ESTUDIO Y RECOMENDACIONES PARA DIAGNOSTICAR LOS PROBLEMAS DEBIDO A LAS INTERFERENCIAS INALÁMBRICAS WLAN/RLAN EN LOS RADARES METEOROLÓGICOS ARGENTINOS

Tesis de Maestría, como requisito para la obtención del grado académico de MAGISTER EN SISTEMAS DE RADAR E INSTRUMENTACIÓN, presentada ante la Universidad Nacional de Córdoba

Autor: Gabriel Walter Ezequiel GIOVANARDI

Dirección de tesis:

Director: Dr. Juan Pablo PASCUAL

Co-director: Mg. Ing. Jorge COGO

Jurado de tesis:

Mg. Ing. AMADO José Luis

Dr. VENERE Alejandro Javier

Dr. ZERBINI Carlos Alberto

Fecha de la defensa oral y pública:

24 de Febrero de 2023

Resumen

Con la finalidad de hacer un uso eficiente del espectro, se ha dispuesto que los dispositivos WLAN/RLAN compatibles con los estándares 802.11a/n/ac y los radares meteorológicos de banda C compartan el rango de frecuencias de operación. Como consecuencia de dicha decisión, los radares son interferidos por señales WLAN/RLAN aún cuando existen mecanismos previstos para evitarlo y como resultado se enmascaran las reflexiones útiles asociadas a los fenómenos climatológicos.

Frente a esta problemática, en el presente trabajo se desarrolla un procedimiento de medición para detectar y localizar los dispositivos WLAN/RLAN que causan interferencias y degradan el desempeño de los radares argentinos que componen el Sistema Nacional de Radares Meteorológicos (SINARAME). El procedimiento se limita a la detección de tramas inalámbricas propagadas por señales que operan según el estándar IEEE 802.11a/n/ac. La detección permite caracterizar, a nivel ingeniería de protocolo, las señales WLAN/RLAN que se registran en los datos de radar meteorológico.

En primer lugar, se analizan las características de las señales WLAN/RLAN especificadas en las cláusulas IEEE 802.11a, IEEE 802.11n e IEEE 802.11ac. Sobre dicho análisis se diseña un procedimiento de medición de campo, que involucra tanto la determinación de una serie de programas (software) necesarios para llevar a cabo el proceso, como la definición de los requerimientos sobre los dispositivos (hardware) que deben integrarse con los programas, es decir antenas, receptores, sistemas de adquisición. El procedimiento se aplica a una campaña de mediciones experimentales donde se registran las fuentes de interferencia in-situ con el fin de localizar su origen.

Como primer insumo de la actividad de localización, se analizan registros de radar meteorológico, específicamente el producto conocido como reflectividad, donde se identifican los efectos de la interferencia y se determinan aquellas direcciones acimutales críticas en cartografía digital, a modo de orientación para la búsqueda de las fuentes inalámbricas interferentes. La información recolectada durante el trabajo de campo se obtiene mediante una técnica dinámica que integra datos de señal del GPS en tiempo real, adquisiciones que dan cuenta de la actividad de las transmisiones de las señales en el espectro y la captura de tramas inalámbricas 802.11. Como resultado del proceso de medición se describen las características más relevantes y la geolocalización de las fuentes de interferencias.

Por último, se desarrolla un ensayo de laboratorio que consiste en montar transceptores

de los mismos proveedores de los sistemas WLAN/RLAN detectados y en establecer una comunicación entre ellos, realizando las mediciones de forma análoga a lo desarrollado en campo, de modo tal de corroborar el funcionamiento de los dispositivos en un ambiente controlado y completar la información extraída acerca de cómo impactan sus configuraciones en la utilización e invasión del espectro electromagnético.

Agradecimientos

En primer lugar, quiero agradecer a Juan Pablo y Jorge por la compañía y el apoyo en el desarrollo de esta tesis, que lograron que acceda a una forma de trabajo única y flexible en la integración de las distintas partes que conforman a este proyecto, a pesar de la distancia y las circunstancias. Muchas Gracias a ambos.

Asímismo los datos RMA-1 fueron obtenidos por gentileza del Grupo Radar Córdoba y la Secretaría de Infraestructura y Política Hídrica, Ministerio de Obras Públicas del Gobierno Nacional Argentino enmarcados dentro del Proyecto SINARAME. Sinceramente agradecido con el equipo.

Un agradecimiento especial al Sr. Marcelo Tobal, por la compañía y soporte en las campañas de mediciones realizadas.

Al Centro Regional Universitario Córdoba IUA de la Universidad de la Defensa Nacional por brindarme la posibilidad de continuar con mi formación académica accediendo, a través de una beca completa, a la Maestría en Sistemas de Radar e Instrumentación.

También quiero agradecer a Rocío, mi novia y compañera de la vida, por su apoyo incondicional e interés en compartir las alegrías y angustias. TE AMO.

Finalmente agradecer a mi familia, por su apoyo en todas las etapas de mi vida. Este logro es también de ellos.

Índice de Contenidos

Lista de Figuras

Lista de abreviaturas

ADC: *Analog-Digital Converter* - Conversor analógico-digital.

AP: *Access Point* - Punto de acceso.

BSS: *Basic Service Set* - Área de servicio.

CABFRA: *Cuadro de Atribución de Bandas de Frecuencias de la República Argentina.*

CCA: *Clear Channel Assessment* - Evaluación de canal claro.

DFS: *Dynamic Frequency Selection* - Selección dinámica de frecuencia.

DS: *Distribution System* - Sistema de distribución.

ENACOM: *Ente Nacional de Comunicaciones.*

FCS: *Frame Check Sequence* - Secuencia de comprobación de trama.

HT: *High Throughput* - Alto rendimiento.

IEEE: *Institute of Electrical and Electronics Engineers* - Instituto de Ingenieros Eléctricos Electrónicos.

ITU: *International Telecommunication Union* - Unión Internacional de Telecomunicaciones.

LNA: *Low Noise Amplifier* - Amplificador de bajo ruido.

MAC: *Meduim Access Control* - Control de acceso al medio.

MIMO: *Multiple-In Multiple-Out* - Múltiple entrada Múltiple salida.

OFDM: *Orthogonal Frquency Division Multiplexing* - Multiplexación por división de frecuencias ortogonales.

OSI: *Open System Interconection* - Interconexión de sistemas abiertos.

PLCP: *Physical Layer Convergence Procedure* - Procedimiento de convergencia de la capa física.

PMD: *Physical Medium Dependent* - Dependiente del medio físico.

PPI: *Plan Position Indicator* - Indicador de posición en el plano.

PRF: *Pulse Repetition Frequency* - Frecuencia de repetición de pulsos.

PRI: *Pulse Repetition Interval* - Intervalo de repetición de pulsos.

RLAN: *Radio Local Area Network* - Red radioeléctrica de área local.

RMA: *Radar Meteorológico Argentino.*

RSN: *Robust Security Network* - Red con seguridad robusta.

SINARAME: *Sistema Nacional de Radares Meteorológicos.*

SSID: *Service Set Identifier* - Nombre de red.

TBTT: *Target Beacon Transmision Time* - Tiempo de transmisión de baliza objetivo.

TDMA: *Time Division Multiple Access* - Acceso múltiple por división de tiempo.

TU: *Time Unit* - Unidad de tiempo.

UNII: *Unlicensed National Information Infrastructure* - Infraestructura de información nacional no licenciada.

VHT: *Very High Throughput* - Muy alto rendimiento.

WDS: *Wireless Distribution System* - Sistema de distribución inalámbrico.

WLAN: *Wireless Local Area Network* - Red inalámbrica de área local.

Capítulo 1

Introducción

1.1 Contextualización del problema y motivación

Los dispositivos WLAN/RLAN (*Wireless/Radio Local Area Network*, Red de Área Local Inalámbrica/Radioeléctrica) que funcionan en la banda de frecuencias de 5 GHz utilizan OFDM (*Orthogonal Frequency Division Multiplexing*, Multiplexación por División de Frecuencias Ortogonales) y sus transmisiones pueden interferir en las señales de un radar meteorológico que trabaja en el mismo rango de frecuencias (banda C). Esto implica que, al compartir el espectro radioeléctrico, las señales WLAN/RLAN recibidas por el radar enmascaran las reflexiones útiles asociadas a los fenómenos meteorológicos y alteran los productos radar. Actualmente, varios tipos de dispositivos inalámbricos utilizan canales de transmisión en el rango de frecuencias de 5,180 a 5,825 GHz. Mientras, que los radares meteorológicos de tipo Doppler de doble polarización funcionan en la banda de frecuencias de 5,450 a 5,820 GHz.

En el año 2013, la Unión Internacional de Telecomunicaciones (ITU) asignó las bandas de 5,150 a 5,350 GHz y de 5,470 a 5,725 GHz a sistemas de acceso inalámbrico, incluyendo las redes WLAN/RLAN (Barba Leal *et al.*, 2021). Se esperaba que los dos grupos de usuarios coexistieran en el mismo entorno, requiriendo que las redes WLAN/RLAN empleen un sistema DFS (*Dynamic Frequency Selection*, Selección Dinámica de Frecuencia). Sin embargo, a 10 años de la asignación por parte de la ITU, la interferencia debida a redes WLAN/RLAN en radares meteorológicos de banda C continúa siendo un problema a nivel mundial y se encuentra entre los factores limitantes de su desempeño.

Los dispositivos WLAN/RLAN cumplen y funcionan bajo el estándar 802.11 (IEEE Standard 802.11, 2016). De acuerdo a la versión del estándar 802.11 (a, n ó ac), el ancho de banda de los canales varía entre 20, 40, 80 y 160 MHz. En la Figura 1.1 se muestra el espectro y la numeración de canales para cada una de las versiones de 802.11 que operan en

la banda de frecuencias de 5 GHz. Se excluye el espectro de 2,4 GHz ya que no es de interés para este trabajo. También se detallan los canales que incluyen DFS y la porción de la banda que es compartida con los radares meteorológicos.

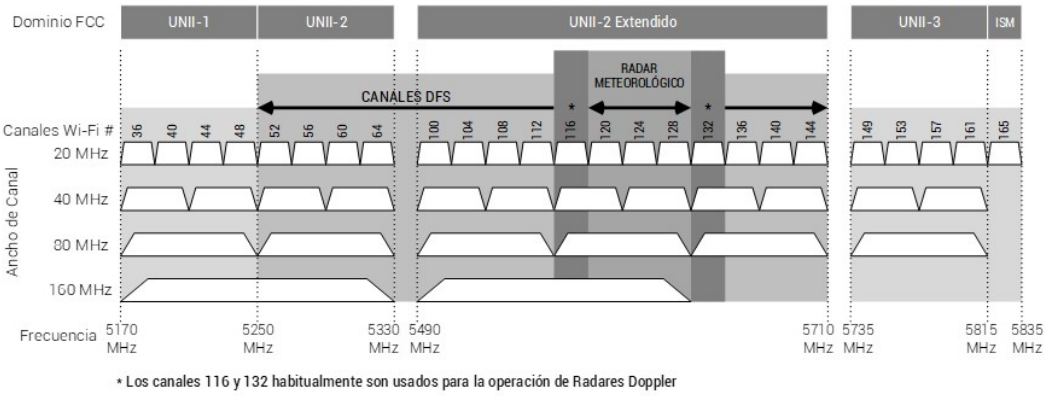


Figura 1.1: Espectro y asignación de canales 802.11.

El radar meteorológico, por su parte, emite un pulso electromagnético y, luego de un período de tiempo igual a dos veces el tiempo de propagación desde el radar al volumen de meteoros, recibe los ecos procedentes de éstos. Una señal radar está compuesta por múltiples ecos provenientes de una gran cantidad de meteoros (lluvia, ceniza, polvo, granizo, insectos, etc.). Los radares argentinos de la serie RMA (*Radar Meteorológico Avanzado*) son de tipo Doppler, de doble polarización simultánea, y operan en la banda C. En el caso del radar RMA-1 de la Figura 1.2 emplazado en la ciudad de Córdoba, opera en la frecuencia de 5,625 GHz (canal 125) con un ancho de banda en el receptor de 50 MHz (ocupando los canales 120, 124 y 128 de la banda de frecuencias según la normativa).

Figura 1.2: Imagen del RMA-1 ubicado en la ciudad de Córdoba.

La información recibida en el radar, puede interpretarse para obtener diferentes productos de utilidad en meteorología, como es el caso de la reflectividad Z de un meteoro que se estima a partir de la potencia de la señal recibida e indica su tamaño y concentración. En la Figura

1.3 se observa un gráfico de indicador de posición en el plano, o PPI (acrónimo de *Plan Position Indicator*) de la reflectividad medida en polarización Horizontal por el RMA-1, bajo condiciones climáticas de *aire claro* (sin presencia observable de fenómenos meteorológicos). Esto se corresponde a un barrido o vuelta completa en acimut del radar, con una elevación de $0,5°$. Las regiones en tonos de gris o celeste (valores bajos de reflectividad) se corresponden al ruido que contamina a la señal observada. Además, en la región de hasta 120 km se observan zonas en tonos rojos y verdes (valores altos y medios de reflectividad) que se atribuyen a *clutter*[1] terrestre debido a las sierras cordobesas. Finalmente, en diferentes ángulos de acimut se observan líneas radiales en tonos azules, verdes y amarillos (valores medios de reflectividad), que se condicen con el efecto esperado debido a la interferencia de redes inalámbricas.

La reflectividad es un dato fundamental para establecer la hoja de ruta en este trabajo, ya que los haces de alta intensidad en dirección radial que se observan en la Figura 1.3 son de utilidad para localizar en acimut las fuentes de interferencia. Las señales WLAN/RLAN aparecen generalmente en el radar con mayor amplitud que los ecos típicos asociados a los fenónemos atmosféricos, provocando que la información meteorológica quede enmascarada.

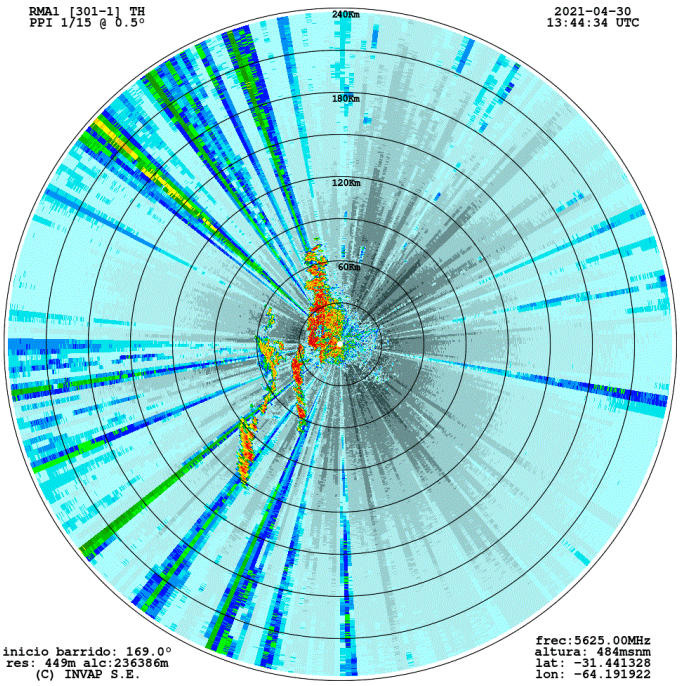


Figura 1.3: PPI de reflectividad para la polarización Horizontal, observado por el RMA-1 en condiciones de aire-claro.

Para que los dispositivos WLAN/RLAN convivan en la misma banda que los sistemas de radar y evitar las interferencias, los equipos de transmisión inalámbrica que operen en esta banda deben implementar un protocolo de Selección Dinámica de Frecuencia (DFS). Este protocolo define un mecanismo por medio del cual, cuando un equipo de comunicaciones detecta una señal de radar en la frecuencia que está operando, debe cambiar de canal de

[1]Señal interferente que se produce por la reflexión de la emisión del radar sobre la superficie que rodea al blanco.

operación por un determinado tiempo.

La convivencia de radares y redes inalámbricas en la misma banda de frecuencias no debería presentar inconvenientes, pero lo cierto es que a partir del despliegue de sistemas y dispositivos WLAN/RLAN modernos equipados con antenas de última generación, han aparecido serias interferencias en los radares. Las mismas se ocasionan, principalmente, debido a fallas en el mecanismo DFS o porque, incluso, no todos los dispositivos cumplen con la implementación del mismo. Este problema no ha sido resuelto completamente, ya que no es posible controlar el despliegue de dispositivos WLAN/RLAN fuera de norma.

El objetivo principal de este trabajo consiste en medir y caracterizar las señales de redes inalámbricas WLAN/RLAN que causan interferencias y degradan el desempeño de los productos de los radares meteorológicos que forman parte de la red SINARAME. Para ello, se estudian los estándares que definen estas señales y se diseña un procedimiento de medición de campo, que luego se aplica para registrar las fuentes de interferencia *in-situ* y localizar su origen. Con el fin de caracterizar las señales interferentes, es necesario explorar la subcapa física (*PHY sublayer*) y las funciones de gestión 802.11 de manera que se logre identificar e inspeccionar el formato de cada una de las tramas en el proceso de descubrimiento y que ocurren en la comunicación de los clientes con los dispositivos AP (*Access Point*, Punto de Acceso).

1.2 Antecedentes

El SINARAME consiste en una red de radares meterológicos y un sistema de centralización de la información en tiempo real, el cual es operado por el Servicio Meteorológico Nacional (SMN) (Rodríguez *et al.*, 2017). Los RMA (*Radar Meteorológico Argentino*) que integran dicha red, son radares Doppler de polarización dual que operan en la banda C, diseñados y puestos en funcionamiento por la Empresa INVAP SE[2].

La etapa de procesamiento de señales de un radar meteorológico se encarga de *estimar* las variables meteorológicas empleadas por los pronosticadores para caracterizar los fenómenos atmosféricos, es decir, los momentos espectrales (Doviak y Zrnić, 1993) y las variables polarimétricas (Ryzhkov y Zrnic, 2019). Esta estimación resulta afectada por diferentes tipos de interferencias que contaminan y enmascaran los ecos provenientes de los fenómenos atmosféricos que se desea observar. Por un lado, el radar recibe reflexiones de la propia onda transmitida, conocidas como *clutter*, que se producen sobre el suelo (*clutter terrestre*) (Doviak y Zrnić, 1993), sobre pájaros o insectos (*clutter biológico*) (Lakshmanan *et al.*, 2010), o sobre turbinas de molinos eólicos (*clutter eólico*) (Nai *et al.*, 2013). Por otro lado, el radar recibe interferencia electromagnética producida por otros sistemas de comunicaciones. Una de ellas es la interferencia WLAN/RLAN descrita en la Sección 1.1.

A partir de esta problemática, en muchos países se han planteado diversas alternativas de

[2]Extraído de la web oficial https://www.invap.com.ar/areas/defensa-seguridad-y-ambiente/radar-meteorologico-banda-c/ el día 22 de junio de 2022.

solución. En Sudáfrica por ejemplo, luego de fracasar en el intento de localizar y sancionar a los usuarios de redes WLAN/RLAN que transmiten señales interferentes, las autoridades decidieron migrar la red de radares meteorológicos de la banda C al rango de frecuencias de 2,7 a 2,9 GHz (Saltikoff *et al.*, 2016).

Vaccarono *et al.* (2019) analizan cómo este tipo de interferencia afecta a los radares que operan en banda C, así como la magnificación de este inconveniente en los últimos años, situándose en la región noroeste de Italia. Asimismo, Carroll *et al.* (2010) reportan los resultados de estudios de intereferencia en un radar de la red TDWR (por sus siglas en inglés de *Terminal Doppler Weather Radar*). El ensayo es bastante exhaustivo, ya que se analizan las señales interferentes presentes en las diferentes etapas de la cadena de recepción del radar. Los autores también analizan las fallas de los mecanismos DFS que pueden haber causado que los transmisores no hayan detectado la presencia del radar.

En el ámbito nacional existen trabajos recientes que abordan el problema y la mitigación de interferencia WLAN/RLAN en radares meteorológicos con soluciones desde el punto de vista del procesamiento estadístico de señales, (Petracca y Lugo, 2017); (Barba Leal *et al.*, 2021); (González y Iglesias, 2001). Petracca y Lugo (2017) y González y Iglesias (2001) proponen técnicas de filtrado basadas en la transformada wavelet y en otras variantes de filtros discretos. Por su parte, Barba Leal *et al.* (2021) propone un esquema de detección del preámbulo de la señal Wi-Fi a la salida del filtro adaptado del radar. El mismo se basa en un test de hipótesis sobre el criterio de Neyman-Pearson (Richards, 2014) y explota la estructura determinística que posee el preámbulo (IEEE Standard 802.11, 2016).

Para intentar mitigar las interferencias se han utilizado distintos enfoques, aunque ninguno ha resultado ser del todo eficiente. Algunas estrategias apuntan a identificar la fuente, con el objetivo de denunciarla ante la autoridad competente y que se ordene el cese de la transmisión. Esta es una solución poco viable cuando se trata de zonas muy urbanizadas donde hay un uso intensivo de las tecnologías WLAN/RLAN (Barba Leal *et al.*, 2021).

En otros casos, aprovechando que las señales interferentes aparecen en el radar con una forma característica, se han propuesto técnicas de procesamiento de imágenes para identificarlas y eliminarlas. Si un acimut se identifica como contaminado puede ser removido y luego se interpola la señal meteorológica a partir de las direcciones acimutales adyacentes. Este método presenta deficiencias, sobre todo cuando el número de emisores perjudiciales aumenta, debido a que la señal útil se pierde por completo en la zona removida y se tienen pocas zonas desafectadas para usar en la interpolación (Saltikoff *et al.*, 2016).

Este problema a nivel mundial y, también nacional, aún no ha sido resuelto completamente, ya que no es posible controlar el despliegue de transmisores WLAN/RLAN en zonas cercanas al radar. Por lo tanto, lo que se pretende con este trabajo es presentar una alternativa para identificar, localizar y documentar las interferencias para posteriormente entregar información certera a SINARAME y que le permita ejecutar las acciones correspondientes ante el organismo regulador.

1.3 Objetivos

Objetivo General

El objetivo general de este trabajo consiste en caracterizar las interferencias debido a los transmisores WLAN/RLAN que degradan el desempeño de los radares meteorológicos de la red SINARAME.

Objetivos Específicos

- Estudiar la señal interferente desde las normas que la definen para determinar sus características de interés para este problema: niveles de potencia, duración de las transmisiones, polarización utilizada, etc.
- Realizar mediciones de campo que permitan registrar la señal interferente in-situ y localizar su origen.
- Vincular los registros de interferencia observada con su efecto sobre los productos del radar meteorológico, tales como: factores de reflectividad, velocidad media, reflectividad diferencial, coeficiente de correlación cruzada, fase diferencial, etc.
- Analizar soluciones para nuestro país desde la legislación vigente.

1.4 Publicaciones asociadas a la tesis

Parte del trabajo abordado en esta tesis dió lugar a una publicación en ARGENCON, congreso bienal de la rama Argentina del IEEE. El mismo fue presentado durante el evento desarrollado entre los días 7 y 9 de septiembre de 2022 en la ciudad de San Juan, Argentina y forma parte de sus actas, disponible en: E. Giovanardi, J. Cogo and J. Pablo Pascual, "Medición de Señales WLAN/RLAN que Interfieren a los Radares Meteorológicos Argentinos", 2022 IEEE Biennial Congress of Argentina (ARGENCON), 2022, pp. 1-7, doi: 10.1109/ARGENCON55245.2022.9939940.

1.5 Organización de la tesis

En el Capítulo 2 se analiza el estado actual del radar RMA-1 y sus características técnicas más relevantes. Se realiza un análisis exploratorio-descriptivo de las características de la señal inalámbrica en sus versiones 802.11 a, n y ac basado en las especificaciones del estándar. Por otro lado, se describe la relación de la norma con el modelo OSI. Posteriormente se desglosa por capas la cabecera del paquete 802.11 y se sintetizan las tramas de interés. También, se describen los dispositivos y sus protocolos de funcionamiento que mayormente interfieren al radar. Por último, se presentan soluciones para el país desde la legislación vigente.

Luego, en el Capítulo 3 se presenta una breve descripción de los recursos de hardware, aplicaciones de software e instrumental utilizados, junto a sus funcionalidades, y rol en el proceso de medición. Se mencionan las alternativas consideradas y se destacan las seleccionadas de acuerdo a los requisitos del software. Se describe la configuración del hardware compatible con el fin de habilitar modos de funcionamiento ocultos bajo plataforma Linux.

En el Capítulo 4 se describe el procedimiento llevado a cabo para realizar las mediciones, desde su preparación hasta su concreción. Se presentan los resultados obtenidos del análisis y filtrado de paquetes inalámbricos, estudio de la actividad de los transmisores en el espectro radioeléctrico, análisis del perfil topográfico y trazado en mapa con seguimiento GPS, relación de las fuentes interferentes con la legislación vigente y la práctica de ingeniería inversa para demostrar cómo funcionan los equipos de comunicaciones que mayormente interfieren al radar.

Finalmente, en el Capítulo 5 se presentan conclusiones y se plantean pasos a seguir como trabajo futuro.

Capítulo 2

Marco Teórico

2.1 Radar Meteorológico Argentino RMA

Un radar es un sistema de detección de objetos que utiliza ondas electromagnéticas para determinar su posición, velocidad y algunas de sus características. El término **RADAR** fue introducido en el año 1940 por la US Navy y es un acrónimo de **RA**dio **D**etection **A**nd **R**anging. En español podría traducirse como detección y medición de distancia a través de ondas de radio (Doviak y Zrnić, 1993).

Durante la Segunda Guerra Mundial se dieron varios avances importantes en la evolución del radar. Este sistema se desarrolló motivado por necesidades militares y en la actualidad posiblemente siga siendo su aplicación dominante: vigilancia, navegación y guiado de bombas o misiles para vehículos por tierra, agua y aire. Sin embargo, hoy tiene un amplio rango de aplicaciones civiles. Para control del tráfico aéreo, control de velocidad en las rutas, aerotransportados para medir características topológicas y ambientales de la tierra, meteorológicos, entre otros.

Un radar mide la distribución espacial de reflectividad en las dimensiones del sistema de coordenadas esféricas: *rango*, *ángulo acimutal* y *ángulo de elevación*. Existen diferentes maneras de llevar a cabo dicha medición. En caso de operar de manera mecánica en acimut y elevación, una posibilidad es que el radar realice un giro de 360° en acimut a velocidad constante con una elevación dada, transmitiendo pulsos de manera regular y "escuchando" las reflexiones producidas por los mismos a diferentes distancias. Una vez concluido el giro, modifica el ángulo de elevación de la antena y repite el proceso.

Los radares pulsados convencionales son sistemas activos que operan transmitiendo energía en forma de ondas electromagnéticas y recibiendo las señales reflejadas por la región y los objetos de interés iluminados (Skolnik *et al.*, 2001). De acuerdo al tipo de aplicación, se

emplean técnicas de procesamiento de señales para extraer información del objetivo (o blanco). La función básica del procesamiento consiste en la detección de la presencia de contribuciones de uno o más objetivos en la señal recibida. Una vez detectados, se puede estimar: la distancia al objetivo, que es proporcional al retardo de tiempo en que la señal recibida cruzó el umbral de detección con respecto al instante en que el pulso fue transmitido, el ángulo relativo a la dirección de apuntamiento de la antena; y la velocidad radial, midiendo el desplazamiento en función del tiempo (Skolnik *et al.*, 2001).

El principio de funcionamiento de los radares meteorológicos es análogo a lo descrito, sólo que los blancos en esta ocasión son fenómenos atmosféricos que reflejan la energía radiada, en general asociada a hidrometeoros.

Si bien los primeros desarrollos de radar pulsado aplicado a observaciones meteorológicas surgieron en la década de 1950, desde el punto de vista de radares operativos existen dos saltos tecnológicos muy importantes. El primero es el *Radar Meteorológico Doppler*, que permite obtener los momentos espectrales de la señal recibida en la dimensión de tiempo lento (Richards, 2014). El segundo hito tecnológico lo conformó el *Radar Meteorológico Polarimétrico*, que además de las capacidades Doppler incorpora la posibilidad de transmitir y recibir las ondas electromagnéticas con más de una polarización. Dado que el estado de polarización de las ondas recibidas es sensible a la forma física y a las propiedades dieléctricas de los hidrometeoros, se puede identificar el tipo de fenómeno meteorológico y mejorar la estimación de la tasa de precipitación.

En Argentina, en el año 2011 se implementó el SINARAME, con el objetivo principal de contar con una red de radares meteorológicos utilizando un sistema de centralización de la información en tiempo real, el cual es operado por el Servicio Meteorológico Nacional (SMN). En este contexto, la empresa INVAP S.E. fue la responsable de la fabricación y puesta en funcionamiento de 12 radares polarimétricos, de banda C, distribuidos a lo largo del país para la Subsecretaría de Recursos Hídricos de la Nación en el marco del programa Sistema Nacional de Radares Meteorológicos (Rodríguez *et al.*, 2017). Se prevé para un futuro extender la red a un total de 30 radares con estas características, capaces de proveer una cobertura completa del territorio nacional.

Los Radares de la serie RMA trabajan en banda C con tecnología Doppler, de doble polarización simultánea, giratorios (máximo de 6 vueltas por minuto) instalados en el interior de un radomo de protección (con forma esférica) formado por secciones hexagonales fabricados en plástico tricapa. La banda C trabaja entre 4 y 8 GHz y es una de las más confiables para operar en condiciones meteorológicas severas, como lluvias y granizo.

En la Figura 2.1 se esquematiza la secuencia de pulsos sin modulación transmitida por un radar pulsado. El radar transmite un pulso de duración τ, del orden de los μs. Luego, espera un tiempo de guarda t_g, seguido del cual abre lo que se conoce como la ventana de recepción, t_w. Durante el intervalo t_w el radar escucha los ecos correspondientes al pulso transmitido. Una vez transcurrido t_w el radar envía un nuevo pulso y se repite el procedimiento. El intervalo de tiempo entre pulsos T, que es del orden de los milisegundos, se conoce como Intervalo

de Repetición de Pulsos ó PRI (acrónimo de *Pulse Repetition Interval*), y su inversa es la Frecuencia de Repetición de Pulsos ó PRF (acrónimo de *Pulse Repetition Frequency*). Esto es lo que se denomina muestreo de tiempo lento. Por otro lado, por cada pulso periódico que se emite, el radar muestrea la señal recibida a una frecuencia de muestreo F_s, la cual es superior a la PRF, y cuya inversa es el período de muestreo $T_s = 1/F_s$. Por ejemplo, la frecuencia de muestreo en esta dimensión, $F_s = 1/T_s$, suele tomar valores del orden de los 100 kHz a los 10 MHz, que es considerablemente grande en relación a otras escalas de muestreo que se presentan en radar, motivo por el cual a la dimensión en rango también se la denomina dimensión *tiempo rápido* (Richards, 2014).

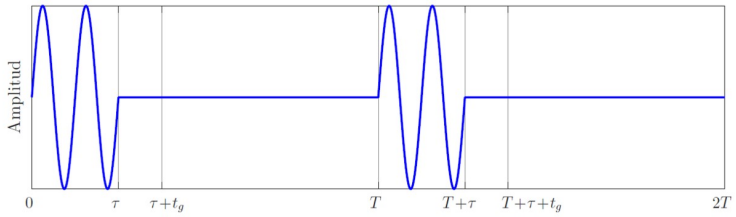


Figura 2.1: Pulso sin modulación transmitidos por un radar pulsado.

Las muestras de la señal recibida por el radar pueden organizarse en una matriz de datos $Y(m, n)$ como se muestra en la Figura 2.2. Las columnas representan los diferentes pulsos emitidos por el radar a su PRF y las filas representan las muestras tomadas a F_s por cada uno de los pulsos emitidos.

Al momento de procesar los datos es de utilidad definir una forma de almacenarlos. Se puede pensar que las muestras adquiridas para un pulso se ordenan en un vector columna, donde el primer elemento corresponde a la distancia R_0. Los elementos de este vector tienen una correspondencia con las distancias en las que se producen las reflexiones, por eso definirá una dimensión en rango.

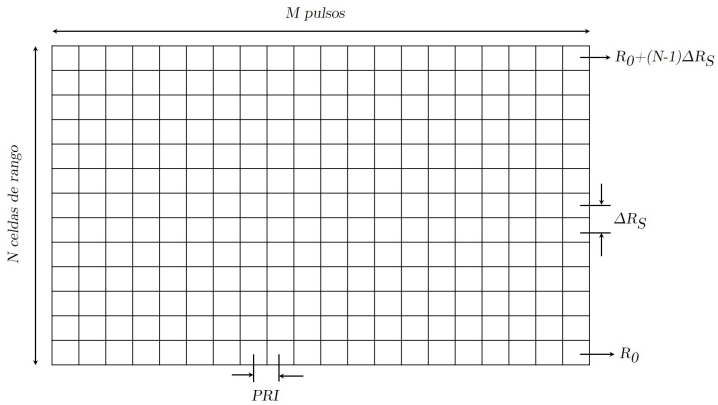


Figura 2.2: Matriz de datos del radar Doppler.

2.1.1 Dimensiones de Muestreo

El radar transmite un pulso y luego del intervalo de tiempo de guarda escucha los ecos que se producen, debido a los objetivos presentes y su entorno en la región iluminada. Para ello, pasado t_g muestra la señal recibida cada T_s durante la ventana de recepción.

Considerando que el retardo de tiempo correspondiente a la primera muestra adquirida es t_0, en ese tiempo la onda se propagó una distancia total de $2R_0$ a la velocidad de la luz, c, es decir que $R_0 = ct_0/2$.

Del mismo modo, si t_1 es el retardo correspondiente a la segunda muestra adquirida, luego la distancia asociada al punto donde se produjo la reflexión es $R_1 = ct_1/2$. Teniendo en cuenta que $t_1 = t_0 + T_s$ entonces,

$$R_1 = \frac{ct_0}{2} + \frac{cT_s}{2} = R_0 + \Delta R_s. \tag{2.1}$$

donde $\Delta R_s = cT_s/2$ es lo que se conoce como la separación entre celdas de rango.

Del análisis anterior se concluye que muestrear la señal recibida cada T_s implica que se contará con muestras separadas una distancia ΔR_s. Sin embargo, no debe confundirse esta separación con la resolución de rango, es decir $\Delta R_s = cT_s/2$ no es necesariamente igual a $\Delta R = c\tau/2$.

El procesamiento de señales correspondiente a la detección de objetivos, en general, se lleva a cabo sobre esta dimensión.

Al transmitir el siguiente pulso de la secuencia, el proceso de adquisión se repite y se cuenta con un nuevo vector, donde cada elemento está asociado a la misma distancia que las del primer vector. Con los sucesivos vectores asociados a cada pulso transmitido, es posible construir una matriz como la que se presenta en la Figura 2.2. Cada elemento de una columna corresponde a la dimensión en rango, donde cada muestra está separada T_s en tiempo o ΔR_s en distancia. Cada elemento de una fila corresponde a una muestra tomada por los distintos pulsos a una misma distancia. Las muestras en esta dimensión se encuentran separadas por el PRI y se conoce como dimensión de pulsos.

La PRF=1/PRI, toma valores en el orden de los 100 Hz a los 100 kHz, por lo que a esta dimensión también se la denomina dimensión *tiempo lento* en contraposición con la dimensión tiempo rápido. El procesamiento Doppler, que permite determinar la velocidad de un objetivo, se lleva a cabo en esta dimensión porque implica variaciones lentas que se dificultan observar en la escala de tiempo de la dimensión tiempo rápido.

En la Figura 2.3, se muestra un diagrama en bloques de la arquitectura básica de un radar Doppler. Los radares Doppler deben contar con un receptor coherente, capaz de determinar la amplitud y fase de las señales recibidas. Por otro lado, también deben ser capaces de controlar o determinar la fase del pulso transmitido. El transmisor del radar RMA está basado en un magnetrón, el cual no permite controlar la fase del pulso mencionado anteriormente, por lo que se utiliza un esquema de pseudo-coherencia. En este tipo de sistemas se debe medir la fase del pulso transmitido por el magnetrón respecto a la del oscilador local de gran estabilidad,

comúnmente denominado STALO. Luego, se utilizará el mismo como referencia para el receptor (Petracca y Lugo, 2017).

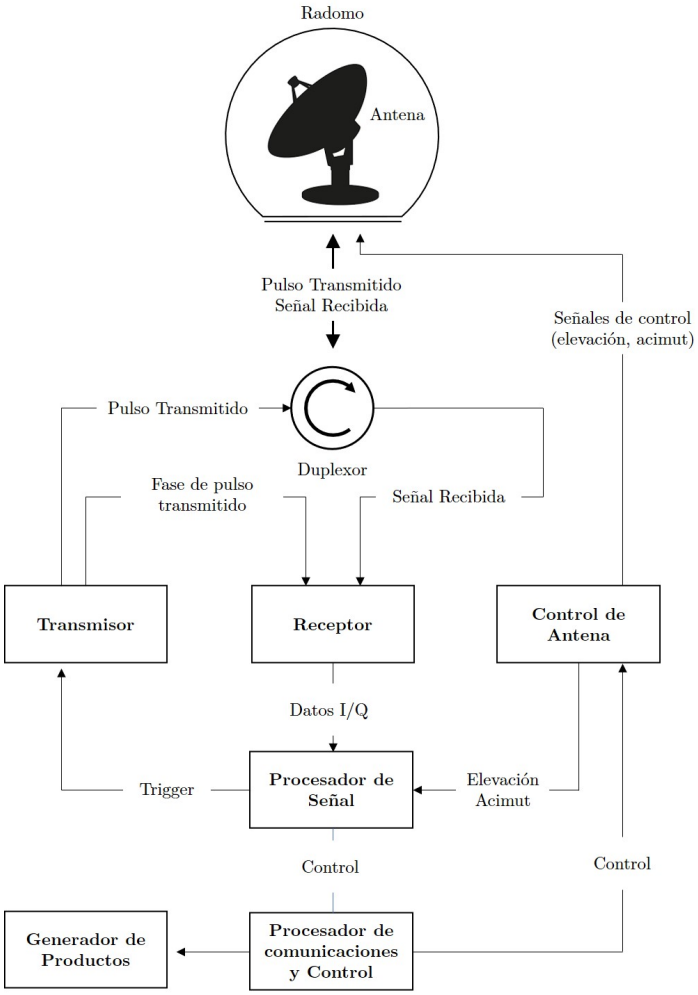


Figura 2.3: Arquitectura básica de un radar Doppler.

En el proceso de transmisión y recepción del radar, la señal de RF es generada en el oscilador local estable STALO y alimenta tanto al excitador como a la etapa de recepción. La señal es modulada antes de ingresar en el transmisor, donde será amplificada y luego de pasar por el Duplexor ingresa a la antena para ser transmitida al espacio libre. Las ondas electromagnéticas que sean reflejadas en un meteoro, ingresan a la antena. Luego de pasar por el Duplexor son amplificadas por un amplificador de bajo ruido LNA (acrónimo de *Low Noise Amplifier*). La señal recibida después de ser amplificada se filtra e ingresa en la etapa de recepción, que comúnmente involucra una o más etapas de mezclado en frecuencia para llevarla a frecuencia intermedia. El mezclado en frecuencia se realiza con la señal de referencia proveniente del STALO. Los receptores coherentes dividen la señal en su componente en fase **I** (*In-phase*) y su componente en cuadratura **Q** (*Quadrature*), por lo que la potencia a partir de la señal recibida estará dada por,

$$P = \frac{I^2 + Q^2}{Z_L} \tag{2.2}$$

donde Z_L es la impedancia de la línea. Por último, las señales en fase y cuadratura son digitalizadas por conversores analógico-digitales ADC (acrónimo de *Analog-Digital Converter*) para su posterior procesamiento en el dominio digital.

El diagrama mostrado en la Figura 2.3 corresponde a un radar Doppler de polarización simple, mientras que el RMA es un radar de doble polarización simultánea. Sin embargo, los elementos básicos que componen el sistema son compartidos por ambos tipos de radar. Un radar polarimétrico proporciona información adicional para poder reconocer y clasificar diferentes tipos de precipitaciones como ser lluvia, granizo, nieve, como así también mejorar las estimaciones de precipitación (Bringi y Chandrasekar, 2004). El radar RMA transmite y recibe la señal en polarización vertical y horizontal de manera simultánea y luego procesa en paralelo las señales recibidas en ambas polarizaciones.

2.1.2 Niveles de Datos

En el radar Doppler, la señal recibida y convertida a banda base o frecuencia intermedia cuenta con dos componentes, en fase (I) y en cuadratura (Q), como se ha descrito en la sección anterior. Esta señal en banda base es muestreada en tiempo rápido a una frecuencia F_S para obtener una matriz de muestras complejas $Y(m, n)$ de tamaño $M \times N$ (número de pulsos x número de muestras de rango) como se detalla a continuación,

$$Y(m, n) = I(m, n) + jQ(m, n) \tag{2.3}$$

donde j es la unidad imaginaria.

Si el radar es polarimétrico, se tendrá una matriz de datos para el canal horizontal y una matriz de datos para el canal vertical,

$$Y_H(m, n) = I_H(m, n) + jQ_H(m, n). \tag{2.4}$$

$$Y_V(m, n) = I_V(m, n) + jQ_V(m, n). \tag{2.5}$$

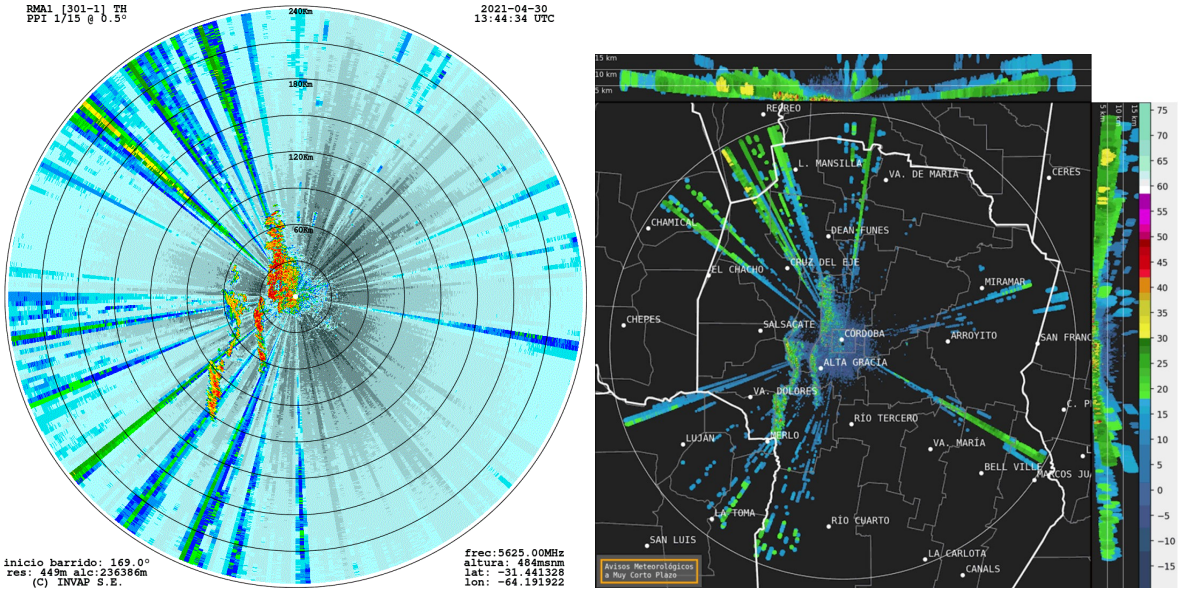
A estos datos se los conoce como de ***Nivel 1*** o datos crudos, ya que aún no han sido procesados para extraerles la información meteorológica.

Luego los datos de Nivel 1 se procesan en una unidad de procesamiento para obtener diferentes productos radar, los cuales tienen significado físico y serán útiles para las aplicaciones meteorológicas. A estos se los denomina datos de ***Nivel 2***.

2.1.3 Productos de Radar

En la Figura 2.4 se muestra el producto de nivel 2 obtenido a partir de los datos crudos con interferencias. Las dos imágenes corresponden a mapas PPI y permiten deducir

cualitativamente, por medio de la reflectividad (dBZ) (a), la concentración de agua precipitable en el medio. Para el caso de la Figura (b) se provee la reflectividad máxima (dBZ) para cada latitud/longitud y altitud, dada una serie de planos verticales equiespaciados en latitud/longitud. Debido a la altura de las Sierras Cordobesas y su cercanía al radar RMA-1, los barridos o PPI más bajos son bloqueados parcial y, en algunos casos, totalmente por la presencia de clutter terrestre. Esto lleva a que, para monitorear la atmósfera detrás de las sierras, deban utilizarse mayores ángulos de elevación de la antena del radar para evitar la obstrucción de la señal. Por esta razón se utiliza el ángulo de elevación de $0,5°$.



(a) PPI de Reflectividad (dBZ) (b) COLMAX (dBZ)

Figura 2.4: Versiones de Mapas de visualización del Producto de Reflectividad (dBZ) en polarización horizontal (H) del RMA-1 en un día despejado.

La reflectividad (Z) es un parámetro de utilidad en meteorología y, esencialmente, es una medida de la potencia recibida producto de las reflexiones de la onda transmitida por el radar en los fenómenos atmosféricos. Las zonas con tormentas severas, por ejemplo, se asocian usualmente a valores altos de reflectividad. En el caso del PPI de Reflectividad (dBZ) de la figura anterior, aparecen resaltadas en color rojo las regiones donde se refleja mucha potencia que, no precisamente es debida a hidrometeoros, sino a reflexiones indeseables en el terreno, específicamente en las sierras de Córdoba.

Un dispositivo WLAN/RLAN que esté ubicado relativamente cerca del radar puede comenzar a transmitir en cualquier instante y mantenerse transmitiendo durante todo el intervalo que dura la ventana de recepción. Los paquetes inalámbricos transmitidos serán detectados por el receptor en cuadratura del radar porque ambos equipos operan en la misma banda de frecuencias. Al hacer el cálculo de la reflectividad, el radar considerará que estuvo recibiendo potencia durante la ventana de recepción. Esto hace que en el acimut donde se recibe la interferencia WLAN/RLAN todas las celdas de rango aparezcan contaminadas, dando lugar

a los haces finos de alta intensidad que se observan en los dos mapas de la Figura 2.4.

2.1.4 Especificaciones Técnicas de los RMA

En este trabajo se utilizan datos del radar RMA-1, el cual dispone de ciertas características que se detallan en la Tabla 2.1 (Rodríguez *et al.*, 2017).

Subsistema	**Características**
Tipo	Radar Meteorológico en banda C, Doble Polarización, Doppler
Frecuencia de operación	5.450 - 5.820 MHz
Ancho de pulso	0,4 a 3 μs
Resolución	60 m celda @ 0,4 μs
PRF	300 a 2.000 Hz
Rango máximo	480 Km
Rango operacional	240 Km
Filtro de clutter	> 23 dB
Productos	DBZH a TH Factor de reflectividad horizontal VRAD Velocidad radial, WRAD Ancho espectral ZDR Reflectividad diferencial PHIDP Desplazamiento de fase diferencial KDP Fase diferencial específica RHOHV Coeficiente de cross-correlación Mapa de clutter
Transmisor	Magnetrón coaxial, modulador de estado sólido, potencia de pico de 350 kWatts
Receptor	Superheterodino, conversión dual, rango dinámico de 93 dB, -110 dBm @ pulsos 3 μs y 3 dB figura de ruido
Dimensiones de antena	4,45 m de diámetro, 182 Kg, reflector Opti-mat/carbono + Cobre Níquel
Ganancia de antena	1° de ancho a 3 dB, 45 dB ganancia mínima @ 5635 MHz
Mecanismo de movimiento	Rango de elevación de -1° a 90°, velocidad de escaneo máxima de 6 rpm. de funciones PPI y RHI, control manual
Radomo	Paneles sándwich geotalc, máxima velocidad de viento 240 Km/h

Tabla 2.1: Especificaciones técnicas de la serie de radares RMA.

2.2 Estándar IEEE 802.11

La utilización de medios de comunicación inalámbricos se encuentra en continua expansión. El medio de comunicación en la transmisión inalámbrica es el de la propagación de ondas electromagnéticas que son transmitidas y recibidas utilizando equipos de transmisión y recepción provistos de antenas.

En términos de las redes de datos inalámbricos, el estándar más aceptado es el que se conoce como IEEE 802.11. Se trata de un estándar descriptivo de redes tipo LAN (acrónimo de *Local Area Networks*) inalámbricas, también conocidas como WLAN/RLAN. En los últimos tiempos, se impuso la denominación de tecnología Wi-Fi a la denominación tradicional del protocolo IEEE 802.11. En realidad, Wi-Fi es un proceso de certificación de equipos que ofrecen niveles de compatibilidad de manufacturación con el propio estándar. La Alianza Wi-Fi (*Wi-Fi Alliance* en inglés) define tipos de productos de red de área local inalámbrica,

basados en el estándar IEEE 802.11. Sólo aquellos productos que completan las pruebas de certificación de interoperatibilidad exigidas por la Alianza Wi-Fi pueden etiquetarse como *Wi-Fi CERTIFIED*. En general, el término Wi-Fi se utiliza como sinónimo de WLAN/RLAN y esta denominación se respeta en esta tesis.

Cualquier dispositivo que pueda usar certificado Wi-Fi, ya sea una computadora portátil, teléfono inteligente, TV inteligente, consola de videojuegos, router AP o enlaces de microondas, puede conectarse y/o ofrecer recursos de red. Un AP puede tener un área de cobertura de varias decenas de metros puertas adentro de alguna edificación (cobertura *indoor*), aunque fuera de edificios, sin obstáculos importantes, puede llegar a mayor distancia (cobertura *outdoor*).

IEEE 802 se refiere a una familia de normas del IEEE (acrónimo de *Institute of Electrical and Electronics Engineers*) que se ocupan de las redes de área local y metropolitana. Está mantenida por el Comité de Estándares 802 LAN/MAN (LMSC, *LAN/MAN Standard Committee*). IEEE 802.11 es un conjunto de especificaciones de control de acceso al medio (MAC, *Medium Access Control*) y de la capa física (PHY, *Physical Layer*) para implementar comunicaciones en las Redes de Área Local Inalámbricas (WLAN). En la Figura 2.5 se muestra la familia de normas 802.11 y el empleo de técnicas de modulación utilizando el aire como medio de transmisión y que comparten el mismo protocolo básico. Estos estándares proporcionan la base de los productos de red inalámbrica que utilizan la marca Wi-Fi. En cuanto al uso de las frecuencias de operación utilizado por 802.11, la regulación del espectro radioeléctrico varía según los países.

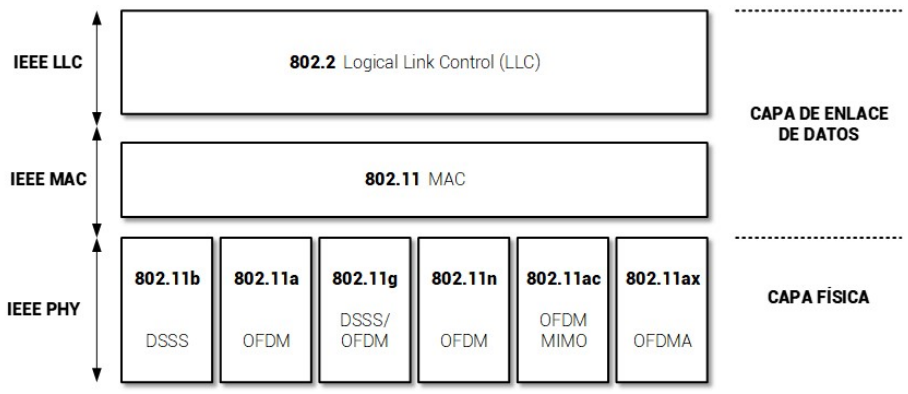


Figura 2.5: Implementaciones del estándar IEEE 802.11.

2.2.1 Versiones del estándar

A continuación, se presentan todas las versiones del estándar correspondientes a la banda de frecuencia de 5 GHz. Se excluyen las versiones del estándar 802.11 que operan en el rango de frecuencias de 2,4 GHz ya que no son de interés para este trabajo.

IEEE 802.11a

Fue la corrección a las especificaciones de la norma original IEEE 802.11-1997 o Modo Heredado (*Legacy Mode* en inglés) que definió los requerimientos para el sistema de

comunicación, capa física con OFDM de 52 subportadoras. Inicialmente fue diseñada para soportar comunicaciones inalámbricas en el rango de frecuencias sin licencia de 5 GHz.

Originalmente descrita como cláusula 17 de la especificación de 1999, ahora se define en la cláusula 18 de 2012 y proporciona protocolos que definen tasas de transmisión de 6 a 54 Mbps.

IEEE 802.11a utiliza el mismo protocolo de enlace de datos y el mismo formato de trama que el 802.11 original, opera en la banda de 5 GHz con una tasa de transferencia máxima de 54 Mbps que realmente se reduce a un rendimiento máximo de unos 20 Mbps. Inicialmente ofrecía 12 canales de frecuencia no solapados, 8 usados en interior y 4 para conexiones punto a punto en exterior. De las 52 subportadoras OFDM, 48 son para datos y 4 portadoras piloto. Las sub-portadoras poseen una separación de 312,5 kHz entre ellas y pueden ser moduladas digitalmente con BPSK, QPSK, 16QAM o 64QAM. Las ventajas de 802.11a son:

- la banda de 5 GHz no está tan usada o llena como la banda de 2,4 GHz por parte de los dispositivos WLAN Wi-Fi;
- ausencia de interferencias de la banda de 2,4 GHz (como hornos microondas, teléfonos inalámbricos, sistemas bluetooth, cámaras de vigilancia inalámbricas, etc.);
- las frecuencias más altas permiten la construcción de antenas más pequeñas con una mayor ganancia del sistema;
- OFDM tiene ventajas de propagación en entornos de trayectos múltiples (reflexiones o rebotes en obstáculos).

Como principal desventaja, tiene un radio de cobertura significativamente menor, ya que las señales son fácilmente absorbidas por muros u otros objetos sólidos.

Los productos con 802.11a empezaron a comercializarse tarde, ya que eran más difíciles de fabricar y muchos países habían abierto parcialmente la banda de 5 GHz, imponiendo serias restricciones al convivir con sistemas radar.

IEEE 802.11n

Durante los siguientes años, se publicaron otras correcciones a los estándares anteriores para finalmente crear un documento (802.11-2007) en el año 2007.

IEEE 802.11n fue aprobada y publicada en el año 2009. Es una corrección del documento 802.11-2007 que mejora los estándares anteriores. En la capa física (PHY) se han añadido técnicas avanzadas de procesamiento de señales y modulación para explotar canales más amplios y usar diversas antenas. Las extensiones del protocolo que funcionan en la capa de enlace de datos (MAC) hacen un uso más eficiente del ancho de banda disponible. En conjunto, estas mejoras de alto rendimiento (HT, *High Throughput* según siglas en inglés) pueden aumentar la velocidad de transmisión de datos hasta 600 Mbps, un poco más que diez veces respecto a los 54 Mbps de 802.11a/g.

IEEE 802.11n funciona tanto en la banda de 2,4 GHz como en la de 5 GHz, siendo esta última una banda opcional en cuanto a compatibilidad. Este estándar se basa en los anteriores

añadiendo a la capa física tecnología MiMo (*Multiple-input Multiple-output*, Múltiple-entrada Múltiple-salida) y canales de 40 MHz. Esto genera la capacidad de transmitir y/o recibir a través de varias antenas, por lo que el estándar define configuraciones de sistemas irradiantes "$M \times N$", que va desde 1×1 hasta 4×4. MiMo utiliza múltiples antenas para ajustar de forma coherente más información de la que es posible utilizando una sola antena. Una forma de conseguirlo es mediante la Multiplexación por División Espacial, que multiplexa espacialmente diversos flujos de datos independientes transmitidos simultáneamente en el ancho de banda designado.

El número de flujos de datos simultáneos está limitado por el número de antenas en uso en ambos lados del enlace. Sin embargo, los equipos de radio suelen limitar aún más el flujo de datos espaciales que pueden transportar datos. La notación $M \times N = Z$ ayuda a identificar la capacidad de un equipo de radio, siendo M el número máximo de antenas de transmisión que se pueden utilizar, N es el número máximo de antenas de recepción, y Z es el valor máximo de flujos de datos espaciales. Por ejemplo, un equipo de radio que puede transmitir en dos antenas y recibir en tres, pero sólo puede enviar o recibir dos flujos de datos sería la configuración $2 \times 3 = 2$.

Otra característica opcional de 802.11n es el ancho de sus canales. Los productos 802.11n pueden utilizar 20 o 40 MHz de ancho, siempre que el AP lo permita. Esto significa que los canales de 40 MHz proporcionan el doble de velocidad de datos en la capa PHY.

IEEE 802.11ac

IEEE 802.11ac (también conocido como estándar VHT, *Very High Throughput*, Muy Alto Rendimiento, según siglas en inglés) utiliza las características de 802.11n (y 802.11a) en la medida de lo posible, para garantizar la compatibilidad entre versiones y la coexistencia.

Las especificaciones 802.11ac proponen un rendimiento multi-estación WLAN de al menos 1 Gbps, y en un solo enlace una velocidad de 500 Mbps. Esto se consigue ampliando el concepto de interfaz de aire trabajado por el estándar 802.11n:

- mayor ancho de banda de canal de RF ($80 + 80$ MHz y 160 MHz);
- mayor cantidad de flujos de datos espaciales MiMo (hasta 8);
- MiMo multiusuario (MU-MIMo);
- intervalo de guarda corto de 40 ns;
- modulación de alta densidad (hasta 256QAM);
- codificación por bloques espacio-temporales (STBC);
- comprobación de paridad de baja densidad (LDPC).

Los dispositivos 802.11ac que utilizan únicamente los parámetros obligatorios (80 MHz de ancho de banda, 1 flujo espacial y 64QAM 5/6) podrán alcanzar una velocidad de datos de

aproximadamante 293 Mbps. Los dispositivos que utilizan los parámetros opcionales (8 flujos de datos, 160 MHz de ancho de banda y 256QAM 5/6 con un intervalo de guarda corto) podrán alcanzar una velocidad de casi 7 Gbps.

2.2.2 Relación con el modelo OSI

La norma 802.11 abarca el funcionamiento y los protocolos de las redes inalámbricas. Sólo se ocupa de las dos capas más bajas del modelo de referencia OSI (*Open System Interconnection*, Interconexión de Sistemas Abiertos), la capa física y la capa de enlace de datos (o capa de control de acceso al medio) como lo indica la Figura 2.5. El objetivo es que toda la serie de estándares 802.11 sean compatibles con las versiones anteriores y que utilicen la misma capa de control de acceso al medio (MAC) o enlace de datos. Por lo tanto, cada uno de los estándares 802.11 sólo difiere en las características de la capa física (PHY).

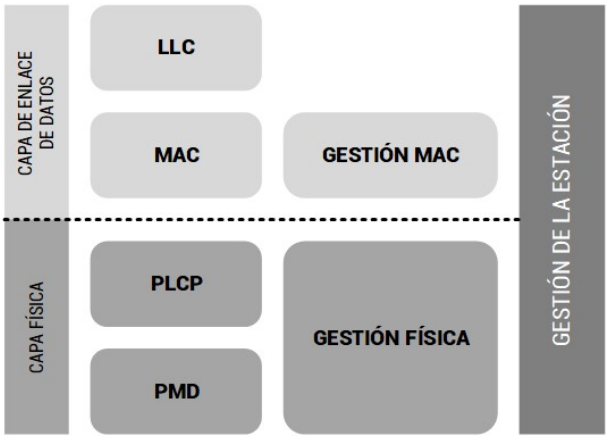


Figura 2.6: Estrutura del estándar 802.11 y su relación con el modelo OSI.

La capa MAC proporciona los medios funcionales y procedimientos para transferir datos entre entidades de red, para detectar y, posiblemente, corregir los errores que pueden producirse en la capa física. También proporciona acceso al tráfico libre con y sin contenciones que ocurren en las diferentes capas físicas. En la capa MAC las responsabilidades se dividen en la subcapa MAC (propiamente dicha) y la subcapa de gestión MAC. En la primera se definen los mecanismos de acceso y los formatos de los paquetes, y la segunda se encarga de la gestión de la energía, la seguridad y los servicios de itinerancia.

La capa física define las especificaciones eléctricas y físicas de los dispositivos. En particular, define la relación entre un equipo de comunicación y el medio de transmisión, que en este caso es la interfaz de aire. Las principales funciones y servicios que realiza esta capa se listan a continuación:

- establecimiento y terminación de una conexión a un medio de comunicación;
- participación en el proceso de comunicación de los dispositivos y en los recursos que se comparten efectivamente entre los usuarios;

- modulación o conversión en la representación de los datos digitales en el equipo del usuario y las correspondientes señales transmitidas por un canal de comunicaciones;

De acuerdo a la Figura 2.6, la capa física se divide en tres subcapas:

1. el PLCP (*Physical Layer Convergence Procedure*, Procedimiento de Convergencia de la Capa Física) actúa como una capa de adaptación y es el responsable del modo CCA (*Clear Channel Assessment*, Evaluación de Canal Claro) y de la construcción de paquetes para diferentes tecnologías de la capa física;

2. la PMD (*Physical Medium Dependent*, Dependiente del Medio Físico) especifica técnicas de modulación y codificación;

3. la subcapa de Gestión Física (*Management PHY*) se encarga de las cuestiones de gestión, como la sintonización del canal.

La subcapa de Gestión de la Estación (*Station Management*) es responsable de la coordinación de las interacciones entre las capas MAC y PHY.

2.2.3 Asignación de canales y Máscara Espectral

Los estándares 802.11a, 802.11n y 802.11ac utilizan el espectro regulado de 5,150 - 5,850 GHz que se subdivide en varios canales cada uno con una frecuencia central y ancho de banda.

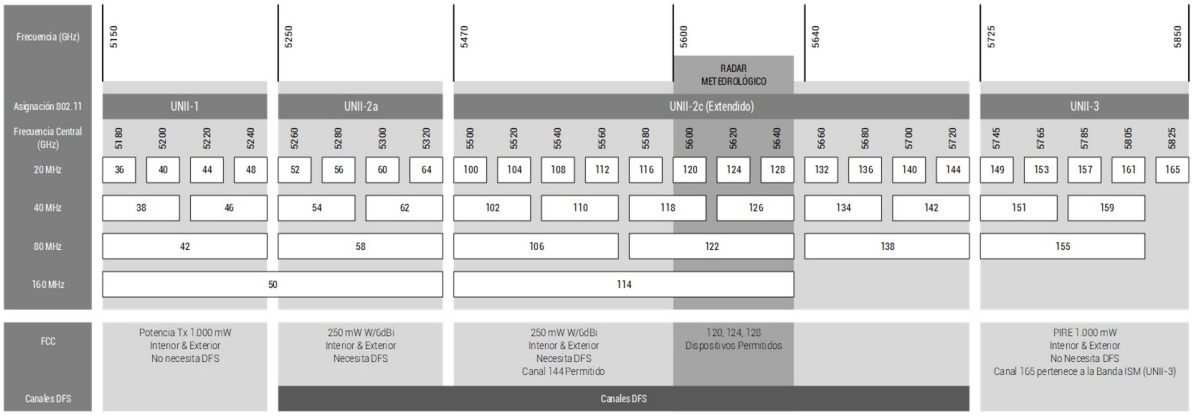
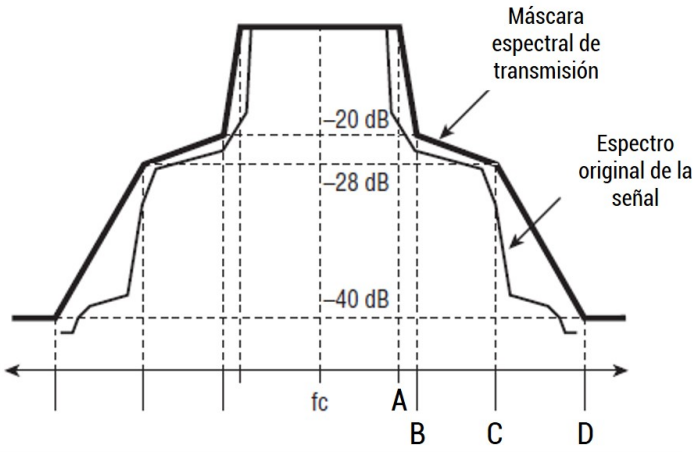


Figura 2.7: Asignación de canales en la banda de 5 GHz.

En la Figura 2.7 se muestra la numeración de los canales subdividida en bandas UNII (*Unlicensed National Information Infrastructure*, Infraestructura de Información Nacional no Licenciada): UNII-1 (5,150-5,250 GHz), UNII-2a (5,250-5,350 GHz), UNII-2c Extendido (5,470-5,725 GHz) y UNII-3 (5,725-5,825 GHz). La porción de la banda de 5,725 - 5,875 GHz es la menos problemática respecto a diferencias en la normativa de los países. La evolución de la capa PHY OFDM permite a los equipos de radio 802.11a utilizar un ancho de banda fijo de 20 MHz y los dispositivos 802.11n pueden optar por el uso de un canal de 20 o 40 MHz de ancho de banda según los requerimientos. El estándar 802.11ac incluye soporte para

un ancho de banda de canal de 20, 40 y 80 MHz de recepción y transmisión (802.11ac Wave 1). El canal de 80 MHz consiste en dos canales adyacentes de 40 MHz. Los canales de 160 MHz están formados por dos canales de 80 MHz que pueden ser adyacentes (contiguos) o no (802.11ac Wave 2). Con este estándar, se permite utilizar un mayor ancho de banda para aumentar el rendimiento. Sin embargo, las bandas de frecuencias de 5 GHz no se han ampliado. Los productos de todos los estándares 802.11 están obligados a compartir el mismo ancho de banda. Sólo si hay espectro disponible pueden utilizar los anchos de banda más amplios. Por este motivo, muchas WLAN 802.11n utilizan sólo canales de 40 MHz en la banda de 5 GHz. En este espectro también aparece la asignación de canales para los radares meteorológicos, cubriendo las bandas de 5.600 a 5.640 MHz (canales 120, 124 y 128), que forman parte de los canales DFS según la normativa.

El estándar 802.11 especifica una máscara espectral que define la distribución de potencia permitida en cada canal. La máscara requiere que la señal se atenúe a ciertos niveles (a partir de su amplitud máxima) en desplazamientos de frecuencia especificados. En la Figura 2.8 se muestra la máscara espectral para la banda de 5 GHz y define las restricciones de potencia de salida. En este sentido, se supone que la energía del canal no se extiende más allá de estos límites. Dada la separación entre canales, la señal superpuesta en cualquier canal debería estar lo suficientemente atenuada para interferir mínimamente a un transmisor en cualquier otro canal.



Ancho de Canal	A	B	C	D
20 MHz	9 MHz	11MHz	20 MHz	30 MHz
40 MHz	19 MHz	21 MHz	40 MHz	60 MHz
80 MHz	39 MHz	41 MHz	80 MHz	120 MHz
160 MHz	79 MHz	81 MHz	160 MHz	240 MHz

Figura 2.8: Máscara espectral para canales de 20, 40, 80 y 160 MHz según esquema de modulación OFDM.

2.2.4 Estructura de la trama de la capa física (PHY)

La capa física 802.11 utiliza transmisiones por ráfagas o paquetes. Cada paquete contiene un preámbulo, una cabecera y datos de carga útil. El preámbulo permite al receptor obtener la sincronización de tiempo y frecuencia, como así también estimar las características del canal para su ecualización. Es una secuencia de bits que los receptores observan para identificar el resto de la transmisión. La cabecera proporciona información sobre la configuración del paquete, como el formato, la velocidad de los datos, etc. Por último, los datos de la carga útil contienen los datos puros que el usuario transporta.

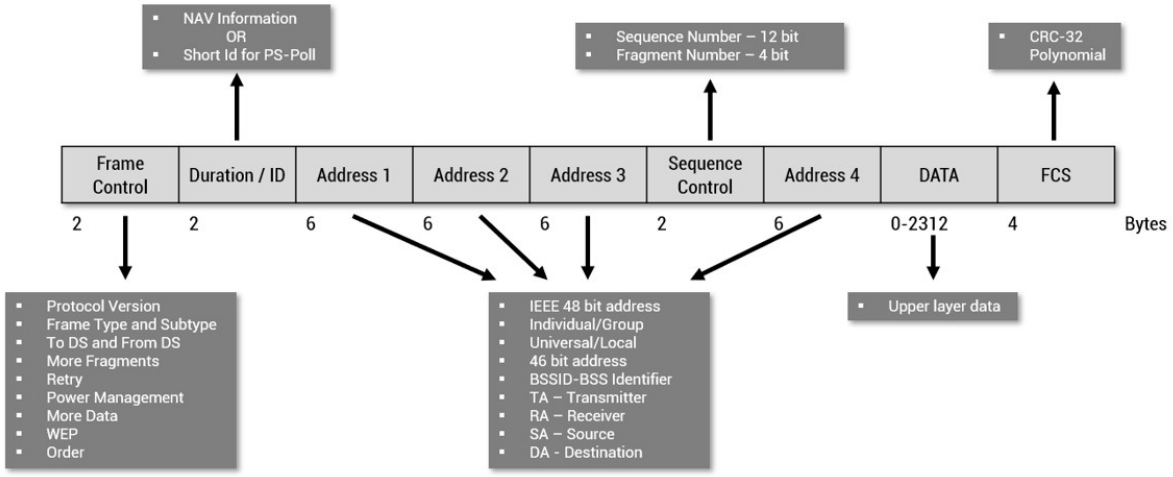


Figura 2.9: Campos y Subcampos de la cabecera MAC 802.11.

Los estándares 802.11 definen tipos de "tramas" para la transmisión de los datos y que se encargan de la gestión y control del enlace inalámbrico. En el nivel superior, estas tramas se dividen en tres funciones: Tramas de Gestión, Tramas de Control y Tramas de Datos. Cada trama consta de una cabecera MAC, una carga útil y una secuencia de comprobación de trama (FCS, *Frame Check Sequence*). Algunas tramas pueden no tener carga útil. En la Figura 2.9 se muestra la cabecera MAC, los primeros bytes forman un campo de control de trama (*Frame Control*) que especifica la forma y función de la trama. Este campo se subdivide a su vez en los siguientes subcampos:

- **Protocol Version**, es un campo de 2 bits y tiene un valor de cero por defecto. El valor no cambia salvo que haya incompatibilidad de revisión con una versión anterior;
- **Type**, este campo tiene un valor de dos bits que identifican el tipo de trama WLAN (Control "00", Datos "01", Gestión "10" o Reservado "11") (ver Tabla 2.2);
- **Subtype**, cuatro bits y contiene los distintos subtipos de tramas enviadas a través de la red. El tipo y subtipo se combinan para identificar la trama exacta (ver Tabla 2.2);
- **ToDS**, este campo tiene un tamaño de 1 bit. Especifica que un paquete está entrando a un Sistema de Distribución (DS, *Distribution System*), por ejemplo, cuando un cliente inalámbrico envía un paquete al AP con destino a internet;

- **FromDS**, este campo tiene un tamaño de 1 bit. Especifica que un paquete está saliendo de un sistema de distribución, por ejemplo, cuando un AP envía un paquete a un cliente inalámbrico;
- **More Fragments**, este campo tiene un tamaño de 1 bit. Indica si el paquete actual se fragmenta cuando el mensaje es demasiado largo para ser enviado de una sola vez. Sólo es aplicable a las tramas de datos y de gestión;
- **Retry**, tiene un tamaño de 1 bit. Los paquetes se pierden a veces en una red inalámbrica. Este campo especifica si el paquete es una retransmisión (valor de 1) o el original (valor de 0). Se aplica a las tramas de datos y de gestión;
- **Power Management**, este campo tiene un tamaño de 1 bit. Indica si la estación está en modo de ahorro de energía o en modo activo;
- **More Data**, tiene un tamaño de 1 bit. Suele indicar a la estación que está en modo de ahorro de energía que hay más datos en camino y que actualmente están en cola de espera en el AP;
- **WEP/Encription**, este campo tiene un tamaño de 1 bit. Indica si el cuerpo de la trama está encriptado o no. Es aplicable a las tramas de gestión y de datos;
- **Order**, tiene un tamaño de 1 bit. Indica el orden en que se reciben los paquetes y que deben ser procesados en dicho orden.

Las tramas son ciertos tipos de información que se envían para la comunicación entre las tarjetas/adaptadores de red (NIC) y las estaciones inalámbricas. Todas las tramas contienen las direcciones MAC de las estaciones de origen, destino y del AP, el número de secuencia, el cuerpo de la trama y la secuencia de comprobación.

Como se mencionó anteriormente, hay tres tipos de tramas MAC que son enviadas en una red inalámbrica, cada una de las cuales se subdividen en varios tipos.

El campo de Dirección 1/2/3/4 (*Address*) tienen un valor de 6 bytes cada uno. La presencia de estos campos de dirección depende del tipo y subtipo de trama. Se compone de los subcampos:

- **BSSID**, es la dirección MAC del AP;
- **TA-Transmitter**, es la dirección del dispositivo transmisor;
- **RA-Receiver**, es la dirección del dispositivo receptor;
- **SA-Sorce**, es la dirección MAC del remitente de un paquete;
- **DA-Destination**, es la dirección MAC de la estación a la que va destinado el paquete.

Las tramas son esenciales para la resolución de problemas en las redes WLAN/RLAN y en la Tabla 2.2 se pueden observar los distintos tipos y su descripción.

2.3 Descubrimiento de la red inalámbrica

La señalización involucrada en diversos mecanismos de una red WLAN/RLAN proporciona información muy importante para descubrir las características de dicha red inalámbrica. En estos mecanismos, entre los que se destacan la autenticación y la asociación, las diferentes estaciones se intercambian tramas de gestión cuyos detalles se describen en la Sección 2.3.5.

Desde el momento en el que se selecciona la red inalámbrica hasta que la conexión se establece exitosamente, el dispositivo o estación inalámbrica pasa por una serie de estados intermedios.

2.3.1 Estados Intermedios (*State Machine*)

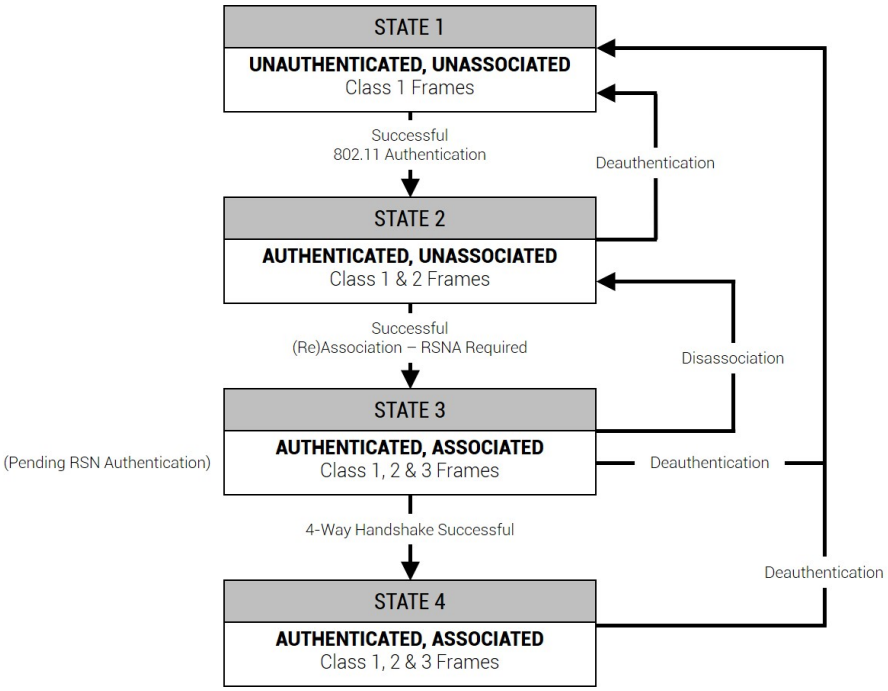


Figura 2.10: Relación entre los estados de transición y los servicios.

Los dispositivos Wi-Fi que operan bajo el estándar 802.11 y que intentan conectarse a un AP, pueden transitar por hasta 4 estados intermedios durante la sesión de conexión cuyo diagrama se muestra en la Figura 2.10 y se describen a continuación.

- **SATE 1**, este es el estado inicial del cliente en su proceso de conexión a la red inalámbrica. El cliente no está autenticado ni asociado, o sea que no está en lo absoluto conectado a la red y simplemente realiza el proceso de escaneo pasivo y escaneo activo, descubriendo las redes alrededor suyo;

- **STATE 2**, el cliente pasa del State 1 al State 2 cuando ha completado exitosamente la "autenticación 802.11". En la práctica este es un proceso bastante simple y algunas veces el concepto de autenticación puede ser malinterpretado o confundido. El State 2 no se refiere a una autenticación tipo usuario/clave (login), y mucho menos tiene que ver con los mecanismos de seguridad WEP, WPA, WPA-2, etc. que se manejan en Wi-Fi.

Type value	**Type description**	**Subtype value**	**Subtype description**
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101	Action
00	Management	1110-1111	Reserved
01	Control	0000-0111	Reserved
01	Control	1000	Block Ack Request
01	Control	1001	Block Ack
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF-End
01	Control	1111	CF-End + CF-Ack
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000	QoS Data
10	Data	1001	QoS Data + CF-Ack
10	Data	1010	QoS Data + CF-Poll
10	Data	1011	QoS Data + CF-Ack + CF-Poll
10	Data	1100	QoS Null (no data)
10	Data	1101	Reserved
10	Data	1110	QoS CF-Poll (no data)
10	Data	1110	QoS + CF-Ack + CF-Poll (no data)
11	Reserved	0000-1111	Reserved

Tabla 2.2: Tipos y Subtipos válidos de tramas.

Actualmente, la autenticación 802.11 consiste en un "saludo" entre ambos dispositivos (el cliente y el AP), quienes intercambian estos mensajes de autenticación como ratificando que ambos son dispositivos 802.11 válidos;

- **STATE 3**, el cliente pasa del State 2 al State 3 cuando ha completado exitosamente la asociación con el AP. En esta transición hacia el State 3, la estación cliente le solicita al AP permiso para unirse y ser parte de su área de servicio (*BSS*, Basic Service Set). Esta solicitiud de asociación es también bastante simple y consiste en el intercambio de un par de mensajes "request" y "response". Dentro de estos mensajes está incluida la información con todos los Data Rates soportados tanto del lado del cliente como del lado del AP. Además, cuando se logra una asociación exitosa con el AP, éste envía un identificador denominado "Association ID", que corresponde al número de asociación del cliente. Hasta este punto el cliente está autenticado y asociado, pero aún queda por completar los mecanismos de seguridad adicionales requeridos para redes con seguridad robusta (*RSN*, Robust Security Network);

- **STATE 4**, la transición del State 3 al State 4 es un poco más elaborada. Entre otras cosas, involucra un proceso conocido como "4-Way Handshake" que generará las llaves de encriptación dinámicas que tanto el cliente como el AP emplearán para proteger (encriptar/desencriptar) las tramas de datos que viajarán en la interfaz de aire.

Cuando el dispositivo Wi-Fi complete progresiva y exitosamente cada uno de estos 4 estados y logre alcanzar el State 4, no solo habrá establecido una asociación con el AP sino que más importante aún, este Punto de Acceso le permitirá transmisitir tráfico a la red.

2.3.2 Sincronización

En el proceso de sincronización, una vez que se enciende una estación, se examina si existen otras estaciones/clientes o algún AP al cual unirse, antes de llevar a cabo cualquier proceso de autenticación o asociación con algunos de ellos. Esto se conoce como "Fase de Descubrimiento".

El AP emite a intervalos regulares una trama Beacon que se puede observar en la Figura 2.11. Las tramas Beacon se envían periódicamente en un tiempo llamado TBTT (*Target Beacon Transmission Time*, Tiempo de Transmisión de Balizas Objetivo) y se expresa en unidades de tiempo (TU) $1TU = 1.024$ microsegundos, por lo tanto, el intervalo de beacon equivale a $100TU = 100 \times 1.024$ microsegundos $= 0,102400$ segundos, y que corresponde a consumir un cierto "tiempo de aire" del medio inalámbrico compartido. Mantienen el sincronismo entre las estaciones que usan la misma capa física ya que incorporan una marca de tiempo. Permiten a las estaciones obtener una lista de puntos APs disponibles buscando tramas Beacon continuamente en todos los canales 802.11.

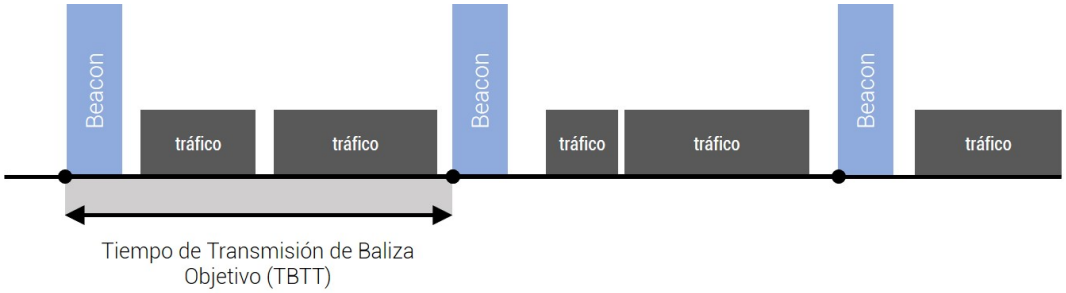
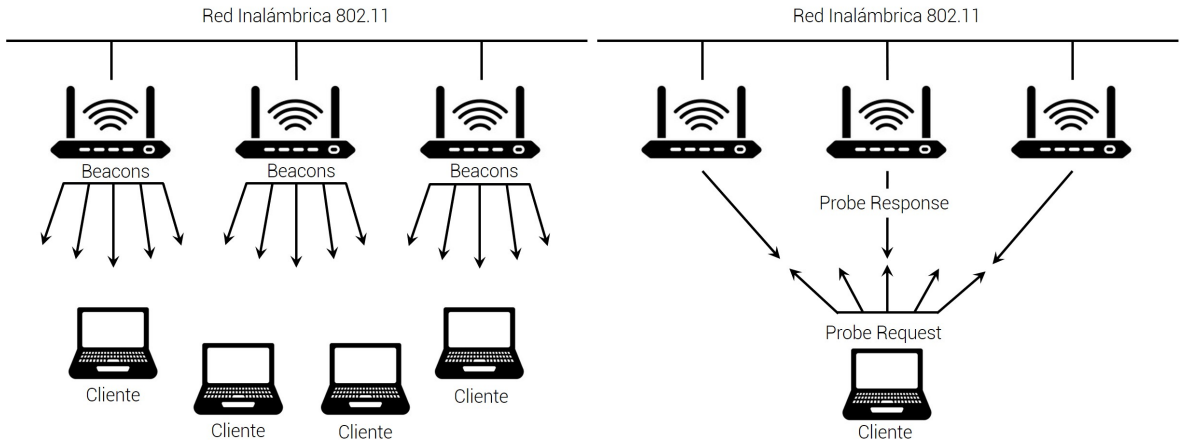


Figura 2.11: Intervalos regulares de la trama Beacon para establecer la sincronización.

Mediante la actividad de descubrimiento el dispositivo cliente busca las redes inalámbricas e identifica los parámetros de esas redes. Para esta fase, el cliente emplea un escaneo pasivo (*passive scanning*) y un escaneo activo (*active scanning*) como se muestra en la Figura 2.12.



(a) Escaneo Pasivo

(b) Escaneo Activo

Figura 2.12: Fase de Descubrimiento y establecimiento de conexión mediante el escaneo pasivo y activo.

Escaneo Pasivo

Esta actividad permite a los dispositivos router AP transmitir continuamente por la interfaz de aire una trama de gestión especial denominada "Beacon" para anunciar dentro de su área de cobertura (o servicio) las características que ofrece su conexión. Ejecutando un escaneo pasivo los clientes continuamente están "escuchando" esta trama de gestión y de esa manera pueden identificar a los APs cercanos. Esta trama Beacon contiene información para que los clientes puedan conocer los parámetros del AP antes de intentar conectarse a la red inalámbrica.

Escaneo Activo

Empleando el escaneo activo, el cliente transmite primero una trama de gestión denominada "Probe Request" para identificar una red específica (búsqueda por SSID) o para descubrir todas las redes disponibles (sin declarar un SSID específico, dejando el campo vacío de la

cabecera). Cuando el AP recibe o escucha un mensaje Probe Request debe responder con "Probe Response" y el contenido del mensaje es similar a la información que ofrece el "Beacon" propagado durante el escaneo pasivo.

2.3.3 Autenticación por red abierta o encriptada

La estación debe ser autenticada por el AP para poder unirse a la red WLAN/RLAN. Con una red abierta, un dispositivo envía una solicitud de autenticación y el AP envía el resultado. En una red segura hay un proceso de autenticación más formal, lo que implica el AP, el cliente y el servidor de autenticación, que suele ser un host que ejecuta un software con los protocolos de seguridad necesarios. Si el servidor de autenticación determina que las credenciales son válidas, el suplicante (dispositivo cliente) puede acceder a los recursos situados en el lado protegido de la red.

2.3.4 Asociación

La asociación es el siguiente paso después de la autenticación y permite la transferencia de datos entre el cliente y el AP. El cliente envía una trama de solicitud de asociación al AP, que responde con una trama de respuesta que permite la asociación o el rechazo.

2.3.5 Tramas de Gestión

A continuación se describen los tipos y subtipos de tramas más importantes y que son necesarias para identificar y caracterizar las fuentes de interferencias. Para el estudio realizado, los tipos de tramas más relevantes han sido las Tramas de Gestión.

Estas tramas son destinadas a la gestión de los enlaces inalámbricos en las redes WLAN/RLAN y se generan durante las siguientes situaciones o tareas:

- solicitud de asociación y disociación del cliente a un AP;
- respuestas de sondeo (tramas Probe Response);
- tramas de desautenticación generadas por el AP.

La cabecera MAC de todas las tramas de gestión es la misma y no depende del subtipo de trama. Tiene una cabecera estándar de 24 bytes formadas por campos como: Control de Trama, Duración/ID, Dirección de Destino, Dirección de Origen, BSSID, Control de Secuencia y FCS.

Trama Beacon

Son tramas/mensajes transmitidos a intervalos regulares por los AP para comunicar en toda su área de servicio las características de la conexión ofrecida a los miembros de un entorno inalámbrico. Esta información la utilizan tanto los clientes que intentan conectarse a la red

WLAN/RLAN como los que ya están asociados. En la Figura 2.13 se muestra la cabecera completa de la trama.

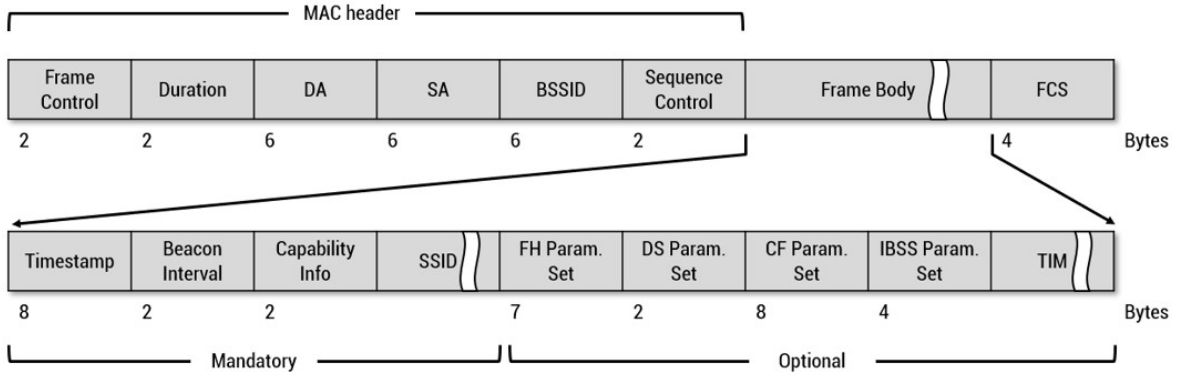


Figura 2.13: Cabecera MAC de Trama Beacon que se desprende de la cabecera MAC de la Trama de Gestión.

En el Beacon está contenida toda la información de la red WLAN/RLAN: SSID, dirección MAC, data-rates soportados, frecuencia o canal de operación, configuraciones de seguridad y una serie de parámetros adicionales.

Trama Probe Request

Son tipos de tramas transmitidas por el cliente inalámbrico para escanear un área en busca de cualquier red 802.11 existente. El cliente debe soportar toda la velocidad de datos requerida por la red antes de ser autorizado a unirse a ella. En la Figura 2.14 se muestra la cabecera MAC de esta trama.

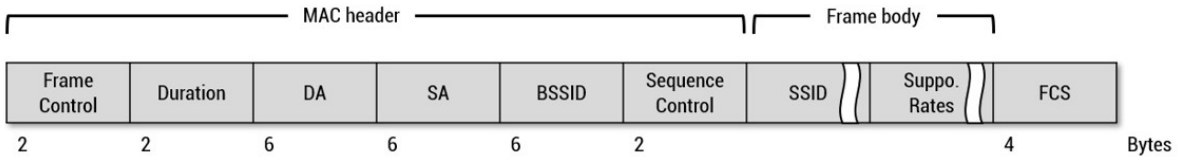


Figura 2.14: Cabecera MAC de Trama Probe Request.

Los clientes envían tramas Probe Request en un canal y esperan durante un pequeño período de tiempo la respuesta (Probe Response). Si no reciben respuesta en este período de tiempo saltan de canal y vuelven a repetir el proceso.

Trama Probe Response

Se trata de tramas de respuesta que la estación inalámbrica transmite a los clientes en su respuesta a su solicitud de sondeo (*Trama Probe Request*). La respuesta incluirá información necesaria sobre la velocidad de datos soportadas y otros requisitos que el cliente debe cumplir antes de poder unirse a la red. Es decir, que el contenido del mensaje es similar a la información que ofrece la trama Beacon.

Cuando una estación recibe una Probe Request, responde con una trama Probe Response. esta trama es unicast ya que va dirigida al cliente que ha realizado la petición. Es enviada a mínima tasa de transferencia.

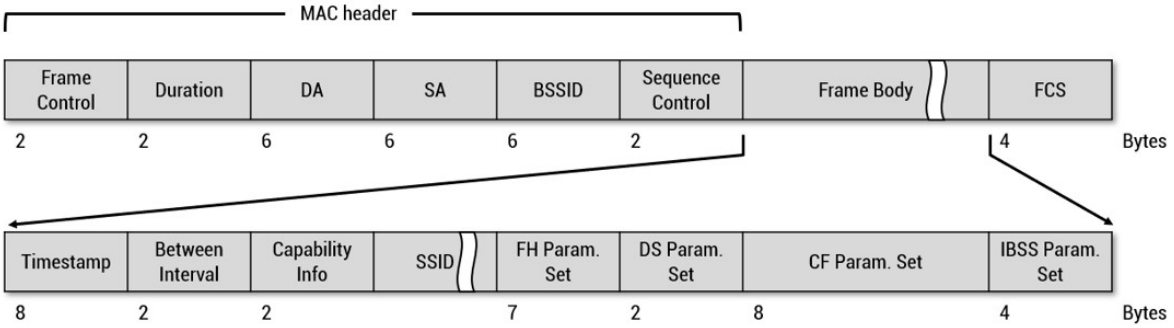


Figura 2.15: Cabecera MAC de Trama Probe Response.

2.3.6 Transferencia de datos

El intercambio de datos ocurre luego de la autenticación y la asociación. El intento de enviar datos a un AP sin la debida autenticación y asociación adecuadas hace que el punto de acceso responda con una trama de desautenticación. Las tramas de datos siempre son reconocidas con un mensaje de "Acknowledgement" como acuse de recibo. El AP reenvía las tramas de datos recibidas del cliente al destino requerido en la red, como también reenviará los datos dirigidos al cliente desde la red.

2.3.7 Estructura de los Enlaces Punto a Punto

En el estándar IEEE 802.11 se distinguen tres tipos de protagonistas de la comunicación de datos:

- TRANSMISOR, es la estación o AP que baja la trama al medio inalámbrico, aunque no necesariamente es el que la genera;
- RECEPTOR, puede ser un intermedio, por ejemplo, el AP. En todo caso, es el receptor de la trama en el medio inalámbrico;
- DESTINO, es el que procesa la trama para pasarla a niveles superiores. La dirección de destino es el identificador IEEE MAC que corresponde a la estación que destinará la información a las capas supriores para su procesamiento final.

De acuerdo a la estructura de la trama inalámbrica mencionada en la subsección 2.2.4, el campo de Control de Trama (Frame Control) define dos bits correspondientes a los subcampos "ToDS" y "FromDS" que definen la dirección de los mensajes en relación al sistema de distribución (DS). En el caso particular de establecer un puente inalámbrico (*WDS*, Wireless Distribution System) como mecanismo de transmisión, donde se configura una WLAN/RLAN

entre dos AP a modo de enlace entre redes (enlace punto a punto de microondas), ambos bits se ajustan en “ToDS=1” y “FomDS=1”. La comunicación inalámbrica es entre puntos de acceso.

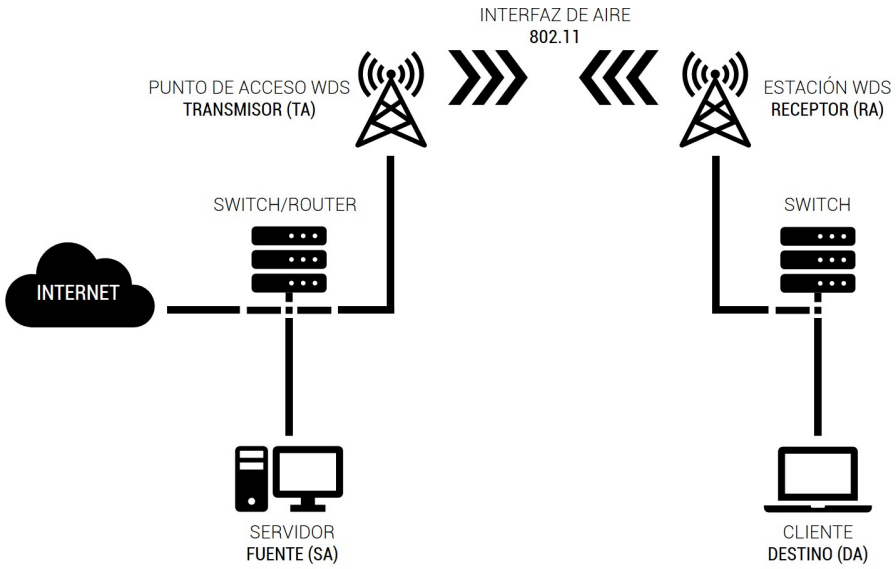


Figura 2.16: Comunicación por puente inalámbrico WDS.

En la Figura 2.16 se representa el caso en que su utilizan las cuatro direcciones en el campo de la trama MAC 802.11 (ver Figura 2.9), porque hay cuatro protagonistas en juego en este enlace. La Dirección 1 (*Address 1*) corresponde a la Estación WDS siendo el Receptor (RA) de la trama enviada por el medio inalámbrico, la Dirección 2 (*Address 2*) es el dispositivo configurado como Punto de Acceso WDS en el enlace de microondas, siendo el Transmisor (TA) de la trama. La Dirección 3 (*Address 3*) es el Destino (DA) que corresponde al Cliente y, por último, la Dirección 4 (*Address 4*) pertenece a la dirección física MAC de la Fuente u origen (SA) de la trama, en este caso el dispositivo Servidor que provee el servicio de Internet.

La arquitectura Cliente -Servidor mostrada en la Figura 2.16 es la que habitualmente utilizan los ISP (*Internet Service Provider*, Proveedor de Servicio de Internet) para distribuir el acceso a la red de redes entre sus diversos clientes. WDS puede funcionar también en modo Repetidor Inalámbrico con el propósito de extender la red.

Otro servicio que utiliza este tipo de red inalámbrica de forma operativa es la transmisión de video y audio en tiempo real que se emplea en el monitoreo de cámaras de vigilancia. Esta funcionalidad permite utilizar todo el ancho de banda disponible para la transmisión de paquetes a alta velocidad utilizando la tecnología IP.

Estos escenarios son válidos siempre y cuando exista una línea de vista clara entre los dos puntos (Punto de Acceso WDS y Estación WDS). En lo que respecta a la configuración del Punto de Acceso debe tener una dirección IP asociada, un SSID, el código de país (para adecuarse a las legislaciones vigentes), el estándar IEEE 802.11, el ancho de banda del canal, la frecuencia de operación, la potencia de salida sin saturación de señal y la máxima tasa de transferencia. Dentro las opciones avanzadas se pueden activar funciones especiales que

optimizan el funcionamiento del equipo al máximo en el ancho de banda disponible, ya que éstas utilizan protocolos y algoritmos potentes que mejoran la calidad de aire y el uso de distintos canales de frecuencias, como por ejemplo, la activación de canales DFS según la normativa.

En el lado de punto remoto (Estación WDS), también se configuran parámetros similares respecto a la unidad base (Punto de Acceso WDS). Los parámetros de código de país, modo, potencia y seguridad se configuran igual que la estación base. La diferencia se encuentra en la configuración del ancho de banda del canal y la asociación a la dirección MAC (dirección física) del dispositivo AP WDS.

2.4 Marco Normativo en las redes inalámbricas

Uno de los principales atractivos de las redes inalámbricas es que usan una porción del espacio radioeléctrico en la que no hay que pagar por su uso y es libre. Pero, es requisito fundamental atenerse a las reglas de uso que impongan los organismos reguladores. Tampoco es necesario obtener una licencia de explotación siempre que el uso de la red sea privado. En este sentido, las telecomunicaciones recorren un amplio camino hacia un sector complejo, multifactorial e impredecible. Parte de esta complejidad proviene del fenómeno de la globalización, de la actividad económica y social y del cambio tecnológico que la impulsa.

En consonancia con los lineamientos trazados desde el Gobierno Nacional, tendiente a promover una política social estratégica que posibilite recuperar la participación del Estado en la formulación de políticas e instrumentos de crecimiento, inclusión y desarrollo social, se han implementado diversos proyectos con el objetivo de mejorar los sistemas de información y comunicación en materia de Telecomunicaciones y del Espectro Radioeléctrico optimizando recursos e innovando tecnológicamente.

El marco legislativo actual se configura en torno a un conjunto de normativas, decretos, leyes, notas técnicas, resoluciones donde se incluyen:

- Unión Internacional de Telecomunicaciones (UIT);
- Ente Nacional de Comunicaciones (ENACOM);
- Cuadro de Atribución de Bandas de Frecuencias de la República Argentina (CABFRA);
- Ley Argentina Digital.

En nuestro país, las comunicaciones inalámbricas están reguladas por el ENACOM. Según la Resolución N° 581/2018 “Bandas de espectro radioeléctrico de uso compartido. Instrucciones para su atribución y disposición”, se reglamenta el uso de bandas de frecuencias para la operación de diferentes tecnologías de transmisión de información, en modalidad compartida y de libre utilización con el fin de garantizar soluciones normativas sólidas y consistentes. En este marco, resulta imprescindible que el espectro compartido se encuentre asociado a las

normas técnicas correspondientes, a fin de asegurar que no existan incompatibilidades técnicas y proveer una adecuada protección contra las interferencias, ya sean atribuidos con carácter primario o secundario.

Además, dicha resolución expresa que de ninguna manera se interfiera con la prestación de servicios atribuidos en forma exclusiva. En este sentido, existe un marcado consenso en cuanto al rol del Estado de fomentar la coexistencia de diferentes servicios, aplicaciones y tecnologías en una misma banda de frecuencias, siempre que no produzcan interferencias que imposibiliten el uso para el que fueron atribuidos.

En el Artículo N° 4 se resuelve que los equipos utilizados para la emisión en las bandas de frecuencias de uso compartido deben cumplir con las siguientes condiciones:

- deben observar las normas vigentes en materia de radiaciones no ionizantes, no pudiendo exceder los límites establecidos;
- deben funcionar y emitir de conformidad con los estándares técnicos definidos por el Ente Nacional de Comunicaciones (ENACOM) y operar exclusivamente en las bandas de frecuencias establecidas;
- deben estar debidamente homologados o contar con los certificados de homologación que determine el ENACOM.

En el Artículo N° 5 inciso 5.1, se resuelve que las emisiones en las bandas de frecuencias de uso compartido no podrán causar interferencias a las estaciones autorizadas de un servicio autorizado en dichas bandas con atribución a título primario. Que asimismo, por el inciso 5.2 del citado artículo, el usuario de bandas de frecuencias de uso compartido que causare interferencia perjudicial a una estación de un servicio autorizado en la banda con atribución a título primario, deberá suspender la emisión y no podrá reanudarla hasta que se haya subsanado el conflicto interferente.

En el caso de la potencia de emisión, y ante el uso compartido de la misma banda de frecuencias con los sistemas de radar meteorológico (rango de frecuencias de 5.470-5.600 MHz y 5.650-5.725 MHz), pueden transmitir como máximo según la normativa, una potencia conducida de 24 dBm y una P.I.R.E (Potencia Isotrópica Radiada Efectiva) de 30 dBm.

El incumplimiento de la Resolución Ministerial por parte de los usuarios de las bandas de frecuencias de uso compartido, estará sujeto a la aplicación del régimen de medidas precautorias y de sanciones dispuestos por la Ley Argentina Digital N° 27.078 y las normas reglamentarias vigentes en la materia.

2.5 Reflexiones Finales

A modo de cierre de este Capítulo, se han presentado las características técnicas más relevantes del Radar Meteorológico Argentino (RMA), considerando las dimensiones de

muestreo como estrategia de funcionamiento con el fin de obtener, mediante el procesamiento de los datos, productos radar que permitan analizar los distintos fenómenos meteorológicos.

A partir del análisis del producto radar PPI de reflectividad, se pueden identificar las direcciones acimutales estimadas en las que se observa potencia debida a la/s fuente/s de interferencia/s. Estas interferencias se deben principalmente a dispositivos WLAN/RLAN que funcionan en la banda de 5 GHz y que por lo general, cumplen con el estándar IEEE 802.11. Estos equipos utilizan OFDM para incrementar la robustez frente a interferencia de banda angosta. Las especificaciones del estándar 802.11 con respecto al modelo OSI están enfocadas a la capa física PHY y a la subcapa MAC para redes WLAN/RLAN. La subcapa MAC establece un conjunto de reglas para determinar cómo acceder al medio y enviar los datos, pero los detalles de transmisión y recepción de éstos pertenecen a la PHY. Este trabajo se centra en el análisis de la capa PHY y la subcapa MAC, ya que en este punto se diseñan los requisitos para el hardware de los dispositivos que utilizan las diferentes técnicas de los estándares 802.11. Por este motivo, se estudia la señal interferente desde la norma que la define para determinar sus características de interés.

Las tramas son esenciales para comprender el funcionamiento de una red inalámbrica WLAN/RLAN y poder solucionar problemas. Una vez que se entiende una red inalámbrica a nivel de paquetes, será fácil identificar y comprender las distintas tramas que se transportan por la interfaz de aire.

En cuanto al medio físico, se ha presentado el enlace punto a punto de microoondas que es la arquitectura que actualmente se utiliza para la transferencia de datos. En este sentido, en el intento por convivir y competir por el uso del espectro radioeléctrico, dicha transmisión puede interferfir a otros sistemas o servicios que funcionan en bandas de frecuencias legales. Por esta razón, se presenta el marco normativo implementado por el ENACOM que regula las actividades de los sistemas inalámbricos en la banda de frecuencias de 5 GHz. Desde el punto de vista técnico, estos dispositivos presentan una solución favorable, pero pueden ignorar tanto parcial como de forma completa las regulaciones legales vigentes.

Capítulo 3

Descripción de equipamiento y selección de recursos

3.1 Introducción

En este capítulo se presenta una breve descripción de los recursos de hardware, software y aplicaciones utilizados en el proceso de medición. Para la selección de los elementos apropiados, previamente se testearon muchas alternativas, desde la instalación y uso de un sistema operativo distinto al que se acostumbra a manipular cotidianamente con sus respectivos paquetes y dependencias, hasta dispositivos inalámbricos internos y externos en sus diversos modos de operación y control.

En un primer momento, se probaron alternativas de software según la compatibilidad con el sistema operativo. Bajo plataforma Windows, y teniendo en consideración que la mayoría de las aplicaciones son propietarias y requieren de licencias para acceder a su uso, se necesitaba de un programa capaz de escanear el entorno inalámbrico para detectar las distintas fuentes WLAN/RLAN y analizar el estado de la red, su rendimiento, conexiones, identificación de velocidades de transmisión y el uso de canales de acuerdo a su frecuencia. Desde Linux, la configuración del hardware y software demandó mucho más tiempo y trabajo. Debido a que es una arquitectura libre y abierta, la gama de aplicaciones y programas es extensa y con similares e incluso mejores funcionalidades que en Windows.

Luego, de acuerdo a los requisitos y funcionalidades del software, se hizo necesario adquirir y configurar dispositivos de hardware que sean compatibles, como en el caso de las aplicaciones en Windows, o que se permita habilitar modos de funcionamiento ocultos, como el "modo promiscuo o monitor" bajo plataforma Linux.

3.2 Instalación y prueba del Software

3.2.1 Software en Windows

A continuación, se describen cada uno de los programas que se instalaron bajo plataforma Microsoft Windows 10 versión Pro con las últimas actualizaciones incoporadas.

Acrylic Wi-Fi Professional

Luego de una exhaustiva investigación por la web acerca de los diferentes tipos de software, se probó con la instalación del programa Acrylic Wi-Fi Professional[1] versión 3.0.5770 de la empresa Tarlogic Research para visualizar, monitorizar, analizar y auditar redes inalámbricas en la banda de 5 Ghz. Esta herramienta permite visualizar la potencia de señal de los APs en tiempo real y la ocupación de canales: UNII-2 (Middle) (canales 52, 56, 60 y 64), UNII-2 (Extended) (canales 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 y 140) y UNII-3 (canales 149, 153, 157 y 161) para analizar su comportamiento cubriendo el rango de frecuencias del sensor radar (BW 5.450-5.820 MHz). Además, presenta la identificación de las señales inalámbricas de acuerdo a su SSID y su dirección física MAC, además del ancho de canal y el estándar predominante 802.11 b, g, n y ac. En la Figura 3.1 se presenta la pantalla inicial del programa, donde se observan las distintas redes, canales de funcionamiento y otras características técnicas como nivel de potencia de señal (RSSI), relación Señal/Ruido (SNR), cláusula o estándar, etc.

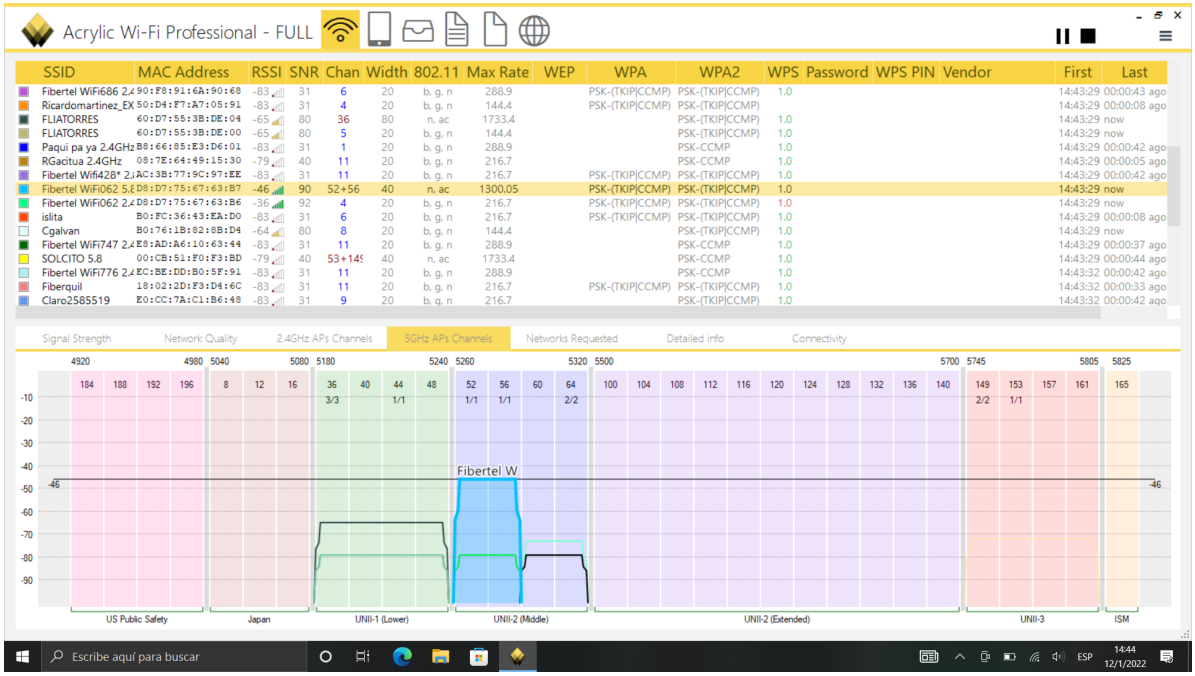


Figura 3.1: Software Acrylic Wi-Fi Professional.

Esta aplicación dispone de una función especial, que es localizar de forma estimada cada

[1]Extraído de la web oficial https://www.acrylicwifi.com/programas-software-herramientas-wifi/analizador-wifi-acrylic-wifi-profesional/ el día 10 de enero de 2022.

una de las redes mediante el uso de señales GPS. Dicha función necesita de un dispositivo externo capaz de recibir las señales de los satélites, necesarias para estimar la posición. Un teléfono inteligente de última generación Samsung Galaxy S10 con sistema operativo Android cumpliría con estos requerimientos, como se detalla en la Sección 3.3, para vincularse a través de una interfaz virtual de tipo serie (puerto COM) mediante conexión bluetooth. Es necesaria la instalación de una aplicación Android en el teléfono para lograr la transmisión de los datos al software Acrylic. Luego, esta captura se almacena en un fichero .pcap para posteriormente convertir a un archivo .kmz e importar desde Google Earth online y visualizar en un mapa satelital las coordenadas estimadas de las señales Wi-Fi en tiempo real. Este procedimiento se esquematiza en la Figura 3.2.

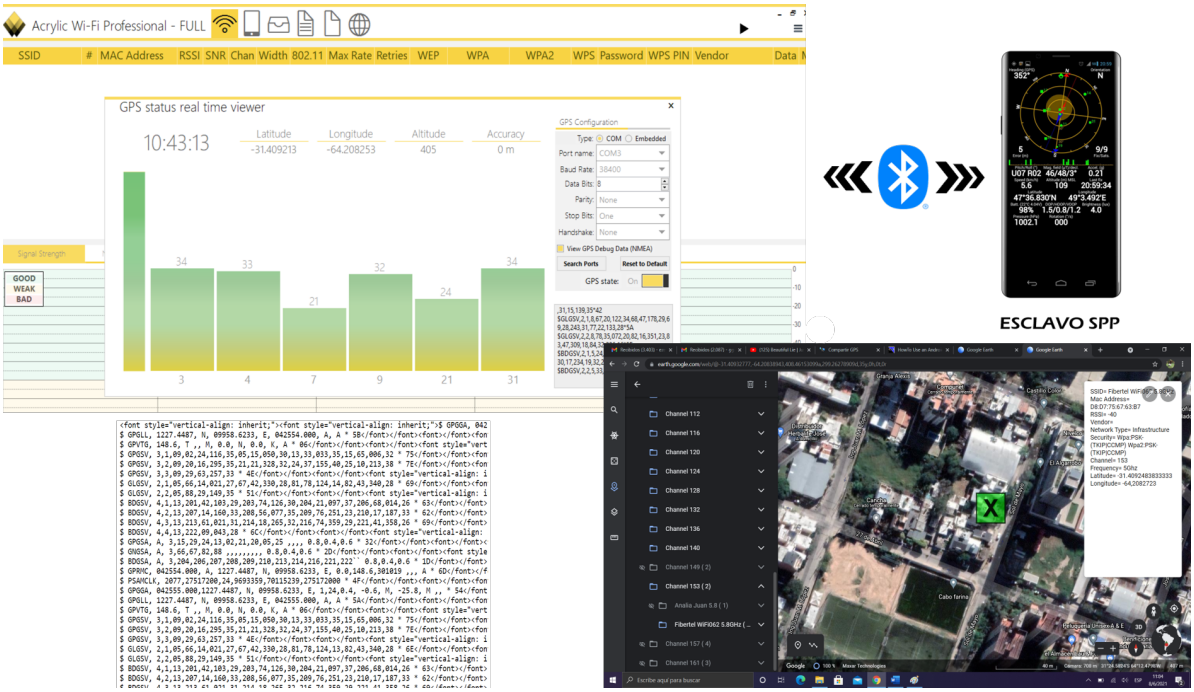


Figura 3.2: Función GPS activa y exportación a Google Earth online.

Cabe aclarar que los datos de latitud y longitud de los APs son recibidos a partir del registro de la señal Wi-Fi según el nivel de sensibilidad y la ubicación física del adaptador inalámbrico. Esto quiere decir, que no corresponde a la posición exacta del AP. Se necesita de otros datos para triangular su posición con un mínimo margen de error.

Google Earth Pro: Versión Escritorio

Es una herramienta de versión gratuita que contiene información geoespacial y datos geográficos disponibles de manera pública. Además, incluye imágenes de alta resolución extraídas de imágenes satelitales, fotografías aéreas, información geográfica obtenidas de modelos GIS (siglas en inglés de Sistema de Información Geográfica) y datos generados por computadora. Este software permite la importación de imágenes externas para anexar sobre el mapa mediante capas, trazar todo tipo de información extra a través de waypoints y líneas, y el uso de funciones especiales como Google Street View que facilitan la identificación y

localización de las diferentes fuentes de interferencias. En la siguiente figura, se observa una imagen satelital de la zona de interés y el uso de las herramientas de líneas, waypoints y Street View para facilitar el trabajo sobre el mapa.

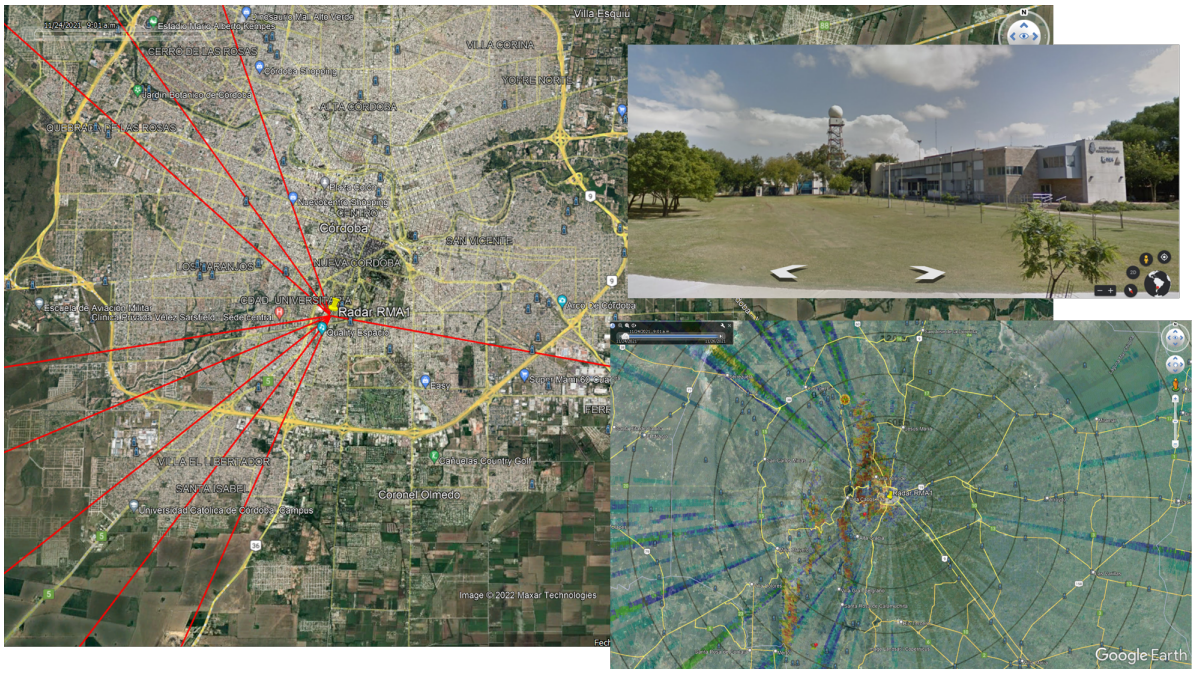


Figura 3.3: Software Google Earth con importación de imagen y función Street View.

Radiomobile[2]

Este es un programa de libre distribución orientado al cálculo de radioenlaces de microondas de larga distancia que funcionan en la zona más baja de la atmósfera, denominados enlaces troposféricos. Utiliza perfiles geográficos combinados con información de equipos transceptores (potencia de TX y RX, sensibilidad del receptor, características de las antenas, pérdidas, características del terreno, etc.) que quieren simularse.

Este software implementa con buenas prestaciones el modelo Longley-Rice, modelo de predicción troposférica para transmisión de radiofrecuencia sobre terreno irregular en enlaces de largo-medio alcance. Asimismo, posee múltiples utilidades de apoyo al diseño y simulación de los enlaces y de las redes de telecomunicaciones.

RadioMobile usa los datos de elevaciones de la NASA del proyecto SRTM (acrónimo de *Shuttle Radar Topography Mission*) y a partir de estos, produce mapas de elevaciones que pueden superponerse a mapas topográficos de fuentes de Internet como Map Quest, Google Maps, Internet Open Street Maps, etc.

Navegador Web y Aplicaciones Java

Los navegadores web con soporte Java Applet (Mozilla Firefox o Google Chrome) son esenciales para la ejecución de software embebido, como airOS, airView, airMax, airControl, entre otros, utilizados para el control y configuración de dispositivos inalámbricos de exterior

[2]Extraído de la web oficial http://radiomobile.pe1mew.nl/ el día 10 de enero de 2022.

que se instalan en el lado del cliente. Estos equipos disponen de una interfaz de usuario web a la que se ingresa con una dirección IPv4 (previamente configurada en el adaptador ethernet de la computadora que pertenezca a la misma subred) y autenticación de usuario y contraseña para el acceso a la pantalla principal del mismo.

3.2.2 Software en Android

Share GPS

Es una aplicación gratuita disponible para su descarga en Google Play Store. Permite compartir datos de ubicación en tiempo real. Todas las opciones de configuración están habilitadas solamente para una única sesión de conexión. Por lo tanto, su uso es limitado, y en caso de crear más conexiones se deberá adquirir la versión completa del programa y pagar por ello. Con esta aplicación se utiliza un teléfono inteligente como dispositivo GPS externo y transferir sus datos mediante múltiples métodos: serial, bluetooth, usb o TCP/IP para el envío de tramas NMEA estándar[3] (tramas de datos GPS). Para conexiones locales con un programa como Google Earth, puede convertir la computadora portátil en un dispositivo de navegación de pantalla. También permite compartir datos de ubicación de forma remota utilizando el protocolo TCP/IP si existen conexiones Wi-Fi o 3G/4G.

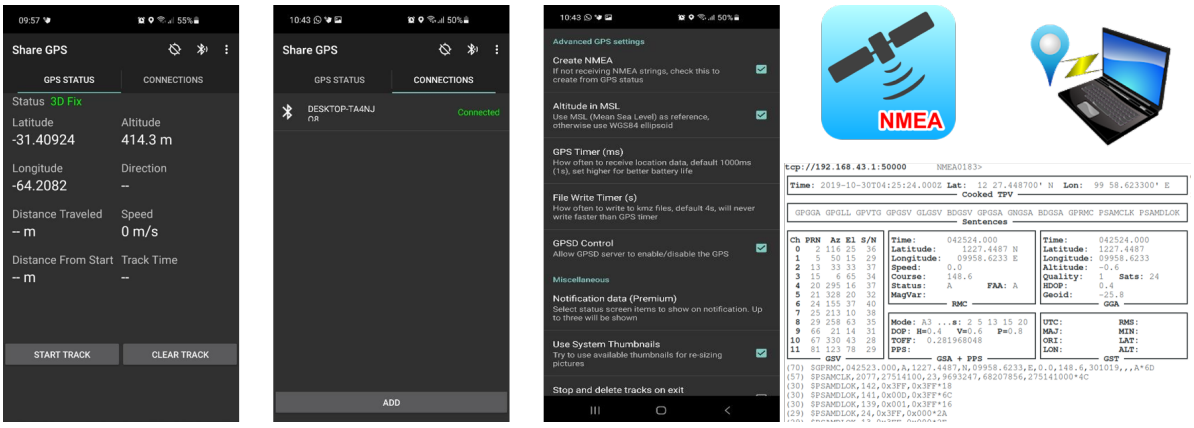


Figura 3.4: Aplicación Share GPS para transferencia de señal GPS.

3.2.3 Software en Linux

En esta sección se presentan las alternativas de software consideradas en la versión de Linux Ubuntu 20.04 LTS Focal Fosa. Como se mencionó, la configuración tanto del software como del hardware con Ubuntu demandó un arduo trabajo, en especial el manejo fluido del sistema operativo, control por línea de comando, instalación de paquetes y dependencias, por citar algún ejemplo. A lo largo del trabajo se comprobó el potencial de las aplicaciones de código libre, no solo por su eficiencia en el funcionamiento sino también por la amplia disponibilidad

[3]NMEA (National Marine Electronics Association). Protocolo que define los requerimientos de datos y tiempo de transmisión en el formato serial a una velocidad de 4800 bps.

de información para ejecutarlas. La mayor dificultad en esta línea fue conseguir los drivers y/o controladores compatibles con el hardware para que funcione de manera correcta.

Sparrow- WiFi[4]

Esta herramienta de reconocimiento espectral Wi-Fi de 2,4 y 5 GHz, funciona de manera similar a su par Acrylic Wi-Fi Professional en Windows. Desarrollada completamente en código Python3, integra tecnología Wi-Fi, Radio Definida por Software (SDR - hackrf), comunicación bluetooth y GPS tradicional. Sus características principales son las siguientes:

- identificación básica de SSID Wi-Fi;
- análisis del espectro en 2,4 y 5 GHz;
- identificación de señal bluetooth;
- visualización de clientes conectados a las redes inalámbricas;
- capacidad de Importar/Exportar desde archivos CSV y JSON para una fácil integración y revisión;
- producción de mapas de Google cuando las coordenadas GPS están disponibles y trazar telemetría Wi-Fi con el tiempo.

Con esta herramienta es posible capturar información sobre la posición de los clientes y su conexión a las distintas redes inalámbricas. Luego, al activar el GPS se visualiza en un mapa la posición estimada. Al igual que en Acrylic Wi-Fi Professional se necesitan de más datos para asegurar la localización exacta de los dispositivos.

Kismet[5]

Es una herramienta de detección de dispositivos y redes inalámbricas, que permite "escuchar" el tráfico inalámbrico (conocido como *sniffear* en inglés) y ser utilizada para la búsqueda de redes inalámbricas Wi-Fi estando en movimiento (conocido como *War-Driving* en inglés). Sniffer es un concepto que se utiliza en el mundo de la informática, específicamente cuando se desea capturar tráfico en entornos inalámbricos 802.11. Existen términos análogos como analizador de tráfico, analizador de protocolos, detección de paquetes, etc. Es una acción que se utiliza cuando se desea capturar información extra de algún dispositivo en particular y requiere del uso de software y hardware especializado. Además, funciona como sistema de detección de intrusiones inalámbricas (*WIDS* por sus siglas en inglés) capaz de generar alertas cuando se presentan casos anómalos en la red. Es un programa de código abierto que permite conexión con interfaces Wi-Fi, bluetooth y hardware SDR. Puede rastrear tráfico 802.11b, 802.11a, 802.11g, 802.11n y 802.11ac.

[4]Extraído de la web oficial https://github.com/ghostop14/sparrow-wifi el día 12 de enero de 2022

[5]Extraído de la web oficial https://www.kismetwireless.net/ el día 13 de enero de 2022.

Kismet se diferencia de otros sniffers debido a su funcionamiento pasivo. Es decir, trabaja de forma silenciosa inyectando pocos paquetes detectables, permitiendo capturar la presencia de varios puntos de acceso y clientes inalámbricos, asociando unos con otros. Es capaz de usar receptores GPS seriales, de red y USB para rastrear la ubicación de las señales. Las funciones más importantes se resumen a continuación:

- verifica que una red específica está bien configurada y que puede trabajar en modo monitor (término que se detalla en la Sección 3.4);
- detecta qué red puede causar interferencia a la red utilizada por el usuario;
- busca redes inalámbricas desde un vehículo en movimiento mediante el método *War-Driving*, lo que permite detectar todos los puntos de acceso que se encuentran alrededor;
- muestra información de los clientes conectados a la red;
- indica al usuario el tipo de protección (clave WEP, WPA, etc.) con mucha precisión;
- funciona con adaptadores en modo monitor y almacena en archivos los paquetes capturados.

Wireshark[6]

Wireshark es un analizador de protocolos de red que permite capturar y explorar, a un nivel microscópico, de forma interactiva el tráfico que atraviesa una red inalámbrica o alámbrica. Dispone de varias características muy potentes y es una herramienta de uso regular por los administradores de redes. Se encuentra disponible como código abierto sin costo (GNU General Public License version).

Los dispositivos Wi-Fi usan el estándar 802.11 para comunicarse entre ellos. Interpretar y analizar correctamente las tramas capturadas requiere experiencia, un buen entendimiento del estándar y conocimiento de los diferentes protocolos involucrados. Wireshark es una herramienta gráfica capaz de detectar y analizar el tipo de tráfico en un momento determinado. Permite analizar los paquetes de datos en una red activa o desde un archivo previamente generado.

Algunas características se enumeran a continuación:

- captura los paquetes directamente desde una interfaz de red;
- permite obtener detalladamente la información del procotolo utilizado en el paquete capturado;
- cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas;

[6]Extraído de la web oficial https://www.wireshark.org/ el día 14 de enero de 2022.

- filtra los paquetes que cumplen con un criterio definido previamente;
- permite obtener estadísticas;
- sus funciones gráficas son muy poderosas, ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos.

Aircrack[7]

Es un paquete de herramientas para evaluar la seguridad de redes inalámbricas. Estas herramientas trabajan de forma integrada para analizar ciertos aspectos de los entornos Wi-Fi, pero enfocadas específicamente en la seguridad.

Las redes inalámbricas funcionan en modos predefinidos que tienen un propósito específico, pero también disponen de estrictas restricciones funcionales. A través de Aircrack se pueden configurar ataques inalámbricos, por lo que se requiere un mayor control sobre las capas inferiores de comunicación de la trama (según estructura del protocolo) para poder enviar y recibir cualquier tipo de datos. En este sentido, la inyección de paquetes significa enviar datos en modo monitor, ya que representa el funcionamiento pasivo del dispositivo.

Algunas de las tareas que permite realizar son las siguientes:

- supervisión y monitoreo, se trata de la captura de paquetes y exportación de datos a archivos de texto para su posterior procesamiento a través de software de terceros como Wireshark;
- ataques, mediante acciones de repetición, desautenticación, puntos de accesos falsos y otros métodos, a través de la inyección de paquetes;
- pruebas, comprobación de los modos de funcionamiento de las tarjetas y adaptadores inalámbricos, potenciando las capacidades de sus controladores y drivers (captura e inyección);
- hackeo de claves de acceso WEP y WPA PSK.

Hay algunas aplicaciones GUI que aprovechan estas características para facilitar la tarea de forma más intuitiva. Sparrow-WiFi y Kismet son algunas de ellas.

Jupyter Notebook[8]

Es una aplicación cliente-servidor que permite crear y compartir documentos en formato JSON que siguen un esquema versionado y una lista ordenada de celdas de entrada y salida. En estas celdas se introduce cualquier tipo de código, texto, fórmulas matemáticas y ecuaciones, o también contenido multimedia. El programa se ejecuta desde la aplicación web cliente que funciona en cualquier navegador estándar. Es necesaria la instalación y ejecución del servidor Jupyter Notebook en el sistema para que funcione correctamente. Los documentos creados

[7]Extraído de la web oficial https://www.aircrack-ng.org/ ell día 18 de enero de 2022.
[8]Extraído de la web oficial https://docs.jupyter.org/en/latest/ el día 16 de enero de 2022.

se exportan en formato HTML, Markdown o Python, y también permite compartir con otros usuarios por correo electrónico, DropBox o GitHub o a través del visor integrado de Jupyter Notebook.

Este tipo de aplicación se utilizará en la fase de análisis de datos, para generar resultados en forma de imágenes que reflejen el trabajo de las mediciones realizadas en campo.

Una vez recopilados los datos por Kismet o Wireshark, se exportan como archivo csv e importan en Jupyter Notebook. La ventaja de esto es que se extraen rápidamente los datos de las capturas generadas con los Sniffers utilizando la biblioteca Pandas de Python y se generan fácilmente gráficos y tablas para mostrar las relaciones.

3.3 Dispositivos de Hardware

En esta sección se presentará una breve descripción de todos los dispositivos de hardware disponibles y adquiridos, para cumplir con el propósito de interceptar las señales inalámbricas 802.11.

Tarjeta Inalámbrica Intel Wireless 8260[9]

Tarjeta inalámbrica interna de banda Dual 2,4 y 5 GHz con antenas incorporadas TX/RX 2×2, que trabaja a una velocidad máxima de transmisión de 867 Mbps. Compatible con Windows 10 64-bit y Linux. Dispone de certificación Wi-Fi 802.11ac. Esta interfaz fue el primer modelo de prueba para preparar los esquemas de configuración para la puesta a punto de la mayoría de los programas en Linux.

Adaptador Externo USB Netgear A6200

Dispositivo externo con puerto USB. Trabaja en las dos bandas de frecuencias 2,4 y 5 GHz y admite los estándares 802.11a, b, g, n y ac. La transmisión y recepción de los datos se logra con 2 antenas LDS (acrónimo de *Laser Direct Structuring*[10]) logrando velocidades de 866 Mbps en 802.11ac y 300 Mbps en 802.11n. Este hardware se adquirió de acuerdo a los requisitos de compatibilidad del software Acrylic Wi-Fi Professional para funcionar de manera distinta al *modo nativo* (término definido en la Sección 3.4) por defecto y permitir la captura de tráfico inalámbrico en modo monitor. Este modelo de adaptador figura dentro de la lista de dispositivos compatibles con el software en modo monitor y no depende de otras capacidades de integración o extensiones de software bajo licencia, como por ejemplo Acrylic Wi-Fi Sniffer[11].

[9]Extraído de la web oficial https://ark.intel.com/content/www/es/es/ark/products/86068/intel-dual-band-wirelessac-8260.html el día 18 de enero de 2022.

[10]LDS es una tecnología que crea dispositivos de interconexión tridimensional (3D-MID) tomando un componente de moldeado de inyección de plástico e integrando un trazado de circuito en la superficie a lo largo del contorno del componente.

[11]Información disponible en web oficial https://www.acrylicwifi.com/programas-software-herramientas-wifi/sniffer-wifi-para-windows/.

Adaptador USB CPE 600D[12]

Este dispositivo es una placa USB inalámbrica de alta potencia que admite los estándares a/b/g/n/ac y trabaja en las frecuencias de 2,4 y 5,8 GHz. La transmisión de los datos se logra con su antena direccional de 12 dBi de ganancia. Tiene una velocidad de transferencia de 150 Mbps en 2,4 GHz y 433 Mbps en 5,8 GHz.

Actualmente hay dos fabricantes de chipsets Wi-Fi USB en actividad: **Mediatek** (antiguamente llamadado Ralink) y **Realtek**. Este adaptador tiene integrado un chipset único WiFi Ralink RTL8811CU, que cumple con los estándares IEEE 802.11ac ofreciendo una conectividad inalámbrica estable. Cuenta con una arquitectura optimizada de RF y algoritmos de banda base que proporcionan un alto rendimiento con un bajo consumo.

Mediatek implementa drivers a medida para el kernel de Linux, motivo por el cual, la mayoría de los controladores están incluidos en el núcleo del sistema operativo GNU-Linux y las actualizaciones son automáticas. Sin embargo, no siempre funcionan los dispositivos inalámbricos en su primera conexión con la computadora, como es el caso de este adaptador.

Adaptador USB TP-LINK AC1900 Archer T9UH[13]

Adaptador externo USB de Dual Band que funciona en 2,4 y 5 GHz. En su placa tiene integradas antenas, conformando un sistema MiMo (acrónimo de *Multiple In Multiple Out*) de 4×4, que permite realizar beamforming inteligente de alta directividad y ganancia.

Figura 3.5: Especificaciones técnicas del Adaptador externo USB TP-LINK AC1900 ARCHER T9UH.

Fuente: https://www.tp-link.com/ar/home-networking/adapter/archer-t9uh/specifications/.

Admite los estándares IEEE 802.11ac/n/a en 5 GHz e IEEE 802.11b/g/n en 2,4 GHz. La tasa de transmisión es de 1300 Mbps a 5 GHz y 600 Mbps en 2,4 GHz. Admite tres modos

[12]Extraído de web oficial https://nisuta.com/producto/NSWIUCPE600D el día 18 de enero 2022.

[13]Extraído de la web oficial https://www.tp-link.com/es/home-networking/adapter/archer-t9uh/ el día 19 de enero de 2022.

de funcionamiento: Ad-Hoc, Infraestructura y Monitor. Soporta encriptación 64/128 bit WEP, WPA-PSK/WPA2-PSK, 802.1x y la tecnología de modulación DBPSK, DQPSK, CCK, BPSK, QPSK, 16-QAM, 64-QAM Y 256-QAM. En la Figura 3.5 se muestran las características técnicas del dispositivo.

Ubiquiti NanoStation airMAX Loco M5 CPE Wireless

Este recurso que integra hardware y software, representa una solución para desarrollar enlaces Punto a Punto o Punto Multipunto inalámbricamente y transportar contenido IP como datos, vídeo, voz, telemetría, etc.

Cuenta con un microprocesador Atheros MIPS 24KC de 400 Mhz, y una memoria de 64 MB SDRAM y 8 MB Flash. Dispone de un puerto Ethernet 10/100 Base-TX (Cat. 5, RJ-45). Su consumo es de 5.5 Watts y se alimenta por tecnología PoE (acrónimo de *Power over Ethernet*).

La antena tiene una ganancia direccional de 13 dBi y trabaja con polarización horizontal o vertical. Posee implementada la tecnología APP (*Adaptive Antenna Polarity*, Polarización de Antena Adaptativa) que selecciona automáticamente la polarización de la antena. También integra la tecnología *Inner Feed*, un sistema que integra el cabezal de radiofrecuencia a la entrada de la antena, lo que evita utilizar cables en RF y elimina las pérdidas que éstos producen. Para optimizar el uso del espectro de radiofrecuencia utiliza airMax, un protocolo propietario que utiliza la transmisión TDMA (Acceso Múltiple por División de Tiempo). Esto permite a cada cliente enviar y recibir datos mediante tiempos pre-asignados programados por un punto de acceso inteligente.

Además, integra otras funciones como airSelect para optimizar las colisiones de los nodos y maximizar la eficiencia del tiempo de aire.

Smartphone Samsung Galaxy S10

Teléfono inteligente de última generación con sistema operativo Android 11. Este equipo tiene integrado un receptor para señales GPS que será útil, en conexión con la computadora que realizará las mediciones mediante puerto USB, para localizar las señales WLAN/RLAN. Para configurar al teléfono inteligente como receptor del GPS y compartir los datos se necesita de la aplicación Share GPS disponible para su descarga en Google Play Store. El trabajo de localización lo realiza el chip Skyworks SKY78160-5, que recibe las señales de los satélites A-GPS, Glonass, Beidou y Galileo.

Tablet Samsung Galaxy S7

Equipo de última generación con sistema operativo Android. Al igual que el teléfono inteligente presentado anteriormente, este dispositivo se utilizará como alternativa para extraer sus datos del GPS mediante la aplicación Share GPS.

Batería Recargable 12V/7A

Batería de Gel 12 V 7 Ah recargable necesaria para alimentar el nodo Ubiquiti NanoStation airMAX Loco M5 (configurado como AP) cuando se aplica el método War-Driving.

3.4 Selección de recursos

En esta sección se establecen los criterios claves que delimitaron la selección de cada una de las alternativas de software, hardware, recursos y/o herramientas para iniciar las configuraciones previas y pruebas necesarias para el proceso de medición.

Teniendo en cuenta el objetivo específico de localizar las señales interferentes, estas pruebas iniciales definirán una hoja de ruta que luego será implementada en varias mediciones en el contexto donde se desenvuelve el radar RMA-1.

Inicialmente, el uso del software Acrylic Wi-Fi Professional en plataforma Windows sirvió de gran ayuda para dar cuenta de la integración de herramientas y funciones para identificar dispositivos inalámbricos en distintos escenarios. Con el fin de analizar el espectro radioeléctrico para localizar puntos de acceso y fuentes WLAN/RLAN, es necesaria la integración de dispositivos de hardware externo y otras aplicaciones que trabajan en plataformas distintas para sniffear el tráfico de la red. En este aspecto, es menester el despliegue en paralelo de dos computadores portátiles, cada una con sistemas operativos diferentes: Windows 10 y Ubuntu Linux.

Acrylic Wi-Fi Professional es un gran software con una potencialidad enorme, que se ve limitado al ser ejecutado en Windows. Se realizaron pruebas con dos adaptadores inalámbricos: la placa Wi-Fi interna con antenas 2×2 TX/RX (Intel Wireless 8260) y el adaptador inalámbrico externo USB Nisuta CPE 600D con antena integrada de gran directividad y ganancia de 12 dBi. Las pruebas con el segundo adaptador brindaron un espectro de frecuencia más detallado, debido a su gran ganancia de antena y potencia TX.

Las tarjetas de redes inalámbricas, al igual que los adaptadores externos, tienen tres modos de funcionamiento. El primero de ellos, y el más habitual, es el modo ***Nativo*** o ***Infraestructura***. Este modo es el utilizado para conectar los distintos dispositivos a una red inalámbrica. El otro modo es el denominado ***Ad-Hoc***, que es utilizado para conectar dos equipos inalámbricamente sin la necesidad de un punto de acceso inalámbrico como intermediario. El tercero, es el modo ***Monitor***, en el cual la tarjeta/adaptador "escucha" la interfaz de aire con el fin de identificar las comunicaciones inalámbricas que estén bajo su radio de cobertura. Tiene un funcionamiento similar al modo promiscuo utilizado en las redes cableadas. En el Anexo A.1.1 se detallan minuciosamente las características del modo Monitor y su habilitación en Linux.

En el caso de Acrylic Wi-Fi Professional, el modo Monitor (modo promiscuo o modo escucha) y el modo Nativo o normal son las dos formas de captura de datos soportados. Para habilitar el modo Monitor en el programa, es necesario instalar el driver NDIS de un adaptador compatible sin necesidad de software adicional (según lista de tarjetas compatibles[14]) utilizando el adaptador USB Netgear A6200, o accediendo a software complementario como Acrylic Wi-Fi Sniffer, como es el caso del adaptador inalámbrico externo USB TP-LINK AC1900 Archer

[14]Hardware de captura en modo monitor desde web oficial https://www.acrylicwifi.com/programas-software-herramientas-wifi/analizador-wifi-acrylic-wifi-profesional/requisitos-y-compatibilidad/.

T9UH.

De acuerdo a lo descrito párrafos atrás en cuanto a las limitaciones del software, no fue posible realizar las pruebas con este adaptador, debido que es requisito necesario la adquisición de licencia del software complementario. Esta limitación truncó la continuidad en el uso del software.

Otra cuestión es la limitación del hardware compatible. El adaptador Netgear A6200 no trabaja en todos los canales de la banda de frecuencia de 5 GHz. Esto quiere decir que no registra en su firmware los canales habilitados y DFS de la banda. Un aspecto importante para tener en cuenta en las mediciones de campo.

Para finalizar la descripción, en la Figura 3.6 se presenta un cuadro comparativo entre los modos nativo y monitor para este software.

MODOS DE FUNCIONAMIENTO		INFORMACIÓN DISPONIBLE DE LA CAPTURA
NATIVO	Es compatible con cualquier tarjeta WiFi del mercado en modo de captura nativa o modo normal. Cuando se realiza una monitorización en modo de captura nativa, la tarjeta WiFi se comporta como un adaptador WiFi estándar. La tarjeta, utilizando los mecanismos nativos de Windows, captura solo un tipo específico de paquetes, concretamente paquetes Beacon, que son los originados por los puntos de acceso. Estos paquetes son emitidos múltiples veces por segundo por los puntos de acceso para indicar qué red o redes están disponibles en ese momento. Las herramientas de Acrylic Wi-Fi analizan e interpretan estos paquetes, mostrando la información que contienen y almacenándola en ficheros pcap o en el proyecto en curso. Para realizar una captura de datos nativa, no se requiere de ningún hardware especial, basta con disponer de una tarjeta wifi integrada o usb.	• SSID. • Direcciones MAC. • Intensidad de señal. • Canales. • Ancho de banda. • IEEE 802.11. • Tasa máxima de envío de paquetes. • Tipo de encriptación (WEP, WPA, WPA2, WPS, WPS PIN). • Contraseña. • Fabricante. • Primera detección del AP. • Tipo de conexión que se ha establecido.
MONITOR	El modo monitor es el modo de captura de datos que permite hacer uso de la tarjeta WiFi en modo *escucha* o modo *promiscuo*. En este modo la tarjeta es capaz de capturar todos los tipos de paquetes WiFi, Management (incluidos los *Beacon*), Data y Control. De esta manera, es posible visualizar no solo los puntos de acceso sino también los clientes que están emitiendo dentro de las bandas de frecuencia WiFi. Existen 3 formas de activarlo: • Mediante **Acrylic Wi-Fi Sniffer:** permite la captura en modo monitor de una manera sencilla y debido a que fue diseñado para ser una alternativa fácil de usar y económica para la captura en modo monitor en Windows, puede recuperar todos los datos disponibles incluyendo información sobre los valores SNR (Signal-to-Noise Ratio). • A través del driver NDIS: está incluido en los productos de Acrylic Wi-Fi y permite la captura en modo monitor para 802.11a/b/g/n (anchos de canal de 20MHz), para activar el modo de captura monitor es necesario disponer de una tarjeta compatible e instalar el driver, lo cual se puede hacer desde la propia aplicación de Acrylic WiFi entrando en el menú, pulsando "change" en el selector de interfaz WiFi y pulsando el botón "Install NDIS Driver". • Por tarjeta AirPCAP: se utiliza un hardware específico de análisis Wi-Fi, tales como las tarjetas AirPcap, desarrolladas por Riverbed. Este tipo de tarjetas actualmente se encuentran descatalogadas y no soportan los nuevos estándares 802.11ac/ax. Soportan captura nativa y modo monitor. Si realizamos una captura en modo monitor con una tarjeta AirPcap, podremos visualizar, además de todos los datos disponibles con una captura en modo monitor empleando una tarjeta compatible con el driver de NDIS, información sobre los valores SNR (Signal-to-Noise Ratio).	Realizando una captura de datos en modo monitor, Acrylic Wi-Fi Professional ofrece, además de toda la información disponible con la captura en modo normal, información sobre: • Dispositivos clientes conectados a los diferentes puntos de acceso. • Reintento de envío de paquetes (Retries). • Paquetes de datos (Data). • Paquetes tipo Management (Mgt). • Latitud y longitud (mediante conexión con dispositivo GPS).

Figura 3.6: Cuadro comparativo entre los modos nativo y monitor en Acrylic Wi-Fi Professional.

Fuente: https://www.acrylicwifi.com/blog/modo-monitor-wifi/.

Por las razones enunciadas anteriormente, el software Acrylic Wi-Fi Professional se descartó para las mediciones de campo. En plataforma Linux, existe una herramienta similar a Acrylic llamada Sparrow Wi-Fi. Sus características y funcionalidades son muy parecidas. El modo Nativo es compatible con la mayoría de las tarjetas inalámbricas y puede anexarse la señal de GPS para localizar señales WLAN/RLAN de forma aproximada. Es compatible con el modo Monitor haciendo uso de un subprograma que se ejecuta en segundo plano llamado Aircrack. Al igual que Acrylic, este programa cumple bien su función en un nivel local, observando el despliegue de las redes inalámbricas en el espectro radioeléctrico. En cuanto a aspectos negativos, por un lado, la captura en modo Monitor no siempre funciona con algunos modelos de adaptadores Wi-Fi externos, lo que signifca utilizar siempre el mismo método de

habilitación para todas las tarjetas con Aircrack; y por otro, la información disponible es muy acotada cuando se realizan las capturas en este modo. Por estas razones, también se descartó su aplicación en las mediciones.

Las prácticas con Acrylic Wi-Fi Professional y Sparrow Wi-Fi permitieron acceder a una amplia gama de posibilidades que abarca desde la estructura de datos, con la organización y categorización de información detallada, hasta aspectos técnicos-funcionales para el desarrollo de habilidades y destrezas con ciertas herramientas y aplicaciones con características potenciales.

A partir del análisis realizado, se propone trabajar con funcionalidades por separado, de forma aislada, y luego integrar todo en una etapa posterior de procesamiento. Con este propósito se seleccionaron las herramientas y aplicaciones que se enumeran en el cuadro de la Figura 3.7, y se dió inicio a una serie de ensayos previos a las mediciones *in-situ*.

Figura 3.7: Recursos seleccionados para iniciar las prácticas previas a las mediciones en campo.

Una vez establecidos los parámetros definitivos que constituyan un patrón o indicador formal, estas actividades se trasladarán a un nivel más complejo como lo es el entorno radar. Este escenario está compuesto por parámetros aleatorios y complejos que varían con el terreno, la densidad urbana, obstáculos, contaminación del espectro radioeléctrico, reflexiones, y otros índices que perjudican los productos radar.

En la búsqueda de este patrón, se necesita de una convivencia de sistemas en paralelo. Para un buen desempeño es requisito, por un lado, un equipo portátil con sistema operativo Windows para ejecutar:

- airView, es una especie de analizador de espectro en tiempo real embebido en el sistema operativo airOS del AP Ubiquiti NanoStation airMAX Loco M5 HP. También se necesitarán de otras funcionalidades como Site Survey para realizar un barrido rápido del espectro electromagnético y visualizar los canales ocupados con tráfico en la banda de frecuencia de 5 GHz;
- Google Earth, para generar referencias de las distintas señales interferentes, según su acimut, utilizando navegación en 2D/3D y Google Street View con imágenes actualizadas que sirvan de soporte para calibrar la ubicación de puntos de interés;
- RadioMobile, para la generación de los perfiles topográficos de los puntos de interés, siendo el otro extremo el sensor radar, utilizando mapas descargados de internet desde bases de datos actualizadas. Esto permitirá un análisis más detallado de la ubicación de la interferencia en referencia a su altura sobre el nivel del mar comparada con la posición del radar.

Por otro lado, se necesita de una computadora portátil funcionando con Ubuntu Linux equipada con las siguientes características:

- captura de tráfico WLAN/RLAN mediante la interfaz inalámbrica TP-LINK AC1900 Archer T9UH en modo Monitor activado;
- conexión con señal GPS por puerto USB provista por smartphone Samsung Galaxy S10 a través de la aplicación Android Share GPS ejecutada en el móvil;
- suite Aircrack para activar el modo Monitor en la interfase inalámbrica TP-LINK;
- Kismet y Wireshark, programas sniffer para la captura de paquetes y tramas que circulan por la interfaz de aire de los distintos puntos de acceso y redes inalámbricas.

En la Figura 3.8 se presenta una imagen que refleja la convivencia de los tres sistemas de acuerdo a la selección de los recursos. Esto se explica con más detalle en Capítulo 4.

Figura 3.8: Desempeño de equipos en paralelo para la integración de los datos.

3.5 Experiencia en plataforma Linux Ubuntu

El proceso de familiarización con un sistema operativo Linux no es tan fácil debido a que es de código abierto, por lo que hay variaciones entre las distribuciones y se vuelve imposible generar una guía práctica que involucre a todas. La mayoría de los controladores son también de código abierto e integrados al sistema, y cada distribución emplea un proceso distinto de instalación. La mayor dificultad fue la obtención de los drivers y controladores de los dispositivos de hardware, lo que implica la compilación de los mismos de acuerdo a las necesidades. Con respecto a esto, las políticas de licencia varían entre las diferentes distribuciones de Linux, y en el caso de Ubuntu, solicita a los usuarios que eviten el uso de hardware patentado o cerrado.

Sin embargo, la ventaja frente a Windows es que la mayoría de las tarjetas y adaptadores inalámbricos son compatibles para trabajar en modo Monitor y no dependen de licencias de aplicaciones adicionales por su naturaleza de software libre y de código abierto. Por esta razón, la captura de datos y tráfico inalámbrico se realizará con este sistema operativo.

3.5.1 Instalación del adaptador inalámbrico USB

El adaptador seleccionado para realizar la captura de paquetes y la inyección de datos de forma pasiva es el dispositivo de hardware TP-LINK AC1900 Archer T9UH.

Desde la web oficial, la versión más reciente del controlador (T9UH Archer ver 2.0) es compatible con el entorno Windows 10. Por esta razón, el trabajo consistió en conseguir una versión compatible con el último kernel de Ubuntu.

Cabe remarcar que la última versión del adaptador fue discontinuada por el fabricante debido a un cambio en el chipset RTL8814AU[15] y no hay diferencias notables desde el punto de vista funcional del adaptador entre sus dos versiones del controlador. El adaptador funciona perfectamente en Linux.

3.5.2 Receptor de GPS

Las aplicaciones para un receptor externo de señales GPS son muy variadas de acuerdo a las actividades que se desean realizar y a las funcionalidades. Para este trabajo, el uso del mismo es necesario para compilar una lista de puntos de acceso Wi-Fi con sus coordenadas aproximadas con un mínimo margen de error. El costo de adquisición de este dispositivo excede el presupuesto disponible para llevar a cabo el presente proyecto, por lo que se optó por la alternativa económica de utilizar un receptor de GPS incorporado en el teléfono inteligente provisto de Android.

En esta sección, se explicará cómo transferir en tiempo real las coordenadas GPS desde el teléfono a la computadora portátil con Linux Ubuntu, empleando el protocolo NMEA-0183.

[15] Web oficial https://www.realtek.com/en/products/communications-network-ics/item/rtl8814au consultada el día 20 de enero de 2022

Estándar NMEA-0183

El estándar NMEA-0183, desarrollado por National Marine Electronics Association, define los requisitos eléctricos de señalización, protocolo de transmisión de datos y formatos de sentencias específicas para una transmisión con comunicación serial a una velocidad de 4800 baudios. Esta norma soporta transmisión en un solo sentido desde un único emisor a uno o varios receptores. Los datos transmitidos están codificados en formato ASCII de 7 bits y cada línea es una sentencia que sigue un formato bien definido compuesto por campos separados por comas, los cuales identifican el tipo de información contenida como la posición, la velocidad, la profundidad, entre otros.

Algunas de las sentencias NMEA comunes son las siguientes:

- $GPALM, datos GPS de almanaque;
- $GPGGA, tiempo posición y tipo de data fija;
- $GPGGL, latitud, longitud, hora UTC y posición fija y estado;
- $GPGRS, rangos residuales GPS;
- $GPGSA, GPS DOP (Dilución de la precisión) y satélites activos;
- $GPGST, estadística pseudorango GPS;
- $GPGSV, número de satélites GPS a la vista, elevación, azimut y valores SNR;
- $GPMSS, radio señal a ruido, potencia de señal, frecuencia. Estado de señal guía receptora;
- $GPRMC, data de tiempo, fecha, posición, curso y velocidad. Datos mínimos recomendados;
- $GPVTG, curso sobre Tierra y velocidad de recorrido relativo a la Tierra;
- $GPZDA, mensaje de Timing PPS (Sincronizado a PPS) Tiempo y fecha;
- $PTNL,GGK, tiempo, posición y valores DOP.

La aplicación Share GPS puede enviar las sentencias NMEA desde el móvil a otros dispositivos a través de un método de conexión como Bluetooth, USB o protocolo TCP/IP por red. La forma más fácil es a través de la red utilizando Wi-Fi o comunicaciones móviles 3G/4G. Cabe aclarar que, las conexiones Bluetooth y USB, siendo esta última la que se utilizará en este trabajo, requieren de una configuración adicional. El móvil deberá tener instalada la aplicación Android Share GPS en su sistema para proporcionar continuamente tramas NMEA, y por tanto, utilizar los datos de ubicación geográfica en tiempo real.

La conexión USB requiere que el móvil Android tenga habilitadas las “Opciones de desarrollador” y activar el “Modo de depuración por USB” para enviar datos NMEA. La

computadora portátil necesita previamente de la instalación de un complemento denominado ADB (Puente de depuración Android). La herramienta ADB se encargará de redirigir los datos NMEA a un puerto TCP en la computadora para ser usado por un programa generador de mapas como Google Earth o, en este caso, ayudar a la localización estimada de los puntos de acceso cuando se capture, en paralelo por un programa sniffer, tráfico inalámbrico en modo Monitor.

Datos GPS en Kismet

El programa Kismet puede integrarse con un receptor de GPS para proporcionar coordenadas de geolocalización y mapear los dispositivos[16].

Kismet puede funcionar con varias fuentes GPS, incluso directamente de receptores GPS o recibiendo datos a través de la red.

Tipos de fuentes de información del GPS:

- serie, recepción de datos por dispositivo serie;
- TCP/IP, recepción de datos directamente de la red IP;
- GPSD, leer datos del servicio GPSD;
- virtual, un GPS virtual siempre informa una ubicación estática. Inyecta datos de ubicación a un sensor estacionario, como por ejemplo, un drone.

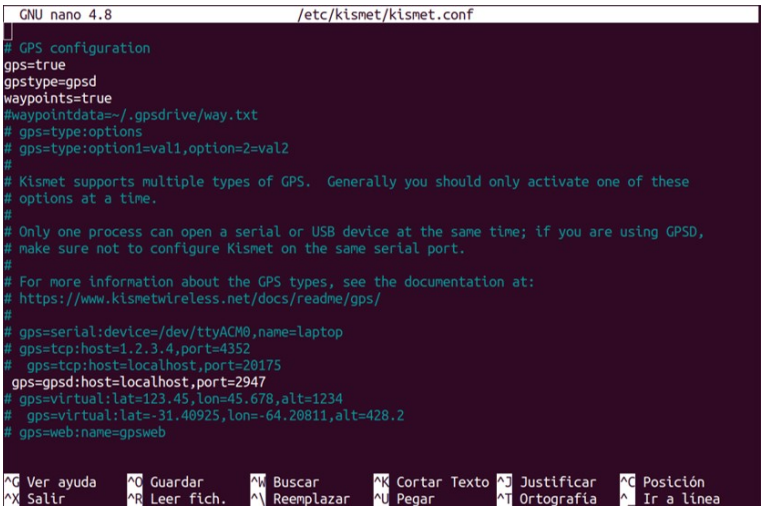


Figura 3.9: Parámetros de configuración GPS.

Para configurar estos datos es necesario ingresar al archivo de configuración del programa. El comando a utilizar es el siguiente:

```
$sudo nano /etc/kismet/kismet.conf
```

[16]Referencia en https://www.kismetwireless.net/docs/readme/gps/

En este fichero figuran todos los parámetros necesarios para que las funciones y servicios se carguen cuando se ejecuta el software. Especialmente, la sección donde se ubican las opciones de configuración GPS.

En la configuración GPS, es necesaria la activación de la línea:

```
gps=gpsd:host=localhost,port=2947
```

Esto corresponde a escuchar el puerto 2947 del servicio GPSD para leer los datos de ubicación y mostrar los mismos en su interfaz web para la geolocalización de los puntos de acceso. En la Figura 3.9 se observan los parámetros vinculados con el sistema GPS.

3.6 Ensayos iniciales en el laboratorio

La primeras pruebas se encuentran/son acotadas a un contexto local para preparar y configurar el hardware y software seleccionado y, con el propósito de conformar una base y extender su alcance a mediciones en campo en un escenario más complejo y abierto, evaluar el desempeño y rendimiento de los recursos.

El primer escenario de estudio se delimita a realizar una actividad denominada "Fase de Descubrimiento" (*Discovery Phase* en inglés) de una red inalámbrica. Este es el primer paso que ejecuta cualquier cliente Wi-Fi en un proceso de conexión a una red WLAN/RLAN. A través de este proceso, el dispositivo cliente realiza un escaneo para buscar redes inalámbricas activas e identifica algunos parámetros de esas redes, incluyendo el nombre lógico denominado SSID, tasa de datos soportadas, frecuencia o canal de operación, configuraciones de seguridad y otros parámetros adicionales.

3.6.1 Inspección de la Trama Beacon

Las tramas Beacons anuncian la existencia de sistemas WLAN/RLAN y son muy importantes para realizar tareas de mantenimiento en la red. Se transmiten a intervalos regulares para que las estaciones clientes o móviles que se encuentran en cercanía de la red WLAN puedan enterarse de su existencia, identificar a la misma y conocer sus parámetros necesarios para asociarse a ella. En redes de Infraestructura, el AP es el encargado de transmitir estas tramas Beacons, quedando el parámetro BSS, de su cabecera MAC, definido por el área mediante la cual estas tramas pueden recibirse. El intervalo de tiempo en el que se emiten estas tramas, dependiendo del modelo del AP, puede ser configurable y puede variar de acuerdo a ciertos requerimientos o conveniencia.

A modo de prueba, y tomando en consideración lo desarrollado en el Capítulo 2 respecto a este tema, se realizará un análisis más detallado de la comunicación entre el cliente y el AP en esta fase de descubrimiento a través de la inspección directa de las tramas de gestión (Beacon, Probe Request y Probe Response) que intercambian estos dispositivos.

En primer lugar, se presenta la configuración inalámbrica del router AP modelo Sagemcom Fast3686 que se utilizará como referencia para después comparar con el contenido de las tramas

de gestión y su actividad en el espectro radioeléctrico cuando transmite la señal Wi-Fi por la interfaz de aire.

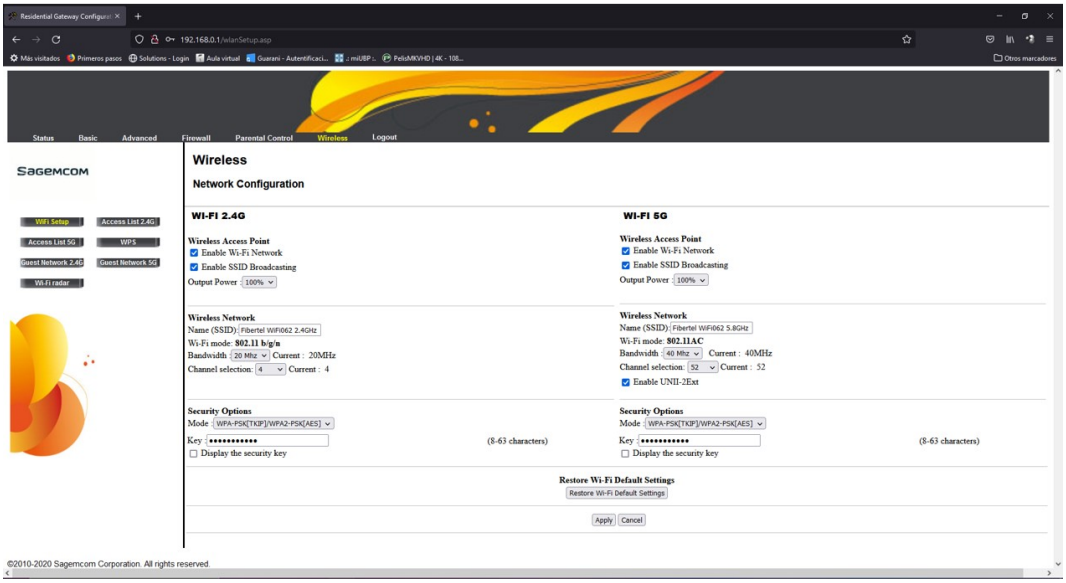


Figura 3.10: Configuración del router AP.

En la figura 3.10 se muestra que el AP trabaja de forma dual en las frecuencias de 2,4 y 5,8 GHz, siendo la última la porción de interés del espectro radioeléctrico ya que el radar funciona en esa banda. El AP trabaja específicamente en el canal 52 (5.260 MHz) ocupando un ancho de banda de 40 MHz. También puede visualizarse la propagación del SSID “Fibertel WiFi062 5.8 Ghz” y la norma predominante de acuerdo al estándar 802.11ac.

Para observar y analizar detalladamente la transmisión del AP en función del tiempo y la frecuencia se necesita un analizador de espectro. En este sentido, se recurre a la configuración del dispositivo Ubiquiti NanoStation airMAX Loco M5 HP en modo AP como soporte para utilizar su función de analizador de espectro denominada “airView”. En entorno Windows, se ingresa por Ethernet a la máquina cliente para acceder a la interfaz web de configuración del dispositivo Ubiquiti para habilitar airView.

En la Figura 3.11 se muestra la actividad del router AP transmitiendo datos de forma constante, según el código de colores de la potencia en dBm. Al momento de la captura, uno de los clientes conectados al router demandaba el servicio de streaming y, de acuerdo a las vistas, se observa la ocupación del ancho de banda para su transmisión y la fluctuación de la potencia de la señal en tiempo real en el canal 52 (5.260 MHz). La pantalla de inicio del analizador se divide en tres opciones de análisis:

- gráfico de cascada (**Waterfall view**), basado en el tiempo que muestra las transmisiones en forma de energía en cada frecuencia. El color señala la amplitud, siendo los colores fríos los niveles más bajo de energía o potencia en los canales, mientras que los más cálidos (amarillo, naranja y rojo) significan mayor potencia o actividad de transmisión;
- gráfico de forma de onda (**Waveform view**), basado en el tiempo que muestra la energía

de la señal en cada frecuencia. Las referencias de colores son similares al gráfico en cascada. En esta vista se muestra también el estado actual de la actividad de RF que hay alrededor;

- gráfico en tiempo real (**Real time view**), muestra un analizador de espectro tradicional que mide la potencia (en valores dBm) en función de la frecuencia.

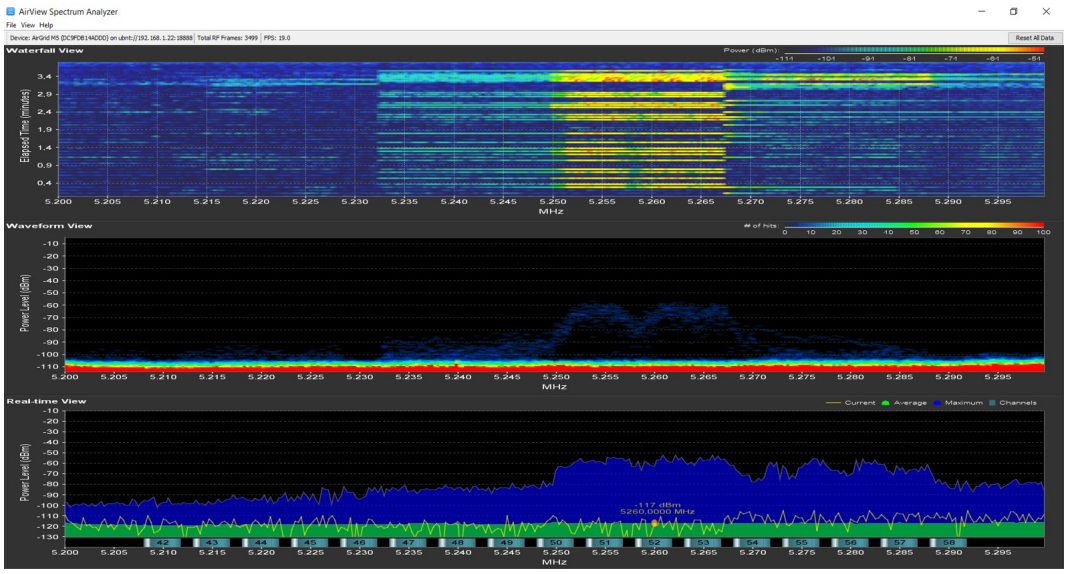


Figura 3.11: Actividad del router AP desde el punto de vista del espectro radioeléctrico.

Lo siguiente es configurar el sistema GPS y vincular la computadora (servicio GPSD) con el teléfono (aplicación Share GPS) para compartir las tramas NMEA por el puerto USB. En la Figura 3.12 se presenta la pantalla de inicio de la aplicación Share GPS con los datos GPS y también la lista de los distintos satélites en xgps con la señal de los sistemas GPS, Glonass, BeiDou y Galileo.

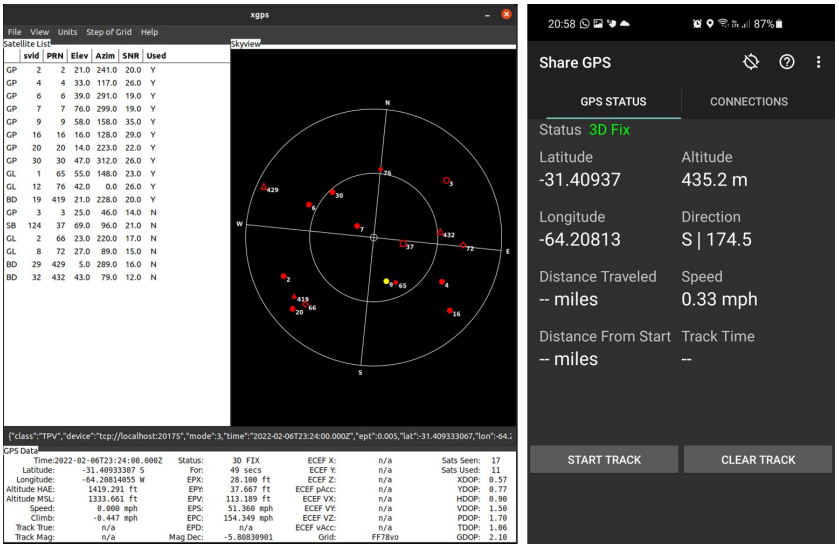


Figura 3.12: Configuración de Share GPS y GPSD.

Asimismo, en la Figura 3.13 se muestra el flujo de datos GPS en los servicios gpsmon y cgps -s. Esto corresponde a las tramas NMEA enviadas por el teléfono y presentadas en distintos formatos. El servicio GPSD escucha las tramas del puerto del teléfono y las replica en el puerto tcp://localhost:2947. Esto se analiza con más detalle en la Sección Anexos.

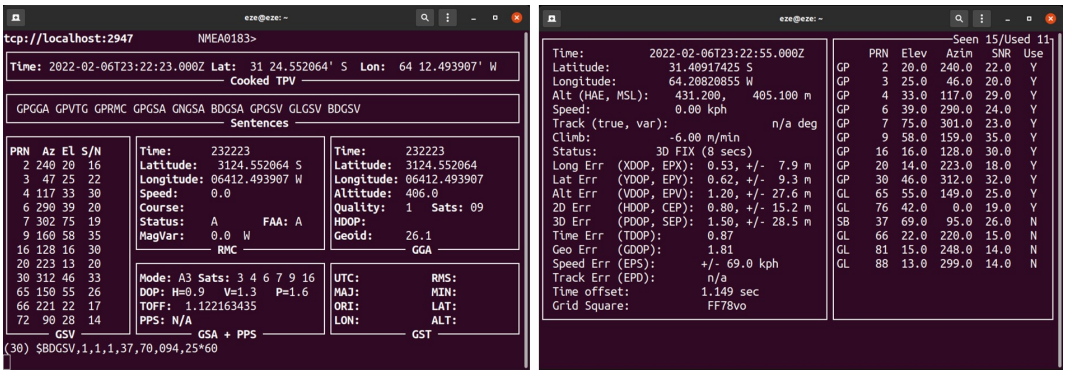


Figura 3.13: Flujo de datos NMEA para ser utlizados por una máquina cliente.

Acto seguido, se inicia la captura de datos y todo tipo de paquetes inalámbricos como tramas Gestión (incluidos los Beacons), Datos y Control. Para una mejor visualización de los datos se ejecuta la interfaz web del programa Kismet en el puerto 2501.

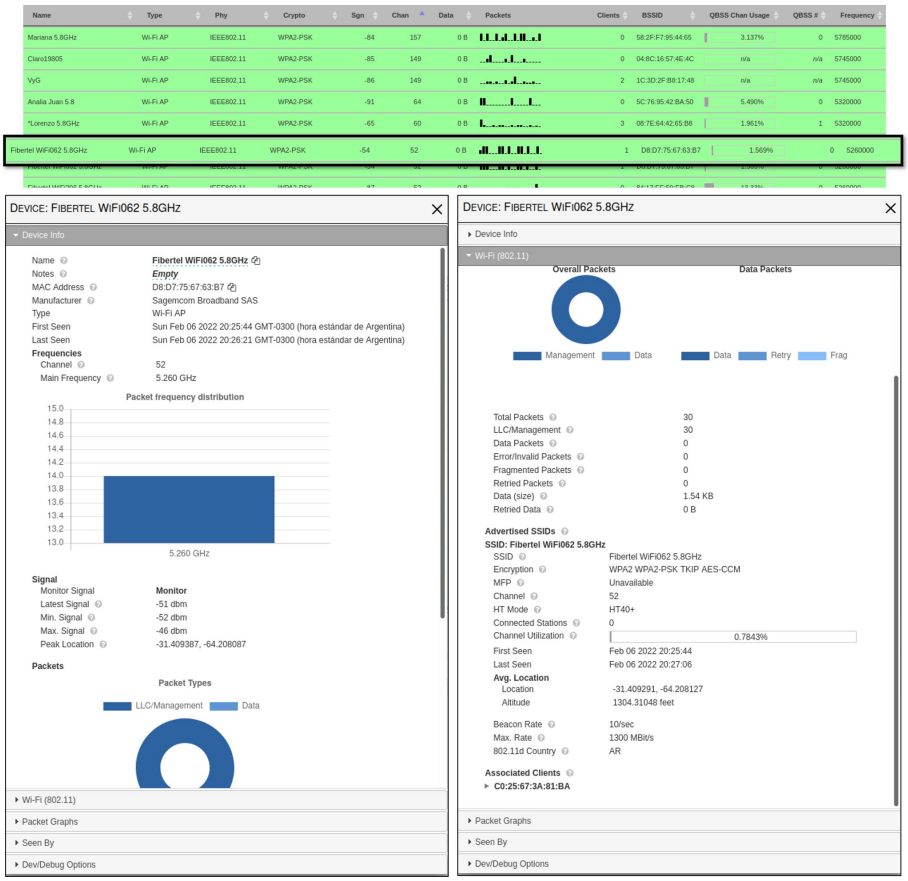


Figura 3.14: Información específica del router de interés.

Kismet presenta rápidamente las redes descubiertas y permite inspeccionar los principales

parámetros de configuración. A modo de comparación con la Figura 3.10 se identifica el SSID "Fibertel WiFi062 5.8Ghz" que es el router AP de prueba a nivel local. Con sólo hacer click en el dispositivo de interés que figura en la lista se abren nuevas ventanas con información específica como: nombre lógico SSID, dirección MAC, fabricante, canal y frecuencia de trabajo, ubicación GPS estimada de la señal inalámbrica según potencia recibida del AP (localización promedio), clientes conectados, total de paquetes capturados, parámetros de seguridad y encriptación, ancho de banda, porcentaje de utilización del canal al momento de la captura, etc.

A partir de un análisis rápido, se observa que los datos coinciden de acuerdo a la configuración del AP y a su actividad en tiempo real en función de la frecuencia.

Para un examen más detallado del tráfico inalámbrico, se realiza una inspección directa por auditoría de red. Por este motivo, se emplea el programa Wireshark para visualizar la comunicación entre el AP y el cliente mediante las tramas de gestión.

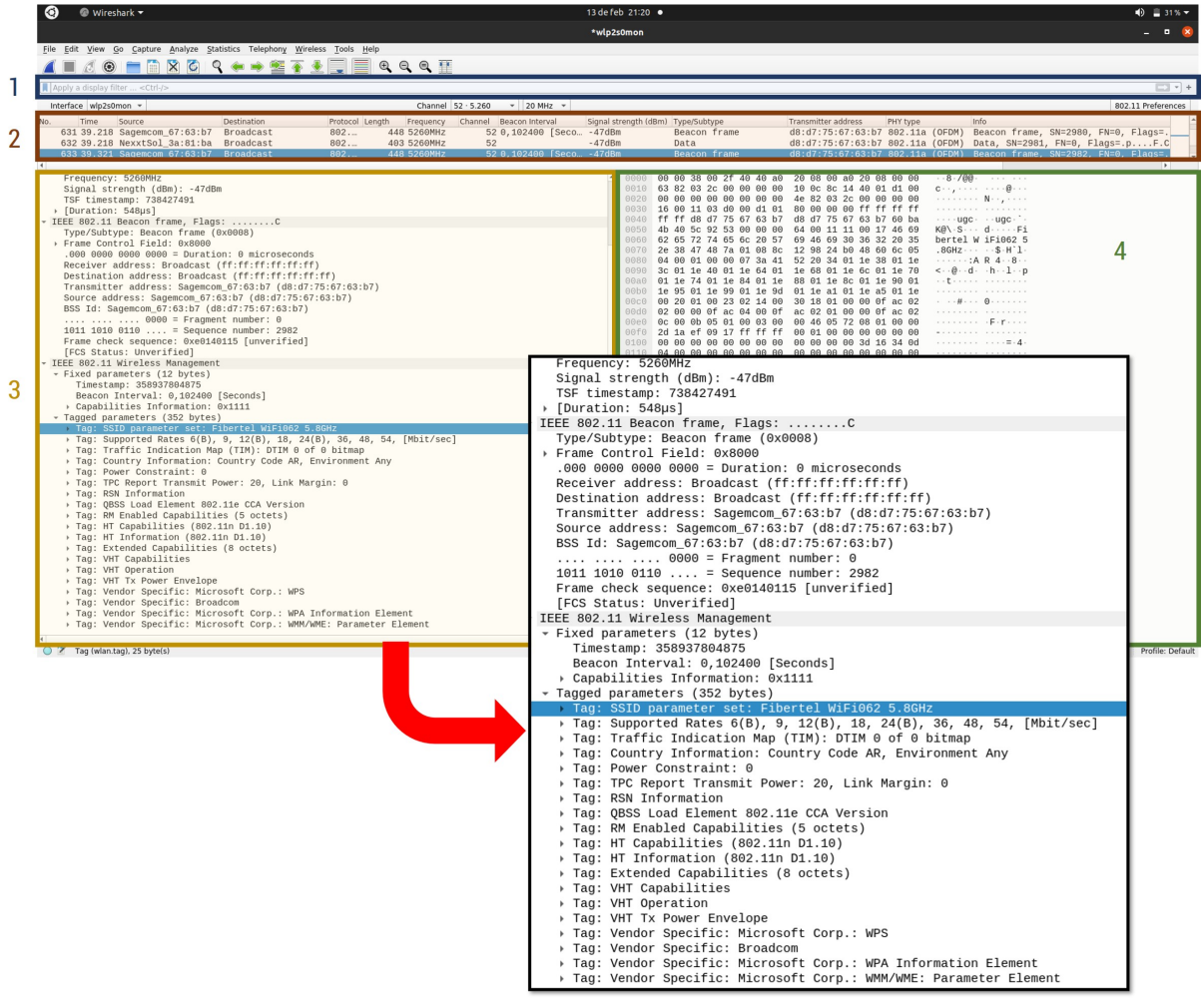


Figura 3.15: Áreas de interés en Wireshark.

En la Figura 3.15 que se presenta en la siguiente página, se visualiza la captura de los paquetes en tiempo real. El paquete seleccionado para análisis es la trama "Beacon".

La pantalla de inicio del programa está dividida en distintas zonas:

- zona 1, es el área de definición de filtros y permite declarar patrones de búsqueda para visualizar los paquetes o protocolos de interés;
- zona 2, corresponde a la lista de visualización de todos los paquetes que se están capturando en tiempo real;
- zona 3, permite desglosar por capas cada una de las cabeceras de los paquetes seleccionados en la zona anterior y navegar por cada uno de los campos de los mismos;
- zona 4, representa, en formato hexadecimal, el paquete en bruto, tal y como fue capturado por la tarjeta de red o adaptador inalámbrico.

Además, en la Figura 3.15 también se pueden identificar los parámetros más significativos en el contenido del beacon, examinando la zona de desglose por capas:

- **Timestamp**, es el valor del timer TSF (*Timing Synchronization Function*, Función de Sincronización de Tiempos) del AP, el cliente usa esta información para mantener su propio reloj (su TSF timer) en sincronía con el AP a fin de asegurar una comunicación exitosa;
- **Beacon Interval**, indica con que regularidad el AP transmite los Beacons, es un parámetro configurable del lado del AP. Habitualmente los Beacons se transmiten 10 veces por segundo (0,102400 segundos);
- **Supported Rates**, incluye la lista de tasas de datos básicas y soportadas por el AP;
- **SSID**, es el nombre lógico de la red inalámbrica. Algunos AP tienen la opción para "ocultar" esta información, dejando vacío este campo en los Beacons que transmiten;
- **RSN Information**, incluye detalles del método de autenticación y la información de cifrado que se soporta;
- **Traffic Indication Map (TIM)**, información empleada para el proceso de ahorro de energía;
- **Vendor Specific**: información adicional específica o única proporcionada por el fabricante. En este punto se observa el fabricante del chipset del radio 802.11 y permite saber si el AP está basado en marcas comerciales como Broadcom, Atheros, etc.

En la Figura 3.16 se puede observar el criterio de búsqueda establecido en la zona de definición de filtros. En este caso, se visualizan solamente los Beacons transmitidos por el AP de prueba.

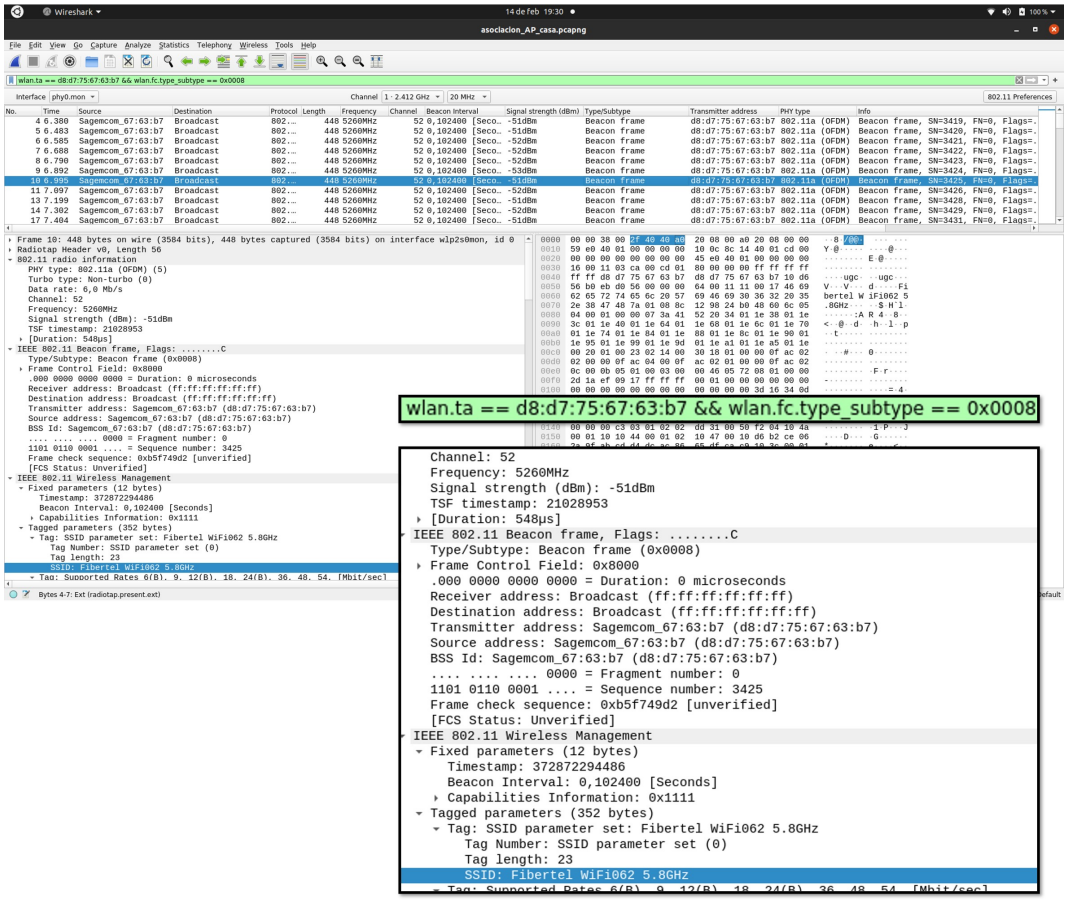


Figura 3.16: Trama Beacon.

El filtro se define de la siguiente forma: el primer término corresponde a la dirección física MAC del router AP, seguido por un operador AND lógico, y el tipo de trama 802.11 de interés (Gestión o Management) incluido el subtipo (0x0008 que corresponde a trama Beacon). A continuación se muestra el filtro completo:

```
wlan.ta == d8:d7:75:67:63:b7 && wlan.fc.type_subtype == 0x0008
```

Una vez seleccionado un paquete Beacon, se analiza el área de la cabecera para descomponer por capas el contenido de la trama. Se identifica el canal de operación (canal 52), la frecuencia (5.260 MHz), la dirección MAC del transmisor que corresponde al AP, la dirección de destino, que en este caso es de difusión o broadcast para que todos los dispositivos cercanos sepan de su existencia a través del SSID, el valor del intervalo del beacon (10 Beacons por segundo), etc. Por medio de la propagación del Beacon por la interfaz de aire, el AP emplea el escaneo pasivo para anunciar dentro de su área de servicio las características que ofrece en su conexión.

3.6.2 Inspección de la Trama Probe Request

Ahora bien, del lado del cliente se emplea el escaneo activo que consiste en transmitir un mensaje de gestión denominado “Probe Request”. Esta trama define el origen de la conexión a un AP específico para asociarse a su red o servicio (conexión a Internet).

Existen dos tipos de tramas Probe Request: **Null Probe Request** y **Directed Probe Request**. En la Figura 3.17 se muestra la captura de una trama Null Probe Request.

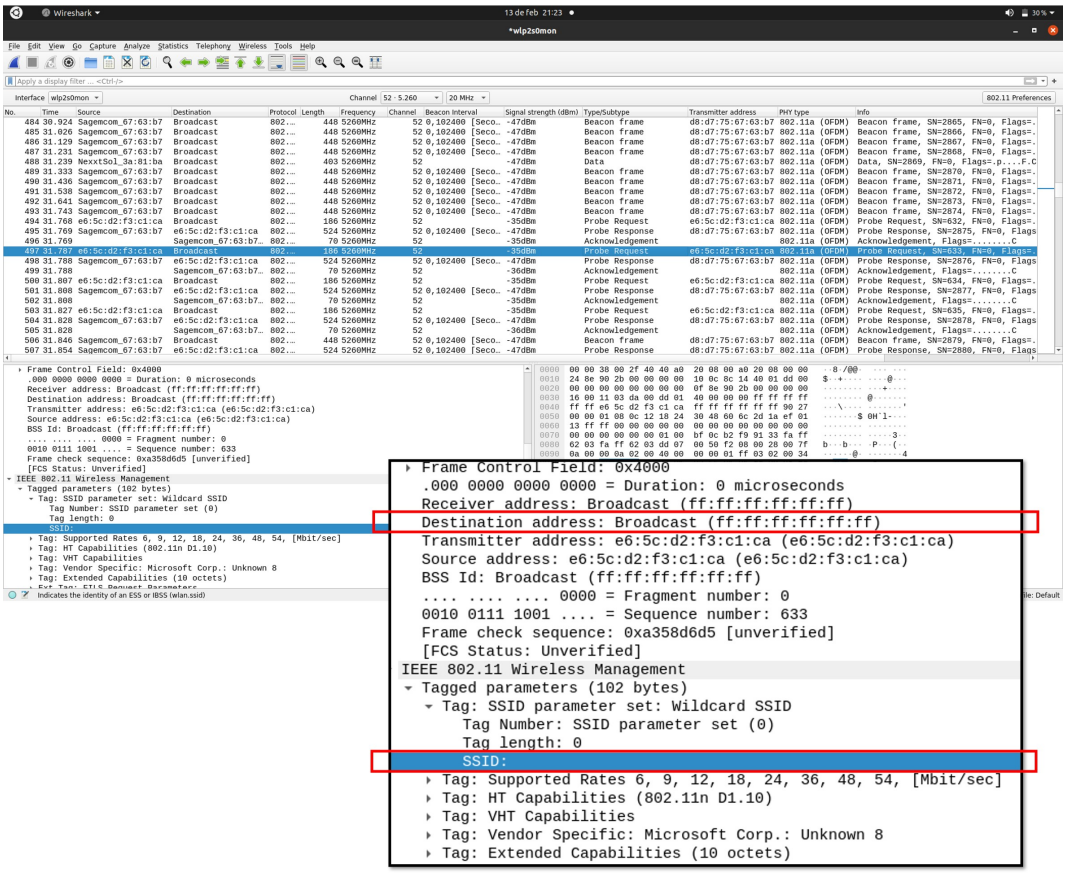


Figura 3.17: Trama Null Probe Request.

Cuando el cliente no está buscando una red en específico, sino que está buscando todas las redes disponibles, transmitirá el mensaje "Probe Request" dejando el campo del parámetro SSID vacío (null). Todos los APs que logren escuchar esta trama deben responder enviando un "Probe Response". En la captura se puede observar que un cliente desconocido (con dirección MAC e6:5c:d2:f3:c1:ca) quiere conocer las redes disponibles. Por esta razón la dirección de destino es la de difusión o Broadcast (ff:ff:ff:ff:ff:ff), sin especificar el SSID.

La trama Directed Probe Request se emplea cuando un cliente busca una red específica. Transmite este mensaje declarando dentro del paquete el parámetro SSID con el nombre lógico de la red inalámbrica que está buscando. Solamente los APs que tengan configurado ese SSID en particular y que logren escuchar el mensaje deben responder con un Probe Response. En la Figura 3.18 se muestra una captura en la que un cliente específico conocido (dispositivo Samsung Galaxy Tab S7 con dirección MAC d6:89:f9:c3:94:7c) transmite la trama Probe Request con el campo SSID definido por el nombre lógico "Fibertel WiFi062 5.8GHz" a la dirección de destino del AP de prueba (Destination address d8:d7:75:67:63:b7).

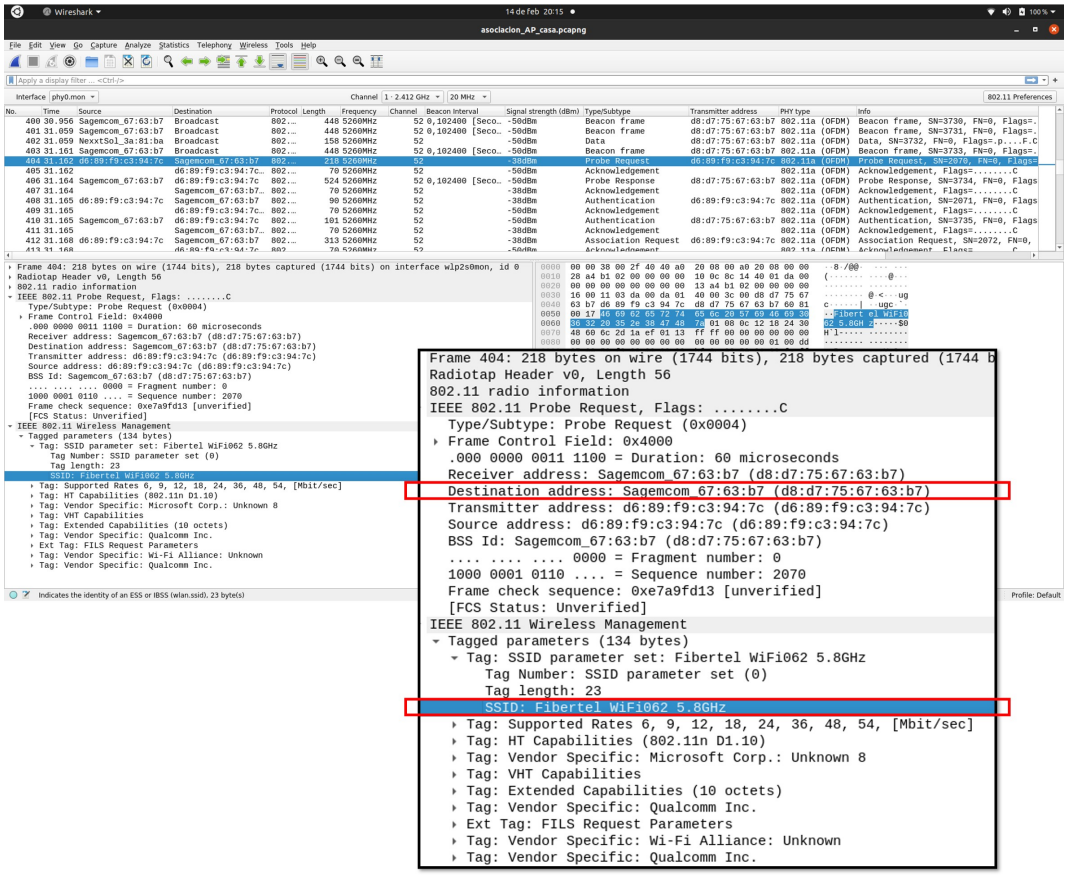


Figura 3.18: Trama Directed Probe Request.

3.6.3 Inspección de la Trama Probe Response

Desde el momento en que se selecciona la red inalámbrica para conectarse, hasta el momento en que la conexión se establece de forma exitosa, tanto el AP como el cliente pasan por una serie de estados intermedios. Una vez que el AP escucha la trama Probe Request enviada hacia él, éste responde con un mensaje Probe Response.

La captura de la Figura 3.19 donde figura el mensaje Probe Response enviado por el AP contiene prácticamente la misma información que un mensaje "Beacon", excepto la información referida a TIM (*Traffic Indication Map*, Mapa de Indicación de Tráfico). Los mensajes Directed Probe Request y Probe Response completan la fase inicial en el proceso de conexión a la red WLAN/RLAN. Para salir de este estado y pasar al siguiente, el cliente (Tablet Samsung S7) debe completar exitosamente lo que se conoce como proceso de "Authentication". En la práctica este es un proceso bastante simple en los sistemas Wi-Fi. Algunas veces esta "Autenticación 802.11" puede ser mal interpretada o confusa, porque no se refiere a una autenticación típica como ingresar un usuario y contraseña, ni tampoco refiere a los mecanismos de seguridad 802.1X/EAP o PSK que se manejan en estos sistemas, sino que consiste en un "saludo" entre ambos dispositivos (cliente y AP), que intercambian mensajes de autenticación ratificando su validez como dispositivos 802.11. Para salir de este estado de autenticación y pasar al estado final de la conexión, el cliente debe completar exitosamente el proceso de

Asociación con el AP. En la Figura 3.20 se muestra la captura de la trama de Gestión y su autenticación exitosa.

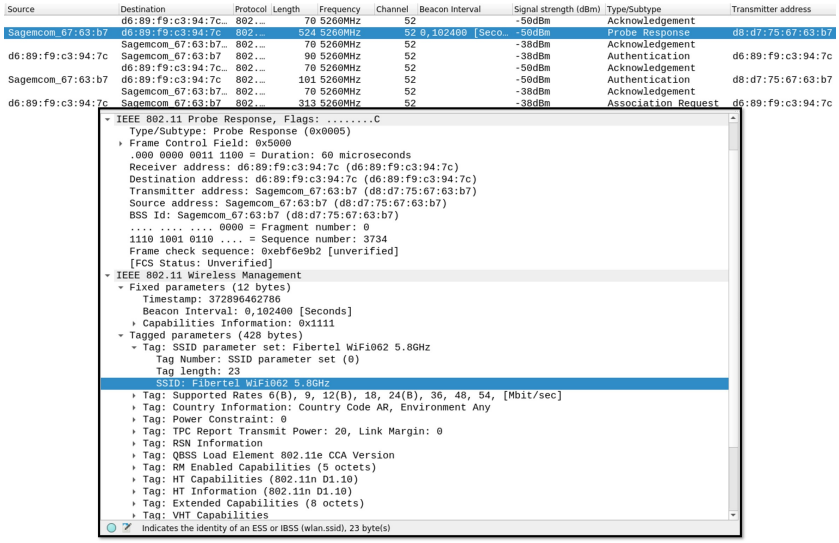


Figura 3.19: Trama Probe Response enviada por el AP de prueba.

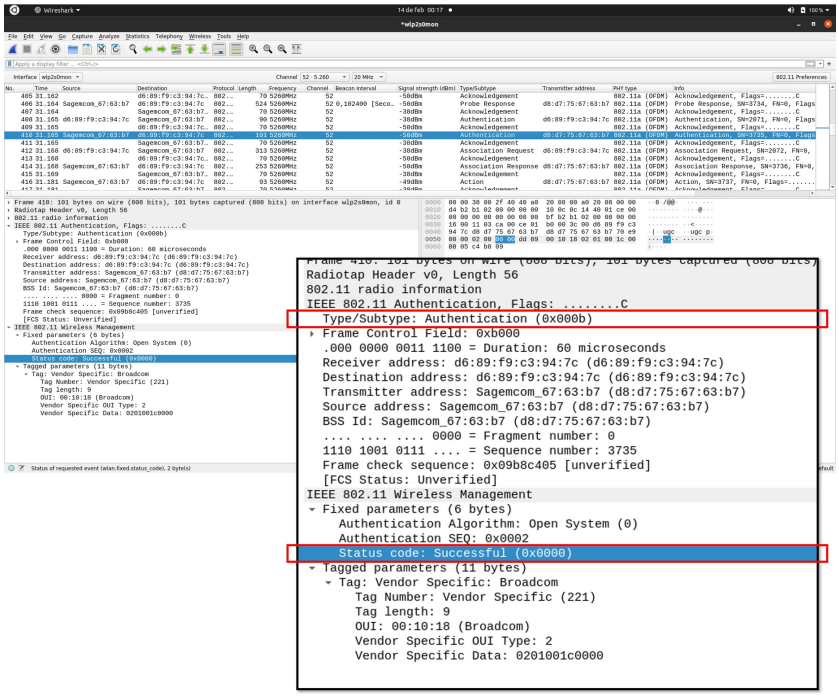


Figura 3.20: Trama Authentication.

Luego de la autenticación, el cliente solicita al AP permiso para unirse y ser parte de su BSS (*Basic Service Set*, Conjunto de Servicios Básicos). Un BSS consiste en un AP con varias estaciones cliente comunicándose entre sí a través del mismo. Las estaciones cliente que son miembros de un BSS tienen una conexión establecida a nivel de capa 2 y se las denomina como "asociadas" al BSS. Esta solicitud de asociación es también bastante simple y consiste en el intercambio de un par de mensajes "request" y "response":

- la estación cliente envía un mensaje "**Association Request**" al AP y éste confirma la recepción devolviendo un Acknowledgement;
- a continuación, el AP envía un mensaje "**Association Response**" a la estación cliente y ésta confirma la recepción con la devolución de un Acknowledgement.

La Figura 3.21 muestra una captura del proceso de asociación del cliente al AP realizada durante la prueba. Las tramas resaltadas corresponden al intercambio de mensajes Request/Response.

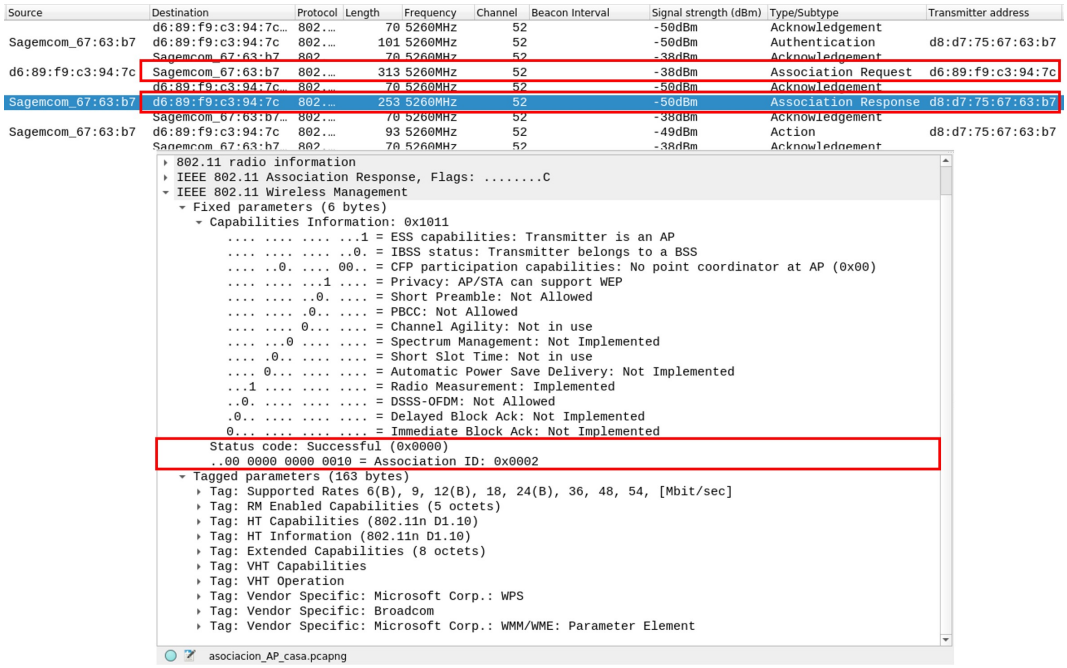


Figura 3.21: Trama Association.

Los mensajes Association Request/Response contienen información con todos los "Data Rates" soportados tanto del lado del cliente como del AP. Esta información se agrupa en dos parámetros: los "basic Data Rates" y los "extended Data Rates". Para que la estación cliente pueda unirse exitosamente al BSS del AP sin ser rechazada, el cliente debe soportar al menos todas las tasas de datos (básicas) que anuncia el AP. La lista extendida es opcional y no debería ser motivo de rechazo de la asociación en caso de que el cliente no la soporte.

Cuando la estación cliente logra una asociación exitosa con el AP, este último envía un mensaje de respuesta Association Response y en su contenido se detalla un parámetro denominado "Association ID" (resaltado en la Figura 3.21). Este identificador es el número de asociación del cliente y es único que el AP otorga a cada cliente asociado exitosamente.

3.7 Reflexiones Finales

A modo de cierre, el propósito de este capítulo es describir las características más sobresalientes de todos los recursos de hardware y herramientas de software que se han

considerado para las mediciones. Para la selección de los instrumentos y aplicaciones finales se establecieron criterios tales como su compatibilidad con el sistema operativo, funcionalidades, utilidad, portabilidad y de aquitectura libre y abierta que ayudaron a filtrar recursos y, de esta forma, construir una base de referencia que sirva como protocolo de medición para recoger y analizar información de ciertos eventos que puedan ocurrir en los ensayos controlados de laboratorio y posteriormente extender su aplicación a un escenario mucho más complejo y dinámico como lo es el sitio radar.

Con estas últimas prácticas se comprobó que el desempeño y rendimiento de los dispositivos de hardware y las aplicaciones de software seleccionados cumplen con los requerimientos y necesidades desde una perspectiva más acotada. La integración de estos elementos y su aplicación será útil para obtener información suficiente para localizar, con un mínimo margen de error, la posición geográfica de las fuentes de interferencias. Mediante la incorporación del sistema GPS, en paralelo con la captura de paquetes y tramas inalámbricas con Kismet y Wireshark y el análisis del espectro radioeléctrico será posible identificar y localizar las fuentes WLAN/RLAN en un ambiente más amplio y variable, en donde pueden ocurrir eventos externos muy dinámicos.

La captura de tráfico inalámbrico en tiempo real, servirá de soporte para comprobar lo que sucede en la interfaz de aire revisando la actividad de los puntos de acceso y clientes cuando se genera alguna conexión o se está transmitiendo flujo de datos constante a gran velocidad. Luego de la captura se puede realizar el filtrado de paquetes mediante una auditoría minuciosa, y de esta manera, desglosar por capas los protocolos y tramas para un análisis más detallado de las fuentes WLAN/RLAN.

No es objetivo de este trabajo repasar todas y cada una de las tramas de gestión y sus parámetros, pero mediante la interpretación del tráfico en tiempo real o a través de un análisis posterior por auditoría de red, aportarán los datos necesarios para conocer los dispositivos y servicios existentes en el entorno radar.

Capítulo 4

Trabajo en campo y resultados

4.1 Introducción

A partir de los programas y dispositivos descritos, en el presente capítulo se desarrolla un procedimiento de medición y se aborda el trabajo de campo llevado a cabo al implementarlo. Si bien el procedimiento es general, el trabajo de campo se concentra en detectar y ubicar la posición de fuentes que actualmente interfieren el RMA-1 emplazado en la ciudad de Córdoba.

En primer lugar, se analizan registros de radar meteorológico, específicamente la reflectividad, donde se identifican los efectos de la interferencia y permite determinar aquellas direcciones acimutales críticas en cartografía digital, a modo de orientación para la búsqueda de las fuentes inalámbricas interferentes. Posteriormente, se describe el proceso de medición durante el trabajo de campo, lo que involucra la integración dinámica de datos del GPS en tiempo real, adquisiciones que dan cuenta de la actividad de las transmisiones de las señales en el espectro y la captura de tramas inalámbricas 802.11.

Como resultado de la medición en campo se describe el proceso de geolocalización de cuatro fuentes de interferencia, incluyendo el registro fotográfico tomado en una etapa posterior. Además, se lleva a cabo la inspección de las tramas con los programas descritos en el capítulo previo, lo que permite extraer las características más relevantes del modo de operación de los dispositivos WLAN/RLAN identificados en las direcciones interferidas y ponen de manifiesto la invasión del espectro radioeléctrico de manera indebida.

Finalmente, se desarrolla un ensayo de laboratorio que consiste en montar transceptores de los mismos proveedores de los sistemas WLAN/RLAN detectados y en establecer una comunicación entre ellos, realizando las mediciones de forma análoga a lo desarrollado en campo, de modo tal de corroborar el funcionamiento de los dispositivos en un ambiente controlado y su impacto en la utilización e invasión del espectro radioeléctrico.

4.2 Procedimiento de Medición

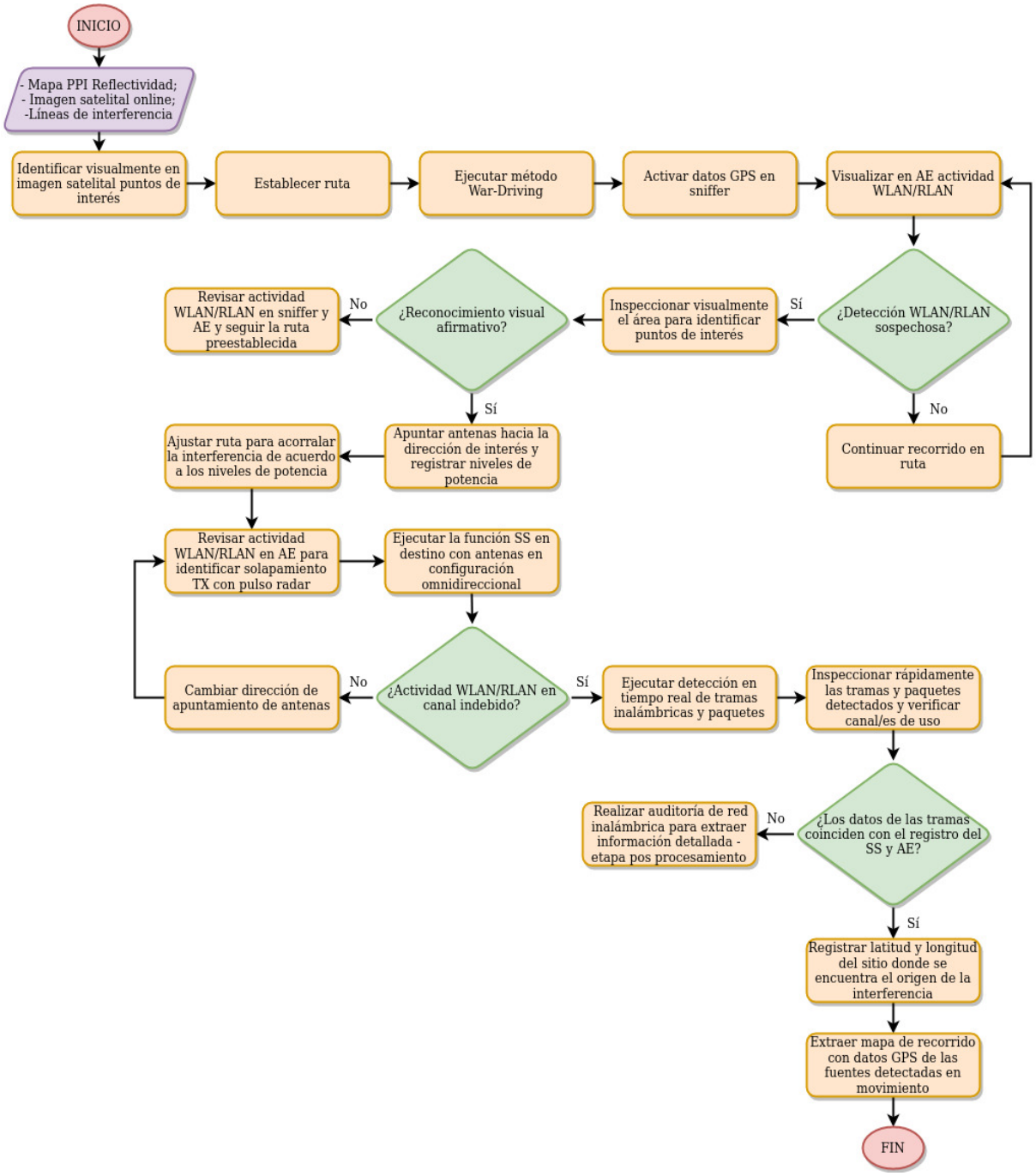


Figura 4.1: Diagrama de bloques del procedimiento de medición.

En la Figura 4.1 se ilustra el diagrama de bloques, integrado por los distintos procesos/funciones y relaciones, que describe el procedimiento de medición de campo.

Inicialmente, como datos de entrada se toma el PPI de reflectividad presentado en la Figura 1.3, donde se identifican las direcciones acimutales en las que se observa potencia debida a la/las fuente/s de interferencia/s. Este gráfico se superpone a la información provista por un archivo importado de Google Earth denominado KML o KMZ almacenado en el directorio local para crear animaciones con fines informativos.

En este caso, el archivo KML pertenece a la imagen satelital (obtenida a través de imágenes satelitales, fotografías aéreas e información geográfica de Google Earth) de la zona de Córdoba centrada en el RMA-1. Luego, se añade (en forma de capas) la imagen de la Figura 1.3 al mapa, lo que permite al software procesar la superposición en tiempo real durante la reproducción y navegación. Los resultados se muestran en la Figura 4.2.

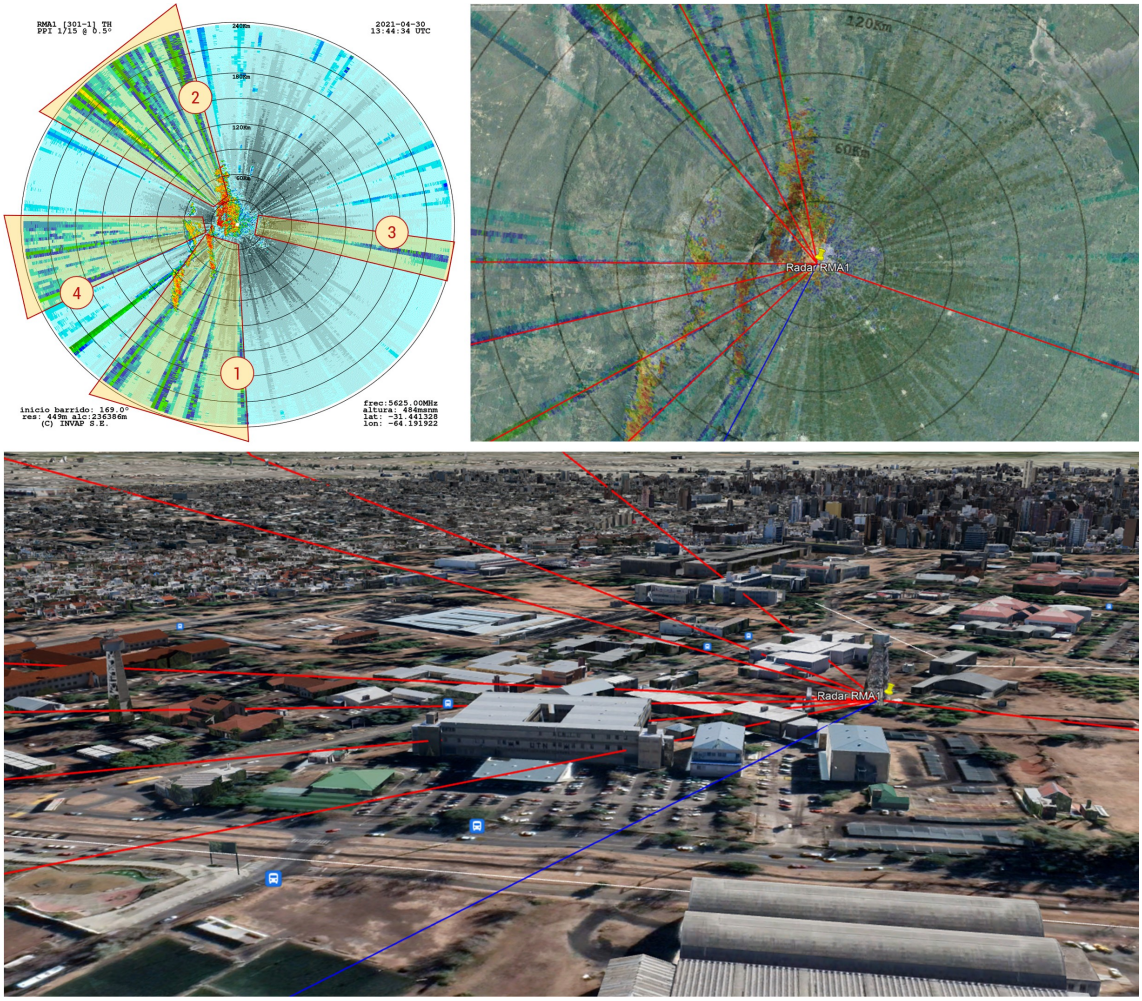


Figura 4.2: Superposición de imágenes y trazado de líneas interferentes según mapa PPI.

Específicamente, en la imagen de arriba a la derecha se aprecia la superposición descrita, en la que se resaltan con líneas rojas rutas estáticas que corresponden a direcciones acimutales identificadas como interferidas. En el mapa se hace una clasificación de las interferencias

teniendo en consideración su intensidad y su ubicación. A cada grupo de interferencias se le asigna un número que se utiliza para ordenar las regiones del proceso de medición en campo.

En la Figura 4.3 se muestra el mapa satelital disponible en Google Maps, en el que se trazó una línea recta en color azul que corresponde al grupo de interferencias número 1 del PPI presentado en la imagen de arriba a la izquierda de la Figura 4.2, para tener una noción de la dirección.

El primer proceso del diagrama de bloques, corresponde a la identificación de posibles fuentes de manera visual con el uso de la herramienta Street View de Google Earth, siguiendo la línea sobre el mapa tomando como referencia infraestructura y/o emplazamiento existente (torres de telecomunicaciones y estructuras edilicias), sistemas radiantes instalados a gran altura, entre otros, que se prevé verificar in-situ.

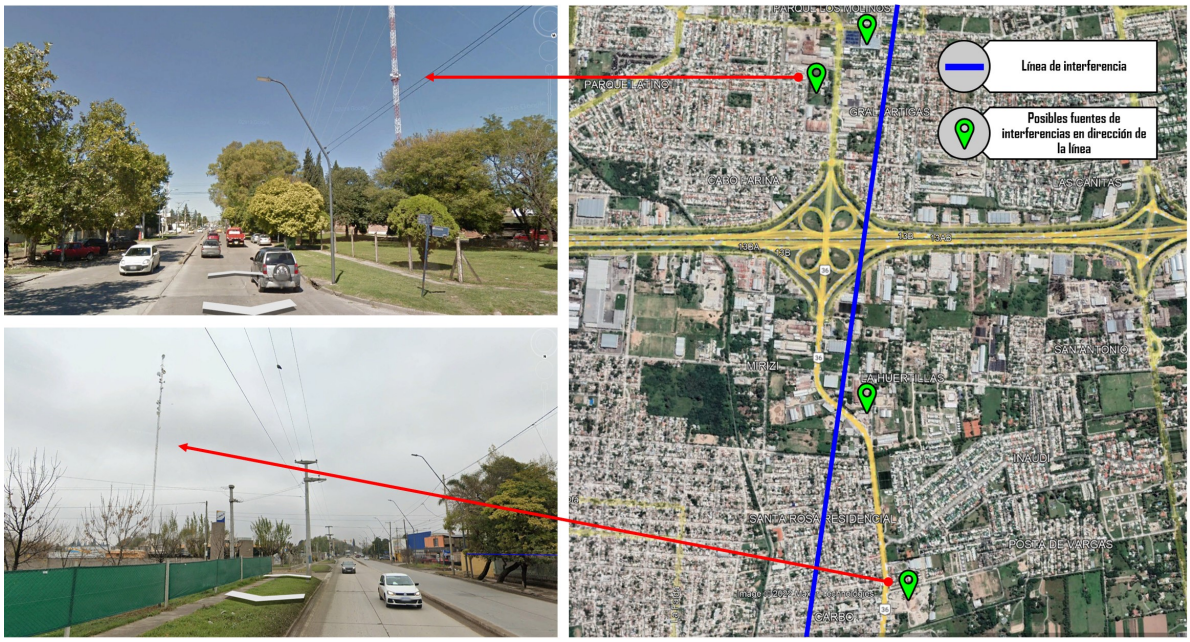


Figura 4.3: Imagen satelital con trazado de línea de interferencia y posibles fuentes identificadas visualmente con la herramienta Street View de Google Earth.

Una vez establecida la ruta (segundo proceso del diagrama) según la dirección acimutal de las posibles fuentes de interferencias se ejecuta el tercer proceso, que es un método de búsqueda en movimiento de redes inalámbricas conocido como "*War-Driving*", para lo cual se emplea un vehículo equipado con el hardware y el software de medición. Esto implica conducir lentamente por una zona específica de la ciudad examinando el medio a través de los recursos de software descritos en la Figura 3.7 del Capítulo 3, con el propósito de detectar señales de RF transmitidas de forma inalámbrica en la banda de 5 GHz. En simultáneo, se registra en tiempo real la actividad de los transmisores WLAN/RLAN en función de la frecuencia con la ayuda de un analizador de espectro (AE).

De acuerdo al diagrama de integración mostrado en la Figura 3.8, el equipamiento se compone de: una computadora portátil con sistema operativo Linux distribución Ubuntu

20.04 LTS preparada para ejecutar los programas de captura de paquetes y tramas inalámbricas (Wireshark y Kismet) que, además, brinda la posibilidad de conectarle un receptor inalámbrico Wi-Fi USB y un teléfono inteligente para extraer la información provista por el GPS; y una computadora portátil con sistema operativo Windows 10 con puerto FastEthernet para conectar vía cable UTP un dispositivo AP Ubiquiti NanoStation airMAX Loco M5 que ofrece, en su gama de funcionalidades, el uso del analizador de espectro mencionado en el párrafo anterior y que está embebido en su software. En la Figura 4.4 se muesta una imagen con parte del equipamiento montado en el vehículo.

Figura 4.4: Equipamiento a bordo del vehículo para ejecutar el método War-Driving.

A la actividad registrada con el analizador de espectro, se adicionan los datos del GPS transmitidos desde un teléfono inteligente a la computadora portátil para ser recuperados vía USB por el software Kismet (cuarto y quinto procesos del diagrama). Este procedimiento permite anexar la información geográfica de latitud y longitud estimadas a las redes descubiertas, mediante la captura de tramas inalámbricas correspondientes al estándar 802.11 con la misma aplicación.

En la etapa de geolocalización se realizan tres acciones. La primera es la verificación in-situ, a través de la inspección visual del área, de los puntos de interés caracterizados por torres/emplazamientos de gran altura con sistemas radiantes instalados en su estructura, algunos de ellos establecidos en el primer proceso. En caso de reconocimiento visual afirmativo, se apuntan las antenas del equipamiento (antenas MiMo del adaptador wireless externo y antenas del dispositivo AP Ubiquiti NanoStation airMAX Loco M5) con el fin de ajustar la ruta de recorrido para acorralar la actividad WLAN/RLAN sospechosa de acuerdo a los niveles de potencia registrado en el AE y Kismet. Esto permite crear un mapa de cobertura de referencia para acercarse al sitio identificado como posible punto interferente. Además, se visualiza la actividad de transmisión WLAN/RLAN en el AE para identificar porciones o

rango de frecuencias que demuestren solapamiento de potencia con la transmisión del pulso radar, tal como se muestra en la Figura 4.5. En destino, se realiza la segunda acción, la cual se basa en ejecutar una función disponible en el equipo AP Ubiquiti NanoStation airMAX Loco M5 denominada "*Site Survey (SS)*". Dicha acción consiste en hacer un barrido omnidireccional con sus antenas integradas cubriendo todos los canales disponibles de la banda de 5 GHz, tal como se muestra en la Figura 4.7, con el objetivo de descubrir redes inalámbricas en el área y que se registran en formato de lista numerada. Dentro de este listado se identifican dispositivos WLAN/RLAN funcionando en frecuencias indebidas o canales DFS. Además, se detallan otros campos de interés: la dirección física MAC correspondiente al BSSID según el estándar, el nombre lógico de la red inalámbrica denominado SSID, el modo de funcionamiento del transmisor o equipo de rediofrecuencia, la encriptación haciendo referencia a su seguridad, la potencia de recepción e indicador Señal/Ruido en unidades dBm y la frecuencia/canal de operación en unidades GHz.

A partir del análisis del Site Survey y registros de niveles de potencia, se ejecuta una tercera acción que consiste en detectar correctamente el origen de la fuente de interferencia. Se capturan paquetes y tramas 802.11 en tiempo real con el software Wireshark y el receptor inalámbrico Wi-Fi USB externo configurado en "Modo Monitor", de manera que permita escuchar todos los paquetes que se propagan de forma inalámbrica por la región incluido principalmente el sitio de interés. Esto se logra apuntando las antenas MiMo del adaptador a los sistemas radiantes instalados en la estructura.

En el modo Monitor, no solamente se escucha lo que envía un AP localmente, sino también el intercambio de información que se establece en redes Wi-Fi vecinas. Para filtrar los paquetes es necesario escanear un canal específico para no perder información sobre el tráfico que emite el AP a los distintos clientes. A partir de este modo, se accede a la subcapa PHY del estándar 802.11 y se pueden conocer las direcciones físicas MAC de todos los clientes que están conectados a un determinado AP, dado que se capturan las tramas de datos que viajan por el aire desde el origen hasta la dirección de destino. En plataforma Ubuntu Linux se habilita el modo Monitor del hardware y se combina con aplicaciones denominadas *sniffers* para capturar gran cantidad de información que luego se manipula de forma lícita. A este proceso de escucha pasivo en el que se adquiere la información que circula por el medio de transmisión sin alterarla se lo conoce como ataque "*Sniffing*".

Wireshark, al igual que Kismet, es una aplicación *sniffer* que permite analizar de forma detallada y minuciosa el tráfico de una red inalámbrica mediante inspección directa. Dispone de una área de definición de filtros en donde se declaran patrones de búsqueda para visualizar los paquetes o tramas de interés. Para escuchar la comunicación entre el AP y los clientes se capturan unas cadenas de datos especiales denominadas tramas de gestión (*Management Frames*), donde está contenida la subtrama "*Beacon Frame*". De la información del Site Survey se extrae la dirección MAC del dispositivo interferente y se establece el filtro de búsqueda para observar sólo los paquetes relacionados con ese AP en particular capturados en tiempo real. Luego, se desglosa por capas cada una de las cabeceras del paquete o trama para analizar en

detalle sus parámetros más significativos. A modo de ejemplo, este proceso se ilustra en la Figura 4.8.

Por último, los dos últimos procesos del diagrama de bloques se relacionan entre sí para registrar los datos de Latitud y Longitud del sitio donde se encuentra el origen de la interferencia. Para esto, Kismet recopila toda la información y lo exporta en un archivo con formato CSV, que es utilizado en la etapa de postprocesamiento para plasmar en el mapa los datos registrados por el GPS. En la Figura 4.6 se muestra, a modo de ejemplo, el mapa de recorrido con información geográfica.

4.3 Resultados

Registro de interferencia - Grupo 1

En la Figura 4.5 se presenta una captura del analizador de espectro utilizado a bordo del vehículo en el proceso de War-Driving, obtenida mediante el apuntamiento de las antenas direccionales del equipo AP Ubiquiti NanoStation airMAX Loco M5 hacia las posibles fuentes de interferencias.

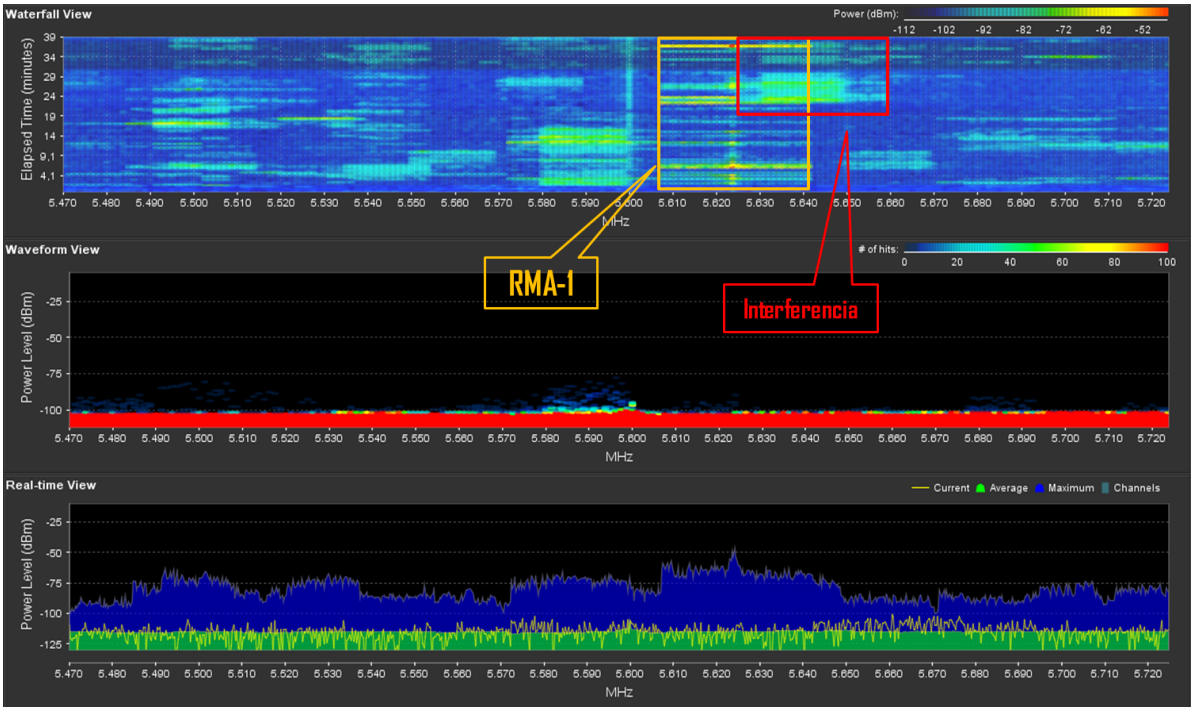


Figura 4.5: Actividad del RMA-1 y la interferencia.

En la parte superior de la figura, se observa el gráfico de cascada (Waterfall view) donde se registran las transmisiones superpuestas en forma de energía en cada frecuencia de la transmisión del pulso RMA-1, con frecuencia central de operación 5.625 MHz, y del dispositivo inalámbrico WLAN/RLAN que produce interferencia. El color señala la amplitud, siendo los colores fríos (azul, celeste y tonos en verde) los niveles más bajos de potencia en los canales, mientras que los más cálidos (amarillo, naranja y rojo) indican mayor potencia de la señal.

También se incluye la sección de forma de onda (Waveform view) para tener una referencia del estado actual de la actividad de RF en el entorno de la frecuencia de operación del radar. Finalmente, el tercer gráfico denotado como Real time view, corresponde a la medición de potencia, en unidad de dBm, en función de la frecuencia. El proceso de geolocalización con la posición estimada, representada por puntos de color azul plasmados en el mapa, de cada una de las redes inalámbricas descubiertas se muestra en la Figura 4.6.

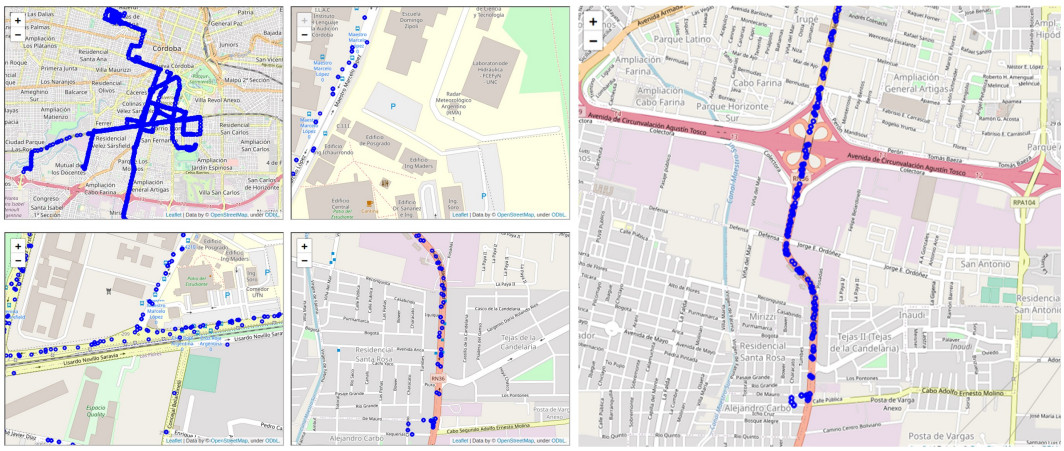


Figura 4.6: Captura de datos GPS asociados a las redes inalámbricas.

Site Survey

Scanned Frequencies:

4.92GHz 4.925GHz 4.93GHz 4.935GHz 4.94GHz 4.945GHz 4.95GHz 4.955GHz 4.96GHz 4.965GHz 4.97GHz 4.975GHz 4.98GHz 4.985GHz 4.99GHz 4.995GHz 5GHz 5.005GHz 5.01GHz 5.015GHz 5.02GHz 5.025GHz 5.03GHz 5.035GHz 5.04GHz 5.045GHz 5.05GHz 5.055GHz 5.06GHz 5.065GHz 5.07GHz 5.075GHz 5.08GHz 5.085GHz 5.09GHz 5.095GHz 5.1GHz 5.105GHz 5.11GHz 5.115GHz 5.12GHz 5.125GHz 5.13GHz 5.135GHz 5.14GHz 5.145GHz 5.15GHz 5.155GHz 5.16GHz 5.165GHz 5.17GHz 5.175GHz 5.18GHz 5.185GHz 5.19GHz 5.195GHz 5.2GHz 5.205GHz 5.21GHz 5.215GHz 5.22GHz 5.225GHz 5.23GHz 5.235GHz 5.24GHz 5.245GHz 5.25GHz 5.255GHz 5.26GHz 5.265GHz 5.27GHz 5.275GHz 5.28GHz 5.285GHz 5.29GHz 5.295GHz 5.3GHz 5.305GHz 5.31GHz 5.315GHz 5.32GHz 5.325GHz 5.33GHz 5.335GHz 5.34GHz 5.345GHz 5.35GHz 5.355GHz 5.36GHz 5.365GHz 5.37GHz 5.375GHz 5.38GHz 5.385GHz 5.39GHz 5.395GHz 5.4GHz 5.405GHz 5.41GHz 5.415GHz 5.42GHz 5.425GHz 5.43GHz 5.435GHz 5.44GHz 5.445GHz 5.45GHz 5.455GHz 5.46GHz 5.465GHz 5.47GHz 5.475GHz 5.48GHz 5.485GHz 5.49GHz 5.495GHz 5.5GHz 5.505GHz 5.51GHz 5.515GHz 5.52GHz 5.525GHz 5.53GHz 5.535GHz 5.54GHz 5.545GHz 5.55GHz 5.555GHz 5.56GHz 5.565GHz 5.57GHz 5.575GHz 5.58GHz 5.585GHz 5.59GHz 5.595GHz 5.6GHz 5.605GHz 5.61GHz 5.615GHz 5.62GHz 5.625GHz 5.63GHz 5.635GHz 5.64GHz 5.645GHz 5.65GHz 5.655GHz 5.66GHz 5.665GHz 5.67GHz 5.675GHz 5.68GHz 5.685GHz 5.69GHz 5.695GHz 5.7GHz 5.705GHz 5.71GHz 5.715GHz 5.72GHz 5.725GHz 5.73GHz 5.735GHz 5.74GHz 5.745GHz 5.75GHz 5.755GHz 5.76GHz 5.765GHz 5.77GHz 5.775GHz 5.78GHz 5.785GHz 5.79GHz 5.795GHz 5.8GHz 5.805GHz 5.81GHz 5.815GHz 5.82GHz 5.825GHz 5.83GHz 5.835GHz 5.84GHz 5.845GHz 5.85GHz 5.855GHz 5.86GHz 5.865GHz 5.87GHz 5.875GHz 5.88GHz 5.885GHz 5.89GHz 5.895GHz 5.9GHz 5.905GHz 5.91GHz 5.915GHz 5.92GHz 5.925GHz 5.93GHz 5.935GHz 5.94GHz 5.945GHz 5.95GHz 5.955GHz 5.96GHz 5.965GHz 5.97GHz 5.975GHz 5.98GHz 5.985GHz 5.99GHz 5.995GHz 6GHz 6.005GHz 6.01GHz 6.015GHz 6.02GHz 6.025GHz 6.03GHz 6.035GHz 6.04GHz 6.045GHz 6.05GHz 6.055GHz 6.06GHz 6.065GHz 6.07GHz 6.075GHz 6.08GHz 6.085GHz 6.09GHz 6.095GHz 6.1GHz

MAC Address	SSID	Device Name	Radio Mode	Encryption	Signal / Noise, dBm	Frequency, GHz / Channel
44:D9:E7:2A:EE:8E	IW-CAMPO-S	Hormi-Block ap	802.11n airMAX	WPA2	-80 / -96	4.93 / 186
78:8A:20:EE:DA:4B	IW-HORMI-E	NanoStation M5	802.11n airMAX	WPA2	-79 / -98	5.015 / 3
F0:9F:C2:EC:4E:1C			airMAX AC	WPA2	-90 / -97	5.1 / 20
B4:FB:E4:B8:AE:37			airMAX AC	WPA2	-73 / -97	5.11 / 22
74:83:C2:64:5C:6F			airMAX AC	WPA2	-89 / -93	5.345 / 69
E0:63:DA:12:CA:8D			airMAX AC	WPA2	-90 / -92	5.44 / 88
74:83:C2:62:A5:7C			airMAX AC	WPA2	-92 / -96	5.465 / 93
78:8A:20:EC:6B:ED			airMAX AC	WPA2	-70 / -91	5.55 / 110
74:83:C2:64:5B:46			airMAX AC	WPA2	-89 / -92	5.565 / 113
78:8A:20:3C:2B:F2	IW-HORMI-SE	010 Hormi - Ca	802.11n airMAX	WPA2	-85 / -90	5.63 / 126
B4:FB:E4:5C:7C:FE			airMAX AC	WPA2	-90 / -91	5.635 / 127
78:8A:20:30:1D:04	TOPTEL4	TOPTEL4	802.11n airMAX	WPA2	-90 / -91	5.68 / 136
E0:63:DA:12:CA:0F			airMAX AC	WPA2	-86 / -91	5.715 / 143
18:E8:29:78:20:3A			airMAX AC	WPA2	-89 / -91	5.76 / 152
E0:63:DA:10:57:9C			airMAX AC	WPA2	-79 / -91	5.765 / 153
18:E8:29:78:F6:D0			airMAX AC	WPA2	-80 / -89	5.79 / 158
18:E8:29:D6:79:8D			airMAX AC	WPA2	-72 / -91	5.83 / 166
74:AC:B9:8A:12:A3			airMAX AC	WPA2	-61 / -91	5.88 / 176

Figura 4.7: Barrido de frecuencia de la herramienta Site Survey.

En la Figura 4.7 se observa el listado de frecuencias liberadas o disponibles para su uso en la banda de 5 GHz en base al análisis de la herramienta Site Survey. Se identifican dos

dispositivos funcionando en frecuencias prohibidas correspondientes a canales DFS que fue descripto en la Sección 2.2.3. Estos dos dispositivos presentan las siguientes características:

- MAC Address 78:8A:20:3C:2B:F2 - SSID “IW-HORMI-SE” - Radio Mode “802.11n airMAX” - Frecuencia 5,63 GHz (canal 126);
- MAC Address B4:FB:E4:5C:7C:FE - Radio Mode “airMAX AC” - Frecuencia 6,635 GHz (canal 127).

En particular, el análisis de interferencia se corresponde con la primera fuente inalámbrica (marcada en color rojo en la lista), debido a que la segunda (color naranja claro) desapareció del área de recepción en un momento de la captura.

Con la aplicación Wireshark se aplica el filtro por dirección física MAC configurándolo como wlan.ta==78:8a:20:3c:2b:f2 tal como se muestra en la Figura 4.8, para presentar únicamente la información correspondiente al AP interferente. Al apuntar el receptor inalámbrico Wi-Fi USB externo a la fuente WLAN/RLAN se capturan en tiempo real los paquetes y tramas. Se selecciona la trama Beacon y se revisa el área de la cabecera para descomponer por capas el contenido de la misma.

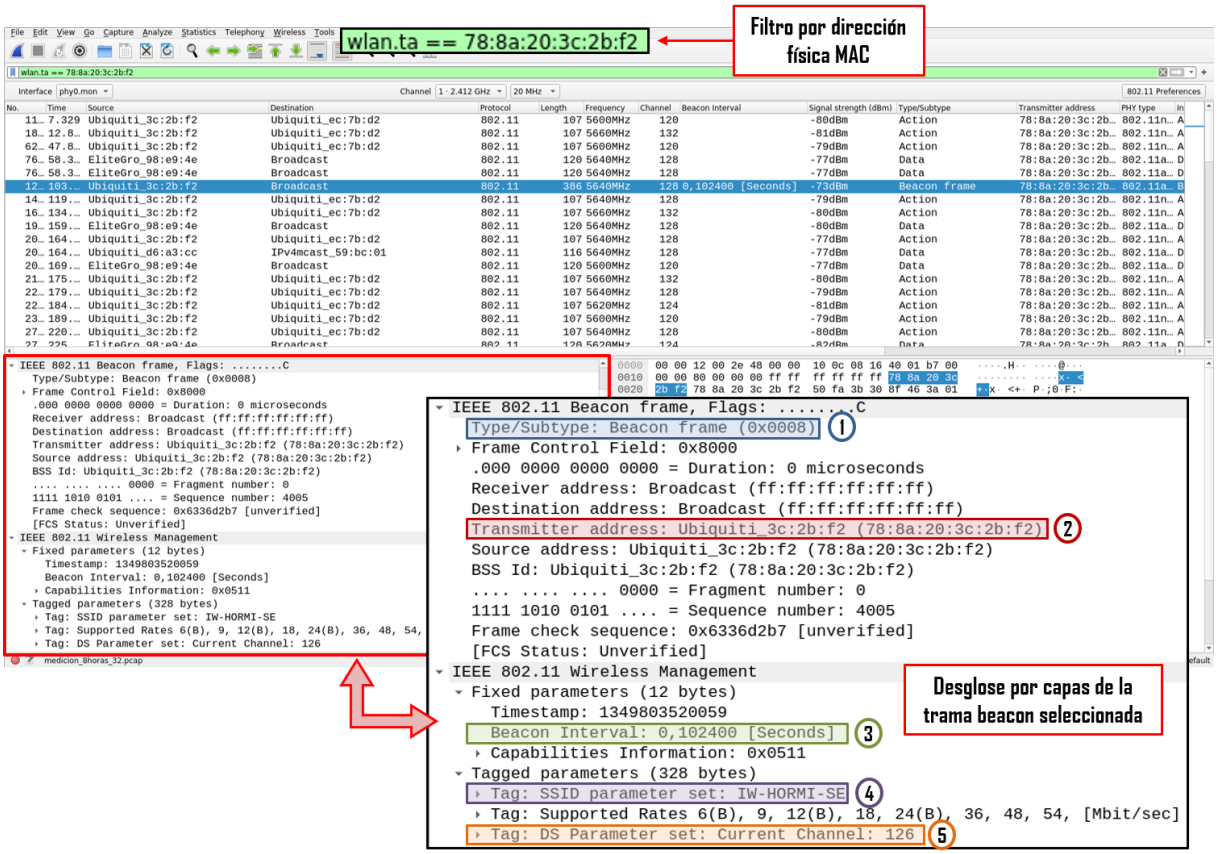


Figura 4.8: Inspección de la trama Beacon utilizando el programa Wireshark.

En esta sección de captura se identifican los datos más relevantes:

1. información del tipo de trama (gestión) incluido el subtipo (0x0008 - beacon);

2. la dirección física MAC del dispositivo transmisor interferente (78:8a:20:3c:2b:f2) que hace referencia al filtro;

3. la duración del intervalo de beacon por defecto (0,102400 segundos);

4. el nombre lógico SSID (IW-HORMI-SE);

5. el canal o frecuencia de operación (canal 126 - 5.630 MHz).

Si bien la fuente de interferencia opera en una frecuencia cercana al radar meteorológico (canal 126 con un ancho de banda de 20 MHz), lo más crítico y llamativo que se observa en la captura de tráfico inalámbrico es la ocupación de varios canales de la banda de frecuencia para el envío de otros datos. Esto se refiere, a la utilización de tramas tales como "*Action*" y la transmisión de datos puros "*Data*", ocupando los canales 120 (5.600 MHz), 124 (5.620 MHz), 128 (5.640 MHz) y 132 (5.660 MHz). Esta ocupación de canales se observa en la Figura 4.9, quedando en evidencia la interferencia directa (canales solapados) a la transmisión del pulso radar del RMA-1. En la Figura 4.10 se muestra el filtrado por dirección física MAC quedando en evidencia la interferencia por canal.

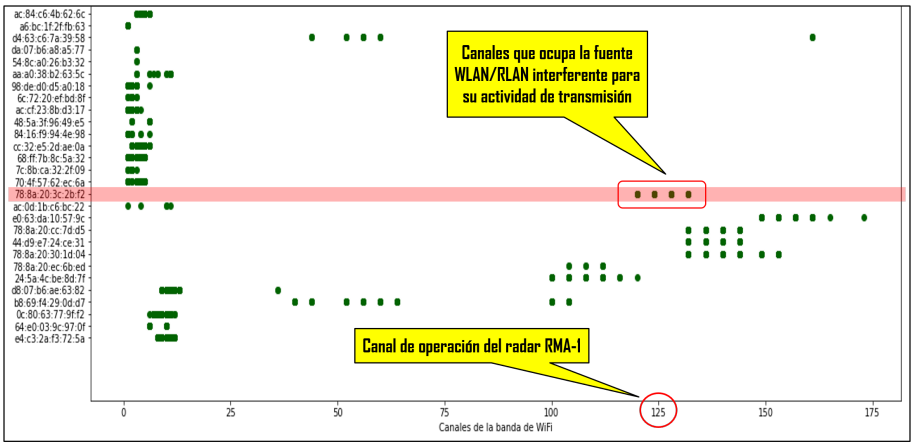


Figura 4.9: Utilización de canales del AP interferente.

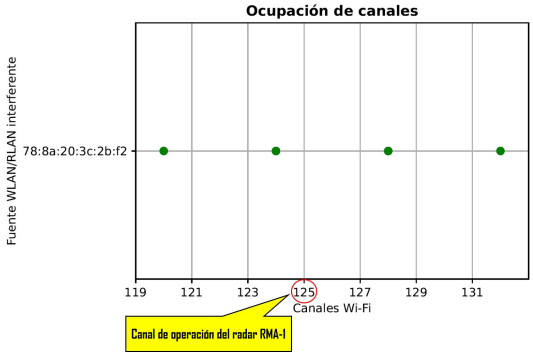


Figura 4.10: Ocupación de canales de la fuente WLAN/RLAN y que interfieren a la transmisión del radar.

El análisis del tráfico inalámbrico capturado completa el proceso de geolocalización. En la Figura 4.11 se observa la posición geográfica y registro fotográfico de la estructura y las antenas donde se infiere que se encuentra la fuente de interferencia. De acuerdo al gráfico PPI presentado en la Figura 4.2, la dirección acimutal correspondiente con esta fuente es de aproximadamente 193° medido a partir del Norte geográfico.

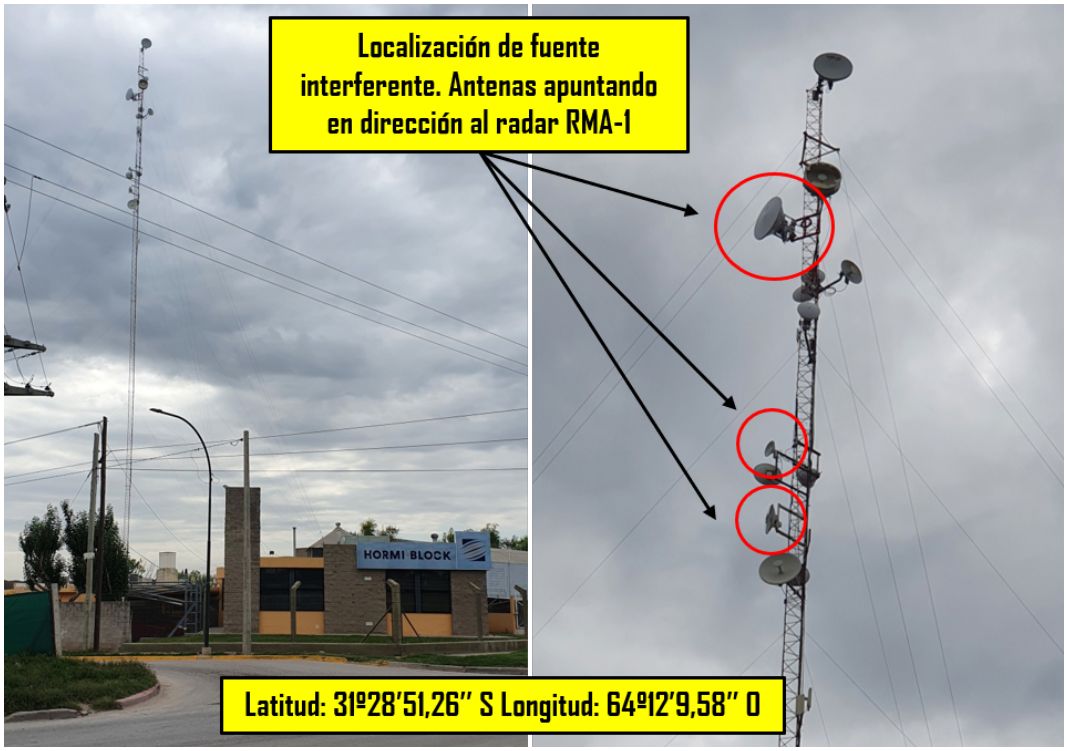


Figura 4.11: Localización de posible fuente de interferencia en una dirección acimutal específica (grupo de interferencias número 1).

Las tres antenas marcadas en rojo en la Figura 4.11 representan posibles candidatas a ser fuentes interferentes, ya que están apuntando en dirección al sitio radar. Las mismas están ubicadas a gran altura sobre un mástil arriostrado de aproximadamente 60 metros de longitud. Adicionalmente a esto, de acuerdo con las curvas de nivel, el perfil topográfico presenta una altura sobre el nivel del mar de 455,12 metros. La antena del radar RMA-1 está instalada sobre emplazamiento de 30 metros de altura y en ese punto de superficie tiene una altura sobre el nivel del mar de 436,68 metros. La topografía del terreno resulta desafiante para el funcionamiento del radar ante las ubicaciones donde se encuentran las posibles fuentes interferentes.

Registro de interferencia - Grupo 2

De acuerdo al gráfico PPI de reflectividad se describen a continuación, las características de la interferencia detectada que corresponde a una de las líneas acimutales del Grupo 2.

Cabe aclarar que esta zona de la ciudad presenta un acceso complicado y es una área densamente urbana, con edificaciones de gran altura y excesivo tránsito vehicular, ya que

cercana a la fuente interferente, circula una de las avenidas principales de la ciudad.

Desde el punto de vista radioeléctrico, es una zona en la que se espera la presencia de numerosas reflexiones de las distintas señales WLAN/RLAN provenientes de otras fuentes cercanas. Por este motivo, el parámetro de directividad en el apuntamiento de las distintas antenas utilizadas en el proceso de medición ha cumplido un rol importante, permitiendo detectar con precisión la fuente inalámbrica interferente.

En la Figura 4.12 se muestra la ejecución de la función Site Survey para la detección de las fuentes WLAN/RLAN existentes en la zona seleccionada.

48:29:52:3E:3F:DC	Payaro 5.8GHz		802.11ac	WPA	-87 / -93	5.28 / 56
F4:C1:14:ED:B2:38	Fibertel WiFi390 5.8GHz		802.11ac	WPA2	-88 / -93	5.28 / 56
90:58:51:68:31:50	Fibertel WiFi593 5.8GHz		802.11ac	WPA2	-91 / -93	5.28 / 56
48:29:52:4A:89:F2	Fibertel WiFi838 5.8GHz		802.11ac	WPA	-92 / -93	5.28 / 56
B8:66:85:15:43:C6	Superintendencia Q.O.R.I 5		802.11ac	WPA2	-86 / -93	5.28 / 56
44:AD:B1:2D:A2:CB	Fibertel WiFi761 5.8GHz		802.11ac	WPA	-90 / -93	5.28 / 56
D0:6E:DE:73:07:AC	Fibertel WiFi885 5.8GHz		802.11ac	WPA2	-75 / -93	5.28 / 56
38:3F:B3:4B:D6:F8	Decime gasti 5.8GHz		802.11ac	WPA2	-90 / -93	5.28 / 56
C0:3C:04:EE:46:8B	Equilibrio 5.8GHz		802.11ac	WPA	-77 / -93	5.28 / 56
34:49:5B:85:0C:0A	Fibertel WiFi968 5.8GHz		802.11ac	WPA	-84 / -93	5.28 / 56
6C:BA:B8:EE:98:45	Fibertel WiFi399 5.8GHz		802.11ac	WPA	-86 / -93	5.28 / 56
58:2F:F7:95:B9:35	MSOCHI 5.8GHz		802.11ac	WPA	-80 / -93	5.28 / 56
B0:FC:36:86:4C:B8	YAVORYCBA		802.11ac	WPA2	-92 / -93	5.3 / 60
84:17:EF:42:5D:18	w4rp1g2		802.11ac	WPA2	-86 / -93	5.3 / 60
08:7E:64:43:F4:E8	Fibertel WiFi791 5.8GHz		802.11ac	WPA2	-91 / -93	5.3 / 60
DC:9F:DB:6E:C9:CC	CUBO	Celda 1 Blrs	802.11n airMAX	WPA	-87 / -96	5.32 / 64
EC:BE:DD:AA:1E:A3	Fibertel WiFi037 5.8GHz		802.11ac	WPA	-82 / -96	5.32 / 64
98:77:E7:39:05:4E	Personal Wifi789 5.8		802.11ac	WPA2	-76 / -96	5.32 / 64
98:77:E7:36:8F:8D	Fibertel WiFi429 5.8GHz		802.11ac	WPA	-90 / -93	5.32 / 64
90:F8:91:68:03:4E	Fibertel WiFi333 5.8GHz		802.11ac	WPA	-86 / -93	5.32 / 64
DC:9F:DB:6E:C8:D0	CUBO S	Celda 2 Blrs	802.11n airMAX	WPA	-73 / -96	5.48 / 96
70:97:41:13:89:C9	Fibertel WiFi t7je 5.8GHZ		802.11ac	WPA2	-93 / -96	5.5 / 100
04:18:D6:E8:0E:82			airMAX AC	WPA2	-66 / -91	5.57 / 114
F0:9F:C2:EC:62:8E			airMAX AC	WPA2	-73 / -96	5.64 / 128
24:A4:3C:82:E9:CA	CDP Local	CDP - Local Cu	802.11n	WPA	-82 / -91	5.715 / 143
78:8A:20:AC:75:64			airMAX AC	WPA2	-89 / -91	5.73 / 146
80:E1:BF:3F:13:D0	Aurorq		802.11ac	WPA2	-91 / -96	5.745 / 149
2C:79:D7:79:EA:B7	Fibertel WiFi153 5.8GHz		802.11ac	WPA	-79 / -90	5.745 / 149
2C:79:D7:7A:4D:77	Fibertel WiFi884 5.8GHz		802.11ac	WPA	-85 / -90	5.745 / 149
44:AD:B1:2D:D4:18	Fibertel WiFi102 5.8GHz		802.11ac	WPA	-81 / -90	5.745 / 149
60:14:B3:2F:04:F8	Fibertel WiFi766 5.8GHz		802.11ac	WPA2	-89 / -90	5.745 / 149

Figura 4.12: Site Survey para la detección de las distintas fuentes WLAN/RLAN.

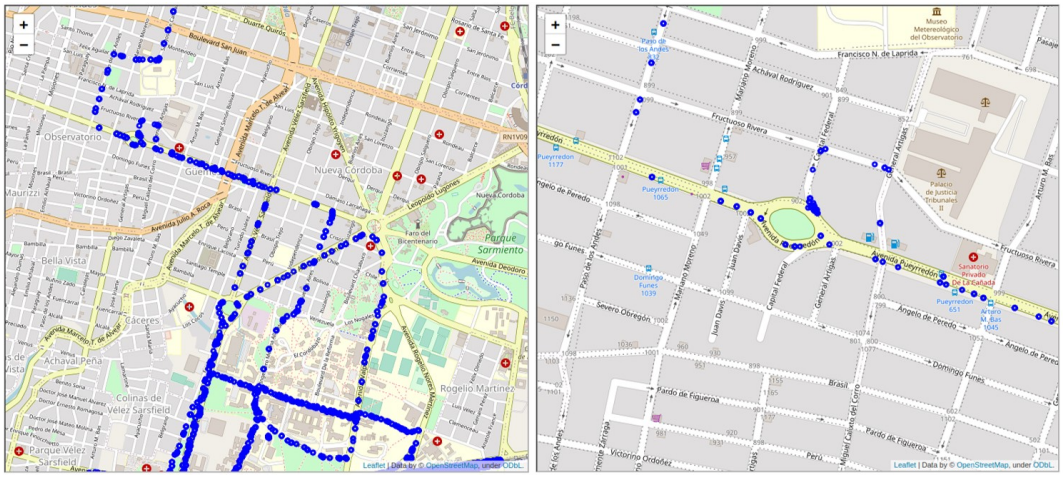


Figura 4.13: Datos del GPS correspondientes a las fuentes detectadas cercanas a la interferencia.

En la imagen anterior se muestra un transmisor con dirección física MAC F0:9F:C2:EC:62:8E en modo airMAX con una frecuencia de operación de 5.640 MHz - canal 128 (canal DFS).

Luego, en la Figura 4.13 se observa las fuentes WLAN/RLAN detectadas en ruta con el proceso de War-Driving. Cada punto de color azul que figura en el mapa es una red inalámbrica detectada por el software Kismet con información de latitud y longitud estimada.

En la Figura 4.14 se presenta la gráfica del analizador de espectro con la transmisión del radar y de la interferencia detectada resaltadas en color amarillo y rojo respectivamente.

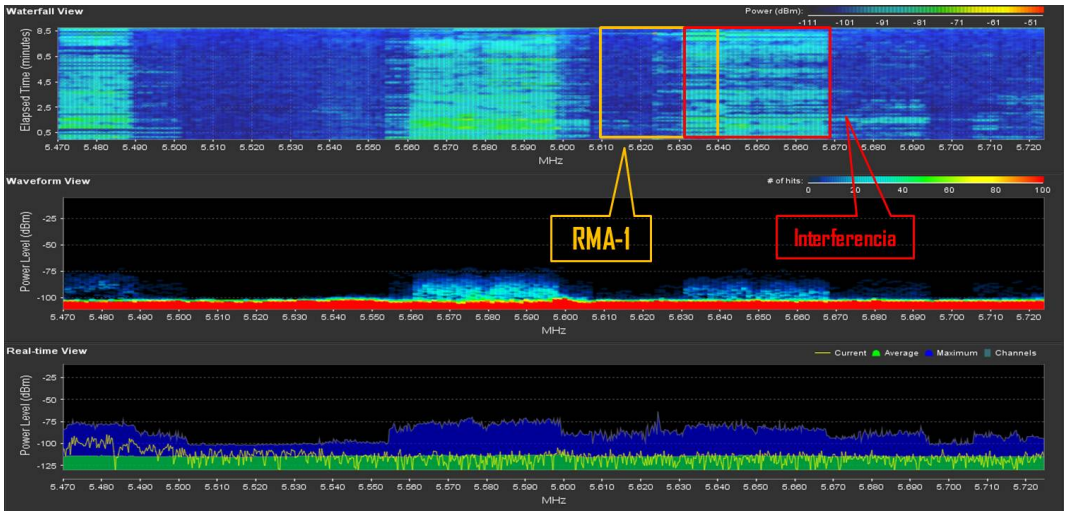


Figura 4.14: Transmisiones de los dispositivos en función de la frecuencia.

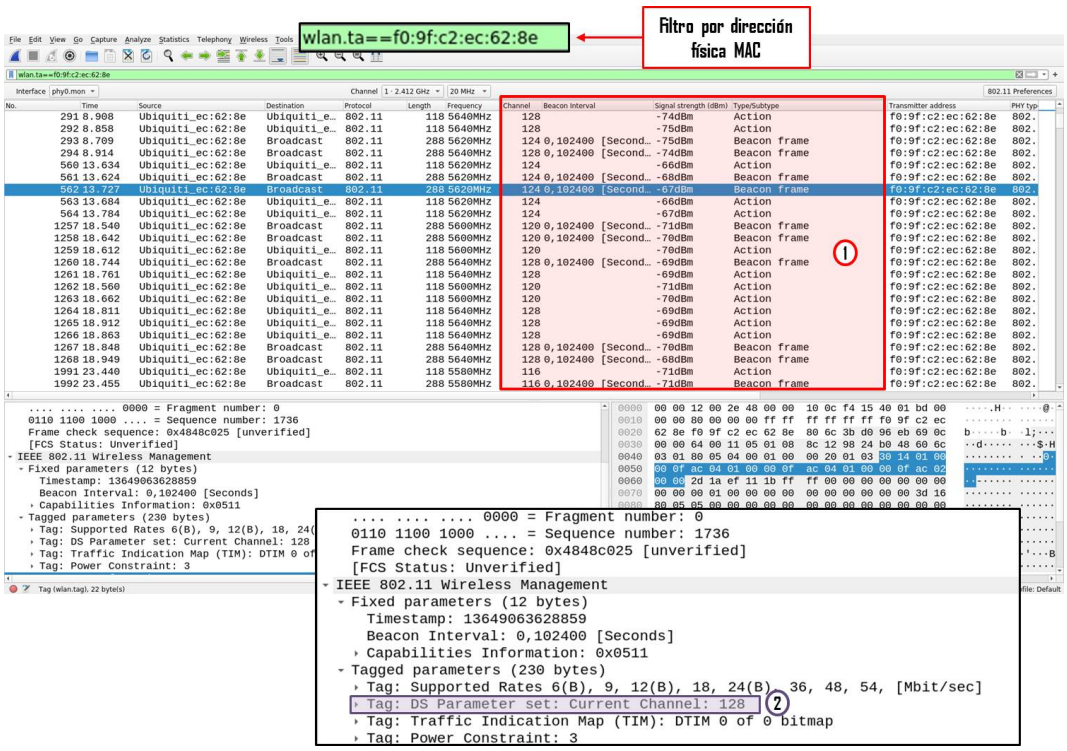


Figura 4.15: Auditoría del tráfico inalámbrico.

En la Figura 4.15 se presenta en forma detallada el tráfico de tramas inalámbricas

transmitidas. Se aplica el filtro por dirección MAC para visualizar sólo los datos de interés. En el área de captura se muestran algunos de los canales de ocupación (señalado con el número 1 - color rojo) para la transmisión continua de paquetes “Action” y “Beacon Frames”.

Además, se observa que el canal de operación del AP interferente es el 128 (marcado con el número 2 - color púrpura), tal como lo indica la función Site Survey. Esto significa que, al tener activado el modo airMAX, puede transmitir tramas Beacon en todo el ancho de banda diponible, propagando sus Beacons para mantener la conexión entre sus distintos clientes.

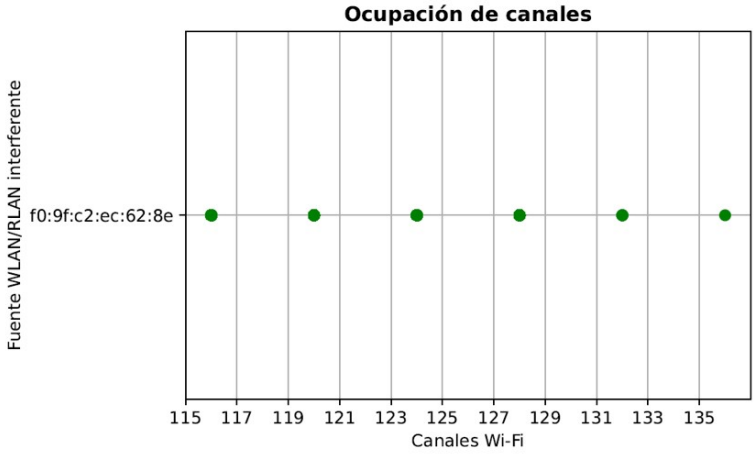


Figura 4.16: Ocupación de canales para la transmisión de las distintas tramas.

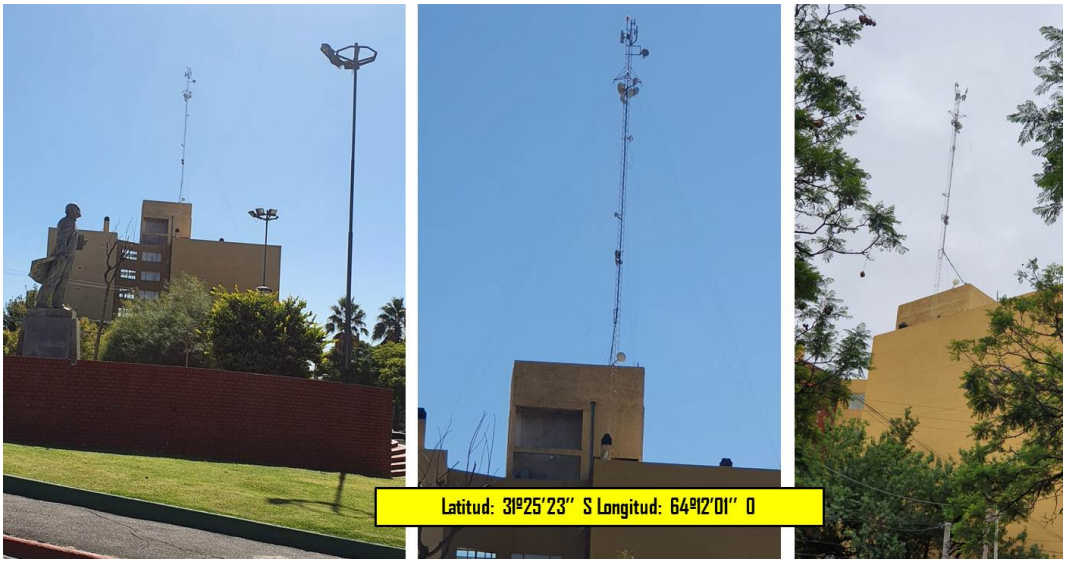


Figura 4.17: Localización de la interferencia con los datos de latitud y longitud.

En la Figura 4.16 se muestra la ocupación completa de los canales. A diferencia de la Figura 4.15, se observa que el AP también tiene a disposición los canales 132 y 136 para la propagación de la señal WLAN/RLAN de los canales ya mostrados en el recuadro en color rojo en el área de captura.

Luego, en la Figura 4.17 se muestra la localización de la posible fuente interferente. Asimismo, se observa que las antenas están instaladas en una torre de aproximadamente 15

metros de altura emplazada sobre un edificio de 25 metros, es decir, se aprovecha la altura de las edificaciones para una línea de vista clara y despejada de obstáculos.

Con los datos recopilados de la medición en campo, se infiere que en esta torre se encuentra el dispositivo WLAN/RLAN que afecta al funcionamiento del radar debido a la transmisión de sus tramas en distintos canales del espectro.

Registro de interferencia - Grupo 3

En la Figura 4.18 se presenta el análisis en función de la frecuencia de la transmisión del dispositivo interferente y la actividad del pulso radar.

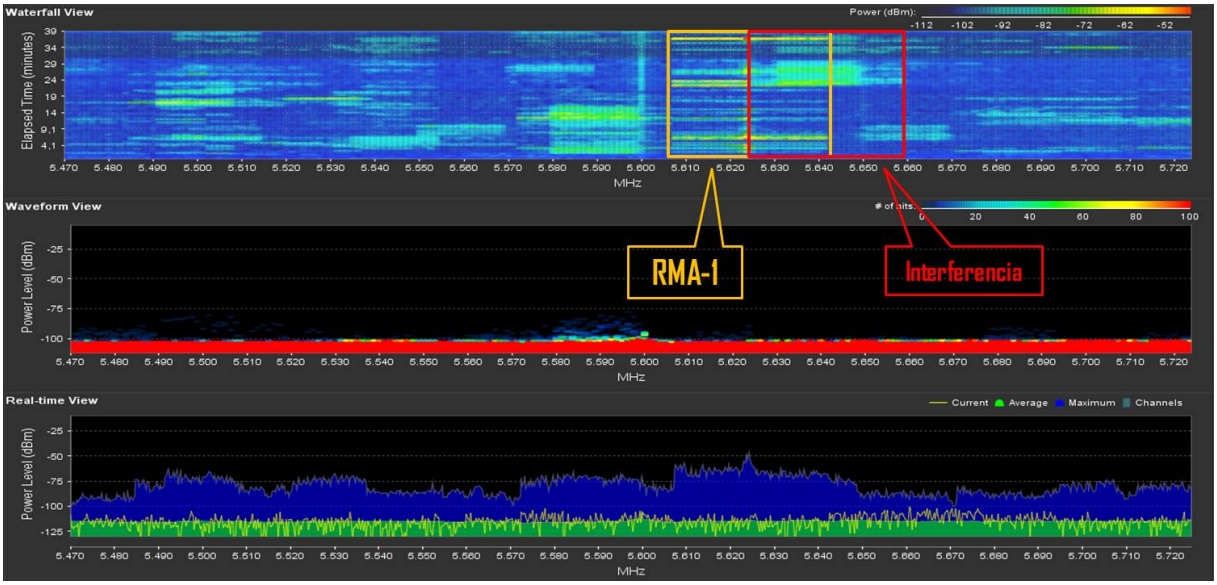


Figura 4.18: Actividad de transmisión.

MAC Address	SSID	Device Name	Radio Mode	Encryption	Signal / Noise, dBm	Frequency, GHz / Channel
A8:6A:BB:E2:61:23	LA MALUCA SRL 5.8GHz		802.11ac	WPA	-80 / -91	5.28 / 56
98:77:E7:38:B0:9F	Fibertel WiFi125 5.8		802.11ac	WPA2	-91 / -91	5.32 / 64
6C:55:E8:BA:FD:E8	MINIS TRAB 5.8GHz		802.11ac	WPA	-84 / -91	5.32 / 64
58:C1:7A:15:C8:81	FCA		802.11ac	WPA2	-78 / -89	5.5 / 100
58:C1:7A:15:C8:82	eduroam		802.11ac	WPA2	-80 / -89	5.5 / 100
58:C1:7A:15:C8:80	unc-libre		802.11ac	NONE	-78 / -89	5.5 / 100
F0:9F:C2:EC:61:C0			airMAX AC	WPA2	-66 / -96	5.64 / 128
70:4F:57:CA:A4:9B	ADIUCaula		802.11ac	WPA	-89 / -96	5.745 / 149
82:2A:A8:C8:EA:44	Gremial6		802.11ac	WPA2	-89 / -96	5.745 / 149
FE:EC:DA:05:CC:9B	FCA Residencia		802.11ac	WPA2	-84 / -88	5.745 / 149
0E:EC:DA:05:CC:9B			802.11ac	WPA2	-84 / -88	5.745 / 149
48:57:02:B0:8D:2C	aguero		802.11ac	WPA2	-90 / -96	5.745 / 149
A4:00:E2:3A:66:34	Clarowifi765		802.11ac	WPA2	-83 / -88	5.745 / 149
FC:EC:DA:05:CC:9B	FCA Aula SUR		802.11ac	NONE	-85 / -88	5.745 / 149
3C:B7:4B:61:D8:60	Fibertel WiFi986 5.8GHz		802.11ac	WPA2	-92 / -96	5.765 / 153
14:DD:A9:6F:EF:68	Codeler_5G-2		802.11ac	WPA2	-85 / -96	5.805 / 161

Figura 4.19: Barrido de frecuencia con Site Survey.

En el barrido de frecuencias mostrado en la Figura 4.19 se resalta en rojo la detección del dispositivo WLAN/RLAN cuya dirección física MAC es F0:9F:C2:EC:61:C0 y tiene habilitado el modo airMAX en el canal 128 (5.640 MHz). Además, tomando como referencia la potencia de recepción (-66 dBm) y la designación de las redes existentes según el nombre lógico (SSID),

se elabora una ruta de recorrido con el fin de localizar la ubicación de la fuente en las inmediaciones del radar.

En la Figura 4.20 se observa sobre el mapa el recorrido establecido y las fuentes WLAN/RLAN detectadas con sus datos del GPS.

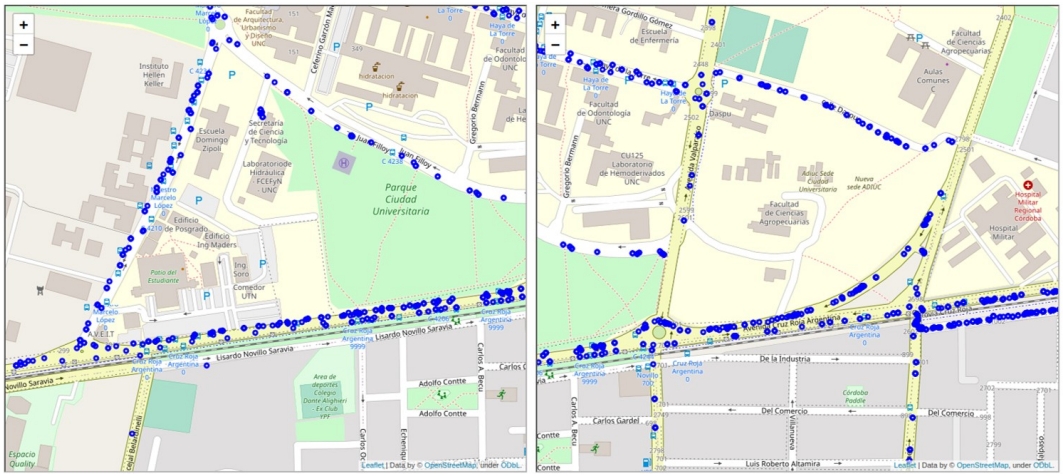


Figura 4.20: Mapa con información estimada de latitud y longitud de fuentes situadas cerca del sitio radar.

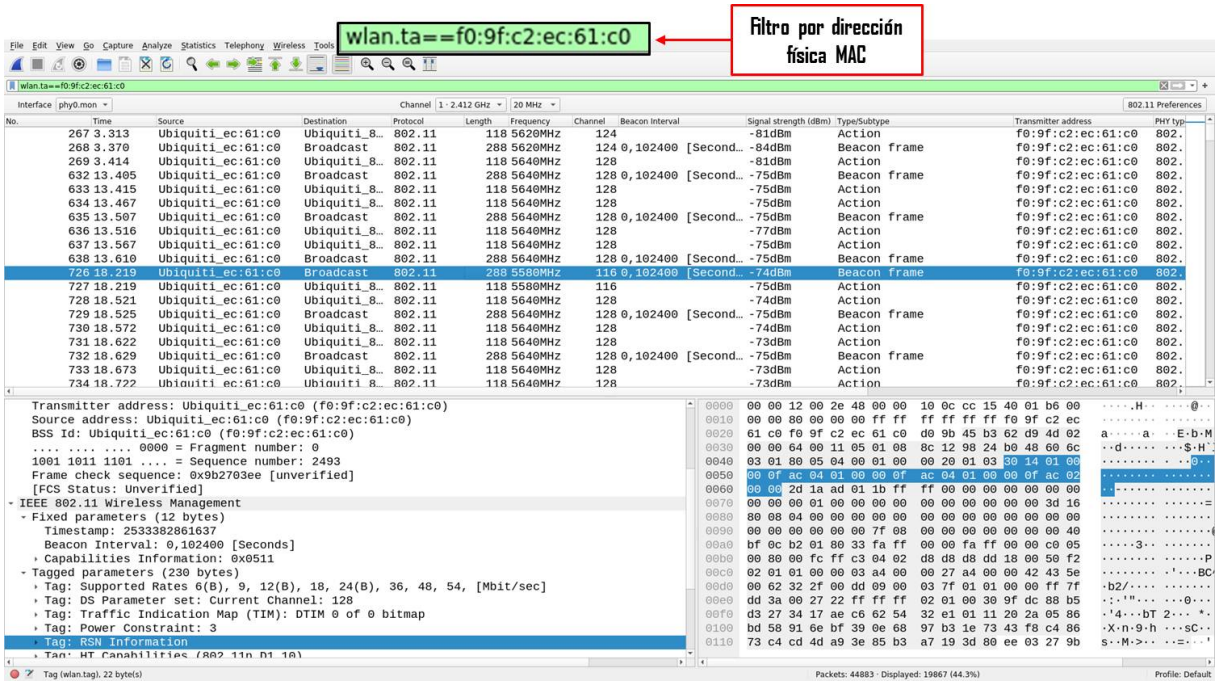


Figura 4.21: Tráfico de tramas inalámbricas de la fuente interferente.

En lo referente al tráfico inalámbrico mostrado en la Figura 4.21, esta fuente interferente presenta características similares a las del dispositivo WLAN/RLAN detectado anteriormente. En la Figura 4.22 se muestra que el canal de operación de la fuente es el 128 (frecuencia central 5.640 MHz) y propaga tramas Action y Beacons en los canales adyacentes ocupando todo el ancho de banda.

Finalmente, en la Figura 4.23, se presenta la localización de la que se infiere que es la fuente de interferencia, que está ubicada en una torre de 12 metros emplazada sobre un edificio de aproximadamente 15 metros de altura.

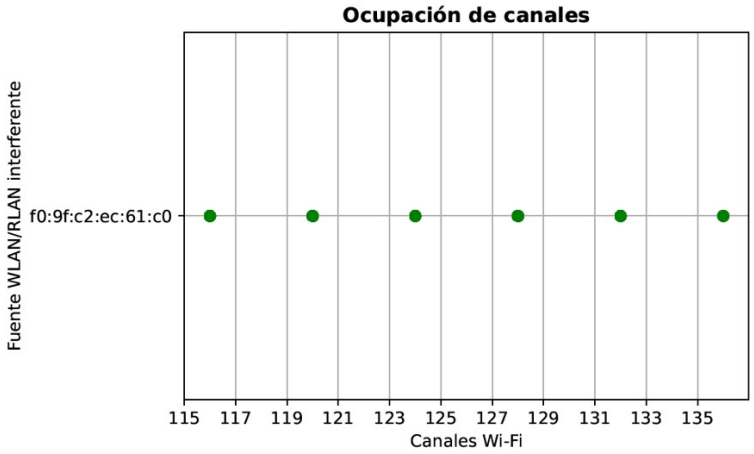


Figura 4.22: Ocupación de canales para la transmisión de tramas inalámbricas.

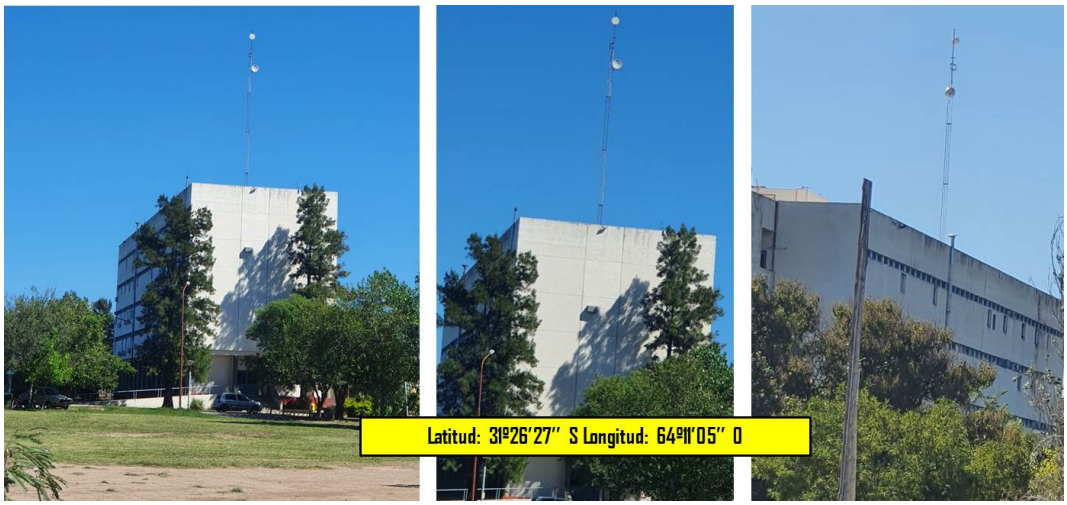


Figura 4.23: Localización de la interferencia en un sitio cercano al radar.

Registro de interferencia - Grupo 4

La fuente interferente detectada que pertenece al Grupo 4, según lo determinado con el PPI de reflectividad, está situada en una zona de la ciudad con acceso restringido por tratarse de un barrio privado. Una vez más, los parámetros de ganancia y directividad de las antenas utilizadas en el proceso de medición para la recepción de los datos han cumplido un rol importante teniendo en cuenta la distancia a la cual se encontraban los dispositivos WLAN/RLAN con respecto al punto de recolección.

El registro de la actividad en función de la frecuencia se muestra en la Figura 4.24 en paralelo a la transmisión del pulso radar.

Luego, en la Figura 4.25 se observa el recorrido empleado con la información GPS de las distintas redes inalámbricas detectadas en la zona.

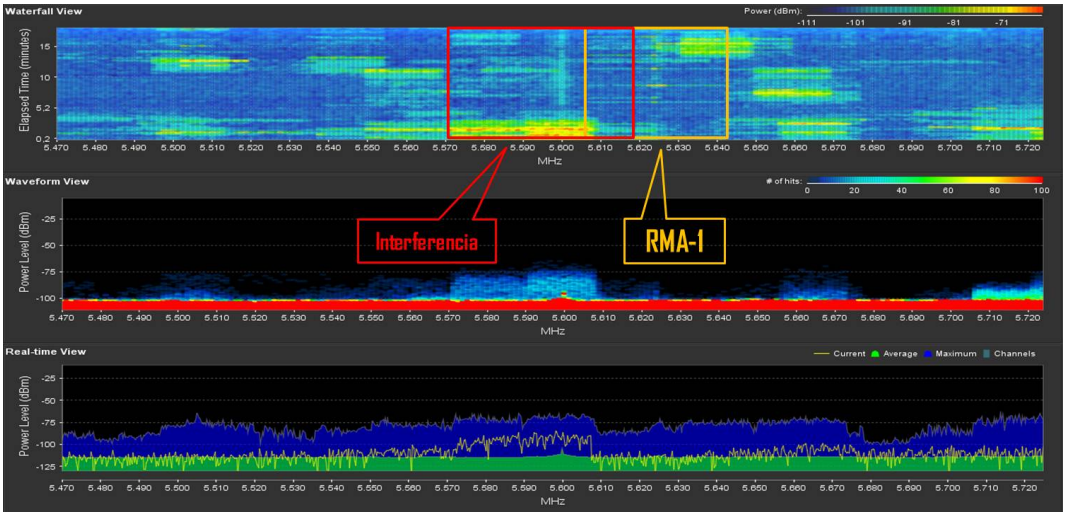


Figura 4.24: Actividad de transmisión en el espectro radioeléctrico.

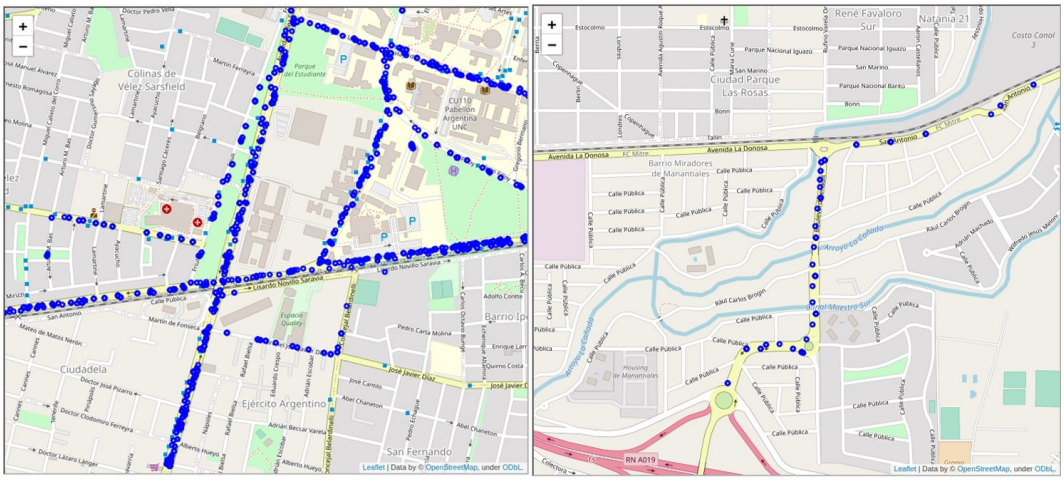


Figura 4.25: Recorrido con el anexo de datos GPS.

Una vez seleccionado el punto para la recolección de los datos se ejecuta la función Site Survey para generar más información acerca de las redes. Esto se muestra en la Figura 4.26, y se identifica un transmisor con la dirección física MAC 78:8A:20:6C:A4:A5 en el canal 120 (5,6 GHz) con función airMAX activada.

Repitiendo el procedimiento de los casos anteriores, se filtra las tramas por dirección MAC empleando el software Wireshark. En la Figura 4.27 se observa la actividad de la fuente WLAN/RLAN alternando los canales 120 y 124 para la transmisión de tramas Action, Beacon Frame y QoS Data. También, se verifica que la frecuencia central de operación del dispositivo es el 120 (5.600 MHz) resaltado en color naranja (número 1 en la imagen) cuando se selecciona la trama de gestión Beacon Frame y se desglosa por capas.

MAC Address	SSID	Device Name	Radio Mode	Encryption	Signal / Noise, dBm	Frequency, GHz / Channel
80:2A:A8:0E:F7:CA	ASAT-WIFITORRES	ASAT-TMAN-AP02	802.11n airMAX	WPA2	-84 / -96	5.16 / 32
D8:07:B6:1A:64:E4	PixelHouse		802.11ac	WPA2	-89 / -95	5.18 / 36
00:27:22:14:FC:87	ifdt-mana-este	ifdt-mana-este	802.11n airMAX	WPA2	-87 / -92	5.37 / 74
DC:9F:DB:6E:C4:AB	ifdt-mana-oeste	ifdt-mana-oest	802.11n airMAX	WPA2	-75 / -90	5.4 / 80
24:A4:3C:78:62:86	ifdt-mana-sur	ifdt-mana-sur	802.11n airMAX	WPA2	-85 / -91	5.5 / 100
74:83:C2:A6:38:8D			airMAX AC	WPA2	-81 / -91	5.505 / 101
DC:9F:DB:6A:10:45	ifdt-mana-torre01	ifdt-mana-torr	802.11n airMAX	WPA	-87 / -92	5.57 / 114
78:8A:20:6C:A4:A5			airMAX AC	WPA2	-66 / -90	5.6 / 120
F4:92:BF:48:27:0F			airMAX AC	WPA2	-87 / -90	5.665 / 133
E0:63:DA:D8:2C:53			airMAX AC	WPA2	-89 / -91	5.67 / 134
78:8A:20:1E:FF:4E	AdM-Sureno	Riberas-AP	802.11n airMAX	WPA2	-78 / -90	5.815 / 163
74:AC:B9:86:D6:6D			airMAX AC	WPA2	-64 / -89	5.85 / 170
18:E8:29:D2:78:FB	ifdt-ptp-manantiales-torres	ifdt-ptp-manan	802.11n airMAX	WPA2	-88 / -90	5.96 / 192

Figura 4.26: Site Survey para la detección de las distintas fuentes WLAN/RLAN en la zona restringida.

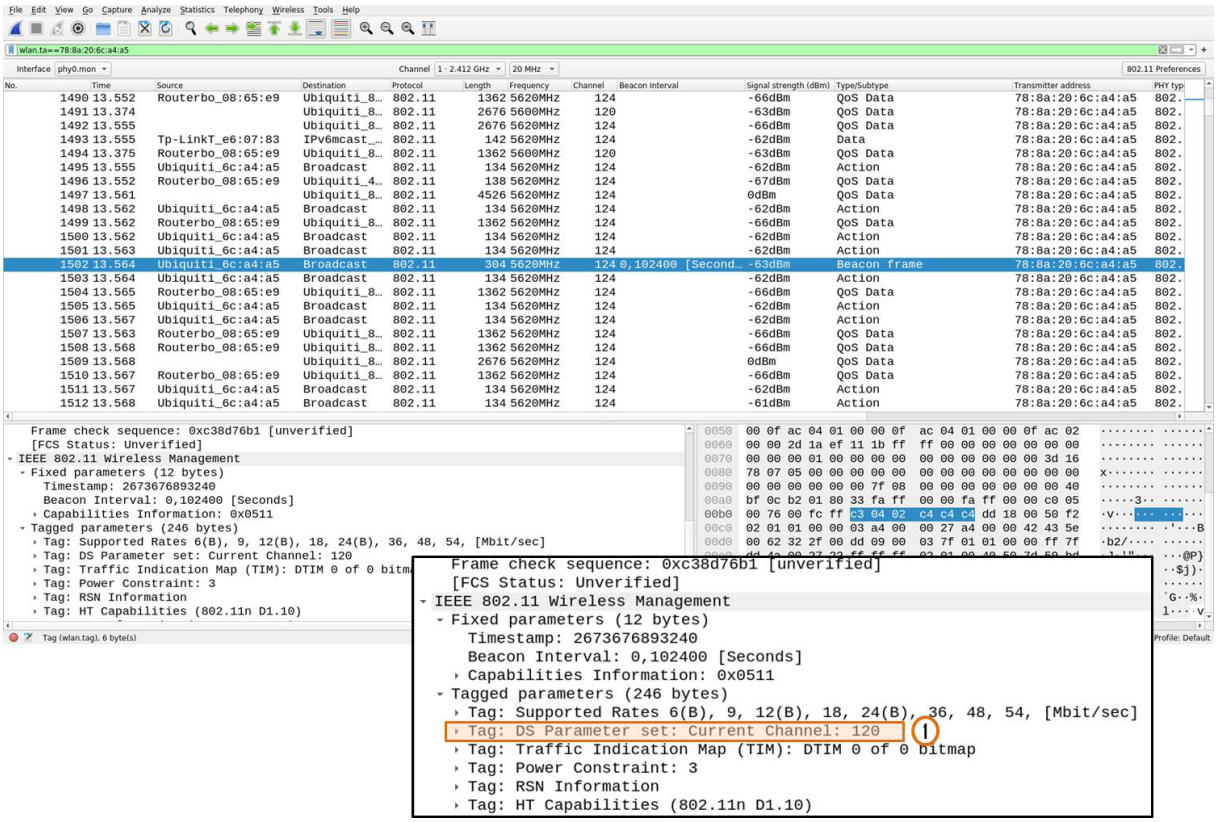


Figura 4.27: Captura de las tramas inalámbricas con software Wireshark.

En la captura de Wireshark presentada en la Figura 4.27, la fuente ocupa solamente los canales 120 y 124 para la transmisión de las tramas. Sin embargo, luego del procesamiento de los datos utilizando Jupyter Notebook, se obtiene una imagen más completa de la totalidad de los canales utilizados por el AP representada en la Figura 4.28. Esta fuente utiliza un ancho de banda mucho mayor comparado con el resto de las interferencias detectadas, ocupando los canales 112, 116, 120, 124, 128, 132 y 136 para la transmisión de los paquetes.

En la Figura 4.29 se observa que las antenas que generan interferencia están instaladas sobre edificaciones de menor altura (aproximadamente a 12 metros sobre el suelo).

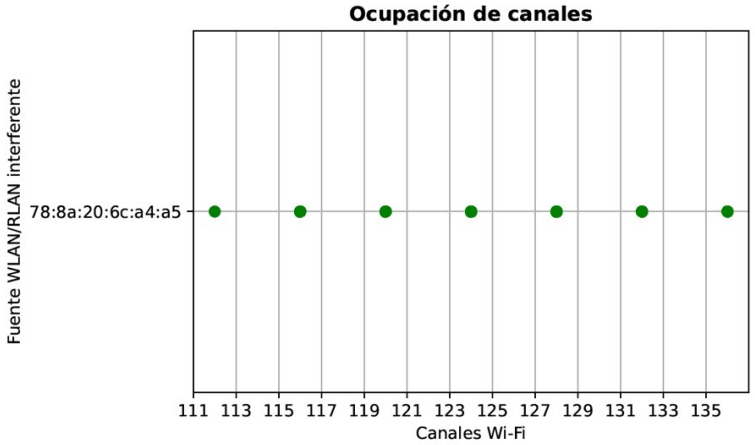


Figura 4.28: Ocupación completa de canales.

Figura 4.29: Localización de fuente interferente situada en un barrio privado.

Lo que influye en este zona de la ciudad es la altura sobre el nivel del mar considerando las curvas de nivel del perfil topográfico en comparación con el sitio radar. Esto impacta directamente en la transmisión del radar considerando que está emplazado sobre una torre de 33 metros sobre el suelo. Esto se esquematiza en la Figura 4.30, cuyo perfil topográfico está representado junto con la línea de vista entre el radar RMA-1 y el dispositivo WLAN/RLAN que genera interferencia detectado a una distancia de 4,36 Km.

A diferencia de los tres registros de interferencia anteriores, en este caso el entorno no permite acorralar los dispositivos WLAN/RLAN identificados, a partir del acercamiento a los mismos y aplicar la estrategia War-Driving en su alrededor. Sin embargo, los datos recolectados en el proceso de medición, sumado al estudio del perfil topográfico y el apuntamiento de las antenas, llevan a suponer que la fuente interferente se encuentra ubicada en la edificación mostrada en la Figura 4.29. Teniendo en cuenta el espíritu del presente trabajo, con este procedimiento se llega a la conclusión de que al menos es una ubicación a ser considerada para una inspección

de los entes de autoridad reguladora en materia de comunicaciones.

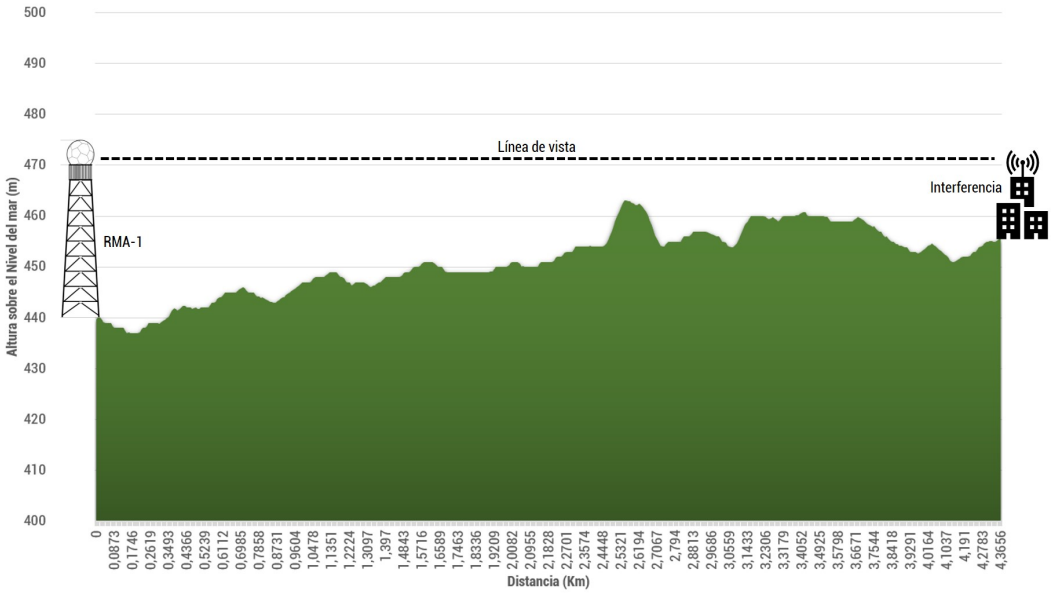


Figura 4.30: Perfil topográfico y línea de vista entre el sitio radar y la interferencia.

4.4 Ingeniería Inversa

La ingeniería inversa es un recurso valioso y representa un proceso que identifica las propiedades y características de un objeto de estudio mediante la realización de un análisis exhaustivo de su estructura de funcionamiento y operación.

En particular, este análisis se traslada, tomando como referencia los resultados finales obtenidos, a la implementación de un ensayo de laboratorio con el fin de realizar evaluaciones y mediciones de los dispositivos WLAN/RLAN detectados para obtener más información acerca de cómo impactan sus funciones en el espectro radioeléctrico.

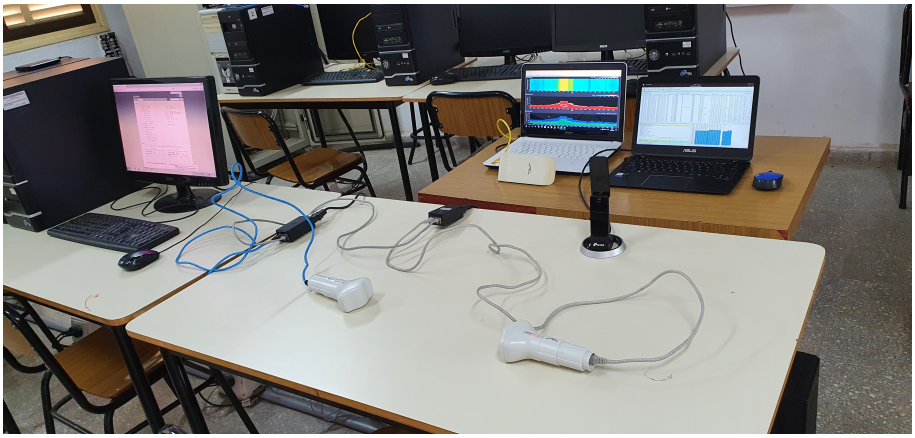
En primer lugar, estas mediciones de laboratorio se llevaron a cabo en el Laboratorio de Redes de la Facultad de Ingeniería del Centro Regional Universitario Córdoba IUA. Gran parte del equipamiento y recursos de hardware es provista por la misma institución en calidad de préstamo.

Para el experimento se configuró un enlace punto a punto de microondas a corta distancia con valores de potencia al mínimo utilizando el equipo Ubiquiti airGRID M5 HP compuesto de dos nodos, cada uno conectado a una computadora de escritorio para el control de sus parámetros internos de configuración. Este enlace posee características similares en cuanto a funcionamiento que los dispositivos localizados en campo.

En la Figura 4.31a se muestran las dos PCs que representan el Transmisor (TX) en modo AP (izquierda) y el Receptor (RX) en modo estación (derecha) según la disposición de la imagen. El TX tiene configurada la dirección IP 192.168.1.22 y el RX la dirección IP 192.168.1.20. Por lo tanto, las tarjetas de red de las dos PCs deben tener direcciones IP compatibles que

pertenecen a la misma subred. En la Figura 4.31b se muestra el equipamiento usado en el proceso de War-Driving, una computadora portátil con Windows 10 para acceder al analizador de espectro del dispositivo Ubiquiti NanoStation Loco M5; y una segunda computadora portátil con sistema Linux Ubuntu para acceder a la captura de tramas inalámbricas en tiempo real recolectadas con el receptor inalámbrico USB externo y el software Wireshark.

(a) Configuración de los nodos TX y RX



(b) Equipamiento War-Driving

Figura 4.31: Despliegue de componentes para el ensayo de laboratorio.

Entre el TX y el RX se transmite un archivo de aproximadamente 21 GB de tamaño para mantener estable la lectura de la interfaz de aire. Además, se activan las funciones “airMAX” y “airSELECT” para verificar el desempeño del enlace en el espectro radioeléctrico.

Se selecciona una frecuencia cercana al radar para configurar en el enlace el canal central de operación (canal 124 - 5.620 MHz).

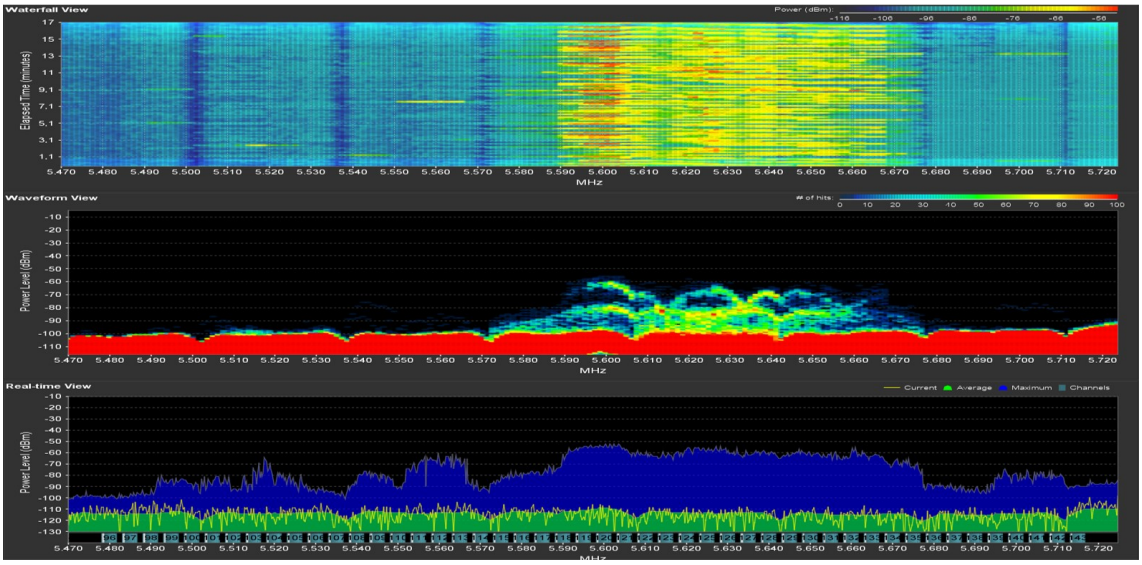
En la Figura 4.32a se observa el comportamiento del enlace en función de la frecuencia. Para transmitir el archivo distribuye los datos en varios canales del ancho de banda para evitar la saturación y mantener la calidad en la transmisión.

El uso de canales adyacentes dentro de la banda de frecuencias se muestra en la Figura 4.32b. Se aplica el filtro en el Wireshark para observar los datos de interés. El filtro está compuesto

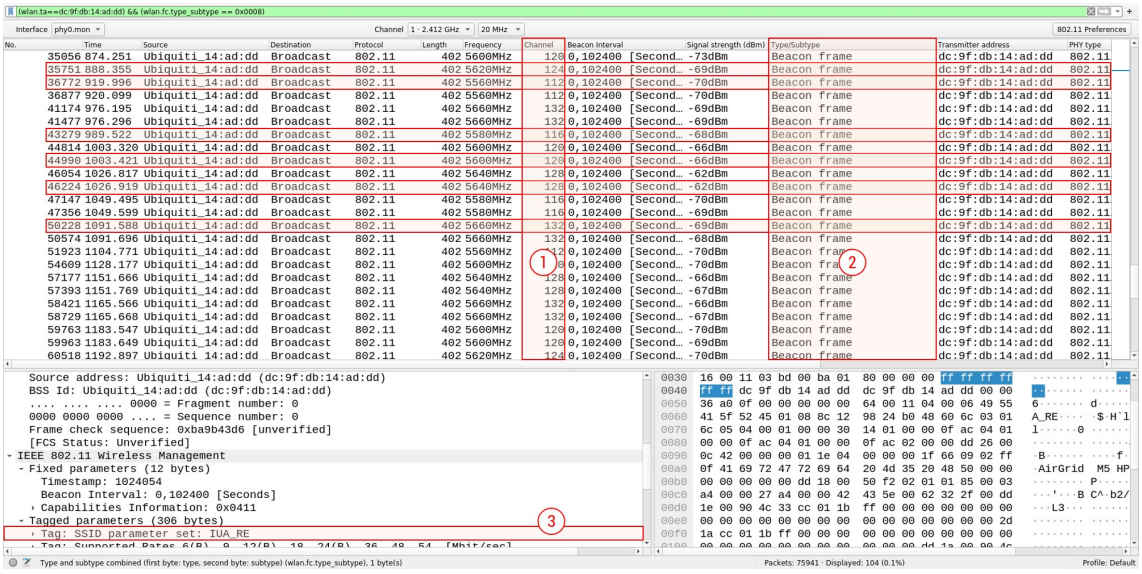
por los siguientes parámetros:

```
(wlan.ta == dc:9f:db:14:ad:dd) && (wlan.fc.type_subtype == 0x0008)
```

El primer término corresponde a la dirección física del AP configurado como TX y el segundo término se refiere al subtipo de trama que, en este caso, el valor hexadecimal 0x0008 corresponde a la subtrama de Gestión "Beacon Frame" (columna remarcada con el número 2). Además, se observa el SSID o dirección lógica del enlace marcada con el número 3. La ocupación de canales en tiempo real corresponde al área resaltada con el número 1.



(a) Visualización del espectro en tiempo real



(b) Auditoría de red mediante Wireshark

Figura 4.32: Resultados de la medición de laboratorio.

En la Figura 4.32 se observa la contaminación del espectro generada por la transmisión Tramas Beacons principalmente en los canales 112, 116, 120, 124, 128 y 132. Cabe aclarar

que la información mostrada corresponde sólo a las tramas mencionadas anteriormente. Sin embargo, este dispositivo ocupa más canales en todo el ancho de banda para transmitir en paralelo las Tramas de Datos puros.

Para el uso del protocolo "airSELECT" es necesario desbloquear una función que habilita todos los canales disponibles en la banda de 5 GHz y que tiene prioridad por sobre los canales DFS que generalmente se reservan para el uso de radares meteorológicos según la regulación del país. Es decir, aún cuando el sistema DFS del AP esté activado, la selección de canales que realiza el protocolo airSelect tiene prioridad y automáticamente ignora el rol que tiene el parámetro DFS con respecto a la detección de radares. Esta función se denomina "**Compliance Test**"y se activa en casi todas las versiones mediante lenguaje de consola.

En la Figura 4.33 se observa la habilitación de dicha función, y se verifica en el área de desglose por capas de una trama Beacon el parámetro "**Tag: Country Information: Country Code UB, Environment Any**".

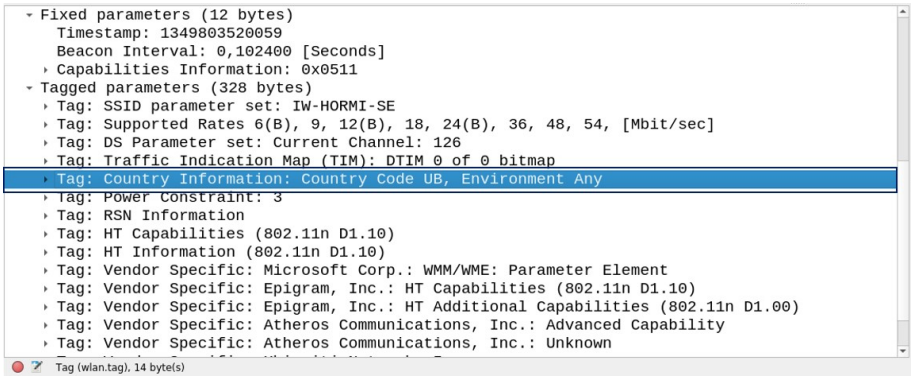


Figura 4.33: Función Compliance Test activada.

En modo normal el fabricante debe cumplir con las normas y reglamentaciones del país, pero la habilitación de esta función implica actuar de manera indebida de acuerdo a las legislaciones vigentes, permitiendo usar canales legales y hasta configurar equipos con valores de potencia de transmisión por encima de 30 dBm.

A través del ensayo de Ingeniería Inversa, se concluye que:

- en modo normal, puede asociarse cualquier cliente al enlace, el cual actúa como un AP inalámbrico convencional;
- en modo airMAX, sólo se pueden asociar clientes o estaciones compatibles con el protocolo propietario en cuestión;
- en modo airSELECT, se prioriza la selección de canales libres por sobre frecuencias DFS. Para esto es necesario, la habilitación de la función "Compliance Test".

4.5 Reflexiones Finales

Las fuentes WLAN/RLAN detectadas disponen de un protocolo que funciona de forma análoga a la tecnología TDMA (*Time-Division Multiple Access*, Acceso Múltiple por División del Tiempo). Se denomina "**airMAX**" y consiste en asignar ranuras, es decir intervalos de tiempo de transmisión, a cada cliente estableciendo diferentes prioridades. Esto implica definir la longitud del intervalo de tiempo destinado a cada cliente de acuerdo a la prioridad, buscando de este modo mejorar el rendimiento de la red respecto a la disponibilidad de ancho de banda. Aquellos clientes con prioridad más alta tienen acceso a más tiempo del AP para intercambiar paquetes de voz y datos con la menor latencia posible.

Para competir por el uso del espectro, estos equipos emplean una tecnología llamada "**airSelect**" que evita las interferencias producidas por otros dispositivos WLAN/RLAN. Para proporcionar un incremento en el rendimiento de la red, este protocolo cambia de canal inalámbrico a través de saltos periódicos siguiendo una lista de frecuencias disponibles. El AP realiza un barrido en los canales disponibles en búsqueda de niveles de interferencias y menor piso de ruido. Si estos canales están limpios los usa un cierto tiempo (habitualmente 3000 milisegundos) antes de realizar un salto al siguiente canal disponible. Cada 100 milisegundos el AP enviará un anuncio con información sobre el próximo salto a sus clientes conectados. Dependiendo de la estrategia que esté utilizando el radar, estos valores son insuficientes, provocando que el dispositivo WLAN/RLAN vuelva a utilizar el canal antes de que el radar haya emitido en esa dirección nuevamente.

En cuanto a capacidad técnica, estos dispositivos WLAN/RLAN en particular disponen de protocolos agresivos para poder explotar sus funcionalidades al máximo y aprovechar un recurso tan escaso como el espectro de radiofrecuencia. Las tecnologías airMAX y airSelect en conjunto son utilizadas para que el AP pueda transmisitir sus tramas Beacon y facilitar al usuario (cliente) la búsqueda de estas redes. Un cliente busca un AP por su SSID y no por su frecuencia utilizando el escaneo activo. En este sentido, el AP propaga estas tramas en todos los canales que componen su ancho de banda total. Esta actividad se ha registrado en las otras fuentes inalámbricas interferentes detectadas y que quedó en evidencia mediante el recurso de la Ingeniería Inversa aplicada a dichos transmisores.

Capítulo 5

Conclusiones y Trabajo Futuro

5.1 Conclusiones

En esta tesis se aborda uno de los principales problemas que enfrentan los radares meteorológicos de la red SINARAME y se trata de la presencia de interferencia de RF generada por la actividad de transmisión de dispositivos WLAN/RLAN en regiones del espectro cercanas, en la banda C (4 - 8 GHz) y que es compartida con este tipo de transmisores de redes inalámbricas.

En particular, se propuso un procedimiento de medición que permite medir, caracterizar y localizar las señales inalámbricas WLAN/RLAN que degradan el desempeño de los radares meteorológicos. Posee la ventaja de ser un método simple, que integra hardware y software de bajo costo, en comparación con el instrumental involucrado en los procedimientos convencionales que se ejecutan utilizando equipos de medición homologados, como por ejemplo, analizadores de espectro de última generación denominados "cazadores de interferencias" equipados con un módulo de recepción GPS y antenas directivas para rastrear señales de acuerdo a su comportamiento en el espectro radioeléctrico.

Asimismo, el procedimiento que se presenta en este trabajo no solo es eficiente para identificar y localizar señales interferentes, sino también para caracterizar cada una de ellas a nivel de protocolo en referencia al estándar inalámbrico IEEE 802.11. El aporte que brinda la captura de tráfico inalámbrico de la fuente de interferencia, adicionalmente a su actividad en función de la frecuencia, es de valiosa importancia ya que permite entender su modo de funcionamiento en su intento por convivir y competir por el uso del espectro.

Con respecto a los resultados obtenidos, cabe destacar que las fuentes interferentes detectadas presentan características muy similiares en cuanto a su actividad de transmisión en el espectro, puesto que todas coinciden en el fabricante. Mediante las capturas de las

tramas y paquetes inalámbricos queda demostrado que estos equipos tienen un comportamiento robusto y potente que contaminan el espectro radioeléctrico empleando diferentes técnicas de transmisión (airMAX, airSELECT y Compliance Test) en la totalidad del ancho de banda configurado y que, para competir por la ocupación de mayor porción del espectro, priorizan el uso de canales libres, canales con transmisión de otros servicios y canales reservados para la actividad de los radares meteorológicos, ignorando por completo funciones esenciales como la habilitación del parámetro DFS.

Desde el punto de vista técnico, estos equipos presentan una solución favorable, pero aparentemente ignoran tanto parcial como de forma completa las regulaciones legales vigentes. En este marco, la dificultad máxima se plantea en el incumplimiento normativo del artículo 5° inciso 5.1 de la Resolución 581/2018, que establece que las emisiones de las bandas de frecuencias de uso compartido no podrán causar interferencias a las estaciones autorizadas de un servicio autrorizado en dichas bandas con atribución a título primario. Que asimismo, por el inciso 5.2 del citado artículo, el usuario de bandas de frecuencias de uso compartido que causare interferencia perjudicial a una estación de un servicio autorizado en la banda con atribución a título primario, deberá suspender la emisión y no podrá reanudarla hasta que se haya subsanado el conflicto interferente. En el caso de la potencia de emisión, y ante el uso compartido de la misma banda de frecuencias con el radar (rango 5.470-5.600 MHz y 5.650-5.725 MHz de acuerdo al registro de frecuencias utilizadas en las capturas de paquetes de las fuentes interferentes), los equipos WLAN/RLAN pueden transmitir como valor máximo según la normativa, una potencia conducida de 24 dBm y una P.I.R.E (Potencia Isotrópica Radiada Efectiva) de 30 dBm. Si estos dispositivos emplean la función “Compliance Test” tienen la posibilidad de incumplir la normativa tanto en la configuración de frecuencias como también los valores de potencia de transmisión.

En el modo de escaneo activo, el cliente también difunde sus tramas Probe Request en todos los canales disponibles del espectro, con menor potencia, para asociarse a un AP específico. En zonas cercanas al radar con alta demanda de usuarios conlleva a un consumo de tiempo de la interfaz de aire en envíos de tramas por parte del AP en respuesta a la petición de los nodos perjudicando la actividad de recepción del propio radar en forma directa.

El perfil topográfico también es una variable a considerar, sobre todo en el sitio donde están emplazadas las fuentes interferentes. La irregularidad del terreno y los accidentes geográficos afectan en las transmisiones de microondas. Para compensar las pérdidas producidas por atenuación en el espacio libre, margen de fading, pérdidas por difracción en los elipsoides de fresnel, entre otros, estos equipos se instalan a gran altura en torres de telecomunicaciones y/o infraestructura existente. En aquellos casos de equipos instalados a baja altura respecto del suelo, las curvas de nivel en ese punto juegan un papel importante para aprovechar la altura sobre le nivel del mar en las transmisiones de datos produciendo interferencias a otros sistemas y servicios.

Asimismo, en cuanto a la selección de frecuencias para la transmisión en la misma banda que comparte con el radar, existe la posibilidad de que el usuario pueda deshabilitar la función DFS

y el dispositivo puede operar en un canal con menos interferencia de equipos WLAN/RLAN presentes en el entorno, ya que los dispositivos con parámetro DFS habilitado dejarán el canal libre al detectar emisiones radar.

Con este trabajo de campo, se concluye que el escenario en el cual opera el radar meteorológico presenta características complejas y variables. La proliferación de antenas y dispositivos WLAN/RLAN tiene un crecimiento exponencial y, sumado a esto, en el intento de estos equipos de convivir y competir por el uso del espectro tratarán de disminuir la brecha tecnológica utilizando algoritmos y protocolos de funcionamiento agresivos que les permita aprovechar al máximo el uso de canales en el ancho de banda disponible. En la actualidad, el entorno inalámbrico se está preparando para convivir con tecnologías de última generación con el reciente despliegue de redes Wi-Fi 6/6E (estándar IEEE 802.11ax) que, si bien funciona en una banda de frecuencias cercanas, utiliza una multiplexación basada en multiusuarios OFDMA (*Orthogonal Frequency Division Multiple Access*, Acceso Múltiple por División de Frecuencias Ortogonales) por lo cual podría complicar aún más el contexto del radar.

5.2 Trabajo Futuro

En base a los resultados obtenidos con este procedimiento de medición, como tarea o actividad a futuro se propone generar documentación técnica que pueda ser de utilidad al organismo regulador ENACOM (*Ente Nacional de Comunicaciones*) para tratar las interferencias perjudiciales presentes en el radar RMA-1 y en los distintos radares que componen la red SINARAME.

Otra línea de trabajo futuro consiste en vincular los registros de interferencia observada con su efecto sobre los productos del radar meteorológico. Una metodología posible consiste en hacer un análisis estadístico desde el dato de radar, teniendo en cuenta sus tiempos de arribo, niveles de potencia y duración de las tramas y asociarlo a los valores esperados de acuerdo a lo que establecen los estándares y lo recogido durante el trabajo de campo. Parte de las actividades descriptas han sido abordadas, debido a que este era un objetivo inicial de la tesis que fue descartado por el volumen de trabajo que conllevan las mediciones de campo.

Como recomendación, se deberá actualizar el método de medición de campo para estudiar el nuevo entorno inalámbrico con la instalación de dispositivos WLAN/RLAN que ofrecen servicio Wi-Fi 6/6E.

Capítulo A

Anexos

A.1 Anexos del Capítulo 3

Comandos utilizados para descargar, compilar e instalar el driver del adaptador wireless USB externo mediante consola.

```
$sudo apt-get update
```

```
$sudo apt-get upgrade
```

```
$sudo reboot now
```

```
$sudo apt install build-essential Linux-headers-$(uname -r) dkms unzip git
```

Una vez descargado, se extrae el driver de la carpeta:

```
$sudo unzip -d /tmp/ ~/Downloads/*master.zip
```

Finalmente se instala y compila del driver:

```
$cd /tmp/*master
```

```
$cd rtl8814au
```

```
$sudo make dkms_install
```

```
$make
```

```
$sudo make install
```

```
$sudo reboot
```

A.1.1 Habilitación del modo Monitor

El modo Monitor, modo escucha o modo promiscuo es un modo de funcionamiento de la tarjeta inalámbrica que se encarga de escuchar todos y cada uno de los paquetes de la red que se propagan por la interfaz de "aire". En este modo, no solamente se escuchará lo que envía un AP localmente, sino también el intercambio de información que hay en otras redes Wi-Fi vecinas. Para filtrar los paquetes es necesario escanear un canal específico para no perder información sobre el tráfico que emite el AP a los distintos clientes. A partir de este modo, se pueden conocer las direcciones MAC de todos los clientes que están conectados a un determinado AP, ya que se capturan las tramas de datos que viajan por el aire desde el origen hasta la dirección destino. Es por este medio que se realizan las auditorías informáticas para estudios de redes y comprobar su seguridad.

Para activar el modo Monitor, es necesario que el chipset de la tarjeta o adaptador inalámbrico y sus controladores o drivers sean compatibles con este modo. De lo contrario no podrá capturar las tramas.

En Ubuntu Linux existen tres formas de habilitar la función Monitor en la mayoría de las tarjetas y adaptadores inalámbricos para la captura de datos e inyección de paquetes. A modo de demostración, se habilitará esta función solamente en la tarjeta inalámbrica de la notebook Intel Wireless 8260, luego se configurará con el adaptador seleccionado.

1) Utilizando iw

Primero, el sistema debe reconocer la interfaz Wi-Fi:

```
$sudo iw dev
```

En la Figura A.1 se puede osbervar que la interfase en cuestión es "wlp2s0" con dirección física MAC 28:C6:3F:AF:39:8A. El modo que aplica para conectarse a la red inalámbrica es de tipo "managed" o administrado que es equivalente al modo Nativo o Infraestructura.

Luego se ejecutan las siguientes tres líneas de comando para apagar la interfase, activar el modo monitor y encender o levantar la interfaz nuevamente:

```
$sudo ip link set wlp2s0 down
```

```
$sudo iw wlp2s0 set monitor none
```

```
$sudo ip link set wlp2s0 up
```

```
eze@eze:~$ sudo iw dev
[sudo] contraseña para eze:
phy#0
        Unnamed/non-netdev interface
                wdev 0x2
                addr 28:c6:3f:af:39:8b
                type P2P-device
                txpower 0.00 dBm
        Interface wlp2s0
                ifindex 2
                wdev 0x1
                addr 28:c6:3f:af:39:8a
                ssid Fibertel WiFi062 5.8GHz
                type managed
                channel 52 (5260 MHz), width: 40 MHz, center1: 5270 MHz
                txpower 22.00 dBm
                multicast TXQ:
                        qsz-byt qsz-pkt flows   drops   marks   overlmt hashcoltx-bytes tx-packets
                        0       0       0       0       0       0       0       00
```

Figura A.1: Interfases disponibles en el sistema.

```
eze@eze:~$ sudo iw dev
phy#0
        Unnamed/non-netdev interface
                wdev 0x2
                addr 28:c6:3f:af:39:8b
                type P2P-device
                txpower 0.00 dBm
        Interface wlp2s0
                ifindex 2
                wdev 0x1
                addr 28:c6:3f:af:39:8a
                type monitor
                txpower 0.00 dBm
                multicast TXQ:
                        qsz-byt qsz-pkt flows   drops   marks   overlmt hashcol tx-bytes        tx-packets
                        0       0       0       0       0       0       0       0               0
```

Figura A.2: Habilitación del modo Monitor con iw.

Se verifica el cambio con el comando “sudo iw dev”. Esto se demuestra en la Figura A.2.

Una vez que se termina la captura de datos, se deberá deshabilitar el modo Monitor con los siguientes tres comandos:

```
$sudo ip link set wlp2s0 down
```

```
$sudo iw wlp2s0 set type managed
```

```
$sudo ip link set wlp2s0 up
```

2) Utilizando iwconfig

El segundo método es mediante el comando “iwconfig”. Primero se comprueba el nombre de la interfaz:

```
$sudo iwconfig
```

En la Figura A.3 se observa el uso del comando anterior, y el nombre de la interfase “wlp2s0” y el modo de funcionamiento “Managed”. En la Figura A.4 se muestra la extracción de la dirección MAC con el comando:

```
$sudo ifconfig
```

```
eze@eze:~$ sudo iwconfig
lo        no wireless extensions.

wlp2s0    IEEE 802.11  ESSID:"Fibertel WiFi062 5.8GHz"
          Mode:Managed  Frequency:5.26 GHz  Access Point: D8:D7:75:67:63:B7
          Bit Rate=400 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
          Link Quality=65/70  Signal level=-45 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:39   Missed beacon:0
```

Figura A.3: Se verifica el nombre de la interfase.

```
eze@eze:~$ sudo ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Bucle local)
        RX packets 43270  bytes 3895504 (3.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 43270  bytes 3895504 (3.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.9  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a45a:8d76:ca4b:3b4f  prefixlen 64  scopeid 0x20<link>
        ether 28:c6:3f:af:39:8a  txqueuelen 1000  (Ethernet)
        RX packets 153489  bytes 81614844 (81.6 MB)
        RX errors 0  dropped 2  overruns 0  frame 0
        TX packets 93743  bytes 30560257 (30.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura A.4: Se extrae la dirección MAC de la interfase en cuestión.

Para activar el modo monitor, se debe apagar la interfase en cuestión, cambiar el modo y luego reestablecer la conexión respectivamente:

```
$sudo ifconfig wlp2s0 down
```

```
$sudo iwconfig wlp2s0 mode monitor
```

```
$sudo ifconfig wlp2s0 up
```

Ejecutar el comando “sudo iwconfig” para verificar el cambio. Esto se demuestra en la Figura A.5.

```
eze@eze:~$ sudo iwconfig
lo        no wireless extensions.

wlp2s0    IEEE 802.11  Mode:Monitor  Tx-Power=-2147483648 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

Figura A.5: Habilitación del modo Monitor.

Luego de concluir con la tarea de captura se apaga el modo monitor con los siguientes tres comandos:

```
$sudo ifconfig wlp2s0 down
```

```
$sudo iwconfig wlp2s0 mode managed
```

```
$sudo ifconfig wlp2s0 up
```

3) Utilizando Airmon-ng

Para utilizar este método se deberá instalar previamente la suite Aircrack con el comando:

```
$sudo apt-get install aircrack-ng
```

Se comprueba el nombre de la interfase mediante la ejecución del comando:

```
$sudo airmon-ng
```

Figura A.6: Verificación del nombre de la interfase.

El próximo comando es para corrobar cuales son los procesos en ejecución que pueden intrferir con la interfase:

```
$sudo airmon-ng check
```

Figura A.7: Procesos activos que pueden interferir en el funcionamiento de la interfase.

Seguidamente, se deshabilitan esos procesos:

```
$sudo airmon-ng kill
```

Figura A.8: Deshabilitación de los procesos activos.

Se activa el modo Monitor en la interfase:

```
$sudo airmon-ng start wlp2s0
```

Figura A.9: Activación del modo Monitor.

En las Figuras A.10 y A.11 muestran que el proceso de activación es un poco diferente a los métodos anteriores. La herramienta Aircrack ha creado una nueva interfaz denominada "wlp2s0mon".

Para corrobar esto, se ejecutan los comandos "sudo ifconfig" y "sudo iwconfig".

```
$sudo ifconfig
```

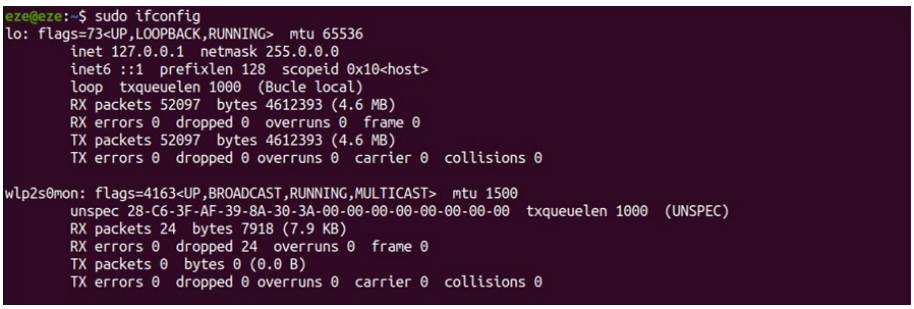


Figura A.10: Verificación mediante ifconfig.

```
$sudo iwconfig
```

Figura A.11: Verificación mediante iwconfig.

Luego de realizar el trabajo de captura e inyección de datos, se deshabilita el modo Monitor con el siguiente comando:

```
$sudo airmon–ng stop wlp2s0mon
```

En la Figura A.12 se muestra la detención del proceso que ejecuta la herramienta Aircrack para recuperar el funcionamiento normal de la interfase inalámbrica.

Figura A.12: Deshabilitación del modo Monitor.

Para retornar a la normalidad, y que el adaptador recupere su función en modo Nativo, se reestablece con el siguiente comando:

```
$sudo service network-manager restart
```

Proceso GPSD

GPSD es un proceso de monitoreo que recopila información de receptores GPS, sistemas de radio GPS-Diferencial o receptores AIS conectados a una máquina host. En el mundo de la informática, y sobre todo en los sistemas UNIX, estos procesos se los denomina "demonios (daemon en inglés)", término erróneo por una cuestión de fonética, que se ejecutan en segundo plano y son autónomos, de manera que no necesitan interacción por parte de un usuario del sistema para arrancar y funcionar.

Los demonios son útiles para hacer funcionar programas independientes de una sesión de usuario, procesos que se inicien de manera automática cuando el sistema arranca o servicios que permanecen a la escucha para ejecutar su tarea cuando son llamados.

El hecho es que los receptores GPS emiten datos en formatos muy diferentes, donde algunos de ellos admiten el protocolo NMEA y otros usan sus propios formatos binarios. Si los programas funcionan directamente con los receptores, entonces cada uno de ellos necesitaría implementar algún tipo de soporte para cada dispositivo. Para simplificar esta tarea se utiliza el servicio GPSD. Este proceso escucha los datos entrantes de los receptores GPS y determina automáticamente el formato de la trama, las reconoce y las pone a disposición en el socket **tcp://localhost:2947** (se puede configurar otro puerto) para cualquier programa en el sistema operativo. En este sentido, cualquier programa puede recibir un flujo de datos GPS siempre que se implemente la escucha desde el puerto tcp://localhost:2947 y comprenda el formato GPSD para trabajar con la mayoría de los receptores GPS.

Conexión de datos NMEA a través de USB

En referencia a lo anterior, es necesario obtener los siguientes paquetes en la distribución Ubuntu. GPSD - Daemon GPS para conectarse mediante socket TCP. Y también, GPSD-clients que son programas auxiliares para GPSD que pueden ayudar a la resolución de problemas:

```
$sudo apt-get install gpsd gpsd-clients
```

Se necesita la herramienta “android-tools” o “android-tools-adb”, imprescindible para la conexión USB de Android:

```
$sudo apt-get update
```

```
$sudo apt-get install android-tools-adb
```

Asegurarse que el móvil tenga habilitada la “depuración USB” y conectar el cable USB a la computadora.

En Share GPS, se debe crear una nueva conexión para NMEA USB. El puerto predeterminado en la aplicación es 50000 y es el indicado para trabajar.

Abrir una consola en Linux y escribir el siguiente comando para comprobar si el sistema detecta la conexión por USB:

```
$lsusb
```

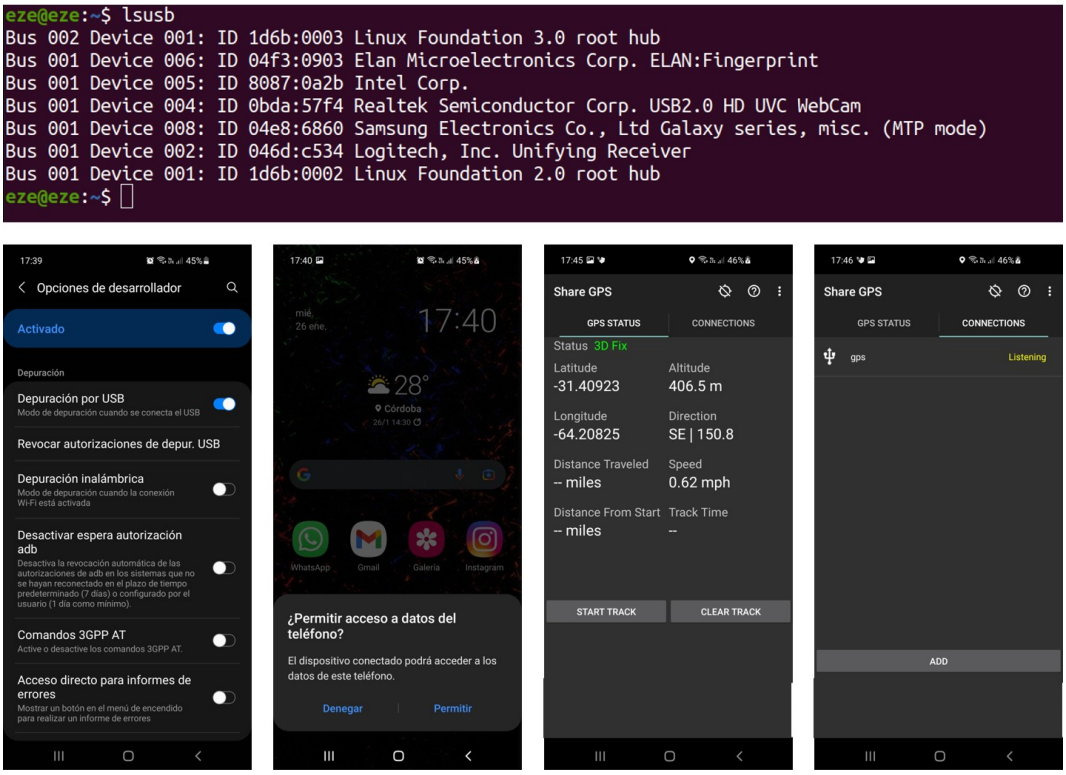


Figura A.13: Verificación de la conexión del dispositivo móvil por USB.

En la Figura A.13 se observa que el móvil tiene habilitada la función de “Depuración por USB”. Luego debe permitirse la conexión en Android para que el sistema Linux reconozca el dispositivo. En la línea “Bus 001 Device 008” se verifica dicha conexión y reconocimiento del teléfono. Una vez ejecutada la aplicación Share GPS en el móvil, se activa automáticamente la función de Ubicación y comienza la recepción de la señal GPS, cuyo Estado “3D Fix” significa que hay más de tres satélites para la corrección. Seguidamente, en la solapa “Conexiones” el

receptor se encuentra en modo escucha para ser utilizado por otros programas, o esperando ser llamado por algún proceso o servicio para compartir los datos GPS.

A continuación, se debe ingresar al fichero de configuración para que el proceso GPSD inicie automáticamente con un dispositivo específico, tal como se muestra en la Figura A.14.

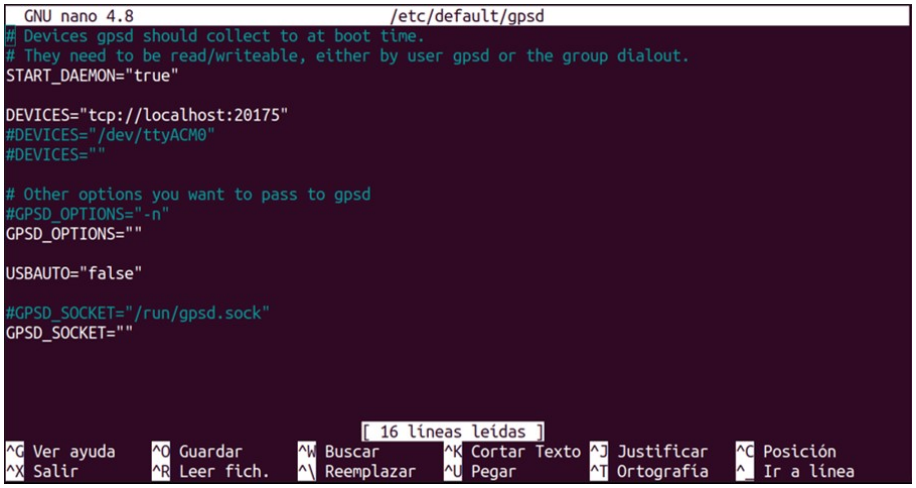


Figura A.14: Archivo de configuración GPSD.

Para acceder a este archivo en cuestión, se ejecuta la siguiente línea de comando:

```
$sudo nano /etc/default/gpsd
```

En el interior de esta configuración se deberá agregar el dispositivo específico en el parámetro "DEVICES" y la línea completa sería la siguiente:

```
DEVICES="tcp://localhost:20175"
```

Se establece el número "20175" para configurar el puerto tcp de la computadora. El mismo será utilizado por el programa ADB para compartir los datos.

El servicio GPSD escuchará las tramas GPS salientes del puerto 20175 de la computadora y las replicará en su propio puerto "tcp://localhost:2947".

También se pueden cambiar los valores de los otros parámetros para especificar aún más el inicio automático del servicio. Para este caso, es suficiente el agregado del dispositivo.

Una vez instaladas las herramientas y actualizados los archivos de configuración, se deberá cargar el dispositivo receptor GPS. Para ello, se ejecuta el siguiente comando:

```
$sudo dpkg–reconfigure gpsd
```

Con el comando anterior, se reestablece el servicio GPSD cargando el archivo de configuración.

También se puede iniciar GPSD introduciendo la siguiente línea:

```
$sudo gpsd –N tcp://localhost:20175
```

La opción "**-N**" es necesaria para que el servicio no pase a un segundo plano. Después de la depuración, cuando se asegura de que todo funciones correctamente, se puede omitir la opción -N.

En caso de alguna falla el programa termina o sigue en funcionamiento, pero otras aplicaciones no recibirían información GPS. Entonces se usa la opción "**-D**", y seguido se especifica un número para aumentar el nivel de depuración. Por ejemplo, "**-D 1**" para una salida breve o "**-D 10**" para una salida más detallada.

El comando sería el siguiente:

```
$sudo gpsd -N -D 10 tcp://localhost:20175
```

El siguiente paso es autorizar al dispositivo móvil para compartir los datos mediante ADB. Esto se verifica con el comando:

```
$sudo adb devices
```

Debería figurar el dispositivo en la lista. Si se indica fuera de línea o no autorizado, se debe verificar en el móvil si necesita autorización y que se reconozca en la lista.

Luego se utiliza ADB para reenviar el puerto tcp del móvil (siendo 50000 como valor predeterminado) al puerto tcp de la computadora 20175. Esto se logra con el comando:

```
$sudo adb forward tcp:20175 tcp:50000
```

En la Figura A.15 se observa que el dispositivo se reconoce en la lista luego de permitir la autorización.

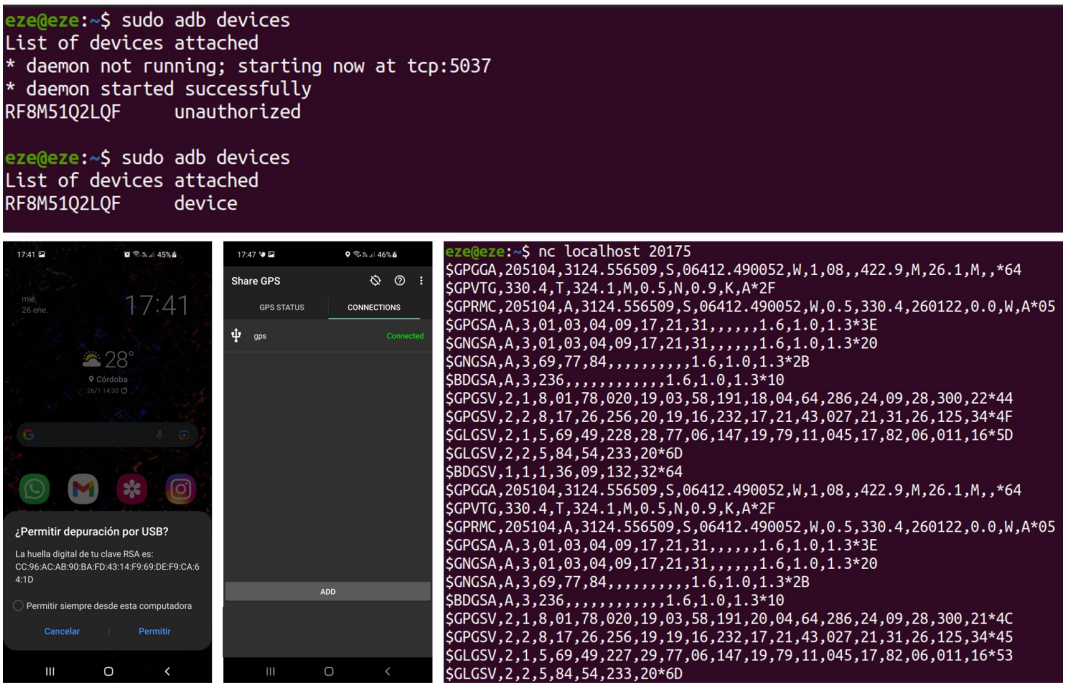


Figura A.15: Autorización del dispotivo móvil y flujo de datos GPS.

Desde Share GPS, el estado figura en modo escucha “Listening”. Para corroborar que ADB y Share GPS funcionan de correctamente se usa el comando nc para verificar si hay datos entrantes:

```
$sudo nc localhost 20175
```

Entonces, el estado de Share GPS cambia a “Conectado” y se reciben las primeras cadenas de datos NMEA.

También se puede realizar una primera lectura con la instrucción:

```
$sudo gpspipe -r > logfile.nmea
```

Existen otros comandos para comprobar el funcionamiento del GPS:

```
$sudo gpsmon
```

```
$sudo cgps -s
```

Los comandos gpsmon y cgps -s presentan las tramas NMEA compiladas en tablas con información estructurada y organizada para ofrecer un nivel de detalle más óptimo.

Y si se quiere obtener información de forma gráfica que muestre la constelación de los satélites, se puede utilizar el comando:

```
$sudo xgps
```

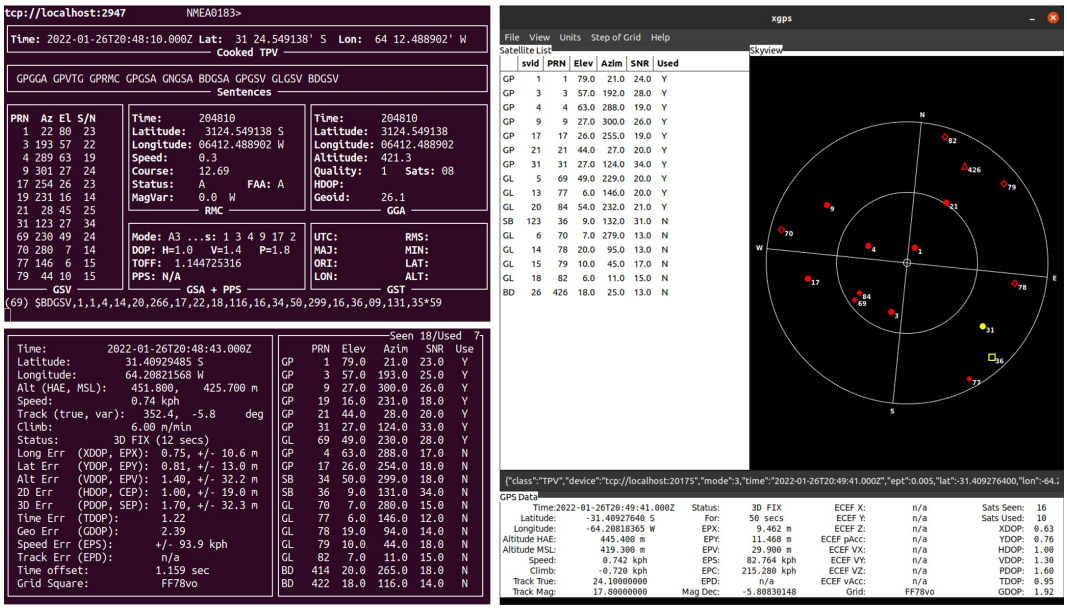


Figura A.16: Flujo de datos GPS mostrados en forma de tablas o gáficos.

De acuerdo a las instrucciones mencionadas anteriormente y que se muestran en la Figura A.16, la información que se procesa de las tramas NMEA es la siguiente:

- Fecha: fecha de la captura;
- Hora: hora de la captura;
- Latitud: de la posición con formato GGMM,MMMM;
- Longitud: de la posición con formato GGGMM,MMMM;
- Variación magnética;
- Satélite en uso: cantidad de satélites usados en la solución de la posición;
- Altitud: altitud de la posición;
- Geoide: valor de geoide de la posición calculada en el área de la muestra;
- PRNs: un arreglo de 12 valores con el PRN de cada satélite usado en la determinación de la posición;
- PDOP: dilución de la precisión en la posición;
- HDOP: dilución de la posición en la componente horizontal;
- VDOP: dilución de la posición en la componente vertical;
- Satélite en vista: cantidad de satélites en vista al momento de la adquisición. Para cada satélite se extrae la siguiente información: PRN identificador del satélite; Elev elevación; Az azimut y SNR relación señal a ruido.

  Preparados los datos GPS, se procede a la habilitación del modo monitor del adaptador externo USB para comenzar con la captura del tráfico entrante y saliente del router AP. A través de consola, se ejecutan los siguientes comandos para activar el modo escucha:

```
$sudo airmon-ng
```

```
$sudo airmon-ng check
```

```
$sudo airmon-ng check kill
```

```
$sudo airmon-ng start wlp2s0
```

Para comenzar con la fase de descubrimiento y escuchar el tráfico entre el AP, dispositivos clientes y otros APs cercanos se ejecuta el programa Kismet con el siguiente comando:

```
$sudo kismet -c wlp2s0mon
```

Bibliografía

Barba Leal, O., F. Rinalde, J. Cogo, y J. Pascual. WLAN signal detection in weather radar data. En *Actas de la XIX Reunión de Trabajo Procesamiento de la Información y Control (RPIC'21)*. San Juan, Argentina (2021).

Bringi, V. N. y V. Chandrasekar. *Polarimetric Doppler weather radar: principles and applications*. Cambridge University Press, 40 West 20th Street, New York, 1 edición (2004).

Carroll, J., F. Sanders, R. Sole, y G. Sanders. *Case Study: Investigation of Interference into 5 GHz Weather Radars from Unlicensed National Information Infrastructure Devices, Part I*. Technical Report TR-11-473, NTIA (2010).

Doviak, R. J. y D. S. Zrnić. *Doppler Radar and Weather Observations, 2nd Ed.*. Academic Press, San Diego Cal. (1993).

González, F. y M. F. Iglesias. Una visión del futuro de las telecomunicaciones. En Figueiras, A., ed., *Una panorámica de las telecomunicaciones*, págs. 356–389. Prentice Hall, Madrid (2001).

IEEE Standard 802.11. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. (2016).

Lakshmanan, V., J. Zhang, y K. Howard. A technique to censor biological echoes in radar reflectivity data. *Journal of Applied Meteorology and Climatology*, 49(3):453–462 (2010).

Nai, F., S. Torres, y R. Palmer. On the mitigation of wind turbine clutter for weather radars using range-Doppler spectral processing. *IET Radar, Sonar & Navigation*, 7(2):178–190 (2013).

Petracca, G. y J. Lugo. Mitigation of WLAN/RLAN interference in meteorological radar using wavelet filtering. En *Actas de la XIV Reunión de Trabajo Procesamiento de la Información y Control (RPIC'17)*, págs. 1–6. Mar del Plata, Argentina (2017).

Richards, M. A. *Fundamentals of Radar Signal Processing*. McGraw-Hill, New York, 2 edición (2014).

Rodríguez, A., C. Lacunza, J. Serra, C. Saulo, H. Ciappesoni, G. Caranti, J. Bertoni, y A. Martina. SiNaRaMe: Integración de una red de radares hidro-meteorológicos en latinoamérica. *Revista Facultad de Ciencias Exactas, Físicas y Naturales*, 4(1):41–48 (2017).

Ryzhkov, A. y D. Zrnic. *Radar Polarimetry for Weather Observations*. Springer, Switzerland (2019).

Saltikoff, E., J. Cho, P. Tristant, A. Huuskonen, L. Allmon, R. Cook, E. Becker, y P. Joe. The threat to weather radars by wireless technology. *Bulletin of the American Meteorological Society*, 97(7):1159–1167 (2016).

Skolnik, M., G. Linde, y K. Meads. Senrad: An advanced wideband air-surveillance radar. *IEEE Transactions on aerospace and electronic systems*, 37(4):1163–1175 (2001).

Vaccarono, M., C. Chandrasekar, R. Bechini, y R. Cremonini. Survey on electromagnetic interference in weather radars in northwestern Italy. *Environments*, 6(12) (2019).