

**INHIBICIÓN DE SERVICIOS DE RADIODIFUSIÓN SONORA EN LA
BANDA DE FM USANDO LA TECNOLOGÍA SOFTWARE DEFINED
RADIO (SDR) E INTERNET OF THE THINGS (IOT)**

LUIS MIGUEL DÍAZ MORALES

**UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICOMECAÑICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y
TELECOMUNICACIONES
BUCARAMANGA**

2019

**INHIBICIÓN DE SERVICIOS DE RADIODIFUSIÓN SONORA EN LA
BANDA DE FM USANDO LA TECNOLOGÍA SOFTWARE DEFINED
RADIO (SDR) E INTERNET OF THE THINGS (IOT)**

LUIS MIGUEL DÍAZ MORALES

**Trabajo de grado presentado como requisito parcial para optar al título de
Magíster en ingeniería de Telecomunicaciones**

**Director
Homero Ortega Boada
Ph.D. En Ciencias de la Ingeniería**

**UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICOMECAÑICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y
TELECOMUNICACIONES
BUCARAMANGA**

2019

CONTENIDO

	pág.
INTRODUCCIÓN	13
1. OBJETIVOS	18
1.1. GENERAL	18
1.2. ESPECÍFICOS	18
1.3. ALCANCES	18
2. MARCO CONCEPTUAL	20
2.1. EL INTERNET DE LAS COSAS (IoT)	20
2.2. RADIO DEFINIDA POR SOFTWARE (SDR)	22
2.3. MODELO GENERAL DEL SISTEMA USANDO SDR E IoT	24
3. PROCESO DE IDENTIFICACIÓN DE REQUISITOS Y DEL DISE- ÑO FUNCIONAL	29
3.1. INGENIERÍA DE REQUERIMIENTOS	29
3.1.1. Descripción general	29
3.1.1.1. Perspectiva del producto	29
3.1.1.2. Funciones del producto	30
3.1.2. Características del usuario	30
3.1.3. Definición de restricciones para la versión piloto	31
3.1.3.1. Aspectos legales sobre los bloqueadores en Colombia	31
3.1.4. Requisitos específicos	32
3.1.4.1. Interfaces de usuario	32
3.1.4.2. Componentes hardware	32
3.1.4.3. Interfaces de software	32
3.1.4.4. Interfaces de comunicaciones	33
3.1.5. Requisitos funcionales	33
3.1.5.1. Diagrama de casos de uso	33
3.1.5.2. Modo usuario general	33

3.1.5.3. Modo administrador de sistema de inhibición	34
3.2. PROCESO DE DISEÑO	36
3.2.1. Diagrama de secuencia	36
3.2.2. Diagrama de clases	39
3.2.3. Diagrama de máquina de estados	41
3.3. INTERFAZ DE USUARIO	45
 4. SOLUCIÓN A NIVEL DE CAPA IOT	 46
4.1. TERMINAL IOT	46
4.1.1. Caracterización de los dispositivos SDR	46
4.1.1.1. Características de los dispositivos SDR	47
4.1.1.2. Modo de operación de sensado del espectro	49
4.1.1.3. Modo de operación de bloqueadores del espectro	53
4.1.1.4. Modelo de bloqueadores cooperativos	54
4.1.1.5. Señales usadas en la red de bloqueadores	56
4.1.1.6. Bloqueo usando tonos	56
4.1.1.7. Bloqueo usando ruido blanco gaussiano	57
4.1.1.8. Multiplexión por División de Frecuencias Ortogonales (OFDM)	57
4.1.1.9. Ruido modulado en FM	58
4.1.1.10. Tono modulado en FM	59
4.1.1.11. Análisis de bloqueo de emisiones clandestinas de radiodifusión sonora en FM que operan en la banda VHF 88-108 MHz	59
4.1.1.12. Simulación del sistema de bloqueo usando diferentes señales interferentes	59
4.1.1.13. Análisis de ancho de banda de las señales usadas para la red de bloquea- dores	65
4.1.1.14. Efecto de interferencia con canales adyacentes	70
4.1.1.15. Análisis de bloqueo cooperativo	74
4.2. CAPA DE ACCESO	80
4.3. CAPA DE GESTIÓN DE DISPOSITIVOS	80
 5. LOS COMPONENTES DE NUBE	 82
5.1. PROCESAMIENTO DE SEÑALES PARA IDENTIFICAR EMISIONES CLANDESTINAS A NIVEL DE BACKEND	82

5.1.1. Métodos de sensado implementados	82
5.1.1.1. El Detector de Energía	82
5.1.1.2. Propuesta para la implementación práctica del detector de energía . .	84
5.1.1.3. Detector de picos basado en los coeficientes de la transformada <i>Wavelet</i>	87
5.1.1.4. Identificación de emisiones clandestinas basado en Transformada <i>Wavelet</i>	89
5.2. ANÁLISIS DEL SENSADO COOPERATIVO	91
5.2.1. Estudio de sensibilidad	92
5.2.2. Estudio de la precisión	95
5.3. BASE DE DATOS	96
 6. CONCLUSIONES	 100
 7. TRABAJO FUTURO	 101
 BIBLIOGRAFÍA	 102

LISTA DE FIGURAS

	pág.
1. Estructura general en modo recepción de la componente de radio de un equipo SDR.	25
2. Estructura general en modo transmisión de la componente de radio de un equipo SDR.	25
3. Modelo general de la plataforma IoT para aplicaciones de SDR.	27
4. Equipos utilizados	28
5. Diagrama de casos de uso para el modo usuario general.	34
6. Diagrama de los Casos de uso para el modo usuario administrador	35
7. Diagrama de secuencia del sistema de inhibición.	37
8. Diagrama de clases comunicación entre el servidor y los dispositivos de la red, almacenamiento y funciones de los dispositivos.	40
9. Diagrama de clases para el procesamiento de los datos del espectro, y el reporte de los mismos.	42
10. Diagrama de clases para el registro, consultas y acceso.	43
11. Diagrama Maquinas de estado para el monitoreo y bloqueo.	44
12. Montaje experimental para encontrar la relación entre la ganancia del UHD y la potencia de salida del dispositivo E310	48
13. Relación existente entre la ganancia del UHD y la potencia medida con el analizador de espectros.	49
14. Diagrama de clases implementado en el terminal IoT.	50
15. Sensado cooperativo centralizado	52
16. Flujograma GNU Radio referente a la clase <code>Scan_spectrum</code>	53
17. Modelo de bloqueadores cooperativos.	55
18. Generación señal OFDM	58
19. Simulación de señal interferente AGWN.	60
20. Simulación de señal interferente OFDM.	60
21. Simulación de ruido gaussiano modulado en FM.	60
22. Múltiples tonos como señal de interferencia.	61

23. Tono modulante en FM como señal de interferencia.	61
24. Simulación de las señales usadas para bloquear.	63
25. Porcentaje de reconocimiento de voz en función de la energía recibida antes de la demodulación.	64
26. Porcentaje de reconocimiento de voz en función de la distancia de correlación.	65
27. Definición de ancho de banda como se formula en el artículo 1, No.1153 del RR.	66
28. Señal simulada y medida del ruido.	68
29. Señal simulada y medida de la OFDM.	68
30. Señal simulada y medida del ruido modulado en FM.	69
31. Señal simulada y medida de un tono modulado en FM.	70
32. Señal simulada y medida de un tono a 10 kHz.	71
33. Canal adyacente bloqueado con una señal de ruido $\mathcal{N}(0, 1)$	71
34. Canal adyacente bloqueado con una señal de OFDM.	72
35. Canal adyacente bloqueado con una señal de ruido modulado en FM.	73
36. Canal adyacente bloqueado con una señal de un tono modulado en FM.	73
37. Canal adyacente bloqueado con una señal de un tono senoidal.	74
38. Modelo general del experimento para comparar las señales usadas por los bloqueadores	75
39. Porcentaje de reconocimiento de voz en función de la energía recibida por el canal para los casos de bloqueo cooperativo y no cooperativo.	77
40. Distancia de correlación en función de la energía del canal	78
41. Porcentaje de reconocimiento de voz en función de la distancia de correlación.	79
42. Picos detectados en el espectro y filtrado basado en el histograma.	90
43. Modelo general del experimento para el análisis del sensado cooperativo.	93
44. Espectro sensado por parte de los equipos de la red.	93
45. Probabilidad de detección en función de C/N.	95
46. Curva ROC del detector de energía.	97
47. Curva ROC del detector de picos.	97
48. Modelo de la base de datos que se implementó en postgresQL.	99

LISTA DE TABLAS

	pág.
1. Requisitos de software para el desarrollo.	33
2. Características generales del equipo SDR.	47

RESUMEN

TÍTULO: INHIBICIÓN DE SERVICIOS DE RADIODIFUSIÓN SONORA EN LA BANDA DE FM USANDO LA TECNOLOGÍA SOFTWARE DEFINED RADIO (SDR) E INTERNET OF THE THINGS (IOT)

AUTOR: LUIS MIGUEL DÍAZ MORALES

PALABRAS CLAVE: INTERNET DE LAS COSAS, RADIO DEFINIDA POR SOFTWARE, MONITOREO DEL ESPECTRO, BLOQUEO DEL ESPECTRO, RADIODIFUSIÓN SONORA.

DESCRIPCION:

Los servicios de radiodifusión sonora son ampliamente usados en los sectores públicos, comerciales, instituciones educativas y comunidades, estos servicios se encuentran adjudicados en la banda VHF 88-108 MHz, su uso requiere de un permiso especial que se solicita ante el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) y la Agencia Nacional del Espectro (ANE), sin embargo algunos usuarios realizan transmisiones sin licencia y se consideran sus transmisiones como clandestinas ocasionando problemas de orden social, técnico, y causando interferencias a otros servicios de radiocomunicación. Por otra parte, los efectos de propagación como desvanecimiento por multitrayectoria, efecto de sombras, ruido radioeléctrico e incertidumbres de los dispositivos afectan la calidad del monitoreo junto con el bloqueo, en este trabajo propone un método para monitorear y bloquear el espectro para la banda 88-108 MHz usando técnicas de sensado y bloqueo colaborativo a través de dispositivos SDR conectados en red empleando técnicas y protocolos de IoT, cómputo en la nube utilizando los algoritmos de monitoreo como el detector de energía y el detector de picos, finalmente, se realiza el bloqueo de emisiones clandestinas usando diferentes señales activando los equipos conectados para realizar el bloqueo cooperativo de radiodifusión

¹Trabajo de investigación

²Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones, Universidad Industrial de Santander. Director, Homero Ortega Boada.

sonora en frecuencia modulada.

ABSTRACT

TITLE: COOPERATIVE SPECTRUM SENSING TECHNIQUES FOR IDENTIFYING AND JAMMING ILLEGAL FM BROADCAST RADIO STATIONS USING SOFTWARE DEFINED RADIO AND INTERNET OF THE THINGS

AUTHOR: LUIS MIGUEL DÍAZ MORALES

KEYWORDS: SPECTRUM SENSING, JAMMING, SOFTWARE DEFINED RADIO, INTERNET OF THE THINGS.

DESCRIPTION:

Radio broadcasting services require a license in order to transmit radio signals; they are allocated in the VHF band 88-108 MHz. It is important to observe automatic spectrum sensing for the radio broadcasting to determine the primary users. Primary users can be defined as the users who have higher priority or legacy rights on the usage of a specific part of the spectrum. In the other hand, secondary users, who do not have a license to exploit this spectrum, can cause interference to primary users because they are outside of the spectrum management system of each country. Many factors in practice such a multi-path fading, shadowing and the receiver uncertainty problem may affect the sensing process. Cooperative Sensing (CS) enhances the sensing performance by exploiting the spatial diversity in the observations of sensing nodes. Among the spectrum sensing techniques, the energy detector is more generic than the other methods, as it does not need any knowledge of the other primary-users signals. Moreover, when the spectrum is sensed in a wide bandwidth and low frequency resolution the peaks of FM signals correspond to the carrier frequency.. In this work is proposed a system for identifying and jamming illegal FM broadcast radio stations, using techniques of cooperative spectrum sensing and spectrum jamming with the technologies SDR and IoT.

¹Research work

²Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones, Universidad Industrial de Santander. Director, Homero Ortega Boada.

INTRODUCCIÓN

La radiodifusión sonora, junto con la televisión, representan las principales posibles realizaciones del servicio de radiodifusión a que se refiere el Reglamento de Radio (RR) de la Unión Internacional de Telecomunicaciones Sector radio (UIT-R). Debido a su importancia para la sociedad la radiodifusión tiene atribuidas bandas de frecuencia que permiten amplias coberturas, el uso de altas potencias de emisión, así como técnicas de modulación que permiten el uso de equipos de bajo costo del lado de los usuarios que se benefician de las emisiones, por lo tanto es común el uso de la Modulación de Amplitud (AM) y Modulación de Frecuencia (FM) entre otras, así como las iniciativas para una evolución hacia técnicas digitales. Precisamente las mismas ventajas que hacen que la radiodifusión sea uno de los servicios que más impactan a la sociedad lo convierten en el objetivo donde se presentan los mayores casos de ilegalidad en el uso del Espectro Radioeléctrico (ERE), lo cual está representado principalmente por emisiones clandestinas que amenazan la calidad de las emisiones legales. En este aspecto también entran en juego de otras amenazas, por ejemplo la posibilidad de producir interferencias a otros servicios vitales como es el caso de los servicios aeronáuticos, la congestión del espectro que se traduce en dificultades para poder darle a esas bandas el mejor uso posible aprovechando nuevas tecnologías como las que aprovechan los espacios blancos que dejan los servicios de radiodifusión, también es posible hablar de posibles afectaciones a la salud de las personas e incluso de posibles amenazas sociales que pueden surgir con la emisión de contenidos que quedan fuera de control que pueden atentar contra la Constitución Política, la vida, honra, y bienes de los ciudadanos. Colombia es especialmente sensible a esta problemática la cual ha sido abordada por la Agencia Nacional del Espectro (ANE) mediante diversas acciones técnicas y legales, que por ahora resultan insuficientes.

Una oportunidad para contribuir a la solución de esta problemática se encuentra en las tecnologías como radio definida por software SDR por sus siglas en inglés). Estas son clave también para los nuevos sistemas de comunicación como es el caso de los que se apoyan en la radio cognitiva (CR por sus siglas en inglés) que vale la pena traer a colación por varias razones como las siguientes: la CR busca impulsar el uso de sistemas de comunicación que aprovechan al máximo los espacios blancos del espectro

que dejan otros servicios de comunicaciones; los espacios blancos de mayor interés en la actualidad son los que dejan los servicios de radiodifusión; para que un sistema aproveche los espacios blancos del espectro es necesario poder identificar esos espacios blancos lo que significa que es necesario monitorear el espectro en las bandas de interés; también es necesario que estos sistemas tengan la posibilidad de adaptar fácilmente los parámetros de radio como la banda de frecuencias, la potencia, el ancho de banda, entre otros de acuerdo a las posibilidades que esos espacios blancos ofrecen. Por lo tanto, hay una coincidencia entre las ventajas que ofrece la CR y las necesidades que tienen los sistemas de apoyo a tareas de vigilancia y control de emisiones clandestinas y se trata de soluciones que usualmente integran componentes de hardware, de software, de comunicaciones en red y de procesamiento digital lo cual justifica plenamente el uso de SDR en el presente trabajo en una solución compuesta por: monitoreo del espectro y bloqueo del espectro.

En una iniciativa de monitoreo del espectro los problemas de sombras, desvanecimiento, multi-trayectoria, entre otros fenómenos asociados a la propagación¹, pueden afectar el rendimiento del monitoreo del espectro si se usa un sólo nodo (sensado no cooperativo)²³. Estos problemas se pueden reducir mediante la utilización de múltiples nodos de sensado (sensado cooperativo), donde cada nodo distribuido espacialmente recibe información del entorno y reporta los datos para tomar una decisión más integral.

Otro concepto importante que ha tenido crecimiento los últimos años es el internet de las cosas (IoT por sus siglas en inglés) que permiten que cualquier cosa tenga facilidades para comunicarse bien sea para lograr transmitir a través de la distancia los estados físicos de las cosas con el apoyo de sensores, o incluso para implementar servicios inteligentes que combinan técnicas de sensado con técnicas de actuación, técnicas

¹Anusha, Veluru Sai; Nithya, G. K. y Rao, Sethuraman N. «A comprehensive survey of electromagnetic propagation models». En: *Proceedings of the 2017 IEEE International Conference on Communication and Signal Processing, ICCSP 2017* 2018-Janua (2018), págs. 1457-1462. DOI: 10.1109/ICCSP.2017.8286627.

²Patil, Vilaskumar M. «A Survey on Spectrum Sensing algorithms for Cognitive Radio». En: *2018 7th International Conference on Modern Circuits and Systems Technologies (MOCAST)* 1.3 (2016), págs. 1-5.

³Cichon, Krzysztof; Kliks, Adrian y Bogucka, Hanna. «Energy-Efficient Cooperative Spectrum Sensing: A Survey». En: *IEEE Communications Surveys and Tutorials* 18.3 (2016), págs. 1861-1886. ISSN: 1553877X. DOI: 10.1109/COMST.2016.2553178.

de procesamiento de los datos en la nube, incluyendo el *Big Data*. Existen diferentes arquitecturas de IoT⁴ que en conjunto con aplicaciones de seguridad, ciudades inteligentes, salud, transporte inteligente, agricultura, entre otros campos de aplicación, están transformando la forma de interacción y de toma de decisiones con el fin de mejorar diversos procesos. Este trabajo de investigación se apoya en una plataforma web basada en IoT y es un resultado del proyecto “Plataforma IoT para el desarrollo de servicios inteligentes de apoyo al monitoreo ambiental” apoyado por la vice-rectoría de investigación y extensión de la Universidad Industrial de Santander. En esta plataforma se ha implementado una red de bloqueadores como un sistema de inhibición que incluye sensado cooperativo y bloqueo cooperativo utilizando dispositivos SDR conectados en red aplicando conceptos de IoT con el fin de detectar y bloquear emisoras clandestinas que operan en la banda VHF 88-108 MHz.

En el sistema implementado, los datos recolectados por los nodos de sensado son enviados hacia: un servidor web y un servidor de base de datos, con fines de procesamiento y almacenamiento. En la etapa de procesamiento se proponen dos técnicas para encontrar emisiones clandestinas: detector de energía con cálculo de umbral dinámico, y el detector de picos que utiliza el algoritmo basado en la coincidencia de patrones de la transformada continua de *wavelet* (CWT por sus siglas en inglés)⁵, estas técnicas se estudian para el sensado cooperativo y no cooperativo. Por otra parte, se estudia el bloqueo cooperativo y no cooperativo con el fin de realizar ataques de denegación del servicio (DoS por sus siglas en inglés) a emisiones clandestinas generadas y controladas en condiciones de laboratorio con fines de investigación, y estudiar la calidad del bloqueo empleando señales de ruido, ruido en FM, OFDM y múltiples tonos.

El presente documento consta de seis capítulos: el primer capítulo hace referencia a los objetivos y alcances del trabajo de investigación; el segundo capítulo muestra un marco conceptual acerca de IoT y SDR junto con el modelo que permite integrar estas dos tecnologías, los siguientes capítulos explican de manera detallada cada etapa de la

⁴Uckelmann, Dieter; Harrison, Mark y Michahelles, Florian. *Architecting the Internet of Things*. Springer, págs. 4-20. ISBN: 9783642191565. DOI: 10.1007/978-3-642-19157-2.

⁵Du, Pan; Kibbe, Warren A. y Lin, Simon M. «Improved peak detection in mass spectrum by incorporating continuous wavelet transform-based pattern matching». En: *Bioinformatics* 22.17 (2006), págs. 2059-2065. ISSN: 13674803. DOI: 10.1093/bioinformatics/btl355.

metodología usada para resolver el problema de monitoreo y bloqueo de emisiones clandestinas; el capítulo 3 explica el comportamiento del sistema mediante la representación de diagramas UML y presentación de requisitos tenidos en cuenta en la etapa de diseño; el capítulo 4 explica lo relacionado con la capa IoT: sensado y bloqueo cooperativo junto con el estudio referente a los bloqueadores, la capa física de comunicación y el protocolo IoT utilizado para la recepción y sesión de dispositivos; el capítulo 5 explica el procesamiento de señales para identificar emisiones clandestinas que se implementa en el servidor, donde principalmente se presentan los métodos de sensado junto con el análisis de estos; por último, el capítulo 6 presenta las conclusiones relacionadas al trabajo de investigación.

1. OBJETIVOS

1.1. GENERAL

Implementar un prototipo de red de inhibición de servicios de radiodifusión sonora FM en la banda 88-108 MHz, usando la tecnología SDR como un servicio IoT y combinando técnicas de monitoreo y bloqueo para demostrar la viabilidad de mejorar la calidad de bloqueo de emisiones clandestinas.

1.2. ESPECÍFICOS

- Realizar un diseño básico del prototipo de red de inhibición para identificar los elementos que lo componen y sus funcionalidades en función principalmente de las necesidades del investigador.
- Implementar el monitoreo del espectro radioeléctrico, para identificar emisiones clandestinas en la banda de 88-108 MHz, usando IoT.
- Implementar el prototipo de terminal de monitoreo y bloqueo en red.
- Desarrollar una plataforma IoT para la administración de los dispositivos SDR a través de un servidor.
- Realizar las pruebas de viabilidad.

1.3. ALCANCES

El proyecto de investigación tiene los siguientes alcances de acuerdo con los objetivos específicos:

- El diseño se limita al uso de las metodologías de desarrollo del grupo Radiogis para la implementación de terminales y servicios IoT, pero solo en función de los propósitos de la investigación.
- El prototipo y los estudios se limitan a la banda de 88-108 MHz.
- El número de dispositivos a conectar en red son dos como mínimo.
- Los módulos a desarrollar en cada dispositivo SDR consisten de:
 - Un módulo software para enviar información del espectro a la base de datos.
 - Un módulo software para bloquear las emisiones clandestinas.
 - Un módulo software para comunicarse con el servidor que administra los dispositivos.
- La plataforma IoT inicialmente prestará los servicios de:
 - Búsqueda y bloqueo de emisiones clandestinas en la banda VHF 88-108 MHz.
 - Control de activación del sistema de monitoreo y bloqueo.
- Diseño de la aplicación como interfaz para los usuarios.
- El estudio de la viabilidad se limita a:
 - Crear un ambiente controlado de emisiones clandestinas.
 - Obtener resultados de bloqueo con un solo nodo monitor-bloqueador.
 - Obtener resultados de bloqueo usando más de un nodo monitor-bloqueador.
 - Realizar un análisis comparativo que permita demostrar si la opción de red tiene ventajas con respecto a la de un solo nodo.

2. MARCO CONCEPTUAL

Este capítulo presenta las tecnologías utilizadas para crear el sistema de servicios de servicios de radiodifusión sonora en FM. El objetivo de este capítulo es mostrar al lector una visión general acerca de las técnicas relacionadas con IoT y con SDR, comprendiendo la estructura general de ambas tecnologías. También, se propone un modelo para combinar esas dos tecnologías como una solución al problema relacionado con las emisiones clandestinas en radiodifusión sonora.

2.1. EL INTERNET DE LAS COSAS (IOT)

El crecimiento de Internet ha traído cambios significativos en las economías y sociedades, provee de una notable de infraestructura de red y amplias facilidades de comunicación que van evolucionando a medida que cambian las necesidades de los usuarios. Una de esas necesidades al día de hoy consiste en poder llegar a brindarle a cualquier cosa la posibilidad de conectarse a Internet tal y como lo hacen los humanos. Por eso, Internet se está convirtiendo en un medio de conexión para máquinas, vehículos, accesorios y sensores promoviendo las bases para nuevas aplicaciones. El término IoT se refiere a la conexión de dispositivos, sensores, objetos, habitaciones, máquinas, vehículos, entre otros a través de redes fijas e inalámbricas. Esas cosas pueden interactuar con el entorno y enviar la información a otros objetos a través de una comunicación máquina a máquina (M2M). Las diferentes aplicaciones tienen efectos en los sistemas de transporte a través de autos inteligentes, logística y sistemas de tráfico, pero también abundan soluciones orientadas al control del medio ambiente, soluciones para edificios inteligentes¹, para la salud mediante el tele-monitoreo permitiendo a los profesionales en la salud realizar una gestión remota de las patologías de los pacientes². En fin, a futuro es posible que las cosas trabajen tanto o más que los humanos, incluso percibiendo ingresos por ese

¹COMMUNITIES, COMMISSION OF THE EUROPEAN. *Communication on future networks and the internet*. Inf. téc. Bruselas, 2008.

²Dohr, A y col. «The Internet of Things for Ambient Assisted Living». En: *2010 Seventh International Conference on Information Technology: New Generations*. 2010, págs. 804-809. DOI: 10.1109/ITNG.2010.104.

trabajo, por ejemplo mediante el uso de criptomonedas.

La arquitectura IoT es un sistema que puede ser físico, virtual o un híbrido, conformando un conjunto de numerosas cosas, sensores, actuadores, servicios en la nube, protocolos IoT específicos, capas de comunicación, capas de usuarios y desarrolladores. En³ se presentan los bloques funcionales que presenta un sistema basado en IoT, como se describen a continuación:

- **Dispositivos:** son sensores, actuadores, controladores, pueden intercambiar datos con otros dispositivos y la aplicación, o coleccionar los datos de otros dispositivos y enviarlos a servidores centralizados o aplicaciones basadas en la nube como *back-ends* para procesar los datos. Los dispositivos proveen interfaces de comunicación para sensores, conexión a internet y memoria de almacenamiento.
- **Comunicación:** Esta etapa realiza la conexión entre los dispositivos y los servidores remotos, generalmente estos protocolos de comunicación trabajan en las capas de enlace de datos, de red, transporte y aplicación.
- **Servicios:** son varios tipos de funcionalidades como modelamiento de dispositivos, control de dispositivos, publicación y análisis de datos, y descubrimiento de dispositivos.
- **Gestión:** busca gobernar el sistema IoT para crear una buena administración del sistema.
- **Seguridad:** esta etapa provee funciones como autenticación, autorización, privacidad, integridad en los mensajes, contenido y datos.
- **Aplicación:** este bloque funcional es el más importante en términos de usuarios debido a que provee la interfaz necesaria para los módulos de control, monitorización y otros aspectos del sistema IoT, permite a los usuarios visualizar y analizar el estado del sistema.

³Ray, P. P. «A survey on Internet of Things architectures». En: *Journal of King Saud University - Computer and Information Sciences* (2016). ISSN: 22131248. DOI: 10.1016/j.jksuci.2016.10.003. URL: <http://dx.doi.org/10.1016/j.jksuci.2016.10.003>.

2.2. RADIO DEFINIDA POR SOFTWARE (SDR)

SDR es una de las tecnologías emergentes mas importantes en el futuro de los servicios de radiocomunicación. SDR se apoya principalmente en el uso de una clase reprogramable y configurable de dispositivos que permite que un mismo equipo pueda adaptarse, mediante actualizaciones de software, como solución a una amplia gama de sistemas de comunicación. Estos sistemas de comunicación pueden ser de comunicación digital o comunicación analógica, también pueden corresponder a sistemas actuales, futuros o incluso a sistemas del pasado⁴. SDR está comprometido en posibilitar el desarrollo de sistemas de radio que son multi-servicio, multi-estándar, multi-banda, reconfigurables y reprogramables a través de software⁵.

Una solución basada en SDR tiene tres componentes principales: el canal inalámbrico, que corresponde a las ondas electromagnéticas que viajan en el mundo físico, la componente de radio (también conocida como componente de hardware), y la componente de software. La componente de radio sirve como intermediario entre el canal inalámbrico y la componente de software. De modo que en SDR se tienen 3 tipos de señales: En el canal inalámbrico se tienen las ondas electromagnéticas de radiofrecuencia (RF); En los circuitos RF de la componente hardware se tienen señales eléctricas y es la antena la que juega el papel de traductor entre señales electromagnéticas de RF y señales eléctricas de RF; A diferencia de las anteriores componentes, en la de software las señales se caracterizan por ser una versión banda base discreta de la señal eléctrica RF, por lo tanto conserva la misma forma del espectro de la señal eléctrica RF, pero está centrado en la frecuencia cero. Esa señal banda base discreta que se maneja en la componente de software es además compleja y por ello se conoce como la Envolvente Compleja de la señal RF. Al estar el espectro centrado en la frecuencia facilita el uso óptimo de técnicas digitales, comenzando por el uso de una frecuencia de muestreo óptima y siguiente por la aplicación de cualquier cantidad de algoritmos digitales conocidos o en estudio. En la

⁴Arslan, Hüseyin y Ahmed, Sadia. *Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems*. 2007, págs. 110-120. ISBN: 978-1-4020-5541-6. DOI: 10.1007/978-1-4020-5542-3. URL: <http://www.springerlink.com/index/10.1007/978-1-4020-5542-3>.

⁵Venosa, Elettra; Harris, Fredric J. y Palmieri, Francesco A.N. *Software Radio, Sampling Rate Selection, Design and Synchronization*. Springer, 2012, págs. 1-5. ISBN: 9781461401124. DOI: 10.1007/978-1-4614-0113-1.

componente de software también es posible configurar o manipular algunos parámetros de algunos varios elementos del hardware como por ejemplo la frecuencia central, el ancho de banda, la amplificación, la frecuencia de muestreo.

La clave de la revolución que están produciendo las técnicas basadas en SDR consiste precisamente en lograr separar el hardware mínimo necesario en un sistema de comunicaciones, de todo aquello que puede ser realizado mediante software, de modo que el hardware comprende justo lo necesario para entregar la envolvente compleja a la componente de software. Lo demás es lo que resulta del aprovechamiento de estos hechos. Por ejemplo en la industria es posible hacer que los equipos de un operador se actualicen a una nueva generación con solo hacer una actualización de software siempre y cuando el hardware de esos equipos sea compatible con la nueva generación. Otro ejemplo es el laboratorio de radio comunicaciones de la UIS, donde un mismo equipo de hardware es usado para estudiar sistemas de comunicaciones analógicos como la radiodifusión AM, FM, pero también los más sofisticados sistemas de comunicaciones digitales, también se han usado para el seguimiento de satélites y se está buscando su uso como un laboratorio de radioastronomía.

Entrando en detalle a la componente de radio o componente de hardware de un sistema SDR, encontramos que usualmente está formada por:

- **Recepción** como se muestran en la figura 1, donde la señal electromagnética se transforma en una señal eléctrica a través de una antena, un amplificador de bajo ruido (LNA por sus siglas en inglés) amplifica la señal eléctrica entregada por la antena, sin embargo, en este punto la señal no está lista para ser muestreada debido a que está en la versión paso-banda, es decir, la densidad espectral de potencia (PSD por sus siglas en inglés) se encuentra centrada en la frecuencia de operación del servicio de radiocomunicación y es necesaria su transformación a la versión banda-base donde la PSD está centrada en la frecuencia cero, los componentes que hacen posible esta conversión son el oscilador controlado por voltaje (VCO por sus siglas en inglés), el *Phase Locked Loop* (PLL) y el mezclador. El VCO genera una señal a una frecuencia proporcional al voltaje de entrada donde el PLL se asegura que la señal generada por el VCO se encuentre fija a la frecuencia

específica del servicio de radiocomunicación que se desea recibir, las señales del VCO se generan en fase I (0°) y cuadratura Q (90°) y los mezcladores y los filtros se encargan de llevar la señal paso-banda a una señal banda-base compleja con una señal real que es la misma señal en fase y una imaginaria que es la misma señal en cuadratura. También se aplica un control automático de ganancia (AGC por sus siglas en inglés), y finalmente, un ADC se encarga de entregar la señal digital. La componente de hardware incluye también unos elementos de software con el fin de complementar las acciones que no pudieron ser llevadas a cabo completamente por el hardware, por ejemplo entregar la señal con una frecuencia de muestreo particular, configurable, en lugar de la frecuencia de muestreo fija que se maneja en el ADC, por eso la señal del ADC pasa a un DSP o se entrega a un equipo host a través de la interfaz de red.

- **Transmisión** como se muestra en la figura 2, donde la señal banda-base digital generada por el DSP o por el equipo host se envía hacia un DAC para que sea transformada a señal eléctrica, el VCO, PLL y mezclador transforman la señal banda-base a paso-banda (proceso inverso de la recepción) y se incrementa su potencia de salida mediante un amplificador que está conectado a una antena, finalmente, la señal cuando sale de la antena se transforma en electromagnética e interactúa con el mundo físico.

2.3. MODELO GENERAL DEL SISTEMA USANDO SDR E IOT

Para el desarrollo del sistema de inhibición de emisiones clandestinas se propone el modelo que se muestra en la figura 3. Este modelo está conformado por un tipo de dispositivos SDR que vienen con sistema embebido que permite que la componente de software quede embebida en el equipo. El modelo consta de 3 capas: La capa IoT, la capa de componentes de nube, y la capa cliente. A continuación se brinda una explicación breve de cada una de ellas:

1. Capa IoT: esta capa contiene dos subcapas: la subcapa terminal IoT que hace referencia a los dispositivos con capacidades de sensado y actuación, además,

Figura 1: Estructura general en modo recepción de la componente de radio de un equipo SDR.

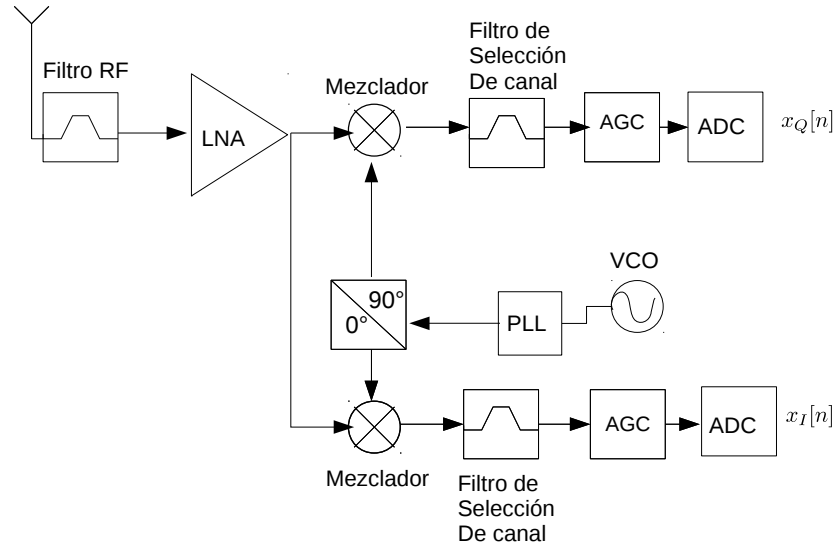
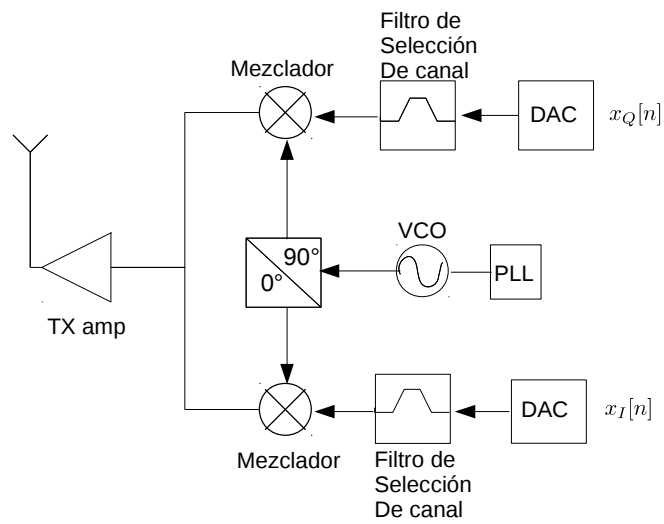


Figura 2: Estructura general en modo transmisión de la componente de radio de un equipo SDR.

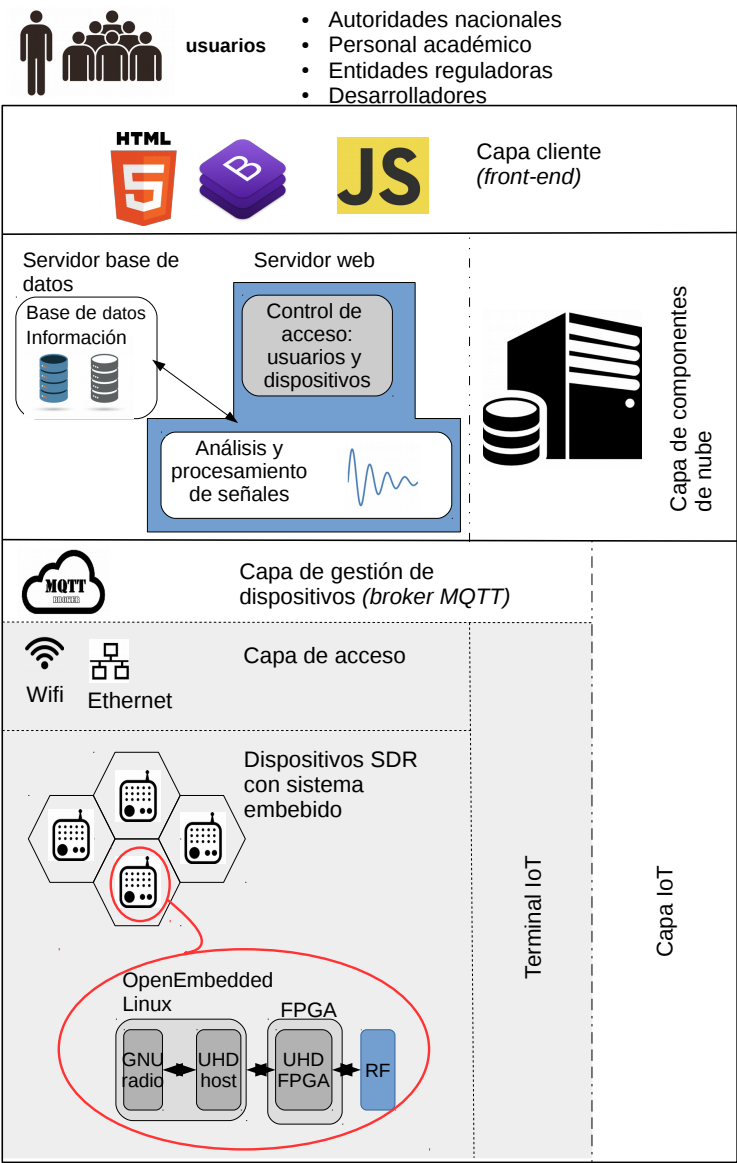


pueden conectarse a internet mediante la subcapa de acceso, y finalmente, la subcapa gestión de dispositivos hace referencia a los recursos de red para que los dispositivos se mantengan conectados y comunicados entre sí. Para los propósitos de este trabajo de investigación, en la subcapa de terminales IoT se usaron varios equipos USRP E310 los cuales tienen embebido el componente de radio y de software, así como facilidades para conectarse a Internet por WiFi y por cable Ethernet. En la subcapa de gestión de dispositivos IoT se usó el protocolo MQTT para mantener los dispositivos conectados.

2. Capa de componentes de nube: En esta capa se tiene el servidor de base de datos, donde está la base de datos que almacena los resultados del monitoreo y la información de los dispositivos y usuarios, el servidor web que contiene: el sistema de análisis y procesamiento de señales donde se encuentran los algoritmos utilizados para encontrar emisiones clandestinas, y el control de acceso de usuarios y dispositivos donde el sistema permite realizar el registro, seguimiento, configuración de cada uno de terminales IoT junto con el acceso por usuarios. Todo lo que se realiza en esta capa corresponde a una solución en la nube que desde el punto de vista de un servicio se conoce como el *back-end* ya que representa todo el trabajo que se realiza para prestar el servicio, pero que está oculto a los usuarios.
3. Capa cliente: esta capa corresponde a los recursos con los que un usuario interactúa o accede a un servicio, usualmente, el cliente accede a través de una página HTML que está acompañada de estilos CSS y aplicaciones JavaScript. También, es posible distinguir una capa adicional a las ya mencionadas, la capa de los usuarios, donde se encuentran las personas que hacen uso del servicio y ayudan a definir los requisitos del sistema.

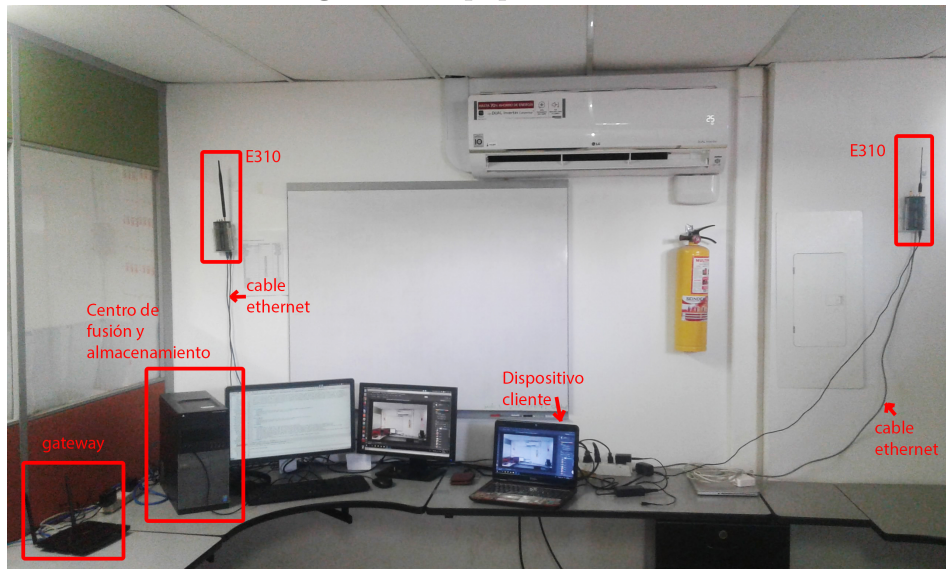
Siguiendo el modelo presentado, se implementó un laboratorio de pruebas el cual ha sido capturado en la foto de la figura 4. En este laboratorio la capa de componentes en la nube es el computador de escritorio designado para ejecutar el servidor web, servidor de base de datos, y capa de gestión de dispositivos (*broker* MQTT), los terminales IoT son los equipos SDR E310 junto con el cable ethernet hace parte de la capa de acceso, el router es la puerta de enlace (*gateway*) que permite crear una red local de dispositivos

Figura 3: Modelo general de la plataforma IoT para aplicaciones de SDR.



conectados, y el computador portátil puede comportarse como cliente donde se navega en la interfaz web.

Figura 4: Equipos utilizados



Los siguientes capítulos explican la metodología basada en el modelo general de la plataforma IoT para aplicaciones de SDR, esta inicia con la especificación de requisitos por parte de los usuarios, el diseño de la solución a nivel funcional a través de UML, descripción detallada de la capa IoT donde se estudian los terminales IoT junto con su configuración y análisis (monitoreo y bloqueo cooperativo), y por último, la capa de componentes en la nube donde se presenta de manera detallada el análisis del procesamiento de señales utilizado para determinar emisiones clandestinas y el modelo de la base de datos.

De esta manera, se logró proponer no solo un modelo a seguir en la implementación de la solución, sino que se establecieron las bases para implementar el laboratorio requerido para las pruebas, es decir, crear un ambiente con equipos y software en condiciones de laboratorio para desarrollar todas las pruebas necesarias para el proyecto.

3. PROCESO DE IDENTIFICACIÓN DE REQUISITOS Y DEL DISEÑO FUNCIONAL

En este capítulo se presenta la primera etapa de la metodología para desarrollar una solución IoT, comenzando por la ingeniería de requerimientos que surge a partir de las necesidades de los usuarios y da como resultado los casos de uso del sistema de inhibición, también, se presentan las bases para el diseño UML del diagrama de secuencia, diagrama de clases y diagrama de máquina de estados.

3.1. INGENIERÍA DE REQUERIMIENTOS

Los requisitos del sistema de inhibición se deducen principalmente a partir de las necesidades que expresan los usuarios del servicio de inhibición de emisiones clandestinas usando SDR e IoT. En este proyecto, la identificación de los requisitos se realiza siguiendo el estándar IEEE STD 830-1998¹. Este estándar describe los enfoques recomendados para lo que se conoce como ingeniería de requerimientos de software. En el presente proyecto se proponen usar estas mismas recomendaciones para soluciones IoT que combinan hardware y software.

3.1.1. Descripción general

3.1.1.1. Perspectiva del producto En el sistema de inhibición de emisiones clandestinas de radiodifusión sonora en FM, la administración de los terminales IoT se realizará de manera centralizada utilizando tecnologías web. Los terminales IoT deben encargarse de brindar funcionalidades de RF, pero también deben tener capacidades para conectarse como un nodo de red al sistema de inhibición para realizar acciones de

¹IEEE. *IEEE Std 830-1998- IEEE Recommended Practice for Software Requirements Specifications*. 2009. URL: <https://standards.ieee.org/findstds/standard/830-1998.html> (visitado 01-01-2018).

monitoreo y bloqueo de emisiones clandestinas. También es necesario asegurar que el sistema pueda operar por usuarios, es decir, definir las acciones que son permitidas de acuerdo al tipo de usuario.

3.1.1.2. Funciones del producto La plataforma hace parte del sistema de inhibición, ésta tiene las siguientes funcionalidades:

1. Menú usuarios primarios.
2. Menú ingresar.
 - Registrar usuario.
 - Operaciones.
 - Bloqueo.
 - Análisis de emisiones clandestinas.
 - Método detector de energía.
 - Método detector de picos.
 - Salir.
3. Último espectro sensado.

3.1.2. Características del usuario Los servicios que brinda el sistema de inhibición podrán ser usados por personal académico, autoridades nacionales del espectro pero también por los desarrolladores que necesitarán acceso a información privilegiada del sistema. Además, el sistema contará con un usuario administrador que se encargará de actualizar, eliminar usuarios primarios de acuerdo al plan Técnico de radiodifusión sonora FM, y operar el sistema de inhibición de acuerdo a las necesidades y a la reglamentación vigente.

3.1.3. Definición de restricciones para la versión piloto

- El sistema de inhibición debe estar reglamentado en Colombia para su uso de acuerdo con la resolución 2774 del 5 de agosto del 2013.
- Para los propósitos de la presente investigación no se usarán amplificadores de RF, por lo tanto la potencia máxima de cada nodo estará determinada por las capacidades de los dispositivos SDR.
- La comunicación entre el servidor y los dispositivos SDR se realizará mediante el protocolo MQTT, y la comunicación entre el cliente y el servidor mediante HTTP.
- Los dispositivos SDR contarán con sistema de software embebido, y herramientas de conexión en red que permitan a los dispositivos SDR comportarse como un Terminal.

3.1.3.1. Aspectos legales sobre los bloqueadores en colombia La Constitución Nacional en el Art. 75 establece que “el espectro electromagnético es un bien público enajenable e imprescriptible sujeto a la gestión y control del Estado. Se garantiza, además, la igualdad de oportunidades en el acceso a su uso en los términos que fije la ley”². El MinTIC otorga los permisos para el uso del espectro radioeléctrico, se encarga de la asignación, y la gestión de dicho recurso conforme a los Art. 11 de la Ley 1341 de 2009 y 7 del Decreto ley 4169 de 2011.

El Art. 64 de la ley 1341 de 2009 en su numeral 3, establece que constituye infracción utilizar el espectro radioeléctrico sin el correspondiente permiso o en forma distinta a las condiciones de asignación. El párrafo del artículo citado establece que cualquier proveedor de red o servicio que opere sin previo permiso para uso del espectro será considerado como clandestino. Los Art. 25 y 26 numeral 4 de la ley citada, establecen que la ANE tiene dentro de sus funciones ejercer la vigilancia y control del espectro radioeléctrico.

²Constitución política de Colombia de 1991, Art. 75

La resolución No. 2774 de 5 agosto de 2013 establece que los bloqueadores, inhibidores y amplificadores de señales de RF, sólo podrán ser utilizados en los casos autorizados por el MINTIC, conforme a las disposiciones presentadas en la resolución citada. El MinTIC puede autorizar a las entidades públicas y a las entidades del sector financiero el uso de bloqueadores por razones de seguridad y de interés general. El Art. 5 de la presente resolución establece autorizaciones especiales a los organismos de seguridad del estado, los cuales pueden usar bloqueadores fijos o móviles de manera exclusiva en los casos relacionados con la seguridad pública, sin solicitar permiso ante el MinTIC.

3.1.4. Requisitos específicos

3.1.4.1. Interfaces de usuario La solución final requiere que exista una página web donde los usuarios puedan seleccionar todos los menús descritos en 3.1.1.2 Funciones del producto que conforman la plataforma.

3.1.4.2. Componentes hardware

- Equipos SDR con sistema operativo embebido, sobre el cual se desarrollarán librerías con un protocolo para IoT.
- Antenas omnidireccionales.
- Conexión de equipos USRP a través de Ethernet o WiFi.
- Computador que soporte un servidor web, *Broker* MQTT y servidor de base de datos.
- Router.

3.1.4.3. Interfaces de software Los recursos seleccionados para el desarrollo del sistema de inhibición tienen las siguientes características

Tabla 1: Requisitos de software para el desarrollo.

SO	Linux 4.15.0-32-generic , Ubuntu 16.04
BD	PostgreSQL 10
Lenguaje servidor (<i>backend</i>)	Python3
Cliente (<i>frontend</i>)	HTML5, CSS, Javascript
Librerías python	scipy, argon2-cffi, bcrypt, dj-database-url dj-static, Django v1.11.5, django-bootstrap3, django-chartjs, django-toolbelt, matplotlib, numpy, paho-mqtt, pandas, pycopg2, pycopg2-binary, Pillow.
Servidor web	Apache2
Broker MQTT	mosquitto version 1.4.8

3.1.4.4. Interfaces de comunicaciones La interfaz de comunicación entre el servidor y los nodos del sistema de inhibición es a través de MQTT, y la comunicación entre el cliente y el servidor es a través de HTTP; ambos protocolos están sustentados en TCP-IP.

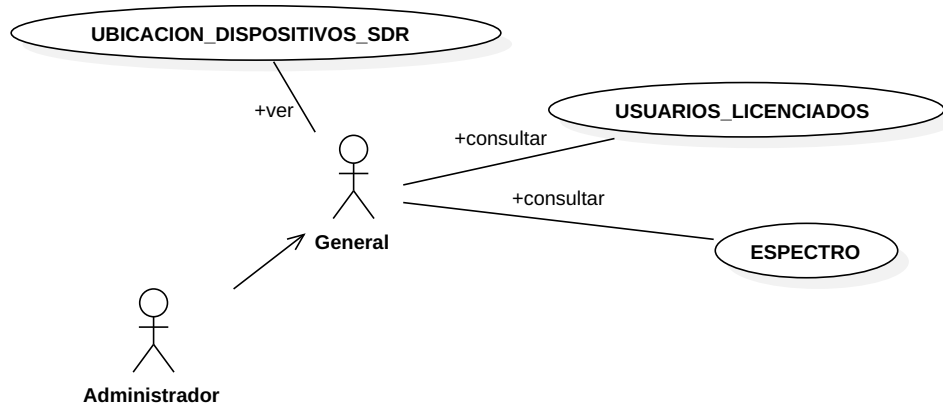
3.1.5. Requisitos funcionales Los requisitos funcionales describen el núcleo del funcionamiento del sistema, esta sección describe detalladamente los requisitos; de acuerdo con las restricciones vistas en 3.1.3, los requisitos se presentan para el usuario general, y del usuario administrador de la red, este último tiene privilegios en el uso del sistema.

3.1.5.1. Diagrama de casos de uso El esfuerzo principal de la ingeniería de requerimientos es desarrollar un modelo del sistema que se va a construir, los casos de uso son el insumo para el proceso de diseño, y representan el comportamiento del sistema como se muestra a un usuario exterior. El sistema se diseña principalmente para dos tipos de usuarios: general y administrador de la red.

3.1.5.2. Modo usuario general El modo usuario general permite realizar actividades básicas en la plataforma como ver la ubicación de los dispositivos SDR, consultar los usuarios licenciados del espectro, y consultar el último espectro sensado

por el sistema de inhibición, como se muestra en la figura 5, sin tener comunicación directa con los dispositivos, debido a que el uso de bloqueadores está reglamentado en Colombia por la ley.

Figura 5: Diagrama de casos de uso para el modo usuario general.

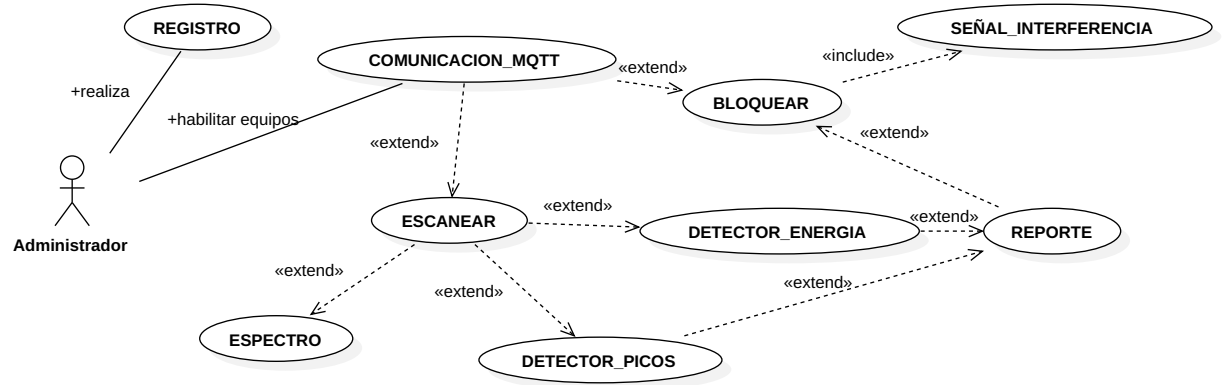


3.1.5.3. Modo administrador de sistema de inhibición El modo administrador del sistema de inhibición incluye los casos de uso del usuario general y nueve casos de uso adicionales que se relacionan entre sí a través del diagrama de casos de uso que se presenta en la figura 6, y se explica a continuación:

1. REGISTRO: este caso de uso permite registrar nuevos usuarios del sistema de inhibición de emisiones clandestinas y nuevos usuarios licenciados para el uso del espectro en la banda definida.
2. COMUNICACIÓN MQTT: este caso de uso se encarga de administrar la comunicación con los terminales IoT.
3. ESCANEAR: este caso de uso controla el proceso de escaneo del espectro por parte de los terminales IoT.
4. ESPECTRO: este caso de uso hace referencia al almacenamiento en la base de datos del espectro.

5. DETECTOR_PICOS: este caso de uso hace referencia al método de procesamiento del espectro que se explica en la sección 5.1.1.4.
6. DETECTOR_ENERGIA: este caso hace referencia a otro método de procesamiento del espectro que se explica en la sección 5.1.1.1.
7. REPORTE: este caso de uso reporta al usuario los resultados del proceso de monitoreo de emisiones clandestinas después de aplicar los métodos de procesamiento del espectro seleccionado.
8. BLOQUEAR: este caso de uso permite usar el modo de bloqueadores de forma manual eligiendo la banda de interés para el usuario, o de manera automática con base en el resultado del monitoreo.
9. SEÑAL_INTERFERENCIA: este caso de uso se refiere al tipo de señal usada para interrumpir las comunicaciones de las emisiones clandestinas como se explica en la sección 4.1.1.5.

Figura 6: Diagrama de los Casos de uso para el modo usuario administrador



El administrador debe tener autorización especial para el uso del sistema de inhibición debido a que este usuario interactúa directamente con los equipos SDR realizando actividades de monitoreo, procesamiento, y bloqueo del espectro.

3.2. PROCESO DE DISEÑO

3.2.1. Diagrama de secuencia El sistema de inhibición de emisiones clandestinas se encuentra conformado principalmente por: administrador, componentes de nube (servidor y base de datos), *Broker* MQTT, dispositivos SDR (que actúan como terminales IoT) y transmisiones de radio (banda VHF); el diagrama de secuencia representa una interacción entre ellos como un gráfico bidireccional. La dimensión horizontal muestra los mensajes intercambiados por los diferentes actores, y la dimensión vertical es el eje del tiempo. El diagrama de secuencia para el análisis y bloqueo de emisiones clandestinas mostrado en la figura 7 se describe a continuación:

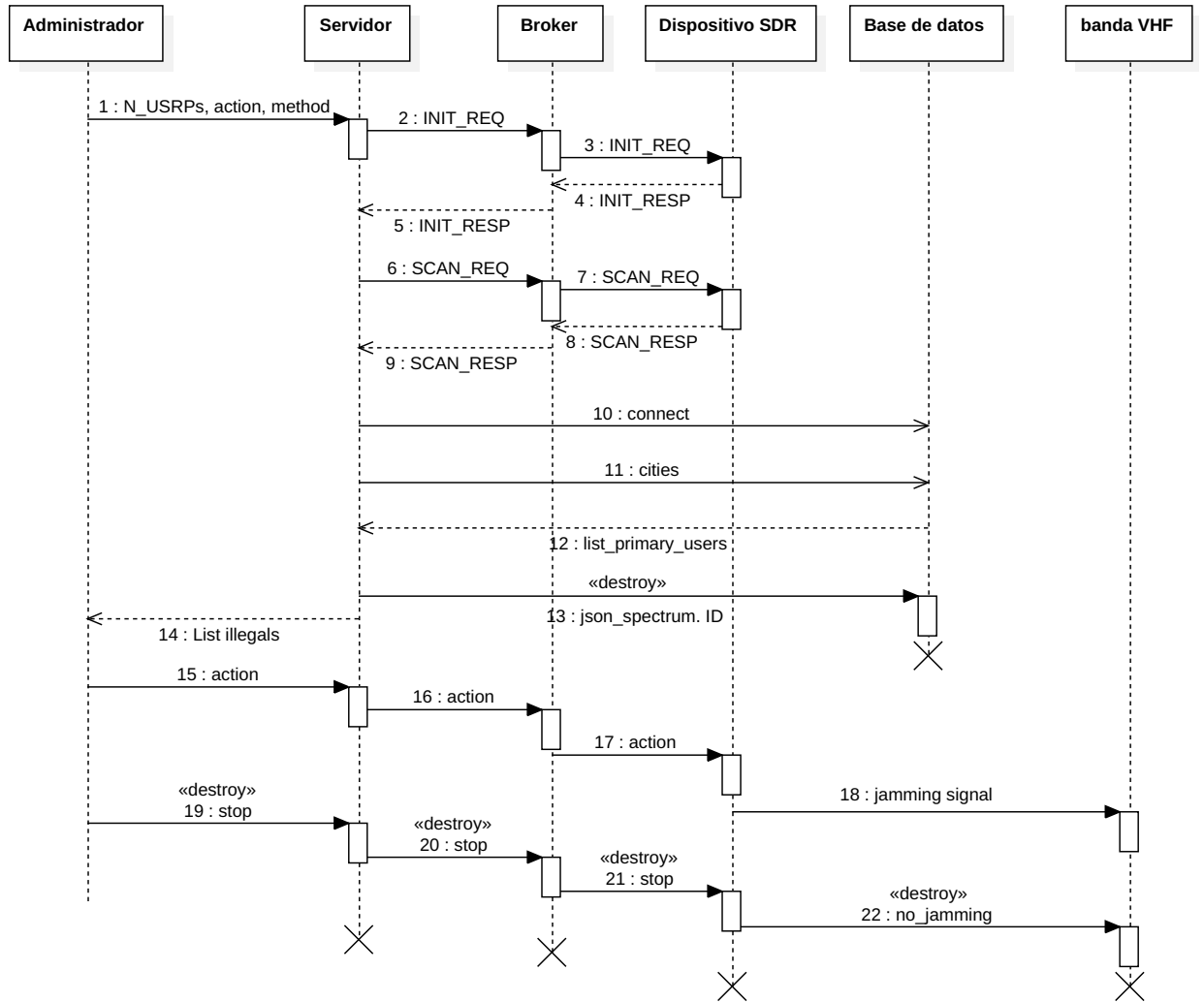
- El administrador selecciona el número de USRPs, la acción de inicio, y el método de procesamiento (*NUSRPs*, *action*, *method*) a través del protocolo HTTP por el método POST.
- El *backend* del servidor toma los USRPs seleccionados (*NUSRPs*) y configura los tópicos MQTT de los dispositivos seleccionados para enviar el mensaje *INIT_REQ* al *broker* MQTT, el *broker* verifica que la sesión establecida por el servidor sea correcta mediante autenticación, si es correcta, el *broker* publica el mensaje a través de los tópicos establecidos.

El mensaje *INIT_REQ* permite a los dispositivos USRP interpretar la información configurada en el *backend* como el número de cuadros de tiempo, número promedio de muestras, tamaño seleccionado para la FFT y comprobar que las instrucciones provengan propiamente del servidor mediante unas palabras clave y una contraseña configurada, *INIT_REQ* se codifica en formato JSON y tiene la siguiente estructura:

```
INIT_REQ = {"ServerDesc":["server", "django"],"frames": N, "K": K, "fft  
size": L, "flag": "exit",  
"SECRET KEY": "pt0mha8+j_51q81(1d)6ng36yp*b0i@9i&&ejfs"}
```

- Cada dispositivo USRP está suscrito a un tópico que lo identifica, si los dispositivos interpretan correctamente el *INIT_REQ* devuelven un *INIT_RESP* codificado

Figura 7: Diagrama de secuencia del sistema de inhibición.



en JSON al *broker*, y el *broker* devuelve la confirmación `INIT_RESP` al servidor. El mensaje `INIT_RESP` tiene la siguiente estructura:

```
INIT_RESP = {"state":"available USRP"}
```

- El servidor confirma el estado de los USRP y publica al *broker* un `SCAN_REQ` codificado en JSON que contiene los parámetros hardware y etiquetas para configurar en los dispositivos SDR, estos parámetros son: la frecuencia central en la que opera el mezclador, la frecuencia de muestreo para que el banco de filtros seleccione la banda de interés, y la antena en modo recepción para iniciar el proceso de sensado de datos del espectro, el mensaje `SCAN_REQ` está estructurado de la siguiente forma:

```
SCAN_REQ = { "Center Freq":fc, "sample_rate": 16000000, "Antenna": "RX",  
"flag":1, "freq_list":[] }
```

- Los dispositivos inician el proceso de sensado del espectro, los datos RAW (sin procesar) se almacenan temporalmente en la SD del dispositivo SDR, se leen por cuadros de tiempo, se codifican en JSON para crear la respuesta `SCAN_RESP`, y se envían al *Broker* MQTT con la siguiente estructura:

```
SCAN_RESP:{"signal":[[x1,y1],...], "Device":"ID" }
```

- El *broker* MQTT redirecciona la información del espectro al servidor donde el algoritmo de procesamiento seleccionado en el paso 1 de la figura 7 (métodos descritos en 5.1.1) realiza una solicitud de conexión a la base de datos para consultar los usuarios primarios por ciudad, en este proyecto se trabaja con datos de usuarios primarios para el Área Metropolitana de Bucaramanga.
- La base de datos devuelve la lista de usuarios primarios por ciudad, y el servidor actualiza el ID de últimos datos sensados por los dispositivos después de pasar por el CF, y finalmente se cierra la conexión con la base de datos.
- Los algoritmos de procesamiento, descritos en la sección 5.1.1, determinan si en los datos analizados hay o no presencia de emisiones clandestinas, el servidor envía la acción al *broker* MQTT para que este redirija la información a los dispositivos SDR, la acción consiste en enviar un `SCAN_REQ` con la bandera de bloqueo y antena

de transmisión, es decir, "flag": 0, "Antenna": "TX", la información de las emisiones clandestinas se encuentra en "Center Freq".

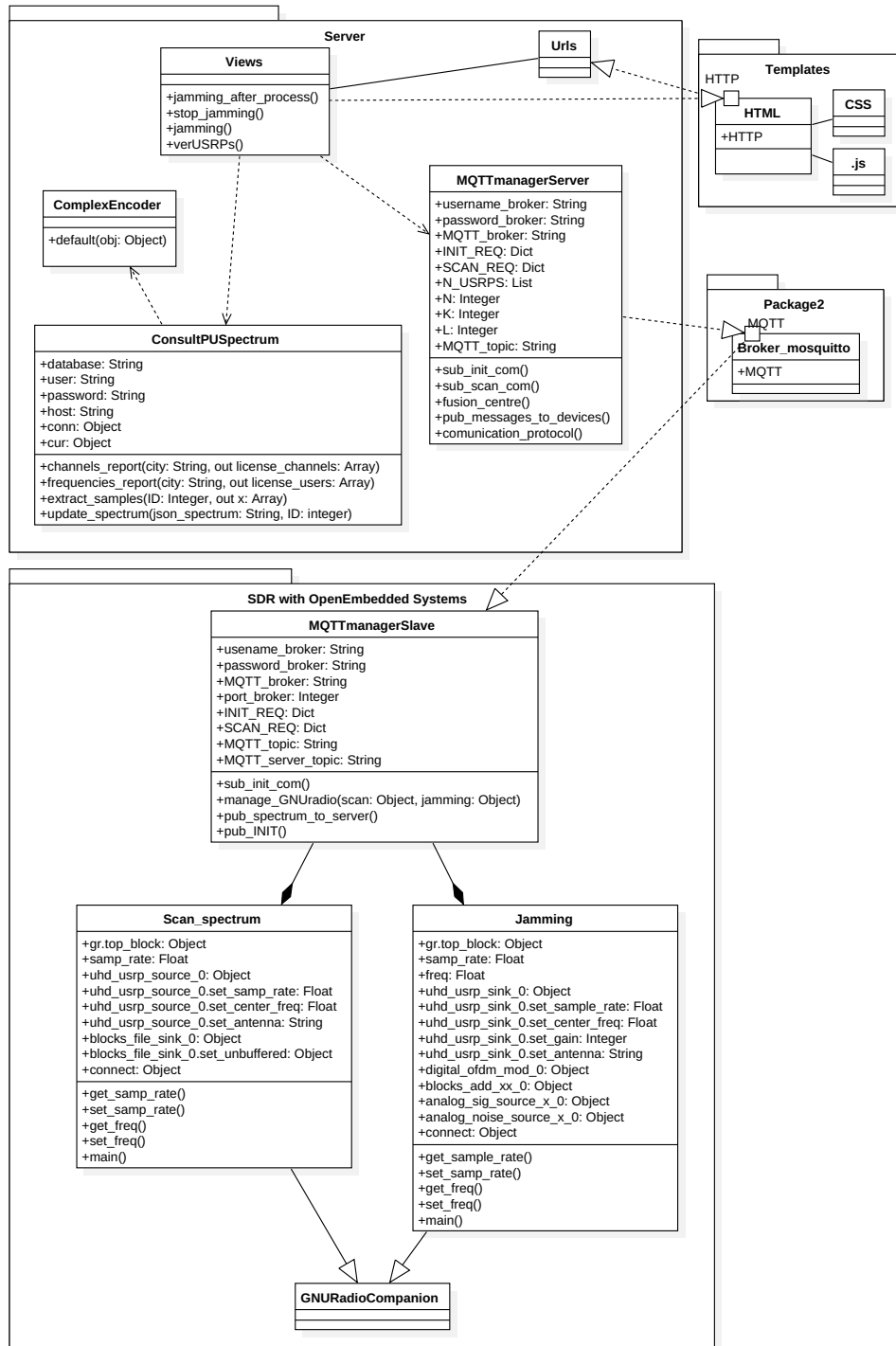
```
SCAN_REQ = {"Center Freq":freq*1000000, "sample_rate": 250000,  
"Antenna": "TX", "flag": 0}
```

- Los dispositivos SDR seleccionan el método de bloqueo y son configurados de acuerdo a la información `SCAN_REQ`, ver sección 4.1.1.5 donde se muestran las señales usadas para interferir las emisiones clandestinas.
- El proceso de bloqueo finaliza cuando el usuario administrador considere conveniente detener el bloqueo.

3.2.2. Diagrama de clases El diagrama de clases modela la estructura estática del sistema mediante objetos y sus relaciones: asociación, generalización, y varias clases de dependencia como realización y uso. Las clases se dibujan como rectángulos, que tienen sus atributos y operaciones, las relaciones entre clases se representan mediante líneas que conectan los rectángulos de las clases. Una clase representa un concepto discreto dentro de la aplicación que se está modelando. El diagrama de clases es creado con relación a los casos de uso, y es una herramienta valiosa al momento de programar porque define los objetos con sus atributos y métodos, junto con las relaciones creadas con otras clases u objetos. La figura 8 muestra el diagrama de clases referente a los casos de uso `COMUNICACION_MQTT`, `ESCANEAR`, `ESPECTRO`, `BLOQUEAR` y `SEÑAL_INTERFERENCIA`, es importante resaltar que en este diagrama de clases existen dos paquetes, uno se ejecuta en el servidor y el otro en el terminal IoT, la única forma de comunicación entre estos dos paquetes es a través de la interfaz del *broker* MQTT en el que se intercambian los diferentes mensajes descritos en el diagrama de secuencia. Para la gestión de la comunicación MQTT están las clases `MQTTmanagerServer` (presente en el servidor) y `MQTTmanagerSlave` (presente en cada terminal IoT).

La figura 9 muestra el diagrama de clases con relación a los casos de uso: `DETECTOR_ENERGIA`, `DETECTOR_PICOS`, y `REPORTE`; la clase `SensingTechniques` se encarga de gestionar los métodos de sensado y está formada por las clases: `Noise_validator` que hereda los métodos de `Energy_detector` (ver sección 5.1.1.1), y la clase

Figura 8: Diagrama de clases comunicación entre el servidor y los dispositivos de la red, almacenamiento y funciones de los dispositivos.



`Spectrum_monitoring` que contiene los métodos del detector de picos (ver sección 5.1.1.4), también se encuentran las clases `Urls`, `Views` y la interfaz de comunicación con el usuario, estas últimas clases son propias del *framework web* Django utilizado para este proyecto.

Por último, en la figura 10 se encuentra el diagrama de clases referente a los casos de uso REGISTRO, USUARIOS_LICENCIADOS y ESPECTRO, este diagrama de clases muestra los objetos referentes a los formularios, modelos y conexión externa a la base de datos, para codificar y guardar el espectro codificado con JSON en la base de datos.

Las figuras 8- 10 muestran la estructura de programación que se realiza en el *Back-End* (presentado en el modelo de la figura 3), donde la base de datos de información y control, control de acceso de usuarios y dispositivos, y el análisis y procesamiento de señales se conectan y se complementan mediante la interacción de los diferentes mensajes descritos en el diagrama de secuencia.

3.2.3. Diagrama de máquina de estados El diagrama de máquina de estados representa los estados del sistema, interacción de los elementos del modelo de capas, y sus transiciones con base a los eventos que recibe, modela las posibles historias de vida de los objetos. En la figura 11 se muestra el diagrama de máquina de estados para las acciones principales de monitoreo y bloqueo de emisiones clandestinas teniendo en cuenta los actores servidor (color azul), *Broker* MQTT (color rosado), usuario (color gris), base de datos (color verde) y equipo SDR (color amarillo), algunos estados representan métodos del diagrama de clases, su análisis es un poco más complejo porque trata de mezclar lo usado en los diagramas de secuencia y clases. En el equipo SDR se destaca el uso de etiquetas para monitoreo y bloqueo como se mostró en el diagrama de secuencia, el *Back-End* del servidor cumple un papel importante porque centraliza los procesos de consulta de base de datos, comunicación MQTT, procesamiento, y reporte de información al usuario.

Figura 9: Diagrama de clases para el procesamiento de los datos del espectro, y el reporte de los mismos.

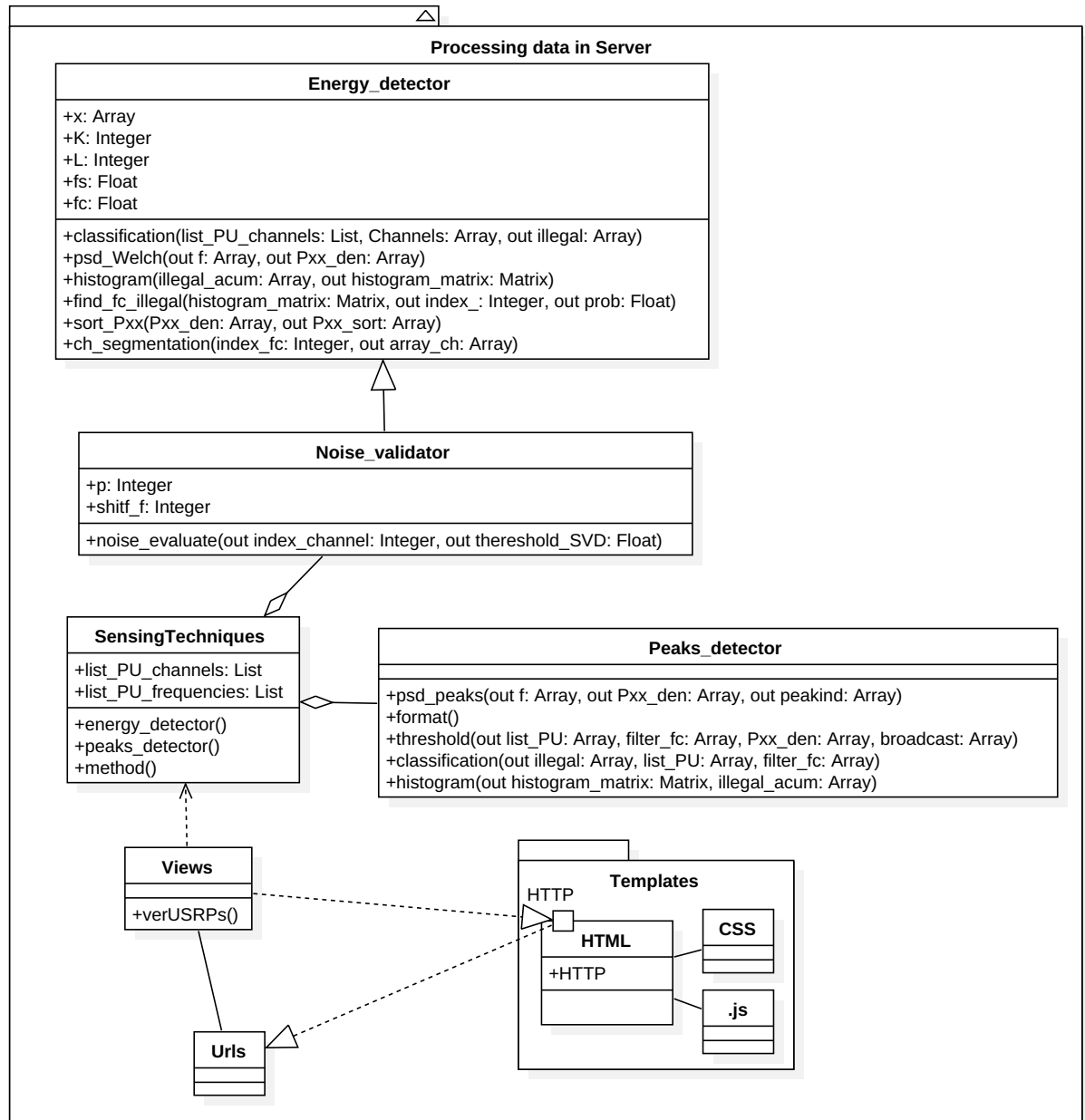


Figura 10: Diagrama de clases para el registro, consultas y acceso.

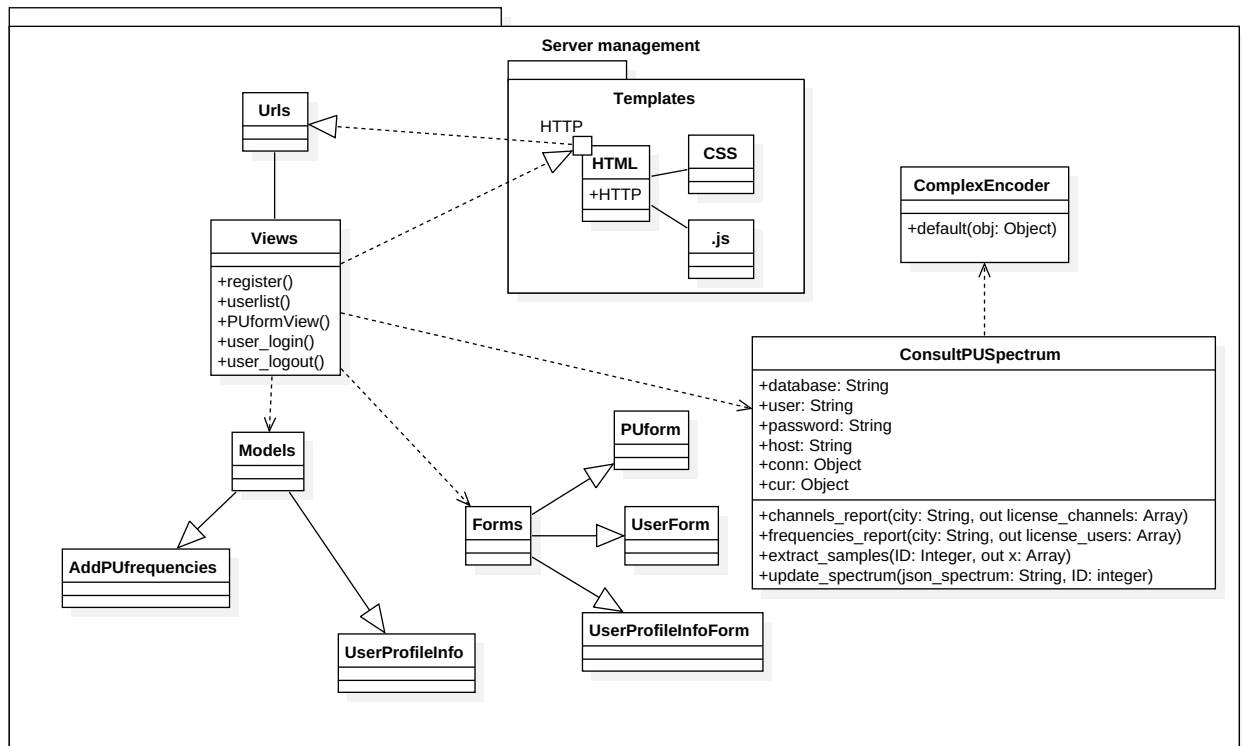
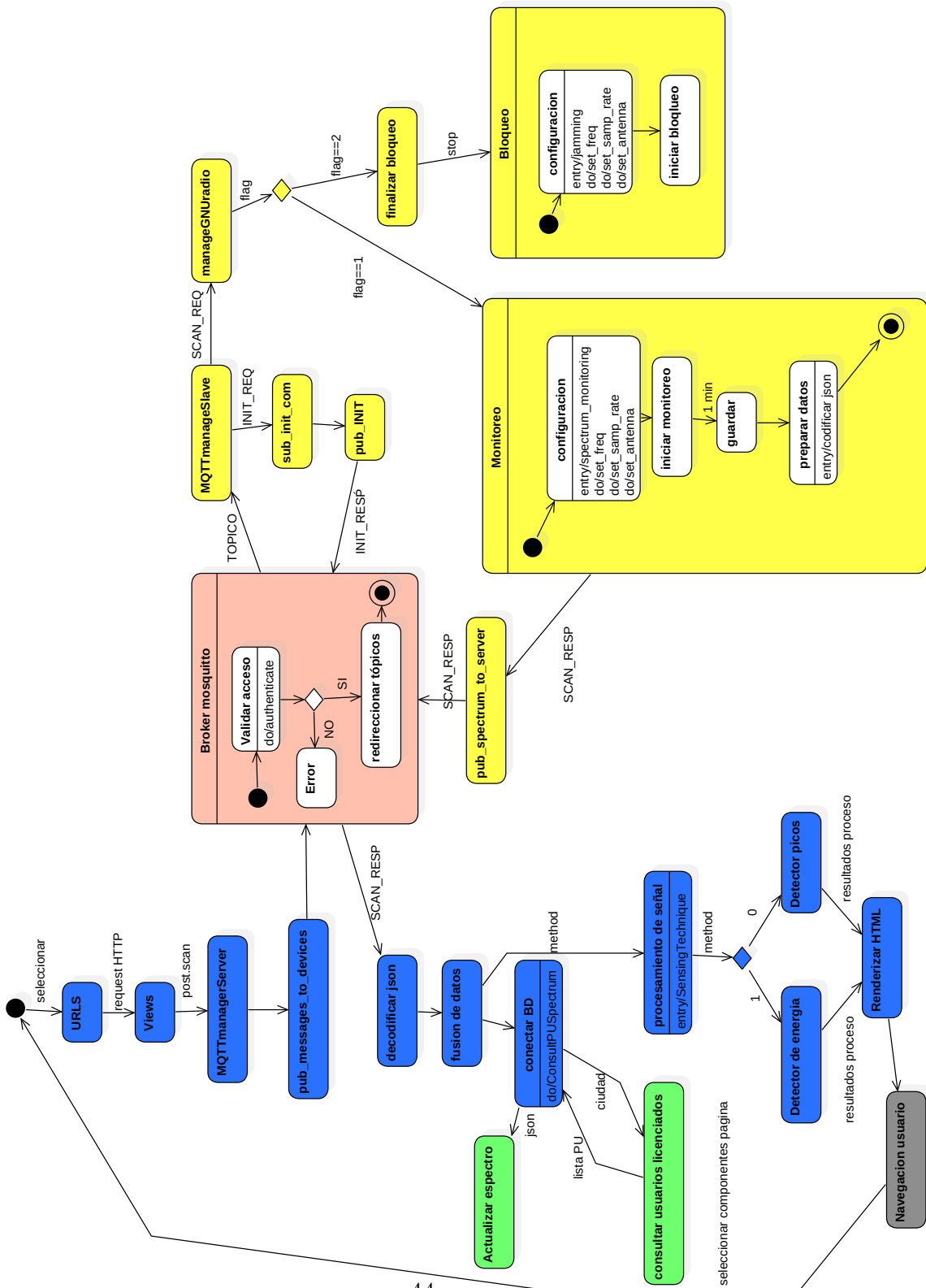


Figura 11: Diagrama Maquinas de estado para el monitoreo y bloqueo.



3.3. INTERFAZ DE USUARIO

Esta es la última capa del modelo presentado en la figura 3, el usuario tiene comunicación con el servidor web a través HTTP, por medio de interfaz web como HTML, CSS y JavaScript. A través de estas interfaces web, el usuario puede navegar el sitio y dependiendo de su condición (usuario general o administrador) realizar las diferentes acciones descritas en los casos de uso de la sección 3.1.5.1.

4. SOLUCIÓN A NIVEL DE CAPA IOT

Este capítulo presenta el siguiente paso de la metodología para desarrollar el sistema de emisiones clandestinas que consiste en la implementación de la Capa IoT presente en el modelo de la Figura 3. Esta capa está conformada por la subcapa de terminal IoT y la subcapa de gestión de dispositivos mediante el *Broker* de dispositivos MQTT. El terminal IoT está representado usualmente por los dispositivos SDR, que incluye software y hardware pero también los modos de operación (sensado y bloqueo), así como los elementos de conectividad asociados a la sub-subcapa de acceso. A los modos de operación están relacionados con los modelos de sensado y bloqueo cooperativo, las señales utilizadas por los bloqueadores. En este capítulo también se presenta un análisis del bloqueo de emisiones clandestinas mediante simulación y pero también mediante una implementación de pruebas. Finalmente, se describe el *Broker* MQTT es que es lo esencial en la sub-capas de gestión de dispositivos.

4.1. TERMINAL IOT

Un terminal IoT hace referencia a un dispositivo que tienen todos los recursos necesarios para conectarse y ser reconocido por la capa de gestión de dispositivos. Para nuestro caso, usamos varios terminales IoT representados usualmente por equipos SDR dotados conectividad WiFi y/o Ethernet y que ha sido complementado con software embebido para soportar el protocolo de comunicación de IoT (MQTT). Un terminal IoT está orientado hacia un problema particular de una aplicación IoT.

4.1.1. Caracterización de los dispositivos SDR Toda solución IoT pasa por una etapa previa de caracterización de las cosas que se van a usar como terminales IoT ya que la mayoría de las dificultades se presentan no se tiene en cuenta el rango de operación de los equipos. Los dispositivos SDR usados en el presente trabajo pueden ser vistos como sensores del espectro radioeléctrico (ERE) y a la vez como actuadores sobre el ERE. Además cuentan con conectividad IP mediante Ethernet y WiFi, así

como con la posibilidad de convertirse en un terminal IoT propiamente dicho. A continuación se presentan los resultados del estudio realizado a los dispositivos SDR usados, comenzando por sus características y modos de operación (sensado y bloqueo).

4.1.1.1. Características de los dispositivos SDR En este proyecto se han seleccionado como dispositivos SDR los equipos USRP E310. Ellos tienen sistema *OpenEmbedded* Linux con librerías GNU Radio y UHD instaladas que le permiten operar de forma autónoma. Las características del equipo E310 se resumen en la siguiente tabla:

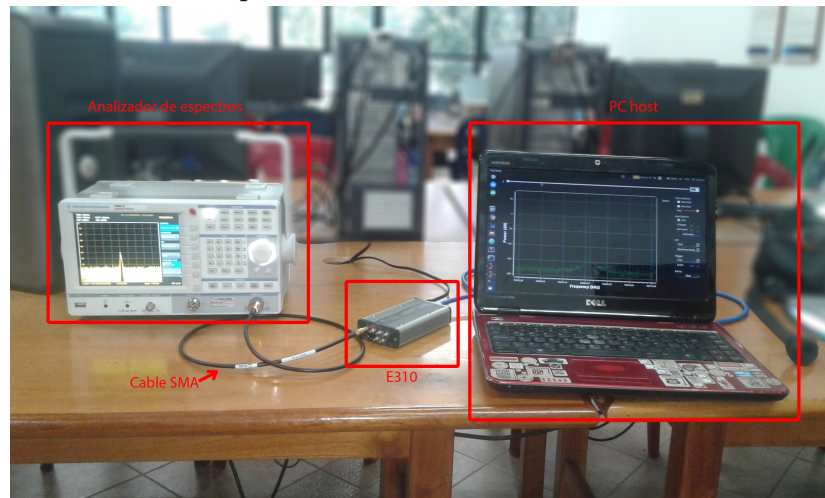
Tabla 2: Características generales del equipo SDR.

USRP E310	
Xilinx Zynq 7020 SoC	ARM Cortex A9 866 MHz con FPGA
Banco de filtros RF	Tx, Rx
UHD	V3.9.1
RFNoC	Si
Audio Jack	Si
2x2 MIMO transceiver	Si
Rango de frecuencias (Rx)	70 MHz - 6 GHz
Rango de frecuencias (Tx)	47 MHz - 6 GHz
Ancho de banda instantáneo (AD9631 RFIC)	56 MHz
SO	OpenEmbedded Linux, basado en el proyecto YOCTO Linux
Máxima potencia de entrada (Rx)	0 dBm
Máxima potencia de salida (Tx)	15 dBm

El transceptor AD9631 RFIC presente en el dispositivo E310 puede soportar un ancho de banda de 56 MHz, sin embargo, para procesar señales en ese ancho de banda se requiere implementar algoritmos en la FPGA usando herramientas como RFNoC, las cuales no se consideraron necesarias en este trabajo ya que el proceso de transferencia y procesamiento de datos sensados del ERE impone también restricciones adicionales.

La tasa de muestreo máxima que se puede obtener de la FPGA a los núcleos ARM (procesador) es de 16 MS/s, lo cual se comprobó usando las herramientas del UHD `rx_samples_to_file` en el PC host, y corriendo un programa en modo embebido en el equipo E310 donde se varía la tasa de muestreo, de manera que cuando se superan los 16 MS/s se generan alertas en el UHD que indican que se ha superado la tasa de muestreo permitida. Otra característica importante es encontrar una relación entre los valores de ganancia Tx utilizados por software y los valores reales de ganancia Tx. Esto se realizó utilizando un E310, operando en modo transmisor, y un analizador de espectros como se muestra en la Figura 12. La prueba de caracterización consistió en:

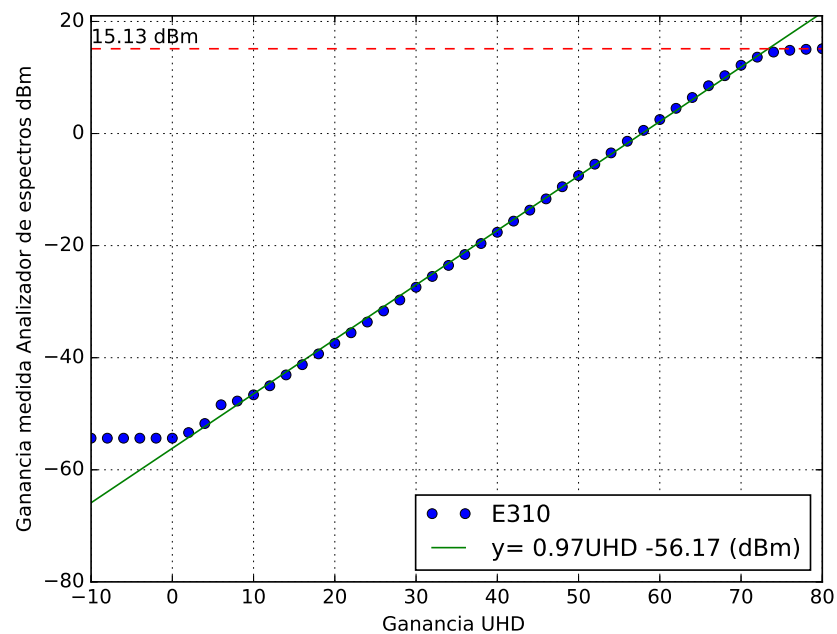
Figura 12: Montaje experimental para encontrar la relación entre la ganancia del UHD y la potencia de salida del dispositivo E310



- Generar tonos desde el E310 a diferentes frecuencias (dentro de la banda 88-108 MHz) para verificar la linealidad del amplificador Tx presente en el equipo E310.
- Generar un tono desde el E310 a frecuencia central o frecuencia de portadora que esté en la banda VHF 88-108 MHz.
- Fijar una frecuencia central e ir variando la ganancia del UHD en GNURadio, esto se puede hacer en modo embebido o en modo *network* a través de la interfaz GUI de GNURadio.
- Tabular y graficar los datos obtenidos por el analizador de espectros para encontrar la zona lineal de operación.

La Figura 13 muestra la relación existente entre los valores de ganancia dados por software en el UHD y la potencia medida por el analizador de espectros, la potencia máxima de salida del dispositivo E310 es 15.13 dBm, la gráfica verde muestra la aproximación lineal entre la ganancia dada en UHD y el valor real medido.

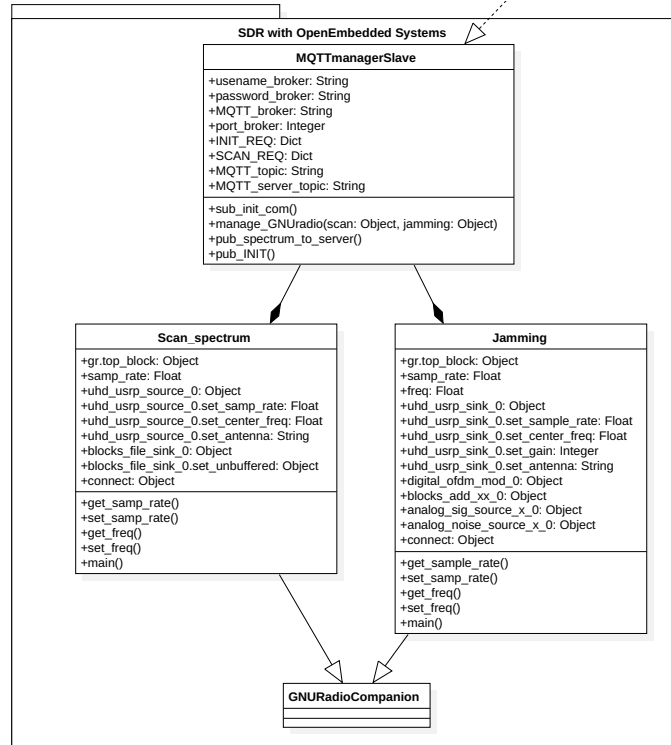
Figura 13: Relación existente entre la ganancia del UHD y la potencia medida con el analizador de espectros.



Para que el dispositivo E310 se comporte como terminal IoT se requiere instalar la librería `paho-mqtt` e implementar la administración por MQTT de los flujogramas de GNU Radio desarrollados para realizar sensado y bloqueo del espectro como operaciones que se ejecutan en modo embebido. La Figura 14 muestra el diagrama de clase que se implementa en cada dispositivo SDR de la red. La clase `MQTTmanagerSlave` se encarga de gestionar los flujogramas de GNU Radio; `Scan_spectrum` y `Jamming` que son los modos de operación de los equipos SDR para sensado y bloqueo del espectro.

4.1.1.2. Modo de operación de sensado del espectro Los nodos de sensado (terminales IoT en recepción) ha sido pensado para ser distribuidos espacial-

Figura 14: Diagrama de clases implementado en el terminal IoT.



mente para monitorear las señales RF que se encuentran en la banda de frecuencias VHF que está entre 88 y 108 MHz. También se prevé la posibilidad de que, por órdenes del usuario administrador, estos nodos cooperen, permitiendo que el sistema se comporte como un sistema de sensado cooperativo, lo cual permite lograr una mejor calidad en el monitoreo del espectro si se compara con un nodo individual, ya que se realiza la observación de la banda de interés desde diferentes puntos, lo cual permite disminuir problemas de sombras, desvanecimiento por multi-trayectoria de señales en RF entre otros fenómenos asociados a la propagación¹.

De lo anterior se deduce que el sensado cooperativo es una forma de diversidad espacial

¹Cichon; Kliks y Bogucka, «Energy-Efficient Cooperative Spectrum Sensing: A Survey», óp.cit.

para el monitoreo del espectro y se clasifica en tres categorías: centralizado²³⁴, distribuido⁵ y *relay assisted*⁶⁷, de acuerdo en la forma como intercambian datos a través la red. Este trabajo de investigación enfoca sus estudios en el sensado cooperativo centralizado que tiene un núcleo llamado centro de fusión (CF) como se muestra en la Figura 15. De acuerdo al modelo de la plataforma presentado en la Figura 3, el CF hace referencia a todas las tecnologías que se encuentran en la capa de componentes de nube. El proceso de monitoreo comienza en el CF, donde se selecciona la frecuencia central, la frecuencia de muestreo y el ancho de banda, los cuales son luego transformados en instrucciones que se envían a todos los equipos SDR conectados en red. Seguidamente, todos los equipos SDR conectados que reciben las instrucciones reportan la información del espectro sensado a través del medio de acceso disponible (Capa de Acceso), que para nuestro caso es WiFi ISM mediante IEEE 802.11n en 2.4 GHz o Ethernet (ver 4.2).

En el modelo del sistema cooperativo de sensado que se observa en la Figura 15, la señal sensada de radio $s[n]$ viaja por caminos diferentes antes de llegar a cada uno de los nodos del sistema de sensado. Para lograr una representación matemática sencilla de este proceso, es posible suponer que $s[n]$ pasa en cada caso por un canal representado como un sistema LIT con respuesta al impulso del canal $h_i[n]$ y que el canal agrega, además, ruido aditivo blanco gaussiano (AGWN por sus siglas en inglés) $w_i[n]$; Cada

²Ghasemi, Amir y Sousa, Elvino S. «Collaborative spectrum sensing for opportunistic access in fading environments». En: *2005 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005* (2005), págs. 131-136. DOI: 10.1109/DYSPAN.2005.1542627.

³Visotsky, E.; Kuffher, S. y Peterson, R. «On collaborative detection of TV transmissions in support of dynamic spectrum sharing». En: *2005 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005* (2005), págs. 338-345. DOI: 10.1109/DYSPAN.2005.1542650.

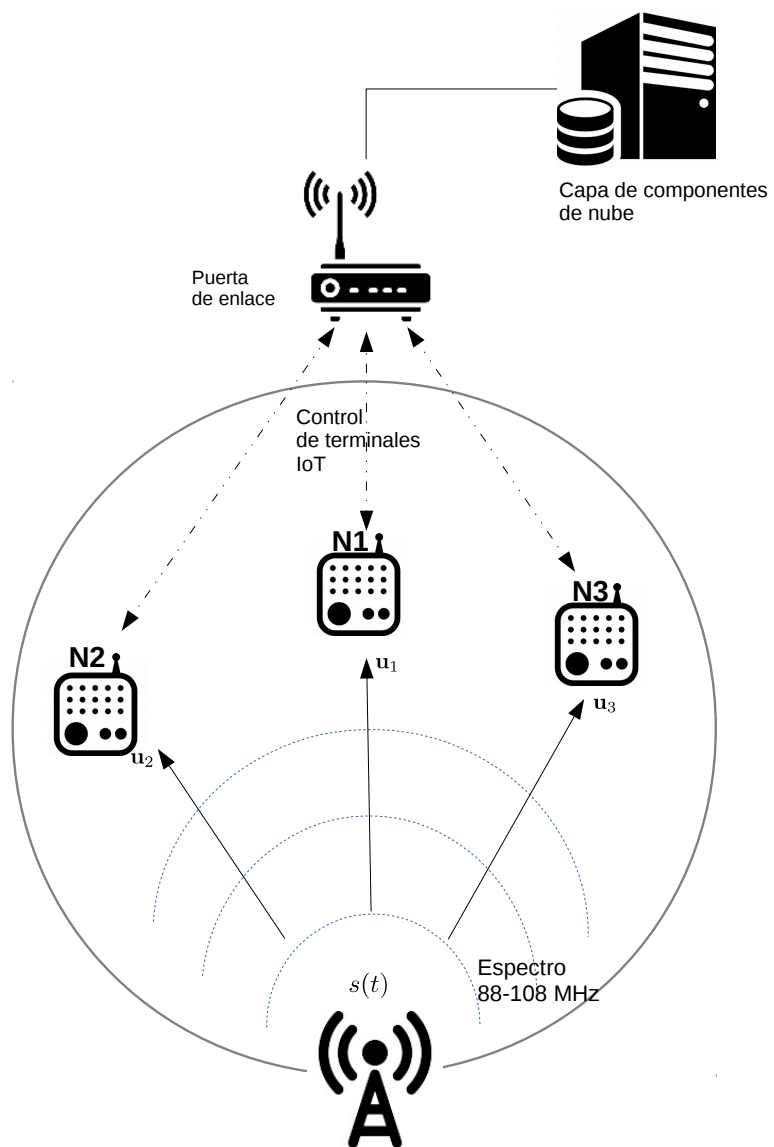
⁴Unnikrishnan, Jayakrishnan y Veeravalli, Venugopal V. «Cooperative Sensing for Primary Detection in Cognitive Radio». En: *IEEE Journal of Selected Topics in Signal Processing* 2.1 (2008), págs. 18-27. ISSN: 1932-4553. DOI: 10.1109/JSTSP.2007.914880. URL: <http://ieeexplore.ieee.org/document/4453896/>.

⁵Li, Zhiqiang; Yu, F. Richard y Huang, Minyi. «A cooperative spectrum sensing consensus scheme in cognitive radios». En: *Proceedings - IEEE INFOCOM* (2009), págs. 2546-2550. ISSN: 0743166X. DOI: 10.1109/INFCOM.2009.5062184.

⁶Ganesan, Ghurumuruhan y Li, Ye. «Cooperative spectrum sensing in cognitive radio, part I: Two user networks». En: *IEEE Transactions on Wireless Communications* 6.6 (2007), págs. 2204-2212. ISSN: 15361276. DOI: 10.1109/TWC.2007.05775. arXiv: 1105.2978v1.

⁷Ganesan, Ghurumuruhan y Li, Ye (Geoffrey). «Cooperative spectrum sensing in cognitive radio, part II: Multiuser networks». En: *Ieee Transactions on Wireless Communications* 6.6 (2007), págs. 2214-2222. ISSN: 1536-1276. DOI: 10.1109/TWC.2007.05776.

Figura 15: Sensado cooperativo centralizado

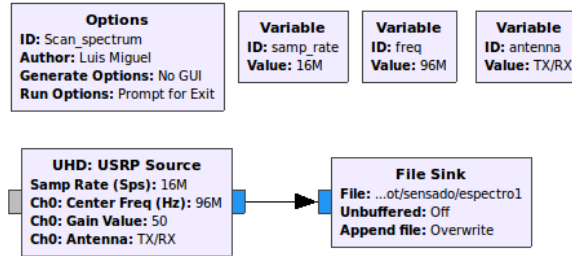


dispositivo SDR recibe una señal $u_i[u]$ que es el resultado de la convolución entre $s[n]$ y $h_i[n]$. Finalmente, todas las señales $u_i[n]$ viajan hasta el CF, donde se combinan como la suma de las señales individuales de cada sensor, donde M es el número total de dispositivos de sensado del espectro, como se muestra la siguiente expresión:

$$\begin{aligned} x[n] &= \frac{1}{M} \sum_{i=0}^{M-1} u_i[n] \\ u_i[n] &= h_i[n] * s[n] + w[n] \end{aligned} \quad (4.1)$$

De acuerdo a los diagramas UML planteados en el capítulo 3, la clase encargada de manejar el monitoreo se llama **Scan_spectrum**, esta clase escanea la señal RF en sus componentes fase y cuadratura, y almacena la señal directamente en la memoria SD del terminal IoT, dado que esta clase hereda las librerías de GNU Radio se puede ver como un flujograma en modo “No GUI” como se muestra en la Figura 16, luego la clase **MQTTmanagerSlave** se encarga de hacer lectura de la señal $x[n]$, codificarla en formato JSON, y reportar los datos al centro de fusión y almacenamiento como se muestra en la Figura 15. Si nos ubicamos dentro del modelo presentado en la Figura 3, el centro de fusión y almacenamiento corresponde a todos los recursos que se encuentran en la capa de componentes de nube.

Figura 16: Flujograma GNU Radio referente a la clase **Scan_spectrum**.



4.1.1.3. Modo de operación de bloqueadores del espectro Para este modo de operación el terminal IoT se comporta como transmisor de RF encargado de interrumpir las comunicaciones entre la transmisión y recepción de las comunicaciones inalámbricas, causando ataques Dos a emisiones clandestinas que operan en la banda VHF 88-108 MHz. Las técnicas de bloqueo pueden ser desde simples interferencias que transmiten continuamente, hasta ataques más sofisticados que explotan las

vulnerabilidades del protocolo⁸⁹. Existen diferentes modelos de bloqueo que dependen de las estrategias de los atacantes, la simplicidad y efectividad, a continuación se revisan algunos:

- **Bloqueador constante**, este bloqueador emite continuamente señal sin tener en cuenta el protocolo utilizado entre el transmisor y el receptor.
- **Bloqueador de engaño**, este bloqueador emite continuamente paquetes regulares de acuerdo al protocolo utilizado entre el transmisor y el receptor. Engaña a los otros nodos para hacerles creer que se produce una transmisión legítima.
- **Bloqueador aleatorio**, un atacante mantiene activo un bloqueador aleatorio durante t_j segundos y durante t_s mantiene el reposo. Este bloqueador en términos energéticos es más eficiente que el bloqueador constante y de engaño.
- **Bloqueador reactivo**, este bloqueador sensa constantemente el canal, en el momento que detecta paquetes envía una señal interferente con el fin de causar una colisión con el receptor.

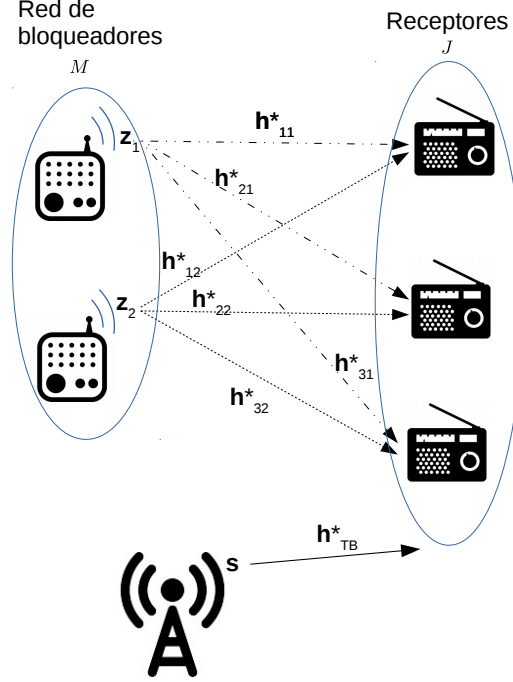
4.1.1.4. Modelo de bloqueadores cooperativos Supongamos que se tiene un sistema de radiodifusión sonora FM donde se emite una señal s para que sea sintonizada por J receptores, como se muestra en la Figura 17; una red de bloqueadores compuesta por M dispositivos SDR que envían señales de interferencia z_i para que los receptores no puedan demodular la señal FM de radio y extraer información.

De acuerdo con el modelo de la Figura 17, la señal recibida por los receptores de la emisora clandestina cuando los bloqueadores están activos, tiene la siguiente forma:

⁸Pelechrinis, Konstantinos; Iliofotou, Marios y Krishnamurthy, Srikanth V. «Denial of Service Attacks in Wireless Networks: The Case of Jammers». En: *IEEE Communications Surveys & Tutorials* 13.2 (2011), págs. 245-257. ISSN: 1553-877X. DOI: 10.1109/SURV.2011.041110.00022.

⁹Grover, Kanika; Lim, Alvin y Yang, Qing. «Jamming and anti-jamming techniques in wireless networks: a survey». En: *International Journal of Ad Hoc and Ubiquitous Computing* 17.4 (2014), pág. 197. ISSN: 1743-8225. DOI: 10.1504/IJAHUC.2014.066419. URL: <http://www.scopus.com/inward/record.url?eid=2-s2.0-84919822418%7B%5C%7DpartnerID=tZ0tx3y1>.

Figura 17: Modelo de bloqueadores cooperativos.



$$\mathbf{Y} = \begin{pmatrix} \mathbf{h}_{1TB}^* \\ \mathbf{h}_{2TB}^* \\ \mathbf{h}_{3TB}^* \end{pmatrix} \circ \begin{pmatrix} \mathbf{s} \\ \mathbf{s} \\ \mathbf{s} \end{pmatrix} + \left(\begin{bmatrix} \mathbf{h}_{11}^* & \mathbf{h}_{12}^* \\ \mathbf{h}_{21}^* & \mathbf{h}_{22}^* \\ \mathbf{h}_{31}^* & \mathbf{h}_{32}^* \end{bmatrix} \circ \begin{bmatrix} \mathbf{z}_1 & \mathbf{z}_2 \\ \mathbf{z}_1 & \mathbf{z}_2 \\ \mathbf{z}_1 & \mathbf{z}_2 \end{bmatrix} \right) + \mathbf{N} \quad (4.2)$$

$$\mathbf{Y} = \mathbf{H}_{TB} \circ \mathbf{S} + (\mathbf{H} \circ \mathbf{Z}) + \mathbf{N}$$

donde $\mathbf{H}_{TB} \in \mathbb{C}^{J \times M}$ es la matriz compuesta por la respuesta al impulso del canal entre la estación ilegal de radio y cada uno de los receptores (J), $\mathbf{S} \in \mathbb{C}^{J \times M}$ es la matriz de tamaño N de la señal transmitida por la estación ilegal de radio y viaja por J caminos diferentes, $\mathbf{H} \in \mathbb{C}^{J \times M}$ corresponde a la matriz del canal entre la red de bloqueadores y los receptores, $\mathbf{Z}$ es la matriz que almacena las señales replicadas de los bloqueadores, y $\mathbf{N}$ es el ruido blanco gaussiano.

Los bloqueadores cooperativos han sido estudiados en¹⁰ con el propósito de mejorar la seguridad en un modelo transmisión-recepción, cuando existen usuarios que intentan escuchar el mensaje, los bloqueadores intentan confundir los usuarios no autorizados, enviando señales codificadas, y asignando diferentes pesos a cada nodo; asumiendo el conocimiento de la respuesta al impulso del canal y nodos con antenas omnidireccionales. En¹¹ investigan la transmisión segura robusta diseñando el problema en canales MISO, donde los bloqueadores cooperativos de múltiples antenas introducen señales de interferencia para degradar los canales de usuarios que intentan escuchar la transmisión y asisten a la recepción en el destino legítimo.

4.1.1.5. Señales usadas en la red de bloqueadores Las señales de bloqueo causan interferencia intencional que interrumpe la comunicación entre el transmisor y el receptor. Entre los parámetros que caracteriza una señal de bloqueo está el ancho de banda utilizado por la señal, el tiempo en el que está activa la señal, la direccionalidad de las antenas utilizadas para atacar al receptor, y el tipo de modulación utilizada. En este trabajo de investigación se estudiaron las siguientes señales:

4.1.1.6. Bloqueo usando tonos Esta técnica ubica un único tono o múltiples tonos dentro del ancho de banda de la señal que se desea bloquear, matemáticamente, la versión banda base se representa mediante:

$$z(t) = A \sin(2\pi ft) \quad (4.3)$$

donde se escogió $f = 10$ kHz como frecuencia de operación.

¹⁰Dong, Lun y col. «Improving wireless physical layer security via cooperating relays». En: *IEEE Transactions on Signal Processing* 58.3 PART 2 (2010), págs. 1875-1888. ISSN: 1053587X. DOI: 10.1109/TSP.2009.2038412. arXiv: 1602.06847.

¹¹Zhang, Qi y col. «Cooperative jamming aided robust secure transmission for wireless information and power transfer in MISO channels». En: *IEEE Transactions on Communications* 63.3 (2015), págs. 906-915. ISSN: 00906778. DOI: 10.1109/TCOMM.2015.2405063.

4.1.1.7. Bloqueo usando ruido blanco gaussiano La red de bloqueadores transmite una señal de ruido para saturar el canal y evitar que los receptores puedan demodular la señal y recibir el mensaje. El ruido por cada nodo de la red en su versión banda base tiene la siguiente forma:

$$z(t) = n_I(t) + jn_Q(t) \quad (4.4)$$

donde $n_I(t) \sim \mathcal{N}(\mu, \sigma^2)$ y $n_Q(t) \sim \mathcal{N}(\mu, \sigma^2)$, μ es la media y σ^2 es la varianza. La densidad de probabilidad gaussiana $\mathcal{N}^{12}$ está definida como:

$$f(x|\mu, \sigma^2) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \quad (4.5)$$

El bloqueador que usa señal interferente de ruido blanco gaussiano se considera un bloqueador de banda ancha, debido a que el AWGN mantiene constante la densidad espectral de potencia (PSD por sus siglas en inglés) en todas las frecuencias.

4.1.1.8. Multiplexión por división de frecuencias ortogonales (ofdm) En OFDM el canal es dividido en subcanales de banda angosta, donde se transmite en paralelo para mantener una alta tasa de transmisión e incrementar la duración del símbolo para combatir la interferencia intersímbolo (ISI por sus siglas en inglés)¹³. La señal modulada por OFDM se representa por la siguiente ecuación:

$$z[n] = \sum_{k=0}^{N-1} s_k e^{j\frac{2\pi kn}{N}} \quad (4.6)$$

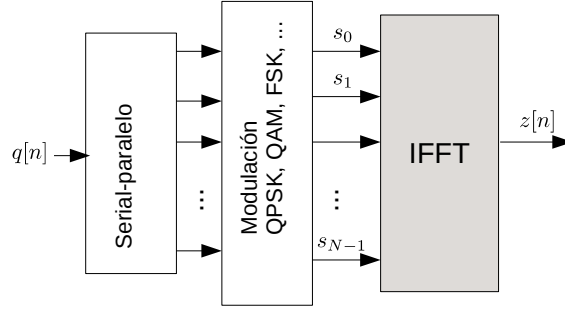
donde N es el número de portadoras OFDM, s_k corresponde a los símbolos complejos transmitidos que pueden corresponder a las modulaciones BPSK, QPSK, QAM, etc. La expresión $e^{j\frac{2\pi kn}{N}}$ corresponde a la transformada inversa de Fourier. La señal discreta que

¹²Riedi, Rudolf H. «An Introduction to Statistical Signal Processing». En: *Journal of the American Statistical Association* 101.475 (2006), págs. 1317-1317. ISSN: 0162-1459. DOI: 10.1198/jasa.2006.s133. URL: <http://www.tandfonline.com/doi/abs/10.1198/jasa.2006.s133>.

¹³Taewon Hwang y col. «OFDM and Its Wireless Applications: A Survey». En: *IEEE Transactions on Vehicular Technology* 58.4 (2009), págs. 1673-1694. ISSN: 0018-9545. DOI: 10.1109/TVT.2008.2004555. URL: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4607239>.

contiene el mensaje aleatorio $q[n]$ pasa por un proceso de paralelización donde se modula digitalmente y se extraen los símbolos s_k , la señal $z[n]$ se obtiene de la transformada rápida inversa de Fourier (IFFT por sus siglas en inglés) de los símbolos complejos, gráficamente el proceso se muestra en la Figura 18.

Figura 18: Generación señal OFDM



4.1.1.9. Ruido modulado en fm Este tipo de señal utiliza el ruido blanco gaussiano como mensaje y lo modula en FM. La señal FM en su versión banda base se representa mediante la siguiente ecuación:

$$z[n] = Ae^{j2\pi\frac{\Delta f}{f_s}\sum_{k=-\infty}^n w[k]} \quad (4.7)$$

donde $w[n] \sim \mathcal{N}(0, 1)$, Δf es la desviación de frecuencia, f_s es la frecuencia de muestreo, y A es la amplitud de la señal. La sensibilidad especifica el cambio de fase basado en una nueva muestra de entrada, es definida como:

$$\beta = \frac{\Delta f}{f_s} \quad (4.8)$$

Dependiendo del valor de la sensibilidad, es posible encontrar dos casos de modulación en frecuencia¹⁴:

¹⁴Haykin, Simon. *Sistemas de Comunicacion*. 1.^a ed. Mexico, DF: LIMUSA WILEY, 2002, págs. 107-130.

- FM banda angosta, β es pequeña comparada con un radián.
- FM banda ancha, β es grande en comparación con un radián.

4.1.1.10. Tono modulado en fm Este tipo de señal utiliza una señal senoidal como mensaje y la modula en FM, como se muestra en la siguiente ecuación:

$$z[n] = Ae^{j2\pi \frac{\Delta f}{f_s} \sum_{k=-\infty}^n \sin(2\pi f k)} \quad (4.9)$$

donde f es la frecuencia del tono que puede estar en el rango $0 < f \leq 15$ kHz, este rango de frecuencias es debido a que típicamente el ancho de banda de la señal de audio para radiodifusión sonora según la recomendación ITU-R 1138-2¹⁵ es de 15 kHz.

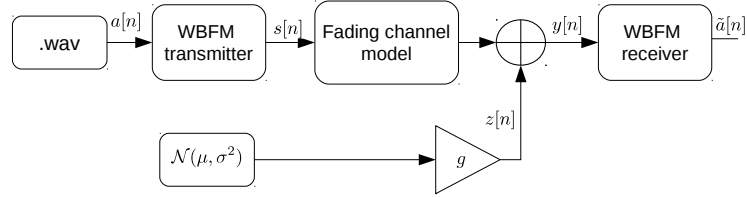
4.1.1.11. Análisis de bloqueo de emisiones clandestinas de radiodifusión sonora en fm que operan en la banda vhf 88-108 mhz

4.1.1.12. Simulación del sistema de bloqueo usando diferentes señales interferentes Se realizaron varias simulaciones en GNUradio para probar el rendimiento de las diferentes señales interferentes descritas en la sección 4.1.1.5. Una señal de audio sin compresión (extensión .wav) fue modulada en FM, luego se hizo pasar por un simulador canal de desvanecimiento de Rician Alimohammad, A. y col. «Compact Rayleigh and Rician fading simulator based on random walk processes». En: *IET Communications* 3.8 (2009), pág. 1333. ISSN: 17518628. DOI: 10.1049/iet-com.2008.0297. URL: <http://digital-library.theiet.org/content/journals/10.1049/iet-com.2008.0297>, se agregó una señal de interferencia con ganancia variable g , finalmente, simulando la parte receptora, se realizó la demodulación FM la señal recibida $\tilde{a}[n]$ como se observa en las figuras 19, 20, 21, 22 y 23.

¹⁵UIT-R. «ITU-R SM.1138-2 Determination of necessary bandwidths including examples for their calculation and associated examples for the designation of emissions». En: 1995.June (1998).

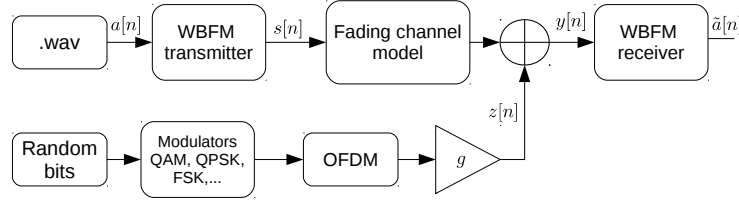
En la Figura 19 se muestra el modelo de la simulación para el caso en que la señal interferente es un ruido blanco gaussiano.

Figura 19: Simulación de señal interferente AGWN.



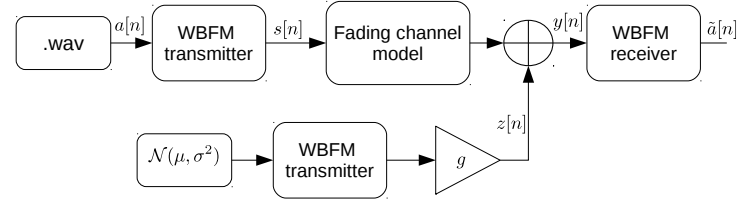
El caso en que la señal interferente es de tipo OFDM se representa en la Figura 20, donde se utilizaron bits aleatorios con una misma semilla, luego pasaron por un modulador digital (8PSK) y finalmente por un bloque OFDM.

Figura 20: Simulación de señal interferente OFDM.



El siguiente caso es cuando una señal de ruido con distribución normal se pasa por un modulador FM como se muestra en la Figura 21.

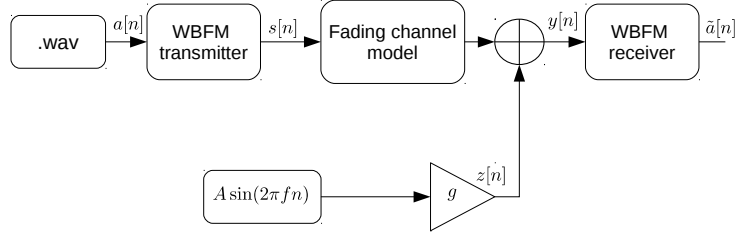
Figura 21: Simulación de ruido gaussiano modulado en FM.



También, se realizó la simulación usando un tono senoidal como se muestra en la Figura 22 donde el tono opera de manera simple sin realizar ninguna transformación, su

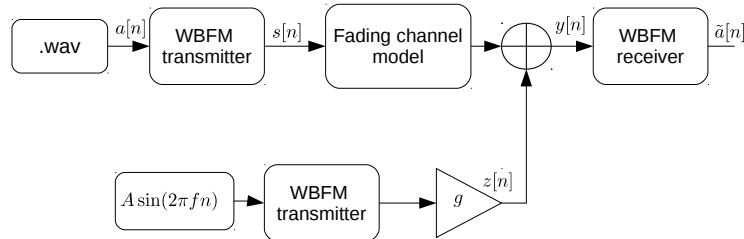
frecuencia de operación fue de 10 kHz.

Figura 22: Múltiples tonos como señal de interferencia.



Finalmente, se realizó la simulación de un tono modulante en FM, el tono se seleccionó a una frecuencia de 1 kHz, la modulación FM del tono se realizó con una desviación de frecuencia de $\Delta f = 75$ kHz, su esquema general se muestra en la Figura 23.

Figura 23: Tono modulante en FM como señal de interferencia.



Las simulaciones se realizaron variando la ganancia g de las señales de los bloqueadores con el fin de comparar la señal de audio recibido ($\tilde{a}[n]$) con el audio original ($a[n]$) como se muestra en las figuras 19, 20, 21, 22 y 23 mediante diferentes análisis como: distancia de correlación y porcentaje de palabras reconocidas por un reconocedor de voz. La distancia de correlación permite encontrar la señal que mejor se comporta al momento de cambiar la forma del audio recibido de la emisión clandestina, este análisis se realiza mediante la comparación de los espectrogramas de audio original y recibido, la distancia de correlación es una medida para encontrar la dependencia entre dos señales. El espectrograma permite analizar la señal en tiempo-frecuencia y se calcula mediante

la transformada de Fourier de tiempo corto (STFT por sus siglas en inglés)¹⁶¹⁷ que está definida matemáticamente como:

$$A_l[k] = \sum_{n=-N/2}^{N/2} g[n]a[n + lH]e^{-j2\pi kn/N}, \quad l = 0, 1, 2, \dots \quad (4.10)$$

donde $a[n]$ es la señal de audio, l número de cuadro temporal, $g[n]$ es una ventana, para este trabajo se utilizó una ventana tipo Blackman-Harris, y H es el número de muestras para análisis. Se calculó la distancia de correlación con la magnitud de los espectrogramas para el audio original y el audio recibido.

$$\begin{aligned} \mathbf{d}_l &= 1 - \frac{\langle |A_l[k]|^2 - \mu_{a,l}, |\tilde{A}_l[k]|^2 - \mu_{\tilde{a},l} \rangle}{\| |A_l[k]|^2 - \mu_{a,l} \|_2 \| |\tilde{A}_l[k]|^2 - \mu_{\tilde{a},l} \|_2} \\ d_{corr} &= \|\mathbf{d}\|_2 \end{aligned} \quad (4.11)$$

donde $\langle \cdot, \cdot \rangle$ es el producto punto entre las magnitudes centradas del espectrograma por cada cuadro de tiempo, $\tilde{A}_l$ es el espectrograma del audio demodulado por el receptor, $\mu_{a,l}, \mu_{\tilde{a},l}$ son las medias correspondientes a las magnitudes de los espectrogramas del audio original y audio recibido respectivamente por cada cuadro de tiempo. La distancia de correlación se calculó para analizar el efecto de los bloqueadores en la forma del espectro del audio recibido a medida que se incrementaba la ganancia de los bloqueadores.

En la Figura 24 se presentan los resultados del análisis de la norma de la distancia de correlación con respecto a la energía de la señal recibida, la distancia de correlación aumenta a medida que se eleva el coeficiente de amplificación (g) de la señal interferente. Con base en los resultados de las las simulaciones presentados en la Figura 24 se observa que las señales AGWN y OFDM tienen un crecimiento más rápido en la distancia de correlación a medida que se incrementa la energía de la señal de bloqueo, también, se observan tres zonas que podemos agrupar de la siguiente forma:

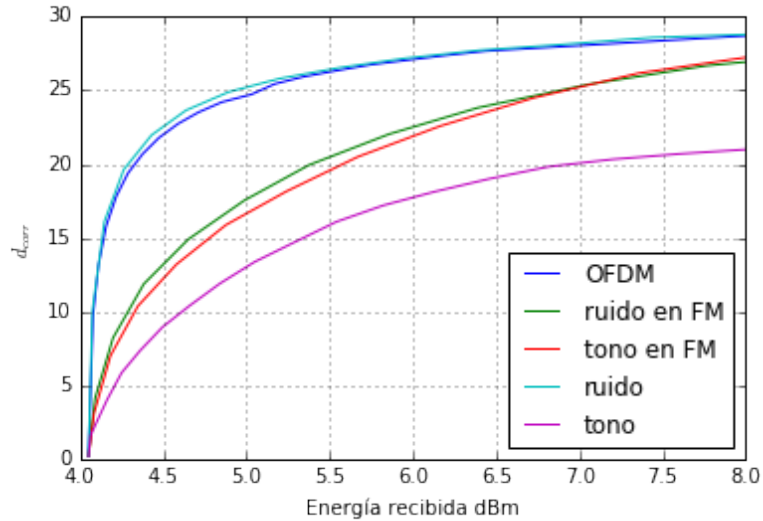
¹⁶Ersoy, Okan K. «A Comparative Review of Real and Complex Fourier-Related Transforms». En: *Proceedings of the IEEE* 82.3 (1994), págs. 429-447. ISSN: 15582256. DOI: 10.1109/5.272147.

¹⁷Lim, J.S. «Signal Reconstruction and Estimation from Short-Time Fourier Transform Representation: A Summary of Recent Results». En: *IFAC Proceedings Volumes* 18.5 (1985), págs. 1421-1424. ISSN: 14746670. DOI: 10.1016/S1474-6670(17)60764-X. URL: <https://linkinghub.elsevier.com/retrieve/pii/S147466701760764X>.

- Señal OFDM y ruido AGWN.
- Señal ruido modulado en FM y tono modulado en FM.
- Señal de un tono.

De acuerdo a las gráficas de la distancia de correlación presentes en la Figura 24, las señales que tienen los efectos más negativos sobre la forma del espectro del audio de prueba son la OFDM y el ruido, y la señal que presenta menor distancia de correlación es el tono senoidal, sin embargo, este criterio no es suficiente para determinar cual es la mejor señal para usar en la red de bloqueadores, para ello también se va a analizar el ancho de banda ocupado, comportamiento con el canal adyacente, y análisis de la información perdida usando un reconocedor de voz, este último es de los más importantes porque se basa en la información perdida a diferencia de la distancia de correlación que sólo compara de acuerdo a la forma del espectro del audio de la señal recibida.

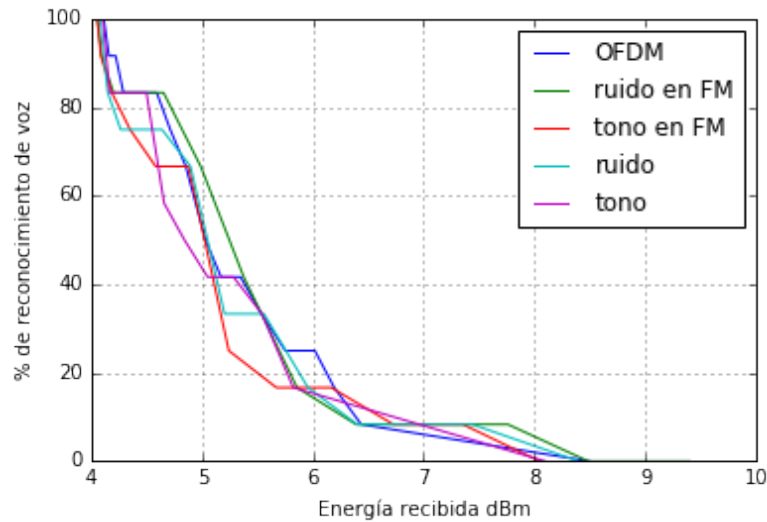
Figura 24: Simulación de las señales usadas para bloquear.



Se analizaron las señales de bloqueo usando un reconocedor de voz para transcribir el audio recibido en texto y así poder realizar comparaciones entre el número de palabras enviadas y el número de palabras recibidas, el reconocedor de voz usado es una API de google que se conecta a *Google Cloud Speech API*, por lo que no se hará énfasis detallado en su funcionamiento porque su procesamiento está en la nube y los modelos

de entrenamiento del algoritmo son propios de la compañía, inicialmente, se envió un audio de prueba en el que se garantizara que el reconocedor de voz pudiera transcribir el 100 % de la información enviada, este audio de prueba se representa con $a[n]$ y se puede observar en los diagramas de bloques de las figuras 19, 20, 21, 22 y 23 luego, se realizaron las simulaciones para recibir la señal de audio demodulada $\tilde{a}[n]$ mientras se incrementaba la ganancia g de cada bloqueador, finalmente, cada señal de audio demodulada se envió a la API para comparar la información transcrita de la señal recibida cuando el bloqueador está activo con la señal transcrita del audio original y encontrar el porcentaje de palabras reconocidas por la API. La Figura 25 muestra los resultados del análisis de del porcentaje de palabras reconocidas por la API en función de la energía medida en la señal recibida, donde se puede observar el comportamiento que siguen las 5 señales estudiadas.

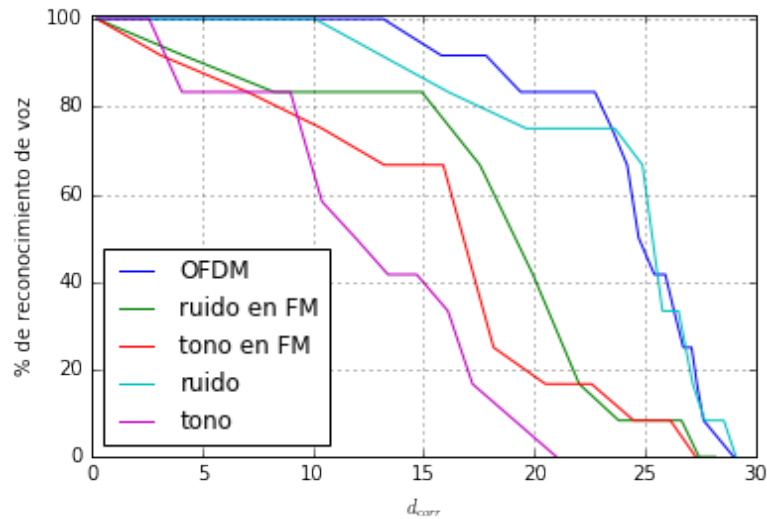
Figura 25: Porcentaje de reconocimiento de voz en función de la energía recibida antes de la demodulación.



La Figura 26 muestra el porcentaje de reconocimiento de voz en función de la distancia de correlación usando las diferentes señales de bloqueo, esta gráfica permite observar los puntos en los que la distancia de correlación se traduce en pérdida de información, cada señal utilizada tiene su propio comportamiento de la distancia de correlación debido a que cada señal es diferente, sin embargo, el porcentaje de reconocimiento de voz se ve afectado a medida que incrementa la distancia de correlación, con base en esta relación se puede encontrar la señal que requiere menor distancia de correlación

para lograr mayor pérdida de información, lo que significa menor energía en la señal de bloqueo, la señal del tono senoidal es la primera en llegar a cero en el porcentaje de reconocimiento de voz cuando la distancia de correlación supera el valor de 20, la distancia de correlación es una medida adimensional.

Figura 26: Porcentaje de reconocimiento de voz en función de la distancia de correlación.



4.1.1.13. Análisis de ancho de banda de las señales usadas para la red de bloqueadores Ahora, analizaremos las señales de bloqueo respecto a el ancho de banda ocupado. Los valores del ancho de banda dependen del tipo de emisiones definidas en la sección 3 del Reglamento de Radiocomunicaciones¹⁸. La recomendación UIT-R SM.328-10¹⁹ emplea métodos analíticos para determinar el ancho de banda ocupado por una señal, y la recomendación UIT-R SM 1138²⁰ incluye las fórmulas necesarias para calcular el ancho de banda dependiendo el tipo de señal a estudiar,

¹⁸UIT. «Reglamento de Radiocomunicaciones». En: XXXIII.2 (2016), págs. 81-87. ISSN: 0717-6163. DOI: 10.1007/s13398-014-0173-7.2. arXiv: 9809069v1 [arXiv:gr-qc]. URL: <http://www.ncbi.nlm.nih.gov/pubmed/15003161%7B%5C%7D5Cnhttp://cid.oxfordjournals.org/lookup/doi/10.1093/cid/cir991%7B%5C%7D5Cnhttp://www.scielo.cl/pdf/udecada/v15n26/art06.pdf%7B%5C%7D5Cnhttp://www.scopus.com/inward/record.url?eid=2-s2.0-84861150233%7B%5C%7DpartnerID=tZ0tx3y1>.

¹⁹UIT-R. *UIT-R SM.328-10 Definiciones Emisión no esencial Emisiones no deseadas*. 1999. ISBN: 1948195119.

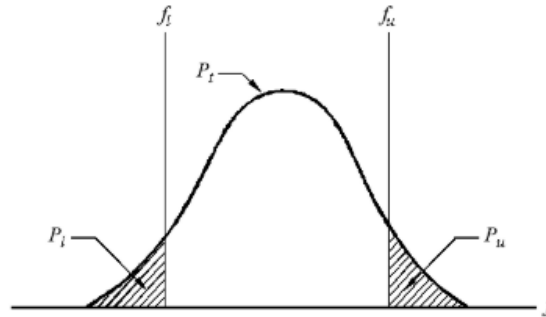
²⁰Íd., «ITU-R SM.1138-2 Determination of necessary bandwidths including examples for their calculation and associated examples for the designation of emissions», óp.cit.

por ejemplo, para una señal modulada en frecuencia de radiodifusión sonora el ancho de banda se calcula de la siguiente forma:

$$B = 2f_{maxm} + 2\Delta f K \quad (4.12)$$

donde B es el ancho de banda, Δf es la desviación de frecuencia, K es un factor que varía de acuerdo al tipo de emisión, típicamente este valor es 1 para radiodifusión sonora, $\Delta f = 75$ kHz y $f_{maxm} = 15$ kHz como ancho de banda para la voz. Para encontrar el ancho de banda de manera empírica, la recomendación UIT-R SM.328-10 dice se puede integrar entre dos límites de frecuencia la PSD encontrada como se muestra en la Figura 27.

Figura 27: Definición de ancho de banda como se formula en el artículo 1, No.1153 del RR.



De acuerdo con la Figura 27, P_t es la potencia total, P_l es la potencia inferior fuera de banda, P_u es la potencia superior fuera de banda, f_l es la frecuencia inferior, y f_u es la frecuencia superior. f_l es la frecuencia más alta que en la que se cumpla la siguiente condición $P_l > \frac{\beta}{2} P_t$, desde el otro lado del espectro para encontrar f_u se busca la frecuencia más baja que cumpla la siguiente condición $P_u > \frac{\beta}{2} P_t$, por lo tanto, el ancho de banda es $f_u - f_l$.

De acuerdo con lo anterior se realizaron simulaciones para comprobar que las señales utilizadas en la red de bloqueadores tengan el comportamiento esperado, una vez finalizado ese proceso se capturó el espectro realizando transmisiones usando el terminal IoT USRP E310 y se calculó el ancho de banda de la señal de acuerdo con UIT-R SM.328-

10, luego, se comparó el espectro medido con el espectro simulado en GNUradio para observar las diferencias entre la señal real banda-base y la señal simulada. Las gráficas se centraron a la frecuencia de 94 MHz donde se hicieron las pruebas de transmisión, la selección de esta frecuencia se tuvo en cuenta con base en la información del Min-TIC para el Área Metropolitana de Bucaramanga (AMB), y también se comprobó que estuviera libre realizando mediciones previas en el laboratorio.

La Figura 28 representa el espectro del ruido blanco como señal interferente, la simulación (línea azul) muestra el comportamiento de ruido blanco, es decir, que la densidad espectral de potencia es uniforme en todas las frecuencias, sin embargo, la simulación no se realizó para todas las frecuencias, por eso la línea azul no es continua en todo el ancho de banda observado, debido a que se utilizó una frecuencia de muestreo de 125 kHz. El espectro capturado (línea verde) muestra un comportamiento diferente al de la señal simulada, esto es debido a que el USRP E310 tiene un banco de filtros en transmisión y recepción para evitar transmitir y recibir información de otras bandas. Para la transmisión se utilizó una frecuencia de muestreo 125 kHz en el DAC, en recepción se usó una frecuencia de muestreo de 500 kHz en el ADC. Se calculó el ancho de banda de la señal de ruido recibida y dio como resultado 115.66 kHz, este ancho de banda se representa gráficamente por la señal que está en medio de las dos líneas verticales rojas, y las líneas verticales negras punteadas representan el límite máximo en ancho de banda.

La Figura 29 representa el espectro de la señal OFDM que se usó para interferir emisiones clandestinas, la gráfica azul representa la simulación y la gráfica verde representa la medición realizada con el USRP E310. La señal OFDM utilizada tiene un total de 128 portadoras de las cuales se usaron 100, la frecuencia de muestreo del DAC (para transmisión) fue de 125 kHz, y la frecuencia de muestreo en el ADC (para recepción) fue de 500 kHz. Se calculó el ancho de banda de la señal recibida y dio como resultado 188.96 kHz, este ancho de banda se representa gráficamente por la señal que está en medio de las dos líneas verticales rojas, y las líneas verticales negras punteadas representan el límite máximo en ancho de banda.

La Figura 30 representa el espectro de la señal de ruido modulado en FM, la gráfica

Figura 28: Señal simulada y medida del ruido.

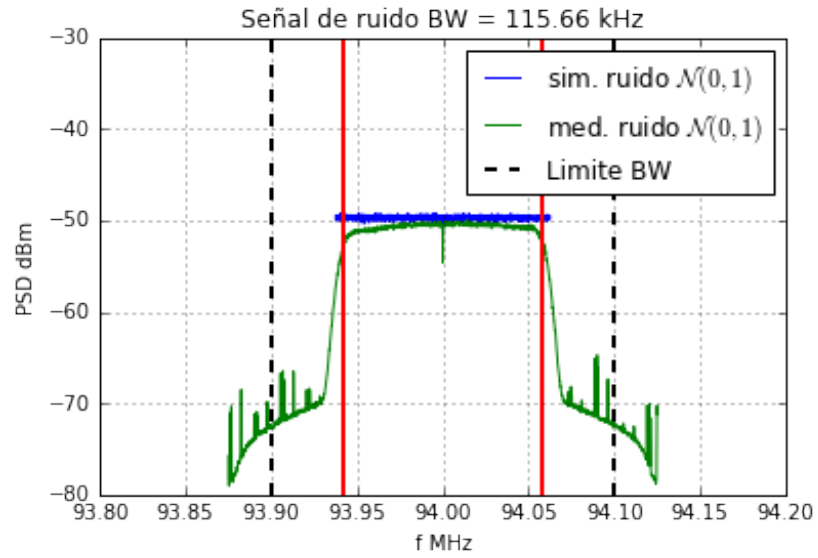
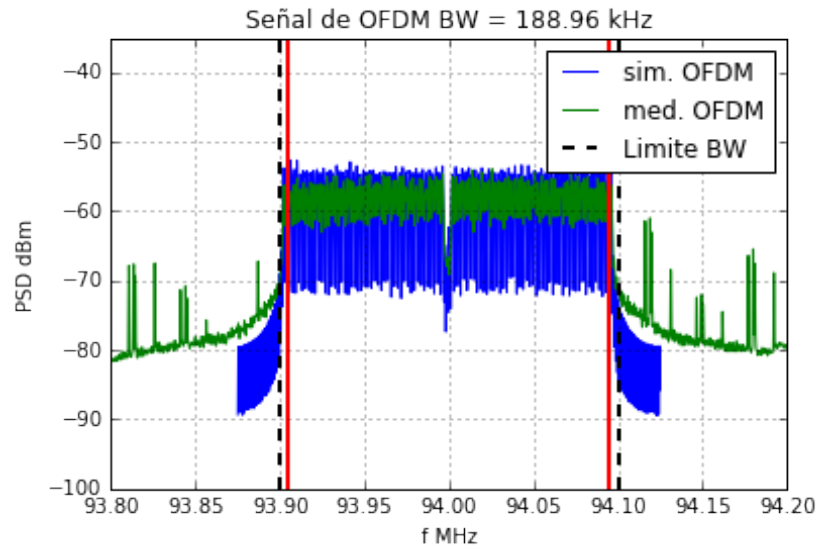
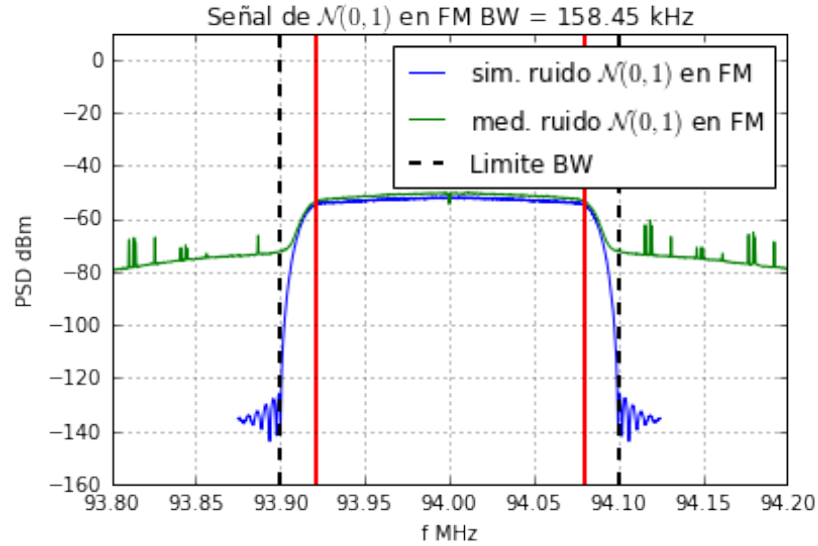


Figura 29: Señal simulada y medida de la OFDM.



azul corresponde a la simulación, y la gráfica verde corresponde a la señal medida por el USRP E310, la señal de ruido $\mathcal{N}(\mu, \sigma)$ se utilizó con una media ($\mu = 0$) y desviación estándar ($\sigma = 1$), la modulación FM se utilizó con un $\Delta f = 75$ kHz que es la desviación de frecuencia máxima permitida de acuerdo con el Plan Técnico de Radiodifusión Sonora para Colombia. Se calculó el ancho de banda de la señal recibida y dio como resultado 158.45 kHz, este ancho de banda se representa gráficamente por la señal que está en medio de las dos líneas rojas, y las líneas verticales negras punteadas representan el limite máximo en ancho de banda.

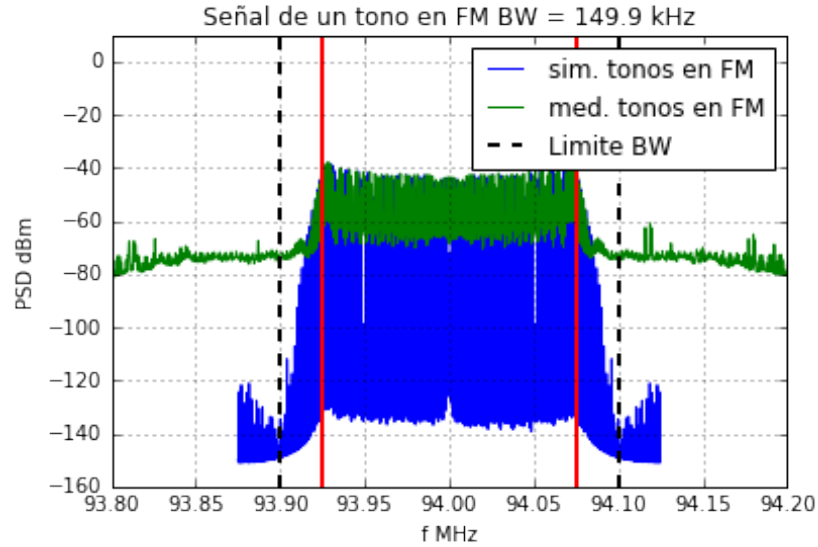
Figura 30: Señal simulada y medida del ruido modulado en FM.



La Figura 31 representa el espectro de un tono modulado en FM, la gráfica azul corresponde a la simulación y la gráfica verde corresponde a la señal medida por el USRP E310. El tono utilizado fue una señal senoidal con frecuencia de 1 kHz, la modulación FM se utilizó con un $\Delta f = 75$ kHz al igual que en el ruido modulado en FM. Se calculó el ancho de banda de la señal recibida y dio como resultado 149.9 kHz, este ancho de banda se representa gráficamente por la señal que está en medio de las dos líneas rojas, y las líneas verticales negras punteadas representan el limite máximo en ancho de banda.

Por último, la Figura 32 representa el espectro de un tono simulado (gráfica azul) y medido (gráfica verde) a 10 kHz, el ancho de banda medido es de 20.63 kHz, teórica-

Figura 31: Señal simulada y medida de un tono modulado en FM.



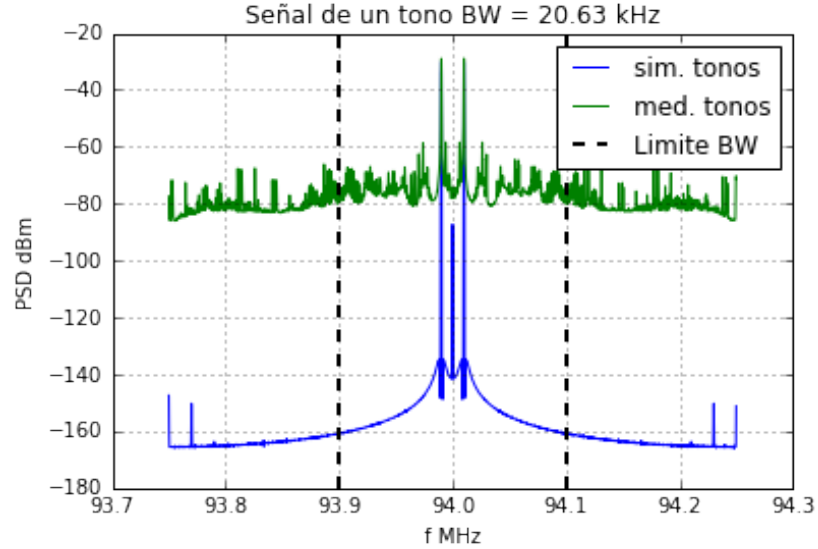
mente tendría que ser 20 kHz, sin embargo, el método para calcular el ancho de banda se basa en una aproximación con la FFT.

De las 5 señales estudiadas anteriormente podemos observar que las señales medidas (gráfica verde de las figuras 28, 29, 30, 31 y 32) presentan emisiones no deseadas (por fuera de la línea punteada negra), éstas emisiones también son conocidas como emisiones espurias que corresponden a emisiones armónicas, parásitas, productos de intermodulación y de conversión de frecuencia.

4.1.1.14. Efecto de interferencia con canales adyacentes Para visualizar el efecto que podría tener la señal de bloqueo sobre los canales adyacentes se realizó un experimento en el caso donde el bloqueo ocurre en un canal adyacente a una emisora comercial que trabaja en 90.7 MHz. También se capturó el espectro de la emisora sin realizar bloqueo de canal adyacente con el fin de graficar su comportamiento promedio durante un periodo corto de tiempo, esto se realizó con el fin de observar el comportamiento normal de los canales adyacentes a la emisora comercial de prueba.

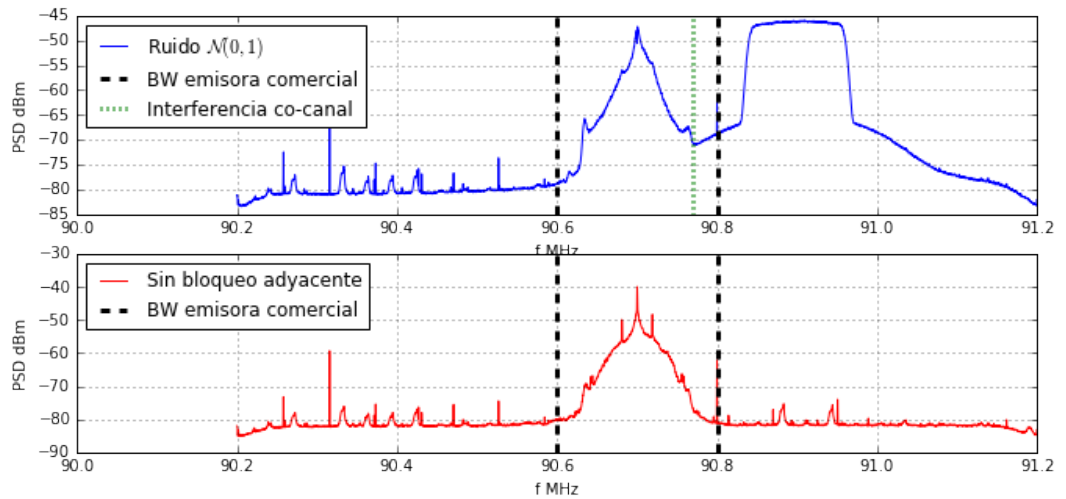
La Figura 33 muestra el bloqueo de un canal adyacente con señal de ruido donde una

Figura 32: Señal simulada y medida de un tono a 10 kHz.



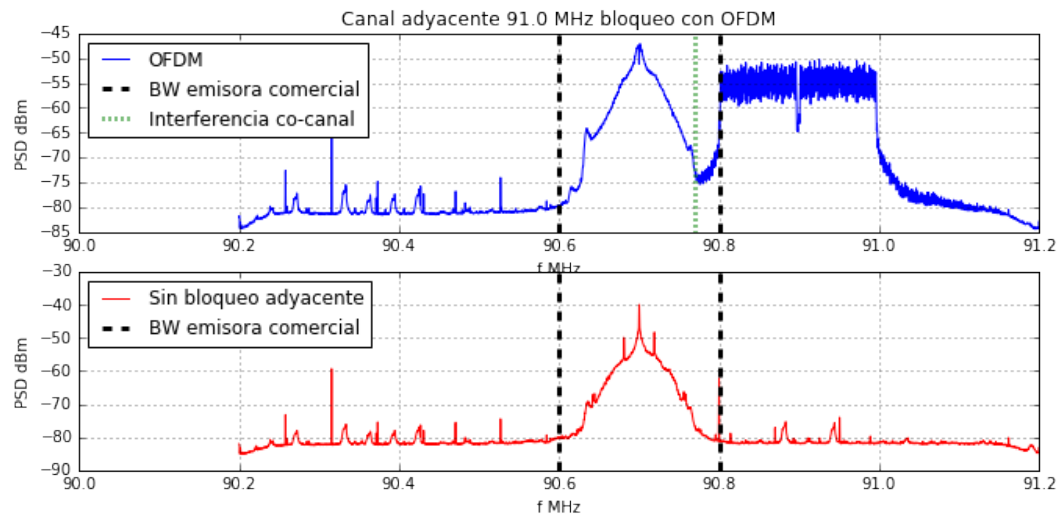
parte de la señal de bloqueo entra en una zona prohibida de la emisora comercial, esta zona prohibida son los 200 kHz definidos por la recomendación ITU-R BS.450-3 para Colombia (delimitada por las líneas verticales negras punteadas), entre la línea vertical verde punteada y la línea vertical negra punteada se observa gráficamente la interferencia co-canal que se refleja en distorsiones al demodular el audio, la gráfica roja muestra la emisora comercial sin bloqueo de canal adyacente.

Figura 33: Canal adyacente bloqueado con una señal de ruido $\mathcal{N}(0,1)$.



La Figura 34 muestra el bloqueo de un canal adyacente con una señal de OFDM donde al igual que con la señal de ruido, una parte de la señal de bloqueo entra a la zona prohibida, este efecto se puede observar con la señal delimitada entre la línea vertical verde punteada y la línea vertical negra punteada, la gráfica roja muestra la emisora comercial sin bloqueo de canal adyacente, es decir, como opera normalmente.

Figura 34: Canal adyacente bloqueado con una señal de OFDM.



La Figura 35 muestra el bloqueo de un canal adyacente con una señal de ruido modulado en FM donde al igual que con las señales de ruido y OFDM se observa que una parte de la señal de bloqueo entra a la zona prohibida, este efecto se puede observar con la señal delimitada entre la línea vertical verde punteada y la línea vertical negra punteada, la gráfica roja muestra la emisora comercial sin bloqueo de canal adyacente.

La Figura 36 muestra el bloqueo de un canal adyacente con una señal de un tono modulado en FM, donde gráficamente se observa que la señal de bloqueo aparentemente no tiene efecto sobre la emisora vecina, esta es una característica necesaria que debe cumplir la señal de bloqueo, la gráfica roja muestra el comportamiento usual de la emisora cuando sus canales adyacentes están aparentemente libres de otras emisoras.

La Figura 37 muestra el bloqueo de un canal adyacente con una señal de un tono senoidal, gráficamente se observa que la señal de bloqueo no tiene efecto sobre la emisora

Figura 35: Canal adyacente bloqueado con una señal de ruido modulado en FM.

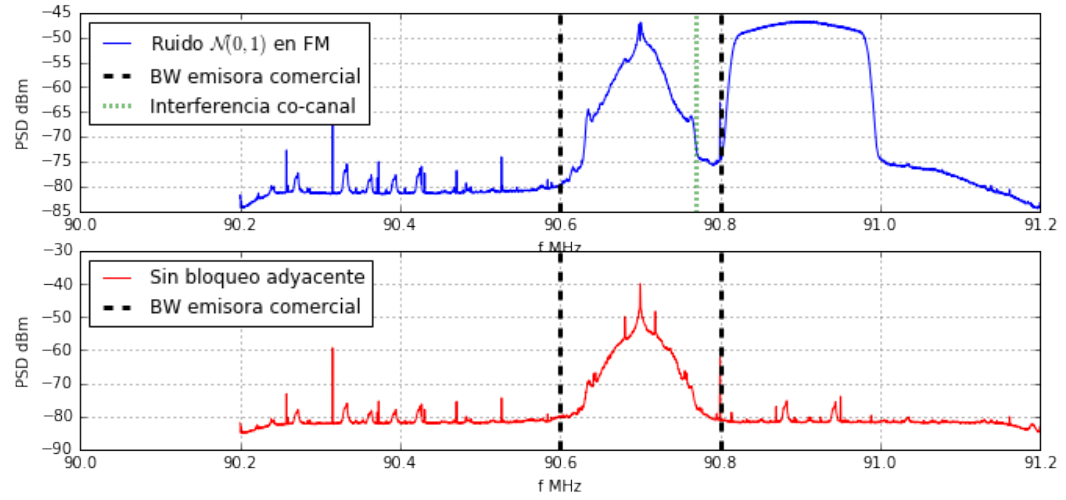
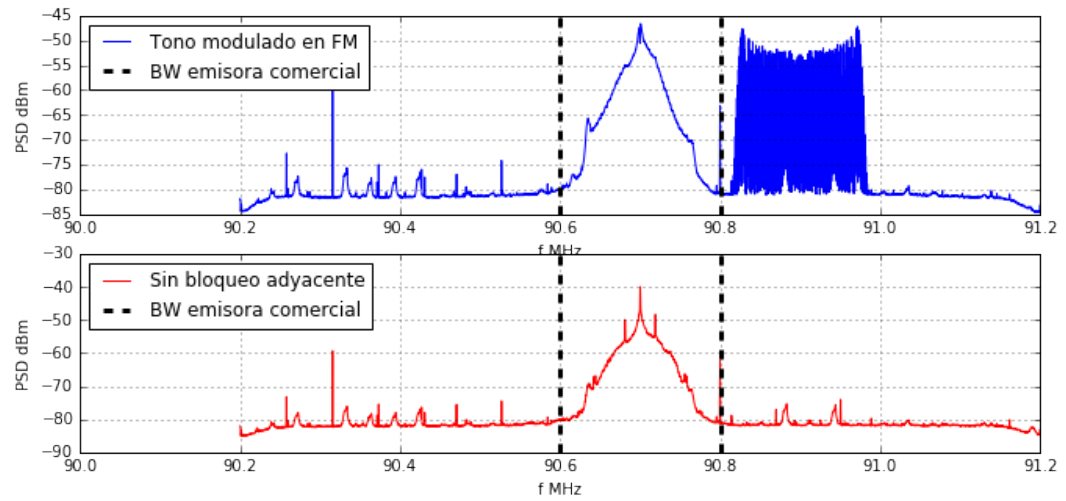
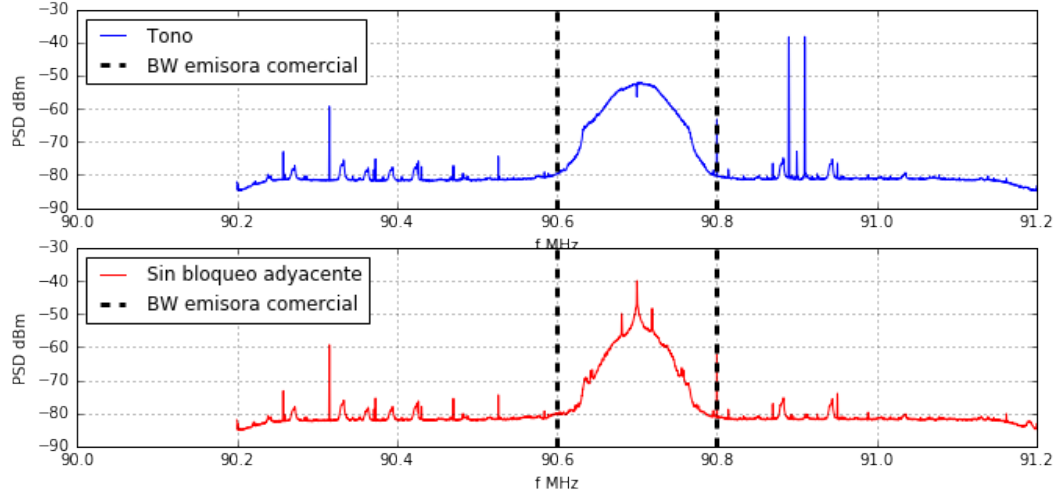


Figura 36: Canal adyacente bloqueado con una señal de un tono modulado en FM.



vecina al igual que con la señal del tono modulado en FM, este efecto también se puede notar en la calidad del audio demodulado de la emisora donde no se presenta molestia alguna para el usuario final.

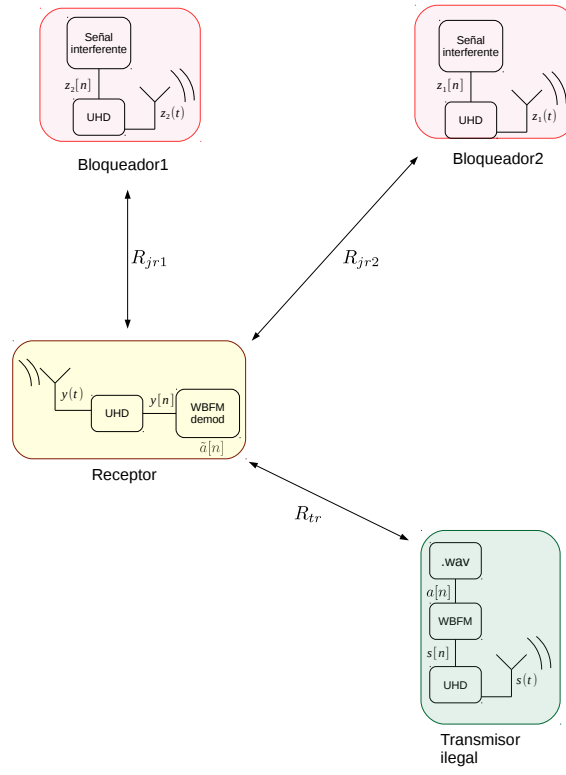
Figura 37: Canal adyacente bloqueado con una señal de un tono senoidal.



4.1.1.15. Análisis de bloqueo cooperativo La implementación del prototipo de bloqueadores fue construida para experimentar, y verificar el bloqueo de emisiones clandestinas en FM para la banda de 88-108 MHz. Para analizar el bloqueo cooperativo se utilizaron 4 USRP E310: un receptor, un transmisor y dos bloqueadores; como se muestra en la Figura 38, la transmisión ilegal consistió en enviar un archivo de audio (extensión .wav), señal $a[n]$, pasado por un modulador FM banda base antes de ser transmitida $s[n]$, luego, la señal se transforma a paso-banda por la componente de radio en transmisión, finalmente, se convierte en onda electromagnética cuando sale de la antena, señal representada por $s(t)$. El transmisor fue un USRP E310, en la gráfica se representa por el bloque verde, luego, se realiza una comparación entre la señal original $a[n]$ y la señal $\tilde{a}[n]$ (señal demodulada por el receptor, representada por el bloque amarillo) cuando los bloqueadores están activos (bloques rojos).

La comparación entre las señales $a[n]$ y $\tilde{a}[n]$ analiza la distancia de correlación en función de la energía recibida, el porcentaje de reconocimiento de voz en función de la energía

Figura 38: Modelo general del experimento para comparar las señales usadas por los bloqueadores



recibida, y el porcentaje de reconocimiento de voz en función la distancia de correlación, el experimento se realizó de tres formas de acuerdo a la combinación en la activación de los bloqueadores como se describe a continuación:

- Con el bloqueador 1 activo y el bloqueador 2 desactivado (bloqueador no cooperativo T_{j1}).
- Con el bloqueador 1 desactivado y el bloqueador 2 activo (bloqueador no cooperativo T_{j2}).
- Con el bloqueador 1 activo y el bloqueador 2 activo (bloqueador cooperativo $T_{j1} + T_{j2}$).

La Figura 39 muestra el comportamiento de del porcentaje de reconocimiento de voz cuando los bloqueadores se comportan de manera no cooperativa T_{j1} y T_{j2} (gráficas azul y verde), y cuando se comportan de manera cooperativa $T_{j1} + T_{j2}$ (gráfica roja).

De la Figura 39 se puede observar que con el bloqueo cooperativo se requiere menor energía para que el porcentaje de reconocimiento de voz disminuya rápidamente acercándose a cero, es decir, un porcentaje de reconocimiento de voz igual a cero significa que no fue posible extraer información con el reconocedor de voz, interrumpiendo la comunicación entre el transmisor y el receptor. La señal de bloqueo que primero llegó a cero en el porcentaje de reconocimiento de voz fue la señal de un tono senoidal.

La Figura 40 muestra la distancia de correlación en función de la energía recibida para el bloqueo cooperativo (gráfica roja) y no cooperativo (gráficas azul y verde) en las 5 señales usadas en la red de bloqueadores. De esta Figura se puede observar que la distancia de correlación incrementa más rápido cuando se utiliza el bloqueo cooperativo, también, se compararon las diferentes señales interferentes para el bloqueo cooperativo, y se observa que la señal de un tono presenta un crecimiento más lento en la distancia de correlación a medida que incrementa la energía del canal.

La Figura 41 muestra el porcentaje de reconocimiento de voz en función de la distancia de correlación, el efecto del bloqueo cooperativo no es tan alto como en las gráficas

Figura 39: Porcentaje de reconocimiento de voz en función de la energía recibida por el canal para los casos de bloqueo cooperativo y no cooperativo.

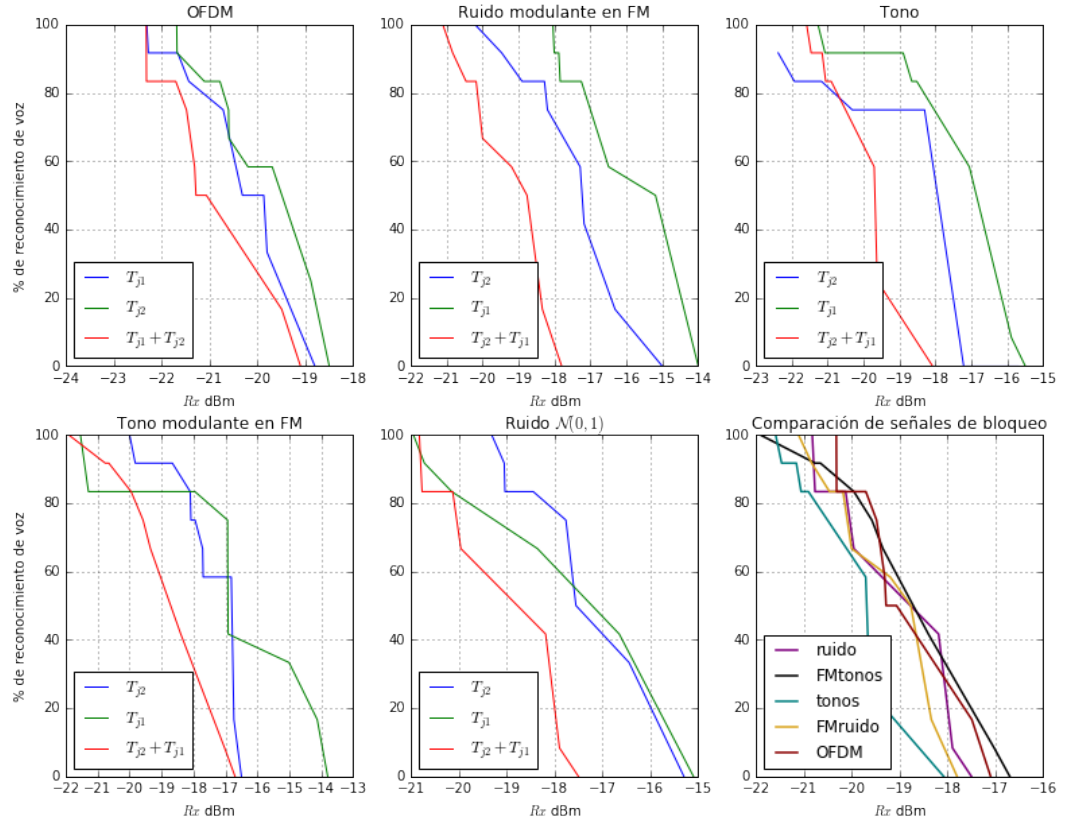


Figura 40: Distancia de correlación en función de la energía del canal

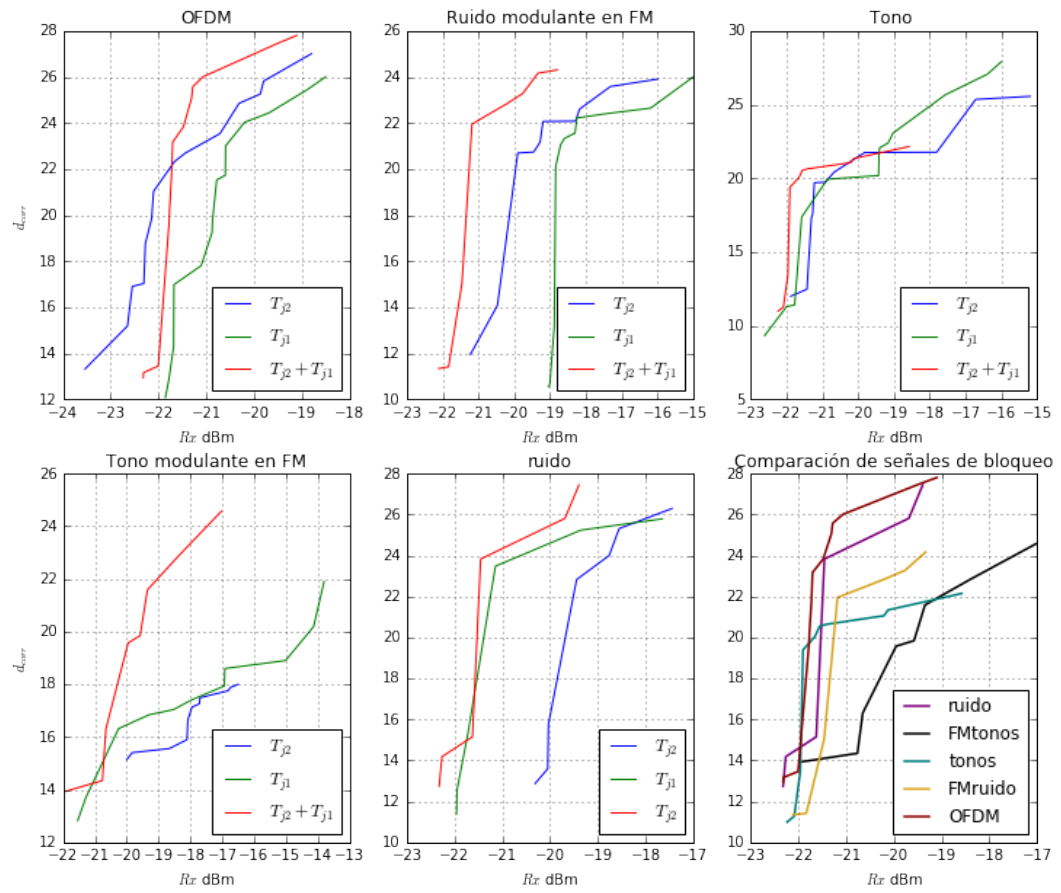
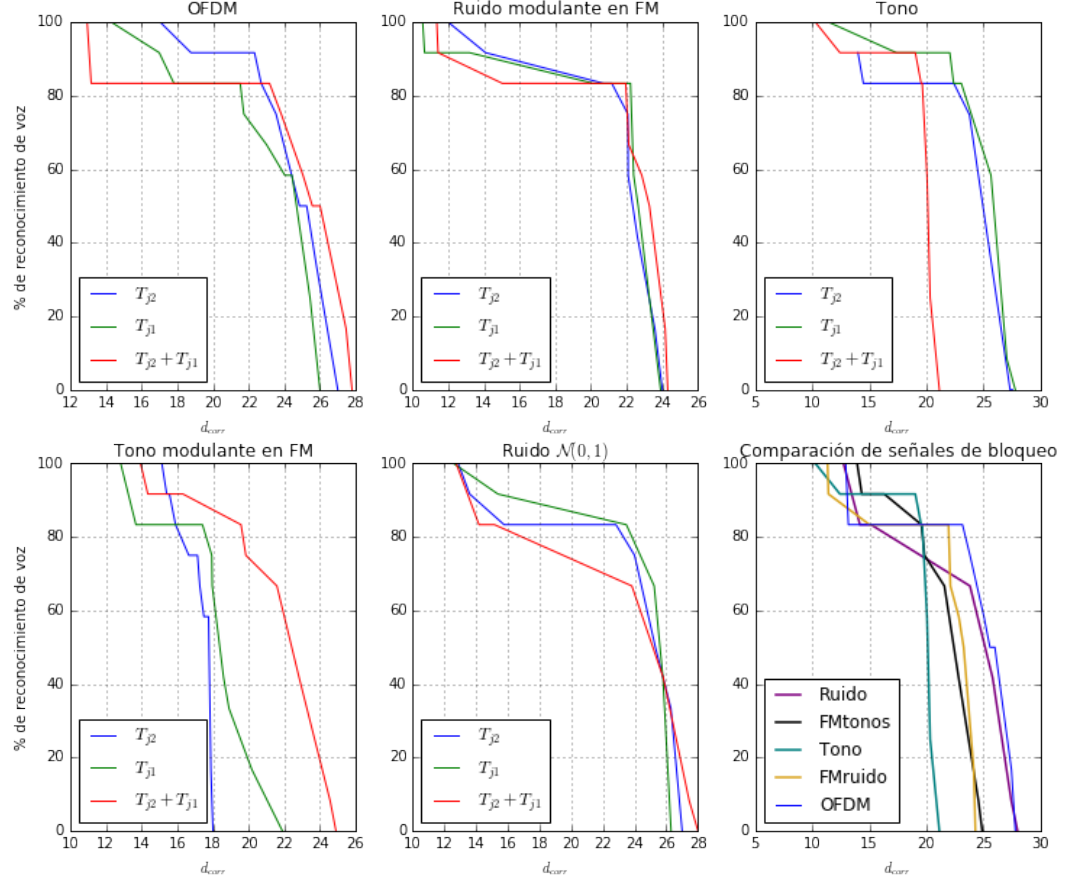


Figura 41: Porcentaje de reconocimiento de voz en función de la distancia de correlación.



40 y 41, sin embargo, se puede apreciar la relación existente entre el porcentaje de reconocimiento de voz y la distancia de correlación, al comparar las señales de bloqueo se permite establecer la señal que requiere menor distancia de correlación para que el porcentaje de reconocimiento de voz sea cero, esta señal es el tono senoidal.

Esta sección de simulación y análisis de datos reales permitió establecer la señal de bloqueo que mejor se comportaría a la hora de interrumpir la comunicación entre un transmisor y un receptor que operen clandestinamente, se tuvieron en cuenta parámetros de ancho de banda, comportamiento con el canal adyacente, porcentaje de palabras perdidas, distancia de correlación y energía de la señal recibida. La señal del tono senoidal presenta menor ancho de banda, su interferencia con el canal adyacente es

nula, requiere menor energía utilizada en los bloqueadores para lograr un porcentaje de reconocimiento de voz cero a pesar de presentar la distancia de correlación mas baja, por lo tanto la señal del tono senoidal será utilizada en la solución IoT como señal de bloqueo, es decir, la señal que se comportará como un actuador en el espectro radioeléctrico.

4.2. CAPA DE ACCESO

Esta capa controla la manera en que se ubican los datos en los medios de comunicación, codifica en señales las tramas del enlace de datos. La incorporación de esta capa junto con el sistema embebido permite que el dispositivo SDR actúe como un terminal IoT. Entre las tecnologías de radio usadas en IoT se encuentra WiFi/IEEE802.11, redes móviles 3G/4G y 5G en un futuro, HSDPA, LTE/LTE-A, ZigBee, Z-Wave, Bluetooth y otros estándares 802.15.4²¹, también puede utilizarse conexión cableada como Ethernet. Sin embargo, para este trabajo de investigación, las interfaces de comunicación que tienen los terminales IoT utilizados son: Ethernet y WiFi (IEEE 802.11n).

4.3. CAPA DE GESTIÓN DE DISPOSITIVOS

Esta capa se compone de dos partes: la primera, corresponde a las librerías MQTT (*Message Queue Telemetry Transport*) que se deben instalar en el terminal, la segunda, corresponde a un *broker* MQTT que se encuentra externo al terminal, este *Broker* MQTT es el núcleo de la comunicación entre terminales IoT y servidor web, mantiene la conexión constante con los terminales IoT redireccionando la comunicación entre los diferentes terminales IoT junto con la comunicación establecida entre el servidor web y los terminales IoT. Este *broker* MQTT podría estar en la capa de componentes de nube, sin embargo, su modo de operación involucra que el dispositivo pueda operar el protocolo MQTT de manera que no puede trabajar aislado del dispositivo haciendo que opere en

²¹Rawat, Priyanka; Singh, Kamal Deep y Bonnin, Jean Marie. «Cognitive radio for M2M and Internet of Things: A survey». En: *Computer Communications* 94 (2016), págs. 1-29. ISSN: 01403664. DOI: 10.1016/j.comcom.2016.07.012. URL: <http://dx.doi.org/10.1016/j.comcom.2016.07.012>.

la capa IoT, también, opera como un puente entre la capa de componentes de nube y la capa IoT. MQTT es un protocolo para conectividad IoT/M2M (*Machine to Machine*), este protocolo es ligero y basa su transporte de mensajes como publicador/suscriptor²². El dispositivo publicador envía el mensaje al *Broker* a través de un tópico, el dispositivo o los dispositivos que deseen recibir el mensaje del publicador se suscriben al tópico utilizado por el publicador.

Los tópicos son identificadores en los que se suscriben los dispositivos para establecer comunicación M2M, o enviar un mensaje de difusión, los tópicos son *strings* que tienen una estructura jerárquica separada por /, por ejemplo:

"BUCARAMANGA/UIS/E3T/bloqueador1".

²²OASIS MQTT. *MQTT Version 3.1.1*. 2014. URL: <http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html>.

5. LOS COMPONENTES DE NUBE

En este capítulo se desarrolla el siguiente paso de la metodología para dar soluciones IoT el cual está relacionado con los componentes de la solución en la nube, donde se tiene un énfasis importante en el almacenamiento y sobre todo en el procesamiento de las señales para identificar las emisiones clandestinas. Por lo tanto, aquí se incluyen los métodos y algoritmos propuestos y desarrollados para analizar el espectro en la banda 88-108 MHz adjudicada el servicio de radiodifusión sonora. También se analizará el rendimiento de estas soluciones en la detección de emisiones clandestinas para lo cual va acompañado de una implementación de unas condiciones controladas de laboratorio. Con respecto al almacenamiento en la nube, se incluye también la descripción de la visión general de la solución implementada con una base de datos en postgresQL.

5.1. PROCESAMIENTO DE SEÑALES PARA IDENTIFICAR EMISIONES CLANDESTINAS A NIVEL DE BACKEND

Cabe recordar que el Backend de una solución IoT es todo aquello que se implementa en la nube, excluyendo los elementos de conectividad, que está oculta de los usuarios finales, quienes acceden a esta capas solo mediante aplicaciones finales. En nuestro caso, la solución de Back-End incluye una base de datos y un módulo de procesamiento en la nube que reúne los métodos de sensado para el procesamiento de señales presentado en el diagrama de clases de la Figura 9. Este procesamiento se realiza en el servidor web y sus algoritmos se implementaron en Python 3.

5.1.1. Métodos de sensado implementados

5.1.1.1. El detector de energía El detector de energía es una técnica que no requiere conocimiento acerca de la señal que ocupa la banda de manera legal o ilegal. El detector de energía mide la energía de la señal sobre un intervalo de tiempo y compara

su salida con un umbral que depende del nivel de ruido¹. Para el caso dado es posible suponer que la señal de interés está viajando por un canal de ruido blanco aditivo gaussiano, de modo que el detector de energía puede ser modelado matemáticamente mediante la siguiente expresión:

$$y[n] = \begin{cases} w[n], & H_0 \\ x[n] + w[n], & H_1 \end{cases} \quad (5.1)$$

Donde H_0 es la hipótesis nula para señal no transmitida, H_1 es la hipótesis para señal transmitida, $x[n]$ es la señal que reúne los aportes de los diferentes dispositivos como se ha explicado ya en la ecuación (4.1), y $w[n]$ es una señal de ruido blanco gaussiano. Desde este punto de vista, es posible identificar espectralmente a $x[n]$ usando el periodograma de Welch. Como es bien conocido^{2,3}, el periodograma de Welch representa un promediado de L ventanas espectrales en magnitud al cuadrado, con lo cual se obtiene una forma bastante definida para $x[n]$ en el dominio de las frecuencias. De acuerdo a la versión dada en⁴⁵, el periodograma de Welch se aplica a la señal $y_i[n]$ de la siguiente manera: $y[n]$ es la señal que nos interesa analizar. De ella tomamos un intervalo de tiempo de interés dado por N muestras. Ese intervalo lo podemos dividir en segmentos de KL muestras por segmento, y cada segmento de esos lo subdividimos en K subsegmentos más pequeños de L muestras por subsegmento. De modo que la señal $y[n]$ puede ser vista como K señales de duración L que pueden ser representadas así:

¹Digham, F F; Alouini, M S y Simon, Marvin K. «On the Energy Detection of Unknown Signals Over Fading Channels». En: *Communications, IEEE Transactions on* 55.1 (2007), págs. 21-24. ISSN: 0090-6778. DOI: 10.1109/TCOMM.2006.887483, pág. 23.

²Welch, Peter D. «The Use of Fast Fourier Transform for the Estimation of Power Spectra: A Method Based on Time Averaging Over Short, Modified Periodograms». En: *IEEE Trans. Audio and electroacoustic* 15 (1967), págs. 70-73.

³Sarvankar, Heli y col. «Cooperative and Noncooperative Spectrum Sensing Techniques Using Welch's Periodogram in Cognitive Radios». En: *IEEE. Aalborg, Denmark: Cognitive Radio y Advanced Spectrum Management*, 2008. CogART 2008. First International Workshop on, 2008, págs. 6-10. DOI: 10.1109/COGART.2008.4509987.

⁴Welch, «The Use of Fast Fourier Transform for the Estimation of Power Spectra: A Method Based on Time Averaging Over Short, Modified Periodograms», óp.cit.

⁵Sarvankar y col., «Cooperative and Noncooperative Spectrum Sensing Techniques Using Welch's Periodogram in Cognitive Radios», óp.cit.

$$\begin{aligned} 0 \leq n \leq L-1 \\ y_i[n] = y[iB+n]g[n], \quad 0 \leq i \leq K-1 \end{aligned} \quad (5.2)$$

Donde $g[n]$ es una ventana, para este trabajo se utilizó una ventana tipo *flat*top, B es el tamaño del salto o distancia de *offset* de la señal, si $B < L$, los segmentos se superponen, y para $B = L$ los segmentos son contiguos. El periodograma para un segmento de señal de tamaño KL se calcula de la siguiente forma:

$$\mathbf{p} = P[f] = \frac{1}{K} \sum_{i=0}^{K-1} \left| \sum_{n=0}^{L-1} y_i[n] e^{-2\pi j n f / L} \right|^2 \quad (5.3)$$

donde $\mathbf{p} \in \mathbb{R}^{L \times 1}$ es la representación vectorial del periodograma de Welch para cada segmento de la señal $y[n]$.

5.1.1.2. Propuesta para la implementación práctica del detector de energía El periodograma de Welch puede ser fácilmente implementado mediante la FFT en magnitud al cuadrado aplicada a cada ventana de L muestras de la señal $y_i[n]$ hasta alcanzar un número de K ventanas para finalmente promediar las K imágenes espectrales obtenidas en una sola que representamos como el vector $\mathbf{p}$.

El siguiente paso consiste en encontrar un periodograma para cada observación temporal, es decir, representar la información en una matriz $\mathbf{P} = (\mathbf{p}_0, \mathbf{p}_1, \dots, \mathbf{p}_m) \in \mathbb{R}^{L \times D}$ donde D es el número de cuadros temporales y L el tamaño de la FFT, La matriz $\mathbf{P}$ puede ser subdividida por canales que representan el ancho de banda asignado al servicio de radiodifusión sonora en FM. De acuerdo a la recomendación ITU-R BS.450-3, para Colombia la separación entre canales es 200 kHz⁶. La segmentación dada por

⁶ITU-R. «RECOMENDACIÓN UIT-R BS . 450-3 Transmisiones monofónicas Transmisiones estereofónicas». En: *Radiocomunication sector of ITU* (2001).

canales de la matriz $\mathbf{P}$ se representa mediante la siguiente expresión:

$$\mathbf{P}_j = \begin{pmatrix} P_1[f + jM] \\ P_2[f + jM] \\ \vdots \\ P_m[f + jM] \end{pmatrix} \quad (5.4)$$

$$M = 200000L/f_s$$

donde f_s es la frecuencia de muestreo del sistema de sensado, y debe cumplir que $f_s \gg 200$ kHz, M es la cantidad de muestras que representan 200 kHz de espectro, j es el índice del canal estudiado en la banda de radiodifusión sonora en FM.

Ahora se requiere determinar el umbral a partir del cual se decide si el canal está ocupado o no, es decir, si hay presencia de emisoras. El problema está en que, en la práctica, usando tecnología SDR, el piso de ruido puede variar de un canal a otro o inclusive puede variar con el paso del tiempo. Un primer acercamiento al problema lo ofrece la recomendación ITU-R SM 1753-2⁷ que propone un método analítico para determinar si una medición de ruido corresponde a ruido de tipo no gaussiano. Aplicando ese método se puede determinar el canal con la menor presencia de la señal de interés, para luego identificar comparativamente los canales con mayor presencia de ruido y menor presencia de la señal de interés.

A continuación se explica el método que propone la recomendación ITU-R SM 1753-2 para luego pasar a explicar como se aprovechó para los fines del presente proyecto. El método que se compone de tres pasos:

1. Usar los valores de la señal I/Q $y[n]$ de longitud N y construir la matriz de autocorrelación.
2. Descomponer la matriz de autocorrelación usando el método de descomposición

⁷ITU-R. *Recommendation ITU-R SM.1753-2 Methods for measurements of radio noise SM Series*. Inf. téc. 2010.

en valores singulares (SVD por sus siglas en inglés).

3. Evaluar los valores singulares obtenidos y decidir si el ruido es gaussiano.

Para calcular dinámicamente el umbral de decisión, se propone una modificación a la metodología de la recomendación ITU-R SM 1753-2 y consiste en lo siguiente: no se tomó la señal I/Q del paso 1. y en su lugar se tomó el periodograma calculado por cada observación temporal, luego se calculó la matriz de autocorrelación por cada canal j ($\mathbf{R}_j$), y se descompuso la matriz de autocorrelación usando el método SVD como se muestra en la siguiente ecuación:

$$\begin{aligned}\mathbf{R}_j &= E\{\mathbf{P}_j \mathbf{P}_j^T\} \\ \mathbf{R}_j &= \mathbf{U} \mathbf{\Sigma} \mathbf{V}^T\end{aligned}\tag{5.5}$$

donde $E\{.,.\}$ es el valor esperado, $\mathbf{P}_j$ es la matriz que representa las observaciones de los periodogramas por canal, la matriz diagonal $\mathbf{\Sigma}$ contiene los valores singulares de los cuales se puede evaluar el canal que tiene la menor presencia de señal primaria basado en que $w[n]$ es AGWN. El paso 3 del método presentado por la recomendación ITU-R SM 1753-2 utiliza la métrica $\mathbf{v}_j$ donde se estudian los valores singulares presentes en $\mathbf{\Sigma}$, esta métrica se define como:

$$\mathbf{v}_j = \sqrt{\frac{\sigma_0^2 + \sigma_1^2 + \dots + \sigma_k^2}{\sigma_1^2 + \sigma_0^2 + \dots + \sigma_M^2}}, \quad k > \frac{M+1}{2}\tag{5.6}$$

El umbral λ es calculado con base en el argumento mínimo de $\mathbf{v}$, y la energía del canal correspondiente al índice dado por el argumento mínimo encontrado, como muestra la siguiente ecuación:

$$\begin{aligned}c &= \arg \min \mathbf{v} \\ \mathbf{G} &= \mathbf{P}_c \\ \lambda &= \frac{1}{D} \sum_{i=0}^{D-1} \sum_{j=0}^{M-1} \mathbf{G}_{i,j}\end{aligned}\tag{5.7}$$

La observación temporal D permite encontrar el comportamiento del umbral λ con el fin de realizar una decisión estadística para determinar la probabilidad de detección

usando la PDF Chi-square no central con N grados de libertad⁸⁹. La probabilidad de detección de ocupación de canal puede ser formulada como:

$$\begin{aligned} \mathbf{q}_j &= 1 - \Gamma\left(\frac{\sigma_s^2[j]}{\sigma_w^2[c]}, \frac{\lambda}{\sigma_w^2[c] + \sigma_s^2[j]}\right) \\ \mathbf{q}_j &= Pr(\mathbf{e}_j > \lambda | H_1) \\ \mathbf{e}_j &= \sum_{f=0}^{M-1} P[f + jM] \end{aligned} \quad (5.8)$$

donde σ_w es la varianza del ruido, σ_s es la varianza de la señal, $\mathbf{e}_j$ es la energía de cada canal, y $\Gamma(.)$ es la función gamma incompleta¹⁰, el vector $\mathbf{q}$ es calculado para cada observación temporal, los canales ocupados se determinan si $\mathbf{q}_j > 0,95$. Estos canales fueron analizados y comparados con la base de datos de usuarios primarios suministrada por el MINTIC, esta base de datos es implementada en el *Back-End*. Si los canales ocupados no están en la base de datos se almacenan en un vector para cada observación temporal del espectro de la siguiente forma:

$$\mathbf{b} = [\mathbf{ch}_1, \mathbf{ch}_2, \dots, \mathbf{ch}_{N_T}] \quad (5.9)$$

donde $\mathbf{ch}$ es el vector que contiene los canales no encontrados en la base de datos, N_T es el total de cuadros u observaciones, cada observación tiene un tamaño de KL . El histograma de frecuencias del vector $\mathbf{b}$ determina las transmisiones ilegales si estas superan el 95 % de apariciones,

5.1.1.3. Detector de picos basado en los coeficientes de la transformada *wavelet* Los picos del periodograma de Welch contienen información acerca de las frecuencias de portadora de las estaciones de radio cuando se analiza un

⁸⁹Digham; Alouini y Simon, «On the Energy Detection of Unknown Signals Over Fading Channels», óp.cit.

⁹Urkowitz, H. «Energy detection of unknown deterministic signals». En: *Proceedings of the IEEE* 55.4 (1967), págs. 523-531. ISSN: 0018-9219. DOI: 10.1109/PROC.1967.5573. URL: <http://ieeexplore.ieee.org/document/1447503/>.

¹⁰Patil, Vilaskumar M. y Patil, Siddarama R. «A survey on spectrum sensing algorithms for cognitive radio». En: *2016 International Conference on Advances in Human Machine Interaction, HMI 2016* 11.1 (2016), págs. 149-153. ISSN: 1553877X. DOI: 10.1109/HMI.2016.7449196.

gran ancho de banda y se tiene baja resolución espectral. El problema que surge ahora consiste en lograr identificar las emisoras, lo cual se traduce en una identificación automática de los picos que ofrece el periodograma de Welch. Uno de los métodos de mayor interés es la detección de picos basada coincidencia de patrones mediante transformada wavelet continua ó simplemente CWT¹¹. El método proviene de la espectroscopia de masas, pero se emplea también ampliamente en los sistemas de medición usados en las comunicaciones donde es común la necesidad de detectar picos.

La CWT es una herramienta matemática que necesita una base *wavelet*. Esta base es una pequeña ondícula con características oscilatorias donde su energía está concentrada en el tiempo, una base *wavelet* permite analizar las variaciones temporales y no estacionarias de las señales mediante la descomposición 2D en escala-desplazamiento, matemáticamente la CWT se representa como¹²:

$$\mathbf{C}(a, b) = \int_R s(t) \psi_{a,b}(t) dt, \quad \psi_{a,b}(t) = \frac{1}{\sqrt{a}} \psi\left(\frac{t-b}{a}\right), \quad a \in R^+ - \{0\}, b \in R \quad (5.10)$$

donde a es la escala, b es el desplazamiento y ψ es la función sombrero Mexicano como base *wavelet*, $s(t)$ es la señal sobre la cual se hace la transformada, y La matriz $\mathbf{C}$ tiene diferentes escalas y desplazamientos de la CWT.

El método consiste en cuatro pasos:

- Se calcula la transformada continua de *Wavelet* (CWT por sus siglas en inglés) a la señal de entrada.
- La transformada CWT retorna un vector de índices que señala la posición de los picos de la señal de interés.

¹¹Du; Kibbe y Lin, «Improved peak detection in mass spectrum by incorporating continuous wavelet transform-based pattern matching», óp.cit.

¹²Gao, Robert X. y Yan, Ruqiang. «Wavelets: Theory and applications for manufacturing». En: *Springer US* (2011), págs. 33-48. ISSN: 0717-6163. DOI: 10.1007/978-1-4419-1545-0. arXiv: arXiv:1011.1669v3.

- Traslapando la señal de interés con la Transformada Wavelet se obtiene la señal que solo incluye los picos detectados.

5.1.1.4. Identificación de emisiones clandestinas basado en transformada *wavelet*

Para la identificación de emisiones clandestinas se propone un algoritmo que se basa en el detector de picos explicado anteriormente pero aplicado al dominio de las frecuencias, es decir, a los periodogramas de Welch. Se ha usado un método bien conocido¹³ para calcular la Transformada de Wavelet con una ondícula tipo sombrero mexicano para obtener el vector de los índices, que en este caso aplican al dominio de las frecuencias. Para cada observación temporal m del espectro se calculan los índices de los picos del espectro. Sin embargo, el rendimiento del detector de picos es susceptible al ruido, como se muestra en la Figura 42 donde, en color rojo, pueden apreciarse no solo los picos de interés sino muchos otros que corresponden a ruido. Por lo tanto, el siguiente paso consiste en establecer un Umbral de decisión para lograr separar sólo los picos de interés como se muestra en la Figura 42 en color verde.

Para establecer el Umbral de Decisión se usa la información encontrada en el percentil calculado con base en las condiciones iniciales del canal. El valor del percentil se calcula por el método *nearest-rank*.

$$n = \frac{P}{100}L \quad (5.11)$$

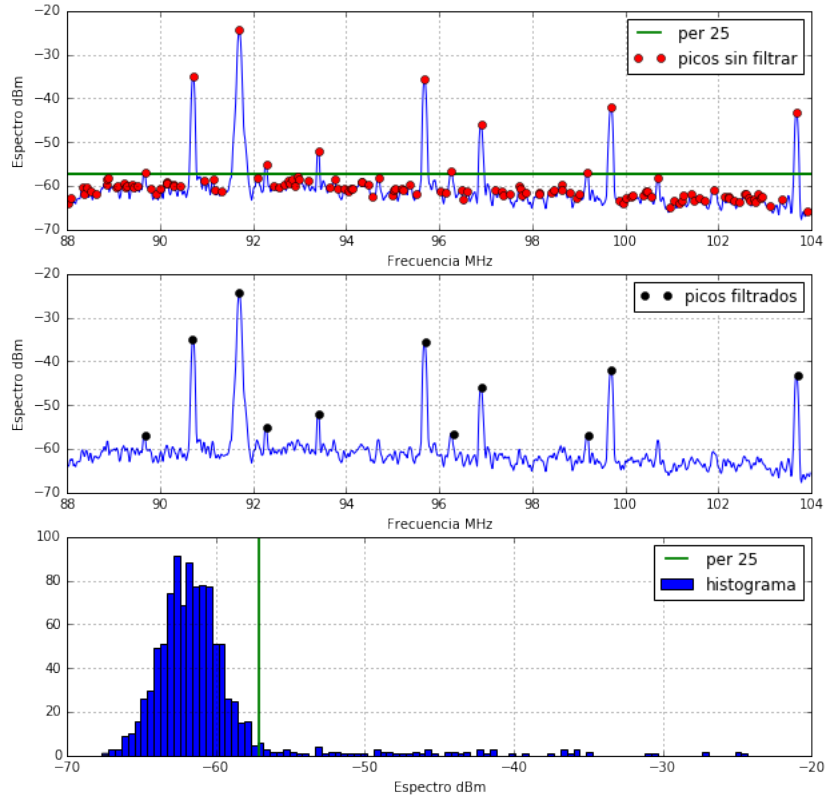
donde P es el percentil que se quiere calcular, L es el tamaño del periodograma Welch, n es el índice que corresponde al percentil P del vector del periodograma de Welch ordenado de menor a mayor. El valor de P es calibrado dependiendo de las condiciones del canal y frecuencia de muestreo, por lo cual se recurre a la búsqueda de un histograma que resuma el comportamiento de los valores del Periodograma de Welch. La Figura 42 muestra ese histograma de frecuencias para una observación del periodograma de Welch, las barras que están antes de la línea verde vertical representan el ruido, mientras que los picos de interés están después del percentil definido como umbral, que en este caso es el percentil 25, es decir, un cuarto de rango de valores en el eje horizontal del histograma.

¹³Du; Kibbe y Lin, «Improved peak detection in mass spectrum by incorporating continuous wavelet transform-based pattern matching», óp.cit.

Finalmente, surge la necesidad de identificar cual de esas emisoras detectadas son ilegales. Para ello, los resultados anteriores son ahora comparados con la base de datos usuarios primarios suministrada por el MinTIC e implementada, en nuestro caso, en el *Back-End*. El proceso de clasificación es similar al detector de energía; las frecuencias de portadora no encontradas en la base de datos se almacenan en el vector $\hat{\mathbf{b}}$.

$$\hat{\mathbf{b}} = [\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_N] \quad (5.12)$$

Figura 42: Picos detectados en el espectro y filtrado basado en el histograma.



donde $\mathbf{g}$ corresponde a las frecuencias de portadora, la diferencia del proceso está en que la ecuación (5.9) almacena los canales y la ecuación (5.12) las frecuencias de portadora detectadas por canal. Las frecuencias de portadora que superen el 95 % del histograma de frecuencias son consideradas ilegales.

5.2. ANÁLISIS DEL SENSADO COOPERATIVO

En esta sección se busca comparar el desempeño del algoritmo detector de energía y detector de picos cuando funcionan de manera individual, pero sobre todo demostrar la viabilidad del sensado colaborativo. La solución se prevé en una comparación de dos aspectos:

- La sensibilidad respecto a la relación portadora a ruido (C/N). Es decir, cual método logra detectar una emisión clandestina con la menor relación C/N .
- La precisión que se refiere al grado de certeza que cada método puede tener, lo cual se puede lograr con ayuda de curvas ROC.

El experimento se realizó de la siguiente manera:

- Se seleccionaron 8 sub bandas de frecuencias para ser usadas como canales de 8 emisoras clandestinas. La selección se realizó de manera cuidadosa para no realizar ningún tipo de afectación y para que la cobertura no fuese más allá de los límites del área de experimentación.
- El experimento se realizó para 8 casos de frecuencias, uno por cada sub banda seleccionada para las emisiones clandestinas. En cada caso:
 - Se usó solo una emisora clandestina, lo que equivale al uso de una sub banda.
 - Se probaron 11 diferentes casos de potencias de emisión.
- De manera cada ensayo está compuesto de 88 emisiones
- Finalmente, se realizaron 10 repeticiones o ensayos, para un total de 880 emisiones.

Los aspectos procedimentales del experimento son los siguientes:

- En la Figura 43 se tiene una representación de la solución usada en las pruebas, para lo cual se usaron 3 equipos USRP E310: uno como transmisor y dos como nodos de sensado sincronizados a través de MQTT.
- Los nodos N1 y N2 sensan el espectro y envían los datos obtenidos al Centro de Fusión para su almacenamiento y procesamiento.
- En el Centro de Fusión la información se procesa de manera que sea posible comparar dos estrategias de sensado: el sensado individual, el que entrega cada nodo N1 y N2 y el sensado colaborativo, combinando los aportes de los dos nodos.

La señal recibida por cada nodo (N1 y N2) es afectada por canales $\mathbf{h}_1$ y $\mathbf{h}_2$ de manera diferente. En la Figura 44 se muestra el periodograma de Welch en un instante de tiempo donde se observa gráficamente la diferencia existente entre las señales sensadas (gráficas azul y verde), y la combinación de las dos anteriores (gráfica roja) obtenida mediante la ecuación (4.1). Como podemos ver, los datos combinados, al unir los aportes de los dos nodos, aumentan las posibilidades de detectar la señal.

5.2.1. Estudio de sensibilidad El estudio de sensibilidad se realizó para comparar el sensado colaborativo con el detector de energía y el sensado colaborativo con el detector picos. Consiste en identificar los niveles de sensibilidad que tienen los dos métodos de detección con respecto a la relación C/N. Para este fin, Para cada una de las emisiones clandestinas generadas se calcula la probabilidad de detección P_d la cual se representa mediante la siguiente expresión:

$$P_d = \begin{cases} 1, & \text{si } l = m = \hat{m} \wedge (\mathbf{b} \vee \hat{\mathbf{b}}) \in \mathbf{t} \\ 1/\hat{m} \vee 1/m, & \text{si } \hat{m} > l \vee m > l \wedge \mathbf{t} \in (\mathbf{b} \vee \hat{\mathbf{b}}) \\ 0, & \text{si } (\mathbf{b} \vee \hat{\mathbf{b}}) \notin \mathbf{t} \end{cases} \quad (5.13)$$

Donde:

- $\mathbf{t}$ es el vector correspondiente a las emisiones generadas

Figura 43: Modelo general del experimento para el análisis del sensado cooperativo.

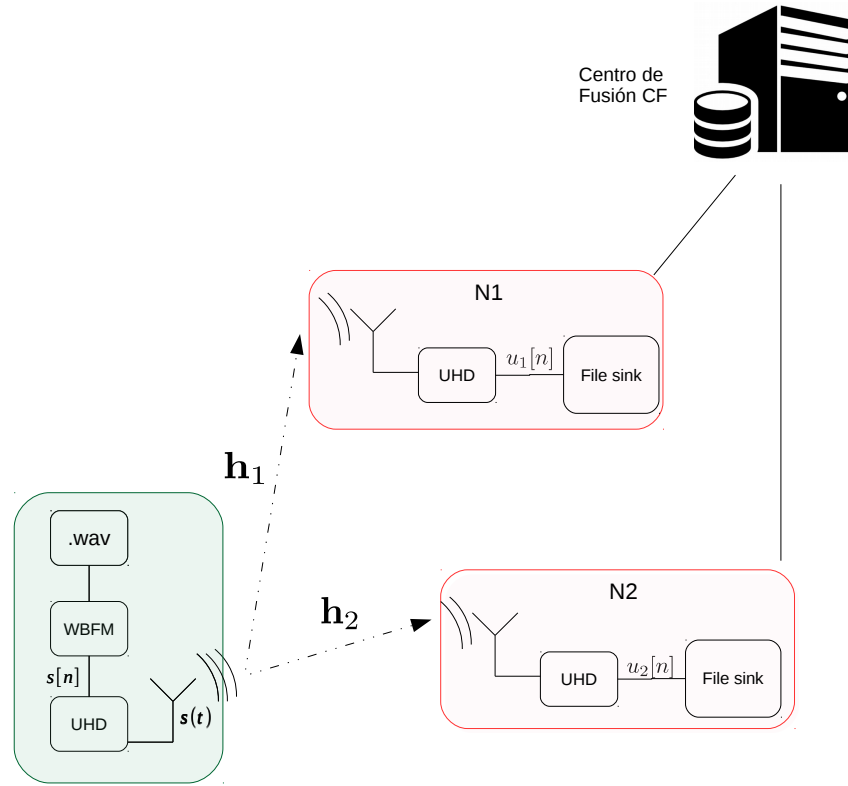
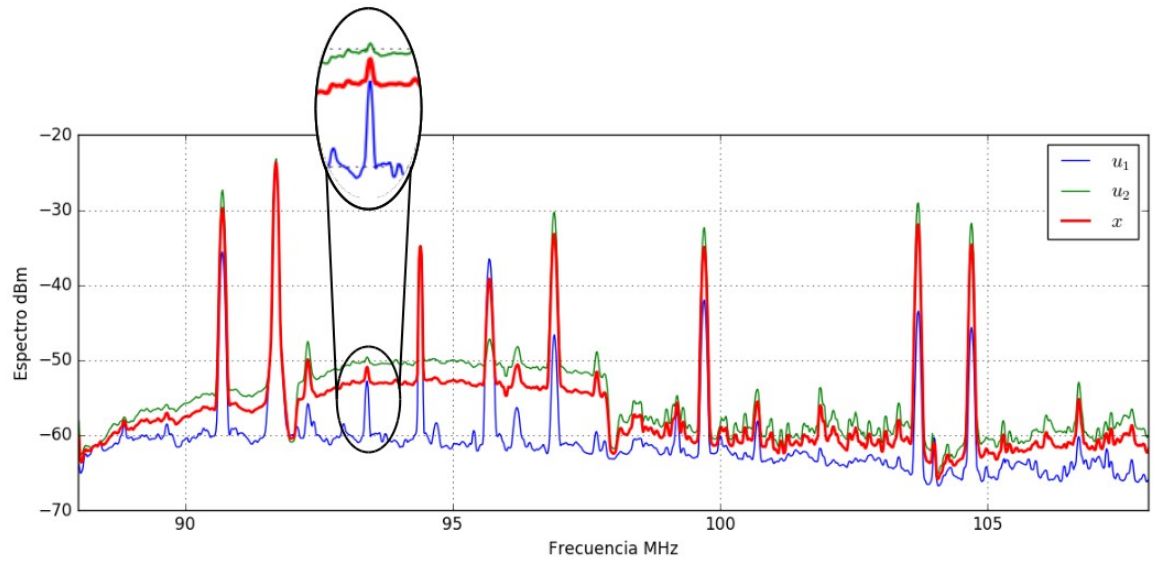


Figura 44: Espectro sensado por parte de los equipos de la red.



- l es el número de las transmisiones clandestinas generadas al tiempo, es decir, el tamaño de $\mathbf{t}$ y tenemos que $l = 1$ para nuestro experimento, ya que para cada caso solo se generó una emisión clandestina. En una aplicación real existe la posibilidad de un número mayor, es decir, varias emisiones clandestinas al tiempo.
- $\mathbf{b} \in \mathbb{R}^{1 \times \hat{m}}$ es el vector que entrega el detector de energía indicando los canales detectados con emisiones clandestinas.
- $\hat{\mathbf{b}} \in \mathbb{R}^{1 \times \hat{m}}$ es el vector que entrega el detector de picos indicando los canales detectados con emisiones clandestinas.
- m es el tamaño del vector $\mathbf{b}$
- $\hat{m}$ es el tamaño del vector $\hat{\mathbf{b}}$

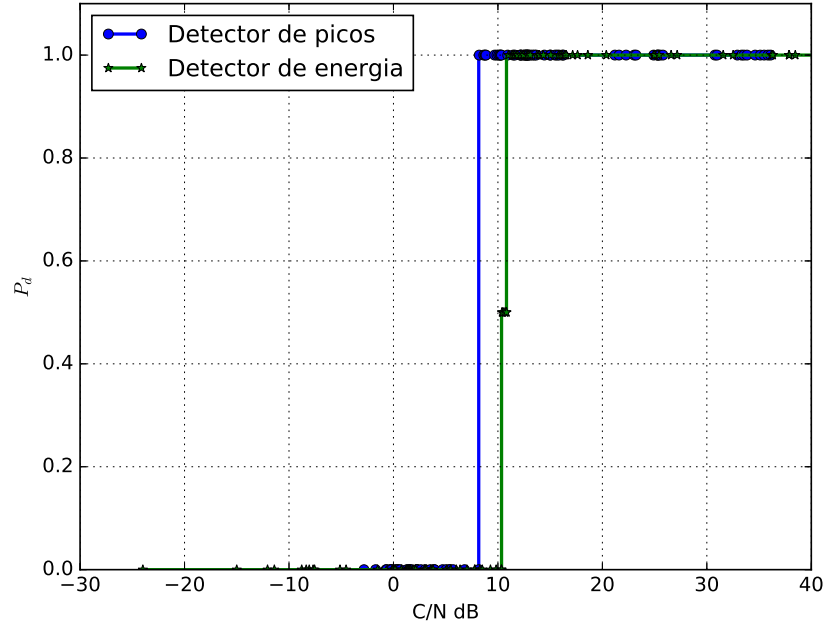
Las falsas emisiones detectadas penalizan la probabilidad de detección P_d de acuerdo con la ecuación (5.13) cuando el número de emisiones detectadas es mayor que el número de emisiones generadas.

Para analizar la probabilidad de detección P_d en función de la relación portadora-ruido C/N de la señal clandestina se siguieron los siguientes pasos:

- La distancia entre los nodos N1 y N2 se dejó fija
- Se varió la potencia de transmisión en la estación ilegal generada en condiciones de laboratorio.

Los resultados del estudio de la P_d en función de C/N se presentan en la Figura 45, donde la gráfica azul representa al detector de picos, y la gráfica verde representa al detector de energía, de las cuales podemos concluir que el detector de picos (gráfica azul) es más sensible en la detección de emisiones clandestinas (gráfica verde).

Figura 45: Probabilidad de detección en función de C/N.



5.2.2. Estudio de la precisión El siguiente paso consiste en evaluar los clasificadores de emisiones clandestinas. Para ello se determinó la curva característica operativa del receptor (ROC por sus siglas en inglés), esta curva es una técnica que se usa mucho en ciencia de datos¹⁴ para visualizar, organizar y seleccionar clasificadores basados en su rendimiento. Dado un clasificador y una instancia existen cuatro posibles resultados:

- Verdadero positivo.
- Falso negativo.
- Verdadero negativo.
- Falso positivo.

¹⁴Bradley, Andrew P. «The use of the area under the ROC curve in the evaluation of machine learning algorithms». En: *Pattern Recognition* 30.7 (1997), págs. 1145-1159. ISSN: 00313203. DOI: 10.1016/S0031-3203(96)00142-2.

La tasa de verdaderos positivos (tp) es estimada por la relación de positivos correctamente clasificados sobre el total de positivos, y la tasa de falsos positivos o falsa alarma (fp) es estimada por la relación de negativos incorrectamente clasificados sobre el total de negativos. La curva ROC es una gráfica con tp en el eje de las ordenadas y fp en el eje de las abscisas¹⁵, esta representa el *trade-off* entre los verdaderos positivos (beneficios) y los falsos positivos (costos).

El área bajo la curva ROC (AUC por sus siglas en inglés) de un clasificador, es probabilidad de que el clasificador clasifique una instancia positiva elegida al azar más alta que una instancia negativa elegida al azar¹⁶. La Figura 46 muestra la curva ROC obtenida por el método detector de energía, la gráfica azul representa el sensado cooperativo y la gráfica verde representa el sensado no cooperativo, el AUC para el sensado cooperativo es 0.895, y el AUC con el sensado no cooperativo es de 0.739. La Figura 47 muestra la curva ROC cuando los datos del espectro se procesan utilizando el método detector de picos, el AUC para el sensado cooperativo es de 0.755, y el AUC sin el sensado cooperativo es de 0.673.

La información de las curvas ROC en las figuras 46 y 47 muestran que el sensado cooperativo tiene mejor rendimiento en la detección de emisiones clandestinas debido a que el AUC es más alto en ambos casos; entre los dos métodos de monitoreo del espectro, el detector de energía presenta mayor AUC por lo que presenta menor cantidad de falsos positivos en comparación con el detector de picos.

5.3. BASE DE DATOS

La base de datos se implementó en PostgreSQL y se desarrolló bajo el modelo mostrado en la Figura 48 donde se observan dos zonas separadas por colores, estas zonas corresponden a información (representada en la zona de color rosado), y usuarios y *Back-End*

¹⁵Fawcett, Tom. «An introduction to ROC analysis». En: *Pattern Recognition Letters* 27.8 (2006), págs. 861-874. ISSN: 01678655. DOI: 10.1016/j.patrec.2005.10.010. arXiv: /dx.doi.org/10.1016/j.patrec.200 [http:].

¹⁶Bradley, «The use of the area under the ROC curve in the evaluation of machine learning algorithms», óp.cit.

Figura 46: Curva ROC del detector de energía.

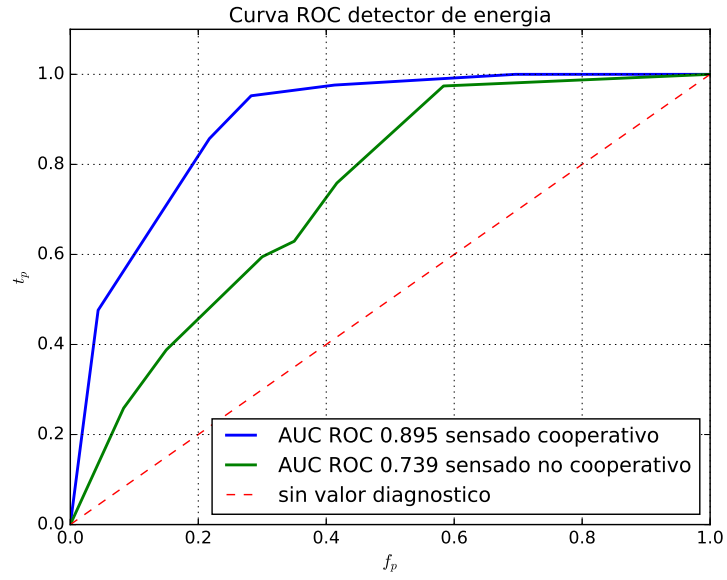
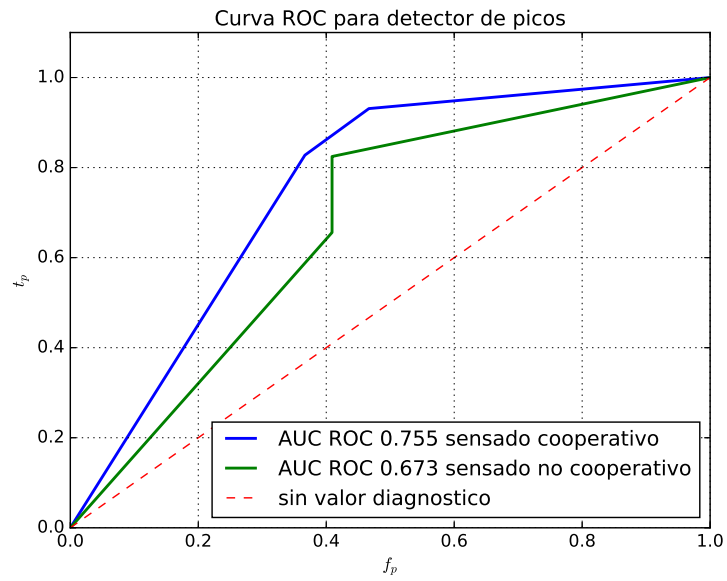


Figura 47: Curva ROC del detector de picos.



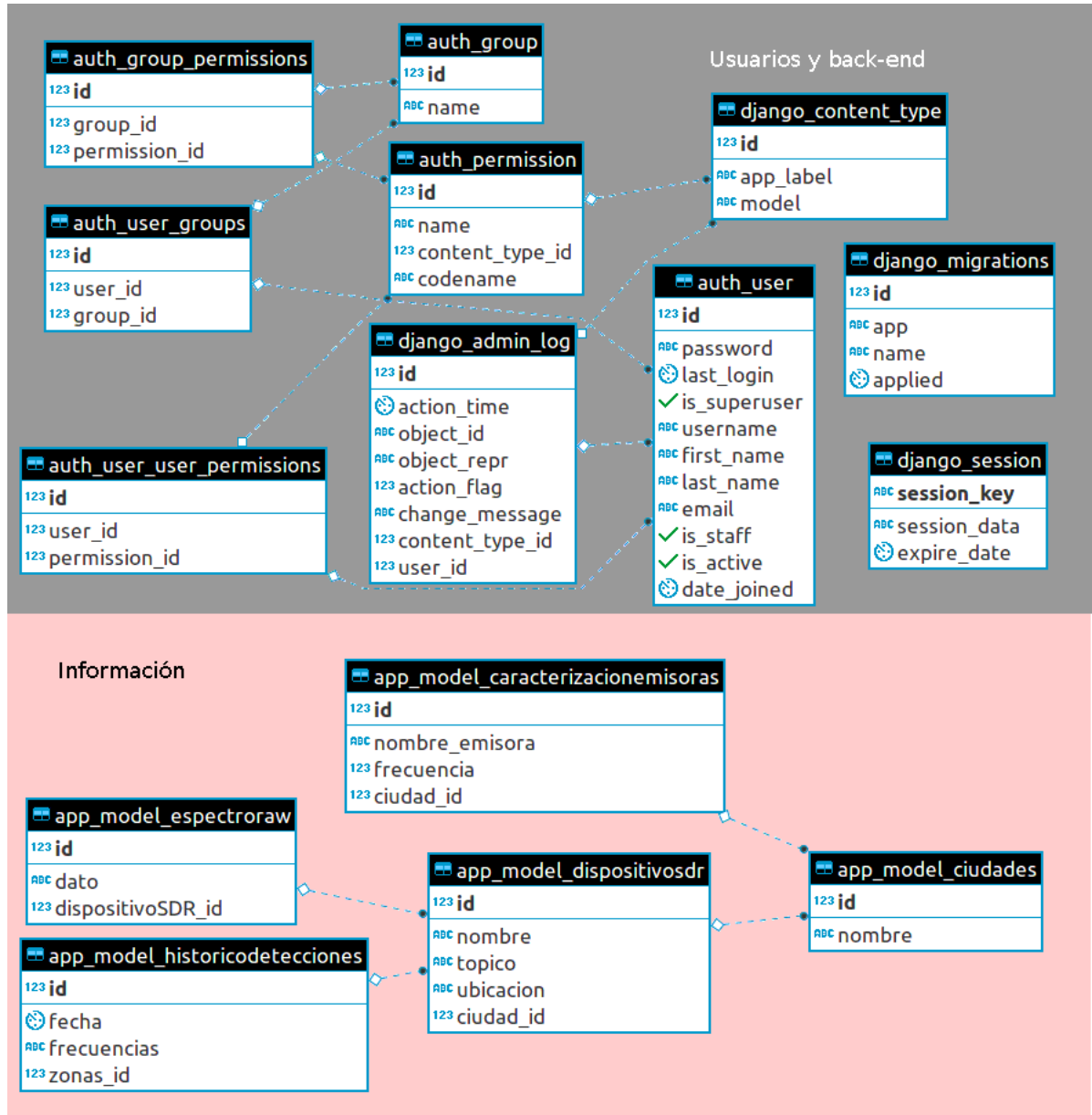
representadas en la zona de color gris.

En la zona de información se pueden observar 5 tablas relacionadas que hacen referencia a los datos sensados, frecuencias legales, dispositivos usados, ciudades y histórico de detecciones, a continuación se hace una descripción referente a los datos que contienen las tablas en la zona de información del modelo de la Figura 48:

1. **app_model_espectroraw**: contiene los datos provenientes del sensado cooperativo (descrito en la sección 4.1.1.2), estos datos se almacenan en formato JSON y en banda-base en formato de señal I/Q como lo entrega el dispositivo SDR.
2. **app_model_caracterizacionemisoras**: contiene los datos provenientes las emisoras que están legalmente asignadas por ciudades, frecuencia y nombre de la emisora, esta información se extrae del MinTIC en la subdirección de radiodifusión sonora. Para este trabajo de investigación sólo tomó la información relacionada con el área metropolitana de Bucaramanga debido a que se usaron dos dispositivos dentro del grupo de investigación RadioGis de la Universidad Industrial de Santander.
3. **app_model_dispositivosdr**: contiene los datos relacionados con el tipo de dispositivo SDR utilizado, el tópico MQTT que identifica al dispositivo en la capa de gestión de dispositivos, la ubicación y el identificador de ciudad donde se encuentra.
4. **app_model_ciudades**: Contiene la lista de ciudades que tienen emisoras asignadas por el MinTIC.
5. **app_model_historicodetecciones**: contiene los resultados históricos de las emisiones clandestinas detectadas después de procesar los datos, junto con las zonas donde se identificaron las emisiones.

Las tablas referentes a usuarios y *back-end* son propias del *framework* web Django que se utilizó para este proyecto por lo tanto no se entrará en detalle.

Figura 48: Modelo de la base de datos que se implementó en postgresQL.



6. CONCLUSIONES

- Se ha diseñado e implementado un prototipo del sistema de inhibición de emisiones clandestinas en el servicio de radiodifusión sonora en FM para la banda 88-108 MHz usando las tecnologías SDR como un servicio IoT mediante la construcción de un modelo que incluye una plataforma web que permite operar la red de monitoreo y bloqueo de emisiones clandestinas utilizando el protocolo MQTT para establecer comunicación entre el servidor y los dispositivos SDR, y el protocolo HTTP para la comunicación entre el usuario y el servidor.
- El monitoreo del espectro radioeléctrico para encontrar emisiones clandestinas en la banda 88-108 MHz ha sido desarrollado empleando dos métodos: detector de energía con umbral dinámico y detector de picos.
- Con base en las señales usadas en la red de bloqueadores, la señal de bloqueo que mejor se adapta a una transmisión real es la señal senoidal, esta señal requiere menor energía en la transmisión para que la información relacionada al audio de una transmisión considerada ilegal no se pueda reconocer y por lo tanto ocasione su pérdida.
- El sensado cooperativo permite mejorar el rendimiento de los clasificadores para encontrar emisiones clandestinas, esto se puede evidenciar mediante el cálculo del AUC ROC para sensado cooperativo y no cooperativo; con base en los análisis de las curvas ROC el método detector de energía con umbral dinámico presenta un AUC de 0.895 y el método detector de picos presenta un AUC 0.755 para el sensado cooperativo, esta métrica nos permite determinar que el detector de energía presenta mejor comportamiento a la hora de clasificar emisiones clandestinas.
- Los resultados muestran que el bloqueo cooperativo aumenta el rendimiento de los bloqueadores debido a que se logra un mayor efecto en la pérdida de la información contenida en el audio de una emisión clandestina en FM.

7. TRABAJO FUTURO

Como trabajo futuro de esta investigación es la agregación de más servicios en el procesamiento de la nube como: aplicar técnicas de *machine learning* para estudiar anchos de banda, potencias de transmisión, análisis de interferencias, radiogonometría con el método de diferencia de tiempo de llegada (TDOA) para localizar la ubicación del transmisor clandestino aprovechando la distribución espacial de los nodos de sensado; estudiar otros servicios de radiocomunicaciones como radiodifusión de TV, redes móviles, radionavegación aeronáutica y marítima, radioastronomía, entre otros servicios que estén dentro del rango de operaciones de los dispositivos SDR utilizados. En términos de diseño de hardware RF se requiere adaptar el sistema con amplificadores, filtros, y antenas de transmisión para ampliar la cobertura de los bloqueadores.

BIBLIOGRAFÍA

ALIMOHAMMAD, A.; FARD, S.F.; COCKBURN, B.F. y SCHLEGEL, C. «Compact Rayleigh and Rician fading simulator based on random walk processes». En: *IET Communications* 3.8 (2009), pág. 1333. ISSN: 17518628. DOI: 10.1049/iet-com.2008.0297. URL: <http://digital-library.theiet.org/content/journals/10.1049/iet-com.2008.0297>.

ANUSHA, Veluru Sai; NITHYA, G. K. y RAO, Sethuraman N. «A comprehensive survey of electromagnetic propagation models». En: *Proceedings of the 2017 IEEE International Conference on Communication and Signal Processing, ICCSP 2017* 2018-Janua (2018), págs. 1457-1462. DOI: 10.1109/ICCSP.2017.8286627.

ARSLAN, Hüseyin y AHMED, Sadia. *Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems*. 2007, págs. 110-120. ISBN: 978-1-4020-5541-6. DOI: 10.1007/978-1-4020-5542-3. URL: <http://www.springerlink.com/index/10.1007/978-1-4020-5542-3>.

BRADLEY, Andrew P. «The use of the area under the ROC curve in the evaluation of machine learning algorithms». En: *Pattern Recognition* 30.7 (1997), págs. 1145-1159. ISSN: 00313203. DOI: 10.1016/S0031-3203(96)00142-2.

CICHON, Krzysztof; KLIKS, Adrian y BOGUCKA, Hanna. «Energy-Efficient Cooperative Spectrum Sensing: A Survey». En: *IEEE Communications Surveys and Tutorials* 18.3 (2016), págs. 1861-1886. ISSN: 1553877X. DOI: 10.1109/COMST.2016.2553178.

COMMUNITIES, COMMISSION OF THE EUROPEAN. *Communication on future networks and the internet*. Inf. téc. Brusseles, 2008.

DIGHAM, F F; ALOUINI, M S y SIMON, Marvin K. «On the Energy Detection of Unknown Signals Over Fading Channels». En: *Communications, IEEE Transactions on* 55.1 (2007), págs. 21-24. ISSN: 0090-6778. DOI: 10.1109/TCOMM.2006.887483.

DOHR, A; MODRE-OPSRIAN, R; DROBICS, M; HAYN, D y SCHREIER, G. «The Internet of Things for Ambient Assisted Living». En: *2010 Seventh International Conference on Information Technology: New Generations*. 2010, págs. 804-809. DOI: 10.1109/ITNG.2010.104.

DONG, Lun; HAN, Zhu; PETROPULU, Athina P. y POOR, H. Vincent. «Improving wireless physical layer security via cooperating relays». En: *IEEE Transactions on Signal Processing* 58.3 PART 2 (2010), págs. 1875-1888. ISSN: 1053587X. DOI: 10.1109/TSP.2009.2038412. arXiv: 1602.06847.

DU, Pan; KIBBE, Warren A. y LIN, Simon M. «Improved peak detection in mass spectrum by incorporating continuous wavelet transform-based pattern matching». En: *Bioinformatics* 22.17 (2006), págs. 2059-2065. ISSN: 13674803. DOI: 10.1093/bioinformatics/bt1355.

ERSOY, Okan K. «A Comparative Review of Real and Complex Fourier-Related Transforms». En: *Proceedings of the IEEE* 82.3 (1994), págs. 429-447. ISSN: 15582256. DOI: 10.1109/5.272147.

FAWCETT, Tom. «An introduction to ROC analysis». En: *Pattern Recognition Letters* 27.8 (2006), págs. 861-874. ISSN: 01678655. DOI: 10.1016/j.patrec.2005.10.010. arXiv: /dx.doi.org/10.1016/j.patrec.200 [http:].

GANESAN, Ghurumuruhan y LI, Ye. «Cooperative spectrum sensing in cognitive radio, part I: Two user networks». En: *IEEE Transactions on Wireless Communications* 6.6

(2007), págs. 2204-2212. ISSN: 15361276. DOI: 10.1109/TWC.2007.05775. arXiv: 1105.2978v1.

GANESAN, Ghurumuruhan y LI, Ye (Geoffrey). «Cooperative spectrum sensing in cognitive radio, part II: Multiuser networks». En: *Ieee Transactions on Wireless Communications* 6.6 (2007), págs. 2214-2222. ISSN: 1536-1276. DOI: 10.1109/TWC.2007.05776.

GAO, Robert X. y YAN, Ruqiang. «Wavelets: Theory and applications for manufacturing». En: *Springer US* (2011), págs. 33-48. ISSN: 0717-6163. DOI: 10.1007/978-1-4419-1545-0. arXiv: arXiv:1011.1669v3.

GHASEMI, Amir y SOUSA, Elvino S. «Collaborative spectrum sensing for opportunistic access in fading environments». En: *2005 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005* (2005), págs. 131-136. DOI: 10.1109/DYSPAN.2005.1542627.

GROVER, Kanika; LIM, Alvin y YANG, Qing. «Jamming and anti-jamming techniques in wireless networks: a survey». En: *International Journal of Ad Hoc and Ubiquitous Computing* 17.4 (2014), pág. 197. ISSN: 1743-8225. DOI: 10.1504/IJAHUC.2014.066419. URL: <http://www.scopus.com/inward/record.url?eid=2-s2.0-84919822418%7B%5C%7DpartnerID=tZ0tx3y1>.

HAYKIN, Simon. *Sistemas de Comunicacion*. 1.^a ed. Mexico, DF: LIMUSA WILEY, 2002, págs. 107-130.

IEEE. *IEEE Std 830-1998- IEEE Recommended Practice for Software Requirements Specifications*. 2009. URL: <https://standards.ieee.org/findstds/standard/830-1998.html> (visitado 01-01-2018).

ITU-R. «RECOMENDACIÓN UIT-R BS . 450-3 Transmisiones monofónicas Transmisiones estereofónicas». En: *Radiocomunication sector of ITU* (2001).

— *Recommendation ITU-R SM.1753-2 Methods for measurements of radio noise SM Series*. Inf. téc. 2010.

LI, Zhiqiang; YU, F. Richard y HUANG, Minyi. «A cooperative spectrum sensing consensus scheme in cognitive radios». En: *Proceedings - IEEE INFOCOM* (2009), págs. 2546-2550. ISSN: 0743166X. DOI: 10.1109/INFCOM.2009.5062184.

LIM, J.S. «Signal Reconstruction and Estimation from Short-Time Fourier Transform Representation: A Summary of Recent Results». En: *IFAC Proceedings Volumes* 18.5 (1985), págs. 1421-1424. ISSN: 14746670. DOI: 10.1016/S1474-6670(17)60764-X. URL: <https://linkinghub.elsevier.com/retrieve/pii/S147466701760764X>.

OASIS MQTT. *MQTT Version 3.1.1*. 2014. URL: <http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html>.

PATIL, Vilaskumar M. «A Survey on Spectrum Sensing algorithms for Cognitive Radio». En: *2018 7th International Conference on Modern Circuits and Systems Technologies (MOCAST)* 1.3 (2016), págs. 1-5.

PATIL, Vilaskumar M. y PATIL, Siddarama R. «A survey on spectrum sensing algorithms for cognitive radio». En: *2016 International Conference on Advances in Human Machine Interaction, HMI 2016* 11.1 (2016), págs. 149-153. ISSN: 1553877X. DOI: 10.1109/HMI.2016.7449196.

PELECHRINIS, Konstantinos; ILIOFOTOU, Marios y KRISHNAMURTHY, Srikanth V. «Denial of Service Attacks in Wireless Networks: The Case of Jammers». En: *IEEE*

Communications Surveys & Tutorials 13.2 (2011), págs. 245-257. ISSN: 1553-877X. DOI: 10.1109/SURV.2011.041110.00022.

RAWAT, Priyanka; SINGH, Kamal Deep y BONNIN, Jean Marie. «Cognitive radio for M2M and Internet of Things: A survey». En: *Computer Communications* 94 (2016), págs. 1-29. ISSN: 01403664. DOI: 10.1016/j.comcom.2016.07.012. URL: <http://dx.doi.org/10.1016/j.comcom.2016.07.012>.

RAY, P. P. «A survey on Internet of Things architectures». En: *Journal of King Saud University - Computer and Information Sciences* (2016). ISSN: 22131248. DOI: 10.1016/j.jksuci.2016.10.003. URL: <http://dx.doi.org/10.1016/j.jksuci.2016.10.003>.

RIEDI, Rudolf H. «An Introduction to Statistical Signal Processing». En: *Journal of the American Statistical Association* 101.475 (2006), págs. 1317-1317. ISSN: 0162-1459. DOI: 10.1198/jasa.2006.s133. URL: <http://www.tandfonline.com/doi/abs/10.1198/jasa.2006.s133>.

SARVANKO, Heli; MUSTONEN, Miia; HEKKALA, Atso y AARNE, M. «Cooperative and Noncooperative Spectrum Sensing Techniques Using Welch 's Periodogram in Cognitive Radios». En: *IEEE. Aalborg, Denmark: Cognitive Radio y Advanced Spectrum Management, 2008. CogART 2008. First International Workshop on, 2008*, págs. 6-10. DOI: 10.1109/COGART.2008.4509987.

TAEWON HWANG; CHENYANG YANG; GANG WU; SHAOQIAN LI y YE LI, G. «OFDM and Its Wireless Applications: A Survey». En: *IEEE Transactions on Vehicular Technology* 58.4 (2009), págs. 1673-1694. ISSN: 0018-9545. DOI: 10.1109/TVT.2008.2004555. URL: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4607239>.

UCKELMANN, Dieter; HARRISON, Mark y MICHAHELLES, Florian. *Architecting the Internet of Things*. Springer, págs. 4-20. ISBN: 9783642191565. DOI: 10.1007/978-3-642-19157-2.

UIT. «Reglamento de Radiocomunicaciones». En: XXXIII.2 (2016), págs. 81-87. ISSN: 0717-6163. DOI: 10.1007/s13398-014-0173-7.2. arXiv: 9809069v1 [arXiv:gr-qc]. URL: <http://www.ncbi.nlm.nih.gov/pubmed/15003161%7B%5C%%7D5Cnhttp://cid.oxfordjournals.org/lookup/doi/10.1093/cid/cir991%7B%5C%%7D5Cnhttp://www.scielo.cl/pdf/udecada/v15n26/art06.pdf%7B%5C%%7D5Cnhttp://www.scopus.com/inward/record.url?eid=2-s2.0-84861150233%7B%5C%%7D5CnpartnerID=tZ0tx3y1>.

UIT-R. «ITU-R SM.1138-2 Determination of necessary bandwidths including examples for their calculation and associated examples for the designation of emissions». En: 1995.June (1998).

— *UIT-R SM.328-10 Definiciones Emisión no esencial Emisiones no deseadas*. 1999. ISBN: 1948195119.

UNNIKRISHNAN, Jayakrishnan y VEERAVALLI, Venugopal V. «Cooperative Sensing for Primary Detection in Cognitive Radio». En: *IEEE Journal of Selected Topics in Signal Processing* 2.1 (2008), págs. 18-27. ISSN: 1932-4553. DOI: 10.1109/JSTSP.2007.914880. URL: <http://ieeexplore.ieee.org/document/4453896/>.

URKOWITZ, H. «Energy detection of unknown deterministic signals». En: *Proceedings of the IEEE* 55.4 (1967), págs. 523-531. ISSN: 0018-9219. DOI: 10.1109/PROC.1967.5573. URL: <http://ieeexplore.ieee.org/document/1447503/>.

VENOSA, Elettra; HARRIS, Fredric J. y PALMIERI, Francesco A.N. *Software Radio, Sampling Rate Selection, Design and Synchronization*. Springer, 2012, págs. 1-5. ISBN: 9781461401124. DOI: 10.1007/978-1-4614-0113-1.

VISOTSKY, E.; KUFFHER, S. y PETERSON, R. «On collaborative detection of TV transmissions in support of dynamic spectrum sharing». En: *2005 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005* (2005), págs. 338-345. DOI: 10.1109/DYSPAN.2005.1542650.

WELCH, Peter D. «The Use of Fast Fourier Transform for the Estimation of Power Spectra: A Method Based on Time Averaging Over Short, Modified Periodograms». En: *IEEE Trans. Audio and electroacoustic* 15 (1967), págs. 70-73.

ZHANG, Qi; HUANG, Xiaobin; LI, Quanzhong y QIN, Jiayin. «Cooperative jamming aided robust secure transmission for wireless information and power transfer in MISO channels». En: *IEEE Transactions on Communications* 63.3 (2015), págs. 906-915. ISSN: 00906778. DOI: 10.1109/TCOMM.2015.2405063.