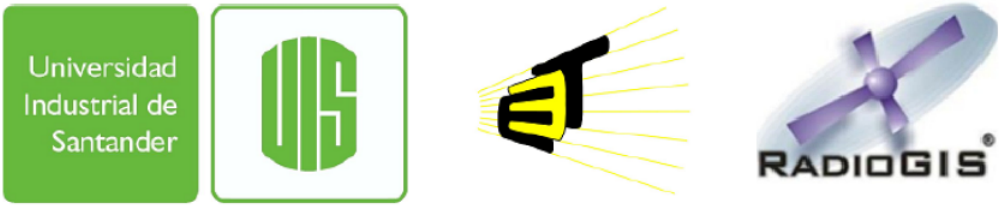
CARACTERIZACIÓN DE UN SISTEMA DE BLOQUEO DE EMISIONES CLANDESTINAS BASADO EN TECNOLOGÍA SDR

Tania Lorena Santos Duarte



UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO-MECÁNICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2017

CARACTERIZACIÓN DE UN SISTEMA DE BLOQUEO DE EMISIONES CLANDESTINAS BASADO EN TECNOLOGÍA SDR

Tania Lorena Santos Duarte

Trabajo de grado para optar al título de Ingeniero Electrónico

Director
Homero Ortega Boada
PhD en Ciencias de la Ingeniería y Radiocomunicaciones.

Codirector
Juan Pablo Moreno Acosta
Ingeniero Electrónico

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO-MECÁNICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2017

Dedicado a

Dios sabe por que hace sus cosas, hoy se que pasaron de la forma que pasaron para darme cuenta -aún más- de cuán amada, bendecida, protegida y afortunada soy, de cuán agradecida tengo que estar cada día por tener un papá y una mamá que dan todo por mi, que hacen mis sueños realidad, que me ven volar alto y me lo permiten. Por tener dos príncipes que hicieron y hacen de mi día y mi vida infinitamente mejor. No puedo expresar con palabras lo que siento hoy, pero diciendo que me desborda el corazón me acerco, los amo fuerte y grande.

Gracias

Tabla de contenido

Índice de figuras

Índice de tablas

Nomenclatura

EW	Electronic War
SDR	Software define radio
$USRP$	SUniversal Software Radio Peripheral
UHD	USRP Hardware Driver
$S - JAMMER$	Sistema de bloqueo de emisiones clandestinas
$Anti - jamm$	Técnicas que impiden el bloqueo

Letras Griegas

λ Longitud de onda

RESUMEN

Título: Caracterización de un sistema de bloqueo de emisiones clandestinas basado en tecnología SDR[1]

Autor:
Tania Lorena Santos Duarte[2]

Palabras Clave: Programa Nacional de Electrónica, Telecomunicaciones e Informática, sistemas de bloqueo, jamming, jammer, interferencia de señales, FM

DESCRIPCIÓN

Este trabajo realiza un estudio de viabilidad técnica para la implementación de un prototipo de bloqueo de emisiones clandestinas basado en tecnología SDR como apoyo a los procesos de control de emisiones no licenciadas en la banda de radiodifusión sonora en frecuencia modulada FM.

El trabajo inicialmente presenta los conceptos teóricos y la fundamentación básica de un equipo *jammer*, se describe las componentes hardware y software del dispositivo, con el objetivo de conocer el equipo de bloqueo a fondo y desarrollar una metodología que permita obtener las características principales a partir de pruebas de laboratorio y simulaciones.

Finalmente se mide el desempeño de la solución mediante la metodología propuesta para formular conclusiones de viabilidad y tener una mejor compresión de las capacidades de equipos de radio definido por software como solución a sistemas de bloqueo de señales.

[1]Trabajo de Grado

[2]Facultad de Ingenierías Físico-Mecánicas. Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones. Director: Homero Ortega Boada, PhD en Ciencias de la Ingeniería y Radiocomunicaciones. Codirector: Juan Pablo Moreno Acosta, Ingeniero Electrónico.

ABSTRACT

Títle: Characterization of a clandestine emission blocking system based on SDR technology[1]

Author:
Tania Lorena Santos Duarte[2]

Key Words: National Program of Electronics, Telecommunications and Computer science, blocking systems, jamming, signal interference

DESCRIPTION

This project conducts a technical feasibility study for the implementation of a clandestine emission blocking prototype based on SDR technology as support to the processes of emissions unlicensed control in the sound broadcasting band in frequency modulation FM.

The work initially presents theoretical concepts and basic foundation of a jammer team, describes hardware and software components of the device, aiming to know the blocking team in depth and develop a methodology to obtain the main features from laboratory tests and simulations.

Finally, the performance of the solution is measured by the proposed methodology to formulate feasibility conclusions and to have a better understanding of the capacities of software defined radio equipment as a solution to signal blocking systems.

[1]Bachelor Thesis

[2]Facultad de Ingenierías Físico-Mecánicas. Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones. Director: Homero Ortega Boada, PhD en Ciencias de la Ingeniería y Radiocomunicaciones. Codirector: Juan Pablo Moreno Acosta, Ingeniero Electrónico.

INTRODUCCIÓN

Gracias a la Radio Definido por Software hemos dado un salto, pasando de ser consumidores puros de sistemas de comunicaciones a creer que podemos llegar a ser actores de esa industria. De esta manera, hoy estamos apostándole al uso del SDR para la creación de un sistema de bloqueo de emisiones clandestinas. El grupo de investigación RadioGis espera lograr crear en poco tiempo una red inteligente de bloqueadores de emisiones clandestinas que combinan SDR, IoT y soluciones en la nube, como una solución innovadora que servirá de apoyo a las autoridades para ejercer control sobre este tipo de emisiones con posibilidad de usar equipo SDR, para lo cual pudiera aprovecharse la tecnología USRP que tiene la Universidad Industrial de Santander.

El proyecto parte de la necesidad expresada por el Ministerio de Tecnologías de la Información y las Comunicaciones de contar con herramientas que le permitan tomar acciones prácticas y efectivas sobre las emisiones clandestinas persistentes en las bandas de radiodifusión sonora FM. La Agencia Nacional del Espectro en el marco del artículo 26 de la Ley 1341 de 2009 numeral 11 en cumplimiento en sus funciones relacionadas con la vigilancia y control de espectro realiza el cese de emisiones clandestinas a través actividades administrativas que involucran el decomiso preventivo de los equipos de radiocomunicación usados sin autorización. Sin embargo, en algunas situaciones este proceso administrativo no se puede llevar a cabo debido a la ubicación del infractor, impidiendo adelantar los procesos de decomiso.

El grupo de investigación RadioGis ha estudiado diferentes alternativas de carácter técnico y se ha evidenciado que el empleo de equipos transmisores que causan una interferencia intencional (bloqueo o inhibición) sobre canales específicos, podrían ayudar a desestimular en la población colombiana el uso ilegal del espectro radioeléctrico, durante este proceso se ha encontrado que los productos disponibles en el mercado tienen un

funcionamiento limitados al bloquear frecuencias y canales específicos. En este sentido es preciso el uso de tecnología SDR, para lograr abrir un abanico de oportunidades no solo para las tareas de bloqueo sino para tareas relacionadas con la gestión y control del espectro radioeléctrico. Por lo tanto, el grupo de investigación RadioGis se ha planteado el reto de desarrollar un primer prototipo de un sistema de transmisión para ser usado prioritariamente como bloqueador de emisiones clandestinas basado en tecnología SDR, pero surge la necesidad de contar con un herramienta que permita comprobar si los dispositivo USRP con los que cuenta el grupo de investigación RadioGis tienen las características apropiadas para llegar a ser usados como bloqueador de emisiones clandestinas. Por otro lado este proyecto de grado plantea extraer las características que delimiten las capacidades de un equipo compuesto por un USRP, un amplificador, una antena y una parte lógica implementada en GNU Radio y comprobar si dicho prototipo es viable como una solución de bloqueo de señales, mediante una metodología de pruebas que permita concluir las ventajas y desventajas del uso de las tecnologías SDR identificando las falencias o posibles mejoras en el prototipo para su implementación en futuros proyectos.

Capítulo 1
FUNDAMENTOS DE LAS TÉCNICAS DE JAMMING

El presente capítulo muestra una introducción a los fundamentos básicos de la guerra electrónica y los tres pilares que la comprenden, ataque electrónico, protección electrónica y soporte electrónico, además realiza la definición del término *jammer* como dispositivo que permite afectar o negar durante un periodo de tiempo la transferencia de información a un terminal. También presenta las diferentes técnicas de ataque electrónico que se pueden implementarse denominadas *jamming* y se explica la técnica *jamming de cobertura* eje principal del sistema de bloqueo de emisiones clandestinas, por último se realiza una búsqueda de referentes de los dispositivos *jammer* con el fin de realizar una contextualización de la sistemas de bloqueo de señales de radio en la actualidad.

1.1. Fundamentos de guerra electrónica

La guerra electrónica es toda una nueva sección dentro de la estrategia militar que va cobrando importancia conforme las comunicaciones se convierten en una parte crítica en la guerra. Actualmente la guerra electrónica se aplica a actividades tecnológicas y electrónicas que se realizan con el objetivo de explotar, reducir, impedir la intercepción o negación de las comunicaciones. Se limita a la banda de radiofrecuencia del espectro, comenzado desde la porción menos energética del espectro electromagnético, situada entre los 3 kilohercios (KHz) y 300 gigahercios (GHz). Esto incluye específicamente las medidas de audio frecuencia en el extremo inferior, e infrarrojos y electroópticos en el extremo superior.

La guerra electrónica se define como toda aquella actividad que implica el uso de la energía electromagnética para obtener el control del espectro electromagnético, con el objetivo de un posterior ataque o protección tanto de información como de los equipos. La guerra electrónica está compuesta por tres divisiones: soporte electrónico, ataque electrónico y protección electrónica [16].

1.1.1 Soporte electrónico

Es un componente de la guerra electrónica encargado de buscar, interceptar, identificar y ubicar las fuentes intencionales y no intencionales de energía electromagnética radiada, con el propósito de reconocimiento, orientación, planificación y recopilación de información sobre el sistema de comunicación que infrinja la norma para el apoyo del ataque electrónico. [18]

1.1.2 Ataque electrónico

Abarca todas las acciones cuyo objetivo es evitar que un sistema de comunicación intercambie información de forma efectiva mediante la radiación de energía a sus fuentes. [18] Dichas acciones se pueden clasificar en tres grupos en función del ataque que perpetran [6]:

- **Energía dirigida (*directed energy*):** Los ataques basados en energía dirigida radican en la radiación excesiva de señales electromagnéticas que dañe los sistemas de comunicaciones de manera permanente. Los dispositivos que utilizan esta técnica demandan grandes cantidades de energía.

- **Engaño (*deception*):** Llamado también jamming de engaño (*deception jamming*) o jamming inteligente (*smart jamming SJ*), no tiene como objetivo destruir o dificultar las comunicaciones, sino engañar al receptor. El objetivo de esta técnica es disminuir la confianza del receptor alterando sus propias transmisiones mediante engaños. El jamming de engaño depende de la aplicación o tipo de sistema atacado.

- **Jamming de cobertura (*cover jamming*):** Consiste en el envío de señales electromagnéticas directamente hacia la fuente objetivo de manera que con el aumento del ruido, la relación de señal-ruido (SNR) disminuya y esto conlleve a dificultar, impedir o afectar la línea de tiempo de la comunicación.

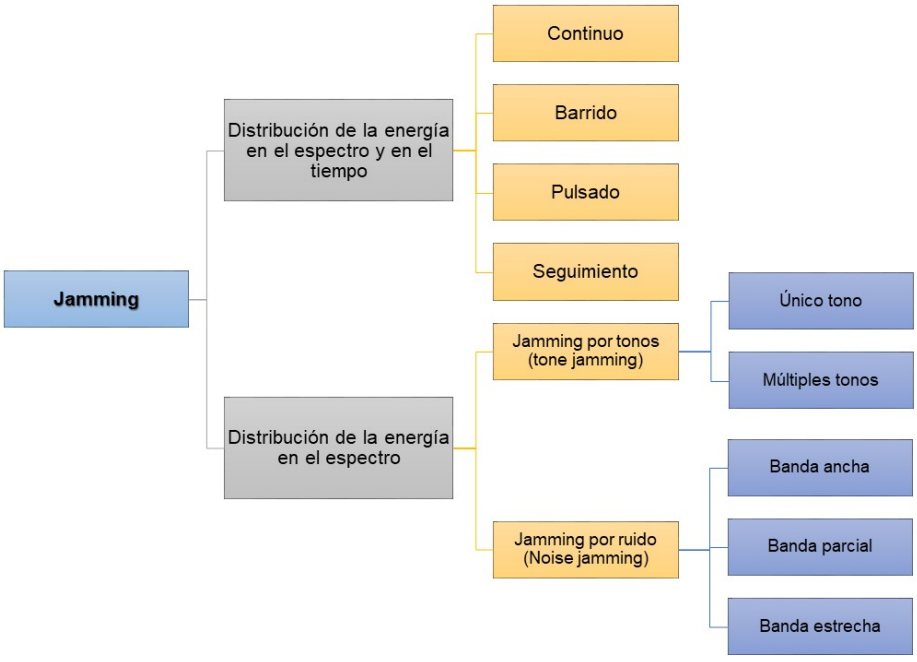
1.1.2.1 Jamming y sus técnicas

El jamming es un ataque que se realiza mediante la emisión de energía electromagnética al receptor víctima. La OTAN define el

jamming como: La emisión, re-emisión o reflexión deliberada de energía electromagnética con el objetivo de perjudicar la efectividad de los dispositivos electrónicos, equipos o sistemas enemigos. [13]

El término jamming no posee una traducción acertada que englobe todo el concepto, en su más puro significado, jamming se define como la interferencia o perturbación intencionada de una comunicación con el fin de evitar o al menos entorpecer el intercambio de información [18]. Para ello, se introduce energía en el receptor, en el momento en el que se va a recibir la señal objetivo [12]. Por lo tanto, lo que se consigue es disminuir la relación señal a ruido en recepción, haciendo que se cometan errores al recuperar la información. La energía necesaria para evitar o perjudicar significativamente la comunicación depende de la naturaleza de la señal objetivo, y de la robustez de la comunicación. En la figura 1 se presentan los diferentes tipos de Jamming de acuerdo a su distribución de energía [13] [18].

Figura 1: Técnicas de jamming



1.1.3 Protección electrónica

Son acciones y contra medidas empleadas con la finalidad de proteger un sistema de comunicaciones de acciones de ataque externos [16] . También conocido como técnicas Anti-Jam, utiliza técnicas que impiden el bloqueo, la interferencia y manipulación de la información, en esta categoría se incluyen

la codificación y encriptación [17]

1.2. Jamming de cobertura

El terminal S-jammer diseñado, emplea la técnica de jamming de cobertura por banda parcial [18], puesto que envía señales de interferencia de manera intencional hacia la fuente objetivo, para dañar las comunicaciones al mantener el canal de comunicaciones ocupado.

Esta técnica comienza a interferir solo cuando observa que se produce una actividad de red en un determinado canal identificado como no deseado, introduciendo energía a través de todo el ancho del espectro de frecuencias en que opera el blanco que va hacer objetivo del ataque, con el objetivo de que al aumentar el ruido en el canal que se traduzca, la relación señal a ruido se reduzca , esta técnica es un ataque directo a la capacidad del canal de un sistema de comunicación.

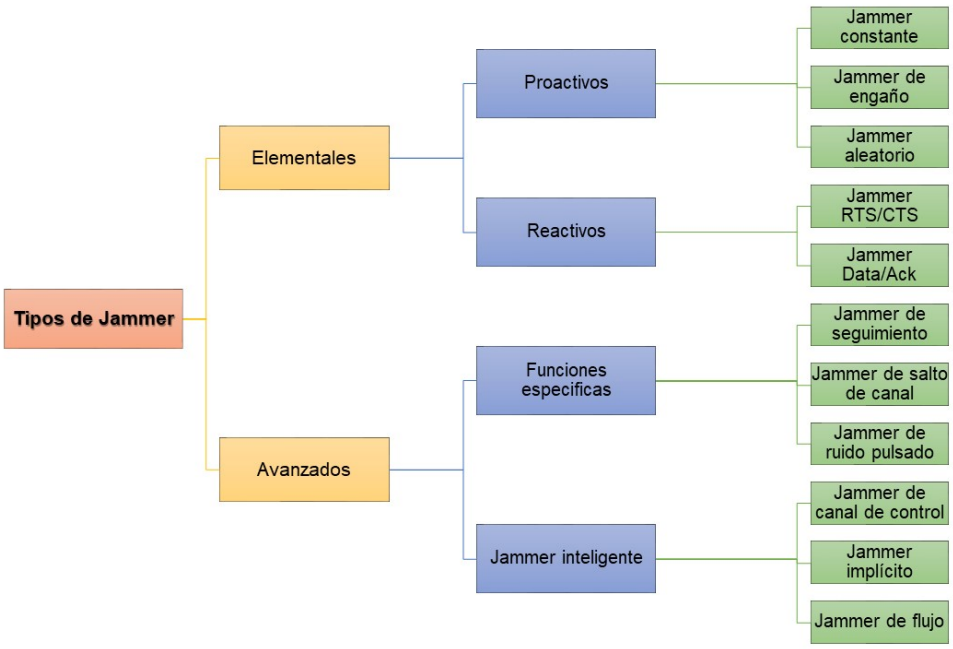
1.3. El jammer

Se considera Jammer todo dispositivo que permita afectar o negar durante un periodo de tiempo determinado, el acceso a una terminal receptora a la información proveniente de un transmisor, empleando *técnicas de "Jamming"* deteriorando perjudicialmente la calidad de la señal vista desde la terminal afectada [20]. Un jammer intenta lograr esto radiando energía de una señal no deseada hacia los receptores de los sistemas de comunicación. De esta manera, sí el nivel de la señal no deseada es lo suficientemente fuerte, causará que los receptores no puedan demodular la señal proveniente del transmisor original, suponiendo que la señal no deseada enviada por el jammer no es una réplica de lo que fue transmitido originalmente, la comunicación es negada en el enlace RF [18].

También suele considerarse inhibidores de frecuencias debido a que el término jammer no posee una traducción en concreto, son comúnmente utilizados en los servicios móviles en coberturas limitadas, la recepción de señales GPS sobre una zona, puntos de acceso WI-FI, enlaces Bluetooth, entre otros. La estrategia que emplea un jammer depende directamente de la aplicación, el autor en [7] clasifica el jammer en elemental o avanzado dependiendo de su funcionalidad.

El jammer elemental es aquel que envía paquetes de datos o bits aleatorios al canal objetivo poniendo a todos los demás nodos incomunicados, este jammer no cambia de canal de manera autónoma solamente hasta que se agota su energía o por requerimiento del usuario [6], se pueden dividir en dos subgrupos: proactivo y reactivo. El jammer avanzado puede cambiar de canal atacado y atascar en diferentes anchos de banda para diferentes períodos de tiempo, usado principalmente como estrategia para bloquear sistemas FHSS Y DSSS, además cuenta con un aumento en el rendimiento de bloqueo, independientemente del uso de energía pues conserva la potencia al limitar su ataque a un solo canal antes de saltar a otro. Se clasifica en dos subtipos: función específica e inteligente-híbrido [7] [23]. En la figura 2 se observan los tipos de Jammer de acuerdo a su aplicación.

Figura 2: Tipos de jammer para comunicaciones inalambricas



1.3.1 Situación Actual de los Jammers

El desarrollo de prototipos de este tipo de tecnologías no presenta mayor dificultad en una implementación de bajo nivel y está se facilita sí el servicio que se dispone como objetivo no presenta algún tipo de protección anti-jam. Entre los años 2000 y 2017 los autores en [4] [9] [2], presentaron alternativas de fácil desarrollo para el bloqueo de señales GSM, Spread spectrum y Wifi. No obstante, para aplicaciones más elaboradas se innova en las técnicas y contra-

medidas como las presentadas en [3] [5] [11], para facilitar el éxito del ataque sobre sistemas protegidos.

En Colombia y conforme a lo establecido en el numeral 11 del artículo 26 de la Ley 1341 de 2009, son funciones de la ANE "Ordenar el cese de operaciones no autorizadas de redes, el decomiso provisional y definitivo de equipos y demás bienes utilizados para el efecto, y disponer su destino con arreglo a lo dispuesto en la ley, sin perjuicio de las competencias que tienen las autoridades Militares y de Policía para el decomiso de equipos", con el fin de regular el uso del espectro electromagnético, siendo este de uso público inajenable e imprescriptible sujeto a la gestión y control del Estado, se han presentado soluciones que faciliten tratar esta problemática con la presentada por el autor en [4] que expone un estudio de sistemas de detección e inhibición para emisores celulares, los autores en [2] [19] expone sobre el diseño e implementación de prototipos inhibidores de señales.En [1], [10] y [21] se analizan las necesidades de gestión del espectro radioeléctrico que surgirán con la entrada inminente de la Radio Cognitiva (CR) a fin de compartir espectro no utilizado en función de diferentes parámetros. En [8] se describe IoT a nivel de modelo, mientras [22], [15] complementa este concepto con servicio de sensado en lo que se conoce como *Sensor Information Tecnhology* (SensIT) . En [14] se propone una estrategia de implementación de algoritmos de radio propagación con computo en la nube, que pueden ser vistos como equipos de medición virtuales en una plataforma de apoyo a la gestión del espectro radioeléctrico.

En el año 2015 se realizó el convenio 035 entre la ANE y la UIS, con el objeto de "desarrollar un sistema de medición del uso del espectro radioeléctrico basado en la Radio Definida por Software (SDR), que combine técnicas de análisis espectral con una visión de análisis que se apoye en bases cuasi ortogonales y valorar su desempeño respecto al uso de los métodos convencionales en tareas de observación del espectro y medición de niveles RNI, complementado con materiales pedagógicos para impulsar el desarrollo de soluciones de gestión del espectro radioeléctrico con SDR en Colombia". Los resultados de la investigación realizada en el marco del convenio mencionado evidencian la posibilidad de usar dispositivos SDR, para aplicaciones tales como el bloqueo de señales radioeléctricas en canales específicos. Dichas soluciones deben estar regidas cumpliendo las especificaciones dictadas en la Resolución 2774 de 2013 Mediante la Resolución 2774 de 2013 y otras consideraciones técnicas.

Capítulo 2
DESCRIPCIÓN DEL EQUIPO S-JAMMER

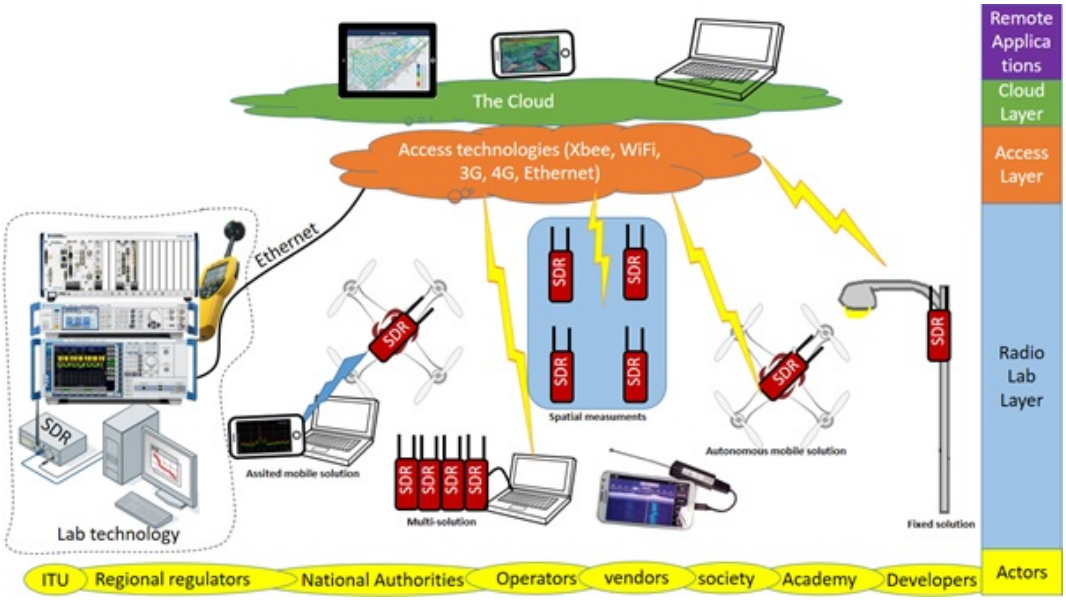
El terminal S-jammer diseñado es un prototipo cuyo componente principal es un transreceptor basado en tecnología SDR, para el bloqueo de señales clandestinas en la banda de radio difusión sonora FM, haciendo uso de la técnica de bloqueo de jamming por cobertura, que busca la disminución de la relación señal a ruido en el transmisor ilegal, mediante la radiación directa de ruido. Está compuesto de dos partes, el software y el hardware, dentro de las componentes del software encontramos aplicaciones basadas en GNU Radio encargadas de realizar el monitoreo del espectro para la detección de señales clandestinas y el bloqueo controlado de la emisión ilegal. Entre las componentes de hardware encontramos un amplificador FM, una antena dipolo de alta potencia, un sistema de alimentación y una línea de transmisión.
Este terminal pertenece a un servicio llamado S-Jammer que el grupo de investigación RadioGis se encuentra desarrollando y consta de una red inteligente de bloqueadores de emisiones clandestinas que combinan SDR, IoT, conectividad IP y soluciones en la nube.

2.1. Modelo de capas del servicio S-JAMMER

El modelo del servicio S-Jammer consiste en establecer un marco de entendimiento entre los diferentes actores y así incrementar cada vez más el número de personas y entidades que pueden aportar a este campo. A su vez reduce la complejidad para que cualquier usuario lo pueda interpretar y replicar de manera sencilla. Para el modelo de capas se usa el modelo RIoT desarrollado por el grupo de investigación RadioGis para impulsar el desarrollo de soluciones de radiocomunicaciones y que se describe a continuación. En este modelo, los componentes de radio son vistos como cosas conectadas a

internet y por eso el modelo se ha llamado Modelo de radio IoT (RIoT) como se observa en la figura 3.

Figura 3: Modelo RoIT



Fuente: Grupo de investigación RadioGis

- **Capa de los actores** Esta capa señala la importancia de comenzar cualquier desarrollo a partir de necesidades reales, pero también refleja la necesidad de compromiso de diferentes autoridades y actores en general.

- **Capa RadioLab** Esta capa abarca todas las tecnologías con las cuales tienen contacto los investigadores de RF, usualmente equipos de medición. Para esto se cuenta con dos ambientes principales; por una parte está Lab technology, que encierra todos los recursos usados por los investigadores para diseñar, crear, configurar, calibrar y hacer el mantenimiento a la tecnología SDR y, por otra parte, los prototipos, donde se prueban los desarrollos en un ambiente real. c

  El terminal S-JAMMER se ubica en esta capa, pues en esta es donde se desarrollan las herramientas de medición, las cuales pueden ser vistas como equipos o como sensores, aunque también puede darse el caso de ser vistos como algoritmos o como sensores virtuales. Para nuestro caso particular, el terminal S-jammer cuenta con un sistema de monitoreo de espectro para la detección de emisiones clandestinas que permite escanear el espectro en función de las necesidades del operador de la

red para identificar posibles infractores, además efectúa el análisis sobre las señales para la vigilancia sobre las bandas que se estén bloqueando controlando el nivel de señal enviada, extrae los parámetros mas importantes con el propósito de brindar soporte electrónico para orientar y planificar posteriores ataque hacia las fuentes ilegales haciendo posible que la emisión no se siga llevando acabo. Para lograr esto el terminal S-Jammer cuenta con una seria de equipos que proporcionan la realización de estas acciones, compuestos por equipo radio periférico USRP, un amplificador de ganancia y una antena dipolo de media onda .

- **Capa de Acceso** Abarca las tecnologías necesarias para que las soluciones de la capa RadioLab tengan conexión a internet. Cualquier tecnología de comunicación tiene cabida aquí como Xbee, Wifi, comunicaciones móviles 3G o 4G y hasta cable por puerto Ethernet. Se resuelven principalmente dos problemas: conexión inalámbrica entre el usuario y equipos o incluso entre equipos y equipos; y el establecimiento de una compuerta a Internet para esos equipos.

- **Capa de la nube** Esta capa abarca los recursos que pueden ofrecer un valor agregado a la solución, tales como bases de datos, procesamiento en la nube

- **Capa de aplicaciones** Son las aplicaciones que permiten a usuarios conectados a la nube acceder a la información o tomar control de las tecnologías de la capa RadioLab.

2.2. Componentes de software

La radio definida por software es una tecnología que implementa a través de software componentes típicamente implementados en hardware, es de gran utilidad gracias a su capacidad de manejar varios protocolos en tiempo real y la versatilidad para reconfigurar sus funcionalidades a aplicaciones específicas, a largo plazo se prevee que el SDR se convierta en la tecnologia dominante en las radiocomunicaciones. Con la implementación de un terminal S-Jammer haciendo uso de la tecnología SDR se espera resolver problemas como ancho de banda, conectividad, posibilidad de control remoto, selección de máscaras especiales para el bloqueo, entre otros. La herramienta usada para el desarrollo de las aplicaciones del S-Jammer es GNU Radio que combina la programación en lenguajes como Python y C++, facilitando la administración de recursos y el cumplimiento de tareas específicas. Adicionalmente, cuenta con una interfaz gráfica que

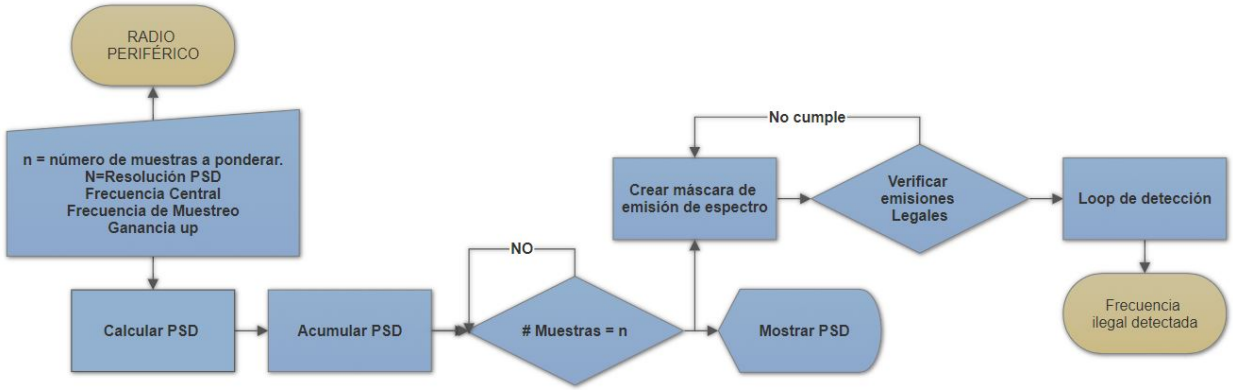
mediante la interconexión de bloques y su configuración provee soluciones de manera sencilla. Las dos componentes de software del terminal S-Jammer implementadas en GNU Radio serán descritas a continuación.

2.2.1 Sistema de monitoreo del espectro para detección de emisiones clandestinas

El soporte electrónico encargado de determinar los parámetros de la señal blanco del ataque, se realiza mediante un sistema de monitoreo del espectro, el cual pondera la densidad espectral de potencia de la muestra obtenida mediante un radio periférico, el funcionamiento del monitoreo depende de cinco variables, que son la resolución del espectro a visualizar; la frecuencia de muestreo; la frecuencia central de la muestra; el número de muestras a ponderar y un parámetro de ganancia up que limita la decisión entorno la potencia de las señales a detectar.

El sistema de monitoreo toma los datos del radio periférico, aplica la transformada rápida de Fourier, esta representación se configura con la variable N, que determinar la resolución de la representación de la densidad espectral de potencia de la señal. El espectro obtenido se acumula *n-veces* y se promedia con el fin de estabilizar el piso de ruido de la muestra, antes de crear la máscara de comparación, se detectan las emisiones en la muestra que pertenecen al Plan Técnico Nacional de Radiodifusión Sonora FM, haciendo uso de la media de la muestra ponderada y las emisiones detectadas legales, se crea una ***máscara de emisión de espectro*** como base de comparación. Por último se realiza un loop de comparación entre las muestras nuevas ponderadas y las máscara creada, como resultado de esta comparación se obtienen las frecuencias de las emisiones ilegales detectadas, el diagrama de flujo del funcionamiento de monitoreo se presentan en la figura 4.

Figura 4: Diagrama de flujo sistema de monitoreo.



El sistema de monitoreo se construyó en lenguaje de programación python y se implementa mediante un bloque jerárquico en GNU Radio Companion, una de sus principales ventajas es su capacidad de adaptarse a la muestra haciendo uso de parámetros como frecuencia de muestreo y frecuencia central, por otro lado permite disminuir el consumo de recursos de procesamiento disminuyendo la resolución de la densidad espectral de potencial a procesar, además permite al usuario establecer los criterios de detección de señales.

2.2.2 Sistema de ataque de emisiones clandestinas

Para el ataque a sistemas de comunicaciones de voz analógicas el nivel necesario para degradar o interferir una transmisión es de un 30 % o mas de la transmisión de voz [16]. Para lograr que la transmisión no sea efectiva y la información no se entienda se debe tener una relación señal a jammer de -6 dB J/S para considerarse adecuada para la interrupción de la transmisión [16]. Para llevar acabo este bloqueo de señales el S-JAMMER cuenta con un sistema de ataque desarrollado en GNU Radio que hace uso de la técnica *jamming de cobertura por banda parcial* radiando energía hacia la fuente cubriendo una parte de la señal que se quiere atacar elevando el nivel de ruido de fondo.

Este sistema de ataque electrónico realiza el envió de ruido gaussiano solamente en el canal que esta infringiendo, produciendo que todos los nodos de recepción en ese canal cambien a nodos no operativos. Esta operación se realiza sólo cuando observa de una actividad en un canal no asignada por el Plan Técnico Nacional de Radiodifusión Sonora FM. La señal enviada por esta técnica es un señal portadora de ruido de alta potencia que se desplazando entre las bandas de interés, es decir, entre la banda previa-

mente identificada como frecuencia ilegal no permitidas por el Plan Técnico Nacional de Radiodifusión Sonora en Colombia ,pero en ninguna circunstancia con la intensión de dañar los equipos, solamente inhabilita la transmisión de señal, mediante la disminución de la relación señal a ruido de esta, siendo un ataque directo a la capacidad del canal del sistema de comunicación.

2.3. Componentes de hardware

2.3.1 Dispositivo USRP E310 El USRP E310 es una plataforma flexible de bajo costo para sistemas de radio definido por software perteneciente a la serie embebida desarrollada por Matt Ettus, diseñada para trabajar como un procesador externo que permite implementar de forma rápida, sistema flexibles y potentes de SDR, este dispositivo utiliza el framework OpenEmbedded para crear distribuciones personalizadas de linux que se adaptan a las necesidades específicas de una aplicación. Esta plataforma autónoma dispone de un procesador de banda base dual ARM Cortex A9 a 667 MHz con 1GB DDR de RAM e referencia así como una FPGA Xilinx 7 que se encarga de gran parte del control y el procesamiento de las señales de Radio Frecuencia (RF) con una memoria RAM dedicada DDR3 de 512MB; un conversor A/D dual de 61.44 MS/s con 12 bits. Además posee un transceptor 2X2 MIMOAD9361 de Analog Device de hasta 56 MHz de ancho de banda instantáneo con frecuencias de operación de 70 MHz a hasta 6 GHz y un consumo de energía de 2 a 6 vatios. Para la detección de la posición y la sincronización de la hora cuenta con un receptor GPS integrado, así como dos puertos USB host para aumentar la capacidad de almacenamiento. Para el seguimiento y análisis de espectro en señales en tiempo real y de banda ancha, tanto en transmisión como en recepción el equipo utiliza conmutadores para seleccionar entre un banco de filtros RF disponibles para mejoran la selectividad del transceptor para distinguir con precisión una amplia gama de señales espectrales.

El dispositivo utiliza la API de software UHD para conectarse a un equipo de computo.La interfaz de hardware USRP (UHD) es el controlador oficial preinstalado para todos los dispositivos USRP de Ettus Research, siendo éste soportado por sistemas operativos como Linux, Mac OSX y Windows, así como compatible con software de terceros, como GNU Radio, LabVIEW, Matlab Amarisoft LTE eNodeB, OpenBTS, Iris. La tabla 1 contiene las especificaciones técnicas del dispositivo.

Tabla 1: Especificaciones técnicas USRP e310

Especificaciones	**E310**	**Unidad**
Entrada DC	5-15	V
Consumo de potencia	2-6	W
Frecuencia de muestreo ADC(máx)	61.44	MS/s
Resolución de muestreo ADC(máx)	12	bits
Potencia de salida	>10	dBm
Dimensiones	13.3x6.82x26.4	cm
Peso	0.365	Kg

Este dispositivo cuenta con una serie de características deseables como lo son: bajo precio, tamaño reducido, conectividad y capacidad de procesamiento y almacenamiento que pueden ser aprovechadas para el control de las señales transmitidas de la solución propuesta. El dispositivo USRP e310 se puede configurar de dos formas el modo network y el modo embebido.

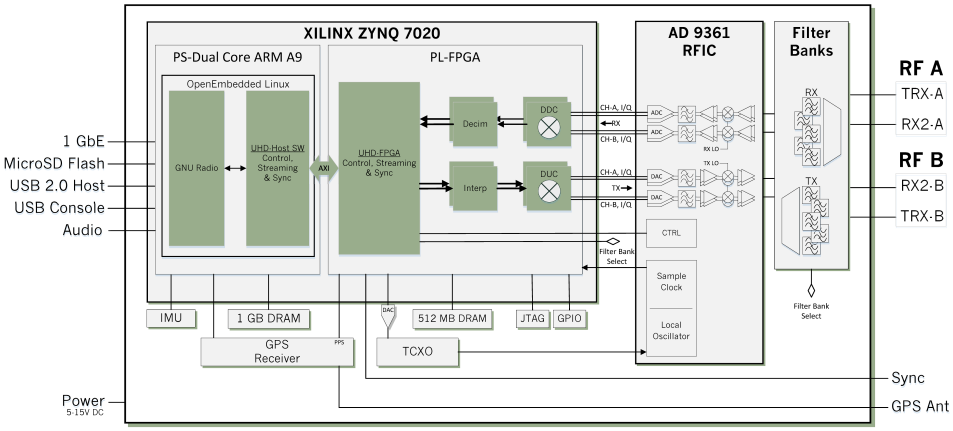
Modo network: Es la configuración usada cuando el equipo USRP puede ser visto sólo como el módulo encargado de obtener la envolvente compleja de la señal de interés que captura la antena. Este modo corresponde a la configuración mas común en los laboratorios experimentales por ser la solución más económica y a la vez más potente. Consiste en lograr un complemento perfecto entre el hardware del USRP y un computador con el software apropiado. El término network es usado debido a que el hardware se conecta al computador usualmente por un puerto Giga Ethernet de manera directa. la aplicación que se desarrolla como soporte para las mediciones sólo puede ser configurada desde el computador.

Modo embebido: Se trata del equipo funcione independientemente de un computador, debido a que el equipo incluye las capacidades de cómputo, almacenamiento y programación. En este modo, eventualmente se puede usar un computador con propósitos de visualización o como herramienta para pruebas, mantenimiento del equipo y de la aplicación embebida. El USRP ejecuta un cliente DHCP en el puerto Ethernet de 1 Gigabit, para hacer la conexión a la red del dispositivo , el dispositivo debe aparecer como hostname ettuse300 en la terminal después de esto se puede programar el dispo-

sitivo a través de SSH.

La arquitectura de este dispositivo cuenta con una placa madre que proporciona los siguientes subsistemas: generación de sincronización, FPGA, ADC, DAC, la interfaz de procesador central, oscilador local y regulación de potencia. Estos son los componentes básicos que se requieren para el procesamiento de banda base de señales. Un front-end modular, se utiliza para las operaciones analógicas, conversión, filtrado, y otras condiciones de la señal. Esta modularidad permite el uso del USRP para aplicaciones que operan entre 70 MHz y 6 GHz. En la figura 5 se aprecia la arquitectura que de el USRP E310

Figura 5: Arquitectura del USRP E310



Fuente: https://www.ettus.com/content/

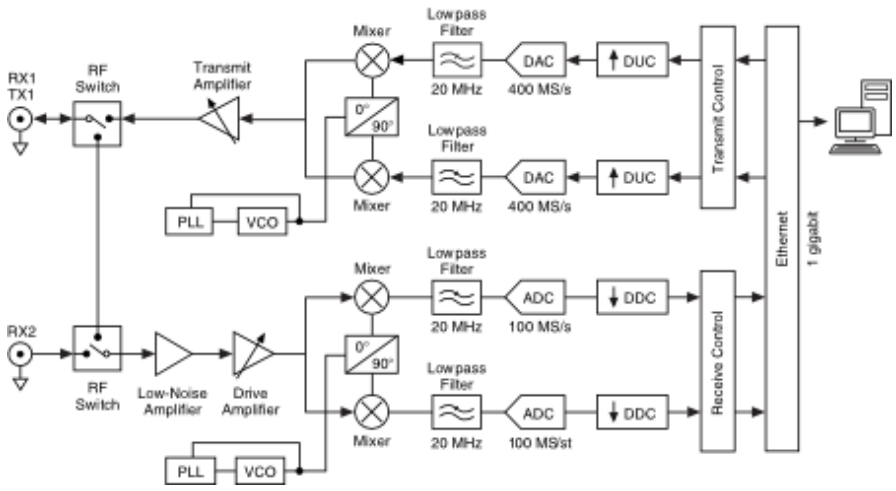
En la distribución de las operaciones de la FPGA realiza varias acciones de DSP, que facilitan en ultimas la traducción de señales reales en el dominio analógico a tasa más baja, señales de banda base a complejos en el dominio digital. Generalmente, estas muestras complejas se trasladan a las aplicaciones que se ejecutan en el procesador central, que ejecuta operaciones de DSP. El código de la FPGA es de código abierto y se puede modificar para acceder a las operaciones de alta velocidad, baja latencia producidas en la FPGA.

2.3.2 Dispositivo USRP 2920

El USRP 2920 es un transreceptor de radio frecuencia ajustable con un convertidor analógico-digital de alta velocidad y un convertidor digital-analógico de dos canales para la transmisión de señales de banda base I y Q muestreadas en su entrada a una rata fija e invariable de 100 MS/s cuantizadas a 14 bits/muestra hacia un equipo de computo principal mediante Gigabit Ethernnet, es frecuentemente usado en emisión FM, espacio en blanco, seguridad pública, dispositivos móviles terrestres, entre otros.

Los datos digitalizados I/Q siguen caminos paralelos a través de un proceso de conversión descendente digital (DDC) que mezcla, filtra y diezma la señal, donde el usuario tiene la posibilidad de graduar la velocidad de la señal de entrada hasta una velocidad de 100 MS/s. Las muestras convertidas a la baja, cuando se representan como números de 32 bits (16 bits cada uno para I y Q), se pasan al equipo host con una velocidad de hasta 20 MS/s a través de una conexión Gigabit Ethernet estándar.

Figura 6: Arquitectura del USRP 2920



Fuente: http://www.ni.com/documentation/en/labview-comms/2.0/2920/block-diagram/

Para la transmisión, las muestras de la señal de I / Q en banda base son sintetizadas por el ordenador central y alimentadas al USRP-2920 con una velocidad de hasta 20 MS/s sobre Gigabit Ethernet, cuando se representan con 32 bits (16 bits cada uno para los componentes I y Q) . El hardware USRP interpola la señal entrante a 400 MS / s usando un proceso digital de conversión ascendente (DUC) y luego convierte la señal

a analógica con un convertidor digital-analógico (DAC) de 16 bits de doble canal. La señal analógica resultante se mezcla entonces hasta la frecuencia portadora especificada.

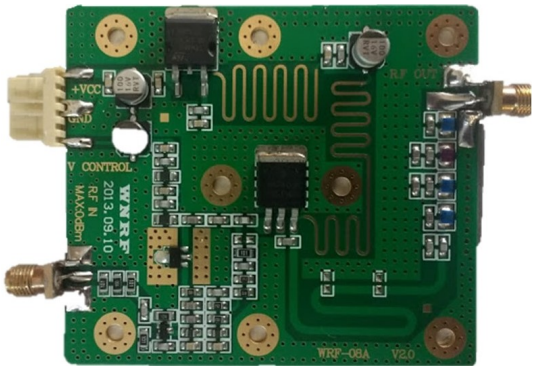
De igual forma se debe que tener en cuenta que el rango dinámico del ADC es 1 Vp-p, el ancho de banda máxima real es de 20 MHz para 16 bits/muestra; 40 MHz para 8 bits/muestra, la rata máxima real de muestreo I/Q: 25 MS/s a 16 bits/muestra; 40 MS/s a 8 bits/muestra. El manual de usuario aclara que estos valores pueden verse limitados aún más por las específicaciones del computador usado y por la velocidad de la conexión entre el USRP y el computador. La esquema presenta el USRP 2920 se presenta en la figura 6 y sus especificaciones técnicas se encuentran el la tabla 2.

Tabla 2: Especificaciones técnicas USRP 2920

Especificaciones	**2920**	**Unidad**
Entrada DC	12-15	V
Consumo de potencia		W
Frecuencia de muestreo ADC(máx)	25	MS/s
Resolución de muestreo ADC(máx)	16	bits
Rango de frecuencia	0.05 a 2.2	GHz
Dimensiones	15.87x4.82x21.20	cm
Peso	1.193	Kg
TRANSMISIÓN		
Rango de ganancia	0 a 31	dB
Potencia de salida (máx)		
50 MHz a 1,26 GHz	50 a 100	mW
1,26 GHz a 2,26 GHz	30 a 70	mW
RECEPCIÓN		
Potencia de entrada	12-15	dBm
Rango de ganancia	0 a 31,5	dB

2.3.3 Amplificador El amplificador escogido para el prototipo S-Jammer encargado de amplificar la señal de bloqueo transmitida desde el USRP es el RF Pallet Módulo 87MHz-108MHz fabricado y comercializado por la empresa FMUSER International Group INC. En su estructura cuenta con un amplificador de radio frecuencia, un circuito pasa bajas, un regulador de voltaje y un circuito de control de potencia controlado por voltaje. El dispositivo en físico así como los conectores SMA y el conector para el control de voltaje y alimentación anexados se muestran en la figura 7

Figura 7: Amplificador FMUSER RFU-10A



Este amplificador tiene la ventaja de presentar una relación con respecto a la frecuencia de portadora de -65 dBc, lo cual es útil para acotar el envió de señales de bloqueo a un solo canal con el fin de no intervenir en señales legales durante el proceso de ataque a las emisiones clandestinas y así evitando el riesgo a una invasión indebida de banda de frecuencias que están por fuera de las seleccionadas como clandestinas. Además cuenta con un rango en frecuencias de funcionamiento optimo desde los 76 MHz hasta los 110 MHz en trabajo continuo, su entrada es de aproximadamente entre -10 a 0 dBm satisfaciendo su excitación con el rango de las señales de salida que proporcionadas por los USRP que se encuentran en el grupo de investigación RadioGis. Las especificaciones técnicas general del dispositivo se presentan en la tabla 3.

Tabla 3: Especificaciones técnicas Amplificador FMUSER RFU-10A

Especificaciones	**Valor**	**Unidad**
Tensión de alimentación	12-16	V
Corriente de funcionamiento	$\leq$1.5	A
Rango de frecuencia	87-108	MHz
Ancho de banda	20	MHz
Potencia máx. de entrada	0	dBm
Potencia de salida	>8	W
Flatness	<1	dBm
Temperatura de funcionamiento	-20 a 50	^{o}C
Dimeniones	80x70x5	mm

2.3.4 Linea de transmisión. La guía de onda utilizada para transportar eficientemente la energía de radiofrecuencia desde el transmisor compuesto por un USRP y el amplificador de ganancia FM RFU-10A a la antena dipolo de media onda de alta

potencia es un cable coaxial Heliax FSJ4-50B (figura 8), y tiene una longitud de 5 metros, que está determinada por la relación 4 veces la longitud de la antena, necesaria para disminuir la reflexión de la onda de la energía transmitida.

Figura 8: Cable coaxial Heliax FSJ4-50B 1/2 in

Fuente: http://www.lianstar.com/pic/cable-coaxial-de-1-2.jpg/

Este cable posee una impedancia característica 50Ω y cuenta con aislamiento de polietileno para minimizar la pérdida de señal y excelentes características eléctricas tales como la baja amortiguación y bajo coeficiente de reflexión. Estas propiedades tienen la ventaja de reducción de la estática en la transmision de señales y la disminución el ruido de otras fuentes en la recepción de señales. Las principales especificaciones técnicas brindadas por el fabricante, se aprecian en la tabla 4.

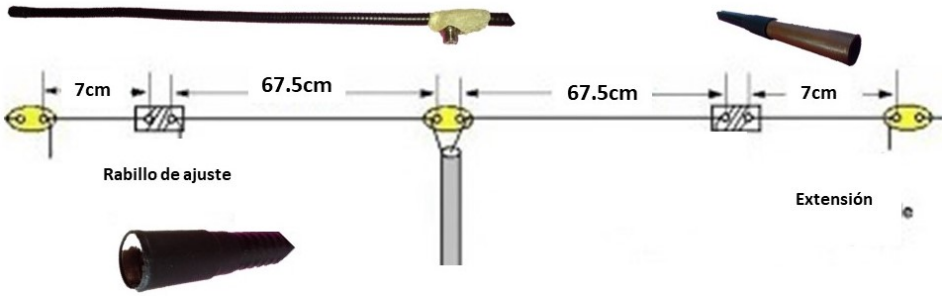
Tabla 4: Especificaciones cable coaxial Heliax FSJ4-50B

Especificaciones	**Valor**	**Unidad**
Diámetro nominal	1/2	in
Peso del cable	0.21	kg/m
Diámetro sobre la chaqueta	13.462	mm
Resistencia de aislamiento	100000	MΩ*km
Impedancia	50 ± 1	Ω
Frecuencia de funcionamiento	1 a 10200	MHz
Potencia máxima	15,6	kW
Velocidad	81	%

2.3.5 Antena dipolo de media onda de alta potencia. La antena usada en este prototipo en la parte de transmisión de señales de bloqueo, es una antena dipolo de media onda de alta potencia que en el plano azimuth (polarización vertical)

exhibe un campo omnidireccional, y en el plano de elevación (polarización horizontal) el campo es direccional y está compuesto por dos lóbulos. La antena esta construida con un cable Heliax FSJ4-50B de longitud 1,35 metros para una frecuencia de trabajo inferior a 107.5 Mhz y en sus extremos posee unos conectores de 7 cm de longitud que permiten añadir una extensión con el fin de aumentar la longitud de onda y así disminuir la frecuencia de operación de la antena a frecuencias inferiores pertenecientes a la banda de interés.

Figura 9: Antena dipolo de media onda



La longitud de cada unas de las ramas de la antena dipolo es de 67,5 cm, obtenido de la ecuación 2.1, el conector usado en esta antena son Pl-259 hembra. Una ventaja de este tipo de antena es que reduce significativamente el nivel al que se reciben señales no deseadas, o alternativamente, la potencia radiada efectiva transmitida de transmisores hostiles sin producir interferencia. Además debido al grosor de la antena de 1/2 in puede ser usada para transmitir potencia superiores a los 500W . La impedancia características teórica de esta antena es de 50Ω evitando el uso de un balum de relación 1:1 como acople de impedancias entre la antena dipolo de media onda y la linea de transmisión.

$$LongitudDelRamal = \frac{\lambda}{4} = \frac{VelocidadLuz(m)}{4 * frecuencia(Hz)} \tag{2.1}$$

2.3.6 Fuente de alimentación La fuente de alimentación usada en el terminal S-jammer para la alimentación del amplificador de ganancia FM RFU-10A es una fuente AC/DC de la familia LRS-75-12 (figura 10) fabricada por la empresa Mean Well. Es una fuente de una sola salida de tipo cerrado variable de 10 V a 14 V en su tensión salida y hasta 6 A de corriente de salida. Esta fuente ofrece un bajo consumo

de energía sin carga menor a 0.2 W y permite que el sistema final satisfaga fácilmente los requerimientos energéticos del prototipo.

Figura 10: Fuente de alimentación LRS-75-12

Fuente: http://www.mouser.com/ds/2/260/LRS-75-SPEC-806318.pdf/

Tiene una gama de funciones de protección contra corto circuito, sobrecarga y sobre voltaje, cumple con las normas internacionales de seguridad IEC/EN61558-1, y IEC/EN 60335-1, de alta eficiencia, larga duración y alta confiabilidad de suministro de energía para diversas aplicaciones industriales. Las especificaciones técnicas de la fuente se observan en la tabla 5.

Tabla 5: Fuente de alimentación LRS-75-12

Especificaciones	**Valor**	**Unidad**
Tensión de salida	12	V
Corriente de salida	6	A
Potencia de salida	72	W
Tensión de entrada	120 a 373, 85 a 264	VAC
Dimensiones	97x99x30	mm
Peso de la unidad	300	g

Capítulo 3
METODOLOGÍA PARA LA CARACTERIZACIÓN DEL S-JAMMER

La metodología diseñada para caracterizar el S-Jammer centra sus esfuerzos en extraer los parámetros que muestran las capacidades y debilidades del mismo, se fundamenta en el análisis de los componentes de software y hardware del dispositivo, y el desarrollo de simulaciones que permitan reflejar de forma fiel el comportamiento del equipo en distintas condiciones de operación, con el fin de obtener parámetros que delimiten las capacidades del S-Jammer como la potencia de transmisión, la banda de operación, el área efectiva, interferencia, entre otros. Esta metodología es dividida en tres secciones que son *HARDWARE, SOFTWARE* y *TERMINAL*, planteando pruebas donde es necesario el uso de instrumentos de medición como el analizador de espectros, analizador de redes y el vatimetro RF, además de equipos radio periféricos y de computo.

3.1. Metodología de caracterización hardware

El dimensionamiento del S-Jammer parte desde la caracterización de cada uno de sus componentes de hardware, pues son estos los que limitan la capacidad de su funcionamiento en frecuencia, la potencia capaz de interpretar durante el monitoreo, la potencia de jamming transmitida y las pérdidas que presenta el dispositivo debido fenómenos como la reflexión y retorno. Es importante antes de realizar las pruebas de caracterización, conocer adecuadamente la herramientas de medición, su capacidades, limitaciones y cuidados.La metodología de caracterización del Hardware se presenta en la tabla 6.

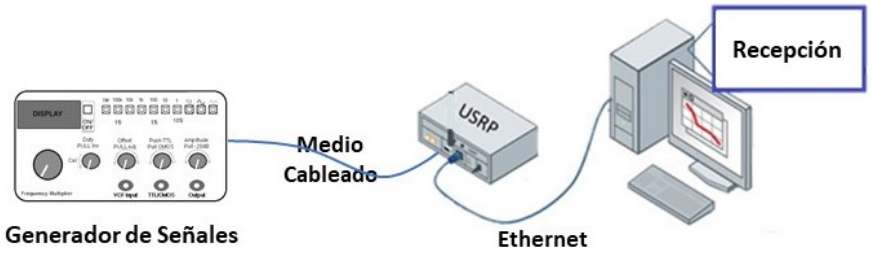
Tabla 6: Metodología de caracterización del hardware

Metodología de caracterización de Hardware				
Sección	**Radio periféricos**	**Amplificador**	**Línea de transmisión**	**Antena**
Objetivos	-Determinar la máxima ganancia del amplificador Rx. -Determinar la máxima potencia de transmisión. -Verificar la linealidad de la transmisión y recepción en la banda de interés. -Determinar la mínima potencia capaz de interpretar en recepción.	-Determinar la máxima potencia amplificada. -Verificar la linealidad en la banda de interés. -Visualizar amplificación en función de la frecuencia de portadora. -Verificar amplificación en función del voltaje de alimentación.	-Determinar la pérdidas en la línea. -Determinar la impedancia característica - Parámetros de transmisión	-Determinar la frecuencia de resonancia. -Determinar el ancho de banda -Determinar la relación de onda estacionaria y la impedancia característica.
Equipos	-USRP -Analizador de espectros -Generador de señales -Conectores -Atenuador -Equipo de computo -Medio cableado Los diagramas de conexión se presentan en la Figuras 11 y 12	-USRP -Amplificador FM -Fuente de alimentación -Conectores -Watimetro -Carga fantasma -Equipo de computo -Medio cableado El diagrama de conexión se presenta en la Figura 13	-Analizador de redes -Conectores -Línea de Transmisión -Sonda de medición El diagrama de conexión se presenta en la Figura 14	-Analizador de redes -Conectores -Antena -Sonda de medición Diagrama de conexión se presenta en la Figura 15
Parámetros de control	-Ganancia del amplificador Tx, controlada por el bloque UHD USRP Sink. -Potencial de la señal de prueba. -Ganancia del amplificador Rx, controlado por el bloque UHD USRP Source. -Frecuencia de portadora de la señal de prueba.	-Ganancia del amplificador Tx, controlado por el bloque UHD USRP Sink. -Frecuencia de portadora de la señal de prueba. -Voltaje de alimentación del amplificador.	-Respuesta en magnitud -Respuesta en Fase -Carta de Smith	-Respuesta en magnitud. -Respuesta en fase. -Carta de Smith
Pruebas	Etapa 1: Recepción -Fijar ganancia Rx, controlada por UHD Source en 0dB -Variar potencia y variar frecuencia de portadora de la señal de prueba Registrar resultados en recepción Etapa 2: Transmisión -Variar ganancia Tx, controlada por UHD Sink variable. -Variar frecuencia de portadora de la señal de prueba -Registrar resultados de recepción	Etapa 1: Voltaje constante -Variar ganancia Tx, controlada por UHD Sink variable. -Variar frecuencia de portadora de la señal de prueba Registrar mediciones del watimetro Etapa 2: Voltaje variable -Variar ganancia Tx, controlada por UHD Sink variable. -Variar frecuencia de portadora de la señal de prueba Registrar mediciones del watimetro	Etapa 1: Dos puertos -Calibración del dispositivo - Configuración modo network -Configurar puertos de prueba	Etapa 1: Un puerto -Calibración del dispositivo - Configuración modo network -Configurar puerto de prueba

A continuación, se presenta una descripción mas profunda de las pruebas planteadas en la metodología.

- **Etapa 1. Prueba de recepción radio periféricos.** La prueba de recepción radio periféricos tiene como objetivo determinar la mínima potencia capaz de interpretar el dispositivo USRP. Esta prueba cuenta con un equipo generador de señales encargado de la emisión de una señal de un solo tono, con valores de potencia entre -120 dBm y 0 dBm, y con portadora constante en la banda de interés Fm. También es necesario el uso de un medio de transmisión cableado para reducir pérdidas, la recepción se realizará en el dispositivo USRP a estudiar. La visualización de los datos se hace en un equipo de computo con GNU radio y UHD instalados.

Figura 11: Prueba recepción del USRP.



Inicialmente se configura la señal de un solo tono con una potencia constante de -30dBm y se varia la frecuencia de portadora dentro de la banda de interés FM, el usuario registra los datos de recepción para verificar la linealidad de la recepción en el USRP con el fin de detectar pérdidas dentro de la banda de interés FM.

A continuación se determina una frecuencia de portadora constante dentro de la banda de interés, el amplificador Rx del USRP que se controla con el bloque USRP UHD Source tendrá una ganancia de 0 dB y la amplitud de la señal generada toma el menor valor que provee el generador de señales, el usuario verifica que la señal este por debajo del piso de ruido en la recepción, posterior a esto, aumenta la amplitud a pasos de 2 dBm hasta que la señal supere el piso de ruido y sea reconocible en el ordenador, este valor será tabulado como el menor valor capaz de interpretar el USRP, se seguirá registrando los valores de recepción hasta que la señal emitida tenga un valor en amplitud de 0 dBm.

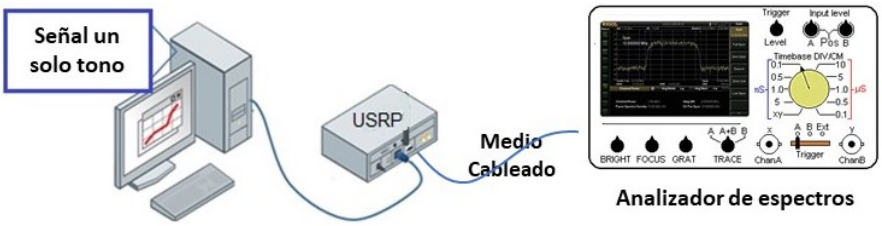
Por último, se aplica la máxima ganancia que pueda proporcionar el USRP UHD Source de acuerdo al dispositivo USRP, se realiza el barrido en amplitud desde el menor valor transmitido por el generador, de esta forma se encuentra el menor valor capaz de interpretar el USRP con la máxima ganancia en recepción y se busca el valor en que la recepción presenta problemas de saturación debido a dicha ganancia. Todos los procesos se realizan 10 veces y se tabulan para obtener mayor confianza en los resultados, se recomienda corroborar el valor de potencia transmitida por el generador de señales, esto se realiza haciendo la recepción en un equipo de alta gama como lo es un analizador de espectros.

- **Etapa 2. Prueba de transmisión radio periféricos** La potencia que transmite un USRP es del orden de los mili-watts, esta prueba tiene como objetivo determinar la máxima potencia que puede proporcionar este dispositivo, y de igual forma busca encontrar la relación entre la ganancia del amplificador Tx controlado por el bloque UHD USRP Sink y la potencia transmitida.

  Para desarrollar esta prueba se necesita un dispositivo USRP que sea el encargado de emitir una señal de un solo tono, con el fin de evitar problema relacionados a la conversión realizada por el DAC, se recomienda que la señal emitida tenga una amplitud de 0.8m y una frecuencia de 1 KHz, la frecuencia de portadora será cualquiera perteneciente a la banda de interés que se encuentre libre, el medio de transmisión empleado será cableado con el fin de reducir pérdidas.

  La recepción está a cargo de un dispositivo analizador de espectros, este equipo se debe someter al proceso de calibración antes de llevar a cabo la toma de datos, además se debe realizar una correcta configuración de la resolución de vídeo, span, frecuencia de portadora y referencia de piso de ruido para evitar mediciones erróneas .Por último se recomienda el uso de un atenuador en la emisión con el fin de proteger el equipo de recepción. El esquema de la prueba se observa en la figura 12.

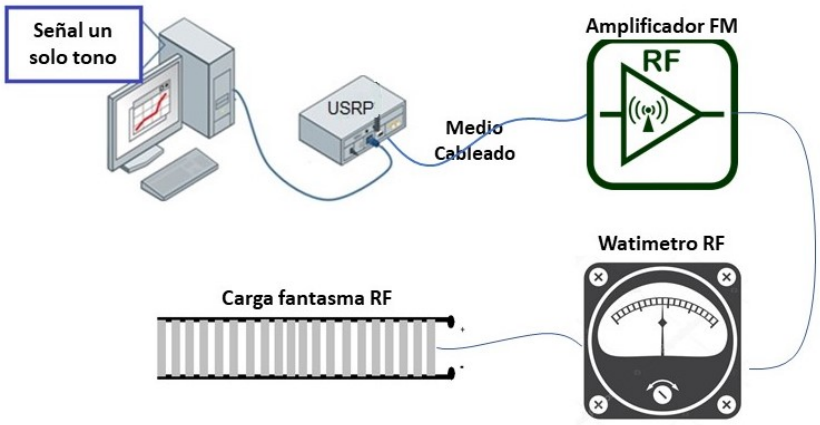
Figura 12: Prueba recepción del USRP.



Las variables que presenta esta prueba son la ganancia del bloque USRP UHD sink y la frecuencia de portadora, el usuario debe realizar un barrido en frecuencia portadora desde 88MHz a 108MHz con una ganancia constante de 20dB para visualizar la linealidad en la potencia de transmisión respecto a la frecuencia de portadora. Posterior a esto, se determina una frecuencia de portadora constante perteneciente a la banda de interés y que se encuentre libre, y se realiza un barrido en el valor de la ganancia del bloque partiendo desde -10dB hasta que la señal recibida presente saturación, es decir, que la potencia recibida no varíe. Las pruebas se realizan 10 veces y sus resultados son tabulados con el fin de obtener mayor confianza en las mediciones.

- **Prueba amplificador FM** El amplificador de ganancia FM define en gran parte las capacidad de cobertura del dispositivo S-jammer, el objetivo de esta prueba es determinar la máxima potencia amplificada que puede generar este dispositivo de acuerdo al voltaje de alimentación, además busca verificar el comportamiento que presenta en la banda de interés. La señal de entrada del amplificador será generada por un radio periférico, dicha señal es de un solo tono y frecuencia constante, la amplitud y frecuencia de portadora serán variables de control de la prueba, es importante no superar la máxima potencia de señal a la entrada del amplificador. La emisión se realiza a través de un medio cableado, la salida amplificada será medida en un watimetro RF, para evitar problemas de interferencia y daño de dispositivos debido a onda reflejada y potencia de la señal, el cierre se realiza con una carga fantasma que se encargará de consumir toda la energía, el esquema de la prueba se muestra en la figura 13.

Figura 13: Prueba amplificador de ganancia.

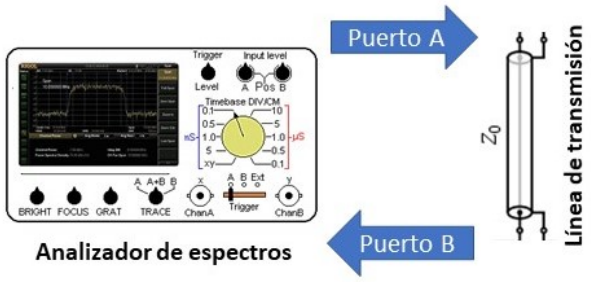


La prueba consta de dos etapas, la primera etapa cuenta con alimentación del amplificador constante y las variables de control serán la frecuencia de portadora de la señal emitida, que pertenecerá a la banda de interés FM y la ganancia del amplificador Tx del radio periférico controlada por el bloque UHD USRP Sink. El proceso de verificación de linealidad en la banda de interés se realiza igual que el presentado en el test de transmisión de los radio periféricos, emitiendo una señal de potencia constante y variando la frecuencia de portadora, posterior a esto se define frecuencia de portadora y se realiza un barrido en la ganancia del amplificador Tx, este proceso se realiza 10 veces y se tabula para obtener mayor confianza en los resultados.

La segunda etapa de la prueba, tiene dos variables de control que son el voltaje de alimentación del amplificador y la ganancia Tx, la frecuencia de portadora será constante. El usuario define el voltaje de alimentación y la frecuencia de portadora de la señal emitida, realiza un barrido en la ganancia Tx sin superar el límite de potencia en la entrada del amplificador, luego varia el voltaje de alimentación y repite el proceso. La prueba se realiza 10 veces y los resultados son tabulados y estudiados.

- **Prueba linea de transmisión** Los parámetros a obtener en esta prueba de la línea de transmisión son la impedancia característica y las pérdidas de línea, es necesario un dispositivo analizador de redes de dos puertos y se debe hacer la respectiva calibración de cada puerto. El esquema de la prueba se presenta en la figura 14.

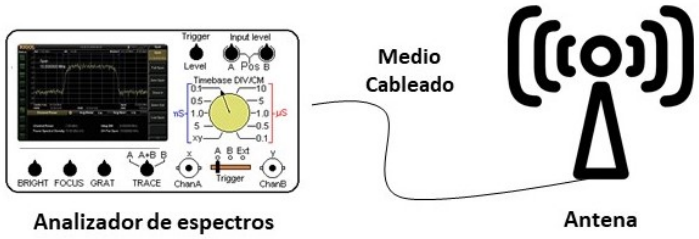
Figura 14: Prueba línea de transmisión.



El usuario hace uso de los parámetros S que constituyen las magnitudes de medida básicas de un analizador de redes, a partir de estos se obtiene el coeficiente de reflexión de entrada(s_{11}), el coeficiente de transmisión directa (S_{21}), el coeficiente de transmisión reflejada(s_{12}) y el coeficiente de reflexión de salida(S_{22}).Por último la respuesta en magnitud determina la variación en las perdidas de acuerdo la frecuencia de operación.

- **Prueba antena dipolo** El objetivo de esta prueba es encontrar el ancho de banda, la frecuencia de resonancia, coeficiente de reflexión y la impedancia característica de la antena, para lograr esto es necesario un analizador de redes capaz de obtener la respuesta en magnitud y fase de la antena, antes de realizar la prueba, el analizador debe pasar por un proceso de calibración del puerto a usar. Se sugiere omitir la línea de transmisión debido a que la mayoría de analizadores de redes comerciales no proveen una potencia de análisis alta y debido al grosor y la longitud de la línea, una potencia pequeña conlleva a generar resultados erróneos en la medición. El esquema de la prueba se presenta en la figura 15.

Figura 15: Prueba antena de transmisión del dispositivo S-Jammer.



La prueba se debe realizar en un espacio abierto, además la antena se debe posicionar a una altura próxima de 2 metros y moverla hasta encontrar una respuesta en frecuencia cercana a la esperada, en este caso la frecuencia de diseño de la antena para evitar distorsión en las medidas. Se recomienda que la antena se conecte al puerto de mayor potencia del dispositivo analizador de espectros, pues la antena es capaz de recibir grandes cantidades de potencia, y puede dañar el dispositivo de medición.

El usuario posiciona un marcador en el mínimo más significativo de la respuesta en magnitud, la frecuencia donde se ubica dicho punto determina la frecuencia de resonancia de la antena. De acuerdo a la configuración de potencia emitida del analizador hacia la antena, el usuario ubicará dos marcadores en la línea horizontal que representen el 30 % de la señal transmitida, esto con el fin de determinar el ancho de banda de la antena a partir del porcentaje de reflexión de la señal.

3.2. Metodología de caracterización software del S-Jammer

El sistema de monitoreo del espectro para la detección de emisiones clandestinas y el sistema de ataque de emisiones clandestinas que componen el terminal S-jammer, son piezas claves del mismo, pues son estos quienes definen básicamente la introducción de la tecnología SDR como un solución viable para el desarrollo de dichos bloqueadores. Las pruebas controladas tienen como objetivo verificar el correcto funcionamiento de monitoreo y el bloqueo, se realizan haciendo uso de radios periféricos que emulen un escenario real compuesto por un transmisor FM ilegal y el terminal S-jammer.En la tabla 7 presenta la metodología desarrollada para la verificación de funcionamiento de las componentes de software.

Tabla 7: Metodología de caracterización del software

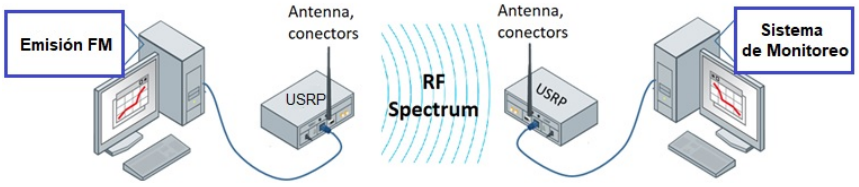
Metodología de caracterización de Software		
Sección	Sistema de monitoreo del espectro para la detección de emisiones clandestinas	Sistema de ataque de emisiones clandestinas
Objetivos	Verificar la correcta detección de emisiones legales. Verificar la detección de emisiones ilegales dentro de la banda de interés	Verificar el bloqueo de emisiones clandestinas.
Equipos	Radio periféricos Antenas Equipo de computo	Radio periféricos Antenas Equipo de computo Analizador de espectros
Parámetros de control	Frecuencia de muestreo Resolución de ventana Número de muestras a ponderar Frecuencia central Ganacia up	Frecuencia de muestreo Frecuencia de portadora Amplitud de la señal de bloqueo
Pruebas	Definir frecuencia de portadora emisión FM ïlegal". Definir frecuencia de muestreo en recepción Definir frecuencia central en recepción Etapa 1: Variación del número de muestras a ponderar. -Observar emisiones detectables en la muestra. -Variar el número de muestras a ponderar. -Observar el comportamiento del piso de ruido. Etapa 2:Variación de resolución PSD Variar la resolución del sistema de monitoreo -observar el número de emisiones que componen la máscara de comparación	Definir la frecuencia de la portadora de bloqueo Realizar una demodulación FM en la recepción Etapa 1: Bloqueo -Iniciar el ataque sobre la emisora FM -Variar la potencia del ataque -Observar el efecto sobre la emisión FM

- **Prueba sistema de monitoreo del espectro para detección de emisiones clandestinas** El sistema de monitoreo del espectro para la detección de emisiones clandestinas, es pieza importante del S-Jammer. La prueba de software debe verificar la correcta detección de señales ilegales en la banda FM y determinar la capacidad de detección de señales clandestinas, de acuerdo a las configuraciones del sistema que provee el usuario.

  Para lograr esto, se debe contar con un dispositivo USRP que permita posicionar una emisión FM en una frecuencia libre dentro de la banda de interés y a su vez que realice variaciones en la potencia de emisión, también es necesario otro equipo USRP que integre el sistema de monitoreo del S-Jammer para realizar la recepción y el respectivo proceso de detección de la emisión clandestina, además son necesarios dos equipos de computo con sistema operativo basado en linux y

con USRP hardware drive(UHD) instalado para la visualización de las señales a estudiar. La prueba se realiza a baja potencia, es decir usando el amplificador Tx del USRP y el medio para la trasmisión de señales es el aire como se observa en la figura 16.

Figura 16: Prueba del sistema de monitoreo de emisiones clandestinas.



La prueba consta de dos etapas, inicialmente la variable de control será la resolución de la ventana de muestra de la densidad espectral de potencia, la configuración de frecuencia central y frecuencia de muestro depende del radio periférico de recepción, el número de muestras a ponderar y ganancia up será propuesta por el usuario. El usuario verificará que las emisiones que componen la máscara de comparación se encuentren dentro del Plan Técnico Nacional de Radiodifusión Sonora colombiano , además debe observar que se detecte la señal ilegal controlada generada.

El número de muestras a ponderar será la variable de control de la segunda etapa, los parámetros de frecuencia central, frecuencia de muestreo, resolución de ventana y ganancia up serán configuraciones acorde a la emisión ilegal controlada generada, el usuario estudiará la implicación de la definición del número de muestras con el fin de mejorar la muestra a la que se le realiza el monitoreo a través de la estabilización del piso de ruido.

- **Prueba sistema de ataque de emisiones clandestina:** La prueba tiene como objetivo verificar la capacidad del sistema de ataque de realizar un bloqueo de una señal FM. Para llevar a cabo este laboratorio, se debe contar con un USRP que integre el sistema de ataque, y realizar la respectiva configuración de la señal de bloque en cuanto a parámetros como frecuencia de portadora, amplitud de la señal de bloqueo y la frecuencia de muestreo. Además es necesario otro dispositivo USRP encargado de la recepción y la demodulación FM, el usuario verifica a través del audio demodulado el comportamiento de una emisión legal perteneciente al

Plan Técnico Nacional de Radiodifusión Sonora la perdida de información debido al bloqueo. El medio de transmisión a usar es el aire.

3.3. Metodología del terminal S-JAMMER

La realización de pruebas del terminal S-jammer, representan un reto logístico debido a que la potencia que este dispositivo puede transmitir podría generar interferencia en canales diferentes a los que se desean bloquear. Por otro lado fenómenos físicos y naturales como la difracción de borde cuchilla, la refracción, irregularidad en los terrenos, entre otros podrían generar error en el proceso de medición y posterior análisis de resultados. Es por esto que el proceso de desarrollo de simulaciones que permitan visualizar la capacidades del terminal de bloqueo de manera fiable juegan un papel importante. Además permiten reproducir pruebas en distintas condiciones de relieve, posición y modelos de propagación, teniendo en cuenta aspectos como el clima y la humedad. En la tabla 8 se presenta la metodología desarrollada para la obtención de parámetros del desempeño del dispositivo.

Tabla 8: Metodología de simulación

Metodología de Simulación		
Sección	Cobertura	Enlace de Interferencia
Software	Radio Mobile	SEAMCAT
Objetivos	Determinar el área efectiva del dispositivo. Determinar la calidad del enlace. Comparar el efecto en el funcionamiento del dispositivo con una antena direccional y un omnidireccional. Determinar interferencias.	Determinar el valor de potencia del enlace victima. Determinar el valor de potencia del enlace de interferencia.
Parámetros de control	Potencia del transmisor Sensibilidad del transmisor Distancia Pérdidas de línea Pérdidas adicionales al cable Altura de la antena Tipo de antena	Potencia del transmisor Frecuencia de operación Posición del receptor Polarización de la antena tipo de antena Sensibilidad de recepción

- **Radio Mobile** Es un software de libre distribución para el cálculo de enlaces de radio de larga distancia en terreno irregular que implementa el modelo Longley-Rice de predicción troposférico, desarrollado por el Institute for Telecommunica-

tions Science para transmisiones de radio de largo-medio alcance. Este programa utiliza perfiles geográficos de la zona de trabajo combinados con la información de los equipos de radiofrecuencia (potencia, sensibilidad del receptor, características de las antenas, perdidas, tipo de enlace) que se desea simular, permitiendo que las simulaciones reflejen de forma fiel los equipos reales que se piensan usar en las pruebas para las cuales están destinados en los diferentes escenarios.

El objetivo de la presente sección es describir la configuración de las diferentes componentes del software para la simulación de áreas de coberturas y calidad de enlace, en este caso se usará para el dimensionamiento del S-Jammer. Dentro de los componentes se destacan los parámetros de entrada y salida, parámetros del ambiente, la configuración de la red y el tipo de propagación que se puede usar. La versión usada del software es la 11.6.5 (consultada el 11/09/17) descargada de la pagina oficial de Radio Mobile. El proceso de desarrollo de simulación se describirá a continuación.

Definición de la zona de análisis Se realiza definiendo la ubicación de los equipos a usar y los mapa de elevación de la zona de trabajo, mediante el ingreso de las coordenadas de latitud y longitud del centro de la región de interés. La georeferenciación se puede realizar manualmente rellenando las casillas de latitud y longitud, o a través de las 3 opciones siguientes: usando la posición del cursor, seleccionando el nombre de la ciudad o mediante mapa del mundo.

Parámetros de entrada Se define los parámetros de entrada de los sistemas de transmision y recepción (Definición Unidades como se refiere Radio Mobile a las terminales pertenecientes a una red), en la tabla 9 se presentan los 4 grupos de parámetros de entrada para la configuración del programa, así como los valores que pueden tomar y sus unidades.

Los parámetros del sistema son aquellos que están relacionados directamente al sistema de comunicaciones que se desea simular. Se debe aclarar que la frecuencia es la frecuencia de la portadora, la distancia es la longitud del recorrido entre el transmisor y el receptor, la altura de la antena es de cada terminal y se mide por encima del suelo. Los parámetros ambientales son aquellos que describen el escenario de simulación, en los cuales se destacan el parámetro de irregularidad

del terreno es decir el rango promedio de las elevaciones entre los cuales se da las opciones de plano, colina, montañas, terreno promedio entre otros. En cuanto a características atmosféricas y su variabilidad en el tiempo existen opciones de climas como ecuatorial, subtropical continental, templado continental, templado marítimo entre otros.

Tabla 9: Parámetros de entrada para Radio Mobile

Parámetros del sistema		
Especificaciones	**Valor**	**Unidad**
Potencia de Tx	10 a 1	nW a MW
Sensibilidad de Rx	0.01 a 2000	μV
Frecuencia	20 a 20000	MHz
Distancia	1 a 2 000	m
Perdidas de la linea	0 a 500	dB
Perdidas adicionales del cable	Depende de la altura de la antena	dB/m
Altura de la antena		
Tipo de antena	6 opciones	
Polarización de la antena	Vertical u horizontal	
Parámetros ambientales		
Refractividad de la superficie	250 a 400	unidades N
Conductividad del suelo	Dadas por el modelo Longley-Rice	S/m
Permitividad relativa al suelo	Dadas por el modelo Longley-Rice	
Climas	7 opciones	
Parámetros de implementación		
Criterio de ubicación	Aleatorio, cuidadoso	
Parámetros estadísticos		
Confiabilidad	0.1 a 99.9	%

Por último los parámetros estadísticos son aquellos que describen el tipo y variabilidad estadística que el usuario desea obtener, y es expresada en términos de la confiabilidad. El modo elegido esta sujeto a porcentajes de localizaciones, tiempo y escenarios entre los cuales se cuenta con: modo accidental se utiliza para evaluar interferencias. El modo difusión es para unidades estacionarias y Mobile para comunicaciones móviles y en el modo intento el programa hace única prueba para enviar un mensaje del transmisor al receptor en la simulación.

Asociación de unidades simuladas a la red Una vez ingresados los parámetros de entrada y la cantidad de unidades que se quieren simular, se debe configurar la red a la que va pertenecer cada una de las unidades, esta red la

puede definir el usuario dependiendo del servicio que se desea implementar en este caso la banda de 88 a 108 MHz, para lograrlo se seleccionan las casillas que pertenecerán a la red de la lista de unidades previamente ingresadas

Para cada unidad, se necesita determinar qué tipo de sistema es y cuál es su papel en la red, además especificar si la altura sobre el suelo de la unidad es distinta a la altura especificada por el sistema genérico. De igual modo se debe ajustar la red con la que se va a trabajar, se tiene que introducir el número de redes (enlace o cadena de enlaces), número de unidades y número de sistemas de las que se quiere disponer.

Orientación de antenas Esta sección esta encargada de manipular las antenas que usa cada miembro, teniendo la opción de direccionamiento hacia alguna unidad en especifico o mediante la opción fijo, manipular con mayor exactitud la antena en valores como azimut y elevación ingresando valores deseados y apreciar como afectan el patrón de radiación de la antena. Radio Mobile proporciona una sección donde el usuario puede subir a la aplicación fichero con la extensión .ant con los datos del patrón de radiación, la ganancia de la antena, azimut y elevación, con el propósito de crear patrones personalizados y específicos para las antenas que buscamos instalar en nuestros sistemas a simular.

Análisis de resultados Como resultados se analizará la calidad de los enlaces, la opción para este caso es ***enlace de radio***. En esta herramienta permite visualizar la condición de los enlaces midiendo el parámetro Rx relativo que permite conocer el margen de potencia, respecto a la sensibilidad del receptor representado mediante colores. El color verde representa que se esta recibiendo de forma optima la señal y el enlace es viable, el color rojo (de acuerdo al criterio de -3 [dB]) representa que no se recibe el mensaje puesto que la potencia no es suficiente. Estos resultados proporcionan una idea de la calidad del enlace que puede proporcionar el sistema a simular con los parámetros que se ingresaron en el respectivo zona de trabajo

Además ***enlace de radio*** proporciona un informe detallado con los resultados de relativos del enlace como: Azimuth y elevación con la que esta orientada la ante-

na transmisora Tx, pérdidas por espacio libre, distancia del enlace, el peor de los casos para el ángulo de Fresnel para el trayecto, y el parámetro más importante el Nivel Rx [dBm], el cual permite conocer el valor de la potencia recibida en el receptor Rx. De igual forma esta sección permite visualizar el perfil orografía de este enlace. Y debajo se describen los sistemas y topografía de cada una de las terminales que se configuraron anteriormente para la red.

Por otro lado se hace uso de la herramienta ***Cobertura de radio*** que permite dibujar el área de cobertura de la unidad radio mediante cuatro tipos de gráficas

- **Polar simple:** Esta solución calcula el área de cobertura de una única estación transmisora estática, realizando un barrido radial en torno a la misma de acuerdo a las coordenadas polares. El mapa representado muestra el contorno del área de cobertura, su superficie y usa los colores del arcoiris para resaltar los distintos niveles de señal recibida o emplear los valores fijados en la pestaña "Estilo" por si se quiere seguir alguna recomendación sobre niveles de potencia. Para la definición de los umbrales medidos puede emplearse la unidad-S (relativa a la sensibilidad del receptor) oμV, dBm y μV/m.
- **Cartesiano combinado:** este modo utiliza una o varias estaciones fijas para calcular el área de cobertura que ofrecen a un terminal especifica, en coordenadas cartesianas. La herramienta permite representar los niveles de señal y visualizar el solapamiento entre varias estaciones.
- **Zona de Fresnel:** colorea sobre el mapa de elevaciones las áreas que cumplen el intervalo despejado libre de obstaculos de la primera zona de Fresnel especificado. Realizando un estudios de LOS (Line of Sight) para comprobar la viabilidad de establecer un enlace entre dos estaciones.
- **Interferencias:** Se usa esta opción para analizar si algún punto de la estructura de la red se sospecha que puede producirse dificultades en la comunicaciones debido a problemas de interferencia, a partir de las especificaciones del mínimo nivel de señal requerido y margen de interferencia entre dos estaciones transmisoras, la herramienta representa las regiones con un nivel de interferencia aceptable y aquellas zonas que no mantienen una relación señal/ruido aceptable.

❖ **SEAMCAT®(Spectrum Engineering Advanced Monte-Carlo Analysis Tool)**

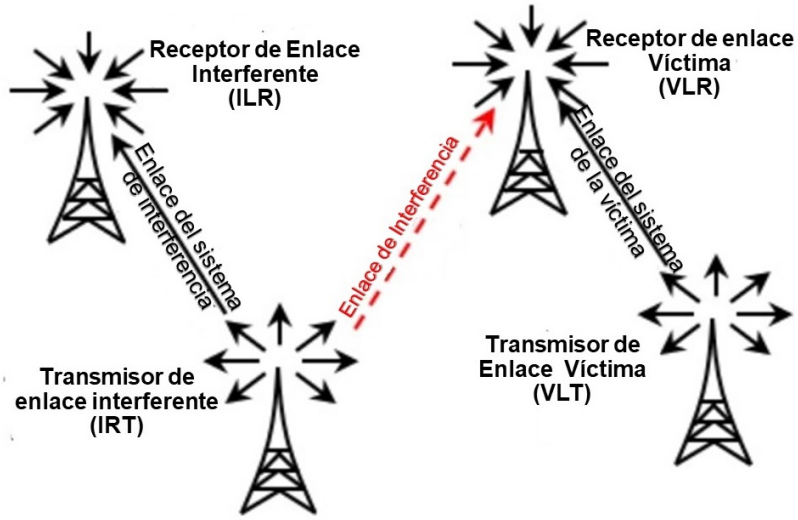
Es un software de libre distribución basado en un modelo de simulación estadístico de Monte Carlo que permite, el modelado de diferentes escenarios de interferencia de radio para realizar estudios de compartición y compatibilidad entre sistemas de radiocomunicaciones en las mismas bandas de frecuencias o adyacentes.

SEAMCAT cuenta con tres principales bloques computacionales para desarrollar la solución: Generación de eventos, Simulación CDMA (CDMAE) y Cálculo de interferencias (ICE). A continuación se presenta las herramientas utilizados y la secuencia a realizar para la simulación de un sistema genérico es decir para el terminal S-Jammer con el objetivo de poder identificar diferentes escenarios de interferencias que excedan el criterio de protección para la banda de radio difusión sonora.

- **Definir el escenario de simulación de programación:** Se debe crear un espacio de trabajo, el usuario debe primero proceder a revisar y modificar los parámetros del escenario para que el escenario de simulación resultante, refleje la configuración de los sistemas de radiocomunicaciones simulados. Un escenario típico consiste en:

  Un enlace de víctima que describe el sistema de comunicación que se interfiere, y al menos un enlace de interferencia que describe los sistemas de interferencia que pueden causar interferencia al enlace de la víctima como se observa en la figura 17.

Figura 17: Sistema genérico.



El flujo de trabajo típico de la programación del escenario sería el siguiente:

Enlace de la víctima:: En este apartado se define todos los parámetros técnicos de los enlaces modelados, ingresando las características principales del transmisor, receptor de enlace de víctima (VLR) y transmisor de enlace de víctima (VLT) (como la potencia del transmisor, la frecuencia de operación, distancia, altura de las antenas, tipo de propagación radio de cobertura entre otras) así como la ubicación física (mutua) del transceptores y la victima .

Enlaces de interferencia Esta pestaña tiene como objetivo actualizar los parámetros del enlace de interferencia en el escenario, crear nuevos enlaces de interferencia o eliminar los existentes. Cada enlace de Interferencia estará definido por dos elementos: un transmisor de enlace de interferencia (ILT) y un receptor de enlace de interferencia (ILR) . El enlace interferente recién creado se inicializa automáticamente con los parámetros predeterminados del primer transmisor y receptor

Configuración de control de simulación Las configuraciones de control de simulación se utilizan para determinar el tiempo de ejecución y depuración de generación de eventos de Seamcat. La configuración de control se puede acceder desde la pestaña Control de simulación. Las muestras generadas de la deseada y todas las señales interferentes se almacenan en matrices

de datos separadas de longitud N .

Resultados Generado la cantidad N de valores aleatorios definidos por el usuario que se decidió simular para los parámetros y eventos de interferencias diferentes se procesa para calcular:

- Fuerza de Señal Recibida deseada (dRSS) Es la intensidad de la señal deseada recibida en el Receptor de Enlace de Víctima (VLR) del Transmisor de Enlace de Víctima (VLT).
- Fuerza de Señal Recibida Interferente (iRSS): Es la intensidad de una señal del transmisor de enlace de interferencia (ILT) recibido en el VLR.

Para los sistemas genéricos, existen tres mecanismos de interferencia principales considerados por SEAMCAT, por lo que se generan tres vectores diferentes de iRSS para cada tipo de señal de interferencia respectiva:

Interferencia no deseada vector de señal iRSSunwanted - las emisiones no deseadas de TI que caen en la anchura de banda de recepción de VR.

Interferencia de bloqueo vector de señal de bloqueo iRSS es la potencia de emisión total de IT reducida por la función de atenuación de bloqueo (selectividad) de VR.

Interferencia de intermodulación vectores de señal iRSSintermod es la potencia de los productos de intermodulación, reducida por la función de atenuación de intermodulación de VR.

Una vez generadas las muestras de señales deseadas (dRSS) y no deseadas (iRSS) se continua con la evaluación de probabilidad de interferencia para el escenario simulado. La probabilidad de interferencia es calificada por el ICE con la siguiente elección de parámetros de entrada:
- Modo de cálculo: compatibilidad o traducción
- Qué tipo de señal de interferencia se considera para el cálculo: no deseado , bloqueo , intermodulación o su combinación

-Criterio de interferencia: C/I, C/(N+I), (N+I)/N ó I/N

- **Escenario genérico del S-Jammer** Se propone un escenario real de pruebas del dispositivo pero se debe tener en cuenta que para la realización de estas pruebas se debe contar con los permisos legales para realizar transmisiones de alta potencia, con el objetivo de realizar la verificación de lo que previamente se ha identificado pudiendo hacer una idea de los alcances y posibles limitaciones. Los pasos a seguir se muestran a continuación.

  Definición de la zona de análisis: Se realiza la definición del evento de medición los datos medidos deben ser referenciados con fecha, hora y posición geográfica los equipos a usar, el cual constituye la base de análisis cuantitativo sobre la variable de interés.

  Configuración del los parámetros de los equipos de medición: Los equipos usados para este análisis son una transmisor, un receptor y el terminal S-Jammer. Los parámetros a configurar se muestran a continuación:
  Para el transmisor se debe tener en cuenta, Frecuencia central de operación (Fc), el ancho de banda de canal (BW), la potencia de transmisión (Ptx), la ganancia de la antena transmisora (G) y la distancia al receptor (d), el direccionamiento de la antena. Para el receptor a usar se debe tener tener en cuenta que tendría la misma frecuencia de operación y ancho de banda del canal que el transmisor además se debe identificar parámetros como la sensibilidad y selectividad del mismo . Los parámetros a tener en cuenta para el S-Jammer siendo un jammer por cobertura por banda parcial serian: la frecuencia central de operación (fcjamm), el ancho de banda atacado (BWjamm), la potencia de transmision en la banda de operación (Pjamm), la distancia al receptor y la distancia hacia al transmisor (djamm)

  Elección del modelo de propagación Estos modelos de propagación requieren modelos informáticos del entorno para soportar el análisis de cada trayectoria de reflexión en el entorno de propagación. Debido a que la guerra electrónica es dinámica por naturaleza, es una práctica común [16] no utilizar estos análisis informáticos detallados, sino más bien utilizar tres aproxima-

ciones importantes para determinar la pérdida de propagación apropiada en aplicaciones prácticas. Estos tres modelos son:

Línea de visión: Denomina pérdidas de espacio libre, pérdida de propagación o pérdida de rango cuadrático. Se aplica en el espacio entre transmisores y receptores en cualquier otro entorno en el que no haya reflectores significativos y el suelo esté muy lejos en comparación con la longitud de onda de señal. Donde d es la distancia desde el transmisor al receptor y el área efectiva de la antena receptora isotrópica (es decir, ganancia unitaria). La perdida es un número mayor que uno, por lo que se puede dividir la potencia transmitida por la pérdida para obtener la potencia de recepción. Así, determinar la relación de pérdidas dividiendo la superficie de la esfera por el área de la antena receptora.

Dado que se considera que la comunicación se hace a través de un trayecto en espacio abierto sin obstáculos, las pérdidas de potencia (tanto para el transmisor como para el jammer) se calculan usando la ecuación de Friis 3.1 para propagación en espacio libre.

$$L = G_T G_R (\frac{\lambda}{4\pi d})^2 \tag{3.1}$$

Donde L es la ganancia (negativa, por lo tanto son pérdidas), GT y GR son las ganancias de las antenas de transmisión y recepción respectivamente, d es la distancia entre transmisor y receptor y λ es la longitud de onda de la señal. Esta ecuación es aplicable si d $\gg \lambda$ y el ancho de banda de la señal es lo suficientemente estrecho como para considerar que una única longitud de onda para toda la banda.

Dos rayos: Cuando las antenas de transmisión y recepción están cerca de una única superficie reflectora dominante (es decir, el suelo o el agua) y los patrones de antena son lo suficientemente anchos para permitir una iluminación significativa de esa superficie, se debe considerar el modelo de propagación de dos rayos. Como veremos, la frecuencia transmitida y las alturas reales de la antena determinan si se aplica el modelo de propagación de dos rayos o línea de vista. La propagación de dos rayos también se denomina

"40 log d"porque la pérdida varía con la cuarta potencia de la distancia de enlace. La pérdida dominante en la propagación de dos rayos es la cancelación de fase de la onda directa por la señal reflejada desde el suelo o el agua. La cantidad de atenuación depende de la distancia del enlace y la altura de las antenas transmisoras y receptoras por encima del suelo o del agua.

$$L = \frac{d^4}{h_T^2 h_R^2} \tag{3.2}$$

Dónde D = la distancia del enlace, hT = altura de la antena transmisora, hR = altura de la antena receptora

Medición de la Relación señal a jammer El mecanismo mediante el cual un interferente de comunicación interfiere con la comunicación mediante el envio de señales no deseadas en el receptor de destino junto con las señales deseadas que se están recibiendo. Las señales no deseadas debe ser lo suficientemente fuerte para que el receptor no pueda recuperar la información requerida de las señales deseadas. La relación entre la señal de interferencia (en el receptor) y la señal deseada (en el receptor) se denomina relación de interferencia a señal (J / S). El enlace entre el receptor y el jammer y el enlace entre el transmisor y el receptor deseado pueden emplear cualquiera de los modelos de propagación descritos anteriormente. No tienen que tener el mismo modelo de propagación. Por esta razón, las fórmulas de relación de interferencia a señal en esta sección incluyen términos generales para la pérdida. La fórmula para la comunicación J / S 3.3 es:

$$\frac{J}{S} = ERP_J - ERP_S - L_J + L_S + G_{RJ} - G_R \tag{3.3}$$

J / S es la relación de la potencia de interferencia a la potencia de señal deseada en la entrada al receptor que está atascada (en dB) ERPj es Potencia radiada efectiva del jammer (en dBm); ERPs es Potencia radiada efectiva del transmisor de señal deseado (en dBm); Lj es La pérdida de propagación del jammer al receptor (en dBi); Ls es La pérdida de propagación del transmisor de señales deseado al receptor (en dB); Grj es La ganancia de la antena receptora en la dirección del jammer (en dBi); Gr es Ganancia de la antena de recepción en la dirección del transmisor de señal deseado (en dBi)

Capítulo 4
PRUEBAS Y VALIDACIONES

4.1. Aplicación metodología de hardware

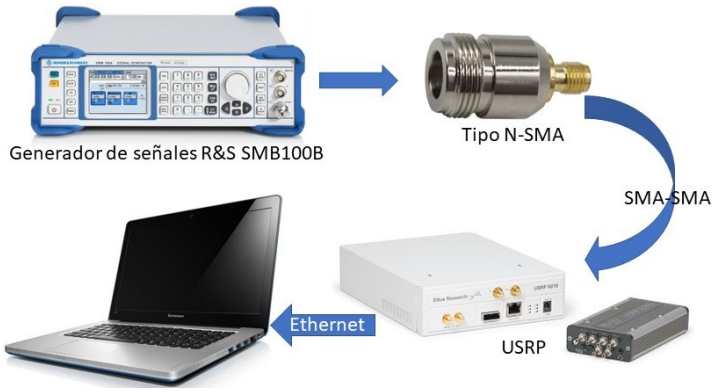
4.1.1 Radio periféricos Los dispositivos USRP 2920 y USRP e310, con los cuales cuenta el grupo de investigación RadioGis se someten a las pruebas de recepción y transmisión descritas en el capitulo anterior, con el fin de determinar cual se adapta mejor a las necesidades del prototipo S-Jammer desarrollado.

4.1.2 Recepción El equipo usado como transmisor en esta prueba es el generador de señales *Rohde&Schwarz SMB100A* que cuenta con frecuencias de trabajo desde los 9 KHz hasta los 6 GHz, para obtener la señal de un solo se hace uso del modo *RF ON-OFF*, las variables de control son las frecuencia de portadora configurada mediante el botón *FREQ* y la ganancia de transmisión en dBm configurada mediante el botón *LEVEL*, este generador puede reproducir señales desde -145 dBm hasta 30 dBm.

Para realizar la conexión con el USRP y el generador de señales SMB100A es necesario un conector tipo N macho-SMA y una cable SMA-SMA. La recepción se realizó en los dos dispositivos USRP de manera individual, la conexión entre el USRP y el equipo de computo Intel Core i5, 2.53 GHz 2.7 se realiza vía Ethernet. Los bloques usados en la aplicación GNU Radio para la recepción de señales son: *UHD USRP SOURCE*, que permite la comunicación entre el USRP y el equipo de computo, y el bloque *QT GUI Frequency Sink* que muestra la transformada rápida de Fourier de la señal recibida y a su vez nos permite hacer uso de diferentes funciones de ventanas permitiendo que el análisis se centre en la señal de longitud limitada. Para esta prueba se usó la ventana *Flat top* la frecuencia de muestreo para la recepción es de 32 Khz. El diagrama de

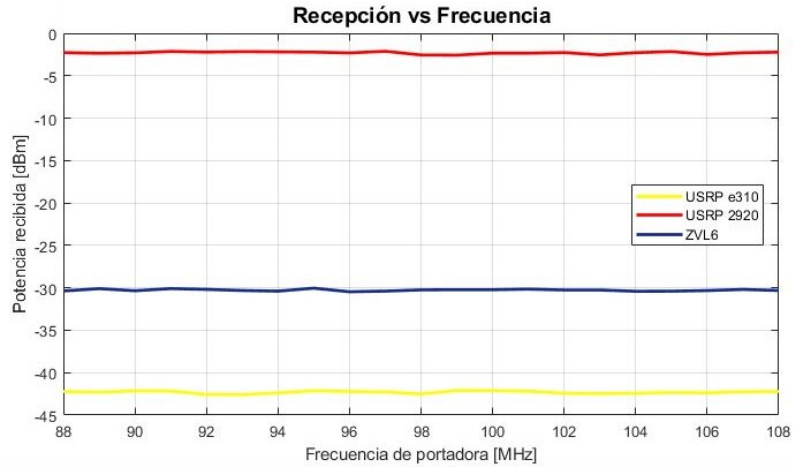
conexión y el montaje de los equipos para la realización de esta prueba se muestra en la figura 18.

Figura 18: Esquema de conexión prueba de recepción USRP



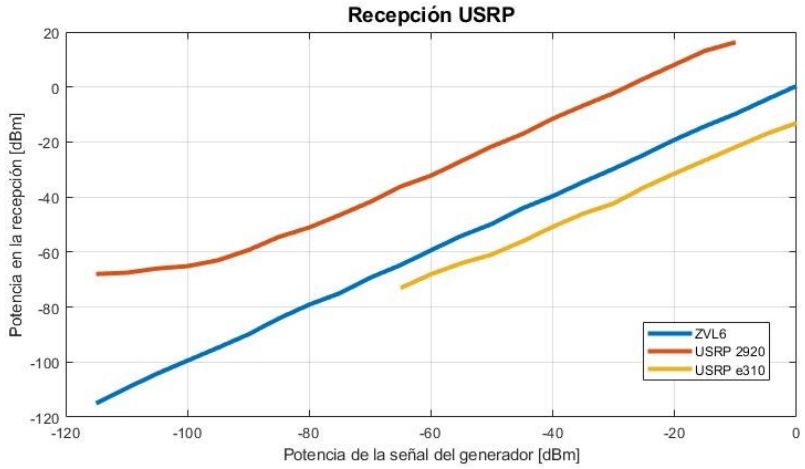
De acuerdo a la metodología propuesta en el capítulo anterior, la primera etapa de la prueba de recepción se llevó a cabo emitiendo una señal de amplitud constante de -30 dBm variando la frecuencia de portadora entre 88MHz y 108MHz con paso de 1MHz.Como referencia de comparación la recepción se realizó también en el dispositivo analizador de redes vectoriales R&S ZVL6, que es un dispositivo de alta gama en el análisis de espectros. Los resultados de la prueba evidencian que la potencia de recepción no varia significativamente con el cambio de frecuencia de portadora, demostrando la linealidad en recepción de los dispositivos USRP en la banda de interés, sin embargo los valores de potencia recibida presentados por los USRP 2920 y E310 fueron de -2,21dBm y -42,3dBm respectivamente, mientras que en el analizador R&S ZVL6 se observa el valor transmitido de -30,2dBm,como se observa en la figura 19, indicando errores en la lectura realizadas por los dispositivo USRP.

Figura 19: Potencia recibida por los USRP e310 y 2920 variando la frecuencia de portadora



La segunda etapa de la prueba se desarrolló con una frecuencia de portadora de 94MHz para la señal de un solo tono, la potencia trasmitida por el generador de señales varió desde -120dBm a 0dBm, en la figura 20 se observan los resultados obtenidos. Se aprecia que el error en recepción respecto a señal emitida presentado en la etapa inicial se mantiene, la diferencia entre la señal enviada tomando como referencia los valores obtenidos en el analizador R&S ZVL6 y la recibida en los USRP tiene un valor promedio de 30,8dBm y -10,6dBm para las referencias 2920 y e310 respectivamente, esta se presenta debido a la amplificación Rx de los USRP pues carecen de una rango dinámico para sub-muestrear señales de baja potencia. Además se observa que el USRP e310 interpreta señales con una potencia mayor a -75dBm a diferencia del USRP 2920, que gracias su amplificador Rx interpreta señales mayores a -115dBm.

Figura 20: Potencia recibida por los USRP e310 y 2920 variando la potencia transmitida



A pesar del error en el valor en la potencia de recepción del USRP 2920, este dispositivo presenta mejor recepción que el USRP e310 al ser capaz de interpretar emisiones con potencias mayores a -115dBm, aunque el valor se presente con un error de +30dBm, postula a este periférico como la mejor opción para realizar el monitoreo del espectro radio eléctrico en el dispositivo S-Jammer.

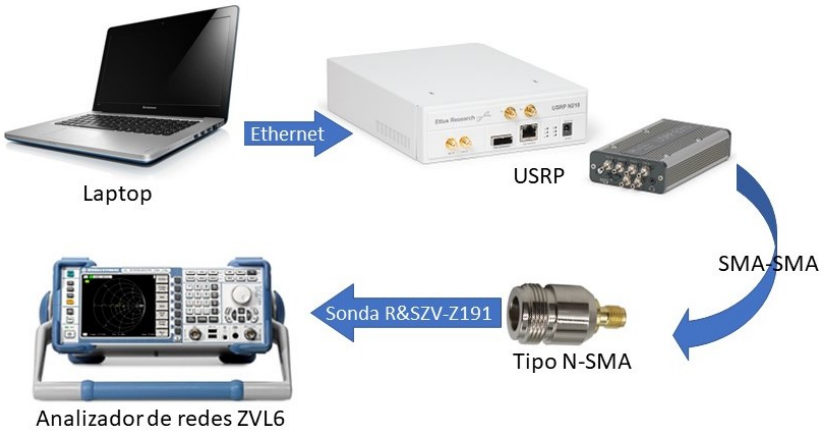
4.1.3 Transmisión Los dispositivos USRP 2920 y e310 serán los dispositivos encargados de realizar la transmisión de la señal de un solo tono en esta prueba, la señal enviada se configuró haciendo uso la aplicación GNU Radio instalada en el equipo de computo Intel Core i5, 2.53 GHz 2.7, esta señal es un coseno de un solo tono de frecuencia de operación de 1 kHz, amplitud de 0,8 , frecuencia de muestreo de 32 KHz.

El barrido de ganancia de emisión se realizó con una variable *slider* controlando el amplificador TX de los dispositivos USRP mediante la ganancia del bloque, el bloque UHD USRP *sink* que permite la comunicación entre los USRP y el software y con otro bloque *slider* se controló la frecuencia de portadora de emisión dentro de la banda de interés FM.

El medio de transmisión utilizado entre los dispositivos USRP hacia el equipo de recepción es un medio cableado, conformado por un cable SMA-SMA con un convertidor SMA-N hembra y la sonda R&SZV-Z191. El equipo de recepción es un analizador de redes vectoriales ZVL6 de la empresa Rohde & Schwarz, para el cual antes de efectuar

cualquier medición es necesario realizar una calibración mediante el kit de calibración ZV-Z121, este proceso elimina errores sistemáticos reproducibles en los resultados de las medidas.

Figura 21: Esquema de conexión prueba de transmisión USRP



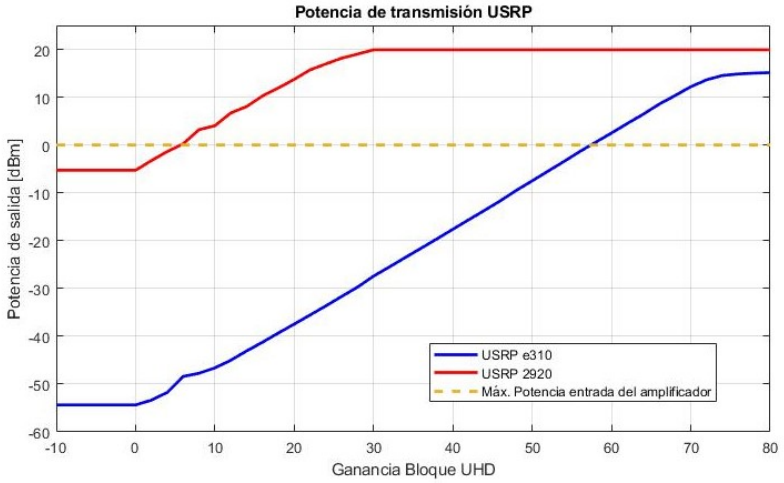
El analizador vectorial cuenta con una interfaz de calibración que se accede mediante la tecla MEAS ubicada en el extremo superior derecho del dispositivo, se debe seleccionar el intervalo de barrido de 9 KHz a 6 GHz, número de puntos 2000 y los valores de *SPAN*, frecuencia central son valores dependientes de la frecuencia inicial y final previamente asignados, los parámetros de medición a seleccionar son la medida de ancho de banda (fast sweep 100 kHz) y el tipo de dispositivo Passive DUT (-10 dBm), después de esto se debe conectar la sonda al terminal *OPEN* del kit de calibración, esto debe desplegar un gráfico en el analizador correspondiente a la carga en circuito abierto indicando que se ha realizado el barrido en frecuencia para la carga de referencia, conecte la sonda el puerto uno a la terminal *SHORT* del kit de calibración, esto debe desplegar un gráfico en el analizador correspondiente a la carga de corto circuito indicando que se ha realizado el barrido en frecuencia para la carga de referencia, enseguida se debe conectar la sonda a la terminal *MATCH* del kit de calibración esto debe desplegar un gráfico en el analizador correspondiente a la carga acoplada indicando que se ha realizado el barrido en frecuencia para esta carga de referencia.

La medición se llevó acabo en el analizador R&S ZVL6 en el modo analizador de espectro con SPAN de 20 MHz, referencia en 0 dBm, RBW en 100 KHz, VBW en 10 MHz y el retardo de medida la periodicidad de la medida cada 1s.

Para realizar esta prueba los dispositivos y su esquema de conexión se observan en la figura 21. Además el usuario mediante la aplicación GNU Radio configura la amplitud y la frecuencia de la señal transmitida , de igual forma la ganancia y la frecuencia de portadora usando los bloques SIGNAL SOURCE y UDH USRP Sink respectivamente.

La potencia transmitida por el radio periférico al amplificador juega un papel importante, pues debe ser capaz de excitarlo, por otro lado se debe evitar superar la máxima entrada del amplificador para evitar daños en el dispositivo. Los dispositivos USRP 2920 y e310, realizaron la emisión de la señal de un tono de amplitud 0.8m y frecuencia 1 kHz con una frecuencia de portadora de 94 MHz, la potencia recibida en el analizador de espectros en función de la variación de la ganancia del bloque de UHD USRP Sink que controla el amplificador Tx de los radio periféricos, se muestra en la figura 22.

Figura 22: Potencia transmitida por los USRP e310 y 2920

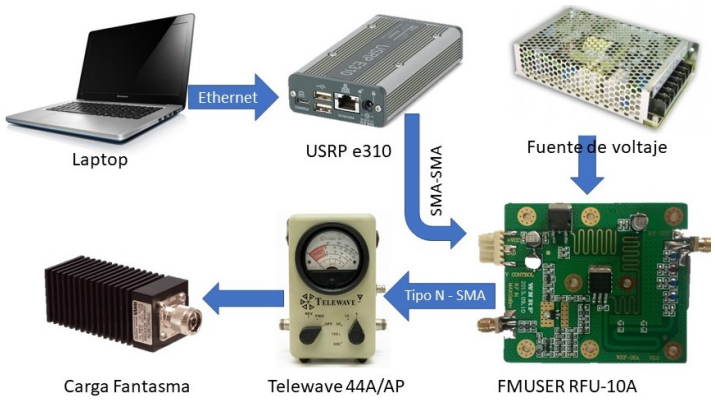


Los resultados obtenidos de la prueba muestran que la potencia máxima transmitida por los USRP 2920 y e310 es de 19,91 dBm y 15,03 dBm respectivamente, superando la máxima entrada que admite el amplificador FM de 0dBm, sin embargo la variación que presenta la potencia transmitida en función de la ganancia que controla el amplificador Tx de los radio periféricos, es menor en el USRP e310 pues para alcanzar los 0dBm debe superar un valor de 56dB mientras que en el USRP 2920 es de 5dB, la relación potencia transmitida por unidad de ganancia del bloque UDH es de aproximadamente 1,14dBm para el 2920 y 0,97dBm para el e310, luego la principal diferencia se encuentra en la potencia mínima transmitida que se presenta cuando el bloque de transmisión UHD

tiene una ganancia de 0dB, que es de -5,28dBm en la referencia 2920 y de -54,36 dBm en el e310, es por esto que se postula el USRP e310 como la mejor opción para montar el sistema de ataque de emisiones clandestinas del dispositivo S-Jammer.

4.1.4 Amplificador de ganancia Para realizar el estudio del amplificador, se desarrollaron pruebas haciendo uso del USRP e310 como transmisor debido a que presenta una mayor variación en la potencia de salida con el cambio de ganancia Tx controlada por el bloque UHD USRP Sink por debajo de la potencia máxima de entrada del amplificador RF a diferencia del USRP 2920, como se observa en la figura 21. Para realizar la conexión entre el USRP e310 y el amplificador de ganancia FMUSER FMU-10A se hizo uso de un cable SMA-SMA. De igual manera para esta prueba se hizo uso de un watimetro RF modelo TELEWAVE 44A-AP debido a la alta potencia que maneja el prototipo S-JAMMER, este watimetro cuenta con una no tan buena sensibilidad puesto que puede interpretar señales mayores a 0.125 W pero tiene la ventaja de medir la relación de onda estacionaria permitiendo realizar comparaciones entre las diferentes mediciones. Por ultimo hace uso de una carga fantasma de 100W, encargada de sustituir la antena de emisión con el fin de evitar que el transmisor cause interferencia en otros equipos. En la figura 23 se muestra el diagrama de conexión y el montaje de los equipos para la realización de esta prueba.

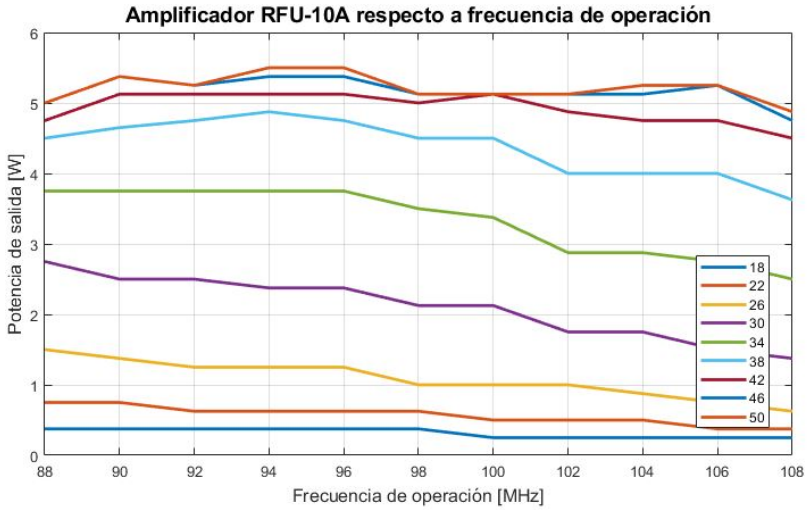
Figura 23: Esquema de conexión prueba del Amplificador RF



Esta prueba consiste en enviar desde la aplicación GNU Radio instalada en un equipo de computo portátil Intel core i5 a 2.53GHz con RAM de 6GB una señal coseno de un solo tono de frecuencia 1 kHz y amplitud de 0.8m, mediante USRP hardware driver (UHD), las variables de control serán la frecuencia de operación del bloque UHD Sink y la ganancia RF del mismo y la ganancia de la señal portadora.

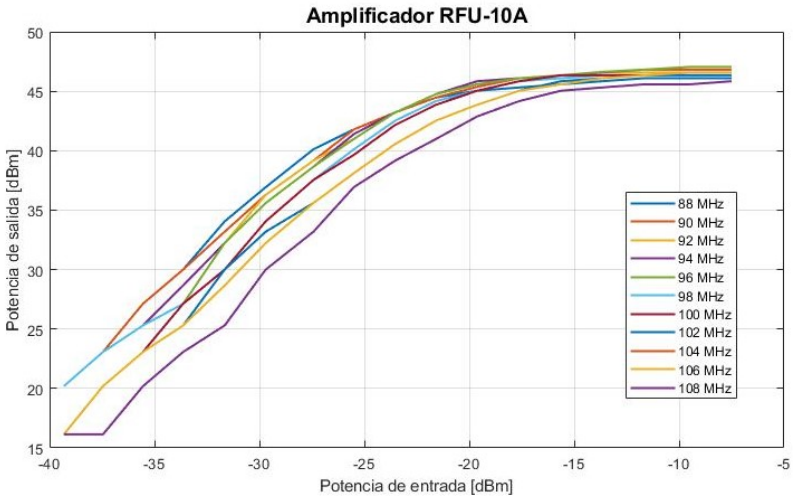
❖ **Amplificación con voltaje de alimentación constante**. Con la señal de prueba definida, la primera etapa de esta prueba se ejecuta con una alimentación de 14 V, variando la frecuencia de portadora en la banda de interés FM, además se aplican valores de ganancia de bloque UHD USRP Sink constante, con el fin de verificar la linealidad de la amplificación, la figura se 24 presentan los resultados obtenidos, donde se observa que cuando la ganancia del bloque acerca a la potencia en la entrada al máximo valor de potencia permitido (0dBm), el valor de la potencia de transmisión se satura.

Figura 24: Amplificador RFU-10A en función de la frecuencia de operación



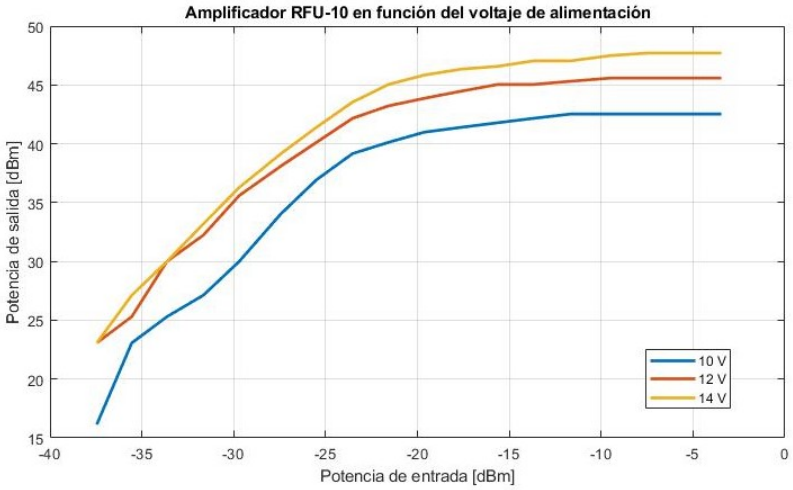
Además también se observa que para ganancias de bloque USRP UHD Sink menores a 38dB, la potencia amplificada disminuye en las frecuencias altas de la banda FM afectado la linealidad de la amplificación, esto debido al efecto del filtro paso bajo del dispositivo. Por otro lado, en la figura 25, se observa que el amplificador con una valor de potencia de entrada de -7,5dBm, genera una potencia máxima de 5,5W en la frecuencia de portadora de 96MHz, la potencia mínima amplificada tiene un valor de 4,875W en la frecuencia de 108MHz.

Figura 25: Amplificador RFU-10A en función de la potencia de entrada



- **Amplificación variando el voltaje de alimentación.** Esta etapa se realizó con una portadora constante de 94MHz, y las variables de control fueron la potencia de entrada en el amplificador variando desde -37dBm a -3,45dBm, y el voltaje de alimentación variando desde 10v a 14v, los resultados de esta prueba se presentan en la figura 26, donde se observa que amplificador tiene el mismo comportamiento respecto a la potencia de entrada, sin embargo la potencia máxima capaz de transmitir en la portadora aumenta aproximadamente en 0,5425W por voltio de alimentación.

Figura 26: Amplificador RFU-10A en función de la fuente de alimentación

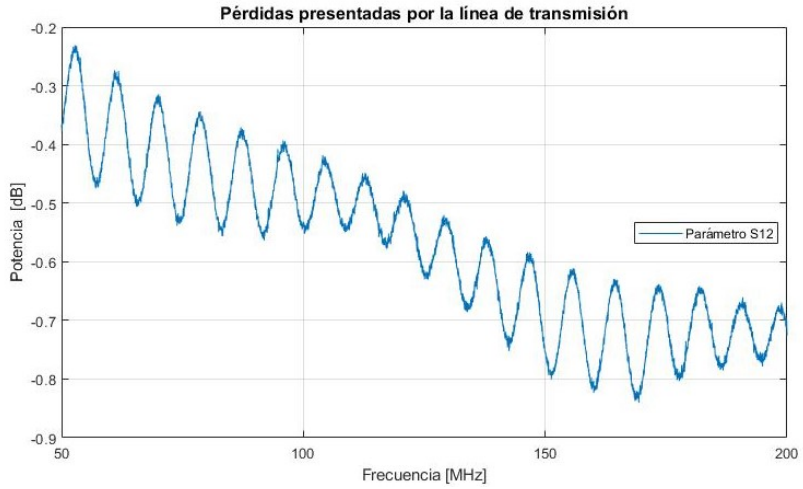


4.1.5 Línea de transmisión Esta prueba se llevó acabo mediante el analizador de redes vectoriales ZVL-6 configurado en modo analizador de redes, para realizar las medidas fue necesario el uso de dos sondas R&SZV-Z191 con su respectiva calibración en ambos puertos, se conectó la línea de transmisión completamente extendida para evitar inducciones (Figura 27).

Figura 27: Esquema de conexión prueba línea de transmisión

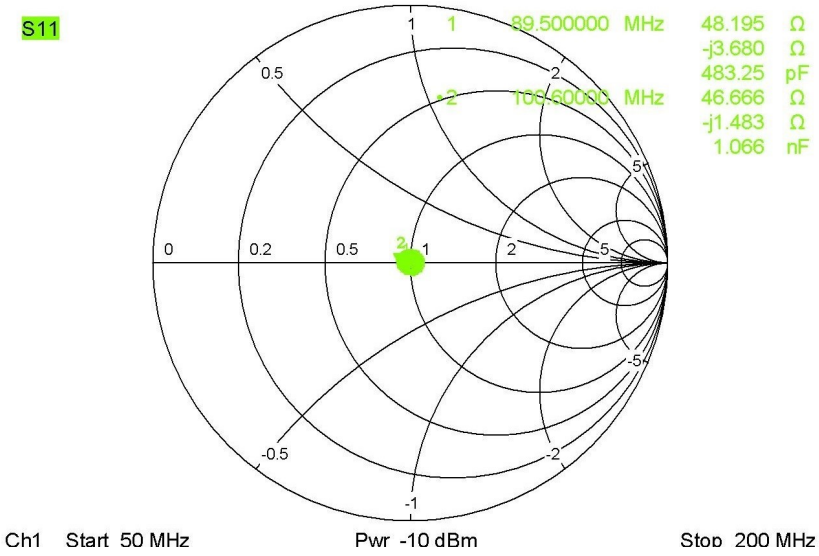
Para este análisis la línea se tomó como una red de dos puertos con el motivo de observar ondas incidentes y reflejadas de tensión y corriente, el analizador puede representar dicha magnitud en forma de diagrama polar, carta de Smith o en un gráfico de bode (magnitud y fase). Se puede visualizar en forma logarítmica o lineal y otras presentaciones de utilidad como son la parte real o imaginaria. Los markers permiten medir en un punto concreto de frecuencia, la impedancia, efectos de las perdidas, el valor inductivo o capacitivo del componente entre otros. La figura 28 muestra la respuesta en magnitud del coeficiente de transmisión reflejada S_{12}, donde se observan que las pérdidas presentadas por la línea en la banda de interés Fm, varían entre -0,392dB y -0,533dB.

Figura 28: Pérdidas presentadas por la línea de transmisión.



La representación de la carta de Smith del coeficiente de reflexión de entrada S_{11} (figura 29), muestra el comportamiento resistivo de la línea, al presentar valores de reactancia pequeños causando máxima transferencia de energía y definiendo la impedancia característica alrededor de los 47Ω, acorde a la presentada en las especificaciones técnicas del cable Heliax de cual se compone la línea.

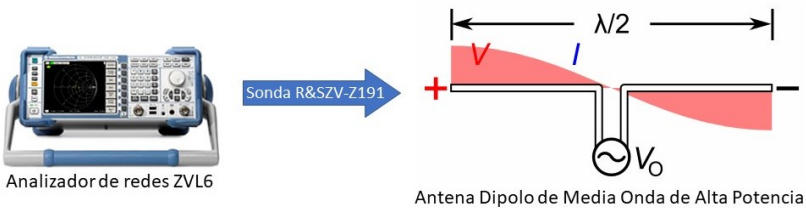
Figura 29: Impedancia característica vista desde el puerto S_{11}.



4.1.6 Antena dipolo de media onda En esta prueba se hizo uso del analizador de redes vectoriales ZVL-6 de Rohder& Schwarz en modo analizador de redes, se

hace uso del puerto 2, con el fin de proteger el equipo pues debe soportar potencias altas incidentes en la antena. La conexión entre antena y analizador usó un conector TIPO N a macho PL 259 y una sonda R&SZV-Z191, antes de realizar cualquier medición se llevo acabo el proceso de calibración del equipo mediante el kit ZV-Z135 previamente descrito. El esquema de conexión utilizado se presenta en la figura 30.

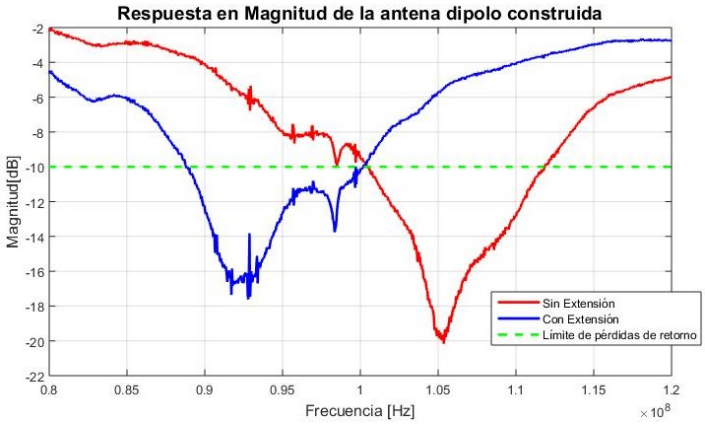
Figura 30: Esquema de conexión prueba de la Antena dipolo



Se configuró el analizador de redes con un SPAN de 150 MHz, referencia de 0dBm y retardo de medida en la periodicidad de la medida cada 1s. Las frecuencia de resonancia esperada para la antena sin extensión es de 106,5MHz y con extensión es de 93,5MHz.

- **Respuesta en frecuencia** El ancho de banda de una antena se refiere al rango de frecuencia en la cual puede operar de forma satisfactoria. Se obtiene de la respuesta en en frecuencia de la antena, donde el ancho se determina con los valores de frecuencia para los cuales la antena tiene pérdidas de retorno menor a los -10 dB que desde la escala lineal representa el 30 % de la señal con la cual se alimenta desde el puerto de prueba. La figura 31, presenta los resultados del comportamiento de la antena diseñada y el límite de pérdidas por retorno base de la comparación.

Figura 31: Potencia reflejada de la antena

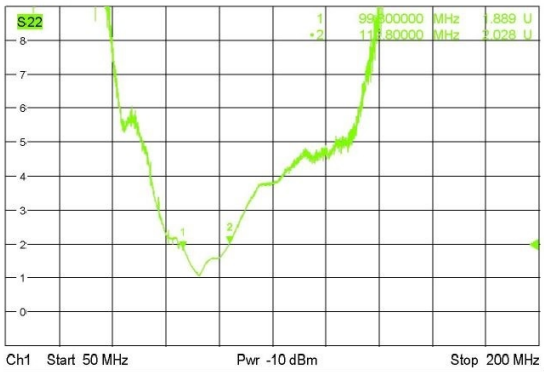


La antena diseñada presenta un ancho de banda de 11MHz con frecuencias de operación desde los 100,5MHz a 111,6MHz, y su frecuencia de resonancia es de 105.4MHz, la cual se obtiene en el punto más bajo de la respuesta en magnitud, pues es este donde la reactancia disminuye causando máxima transferencia de energía. El comportamiento de antena con los conectores de extensión modifican la frecuencia de resonancia de la antena a 92,15MHz y mantiene el ancho de banda de la antena en 11MHz, donde las frecuencias de operación se encuentran entre 88,8MHz a 100,2MHz.

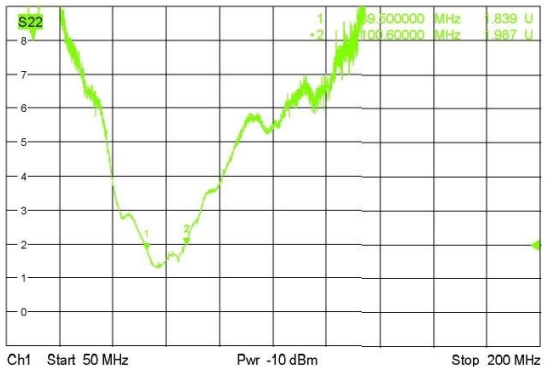
- **relación de onda estacionaria ROE** El analizador de redes vectoriales ZVL6 nos permite medir parámetros de dispersión. Estos parámetros describen completamente el comportamiento de un dispositivo bajo condiciones lineales en determinado rango de frecuencia, en este caso la banda FM de 88MHz a 108MHz. La relación de onda estacionaria que provee la antena diseñada se presentan en la figura 32.

Figura 32: Relación de ondas estacionaria

(a) ROE sin extensión.



(b) ROE con extensión.



La relación de onda estacionaria resultante de la prueba demuestra que el ancho de banda y las frecuencias de operación obtenidas, son las correctas pues el ROE en dichas frecuencias debe ser menor a 2U, que es el valor aceptable para considerar que la antena tiene buen nivel de adaptación puesto que equivale a que un 90 % de la potencia transmitida está siendo irradiada por la antena.

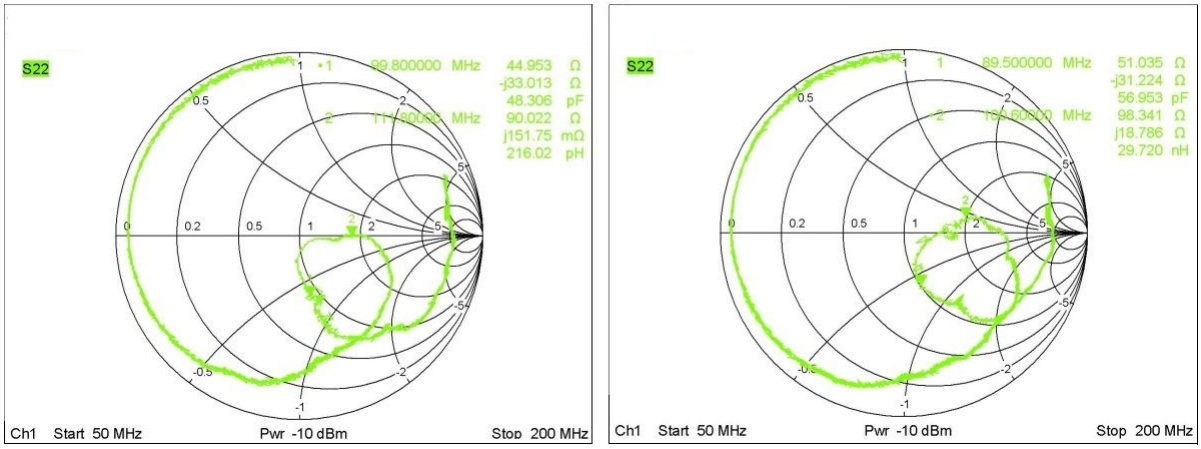
- **Impedancia característica** Para una transferencia de energía eficiente, la impedancia del radio, la antena, y la linea de transmisión que las conecta debe ser

la misma. Las antenas y sus líneas de transmisión generalmente están diseñadas para una impedancia de 50 Ω.

El diagrama de Smith, es un diagrama circular que permite trazar el mapa de los coeficientes de reflexión complejos como valores de impedancia normalizados. En este diagrama las cuadriculas corresponden a puntos de reactancia y resistencia constante. Los diagramas resultantes de esta prueba se muestran en la figura 33, donde se encontró que para las frecuencias 88,8MHz a 100,2 MHz la impedancia característica es igual 51.035 Ω y para la frecuencia 100,5 a 111,6 MHz es igual a 44,953 Ω.

Figura 33: Representación en la carta de Smith de la antena diseñada.

(a) Sin extensión. (b) Con extensión.



4.2. Aplicación metodología de software

4.2.1 Sistema de monitoreo del espectro radio eléctrico

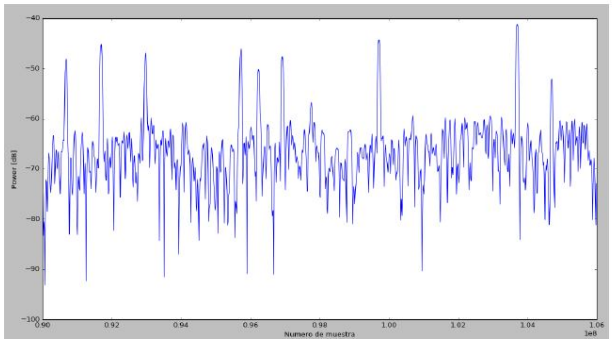
La prueba se realiza según los lineamientos presentados en la sección anterior, se hace uso de dos USRP e310, uno encargado de realizar una emisión FM en la frecuencia de 94MHz, el otro se realiza el monitoreo del espectro con frecuencia de muestreo de 16MHz y frecuencia central de 98MHz, esto le permite aplicar el monitoreo desde los 90MHz a 106MHz.

- **Variación del número de muestras a ponderar** Esta prueba se realizó con

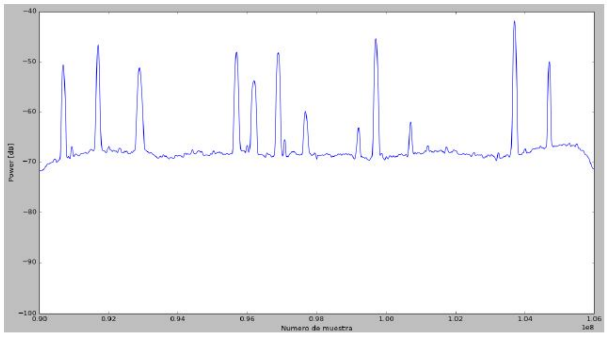
una resolución de ventana de 1024, el aumento del número de muestras a ponderar disminuye las variaciones en el piso de ruido permitiendo la visualización de señales de baja potencia dentro del espectro analizado, además la cantidad de muestras influye directamente en el tiempo de procesamiento que le toma al algoritmo realizar la detección. Los efectos de la ponderación se aprecian en la figura 34, donde se observa claramente que al realizar la ponderación del espectro se puede determinar un valor de piso de ruido de referencia, además se observan claramente los picos de señales que serán sometidos a verificación de legalidad.

Figura 34: Comparación entre una muestra del espectro sin ponderar y una ponderada

(a) Sin ponderar



(b) Ponderado

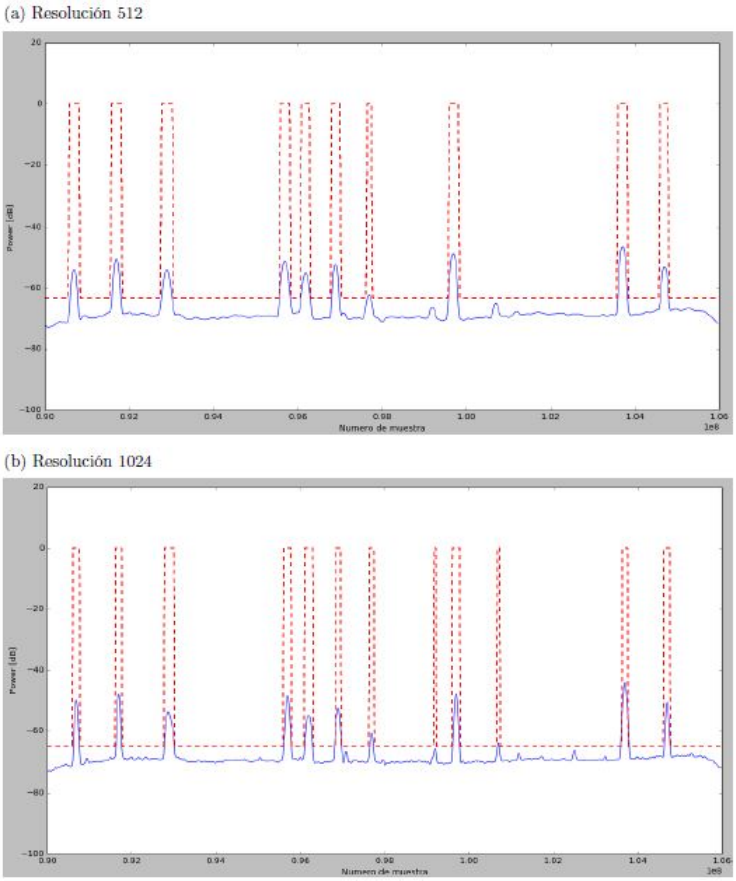


❖ **Variación de la resolución de la ventana de prueba** La resolución de ventana determina el valor en frecuencia que representa cada muestra de la densidad espectral de potencia con la que interactúa el monitoreo, se determinó comparar una resolución de 512 y 1024, esto significa que por cada muestra de representación se tiene 31250Hz y 15635Hz respectivamente. El número de muestras a ponderar se define en 500 y ganancia up tiene un valor de 3dB para el ajuste de la decisión de la máscara de emisiones.

Los resultados del sistema de monitoreo obtenidos se presentan en la figura 35 donde se aprecia que con un número de muestras a ponderar constante de 500, la resolución de la ventana de la densidad espectral de potencia influye directamente en la cantidad de señales que puede detectar el monitoreo, pues al aumentar la resolución el número de hercios por unidad disminuye, luego una emisión FM con ancho de banda de 200 KHz pasaría de representarse por 6 unidades a 13 en una resolución de 512 y 1024 respectivamente, aumentando la cantidad de información

procesable para identificar una emisión en comparación del valor del piso de ruido. Sin embargo el proceso de detección de la señal FM ilegal controlada ubicada en la frecuencia de 94MHz se cumplió.

Figura 35: Variación de la resolución de la PSD a procesar



4.3. Aplicación metodología del terminal S-Jammer

- **Simulación de cobertura y calidad de enlace:** Se definieron tres zonas de análisis en el área metropolitana donde estarán ubicadas los tres transmisores S-Jammer con las mismas características y una posición para el receptor de referencia IC-R8500, con el objetivo de visualizar el comportamiento de los tres transmisores en terrenos diferentes de trabajo haciendo uso del modelo Longley-Rice en cuanto a calidad de los enlaces, interferencia, solapamiento y área efectiva. Las coordenadas geográficas de las tres ubicaciones del transmisor S-Jammer y receptor son las siguientes:

Tabla 10: Coordenadas geográficas del transmisor y receptor

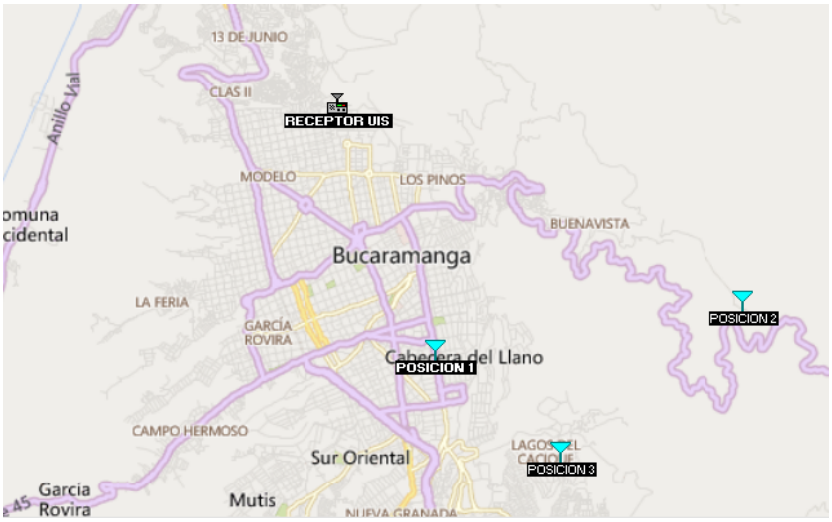
Transmisor S-JAMMER		
	Latitud	**Longitud**
Posición 1	7,115318	-73,11068
Posición 2	7,120715	-73,07698
Posición 3	7,104284	-73,09692
Receptor IC-R8500		
	Latitud	**Longitud**
Posición 1	7,142331	-73,12157

Posteriormente se asignó el nombre a la red para este caso Radiodifusión FM y se definió la frecuencia de trabajo mínima y la frecuencia de trabajo máxima que pertenecen a la banda FM de 88 MHz – 108 MHz, los dispositivo configurados fueron 4, la tabla x muestra las especificaciones técnicas del transmisor y receptor que requiere el simulador asignado.

	TRANSMISOR	**RECEPTOR**
Potencia TX	7	1
Sensibilidad	1 μV	0.4 μV/320 mV
Tipo de antena	Dipolo de media onda	Omnidireccional
Ganancia de antena	0 dBi	0 dBi
Altura de la antena	5 m	2 m
Polarización	Vertical	Horizontal

Debido a que Bucaramanga se encuentra en una zona tropical se marcó la opción del clima como continental templado esto afectara las condiciones de propagación, la refractividad de la superficie de 301 Unidades-N valor promedio para las condiciones atmosféricas promedio en un clima templado continental, conductividad del suelo 0.005 [S/m], permitividad relativa de 15. De igual forma se definió el tipo de topología para la red para este caso es una red de voz. Se definió el número de terminales pertenecientes a la red Radiodifusión FM, así como sus sistemas y su papel dentro de esta según la topología. En la figura 36 se muestra la posición de las tres unidades transmisoras y el receptor pertenecen a esta red. En cada unidad seleccionada se determino su rol, que es el comportamiento o función de la terminal dentro de la topología de la red.

Figura 36: Transmisores S-Jammer y receptor



Posteriormente se añadieron los patrones de radiación de antena proporcionados por el Radio Mobile de una para una antena dipolo de media onda usado por el transmisor S-Jammer. Para el análisis de la red se hace uso de la opción *enlace de radio* pudiendo obtener para cada ubicación el perfil terrestre del enlace directo, parámetros como la distancia entre los emisores, pérdidas, ángulo de elevación, azimut y a su vez el parámetro que más interesa el nivel de señal relativo que es la unidad que indica si la señal que llega al receptor es de suficiente potencia para dar cobertura, es decir para el caso de el S-jammer para bloquear la estación receptora llamada *RECEPTOR UIS*. Los resultados se muestran en la tabla 11.

Tabla 11: Detalles de las simulacion brindadas por Enlace de Radio

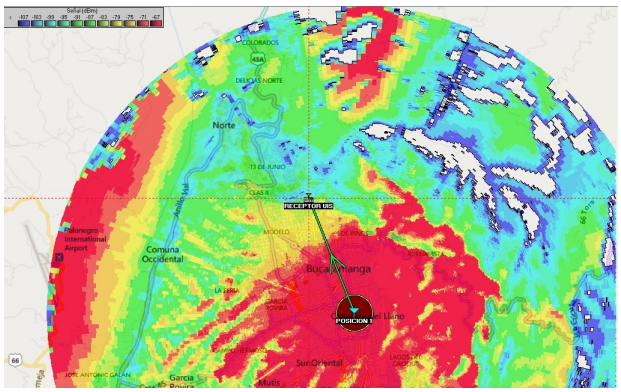
	Posición 1	**Posición 2**	**Posición 3**
Campo E Requerido	11,3 dBμ/m	11,3 dBμ/m	11,3 dBμ/m
Espacio Libre	82,4 dB	87,1 dB	86,2 dB
Peor zona de Fresnel	0,7F1	0,6F1	0,9F1
Distancia	3,23 Km	5,47 Km	5,03 Km
Nivel Rx	26,6 dB	51 dB	22,6 dB
Rx relativo			
Potencia Radiada	PIRE= 3,91W PRE=2,38 W	PIRE= 6,19W PRE=3,78 W	PIRE= 3,91W PRE=2,38 W
Campo E	37,9 dBμ/m	62,3 dBμ/m	33,8 dBμ/m

En la tabla 11 podemos observar que la intensidad de campo requerido para lograr la cobertura al receptor es de 11,3 dBμ/m siendo la posición 2 de 62,3 dBμ/m con

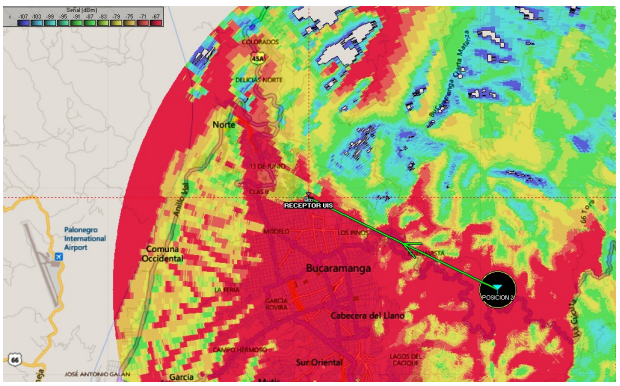
la mejor transmisión debido a que tiene la mejor linea de vista hacia el receptor con un rango de Rx relativo de 51 dB aun siendo la posición con más distancia entre el transmisor y el receptor. En cuanto a los análisis de cobertura mediante el modo polar simple se realizaron las simulaciones para los tres diferentes escenarios, en la figura 37 podemos observar las diferentes intensidades de campo producidas por el transmisor S-Jammer en cuento al umbral de recepción que presenta la referencia IC-R8500, presentando el nivel de señal recibida en dBm impuesto por el transmisor en todos los puntos del área de cobertura, generando una mancha con distintos colores que representan los diferentes rangos de recepción de la señal, el rango va desde -107 dBm hasta -67 dBm.

Figura 37: Coberturas de los transmisores S-JAMMER en los diferentes escenarios

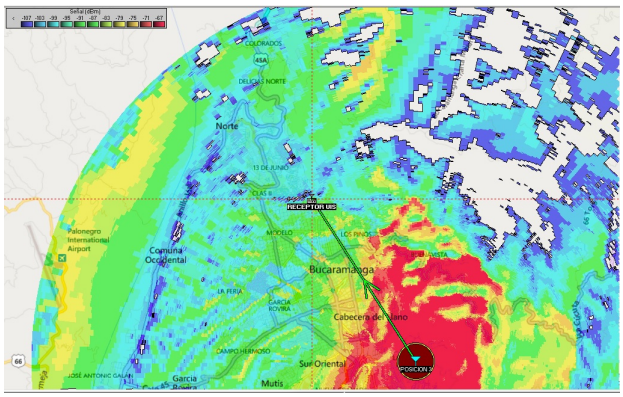
(a) Posicion 1



(b) Posicion 2



(c) Posicion 3

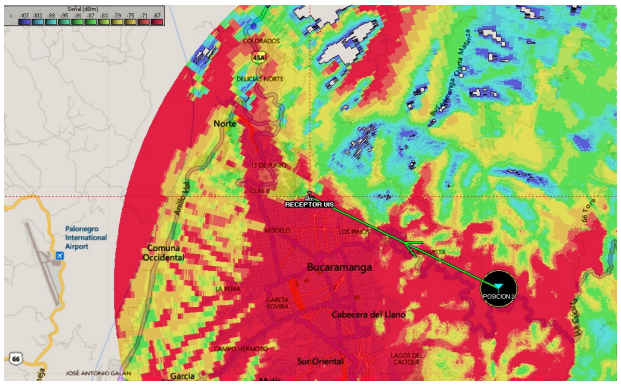


De la figura 37 se concluye que para el caso del receptor IC-R8500 con selectividad de 2kHz/-6 dB y sensibilidad de 0.4 μV/320mV para la banda FM en los

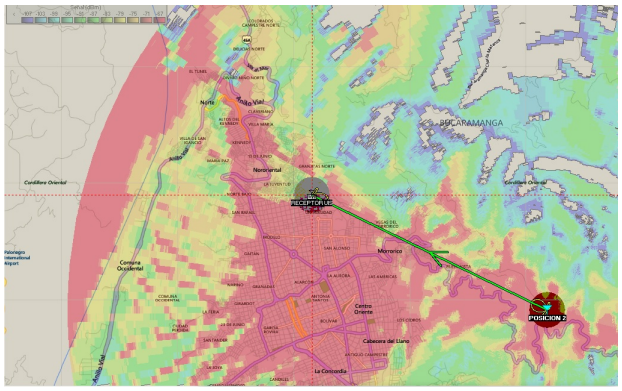
tres escenarios existe una buena calidad del enlace, por lo tanto se bloquearía al receptor con un porcentaje superior al 40 % dando la opción de ser afectada por cada transmisor independiente de su ubicación, con la menor probabilidad de bloqueo el transmisor en la posición 3 debido a la obstrucción de una montaña a 1,27 km y debido a las perdidas . Además se realizó un análisis del comportamiento del transmisor S-Jammer el uso de diferentes dipolos de antena, como lo son una antena yagui direccional.

Figura 38: Comparación entre una antena direccional y omnidireccional

(a) Omnidireccional

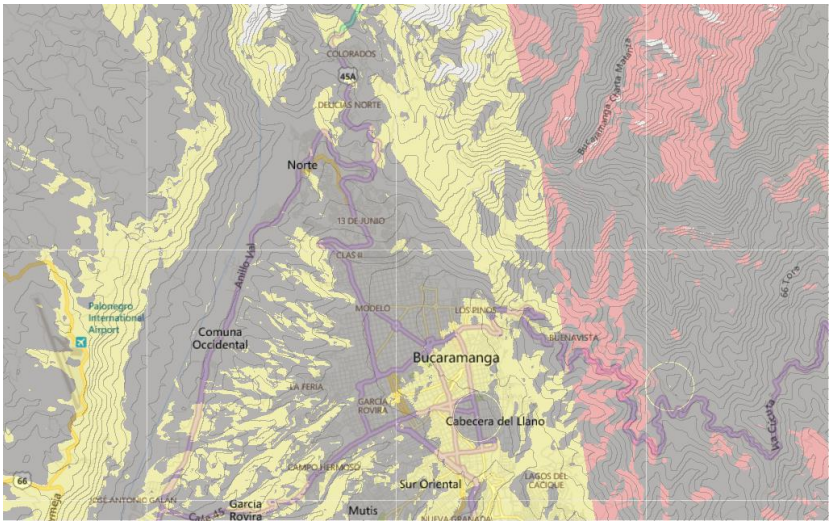


(b) Yagui



Para el estudio de cobertura múltiple radio mobile determina la cobertura total que alcanza una red de estaciones, permitiendo analizar la cobertura conjunto de varios transmisores, obteniendo grado de solapamiento entre ellas hacia una terminal fija, dicho solapamiento indica los sectores donde existe exceso de potencia y las áreas con varios servidores con alto nivel de señal lo que podría ocasionar interferencias de acuerdo a la recomendación *ITU-R P.1546-5* la importancia de determinar la distancia geográfica mínima entre las estaciones que trabajan en canales que utilizan las mismas frecuencias o en canales adyacentes, a fin de evitar la interferencia inaceptable debida a la propagación troposférica a gran distancia

Figura 39: Niveles de solapamiento entre dos transmisores.



Los resultados obtenidos en Radio mobile del solapamiento entre el transmisor localizado en la posición 1 y posición 2 se observa en la figura 39. En la parte inferior de la misma se puede apreciar para cada coordenada si existe o no traspaso; diferenciando tres zonas: Sin traspaso (cuando el nivel de la señal actual es mayor que el umbral de traspaso), Traspaso posible (si el nivel de señal es menor al umbral de traspaso pero no encuentra otro transmisor con suficiente señal) y Traspaso a (cuando el nivel de señal actual es inferior al umbral de traspaso y la señal proveniente del transmisor de posición 2 tiene el nivel suficiente para realizar el traspaso, teniendo en cuenta el parámetro "histéresis de traspaso").

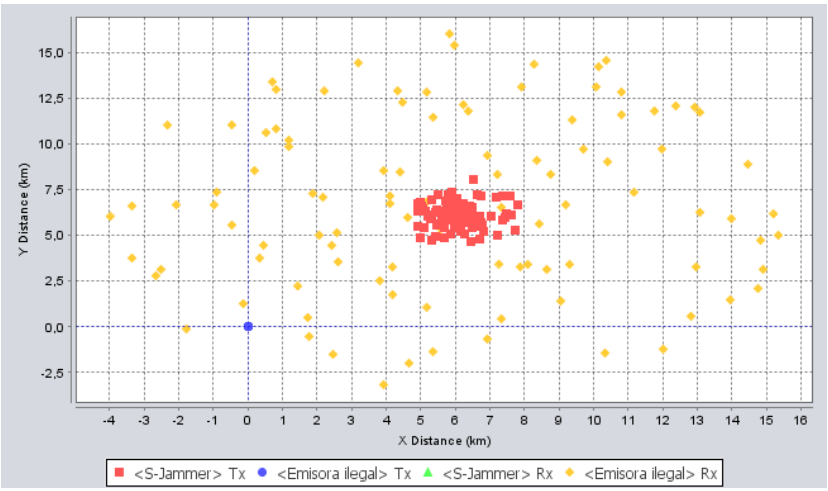
❖ **Simulación de enlace de interferencia** Acorde a la metodología presentada en el capítulo anterior, inicialmente se define el escenario de simulación que es un sistema genérico, en este caso compuesto de un transmisor victima (VLT), que representa una emisora clandestina FM, con frecuencia de operación 94MHz, una potencia de 60dBm y una antena que proporciona la librería de SEAMCAT de nombre *DVB-T Tx UHF-VHF* con polarización tanto vertical como horizontal. La ubicación entre emisor y receptor victima esta determinada por $Delta\ x = 6Km$ $y\ Delta\ y = 6Km$ con cobertura de 10Km. El transmisor de enlace de interferencia (IRT), será el dispositivo S-Jammer, con frecuencia de operación 94MHz, con potencia de 37,78dBm (6w) y antena con polarización horizontal. Los principales parámetros del enlace victima y de interferencia de presenta en la tabla –.

Tabla 12: Parámetros de configuración SEAMCAT

	VLT	**IRT**	**Unidad**
Potencia Tx	60	37.78	dBm
Antena	DVB-T Tx UHF-VHF	Dipolo	
Polarización	Vertical-Horizontal	Horizontal	
Cobertura	10	5	Km
Ancho de antena	3	1.43	m
Posición relativa x	6	VLT	Km
Posición relativa y	6	VLT	Km
Modelo de propagación	Extended Hata	ITU-R P.1546-5	
Sistema	Radio Difusión sonora	Radio Difusión sonora	

La simulación se realizó para un total de 40000 eventos, donde el modelo de propagación de los dispositivos está configurado bajo la norma de métodos de predicción de punto a zona para servicios terrenales en la banda de frecuencia 30 a 3000MHz *ITU-R P.1546-5*, configurada para sistemas de radio difusión análogos y con definición de entorno general para ambientes urbano denso y rural. El escenario de simulación se muestra en la figura 40 donde se observa la ubicación de 1000 de los 40000 eventos simulados, además de la ubicación de los receptores sobre los cuales son la referencia para la obtención de las varibales iRSS y dRSS.

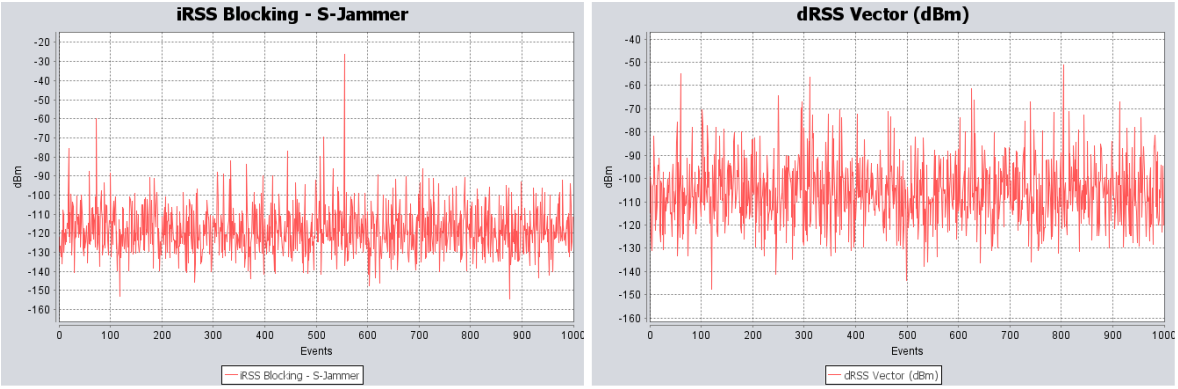
Figura 40: Escenario de simulación SEAMCAT



La potencia media resultante para dRSS es de -105,49 dBm con una desviación estándar de 14,09 dB, la potencia media de la señal iRSS de bloqueo es de -

112,15dBm con una desviación estándar de 11,32dB, con los valores de las potencias medias obtenidas de la figura 41, observamos que a pesar de que la emisión ilegal VTL posee una mayor potencia de emisión, el enlace IRT provocado por el S-Jammer obtiene un valor de potencia 7dBm por debajo y acorde a lo presentado por el autor en [16], inicialmente se puede deducir que el dispositivo de bloqueo puede interferir la señal de la emisora ilegal.

Figura 41: Valores iRSS y dRSS SEAMCAT



El criterio de interferencia utilizado por el software de simulación es el C/I, que determina la existencia de interferencia sí la relación entre la señal de portadora y el ruido no supera el mínimo establecido, el valor de C, esta dado por la relación entre la potencia esperada por la victima/ la potencia deseada esperada (dRSS), mientras que el valor I corresponde al valor de potencia de interferencia iRSS. Acorde a este criterio, indica que el dispositivo tiene una probabilidad del 73,41 % de bloquear la emisión ilegal. Además que la probabilidad de interferencia no directa (Unwanted) es de 32,76 %.

Capítulo 5
TRABAJOS FUTUROS

Gracias al SDR se podría desarrollar un sistema de monitoreo de emisiones clandestinas donde se no solo se detecte las señales que no se encuentran en el Plan Técnico Nacional de Radiodifusión sonora, sino que asegure el cumplimiento de la normativa en las frecuencias asignadas. Además se podría desarrollar un sistema de bloqueo de emisiones clandestinas enfocado para otros servicios como televisión digital, GSM , Wi-Fi, entre otras haciendo uso de las diferentes técnicas jamming enfocadas a cada aplicación.

Implementar una red de bloqueo inteligente que integre el sistema de monitoreo de emisiones clandestinas y el sistema de ataque mediante protocolo TCP/IP con conectividad en la nube que permita tener acceso de manera remota desde un centro de gestión
.

Capítulo 6
CONCLUSIONES

Este proyecto evaluó la posibilidad de combinar el uso componentes fundamentales de equipos de radio difusión sonora y aplicaciones desarrolladas en sistema de comunicaciones con SDR. El componente principal del prototipo de bloqueo desarrollado fue un transreceptor basado en tecnología SDR, sobre el cual se montó un sistema de aplicaciones embebidas desarrolladas en GNU Radio. Los resultados de la aplicación de la metodología desarrollada comprueban la viabilidad de esta solución para tratar las emisiones clandestinas en las bandas de radio difusión sonora FM.

La pruebas diseñadas para extraer los parámetros que delimitan el terminal S-Jammer pueden de ser ayuda no solo para la caracterización de dispositivos con aplicaciones al bloqueo de señales y análisis más profundo de la coexistencia de diferentes sistemas, sino también para la extracción de parámetros específicos en elementos como lo son antenas, amplificadores entre otros de manera individual.

Los equipos USRP con los que cuenta el grupo de investigación RadioGis sometidos a la metodología desarrollada cumplen con las características necesarias para la implementación de un sistema de monitoreo del espectro radioeléctrico complementado con un sistema de ataque de emisiones clandestinas aportando una solución a la lucha contra las emisiones ilegales persistentes en las bandas de radiodifusión FM

Los resultados de las pruebas de recepción realizadas a los radio periféricos indican que el USRP 2920, tiene mayor capacidad a diferencia del USRP e310, al interpretar señales de potencia mayores a -118 dBm gracias al amplificador de bajo ruido que posee, postulandolo como la mejor opción para realizar el monitoreo del espectro para la

detección de emisiones clandestinas. Los radio periféricos estudiados emiten potencias máximas similares, sin embargo la relación entre la ganancia del amplificador Tx y la potencia de salida es menor en el USRP e310, lo que le permite transmitir una mayor cantidad de potencias hacia el amplificador RF sin superar el límite de potencia en su señal de entrada, otorgando un mayor control en la potencia transmitida amplificada.

La metodología desarrollada sienta bases para la extracción de parámetros principales y lineamientos con el fin de tener una mejor compresión de las capacidades de equipos de radio definido por software como solución al desarrollo de sistemas de bloqueo de señales.

Bibliografía

[1] Bhattacharya, P. P., Khandelwal, R., Gera, R., and Agarwal, A. Smart Radio Spectrum Management for Cognitive Radio. *International Journal of Distributed and Parallel Systems 2*, 4 (2011), 12–24.

[2] Bravo, M. D., Carvajal, J. G., and Torres, A. F. Diseño e implementación de un prototipo Inhibidor de señales para un salon de clases-, 2014.

[3] Canet, C. Evaluación y Oportunidades de una Estación Base GSM definida por Software, Barcelona, 2016,138p. *Escuela Técnica Superior de Ingeniería de Telecomunicaciones de Barcelona*.

[4] Carmona, A. Estudio de sistemas de detección e inhibición para emisores celulares presentes en redes comerciales, Medellin, 2013, 77p. *Universidad EAFIT*.

[5] Diaz, J. F. Aplicación de técnicas anti-jamming a un sistema de comunicaciones convencional para su explotación en entornos tácticos, madrid, 2012, 94p. *Escuela Politécnica Superior Universidad Autónoma de Madrid*.

[6] Feléz, M. Modelado y simulación de un sistema de guerra electrónica (jamming) en una transmisión de datos inalámbrica crítica en seguridad, Zaragoza, 2012, 80p. *Universidad de Zaragoza, Escuela de Ingeniería y Arquitectura*.

[7] Grover, K., Lim, A., and Yang, Q. Jamming and anti-jamming techniques in wireless networks: a survey. 2014, 197p, Vol: 17. *International Journal of Ad Hoc and Ubiquitous Computing*.

[8] Huang, Y., and Li, G. Descriptive models for Internet of things. *Proceedings of 2010 International Conference on Intelligent Control and Information Processing, ICICIP 2010*, PART 2 (2010), 483–486.

[9] Jisrawi, A. GSM-900 Mobile Jammer, 2010, 28p. *Jordan Universty of Science and Technology, Electrical Engineering Department*.

[10] Kaabouch, N., and Hu, W.-C. *Handbook of Research on Software-Defined and Cognitive Radio Technologies for Dynamic University of North Dakota, US Spectrum Management*, vol. i. 2014.

[11] Lohn, J. D., Becker, J. M., and Linden, D. S. An evolved anti-jamming adaptive beamforming network, 2011, (217-234p). *Springer Science+Business Media, LLC*.

[12] Muyulema, P. S. Estudio técnico, diseño e implementación de un dispositivo inhibidor de señales del servicio móvil avanzado (SMA), Riobamba, 2014, 145p. *Escuela Superior Politécnica de chamborazo, Facultad de informática y electrónica*.

[13] NATO Standardization Agency. Nato Glossary of Terms and Definitions (English and French), North Atlantic Treaty Organization, 2014, 443p.

[14] Ortega, H., Flórez, M. G., Rodríguez, J. D., Muñoz, M. A., Pico, C. A., and Forero, C. A. Implementation of DeJong radio propagation algorithm as a virtual sensor for cloud services to enhance radio spectrum management. *IEEE Colombian Conference on Communications and Computing, COLCOM 2015-Conference Proceedings*.

[15] Perera, C., Zaslavsky, A., Christen, P., and Georgakopoulos, D. Sensing as a Service Model for Smart Cities Supported by Internet of Things, 2014, 12p. *Transactions on emerging Telecommunications Techonologies*.

[16] Poisel, R. Modern Communications Jamming Principles and Techniques, 2011. *Artech House Vol: 2nd*.

[17] Poisel, R. A. Electronic warfare receivers and receiving systems, 2014. 540p. *Artech House 1st edition*.

[18] Poisel, R. A. *Introduction to communication electronic warfare systems. 2002, 574p*, vol. 1st edition.

[19] Sylvia, L. N. S. Sistema de interferencia de señal celular en dispositivos con tecnología GSM, Ambato, 2015, 116p. *Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial*.

[20] Torres, K. Desarrollo de un dispositivo jammer para el bloqueo de señal GSM, Lima. 2014, 77p. *Pontificia Universidad Católica del Perú*.

[21] Wang, F., Krunz, M., and Cui, S. Price-Based Spectrum Management in Cognitive Radio Networks, 2008, (70-78p). *2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications*.

[22] Weber, R. H. Internet of Things - New security and privacy challenges,2010, 23-30p, Vol: 26. *Computer Law and Security Review*.

[23] Xu, W., Trappe, W., Zhang, Y., and Wood, T. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks, 2015, 46-57p. *University Rutgers*.