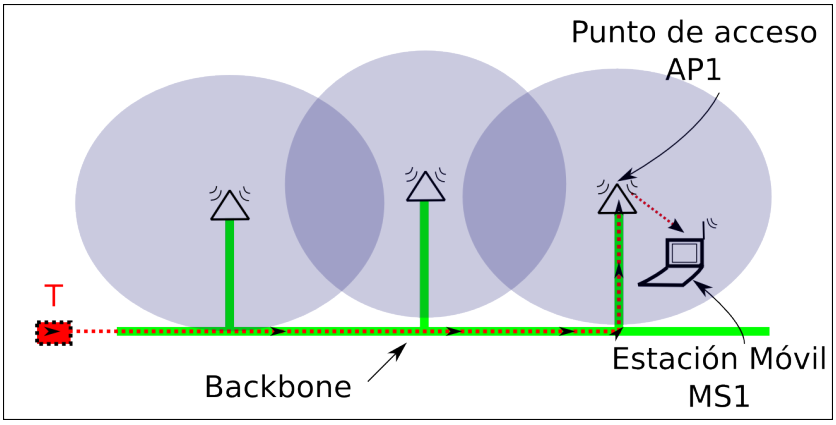


Figura 2.2: Sistema de Distribución

La membrecía en un BSS es dinámica, es decir, las MS entran y salen. Para ser parte de un BSS, la estación debe asociarse y sincronizarse con la red siguiendo los protocolos descritos en el estándar.

2.2.1. Redes independientes (*ad-hoc*)

Una "red independiente", también conocida como red *ad-hoc*, está formada por un conjunto de servicio independiente (IBSS: *Independent Basic Service Set*). Un IBSS es formado por un conjunto de MS que pueden comunicarse directamente, es decir, no se requiere de un dispositivo especial que regule la red. La Figura 2.3 muestra un ejemplo.

2.2.2. Redes infraestructura

A diferencia de las redes independientes descritas en la Sección 2.2.1, las redes de tipo infraestructura requieren una entidad, denominada AP, encargada de gestionar el tráfico de la red. Las estaciones no se comunican directamente entre sí, sino que deben enviar el tráfico al AP y éste lo transmite hacia el destino. Dado que toda la comunicación debe realizarse a través del AP, el BSA depende de la cobertura que tenga la señal de los AP (ver Figura 2.4). Toda estación que forma parte de la red debe estar asociada con un AP; una estación solo puede asociarse con un AP a la vez. Como se puede ver en la Figura 2.5, los procesos de autenticación y posterior asociación, son

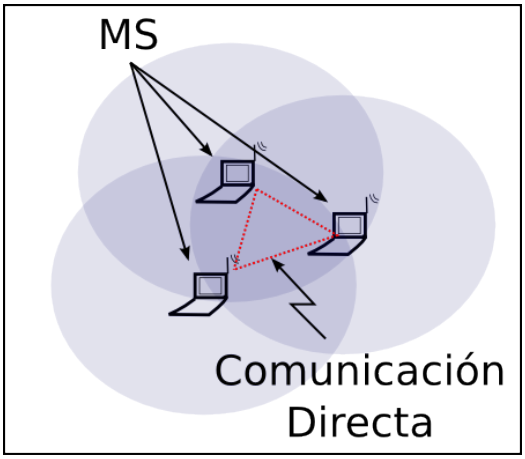


Figura 2.3: BSS Independiente

iniciados por la estación y el AP podrá autorizar o negar la asociación en base a la configuración de la red.

Las redes infraestructura presentan las siguientes ventajas [20]:

- Un BSS infraestructura está definido por la cobertura del AP. Todas las estaciones deben mantenerse dentro del alcance del AP, pero no hay restricción en la ubicación o distancia entre las estaciones;
- Mayor cobertura, dado que las MS se comunican a través del AP;
- Los AP pueden asistir a las estaciones en el ahorro de energía, pues el AP podría almacenar tramas mientras que la estación apaga temporalmente la interfaz de red. Luego, la estación activa la interfaz únicamente para transmitir y recibir tramas que han sido acumuladas en el AP.

2.2.3. Área de servicio extendido

Un conjunto de servicio extendido (ESS: *Extended Service Set*) [1] permite interconectar varios BSS que se encuentran conectados a un mismo DS. Todos los BSS que forman un conjunto de servicio extendido (ESS: *Extended Service Set*) comparten el mismo identificador del conjunto de servicio (SSID: *Service Set Identifier*), que funge como el nombre o identificador de la red.

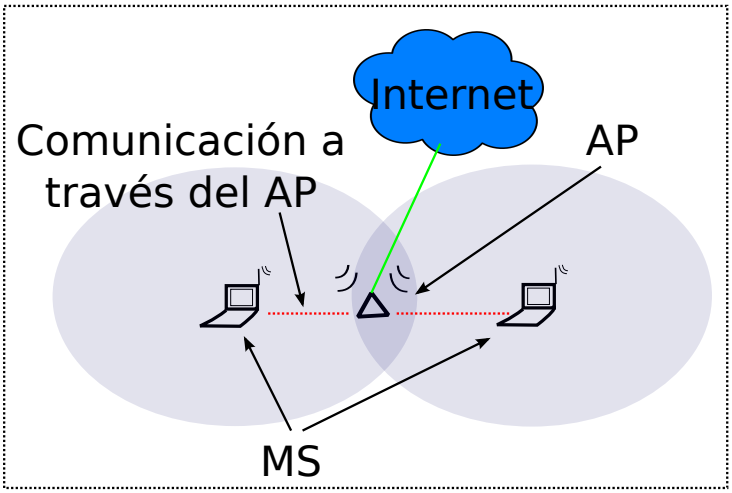


Figura 2.4: Red tipo infraestructura

El concepto central es que cualquier estación perteneciente al ESS puede comunicarse con otras estaciones en el ESS a nivel de la capa 2, manteniendo la configuración en las capas superiores. Adicionalmente el ESS permite ampliar la movilidad de las MS al interconectar varios AP que aumentan el BSA.

2.3. Aspectos de Movilidad

La movilidad se puede definir como la capacidad de movimiento de una estación mientras se mantiene conectividad a la red. Una de las características de las redes inalámbricas es que soportan movilidad de los clientes; sin embargo, se pueden distinguir distintos grados de movilidad. En [19] se diferencian los siguientes grados:

- **Dispositivos fijos** (presentan una única ubicación): son instalados una vez y luego pueden mantener comunicación con la red, siempre en la misma ubicación. La razón principal para utilizar una red inalámbrica es evitar el cableado. Aunque los dispositivos no sean móviles, el canal de propagación utilizado puede cambiar en el tiempo. Esto debido a variaciones en el medio y/o en el entorno (personas caminando, reorganización de equipos, etc.).

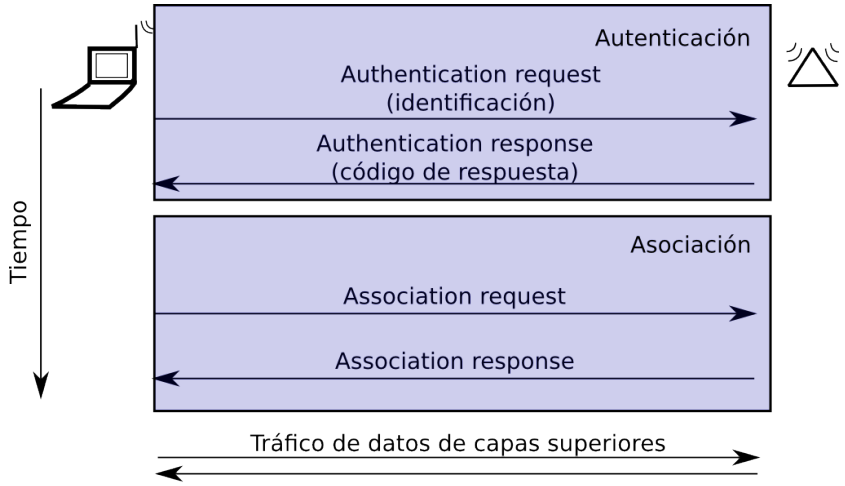


Figura 2.5: Autenticación y asociación a un AP utilizando el sistema de autenticación abierta (OSA: *Open System Authentication*)

- **Dispositivos nómadas**: son ubicados en un lugar fijo por un tiempo determinado; luego se mueven a una nueva ubicación. Esto significa que por el período de tiempo que mantienen una ubicación se comportan como dispositivos fijos. Sin embargo, al cambiar de ubicación, el entorno puede cambiar radicalmente. Ejemplo de esto son las computadoras portátiles.

- **Baja movilidad**: muchos dispositivos de comunicación operan a velocidad de un peatón. El efecto de la baja velocidad y la poca movilidad implica que el entorno cambia en forma progresiva, con redes que aparecen y desaparecen frecuentemente y a intervalos irregulares, variando también las características percibidas de las redes, por ejemplo: potencia de la señal, calidad de la conexión, retardo, entre otros. En esta categoría se pueden incluir los teléfonos celulares y teléfonos inalámbricos. Este trabajo toma como marco de referencia la baja movilidad.

- **Alta movilidad**: usualmente contempla velocidades entre $30\,km/h$ y $150\,km/h$. Un ejemplo son los teléfonos celulares utilizados en carros. En esta categoría, el cambio de estación base puede ser frecuente.

- **Ultra alta movilidad**: está representada por redes que operan con trenes de alta velocidad y aviones, que se desplazan a velocidades ma-

yores a los $300\,km/h$.

En las redes IEEE 802.11 se provee un servicio de baja movilidad a nivel de las capas física y de enlace de datos; desde esta perspectiva la movilidad de una MS se puede clasificar en:

1. **Sin transición**: implica que la estación se mantiene asociada a un AP y por tanto dentro de su área de cobertura. Dadas las características del medio de transmisión usado en las redes IEEE 802.11, es difícil distinguir entre una estación físicamente estática y una estación en movimiento, pues los efectos de la propagación de la señal y cambios en el entorno provocan que las estaciones parezcan estar siempre en movimiento.

2. **Transición de BSS**: IEEE 802.11 provee movilidad a las estaciones dentro de un ESS, es decir, las estaciones en movimiento pueden cambiar de BSS, para ello deben desasociarse del AP actual y asociarse a otro AP perteneciente al mismo ESS. La transición entre BSS requiere que los AP intercambien información sobre la estación en cuestión, particularmente es necesario informar con cual AP se encuentra asociado. La transición de BSS es iniciada por la estación, quien monitorea la calidad[1] del AP y, posiblemente, inicia el proceso de re-asociación con un nuevo AP. La Figura 2.6 ilustra la transición de BSS.

3. **Transición de ESS**: la transición a un BSS perteneciente a otro ESS no está descrito por el estándar, implica una interrupción de red a nivel de la capa enlace y posiblemente en las capas superiores.

Cuando una MS se mueve hacia los límites del alcance de un AP y entra en el rango de otro, ésta debe realizar una transición hacia el nuevo AP. El proceso que permite la transición se conoce como *handover*. Luego de un *handover* la ruta que deben seguir las tramas emitidas por la MS deben atravesar un AP diferente para alcanzar su destino. Si el *handover* es realizado entre un par de AP pertenecientes a distintos ESS el estándar IEEE 802.11 no garantiza la conectividad a las capas superiores, lo que implica que el usuario experimentará interrupción en la conexión a la red y uno o más de los paquetes en transito se perderá

[1]La definición de calidad de un AP es subjetiva. Puede incluir factores como potencia de la señal, calidad de la conexión, latencia, entre otros.

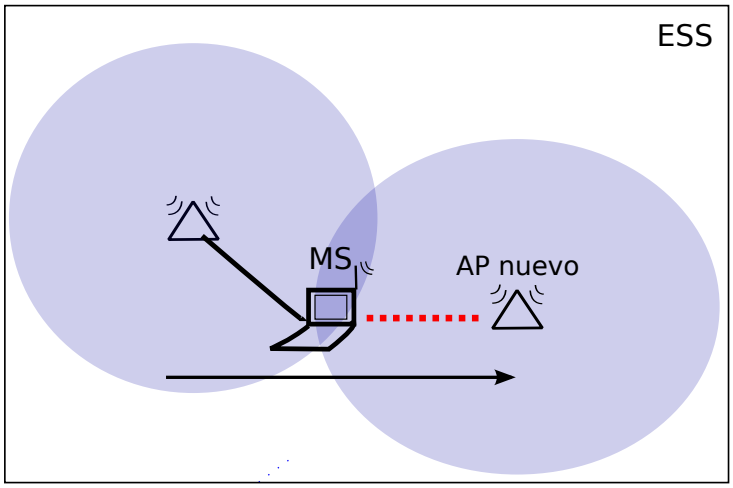


Figura 2.6: Transición de BSS de una MS

2.4. Requerimientos de servicio

Existe variedad de usuarios y aplicaciones para las redes inalámbricas, cada uno con requerimientos diferentes. Además del tipo de movilidad de los clientes de la red, las necesidades y aplicaciones se pueden describir en términos de: tasa de transmisión y retardo.

2.4.1. Tasa de transmisión

Los servicios usados en las redes presentan distintas necesidades en cuanto a la tasa de transmisión se refiere. Algunas redes presentan necesidades de transferencia bajas y con transferencias eventuales, por ejemplo, en una red de sensores, los sensores miden variables y transmiten a intervalos que pueden ir de unos pocos milisegundos a varias horas. Por su lado redes que implican transmisión de voz usualmente requieren entre 5 $kbps$ y 64 $kbps$. Por ejemplo, telefonía celular (alrededor de 10 $kbps/s$) y teléfonos inalámbricos (32 $kbps$) [19]. Otras aplicaciones, como lectura de noticias o correo electrónico, transmisión de multimedia (ejemplo: *streaming* de audio o vídeo) presentan requerimientos superiores.

2.4.2. Retardo

Las aplicaciones presentan distintos niveles de susceptibilidad al retardo introducido por los distintos servicios de la red, también conocido como latencia de la red. Algunas aplicaciones presentan necesidades muy estrictas respecto al retardo, por ejemplo, aplicaciones como correos y chat tienen exigencias bajas, mientras que sesiones remotas, juegos en red, telefonía y vídeo conferencia son altamente susceptibles al retardo, al punto que retardos en la red mayores de 400 ms son inaceptables [22].

Las restricciones de retardo y tasa de transmisión varían según el tipo de aplicación de red. En la Figura 2.7, se presenta el panorama de algunas aplicaciones.

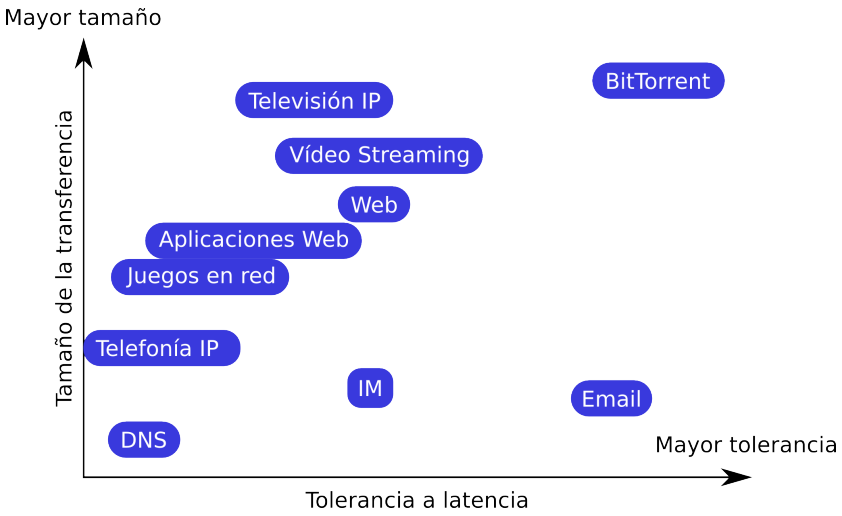


Figura 2.7: Necesidad de las aplicaciones en términos de latencia y tamaño de transferencia

2.5. Control de acceso al medio

Las transmisiones en redes IEEE 802.11 son realizadas en *broadcast*, es decir, las estaciones comparten el medio por lo que las transmisiones pueden ser escuchadas por varias estaciones, trayendo como consecuencia que si varias estaciones ocupan el medio simultáneamente las señales involucradas se

solapan provocando la corrupción de las transmisiones. Este suceso es conocido como colisión. A fin de evitar colisiones se debe tener un mecanismo de acceso al medio que limite el uso del medio por una estación en cada instante de tiempo.

El problema central del control de acceso al medio consiste en maximizar la utilización del medio, coordinándolo a fin de evitar que varias estaciones transmitan simultáneamente. El objetivo es determinar cual de las estaciones obtiene el acceso al medio cuando varias estaciones compiten por él.

De acuerdo a las características del medio y la red se han desarrollado varias estrategias. En el caso de las redes IEEE 802.11 el protocolo de acceso al medio debe permitir el uso del medio por parte de distintas estaciones independientes que utilizan un medio no guiado y al mismo tiempo enfrentar los siguientes problemas: terminal oculta (*hidden terminal problem*) y terminal expuesta (*exposed terminal problem*).

El *problema de la terminal oculta* viene dado por la incapacidad que tienen las estaciones para identificar las transmisiones de todas las demás estaciones, por lo que el medio puede ser ocupado simultáneamente por más de una estación, generando colisiones. Por ejemplo, en la Figura 2.8 las estaciones 1, 2 y 3 tienen un alcance denotado por los círculos respectivos, es decir, cada estación solo conoce lo que se encuentra dentro de su radio de alcance. Si la estación 1 y la estación 3 transmiten hacia la estación 2 se generará una colisión y ninguna de las dos podrá detectarla.

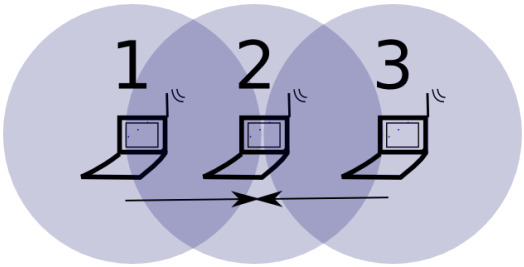


Figura 2.8: Problema de la terminal oculta

Según la disposición de las estaciones es posible encontrar estaciones que no trasmitan debido a que observan el medio ocupado, cuando podría transmitir sin incurrir en colisiones que afecten la comunicación. Esto problema se conoce como *problema de la terminal expuesta*; se puede observar en la Figura 2.9. Si la estación 2 mantiene transmisión hacia la estación 1 entonces la

estación 3 se abstendrá de realizar transmisiones hacia 4. Sin embargo, ambas transmisiones podría realizarse simultáneamente pues la colisión generada no alcanzará el área de recepción de 4.

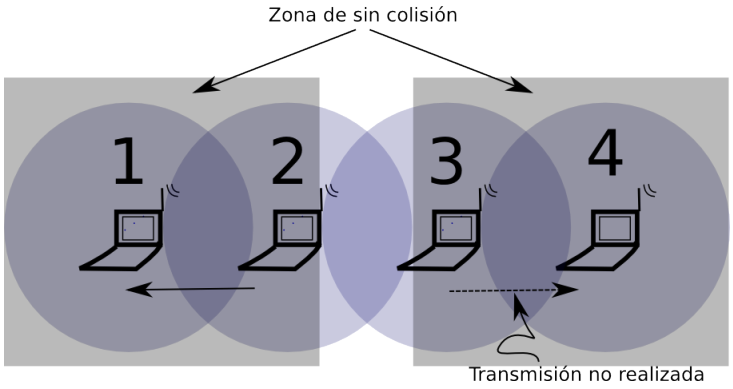


Figura 2.9: Problema de la terminal expuesta

2.5.1. Función de coordinación distribuida

El estándar IEEE 802.11 define tres mecanismos para coordinar el acceso al medio y evitar la colisiones. El primer modo es denominado función de coordinación distribuida (DCF: *Distribution Coordination Function*), en el que las estaciones actúan en forma independiente sin coordinación central. El segundo se conoce como función de coordinación puntual (PCF: *Point Coordination Function*), en donde el AP coordina el acceso al medio. Este es poco usado en la práctica, pues es difícil prevenir que estaciones cercanas, pertenecientes a otras redes, ocupen el medio [23]. Por último, está el mecanismo llamado función de coordinación híbrida (HCF: *Hybrid Coordination Function*), que combina características de la DCF y PCF.

A fin de manejar el problema de la estación oculta, se utiliza el siguiente mecanismo: antes de transmitir, la estación origen envían una trama denominada *solicitud de envío (RTS: Request to Send)* hacia la estación destino, indicando la necesidad de transmitirle información. Luego, la estación destino responde con una trama denominada *libre para envío (CTS: Clear to Send)*, informando a la estación origen que puede transmitir. Una vez que ambas tramas han sido transmitidas exitosamente y debido a que las transmisiones IEEE 802.11 pueden ser escuchadas por todas las estaciones que se

encuentran en el radio de alcance del transmisor, las estaciones que podrían provocar una colisión estarán al tanto de la transmisión en curso por lo que deben abstenerse de transmitir.

En cualquier caso, las redes IEEE 802.11 mantienen un espacio inter-trama. Se distinguen cinco tipos:

- *Short Interframe Space (SIFS)*: es utilizado para transmisiones de alta prioridad, tales como: RTS/CTS, ACK positivos, la segunda y siguientes tramas de una ráfaga.
- *Point Coordination Function Interframe Space (PIFS)*: es utilizado en las redes que operan utilizando PCF.
- *Distributed Coordination Function Interframe Space (DIFS)*: usado en las redes que operan utilizando DCF. Indica el periodo que el medio debe permanecer desocupado antes de que las estaciones puedan transmitir tramas de datos y tramas de administración.
- *Arbitration Interframe Space (AIFS)*: usado por las características que gestionan la calidad de servicio (QoS: *Quality of Service*).
- *Extended Interframe Space (EIFS)*: indica el periodo que el medio debe permanecer desocupado luego de que se ha detectado una trama corrupta, permitiendo que una transmisión errónea se complete antes de iniciar una nueva transmisión.

Los valores de los espacios inter-tramas se relacionan según las ecuaciones 2.1a, 2.1b y 2.1c.

$$PIFS = SIFS + SlotTime \tag{2.1a}$$
$$DIFS = SIFS + 2 \times SlotTime \tag{2.1b}$$
$$EIFS = SIFS + DIFS + ACKTxTime \tag{2.1c}$$

donde:

ACKTxTime es el tiempo (en microsegundos) necesario para transmitir una trama ACK a la velocidad de transmisión del medio físico más baja;

SlotTime es el valor del "slot" de tiempo usado. Depende de la capa física. El cuadro 2.1 muestra los valores para las redes IEEE 802.11a, IEEE 802.11b e IEEE 802.11g.

Tabla 2.1: Espacio inter-trama (IFS)

Estándar	**802.11a**	**802.11b**	**802.11g**
SlotTime (μs)	9	20	9
SIFS (μs)	16	10	10
PIFS (μs)	25	30	19
DIFS (μs)	34	50	28

La DCF emplea acceso múltiple por detección de portadora con evasión de colisiones (CSMA/CA: *Carrier Sense Multiple Access with Collision Avoidance*) para evitar las colisiones y opera como sigue [1]: las estaciones deben revisar el medio para determinar si ocupado, es decir, si otra estación está transmitiendo. Si el medio está desocupado se efectúa la transmisión. El algoritmo distribuido CSMA/CA especifica que entre dos tramas contiguas y pertenecientes a la misma ráfaga, el medio debe permanecer desocupado por un periodo denominado SIFS. Si el medio se encuentra ocupado, entonces la estación deberá diferir la transmisión hasta que el medio esté desocupado. Luego, cuando se determina que el medio se encuentra desocupado por un periodo determinado, la estación deberá realizar una espera adicional denominada *backoff*.

Para realizar el *backoff* la estación computa un contador de *backoff*, este contador se decrementa mientras que el medio está libre durante el periodo SIFS, DIFS, espacio de arbitraje inter-tramas (AIFS: *Arbitration Interframe Space*) o espacio inter-tramas extendido (EIFS: *Extended Interframe Space*), según corresponda. Si se detecta que el medio está ocupado, el contador debe "congelarse" hasta que vuelva a estar desocupado. Cuando el contador llega a cero la estación puede transmitir. La duración del *backoff* es calculada según la ecuación 2.2.

$$b = random() \times SlotTime \tag{2.2}$$

donde:

b representa la duración del *backoff*.

random() es una función que retorna un número entero pseudo aleatorio de una distribución uniforme sobre el intervalo [0, CW]. CW (*Contention Window*), pertenece al intervalo $aCWmin \leq CW \leq aCWmax$. $aCWmax$ y $aCWmin$ son valores dependientes de la capa física.

SlotTime es el valor del "slot" de tiempo usado. Depende de la capa física (ver cuadro 2.1).

2.6. Tramas

El estándar diferencia 3 tipos de tramas: tramas de datos (*data frames*), tramas de control (*control frames*) y tramas de administración (*management frames*). Cada una de estas con distintos subtipos. Las tramas de datos transportan datos de las capas superiores en su cuerpo. Las tramas de control permiten realizar operaciones de acceso al medio (tramas RTS y CTS) y confirmación de recibo (ACK: *acknowledgment*). Las tramas de administración gestionan la asociación, autenticación, movilidad entre distintos AP, descubrimiento de redes, entre otros.

Cada estación de la red debe estar en capacidad de construir e interpretar tramas. El formato de las tramas varía de acuerdo al tipo. La Figura 2.10 describe los campos comunes de una trama de administración, incluyendo el espacio en bytes ocupado.

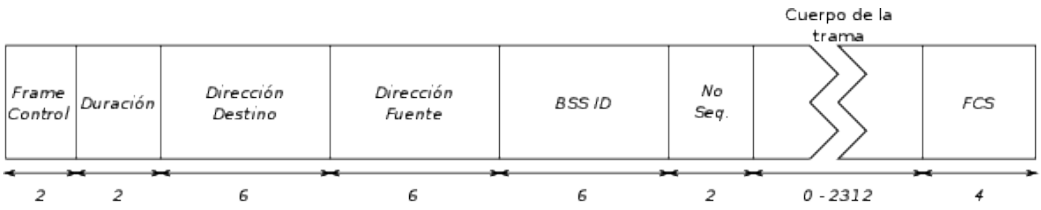


Figura 2.10: Forma de una trama de administración

El cuerpo de la trama depende del tipo (datos, control o administración) y subtipo, siendo los subtipos *Beacon*, *Probe Request* y *Probe Response* de especial interés en el proceso de descubrimiento.

2.6.1. Beacon

El cuerpo de la trama de administración "Beacon" contiene información sobre el BSS. Estas tramas son transmitidas por los AP periódicamente, advirtiendo información de la red. Los beacons también son utilizados para sincronizar las estaciones que forman el BSS. En la Figura 2.11 se muestra la estructura de un Beacon. Entre los campos presentes resaltan los siguientes:

- *Timestamp*: 8 bytes que representan el valor de la función de sincronización (TSF: *timing synchronization function*), función utilizada para mantener sincronizados todas las estaciones pertenecientes a un BSS [20].
- *Beacon interval*: indica el intervalo, en TU, de transmisión de los Beacons[2] [20].
- *Capability*: campo de 2 octetos utilizado para mostrar las capacidades de la red [20].
- *Service Set Identifier*: mantiene el identificador del BSS [20].
- *Supported rates*: las velocidades de transmisión soportadas por la estación [20].

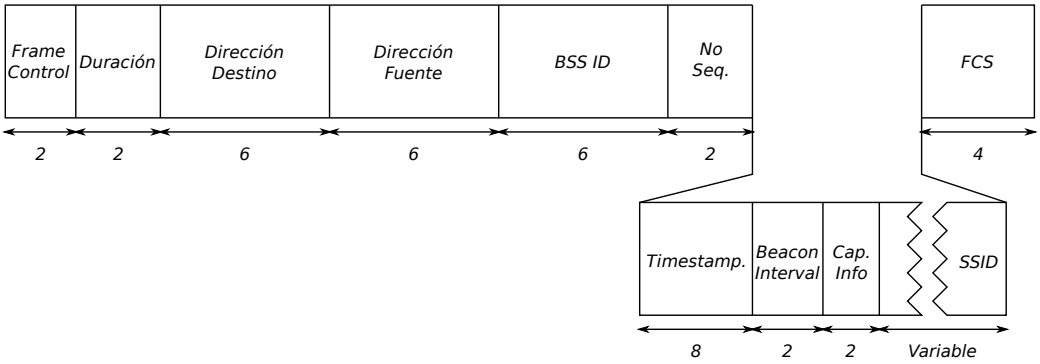


Figura 2.11: Forma de una trama Beacon

[2] 1 unidad de tiempo (TU: *Time Unit*) equivale a $1024\,\mu s$.

2.6.2. Probe Request

Las tramas *Probe Request* son utilizadas por las estaciones a fin de conocer las redes IEEE 802.11 existentes en su entorno. La estación que genera un *Probe Request* utiliza el campo SSID para dirigirlo al *broadcast* o a un AP particular. Los AP que reciben *Probe Request* responden a la estación que lo originó con un *Probe Response*.

La Figura 2.12 muestra la estructura de una trama *Probe Request*. Además de los campos obligatorios en todas las tramas MAC 802.11, estas tramas contienen los siguientes campos:

- *SSID*: identificador de la red, pudiendo utilizarse la dirección del *broadcast*.
- *Supported Rates*: velocidades de transmisión soportadas por la estación.
- *Extended Supported Rates*: si la estación soporta más de ocho velocidades de transmisión se utiliza este campo.

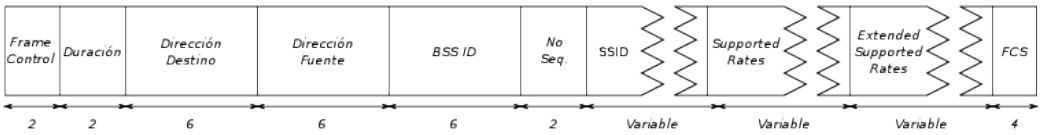


Figura 2.12: Estructura de una trama *Probe Request*

2.6.3. Probe Response

Ante la presencia de un *Probe Request*, las redes compatibles envían, a la estación que originó el *Probe Request*, un *Probe Response*. Los *Probe Responses* contienen información sobre la red y que será necesaria para el proceso de asociación.

En las redes infraestructura el AP es el encargado de atender los *Probe Request* y transmitir los *Probe Responses*, en una red IBSS la responsabilidad es compartida y cada estación será responsable de transmitir los *Probe Responses* durante un intervalo denominado *Beacon interval*.

La Figura 2.13 muestra la estructura de un *Probe Response*, vale la pena destacar algunos de los campos presentes en las tramas *Probe Response*:

- *Timestamp*: temporizador utilizado para sincronizar las estaciones que forman la red.
- *Beacon interval*: representa el número de TU entre la transmisión de *beacons*.
- *Current Channel*: indica el canal en el que opera el AP.

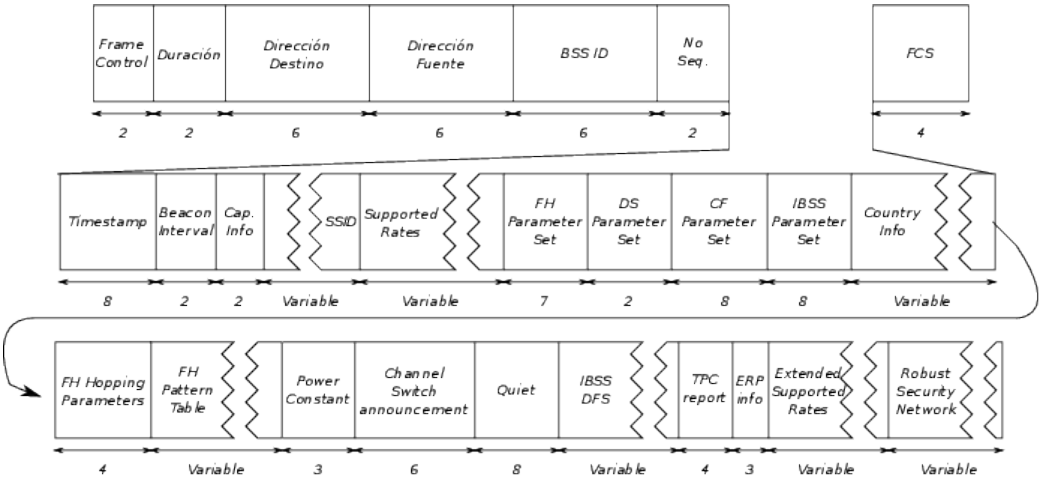


Figura 2.13: Estructura de una trama *Probe Response*

2.7. Conexión a una red IEEE 802.11

El proceso de conexión a una red IEEE 802.11 puede ser dividido en los siguientes pasos: descubrimiento de las redes disponibles, selección de un candidato, autenticación y asociación a la red seleccionada. Durante la etapa de descubrimiento la MS obtiene una descripción de los AP disponibles en su entorno. Durante esta etapa se interrumpe el tráfico de datos. Luego, en el proceso de selección del candidato, se debe seleccionar uno de los AP, la selección puede ser realizada por el usuario de manera manual o automáticamente siguiendo alguna estrategia previamente definida. Finalmente, el proceso de autenticación y asociación implica un intercambio de tramas de la capa de control de acceso al medio (MAC: *Medium Access Control*) y posiblemente involucra tráfico en capas superiores, dependiendo de la configuración de la

red. La Figura 2.14 se observa el intercambio de tramas de capa MAC en una red que utiliza autenticación OSA.

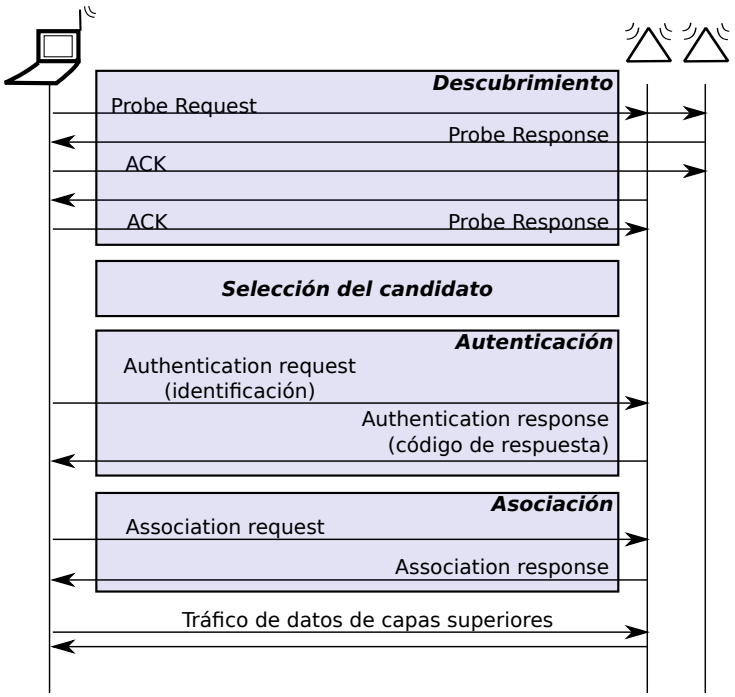


Figura 2.14: Proceso de conexión a una red con Sistema de Autenticación Abierta

2.8. Descubrimiento de redes IEEE 802.11

El proceso de descubrimiento es realizado mediante el escaneo de los canales disponibles. El estándar divide la banda de los $2.4\,GHz$ en 11 canales (pueden ser 13 o 14 en algunos países), por lo que la MS debe ajustar su configuración para explorar distintos canales, impidiendo el tráfico de red durante el escaneo.

De acuerdo con el estándar [1], hay dos tipos de escaneo: pasivo y activo. Durante el escaneo pasivo la MS itera sobre los canales disponibles, esperando en cada uno por *Beacons*, que contienen información sobre la red. La periodicidad de transmisión de los *Beacons* depende de la configuración de cada AP. Por otro lado, en el escaneo activo, la MS itera sobre los canales disponibles

difundiendo Probe Requests (P_{rq}). Luego de transmitir cada P_{rq}, espera por eventuales respuestas de los AP en forma de tramas Probe Responses (P_{resp}). Los P_{rq} son transmitidos en *broadcast* y los P_{resp} en *unicast*.

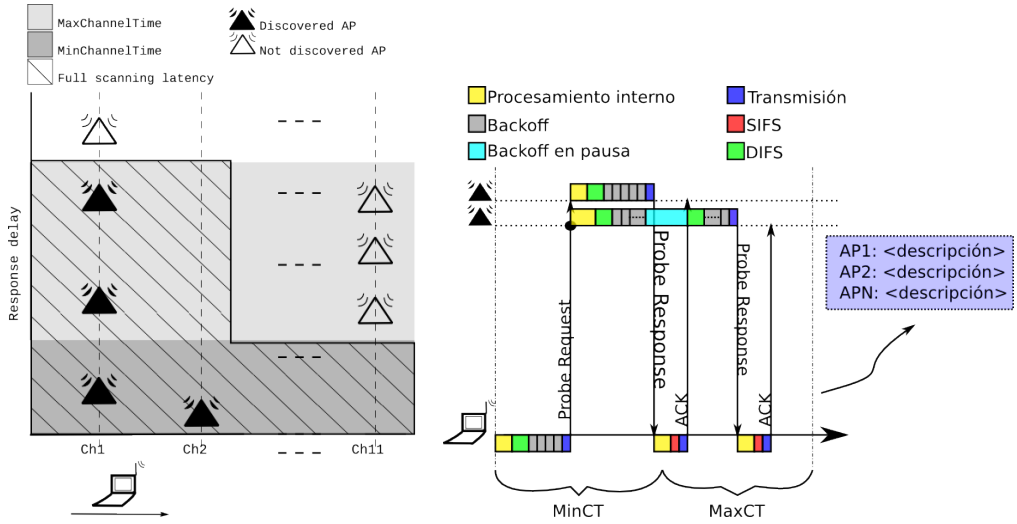
El estándar indica el siguiente algoritmo para el escaneo activo:

1. Acceder al medio siguiendo el procedimiento DCF (ver Sección 2.5.1);
2. Transmitir un P_{rq} a cada dirección indicada en la llamada o, si no se indica dirección, al *broadcast*;
3. Iniciar el temporizador (T) en cero;
4. Si no se detecta actividad en el canal antes que T alcance MinChannelTime (MinCT), cambiar al siguiente canal y repetir el proceso. En caso contrario, esperar hasta que T alcance MaxChannelTime (MaxCT) y repetir el proceso.

Como se mencionó, se tienen dos tiempos de espera: MinCT y MaxCT. El primero permite detectar actividad en el canal y que la MS reciba eventuales P_{resp}, el segundo añade un tiempo de espera de manera que los P_{resp} puedan resolver el acceso al medio de manera apropiada, pues en presencia de varias estaciones aumenta la posibilidad de colisiones y retransmisiones, incrementando el tiempo necesario para que la MS reciba las respuestas. Los valores para MinCT y MaxCT no son especificados en el estándar, dando flexibilidad a los fabricantes ajustarlos.

Como se muestra en la Figura 2.15a, una MS difunde un P_{rq} en un canal dado. Luego, como se representa en los iconos AP, los P_{resp} acceden al medio y se ordenan siguiendo el mecanismo CSMA/CA. Como se puede observar en la figura, la posición de los iconos en el tiempo forman la topología observada por la MS, que depende del ajuste apropiado de los temporizadores. En el área sombreada se indica una aproximación de la duración total del escaneo, que está estrechamente relacionada con la duración de MinCT y MaxCT y de la secuencia de canales revisados [11]. Como sugiere [8] y siguiendo la Figura 2.15, la duración del escaneo completo (ϕ) está acotada por la Ecuación 2.3, donde N_{ch} corresponde al número de canales escaneados. Note que la expresión considera $MaxCT \geq MinCT$ y que ambos se inicializan simultáneamente.

$$N_{ch} \times MinCT \leq \phi \leq N_{ch} \times MaxCT \tag{2.3}$$



(a) Topología observada (b) Detalles del escaneo activo

Figura 2.15: Escaneo activo en redes IEEE 802.11

2.9. *Handover* IEEE 802.11

El *handover*, también llamado *handoff*, es el cambio del AP con el que la estación mantiene conexión. En el caso de las redes IEEE 802.11, un *handover* implica la ejecución de varias acciones que acarrean la interrupción de la transmisión de tramas. La duración de la interrupción se conoce como *handover time*. Esta interrupción supone un impacto en la conexión de red desde el punto de vista de las capas de red superiores, por lo que es deseable reducir el *handover time* tanto como sea posible de manera que la interrupción no sea percibida o, a lo sumo, el retardo experimentado se mínimo [24].

2.9.1. Fases del *handover*

El proceso de *handover* puede ser dividido en cuatro etapas [25]:

1. Detección de la necesidad de *handover*: requiere vigilar la calidad del enlace. Varías métricas pueden ser utilizadas, la más común es tomar la intensidad de la señal. Esta etapa puede ser ejecutada sin interrumpir la conectividad.

2. Descubrimiento de AP disponibles, llamado escaneo: el objetivo del es-

caneo es identificar los AP disponibles y sus características. El escaneo puede ser activo o pasivo y su ejecución podría implicar la interrupción de la conexión. Según [8], el escaneo activo ocupa alrededor del 90 % del *handover time* .

3. Re-autenticación: debido a la autenticación, es necesario que una estación muestre su identidad antes de transmitir tramas a la red.

4. Re-asociación: permite mover la asociación desde el AP origen al AP con el cual estará asociado luego de la ejecución del *handover*. Este proceso informa al DS de que la estación se ha movido de un BSS a otro.

Cada una de las fases del *handover* contribuye con retardos e interrupciones al proceso de conexión. Por ejemplo, los experimentos mostrados en [24] indican que el descubrimiento ocupa alrededor de $87\,ms$, mientras que las etapas de autenticación y asociación ocupan $1\,ms$. Las pruebas se realizaron en un entorno controlado, con la MS configurada con una tarjeta de red (NIC: *Network Interface Card*) marca ORiNOCO.

2.10. Aspectos de las ondas electromagnéticas

Las comunicaciones inalámbricas aprovechan el espectro electromagnético para transmitir información. Para ello la información es codificada en ondas de radio. Estas ondas son afectadas y alteradas por aspectos como la **absorción**, que las debilita cuando atraviesan algún obstáculo. El nivel de absorción varía en función de la longitud de onda y del material que forma el obstáculo. Por otro lado, los obstáculos también causan **reflexión**, provocando que la onda cambie su curso, causando efectos como la **multiruta** (la señal alcanza el objetivo a través varias rutas y en momentos diferentes). Por otro lado, las **interferencias** también juegan un papel importante en la variación de las señales de radio utilizadas por las redes IEEE 802.11, que operan en bandas que no requieren licencia. Las interferencias son ocasionadas por otras ondas que se solapan con la onda de interés, produciendo una **interferencia constructiva** o **interferencia destructiva**. En la interferencia constructiva las ondas se suman, mejorando la transmisión. En la interferencia destructiva las ondas se anulan, degradando la transmisión [21].

Como se puede observar, estos aspectos provocan variaciones no deterministas en las ondas electromagnéticas utilizadas por las redes IEEE 802.11, que repercuten en transmisión de las tramas. Esto es especialmente relevante en los despliegues en ciudades, donde existen una gran cantidad de redes y obstáculos, con formas y materiales diferentes.

Capítulo 3

Escaneo de redes IEEE 802.11: Estado del Arte

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

1. *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 involucradas. Esto con el único fin de acelerar el proceso de descubrimiento.

    - 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.

2. *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 [12, 26, 27].

3.1. Caracterización del escaneo activo

Distintos estudios [8, 12, 28] han reportado diferencias en las estrategias de escaneo activo utilizadas por interfaces de red IEEE 802.11 distintas. Las diferencias incluyen: uso de caché para mantener información del entorno [29], secuencia de canales explorados [11, 30], frecuencia de ejecución del proceso de escaneo [31–33] , posibilidad de interrumpir el escaneo [34, 35], número de tramas utilizadas durante el proceso [8], entre otros.

En [28] se presentan experimentos que hacen uso de una misma interfaz IEEE 802.11 y distintos controladores, 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, haciendo uso del mismo controlador con interfaces de fabricantes distintos de red también altera el escaneo activo. Todo esto sugiere que el comportamiento del escaneo activo es alterado por distintos factores, entre ellos: el hardware de la interfaz IEEE 802.11 y su controlador.

El estudio presentado por Gupta et al. [8] fue de los primeros que evaluaron y caracterizaron las interfaces IEEE 802.11 en función del escaneo activo. Es importante destacar que las pruebas presentadas en [8] 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 Probe Request (P_{rq}), el número total de P_{rq} transmitidos en todos los canales, número de P_{rq} 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 [28]. También detectaron que, dependiendo del algoritmo de escaneo activo, uno o más P_{rq} pueden ser transmitidos por la estación móvil (MS: *Mobile Station*) cuando se está revisando un canal particular. Así mismo, encontraron diferencias en el tiempo dedicado a la revisión de cada canal. De acuerdo con estudios realizados, las interfaces invierten un mayor tiempo en revisar el canal 6 [28].

3.2. 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 software (en forma de módulos del kernel), de manera que las interfaces IEEE 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 driver/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 Figura. 3.1, que a diferencia del algoritmo descrito en la norma [1], sustituye los temporizadores MinChannelTime (MinCT) y MaxChannelTime (MaxCT) por uno único denominado `IEEE80211_CHANNEL_TIME`. En el kernel se utilizan dos tiempos de espera: `IEEE80211_SCAN_PROBE_-DELAY` e `IEEE80211_CHANNEL_TIME`. El primero es el tiempo que espera la MS antes de transmitir el P_{rq} y luego que la interfaz ajusta el canal de operación. El segundo es el tiempo que la interfaz permanece a la espera de Probe Response (P_{resp}) en cada canal luego de transmitido el P_{rq}. Como se puede ver, esta estrategia hace uso de un único temporizador luego de transmitido el P_{rq}. Además, el tiempo de espera en el canal es independiente de la presencia o no de actividad en el canal.

Los valores de `IEEE80211_PROBE_DELAY` e `IEEE80211_CHANNEL_TIME` dependen de la configuración del kernel y son calculados de acuerdo a Ecuación 3.1 y Ecuación 3.2.

$$\text{IEEE80211\_PROBE\_DELAY} = \text{HZ} \;/\; 33 \tag{3.1}$$

$$\text{IEEE80211\_CHANNEL\_TIME} = \text{HZ} \;/\; 33 \tag{3.2}$$

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 en la configuración por omisión para versiones recientes del kernel de Linux, donde `HZ=1000`, `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 3.3 los estudios sobre la optimización del proceso de descubrimiento, en

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

Figura 3.1: Escaneo en el kernel de Linux

la Sección 3.4 los trabajos sobre la optimización de los temporizadores usados en el escaneo y en la Sección 3.5 se comentan sobre el proceso de escaneo y su relación con el *handoff*.

3.3. Sobre la optimización del proceso de descubrimiento

En [8] se presenta un estudio detallado del proceso de *handoff* de capa MAC y su duración en redes *indoor*. 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 MS espera en cada canal luego de transmitido un P_{rq}, 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 está acotada por la Ecuación 3.3.

$$N_{ch} \times MinCT <= t <= N_{ch} \times MaxCT \tag{3.3}$$

Los experimentos realizados por [8] consisten de tres redes IEEE 802.11b que coexisten en un edificio, una MS y un *sniffer* usado para capturar los paquetes intercambiados por la MS y la red. Realizaron distintas pruebas, cada una caracterizada por el uso de una interfaz IEEE 802.11 particular y una de las redes, en total se probaron nueve escenarios combinando tres interfaces de red en la MS (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 IEEE 802.11 del punto de acceso (AP: *Access Point*) y las MS) 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 IEEE 802.11 presentan distintos algoritmos de escaneo, destacando las siguientes diferencias:

- La interfaz Cisco transmite once (11) P_{rq}, uno por cada canal, con un tiempo de espera por canal de entre $17\,ms$, si no se reciben P_{resp} (MinCT) y $38\,ms$, en caso contrario (MaxCT);
- La interfaz Lucent transmite solo tres P_{rq} 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 P_{resp};
- 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 [24] indican que el tiempo de respuesta de los AP 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 AP y la congestión de la red puede aumentar. Así mismo, en [36], se revisa la Ecuación 3.4, que fue introducida por Montavont et. al en [31]. 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.

$$S = Ch_o \times T_o + Ch_v \times T_v \tag{3.4}$$

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 MS detecta actividad en un canal pero sin obtener P_{resp} se desperdicia $MinCT$;

2. Cuando la MS revisa un canal vacío se desperdicia $Probe\,Delay + MinCT$;

3. Por último el tiempo que transcurre desde que se recibe el último P_{resp} hasta que se cumple MaxCT. En este caso se desperdicia un intervalo dependiente de cada situación.

En [11] 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 AP alguno 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 Ecuación 3.5, que relaciona MinCT, MaxCT y la probabilidad $P(ch)$ de actividad en el canal ch.

$$L = \sum_{ch=1}^{n} (1 - P(ch)) \times MinCT + P(ch) \times (MinCT + MaxCT) \quad (3.5)$$

En [36] 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 AP). 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 AP. Los resultados son confirmados en [11], donde realizaron pruebas experimentales con distintas configuraciones de despliegues de AP 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 que los valores de MinCT y MaxCT deben estar en los intervalos indicados en las Ecuaciones 3.6 y 3.7, 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 P_{rq}.

$$6\,ms \leq MinCT \leq 34\,ms \tag{3.6}$$

$$8\,ms \leq MaxCT \leq 48\,ms \tag{3.7}$$

Otro resultado presentado en [11] indica que la presencia o no de tráfico en la red altera considerablemente el tiempo de respuesta de los AP, por ejemplo, en un despliegue ideal, donde solo se tiene un AP en los canales no solapados y sin tráfico en la red, obtienen un P_{resp} 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 IEEE 802.11. De acuerdo con Ecuación 3.3 y Ecuación 3.5, 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, la ejecución por etapas del algoritmo de escaneo o el uso de sistemas que asistan el descubrimiento aprovechando conocimiento previo de la topología.

3.4. Optimización de los temporizadores del escaneo

Tal como se observa en la Ecuación 3.3 y la Ecuación 3.5, 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.

3.4.1. Estrategias estáticas

En [24] los autores estudian técnicas para reducir la duración del *handoff* en redes IEEE 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 MS conocer que es necesario iniciar el proceso de *handoff*. La búsqueda

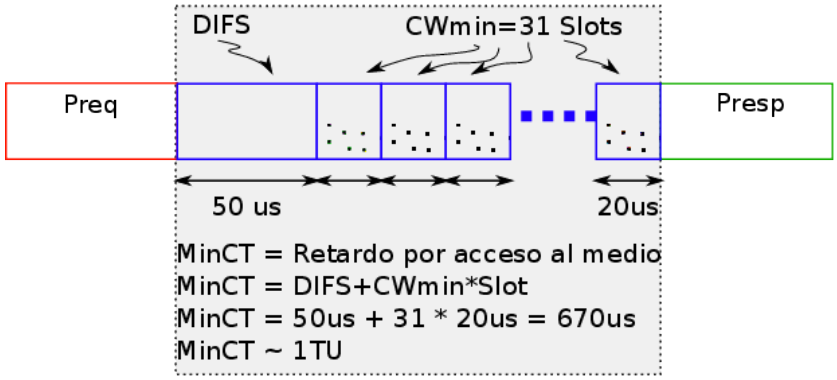


Figura 3.2: MinCT para redes IEEE 802.11b

permite que la MS conozca los AP disponibles en el entorno. Finalmente, durante la ejecución, la MS selecciona uno de los AP del entorno y establece un nuevo enlace con este último. La búsqueda se refiere a la ejecución del proceso de descubrimiento de los AP, 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 AP para responder un P_{rq} dado que el AP y el canal se encuentran desocupados. Si se desprecia el tiempo de generación de P_{rq} y P_{resp}, MinCT corresponde al tiempo que el AP debe esperar para acceder al medio. Éste es calculado en la Figura 3.2. Los autores de [24] 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 AP que se encuentre compitiendo. En [24] 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 AP sobrecargados.

Los trabajos presentados en [33] y [37] establecen valores aún menores para MaxCT, fijándolo en $5\,ms$ el primero y $6\,ms$ el segundo. En [33], muestran el resultado de múltiples mediciones de los tiempos de respuesta de los AP bajo distintas condiciones: sin tráfico, con tráfico TCP desde y hacia el AP y con tráfico UDP desde y hacia el AP. En promedio, el tiempo de respuesta

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

de un AP ante un P_{rq} 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 P_{resp}. Estos resultados contrastan con otros estudios, particularmente los presentados en [37], que indica que alrededor del 40 % de todas las respuestas de los AP 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 AP operando, pues las pruebas experimentales reportadas en [33] se realizaron en una oficina con solo dos AP en operación, mientras que en [37] se realizaron en un campo universitario, donde se reportó la presencia de diez AP en promedio. Sin embargo, los resultados indican que los AP 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 AP con buena señal es de $6.054\,ms$ con una desviación estándar de $1.58\,ms$. Tomando en cuenta estos datos, [37] utiliza $6\,ms$ para MaxCT. En [38] se realizan simulaciones y pruebas en ambientes controlados en donde estudian los valores de MinCT y MaxCT. Los autores de [38] 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 P_{resp} recibidos en cada canal y con diferentes configuraciones del despliegue de los AP. La principal observación de los experimentos realizados en [38] 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.

3.4.2. Estrategias dinámicas

Otra posible estrategia, presentada en [11] y discutida ampliamente en [39], 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 AP. De forma análoga, los valores de MinCT y MaxCT son incrementados en la medida en que no se detecten AP. La ejecución del algoritmo es como se muestra en la Figura 3.3, donde los valores de MinCT y MaxCT son incrementados simultáneamente en $\Delta T = 50\,\%$ de últimos valores exitosos (valores de MinCT

```
1: N = número de AP descubiertos en el canal i
2: Q = mayor señal de entre los AP 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 3.3: Escaneo dinámico [11]

y MaxCT donde se detectó al menos un AP), 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.

3.5. 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 involucrados. 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.

3.5.1. Escaneo periódico

Como se ha mencionado, una MS 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 menor duración.

En [31] 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 AP disponibles antes de iniciar el *handoff* y mientras la MS mantiene conexión. El escaneo anticipado permite construir una lista de los AP disponibles. En la lista se mantiene el identificador del AP (dirección MAC), el canal en el que está operando y el SSID (*Service Set Identifier*).

En el proceso descrito en [31], la MS inicia una fase del escaneo usando dos periodos distintos. Estos periodos dependen de la calidad de la señal del AP con el que mantiene la conexión actual. Si la señal es suficientemente buena ($[-50\,dBm; -75\,dBm]$), la MS 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 AP 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 MS descubre al menos un AP durante el escaneo anticipado, el periodo se vuelve a fijar a los valores iniciales, es decir, 1 o 2 segundos.

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

En Liao y Gao [32] se presenta una estrategia denominada *smooth scanning* para 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 MS en movimiento, es posible que al finalizar todas las subfases se tenga información des-actualizada. Una MS 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 MS se desplaza a velocidad de peatón (unos $1.5\,m/s$), entonces la MS se desplazará unos $3\,m$, por lo que este método

puede ser efectivo si los AP presentan un solapamiento de más de $3\,m$.

La estrategia presentada en [33], similar al *smooth scanning*, es utilizada durante el *handoff* en redes IEEE 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 AP y esos AP utilizan el mismo SSID que el del AP actual. De igual manera, los AP con los que la MS ha mantenido conexión también son registrados.

En [34] y [35] 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 [34] y [35] se aprovecha del buffer con que cuentan los distintos elementos de una red. Así, la MS 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 AP o porque la señal del AP 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*.

3.5.2. Escaneo selectivo

Como se mencionó en las secciones anteriores, durante un escaneo activo la MS 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 [29], 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 des-

cubrimiento. 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 P_{rq} por cada canal y se espera por respuesta de los AP (P_{resp});

2. Los canales en los que se recibe al menos un P_{resp} 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 AP;

3. Se selecciona el mejor de entre los AP encontrados. Los autores de [29] califican los AP de acuerdo al nivel de la señal recibida (nivel de RSSI);

4. El canal en el que opera el AP 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 AP adyacentes y operando en el mismo canal son bajas;

5. Si no es posible seleccionar un AP, 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 AP, 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 AP 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 AP actual (AP al que se encuentra conectada la MS) como campo

clave. Luego, cada entrada en la tabla contiene una lista de las direcciones MAC de los AP adyacentes al AP actual y que fueron descubiertos durante los escaneos selectivos realizados previamente. Esta lista es creada por la MS a medida que se desplaza por el entorno y realiza *handoff* de un AP a otro. La tabla que contiene el caché está limitada a 10 filas y 2 columnas, por lo que la MS mantendrá información sobre el entorno de los últimos 10 AP con la que estuvo conectado, y en cada caso solo los 2 AP con mejor señal serán registrados. El caché es aprovechado de la siguiente manera:

1. Cuando la MS se asocia a un AP, el AP y la información del entorno (otros AP 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 AP actual);

3. Si no se logra encontrar un AP, entonces se realiza el escaneo selectivo descrito anteriormente;

Una estrategia diferente es presentada en [30], que propone utilizar la probabilidad de que un AP se encuentre operando en el canal C para determinar la secuencia en que se deben revisar los canales del espectro. En [30] el orden en que se realiza la revisión de los canales resulta crítico, pues el escaneo presentado termina cuando se encuentra un AP que provea conectividad. Bajo condiciones encontradas en la práctica, en donde los AP se distribuyen principalmente en los canales no solapados 1, 6 y 11, la estrategia presentada en [30] encuentra un AP disponible luego de revisar 3.64 canales en promedio.

3.5.3. Escaneo asistido

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 AP y en los enlaces se representa la ruta de movilidad posible entre los AP. 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 AP mantiene un GV con la información de su entorno, es

```
1: for all Canal i donde existen AP en el entorno do
2:     Difundir P_rq en el canal i
3:     Iniciar temporizador
4:     while True do
5:         Recibir P_resp
6:         if Se recibió P_resp antes de que MinCT expire then
7:             break
8:         else if Los AP 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 3.4: Escaneo utilizando GV

decir, mantiene una lista de los AP vecinos. Las estaciones obtienen el GV local del AP actual una vez que se ha establecido el enlace. Durante un *handoff*, las MS transmiten información sobre el AP anterior al AP actual, de esta manera el AP actual es capaz de conocer la información de los AP a su alrededor y al mismo tiempo construir el GV que le corresponde. Cuando una MS establece un enlace con un AP, éste le transfiere información sobre el entorno, de esta manera la MS 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 AP debe descubrir y mantener registro de las características de su entorno, lo que implica modificaciones en la funcionalidad y forma de operación de los AP. 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 AP de modelo, hardware y software diferente [17].

En [40] utilizan un GV global que mantiene información de toda la red en la MS. Gracias al GV, la MS 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 Figura 3.4 se describe el proceso presentado en [40], que modifica el algoritmo de escaneo completo para hacer uso del GV.

En [41] se presenta una estrategia similar a la descrita en [40], pero sugiere

aprovechar la información almacenada en los GV para transmitir los P_{rq} utilizando *unicast* en lugar de *broadcast*.

Otra modificación a la estrategia de los GV, denominada *GV-Podado* y propuesta en [40], consiste en recolectar información sobre el solapamiento o no de los AP, es decir, los AP que no pueden ser alcanzados simultáneamente por una MS. Según esta estrategia, si AP_i y AP_j son no solapados y se recibe un P_{resp} de AP_i, entonces es imposible recibir P_{resp} de AP_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 [40] indican mejoras respecto al algoritmo escaneo completo de 80.7 % y 83.9 % para las estrategias GV y GV-Podado respectivamente.

En [31] presentan y evalúan una estrategia denominada "AP Adyacentes". Ésta se basa en el hecho de que cada AP conoce su entorno, por lo que puede identificar los AP que le son adyacentes. Cuando las redes son desplegadas, los AP pueden ser configurados con una lista de los AP adyacentes en términos de área de cobertura. Esta información es mantenida por la lista de AP vecinos y es transmitida a las estaciones. Luego, la MS tiene información sobre el entorno y en caso de requerir cambiar de AP; durante un *handoff* por ejemplo, primero intentará asociarse con los AP de la lista de adyacentes, si la asociación fracasa con todos los AP de la lista, entonces se ejecuta el proceso de descubrimiento descrito en el estándar.

Capítulo 4

Caracterización de despliegues espontáneos

Las redes encontradas en las ciudades presentan características de despliegues espontáneos, realizados sin coordinación ni planificación central, con equipos y configuraciones desconocidas. Para estudiar y caracterizar estos despliegues se preparó un conjunto de experimentos "*indoor*" y "*outdoor*". Con los experimentos "*indoor*" se pretendió preparar y evaluar la plataforma de pruebas que luego será utilizada en la campaña de medidas en despliegues "*outdoor*" reales. La campaña de medidas en despliegues reales se realizó en la ciudad de Rennes, Francia[1], a lo largo de 11 km del recorrido ilustrado en la Figura 4.1. La recolección consistió en un usuario caminando a lo largo del recorrido, con una estación móvil (MS: *Mobile Station*) que realizaba un escaneo completo, incluyendo los canales 1 al 11, a intervalos de 1 segundo. En cada escaneo se transmitió un Probe Request (P_{rq}) y espera Probe Response (P_{resp}) durante 250 ms. Durante la campaña se recolectó información de 3441 conjuntos de servicio básico (BSS: *Basic Service Sets*) o redes diferentes[2].

4.1. Plataforma experimental

Para recolectar la información de las redes se diseñó e implementó una plataforma que realizaba el escaneo de redes IEEE 802.11 continuamente, a la vez que recolectaba información sobre la red: identificador del conjunto

[1]En colaboración con el laboratorio 4G de Telecom Bretagne

[2]En algunos casos se detectó más de un BSS operando en el mismo hardware.

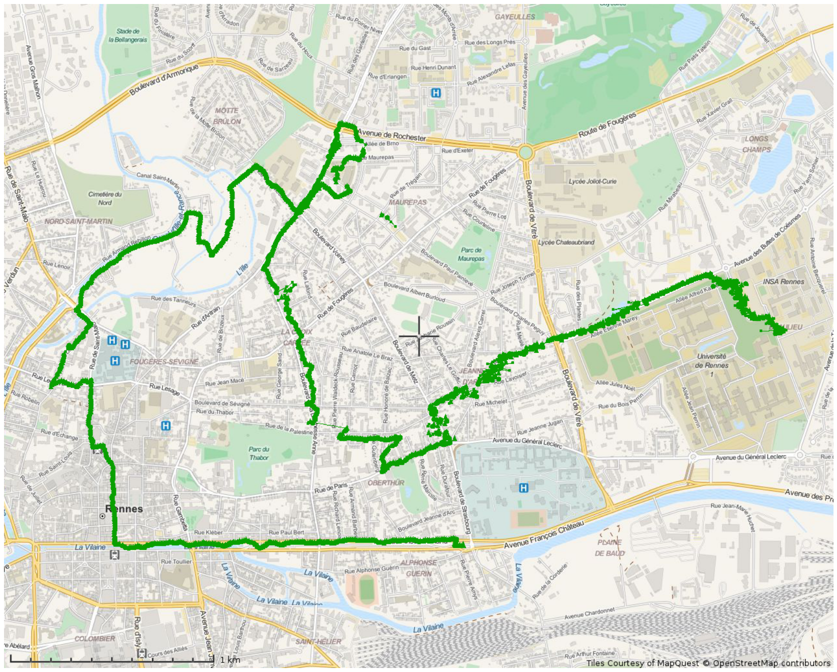


Figura 4.1: Ruta de la campaña de medidas

de servicio (SSID: *Service Set Identifier*), Identificador del Conjunto de Servicio Básico (BSSID: *Basic Service Set Identifier*), mecanismo de seguridad utilizado y canal en el que operaba. Así como también del proceso de descubrimiento: latencia, retransmisiones y potencia de los P_{resp} registrados. Los principales componentes de la plataforma son:

- Computador portátil, marca Hewlett-Packard, modelo nc-2400;
- Interfaz de red, marca Intel, modelo PRO/Wireless 3945ABG-Golan. Operando con el módulo por defecto del kernel de Linux;
- Debian GNU/Linux Jessie;
- Kernel de Linux, versión 3.11-rc6, modificado de acuerdo a lo indicado en la Sección 4.2;
- Herramienta `iw`[3], versión 3.13;

[3]http://wireless.kernel.org/en/users/Documentation/iw

- Conjunto de programas en *Bash* para automatizar las pruebas.

La herramienta `iw` permite iniciar el escaneo activo y retorna información sobre las redes disponibles, sin embargo, no muestra información sobre el intercambio P_{rq}—P_{resp}. Entonces, para registrar el intercambio P_{rq}–P_{resp} y medir su latencia se modificó el kernel según lo descrito en la siguiente sección.

4.2. Latencia de las respuestas

En el estudio del escaneo activo resulta de interés la latencia de las respuestas, esto es, el tiempo que transcurre desde la transmisión de un P_{rq} y cada uno de los P_{resp} que le suceden. Debido a que cada BSS debe responder a los P_{rq} que recibe, es común detectar respuesta de múltiples BSS, más aún, es posible que la MS detecte más de una respuesta de un BSS. Esto se debe a que los P_{resp} son transmitidos en *unicast*, por lo que son retransmitidos si no se recibe un ACK. De esta dinámica es claro que cada intercambio P_{rq}—P_{resp} tiene asociada una latencia. En la Figura 4.2 se observan las respuestas de dos BSS, AP1 transmite 1 P_{resp} mientras que AP2 transmite 2, para un total de 3 P_{resp} detectados, cada uno con una latencia diferente.

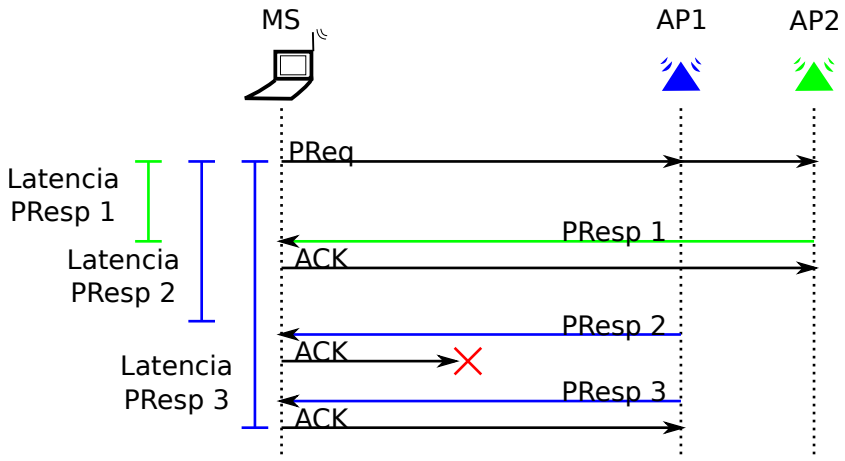


Figura 4.2: Latencia de un P_{resp}

Las computadoras instaladas con el kernel de Linux ofrecen la posibilidad de acceder y modificar a la implementación del escaneo activo. Versiones recientes del kernel de Linux implementan los mecanismos de acceso al medio

a través de un framework que mantiene parte de las operaciones en software. Esta perspectiva permite, por un lado, simplificar el soporte de nuevos dispositivos y la mejoras de los ya soportados. Por otro lado, simplifica la realización de estudios y ejecución de pruebas. El framework provee el módulo llamado `mac80211.ko`, que implementa el escaneo activo y otras operaciones de la capa control de acceso al medio (MAC: *Medium Access Control*). Aprovechando este framework se implementó un mecanismo para la medición precisa de la latencia, así como también el ajuste de los temporizadores asociados al algoritmo de escaneo activo [16].

La Figura 4.3 muestra los módulos y funciones más relevantes asociadas al escaneo en el kernel de Linux. Las funciones `ieee80211_scan_send_probe` (marcada A) e `ieee80211_scan_rx` (marcada B) forman parte del proceso de escaneo en el kernel de Linux y son de interés para medir la latencia. En A, se transmiten los P_{rq} hacia el medio y, en B se reciben los P_{resp}. Estas dos funciones se modificaron para registrar el paso de los P_{rq} y P_{resp}. De esta manera la latencia asociada a cada respuesta (P_{resp}) toma en cuenta los tiempos procesamiento dentro del kernel. Con esta información se calcula la latencia de cada respuesta (l_i), que está dada como la diferencia entre el instante de tiempo en que se recibe el P_{resp} i (t_i) y el instante de tiempo en que se transmitió el P_{rq} ($t_{P_{rq}}$). Entonces:

$$l_i = t_i - t_{P_{rq}} \tag{4.1}$$

Con el objeto de validar la plataforma se realizaron pruebas utilizando la metodología descrita en [8], que utiliza *sniffers* de red para registrar el intercambio de tramas en el medio. Dos *sniffers* se ubicaron suficientemente cerca de la MS que ejecuta el escaneo activo con el kernel modificado, de esta manera pueden capturar las tramas que van desde y hacia la MS. Luego, se ejecutaron 39 escaneos donde se midió la latencia utilizando ambos métodos.

La Figura 4.4 compara los valores de latencia calculada con cada uno de los métodos, estos muestran que las mediciones realizadas en el kernel son, en promedio, 1.8 ms mayores. Esta diferencia es atribuida al uso de *sniffers*, que capturan los P_{rq} y los P_{resp} cuando están en el medio, es decir, una vez que han salido de la MS y antes que la MS los registre, por lo que no se toman en cuenta los tiempos de procesamiento dentro de la MS. En el caso que nos compete, consideramos más apropiado medir la latencia desde el kernel, pues es más cercana a la experimentada por el usuario final a través de las interfaces disponibles a la capa aplicación.

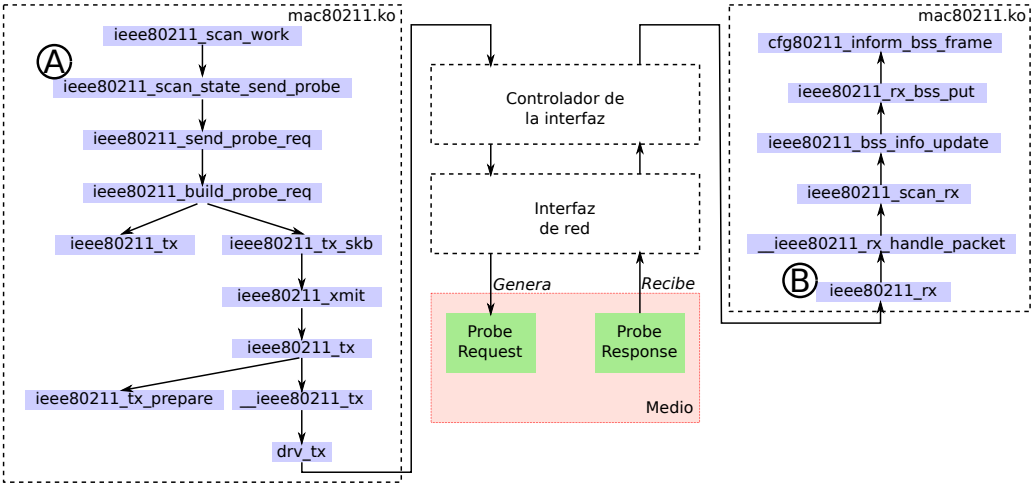


Figura 4.3: Ruta del P_{rq} y P_{resp} en el kernel de Linux

4.3. Experimentos controlados

En [17] condujimos una serie de experimentos con el objeto de preparar y probar la plataforma y la metodología, así como también para estudiar, a través de pruebas de caja negra, la respuesta de los punto de acceso (AP: *Access Point*) en diferentes despliegues, pero controlados y bien conocidos.

En cada uno de los experimentos descritos se utilizó la MS y uno o más AP según la configuración en evaluación. La MS se configuró para transmitir 1 P_{rq} por el canal 6, esperando durante $60\,ms$ antes de pasar al siguiente canal. Consideramos que $60\,ms$ es un tiempo suficiente para recibir todos los posibles P_{resp} en el escenario considerado de baja concurrencia.

Se realizaron 39 repeticiones de cada una de las configuraciones descritas más adelante. La totalidad de los experimentos se realizó en una edificación donde no operaban otras redes o dispositivos IEEE 802.11. De igual manera, se aseguró que dispositivos que operan en la misma frecuencia de radio, tales como microondas, teléfonos inalámbricos y dispositivos bluetooth estuvieran desconectados. La MS y los AP se ubicaron con línea de visión y a una distancia de $1.5\,m$, de manera que no se tenían obstáculos y se tenía una señal con buena ganancia.

En los experimentos se utilizaron los siguientes AP:

- **R1**: Linksys WRT54G, DD-WRT v24-sp2.

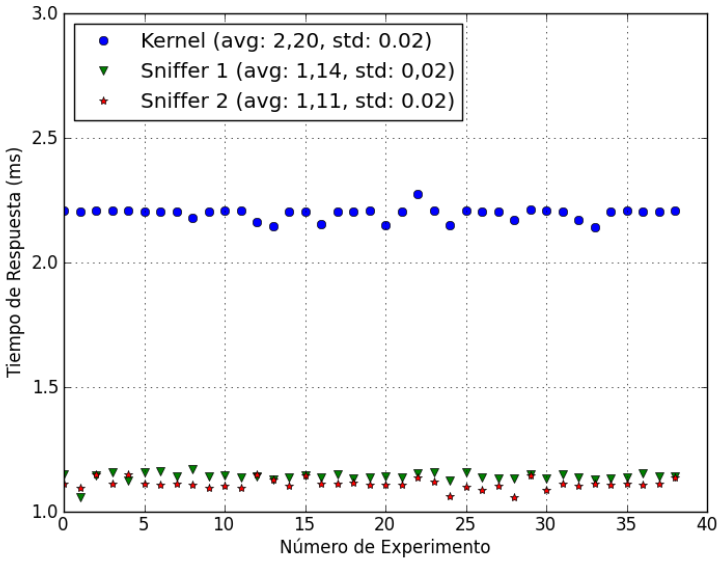


Figura 4.4: Latencia de los P_{resp} medida desde el kernel y desde el *sniffer*

- **R2**: Linksys WRT160N, v2.0.0.2.
- **R3**: Linksys WRT350N, v1.03.2.
- **R4**: TP-Link WR642G, v3.7.2.
- **R5**: Netgear WNR2000, v1.2.0.8NA.
- **R6**: Linksys WRT54G, DD-WRT v24-sp2.
- **R7**: Linksys WRT54G, DD-WRT v24-sp2.

- **Configuración 1**: con esta configuración se evalúa la diferencia en la latencia de respuesta para diferentes marcas y modelos de AP. Se realizó un total de 5 pruebas, cada una con único AP operando. Se usaron los AP: R1, R2, R3, R4 y R5.

  En la Tabla 4.1 se presenta la latencia media para cada modelo, se puede observar que hardware/firmware diferente implica diferencias en la latencia de los P_{resp}, los resultados coinciden con el presentado por [42],

Tabla 4.1: Latencia en los P_{resp} para diferentes AP

AP	Media (ms)	Desviación Estándar (ms)
R2	1.28	0.18
R3	1.93	0.06
R1	2.20	0.02
R4	2.66	0.50
R5	3.51	0.45

donde los autores reportan variaciones en la latencia para diferentes modelos de AP. Ellos atribuyen las variaciones a las diferentes heurísticas implementadas por los fabricantes [43].

- **Configuración 2**: en esta prueba se revisa el impacto de la contención en la latencia. En este caso se desplegaron varios AP con las mismas características (fabricante, modelo y firmware). Todos operando en el canal 6, las configuraciones restantes se mantuvieron con los valores por defecto. Inicialmente se puso en operación un AP (R1), luego dos (R1 y R6) y finalmente tres (R1, R6 y R7). La Figura 4.5 presenta la latencia del primer P_{resp} detectado. Se resalta que: 1) la latencia aumenta en forma proporcional con la ocupación del canal (el número de AP operando en el mismo canal). 2) incrementa la dispersión de la latencia a medida que aumenta la ocupación del medio. Este comportamiento puede ser explicado a través del proceso seguido para el acceso al medio (acceso múltiple por detección de portadora con evasión de colisiones (CSMA/CA: *Carrier Sense Multiple Access with Collision Avoidance*)), cada vez que una estación intenta transmitir una trama se debe revisar el medio (*carrier sense*), en caso de detectar el canal ocupado se debe realizar un *backoff*, que pone en espera la transmisión durante un período de tiempo aleatorio.

4.4. Experimentos en despliegues reales

En la campaña de medidas realizada en la ciudad de Rennes, Francia, en el recorrido de 11 Km mostrado en la Figura 4.1 se transmitieron un total de 11166 P_{rq}, de los cuales el 37.26 % recibió al menos un P_{resp} (Figura 4.7a). Se registraron 19165 P_{resp} en total, que fueron generados por 3441 BSS que

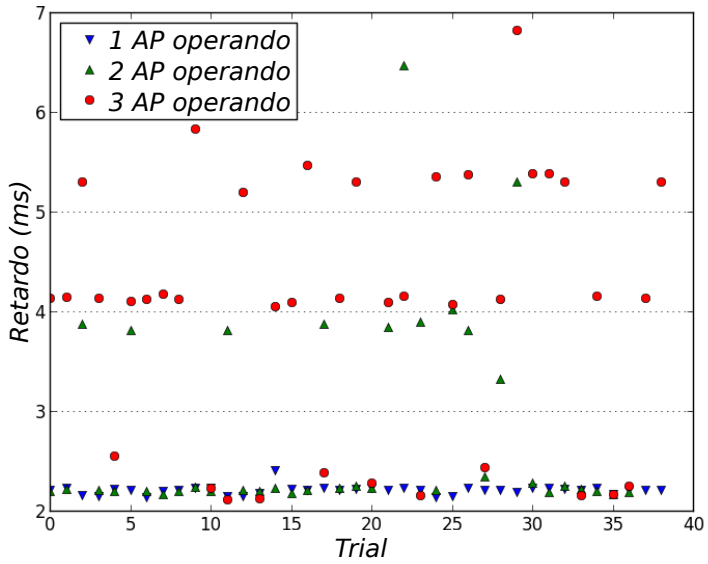
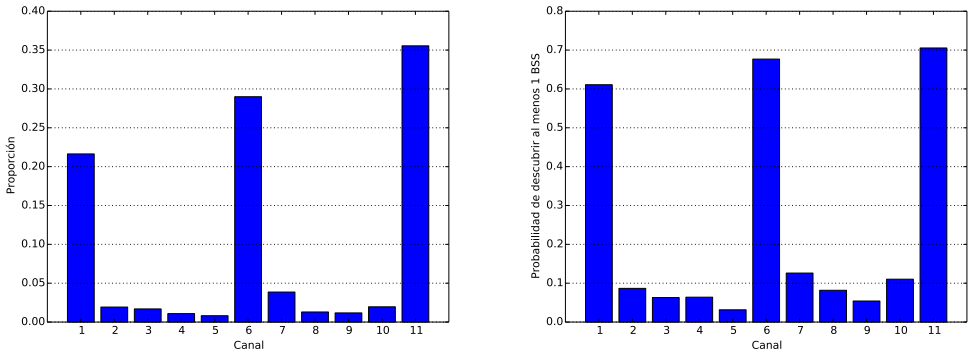


Figura 4.5: Latencia para el primer P_{resp} en función del número de AP operando.

operaban en 1937 AP, lo que implica que, en algunos casos, varias redes operan en el mismo dispositivo físico (ver Sección 4.6).

En la Figura 4.6a se observa la distribución de los canales, 86.18 % de las redes se encontraron en los canales 1, 6 y 11, esta combinación de canales es bien conocida debido a que no se solapan entre sí. De acuerdo con nuestra experiencia, es común que los fabricantes asignen uno de estos tres canales a la configuración por defecto de los AP. Por otro lado, en la Figura 4.6b se presenta la probabilidad de encontrar al menos un BSS en un canal dado, estimada como el número de veces que se descubrió al menos un BSS en relación con el número de escaneos realizados. Como es de esperar, las probabilidades más altas corresponden a los canales 1, 6 y 11, con valores de 0.62, 0.68 y 0.71 respectivamente.

La Figura 4.7a y la Figura 4.7b muestran, respectivamente, el número de P_{resp} y de BSS detectados con cada P_{rq} transmitido. En ambos casos, se incluyen los P_{resp} recibidos en los 11 canales del espectro estudiados así como las retransmisiones. La curva continua incluye la totalidad de los P_{rq} mientras que la curva punteada solo incluye los P_{rq} que obtuvieron al menos



(a) Distribución de los BSS en los canales (b) Probabilidad de encontrar al menos un BSS en un canal

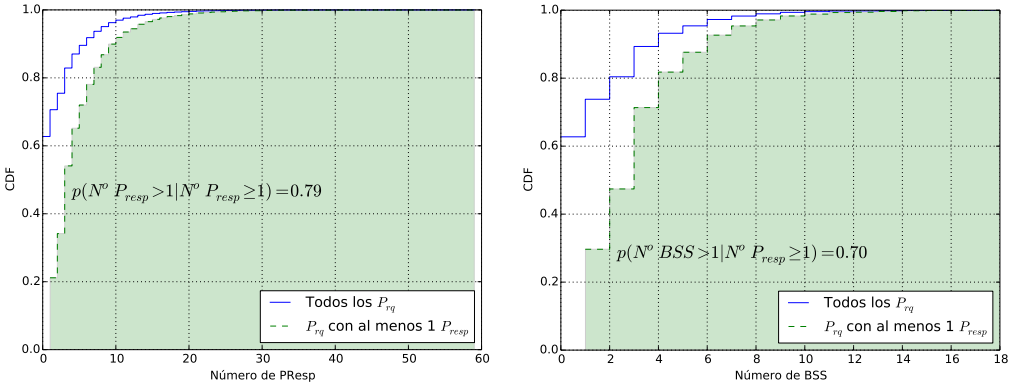
Figura 4.6: Utilización de canales

un P_{resp}. Se observó un máximo de 18 BSS descubiertos y 59 P_{resp} detectados luego de un P_{rq} (incluyendo retransmisiones). Notese que el 62.74 % de los P_{rq} no provocaron respuesta alguna.

De la Figura 4.7a se puede calcular la probabilidad de recibir dos o más P_{resp} dado que se recibió al menos uno (curva punteada). Tal como se muestra en la Ecuación 4.2 esta probabilidad es 0.79 (representado en verde en la figura).

$$\begin{aligned} p(N^o P_{resp} > 1 | N^o P_{resp} \geq 1) &= 1 - p(N^o P_{resp} \leq 1 | N^o P_{resp} \geq 1) \\ p(N^o P_{resp} > 1 | N^o P_{resp} \geq 1) &= 1 - 0.21 \\ p(N^o P_{resp} > 1 | N^o P_{resp} \geq 1) &= 0.79 \end{aligned} \tag{4.2}$$

De forma análoga, partiendo de la Figura 4.7b, en la Ecuación 4.3 se estima la probabilidad de descubrir dos o más BSS dado que se recibió al menos un P_{resp}. De acuerdo con los experimentos realizados esta probabilidad es 0.70, lo que indica una densidad grupal, que, como se discutió en la Sección 4.3, provoca: 1) aumento en la latencia de los P_{resp} y 2) mayor dispersión de la latencia de los P_{resp}. Recuerde que los P_{resp} recibidos por la MS pueden ser retransmisiones, por lo que cantidad de BSS descubiertos puede ser menor que el número de P_{resp} registrados.



(a) Número de P_{resp} detectados por P_{rq} (b) Número de BSS detectados por P_{rq}

Figura 4.7: Descubrimientos por P_{rq} (temporizador $= 250\,ms$)

$$
\begin{aligned}
p(N^oBSS > 1|N^oP_{resp} \geq 1) &= 1 - p(N^oBSS \leq 1|N^oP_{resp} \geq 1) \\
p(N^oBSS > 1|N^oP_{resp} \geq 1) &= 1 - 0.30 \\
p(N^oBSS > 1|N^oP_{resp} \geq 1) &= 0.70
\end{aligned} \tag{4.3}
$$

En la Figura 4.7b, al comparar la curva continua con la curva punteada, se observa una diferencia importante en la distribución del número de BSS descubiertas.

$$
\begin{aligned}
p(N^oBSS > 1) &= 1 - p(N^oBSS \leq 1) \\
p(N^oBSS > 1) &= 1 - 0.74 \\
p(N^oBSS > 1) &= 0.26
\end{aligned} \tag{4.4}
$$

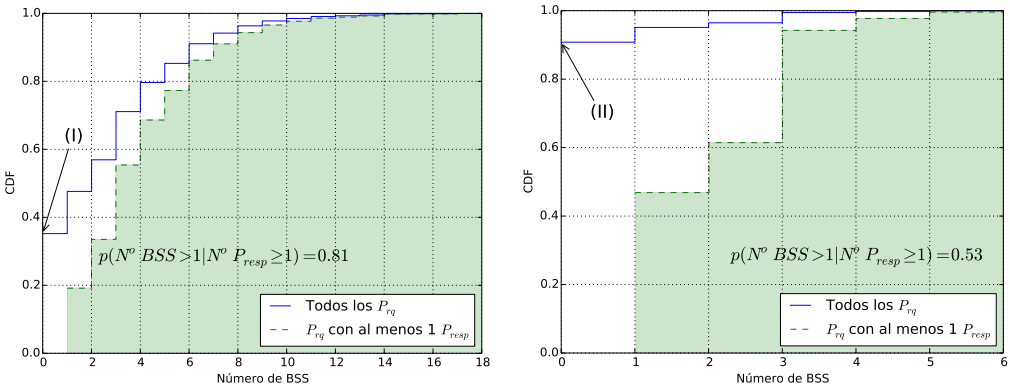
Adicionalmente, tomando en cuenta que el 86.18 % de los BSS operan en los canales 1, 6 y 11, dividimos los BSS detectados en dos grupos:

(a) los que operan en los canales 1, 6 y 11

(b) los que operan en los canales 2, 3, 4, 5, 7, 8, 9, 10

En la Figura 4.8 se discrimina la probabilidad de detectar 2 o más BSS de acuerdo a los grupos (A) y (B). Es claro que en el grupo (A) existe una

mayor probabilidad de encontrar múltiples BSS en operación y por tanto, respondiendo a los escaneos realizados por la MS, también destaca que en el grupo (B) se encontro un máximo de 6 BSS, mientras que en (A) se detecto hasta 18 BSS. Note además, que en la Figura 4.8a la probabilidad de encontrar cero BSS es 0.35 (marcada I), mientras que en la Figura 4.8b es de 0.91 (marcada II), lo que es consistente con las probabilidades mostradas en la Figura 4.6b.



(a) Canales 1, 6, 11 (b) Canales 2, 3, 4, 5, 7, 8, 9, 10

Figura 4.8: Número de BSS detectados por P_{rq} (temporizador = 250 ms)

Hemos observado el número de P_{resp} recibidos del mismo BSS, esto podría tomarse como un indicador de la eficiencia del medio y del proceso de descubrimiento, pues múltiples P_{resp} implican un incremento en la contención del medio causada por tramas con información repetida. De acuerdo con la Figura 4.9, el 80 % de los BSS se detectó con un único P_{resp}. De los restantes se recibieron al menos dos P_{resp}, es decir, la trama recibida más una retransmisión. Del total de los P_{resp} registrados el 34.45 % son retransmisiones, este número debe ser tomado como una cota inferior, pues es posible que algunas retransmisiones no hayan sido decodificadas por la MS. En este trabajo se considera que una trama es una retransmisión si se detecta otra trama con la misma información, es decir, el mismo número de secuencia, la misma dirección de origen y que responde al mismo P_{rq}. No se toma en cuenta el campo "*retry*", presente en las tramas IEEE 802.11, debido a que durante los experimentos realizados se observó que este campo es usado incorrectamente por algunos dispositivos, por ejemplo, transmitiendo todas las tramas con

este campo activo.

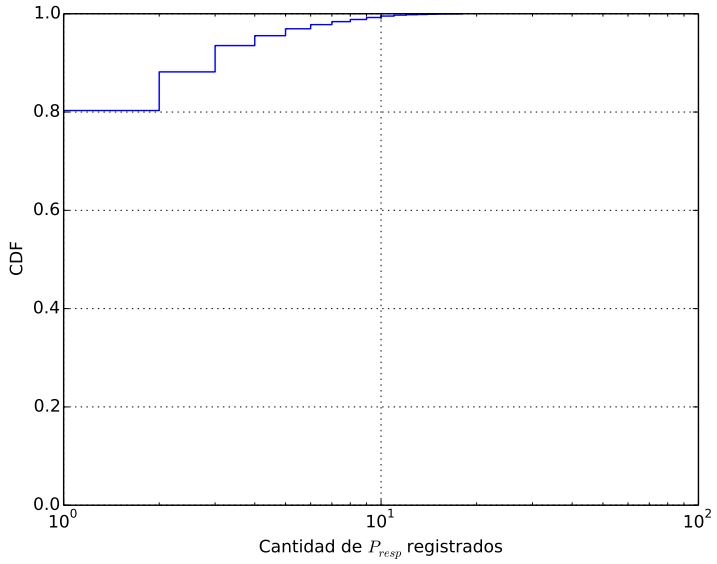


Figura 4.9: Número de P_{resp} del mismo BSS

Finalmente, una revisión a la potencia de la señal con que se registraron los P_{resp} (Figura 4.10) indica que más del 41 % de los P_{resp} fueron recibidos con una potencia superior a $-80\,dBm$, considerada suficientemente fuerte de acuerdo con el estándar [1].

4.5. Latencia de las respuestas

La latencia de las respuestas se resume en la Figura 4.11, que muestra la CDF de la latencia del primer y último P_{resp} luego de cada P_{rq} (se incluyen los 11 canales), esto es, el tiempo transcurrido entre la transmisión del P_{rq} y el primer y último P_{resp} detectado por la MS. Se puede observar que el primer P_{resp} es recibido en menos de $8\,ms$ en cerca del 80 % de las muestras recolectadas, mientras que el último es recibido antes de $36\,ms$ en el 80 % de las muestras ($41\,ms$ si se consideran las retransmisiones). Además el 98 % de los P_{resp} es recibido en $100\,ms$ o menos. Note además que el los valores de latencia son discretos debido a que las medidas se tomaron en términos de *jiffies*[4].

[4]En la configuración utilizada y descrita en la Sección 4.2 1 jiffie equivale a $1\,ms$

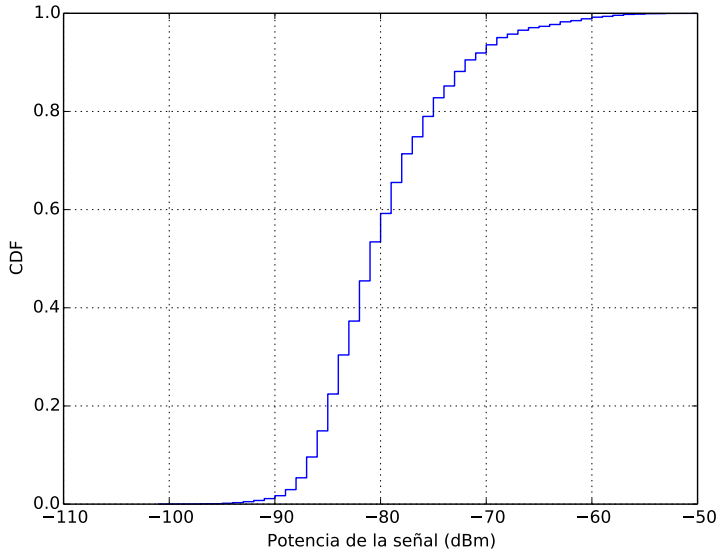


Figura 4.10: Distribución de la potencia entre los P_{resp} registrados

4.6. Múltiples redes en un AP

De acuerdo con lo observado en las muestras tomadas, es común que un AP sirva a más de un BSS simultáneamente. Hemos notado que los BSS en el mismo dispositivo AP utilizan un BSSID similar, así que usamos los BSSID en conjunto con la función de sincronización de temporizadores (TSF: *Timing Synchronization Function*) para identificar los BSS que operan en el mismo BSS. Se considera que dos BSS se encuentran en el mismo AP si los 4 bytes centrales del BSSID son iguales, por ejemplo, 11:AA:BB:CC:DD:00 y 22:AA:BB:CC:DD:12 son considerados iguales. Dado que se han observado BSSID duplicados y para reducir falsos positivos, la TSF reportada en los P_{resp} es utilizada para mejorar la clasificación, esto es, se considera que dos BSS operan en el mismo AP si el valor de la TSF reportado por los P_{resp} de cada BSS difiere en menos[5] de 120 s. Note que, debido a P_{resp} no detectados, este procedimiento puede asumir una densidad de BSS por AP inferior a la real.

El número de BSS por AP se distribuye de acuerdo a la Figura 4.12a, donde se puede observar que el 48.37 % de los dispositivos sirve más de un BSS, contribuyendo así al incremento en la escala de los despliegues. Una

[5]Se seleccionó este valor debido a la precisión de los datos registrados

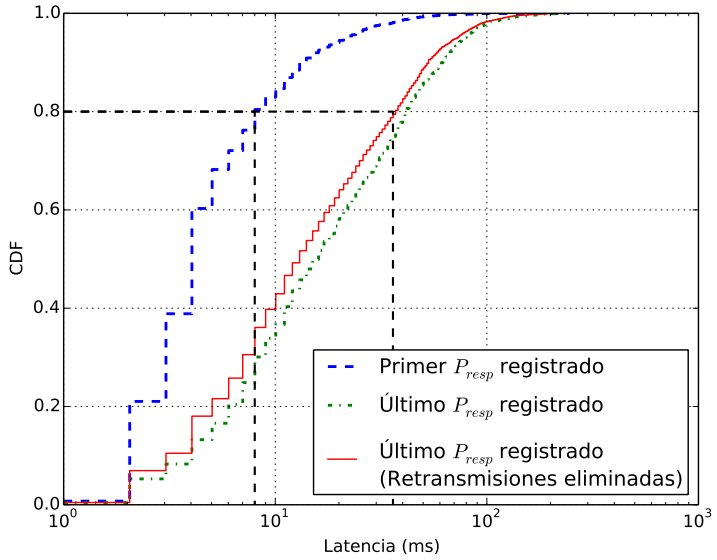
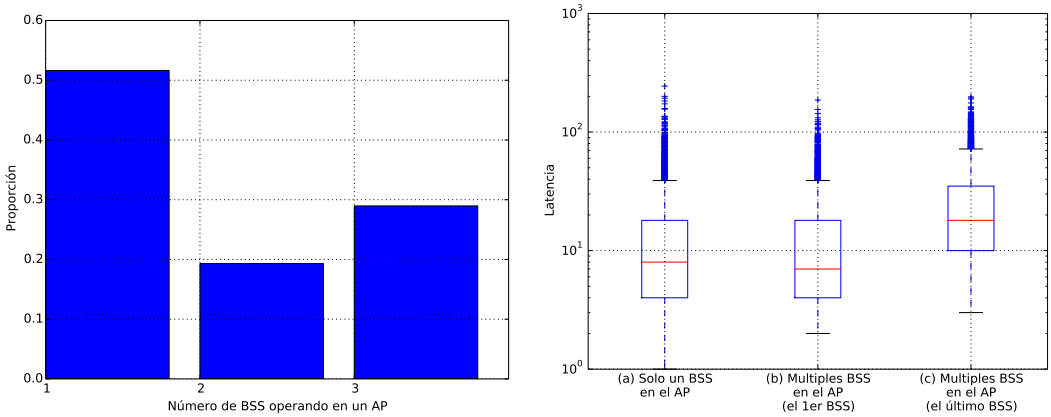


Figura 4.11: Distribución de los tiempos de respuesta de los P_{resp}

revisión detallada de los SSID indica que la mayor parte de estos BSS pertenecen a los ISP que operan en la ciudad, tales como *Free*, *SFR* y *Orange*. Estos configuran 3 redes: 1 privada para el suscriptor y dos que sirven para formar una red comunitaria [39, 44].

En la Figura 4.12b se presenta la latencia de los BSS. Se distinguen tres *box-plots* clasificados de acuerdo a la cantidad de BSS operando por AP. El *box-plot* (a) agrupa los BSS que operan solos en cada AP. Los *box-plots* (b) y (c) agrupan la latencia de los BSS que operan en AP compartidos, es decir, AP que soportan más de una red. En el *box-plot* (b) se presenta la latencia del primer BSS de cada AP (BSS con menor latencia). En el *box-plot* (c) se presenta la latencia del último BSS de cada AP (BSS con mayor latencia). Se puede observar que la densidad de BSS por AP afecta la latencia de los BSS, esto es, los P_{resp} generados por los BSS que operan solos tienen registrar una latencia más baja, esto puede ser ocasionado debido a que las BSS acceden al medio utilizando, posiblemente, interfaces de red virtuales que son atendidas secuencialmente por una única interfaz real.

Para aclarar el párrafo anterior suponga el siguiente ejemplo. En el AP-1 opera únicamente el BSS-11 con latencia de $5\,ms$. Por otro lado, en AP-2 operan tres BSS: BSS-21, BSS-22 y BSS-23. Cada uno con latencias de $3\,ms$, $10\,ms$ y $5\,ms$ respectivamente. Note que de los BSS que operan en AP-2,



(a) Número de BSS por AP (b) Latencia

Figura 4.12: Múltiples BSS en por AP

BSS-21 es el primero en responder, por lo sería representado en (b), mientras que BSS-22 es el último y sería representado en (c). BSS-23 no se representa. Por su lado, BSS-11 opera solo, por lo que estaría representado en (a).

Al comparar (a) y (b) se observa que en (b) la latencia tiene una cota inferior de $2\,ms$, mientras que en (a) las muestras pueden alcanzar latencias de $1\,ms$, sin embargo, no se nota una diferencia significativa en los cuartiles 1, 2 y 3. Por otro lado, una comparación de (a) con (c) sugiere que existe una mayor latencia cuando se tienen múltiples BSS en el mismo AP, según las pruebas recolectadas la mediana de (c) es $10\,ms$ mayor que en (a).

4.7. Canales solapados

De acuerdo con el estándar [1], los dispositivos IEEE 802.11b/g operan en la banda de los $2.4\,GHz$, dividida en 11 canales (13 o 14 en algunos países), desde $2412\,MHz$ hasta $2462\,MHz$, cada uno con un ancho de $22\,MHz$ en IEEE 802.11b y $20\,MHz$ en IEEE 802.11g. Con una distancia entre las frecuencias centrales de $5\,MHz$ para ambas revisiones. Estas características causan solapamiento entre canales vecinos. Por ejemplo, en la Figura 4.13, la zona naranja representa como el canal 6, centrado en $2467\,MHz$, solapa parcialmente los canales 7 ($2472\,MHz$), 8 ($2477\,MHz$) y 9 ($2482\,MHz$). Esto provoca que dispositivos que operan en canales vecinos compartan, parcial-

mente, el espectro de radio, por lo que las interfaces de red podrían decodificar tramas generadas en canales solapados.

El solapamiento de canales provoca el incremento de la contención en el acceso al medio, debido a la detección de portadoras espurias (*spurious carrier sensing*) [45]. Por otro lado, este comportamiento puede ser aprovechado para mejorar el escaneo, pues es posible descubrir AP que operan en canales diferentes al canal en el que se transmite el P_{rq}.

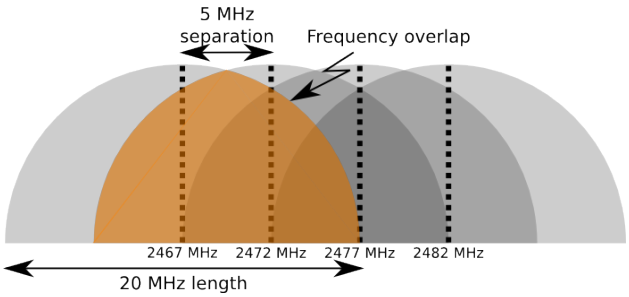


Figura 4.13: Solapamiento de canales

De los 19165 P_{resp} registrados por la MS, 3941 se detectaron en canales solapados, lo que representa el 20.6 % del total. La Tabla 4.2 presenta la proporción de los BSS descubiertos por canal. Esto es, el cociente entre los BSS descubiertos en un canal dado y los BSS que operan en cada canal. Las filas indican el canal en el que se recibió el P_{resp}, las columnas el canal en el que se originó el P_{resp} (canal en el que opera el BSS descubierto). Por ejemplo, la fila 6, columna 5, indica que, en promedio, mientras se escaneaba el canal 5 se descubrió el 37 % de los BSS disponibles que operaban en el canal 6.

Por otra parte, hemos notado que (según la Tabla 4.2) los canales no solapados 1-6-11 gozan de mayor precisión en la detección de redes operando en el mismo canal, observe que el intervalo de confianza asociado a la proporción descubierta es 1 para los tres canales.

La Figura 4.14 muestra el promedio de BSS descubiertos por canal mientras se escanean los canales 1, 6, 11, esta figura no toma en cuenta los P_{rq} que no obtuvieron respuesta. Las barras sombreadas representan el promedio de BSS disponibles, mientras que las barras de color indican el promedio de BSS detectados mientras se escanea un canal dado.

El total de BSS disponibles se define como el número total de BSS operando en un canal dado, sin importar en cual canal se encontraba la MS

Tabla 4.2: Porcentaje de BSS detectados en los canales solapados (intervalo de confianza del 95 %)

		Originado en canal (% ± intervalo 95 %)										
		1	2	3	4	5	6	7	8	9	10	11
Detectado en canal	1	95 ± 1	9 ± 6									
	2	22 ± 3	94 ± 5	8 ± 7	2 ± 3							
	3	3 ± 1	14 ± 7	8 ± 3	10 ± 7							
	4		2 ± 3	12 ± 8	91 ± 7	3 ± 6	1 ± 1					
	5				9 ± 7	75 ± 14	13 ± 2					
	6				2 ± 3	37 ± 16	98 ± 1	20 ± 6				
	7					3 ± 6	15 ± 2	89 ± 4	11 ± 7		1 ± 2	
	8						2 ± 1	9 ± 4	88 ± 7	9 ± 8	10 ± 5	
	9							1 ± 1	10 ± 7	98 ± 4	28 ± 8	8 ± 2
	10								1 ± 2	9 ± 8	1 ± 5	22 ± 2
	11							1 ± 2			17 ± 7	93 ± 1

cuando se descubrieron. Note que las barras sombreadas (BSS disponibles) siempre son mayores que las que indican los BSS descubiertos, esto es debido a que algunos BSS se detectaron únicamente mientras el escaneo se ejecutaba en un canal diferente a su canal de operación, lo que sugiere que un escaneo completo (*full scanning*) puede descubrir una topología más completa.

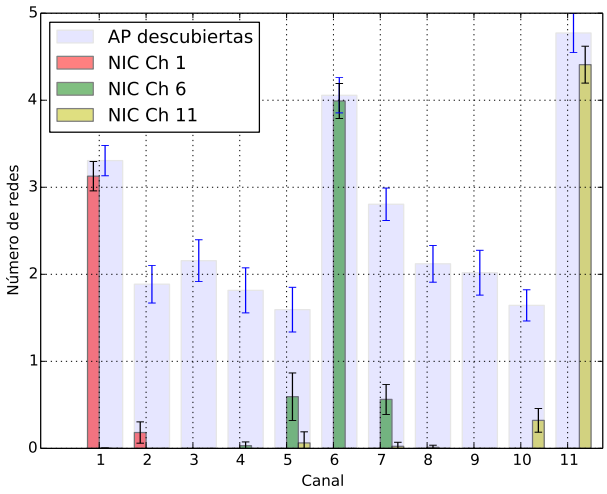


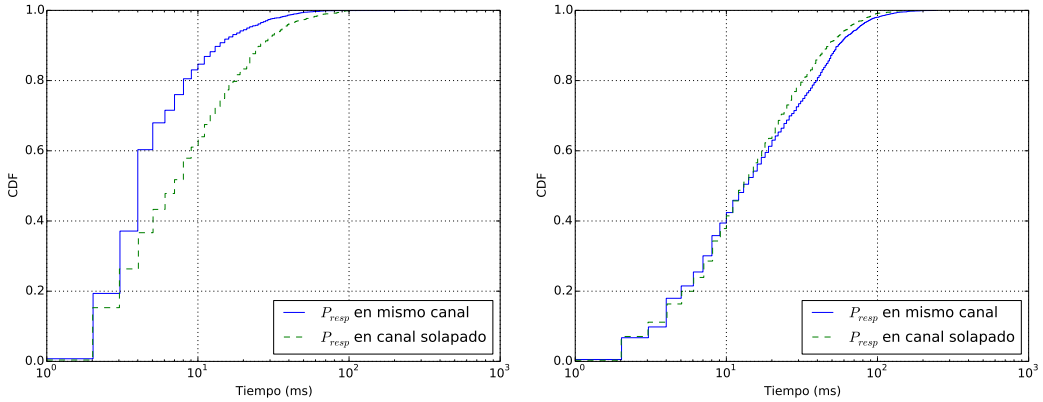
Figura 4.14: Número promedio de BSS descubiertos por canal.

4.7.1. Latencia de los Probe Response

En la Figura 4.15 se compara la latencia de los BSS descubiertos en el canal de operación y los que se detectaron en canales diferentes al de

operación, esto es, descubiertos en un canal solapado. En la Figura 4.15a, donde se compara la latencia del primer P_{resp} recibido luego de cada P_{rq}, se observa que los P_{resp} generados y recibidos en el mismo canal presentan una latencia inferior a la que corresponde a los P_{resp} que se transmitieron y recibieron en canales diferentes.

Por otro lado, en la Figura 4.15b se presenta la latencia del último P_{resp} luego de cada P_{rq}. En esta figura las curvas no presentan diferencias significativas, por lo que se considera que la latencia del último P_{resp} presenta la misma distribución sin importar si fue transmitido y recibido en el mismo canal o no.



(a) Primer P_{resp} registrado

(b) Último P_{resp} registrado

Figura 4.15: Latencia de los P_{resp}

4.8. Discusión

En este capítulo se caracterizaron los despliegues presentes en la ciudad de Rennes, Francia. Para ello fue necesario estudiar proceso de escaneo activo en el kernel de Linux, permitiendo implementar una plataforma para recolectar información de las redes y medir la latencia de los P_{resp}.

Las pruebas realizadas mostraron que la latencia de los P_{resp} es afectada por el modelo/fabricante del AP que lo genera, así como también la ocupación del medio (ver Sección 4.3). Debido a que los AP utilizan la función de coordinación distribuida (DCF: *Distribution Coordination Function*) para

acceder al medio y responder un P_{rq}, un aumento en la ocupación se traduce en el incremento de las probabilidades de colisión y por tanto de la latencia.

A lo largo del despliegue estudiado se recibió respuesta al 37.26 % del total de P_{rq} transmitidos, con el $86,18\,\%$ de las redes distribuidas en los canales 1, 6 y 11. En estas condiciones, el primer P_{resp} luego de cada P_{rq} se recibió en $8\,ms$ o menos en el 80 % de los escaneos ejecutados. Por otro lado, se destaca que las redes se encuentran en posiciones cercanas, esto es, al descubrir una red se tiene una probabilidad de 0.70 de detectar otras en el mismo escaneo/canal.

La evaluación del efecto del solapamiento de los canales en el escaneo indica que algunas redes se detectaron únicamente en canales diferentes al canal en el que operan, lo que sugiere que la ejecución de escaneos completos (*full scanning*) descubre topologías más completas que los escaneos parciales, esto es, escaneo de un subconjunto de los canales disponibles. Además, los P_{resp} detectados en canales solapados presentan una latencia superior a los que se transmitieron y descubrieron en el mismo canal.

Capítulo 5

Dinámicas en el proceso de descubrimiento a gran escala: hacia un sistema de gestión central

El proceso de descubrimiento en redes IEEE 802.11 está sujeto a las normas de acceso descritas en el estándar [1]. Durante el escaneo la estación móvil (MS: *Mobile Station*), los puntos de acceso (AP: *Acess Points*) y otros dispositivos IEEE 802.11 deben compartir el medio, por lo que deben coordinar su acceso. Como se mencionó en la Sección 2 el acceso al medio está regulado por la función de coordinación distribuida (DCF: *Distribution Coordination Function*) que utiliza acceso múltiple por detección de portadora con evasión de colisiones (CSMA/CA: *Carrier Sense Multiple Access with Collision Avoidance*) por lo que, cuando el medio se encuentra ocupado, las estaciones deben realizar *backoff* aleatorio antes de acceder al medio. Esto, sumado a las anomalías del espectro radio eléctrico (multiruta, difracción o interferencias) provocan que los resultados del escaneo presenten una dinámica no determinista. En los experimentos presentados en este capítulo se estudian las variaciones en las topologías reportadas por escaneos sucesivos, todo esto obedece al dinamismo de los procesos que afectan el descubrimiento, entre los que destacamos el acceso al medio dirigido por la DCF y la presencia de objetos móviles que alteran las características del entorno.

5.1. Descripción del experimento

Con el objeto de evaluar el proceso de descubrimiento y las diferencias que pueden presentarse en los resultados de una secuencia de escaneos en el mismo despliegue, se ejecutó una campaña de descubrimiento diseñada para tal fin. Usando la plataforma descrita en la Sección 4.1, se ajustó el proceso de descubrimiento para escanear los canales 1, 6 y 11, también se modificó el tiempo de espera por canal a 5, 10, 15, 20, 30, 50, 100 o 500 ms de acuerdo a la prueba realizada. De la ruta descrita en la Sección 4, se seleccionó la ubicación indicada en la Figura 5.1 por tener una alta densidad de redes. Con la MS estática se realizaron 8 series de 100 escaneos cada una, sumando en total 800 muestras de las cuales extraemos las principales conclusiones expuestas en este capítulo. En cada serie se utilizó uno de los tiempos de espera por canal indicados anteriormente, con pausas de 2 s entre un escaneo y el siguiente, tal como se describe en la Figura 5.2. La duración total de la campaña fue de aproximadamente 1 hora.

Durante cada prueba se registraron los siguientes datos:

- Canal en que se transmitieron los Probe Requests (P_{rq})
- Latencia de los Probe Responses (P_{resp})
- Canal en que se originó cada P_{resp}
- Potencia con que se registraron los P_{resp}

5.2. Descubrimiento de la topología

El porcentaje de la topología descubierta o fracción descubierta (DR: *Discovery Ratio*) se define como el cociente entre la cantidad de AP descubiertos en un escaneo y la cantidad total de AP disponibles [10]. En un escenario donde se conoce a priori la totalidad de los AP existentes resulta trivial estimar este valor luego de cada escaneo, sin embargo, en un escenario desconocido la topología debe descubrirse de manera progresiva, con cada escaneo actualizando la topología conocida. Por esta razón definimos la topología existente (TE) como los AP existentes en el entorno al momento de la ejecución del escaneo y, topología descubierta (TD) como los AP descubiertos progresivamente, partiendo de un estado inicial donde la topología es desconocida.

Figura 5.1: Ubicación del punto de recolección estático

En un escenario con la topología desconocida el DR puede estimarse usando la topología descubierta hasta el último escaneo. Suponga, por ejemplo, una secuencia de 2 escaneos, el primero identifica AP1 y AP2, en cuyo caso la topología está formada por estos dos y $DR = 100\,\%$. El segundo escaneo identifica AP1 y AP3, por lo que TD = {AP1, AP2 y AP3}; y DR = 66.7 %.

5.2.1. Topología descubierta por escaneo

A cada escaneo se asocia un valor de DR, obtenido como el cociente entre el número de AP descubiertos durante el escaneo activo (d) y el número total de AP existentes TE. En esta sección DR se estima según la Ecuación 5.1.

$$DR = \frac{d}{TE} \tag{5.1}$$

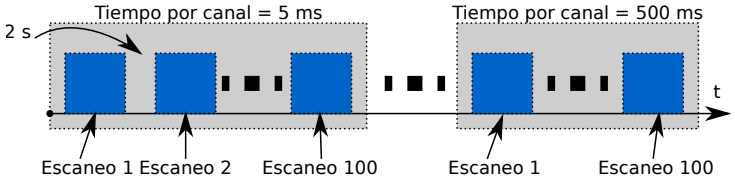


Figura 5.2: Recolección de datos en campaña estática

Como se mencionó, el mismo algoritmo presenta distintos valores de DR en una secuencia de escaneos, en la Figura 5.3 se puede observar cuan variable es el DR para distintos valores de tiempo de espera por canal. La figura muestra el histograma del DR, esto es, el DR en las abscisas y la frecuencia en las ordenadas, cada figura describe los resultados asociados a uno de los tiempos por canal. En las figuras se distinguen 4 curvas, cada una asociada a un conjunto de potencias: en gris todas las potencias, en rojo $[-79; inf)$, amarillo $[-82; -79)$ y azul $(-inf; -82)\, dBm$.

Por ejemplo, de la Figura 5.3 se interpreta que usando $15\, ms$ de tiempo de espera, el algoritmo descubrió el $9.3\,\%$ de los AP existentes en el $16\,\%$ de los escaneos realizados, en forma análoga, descubrió el $4\,\%$ de los AP con potencia superior a $-79\, dBm$ en $29\,\%$ de las ocasiones o, de forma equivalente, la probabilidad de encontrar $9.3\,\%$ de los AP con un temporizador de $15\, ms$ es de 0.16.

Al ajustar el tiempo de espera por canal se puede observar los siguiente:

1. El DR tiende a aumentar con el aumento del tiempo de espera, se observa como las barras grises de la Figura 5.3 correspondiente a $5\, ms$, se concentran en el intervalo $[0; 5.3]$, mientras que en las figuras sucesivas los intervalos se desplazan hacia la derecha hasta $[9.3; 24]$ para $500\, ms$. Por otro lado, las barras rojas, que representan los AP de potencia alta, presentan variación menor; desplazándose del intervalo $[0; 4]$ cuando para el temporizador de $5\, ms$ hasta $[0; 10.7]$ para el temporizador de $500\, ms$. De igual manera sucede con las barras amarillas y azules, AP con potencia media y baja respectivamente.

2. A medida que aumenta el tiempo de espera se tiene una mayor diversidad en los valores del DR, por ejemplo, de 5 valores para $5\, ms$ a 15 valores cuando se tiene $100\, ms$ (Figura 5.3) de espera por canal.

3. A mayor tiempo de espera mayor estabilidad en términos de la cantidad de las tasas posibles del DR. Esto puede observarse en la Tabla

Tabla 5.1: Variabilidad del descubrimiento

Tiempo por canal	$\bar{x}$	σ	C_v	**Núm. de tasas de DR**
$5\,ms$	1.9333	1.2129	0.6274	5
$10\,ms$	3.2533	1.8118	0.5569	6
$15\,ms$	6.3067	2.4503	0.3885	9
$20\,ms$	8.0400	2.7870	0.3466	11
$30\,ms$	10.0400	3.5450	0.3531	13
$50\,ms$	14.0533	4.1502	0.2953	15
$100\,ms$	18.0933	3.9067	0.2159	15
$500\,ms$	16.9467	4.1667	0.2459	14

5.1, que presenta la media ($\bar{x}$), la desviación estándar (σ), el coeficiente de variación[1] (C_v) y la cantidad tasas del DR posibles. Los valores presentados se calcularon sin discriminar los datos por potencia de señal. El coeficiente de variación permite observar la relación entre el tamaño de la media y la variabilidad de una variable, DR en este caso. Mientras mayor el C_v más heterogéneos serán los valores de DR, por lo que de la Tabla 5.1 se desprende que a mayor tiempo de espera, menor la heterogeneidad.

4. A mayor tiempo de espera, mayor es el número total de redes detectadas. Esto se puede atribuir a que algunas redes pueden presentar condiciones que retrasan el envío del P_{resp}, por lo que al aumentar el tiempo de espera se incrementa la probabilidad de recibir respuestas lentas.

5.2.2. Descubrimiento de la topología

Como se mostró en la Sección 5.2.1, escaneos sucesivos en la misma ubicación pueden reportar topologías diferentes, con cada escaneo aportando información a la TD. La Figura 5.4 presenta la evolución de la proporción de la topología descubierta en escaneos sucesivos. En la figura la TE es estimada tomado en cuenta el resultado acumulativo de la totalidad de los escaneos, incluyendo todos los tiempos de espera, luego, la TD se compara con la TE y

[1] $C_v = \frac{\sigma}{|\bar{x}|}$

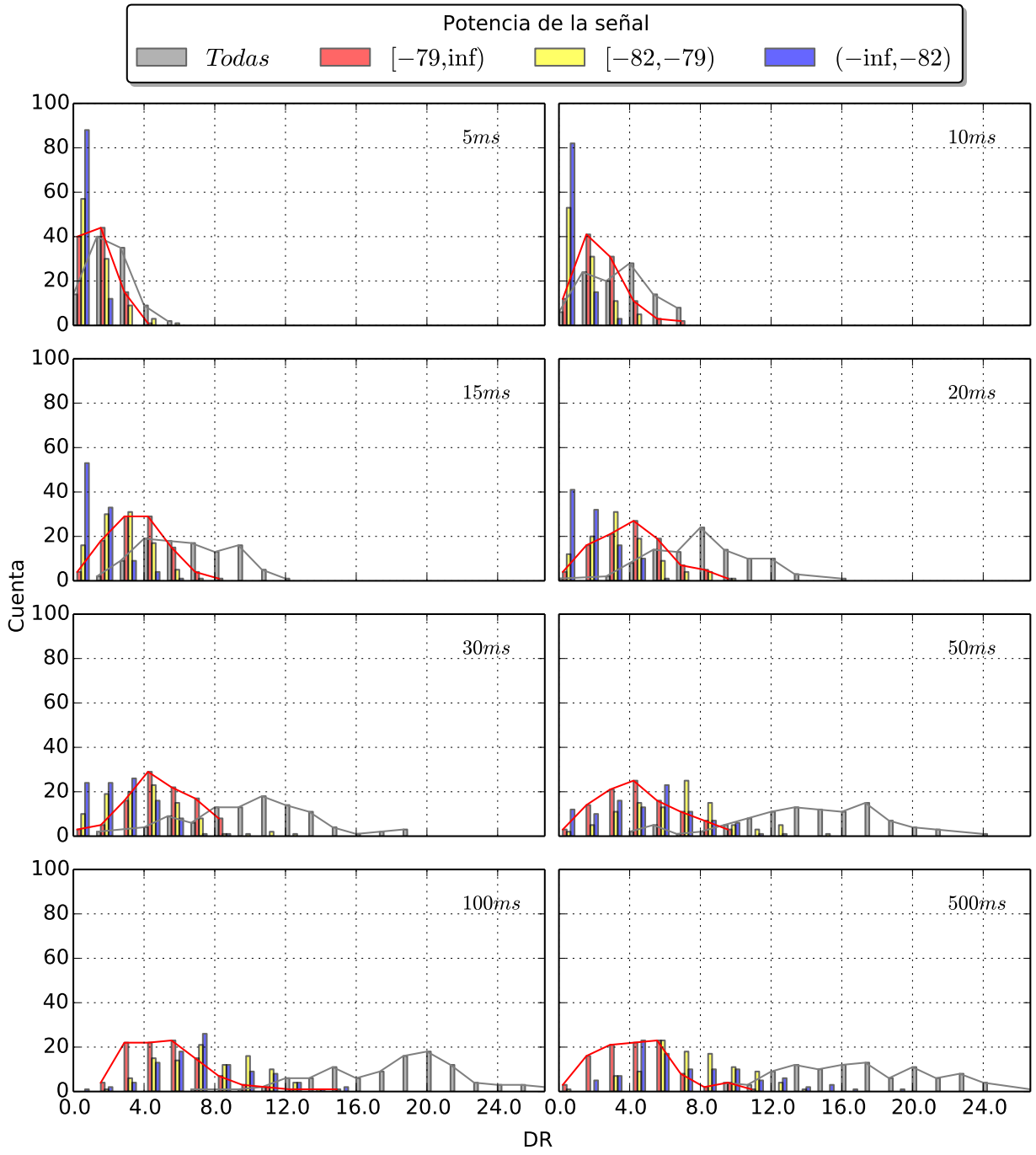


Figura 5.3: Fracción del total de AP existentes descubiertos

se estima el DR alcanzado por la sucesión de escaneos. Observe que los primeros escaneos aportan la proporción más significativa de la topología. Por ejemplo, con 500 ms los primeros 20 escaneos alcanzan a descubrir el 54.67 % de la TE. También se observaron algunas excepciones donde escaneos intermedios realizan un aporte significativo, como los mostrados en las regiones A y B de la figura. En la región A muestra como luego de dos escaneos se agrega 4 % de la topología. Un aporte mayor se observa en la región B, donde la curva cian gana 10.6 % de la topología luego de 4 escaneos.

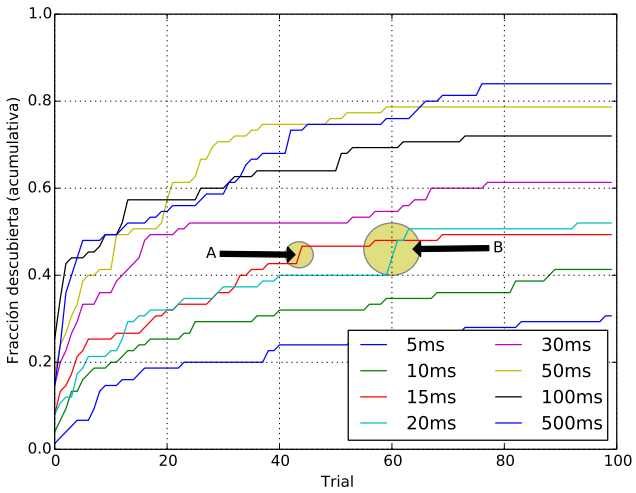


Figura 5.4: Evolución del descubrimiento para secuencias de 100 escaneos

En la Figura 5.5 se muestra la evolución del descubrimiento, normalizando las curvas utilizando como línea base el número máximo de AP descubiertos para cada tiempo de espera. Esta figura muestra que con 20 escaneos o menos se alcanzó a conocer el 60 % de la topología máxima asociada a cada tiempo de espera. Por ejemplo, con tiempo de espera por canal de 100 ms (curva negra) se descubrió un total de 63 AP luego de 100 escaneos, sin embargo, para el escaneo 20 ya se habían registrado 50, que representa el 80 % del total máximo descubierto al usar ese temporizador.

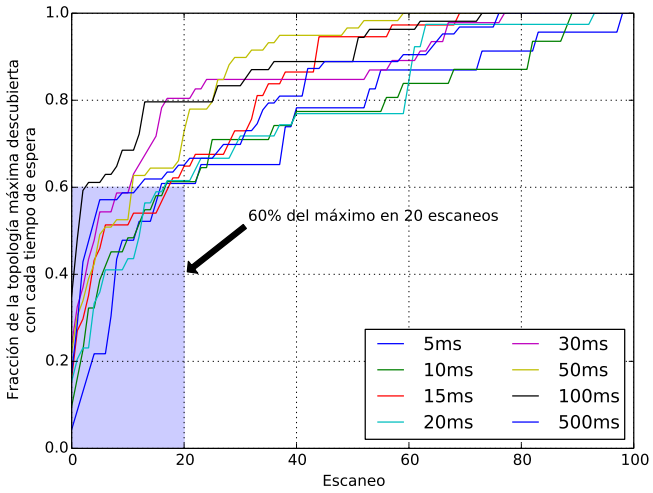


Figura 5.5: Evolución del descubrimiento en relación al máximo alcanzado por cada temporizador

5.3. Variación en la potencia registrada

En un escenario donde la MS y los AP mantienen una posición fija, la potencia con que se perciben las tramas intercambiadas varía en sucesivos escaneos, esto puede ser debido a diferentes causas, entre las que se cuentan: obstáculos que aparecen y desaparecen, interferencias positivas y negativas, propagación multiruta, entre otros. La Figura 5.6 representa las redes descubiertas y su potencia. En las ordenadas se representan las redes, en las abscisas el escaneo. Las redes están ordenadas de acuerdo a la mediana de la potencia registrada a lo largo de todos los experimentos realizados. La dinámica con que se percibe un AP en un escaneo es indicada mediante una escala con el espectro de colores, desde purpura, para $-89\,dBm$, hasta rojo, para $-68\,dBm$.

Es claro que a mayor tiempo de espera en el canal mayor cantidad de AP descubiertos. De igual manera, también aumenta la regularidad de aparición de cada AP. En la abscisa se observa que los puntos cambian el color, es decir, la potencia registrada varía. Por ejemplo, la red 75 varía entre los colores amarillo a rojo.

Para mostrar las variaciones en la potencia, se cuenta la cantidad de

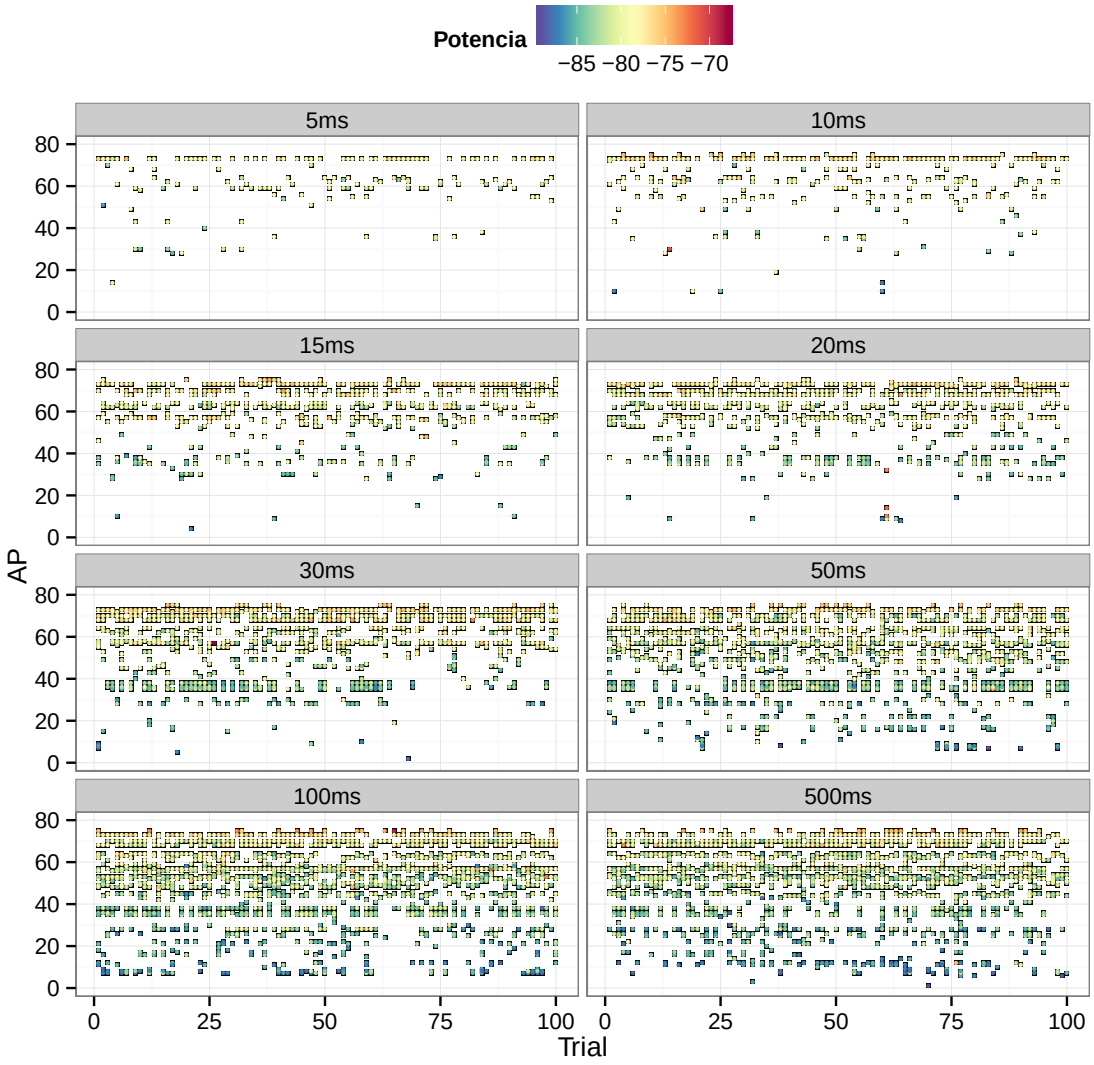
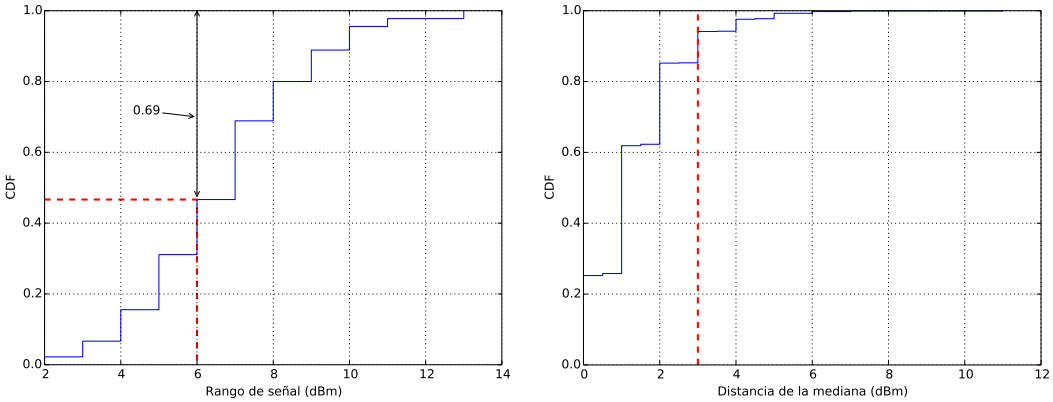


Figura 5.6: Potencia con que se perciben los AP en cada escaneo



(a) CDF correspondiente al rango de la potencia de las señales con que se registraron los AP

(b) CDF correspondiente a la diferencia entre la potencia registrada en un escaneo y la mediana de las potencias asociadas a un AP

Figura 5.7: Variación de la potencia registrada

valores de potencias con que se detectó cada AP luego de una secuencia de escaneos. Si se reciben múltiples P_{resp} del mismo AP durante un escaneo, se registra el de mayor potencia. A objeto de evitar sesgos introducidos debido a P_{resp} no registrados debido a tiempos de espera cortos, se utilizaron los datos del experimento correspondiente a $500\,ms$ de tiempo de espera por canal[2]. Además, se toma el subconjunto de los AP que se registraron en 2 o más escaneos.

En la Figura 5.7a se presenta la CDF del número de potencias diferentes con que se detectó cada uno de los AP. Según la figura, ninguno de los AP se registró con la misma potencia en la totalidad de las muestras, por el contrario, el 69 % de los AP registró 6 o más valores, indicando que en escaneos sucesivos la potencia de un AP puede variar en un rango significativo. Esto es, en un escaneo un AP podría registrarse con potencia de $-72\,dBm$ y posteriormente con $-78\,dBm$.

Por otro lado, en la Figura 5.7b se comparan las potencias registradas para un AP con respecto a la mediana de las potencias de ese mismo AP. Para cada AP se estima *la mediana de la potencia* con que se descubrió en cada escaneo. Luego, se calcula la función de distribución acumulada de las

[2]Ver Sección 4.1 para descripción de la plataforma usada.

diferencias entre la mediana de sus potencias y cada potencia.

Se usa la mediana como métrica porque se considera un buen indicador de la potencia con que se registrarán sucesivos P_{resp}. Esta hipótesis es consistente con lo mostrado en la Figura 5.7b, donde se observa que el 94.14 % de los AP se detectaron con una potencia que difiere de la mediana en $\pm 3\,dBm$ o menos.

Entonces, se discriminan las redes detectadas en cada escaneo de acuerdo a la potencia percibida en tres grupos, cada uno de $3\,dBm$ y centrados en $-80\,dBm$, sensibilidad que deben tener las estaciones para decodificar tramas [1], tal como se muestra en la Figura 5.8.

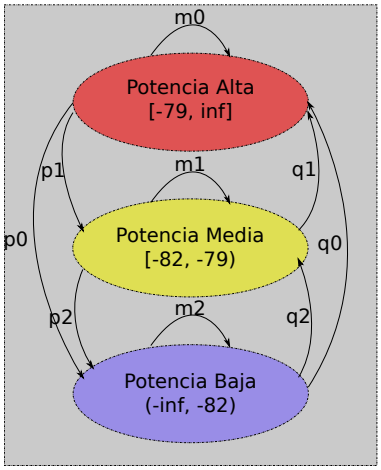


Figura 5.8: Clasificación de los AP por señal

Note que escaneos sucesivos pueden clasificar una red en grupos diferentes, por ejemplo, suponga que durante el escaneo N se detecta AP1 con potencia $-78\,dBm$ (grupo de *Potencia Alta*) y en el escaneo M con potencia $-83\,dBm$ (grupo de *Potencia Media*). Donde N y M representan los escaneos que detectaron AP1 por primera y segunda vez respectivamente. Este escenario describe una transición de grupo. En la Tabla 5.2 se listan las probabilidades de que un AP sea clasificado en el mismo grupo en dos escaneos sucesivos. La probabilidad más alta se presenta en el grupo de *Potencia Alta* del temporizador $10\,ms$, que corresponde a 0.79. El complemento de la tabla representa la probabilidad de que una MS, que utiliza un temporizador particular, *clasifique un AP en grupos diferentes en dos escaneos sucesivos.*

En la Figura 5.8 también se describen las transiciones de clasificaciones

Tabla 5.2: Probabilidad de que un AP se clasifique en el mismo grupo en dos escaneos sucesivos

$t(ms)$	**P(Alta)** m0	**P(Media)** m1	**P(Baja)** m2
$5ms$	0.69	0.42	0.00
$10ms$	0.79	0.49	0.23
$15ms$	0.68	0.46	0.50
$20ms$	0.68	0.45	0.47
$30ms$	0.70	0.43	0.52
$50ms$	0.54	0.48	0.52
$100ms$	0.55	0.43	0.59
$500ms$	0.48	0.46	0.59

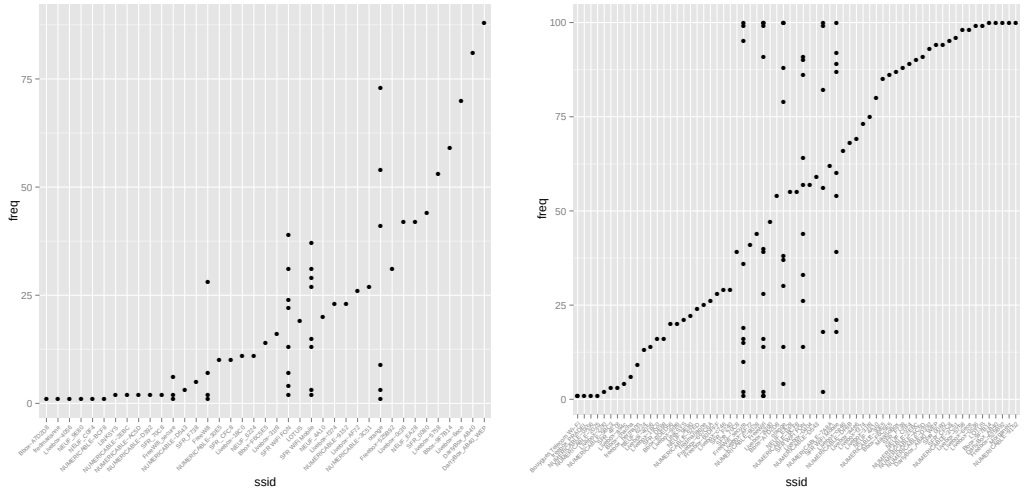
que puede presentar un AP. En la Tabla 5.3 se muestra la probabilidad asociada a cada transición, estimada a partir de los experimentos realizados en este trabajo.

Tabla 5.3: Probabilidad de cambio de señal de la red

$t(ms)$	**p0**	**p1**	**p2**	**q0**	**q1**	**q2**
$5ms$	0.03	0.28	0.12	0.89	0.11	0.46
$10ms$	0.04	0.17	0.05	0.31	0.46	0.46
$15ms$	0.05	0.27	0.10	0.37	0.13	0.44
$20ms$	0.03	0.29	0.18	0.43	0.10	0.36
$30ms$	0.03	0.27	0.22	0.38	0.09	0.35
$50ms$	0.10	0.36	0.25	0.38	0.09	0.27
$100ms$	0.08	0.36	0.30	0.34	0.08	0.27
$500ms$	0.12	0.40	0.28	0.33	0.09	0.25

5.4. Efecto de los beacons en el escaneo activo

Durante la ejecución del escaneo activo la interfaz de red captura P_{resp} generados como consecuencia de la transmisión de un P_{rq}, además, la interfaz



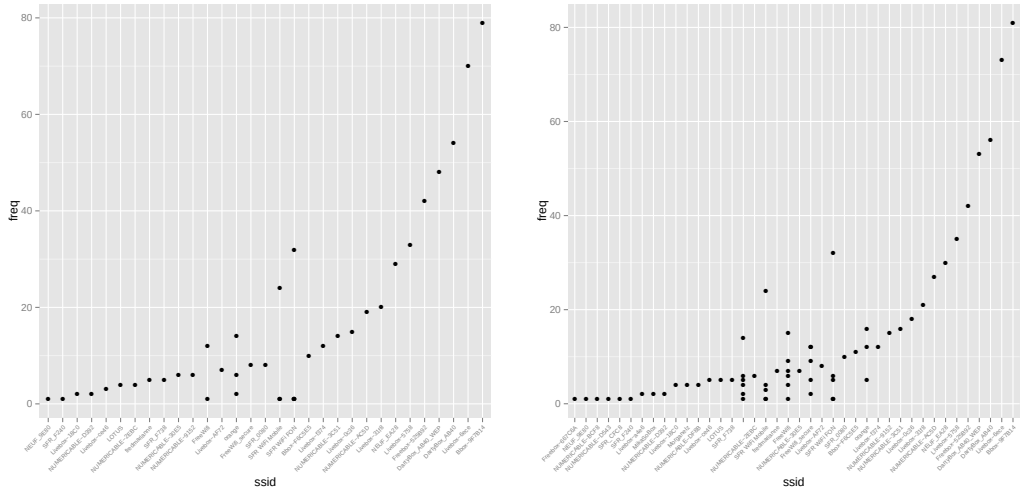
(a) Solo P_{resp} (b) Incluye P_{resp} y beacons

Figura 5.9: Frecuencia de descubrimiento de redes para temporizador de $500\,ms$

también registra beacons. Como se indicó en la Sección 2, los beacons son tramas administrativas utilizadas para: 1) sincronizar los dispositivos que componen la red y 2) para advertir sobre la presencia de la red.

Los beacons son transmitidos de manera periódica, comúnmente cada $100\,ms$ [20], de manera que los algoritmos de escaneo los aprovechan en el descubrimiento. Los resultados presentados en los capítulos anteriores consideran únicamente los P_{resp}. Como se observa en la Figura 5.9a, que utiliza P_{resp} únicamente y correspondiente al temporizador de $500\,ms$, detectaron 63 redes, 7 de cuales se detectaron en más del 50 % de los escaneos. Por otro lado, en la Figura 5.9b, correspondiente al mismo temporizador e incluyendo además los beacons, se observan 117 redes detectadas, que representa 85.71 % de incremento. De las 117 redes descubiertas 57 son detectadas en más del 50 % de los escaneos. De acuerdo con los experimentos mostrados, el uso de beacons implica una mejora en dos sentidos: aumenta el número de redes registradas y aumenta la frecuencia con que se descubre cada red.

Sin embargo, el incremento resulta menor a medida que se tienen temporizadores bajos, observe las Figuras 5.10a y 5.10b que utilizan un temporizador de $20\,ms$, donde la diferencia en el descubrimiento resulta inferior.



(a) Solo P_{resp} (b) Incluye P_{resp}y beacons

Figura 5.10: Frecuencia de descubrimiento de redes para temporizador de $20\,ms$

Esto es debido a que la transmisión de beacons es realizada periódicamente, y es independiente del escaneo activo. Si suponemos la transmisión de beacons cada $100\,ms$, durante $500\,ms$ cada una de las redes transmitirá entre 4 y 5 beacons, aumentando considerablemente la posibilidad de que la MS decodifique correctamente la trama, sin embargo, partiendo de la Figura 6.1, presentada en el siguiente capítulo, se observa que luego de la transmisión de un P_{rq} hay una disminución en el número de beacons recibidos durante un periódo de $100\,ms$. Presumimos que este efecto es consecuencia de los P_{resp} generados.

En la Figura 5.11 se observa el promedio de beacons recibidos de cada red luego de 100 escaneos ($\overline{bAPi}$), esto es, se cuentan los beacons del APi recibidos en el escaneo n ($bAPi_n$), luego se calcula el promedio a lo largo de todos los escaneos, según la siguiente ecuación:

$$\overline{bAPi} = \frac{\sum_{n=1}^{100} bAPi_n}{100} \tag{5.2}$$

Observe que con el temporizador de $20\,ms$ el promedio de beacons recibidos es inferior a 1 para el 100 % de los AP. Por otro lado, con $500\,ms$, del 44.4 % de las redes registradas se recibió, en promedio, 1 o más bea-

cons. Finalmente, solo el 14.5 % de los AP registró un promedio superior a 3 beacons.

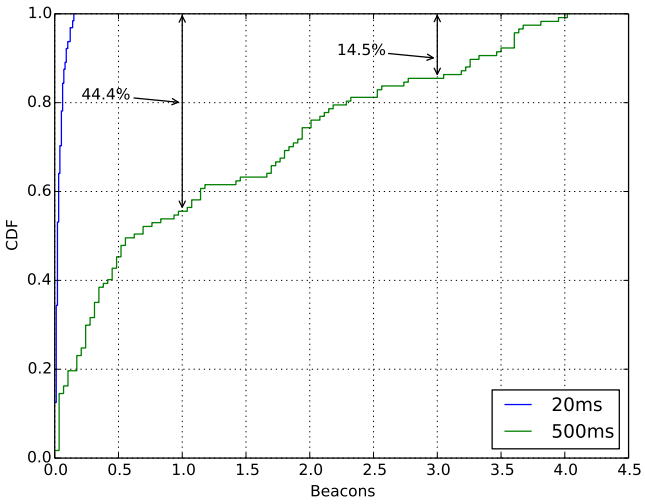


Figura 5.11: Número promedio de beacons recibidos de cada AP luego de 100 escaneos

5.5. Discusión

En este capítulo se discutió la dinámica del proceso de descubrimiento, que es afectado por las anomalías del espectro radio eléctrico y es regulado por la DCF, que obliga a las MS a realizar *backoff* aleatorios para conseguir un espacio para la transmisión de las tramas a la vez que se reducen las colisiones. Estas características de las redes IEEE 802.11 provocan que la dinámica de las respuestas de los AP, y a su vez del proceso de descubrimiento, sea no determinista.

Los experimentos presentados mostraron que en topologías densas el escaneo descubre solo una fracción de la topología existente, siendo 24 % el máximo valor de DR registrado para un escaneo, esto es con un tiempo de espera por canal de 500 ms. Adicionalmente, en una secuencia de escaneos se obtienen distintos resultados, con variaciones en términos de: AP descubiertos y potencia con que se perciben. Sin embargo, la variación en la potencia está bien acotada a 3 dBm alrededor de la mediana. Todo esto indica que son necesarios múltiples escaneos para descubrir la topología completa.

Capítulo 6

Sistema de descubrimiento distribuido asistido

En secciones previas se discutieron características relevantes de los despliegues IEEE 802.11 actuales, que presentan características propias de sistemas que surgen de manera espontánea, es decir, las redes que componen los despliegues presentan características y configuraciones diferentes, operando sin planificación ni coordinación central. Estos grandes despliegues, presentes en zonas urbanas podrían ser aprovechados para expandir el alcance de las redes y la movilidad de sus usuarios [46].

Los despliegues actuales, con sus características caóticas (ver Sección 4), presentan las siguientes limitaciones:

- El descubrimiento de las redes es relativamente lento [8, 11];
- Las estrategias de escaneo actuales no toman en cuenta el dinamismo intrínseco en el proceso de descubrimiento;
- Las estrategias de escaneo actuales no consideran las necesidades de los usuarios y aplicaciones [10];
- Las redes desplegadas espontáneamente operan sin coordinación, inundando el espectro con respuestas que podrían ser consideradas irrelevantes, lo que podría afectar la capacidad del medio. Ejemplo de esto se muestra en la Figura 6.1, que muestra cómo los Probe Response (P_{resp}) generados durante un escaneo activo y los beacons aparecen durante un período particular.

Es por ello que en esta sección se propone un sistema distribuido que asista el proceso de descubrimiento de redes IEEE 802.11, que tome en consideración las características de los despliegues y la dinámica del proceso de descubrimiento.

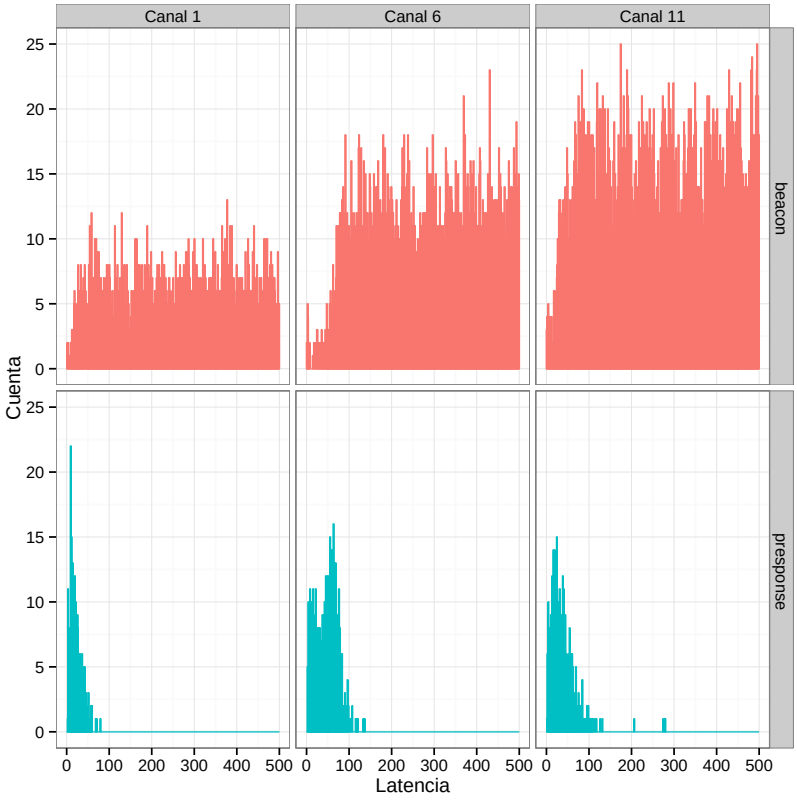


Figura 6.1: Tiempo de recepción de los P_{resp} y Beacons durante el escaneo (temporizador 500ms)

6.1. Estrategia general

En los experimentos realizados se ha observado que para conocer el número de redes disponibles en un punto, así como su potencia, es necesario realizar varios escaneos consecutivos, con cada escaneo aportando información de nuevos puntos de acceso (AP: *Acess Points*) y actualizando los datos de

los ya registrados.

Con el objeto de simplificar esta propuesta, la topología de las redes es organizada en un plano bidimensional dividido en celdas. A su vez, suponemos que las estación móvil (MS: *Mobile Station*) cuentan con un sistema que permite su geolocalización, por ejemplo, un GPS, disponible en muchos dispositivos móviles actuales. Esto permitirá que cada MS tenga una buena aproximación de la celda en la que se encuentra ubicada.

En nuestro caso, definamos una celda como la unidad asociada a un área bien definida del plano, identificada por su ubicación, y la lista que describe la topología de esa área. De esta manera, la información de las redes disponibles en cada celda es aportada por los escaneos realizados por las MS dentro de los límites de la celda. La información de las diferentes celdas presentes en el despliegue es representada como una entrada en la base de datos de la topología, gestionada por un entidad central, que es consultada y actualizada por las MS.

6.2. Descubrimiento de la topología en cada celda

En la Sección 5.2 se definió topología descubierta (TD) como la topología descubierta progresivamente, partiendo de un estado donde no se tiene información sobre las redes en la celda. Entonces, escaneos sucesivos, realizados por los distintos MS que ingresen a la celda, incrementan la TD.

Suponga que $AP1$, $AP2$, $AP3$ y $AP4$ forman la topología real de una celda, entonces, en la Figura 6.2 se muestra el proceso de descubrimiento realizado por dos MS ($MS1$ y $MS2$) ubicadas en la misma celda. Inicialmente TD está vacía, luego, $MS2$ ejecuta un primer escaneo que actualiza la topología de la celda con la información de $AP1$ y $AP4$. Un segundo escaneo de $MS2$ aumenta el número de los AP en TD al incluir $AP3$. Finalmente, $MS2$ ingresa a la celda, ejecuta un escaneo y actualiza la información correspondiente a $AP1$ y agrega $AP2$.

La existencia de redes esporádicas, que ingresan a la celda de forma temporal, debido por ejemplo a teléfonos celulares con *tethering* o servicios de transporte público con servicios IEEE 802.11, así también por los cambios en el entorno que provocan que algunos de los AP desaparezcan del alcance de la celda, es necesario establecer una política que permita eliminar la infor-

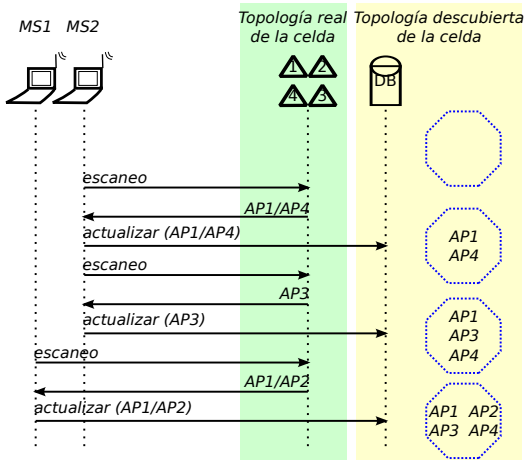


Figura 6.2: Descubrimiento progresivo de una celda

mación de los AP no alcanzables. Se propone entonces el uso de contadores de vencimiento, de manera que si un AP no es observado durante los últimos n_exp escaneos su información se elimine de la base de datos.

El valor de n_exp puede determinarse en función de las discusiones presentadas en la Sección 5.2.2, que indican que, independientemente del tiempo de espera por canal, las estrategias de escaneo estudiadas alcanzan el 80 % del descubrimiento máximo correspondiente a ese algoritmo en 60 escaneos. Así, con $n\_exp = 60$.

6.3. Emulación de la construcción del conocimiento de la topología

Como se discutió en el Capítulo 5, el descubrimiento de las redes en el entorno de una MS requiere la ejecución de múltiples escaneos y es sensible al tiempo de espera usado en cada escaneo, pues afecta la fracción de la topología aportada en cada escaneo. En la Figura 6.3 se emula la dinámica del proceso de descubrimiento propuesto para diferentes temporizadores, a partir de los experimentos descritos en la Sección 5.1. En la figura cada color corresponde a un temporizador. La curva superior muestra el descubrimiento acumulado comenzando con los temporizadores más altos, cambiando el temporizador cada 100 escaneos. La curva inferior se construye de manera inversa, es decir, los primeros escaneos corresponden a los temporizadores

más bajos y los últimos a los más altos.

Se observa que al utilizar temporizadores más altos implica que el descubrimiento de la topología será más acelerado, es decir, con menos escaneos se descubre una mayor cantidad de AP. Note que en la curva superior se descubre el 80 % de la topología en 67 escaneos con el temporizador de 500 ms, mientras que en la curva inferior se necesitan 502 ejecuciones. Una MS que participa en el descubrimiento distribuido puede ajustar el temporizador utilizado en los escaneos de acuerdo las necesidades de red, si las condiciones de red lo permiten utilizaría un temporizador alto, por el contrario, si el tráfico de red es sensible a interrupciones prolongadas utilizaría temporizadores bajos. De esta manera, el sistema central se mantiene actualizado sin que el servicio de red en las MS se vea afectado por el proceso de descubrimiento y actualización de la entidad central.

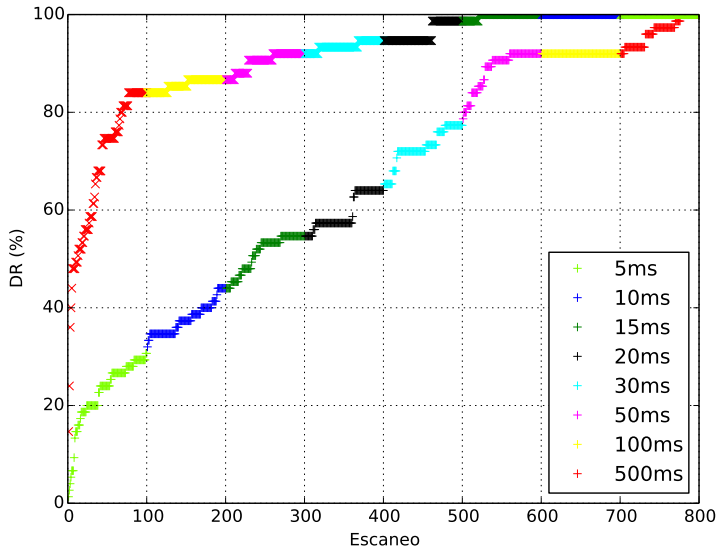


Figura 6.3: Evolución del descubrimiento acumulativo tomando P_{resp} únicamente

6.4. Arquitectura del sistema

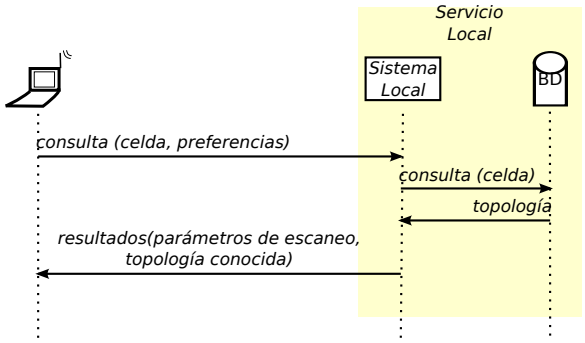
La propuesta está orientada a un sistema que centraliza la información sobre las redes, por lo tanto se plantea un sistema cliente-servidor. Los clientes

interactúan con la entidad central de dos maneras:

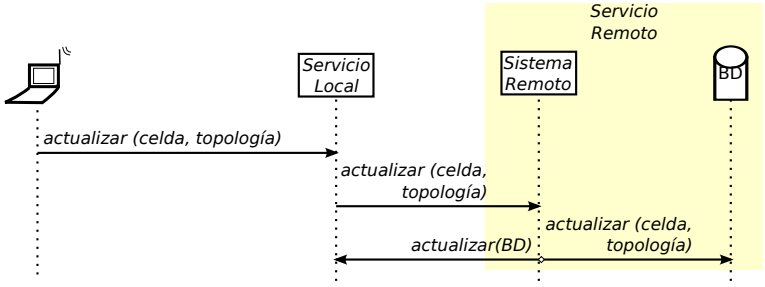
1. Actualizando la información sobre la topología en una celda
2. Consultando la información sobre la topología de una celda

El acceso a la entidad central requiere comunicación entre el cliente y el servidor, es decir, se necesita de conexión a la red, sin embargo, una MS que inicia el proceso de descubrimiento puede no tener acceso a la red, por lo que cada MS mantiene un caché local con la topología de las celdas visitadas frecuentemente y de sus vecinas. El caché es actualizado con información de la entidad central en forma periódica mientras se tiene conexión a la red.

En la Figura 6.4 se muestran las interacciones entre el cliente y el sistema para el descubrimiento asistido. Toda la interacción del cliente con la entidad se realiza a través del servicio local, encargado de gestionar las consultas y actualizaciones, lo que permite la asistencia al descubrimiento aún sin acceso a la red.



(a) Consulta al sistema



(b) Actualización del sistema

Figura 6.4: Interacción con el sistema

La Figura 6.5 muestra el algoritmo general que usaría una MS que hace uso de la entidad central. Como se observa, la interacción siempre es realizada con el caché presente en la MS, este es actualizado luego de enviar información del último escaneo a la entidad central, lo que garantiza independencia de la conexión de red.

Note que el sistema asiste el proceso de descubrimiento con información sobre la topología esperada. Por lo que la consulta realizada por la MS incluye su geolocalización e información sobre los requerimientos de servicio, con estos insumos el servidor es capaz de retornar la topología esperada, así como los parámetros de escaneo apropiados para optimizar el descubrimiento en términos de los requerimientos.

```
1: Obtener geolocalización
2: Enviar consulta al caché local
3: if Consulta exitosa then
4:     Actualizar parámetros para escaneo
5:     Ejecutar escaneo
6: else
7:     Ejecutar escaneo con parámetros por defecto
8: end if
9: if Redes disponibles then
10:    Seleccionar red
11:    Conectar a la red
12:    if Conexión exitosa then
13:        Actualizar TD en la entidad central
14:        Actualizar caché local
15:    end if
16: end if
```

Figura 6.5: Algoritmo para interacción con entidad central

6.5. Discusión

En este capítulo se propuso un sistema que asista el proceso de descubrimiento de redes. El sistema tiene un arquitectura cliente-servidor, los clientes, operando en las MS, descubren en forma distribuida las redes presentes en distintos despliegues, a la vez que envían la información hacia un servidor

que centraliza el acceso al conocimiento de las topologías y lo pone a disposición de las MS que lo requieran. El servidor proporciona un servicio en el cliente, que provee acceso a un caché local y a la vez media el acceso al servidor central. Esto permite que el descubrimiento de redes ejecutado por las MS aprovechen los datos recolectados por otras MS, de manera que ajusten los parámetros del escaneo de redes en función de la topología registrada previamente y de las preferencias de las aplicaciones y/o del usuario.

Capítulo 7

Conclusiones y trabajo futuro

A lo largo de este trabajo se ha discutido sobre el algoritmo de escaneo, también se estudiaron las características de los despliegues espontáneos, centrando la atención en el tiempo de respuesta de las redes y su distribución en los canales de la banda ISM en el rango de los $2.4\,GHz$. Finalmente se estudió el descubrimiento de las redes, evaluando las respuestas y sus características, lo que sugirió la necesidad de una entidad central que gestione información sobre la topología de los despliegues a la vez que asiste el proceso de descubrimiento.

En primer lugar, con respecto a los algoritmos de escaneo activo, se revisaron trabajos sobre el tema. Se destacan, por un lado, trabajos orientados al estudio y caracterización de los algoritmos de escaneo activo y por el otro, estudios orientados a la optimización del escaneo como parte del *handover*. En cualquiera de los casos, de los resultados presentados en los trabajos se infiere que no hay una estrategia de escaneo que resulte optima en todo los despliegues. Por su parte, las optimizaciones propuestas por los autores se clasificaron de la siguiente manera:

- Minimización de los temporizadores
- Selección de canales a escanear
- Escaneo asistido
- Escaneo periódico

En segundo lugar, luego de la revisión de redes IEEE 802.11 desplegadas espontáneamente, se presentó un conjunto de métricas que permiten estudiar

las características de los despliegues y que permiten orientar el diseño de una estrategia de descubrimiento. En el despliegue revisado se destaca que: la latencia del primer conjunto de servicio básico (BSS: *Basic Service Set*) en responder un Probe Request (P_{rq}) es menor o igual a $8\,ms$ en el 80 % de las ocasiones. El 34.45 % de los Probe Response (P_{resp}) detectados son retransmisiones, una cifra no despreciable que podría contribuir a aumentar la latencia del descubrimiento debido a que incrementa la ocupación del medio. Cerca del 50 % de las estaciones base descubiertas sirven más de una red, esto sugiere que el hardware utilizado pertenece a los principales ISP de la región, lo que también contribuye a aumentar la latencia de las respuestas. Respecto a la distribución y aprovechamiento de los canales, los datos mostraron que es posible aprovechar el solapamiento de los canales para descubrir redes que operan en canales distintos al escaneado.

En tercer lugar, la topología de las redes es dinámica, como consecuencia de las características del medio de transmisión utilizado todas las redes se podrían considerar móviles. Esto ocasiona que la topología percibida por las estaciones móviles varíe de un escaneo a otro. Las variaciones observadas son:

- Número de redes descubiertas
- Potencia de la señal con que se perciben las redes
- Tiempo de respuesta de las redes

Además, las variaciones se ven afectadas por la duración de la espera por canal, esto es debido principalmente a: a mayor duración se pueden detectar redes que presentan tiempos de respuesta mayores y detectar P_{resp} retransmitidos. Por otro lado, un mayor tiempo de espera no garantiza el descubrimiento de la topología completa, los experimentos realizados muestran que para conocer la topología de un despliegue espontáneo se requieren múltiples escaneos. Para cualquiera de los tiempos de espera probados, con 20 escaneos se descubrió al menos el 60 % del máximo registrado para ese mismo tiempo luego de 100 escaneos.

Finalmente, se observa la necesidad de un sistema que permita asistir el proceso de descubrimiento, mediante una base de datos que gestione la topología descubierta en ubicaciones particulares (celdas).

Resulta importante destacar que, los resultados presentados en este trabajo se obtuvieron en despliegues densos ubicados en centros urbanos, por lo

que se sugiere que trabajos futuros exploren el comportamiento del escaneo y las características de los despliegues en entornos sub-urbanos y áreas rurales.

También es importante que, en estudios posteriores, se definan parámetros que midan la calidad de las redes y que permitan evaluar la calidad de los punto de acceso (AP: *Access Point*) descubiertas con las primeros escaneos. De manera que el sistema que realiza el proceso de descubrimiento y la estación móvil (MS: *Mobile Station*) puedan seleccionar los más apropiados en función de los requerimientos de servicio. De igual manera, el sistema propuesto requiere el diseño y la implementación, que contemple la forma en que se debe organizar la información en el servidor, la comunicación entre servidor-caché-cliente y estratégia para la optimización de los parámetros del escaneo en función de la topología.

Apéndice A

Descubierta de redes

Número promedio de redes descubiertas por canal. En la Figura A.1 se toman en cuenta todos los Probe Request (P_{rq}) transmitidos durante la campaña de recolección, por otro lado, en la Figura A.2 solo se toman en cuenta que obtuvieron al menos un Probe Response (P_{resp}). En sombreado se representa el promedio de las redes descubiertas luego de la campaña, en rojo se muestra el promedio de las redes descubiertas en el canal dado.

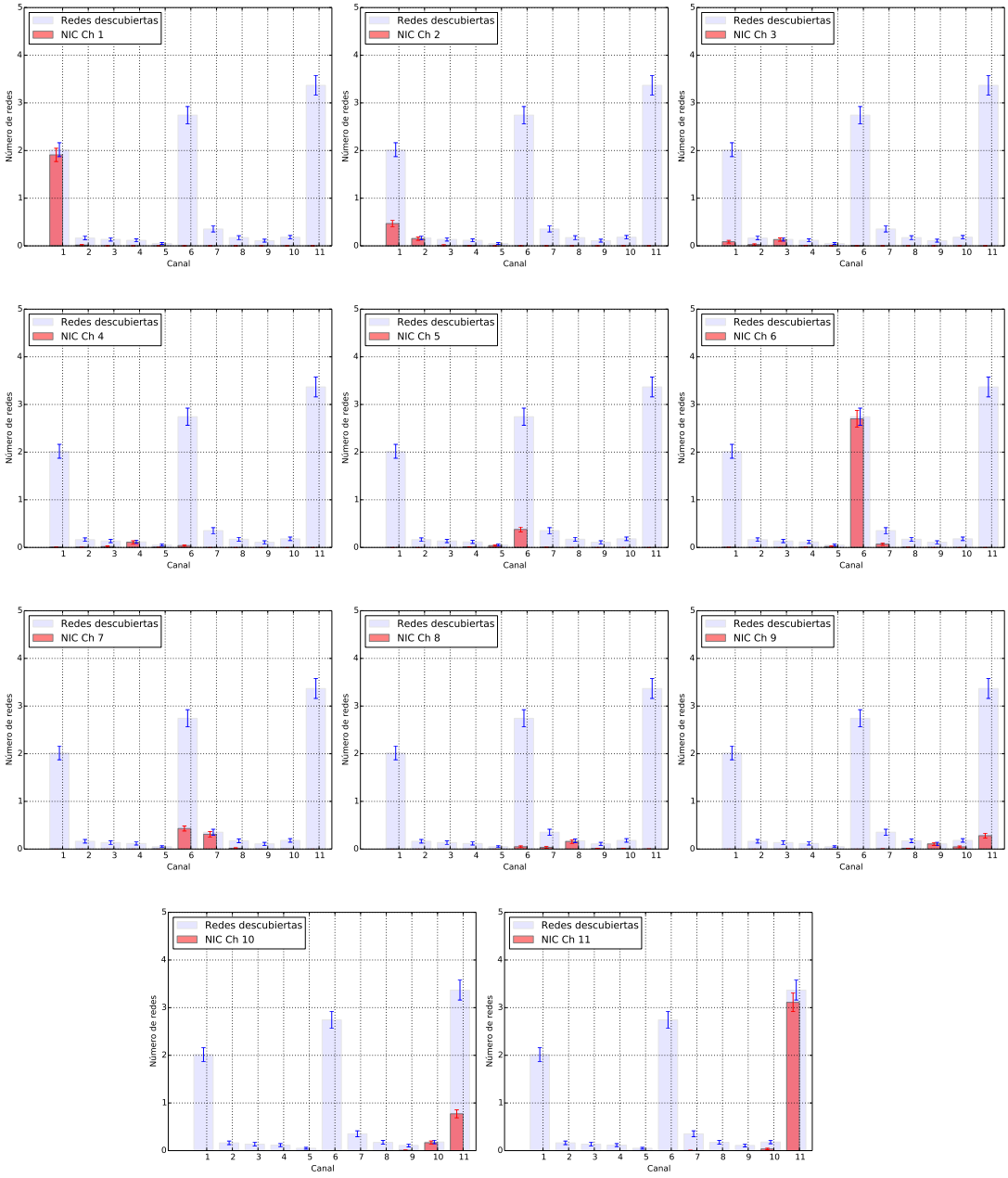


Figura A.1: Redes descubiertas, incluyendo la totalidad de los P_{rq}

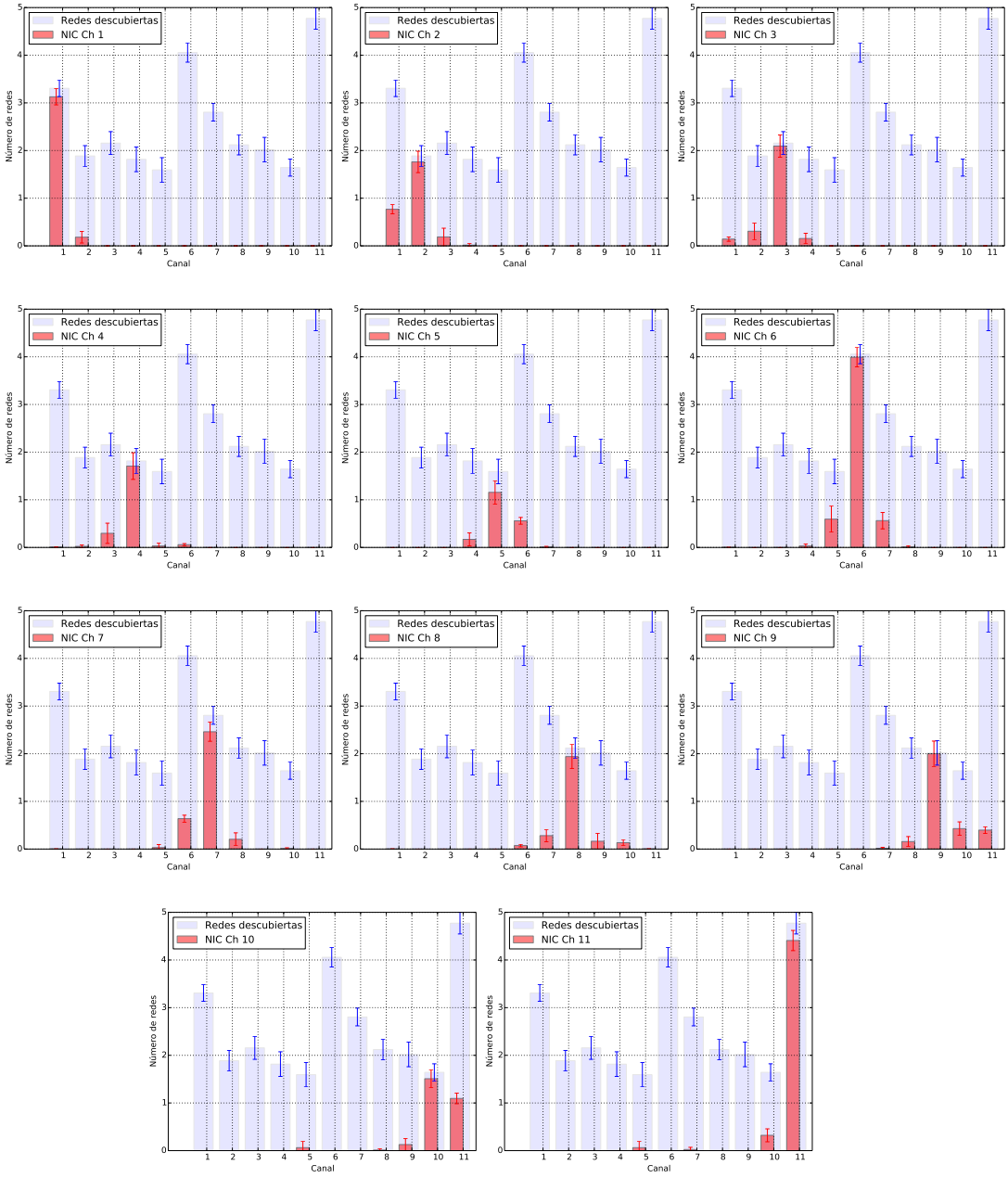


Figura A.2: Redes descubiertas, excluyendo P_{rq} sin respuesta

Apéndice B

Perdida en Probe Request

En el escaneo activo la estación móvil (MS: *Mobile Station*) participa activamente, transmitiendo en *broadcast* un Probe Request (P_{rq}) en cada canal, por lo que no hay garantía de recibo. Para estimar los P_{rq} perdidos durante el descubrimiento se realizó una prueba en laboratorio que consistió en una MS transmitiendo 1000 P_{rq} en el canal 11, mientras un *sniffer* escuchaba las tramas en el medio. Se realizaron dos configuraciones, $C1$ y $C2$. En $C1$ el *sniffer* y la MS se ubicaron lado a lado, en $C2$ el *sniffer* se ubicó al otro extremo del laboratorio, a una distancia aproximada de $8\,m$, con muebles en la línea de visión. Los P_{rq} registrados en el *sniffer* sirven como estimador de los P_{rq} que recibiría un punto de acceso (AP: *Access Point*). Los resultados se muestran en la Tabla B.1.

Configuración	P_{rq} **transmitidos**	P_{rq} **recibidos**	**Perdida**	**Rango de potencia registrado**
$C1$	1000	997	0.3 %	$[-25dBm, -23dBm]$
$C2$	1000	807	19.3 %	$[-84dBm, -53dBm]$

Tabla B.1: Perdida de tramas P_{rq}

Apéndice C

Tiempo entre *Probe Responses*

El tiempo de respuesta en los Probe Response (P_{resp}) correspondientes a un mismo Probe Request (P_{rq}) tiende a disminuir a medida que incrementa la cantidad de P_{resp}. Esto se puede observar en la pendiente de la curva imaginaria formada por el retardo promedio de los P_{resp} mostrados en la Figura C.1

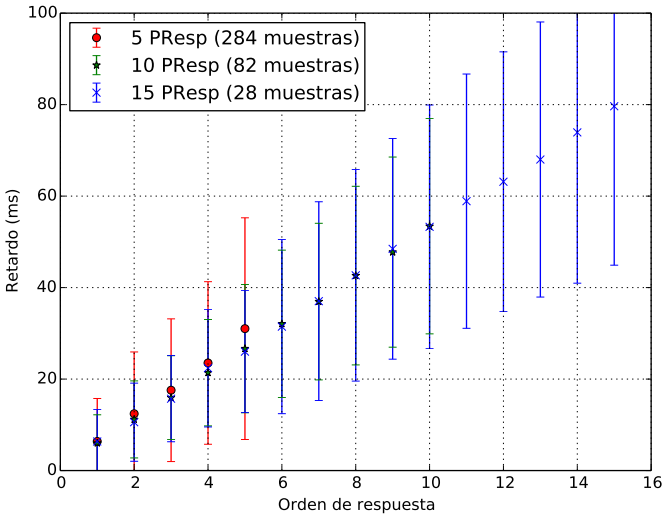


Figura C.1: Retardo promedio de los P_{resp} en relación al orden de llegada

Adicionalmente, la Figura C.2 resume, en gráficos de caja, los tiempos entre respuesta en relación al orden de llegada y la cantidad de P_{resp} detectadas. Se observa que la mediana del tiempo entre respuestas se mantiene por

debajo de $3\,ms$.

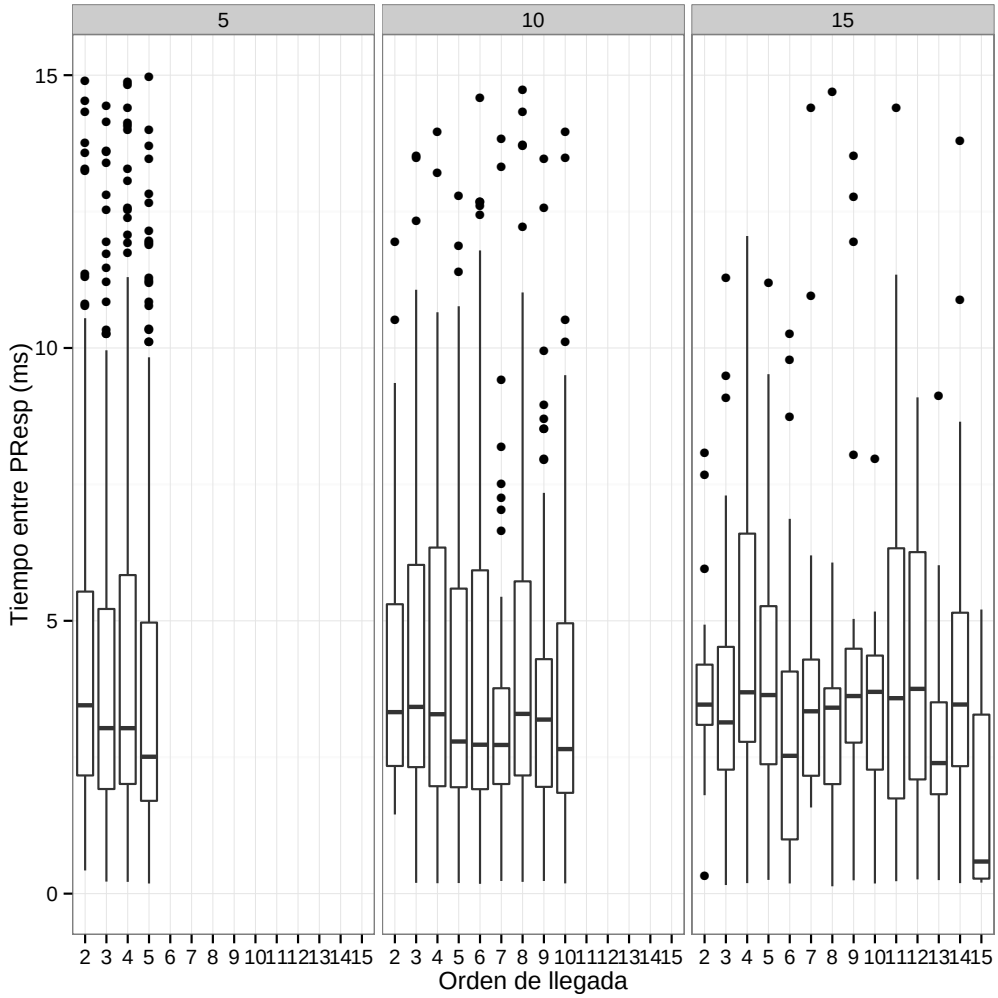


Figura C.2: Tiempo entre P_{resp} en relación al orden de llegada

Glosario

ACK confirmación de recibo o acknowledgement (ACK). 49

AIFS espacio inter-tramas usado por en redes IEEE 802.11 que gestionan la calidad de servicio. 20

AP punto de acceso. 1–3, 6, 8–14, 18, 22–28, 34–46, 51–54, 59–62, 64, 66–69, 71–77, 79, 80, 82–85, 91, 95, 100

BSA área de servicio básico (BSA: *Basic Service Area*). 9, 10, 12

BSS conjunto de servicio básico. 9–11, 14, 15, 28, 47, 49, 53–63, 90, 100

BSSID identificador del conjunto de servicio básico. 48, 59

CDF función de distribución acumulada (CDF: *Cumulative Distribution Function*). 58, 75

CSMA/CA acceso múltiple por detección de portadora con evasión de colisiones. 20, 26, 53, 66

CTS trama de administración utilizada por la entidad coordinadora de una red IEEE 802.11 para otorgar permiso de transmitir datos al medio a una estación que lo solicitó. 18

DCF función de coordinación distribuida, utilizada en las redes de tipo infraestructura para coordinar el acceso al medio. 18–20, 26, 64, 66, 80

DIFS espacio inter-tramas de la función de coordinación distribuida. 19, 20

DR fracción descubierta. 67–70, 72, 80

DS sistema de distribución. 9, 28

DTN red tolerante a retardos. 3

EIFS espacio inter-tramas usado por en caso de detección de transmisión de una trama corrupta. 20

ESS conjunto de servicio extendido. 11, 12, 14

GPS sistema de posicionamiento global (GPS: *Global Positioning System*). 83

HCF función de coordinación híbrida combina funciones de las DCF y PCF en las redes IEEE 802.11. 18

IBSS también conocido como red *ad-hoc*, pues están formadas por distintas MS sin la necesidad de una estación encargada de la coordinación. 10

ISP proveedor de servicio de internet (ISP: *Internet Service Provider*). 60, 90

LAN red de área local. 6

MAC control de acceso al medio. 24, 25, 50

MAN red de área metropolitana. 6

MaxCT MaxChannelTime. 26, 32, 34–40, 45

MinCT MinChannelTime. 26, 32, 34–41, 45

MS estación móvil. 1–3, 6, 8–12, 14, 24–26, 28, 31, 32, 34, 36–38, 40–47, 49–51, 55, 57, 58, 62, 66, 67, 73, 76, 79, 80, 83–88, 91, 95

NIC tarjeta de red. 28

OSA sistema de autenticación abierta. 13, 25

OSI sistema de interconexión de sistemas. 2, 6

P_{resp} Probe Response. 2, 26, 32, 33, 35–39, 43, 45–60, 62, 64, 65, 67, 70, 75–79, 81, 82, 85, 90, 92, 96, 97

P_{rq} Probe Request. 2, 26, 31–36, 38, 39, 43, 45–47, 49–51, 53–58, 62, 64, 65, 67, 77, 79, 90, 92–96

PCF técnica de coordinación de acceso al medio en la que la coordinación está centrada en una estación central denominada punto de acceso (AP: *Access Point*). 18, 19, 100

PIFS espacio inter-tramas utilizado en las redes que operan utilizando función de coordinación puntual (PCF: *Point Coordination Function*). 19

RTS trama de administración utilizada por los dispositivos IEEE 802.11 para reservar el canal cuando desean transmitir datos al medio. 18

SIFS espacio inter-tramas utilizado en las redes IEEE 802.11 para transmisiones de prioridad alta. 19, 20

SSID identificador del conjunto de servicio. 11, 47, 60

TD topología descubierta. 67, 68, 70, 83

TE topología existente. 67, 68, 70, 72

TSF función usada en la sincronización del reloj de los dispositivos pertenecientes a un conjunto de servicio básico (BSS: *Basic Service Set*). 59

UMTS sistema universal de telecomunicaciones móviles. 2

WAN red de área amplia. 6

Bibliografía

[1] "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications." http://standards.ieee.org/about/get/802/802.11.html, 2012. Consultado el 12 de agosto de 2012.

[2] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*. USA: Addison-Wesley Publishing Company, 5th ed., 2009.

[3] We Are Social. http://wearesocial.net/blog/2014/01/social-digital-mobile-worldwide-2014/, 2014. Consultado el 22 de septiembre de 2014.

[4] Statista. http://www.statista.com/statistics/272595/global-shipments-forecast-for-tablets-laptops-and-desktop-pcs/, 2014. Consultado el 22 de septiembre de 2014.

[5] Cisco, "Cisco visual networking index: Global mobile data traffic forecast update, 2011–2016," 2014.

[6] CONATEL. http://www.conatel.gob.ve/index.php/principal/indicadoresanuales, 2014. Consultado el 22 de septiembre de 2014.

[7] V. Mhatre and K. Papagiannaki, "Using smart triggers for improved user performance in 802.11 wireless networks," in *Proceedings of the 4th international conference on Mobile systems, applications and services*, MobiSys '06, (New York, NY, USA), pp. 246–259, ACM, 2006.

[8] A. Mishra, M. Shin, and W. Arbaugh, "An empirical analysis of the IEEE 802.11 MAC layer handoff process," *SIGCOMM Comput. Commun. Rev.*, vol. 33, pp. 93–102, Apr. 2003.

[9] D. Giustiniano, I. Tinnirello, L. Scalia, and A. Levanti, "Revealing transmit diversity mechanisms and their side-effects in commercial ieee 802.11 cards," in *Telecommunication Networking Workshop on QoS in Multiservice IP Networks, 2008. IT-NEWS 2008. 4th International*, pp. 135–141, Febrero 2008.

[10] N. Montavont, A. Arcia-Moret, and G. Castignani, "On the selection of scanning parameters in IEEE 802.11 networks," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on*, pp. 2137–2141, 2013.

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

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

[13] C. A. Bernal, *Metodología de la investigación: Para administración, economía, humanidades y ciencias sociales*. Pearson Educación, 2006.

[14] A. Arcia-Moret, L. Molina, N. Montavont, G. Castignani, and A. Blanc, "Acess point discovery in 802.11 networks," Wireless Days 2014, Noviembre 2014. Artículo aceptado.

[15] L. Molina and A. Arcia-Moret, "Evaluación del proceso de escaneo en redes 802.11: una perspectiva taxonómica," in *1era Conferencia Nacional de Computación, Informática y Sistemas*, Octubre 2013.

[16] A. Arcia-Moret, L. Molina, G. Castignani, and N. Montavont, "Characterizing spontaneous IEEE 802.11 network deployments," in *Network Games, Control and Optimization (NetGCooP), 2012 6th International Conference on*, pp. 1–8, Noviembre 2012.

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

[18] L. Molina and A. Arcia-Moret, "Caracterización de redes 802.11," 3er Congreso Nacional de Estudiantes de Ingeniería, Marzo 2012.

[19] A. F. Molisch, *Wireless Communications*. John Wiley & Sons, 2007.

[20] M. Gast, *802.11 Wireless Networks: The Definitive Guide*. O'Reilly & Associates, Inc, 2 ed., 2005.

[21] Jane Butler et al., *Wireless Networking in the Developing World*. CreateSpace Independent Publishing Platform, 2013.

[22] Cisco, "Understanding delay in packet voice networks." `http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00800a8993.shtml#standarfordelaylimits`. Consultado el 12 de julio de 2012.

[23] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*. Pearson Education, 5 ed., 2011.

[24] H. Velayos and 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.

[25] A. R. Prasad and N. R. Prasad, *802.11 WLANs and IP networking: security, QoS, and mobility*. Artech Hoyse, 2005.

[26] A. Kushki, K. Plataniotis, and A. Venetsanopoulos, "Kernel-based positioning in wireless local area networks," *Mobile Computing, IEEE Transactions on*, vol. 6, pp. 689–705, Junio 2007.

[27] C. Feng, W. Au, S. Valaee, and Z. Tan, "Received-signal-strength-based indoor positioning using compressive sensing," *Mobile Computing, IEEE Transactions on*, vol. 11, pp. 1983–1993, Diciembre 2012.

[28] V. Gupta, R. Beyah, and C. Corbett, "A characterization of wireless NIC active scanning algorithms," in *Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE*, pp. 2385–2390, IEEE, Marzo 2007.

[29] S. Shin, A. G. Forte, A. S. Rawat, and H. Schulzrinne, "Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs," in *Proceedings of*

the second international workshop on Mobility management & wireless access protocols, MobiWac '04, (New York, NY, USA), pp. 19–26, ACM, 2004.

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

[31] N. Montavont, J. Montavont, and T. Noel, "Enhanced schemes for L2 handover in IEEE 802.11 networks and their evaluations," in *IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications PIMRC*, vol. 3, pp. 1429 – 1434, 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.

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

[33] H. Wu, K. Tan, Y. Zhang, and 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.

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

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

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

[37] J. Teng, C. Xu, W. Jia, and 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.

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

[39] G. Castignani, *Exploiting Network Diversity*. PhD thesis, Télécom Bretagne - Université Européene de Bretagne, 2012.

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

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

[42] K. N. Gopinath, P. Bhagwat, and K. Gopinath, "An empirical analysis of heterogeneity in ieee 802.11 mac protocol implementations and its implications," in *Proceedings of the 1st international workshop on Wireless network testbeds, experimental evaluation & characterization*, WiNTECH '06, (New York, NY, USA), pp. 80–87, ACM, 2006.

[43] A. Di Stefano, A. Scaglione, G. Terrazzino, I. Tinnirello, V. Ammirata, L. Scalia, G. Bianchi, and C. Giaconia, "On the fidelity of ieee 802.11 commercial cards," in *Proceedings of the First International Conference on Wireless Internet*, WICON '05, (Washington, DC, USA), pp. 10–17, IEEE Computer Society, 2005.

[44] G. Castignani, L. Loiseau, and N. Montavont, "An evaluation of IEEE 802.11 community networks deployments," in *2011 International Conference on Information Networking (ICOIN)*, pp. 498–503, IEEE, Jan. 2011.

[45] P. Fuxjager, D. Valerio, and F. Ricciato, "The myth of non-overlapping channels: interference measurements in IEEE 802.11," in *Proc. Fourth Annual Conference on Wireless on Demand Network Systems and Services (WONS'07)*, pp. 1–8, 2007.

[46] J. Saldana, A. Arcia-Moret, B. Braem, L. Navarro, E. Pietrosemoli, C. Rey-Moreno, A. Sathiaseelan, and M. Zennaro, "Community Networks. Definition and Taxonomy.." draft-manyfolks-gaia-community-networks-00, June 2014.