Diseño e implementación de un sistema de detección del ataque de emulación de usuario primario malicioso utilizando una máquina de soporte vectorial en redes cognitivas



UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Autor
Yesid Fabián Briceño Murillo
David Alejandro Barbosa Cortés

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS
Facultad Tecnológica
Ingeniería en Telecomunicaciones

Bogotá D.C. Mayo, 2021

Diseño e implementación de un sistema de detección del ataque de emulación de usuario primario malicioso utilizando una máquina de soporte vectorial en redes cognitivas



UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Autor

Yesid Fabián Briceño Murillo,
20181373006, yfbricenom@correo.udistrital.edu.co

David Alejandro Barbosa Cortés,
20181373005, daabarbosac@correo.udistrital.edu.co

Modalidad
Monografía

Presentado para optar al título de: Ingeniero(a) en Telecomunicaciones

Director
Ing. Luis Fernando Pedraza Martínez, Ph.D

Co-Director
Ing. Ernesto Cadena Muñoz, Ph.D

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS
Facultad Tecnológica
Ingeniería en Telecomunicaciones

Bogotá D.C. Mayo, 2021

Dedicatoria

Agradecemos a Dios por la oportunidad de realizar este proyecto, a nuestras familias siendo el motor, fortaleza y compañía sin igual para seguir adelante, a nuestros maestros y colegas que nos ayudaron a la elaboración de la monografía.

Índice

Índice de Figuras 2
Glosario 4
Lista de Abreviaturas y Siglas 7
Resumen 8
1. Introducción 9
2. Planteamiento del problema 10
3. Justificación 10
4. Objetivos 11
4.1. Objetivo General 11
4.2. Objetivos específicos 11
5. Marco de referencia 11
5.1. Antecedentes 11
5.2. Marco teórico 19
5.3. Marco Legal 29
6. Metodología 31
6.1. Diseño de un sistema de detección basado en una máquina de soporte vectorial para la detección del PUE malicioso en redes cognitivas. 31
6.2 Diagrama de Red 33
6.3. Diagrama de Funcionamiento del Sistema 35
6.4. Detección de Energía 36
6.5. Cálculo de la entropía 38
6.6. Entrenamiento y Detección del ataque PUE a través de SVM 40
7. Resultados 44
7.1 Implementación de la máquina de soporte vectorial a través de radio definida por software para detectar el ataque PUE malicioso en redes cognitivas. 44
7.1.1 Adquisición y minería de datos 46
7.1.2 Cálculo entropía y Entrenamiento de la SVM. 49
7.1.3 Support vector machine 50
7.1.4 Interfaz gráfica 53
7.2 Evaluación de los resultados obtenidos con la probabilidad de detección estimada. 55
8. Conclusiones 59
9. Referencias 61

Índice de Figuras

Figura 1. Arquitectura de Radio Cognitiva 22

Figura 2. Ciclo cognitivo para el acceso dinámico al espectro.....22

Figura 3. Presencia del ataque PUE en la red de radio cognitivo.....27

Figura 4. Diagrama de Bloques de la fase 2 a implementar.....31

Figura 5. Diagrama de Bloques del sistema implementado.....33

Figura 6. Diagrama de Bloques del funcionamiento del sistema.....35

Figura 7. Toma en GNU Radio del ataque encendido…….....36

Figura 8. Toma en GNU Radio del ataque apagado.....37

Figura 9. Transformación de datos en formato Hexadecimal IEEE 754.....37

Figura 10. Transformación de datos en formato a coma flotante (Float).....38

Figura 11. Funcionamiento de la máquina de soporte vectorial (SVM) con dos dimensiones.....39

Figura 12. SVM evaluando 2 valores como ejemplo.....40

Figura 13. Ingreso varios valores a la SVM…….. 41

Figura 14. Muestra de 3 hiperplanos de ejemplo…….....41

Figura 15. Ejemplo de SVM con datos reales….....42

Figura 16. Plano de cuadrícula para toma de muestra de entropías.....42

Figura 17. Cuadrícula montada para toma de muestra de entropías.....43

Figura 18. USRP y SDR en toma de muestras de entropías.....43

Figura 19. Entrenamiento de la SVM con los datos de entropía recolectados….....44

Figura 20. Diagrama definitivo del sistema de detección…….....45

Figura 21. Archivo .BIN en codificación UFT-8…….....46

Figura 22. Bloque de programa en Python…….....46

Figura 23. Utilización de la librería xdd. Fuente: Autor…….....47

Figura 24. Limpieza y transformación de los datos obtenidos…. 47

Figura 25. Ejemplo de trama de 32 bits del estándar del IEEE…….....48

Figura 26. Valores transformados a coma flotante …….....48

Figura 27. Código para hallar la entropía de la señal obtenida 49

Figura 28. Ejemplo de muestra de entropías calculadas cuando no hay ataque.....49

Figura 29. Entrenamiento Final de la SVM.....50

Figura 30. Vector Final cuando hay un ataque…….....51

Figura 31. Lectura de información final del usuario, indicando la presencia de un ataque.....…52

Figura 32. Vector Final cuando no hay un ataque……. 52

Figura 33. Lectura de información final del usuario, indicando que no hay un ataque.....53

Figura 34. Interfaz inicial del programa……..…….....53

Figura 35. Mensaje final al usuario de detección de un ataque PUE Malicioso…….....54

Figura 36. Mensaje final al usuario confirmando que la muestra tomada no es un ataque 54

Figura 37. Toma de muestras del ataque …….....55

Figura 38. Gráfica del porcentaje de detección de ataque por posición…….....……56

Figura 39. Porcentaje de detección de ataque por posición…….....…….....57

Figura 40. Porcentaje de eficiencia del sistema…….....……...58

Glosario

Base de Datos	Una base de datos es un conjunto de datos que pertenecen a un mismo contexto, los datos son almacenados sistemáticamente como si fuese una biblioteca virtual, y podrá ser consultada cuando sea necesario.
Entropía	Ecuación matemática para poder explicar algunos procesos, midiendo el grado de desorden con respecto a la probabilidad de ocurrencia de alguna acción.
Espectro Radioeléctrico	El espectro electromagnético, no se puede ver ni sentir, pero está presente en el aire; por medio de esta es posible transmitir señales de radio, televisión, Wi-Fi entre otras.
Frecuencia	Frecuencia es la medida del número de veces que se repite un fenómeno por unidad de tiempo; por ejemplo, el sonido o la luz, cada onda de ellas se repite una determinada cantidad de tiempo, a ello se le denomina frecuencia.
Hiperplano	La palabra hiperplano se define como una extensión de un plano, en el cual divide una línea en dos líneas. En un espacio tridimensional, un hiperplano divide el espacio en dos mitades. Este concepto también puede ser aplicado a espacios de cuatro dimensiones y más, donde estos objetos divisores se llaman simplemente hiperplanos, ya que la finalidad de esta nomenclatura es la de relacionar la geometría con el plano.

Machine Learning	Machine Learning es una nueva disciplina científica del ámbito de la Inteligencia Artificial, que desarrolla sistemas que son capaces de aprender automáticamente; es decir, identifica patrones complejos en millones de datos. La máquina que realmente aprende es un algoritmo que revisa los datos y es capaz de predecir comportamientos futuros.
Minería de datos	Es un campo de la estadística y las ciencias de la computación referido al proceso que intenta descubrir patrones en grandes volúmenes de conjuntos de datos.
Radio cognitiva	Sistema de comunicaciones inalámbricas inteligente que es consciente de su entorno y aprende de su entorno y adaptar su estado interno a las variaciones estadísticas en los estímulos de RF de entrada haciendo los correspondientes cambios en ciertos parámetros de operación.
SDR	Sistema de radiocomunicaciones donde varios de los componentes típicamente implementados en hardware son implementados en software, utilizando un ordenador personal u otros dispositivos de computación embebidos.
SVM	Máquina de soporte vectorial. Originariamente se desarrolló como un método de clasificación binaria, esta aplicación se ha extendido a desarrollos de problemas de clasificación múltiple y regresión. Esta aplicación ha resultado ser uno de los mejores clasificadores, utilizado por muchos software y programas dentro del ámbito de aprendizaje estadístico y machine learning.
PUE	Un atacante envía señales similares a las de los usuarios primarios durante el período de detección del espectro y por lo tanto provoca falsas alarmas a los verdaderos usuarios de la red, si los usuarios primarios en realidad no están presentes.

USRP	Es un periférico diseñado para trabajar en conjunto con un procesador externo (PC, Workstation,) a través de una FPGA y permite la realización de Software Radios.

Lista de Abreviaturas y Siglas

Sigla/Abreviatura	Significado
CR	Radio cognitiva
CRN	Cognitive Radio Network
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
GMSK	codificación Gaussiana de Desplazamiento Mínimo
GSM	Global System for Mobile communications
OFDM	Multiplexación por división de frecuencia ortogonal
PUE	Emulación de Usuario Primario
PUEA	Primary User Emulation Attack
PU	Usuario primario
RF	Radio frecuencia
SR	SR Software Radio
SDR	Radio definido por Software
SU	Usuario secundario
SVM	Máquina de soporte vectorial
UIT	Unión internacional de telecomunicaciones
UHF	Ultra High Frequency
USRP	Universal Software Radio Peripheral
VHF	Very High Frequency

Resumen

Dentro de los servicios de telecomunicaciones que prestan diferentes compañías del sector hacen uso del espectro electromagnético, para ello deben usar bandas del espectro electromagnético licenciadas y por lo general cada país mediante subastas permiten que estas compañías usen espacios de frecuencia para prestar un servicio, sin embargo, el optimizar el espectro juega un papel muy importante y más aún cuando se identifica que hay espacios que están siendo usados de manera ilegal y afectan la operación del servicio[1].

Para este tipo de redes, existen dos tipos de usuarios PU (usuario primario) y SU (usuario secundario), los PU poseen licencias de uso de las bandas y el acceso prioritario a ellas, mientras que los SU no tienen licencias, pero pueden utilizar estas bandas de frecuencia sin interferir en la comunicación de los usuarios primarios y es por ello que estas bandas deben aceptar este tipo de interferencias; aprovechando esta situación, los ataques de emulación de usuario primario permite que un usuario secundario malintencionado manipula su radio para imitar el comportamiento de un usuario primario legítimo, impidiendo que los usuarios secundarios legítimos se puedan conectar a este tipo de frecuencias [2].

Con el fin de identificar estos ataques se hizo la implementación de una SVM (máquina de soporte vectorial) esta hace uso de un hiperplano de separación óptimo donde se realiza la agrupación de datos en dos grupos, el primero representa datos que hacen parte de un ataque malicioso y el otro grupo aquellos que no son un ataque, es así que al definir un margen máximo nos permitirá identificar si la muestra de datos capturadas del espectro corresponde a un ataque o no. Cabe mencionar que se debió realizar un tratamiento previo al dataset creado con los niveles de energía que se toman y con el uso de la entropía, esta nos ayuda a identificar la cantidad de información promedio que contienen las mediciones realizadas.

Al lograr la implementación de la SVM se debió entrenar la misma, es decir, en primera instancia se le entrega a la SVM datos que representan un ataque y otro grupo de datos que no son ataque, estos datos son tomados directamente de las mediciones de espectro sobre las frecuencias de trabajo en diferentes posiciones planteadas, es así con el hiperplano fijar las zonas donde puede caer un posible ataque, es así que al realizar el proceso en tiempo real indicará después de procesar y hacer los respectivos cálculos con toda la información sí hay un ataque malicioso presente en el espectro.

Palabras claves: Espectro Radioeléctrico, Emulación de Usuario Primario, Minería de Datos, Radio Cognitiva, Radio definido por Software.

1. Introducción

La radio cognitiva es una novedosa tecnología, muy eficiente en comunicaciones inalámbricas para optimizar el uso del espectro, pues utiliza las bandas del espectro libre que no están siendo utilizadas sin causar interferencia con otras comunicaciones inalámbricas [27]. Sin embargo, se han realizado ataques de este tipo de tecnología, interrumpiendo los servicios de todos los usuarios conectados a la red. El ataque de emulación de usuario primario disminuye la probabilidad de entrar en el espectro, actuando como negación de servicio gracias a ataques de usuarios maliciosos que acceden a esta red sin licencia; las investigaciones que han abordado este tema se han centrado en los métodos de detección fijo, ya sea por medio de energía, localización, entre otras, pero muy poco se sabe del método de detección en dispositivos móviles [14]. Se diseñó e implementó un sistema de detección móvil para clases de ataque malicioso PUE, con el fin de que la red cognitiva pueda reconocer entre un usuario primario real y un atacante PUE malicioso.

El uso de la Radio Cognitiva optimiza el uso del espectro, sin embargo, implementando la máquina de soporte vectorial en este sistema, la cual permite detectar los ataques de emulación usuarios primarios maliciosos, mejora aún más el uso del espectro. Para ello fue necesario realizar un entrenamiento para que el sistema pueda identificar e informar la presencia de un atacante sobre la frecuencia trabajada. Para realizar este entrenamiento, fue necesario tomar varias mediciones del espectro simulando un ataque, con el equipo USRP-2922 y realizando minería de datos sobre los datos capturados, para poder entregar a la SVM valores de entropía, que se generan a partir de los valores de energía capturados gracias al SDR.

Gracias al entrenamiento realizado, el sistema nos permite detectar en tiempo real un posible ataque de emulación de usuario primario malicioso e indicar qué espacios del espectro están siendo ocupados de manera ilegal, con ello permitirá tomar las acciones necesarias por parte de las entidades de control como la ANE, con el fin de dar de baja a estos ataques.

En sus primeros capítulos se encuentra la introducción, el planteamiento del problema, la justificación y los objetivos, en donde se pretende mostrar la importancia del tema trabajado en este proyecto. El capítulo 6 describe el desarrollo del sistema implementado, el cual se divide en seis fases: el diseño del sistema implementado, el cual explica el desarrollo el primer objetivo específico, también se encuentran los diagramas de funcionamiento del sistema y el diagrama de la red implementada, como se realizó la detección de energía, el cálculo de la entropía y por último el entrenamiento y la explicación sobre la detección del ataque.

Finalmente se entregan los resultados y las conclusiones, estos se encuentran alojados dentro de los capítulos 7 y 8 respectivamente, en ellos se realizan las mediciones y validación de resultados, presentando los dos últimos objetivos específicos planteado para este proyecto.

2. Planteamiento del problema

El espectro electromagnético se divide en diferentes bandas de frecuencia, al hacer uso de estas permite prestar un servicio, esto es realizado por parte de compañías o entidades de telecomunicaciones avaladas y protegidas por las instituciones creadas para tal fin, definidas por la administración de cada país. Debido a la saturación del espectro disponible, se decidió otorgar licencias para poder hacer uso de este; gracias a esta distribución del espectro se han generado "espacios en blanco" que han motivado el uso de mecanismos como las redes de radio cognitiva, con el fin de aprovechar mejor la capacidad del espectro de radiofrecuencias [1].

Para este tipo de redes, existen dos tipos de usuarios que comparten el espectro de radiofrecuencias denominados usuarios primarios y usuarios secundarios, los PU poseen licencias de uso de las bandas y el acceso prioritario a ellas, mientras que los SU no tienen licencias, pero pueden utilizar estas bandas de frecuencia sin interferir en la comunicación de los usuarios primarios y es por ello que estas bandas deben aceptar este tipo de interferencias; permitiendo que este tipo de comunicaciones tenga cierta tolerancia de error y utilicen técnicas para mitigar estos efectos como el ensanchamiento de espectro o saltos de frecuencia [2].

Aprovechando esta situación, se pueden presentar ataques de emulación de usuario primario, denominados PUE (por sus siglas en inglés, Primary User Emulation). En este tipo de ataques un usuario secundario malintencionado manipula su equipo transmisor para imitar el comportamiento de un Usuario Primario legítimo, con lo cual ocupa la banda de frecuencia como si fuera un PU. Esta acción impide que los usuarios secundarios legítimos se puedan conectar a la misma frecuencia, y disminuye la cantidad de usuarios que pueden entrar en estas bandas del espectro [3].

3. Justificación

Un estudio realizado [3] donde se pone en consideración la banda comprendida entre los 30 MHz y los 3 GHz, se evidencia que ciertos espacios de frecuencias no están siendo extensivamente utilizadas, mostrándose por ejemplo que las frecuencias utilizadas para la televisión tan solo usan aproximadamente el 25 % del espectro que tienen licencia para realizar sus transmisiones, lo cual deja en evidencia que la escasez en la disponibilidad de frecuencias en el espectro se debe primordialmente a la asignación fija de frecuencias[5], igualmente las bandas de frecuencia para telefonía celular no son la excepción y se repite este comportamiento. Es por esto que la CR y el uso de SDR permite el desarrollo de soluciones que optimizan los parámetros de funcionamiento, aprovechando de la mejor manera el espectro disponible, al tiempo que pueden aprender de los resultados obtenidos a través de la minería de datos.

Cabe mencionar que actualmente se realizan muchos ataques de seguridad con propósitos egoístas o maliciosos sobre los sistemas de radio cognitiva, pero, se debe tener en cuenta que el ataque PUE

es el más frecuente y el que puede llegar a causar más daño sobre estos sistemas, es por ello que el desarrollo de este proyecto busca solventar esta problemática, al diseñar e implementar un sistema de detección del ataque de emulación de usuario primario malicioso, donde mediante el uso de dispositivos de radio definidos por software es posible generar ataques a la red de radio cognitiva móvil que incluyen la alteración de los datos de detección y la emulación de las señales procedentes de una red primaria [44], lo cual permite obtener las características de este tipo de ataque y esta información es enviada a una máquina de soporte vectorial basada en software libre y mediante un proceso de entrenamiento permite la detección del ataque PUE al momento de ingresar datos tomados en el espectro.

4. Objetivos

4.1. Objetivo General

- Diseñar e implementar un sistema de detección para el ataque de emulación de usuario primario malicioso utilizando una máquina de soporte vectorial en redes cognitivas.

4.2. Objetivos específicos

- Diseñar un sistema de detección basado en una máquina de soporte vectorial para la detección del PUE malicioso en redes cognitivas.
- Implementar la máquina de soporte vectorial a través de radio definida por software para detectar el ataque PUE malicioso en redes cognitivas.
- Evaluar los resultados obtenidos con la probabilidad de detección estimada.

5. Marco de referencia

5.1. Antecedentes

A continuación, se presentan algunos de los documentos más relevantes que se encontraron en la primera fase del desarrollo el proyecto, mediante los cuales se establece punto de partida de los diferentes métodos o modelos usados en la detección de ataques haciendo uso de la radio cognitiva, esto con el fin de lograr la optimización del uso del espectro electromagnético y encontrar estos espacios que son normalmente atacados por usuarios malintencionados.

5.1.1. Detección de espectro para radio cognitiva

Como primera medida se identifica la importancia que cumple la radio cognitiva en la búsqueda de usuarios licenciados:

> *"Este artículo centra su atención en la capa física de las redes de radio cognitiva (CR), es decir, en las técnicas que se utilizan para detectar la presencia o ausencia de usuarios licenciados en las diferentes bandas del espectro electromagnético. Las técnicas presentadas, con sus ventajas y desventajas, están organizadas jerárquicamente como: técnicas fundamentales (detección de energía, filtro adaptado y características ciclo-estacionarias), técnicas basadas en las fundamentales o evolución (detección de forma de onda, identificación del radiotransmisor, detección de la potencia de fuga en el receptor) y técnicas alternativas típicas del análisis de imágenes (transformada Hough y Wavelet)" [6].*

Este artículo fue elaborado por integrantes de la Universidad Distrital Francisco José de Caldas y la Universidad Nacional de Colombia, donde se analizan las técnicas para detectar algunos ataques, describiéndolos como usuarios licenciados y no licenciados; se mencionan diferentes programas o herramientas para poder utilizar las técnicas de la mejor manera, algo fundamental para este artículo.

5.1.2. Análisis de la Movilidad Espectral en Redes de Radio Cognitiva

Partiendo que el Handoff es el sistema en las comunicaciones celulares donde el fin es transferir el servicio de una estación base a otra cuando la calidad del enlace es insuficiente en una de las estaciones, la radio cognitiva busca optimizar esa detección:

> *"Se presenta una revisión sobre la movilidad espectral en redes de radio cognitiva, describiendo el Handoff espectral, sus clasificaciones, sus enfoques actuales, sus criterios de decisión y sus métricas de evaluación de acuerdo con la literatura actual. La revisión se realizó a partir del análisis de publicaciones recientes de corriente principal con sus respectivas citas, tratando de proveer un marco referencial completo de la literatura actual sobre la movilidad espectral en redes de radio cognitiva" [7].*

El artículo toca un tema importante para la radio cognitiva, es el tema del Handoff y la optimización de la detección, teniendo en cuenta el comportamiento del usuario, al igual que el artículo anterior, se mencionan diferentes técnicas, sin embargo, en este estudio sugiere que se deben diseñar algoritmos adaptativos que permitan optimizar los recursos involucrados durante el Handoff espectral.

5.1.3. Caracterización de usuarios primarios para la implementación de un modelo predictor para la toma de decisiones en redes inalámbricas de radio cognitiva

Identificar las características que componen a un PU permitirá crear modelos de predicción para toma de decisiones:

"Este artículo se basa en la fase de decisión de espectro, una de las funciones más importantes de la Radio Cognitiva ya que tiene la habilidad de seleccionar la mejor banda de espectro disponible, satisfaciendo los requerimientos de calidad de servicio (QoS) y que no ha sido adecuadamente explorada. La fase de "Decisión de espectro" se compone de tres funciones claves que son: Caracterización de espectro, que identifica las condiciones del entorno y las actividades del usuario licenciado; Selección de espectro, se encarga de hallar la banda de espectro más adecuada que cumpla con los requisitos de calidad para los usuarios cognitivos y la reconfiguración, que permite reconfigurar los parámetros de transmisión" [8].

La decisión del espectro de la radio cognitiva es un tema fundamental en el desarrollo de este proyecto, entendiendo un poco en que se basa la Red de Radio Cognitiva y que posibilidades de espectro puede tomar; también nos permite identificar el comportamiento en el espectro de un usuario licenciado y un usuario no licenciado.

5.1.4. Primary User Emulation Attack (PUEA) In Cognitive Radio Network (CRN)

Algunos usuarios secundarios pueden detectar usuarios primarios con el fin de establecer una comunicación, sin embargo, estos pueden caer en un ataque malicioso, acá se compare una técnica de detección:

"En las redes de radio cognitiva, el objetivo principal de los usuarios secundarios es detectar la presencia del usuario principal, para ello existen diferentes técnicas de detección, usando principalmente la detección de energía promedio de los datos de la muestra, matched filter (filtro combinado) y enfoque bayesiano de modelado previo y posterior de señal media. La situación se vuelve engorrosa cuando está presente uno o varios usuarios maliciosos, especialmente emuladores de usuario primario (PUE). Este artículo explica cómo se basaron en el modelo de detección de energía por pérdida de ruta exponencial en una pequeña región, donde tanto el usuario secundario como PUEA se distribuyen aleatoriamente y el uso del modelo Okumura-Hata para enlaces largos de usuario secundario y usuario primario para finalmente graficar el límite inferior de probabilidad de PUEA contra la distancia vacía al PUEA" [9].

Este artículo nos expone el estudio y detección de ataques de emulación a usuarios primarios en las redes móviles, el autor usa una técnica de detección, denominada método de detección por energía, el cual es un método de medición de ocupación de canal, que de manera sencilla permite determinar si un canal está en uso aprovechando el nivel de energía de la señal. El desarrollo de este proyecto nos permite entender dichos conceptos y ver resultados importantes los cuales se tuvieron en cuenta dentro de este proyecto, ya que arrojan una alta funcionalidad y efectividad para poderlos implementar en otros entornos.

5.1.5. Primary User Emulation Attack in Cognitive Radio Networks: A Survey

La radio cognitiva es una tecnología prometedora con el objetivo de resolver el problema de escasez de espectro asignado el espectro dinámicamente a usuarios con licencia, para ello utiliza las bandas de espectro libre que no están siendo utilizadas por los usuarios con licencia sin causar interferencia a la transmisión actual; por esta razón, la detección del espectro es el mecanismo esencial toda la comunicación, si se viola el resultado de la detección del espectro, se interrumpirán las actividades de redes enteras. El Ataque de Emulación de Usuario Primario (PUEA) es una de las principales amenazas para la detección del espectro libre, que disminuye el acceso al espectro probabilidad. En este documento, nuestros objetivos son dar varios problemas de seguridad en redes de radio cognitivas y luego para discutir el PUEA con las técnicas existentes para mitigarlo [10].

Analizando los diferentes tipos de ataques que pueden existir para la red de radio cognitiva, exponen diferentes tipos de ataque a este sistema, y plantean algunas soluciones, de las cuales han mencionado en otros artículos, sin embargo, este documento es muy importante ya que son los pioneros en debatir sobre la vulnerabilidad de esta red y que tipos de ataques existentes pueden haber.

5.1.6. Base de ataque anti-PUE en la identificación de la huella digital del transmisor en radio cognitiva

Los PUE no se ven en redes de comunicación móviles únicamente, es así que se pueden en otro tipo de redes:

> *"La mayoría de los esquemas de seguridad conocidos apuntan a la confirmación de la ubicación del transmisor establecido, pero no está disponible para redes Ad hoc. Se propone un nuevo escenario de seguridad en la capa física, aprovechando la verificación de "huella digital" del transmisor contra ataques de emulación de usuario primario (PUE). El ruido de fase de la portadora ruidosa se extrae de la señal modulada recibida y se aplica directamente para identificar el transmisor. Esquemas de seguridad ataques primarios de emulación de usuario" [11].*

Para poder analizar un poco mejor los PUE, se estudia como es el comportamiento en otro tipo de redes como lo son las redes Ad Hoc, utilizando la red de radio cognitiva para poder analizar un nuevo escenario de seguridad, mirando la huella de las frecuencias usadas y analizando la señal modulada, para poder ver el transmisor de este ataque, algo ideal para cualquier sistema de detección de ataque.

5.1.7. Ataque anti-PUE basado en la verificación de posición conjunta en redes de radio cognitivas

Se busca identificar el origen o posición del transmisor usando principalmente la prueba de relación de distancia:

> *"Se propone un método de verificación de posición conjunta para mejorar la precisión de posicionamiento ya que hay varios métodos de confirmación de la ubicación del transmisor establecido, como las tecnologías de verificación de la prueba de relación de distancia (DRT) y la prueba de diferencia de distancia (DDT) y no es tan preciso cuando se lleva a la práctica. Los resultados de la simulación muestran que el método aquí expuesto es simple y logra una alta precisión en la verificación de la ubicación del transmisor en la red CR, lo que puede mejorar la capacidad de resistir el ataque PUE" [12].*

De este artículo nos basamos en parte para obtener conocimiento sobre la detección del ataque a través de la energía, es decir, si se conoce la cantidad de la energía, se podría conocer un poco más a fondo sobre la posición exacta del transmisor de este ataque. Para ello se realizan diferentes pruebas, comparando las simulaciones en diferentes softwares, dentro de ellas GNU Radio, como la fase práctica.

5.1.8. Rényi Entropy-Based Spectrum Sensing in Mobile Cognitive Radio Networks Using Software Defined Radio

El uso de la radio cognitiva debe apoyarse en herramientas que el mercado nos ofrece en la búsqueda de usar los canales libres y no interferir con comunicaciones establecidas de manera licenciada:

> *"A very important task in Mobile Cognitive Radio Networks (MCRN) is to ensure that the system releases a given frequency when a Primary User (PU) is present, by maintaining the principle to not interfere with its activity within a cognitive radio system. Afterwards, a cognitive protocol must be set in order to change to another frequency channel that is available or shut down the service if there are no free channels to be found. The main contribution of this research is that uses a Software Defined Radio (SDR) system to implement a MCRN in order to measure the behavior of Primary and Secondary signals in both time and frequency using GNURadio and OpenBTS as software tools to allow a phone call service between two Secondary Users (SU)" [13].*

Este artículo es muy importante para el desarrollo de este proyecto, ya que obtuvimos la información de cómo trabajar la entropía con este tipo de datos (basándonos en la energía) y en gran parte de cómo operaba la red para la creación del ataque, como manejar las herramientas de GNU Radio y Open BTS en el USRP, y datos de cómo entablar esa comunicación móvil y cómo obtener esas frecuencias.

5.1.9. Detection of Malicious Primary User Emulation Based on a Support Vector Machine for a Mobile Cognitive Radio Network Using Software-Defined Radio

Uno de los principales propósitos de las redes móviles de radio cognitiva es encontrar las vulnerabilidades como es la emulación de usuario primario:

> *"Mobile cognitive radio networks provide a new platform to implement and adapt wireless cellular communications, increasing the use of the electromagnetic spectrum by using it when the primary user is not using it and providing cellular service to secondary users. In these networks, there exist vulnerabilities that can be exploited, such as the malicious primary user emulation (PUE), which tries to imitate the primary user signal to make the cognitive network release the used channel, causing a denial of service to secondary users. We propose a support vector machine (SVM) technique, which classifies if the received signal is a primary user or a malicious primary user emulation signal by using the signal-to-noise ratio (SNR) and Rényi entropy of the energy signal as an input to the SVM." [14]*.

El SVM es un pilar muy importante de este proyecto, ya que a través de la inteligencia artificial puede determinar si hay o no un atacante, y para lograr ello es fundamental este artículo, ya que va un poco más allá y muestran procedimiento adicional, material valioso para el desarrollo de este proyecto. Este artículo no realizaba la toma de muestra en tiempo real, ya que conlleva un procedimiento bastante robusto.

5.1.10. Al Interior De Una Máquina De Soporte Vectorial

Dentro de la revisión del estado del arte, es importante familiarizarse con conceptos que se están manejando con la SMV, es así que se conocen los procesos que apoyan con el objetivo de la SVM:

> "*Se exponen aspectos teóricos generales y algorítmicos al interior de una Máquina de Soporte Vectorial (MSV), la función kernel asociada y el algoritmo SMO, vitales en la actual solución eficiente de problemas de clasificación, el cual para este artículo general será de gran ayuda para el análisis de las diferentes entropías y poder determinar si es un ataque o no. Se describe de manera detallada la aplicación de los algoritmos en la solución de un problema simple, complementando la extensa literatura teórica existente" [15]*.

Para fines de este proyecto es importante hablar del entrenamiento previo, como se realiza este proceso, amplios conceptos teóricos que son necesarios. También se muestra cómo manejar las entropías, ya que no solo trabaja con la entropía Renyi, sino que trabaja con la entropía de Shannon, lo cual da otra perspectiva, de cómo trabajar este proceso conjuntamente con la SVM.

5.1.11. Detección De Ataques Epilépticos A Partir De Señales Fisiológicas

Como se mencionó anteriormente la SVM es un sistema que se pueden trabajar en otras áreas y apoyan en procesos de detección:

> *"Se analizaron algunas características por medio de métodos estadísticos para escoger cuáles contribuyen en la detección de ataques epilépticos. Se diseñaron diferentes clasificadores de redes neuronales, máquinas de soporte vectorial (SVM) y métodos del vecino más cercano (k-NN) que reconocieran estos patrones y, por último, se evaluó el funcionamiento de estos sistemas para diferenciar las convulsiones. El sistema con mejor rendimiento fue la máquina de soporte vectorial" [16].*

Se pudo observar que es el manejo en otros ámbitos de trabajo, como lo son los ataques epilépticos, también se puede utilizar una SVM, que también se manejan otro tipo de detecciones como el método del vecino más cercano (k-NN), lo cual nos permite un conocimiento un poco más amplio y de las diferentes maneras de cómo manejar la SVM, visto desde otra área de trabajo.

5.1.12. Aprendizaje Automático para la detección de ataques informáticos

> *"Los ciberataques inspiraron a explotar una rama relativamente reciente y en crecimiento de la Inteligencia Artificial como es el Aprendizaje Automático de las máquinas. Esta nueva rama puede usarse en muchas facetas de la vida cotidiana; por tanto, se expone una breve descripción de qué es el Aprendizaje Automático, que aplicaciones se le pueden a dar y, en particular se enfocó en la de la predicción de un tipo de ataque maliciosos como son las producidas por los accesos a URLs maliciosas" [17].*

Dentro de la revisión del estado del arte, es importante familiarizarse con conceptos que se están manejando, como lo es el método de aprendizaje a la SVM, para ello se revisa este artículo para obtener mayor información de cómo se realiza el aprendizaje automático de una inteligencia artificial, aquí lo manejan analizando qué URLs pueden ser maliciosas o pueden ser un ataque, y que el mismo sistema corrija este tipo de incidencias, en la teoría es muy necesario tener esta información.

5.1.13. Modelo basado en técnicas de aprendizaje automático permitirá detectar ataques a sistemas informáticos

La detección de ataques es crucial actualmente en cualquier tipo de sistemas y aún más automatizar estos procesos en los procesos de aprendizaje para identificar los mismos:

> *"La ciberseguridad es un ámbito de trabajo bastante apetecido en la actualidad debido al alto volumen de ataques a los que están expuestos los sistemas informáticos empresariales. El acceso ilegal a información organizacional sensible y con fines maliciosos, haciendo uso de programas que secuestran los datos, como ransomware, ha generado pérdidas cuantiosas en múltiples*

organizaciones. El alto y variado volumen actual de amenazas ha conllevado a que los investigadores desarrollen diferentes herramientas, metodologías y técnicas, con el fin de salvaguardar el activo más importante para las organizaciones hoy en día: la información. Algunas de estas soluciones son desarrollar un modelo basado en GHSOM (Mapas Autoorganizativos de Jerarquía Creciente), mediante la hibridación con otras técnicas como el Modelo de Mezclas Gaussianas o haciendo uso de Máquinas de Soporte Vectorial – SVM" [18].

Se tomaron los resultados y se desarrolló un software basado específicamente para recrear una estructura de red computacional y embeberlo en un Sistema de Detección de Intrusos que pueda evaluar el tráfico, identifique el ataque y determine de qué tipo es. El modelamiento de algunas técnicas de aprendizaje y con herramientas robustas.

5.1.14. Sistema de detección de intrusos para plataformas SCADA mediante algoritmos de aprendizaje automático

Se estudian ataques pueden afectar incluso a la industria y poner en riesgo la seguridad de un sistema específico como son los SCADA:

"Los sistemas SCADA, acrónimo de Supervisor Control And Data Acquisito (supervisión, Control y adquisición de datos), son redes de control que permiten el seguimiento y gestión de procesos industriales de forma remota. Al principio, su máxima prioridad era la disponibilidad de información bidireccional entre la estación de control y las unidades remotas; sin embargo, la creciente escalada de los sistemas industriales, así como la conectividad a internet ha llevado a reconsiderar el viejo paradigma para darle más importancia al tema de la seguridad, con el fin de evitar que un posible ciberataque ponga en peligro el funcionamiento del sistema SCADA" [19].

El presente trabajo propone la creación de un sistema adaptativo para la detección de intrusos o IDS en redes SCADA, mediante el uso de técnicas de aprendizaje automático supervisado, orientado al análisis de variables de los dispositivos de control. Un vector de soporte de máquina tipo "Clase Uno" y un laboratorio de pruebas, permitieron la validación del modelo propuesto.

5.1.15. Ciclo Autonómico de Análisis de Datos para el Diseño de Descriptores para Algoritmos de Aprendizaje Automático

Palo lograr la implementación de una SVM es crucial aplicar un método que permita analizar la información que recibirá la misma en distintos escenarios, es así que se hace uso de la entropía:

"Se propone un método basado en programación genética (GP por sus siglas en inglés), para obtener características faltantes en datos incompletos. En esta técnica se propone un proceso de construcción de características basadas en entropía, para la detección de ataques en redes de

comunicación. Este proceso consta de tres partes: primero, se extraen características de cada cabecera de los paquetes de red" [20].

Este artículo nos muestra cómo realizar un análisis de datos posteriormente a un ciclo de aprendizaje, a través de la entropía de Shannon, usando un intervalo de tiempo específico, y posteriormente se construyen nuevas características con variaciones de entropía con características combinadas.

5.2. Marco teórico

A continuación, se expone algunos conceptos clave que se tuvieron en cuenta como base teórica de este proyecto, como lo es la detección de espectro, la Radio Definida por Software, sistemas de radio cognitivos, algunas características de este, diferentes ataques a la red cognitiva, se explica en qué consiste la Emulación de Usuario Primario, algunas técnicas actuales de detección y defensa de este y finalmente la aplicación de la minería de datos.

5.2.1. Detección De Espectro

El espectro electromagnético cuenta con una amplia región de frecuencias licenciadas donde estas son parcialmente usadas, esto ha ido generando una degradación en la calidad de servicio en algunas zonas espectrales por falta de disponibilidad, mientras que en otras presten una parte del espectro como como en las bandas VHF/UHF como consecuencia de la utilización inadecuada y esporádica, debido a la amplia demanda de espectro [2].

La finalidad de un sistema diseñado para transmisión/recepción de CR en un equipo de comunicaciones inalámbricas, es detectar inteligentemente ya sea un segmento particular del espectro radial que está siendo utilizado, del segmento del espectro que no está siendo utilizado temporalmente, sin interferir con la trasmisión de los usuarios autorizados y que esté consciente del ambiente en el que opera, y pueda dinámicamente y autónomamente ajustar acordemente sus parámetros de operación [3].

Un usuario de CR puede transmitir únicamente en frecuencias que no estén siendo usadas en el espectro que lo rodea, por lo tanto, dicho usuario debe monitorear las bandas disponibles e inteligentemente determinar lo que se conoce como huecos espectrales; es allí donde el término "detección" se convierte en un término más amplio que involucra la obtención de características de uso espectral en múltiples dimensiones como el tiempo, el espacio, la frecuencia y el código. Esto requiere técnicas más robustas para el análisis de señales, que suponen mayor complejidad desde el punto de vista computacional [21].

5.2.2. Radio Definida Por Software (SDR)

El origen de la tecnología de radio definida por software, tiene una relación con el área militar, donde los nuevos equipos de radio debían trabajar en conjunto con los equipos antiguos. También existían casos en los que se realizaban operaciones conjuntas entre aliados, los cuales poseían equipos de comunicaciones incompatibles. Esto quiere decir que una misma pieza de hardware puede realizar diferentes funciones en distintos instantes de tiempo con sólo introducir algún cambio en su configuración mediante software [22].

El concepto de SDR surgió para ofrecer un mejor control al software de un sistema de comunicación ya que estos combinan tanto tecnologías de software como de hardware y de Radiofrecuencia (RF), gracias a la integración se puedan transmitir, recibir y procesar señales de radio con mayor flexibilidad y eficiencia, comparado con un sistema enfocado solamente en la parte de hardware. Un sistema SDR intenta que la mayor parte de los componentes del sistema se lo implementa en software y de esta forma gracias a un dispositivo reprogramable, estos componentes pueden ser reconfigurados con facilidad cuando sea necesario, y los problemas que anteriormente se relacionaban a la parte de hardware, sean ahora problemas de software es decir de código o programación [23].

5.2.2.1. Tipos De SDR

A continuación, se describen 5 tipos de SDR

Tipo I: Para la implementación de este se usa una tarjeta de audio convencional de un host como digitalizador y software de PC como herramienta de procesamiento. Debido a estas características es el tipo de SDR que es más accesible.

Tipo II: Este SDR se encarga de capturar la señal desde algún dispositivo por ejemplo una antena y a partir de allí empieza toda la parte de procesamiento de la información. Esto es implementado debido a un dispositivo especial que realiza el proceso completo.

Tipo III: Este tipo de SDR trabaja capturando la señal desde una IF analógica y la procesa a partir de allí.

Tipo IV: Este SDR es más sofisticado que los anteriores, debido a que trabaja con receptores especiales que toman la señal directamente desde su fuente en la frecuencia de trabajo, gracias a equipos especiales que logran procesar toda la cadena en un mismo.

Tipo V: Este tipo de SDR es muy diferente a los demás debido a que realiza el trabajo en la Nube, son radios software que trabajan online y están implementados en un servidor capaz de proveer p capacidad de procesamiento digital de señales según lo configurado por el usuario y de la referencia

del SDR. Se debe tener en cuenta su gran practicidad debido a que no se requiere de la compra de un equipo para el procesamiento de la señal [24].

5.2.3. Sistemas De Radio Cognitivos

El concepto fue dado por Joseph Mitola en su tesis doctoral en el año 1998, donde nombraba un dispositivo de CR donde fue sugerida como plataformas para sistemas de comunicaciones personales multimodo multibanda [1] ; sin embargo algunas organizaciones como la ITU definen este sistema de Radio Cognitiva como un sistema radioeléctrico que trabaja con tecnología que permite extraer información de su entorno espectral y geográfico, y con ello adaptar de manera automatizada los parámetros y protocolos con los que opera este sistema [25].

Estos sistemas de Radio Cognitiva, está compuesto por equipos de radiocomunicaciones capaces de identificar la ocupación espectral, algo similar a un analizador de espectro, pero de una forma más automática, ya que puede determinar qué banda está disponible y que banda podría tener una ocupación. Este sistema se puede programar para optimizar los parámetros de funcionamiento para aprovechar al máximo el espectro disponible, al tiempo que pueden aprender de los resultados obtenidos y almacenarlos en una Base de Datos.

5.2.4. Características De La Radio Cognitiva

La radio cognitiva se diferencia de la radio convencional en tres aspectos fundamentales: capacidad cognitiva, capacidad de aprendizaje y adaptación, capacidad de auto reconfiguración.

La capacidad cognitiva hace referencia a la facilidad para la obtención de información del entorno y del estado interno de su propio sistema a través de varios sensores. La capacidad de aprendizaje y adaptación permite utilizar esta información para ajustar de manera autónoma y dinámica, los parámetros de operación a través de la capacidad de auto reconfiguración, con el objetivo de optimizar el desempeño del sistema. [26].

En la Figura 1 se muestra la arquitectura de la radio cognitiva: Funciones de interfaz del usuario, aplicaciones del sistema, funciones sensoriales del entorno, funciones de interfaz de usuario de radio reconfigurable, funciones cognitivas y funciones de la Radio Definida por software. Entre cada uno de los componentes funcionales se establecen varias interfaces a través de las cuales se produce el intercambio de datos y señales de control que definen el funcionamiento del sistema [27].



Figura 1. Arquitectura de la Radio Cognitiva [27].

El ciclo cognitivo mostrado en la Figura 2 representa una máquina de estado de las diferentes etapas del proceso cognitivo para el acceso dinámico al espectro. Esta idea fue posteriormente adaptada al concepto de radio cognitiva como tecnología de acceso dinámico al espectro. Como se muestra en esta Figura incluye el análisis y detección del espectro, incluyendo la selección de las bandas de frecuencias optimizadas, adecuado para el uso que el usuario.

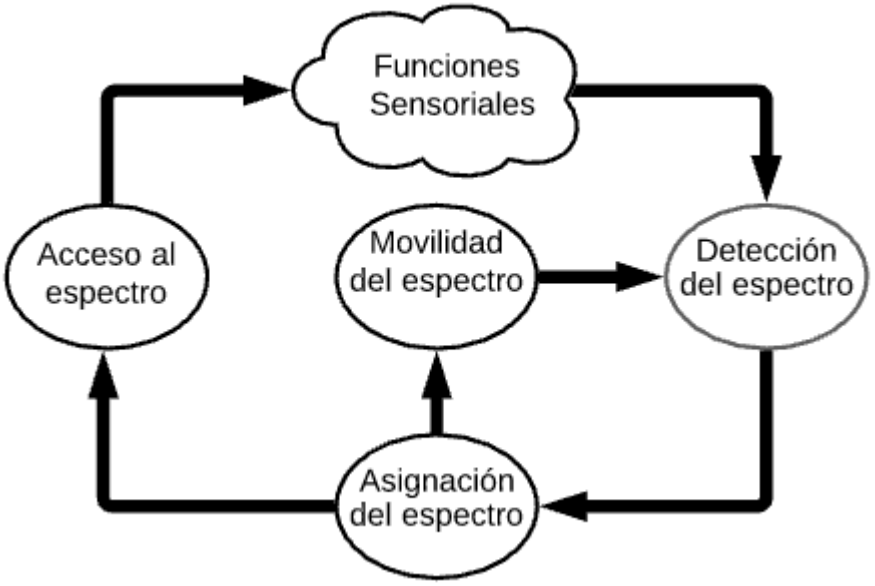


Figura 2. Ciclo cognitivo para el acceso dinámico al espectro [27].

5.2.5. Diferentes Ataques A La Red Cognitiva

Entre los principales tipos de ataque para los cuales es necesario investigar posibles contramedidas cabe destacar los siguientes en la tabla 1:

Ataque	Capa afectada	Descripción
Ataque intencional	Física	El usuario secundario ataca interfiriendo de forma malintencionada y continua, en una banda con licencia a los usuarios primarios y secundarios. Dicho ataque se puede amplificar por el uso de alta potencia de transmisión, transmitida en varias bandas espectrales.
Ataque del receptor primario	Física	El ataque se produce cuando el usuario primario que está más cerca del receptor primario participa en un protocolo de colaboración y envió de transmisiones a usuarios secundarios, para que esta sea detectada por el usuario malintencionado
Ataque de amplificación a la sensibilidad	Física	Una entidad malintencionada puede amplificar la sensibilidad y, por tanto, el número de oportunidades perdidas para reproducir la transmisión primaria

Ataque secundario traslapado del usuario	Física	En las redes cognitivas centralizadas y distribuidas, las redes múltiples secundarias pueden coexistir en la misma región geográfica. En tales casos, las transmisiones de entidades malintencionadas en una red pueden causar daño a los usuarios primarios y secundarios de la otra red sin tener bajo control a la estación base.
Ataque para uso general	Enlace	Un usuario secundario malintencionado es capaz de ajustar los parámetros para un uso general, aumentando el ancho de banda. Si los usuarios secundarios y/o las estaciones base no son capaces de detectar este tipo de comportamiento anormal, puede provocar la privación del medio de transmisión para otros usuarios secundarios
Ataque de detección asíncrono	Enlace	En lugar de sincronizar la actividad de detección con otros usuarios secundarios de la red, un usuario malintencionado puede transmitir asíncrono, cuando otros usuarios secundarios están realizando operaciones de detección
Ataque falso	Enlace	Para los protocolos que confían en los usuarios secundarios que intercambian información. La falsa información de un grupo de usuarios malintencionados puede hacer que los usuarios secundarios tomen acciones inapropiadas, para así modificar los objetivos del protocolo

Ataque NEPA	Red	NEPA tiene la capacidad de hacer que al menos un nodo se comporte de manera malintencionada en la red. El propósito de este nodo consiste en aumentar la interferencia en los canales primarios con mayor tráfico de información.
Ataque CEPA	Red	El ataque CEPA es un caso especial del ataque NEPA, con una ligera modificación en la estrategia de ataque. Un nodo comprometido lanza el ataque CEPA cambiando todas las interfaces del canal prioritario que está siendo utilizado. Sin embargo, la gravedad de este ataque hace que su detección sea fácil
Ataque LORA	Red	El ataque LORA maneja información engañosa sobre las asignaciones del espectro y la transmite a todos los vecinos para impulsar la red en un estado cuasi-estable. Puesto que la asignación del canal del nodo comprometido no se cambia realmente, este ataque es perceptiblemente diferente al NEPA y CEPA, de igual modo es un tipo de ataque mucho más fuerte y barato
Ataques “cross-layer”	física/ enlace / Transporte	El ataque Cross- Layer se encarga de afectar al protocolo de transporte saturando la red
Ataques OFA	física/ enlace / Transporte	Los ataques OFA afectan a los algoritmos de aprendizaje de los dispositivos de radio cognitiva.

Ataques PUE	física/ enlace / Transporte	Los ataques PUE se imita la transmisión producida por un elemento primario para evitar la transmisión en la misma banda por parte de un elemento secundario.

Tabla 1. Ataques a la red Cognitiva [28].

En la Tabla 1, se puede evidenciar algunos ataques a la red cognitiva en diferentes capas del modelo OSI y los posibles daños que pueden generar. Con base a esta información se decide trabajar con el ataque PUE ya que es el ataque específico más estudiado debido a que es el más frecuente y que puede llegar a causar mayores daños.

5.2.6. PUE (Emulación De Usuario Primario)

En los últimos años, han aparecido algunos enfoques relacionados con la seguridad en las redes de radio cognitivas. Describen ataques específicos contra estas redes, pero se han propuesto pocas contramedidas, la mayoría de los estudios sobre seguridad se centran en la detección de PUE. Los ataques pueden resultar en la inyección de datos falsos en el momento de intercambio de información de detección, de la emulación de un usuario primario, utilizando el espectro de forma egoísta o maliciosa, afectando la capa física [29].

Este ataque es realizado por los usuarios secundarios malintencionados que manipulan sus radios para tener comportamientos y características similares a la transmisión de los usuarios primarios. Esto es debido a que los radios cognitivos permiten la reconfiguración de las interfaces de radio. Un atacante equipado con tecnología RC puede modificar su interfaz y emular las características de la señal de un usuario primario. Esta modificación permite a los usuarios secundarios legítimos identificar incorrectamente un usuario secundario como un usuario primario, lo que resulta en un ataque PUE [30].

Las investigaciones muestran que un ataque PUE puede afectar seriamente el rendimiento del espectro y reducir significativamente la disponibilidad de los canales legítimos a los usuarios secundarios, pasando una negación de servicio; puede ser generado por dos tipos de usuarios secundarios malintencionados: usuario malicioso, que tiene como objetivo poner en peligro el funcionamiento de la red y usuario egoísta, que se beneficia de los privilegios que este tiene para establecer una comunicación exclusiva con otro usuario. Estas dos acciones maliciosas reducen significativamente los recursos de acceso a los medios de comunicación disponibles para los usuarios secundarios legítimos. Además, se comprometen las características cognitivas de estos usuarios [31] [32].

En la Figura 3 se ilustra el espectro licenciado por los usuarios primarios que es utilizado por un usuario secundario legítimo. Los SE llevan a cabo la medición del espectro y acceso a las frecuencias ociosas del espectro. Cuando un usuario primario se activa en su banda con licencia, el SU cambia a otro espacio ocioso dentro del espectro de frecuencias. Los ataques PUE (Representados como Cráneos) son realizados en diferentes bandas de frecuencia, ocupando el espectro espacios en blanco y tornando el espectro ocupado. El SU legítimo detecta estas actividades de los atacantes como actividades legítimas de PU perdiendo oportunidades de acceso al espectro [18].

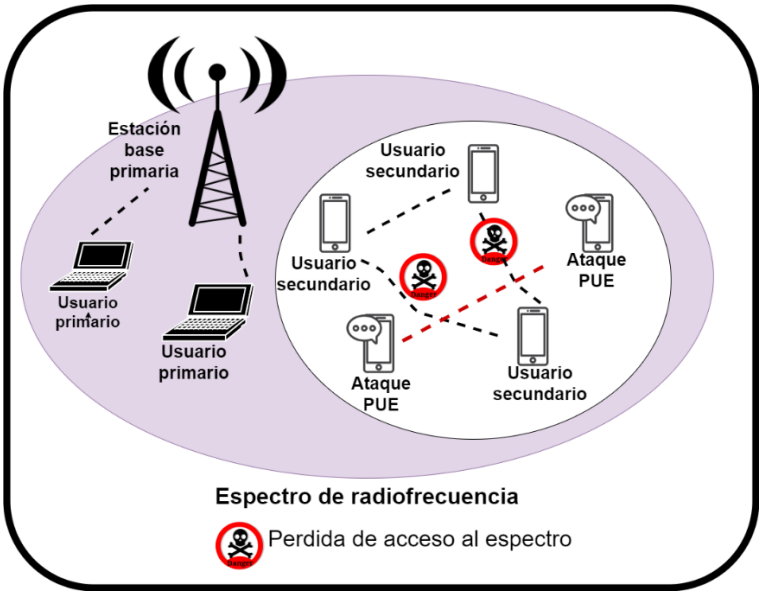


Figura 3. Presencia del ataque PUE en la red de radio cognitivo [33].

5.2.7. Técnicas Actuales Para La Detección Y Defensa Del Ataque PUE

Se han desarrollado diferentes métodos de detección y defensa contra el ataque PUE, ya que es vital para el pleno funcionamiento de las redes CR; por lo tanto, las técnicas de detección tienen que verificar la autenticidad de la señal del PU, a continuación, se mencionan algunas técnicas de detección y defensa según sus métodos utilizados para la mitigación del ataque PUE.

- Método basado en la ubicación: existen tres tipos de técnicas de defensa que se basan en la ubicación del PU, basándose en la transformada de wavelet, en la cual usa una frecuencia para extraer la huella digital del transmisor en el dominio de frecuencia de las señales de transmisión, para distinguir entre la señal PU y el atacante PUE.[34] También se pueden usar algunas técnicas como Diferencia de tiempo de llegada (TDoA, por sus siglas en inglés) para calcular la diferencia en el tiempo de llegada de una señal en dos o más pares de nodos, generalmente por medio de técnicas de correlación, estimar la posición de un emisor y detectar ataques de PUE [35].

Otra técnica muy usual es el método de Mínimo cuadrado ponderado (WLS, por sus siglas en inglés), en la cual se usa para minimizar el error cuadrático, pero se requieren nodos de anclaje adicionales con posición conocida y se requiere una sincronización estrecha entre estos nodos. Para ellos es necesario tener un esquema jerárquico de dos niveles en la red CR y se realizan pruebas de hipótesis M-ary para identificar al atacante PUE. Aquí los nodos de retransmisión adicionales ayudan a detectar el ataque PUE [36].

- Método de aproximación de Fenton: El método de aproximación de Fenton es un modelo analítico para ataques PUE, se utiliza para determinar la media y la varianza de la potencia de recepción en el SU debido tanto al PU como a usuarios maliciosos. El resultado es aplicado sobre una desigualdad de Markov para obtener un límite inferior en la probabilidad de éxito de ataque PUE. [37] Luego, la prueba de razón de probabilidad secuencial de Wald se realiza sobre la función de densidad de probabilidad de recibir señales para detectar un ataque PUE. Estos mecanismos requieren la recolección de una serie de muestras de detección para un análisis, y se obtiene un estimado de detección y sobrecarga, y aquí se evalúa la posición del PU y si todos los usuarios son fijos y emiten energía constante. Los resultados muestran que la probabilidad de ataque PUE aumenta a medida que disminuye la distancia entre PU y SU [38].

- Método de detección de varianza: En este método, el atacante usa un estimador de máxima verosimilitud para inferir la potencia de transmisión del PU y utiliza un enfoque de campo medio para generar la señal PUE. el SU utiliza un método de detección de varianza para mitigar PUE. Para obtener los resultados, debe conocerse la posición de la PU y la distancia entre el PU y el SU y entre el PU y el atacante. Los resultados de la simulación muestran que el método de detección de varianza avanzada funciona mejor que el método de detección ingenuo en presencia de una estrategia de ataque avanzada del atacante PUE [34].

- Método de detección del espectro cooperativo: En un entorno cooperativo, cuando se lanza PUE, los SU brindan información de detección al centro de fusión, que luego se combina de manera óptima con un peso apropiado para maximizar la probabilidad de detección. Los pesos óptimos están relacionados con la información del estado del canal entre SU y PU y entre SU y el atacante. Se supone que la posición y la potencia de transmisión de PU y atacante son constantes, porque no se puede obtener la estimación de canal perfecta de los usuarios de movimiento. Este método propuesto muestra un mejor rendimiento en comparación con el método MRC convencional [39].

Estas son algunos métodos de detección, adicionalmente se destacan los métodos: Verificación de transmisor, ANN, ALDO, Defensa Híbrida, IRIS, Método de encriptación y desplazamiento, Acceso Cross - Layer, DECLOAK, Dogfight, entre otros modelos matemáticos [34].

5.2.8. Minería de datos

Actualmente nos vemos enfrentados en ocasiones a un volumen muy grandes de datos sobre ellos a simple vista es difícil encontrar información que brinde un valor en el proceso que se esté realizando, es así que surge la importancia de encontrar mecanismos que ayuden para este proceso, la minería de datos de conocer inicialmente como el proceso de descubrimiento de nuevas y significativas relaciones, patrones y tendencias al examinar grandes cantidades de datos[44], para este proceso en el que se capturan datos del espectro el volumen de datos en muy amplio y realizar un detalle de manera rápida se vuelve un proceso tedioso, teniendo presente que se busca un descubrimiento automático del conocimiento, es así que a partir de este entregara nuestra SVM y cumplir los objetivos de entrenamiento inicialmente y posterior sistema de detección en tiempo real.

Sin embargo, como se realiza este proceso de extracción o descubrimiento de conocimiento, por lo general sin importar el tipo de data se busca aplicar los mismos pasos, donde se busca un ciclo limpio que ayude en el proceso donde encontramos la minería de datos, los mismo los podemos resumir en lo siguiente:

1. Comprender el dominio de aplicación o sistema, en pocas palabras se busca entender el contexto de donde se obtendrá el volumen de datos.
2. Extraer la base de datos objetivo, es decir, obtenemos los datos del espectro electromagnético.
3. Preparar los datos
4. Minería de datos, el cual consiste por una o más de las siguientes funciones, clasificación, regresión, clustering (se refiere a la agrupación de registros, observaciones, o casos en clases de objetos similares), resumen, recuperación de imágenes, extracción de reglas.
5. Interpretación.
6. Utilizar el conocimiento descubierto, acá la con el uso de la SVM permitirá identificar un posible ataque [45].

5.3. Marco Legal

Para dar un fundamento a este proyecto es importante conocer el conjunto de leyes, normas y reglamentos que están directamente relacionados con este proyecto y apoyan en el proceso de investigación realizado como primera medida.

5.3.1. Constitución Política Colombiana

Al emplear un bien público como es el espectro electromagnético es importante conocer lo que indica la Constitución Política de Colombia donde nos brinda lo que se debe tener presente sobre éste en el artículo 75:

> *"El espectro electromagnético es un bien público inajenable e imprescriptible sujeto a la gestión y control del Estado. Se garantiza la igualdad de oportunidades en el acceso a su uso en los términos que fije la ley. Para garantizar el pluralismo informativo y la competencia, el Estado intervendrá por mandato de la ley para evitar las prácticas monopolísticas en el uso del espectro electromagnético" [40].*

5.3.2. Decreto 930 de 04 de junio de 1992

Por el cual se reglamenta el establecimiento de redes privadas de telecomunicaciones y la utilización del espectro radioeléctrico destinado a estos efectos. Se establece que una red privada es de personas naturales para uso exclusivo, se requiere de una autorización del ministerio cuando se haga uso del espectro radioeléctrico, se haga uso del satélite coordinado para Colombia o se establezca una conexión internacional la cual debe hacerse por un operador de servicios de telecomunicaciones habilitado para ese servicio [41].

5.3.3. Estándar IEEE 802.22

Como se sabe hay un gran número de usuarios secundarios que hacen uso del espectro con el fin de acceder a un servicio como lo puede ser la telefonía móvil celular a manera de ejemplo, allí surge una pregunta ¿cómo se logra un acceso ordenado a estos espacios de frecuencia en el espectro?, es así que se diseñó un protocolo MAC para redes radio cognitivas donde se tiene presente la disponibilidad de un canal de control común para compartir información y el número de transmisores/receptores disponibles por usuario. [27]

En los protocolos MAC para redes radio cognitivas se clasifican tomando en consideración los siguientes aspectos:

> *"Arquitectura de operación: distribuida o centralizada, esquema de acceso en el tiempo: en ranuras de tiempo asignadas, acceso aleatorio o una combinación de ambos esquemas, necesidad de un canal de control común e información requerida del sistema: global o local. En el protocolo IEEE 802.22 la contención entre celdas vecinas se realiza a través del protocolo CBP (Coexistente Beacon Protocol). En este protocolo, las estaciones base de cada celda, al final de cada trama MAC, transmiten un mensaje que permite la comunicación y sincronización dentro de una comunidad de celdas. Cuando una estación base recibe un mensaje de sincronización difiere sus transmisiones para evitar la interferencia entre celdas vecinas" [27].*

6. Metodología

Para alcanzar los objetivos propuestos en el presente proyecto, se trabajó mediante la metodología cuantitativa, gracias a ella se recogieron y analizaron datos cuantitativos, esto permite determinar la fuerza de asociación o correlación entre variables, la generalización y objetivos de los resultados a través de una muestra para hacer inferencia a una población de la cual toda muestra procede [42] , a continuación se describe una diagrama que muestra las 5 fases sobre la cual se desarrolló el proyecto.

6.1. Diseño de un sistema de detección basado en una máquina de soporte vectorial para la detección del PUE malicioso en redes cognitivas.

A continuación, se describe el diseño del sistema de detección basado en una máquina de soporte vectorial para detectar un ataque PUE malicioso en una red cognitiva, distribuida en 5 fases como se muestra en la Figura 4, y posteriormente se expone cada una de ellas.

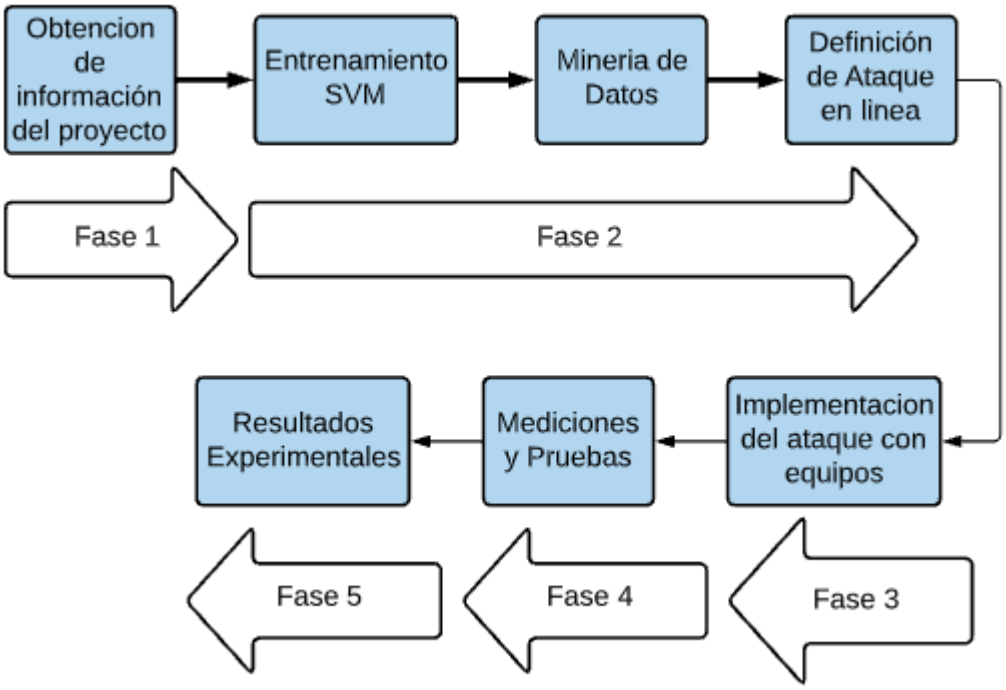


Figura 4. Diagrama de Bloques de las fases implementadas

Fase 1: Esta fue la fase inicial en donde se realizó una revisión bibliográfica de distintos trabajos en la implementación SVM con el fin de detectar ataques de emulación de usuario primario malicioso, con el fin de trazar una ruta de trabajo en el desarrollo del proyecto.

Fase 2: Para este punto se identificaron y se plantearon las tres grandes partes que componen el proyecto y permitan la detección del ataque, allí se debía definir los componentes que involucra en cada una de ellas y las tareas o actividades que debían realizar, para ello se trabajaría en tres bloques:

- **Entrenamiento SVM:** Es necesario enseñarle a la SVM mediante distintas mediciones en qué momentos está activado un ataque y en qué otro momento no, para ello se debieron realizar varias pruebas, las cuales se mostrarán más adelante.

- **Minería de datos**: Entiendo que las mediciones que se realicen del espectro nos entregaron dataset que fueron necesarios entrar a revisar, realizando una limpieza, transformación y depuración de la data capturada con el fin de realizar los respectivos cálculos necesarios para que la SVM pueda realizar la detección de manera automática.

- **Detección del ataque en línea:** Después de plantear el entrenamiento se podrá agrupar todos los bloques de trabajo del proyecto con el fin de lograr definir si existe un ataque en las frecuencias de trabajo.

Fase 3: Definidas las dos anteriores fases se pasa a la implementación o desarrollo del proyecto, allí se empezó con el uso de los dispositivos USRP y del SDR, donde se empezó con el acople de las distintas partes donde permitiera tomar los datos del espectro, el tratamiento de la información y así ser entregada a la SVM quien identifica el ataque, para ello se debió desarrollar bajo lenguaje de programación Python los bloques de acople, tratamiento de información y cálculos necesarios.

Fase 4: Mediciones y pruebas, por medio de las tomas realizadas en el espectro nos permite identificar si el entrenamiento realizado previamente cumple con el objetivo de poder detectar el ataque malicioso.

Fase 5: Validación de los resultados, esta fue una fase experimental en donde se evaluaron las medidas realizadas y ver la fiabilidad de los resultados obtenidos con el fin ver el cumplimiento de los objetivos planteados.

6.2 Diagrama de Red

Con el objetivo de identificar ataques de emulación de usuario primario que buscan quitar la oportunidad a un usuario licenciado poder entrar a esta sección del espectro , se diseñó e implementó un sistema de detección de ataques maliciosos de emulación de usuario primario utilizando minería de datos en redes cognitivas, utilizando la técnica de máquina de soporte vectorial (SVM); este se logró entrenar satisfactoriamente identificando los patrones o características que componen al PUE, realizando el proceso de detección de dicho ataque.

Un sistema de radio cognitiva lo compone una serie de bloques que se encuentran conectados secuencialmente que permite el funcionamiento del mismo, iniciando del motor de razonamiento donde se detectan las frecuencias disponibles, por medio de una interfaz de programación de aplicaciones y un analizador de espectro. Se captura la información del entorno y de una base de conocimiento que incluye las políticas de radiofrecuencia (RF) para tomar decisiones sobre los parámetros de operación. El motor de aprendizaje monitorea estas decisiones y sus resultados, actualizando en función de éstos la base de datos de conocimiento. En la Figura 5 se expone un diagrama de bloques de este sistema y posteriormente se expone todos los elementos que componen este.

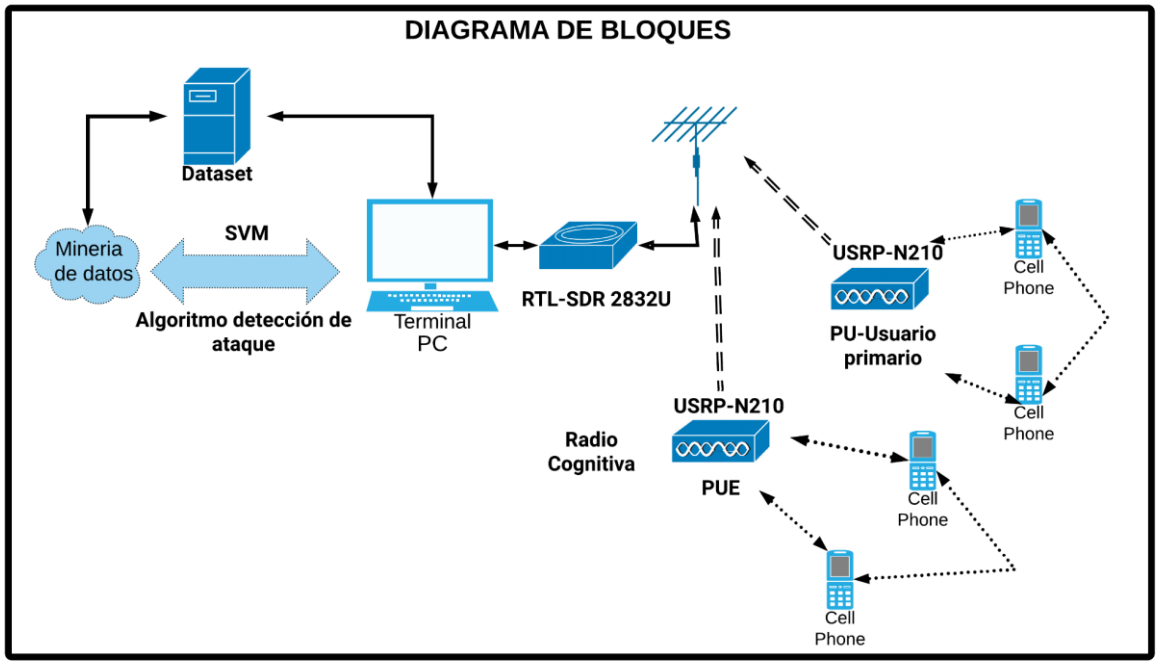


Figura 5. Diagrama de Bloques del sistema implementado. Fuente: Autor

Terminal: Esta terminal realiza distintas actividades dentro de este sistema, ya que por medio de este se llevan a cabo distintos procesos como la recepción, análisis y muestreo de datos obtenidos por el analizador de espectro y con ayuda del software GNU Radio, se realizó la toma de algunos dataset con los datos de la energía sobre este. Aplicando minería de datos sobre las muestras tomadas, pasan a ser analizadas por un algoritmo desarrollado trabajando conjuntamente con la SVM Scikit - Learn, permitiendo identificar las características del PUE y detectando el ataque deseado. Adicionalmente, se encuentra la administración y gestión de la red de radio cognitiva, parte fundamental de este sistema.

RTL-SDR 2832U: Gracias a este equipo se obtienen los distintos datos del espectro electromagnético en las bandas de frecuencia implicadas tanto de la estación de radio cognitiva y los PU, SU y PUE.

Radio Cognitiva (USRP N210): Es el sistema de comunicaciones inalámbricas inteligente que estará consciente del entorno y emplea la metodología para aprender del entorno y adaptar su estado interno a las variaciones estadísticas, teniendo distintos escenarios como el paso entre canales del espectro que estén libres, el enlace entre dispositivos finales y liberación de canales.

PU y SU (Usuario primario y Secundario): Al usuario primario se le asigna un canal o banda de frecuencias de manera exclusiva. Esto implica que ese espectro es utilizado sólo en aquellos instantes donde el Usuario Secundario licenciado accede al mismo, pasando a disposición (Libre) el resto del tiempo.

PUE: Será la estación que realizará el ataque malicioso de emulación de usuario primario, con el fin de ocupar el canal del usuario licenciado y no liberarlo.

Dataset: Con la información obtenida con el analizador de espectro y el software GNU Radio representada en distintas medidas nos permitirá tener un banco de información que se encontrará lista para aplicar minería de datos

Minería de datos: Gracias a esto nuestro base de datos contienen información no plenamente explotada que es valiosa al brindarnos conocimiento, es así que se realizará la limpieza, integración, transformación y reducción de los datos de nuestro dataset para así aplicar una técnica de minería que nos permita obtener el conocimiento necesario para detectar este tipo de ataque.

Sistema de detección: Con el conocimiento previamente adquirido se desarrollará un sistema de detección que nos permita entrenar a nuestra estación de radio cognitiva y en el momento que detecte un ataque, nos brindará una alerta en la terminal de un posible ataque para tomar las decisiones necesarias en el sistema. cómo se mencionó anteriormente como una posible

técnica como lo es support vector machine y entrena nuestro algoritmo para lograr el objetivo de este bloque.

6.3. Diagrama de Funcionamiento del Sistema

En el sistema de detección, inicia cuando cuándo percibe los datos de las señales de energía y SNR, es allí donde el programa se encarga de realizar los cálculos de las entropías, obteniendo una data que será analizada por la SVM que ya está entrenada para determinar si hay o no un ataque malicioso PUE y notificar al usuario el estado de ésta; en caso de detectar el ataque, se finaliza el proceso añadiendo a una lista negra de atacantes, para luego tomar las acciones pertinentes al caso. En la figura 6 se ilustra un diagrama de flujo de este funcionamiento.

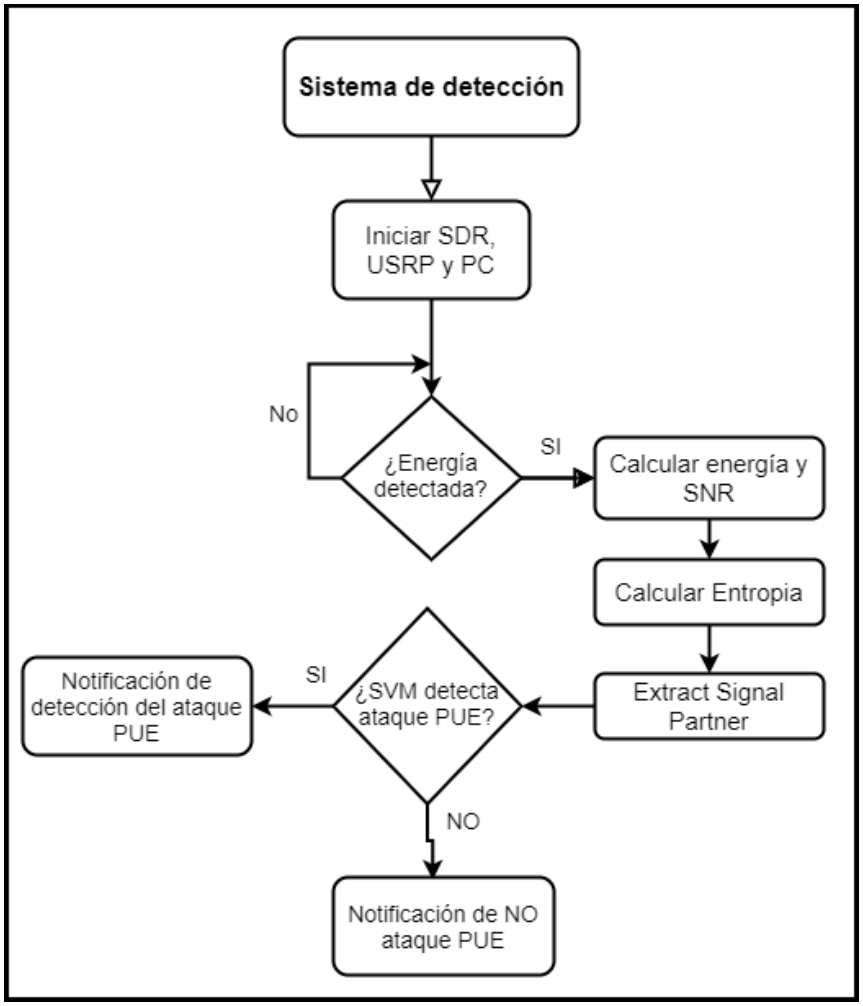


Figura 6. Diagrama de Bloques del funcionamiento del sistema. Fuente: Autor

6.4. Detección de Energía

Para que el proceso de detección de energía haga su trabajo, se realiza un proceso de aprendizaje del SVM, para ello se utilizó la frecuencia de DL en 876.8 MHz y la frecuencia de UL 831.8 MHz de en una llamada telefónica como entrada al sistema. Para algunos valores de SNR, adquirimos la energía en un periodo de tiempo y se calcula la entropía para identificar la señal en cuestión.

Gracias al RTL-SDR se realiza la toma de muestras de la señal, y estos datos se transmiten al PC a través del GNU Radio, donde se puede visualizar la señal y genera un archivo .bin, este entrenamiento se realizó con el ataque encendido Figura 7 y con el ataque apagado Figura 8.

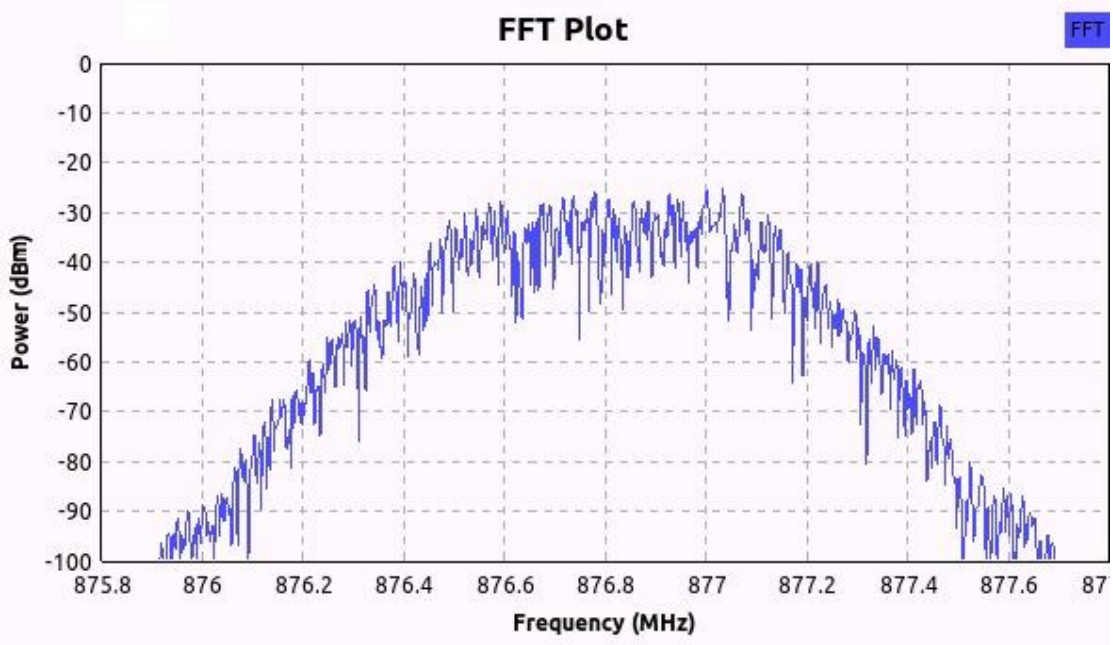


Figura 7. Toma en GNU Radio del ataque encendido. Fuente: Autor

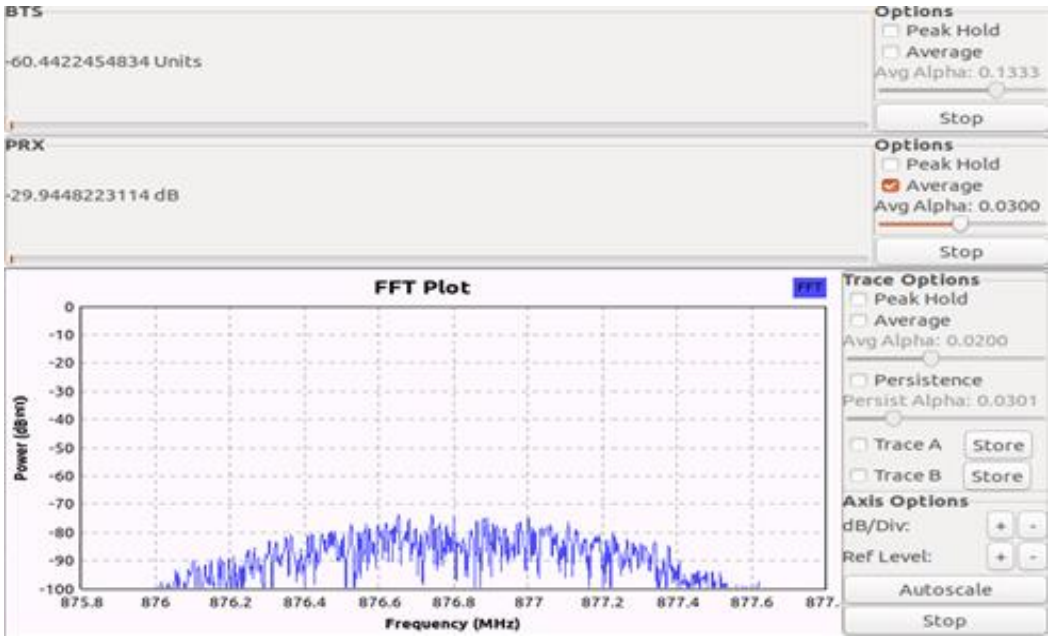


Figura 8. Toma en GNU Radio del ataque apagado. Fuente: Autor

Luego, se empieza el proceso de minería de datos, empezando por la limpieza de datos, ya que el archivo donde guarda los datos el GNU Radio es ilegible y necesita una transformación para poder leer los datos; gracias al comando **xxd -e** podemos leer los datos en formato hexadecimal **IEEE 754** como se muestra en la Figura 9.

```
00144ce0: c275cd27 c27e9d75 c26e074d c28c18d9  '.u.u.~.M.n.....
00144cf0: c268b837 c24ddf6a c2412fa5 c241ec66  7.h.j.M../A.f.A.
00144d00: c25c2cec c27ae46a c264ecd9 c2633f82  .,\.j.z...d..?c.
00144d10: c27e599f c24f6f9d c253e3cf c25ab068  .Y~..oO...S.h.Z.
00144d20: c2600f6c c259f68d c27f5452 c2643cae  l.`...Y.RT...<d.
00144d30: c24ce16c c249c440 c2469902 c24fb050  l.L.@.I...F.P.O.
00144d40: c25b1ecb c255bb0c c2481643 c24752ec  ..[...U.C.H..RG.
00144d50: c25a0475 c25d36b7 c2495cb5 c252d6d3  u.Z..6]..\I...R.
00144d60: c25f609f c258cd8f c25b2111 c254b901  .`_...X..![...T.
00144d70: c257d99c c254e446 c25a1f92 c25f410d  ..W.F.T...Z..A_.
00144d80: c28eb351 c25e8699 c254f15e c26a6bb9  Q.....^.^.T..kj.
00144d90: c2648451 c25c2db4 c2792218 c25d7367  Q.d..-\.."y.gs].
00144da0: c24fe796 c259763c c2724454 c266d103  ..O.<vY.TDr...f.
00144db0: c278419c c268c367 c2662827 c251b766  .Ax.g.h.'(f.f.Q.
00144dc0: c25a6f2b c26957e5 c25fe5ad c2710d79  +oZ..Wi..._.y.q.
00144dd0: c27ce92c c25bf8f3 c276955d c286c63a  ,.|...[.].v.:...
00144de0: c25dc738 c24cf8af c26bb4ba c27d3849  8.]...L...k.I8}.
00144df0: c2782ea5 c24a17c6 c2467e73 c265e06d  ..x...J.s~F.m.e.
00144e00: c276b20a c25c5adf c28a547e c25c548f  ..v..Z\.~T...T\.
00144e10: c25bd7c3 c24f240c c25746d3 c2641fe6  ..[..$O..FW...d.
00144e20: c2713f14 c281843b c25618b7 c24ccc09  .?q.;.....V...L.
00144e30: c26438a3 c272d044 c2842494 c26a906c  .8d.D.r..$..l.j.
00144e40: c2602618 c276098b c2531ae9 c25e1395  .&`...v...S...^.
00144e50: c267e9fa c26cf03a c276fded c25356b6  ..g.:.l...v..VS.
```

Figura 9. Transformación de datos en formato Hexadecimal IEEE 754. *Fuente: Autor*

Se procede a transformar a formato binario IEEE 754 y posteriormente a datos en punto o coma flotante, luego eliminamos datos erróneos de las columnas de los extremos y se acomodan los datos de 4 columnas a solo 1, con el objetivo de tener más ordenada la información; luego de

la transformación de datos a Float o coma flotante, se guardan en un texto plano para poder ser utilizado en el proceso final de entrenamiento, como se muestra en la Figura 10.

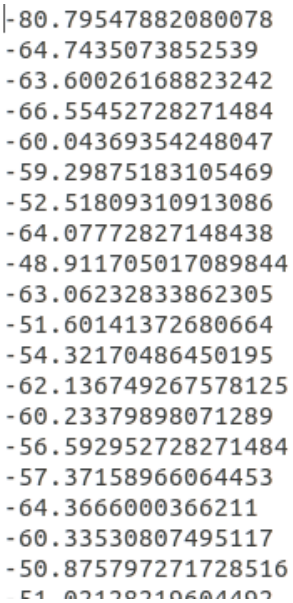


Figura 10. Transformación de datos en formato a coma flotante (Float). Fuente: Autor

Estos datos corresponden al nivel de energía de la señal tomada, se toman 100 valores y se aplica la Entropía sobre estos datos.

6.5. Cálculo de la entropía

Con la detección de la energía realizada es necesario cuantificar la diversidad, incertidumbre o aleatoriedad de los datos capturados, ello lo logramos gracias al uso del cálculo de entropía, para este caso se hizo uso de la entropía Renyi. Este tipo de entropía es usada en ámbitos como economía, finanzas, aprendizaje automático y estadística, sin embargo, para nuestro caso nos ayuda para la detección de la señal de un PUE; sí entramos a comparar con la entropía de Shannon por ejemplo, la entropía Renyi permite obtener una mejor diferencia entre dos distribuciones [46].

Teniendo presente lo anterior esto nos ayudó a encontrar un hiperplano óptimo donde se ubicarán los datos en un espacio separado uno del otro, estos datos se conocen como vectores de soporte, pero ¿qué hace que exista un espacio entre estos grupos de datos? Esto es gracias al cálculo de entropía que se realiza con ataque y sin ataque, como se muestra en la Figura 11.

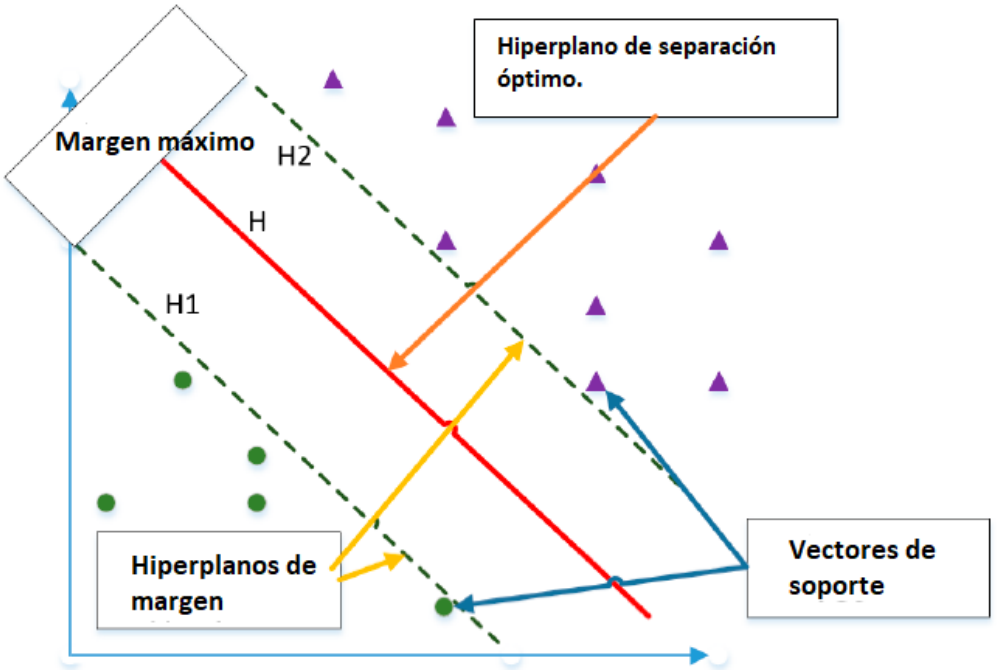


Figura 11. Funcionamiento de la máquina de soporte vectorial (SVM) con dos dimensiones [14].

Para el cálculo de la entropía Renyi se usó la siguiente fórmula:

$$H_\alpha(X) = \frac{1}{1-\alpha} log \sum_{i=1}^{n} \quad p_i^\alpha$$

La entropía de Renyi de orden α , donde $\alpha \geq 0$ y $\alpha \neq 1$. Aquí, X es una variable aleatoria discreta con resultados posibles $1,2\ldots,n$ y probabilidades correspondientes $p_i = Pr(X = i)\ para\ i = 1,\ldots,n$ y el logaritmo es de base 2.

Teniendo presente lo anterior donde la SVM es la encargada de realizar esta predicción, está muy relacionada a una técnica de minería de datos llamada el agrupamiento, allí una serie de vectores poseen ciertos criterios o características que trabajan con los datos de entrenamiento que la SVM posee, con ello al entrar los vectores de las mediciones de tiempo real nos permitió agrupar sobre los que tengan características comunes. Con ello la SVM puede determinar un ataque mediante un algoritmo supervisado, donde se predice si la medida realizada es un ataque o no, a partir de otros datos que son de conocimiento previo gracias al hiperplano.

6.6. Entrenamiento y Detección del ataque PUE a través de SVM

Como se ha mencionado anteriormente, Scikit - Learn es un software de aprendizaje, que opera con el lenguaje Linux, en este caso se utilizó un equipo con sistema operativo Ubuntu, a que está basado en este lenguaje.

Gracias al comando ***source scikit_is_cool/bin/activate*** en la ubicación del programa a ejecutar permite activar el SVM; para lograr entender el funcionamiento de esta aplicación, se realizan varios programas para entender cómo a través de inteligencia artificial separa los valores que uno desee, como preámbulo se toman 2 valores y el SVM se encarga de pintarlos en el plano, y traza una línea en la cual determinó el límite separación de estos dos valores, tal como se muestra en la Figura 12.

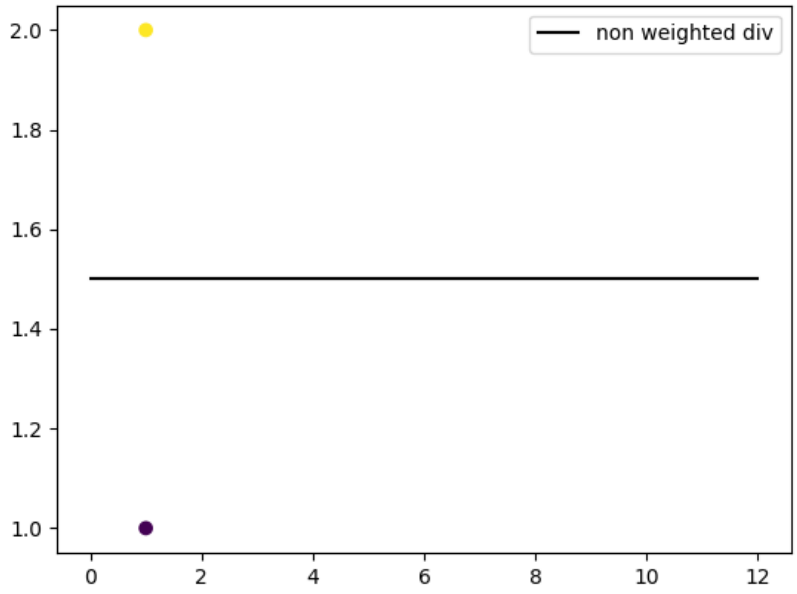


Figura 12. SVM evaluando 2 valores como ejemplo

El paso a seguir, será tomar más puntos y evaluar que tan efectivo puede ser el SVM, para ello, en las Figuras 13 y 14 se muestra cómo se toman en cuenta más puntos y los hiperplanos que puede tomar el SVM para realizar la separación de los datos.

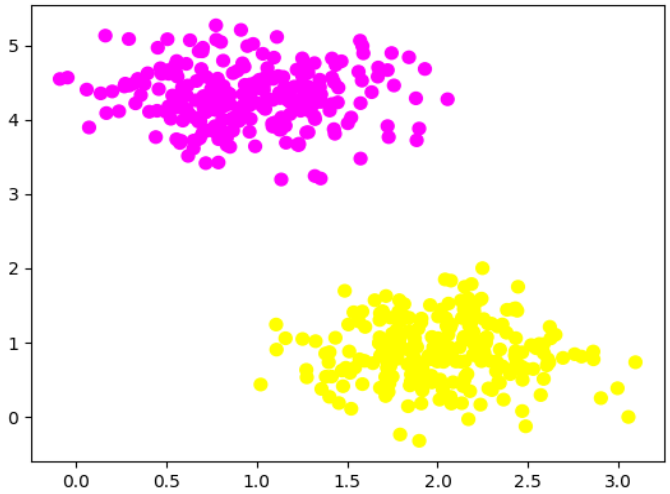


Figura 13. Ingreso varios valores a la SVM

Existe un número infinito de posibles hiperplanos (líneas) que realicen la clasificación, en la Figura 14 se muestran 3 hiperplanos posibles, pero, ¿cuál es la mejor y cómo la definimos?

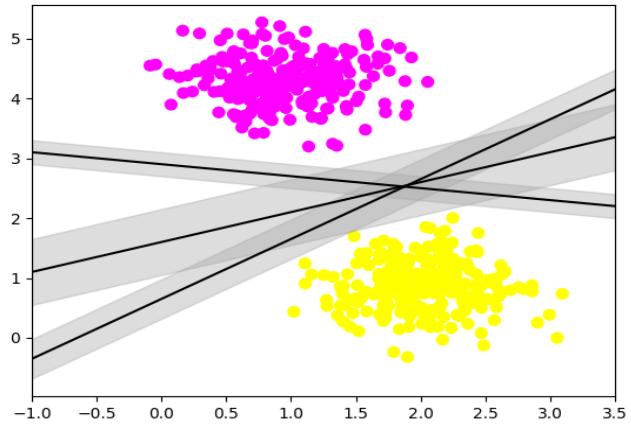


Figura 14. Muestra de 3 hiperplanos de ejemplo

La mejor solución es aquella que permita un margen máximo entre los elementos de las dos categorías y el programa se encarga de optimizar los valores para poder tomar la sección que más se adecue, tal como se muestra en la Figura 15, donde los valores son más distribuidos sobre el eje X, en esta figura se muestra un ejemplo perfecto de un entrenamiento de SVM con datos reales, para ello se configura manualmente los valores de dicho entrenamiento.

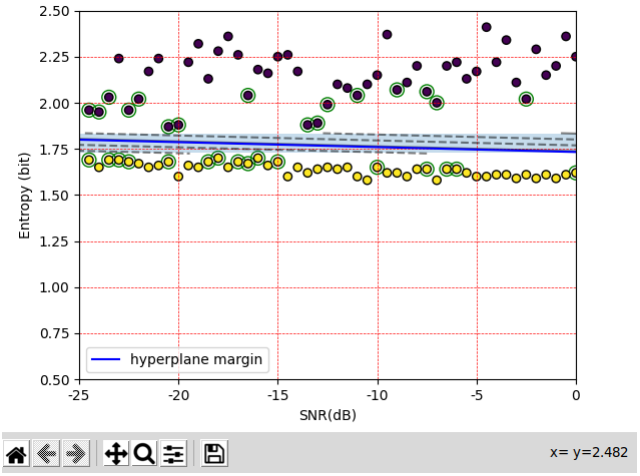


Figura 15. Ejemplo de SVM con datos reales

Entendiendo el procedimiento de trabajo del SVM y del cálculo de entropía, se procede a tomar los valores reales para este proyecto, para ello se toman 10 datos con ataque y 10 datos sin ataque por posición para un total de 1000 datos de entropía, de los cuales se promediaron y se obtuvo 50 datos con ataque y 50 datos sin ataque en un espacio de 3 metros por 1.5 metros, cada posición de un espacio de 30 cm para poder poner la antena de RTL-SDR, y se tomaron los datos en el orden de la Figura 16 con el fin de ver el comportamiento de este en un rango de distancia.

		USRP		
1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25
26	27	28	29	30
31	32	33	34	35
36	37	38	39	40
41	42	43	44	45
46	47	48	49	50

Figura 16. Plano de cuadrícula para toma de muestra de entropías. Fuente: Autor



Figura 17. Cuadrícula montada para toma de muestra de entropías. Fuente: Autor

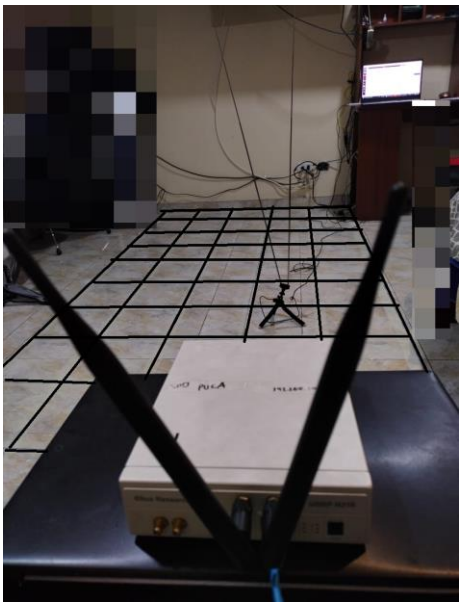


Figura 18. USRP y SDR en toma de muestras de entropías. Fuente: Autor

Luego de las tomas de muestras de las entropías, se guardan los datos de entrenamiento en 2 archivos diferentes, y posteriormente el programa de entrenamiento toma los datos y aplica el SVM para determinar los puntos de inflexión que separa cuando es considerado o no, un ataque. En la Figura 19 se muestra el entrenamiento con la SMV y los datos tomados

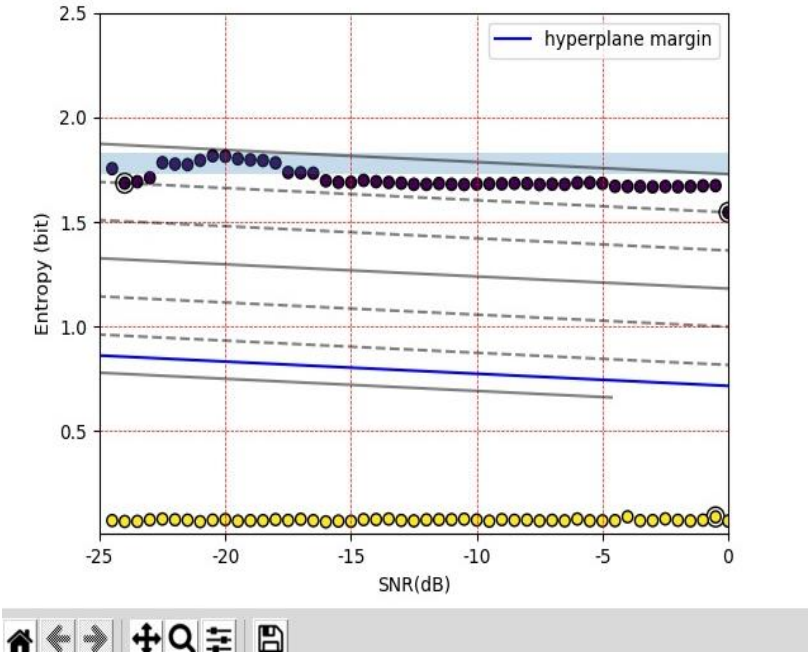


Figura 19. Entrenamiento de la SVM con los datos de entropía recolectados. Fuente: Autor

7. Resultados

A continuación, se mostrarán los resultados en 3 etapas, Propuesta definitiva del sistema, donde se mostrará los resultados obtenidos de la metodología, donde se explicará puntualmente algunos procesos para llegar a definir si hay o no un ataque en la Radio Cognitiva. También se mostrarán los parámetros de la solución donde se expone la configuración general del sistema, bajo algunos parámetros y, por último, validación de la solución donde se presentan los resultados cuantitativos del proyecto.

7.1 Implementación de la máquina de soporte vectorial a través de radio definida por software para detectar el ataque PUE malicioso en redes cognitivas.

En la Figura 20 se comparte un diagrama de bloque que plantea la implementación de la máquina de soporte vectorial a través de la radio definida por software en la detección del ataque de emulación de usuario primario malicioso utilizando una máquina de soporte vectorial en redes cognitivas, allí se encuentra el paso que se realizó desde la adquisición de la señal, hasta los mensajes que se entrega al usuario si hay ataque o no.

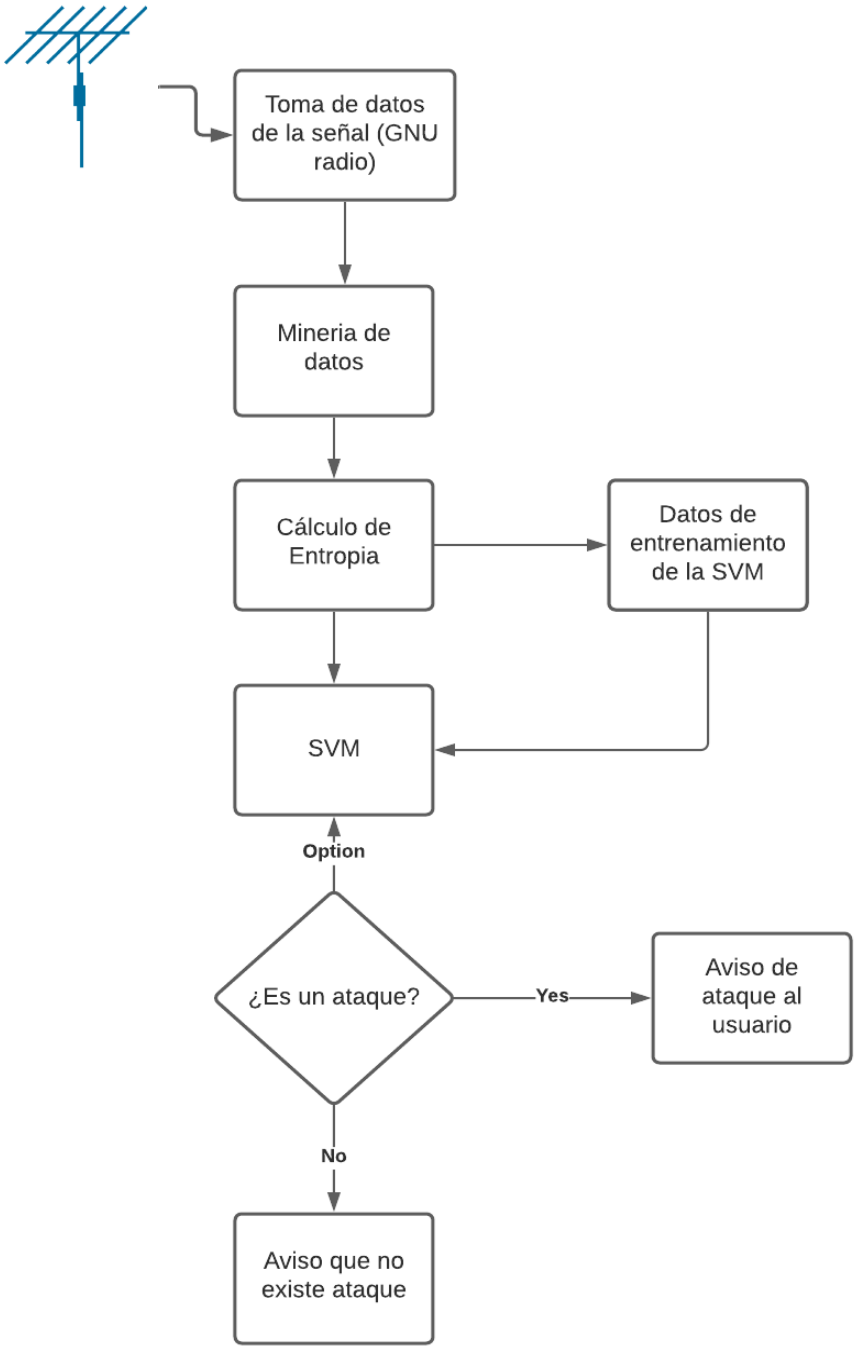


Figura 20. Diagrama definitivo del sistema de detección

7.1.1 Adquisición y minería de datos

El formato de entrega del GNU radio al realizar las mediciones del espectro fueron sobre un formato .BIN el cual se encuentra bajo una codificación UFT-8 como se muestra en la Figura 21, por ende, al ver un archivo nos encontramos con lo siguiente:

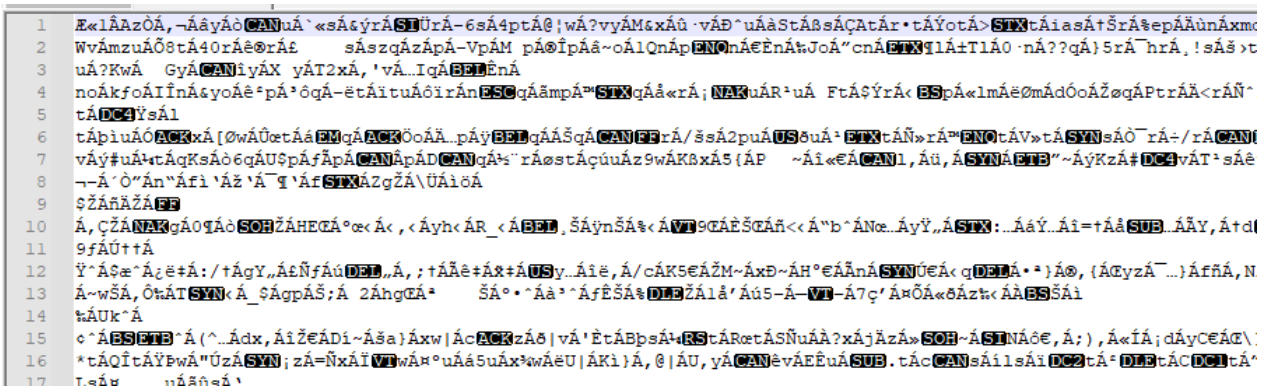


Figura 21. Archivo .BIN en codificación UFT-8

Es allí que se realiza un primer bloque de programa en Python que permite leer la data y llegar a los datos de energía para ser entregados al bloque de cálculo de entropía, como se muestra en la Figura 22:

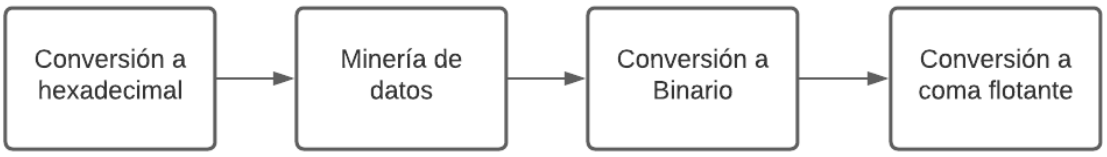


Figura 22. Bloque de programa en Python. *Fuente: Autor*

Es así que se pasa por tres conversiones en cadena que lo representa los cuatro bloques compartidos anteriormente, donde se inicia con el uso de la librería xdd de Python la cual nos devuelve los valores en hexadecimal como se evidencia en la Figura 23:

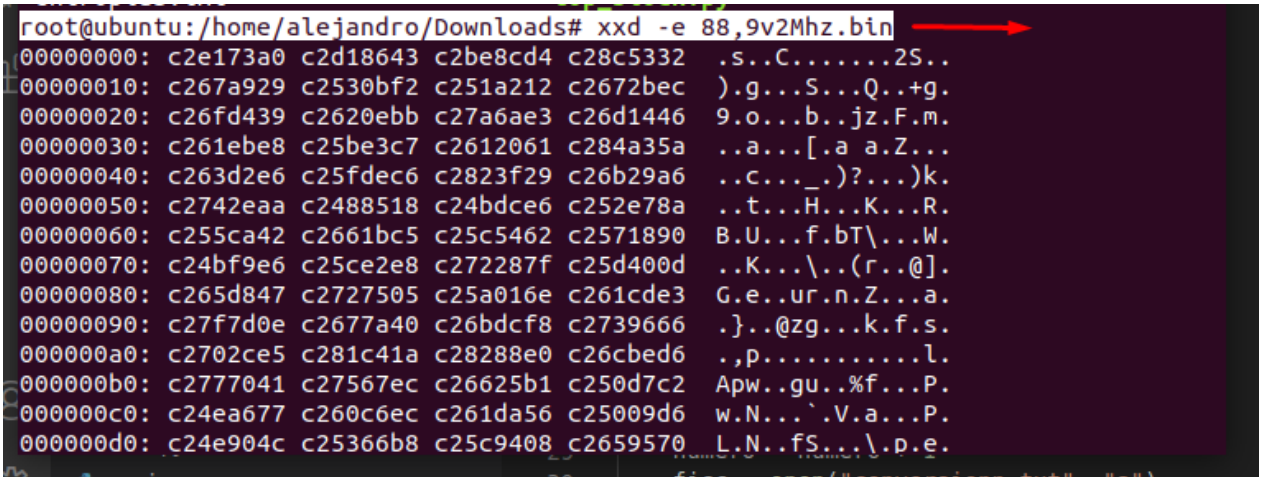


Figura 23. Utilización de la librería xdd. *Fuente: Autor*

Como se puede observar en la Figura 23, se obtuvieron 6 columnas donde se logró identificar que los valores de energía están en las columnas de la 2 a la 4, por ende, se debe hacer uso de los principios de minería de datos para hacer la limpieza y transformación, para ello con línea de código se reemplazó y se eliminaron los caracteres especiales, esto mediante un for ya que la data que vienen del. Bin son bastantes, como se muestra en la Figura 24:

```
for line in f_obj:
    line = line.replace('  ', 'Ω',6)
    line = line.replace(' ', '')
    linea = line.replace('Ω', ' ')


    linea = linea.split()


    valores = linea.pop(0)
    valores = linea.pop(1)
    valores = linea.pop(2)
    valores = linea.pop()
    valores = linea.pop()
    linea = ' '.join(linea)
```

Figura 24. Limpieza y transformación de los datos obtenidos. *Fuente: Autor*

Al eliminar las columnas 1 y 6, nos quedan datos netamente hexadecimales, es así que mediante las siguientes líneas de código se pasa a formato binario:

c=(int(linea,16)) #conversion a binario
c=(format(c,'b'))

Lo anterior se realizó para trabajar bajo el estándar del IEEE 754 de 32 bits para aritmética en coma flotante la cual es la norma o estándar técnico para computación en coma flotante, es decir, a este punto se tiene un binario de 32 bits que se puede resumir de la siguiente:

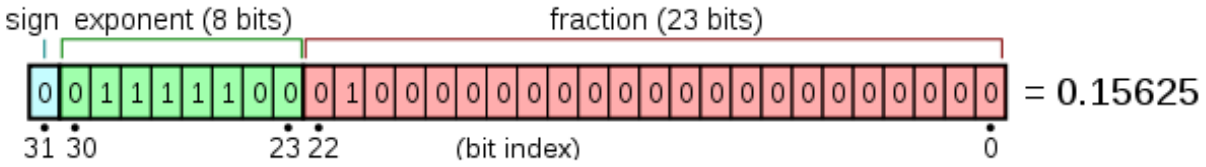


Figura 25. Ejemplo de trama de 32 bits del estándar del IEEE

Es así que se define una función en Python que nos permitiera realizar esta conversión, la función se comparte a continuación:

```
def ieee745(N): # ieee-745 bits (max 32 bit)
                    a = int(N[0])        # sign,     1 bit
                    b = int(N[1:9],2)    # exponent, 8 bits
                    c = int("1"+N[9:], 2)# fraction, len(N)-9 bits
                    return (-1)**a * c /( 1<<( len(N)-9 - (b-127) ))
                   N =c
                   IEEE = ieee745(N)
```

Finalmente obtenemos nuestros valores de energía en coma flotante, como se ven en la Figura 26,

00000000	00	01	02	03	04	05	06	07	08	09	0a
00000000	-44.417747	-26.309694	-17.959232	-15.617810	-15.318590	-15.229339	-15.186803	-15.178725	-15.200726	-15.277393	-15.478088
00000040	-15.242077	-15.266058	-15.286485	-15.277310	-15.250547	-15.211281	-15.158819	-15.024693	-14.935977	-14.964225	-14.966859
00000080	-15.066242	-15.081401	-14.994237	-14.883945	-14.904191	-14.942952	-15.102346	-15.372447	-15.486364	-15.487191	-15.545222
000000c0	-15.167703	-15.189852	-15.092394	-15.047235	-15.021039	-15.039135	-15.050458	-14.968477	-14.894822	-14.876327	-14.923950
00000100	-15.077940	-15.138058	-15.150557	-15.195732	-15.287988	-15.307647	-15.234481	-15.153464	-15.097580	-15.065662	-15.049365
00000140	-15.119379	-15.104891	-15.015971	-15.065321	-15.254680	-15.289298	-15.181207	-15.140522	-15.219819	-15.345972	-15.413093
00000180	-15.721366	-15.429085	-15.046200	-14.862147	-14.881872	-14.958384	-15.058722	-15.146587	-15.179992	-15.196632	-15.221632
000001c0	-15.194293	-15.376852	-15.495275	-15.397949	-15.347317	-15.465545	-15.547481	-15.649318	-15.816868	-15.980035	-15.977331
00000200	-15.455870	-15.579842	-15.620628	-15.570396	-15.512287	-15.384563	-15.080449	-14.924323	-14.964367	-14.969584	-14.925362
00000240	-15.183582	-15.069196	-15.026827	-15.063134	-15.166966	-15.317780	-15.357744	-15.267242	-15.178989	-15.002085	-14.839030
00000280	-15.158402	-15.162427	-15.119732	-15.040195	-14.945130	-14.805767	-14.721588	-14.752211	-14.715647	-14.666873	-14.619589
000002c0	-15.081928	-15.078179	-14.981882	-14.867871	-14.873716	-14.968092	-15.013982	-15.045610	-15.059648	-15.097529	-15.162356
00000300	-14.653089	-14.609032	-14.552946	-14.615017	-14.667298	-14.800156	-14.907630	-14.989451	-15.181066	-15.321128	-15.316193
00000340	-15.389466	-15.486594	-15.457882	-15.421136	-15.388591	-15.234093	-15.058257	-15.070005	-15.131249	-15.200199	-15.217899
00000380	-15.226337	-15.252544	-15.370359	-15.501666	-15.490321	-15.288294	-15.068818	-14.989751	-15.032657	-15.064452	-15.096375
000003c0	-15.170853	-15.251366	-15.295736	-15.192994	-15.167924	-15.136710	-14.942649	-14.817132	-14.876380	-14.925577	-14.921922

Figura 26. Valores transformados a coma flotante

Es así que se almacenan los datos en un archivo .txt, para luego realizar el cálculo de la entropía y posteriormente, éstos sean trabajados por la SVM.

7.1.2 Cálculo entropía y Entrenamiento de la SVM.

Luego de la adquisición y minería de datos de la energía de la señal a evaluar, se hará el cálculo de la entropía, para ello se usaron los siguientes comandos en el programa final como se muestra en la Figura 27.

```
SNR2=pow(10,SNRDB2/10)
sigEner2 = np.linalg.norm(modd2)
sigEner2 =  pow(sigEner2, 2)
noiseEner2 = sigEner2/((SNR2))
noiseVar2 = noiseEner2/len((modd2))
noiseStd2 = math.sqrt(noiseVar2)
noise2 = noiseStd2 * np.asarray(moddd2)#
#noisySig = modd+noise
noisySig2 = modd2
counts, binCenters=np.histogram(noisySig2,bins=15)
binWidth2 = np.diff(binCenters)

nz       = counts>0;
countss = list(filter(lambda x: x2 > 0, counts))
p2                  = countss/np.sum(countss)
#EE= (1/(1-2.5))*math.log(np.sum(pow(p,2.5)))
E2=np.multiply(1/(1-2.5),math.log(np.sum(pow(p2,2.5))))
entrofin2.append(E2)
#print(" EntropiaRe:    ", E)
#print('x ',x)
x2 = x2 + 1
```

Figura 27. Código para hallar la entropía de la señal obtenida

Con los 10000 datos tomados de la energía de la señal, posteriormente pasa por este código obteniendo únicamente 50 valores de entropía y almacenados en una lista como se muestra en la Figura 28, los datos son copiados por el programa a un archivo plano, dejando la huella de las entropías de la señal tomada.

```
1.8684822832365433
1.9745982067841163
1.9937211323672286
1.954982271411183
1.92001091389153
1.8656510182041306
1.8989307922671497
1.876774066960754
1.8692185056664923
1.8695410966112362
1.858741956228477
1.8393635091962706
1.829761991887285
1.8309918946455133
1.8332690592231533
```

Figura 28. Ejemplo de muestra de entropías calculadas cuando no hay ataque.

Previamente a la toma final de energía se realizó el entrenamiento de la SVM, como se muestra en el apartado 6.6. Como resultado se obtiene el siguiente entrenamiento que se muestra en la Figura 29.

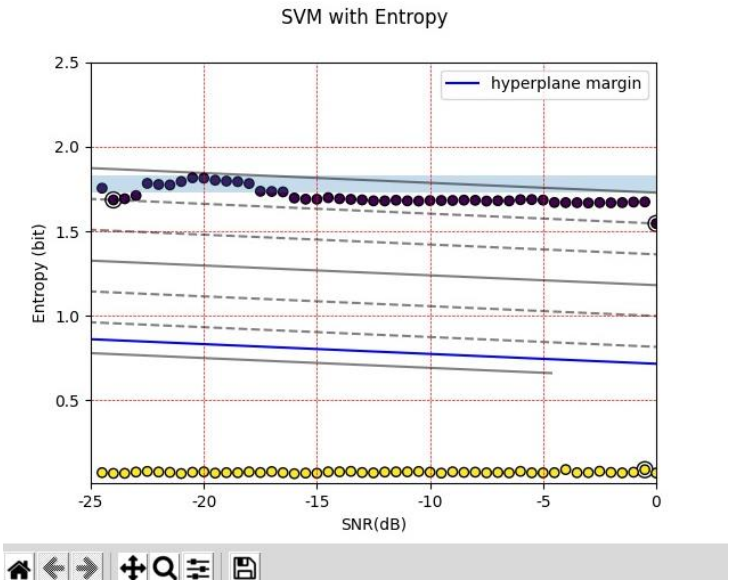


Figura 29. Entrenamiento Final de la SVM

7.1.3 Support vector machine

En la Figura 29 se puede evidenciar que los datos graficados de color Amarillo corresponden a los datos de entropía con ataque, y los datos de color negro cuando no hay ataque, esto es debido a que la entropía cuando el ataque este encendido, la entropía es menor, y se puede considerar que la señal es más estable, caso contrario para la señal cuando el ataque es apagado. La línea de color azul la pinta el SVM gracias a la inteligencia artificial, con base a este límite, podrá determinar automáticamente si es o no un ataque, dependiendo de su entropía.

Luego de realizar el entrenamiento, justo en este momento el programa está listo para hacer uso del SVM; para ello deberá tomar una muestra nueva y repetir parte del proceso de entrenamiento, en este proceso se encuentra la minería de datos para la limpieza y extracción de los datos de energía y cálculo de entropía, luego de tener 50 datos, se realiza una predicción sobre las entropías tomadas, una a una, es aplicado el comando **clf.predict([...])**, donde el SVM determina si es 1 o 0 , comparando con los valores de entrenamiento preestablecidos y se guardaran en un arreglo, y posteriormente se hará el promedio de estos valores en formato INT para que genere un valor Final

de 0 o 1 . A continuación, en la Figura 30, se muestra el vector final cuando hay un ataque, ya que en todas las muestras arrojó un resultado de 1 para la predicción.

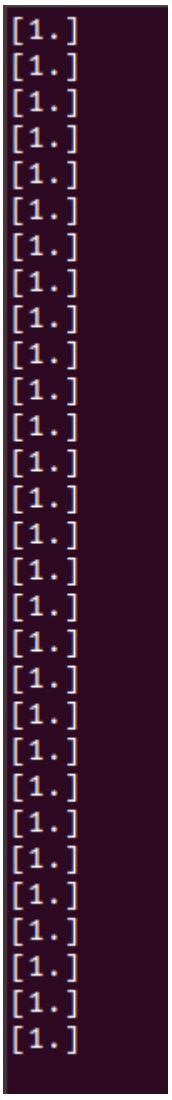


Figura 30. Vector Final cuando hay un ataque

A continuación, en la Figura 31, se muestra el mensaje final por consola del programa realizando el valor promedio de los resultados de las entropías y confirmando que el valor final es igual a 1 e imprime afirmativamente que es un ataque.

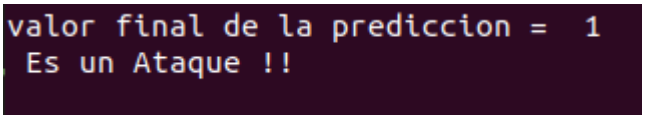


Figura 31. Lectura de información final del usuario, indicando la presencia de un ataque

A continuación, en la Figura 32, se muestra el vector final cuando no hay un ataque, ya que en todas las muestras arrojó un resultado de 0 para la predicción.

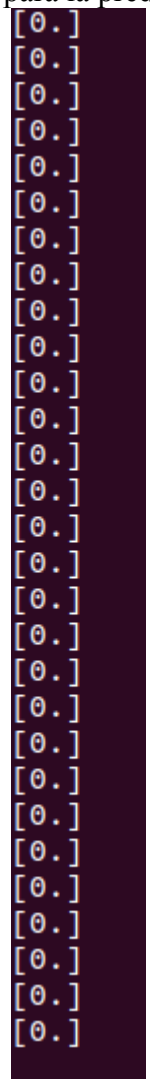


Figura 32. Vector Final cuando no hay un ataque

A continuación, en la Figura 33, se muestra el mensaje final por consola del programa realizando el valor promedio de los resultados de las entropías y confirmando que el valor final es igual a 0 e imprime la negación de un ataque.

```
valor final de la prediccion =  0
 No es un Ataque !!
```

Figura 33. Lectura de información final del usuario, indicando que no hay un ataque

7.1.4 Interfaz gráfica

Con el fin que el programa brindará al usuario una facilidad de uso, se implementó una interfaz gráfica, esta consta de 2 botones como se muestra en la Figura 34, el botón en color verde con el texto "Iniciar Detección de Ataque", posteriormente de tomar la muestra en el GNU Radio, procederá a iniciar el programa de detección de ataque con el botón mencionado y el botón de color rojo "Salir Ventana" simplemente permitirá salir o cerrar la ventana de la interfaz gráfica. Esta interfaz se realizó con la librería tkinter, ya que esta librería facilita la creación de entorno gráfico, facilita mucho la ubicación del texto, imágenes y botones, con bondades de personalización bastantes amplios.

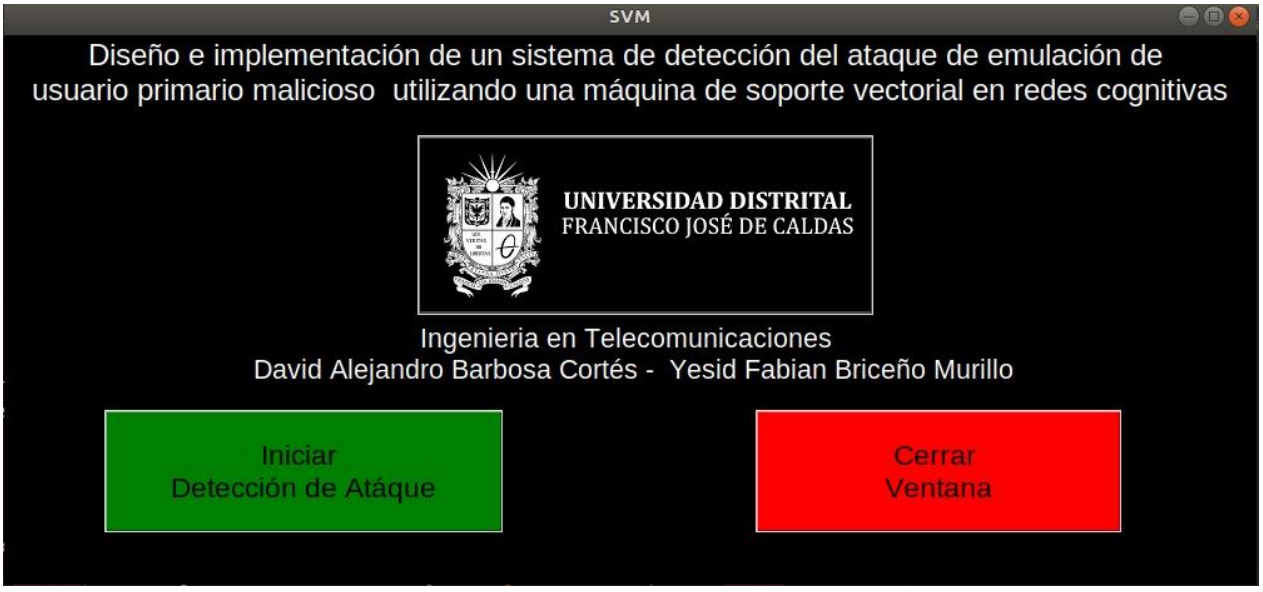


Figura 34. Interfaz inicial del programa

Luego que el usuario inició la detección del ataque, tardará aproximadamente 15 segundos en dar una respuesta al usuario, ya sea que el programa haya determinado que la muestra tomada sea un ataque PUE Malicioso como se muestra en la Figura 35, o por el contrario en la muestra tomada no se haya detectado ataque, como se muestra en la Figura 36



Figura 35. Mensaje final al usuario de detección de un ataque PUE Malicioso



Figura 36. Mensaje final al usuario confirmando que la muestra tomada no es un ataque

7.2 Evaluación de los resultados obtenidos con la probabilidad de detección estimada.

En este punto, ya se pone a prueba el sistema implementado para saber si este es estable o no, y cuál puede ser la probabilidad de error, para ello se procede a tomar 5000 muestras, 100 muestras por cada lugar en la cuadrícula de 50 posiciones, mostrada en la Figura 37.

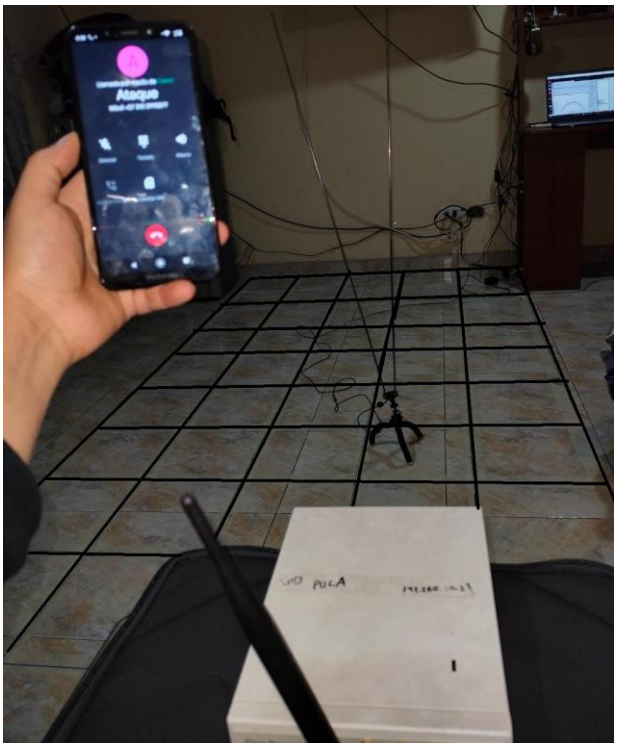


Figura 37. Toma de muestras del ataque

Inicialmente se realizó la detección sobre el downlink, es así que sí la SVM detecta un ataque sobre esta frecuencia se pasa directamente sobre la frecuencia del uplink, con el fin de identificar si hay ocupación del espectro allí también, gracias a esto se puede concluir que si existe un ataque PUE, ya que al no identificar ocupación sobre la banda de Uplink se confirma presencia del ataque, allí confirmamos que la radio cognitiva implementada permite detectar inteligentemente la transmisión de usuarios no autorizados en la banda de frecuencia de 876.8 MHz, para la tabla 2 se comparte los parámetro del experimento, donde se resume lo realizado, frecuencias de trabajo, número de muestras, entre otros.

Parámetro	Descripción
Número de muestras de entrenamiento	1000
Número de muestras para detección de ataque PUE	5000
Número de PU	1
Número de SU	1
Servicio	Telefonía Celular
Frecuencia de Downlink	876.8 MHz
Frecuencia de Uplink	831.8 MHz
Nivel de confianza esperado	95%
Nivel de error	5%

Tabla 2. Parámetros experimentales usados.

Por cada posición se obtuvo un porcentaje de detección, para la Figura 38 se comparte un gráfico que traza el comportamiento que se presentó en detección de ataques.

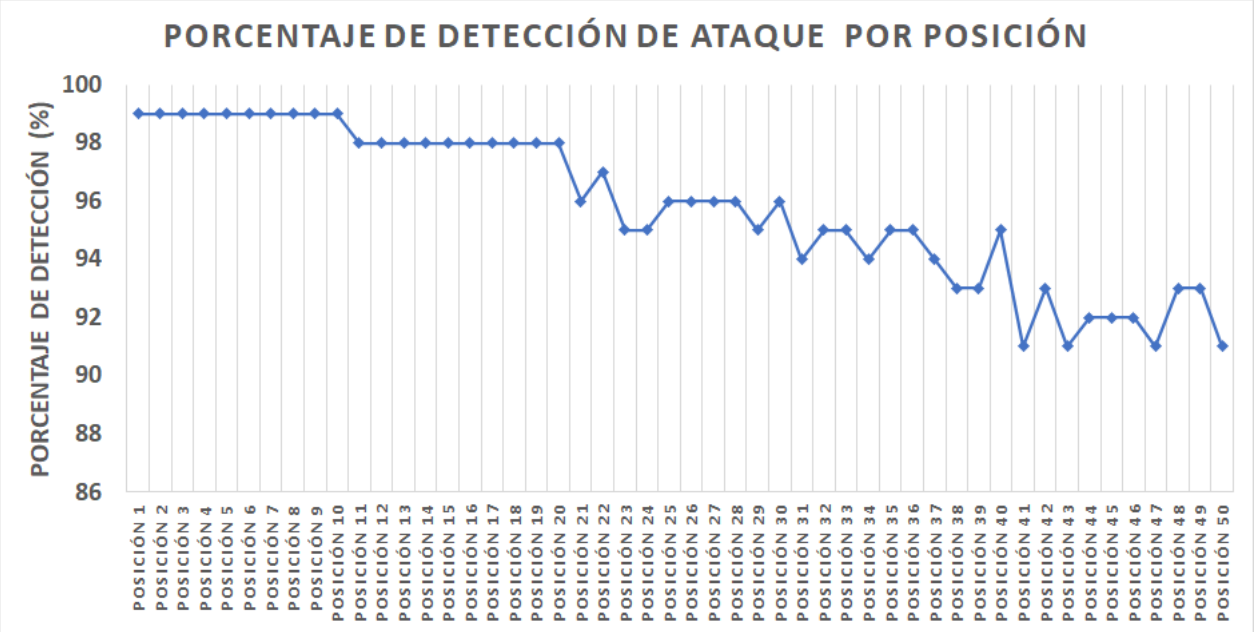


Figura 38. Gráfica del porcentaje de detección de ataque por posición

Teniendo presente que las 10 posiciones más cercanas al USRP presenta un porcentaje de eficiencia del 99%, es así que a lo largo de la gráfica se evidencia un comportamiento decreciente llegando al punto más lejano en la posición 50 donde se presentó un porcentaje de eficiencia del 91%, para la Figura 39 se comparte a detalle el porcentaje de detección por posición.

Posición	Porcentaje de eficiencia del ataque	Posición	Porcentaje de eficiencia del ataque
1	99%	26	96%
2	99%	27	96%
3	99%	28	96%
4	99%	29	95%
5	99%	30	96%
6	99%	31	94%
7	99%	32	95%
8	99%	33	95%
9	99%	34	94%
10	99%	35	95%
11	98%	36	95%
12	98%	37	94%
13	98%	38	93%
14	98%	39	93%
15	98%	40	95%
16	98%	41	91%
17	98%	42	93%
18	98%	43	91%
19	98%	44	92%
20	98%	45	92%
21	96%	46	92%
22	97%	47	91%
23	95%	48	93%
24	95%	49	93%
25	96%	50	91%

Figura 39. Porcentaje de detección de ataque por posición.

Con lo anterior nos permitió calcular el porcentaje de eficiencia total del sistema, ello lo vemos en la Figura 40, demostrando la viabilidad del proyecto y lo desarrollado donde se obtuvo un 95,8%

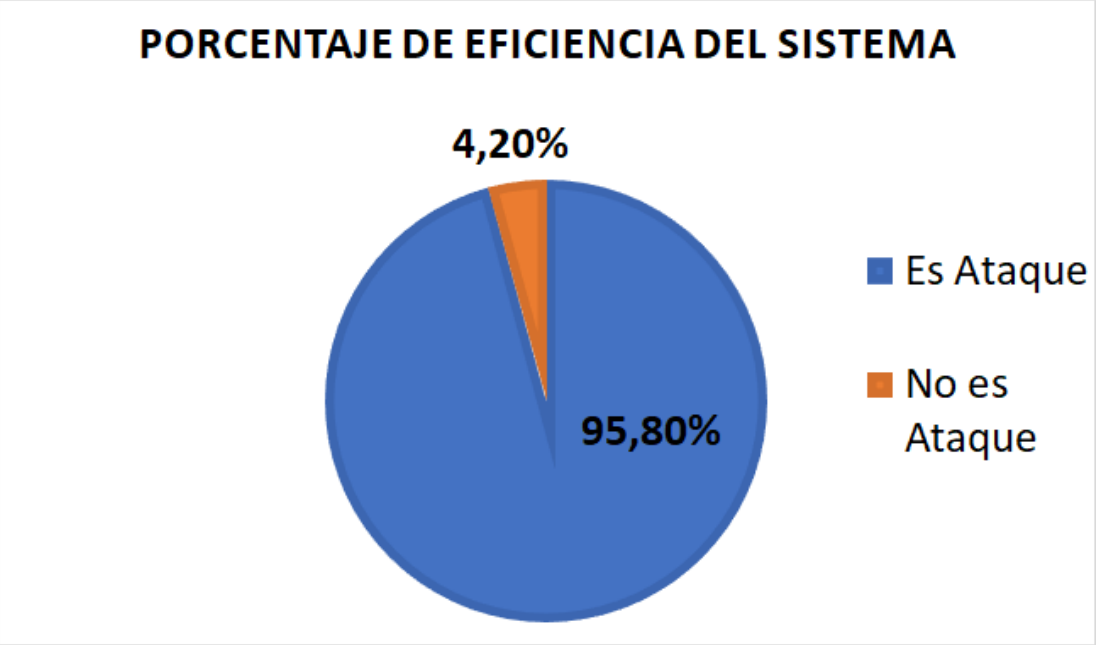


Figura 40. Porcentaje de eficiencia del sistema.

8. Conclusiones

- Se diseñó e implementó un sistema de detección para el ataque de emulación de usuario primario malicioso utilizando una máquina de soporte vectorial con un 95,8 % de eficiencia, por lo tanto, se considera que la solución cumple con el objetivo planteado, brindado un porcentaje de confiabilidad alto, esto teniendo presente que la posición más lejana tuvo un porcentaje de 91%.

- Gracias a la articulación de las herramientas de hardware RTL-SDR, el USRP y con el software libre GNU Radio, fue posible diseñar la construcción de una herramienta que permitiera la detección de ataque de emulación de usuario primario malicioso en tiempo real para las frecuencias trabajadas, es así que resaltamos la importancia del uso de la radio cognitiva ya que gracias al sistema implementado permite detectar inteligentemente la transmisión de usuarios no autorizados en la banda de frecuencia de 876.8 MHz.

- El sistema al identificar que el ataque está encendido observa una señal más estable a comparación de la misma cuando el PUE no está presente; esto se confirma al analizar los valores obtenidos en el cálculo de las entropías correspondientes, facilitando el trabajo al sistema de detección, ya que la diferencia se marca en dos grandes grupos permitiendo la detección en línea, esto se vio en la gráfica arrojada por la SVM en el proceso de entrenamiento.

- Se utilizó la técnica de minería de datos por agrupamiento, ya que esta nos permitió trabajar correctamente la SVM y fue ideal para el trabajo en tiempo real, ya que utiliza un método de entrenamiento y con base en ello, poder determinar si los datos tomados corresponden a un ataque o no.

- Adicionalmente a la técnica de minería de datos mencionada, fue necesario realizar una previa limpieza de los datos, para poder leer adecuadamente la energía de la señal y poder trabajar correctamente los pasos posteriores a este, allí se resalta la importancia del código desarrollado en Python que permitió implementar bloques de trabajo para la conversión de datos en tiempo brindado óptimos de niveles de procesamiento sin alterar los datos capturado, esto apoyándonos en las bondades del Sistema Operativo Ubuntu, al ser un software libre de código abierto nos permitió trabajar diferentes programas sin necesidad de utilizar una licencia, adicionalmente es más estable y más seguro que otros Sistemas operativos.

- El desarrollo de este proyecto es una alternativa viable para ser implementado en las redes de comunicaciones móviles, dado que en las estaciones base de los operadores prestadores de este servicio podrán tomar las medidas del espectro que tienen licenciado con el fin de identificar ataques a su espacio espectral mediante la SVM y tomar así las acciones

correspondientes frente a un ataque, como el trabajado en este proyecto ya que las frecuencias de trabajo son utilizadas en nuestro territorio para comunicaciones móviles.

- Como sistema de seguridad es el adecuado para ejercer la tarea de toma de decisiones y garantizar un nivel de confiabilidad en un sistema de comunicaciones móvil, por lo que podría incentivar de alguna manera el uso de esta tecnología en la industria o en grandes entidades que trabajen con este tipo de redes.

9. Referencias

[1] J. Mithola, G.Q. Maguire. “Cognitive Radio: Making Software Radios More Personal”. Royal Institute Of Technology, disponible en internet https://pdfs.semanticscholar.org/fb5d/1bb23724d9a5a5eae036a2e3cf291cac2c1b.pdf

[2] D. A. López, E. R. Trujillo, O. E. Gualdron. “Elementos Fundamentales que Componen la Radio Cognitiva y Asignación de Bandas Espectrales”. Universidad Distrital Francisco José de Caldas y Universidad de Pamplona, Campus Universitario, Pamplona-Colombia, Inf. tecnol. vol.26 no.1 La Serena 2015. Bogotá, Colombia 2015.

[3] H. R. Márquez Ramos. “Arquitecturas De Radio Cognitiva: Una Revisión Actual”. Distrital Francisco José De Caldas. Tecnura, Vol. 18, Núm. 39, enero-marzo, 2014, Pp. 181-196. Bogotá, Colombia 2015.

[4] J.M. Huidobro, J. Luque Ordoñez. "Comunicaciones Por Radio. Tecnologías, Redes Y Servicios De Radiocomunicaciones. El Espectro Electromagnético". Editorial Y Publicaciones Ra-Ma, S.A. P 526 - 528. Junio 19, 2013

[5] FCC,” Notice of proposed rule making and order” ET Docket No. 03-222, Washington diciembre 2013 Disponible en internet: http://www.fcc.gov

TTY: 1-888-835-5322

[6] L. F. Pedraza, F. Forero, I. P. Páez. “Detección de espectro para radio cognitiva”. Universidad Distrital "Francisco José de Caldas", Universidad Nacional de Colombia. Ingeniare. Rev. chil. ing. vol.20 no.2 Arica ago. 2012. Bogotá, Colombia 2012.

[7] C. Hernández, L. F. Pedraza, I. Páez, C. Rodríguez, “Análisis de la Movilidad Espectral en Redes de Radio Cognitiva”. Universidad Distrital "Francisco José de Caldas", Universidad Nacional de Colombia. Inf. tecnol. vol.26 no.6 La Serena 2015.

[8] J. C. Ordoñez. “Caracterización de usuarios primarios para la implementación de un modelo predictor para la toma de decisiones en redes inalámbricas de radio cognitiva”. Universidad Distrital Francisco José De Caldas. Bogotá, Colombia, 2016. Disponible en internet http://repository.udistrital.edu.co/bitstream/11349/3715/1/CaracterizacionBayesiana.pdf

[9] M. Hanif Rahman, M. Hossain. “Primary User Emulation Attack (PUEA) In Cognitive Radio Network (CRN)”. Department Of Electronics & Communications Engineering East West University. 2016. Disponible en internet: https://pdfs.semanticscholar.org/e361/9b138612afa66208e8987e75487e61785405.pdf

[10] M. T. Masonta, M. Mzyece, N. Ntlatlapa. “Decisión del espectro en redes de radio cognitivas: una encuesta”. IEEE Communications Surveys & Tutorials, 2013 volume 15, páginas 1088-1107.

[11]C. Zhao, W. Wang, L. Huang, Y. Yao. “Base de ataque anti-PUE en la identificación de la huella digital del transmisor en radio cognitiva”. 2009 quinta Conferencia Internacional sobre

Comunicaciones Inalámbricas, Redes y Computación Móvil. 30 de octubre de 2009, 10.1109 / WICOM.2009.5305529.

[12] L. Huang, L. Xie, H. Yu, W. Wang, Y. Yao. “Ataque anti-PUE basado en la verificación de posición conjunta en redes de radio cognitivas”. 2010 conferencia internacional sobre comunicaciones y computación móvil. 24 de mayo de 2010, 10.1109 / CMC.2010.26.

[13] E. Cadena Muñoz, L.F. Pedraza Martinez, C.A. Hernandez. “Rényi Entropy-Based Spectrum Sensing in Mobile Cognitive Radio Networks Using Software Defined Radio”. Entropía 2020, 22, 626.

[14] E. Cadena Muñoz, L.F. Pedraza Martínez, J.E. Ortiz Triviño. “Detection of Malicious Primary User Emulation Based on a Support Vector Machine for a Mobile Cognitive Radio Network Using Software-Defined Radio”. Electrónica, EISSN 2079-9292, publicado por MDPI AG. Agosto 2020

[15] L. Jiménez Moscovitz, P. Rengifo Rengifo. “Al Interior De Una Máquina De Soporte Vectorial”. Revista de ciencias, Pág. 73-85, 19 Octubre 2010

[16] S. Carrizosa Botero, E. Mejía Mejía. “Detección De Ataques Epilépticos A Partir De Señales Fisiológicas”. Universidad EIA BIOM0330. Envigado, 2019

[17] A. Zurita, J. Duran Cals. "Aprendizaje automático para la detección de ataques informáticos"TFG En Enginyeria Informàtica, Escola D’enginyeria (EE), Universitat Autònoma De Barcelona (UAB). ID de corpus: 192128309 , 2016.

[18] L. Solano Naizzir. “Modelo basado en técnicas de aprendizaje automático permitirá detectar ataques a sistemas informáticos”. Repositorio Universidad De la Costa.CC0 1.0 Universal. 27 de Julio del 2019

[19] J. A. Baena, J. F. Duitama. "Machine Learning-based Approach to Detect Online Performance Problems in Distributed Systems". Innovación y Tendencias en Ingeniería (CONIITI) 2019 Congreso Internacional de, pp. 1-6, 2019.

[20] R. Vargas, J. Aguilar, E. Puerto. “Ciclo Autonómico de Análisis de Datos para el Diseño de Descriptores para Algoritmos de Aprendizaje Automático”. Revista Venezolana de Computación ISSN: 2244-7040, Vol. 5, No. 2, pp. 1-11, Diciembre 2018, Selección de los Mejores Artículos de CoNCISa 2018

[21] C. Hernández, L. Pedraza, I. Páez, E. Rodríguez. “Análisis de la Movilidad Espectral en Redes de Radio Cognitiva”. Universidad Distrital Francisco José de Caldas, Facultad Tecnológica, Universidad Nacional de Colombia, Facultad de Ingeniería, Universidad Autónoma Metropolitana Iztapalapa, Departamento de Ingeniería Eléctrica. Inf. tecnol. vol.26 no.6 La Serena 2015. Bogotá, Colombia 2015.

[22] D. García Gómez, J. M. Riera Salís, and P. García del Pino, “Implementación y configuración de un receptor de radio definido por software (SDR) para estudios de propagación,” 2012.

[23] C.V. Merchán Cuno, H. O. Moreno Avilés, “Diseño E Implementación De Un Sistema Radar Utilizando Sistema SDR A Través De Tecnología USRP Para Aplicaciones Topográficas”. Escuela Superior Politécnica De Chimborazo, Facultad De Informática Y Electrónica, 2016.

[24] M.D. Torres Vega, C.S. Vaca Gallardo. “Sistema Embebido De Comunicación Digital De Voz Utilizando Periféricos De Radio Universal Usrp-E110”. Universidad De Las Fuerzas Armadas - Espe, Departamento De Eléctrica Y Electrónica, Ecuador, Julio del 2014.

[25] Unión Internacional de Telecomunicaciones (ITU). “Definiciones de sistema radioeléctrico determinado por programas informáticos (RDI) y sistema radioeléctrico cognoscitivo (SRC)”

Informe UIT-R SM.2152, Pag, 1 y 2. Disponible en internet: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-SM.2152-2009-PDF-S.pdf

[26] S. Haikin. “Cognitive Radio: Brain-Empowered Wireless Communications”. IEEE J. Sel. Areas Commun., 2005, 23(2), 201-220.

[27] R. Bordón López, S. Montejo Sánchez. “La Radio Cognitiva y su Impacto en el Uso Eficiente del Espectro de Radio”. Universidad Central de Las Villas (UCLV), Cuba, 2015

[28] MJ Blasco, J Mut, H Rifa-Pous. “Detección robusta en grupos de señales primarias en redes de radio cognitiva”. Capítulo 4, P 88 -92. Actas de la XI Reunión Española sobre Criptología y Seguridad de la Información (XI-RECSI), 371-376.

[29] J. Blesa, E. Romero, A. Rozas, A. Araujo. “Detección de ataque PUE en CWSN utilizando técnicas de detección de anomalías”. J Wireless Com Network 2013, 215 (2013). https://doi.org/10.1186/1687-1499-2013-215

[30] C. Chen. “Investigation of Primary User Emulation Attack in Cognitive Radio Networks”. Tese de doutorado, Faculty of the Stevens Institute of Technology, Hoboken, EUA, 2011.

[31] R. Chen and J. Park. “Ensuring trustworthy spectrum sensing in cognitive radio networks”. In IEEE Workshop on Networking Technologies for Software Defined Radio Networks, paginas 110 –119, septiembre 2016.

[32] R. Chen, J. Park, and J. Reed. ” Evaluación de los algoritmos de rendezvous ciego para redes radio cognitivas ante interferencias”. IEEE Journal on Selected Areas in Communications, 26(1):25–37, enero 2018.

[33] L.A. Fuentes Mamani, J.C. Huarachi Soto. “Esquema Flexible De Múltiples Criterios Para Detectar Ataques De Emulación De Usuario Primario En Redes Ad Hoc De Radio Cognitivo”. Universidad Católica De Santa María Facultad De Ciencias E Ingenierías Físicas Y Formales. Arequipa, Perú 2014.

[34] D. Das, S. Das, “Primary User Emulation Attace talleres de comunicación informática, 2010, vol., no., pp.1,6, 15-19 March 2010.

[36] O. León, J.Hernández Serrano, M. Soriano. “Cooperative detection of primary user emulation attacks in CRNs”, Computer Networks, Volume 56, Issue 14, 28 Septiembrer 2012.

[37] Anand, S.; Jin, Z.; Subbalakshmi, K. P., "An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks," New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on, vol., no., pp.1,6, 14-17 Oct. 2008.

[38] Jin, Z.; Anand, S.; Subbalakshmi, K. P., "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks," Communications, 2009. ICC '09. IEEE

[39] C. Chen, H. Cheng; Y. D. Yao, "Cooperative Spectrum Sensing in Cognitive Radio Networks in the Presence of the Primary User Emulation Attack," IEEE, vol.10, no.7

[40] C. P. d. Colombia, "Constitución Política DE Colombia" 1991. [En línea]. Available: https://pdba.georgetown.edu/Constitutions/Colombia/colombia91.pdf. [Último acceso: 04 2020].

[41] M. de Comunicaciones, DECRETO 930 DE 4 de junio de 1992. Revista legislación económica, 1992.

[42] P. Fernández; P. Díaz, "Investigación cuantitativa y cualitativa" Cad Aten Primaria, vol 9, pp. 76-78, 2002.

[43] Cadena Muñoz, E., Pedraza-Martínez, L. F., Rodríguez-Colina, E., & others. "Primary user emulation characterization in mobile cognitive radio networks" Visión Electrónica, 14 (1). doi:10.14483/issn.2248-4728,2020

[44]C. Perez López, D. Satín González "Minería de datos. Técnicas y herramientas: técnicas y herramientas" Thomson, Edición 1, pp. 1-3, 2008.

[45]J. Riquelme, R. Ruíz, K. Gilbert "Minería de Datos: Conceptos y Tendencias" Revista Iberoamericana de Inteligencia Artificial. No.29, pp. 11-18, 2006

[46] E. Cadena Muñoz "Detección de emulación de usuario primario con localización dinámica en la red de radio cognitiva móvil mediante diseño cross-layer" Repositorio Universidad Nacional, 2020.