Evaluación del Rendimiento de WiFi Sniffing

JUAN C. AGUILERA C.[1]

[1] *Master's Student in Electronic Engineering, UTFSM*
[*] *juan.aguileraca@sansano.usm.cl*

April 28, 2024

El monitoreo de redes WiFi o *WiFi Sniffing* es el método empleado para rastrear, espiar o monitorear paquetes WiFi. Su implementación se hace a través de un dispositivo capaz de escuchar de forma inalámbrica la red WiFi permitiéndoles detectar y analizar su tráfico, esta clase de dispositivo se conoce como *WiFi Sniffer*. Cuando un dispositivo móvil busca descubrir puntos de acceso WiFi para establecer conexión, usa el modo de exploración activa, emitiendo de forma regular señales de solicitud o *probe request*, las cuales cuentan con la dirección MAC, la fuerza de la señal (RSS), entre otros datos, lo que anuncia la presencia del dispositivo. Esto, junto a las capacidades de los *WiFi sniffers*, ofrece la oportunidad de obtener información sobre las interacciones entre las personas que portan los dispositivos móviles y el entorno. La implementación de esta idea sufre de la falta de una especificación estándar para el despliegue real de los *WiFi Sniffers*. Por esto se presenta un análisis experimental del rendimiento de *WiFi Sniffing* en diferentes entornos inalámbricos utilizando productos disponibles en el mercado. El objetivo de este reporte consiste en recrear los experimentos formulados por el estado del arte, los cuales buscan identificar los posibles factores que afectan el rendimiento del WiFi sniffing. Los resultados recreados concuerdan con el estado del arte en que la mejor estrategia de rastreo consiste en asignar un *WiFi sniffer* a cada uno de los canales no superpuestos lo más cercano al punto de acceso con mejor señal.

1. INTRODUCCIÓN

Con el avance de las tecnologías, en especial en el área de las telecomunicaciones, se ha conseguido una presencia importante de infraestructura WiFi en la gran mayoría de las ciudades y sus espacios urbanos. Esto, junto a las capacidades que tienen los dispositivos móviles actuales para conectarse a la red, ofrece la oportunidad de extraer información relacionada con los usuarios, tales como su ubicación, movimiento y otras actividades, esto mediante el análisis de la conectividad inalámbrica entre estos dispositivos móviles y los puntos de acceso (AP).

Un dispositivo móvil tiene dos formas de explorar la red para encontrar los puntos de acceso cercanos: exploración pasiva y sondeo activo [1]. En el modo pasivo, los puntos de acceso emite señales que promocionan su servicio a los clientes que se encuentran dentro de su rango. Los clientes móviles escuchan pasivamente en cada canal a la espera de una señal periódica de los AP cercanos. Alternativamente, en el modo activo, los dispositivos móviles envían continuamente *probe request* en busca de redes previamente asociadas para su reconexión automática. La exploración activa es preferida a la pasiva, ya que permite explorar los canales de manera más expedita en los dispositivos móviles. Las señales enviadas en modo activo, conocidas como *probe request*, llevan la dirección MAC única del dispositivo móvil en *clear text*. En otras palabras, los dispositivos móviles transmiten constantemente su presencia e identificación cuando buscan una red WiFi disponible dentro de su alcance. Esto ofrece la oportunidad de obtener información de localización relacionada con los usuarios móviles. La obtención de esta información es útil en diversas aplicaciones, como la estimación de la ocupación [2], la monitorización del flujo de tráfico [3] y el análisis de la movilidad de multitudes [4].

Las señales *probe request* no cifradas se pueden capturar colocando dispositivos de escaneo de bajo coste en el entorno, denominados *WiFi Sniffers*. Existen muchos de estos rastreadores WiFi portátiles que utilizan software estándar. Esta capacidad se consigue fácilmente con cualquier dispositivo capaz de activar el modo monitor en su tarjeta de interfaz de red inalámbrica (NIC). Luego, instalando un software de captura de paquetes, es posible capturar todo el tráfico entre puntos de acceso y sus respectivos dispositivo cliente (Figura 1).

En investigaciones anteriores, los *WiFi Sniffers* se han empleado eficazmente para la recolección pasiva de paquetes WiFi. Sin embargo, no existe un estándar establecido para los canales que deben usarse o para escuchar los paquetes en cuanto a detalles de implementación. Los dispositivos envían *probe request* en ráfagas a través de múltiples canales cuando buscan redes cercanas. La frecuencia de estas sondas puede variar en función de factores como el fabricante del dispositivo, el sistema operativo y el estado de la pantalla. Cuando un dispositivo tiene poca batería, puede intentar ahorrar energía reduciendo la frecuencia de las solicitudes de sondeo [5]. Dadas estas limitaciones, un sistema WiFi sniffer debería ser capaz de funcionar a través de múlti-

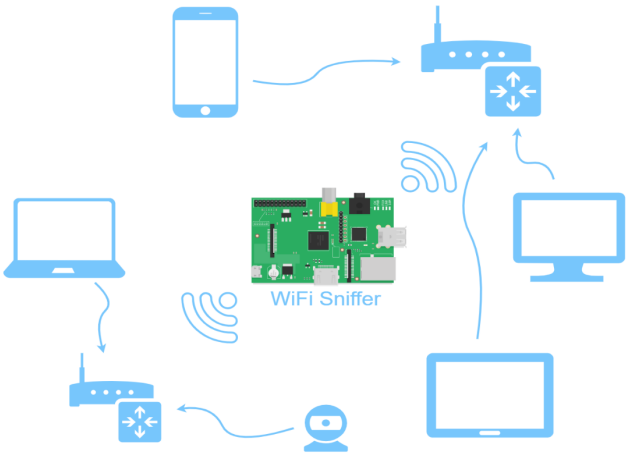

Figura 1. Diagrama de *WiFi Sniffer* capturando paquetes emitidos por todos los dispositivos inalámbricos cercanos.

ples canales para poder recibir un mayor número de tramas simultáneamente.

Normalmente, en el entorno 802.11b/g/n (2.4GHz), se sugiere utilizar un *Wifi Sniffer* de tres canales. Esto implica emplear 3 adaptadores inalámbricos (antenas) en el *Sniffer*, con las antenas configuradas en los canales 1, 6 y 11; sin embargo, esto aumenta el coste y la complejidad de diseño de dichos dispositivos. Por lo que se busca replicar los principios de un esquema de monitorización de canales de este tipo usando un único módulo WiFi, centrándose en lograr un rendimiento óptimo del *sniffer*.

En la literatura se describen dos configuraciones para el rastreo de canales: el salto de canal o *channel hopping*, que implica el cambio rápido entre canales en un intervalo de tiempo determinado, y el seguimiento fijo de un solo canal. Pruebas centradas en el uso de tres canales no solapados demostraron que la monitorización de canal fijo captura más paquetes que el salto de canal [6]. En [7] buscan ampliar esta investigación y explorar qué factores deben tenerse en cuenta para maximizar el rastreo de paquetes en un despliegue real. El trabajo descrito en este reporte busca replicar estos resultados.

Para ello, se realizaron experimentos utilizando distintos esquemas de monitorización de canales. Los resultados preliminares mostraron que **1.** la duración del intervalo de salto de canal marca una diferencia significativa en el número total de paquetes recogidos y en el número de dispositivos detectados cuando el dispositivo de sniffing está saltando por los tres canales no solapados. Aumentar el intervalo de tiempo dedicado a cada canal favorece la detección de más dispositivos; **2.** la supervisión de canales fijos captura más paquetes que los canales de salto en la mayoría de los casos.

Los principales resultados replicados son los siguientes:

1. Se comparó el rendimiento entre 4 estrategias diferentes de salto de canal reportadas en la literatura y el *Wifi Sniffing* de canal fijo. También se ha evaluado el impacto de variar la longitud del intervalo de salto de canal en un mecanismo de salto de frecuencia estándar.

2. Se comparó el rendimiento del *WiFi sniffing* entre un notebook y una OrangePi Zero, en términos de número de paquetes, número de dispositivos capturados y niveles de intensidad de señal recibida (RSS) registrados.

2. ANTECEDENTES Y TRABAJOS RELACIONADOS

Los paquetes WiFi transmitidos entre los dispositivos móviles y los puntos de acceso inalámbricos contienen grandes cantidades de información, lo que ofrece nuevas oportunidades para conocer la ubicación y el comportamiento de movilidad de los usuarios que utilizan la infraestructura WiFi existente.

En las redes de área local inalámbricas (WLAN) convencionales, los dispositivos cliente tienen que descubrir redes para conectarse mediante dos métodos de exploración: pasivo y activo. En la exploración pasiva, los dispositivos cliente recorren varios canales compatibles y escuchan las tramas de datos que transmiten los puntos de acceso para anunciar su presencia. Descubrir la red escaneando todos los canales posibles y escuchando señales de forma pasiva no se considera muy eficiente.

Alternativamente, el escaneo activo es el mecanismo recomendado para mejorar el proceso de descubrimiento y encontrar eficientemente redes inalámbricas cercanas. Los dispositivos cliente mantienen localmente una lista de redes conocidas a las que el dispositivo se ha conectado anteriormente, denominada lista de redes preferidas (PNL). Así, los dispositivos cliente pueden realizar una exploración activa constante para buscar una red conocida a la que conectarse, enviando una *probe request* en cada canal, en lugar de esperar a que la red anuncie su disponibilidad a todos los clientes. El dispositivo cliente sigue enviando *probe requests* automáticamente, independientemente de que haya una conexión en curso con un punto de acceso, para descubrir puntos de acceso nuevos y potencialmente más potentes en sus proximidades y garantizar así la mejor calidad de conexión de red al usuario. De este modo, una estación cliente puede mantener y actualizar una lista de AP conocidos [8].

Existen dos tipos de tramas de *probe request*: sondas directas (*direct probes*) y sondas broadcast (*broadcast probes*). Las sonda directas incluyen un *Service Set Identifier* (SSID) que especifica el AP destino, es decir, solo los AP con un SSID coincidente responderán con una respuesta. Una sonda de broadcast, no se dirige a ninguna red en particular, lo que provoca una respuesta de todos los puntos de acceso en el rango de la señal. Ambos tipos de *probe request* se transmiten sin cifrar y pueden capturarse fácilmente con *WiFi sniffers* baratos. Además, contienen identificadores de dispositivo únicos (direcciones MAC), lo que permite detectar distintos dispositivos y, en última instancia, proporcionar una medida del estado de ocupación y las huellas de movimiento del móvil.

La captura de tramas *probe request* puede lograrse de forma sencilla con cualquier adaptador inalámbrico compatible con IEEE 802.11 configurado en modo monitor mientras escucha en canales WiFi específicos. Cada señal recibida puede dar información típica del dispositivo cliente, como la dirección MAC del dispositivo de origen y el RSS. La dirección MAC de origen es una cadena de 48 bits única en el mundo que identifica el dispositivo, cuyos 3 primeros bytes contienen el identificador único de la organización (OUI) que identifica al fabricante del chip de radio. El RSS mide la potencia media de la señal en el receptor en **dbm** y está relacionado principalmente con la potencia de transmisión y la distancia entre el dispositivo y el receptor.

Recopilar todas las comunicaciones inalámbricas de un dispositivo concreto es difícil por varias razones. En primer lugar, los dispositivos móviles envían los *probe request* por diferentes canales, pero el software de captura de paquetes (por ejemplo, TCPDump o Wireshark) debe configurarse para escuchar en canales específicos. En segundo lugar, algunos paquetes pueden perderse debido a la naturaleza ruidosa del medio inalámbrico.

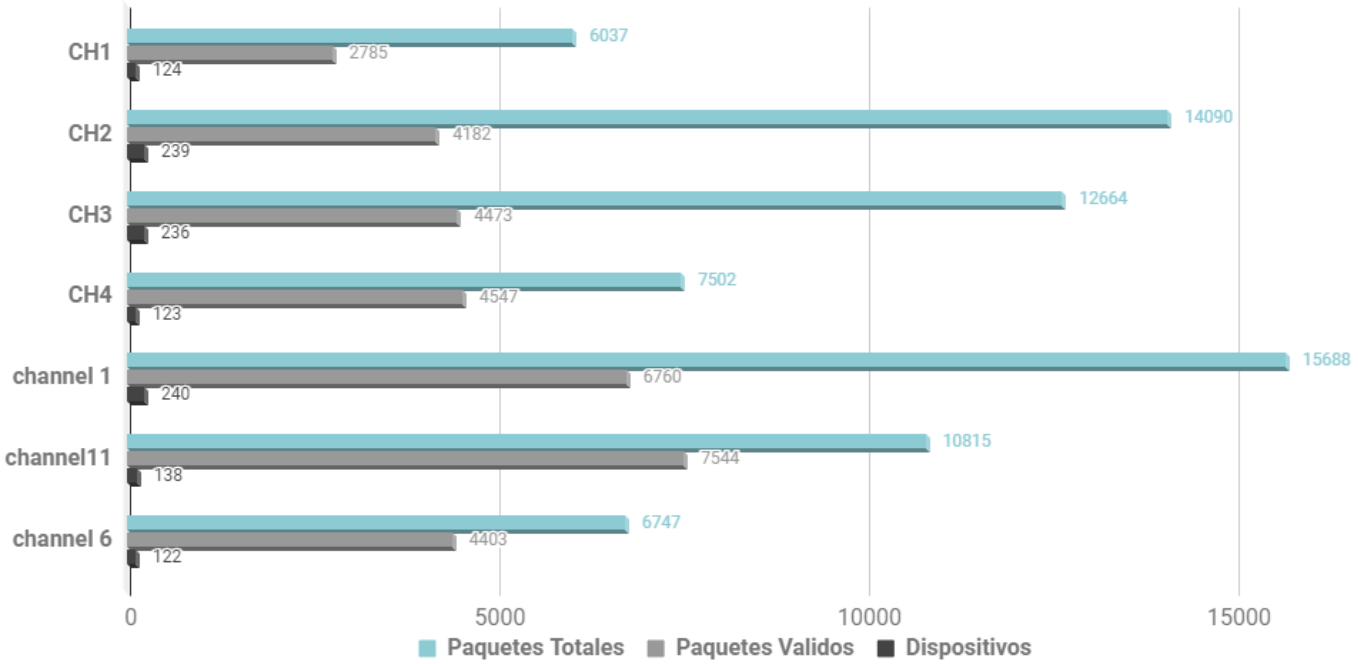

Figura 2. Experimento 1: Número de paquetes totales, Número de paquetes validos (Con OUI única) y Número de dispositivos totales capturados por cada una de las estrategias de monitoreo de canal.

Para cubrir la mayor parte posible del espectro, el *sniffer* puede optar por realizar saltos de canal (*channel hopping*), en los que la tarjeta inalámbrica se configura para escuchar en un canal con un intervalo de tiempo de conmutación designado y luego saltar a otro canal basado en una secuencia de saltos específica. Sin embargo, muchos estudios han demostrado que se capturan más *probe request* cuando no se utiliza el salto de canal [6]. La razón reside en el hecho de que el adaptador inalámbrico solo puede capturar en un único canal en un momento dado. Puede ser conveniente husmear en un único canal de entre los canales no solapados; los canales 1, 6 y 11 son canales no solapados en la banda de 2,4 GHz y los más usados. La elección del canal se supone que no tiene un impacto significativo en las pruebas, pero no parece que se hayan realizado estudios exhaustivos.

Freudiger [6] ha efectuado un estudio experimental exhaustivo sobre cómo influyen los distintos factores en las *probe request*, incluidas las configuraciones de los canales de monitorización, el número de SSID almacenados en la PNL y las configuraciones de los dispositivos. Ha demostrado que tres antenas con cada una ajustada a un canal fijo no solapado recogen el mayor número de sondas. El comportamiento de sondeo está sujeto a los fabricantes de dispositivos, donde el número de sondeos depende linealmente del número de SSID conocidos en general. Un dispositivo con la pantalla desbloqueada muestra más sondas y una señal falsa en las proximidades impulsará una ráfaga creciente de *probe requests*.

YAN LI [7] ha extendido el trabajo de Freudiger para distintos esquemas de salto de canal con monitorización fija de un solo canal. Además, explora otros posibles factores que afectan al número de paquetes *probe request* recibidos en distintos escenarios. Donde revisan distintos factores, como la intensidad de la señal del punto de acceso, la frecuencia de utilización del canal y el número de dispositivos en la zona, y como estos influyen en el número de sondas recibidas. Llegan a la conclusión de que, en un despliegue real, deberían colocarse varios rastreadores en cada subzona, donde el área se ajusta en función de la intensidad de la señal. Para maximizar los *probe request* recogidos, el canal de monitorización óptimo debería ser el asociado al AP más potente de cada subárea, en lugar de elegir entre los tres canales no solapados.

Este trabajo busca replicar la investigación previa propuesta por YAN LI [7], poniendo a prueba alguno de sus experimentos para mostrar resultados en cuanto al rendimiento relativo de distintos esquemas de salto de canal con monitorización fija de un solo canal y la influencia que tiene usar distintos dispositivos de rastreo.

3. MONTAJE EXPERIMENTAL Y RESULTADOS

Para recrear los experimentos en [7], y con el objetivo final de evaluar el rendimiento de las diferentes estrategias de monitoreo de canal con métricas como el número de *probe request* recibidas y la fuerza de la señal recibida, se llevaron a cabo pruebas en espacios dentro de la universidad.

Las pruebas se realizaron en el primer piso de la biblioteca de la Universidad Técnica Federico Santa María.

A. Configuración de la prueba

A.1. Dispositivos y su configuración

Para la mayoría de las pruebas se usó un notebook con tarjeta de red *Intel Wi-Fi AX201* la que ofrece prestaciones dentro de las bandas 2.4 y 5 GHz WiFi. También se utilizó una Orange Pi Zero, la cual cuenta con una tarjeta de red XR819 con capacidades para las bandas de 2.5 y 5 GHz WiFi. Las pruebas en el notebook se realizaron mediante el sistema operativo Manjaro Linux, mientras que en la Orange Pi Zero se utilizó Ubuntu Linux. Para ambos dispositivos, los paquetes a rastrear fueron capturados empleando *TCPDump*, solo los paquetes de *probe*

request fueron guardados al ejecutar las pruebas. Los archivos se guardaron en formato *.pcap* y fueron desplegados mediante *WireShark*. Los datos guardados fueron analizados mediante un script de Python. A pesar de contar con capacidades para los rangos de frecuencia de 2.4 y 5 GHz en ambos dispositivos, solo se consideran los primeros 11 canales en las bandas de 2.4 GHz.

A.2. Consideraciones dirección MAC

En los últimos tiempos las preocupaciones sobre la privacidad han ido al alza, por lo que muchos de los fabricantes de dispositivos móviles implementan la aleatorización de la dirección MAC antes de asociarse a un AP [9]. Para este caso en particular, asumimos que la mayoría de los dispositivos se encontraran conectados previamente a algún AP dentro de la biblioteca en la red de la universidad, lo que revelara su verdadera dirección MAC. Por otro lado, analizando los datos en las pruebas realizadas muestran que de un total de 73.543 paquetes analizados, 47 % de las direcciones MAC contienen OUIs únicos. Para los paquetes con OUIs inválidos se consideran como dispositivos con MAC aleatorizada.

B. Experimento 1: Esquemas de salto de canal

En esta sección se presenta la comparación de resultados al usar distintos esquemas de salto de canal. Para esto se prueban 4 configuraciones de salto de canal que se encuentran en la literatura [10, 11], los cuales corresponden a los siguientes: **1) CH1**: Saltar a través de los canales (802.11b/g/n) de forma secuencial. **2) CH2**: Saltar a través de los 3 canales que no se sobreponen (1, 6 y 11). **3) CH3**: Saltar a través de los canales 1 al 13 al saltar al siguiente canal que no se sobrepone (1,7,13,2,8,3,9,4,10,5,11,6,12). **4) CH4**: Saltar a través de canales específicos (1,6,11,2,7,3,8,4,9,5,10).

Para la monitorización de canales fijos, al igual que las pruebas con los distintos esquemas de saltos de canal, la toma de datos se realizaron a la misma hora en el mismo lugar de la biblioteca en días distintos para asegurar que el tráfico de usuarios con dispositivos móviles fuera consistente. Los datos se tomaron por una hora para cada una de las estrategias de capturas de datos.

Se espera que la mayor cantidad de paquetes sea recibido por las estrategias de canal fijo, seguido por la estrategia de salto en canales no sobrepuestos.

Esto se confirma por los resultados mostrados en la figura 2, donde la mayor cantidad de paquetes se recibió por la estrategia de canal fijo en 1 (*channel 1*), seguido por la estrategia **CH2**. Lo concuerda con los resultados mostrados por el estado del arte.

C. Experimento 2: Impacto del intervalo en salto de canal

En esta sección se presenta la comparación de resultados al emplear dos estrategias de salto de canal con distintos intervalos de salto. Al emplear la estrategia **CH1** con salto de canal cada 0.5 y 1.5 segundos (figura 3) se tiene un mejor desempeño en cuanto al número de paquetes y dispositivos detectados con un intervalo de salto de 0.5 segundos. Para la estrategia **CH2** (figura 4) se observa la misma tendencia. Como los autores de [7] demostraron, el cambio en el tiempo de salto afecta no solo al número de paquetes capturados, sino que al número de dispositivos detectados. Aunque en el experimento realizado por los autores se obtienen resultados contradictorios para el caso de **CH2**, ya que ellos concluyen que para esta estrategia se presenta un mejor rendimiento al aumentar el tiempo entre cada salto de canal entre los canales no superpuestos.

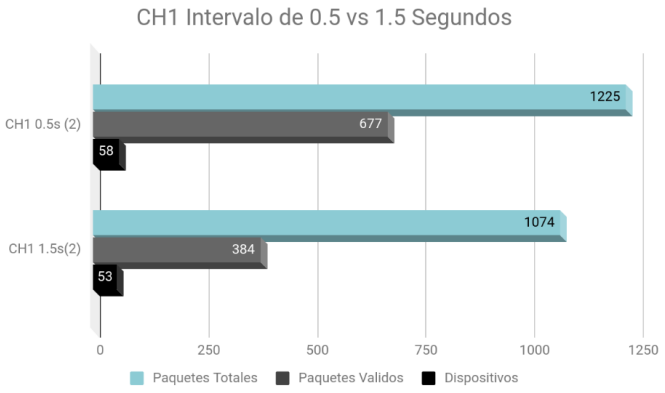

Figura 3. Experimento 2: Comparación de paquetes rastreados usando estrategia CH1 en intervalos de 0.5 y 1.5 segundos.

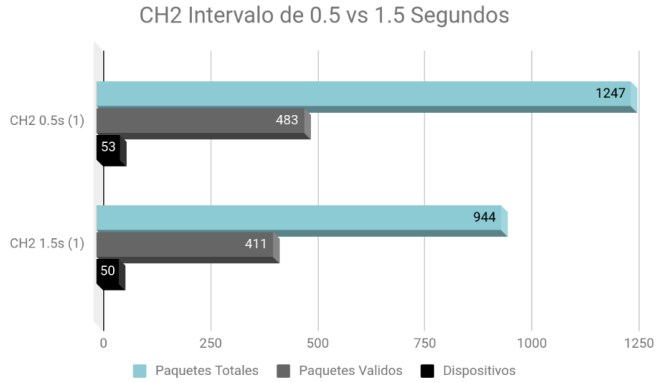

Figura 4. Experimento 2: Comparación de paquetes rastreados usando estrategia CH2 en intervalos de 0.5 y 1.5 segundos.

D. Experimento 3: Comparación de rendimiento entre notebook y Orange Pi Zero

En esta sección se compara el rendimiento entre un notebook y una tarjeta de desarrollo Orange Pi Zero en términos de la cantidad de *probe request* y la fuerza de la señal (RSS) de cada uno de los paquetes capturados.

Ambos dispositivos fueron configurados para rastrear paquetes en el canal 5 (canal por defecto de la Orange Pi Zero que no pudo ser reconfigurado) en un intervalo de salto de 0.5 segundos. Los dispositivos fueron ubicados uno al lado del otro y puestos a rastrear paquetes por una hora al mismo tiempo.

Los resultados muestran que la Orange Pi Zero fue capaz de capturar 5 veces más *probe request* que el notebook (figura 5) y pudo reconocer al doble de dispositivos.

Al analizar la fuerza de la señal de los paquetes capturados por el notebook (figura 6) y por la Orange Pi Zero (figura 7) se puede observar que la Orange Pi Zero es capaz de capturar una gran cantidad de tráfico con fuerza de señal (RSS) cercana a los -80 dbm, mientras que la mayoría del tráfico capturado por el notebook está entre los -60 dbm. Esto muestra que la Orange Pi Zero tiene un área de captura bastante mayor respecto al notebook, lo que le permitió capturar una gran cantidad de *probe request* extras.

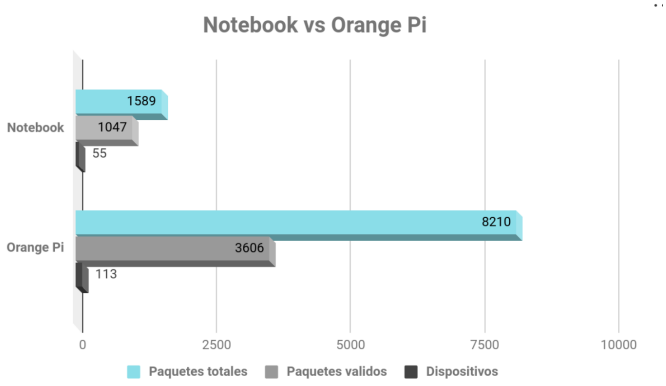

Figura 5. Experimento 3: Cantidad de *probe request* y dispositivos capturados por Notebook y Orange Pi.

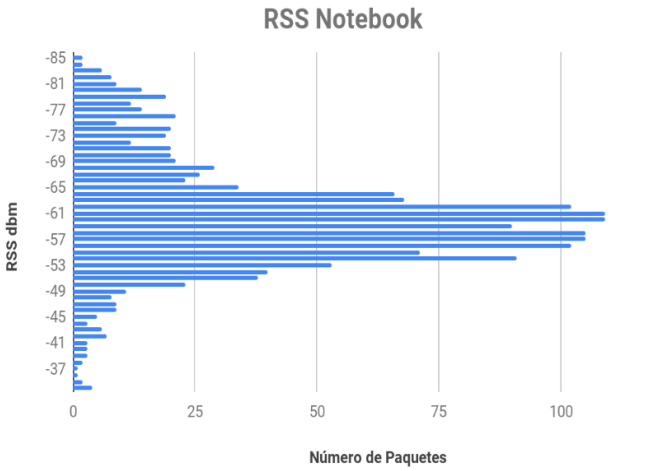

Figura 6. RSS de los paquetes capturados por dispositivo Notebook.

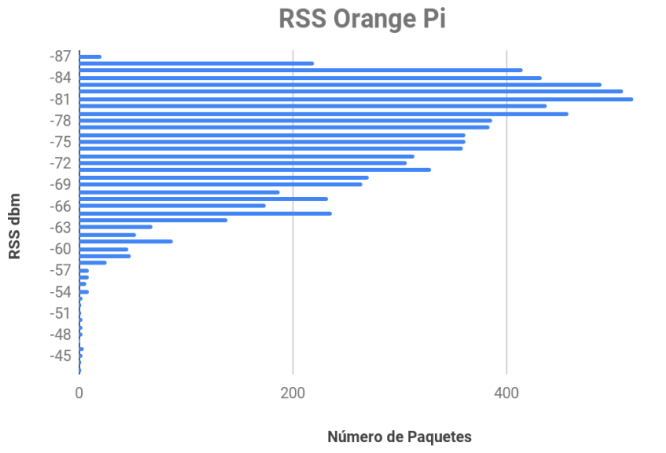

Figura 7. RSS de los paquetes capturados por dispositivo Orange Pi Zero.

4. CONCLUSIONES Y TRABAJO FUTURO

En este trabajo se logró replicar los resultados propuestos por [7] en cuanto a la evaluación del rendimiento de los *WiFi Sniffers* en diferentes configuraciones de canal con distintos dispositivos disponibles en el mercado. Se pudo llegar a resultados similares, lo que nos permite concordar en que la cantidad de paquetes *probe request* capturados se ve afectado por varios factores, como el canal en el que se está rastreando, el intervalo de salto de canal para estrategias de salto de canal así como el dispositivo de rastreo empleado. Finalmente, se recomienda un protocolo de rastreo óptimo para un despliegue real, el cual consiste en asignar un *WiFi Sniffer* lo más cerca posible del punto de acceso en cada subárea y fijar el canal de monitorización para que corresponda al que el AP local más fuerte opera.

En trabajos futuros se espera poder probar las estrategias de salto de canal con dispositivos como la Orange Pi Zero u otros como la Raspberry PI. Quedo por replicar el análisis estadístico en el impacto del uso de distintos canales con estrategias como ANOVA. Uno de los experimentos más importantes que no se pudieron replicar consisten en utilizar 3 *sniffers* configurados en distintos canales fijos, cerca de un AP configurado en un canal de operación fijo, para verificar el impacto que tiene el canal en el que está operando el AP respecto a los paquetes rastreados.

El repositorio con los datasets y scripts empleados para este proyecto se encuentra disponible públicamente en https://github.com/Juanx65/WifiSniffing.

REFERENCIAS

1. G. Bartlett, J. Heidemann, and C. Papadopoulos, “Understanding Passive and Active Service Discovery,” in *Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement,* (Association for Computing Machinery, New York, NY, USA, 2007), IMC ’07, p. 57–70.
2. L. Mikkelsen, R. Buchakchiev, T. Madsen, and H. P. Schwefel, “Public transport occupancy estimation using WLAN probing,” in *2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM),* (2016), pp. 302–308.
3. P. Fuxjaeger, S. Ruehrup, H. Weisgrab, and B. Rainer, “Highway traffic flow measurement by passive monitoring of Wi-Fi signals,” in *2014 International Conference on Connected Vehicles and Expo (ICCVE),* (2014), pp. 396–401.
4. A. Basalamah, “Crowd Mobility Analysis using WiFi Sniffers,” Int. J. Adv. Comput. Sci. Appl. **7** (2016).
5. M. S. Gast, *802.11 Wireless Networks: The Definitive Guide, Second Edition* (O’Reilly Media, Inc., 2005).
6. J. Freudiger, “How talkative is your mobile device?” (2015), pp. 1–6.
7. Y. Li, J. Barthelemy, S. Sun, P. Perez, and B. Moran, “A Case Study of WiFi Sniffing Performance Evaluation,” IEEE Access **8**, 129224–129235 (2020).
8. X. Hu, L. Song, D. Van Bruggen, and A. Striegel, “Is There WiFi Yet? How Aggressive WiFi Probe Requests Deteriorate Energy and Throughput,” (2015).
9. A. E. Redondi and M. Cesana, “Building up knowledge through passive WiFi probes,” Comput. Commun. **117**, 1–12 (2018).
10. K. Friess, “Multichannel-Sniffing-System for Real-World Analysing of Wi-Fi-Packets,” in *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN),* (2018), pp. 358–364.
11. B. Baker, F. Thornton, R. Rogers, C. Hurley, and D. Connelly, *Wardriving and Wireless Penetration Testing*First, first ed.