Medición de Señales WLAN/RLAN que Interfieren a los Radares Meteorológicos Argentinos

Ezequiel Giovanardi*, Jorge Cogo[‡§] y Juan Pablo Pascual[†§]
* CRUC-IUA, Universidad de la Defensa Nacional, Av. Fuerza Aérea Argentina 6500, Córdoba, Argentina
[‡] Universidad Nacional de Río Negro. CITECCA. Anasagasti 1463, Bariloche, Argentina
[†]Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET)
[§]Instituto Balseiro - Universidad Nacional de Cuyo, Av. Bustillo 9500, S. C. Bariloche, Río Negro, Argentina
email: ggiovanardi@iua.edu.ar - juanpablo.pascual@ib.edu.ar - jorgecogo@gmail.com

***Abstract*—The aim of this work is to measure and characterize WLAN/RLAN wireless network signals which interfere with the radars of the argentinian National Meteorological Radar System (SINARAME) and degrade their performance. The standards that define these signals are studied and a measurement procedure is designed, which allows recording the interference sources in-situ and also determining their origin.**

The first step involves the analysis of weather radar records, where the effects of the interference on the generated products are observed to determine critical azimuthal directions on digital cartography, which are used as guidance for the search of the interfering wireless sources.The information collected and analyzed is obtained by a dynamic technique that integrates the acquisition of real-time GPS signal data, sensing in the spectrum of signal transmission, and capturing of 802.11 frames.

With the measurement process results, the geo-location of the interfering sources are obtained and their most relevant characteristics are described.

***Resumen*— El objetivo de este trabajo consiste en medir y caracterizar las señales de redes inalámbricas WLAN/RLAN que causan interferencias y degradan el desempeño de los radares que componen el Sistema Nacional de Radares Meteorológicos (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.**

Como primer paso en la localización, se analizan registros de radar meteorológico en los cuales se observan los efectos de la interferencia sobre los productos generados. Luego, se determinan direcciones acimutales críticas en cartografía digital a modo de orientación para la búsqueda de las fuentes inalámbricas interferentes. La información recolectada y analizada se obtiene mediante una técnica dinámica que integra datos de señal GPS en tiempo real, actividad de transmisión de las señales en el espectro y captura de paquetes 802.11. Como resultado del proceso de medición se describen las características más relevantes y la geo-localización de las fuentes interferentes.

***Keywords*—radar, interferencia, wardriving, inalámbrico, estándar 802.11**

I. Introducción

El Sistema Nacional de Radares Meteorológicos (SINARAME) consiste en una red de radares meteorológicos y un sistema de centralización de la información en tiempo real, el cual es operado por el Servicio Meteorológico Nacional (SMN) [1]. Los RMA (*Radar Meteorológico Avanzado*) que integran dicha red, son radares Doppler de polarización dual que operan en banda C, diseñados y puestos en marcha por INVAP S.E. [2].

La etapa de procesamiento de señales de un radar meteorológico se encarga de obtener (estimar) los observables empleados por los meteorólogos para caracterizar los fenómenos atmosféricos, es decir, los momentos espectrales [3] y las variables polarimétricas [4]. Esta estimación resulta afectada por diferentes tipos de interferencias que contaminan y enmascaran los ecos provenientes de los fenómenos atmosféricos que se desean observar. Por un lado, el radar recibe reflexiones de la propia onda transmitida, conocidas como *clutter*, que se producen sobre el suelo (clutter terrestre) [3], sobre pájaros o insectos (clutter biológico) [5], o sobre turbinas de molinos eólicos (clutter eólico) [6].

Por otro lado, el radar recibe interferencia electromagnética producida por otros sistemas de comunicaciones. En el año 2003, 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 (*Wireless/Radio Local Area Network*) [7]. 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 de Frecuencia Dinámica), que consiste en un mecanismo por medio del cual, cuando un equipo de comunicaciones detecta una señal de radar en la frecuencia que se está operando, debe cambiar de canal de operación por un determinado tiempo [8]. Sin embargo, a casi 20 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.

A partir de esta problemática, en muchos países se han planteado diversas alternativas de solución. En Sudáfrica por ejemplo, luego de fracasar en el intento de localizar y sancionar a los usuarios de redes WLAN/RLAN que transmitían 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 [9].

El análisis de 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, para el caso particular de la región noroeste de Italia puede verse en [10].

Asimismo, en [11] se reportan los resultados de estudios de interferencia en un radar de la red TDWR (*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.

El objetivo principal de este trabajo consiste en caracterizar las interferencias ocasionadas por los transmisores WLAN/RLAN que degradan el desempeño de los productos de los radares meteorológicos que forman parte de la red SINARAME. Para esto es necesario estudiar la señal OFDM (*Orthogonal Frequency Division Multiplexing*, Multiplexación por División de Frecuencias Ortogonales) desde la norma que la define, según el estándar mostrado en [12], para determinar sus características de interés y en base a esto realizar mediciones de campo que permitan registrar las fuentes de interferencia *in-situ* y localizar su origen.

Los datos de radar utilizados en este trabajo pertenecen al radar RMA-1, ubicado en un predio de ciudad universitaria de la provincia de Córdoba. La información recolectada se limita al contexto de dicho radar, siendo que el mismo presenta serias interferencias WLAN/RLAN debido a su emplazamiento en una zona densamente urbana y que se caracteriza por su alta demanda de usuarios que exigen conexión a las redes inalámbricas de alta velocidad para transmisión de datos y uso de servicios digitales.

En este trabajo se presenta una técnica dínamica que integra diferentes sistemas y procesos para detectar interferencias que aparecen en los datos radar, y que son producidas por dispositivos WLAN/RLAN. Posteriormente, se describen las características más sobresalientes de las señales detectadas incluido los datos de su geo-localización. Por último se realizan algunas conclusiones y recomendaciones del proceso de medición en campo.

II. Formulación del problema

Los dispositivos WLAN/RLAN que funcionan en la banda de 5 GHz 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 (*Open System Interconnection*, Interconexión de Sistemas Abiertos) están enfocadas a la subcapa física PHY (*Physical sublayer*) y a la subcapa MAC (*MAC sublayer*) 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 estos pertenecen a la PHY (ver Fig. 1).

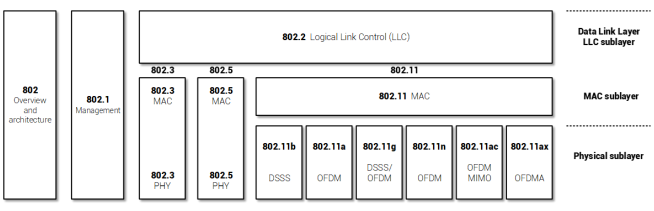

Figura 1. Familia IEEE 802 y su relación con el modelo OSI.

Las interferencias pueden atribuirse a dispositivos WLAN/RLAN que funcionan bajo la especificación IEEE 802.11. En particular, aquellos dispositivos compatibles con las normas IEEE 802.11a, IEEE 802.11g, IEEE 802.11n y IEEE 802.11ac. Todas estas versiones trabajan en banda C y utilizan multiplexación y modulación multiportadora OFDM. De esta manera, usan una gran cantidad de canales paralelos en un ancho de banda reducido (portadoras) para modular la señal.

Además, estos dispositivos y los radares meteorológicos de banda C transmiten en el mismo rango de frecuencias. 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. Actualmente, varios tipos de dispositivos inalámbricos utilizan canales de transmisión en el rango de frecuencias de $5{,}180$ y $5{,}825$ GHz. Mientras, que los radares meteorológicos de tipo Doppler de doble polarización funcionan en la banda de frecuencias de $5{,}450$ y $5{,}820$ GHz.

De acuerdo a la versión del estándar 802.11 (a, g, n o ac) el ancho de banda de los canales variará entre 20, 40, 80 y 160 MHz. En la Figura 2 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.

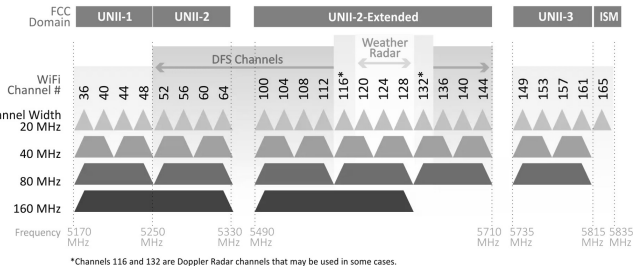

Figura 2. Espectro y asignación de canales en 802.11

En el caso del radar RMA-1, 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 según la normativa).

En la Figura 3 se observa un gráfico de indicador de posición, ó PPI (acrónimo de *Plan Position Indicator*) de la reflectividad medida en polarización Horizontal por el RMA-1 emplazado en la Ciudad de Córdoba, bajo condiciones climáticas de *aire claro* (sin presencia observable de fenómenos meteorológicos). Esto se corresponde a un barrido o vuelta completa 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 terrestre debido a las sierras cordobesas. Finalmente, en diferentes ángulos de azimut se observan líneas radiales en tonos azules, verdes y amarillos (valores medios de reflectividad), que se condicen con el efecto esperado debido

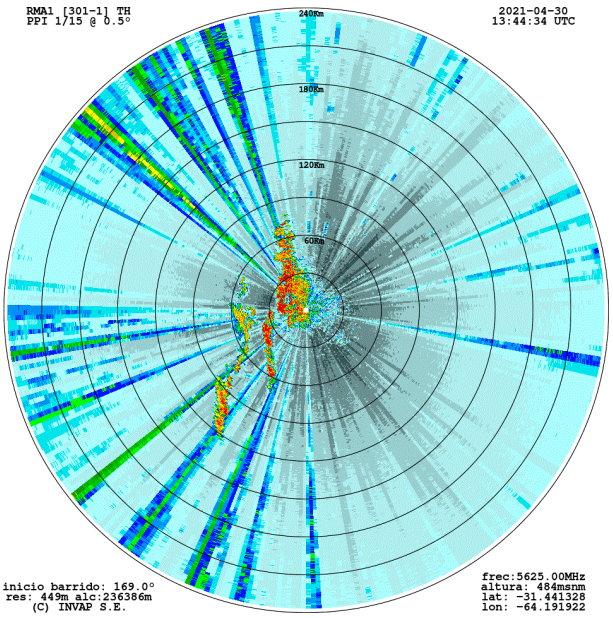

Figura 3. PPI de reflectividad (en dBZ), para la polarización Horizontal, observado por el RMA-1 en condiciones de aire-claro.

a la interferencia de redes inalámbricas.

Cuando un cliente Wi-Fi quiere establecer conexión a una red WLAN/RLAN ejecuta un proceso denominado "*fase de descubrimiento*". Esto implica que el cliente necesariamente debe realizar dos tipos de actividades: escaneo pasivo y escaneo activo. Un Access Point (AP) inalámbrico continuamente transmite por la interfaz de aire una trama de gestión especial denominada "*beacon*" (traducido al español como baliza) para anunciar dentro de su área de cobertura las características que ofrece su conexión. Por un lado, ejecutando un escaneo pasivo, los clientes escuchan esta trama de gestión para identificar los APs cercanos. Esta trama beacon se transmite en intervalos regulares denominado TBTT (*Target Beacon Transmission Time*, Tiempo de Transmisión de Baliza Objetivo) y se expresa en unidades de tiempo (TU). Esto significa que 1 TU = 1024 microsegundos, por lo tanto, el intervalo de beacon equivale a 100 TU (100 x 1024 microsegundos = 0,102 400 segundos), y que corresponde a consumir un cierto "tiempo de aire" del medio inalámbrico compartido. 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. Por otro lado, 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 (difusión por broadcast). 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 la trama beacon.

Para caracterizar las señales interferentes, se toma el control de la subcapa PHY del estándar 802.11 (ver Fig. 1) mediante un proceso de escucha pasivo para conocer la estructura de los datos que son transmitidos en forma de paquetes sobre las comunicaciones inalámbricas, y que posteriormente, se capturan durante el proceso de medición en campo por un software específico.

III. Métodos

Para el procedimiento de medición en campo, se parte del análisis del gráfico PPI de reflectividad (Fig. 3) donde se pueden identificar las direcciones acimutales estimadas en las que se observa potencia debida a la/las fuente/s de interferencia/s.

En la Figura 4 se muestra un mapa satelital online (obtenido a través de imágenes satelitales, fotografías aéreas e información geográfica de Google Earth) y sobre él tiene trazada una línea recta que coincide con las interferencias más críticas del PPI para tener una noción de la dirección. Esto se logra insertando la imagen PPI en forma de capas para superponer a la fotografía satelital.

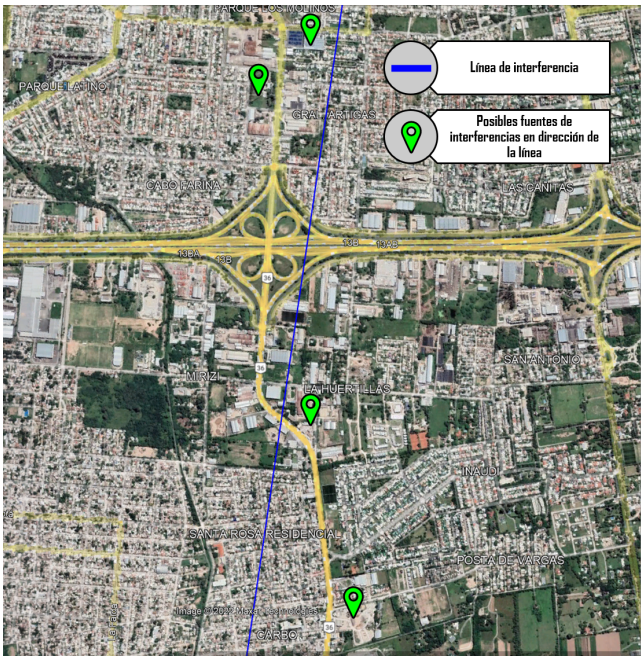

Figura 4. Imagen satelital con trazado de línea de interferencia y posibles fuentes identificadas visualmente.

Luego siguiendo la línea sobre el mapa se identifican posibles fuentes de manera visual tomando como referencia infraestructura y/o emplazamientos existentes (torres de telecomunicaciones y estructuras edilicias), sistemas irradiantes instalados a gran altura, entre otros, para luego verificar in-situ.

Una vez establecida la posición estimada de la/las posible/s fuente/s de interferencia/s, se ejecuta un método dinámico conocido como *War-Driving*, que consiste en equipar un vehículo con herramientas de hardware y software de medición para la búsqueda de redes inalámbricas en movimiento [13]. Esto implica conducir lentamente por una zona específica de la ciudad con el objetivo de escanear a través de los recursos de software la interfaz de aire para detectar señales de RF en la banda de 5 GHz. Mientras se sondea el área, 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.

El equipamiento se compone de: una computadora portátil con sistema operativo Linux distribución Ubuntu 20.04 LTS preparada para ejecutar los softwares de captura de paquetes

y tramas inalámbricas (Wireshark y Kismet) con posibilidad de conexión de un receptor inalámbrico Wi-Fi USB externo y un teléfono inteligente para extraer sus datos GPS; y una computadora portátil con sistema operativo Windows 10 con puerto FastEthernet para conectar vía cable UTP un dispositivo AP Nano Loco M5 que ofrece, en su gama de funcionalidades, el uso de un analizador de espectro que está embebido en su software.

En paralelo a la actividad registrada con el analizador de espectro, se adicionan los datos GPS transmitidos desde un teléfono inteligente a la computadora portátil para ser recuperados vía USB (a través del protocolo de comunicación serial) por el software Kismet para descubrir rápidamente, mediante la captura de paquetes y tramas inalámbricas 802.11, las redes disponibles anexando la información geográfica estimada de latitud y longitud. Este software recopila toda la información y luego la exporta como archivo .csv para obtener los datos GPS en el mapa (ver Fig. 6 en la sección IV).

Para ajustar el proceso de triangulación y mejorar la exactitud en la localización de la fuente de interferencia, se realizan dos acciones: la primera es ejecutar una herramienta disponible en el equipo Nano Loco M5 denominada "*Site Survey*", que consiste en hacer un barrido de todos los canales disponibles de la banda de 5 GHz de forma omnidireccional para descubrir redes inalámbricas en el área.

A partir del análisis del Site Survey, se ejecuta la segunda acción para detectar correctamente la fuente. Esta consiste en capturar paquetes y tramas 802.11 con el software Wireshark y el receptor inalámbrico Wi-Fi USB externo configurado en "*Modo Monitor*". Es un modo de funcionamiento del adaptador inalámbrico que se encarga de escuchar todos y cada uno de los paquetes que se propagan por la interfaz de aire. En este modo, no solamente se escucha 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 toma el control de 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 (siempre que sea compatible su controlador/driver) y se combina con aplicaciones denominadas *sniffers* para capturar gran cantidad de información (paquetes y tramas inalámbricas 802.11), que luego se manipula de forma lícita. A este proceso de ataque pasivo en el que se escucha la información que circula por el medio de transmisión sin llegar a alterar ésta en modo alguno se lo conoce como ataque "*Sniffing*".

Wireshark es una aplicación *sniffer* que permite analizar de forma detallada y minuciosa el tráfico de una red inalámbrica mediante inspección directa. Dispone de un 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*" (*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 desgloza por capas cada una de las cabeceras del paquete o trama para analizar en detalle sus parámetros más significativos. A continuación, se muestran los resultados obtenidos.

IV. Resultados

En la Figura 5 se presenta una captura del analizador de espectro utilizado a bordo del vehículo en el proceso de war-driving y que se obtiene apuntando las antenas direccionales del equipo Nano Loco M5 hacia las posibles fuentes.

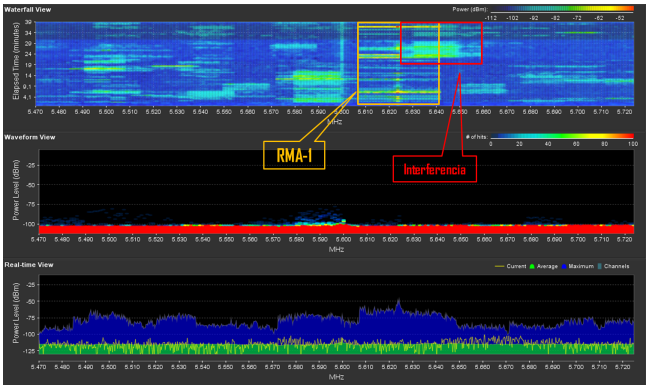

Figura 5. Actividad del RMA-1 y la interferencia.

En la parte superior de la Fig. 5, 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 (frecuencia central de operación 5625 MHz) y del dispositivo inalambrico 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 energía o potencia en los canales, mientras que los más cálidos (amarillo, naranja y rojo) significan mayor potencia o actividad de transmisión. También se revisa la sección de forma de onda (Waveform view) para tener una referencia del estado actual de la actividad RF que hay alrededor y el gráfico en tiempo real (Real time view) que mide la potencia (en valores dBm) en función de la frecuencia.

Para completar la información en la captura de datos y gestionar el proceso de geo-localización, se anexa la señal GPS de cada uno de las redes inalámbricas descubiertas por la aplicación Kismet y se exporta cada ubicación de forma estimada (anillos de color azul) en un mapa digital según el recorrido del vehículo con el método war-driving. Este proceso se muestra en la Figura 6.

En la Figura 7 se observa el listado de frecuencias liberadas o disponibles para uso en la banda de 5 GHz en base al análisis de la herramienta Site Survey. Dentro de este listado se identifican dos dispositivos WLAN/RLAN funcionando en frecuencias indebidas o canales DFS (explicado en la sección II). Además, se detallan otros campos de interés: la dirección física MAC correspondiente al BSSID según el estándar, el nombre lógico de la red denominado SSID, el modo de funcionamiento del transmisor o equipo de

Figura 6. Captura de datos GPS asociados a las redes inalámbricas.

radiofrecuencia, 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 de GHz. 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 5,635 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.

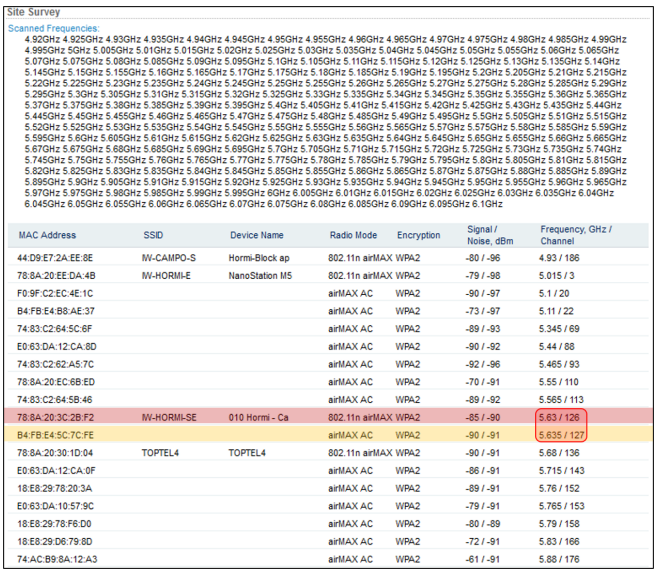

Figura 7. Barrido de frecuencia de la herramienta Site Survey.

Luego, en la aplicación Wireshark (ver Fig. 8) se aplica el filtro por dirección física MAC (wlan.ta == 78:8a:20:3c:2b:f2), para mostrar solamente información relacionada con el AP interferente en cuestión. Se selecciona la trama beacon y se revisa el área de la cabecera para descomponer por capas el contenido de la misma.

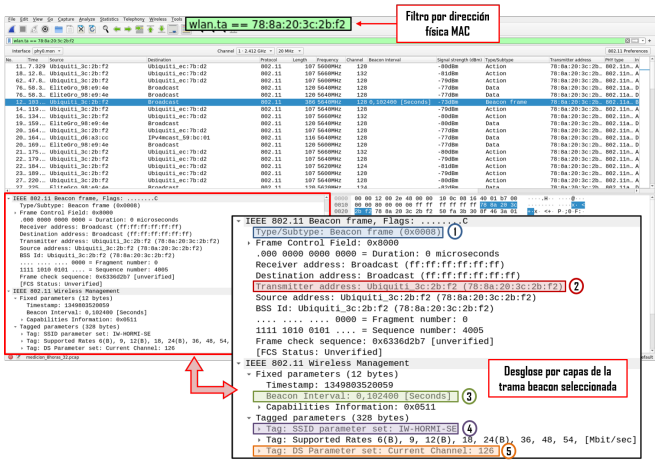

Figura 8. Inspección de la trama beacon utilizando el programa Wireshark.

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 (0,102 400 segundos);
4) el nombre lógico SSID (IW-HORMI-SE);
5) el canal o frecuencia de operación (canal 126 - 5630 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 (5600 MHz), 124 (5620 MHz), 128 (5640 MHz) y 132 (5660 MHz). Esta ocupación de canales se observa en la Fig. 9, quedando en evidencia la interferencia directa (canales solapados) a la transmisión del pulso radar del RMA-1.

El análisis del tráfico inalámbrico capturado completa el proceso de triangulación que garantiza la localización exacta del origen de la fuente de interferencia WLAN/RLAN.

En la Figura 10, se observa la posición geográfica y registro fotográfico de la fuente interferente. De acuerdo al gráfico PPI presentado en la Fig. 3, la dirección acimutal correspondiente con esta fuente es de aproximadamente 193° medido a partir del Norte geográfico.

Con este procedimiento se identificaron y localizaron varias fuentes de interferencias en distintas direcciones acimutales según mapa PPI de reflectividad. Estos resultados no se presentan por ser similares a los mostrados anteriormente.

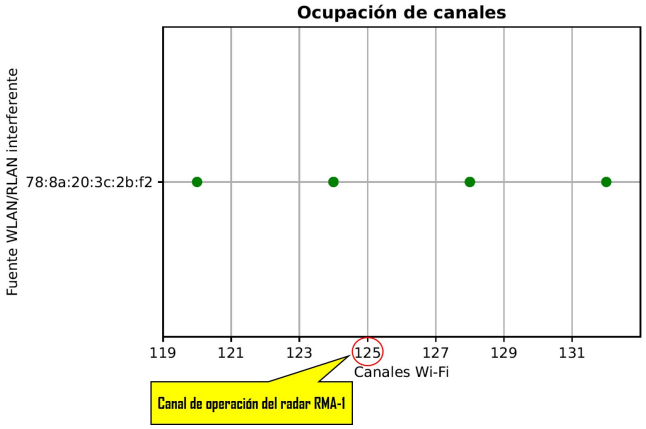

Figura 9. Ocupación de canales de la fuente WLAN/RLAN y que interfieren a la transmisión del radar.

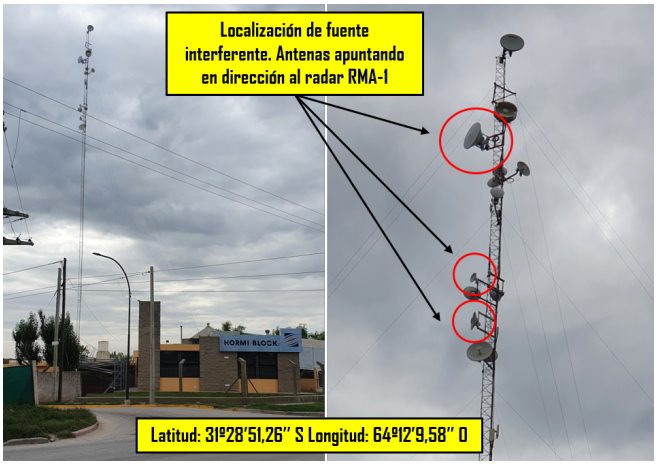

Figura 10. Localización de una fuente de interferencia en una dirección acimutal específica.

V. Conclusión

El procedimiento de medición desarrollado en este trabajo logra el objetivo propuesto. Este método permite medir, caracterizar y localizar las señales inalámbricas WLAN/RLAN que degradan el desmpeño de los radares meteorológicos.

Además, se establece como una alternativa a 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 módulo de recepción GPS y antenas directivas para rastrear señales de acuerdo a su comportamiento en el espectro radioeléctrico. 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 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.

Las fuentes interferentes detectadas presentan características muy similares en cuanto a su actividad en el espectro, puesto que todas coinciden en el fabricante. La captura de sus tramas y paquetes ponen en evidencia el comportamiento, a nivel de protocolo, de la transmisión de datos en todo su ancho de banda. Al tratarse de protocolos propietarios, el análisis de las tramas que intercambian con los clientes ayudó a comprender el funcionamiento de estos tipos de transmisores.

Estas fuentes WLAN/RLAN 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 (cantidad de tiempo de aire) a cada cliente estableciendo diferentes prioridades. Esto implica definir para cada cliente una cantidad de tiempo dependiendo de la prioridad para un mejor rendimiento de la red con respecto a la disponibilidad del ancho de banda. Esto significa que los clientes con una 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.

Para el uso de este protocolo 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. Esto quiere decir que, por más que 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. En modo normal el fabricante debería cumplir con las normas y reglamentaciones de acuerdo al país, pero la habilitación de esta función implicaría actuar de manera indebida ante las regulaciones vigentes, permitiendo usar canales legales y hasta configurar equipos con valores de potencia de transmisión por encima de los 30 dBm.

En cuanto a capacidad técnica, estos dispositivos WLAN/RLAN en particular, disponen de protocolos potentes para poder explotar sus funcionalidades al máximo y aprovechar un recurso tan escaso como lo es el espectro de radiofrecuencia. Las tecnologías airMAX y airSelect en conjunto son utilizadas para que el AP pueda transmitir 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. 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.

Desde el punto de vista técnico, estos equipos presentan una solución favorable, pero aparantemente ignoran tanto parcial como de forma completa las regulaciones legales vigentes. En este marco, la dificultad máxima se plantea en el incumplimiento normativo de los puntos que se detallan a continuación: según el artículo 5° inciso 5.1 de la Resolución 581/2018 del Ministerio de Modernización [14], resuelve que las emisiones de 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 el radar (rango 5470-5600 MHz y 5650-5725 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. En párrafos anteriores, se hizo referencia a la posibilidad que tienen estos dispositivos de incumplir la normativa tanto en la configuración de frecuencias como también los valores de potencia de transmisión con la habilitación de la función Compliance Test.

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.

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 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 potentes 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 WiFi 6/6E (estándar IEEE 802.11ax) que, si bien funciona en 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.

VI. Trabajo Futuro

En base a los resultados obtenidos con este procedimiento de medición, como tarea a futuro se propone generar documentación técnica que acompañe a las declaraciones y presentaciones formales ante el organismo regulador ENACOM (*Ente Nacional de Comunicaciones*) para tratar las interferencias perjudiciales presentes en el radar RMA-1.

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

Agradecimientos

Se agradece al personal responsable del SINARAME por la autorización en el uso de los datos radar correspondientes al RMA-1 para la elaboración de este trabajo.

Referencias

[1] A. Rodríguez, C. Lacunza, J. J. Serra, C. Saulo, H. Ciappesoni, G. Caranti, and A. Martina, "Integración de una Red de Radares Hidro-Meteorológicos en Latinoamérica," *Revista Facultad de Ciencias Exactas, Físicas y Naturales*, 2017.

[2] https://www.invap.com.ar/areas/defensa-seguridad-y-ambiente/radar-meteorologico-banda-c/.

[3] R. J. Doviak and D. S. Zrnić, *Doppler Radar and Weather Observations, 2nd Ed.* Academic Press, 1993.

[4] A. V. Ryzhkov and D. S. Zrnić, *Radar Polarimetry for Weather Observations*. Springer International Publishing, 2019.

[5] V. Lakshmanan, J. Zhang, and K. Howard, "A Technique to Censor Biological Echoes in Radar Reflectivity Data," *Journal of Applied Meteorology and Climatology*, vol. 49, no. 3, pp. 453 – 462, 2010.

[6] F. Nai, S. Torres, and R. Palmer, "On the Mitigation of Wind Turbine Clutter for Weather Radars using Range-Doppler Spectral Processing," *IET Radar, Sonar & Navigation*, vol. 7, no. 2, pp. 178–190, 2013.

[7] R. ITU-R, "Resolution 229 [com5/16]. Use of the bands 5150-5250 MHz, 5250-5350 MHz and 5470-5725 MHz by the mobile service for the implementation of wireless access systems including radio local area networks," *The World Radiocommunication Conference (WRC-03)*, 2003.

[8] R. ETSI, "301 893 v1. 8.1 (2015-03). Broadband Radio Access Networks (BRAN); 5 ghz high performance RLAN; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive," *Harmonized European Standard*, 2015.

[9] E. Saltikoff, J. Y. N. Cho, P. Tristant, A. Huuskonen, L. Allmon, R. Cook, E. Becker, and P. Joe, "The threat to weather radars by wireless technology," *Bulletin of the American Meteorological Society*, vol. 97, no. 7, pp. 1159 – 1167, 2016.

[10] M. Vaccarono, C. V. Chandrasekar, R. Bechini, and R. Cremonini, "Survey on electromagnetic interference in weather radars in northwestern italy," *Environments*, vol. 6, no. 12, 2019.

[11] J. E. Carroll, F. H. Sanders, R. L. Sole, and G. A. Sanders, "Case study: Investigation of interference into 5 ghz weather radars from unlicensed national information infrastructure devices, part i," Tech. Rep., 2010.

[12] I. S. Association *et al.*, "IEEE std 802.11-2016. IEEE Standard for Information technology. Telecommunications and information exchange between systems Local and metropolitan area networks. Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. NY: IEEE; 2016," 2016.

[13] F. J. Díaz, M. Robles, P. Venosa, N. Macia, and G. Vodopivec, "Wardriving: an experience in the city of La Plata," in *XIV Congreso Argentino de Ciencias de la Computación*, 2008.

[14] R. Ministerio de Modernización, "Resolución 581/2018 (RESOL-2018-581-APN-MM). Bandas de espectro radioeléctrico de uso compartido. Instrucciones para su atribución y disposición," *Buenos Aires, Argentina*, 2018. [Online]. Available: https://www.boletinoficial.gob.ar/detalleAviso/primera/191053/20180906