Análisis y Emulación de Inhibición de Señales Electromagnéticas usando RTL-SDR y GNU-Radio

Juan Carlos Nicán Marín

Sebastián Zuluaga Galeano

Ingeniería de Telecomunicaciones

Prof. David Andrés Márquez Viloria

INSTITUTO TECNOLÓGICO METROPOLITANO

MEDELLÍN, 2016

RESUMEN

En este documento se propone un proyecto cuyo objetivo es emular el funcionamiento de los inhibidores de señales electromagnéticas (Jammers) y de sus respectivos detectores (anti-Jammers) en un ambiente controlado y libre para experimentación, realizando pruebas y documentando los resultados útiles como referencia en futuros estudios. El proyecto usa como herramienta investigativa la emulación, que, a diferencia de la simulación, conecta dispositivos físicos a un entorno virtual programable permitiendo obtener resultados de campo realistas con costos muy reducidos y disminuye los tiempos de implementación comparado con el diseño de hardware.

Se inicia con un contexto teórico donde se describen los fundamentos físicos y electrónicos del hardware empleado, para luego contextualizar las propiedades del software necesario en la emulación. Se añade las aplicaciones comunes del sistema obtenido tanto científicas, como comerciales y delictivas.

En la metodología propuesta, se explica cómo se emulará el sistema híbrido: el funcionamiento del bloqueo de señal, las características técnicas de la antena y de su conexión, así como las tecnologías de detección. Por último, se hace referencia al marco jurídico y legislativo correspondiente al rastreo y bloqueo de señales de radiofrecuencia, el cual es necesario conocer para la implementación de estos sistemas sin violar la Ley. Del mismo modo, se aclara que el entregable como tal del proyecto es un algoritmo en GNU-Radio acoplado a antena.

Palabras clave**:** antena RTL-SDR, GNU Radio, Inhibidor, Jammer, Señales Electromagnéticas.

RECONOCIMIENTOS

Agradecemos a todos aquellos que, a lo largo de nuestra formación como personas y estudiantes, nos acompañaron y brindaron su apoyo para alcanzar nuestras metas. A todos los familiares, profesores y amigos que hicieron parte de nuestro sueño de ser ingenieros.

ACRÓNIMOS

NFC Comunicación de campo cercano

RF Frecuencia de radio

ADC Conversión analógica a digital

DAC Conversión digital a análogo

TCL Herramienta de lenguaje de comandos

TIC Tecnologías de la información y la comunicación

MINTIC Ministerio de Tecnologías de la Información y las Comunicaciones

ANE Agencia Nacional del Espectro

FHSS Frequency Hopping Spread Spectrum

DSSS espectro ensanchado por secuencia directo

WBFM Modulación de frecuencia banda ancha

USRP Software radio peripheral universal

SDR Radio definido por software

DFT Transformada discreta de Fourier

TABLA DE CONTENIDO

LISTA DE FIGURAS

1. INTRODUCCIÓN

Dada la creciente demanda en el sector público y privado por dispositivos bloqueadores de radiofrecuencia jammer el presente informe describe la fabricación y el funcionamiento mediante la emulación de estos dispositivos y sus detectores antijammer utilizando en esencia el software libre GNU-Radio y un dispositivo RTL-SDR, indagando la posibilidad de recrearlos con un bajo costo para su futura implementación por profesionales de las Telecomunicaciones.

Como objetivo general se plantea la simulación de un laboratorio que permita el análisis de los inhibidores de señal en un ambiente real y controlado para la documentación de las variaciones presentes en el mismo, como objetivos específicos se pretende diseñar un laboratorio virtual para controlar las antenas USB y emular el funcionamiento de estos dispositivos, generar señales con la capacidad de bloquear otra señal objetivo y la creación de otro dispositivo que detecte la radiofrecuencia del jammer.

Para la organización de la tesis en el capítulo uno se da una visión general de la investigación y sus respectivos objetivos, en el capítulo dos se define que es un jammer, cada uno de sus principales componentes, su sistema de código GNU-Radio y las diversas investigaciones propuestas por profesionales en Telecomunicación, en el tercer capítulo se describe la metodología utilizada en la elaboración del trabajo, la configuración tanto del laboratorio virtual como del software y su correspondiente instalación, en el capítulo cuatro se presentan los resultados obtenidos, y por último, en el capítulo cinco se presentan las respectivas recomendaciones y proyecciones.

1.1 Planteamiento del problema

Como profesionales de las telecomunicaciones, nos proponemos realizar un material de estudio e investigación aplicada que podría servir de referencia a empresas privadas o gubernamentales y a las futuras generaciones de estudiantes de telecomunicaciones, priorizando al Instituto Tecnológico Metropolitano, en el área de los dispositivos inhibidores de radiofrecuencias y su correspondiente detección. Estos dispositivos de telecomunicaciones tienen una creciente demanda privada y pública en el marco de la seguridad empresarial y la defensa militar, por ejemplo, la desactivación de explosivos controlados remotamente. Sin embargo, también conllevan riegos debido a las personas que utilizan tales equipos para actos delictivos.

En este contexto, es valioso conocer el funcionamiento de estos dispositivos desarrollando laboratorios controlados de experimentación, a través de herramientas de software libre como el sistema operativo GNU/Linux, con el fin de estudiar las propiedades de los jammers, radiopropagación y detección. En este trabajo se aprovecharán las ventajas de la emulación que permite estudiar los dispositivos en un entorno real y no virtual, beneficiándose de la implementación combinada del software libre y el hardware que permite recrear y estudiar dispositivos de telecomunicaciones disminuyendo los costos asociados.

Debido a que en la actualidad se usan con mucha frecuencia dispositivos tecnológicos (NFC, Bluetooth, ZigBee o RF) así como sistemas de seguridad local o vehicular, tanto a nivel personal como gubernamental y militar, que se conectan a través de medios inalámbricos. Todos ellos son susceptibles de interferencia o bloqueo de radiofrecuencia. Entonces podemos realizar la siguiente pregunta de investigación:

¿Se Pueden recrear dispositivos inhibidores (jammers) y sus detectores (anti-jammers) con herramientas gratuitas, o de muy bajo costo, para su posterior documentación e implementación por profesionales en Telecomunicaciones?

La hipótesis que plantea este trabajo es que se puede realizar un laboratorio que permita la emulación de inhibidores y sus detectores, usando herramientas de software libre como GNU Radio y dispositivos de bajo costo como RTL-SDR, permitiendo el análisis de este tipo de dispositivos en un ambiente controlado.

1.2 Objetivos

1.2.1 General

Desarrollar una simulación de laboratorio en donde se pueda realizar la implementación y el análisis de dispositivos inhibidores de señales y detección de los mismos en un área específica, usando RTL-SDR y la herramienta de desarrollo libre y abierta para radio definido por software GNU Radio, con el fin de experimentar y documentar variaciones y comportamientos de los dispositivos emulados.

1.2.2 Específicos

- Diseñar un laboratorio virtual sobre el sistema operativo GNU/Linux usando el software GNU Radio que permita manejar el RTL-SDR con el fin de emular el funcionamiento de dispositivos inhibidores de señales.

- Generar señales que permitan realizar la inhibición de otras señales objetivo en las frecuencias de algunos de los sistemas electromagnéticos comerciales más usados para realizar la simulación de los dispositivos inhibidores sobre el entorno GNU-Radio.
- Diseñar y emular un dispositivo que permita detectar señales inhibidoras en un área específica.

En el capítulo I se presenta una breve introducción del proyecto, el planteamiento del problema y los objetivos tanto generales como específicos.

En el capítulo II se exponen los conceptos y teorías necesarias para el entendimiento del proyecto como los tipos de jammer, la Radio Definida por Software, el GNU-Radio y las diversas investigaciones propuestas por profesionales en Telecomunicación.

En el capítulo III se condensa la información relacionada con la elaboración del proyecto como la configuración del software y el hardware, la instalación de librerías RTL-SDR, los parámetros utilizados y los datos de apoyo.

En el capítulo IV se presentan los resultados obtenidos en la tesis mediante la discusión soportada por otros reportes identificando fortalezas, limitaciones y restricciones.

En el capítulo V se presentan las recomendaciones, conclusiones, fortalezas y proyecciones para trabajos futuros relacionados con los inhibidores de radiofrecuencia.

2. MARCO TEÓRICO

2.1 Inhibidor de Señal Jammer

Los inhibidores de radiofrecuencia jammer son dispositivos especializados en el bloqueo de una señal de radiofrecuencia a través de un espectro electromagnético, por el cual se trasmite una onda con ruido por la misma frecuencia del receptor generando una interferencia suficiente entre el dispositivo y la estación base, estos dispositivos inhiben señales telefónicas, Bluetooth, WI Fi y señales GPS. Este proceso de bloqueo de la señal se ve afectado por múltiples factores como la proximidad de una torre, la presencia de edificios hasta la humedad.

Los jammer tienen múltiples beneficios como son el desactivar bombas que son accionadas a través de una llamada celular, el impedir la comunicación de organizaciones criminales con reclusos, prevenir asaltos y ataques a los bancos por la coordinación de delitos hasta tener un alto grado de confidencialidad en las reuniones (Universidad de las Américas Puebla, 2013).

2.2 Tipos de Jamming

Existen diversas estrategias que puede emplear un jammer para la inhibición de señales las cuales dependen de las particularidades del dispositivo, el ambiente y la implementación de dispositivos antijammer, de este modo se tienen los siguientes tipos de jamming:

2.2.1 Jamming por Ruido

La señal emitida por el jammer se modula por una señal sin información denominada ruido la cual puede inhibir total o parcialmente el ancho de banda-ancha del antijammer por lo cual varia el resultado, de esta técnica se distinguen tres tipos de jamming:

2.2.1.1 Jamming por Ruido de Banda Completa

Es un tipo de jamming aplicable a cualquier dispositivo el cual introduce energía en forma de ruido residual abarcando todo el espectro de frecuencias del objetivo, como inconveniente tiene una baja potencia la cual se puede compensar si hay proximidad entre el receptor y emisor.

2.2.1.2 Jammin por ruido de Banda Parcial

En este caso solo se introduce o direcciona el ruido a una parte especifica del espectro mejorando así su potencia.

2.2.1.3 Jamming por ruido de banda angosta

Esta manera de jamming se centra en un único canal del espectro teniendo así la mejor potencia entre los anteriores tipos de jamming, la eficiencia de esta técnica radica en el conocimiento del lugar exacto del espectro para así inhabilitar las señales de interés.

2.2.2 *Jamming* por Tonos

En un sistema DSSS (espectro ensanchado por secuencia directo) es posible utilizar el jamming de tonos que consiste en colocar uno o varios tonos en el ancho de banda donde se encuentra la señal objetivo, por lo tanto, es de suma importancia conocer con exactitud la señal y el lugar en donde se inducirá el tono en frecuencia cero para lograr interferir la trasmisión.

2.2.3 *Jamming* por Pulsos

Esta técnica actúa de manera similar al jamming por ruido con la diferencia de que el jamming por pulsos se enfoca en el tiempo en que el jammer permanece encendido y no en la frecuencia, al trabajar con pulsos la potencia mejora al igual que su eficiencia.

2.2.4 *Jamming* por Barrido

Se puede considerar una técnica complementaria entre el jamming por ruido de banda ancha o banda parcial ya que consiste en introducir un ruido que abarque todo el ancho de banda haciendo un barrido por esta, de tal modo que identifique la frecuencia en la que se encuentra la señal objetivo y utilice su máxima potencia en esta señal específica y no en todo el espectro lo cual optimiza la potencia.

2.2.5 *Jamming* por Seguimiento

Es una técnica que consiste en trasmitir tramos de información a través de escenarios cambiantes como la frecuencia de emisión y el intervalo de tiempo inferior a 400 ms, para ello se utiliza una secuencia de pseudoaleatoria almacenada en unas tablas las cuales el emisor y el receptor conocen, su eficacia se ve afectada por el tiempo en que permanezca encendido el jammer ya que debe no solo debe conocer la frecuencia de la señal sino también medir la energía del espectro, y la aplicación al mismo tiempo en más de un canal.

2.2.6 *Jamming* inteligente

Es una estrategia que tiene como base el estudio del dispositivo objetivo permitiendo la optimización de recursos, dentro de este tipo de jamming se tiene el jamming de engaño en el cual se envía un mensaje falso al receptor o intercepta la señal del receptor y establece una ruta de comunicación incorrecta.

2.3 Detección de *Jammers*

La señal de un jammer es una onda electromagnética que no transmite ningún tipo de información específica, por lo cual puede considerarse como una señal de ruido y se puede medir con dispositivos electrónicos diseñados para este fin. Los antijammers miden el nivel de radiación electromagnética de una zona, pueden detectar la señal emitida por el jammer y al ser conectados a un generador de espectros se puede graficar la onda de la señal y del ruido para su análisis. Los más avanzados pueden detectar la posición del jammer y muchos de los antijammer también se usan para medir el nivel de radiación en una zona y determinar estudios o investigaciones acerca de los efectos de la contaminación electromagnética en las personas.

En este trabajo se emuló un detector básico que permite capturar las señales electromagnéticas en una zona y por medio del software GNU Radio analizar estas señales para determinar si existe algún jammer en dicha zona. El objetivo es comprender como funcionan estos detectores y proporcionar una base para otros proyectos en esta área.

2.4 Radio Definida por Software

Radio Definida por Software o SDR es un sistema de radiocomunicaciones mediante el cual componentes como mezcladores, detectores, filtros, moduladores, entre otros, son implementados en un software capaz de cumplir funciones complejas permitiendo simplificar la cantidad de material y circuitos que componen un equipo de radio; además de habilitar la creación e implementación de dispositivos inalámbricos con diversos modos de operación, reconfiguración y actualización a un bajo costo de desarrollo.

A través del SDR es posible visualizar de forma gráfica un mapeo o una porción de ancho de banda que se está maniobrando y así determinar la actividad telegráfica, el rango de señales y su potencia.

La tecnología SDR se compone por un computador con un adaptador de radiofrecuencia además de una antena con circuitos de amplificación inicial de RF, un oscilador local, un mezclador, una etapa primaria de frecuencia intermedia y un conversor analógico digital (CAD), con la implementación de estos componentes es posible convertir “problemas hardware en problemas software” proporcionando un canal ancho creado para la escucha en donde el software se moverá y decodificara señales presentes en el espacio del espectro permitiendo suprimir cualquier tipo de interferencia, ruidos y señales que se deseen. Estos sistemas SDR están capacitados no solo para la recepción o conversión analógica en digital, también permiten trasmitir internamente en un canal para la escucha.

2.5 Universal Software Radio Peripheral USRP

Software Radio Peripheral universal o USRP es una gama de Radio Definida por Software con un hardware de código abierto el cual permite diseñar e implementar sistemas de radio de software flexibles de gran alcance permitiendo cubrir una amplia gama de frecuencias con gran rapidez.

Esta gama de RDS se implementa con la descarga de GNU Radio generando una apertura completa de código de radio además de un paquete de procesamiento de señales, y finalmente la USRP conectado a un ordenador central a través de un enlace de alta velocidad permite así trasmitir y recibir una ilimitada variedad de señales.

Una de las grandes ventajas del USRP es permitir la implementación a un bajo costo y con mínimo esfuerzo dada su plataforma flexible con GNU Radio, además de contar con una gran comunidad de desarrolladores.

Software Radio Peripheral universal cuenta con un dispositivo analógico de 64 MS 12 bits a los convertidores analógico como cuatro dispositivos digitales de 128 MS de 14 bits a analógico, una interfaz UDB 2.0 de alta velocidad, tiene una capacidad de procesar señales de hasta 16 MHz de ancho además de tener una arquitectura modulable compatible con una gran variedad de RF y placas secundarias.

2.6 Chipset RTL-2832U

El RTL2832U es un demodulador de alto rendimiento con interfaz USB 2.0 el cual posee un ancho de banda de 8MHz. Este demodulador es compatible con los sintonizadores de Frecuencia Media (36.125MHz), baja frecuencia (4.57MHz), o salida de cero si se utiliza un cristal 28.8MHz, además cuenta con alta estabilidad en la recepción portátil. (Carralero & Marichal, 2016)

2.7 Antena para RTL-2832U

Este componente permitirá detectar la radiación electromagnética presente. La antena usada será omnidireccional ya que debe emitir señal en todas las direcciones con el fin inhibir la señal objetivo a su alrededor (Sambhe & Kale, 2008).

La antena que se usará en este proyecto tiene una conexión por medio del puerto USB con interface 2.0, por lo cual se incluyen los drivers necesarios para que se realice la compatibilidad con el sistema operativo.

Esta antena permite un rango de uso desde 25 MHz hasta 1700 MHz el cual abarca frecuencias FM y celulares GSM, entre otras (para bloquear señales WIFI se necesitaría una

antena de 2.4 a 5 GHz). Tiene una impedancia de 75 ohmios y una potencia de 1.5 watts. Todos los valores y rangos de esta antena pueden ser controlados desde el software GNU Radio, ver **¡Error! No se encuentra el origen de la referencia.**.

Figura 1. Antena que se usará en la emulación.
Referencia: RTL-SDR, con set USB RTL2832U.

2.8 GNU-Radio

Este sistema de código libre permite el desarrollo de herramientas a través de bloques de procesamiento de señales en la implementación de software de radio. Como se menciona anteriormente, con este sistema, se puede usar hardware RF externo de bajo costo para crear los radios definidos por software o sin la utilización de hardware utilizando el entorno de simulación (GNU Radio, 2012), en el caso del presente proyecto, se utiliza la implementación del sistema GNU-Radio para emular el inhibidor de señales jammer, con el fin de crear un bloqueador de señales para sistemas de seguridad, por ende es que este software se utiliza en el entornos de aficionados, académicos y comerciales, con el fin de contribuir en investigaciones de comunicación inalámbricas y sistemas de radio para el mundo real.

Según el portal web de GNU-Radio:

“Las aplicaciones de GNU-Radio son escritas a principio utilizando el lenguaje de programación Python, mientras que el suministro de herramientas críticas de procesamiento de señales que requieren alto rendimiento son implementados en C++ usando extensiones de procesamiento de punto flotante, cuando este está disponible. Así, el desarrollador es capaz de implementar, de manera simple, sistemas de radio de alto rendimiento funcionando a tiempo real aprovechando el ambiente de desarrollo de aplicaciones de manera inmediata” (GNU Radio, 2012).

GNU radio se compone como un conjunto de archivos y aplicaciones que proveen las librerías que se necesitan como proceso digital de señales para manipular señales de radio, este sistema corre sobre sistemas GNU/Linux como Ubuntu, el cual se debe instalar con previa antelación. Para construir un sistema de radio con GNU Radio, es necesario crear un grafo, donde los vértices son bloques de procesado de señales y el flujo de datos entre ellos este representado en los bordes. Como se menciona anteriormente los bloques de procesamientos se implementan en C++, estos se encargan de procesar señales continuamente desde puertos de entrada hasta puertos de salida. Un bloque está determinado el número de puerto de entrada, el número del puerto de salida y el tipo de datos que fluyen de uno al otro. Los tipos de datos que comúnmente se usan son “short”, “float” y “complex”. Algunos de los bloques cuentan únicamente con puertos de salida o puertos de entrada, que se usan como fuente de datos y señales en una gráfica, según esto, existen graficas que leen datos de un archivo del ADC, y señales que escriben datos a un archivo, al DAC o a un display gráfico. El sistema GNU Radio cuenta con aproximadamente 100 de estos bloques (Chávez, 2005).

Las gráficas que son utilizadas para GNU Radio corren y son construidas en lenguaje de programación Python, este sistema es interpretativo, interactivo y orientado a objetos, normalmente se compara con otros lenguajes de programación como TCL, Perl, Scheme, Java y Ruby (Phyton, 2016).

En la actualidad Python se desarrolla como un proyecto de código abierto, administrado por la Python Software Foundation, este contiene una serie de módulos, clases, tipos de datos de alto nivel y escritura dinámica, interfaces para diversos sistemas y librerías, además puede usarse como un lenguaje de extensión de aplicaciones donde es necesario una interfaz programable. Una de las ventajas más importantes de Python es su portabilidad, que permite que funcione en sistemas Unix junto con sus derivados, Windows, Dos, Mac y otros.

Según explica Jorge Chávez, Ingeniero en electrónica y comunicaciones de la Universidad de las Américas de Puebla, existen dos factores fundamentales que son los que distinguen a Python de otros lenguajes de programación:

No hay necesidad de compilar código en Python antes de ejecutarlo, por lo que se convierte en un lenguaje de script. El lenguaje busca tener un código más fácil de utilizar (y con reutilizable para otras aplicaciones).

2.9 Aplicación móvil: GPS-Test

La aplicación de GPS Test tiene como objetivo brindar información de la posición y sus alrededores a través del GPS y basado en datos de la altitud de velocidad, detalles de los satélites o las coordenadas básicas. La aplicación tiene herramientas de marcados como altímetro, brújula y *speedo*, una fuente LED de 7 segmentos, fuente de matriz de puntos y un modo de HUD. Es muy versátil ya que funciona bien sin una conexión WiFi o de datos móviles. La aplicación contiene cinco pantallas de información:

1) la señal GPS (SNR) mediante un gráfico de barras que muestra la intensidad de la señal de cada satélite, así como la precisión y el estado del GPS.

2) Posiciones de los satélites desde una vista superior (visión del cielo), que se muestra en una brújula giratoria la cual se puede configurar para ir por la brújula interna o por GPS, permitiendo a los usuarios estimar dónde se debe posicionar un satélite.

3) La ubicación actual en la tierra se muestra como texto y en un mapamundi. También se muestra la posición actual del sol y la curva de transición día / noche.

4) La velocidad actual, el rumbo y la altitud las cuales se muestran como texto.

5) La hora actual leída desde el GPS y la hora local en la zona horaria actual, así como las horas de salida y puesta del sol en su ubicación.

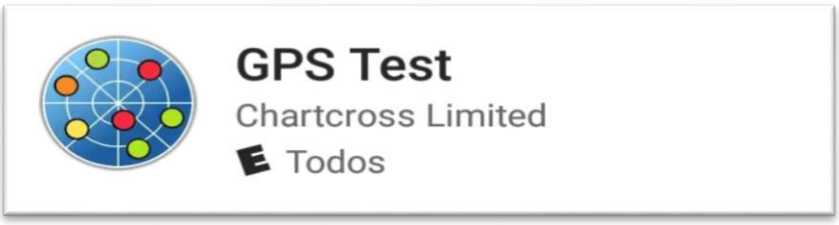


Figura 2 Aplicación móvil GPS test para visualizar satélites.

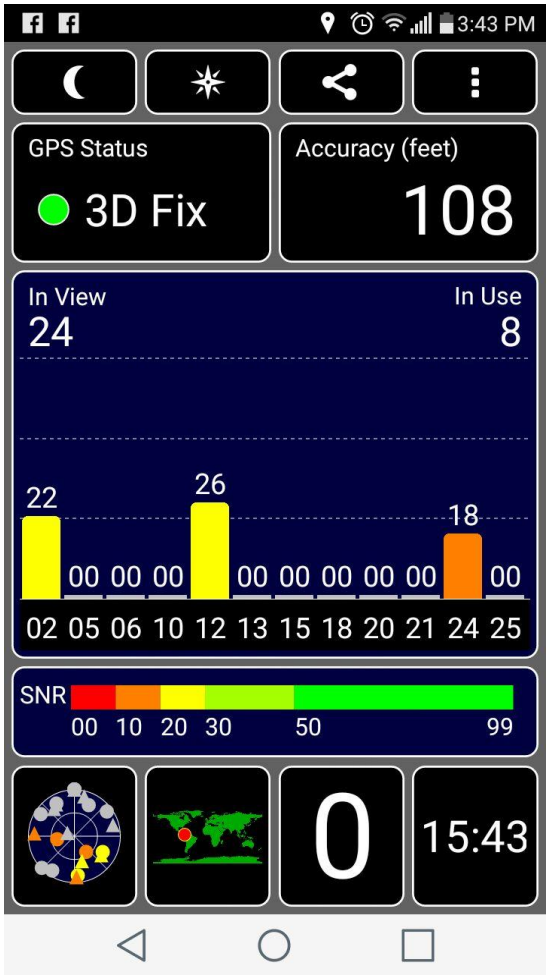


Figura 3. Cantidad de satélites encontrados y la conexión de cada uno

2.10 Legislación Colombiana Acerca de Jammers

El gobierno colombiano por medio del Ministerio de las TIC, regula el uso de los jammers o inhibidores de señal. Se permite la compra y venta libre de estos dispositivos, pero se debe contar con una autorización de las autoridades para poder usarlo, debido a que su fácil adquisición está generando que muchas personas lo usen indiscriminadamente afectado la operatividad de los operadores de servicios de telecomunicaciones o con fines delictivos.

En Colombia la Resolución 2774 del 16 de agosto del 2013 se encarga de regular el uso de los jammers en la que se establecen los mecanismos legales para emplear los inhibidores y amplificadores de señal de manera legal, dejando en claro que solo el Ministerio de las TIC podrá autorizar a quienes los usen, los lugares y horarios de uso (MINTIC, 2013). La Agencia Nacional del Espectro (ANE), aseguró que las autoridades han detectado el uso ilegal de los

inhibidores y amplificadores en universidades, iglesias, clubes sociales, bancos, por desconocimiento a esta resolución, están incurriendo en un delito.

2.11 Revisión de Literatura

En la actualidad los profesionales de ingeniería en telecomunicaciones investigan y desarrollan aplicaciones para la detección y anulación de señales. Los siguientes son artículos científicos publicados en fechas cercanas a la realización de este trabajo.

2.11.1 Bloqueo de señales por jamming reactivo en GNU Radio (Fang & Liu, 2015)

El jamming reactivo solo bloquea la señal cuando los dispositivos están transmitiendo, a diferencia del bloqueo constante, el jamming reactivo es más difícil de rastrear y contrarrestar. El artículo explica que las técnicas: Frequency Hopping Spread Spectrum (FHSS) y Direct Sequence Spread Spectrum (DSSS) son las más utilizadas como contramedidas a los ataques de interferencia. Sin embargo, ambas fallarán si el jammer bloquea todos los canales de frecuencia o tiene un alto potencia de transmisión. En este trabajo, se propone un sistema de comunicación anti-jamming que permite la comunicación en presencia de un amplio espectro de interferencia y una potencia alta. El sistema propuesto transmite mensajes mediante el aprovechamiento del tiempo de reacción, y, por lo tanto, se puede utilizar en escenarios donde los enfoques tradicionales fallan. Los autores desarrollaron un prototipo del sistema propuesto utilizando GNU Radio. La evaluación experimental muestra que cuando un potente bloqueador reactivo está presente, el prototipo mantiene la comunicación, mientras que otros esquemas tales como 802.11 DSSS fallan completamente.

2.11.2 Estudio experimental FM usando GNU-Radio y antena RTL-SDR (Vachhani & Mallari, 2015)

Este artículo se centra en el software libre GNU Radio y estudia su uso como herramienta de investigación en conjunto con USRP y la antena transceptora RTL-SDR. El paquete GNU Radio puede actuar como una herramienta de simulación o como un subsistema de software para emular un hardware transceptor de Radio Definido por Software (SDR). Esto se logra mediante la implementación de un receptor WBFM utilizando RTL-SDR. Finalmente, se concluye comparando un sistema económico emulado en el RTL-SDR, con el hardware USRP más exacto pero costoso.

2.11.3 Diseño inteligente de jammers para señales celulares (Divya & Coll., 2012)

Los autores de este artículo justifican el uso de jammers para aumentar la seguridad y privacidad en diversos lugares, esto se puede hacer mediante el uso de jammers que bloqueen todas las señales de teléfonos celulares. En efecto, en el artículo se describen

técnicas mejoradas para bloquear las señales de teléfonos celulares, su principal objetivo es concentrarse en una banda específica de frecuencia. Este método permite que el jammer sea más preciso y eficaz, tan preciso que puede centrarse en una red individual y sobre un área específica.

El valor agregado de esta investigación en particular es que los servicios de emergencia permanezcan activos, lo que es muy importante en caso de cualquier calamidad, y también tiene un consumo de energía menor que los modelos existentes.

2.11.4 Jammer de banda dual dirigible (Araujo & Santos, 2007)

El Jamming eficiente de los teléfonos celulares es muy demandado por las autoridades de seguridad, especialmente dentro de las cárceles. En consecuencia, este artículo propone una estructura jammer orientable de banda dual. Los autores diseñaron un solo filtro espacial que funcione simultáneamente en ambas bandas de frecuencias de telefonía celular, basado en la metodología de formación de haz de dirección nula. Se abordan consecuentemente los problemas de hardware y software de la emisión propuesta. El rendimiento direccional jammer se ilustra con patrones de haz simulados, que condujeron a resultados funcionales.

3. METODOLOGÍA

3.1 Objetivo 1: Configuración del Laboratorio Virtual bajo Linux

3.1.1 Configuración del Software

3.1.1.1 Instalación de GNU-RADIO

Se utilizó el software libre de programación de sistemas de radio definido por bloques de procesamiento. Este software además de ser libre, permite generar estructuras y programas en rutinas locales de una manera muy intuitiva lo que facilita su manejo y aumenta su versatilidad. Se instala con el comando:

:~$ sudo get-apt install gnuradio

3.1.1.2 Instalación de librerías RTL-SDR

Inicialmente se debe instalar la función rtl-sdr para instalarla se debe tener instalado previamente g++ con el comando "*sudo apt-get install g++"*

Después de esto se debe instalar Cmake, de preferencia la versión más reciente que se puede descargar del siguiente link:

http://www.cmake.org/cmake/resources/software.html">http://www.cmake.org/cmake/resources/software.html

Posterior a esto descomprimimos el archivo descargado de la siguiente manera:

:~$ cd /home/mrdesc/downloads
:~$ tar xzvf cmake-2.8.10.2.tar.gz
:~$ cd cmake-2.8.10.2/
:~$ sudo ./bootstrap
:~$ sudo make
:~$ sudo make install

Una vez hecho esto se instalan las librerías con chip RTL, Boost, Python, C, C++, Qt y otros.

python-dev libfftw3-dev libcppunit-dev fort77 sdcc sdcc-libraries python-wxgtk2.8 git-core guile-1.8-dev libqt4-dev python-numpy ccache python-opengl libgsl0-dev python-cheetah python-lxml doxygen qt4-dev-tools libqwt5-qt4-dev libqwtplot3d-qt4-dev pyqt4-dev-tools python-qwt5-qt4

cmake libusb-1.0-0-dev libitpp-dev libitpp-doc libitpp7 libitpp7-dbg libboost-wave1.49-dev libboost-wave1.49.0 libboost-system1.49-dev libboost-signals1.49-dev libboost-signals1.49.0 libboost-regex1.49-dev libboost-regex1.49.0 libboost-graph1.49.0 libboost-graph1.49-dev libboost1.49-dbg libboost1.49-doc libboost1.49-dev libboost1.49-all-dev

Una vez finalizada la actualización de bibliografía instalaremos rtl-sdr:

:~$sudo git clone git://git.osmocom.org/rtl-sdr.git
:~$ cd rtl-sdr/
:~$ sudo mkdir build
:~$ cd build
:~$ sudo cmake ../
:~$ sudo make
:~$ sudo make install
:~$ sudo ldconfig

El rtl-sdr opera con un "dongle" que posea *chip set RTL2832U*, para más información de la herramienta ingrese a osmo.com, arquitectos y diseñadores de la herramienta.

Para confirmar la correcta instalación de la herramienta se digita el comando: *"~$ sudo rtl_test*" y será devuelto el siguiente pantallazo:

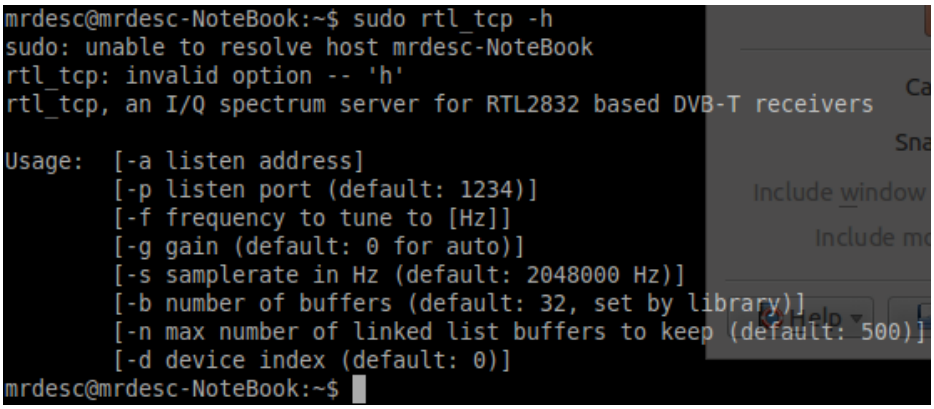


Figura 4. Confirmación de configuración correcta

Una vez terminado este proceso tendremos un rtl-sdr con las siguientes herramientas:

rtl_adsb: Captura el broadcast aéreo enviado por las aeronaves en modo S, para evitar colisiones aéreas, y mejorar el control del tráfico aéreo.

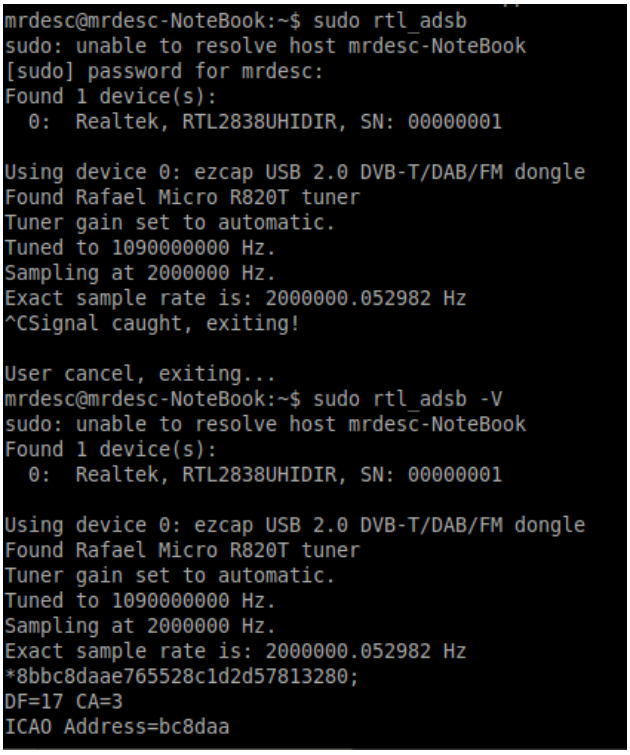


Figura 5. Descripción rtl_adsb

rtl_eeprom: que sirve para identificar la versión y características del equipo utilizado para la capturar datos.

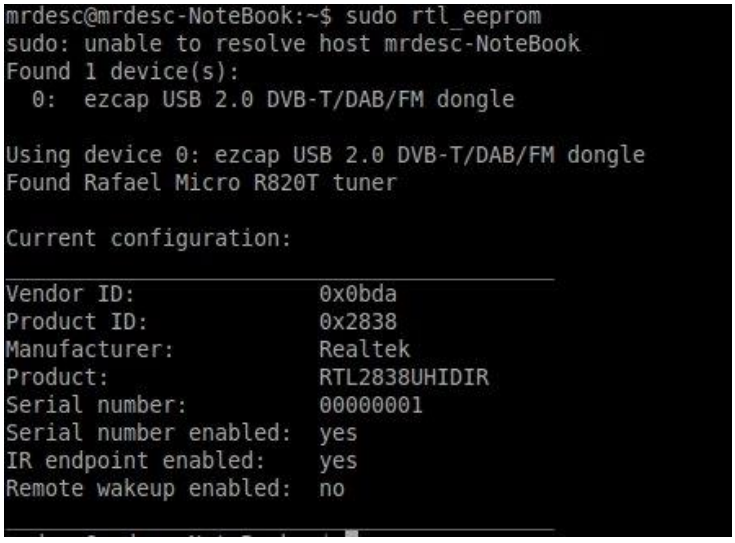


Figura 6. Descripción rtl_eeprom

rtl_fm: Permite hacer captura de datos que están modulados en FM, decodificarlos y reproducirlos:

Figura 7. Descripción rtl_fm

rtl_sdr: Permite capturar señales en frecuencias aleatorias, y además de ello modificar la ganancia del dispositivo.

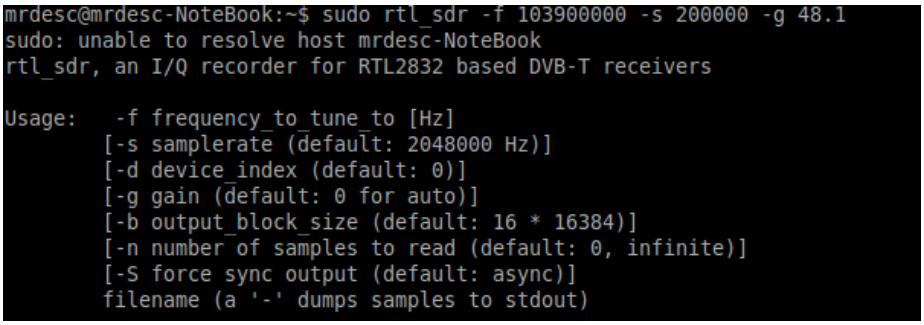


Figura 8. descripción rtl_sdr

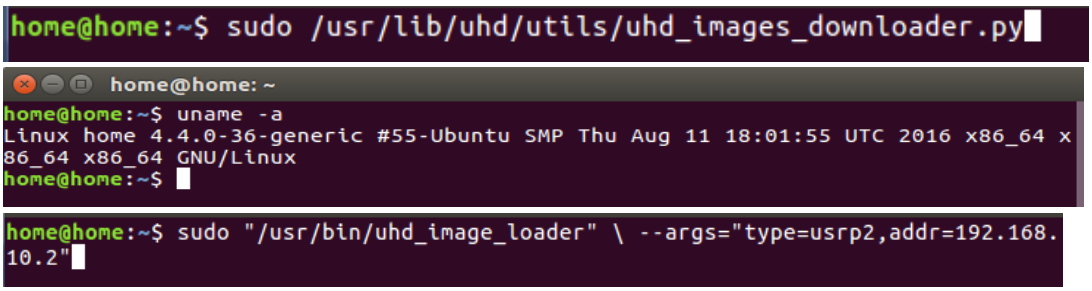
Como complemento se deben instalar las funciones gr-baz, mkdir build, make, que actúan como biblioteca y prerrequisitos necesarios para correr el programa diseñado. Par instalar se deben ingresar los siguientes comandos:

~/build/gr-baz)

:~sudo make install

:~sudo ldconfig

A continuación, se presentan los comandos ejecutados en consola de Ubuntu necesarios para la configuración del radio USRP (drivers). Descarga de imagen y conexión al equipo.



3.1.2 Resultados del Laboratorio Virtual

Después de realizar la instalación del software libre GNU-Radio, su pantalla de inicio (ver Figura 9. Interfaz gráfica de inicio GNU-Radio) muestra las opciones de los bloques para configurar las variables y las librerías dependiendo del proyecto que se vaya a ejecutar.

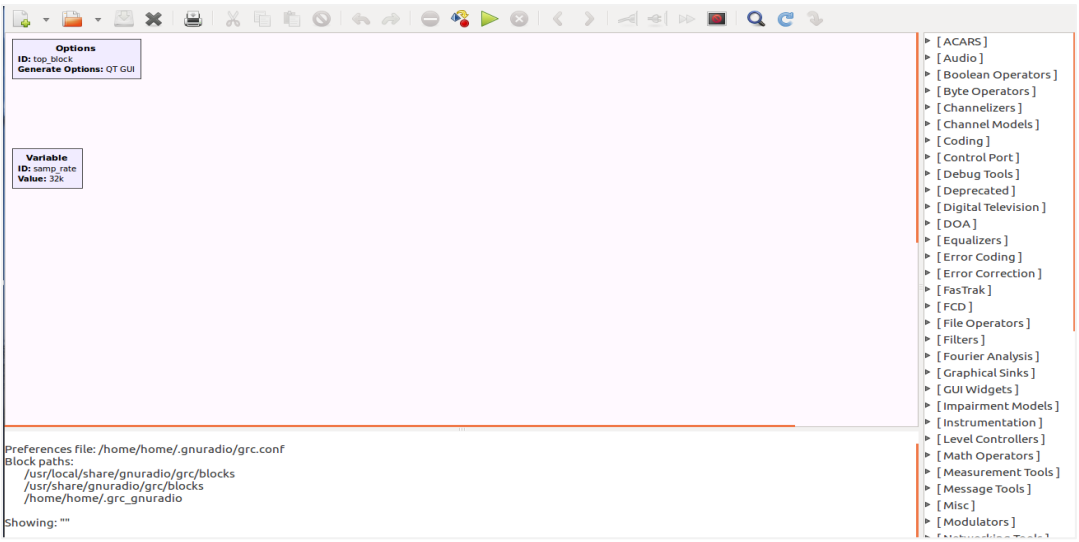


Figura 9. Interfaz gráfica de inicio GNU-Radio

3.1.3 Conexión y configuración de Hardware

En la siguiente fotografía, se observa el PC de la izquierda conectado con la antena RTL-SDR (con set USB RTL2832U) la cual actúa como receptora; y en el PC de la derecha se encuentra conectado el radio USRP, el cual es encargado de transmitir y modular las señales. En ambos PC's se ya encuentra instalado el laboratorio virtual.

Figura 10. Conexión de hardware para laboratorio virtual

La conexión del radio USRP al PC se debe establecer a través del puerto Ethernet y realizar configuración previa de protocolos de comunicación configurando la tarjeta de red del PC con la dirección IP del equipo USRP.

Figura 11. Conexión del radio USRP

La forma de conexión de la antena RTL-SDR es a través del puerto USB y no debe realizarse ninguna configuración ya que viene configurada de fábrica. Sin embargo, viene con CD de instalación dependiendo del sistema operativo.

Figura 12. Conexión antena omnidireccional RTL-SDR, con set USB RTL2832U

3.1.4 Transmisor de señal FM

Una vez instalado el laboratorio virtual, se procede a utilizarlo transmitiendo una señal FM a través del radio USRP.

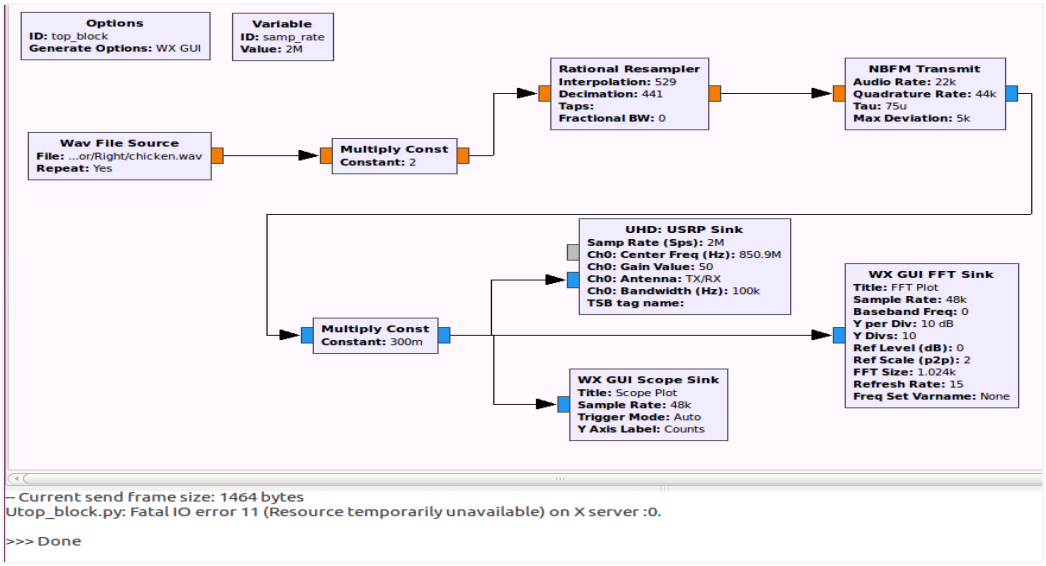


Figura 13. Diagrama de bloques del Transmisor FM

En la Figura 13 se muestra el proceso de emulación de una señal de audio sobre una frecuencia portadora de transmisión la cual está dentro del rango de señales FM, además será transmitida por medio de un equipo de radio USRP y una antena omnidireccional del rango de los 800 MHz hasta los 1,65 GHz, con el cual se inicia laboratorio de transmisión FM.

3.2 Objetivo 2: Generación de Señales Inhibidoras

3.2.1 Jammer de señal GPS Análogo (Diseño base)

El siguiente es un montaje para un inhibidor de sañal GPS análogo, el cual fue programado con funciones análogas, sin embargo, este no lograba bloquear el 100% de las señales GPS, pero fue un paso importante para programar el inhibidor vectorial que veremos en la siguiente sección que funciona usando funciones digitales.

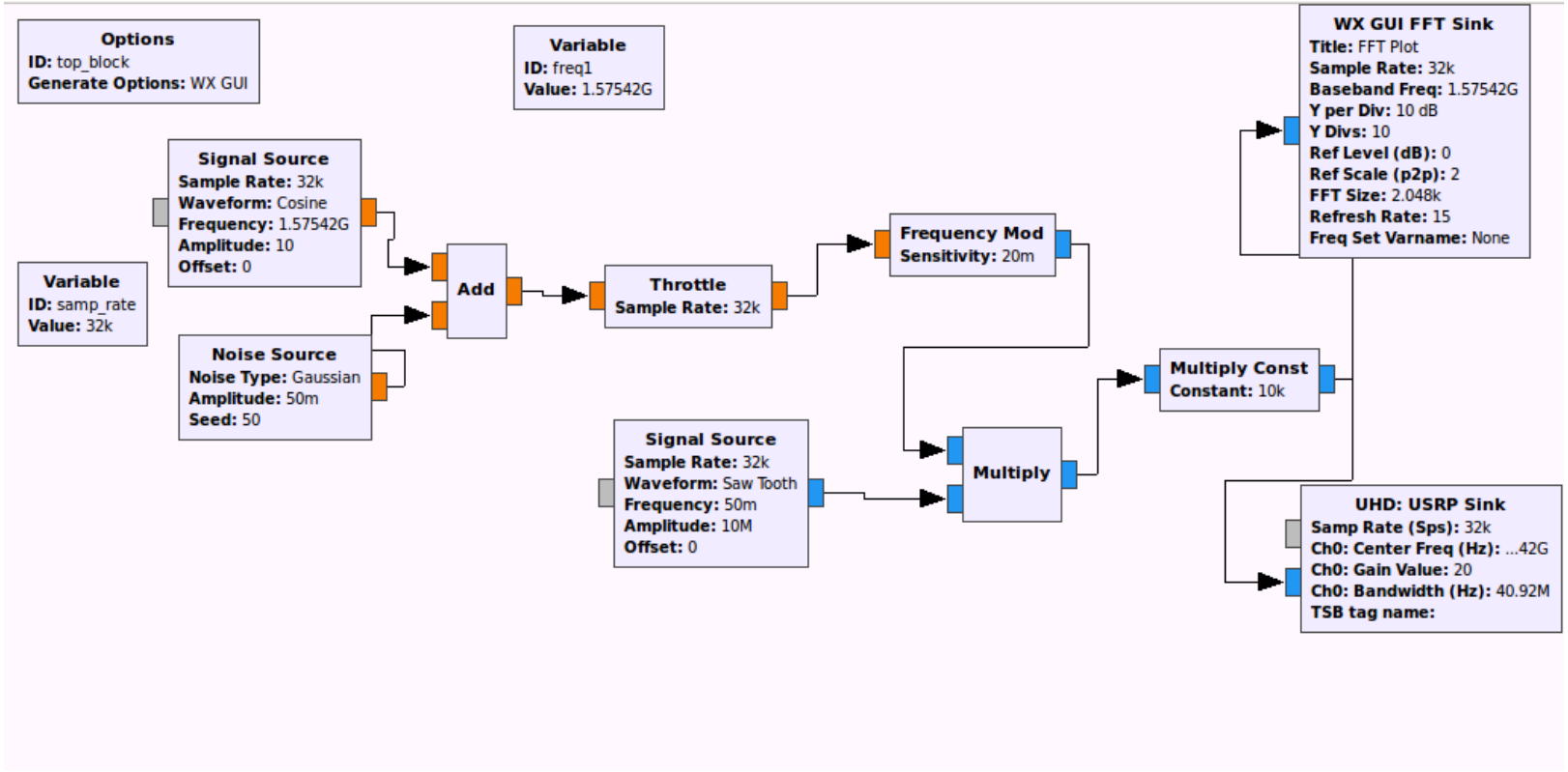


Figura 14. Diagrama del jammer GPS Análogo

A continuación, se presenta una descripción de los componentes usados en el diseño del inhibidor de señal GPS análogo. Algunos de estos bloques también se usan en los siguientes diseños debido a que son bloques básicos en lectura, escritura y procesamiento de las señales.

Signal Source: Se utiliza para generar una variedad de señales como: Seno, Coseno, Cuadrado, Triángulo y Diente de sierra, las cuales presentan un tipo de salida como: Complejo que presenta una salida de valor complejo, Flotante que tiene una salida de valor real, Entero (*Int*) en el cual la salida es un número entero de 32 bits, y por último, un Entero corto *(Short*) el cual extrae un número entero de 16 bits. Estas señales presentan una frecuencia de tipo real mediante la cual se especifica la frecuencia de salida de la fuente de señal, del mismo modo presentan una amplitud de tipo real especificando la amplitud de pico para el seno y el coseno, o la amplitud pico a pico en el caso de las señales cuadrada, triángulo y el diente de sierra.

Cada una de las señales tiene una amplitud de pico generado por el parámetro de amplitud y el valor establecido por el parámetro, por ejemplo, en las señales Seno y Coseno la salida es una onda sinusoidal con una amplitud establecida por el parámetro, y un valor medio establecido por el parámetro de Offset, en la señal Cuadrada la salida es una onda cuadrada con un valor establecido por Desplazamiento + Amplitud / 2, este parámetro también se establece para la señal Triangular, y la señal Diente de sierra donde la salida es una onda de diente de sierra continua positiva.

Noise Source: Se encarga de implementar una fuente de ruido con la capacidad de seleccionar una distribución del ruido de varias distribuciones estándar. Los tipos de ruido son: Uniforme, el cual presenta una distribución uniforme del ruido, Gaussiano el cual selecciona una distribución de Gauss, Laplaciano con una distribución de Laplace y, por último, el Impulso seleccionando una distribución en forma de impulso. Estas fuentes de ruido presentan una amplitud de salida de tipo real y una semilla de tipo Int estableciendo la semilla para el generador de números aleatorios utilizado para crear la fuente de ruido.

Throttle: Limita la transferencia de datos a la velocidad de muestreo especificado para evitar que GNUradio consuma todos los recursos de la CPU cuando el flowgraph no está siendo regulado por hardware externo, es decir: audio de fuente, drenaje *(Drain*) o fuente USRP. Throttle presenta una frecuencia de muestreo de tipo real y un vector longitud de tipo int encargado de especificar la longitud del vector para el procesamiento vectorial.

Frequency Modulation: es la codificación de información en una onda portadora mediante la variación de la frecuencia instantánea de la onda. Los datos digitales pueden ser codificados y transmitidos a través de FM por desplazamiento de la frecuencia de la portadora entre un conjunto predefinido de frecuencias que representan dígitos, una frecuencia puede representar un binario 1 y un segundo puede representar binario 0. Con el fin de ser capaz de extraer toda la información transportada por una señal de FM, es necesario pasar a través de un demodulador, donde la salida de esta etapa proporciona la información que fue transportada por la señal de FM la cual puede dar una mejor relación señal-ruido cuando se utiliza banda ancha, permitiendo que el ruido de amplitud se puede eliminar mediante la limitación de la señal para eliminarlo. Dado que el nivel de desviación es importante para determinar el ancho de banda de la señal, como resultado, la desviación que se utiliza para FM es diferente entre las aplicaciones.

Multiply: Implementa la función IN0 = x in1 x ... x en (N-1) con entradas num de tipo Int las cuales especifican el número de entradas etiquetadas IN0 a través de (N-1), además, presenta un vector longitud del mismo tipo especificando la longitud del vector para el procesamiento vectorial.

Multiply Const: Implementa la función de salida = x constante, la cual especifica la constante de multiplicar con la entrada, presenta también un vector longitud de tipo inti detallando la longitud del vector para el procesamiento vectorial.

3.2.2 Jammer de señal GPS Vectorial (Definitivo)

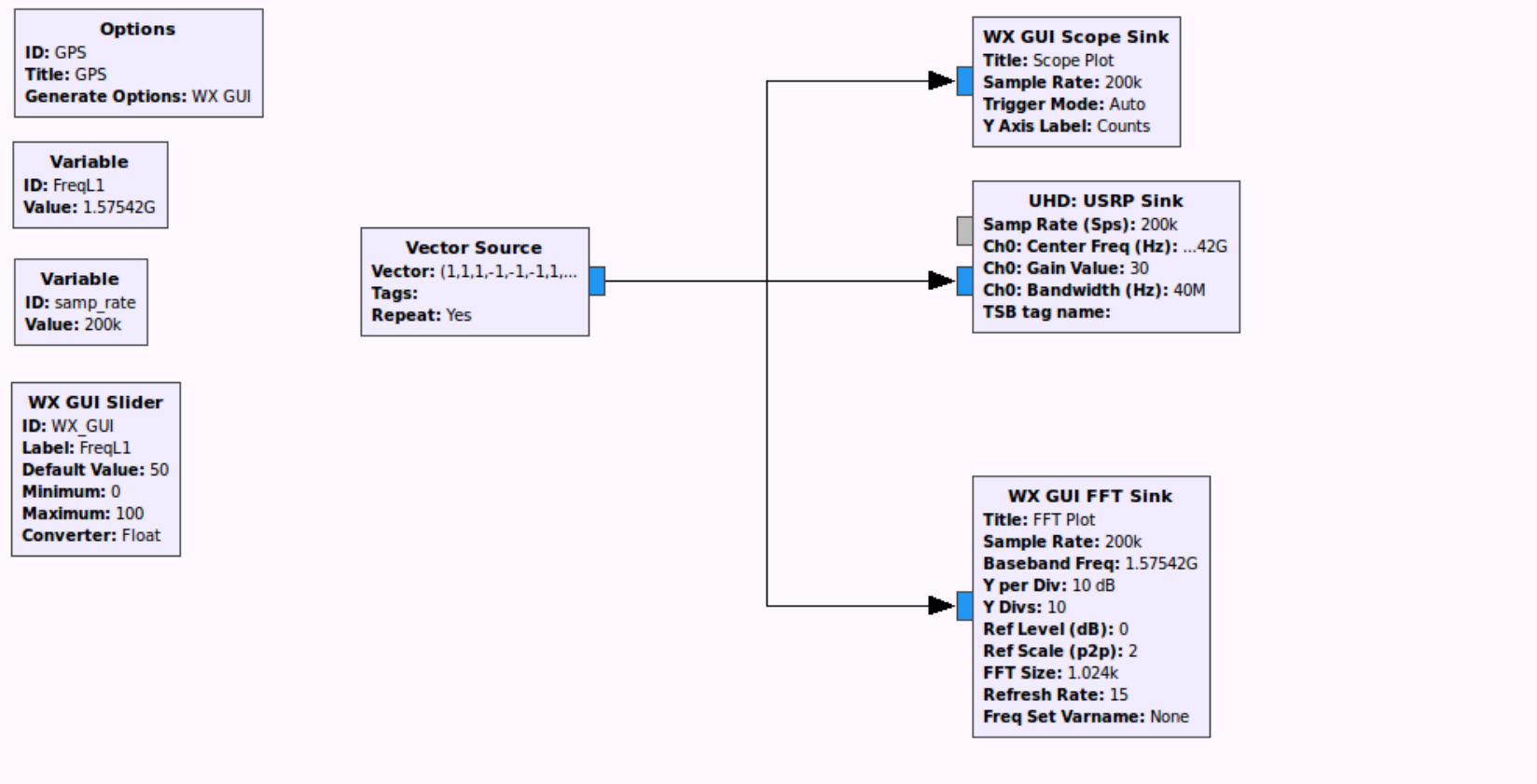


Figura 15. Diagrama del jammer GPS Vectorial

La Figura 15, muestra un inhibidor de señal GPS Vectorial, en este diseño se utilizaron funciones digitales para realizar la inhibición de las señales GPS. De esta forma se logró un mejor bloqueo de la señal GPS, eliminando el 100% de los satélites capturados por el celular usado como equipo de pruebas para confirmar la inhibición. Los bloques usados en este diseño se describen a continuación. Algunos bloques que aparecen en el diseño y no están descritos en esta sección, es debido a que están descritos en la sección anterior donde se presentó el diseño del inhibidor de señal GPS análogo.

Vector Source: Proporciona una fuente de características para capas vectoriales mostrando diferentes formas de cargar la información utilizando una clase de origen vectorial.

WX GUI FFT Sink: Es utilizado para encontrar los componentes de frecuencia de una señal y el ruido presente. Permite analizar de manera específica porciones del espectro usando la FFT. Este bloque convierte una señal de su dominio original (a menudo el tiempo o espacio) a una representación en el dominio de la frecuencia y viceversa. Una FFT calcula rápidamente la transformada de Fourier al factorizar la matriz DFT en un producto de escaso factores (en su mayoría cero), como resultado, se consigue reducir la complejidad de cálculo de la DFT que surge al aplicar simplemente la definición de DFT .

Wav file source: Crea una fuente de datos de un archivo de onda de audio. Este archivo puede ser capturado en GNU Radio con un disipador de archivo de Wav o creado en un editor de audio como Audacity.

Multiply const: este bloque implementa la función de multiplicación de una constante C o por una señal X, según la especificación.

USRP sink: es generador de la onda de radio que permite emitir la señal con la frecuencia especifica, al USRP conectado al PC con Ethernet usando la dirección IP.

3.3 Objetivo 3: Detección de Señal Inhibidora

Para realizar un laboratorio virtual de detección de señales inhibidoras, se planteó la generación de una señal usando el USRP quien realiza las funciones de Jammer y la detección es a través del RTL-SDR 2832. Para producir la señal inhibidora del USRP se usa el transmisor FM de la Sección 3.1.4, es decir, que para este laboratorio se emula un Jammer FM.

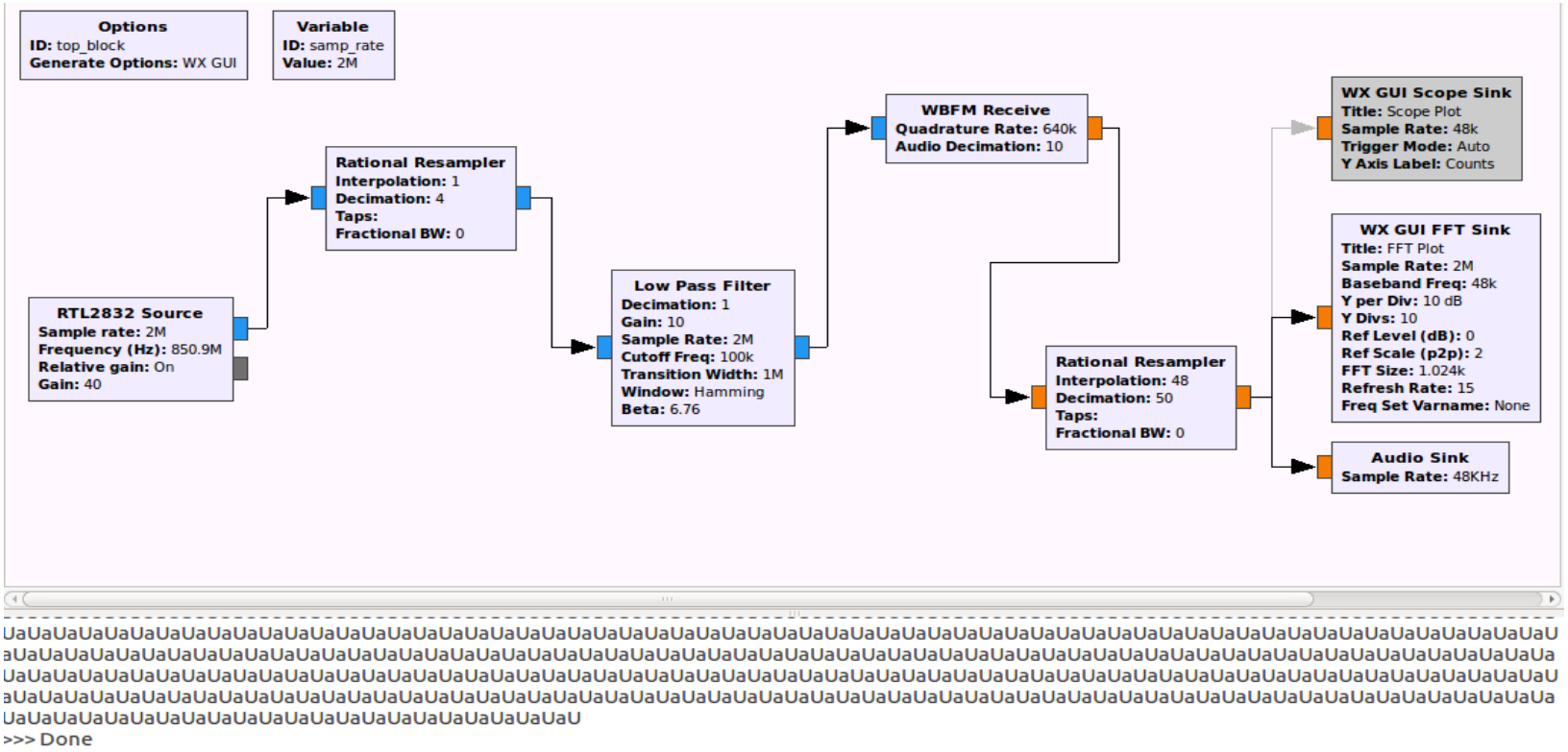


Figura 16. Diagrama de bloques del Receptor FM.

La Figura 16 muestra el esquema de recepción de señales FM que es utilizado para de detección del inhibidor de las señales. Las señales son recibidas en este diseño usando el RTL-SDR 2832. Con este receptor de bajo costo podemos capturar señales en un rango amplio desde FM hasta señales de televisión como se describe en el marco teórico. De esta manera, es posible analizar las señales adquiridas y es posible detectar si existe algún inhibidor de señales en el rango de frecuencias de este receptor.

El diseño permite capturar las señales FM y mostrarlas en dominios del tiempo y la frecuencia lo que permite su análisis. En este diseño se observan los bloques que no se usaron en los diseños anteriores y serán explicados a continuación.

Rational Resampler: Combinado interpolación y decimación, este bloque se utiliza para convertir de una frecuencia de muestreo a otra, siempre que puedan estar relacionados por una relación: Fs_out = Fs_in x interpolación / decimación a la frecuencia que le llega.

Low Pass Filter: es un filtro que permite el paso de señales de menor frecuencia hasta una frecuencia definida de corte. La frecuencia de corte se puede ingresar como parámetro y así poder definir diferentes filtros. En este diseño el filtro opera a una frecuencia de corte de 100 KHz, valor que resulta igual a la mitad del ancho de banda comercial de una emisión de una estación de radio FM.

Audio Sink: Permite reproducir audio en auricular o altavoces estéreo. Existen varios tipos de auriculares los cuales se resumen en el siguiente cuadro con su respectiva aplicación.

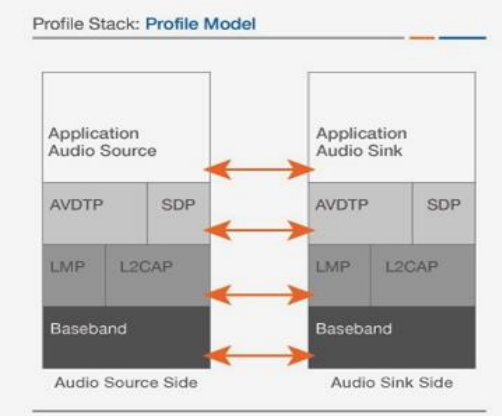


Figura 17. Describe el comportamiento de Audio Sink

WBFM Receive: es un bloque que toma una señal de frecuencia modulada (FM) y la demodula. La tasa de cuadratura son la tasa de muestreo de entrada y la señal de salida. Se puede dar cualquier valor de la desviación máxima, siempre y cuando sea mayor de 20 kHz que es el componente de frecuencia más alto de la señal.

4. RESULTADOS Y DISCUSIÓN

En el presente proyecto se mostraron los avances obtenidos con relación al inhibidor de radiofrecuencias generando un bloqueo de frecuencia a través del equipo USRP en el rango de GPS.

Se procede entonces a interferir a los satélites L1 de uso comercial, los cuales permiten conectarse y generar una triangulación para establecer la posición del equipo GPS que lo requiere. Para visualizar varios de los satélites con los que se pueden establecer conexión se utiliza la aplicación libre llamada GPS Test. Para fijar la posición de un equipo receptor se requiere de mínimo un posicionamiento con tres satélites, establecido esto, se muestra por medio de la aplicación el rango de satélites señalados y una conexión de la misma hora con relación al teléfono, de esta manera el equipo se encuentra en trasmisión.

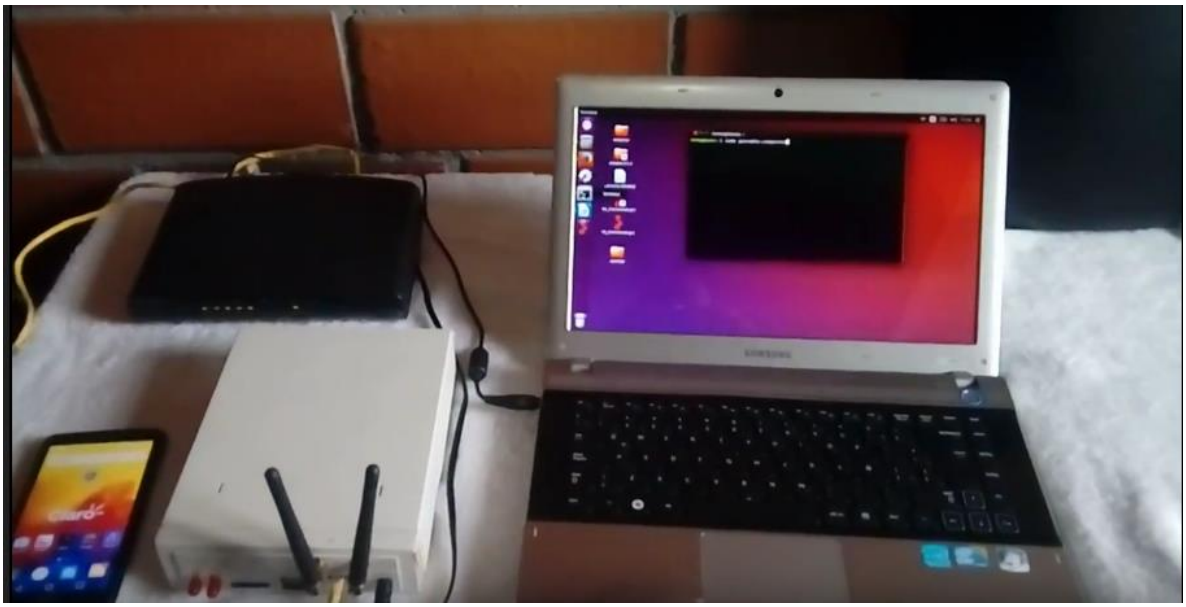


Figura 18. Elementos empleados en la inhibición de señales GPS

Mediante el software libre GNU-Radio y la operatividad a través del radio USRP se busca realizar la inhibición de los satélites GPS. Para esto, primero se ingresa por la terminal de Linux y lanzar el aplicativo GNU Radio con los permisos necesarios. Dentro de la aplicación se buscan los diagramas de bloques previamente diseñados.

Los primeros resultados que se presentan son del inhibidor de señales GPS vectorial, con el vector y varios armónicos previamente definidos, estas señales tienen una amplitud pico a pico entre 1 y -1 (ver Figura 20), los cuales permiten generar un bloque adecuado de la señal GPS y evitar la conexión del celular con los satélites. Posteriormente, se le da correr al programa e inmediatamente se empiezan a verificar los satélites, para confirmar la perdida de conexión de los mismos lo que se ve en el celular mediante la aplicación GPS Test (ver Figura 19, que muestra la desconexión de los satélites, hasta no encontrar satélites disponibles en el momento. En la Figura 21 se observa la señal inhibidora en el dominio de la frecuencia.

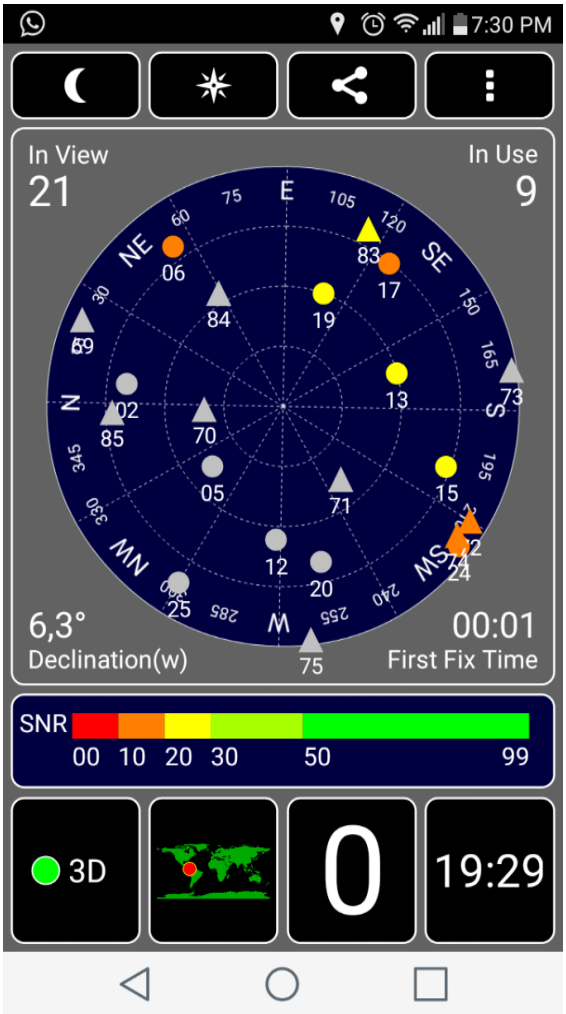


Figura 19. Aplicación GPS Test

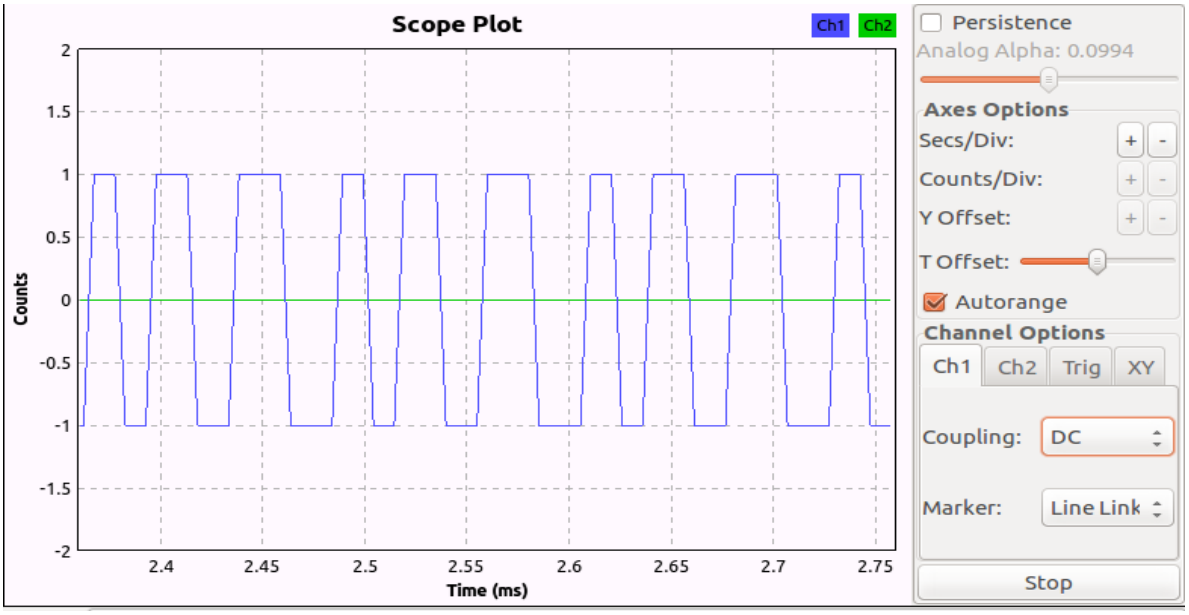


Figura 20. Señal inhibidora de GPS en el dominio del tiempo

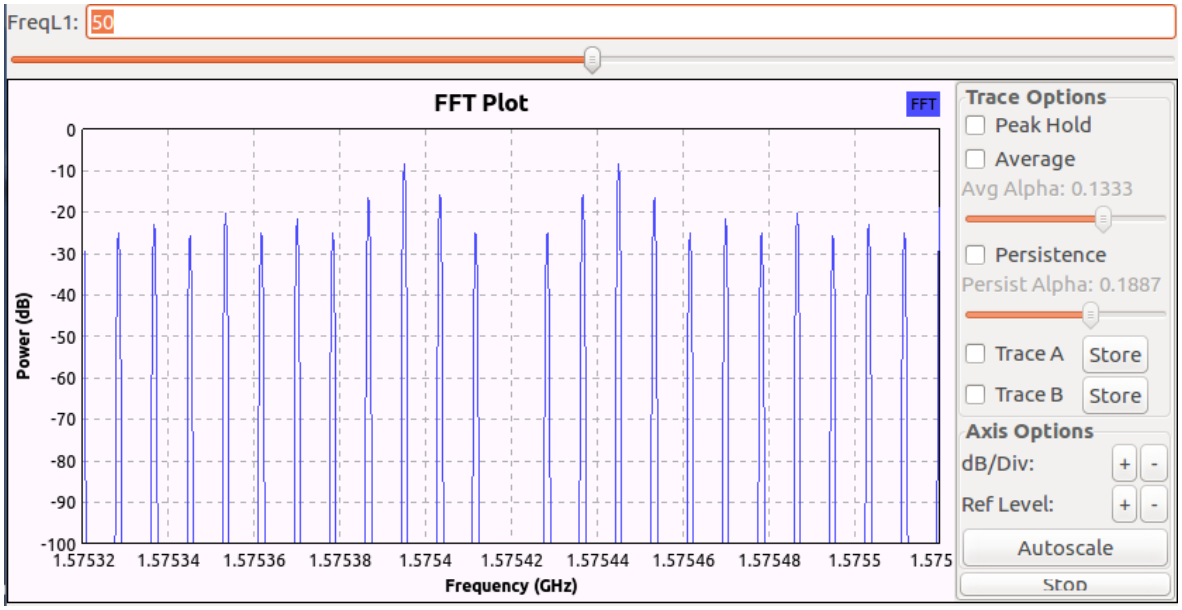


Figura 21. Espectro de frecuencias de la señal inhibidora de GPS

Al detener el programa, se genera una reposición de aquellos satélites que habían estado fuera de alcance, como se había mencionado anteriormente, se necesitan tres satélites en funcionamiento, además, la frecuencia que se genera debe buscar primero el satélite para poder generar la triangulación, mediante esto la aplicación buscara los satélites disponibles y los que están en uso para así establecer conexión, el dispositivo móvil tarda entre 60 y 90 segundos en reestablecer nuevamente la señal y encontrar un posicionamiento con los satélites alrededor.

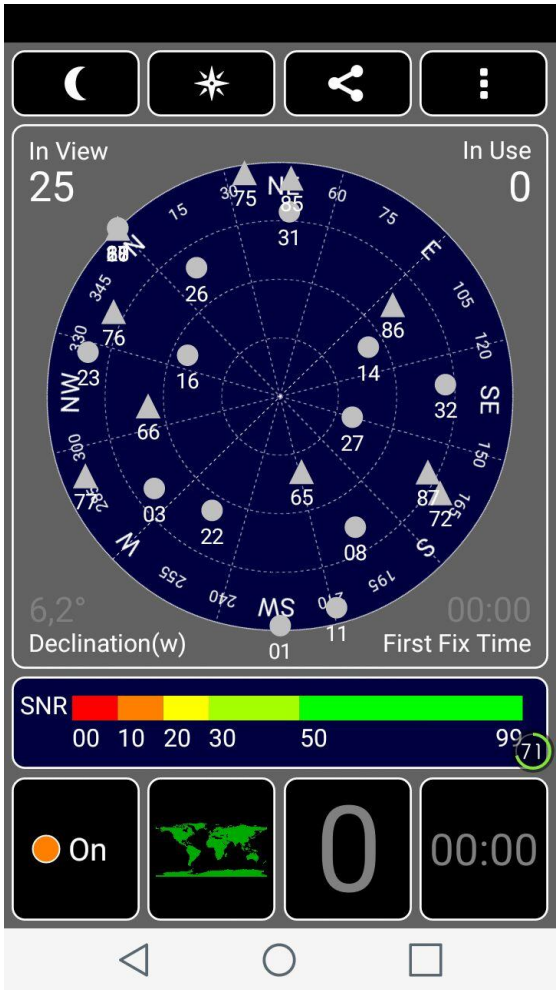


Figura 22. Perdida de la señal GPS

De esta manera, se puede comprobar que el laboratorio virtual puede usarse para la generación de señales inhibidoras de GPS, la trasmisión y recepción de la señal a través de GNU Radio y USRP.

Por otro lado, al momento de ejecutar la transmisión de la señal FM se obtienen dos tipos de graficas: muestreo en el dominio del tiempo y potencia en el dominio de la frecuencia. En esta figura se puede observar en el cuadro superior como en un osciloscopio la señal en el dominio del tiempo y en el inferior la transformada de Fourier, ver Figura 23 .

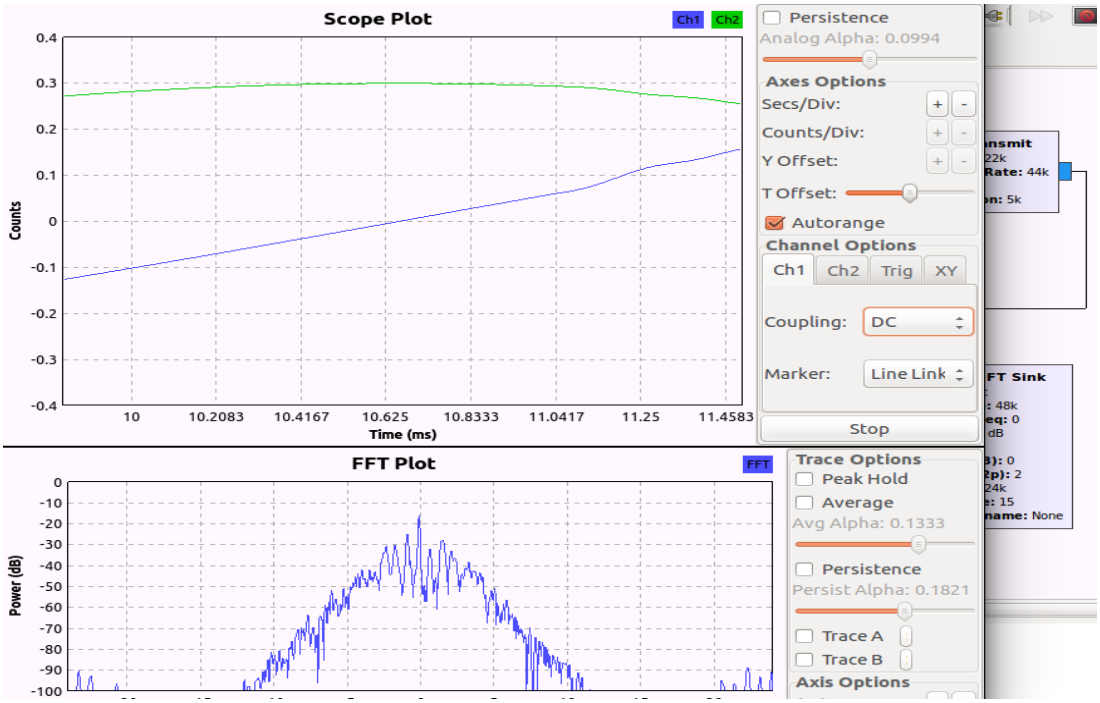


Figura 23. Transmisión de señal FM.

Análogamente, se presenta la gráfica de potencia (dB) en función de la frecuencia, ver Figura 24.

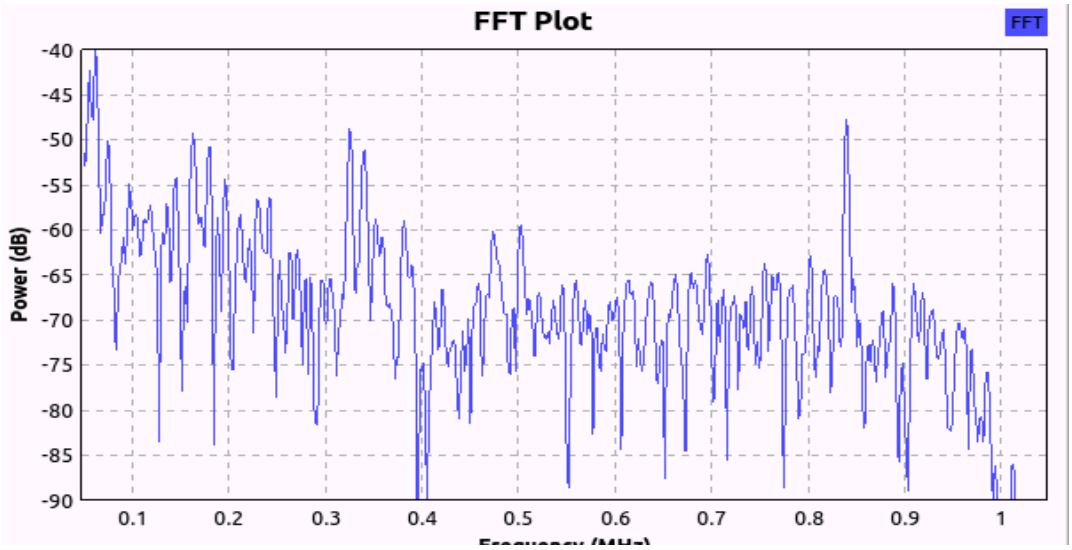


Figura 24. Recepción de señal en rango MHz por el RTL-SDR, con set USB RTL2832U.

La Figura 25, muestra el momento en que se recibe la señal de FM. La señal de color verde es la señal que fue tomada mientras el USRP estaba enviando la señal inhibidora FM, la señal azul es cuando el USRP deja de transmitir la señal inhibidora. En esta forma básica

usando la FFT, y analizando la gráfica ya sea en forma visual o a través de un algoritmo automático de clasificación, es posible detectar cuando se encuentra presente un Jammer en nuestra área de cobertura.

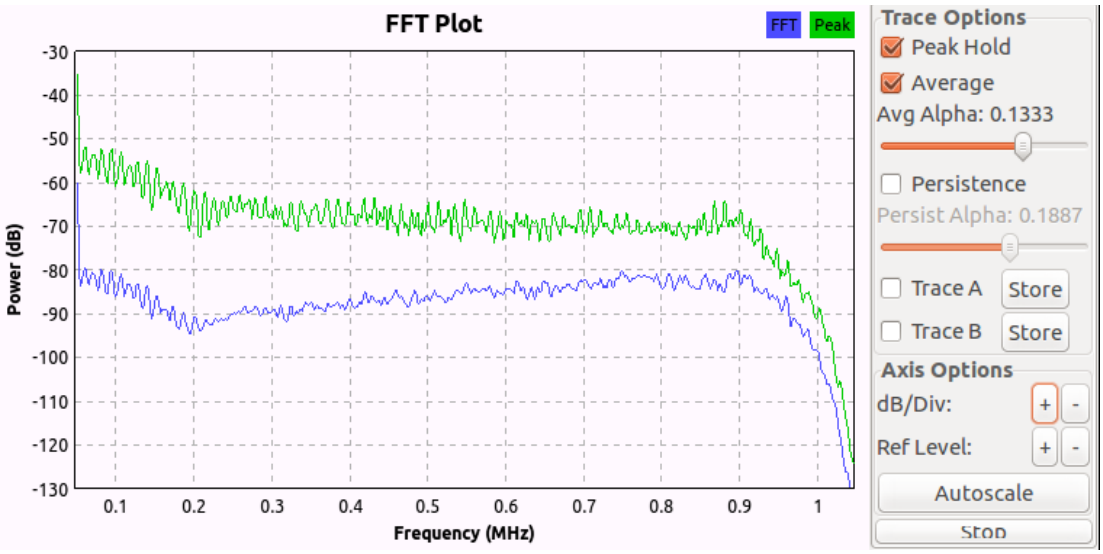


Figura 25. Espectro de frecuencias de la detección de la señal inhibidora.

5. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

Como resultado de la investigación acerca de los inhibidores de radiofrecuencia jammer presentada, se logró simular con éxito el laboratorio virtual implementado con el USRP, RTL-SDR y el software libre GNU-Radio a través de Linux, proporcionando un bloqueo eficaz de la señal GPS, proceso que pudo ser comprobado al usar una aplicación de celular que permite ver los satélites GPS.

Mediante el software GNU-Radio y la operatividad del radio USRP se obtuvo diagramas de bloques que permiten emular tanto señales inhibidoras por medio de un vector de armónicos generando eficazmente el muestreo para inhibir la señal GPS, como adquisición de señales que permitan el análisis de las mismas para realizar detección de señales deseadas.

Como trabajo futuro se propone la implementación de trabajos de grado con el fin de emular la inhibición no solo de señales GPS y FM, sino también señales WI-Fi y teléfonos móviles además de emular los detectores de señales inhibidoras y realizar el antijammer.

REFERENCIAS

Araujo, D., & Santos, J. (29 de octubre de 2007). A dual band steerable cell phones jammer. Obtenido de IEEE.

Divya, E., & Coll., E. E. (15 de marzo de 2012). Design of user specific intelligent cell phone jammer. Obtenido de IEEE.

Fang, S., & Liu, Y. (3 de febrero de 2015). Wireless Communications under Broadband Reactive Jamming Attacks. (IEEE, Ed.)

Garcia Angel Jesus, Pineda Jose Adan, Rojas Daniel Isaias. (2011). Estrategias de "Jamming". DISEÑO Y ELABORACIÓN DE UN JAMMER (p.66). Mexico: INSTITUTO POLITÉCNICO NACIONAL.

GNURadio.org. (6 de julio de 2013). gnuradio.org. (D. Carrillo, Editor) Recuperado el 2015, de https://gnuradio.org/redmine/projects/gnuradio/wiki/EnEspanol

Huang, H. (2011). On a New Type of Denial of Service Attack in Wireless Networks: The Distributed Jammer Network. IEEE.

Livieri, S., & Higo, Y. (mayo de 2007). Analysis of the Linux Kernel Evolution Using Code Clone Coverage. IEEE.

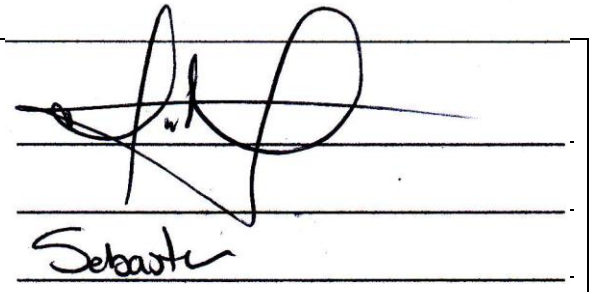
MINTIC. (2013). Ministerio de Tecnologías de Información y Comunicación de Colombia. Obtenido de http://www.mintic.gov.co/portal/604/w3-article-4287.html

Patel, I. (2012). Intelligent FM signal jamming system. IEEE.

Sambhe, V., & Kale, D. (16 de julio de 2008). Antenna for Mobile Phone Jammer. IEEE.

Universidad de las Américas Puebla. (2013). *Descripción de Jamming.* Puebla, México. Obtenido de http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/nocedal_d_jm/capitulo3.pdf

Vachhani, K., & Mallari, R. (10 de agosto de 2015). Experimental study on wide band FM receiver using GNURadio and RTL-SDR. (IEEE, Ed.)

FIRMA ESTUDIANTES 

FIRMA ASESOR 

FECHA ENTREGA: 13 de octubre de 2016

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

RECHAZADO___ ACEPTADO____ ACEPTADO CON MODIFICACIONES_____

ACTA NO._____

FECHA ENTREGA: _____

FIRMA CONSEJO DE FACULTAD_____

ACTA NO._____