Caracterización de Despliegues Espontáneos IEEE 802.11

Laudin Molina, Andrés Arcia-Moret, German Castignani y Nicolás Montavont

***Resumen*—El alto nivel de conectividad y movilidad de los dispositivos actuales, junto con la disminución del costo de las tecnologías de acceso, han permitido la puesta en funcionamiento de una gran cantidad de puntos de acceso de forma completamente descentralizada. En las tecnologías de tipo IEEE 802.11, esto produce que antes de establecerse un enlace con una red, los dispositivos móviles deban descubrir los puntos de acceso disponibles en una topología por lo general desconocida. En este trabajo se estudian e identifican mediante experiencias con plataformas reales, algunas características relevantes de los despliegues de redes 802.11 formados espontáneamente, que podrían ser explotadas con el objetivo de mejorar tanto el proceso de configuración de los puntos de acceso como el rendimiento de las aplicaciones.**

***Palabras claves*—802.11, *ChannelTime*, despliegues espontáneos, *scanning*.**

I. Introducción

Las redes inalámbricas IEEE 802.11 han superado el nivel de expansión y popularidad de las redes Ethernet; que en su momento hicieron posible la expansión de la Internet que se conoce hoy. Las redes 802.11 hacen posible un acceso ubicuo a la Internet, permitiendo además que los usuarios sean parcialmente móviles. En la actualidad los dispositivos móviles como tabletas, teléfonos inteligentes y consolas de juego cuentan con interfaces de red 802.11, permitiendo ejecutar aplicaciones que tendrían un mejor desempeño si tuvieran conectividad a la red en forma ubicua e ininterrumpida. Esto representa un reto para las tecnologías 802.11, pues para lograr un mejor nivel de movilidad los usuarios deben ser capaces de desplazarse entre redes sin interrupciones notables desde las aplicaciones, lo que hoy por hoy no es posible.

Dentro de las tecnologías disponibles en la norma IEEE 802.11 [1], la utilización más frecuente de estas redes se realiza en la banda del espectro de radio correspondiente a los 2.4 GHz. En el dominio regulatorio Americano se definen 11 canales, desde 2412 MHz hasta 2462 MHz. En 802.11b estos canales poseen una longitud de 22 MHz mientras que en 802.11g, que utiliza Multiplexación por División de Frecuencias Ortogonales, (OFDM, *Orthogonal Frequency Division Multiplexing*) la longitud se reduce a 20 MHz. En ambos casos, la separación entre canales es de 5 MHz, lo que implica que los canales vecinos solapan sus frecuencias, produciendo un nivel de interferencia no despreciable, provocando un aumento en la cantidad de colisiones.

Entre las redes 802.11 se distinguen dos tipos de topología: infraestructura y *ad-hoc*. En el tipo infraestructura es necesaria la presencia de una estación base, denominada punto de acceso (AP, *Access Point)*, encargada de coordinar la red. Todas las comunicaciones se realizan a través del AP por lo que las estaciones que forman la red deben establecer y mantener una conexión con éste. Por otro lado, en las redes *ad-hoc* las estaciones son capaces de comunicarse con sus pares sin la presencia de una estación base. Este trabajo se centra en las redes de tipo infraestructura, aunque muchos de los experimentos y resultados podrían ser válidos en las redes de tipo *ad-hoc*.

Dado que el espectro de frecuencia en el que opera el estándar 802.11 es libre, en la práctica se encuentran numerosas redes desplegadas en forma independiente, es decir, sin coordinación ni planificación central, lo que conlleva a redes con características y configuraciones variables y con los puntos de acceso distribuidos sin un patrón predecible. La agregación de estas redes forman despliegues que llamaremos espontáneos.

En un compendio de trabajos [2], [3], [4] se ha observado un alto nivel de divergencia en el comportamiento de los AP a nivel del acceso al medio (MAC, *Medium Access Control*) y en la topología de las redes. Particularmente, hay divergencias en cuanto a la distribución de canales, los niveles de interferencia y mecanismos de seguridad. Esto, aunque propio de sistemas sin planificación, merece ser estudiado para distinguir rasgos característicos útiles, que podrían ser aprovechados para mejorar la movilidad de los usuarios, el uso de las redes 802.11 y el rendimiento de las aplicaciones.

I-A. Trabajos relacionados

En esta sección, se presentan distintos esfuerzos que estudian o caracterizan el despliegue de redes inalámbricas, luego se comentan trabajos que estudian el proceso de descubrimiento en redes 802.11.

Respecto a la evaluación y caracterización de despliegue de redes 802.11, en [2] presentan una serie indicadores para describir las condiciones que enfrenta un usuario que desea conectarse a una red 802.11. Éstos indicadores fueron utilizados para evaluar el potencial de las redes comunitarias 802.11 en la ciudad de Rennes, Francia. Los autores de [2] determinaron que los dos proveedores de acceso a Internet a través de 802.11 más grandes, podrían ofrecer conectividad en forma ininterrumpida a un usuario móvil a lo largo de 450 m,

Artículo recibido el 03 de Enero de 2012. Este artículo fue financiado por la Universidad de Los Andes.

L.M. y A.A.M están con la Universidad de los Andes, Mérida, Venezuela. E-mail: laudin@ula.ve, andres.arcia@ula.ve

G.C. y N.M. están con el *Institut TELECOM/TELECOM Bretagne*, Rennes, Francia. email: german@castignani.com.ar, nicolas@montavont.net

siempre que el usuario sea capaz de cambiar de un AP a otro en forma rápida y eficiente.

Otro trabajo que implica la revisión de despliegues en escenarios reales es presentado en [3], que centra su estudio en mostrar cómo la interferencia en las redes 802.11, desplegadas en forma espontánea, afecta significativamente el desempeño de las aplicaciones. Para ello, toma muestras de las redes inalámbricas desplegadas en distintas ciudades de Estados Unidos de América y muestra que una selección apropiada de los canales, por ejemplo, usando los canales no solapados, es posible mitigar los efectos negativos de la interferencia.

En [4] presentan un análisis de las variaciones en las implementaciones del protocolo 802.11 y su impacto en el segmento de acceso inalámbrico. Además, los autores demuestran que algunos dispositivos 802.11 no se ajustan al estándar, mientras que en otros casos presentan diferencias considerables que podrían impactar negativamente las operaciones de la red.

Algunos sitios Web también recolectan información sobre el despliegue de redes 802.11. Ejemplos populares son Wigle [5], WiFiMap [6] y WeFi [7].

En relación al proceso de descubrimiento, en [8] describen un método que permite evaluar el tiempo de retardo de un *Probe Request* haciendo uso de *sniffers*. El trabajo presenta un análisis detallado sobre el proceso de *handover*, concluyendo que la fase del *scanning* es responsable del 90 % del retardo.

En [9] estudian, mediante simulaciones, la influencia del número de *hosts* en redes 802.11b sobre el número de colisiones, la duración del *scanning activo* y el tiempo de transmisión de los *Probe Response*. Estiman valores ideales de *MinChannelTime* y *MaxChannelTime*, fijándolos en 0,670 ms y 10,24 ms respectivamente. El valor de *MinChannelTime* es calculado mediante análisis teórico, mientras que el valor de *MaxChannelTime* se obtiene de simulaciones.

I-B. Contribuciones

En este trabajo se presentan dos aspectos complementarios en las redes 802.11: por una parte se estudia la implementación y validación del proceso de descubrimiento de despliegues desconocidos utilizando *scanning activo* (descrito en la sección II) y luego se revisan rasgos característicos presentes en despliegues de redes formadas espontáneamente. Para ello se implementa y prueba un procedimiento que permite conocer con precisión el tiempo que ocupa recibir respuesta de un AP ante un *scanning activo*, es decir, el tiempo de recibir un *Probe Response* una vez que se ha emitido un *Probe Request*. Luego se identifican factores que mostraron influencia en el tiempo de respuesta de los AP. Finalmente, utilizando las experiencias adquiridas con las pruebas de laboratorio, se describen las redes desplegadas en el casco central de la ciudad de Mérida en términos que permitan identificar características que podrían ser aprovechadas para mejorar el desempeño de los procesos de descubrimiento de redes 802.11 desplegadas en forma descentralizada y espontánea.

El resto de este trabajo está organizado como sigue. En la sección II se describe el procedimiento necesario para conectarse a una red 802.11. La sección III describe la metodología utilizada en la medición de los tiempos de respuesta de los AP y los experimentos realizados en laboratorio. En la sección IV se presentan los experimentos realizados en ciudad y las características de un despliegue espontáneo. Finalmente, en la sección V se discuten los resultados de los experimentos conducidos y se delinean los trabajos futuros.

II. CONECTÁNDOSE A UNA RED 802.11

En las redes 802.11, toda estación móvil debe mantener enlace con exactamente un AP a fin de pertenecer a la red y enviar y recibir tráfico. El primer paso para establecer la conexión consiste en reconocer los AP disponibles o alcanzables y sus características, para luego se seleccionar el AP con el que se mantendrá el enlace. Luego de seleccionado el AP con el que se establecerá el enlace, la estación iniciará el proceso de asociación y autenticación.

El reconocimiento de los AP puede ser realizado de dos maneras, a saber, *scanning pasivo* y *scanning activo*. En el *scanning pasivo*, el dispositivo cliente está atento a tramas de tipo administración (*management*), denominadas *Beacons*, enviadas periódicamente por los AP, estas tramas contienen información sobre el AP y que permite realizar el proceso de asociación y mantener sincronizadas las estaciones que forman parte de la red. En el *scanning activo*, el dispositivo cliente difunde tramas (denominadas *Probe Request*) en los distintos canales especificados en la norma y espera por tramas de respuesta (denominadas *Probe Response*) de los AP que recibieron su solicitud. Una estación que realiza un *scanning activo* explora todos los canales del espectro de la siguiente manera: el proceso se inicia ajustando la interfaz 802.11 para operar en uno de los canales, se transmite un *Probe Request* y se espera por un periodo denominado *MinChannelTime*. Si cumplido este periodo se ha registrado actividad en el canal, es decir, se han recibido tramas provenientes de algún AP, la estación aumenta el periodo de espera hasta *MaxChannelTime* antes de pasar revisar otro canal. Si luego de *MinChannelTime* no se ha registrado actividad en el canal se pasa a procesar el siguiente canal.

De forma análoga, una estación que se desplaza fuera del alcance de un AP debe realizar un proceso de reconocimiento a fin de seleccionar un AP con el que pueda establecer un nuevo enlace y así mantener conectividad. El proceso de cambiar de un AP a otro es conocido como *handover*. Dada la cobertura relativamente pequeña de un AP (alrededor de 100 mts, variable en función de la interferencia y las características del entorno), una estación que se desplaza debe cambiar frecuentemente el AP con el que mantiene enlace, por lo que la duración total del *scanning* y su efectividad, en términos del porcentaje de AP descubiertos, resulta crítico.

Una estación móvil que debe realizar un reconocimiento de los AP por lo general utiliza el *scanning activo*, pues la duración del *scanning pasivo* depende de la frecuencia con la que los AP transmitan los *beacons*, que en la mayoría de los casos se realiza cada 100 ms, lo que implica que la estación debe esperar en cada canal por un periodo de al menos 100 ms y en consecuencia la duración total del *scanning* será de al menos 1,1 s (100 ms x 11 canales).

Varios estudios se han realizado a fin de estimar el impacto del *scanning activo* en la ejecución del *handover*. De acuerdo

con [8], el *scanning activo* es responsable del 90 % de la duración del *handover*. En [10], evalúan el impacto de *MinChannelTime* y *MaxChannelTime* en la efectividad y duración del *scanning activo*, siendo estos dos aspectos determinantes en la utilidad del descubrimiento. De acuerdo con la Fig. 1, la duración y efectividad del *scanning activo* se puede expresar como una función de *MinChannelTime* y *MaxChannelTime*. Como se observa, un valor muy corto para *MinChannelTime* puede provocar que la estación móvil asuma erradamente que algunos canales se encuentran desiertos, tal como sucede en la Fig.1 cuando la estación revisa el canal 11. Por otro lado, valores de *MinChannelTime* y *MaxChannelTime* muy largos pueden resultar en la estación en estado ocioso, como sucede cuando se revisa el canal 2, en donde la estación espera *MaxChannelTime* aún cuando en *MinChannelTime* ya se habían descubierto todos los AP operando en el canal. Los valores ideales para *MinChannelTime* y *MaxChannelTime* deben permitir descubrir la totalidad de los AP útiles en un tiempo acorde a las necesidades de la red y las aplicaciones en ejecución, tal como sucede cuando se revisa el canal 1, donde se descubre la mayor parte de los AP, ignorando los AP que posiblemente no sean útiles debido a la latencia que provocarían.

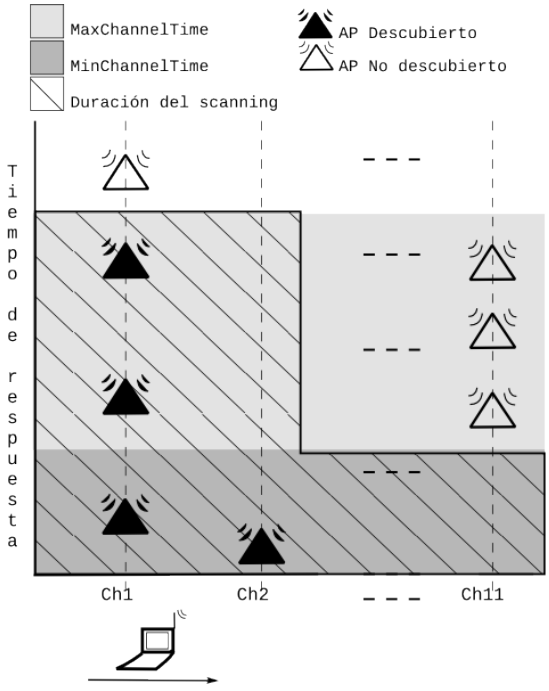


FIG. 1. *Scanning activo*

III. Experimentación en laboratorio

Los experimentos de laboratorio tienen como objeto entender, con pruebas de caja negra, la conducta de los AP de distintos modelos y en configuraciones de red diferente. Así, se identifican posibles causas de retardo en el tiempo de respuesta de un *Probe Response*.

Se diseñaron cuatro configuraciones detalladas en la sección III-C. En cada una se utilizó una estación para ejecutar los *scanning activos*, uno o más AP, según las necesidades del experimento, y dos *sniffers*. Los *sniffers* se utilizaron para reproducir el procedimiento descrito en [8] y a la vez validar la metodología utilizada y presentada en el presente trabajo. La ejecución del *scanning activo* y el uso de los *sniffers* es descrito en la sección III-B.

En cada prueba se ejecutó 39 veces el proceso de *scanning activo*. A fin de reducir los efectos que puedan producir la distancia, los obstáculos u otros dispositivos operando en la misma frecuencia, las pruebas se realizaron bajo condiciones controladas. La estación que realizaba el *scanning activo* y los AP tenían una separación de 1,5 m y mantenían línea visual, tal como se muestra en la Fig. 2, los *sniffers* se posicionaron junto a la estación a fin de no interrumpir la línea visual con los AP. Otros dispositivos 802.11, teléfonos inalámbricos, transmisores de vídeo y equipos que operan en la frecuencia 2,4 GHz fueron desactivados.

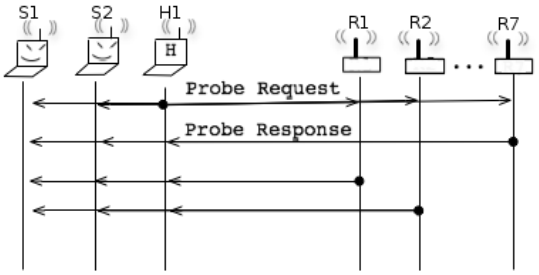


FIG. 2. Configuración del ambiente de pruebas

III-A. Plataforma

- *Access Points*:
  - **R1**: Linksys WRT54G, DD-WRT v24-sp2.
  - **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.
- *Hosts*:
  - **H1**: DELL XPSM1210, chipset INTEL 3945, Debian Wheezy (kernel Linux personalizado, detalle en la sección III-B).
- *Sniffers*:
  - **S1**: HP Pavilion DV 1000, chipset Broadcom. Ubuntu 10.10 (kernel Linux 2.6.35)
  - **S2**: HP Paviliondv4-1129la, chipset Intel Wifi Link 5100, Ubuntu 10.04 (kernel Linux 2.6.32).

III-B. Metodología

Para medir el tiempo de descubrimiento de los AP, la estación que realiza el *scanning activo* se instaló con una versión modificada de la versión 3.0 del kernel de Linux[11], específicamente se modificó el módulo `mac80211`, que implementa el control de acceso al medio. Las modificaciones consisten en identificar el instante de tiempo en que el *Probe Request* es construido por el sistema operativo y enviado al

driver de la interfaz 802.11 listo para ser transmitido al medio y el instante en que el sistema operativo se percata de la llegada de un *Probe Response*. Ésta metodología toma la diferencia entre estos dos tiempos como el tiempo de descubrimiento o retardo asociado a un *Probe Response*.

Durante las pruebas de laboratorio también se utilizó, en forma simultanea, la metodología descrita en [8]. Para ello las estaciones S1 y S2 se configuraron para ejecutar el programa Wireshark[12], un programa que permite configurar una estación para operar como un *sniffer* y así inspeccionar el trafico de red a nivel de la capa MAC. De esta manera, se puede identificar el instante de tiempo en la estación móvil transmite al medio un *Probe Request* y el instante de tiempo en que los AP responden con un *Probe Response*. En los experimentos realizados se utilizaron dos *sniffers* a fin de aumentar la confiabilidad de los resultados.

En la Fig. 3 se comparan los resultados obtenidos por los dos métodos descritos. Tal como se observa, los experimentos presentados en este trabajo siguieren una diferencia de 1,8 ms. Esta diferencia es atribuida al tiempo de procesamiento de las tramas en el kernel y a sesgos que podría introducir el uso de elementos externos a la estación y los AP.

Parte de nuestros experimentos apuntan a la evaluación del tiempo de ejecución de un *scanning*, por lo que el tiempo de retardo desde el punto de vista del kernel resulta más apropiado, razón por la que se descartó la medición mediante *sniffers*. El procedimiento desde el kernel incluye los tiempos de procesamiento (por ejemplo, procesamiento de colas), que obviamente no son tomados en cuenta al utilizar *sniffers*.

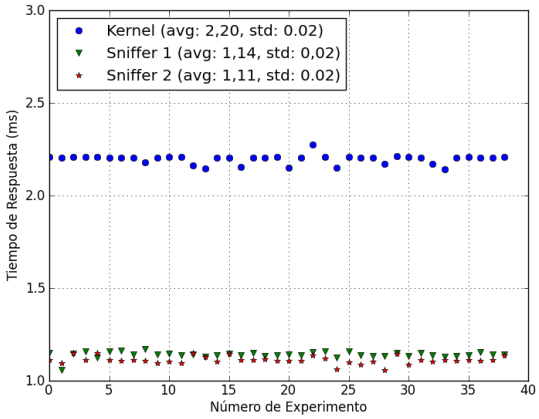


FIG. 3. Dos estrategias para medir el tiempo de descubrimiento

El algoritmo implementado en el kernel se diferencia del algoritmo estándar descrito en la Sección II. En este caso, se ajusta la tarjeta de red en el canal 1, se envía un *Probe Request* por este canal y espera respuestas (*Probe Responses*) por un lapso de 60 ms. Este procedimiento es repetido para cada uno de los 11 canales usados en Venezuela. En adelante, este será el algoritmo utilizado para el *scanning* referido en este trabajo.

III-C. Resultados

- **Configuración 1**: Con la primera configuración se pretende comparar el tiempo de descubrimiento para los AP de distintos modelos y fabricantes. Se realizaron cinco pruebas utilizando los AP: {R1, R2, R3, R4, R5} de manera independiente (uno a la vez) en el canal 6. La Fig. 4 muestra que AP de distintos fabricantes/modelos presentan desempeños diferentes al momento de responder a un *scanning activo*, resultado que es atribuido a las características del *hardware* y *firmware* presentes en cada uno de los AP utilizados. Si bien en [4] no se hace una evaluación exhaustiva del tiempo de respuesta de los AP en función de los modelos, sus resultados concuerdan con los presentados en este trabajo. En [4] muestran diferencias en los tiempos asociados al intercambio *Probe Request – Probe Response*, diferencias atribuidas a las distintas heurísticas utilizadas por los fabricantes de las interfaces de red.

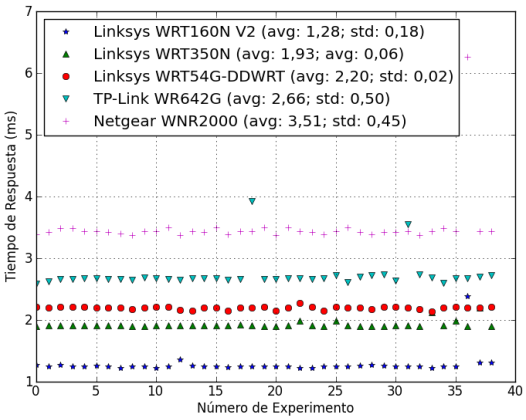
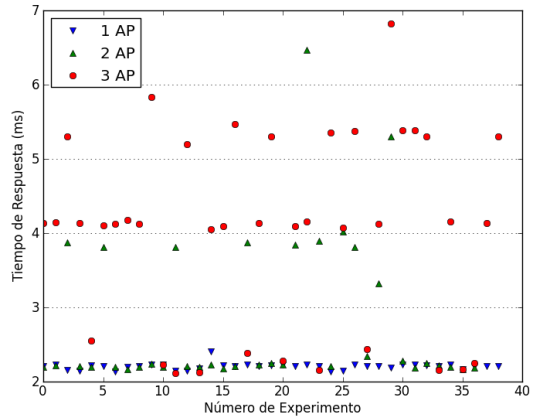
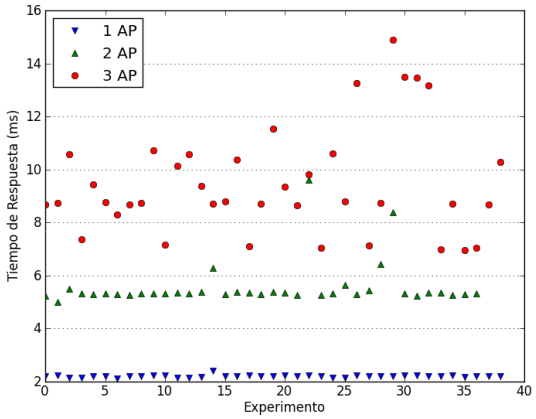


FIG. 4. Retardo para distintos modelos de AP

- **Configuración 2**: En esta prueba se pretende evaluar la influencia de la congestión de un canal en el tiempo de respuesta. Para ello se tomaron varios AP con las mismas características (marca, modelo y firmware) y se configuraron para operar en el canal 6. Inicialmente se configuró sólo un AP (R1), luego se configuraron 2 AP (R1 y R6), luego 3 AP (R1, R6 y R7). La Fig. 5(a) y Fig. 5(b) muestran los tiempos de la primera y última respuesta respectivamente, en ellas se pueden observar dos cuestiones: 1) El tiempo de descubrimiento aumenta en proporción con la ocupación del canal (cantidad de AP operando en la misma frecuencia). 2) El tiempo de respuesta de los AP se vuelve irregular en la medida en que aumenta la ocupación del canal. Atribuimos este comportamiento a la aplicación de la "función de coordinación distribuida" (DCF, *Distributed Coordinated Function*), que es utilizada en la norma IEEE 802.11 para compartir el medio de transmisión. DCF emplea "acceso múltiple por detección de portadora con evasión de colisiones" (CSMA/CA, *Carrier Sense Multiple Access with Collision Avoidance*). De acuerdo con [1], CSMA/CA



(a) Primera respuesta según la cantidad de AP operando en el canal 6



(b) Última respuesta según la cantidad de AP operando en el canal 6

FIG. 5. Tiempos de descubrimiento en laboratorio

obliga a las interfaces que desean transmitir una trama y han detectado que el medio está ocupado, a realizar un *backoff* por un tiempo aleatorio una vez que el medio se encuentra libre y antes de intentar transmitir una trama. En la Fig. 6 se muestra como la DCF afecta el tiempo de respuesta de dos AP operando en el mismo canal. El proceso comienza con la estación enviando un *Probe Request*, dado que AP1 responde primero, reserva el acceso al medio y transmite un *Probe Response*. Luego, AP2 detecta que el medio está ocupado, por lo que debe esperar que AP1 termine la transmisión y luego realizar un *backoff* antes de transmitir. Este proceso debe repetirse cada vez que se detecte que el medio está ocupado.

- **Configuración 3**: En esta configuración se comparan los tiempos de respuesta de un *Probe Response* en un despliegue constituido por 3 AP (R1, R2, R3) operando en el mismo canal (canal 6) con una topología en la que se tienen 3 AP operando en los canales no solapados 1, 6 y 11. Los resultados obtenidos (Fig. 7), indican que una apropiada distribución de los canales mejora el rendimiento de la red, resultados que se ajustan a lo

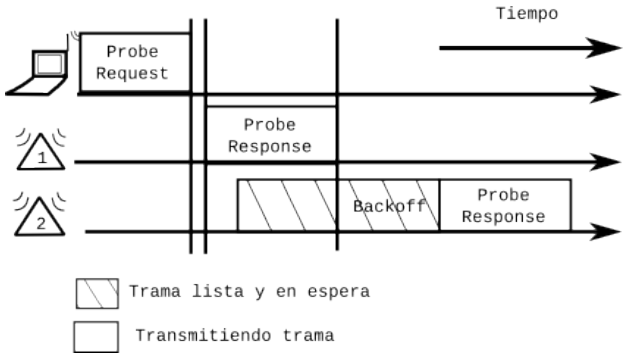


FIG. 6. *Scanning activo* y el *backoff*

observado en la configuración 2.

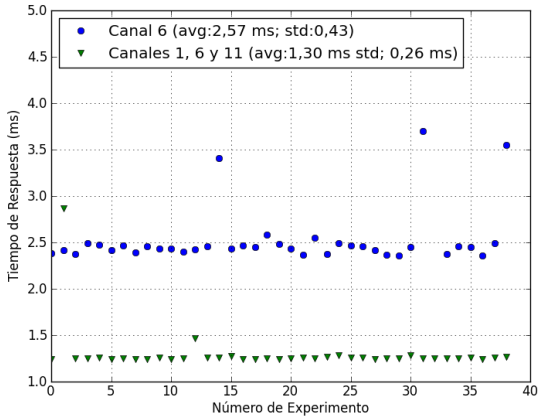


FIG. 7. 3 AP en el canal 6 y 3 AP en los canales 1, 6 y 11

IV. Rasgos característicos de los despliegues espontáneos

A fin de caracterizar la topología de una red 802.11 desplegada en forma espontánea, se recolectó información sobre los AP instalados en el casco central de la ciudad de Mérida, Venezuela, que alberga más de 240.000 habitantes [13]. Para la recolección de datos se tomaron muestras en 44 puntos del recorrido de 2 Km mostrados en la Fig. 8. En cada punto se forzó la ejecución de 10 *scanning activos* a intervalos de 3 segundos. Cada *scanning* se realizó según el procedimiento descrito en la sección III y utilizando la estación H1 inmóvil en cada punto.

La información recolectada corresponde a: mecanismos de seguridad utilizados, frecuencia de radio en la que operan, calidad de la señal y el tiempo de descubrimiento. Cabe destacar que en ningún momento se registró información privada y sólo se utilizó información publicada por los distintos dispositivos.

IV-A. Resultados generales

Un total de 195 AP de 20 fabricantes fueron registrados en todo el recorrido, de estos el 69,59 % (ver Fig. 9(a)) opera en canales no solapados (1, 6, 11), resultado relativamente

FIG. 8. Puntos de recolección de datos en campo

TABLA I
PROBABILIDAD DE RECIBIR *Probe Responses* A N CANALES DEL CANAL EN EL QUE OPERA EL AP QUE LOS ORIGINÓ

Canales de distancia (n)	Probabilidad
0	0,618
1	0,283
2	0,095
3	0,004

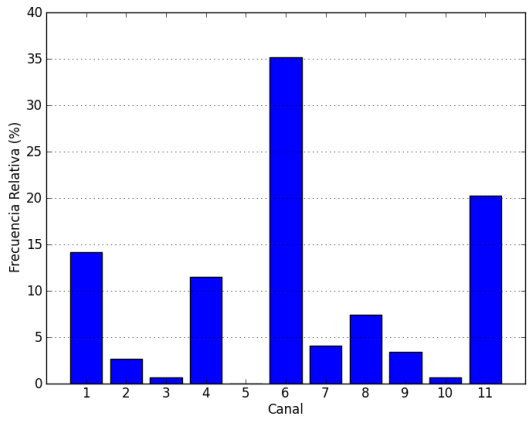
inferior al 78,21 % reportado por [2], correspondiente a un estudio dirigido en Rennes, Francia. Respecto al mecanismo de seguridad utilizado en la capa MAC, se observó que el 89,9 % de los AP utilizan un mecanismo de seguridad en la capa MAC, repartidos de la siguiente manera: 66,5 % utiliza "Acceso Wi-Fi Protegido" (WPA, *Wi-Fi Protected Access*) y 23,4 % utiliza "Privacidad Equivalente a Cableado" (WEP, *Wired Equivalent Privacy*). Solo un 10,1 % opera en modo abierto (OSA, *Open System Authentication*). Finalmente, la Fig. 9(b) indica que el 56 % de los AP tiene señal suficientemente fuerte como para ser utilizados[1].

IV-B. Tipos de respuesta encontrados

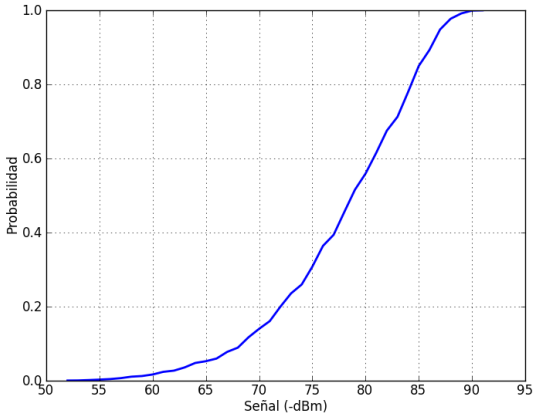
Durante los experimentos se observó que los AP desplegados en ciudad presentan comportamientos diferentes al momento de responder a un *Probe Request*.

1. **Comportamiento ideal**: se espera recibir un *Probe Response* de cada AP por cada *Probe Request* emitido, con cada *Probe Response* recibido en el mismo canal en el que opera el AP. Este comportamiento se contabilizó en el 61,8 % de los *Probe Responses* registrados, que corresponden a $n = 0$ canales de separación entre el canal por el que se recibió el *Probe Response* (i.e., el mismo en el que se envió el *Probe Request*) y el canal en el que realmente opera el AP descubierto, representado en la primera fila de la Tabla I.
2. **Respuestas por canales distintos**: la estación que realiza el *scanning* recibió el 38, 2 % de los *Probe Responses* en un canal diferente del que opera el AP que lo generó. Como se muestra en la Tabla I, los *Probe Response* se encontraron a 1, 2 y hasta 3 canales de distancia del canal en el que opera el AP. Lo que sugiere que la interfaz de red de la estación y/o de algunos AP es capaz de recibir correctamente tramas transmitidas por canales vecinos.

[1]El estándar IEEE 802.12 [1] establece que las interfaces deben tener una sensibilidad de -80 dBm.



(a) Distribución de canales



(b) Calidad de la señal

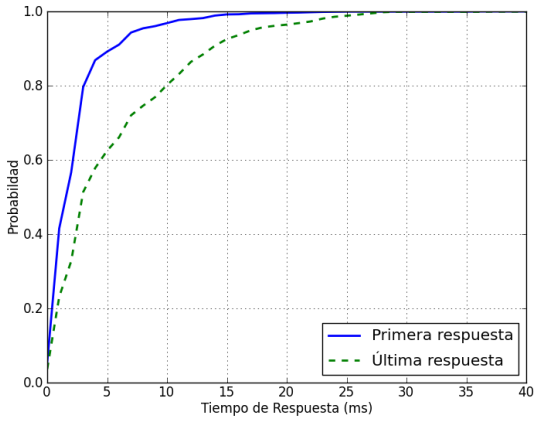
FIG. 9. Resultados generales

3. **Repuestas repetidas**: se presenta en un 23, 08 % de las muestras considerando que este caso se solapa con los 2 casos anteriores. En este caso se recibían 2 o más *Probe Response* en el mismo canal a un mismo *Probe Request*. Dos explicaciones a las que se podría atribuir este comportamiento son: 1) algunos algoritmos implementados en los AP responden a los *Probe Request* con más de un *Probe Response*; 2) retransmisión de los *Probe Responses* por pérdidas de ACKs emitidos por la estación que realiza scanning confirmando la recepción de un *Probe Response*.

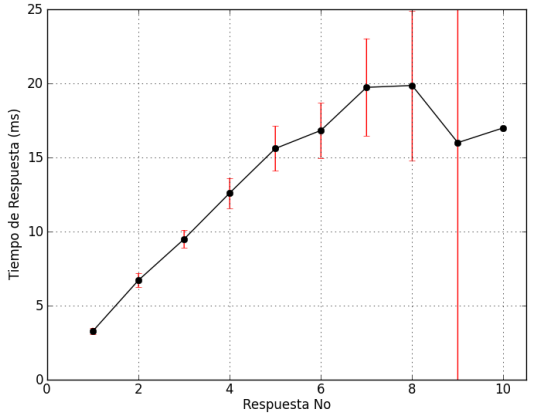
IV-C. Tiempos de respuesta

En la Fig. 10(a), se presenta la frecuencia acumulada para los tiempos de la primera y última respuesta a cada *Probe Request* transmitido, datos relevantes para la selección de los valores que debe tener *MinChannelTime* y *MaxChannelTime* a fin de asegurar descubrir un porcentaje satisfactorio de los AP. Según esto, la probabilidad de recibir el primer *Probe Response* en menos de 6 ms es de 0,9. Y, con probabilidad igual a 0,8 el último *Probe Response* es recibido en 11 ms o menos.

En la Fig. 10(b) se observa el comportamiento del tiempo de respuesta de los *Probe Responses* en el canal 6 (el más poblado). En el eje de las abscisas, se disponen el orden de recepción de las *Probe Responses*. Obsérvese que el tiempo de recepción de las respuestas crece conforme se reciben más respuestas; lo que parece natural. Sin embargo, no todos los puntos del recorrido donde se ejecutó el *scanning*, habían 9 o más AP. Rompiendo así la coherencia de la gráfica.



(a) Primer y último *Probe Responses*



(b) Secuencia de *Probe Response* recibidos

FIG. 10. Tiempos de respuesta de *Probe Response* luego de emitido un *Probe Request* en ciudad

La relación entre la calidad de la señal y el tiempo de respuesta es mostrado en la Fig. 11, donde la curva sugiere cierta estabilidad para todas las respuestas obtenidas con

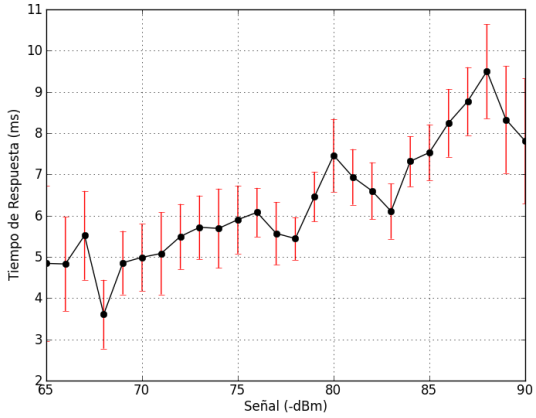


FIG. 11. Tiempo de respuesta en relación a la calidad de la señal

potencias aceptables para la transmisión de datos. De hecho, el 55,92 % de las respuestas con potencias superiores a -80 dBm, donde además se tienen intervalos de confianza, para dicho rango, de entre 0,5 ms y 1,9 ms. Estos resultados sugieren que la gran mayoría de las veces es posible que un usuario móvil pueda conectarse a alguna de estas redes.

IV-D. Fabricantes y tiempos de respuesta

La tabla II resume los tiempos de respuesta de los distintos AP observados durante la campaña de medidas, agrupados por fabricante. Si se comparan los resultados obtenidos en los experimentos de laboratorio presentados en la Fig. 4, se observa que estos tiempos de respuesta son inferiores respecto a aquellos obtenidos durante la campaña de medida, para los mismo fabricantes. Esto puede deberse principalmente a que, en las pruebas en ciudad, el espectro es compartido por varios AP y deben competir por el acceso al medio, provocando retardos mayores en los tiempos de respuesta. Además, a diferencia de las pruebas de laboratorio, en las pruebas en ciudad se presentan interferencias y colisiones.

Por otra parte, en las pruebas en ciudad, los AP del fabricante “Netgear” tienen mejor desempeño que los fabricantes “Cisco-Linksys” y “TP-Link”. Este resultado contrasta con las pruebas en laboratorio, donde el AP “Netgear” obtuvo el desempeño más bajo. Esta diferencia en favor de “Netgear”, podría ser explicada de dos maneras: 1) Una posibilidad es que los modelos de “Netgear” encontrados en las pruebas en ciudad son diferentes al utilizado en las pruebas de laboratorio; específicamente, puede deberse a diferencias de *hardware* o a los algoritmos de *scanning*. 2) Otra explicación se podría basar en los estudios presentados en [4], en donde las diferencias en implementación del estándar 802.11 por los distintos fabricantes, podría provocar que el medio sea compartido de forma injusta, beneficiando algunas interfaces más que otras.

La Fig. 12 muestra la distribución de los AP de acuerdo a los fabricantes, en la figura solo se presentan los fabricantes de los que se encontraron 7 AP o más. Se identificaron un total de 20 fabricantes, lo que vislumbra el nivel de heterogeneidad al que deben enfrentarse las estaciones que interactúan en un despliegue desconocido.

TABLA II
TIEMPOS DE RESPUESTA POR FABRICANTE

Fabricante	Media (ms)	Std (ms)
Netgear	4,07	3,66
Buffalo	4,50	4,71
Cisco-Linksys	5,77	5,84
D-Link	5,88	4,03
Senao Int. Co	6,91	7,09
TP-Link	7,61	5,57
LanPro	8,22	3,99

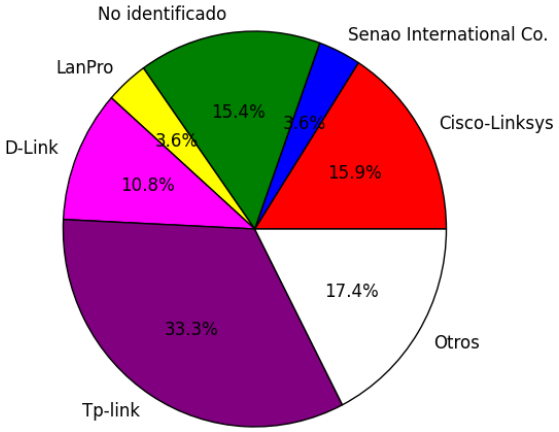


FIG. 12. *Distribución de AP según el fabricante*

V. DISCUSIÓN Y PERSPECTIVAS

En este trabajo se estudió el tiempo de descubrimiento de los AP utilizando datos empíricos. Distintas mediciones se realizaron, sugiriendo que en el casco central de Mérida es posible descubrir el 80 % del los AP disponibles en un canal en 10 ms o menos. Además, otros experimentos realizados indican que los AP utilizables (es decir, con potencia mayor a -80 dBm) responden en 6 ms o menos. Por otro lado, se propusieron y probaron distintas métricas que pueden ser utilizadas para describir las redes 802.11 en una ciudad. En particular, se podrían describir las redes 802.11 en términos de la duración del *scanning* y en consecuencia del *handover*, permitiendo sugerir el nivel de movilidad y el tipo de aplicaciones que pueden ser ejecutadas por un usuario móvil, pues distintas aplicaciones presentan distintos niveles de sensibilidad a interrupciones en la red. Por ejemplo, un usuario altamente móvil requiere cambiar frecuentemente de AP, por lo que topologías con tiempos de *scanning* altos implica que la ejecución del proceso de *handover* provocará interrupciones de red por lapsos significativos, limitando su uso a aplicaciones elásticas. Por otro lado, despliegues con tiempos de *scanning* bajos podrían ser apropiadas para aplicaciones multimedia y de tiempo real.

Los experimentos y resultados obtenidos sientan bases que nos permitirán profundizar el estudio en distintas direcciones que se complementan. Primero, resulta de interés estudiar despliegues espontáneas en redes 802.11 en distintos escenarios, como edificios, instalaciones universitarias y centros comerciales, esto con el fin de determinar formas de aprovechar los despliegues, como por ejemplo, la posibilidad de utilizar las despliegues actuales para formar redes comunitarias, en donde los usuarios móviles podrían aumentar significativamente su movilidad.

También se pretenden evaluar las características y posibles usos de redes comunitarias implementadas utilizando despliegues realizados en forma independientes y espontáneos, tal como los descritos en este trabajo, y compararlas con redes comunitarias implementadas utilizando redes *Mesh*.

REFERENCIAS

[1] **Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications**, IEEE Std. 802.11, 2007.
[2] G. Castignani, L. Loiseau, and N. Montavont, "**An evaluation of IEEE 802.11 community networks deployments**," in Proceedings of 2011 International Conference on Information Networking (ICOIN), Kuala Lumpur, Malaysia, Enero 2011, pp. 498–503.
[3] A. Akella, G. Judd, S. Seshan, and P. Steenkiste, "**Self-management in chaotic wireless deployments**," in Proceedings of the 11th annual international conference on Mobile computing and networking, ser. MobiCom '05, Cologne, Germany, 2005, pp. 185–199.
[4] 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, ser. WiNTECH '06, Los Angeles, USA, 2006, pp. 80–87.
[5] "**Wigle**," http://wigle.net, Consultado en Abril 2012.
[6] "**Wifimap**," http://www.wifimap.com, Consultado en Abril 2012.
[7] "**WEFI**," http://www.wefi.com, Consultado en Abril 2012.
[8] A. Mishra, M. Shin, and W. Arbaugh, "**An empirical analysis of the IEEE 802.11 MAC layer handoff process**," SIGCOMM Computer Communication Review, vol. 33, no. 2, pp. 93–102, Abril 2003.
[9] 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.
[10] G. Castignani, A. Arcia, and N. Montavont, "**A study of the discovery process in 802.11 networks**," SIGMOBILE Mobile Computing and Communications Review, vol. 15, pp. 25–36, Enero 2011.
[11] "**Kernel de Linux**," http://www.kernel.org/pub/linux/kernel/v3.0/linux-3.0.20.tar.bz2, Consultado en Abril 2012.
[12] "**Wireshark**," http://www.wireshark.org, Consultado en Abril 2012.
[13] "**Instituto Nacional de Estadística**," http://www.ine.gob.ve/, Consultado en Enero 2012.