ANÁLISIS DE LAS TÉCNICAS JAMMING PARA EL BLOQUEO E INHIBICIÓN DE SEÑALES DE RADIOFRECUENCIA.

ANA MILENA VELANDIA BENITEZ

JUAN PABLO MORENO ACOSTA

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE INGENIERÍAS FÍSICO-MECÁNICAS

ESCUELA DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES

ESPECIALIZACIÓN EN TELECOMUNICACIONES

BUCARAMANGA

2017

ANÁLISIS DE LAS TÉCNICAS JAMMING PARA EL BLOQUEO E INHIBICIÓN DE SEÑALES DE RADIOFRECUENCIA.

ANA MILENA VELANDIA BENITEZ
JUAN PABLO MORENO ACOSTA

Monografía presentada para optar al título de:
Especialista en Telecomunicaciones

Director:
HOMERO ORTEGA BOADA
Ph.D of Engineering Sciences

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

DEDICATORIA

A nuestras familias, por toda la comprensión y apoyo incondicional, a nuestro mentor, el ingeniero Homero Ortega Boada que nos guio y encamino en la estructura de este proyecto y a Enlaces Inalámbricos Digitales S.A.S., que apoyo y enseño que la teoría y la aplicación son un complemento, y la unión es la mejor manera de transferir conocimiento para su aprovechamiento practico.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

TÍTULO: ANÁLISIS DE LAS TÉCNICAS JAMMING PARA EL BLOQUEO E INHIBICIÓN DE SEÑALES DE RADIOFRECUENCIA.*[1]

AUTORES: ANA MILENA VELANDIA BENITEZ, JUAN PABLO MORENO ACOSTA**

PALABRAS CLAVE: Gestión del Espectro, Guerra Electrónica, Jamming, Jammer, Monitoreo del Espectro, Espectro Radioeléctrico, Ataque Electrónico.

DESCRIPCIÓN:

El siguiente trabajo de monografía es el resultado de un arduo proceso de revisión bibliográfica de las distintas técnicas más importantes que pueden encontrarse para tareas de inhibición y bloqueo de señales de radiofrecuencias, partiendo del análisis del caso de estudio es el diseño de un dispositivo inhibidor de frecuencias para el bloqueo de emisiones de naturaleza ilegal o clandestina que al momento de la presentación de la monografía, el grupo de investigación RadioGIS aún se encuentra adelantando esfuerzos para elevar la solución del bloqueador hacia un alto grado de madurez, como sería el caso del registro de patente. Para alcanzar este objetivo, es necesario realizar una valoración de patentes que puedan ser similares a la idea original del dispositivo e identificar aquellos aspectos que pueden llegar a ser comunes y aquellos de los cuales podrían tener un aspecto innovador, y así ser un documento de consulta que permita ser una herramienta para iniciar el proceso del planteamiento de las posibles reivindicaciones a dar lugar. Por último, se desea además complementar analizando un aspecto de regulación acerca del despliegue y el uso de estos elementos en el territorio colombiano, y posibles campos de aplicación que pueda ser exportada la idea del jamming.

* Monografía

** Facultad de Ingenierías Físico-Mecánicas. Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones. Especialización en Telecomunicaciones. Director: PhD Homero Ortega Boada.

ABSTRACT

TITLE: ANALYSIS OF THE JAMMING TECHNIQUES FOR THE BLOCKING AND INHIBITION OF RADIO FREQUENCY SIGNALS *

AUTHOR: ANA MILENA VELANDIA BENITEZ, JUAN PABLO MORENO ACOSTA**

KEYWORDS: Spectrum Management, Electronic Warfare, Jamming, Jammer, Spectrum Monitoring, Radioelectric Spectrum, Electronic Attack.

DESCRIPTION:

The following monograph work is the result of an arduous process of bibliographic review of the different most important techniques that can be found for tasks of inhibition and blocking of radiofrequency signals, starting from the analysis of the case study is the design of an inhibitory device of frequencies to block illegal or clandestine radio emissions that at the time of the presentation of the monograph, the research group RadioGIS is still making efforts to raise the solution of the blocker to a high degree of maturity, as would be the case of the registration patent. To achieve this goal, it is necessary to carry out a patent assessment that may be similar to the original idea of the device and identify those aspects that may become common and those which could have an innovative aspect, and thus be a reference document. that allows to be a tool to initiate the process of the approach of the possible vindications to take place. Finally, we also want to complement by analyzing an aspect of regulation about the deployment and use of these elements in the Colombian territory, and possible fields of application that the idea of jamming can be exported.

* Monograph work

** Faculty of Physical- Mechanical Engineering. School of Electrical, Electronic and Telecommunications Engineering, Telecommunications Specialization Director Homero Ortega Boada.

INTRODUCCIÓN

Gracias a la Era de la Información [1] los sistemas y redes de comunicaciones inalámbricas cada vez evolucionan a un ritmo acelerado para dar abasto a la gran necesidad que demanda un mundo cada vez más conectado y a la diversificación de soluciones con tendencia TIC,
por tal razón, la tecnología ha ido mejorando la forma de protegerse de los ataques externos que puedan comprometer la seguridad y la integridad de los servicios [2]. Sin embargo, existe la misma tendencia en las tecnologías usadas para afectarlas, ya sea inhabilitando la capacidad del receptor de identificar la información o simplemente comprometiendo o alterando la información y evitar así el éxito de la transmisión.

Los bloqueadores o inhibidores de frecuencias son diseñados y construidos con el fin de afectar la calidad de la transmisión, la recepción o interpretación de la información recibida vista desde un receptor víctima dentro de un área delimitada [3], afectando específicamente a todo sistema que basa en el uso del Espectro Radioeléctrico. Existen una gran variedad y diversos tipos de bloqueadores [4] que se especializan en atacar un Servicio de Radio en específico [5] llegando a resultar muy problemáticos o hasta peligrosos si no son utilizados de manera adecuada, afectando a otros sistemas que no han sido objeto de ataque.

Como un ejemplo puntual estarían los inhibidores de frecuencias para el servicio móvil [4] desplegados en las áreas de los centros penitenciarios [6]. Este tipo de dispositivos son instalados para evitar que los reclusos llamen y reciban llamadas desde el exterior [7], sin embargo, si no se aplican las medidas técnicas necesarias para controlar su cobertura y los niveles de potencia, podrían generar afectación negativa a toda la comunidad vecina, privando así su uso en las áreas cercanas fuera los muros de la cárcel.

Los campos de aplicación que posee este tipo de sistemas de inhibición de frecuencias son extensos, partiendo desde el uso en los sistemas para servicios civil [4], [8] o de carácter privado hasta los organismos y entidades gubernamentales y militares [9], [10]. Incluso es posible encontrar un uso también para aplicaciones ilegales, delictivos y terroristas [11].

Históricamente, existe un contexto en donde su uso se ha convertido en el pilar de diferentes estrategias para atacar y protegerse de los ataques enemigos denominado como "*Guerra Electrónica*" [12]. Cuando se habla de *Guerra Electrónica (GE)* es importante mencionar otro término usado para describir el conjunto de acciones tácticas, así como las técnicas y métodos diseñados únicamente para interferir sobre las comunicaciones de cualquier enemigo, conocido como *Ataque Electrónico* (AE) o simplemente técnicas "*Jamming*" en un lenguaje más general. El termino Jamming no posee una traducción directa del inglés, y por lo general es usado para denominar toda solución, tecnología o dispositivos pensados para afectar los sistemas de comunicación o radar [13] basado en Radiofrecuencia sin importar la naturaleza del servicio afectado.

Con la presentación de este trabajo de Monografía se desea mostrar los resultados de la revisión actual de los tecnologías empleadas para el bloqueo de frecuencias, la identificación de las diferentes técnicas de Jamming existentes [14] para diversos servicios de Radio [4], analizando aspectos de las nuevas soluciones que presenten algún carácter innovador y que permita realizar un aporte al trabajo adelantado por el grupo de investigación *RadioGIS*[2], y por ultimo describir la normatividad vigente que regula el uso de este tipos de dispositivos a nivel local, con el fin de obtener una visión más amplia de nuevas oportunidades y nuevos campos de acción que el grupo pueda incursionar en trabajos futuros.

[2] Grupo de Investigación adscrito a la Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones E3T de la Universidad Industrial de Santander.

CAPÍTULO I
DESCRIPCIÓN DEL PROBLEMA

El grupo de investigación RadioGIS de la Universidad Industrial de Santander trabaja actualmente en el desarrollo de un sistema Jammer basado en la tecnología de Radio Definida por Software (SDR) e integrando el concepto de Internet de las Cosas (IoT). Hasta el momento, el sistema cuenta con la posibilidad de detectar y bloquear las emisiones consideradas clandestinas o ilegales para servicios de radiodifusión en las bandas de frecuencia de FM y Televisión Digital Terrestre que dicta el Cuadro Nacional de Atribución de Bandas de Frecuencia CNABF [15] de la Agencia Nacional del Espectro.

El terminal ha resultado para el grupo de investigación un gran reto en materia de diseño, construcción e implementación, contando además con una serie de resultados y avances que requerirán ser analizadas a fondo en trabajos de grado y tésis posteriores.

Como punto de partida se han planteado siguientes las preguntas problematizadoras que ayudarán acotar las necesidades más inmediatas que aborda el presente trabajo de monografía:

- *¿Será posible determinar otras técnicas de bloqueo o de inhibición para señales de Radio que puedan ser implementadas para mejorar las prestaciones del producto?*
- *¿Hay algún trabajo o estudio previo que presente o comparta la misma solución propuesta para el sistema Jammer?*
- *¿Es posible llegar a la conclusión de que el trabajo del grupo pueda ser patentable basado en una revisión del estado del arte?*
- *¿Qué nuevos aportes se podrían identificar si se compara con otras soluciones y desarrollos?*

Basado en los anteriores interrogantes se presenta a continuación la descripción del caso de estudio de interés, el concepto del terminal Jammer y de la configuración del Sistema en Red que podría darse en conjunto de los terminales Jammers.

1.1 Caso de Estudio

Como se expuso anteriormente, el desarrollo del dispositivo ha sido la aplicación de un proceso continuo por parte del grupo RadioGIS en el tema de la Radio Programada por Software o Software Defined Radio (SDR) en inglés, y que representa una gran oportunidad para la innovación en el área de las telecomunicaciones, motivando la redacción de patentes y publicación de trabajo en revistas indexadas, entre otros. A continuación, se describen aspectos de importancia como el modelo RIoT como base

1.2 Antecedentes de trabajos anteriores

El modelo RIoT

Se trata de un modelo de capas propuesto por el grupo RadioGIS en el marco del proyecto SDRCol2015[3] con el propósito de impulsar el desarrollo de soluciones basadas en SDR en apoyo a la GERE. El modelo consiste en establecer un marco de entendimiento entre los diferentes actores y así incrementar cada vez más el número de personas y entidades que pueden aportar a este campo. Sin embargo, resulta importante identificar unos requerimientos mínimos que el modelo RIoT posee:

- Ser compatible con los modelos conocidos para responder a la combinación de necesidades de ingenieros de RF y de software.

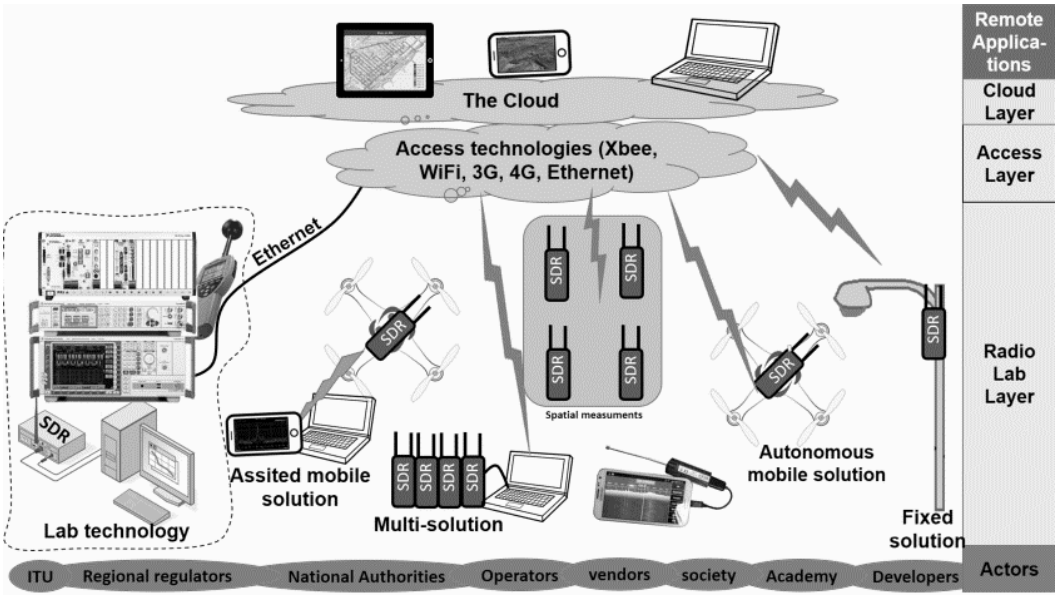
[3] Nombre que recibe el Proyecto de Investigación SDR como apoyo a la gestión del Espectro Radioeléctrico en Colombia ejecutado por el grupo RadioGIS en el año 2015 con financiamiento y en conjunto de la Agencia Nacional del Espectro ANE

- Reconocer que una solución puede ser desarrollada entre expertos de diferentes disciplinas y por lo tanto debe permitir identificar hasta dónde puede llegar cada uno.

- Permitir el desarrollo de soluciones flexibles y escalables, que sean compatibles o complementarias con las que desarrollan otras personas o entidades.

- Permitir el máximo provecho de los avances tecnológicos actuales, como IoT, pero que a su vez permita adaptarse para aprovechar los futuros.

Figura 1 Modelo de capas del RIoT[4]



En este modelo, los componentes de radio son vistos como cosas conectadas a internet y por eso el modelo se ha llamado Modelo de radio IoT (RIoT). A continuación, se describe el modelo capa por capa:

[4] Modelo tomado de los resultados del proyecto SDRCOL2015

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

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

Según lo descrito anteriormente, sobre la capa RadioLab se ubica el desarrollo del dispositivo Jammer que actualmente es caso de estudio, lo que permite mostrar un panorama mucho más amplio para la búsqueda de nuevas aplicaciones que impacten a diferentes áreas.

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

Capa de la Nube. Esta capa abarca los recursos que pueden ofrecer un valor agregado a la solución, tales como bases de datos, procesamiento en la nube, indicadores estadísticos y análisis en tiempo real.

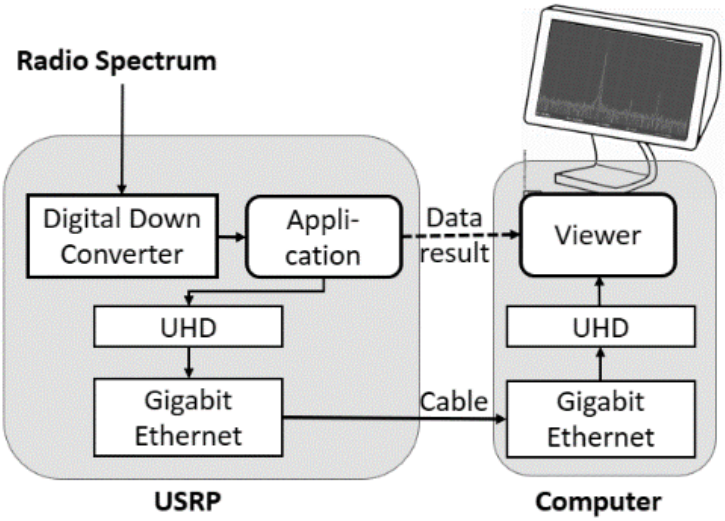
Capa de aplicaciones. Son las aplicaciones que permiten a usuarios conectados a la nube acceder a la información o tomar control de las tecnologías de la capa RadioLab.

Modelo de capas para aplicaciones RIoT

A partir del modelo RIoT se puede visualizar un panorama muy general de todos los factores que pueden intervenir en desarrollos y aplicaciones para Radio, contando cómo interactúan entre sí y su papel dentro de una solución de alto nivel. No obstante, es importante no descuidar la manera en cómo se deben implementar estas soluciones en el ámbito más práctico. Por tal razón se presenta los siguientes modelos usados y validados, representado de cierta manera los cimientos de lo que representa el dispositivo Jammer.

Inicialmente se basa en las experiencias en trabajos anteriores basados en la tecnología de *Universal Software Radio Peripheral USRP*, dispositivo compuesto por transmisores, receptores o transceptores utilizado comúnmente en implementaciones con SDR. Como se aprecia en la Figura 2, se tiene un modelo de capas para una aplicación de SDR para el monitoreo del Espectro, contando con elementos básicos necesarios para su funcionamiento.

Figura 2 Modelo de Capas para aplicaciones de monitoreo del Espectro en SDR.[5]



El sistema de monitoreo desarrollado por RadioGIS utiliza un equipo USRP que cuenta con un sistema embebido sobre el cual se ejecutan las aplicaciones de software, además de una interfaz de comunicación que permite el envío de la información a un equipo remoto para la visualización de los resultados. El envío se realiza por medio de una conexión por red local mediante el protocolo IPv4.

El uso en conjunto del USRP y el sistema embebido permite realizar aplicaciones mucho más flexibles en comparación al modo tradicional, el cual dicta que el USRP debe necesariamente estar conectado a un equipo de cómputo encargado de realizar el procesamiento de las señales provenientes del Espectro, algo muy visto en aplicaciones en laboratorios o académicas, limitadas únicamente a comprobación de fenómenos y no estrictamente al uso sobre campo.

[5] Tomado de los resultados del proyecto SDRCOL2015

En conclusión, el modelo de esta solución en particular puede ser vista simplemente como un down converter digital (DDC) con elementos analógicos y digitales, que entrega en forma digital, a la aplicación, la envolvente compleja de la señal que recibe la antena. Los demás elementos responden a dos realidades: un par de puertos ethernet lo que permite el contacto físico entre USRP y computador; computador y USRP necesitan reconocerse mutuamente y lo hacen a través del USRP Hardware Driver (UHD) gracias a que aprovecha todos los recursos del computador y el USRP para la conexión de los equipos y el flujo de datos por medio del protocolo IP.

1.3 El Jammer bloqueador de Frecuencias

En el punto anterior se describieron los modelos que influyeron para el diseño del equipo Jammer bloqueador de frecuencias, ayudando a fortalecer las bases para obtener un desarrollo maduro y completamente funcional que pueda ser usado en aplicaciones para la solución de distintas problemáticas más cercanas a la realidad del día a día.

Características y requisitos del equipo

A continuación, se describe las características más importantes que describen el dispositivo Inteligente de Jamming, el S-Jammer, nombre que recibe por primera vez en [16], trabajo que resume los resultados obtenidos de la caracterización de sus componentes de capa física. En la Tabla 1 se puede observar las más significativas.

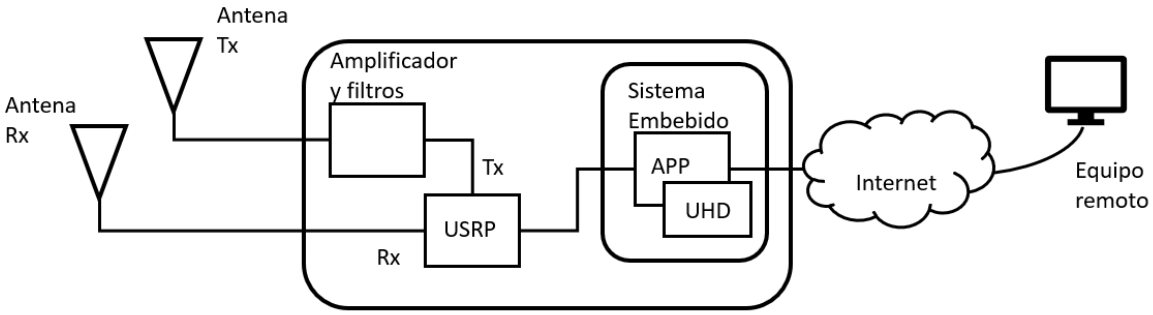
Tabla 1 Descripción de las características técnicas del S-Jammer

Características técnicas del S-Jammer		
Componentes de Hardware	**Componentes de Software**	**Componentes y funciones adicionales**
• Equipo USRP con capacidades de Sistema Embebido • Amplificador de potencia variable • Banco de filtros habilitados para las bandas de frecuencia de operación • Antenas ajustables para las longitudes de ondas requeridas para la operación • Módulo de red Ethernet para conexión hacia internet • Sistema de alimentación para el uso de los equipos • GPS	• Aplicación para el monitoreo del Espectro Radioeléctrico. • Aplicación de Jamming para servicios de Radio • Módulo de configuración de parámetros de transmisión • Interfaz de usuario para administración remota	• Base de datos para emisiones clandestinas • Servidor en la nube para la administración del equipo por Internet • Capacidad para la conexión en red con otros equipos bloqueadores • Escalabilidad para diferentes servicios y aplicaciones de Radio

Como se resumen en la tabla anterior, el sistema de jamming cuenta con distintos componentes fundamentales, los elementos que componen el hardware, el software y demás características que complementan el equipo S-Jammer.

Según se ha mencionado en la descripción del modelo de RIoT, cuando se habla de una aplicación de SDR, intervienen además distintos elementos que potencializan la solución, lo que se traduce a mejores prestaciones y a la mejora continua. No obstante, como cada aplicación se dimensiona a medida para abordar una problemática en especial, es necesario realizar un ajuste y adaptación para que pueda estar en sintonía con el problema local, evitando posibles malinterpretaciones o inconsistencias que puedan presentarse.

Figura 3 Arquitectura del S-Jammer



En la Figura 3 se puede observar detalladamente como se disponen cada elemento que componen al S-Jammer. En primer lugar, el equipo funciona como un transceptor, es decir, como transmisor y receptor, lo cual permite usar recursos para efectuar el jamming en conjunto con un sistema de amplificadores, filtros y una antena, por otro lado, se cuenta con el receptor que puede emplearse para el monitoreo del espectro, así como la identificación de las emisiones clandestinas. Seguido del sistema embebido que posee las aplicaciones de software y el componente de UHD.

Para funcionar como Jammer inteligente, debe emplear otro nodo que permita habilitar el componente de detección de emisiones clandestinas y otro como el Jammer conectados en red gestionada mediante un equipo remoto, lo que comúnmente podría considerarse un servidor dedicado, o sencillamente un computador habilitado para dichas tareas.

Los resultados que presenta este capítulo ayudan a dimensionar mejor el funcionamiento del S-Jammer y comprender mucho mejor el modelo que emplea para su implementación. Un desarrollo complejo como éste, requiere poder identificar unas necesidades muy particulares en una variedad de aspectos como el hardware y el software, que posiblemente puede ser materia de estudio para trabajos de investigación o de implementación. No obstante, hace falta identificar cuáles podrían ser esas capacidades a nivel de jamming que el S-Jammer podría a futuro contar para la potencialización de la inhibición de frecuencias mucho más acorde a las nuevas tecnologías y servicios que cada vez emplean métodos y técnicas para evitar ser objetivo de ataques externos.

CAPÍTULO II
FUNDAMENTOS DE JAMMING

El capítulo a continuación aborda los conceptos teóricos que abarcan las técnicas de jamming de interés [17], en especial aquellas usadas para el jamming inteligente. Como primer punto, se realiza una revisión del contexto del cual surge la práctica del jamming como lo es la Guerra Electrónica [18], describiendo la importancia e impactos que se destacan en el ámbito militar el uso de esta tecnología. Más adelante se mencionarán aquellas técnicas que según el análisis del capítulo 1, podrían complementar las funcionalidades del S-Jammer.

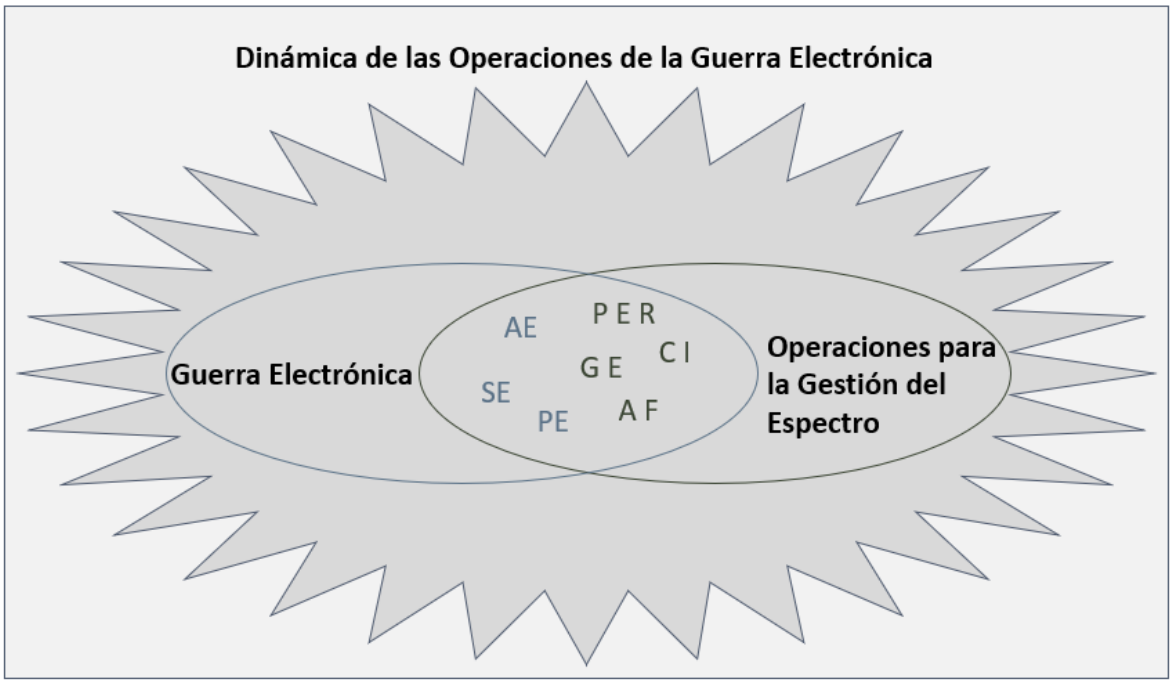
2.1 Contexto de la Guerra Electrónica

2.1.1 Orígenes de la Guerra Electrónica Durante la Segunda Guerra Mundial se vivió una gran revolución sobre la forma de aplacar las fuerzas enemigas, el sabotaje en los sistemas de telecomunicaciones y la interceptación de los mensajes encriptados eran cruciales para el éxito o no en los ataques que los ejércitos realizaban. Al conocer puntos estratégicos de las bases militares, rutas usadas para el transporte de tropas y suministros, era posible realizar tácticas eficaces y reducir el daño que se pudiera recibir por parte del enemigo. Los sistemas de comunicaciones eran considerados los principales objetivos y por este motivo, se usaron métodos para la protección de la información como encriptación de los mensajes y códigos secretos que evitaban al enemigo acceder fácilmente a ella. Muchos avances tecnológicos surgieron a raíz de estos acontecimientos [1], los antiguos sistemas de radio pasaron a ser obsoletos y se convirtieron mucho más seguros, y al mismo tiempo se identificaban las fallas y vulnerabilidades que presentaban dichos sistemas para sus ataques.

2.1.2 La dinámica de la Guerra Electrónica. La Guerra Electrónica es un concepto que ha redefinido la forma en cómo se desarrollan los conflictos militares en el mundo actual. La GE comprende el uso de técnicas, tácticas y tecnologías con el único fin de someter, limitar o destruir el accionar del enemigo teniendo un absoluto poder del Espectro Electromagnético EEM [19]. De igual modo, también se considera acciones de GE la implementación de medidas de protección como también las contramedidas a implementarse para la mitigación de posibles ataques de fuentes externas.

Según la definición anterior la GE maneja 3 pilares importantes denominados Ataque Electrónico (AE), Soporte Electrónico (SE) y por último la Protección Electrónica (PE).

Figura 4. Dinámica de la Guerra Electrónica[6]



[6] Adaptado del inglés de [19]

Como se puede apreciar en la Figura 4, existe una estrecha relación entre las operaciones empleadas en la GE y las tareas para las Operaciones para la Gestión del Espectro Radioeléctrico (OGER) [20]. Como primer punto en común, la Gestión del Espectro cuenta con unas políticas del espectro radioeléctrico (PER) muy claras, necesarias para el despliegue de todo tipo de servicios; la Gestión del Espectro (GE) como tal, que comprende las actividades de administración del recurso que va ligada a las PER, la asignación de frecuencias (AF) y la cooperación internacional (CI). Además, otro aspecto es que ambas operaciones requieren realizar procesos secuenciales como los estudios de viabilidad, planificación, preparación y ejecución, sin olvidar el continuo seguimiento de cada una de las acciones tomadas.

Una analogía entre ambos casos de operaciones puede darse para describir los procesos que compartan cierta similitud como se describió anteriormente, no obstante, existe una evidente diferencia con la finalidad y la naturaleza de cada una, la GE tiene como fin de inhabilitar a sus servicios objetivos y las OGER la de armonizar todos sistemas de comunicaciones licenciados y mantener controladas aquellas que no lo sean, interfiriendo sobre otras de modo directo o indirecto.

2.1.3 Ataque Electrónico. En el contexto de la GE [21] se considera un Ataque Electrónico (AE) a todo esfuerzo aplicado con el objetivo de reducir o suprimir la eficiencia de los sistemas militares basados en el uso del Espectro Electromagnético y Radioeléctrico. Su implementación se basa principalmente en el Jamming Electromagnético (JEM), la Decepción Electromagnética (DE), y demás aplicaciones de AE citados a continuación:

- Contramedidas para evitar la detección de sistemas enemigos
- Sondeo Electromagnético
- La Intrusión Electromagnética
- Generación de pulsos electromagnéticos

Como una rama de la GE, el Ataque Electrónico contiene una diversidad de técnicas perfeccionadas a través del tiempo y la experiencia [19], que, aunque resulten importante como materia de estudio en un contexto de investigación, no son de interés inmediato para este trabajo el revisarlas a profundidad, pero sí de resaltar que existen amplias posibilidades para explotar en este campo de aplicación.

2.1.4 Soporte de Guerra Electrónica. El Soporte Electrónico (SE) se implementa para las tareas de búsqueda, identificación, interceptación y localización de fuentes que intencional o inintencionalmente afecta el módulo que resultan ser perjudiciales para las operaciones tácticas [22].

También se puede analizar el SE como un análogo a lo que serían los sistemas de Monitoreo del Espectro, el análisis de Espacios en Blanco, algoritmos para la identificación de Interferencias de Radio, desde un punto de vista a las comunicaciones móviles convencionales. En fin, el SE podría ser cualquier herramienta que permita al sistema de jamming evaluar las situaciones en tiempo real sobre el campo de batalla, tomar decisiones acerca de los posibles ataques enemigos o apoyar activamente el AE hacia objetivos con un grado de protección anti-jamming, logrando de este modo, ser más efectivos en los resultados de bloqueo o inhibición.

2.1.5 Protección Electrónica. Toda acción tomada para la protección de la infraestructura desplegada en que se basa todos los sistemas comunicaciones y sistemas que emplean el Espectro Electromagnético es considerada como Protección Electrónica (PE) [22]. Sobre esta categoría de GE, se destaca la utilización de sistemas para mitigar los efectos de jamming de ataques externos, posiblemente de fuentes aliadas o enemigas.

La recopilación de diferentes métodos y acciones para la PE se conoce como técnicas anti-jamming. En relación con lo anterior, también es competencia de la PE la gestión del espectro de todos los sistemas, el blindaje electromagnético, y efectuar controles para todas las emisiones, manteniéndolas a niveles aceptables para evitar el fuego aliado.

2.2 Técnicas de Jamming inteligente

En el apartado anterior se mencionó aspectos importantes del Jamming como un resultado de emplear operaciones de Guerra Electrónica dentro de un contexto más ajeno al planteado en la descripción del problema, pero que dicta unas bases muy necesarias para seguir avanzando en el estudio de las técnicas de jamming que se describirán a continuación.

2.2.1 Tipos de Jammer. Como un elemento fundamental, el Jammer constituye el medio con el que se materializa las técnicas de jamming, así mismo, toda acción necesaria para la inhibición de frecuencias requerida. Los efectos de jamming del Jammer depende directamente de la potencia que utiliza la componente encargada de la transmisión, la ubicación asignada e influencia que posee el sistema sobre el objetivo [23]. De igual modo, un Jammer puede emplear distintas técnicas sobre una red con el objetivo de asegurar la interferencia.

Un Jammer puede ser elemental o avanzado dependiendo de su funcionalidad [14]. Los Jammers elementales se clasifican en dos subgrupos fundamentales: los proactivos y los reactivos. Lo más avanzados también se dividen en dos subgrupos: función-específico e híbrido-inteligente. La clasificación detallada de los diferentes Jammers puede encontrarse en la Figura 5.

2.2.2 Jammer proactivo. Los jammers proactivos transmiten directamente, interfiriendo de manera efectiva y señalando donde hay o no comunicación de datos en una red víctima en un área determinada. Su operación se basa en el envío de paquetes de bits aleatorios en el canal de operación, inhabilitando en cierta medida los canales de la víctima. Sin embargo, no soporta el cambio de los canales seleccionados, operando básicamente sólo en frecuencias fijas. Hay tres tipos básico de jammers proactivos: constante, falso y aleatorio.

Jammer constante

El jammer constante representa un elemento básico, esto gracias a que sólo se encarga de saturar los canales de los nodos mediante una emisión particularmente simple y constante sobre un aérea de afectación determinada. Este tipo de ataque es ineficiente en cuanto a energía y muy fácil de detectar por sistemas avanzados, pero muy fácil de usar y pueden afectar redes de comunicaciones hasta el punto de que nadie se puede comunicar en ningún momento.

El jammer constante también es conocido por ser uno de los más utilizados para las tareas sencillas de jamming, especialmente para servicios de broadcasting o radiodifusión, aun así, representa grandes costos en el momento de implementación en comparación a otras soluciones.

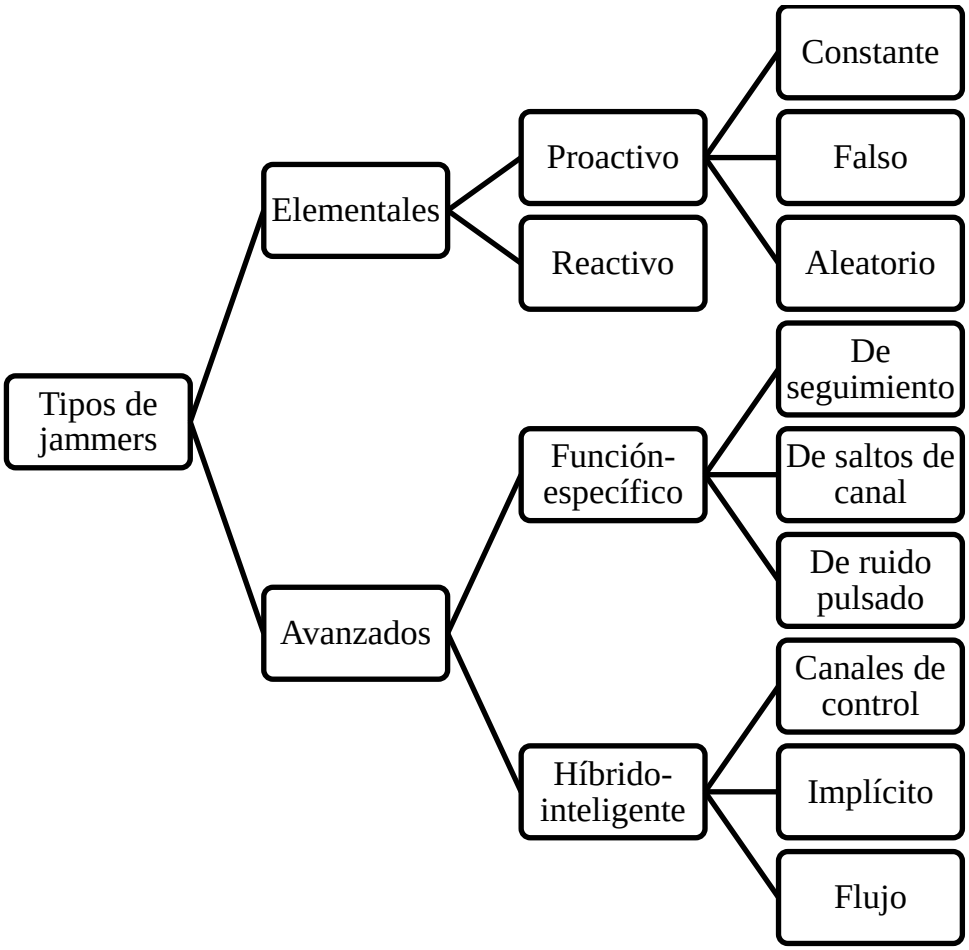
Jammers Falsos

Continuamente los jammers falsos transmiten señales de la misma naturaleza que posee el enlace víctima, en lugar de emitir bits aleatorios como sí lo hacen los jammers constantes. Engaña a otros enlaces o receptores para creer que se está produciendo una transmisión legítima. Comparado con un jammer constante, es más difícil de detectar un falso jammer porque transmite paquetes legítimos en lugar de bits aleatorios. Similar al jammer constante, los falsos jammers son

también ineficientemente energéticos debido a la continua transmisión, pero es muy fácil de implementar.

Requiere un sistema de soporte para realizar un seguimiento a la señal que se desea suplantar, ajustando parámetros de modulación y la potencia necesaria para emular al nodo víctima.

Figura 5 Clasificación de los Jammers según su operación[7]



[7] Adaptado del inglés de [14]

Jammer Aleatorio

Este tipo de jammer funciona por un determinado periodo de tiempo y deja de operar en otro periodo. El uso de este tipo de jamming depende mucho del tipo de servicio al que se desea afectar y el grado del mismo, siendo el tiempo ajustable para garantizar mejores resultados en el bloqueo de frecuencias. Se puede utilizar "Jamming" por ruido, por pulsos, por tonos e incluso por barrido. La potencia es menor debido a que no se encuentra en operación todo el tiempo. La detección es posible al realizar un análisis de la actividad de la red.

2.2.3 Jammer Reactivo. Dentro de los tipos de jammer descritos anteriormente, el reactivo resulta ser el más complejo de todos, ya que su finalidad es el de garantizar una menor posibilidad de ser detectado por otros sistemas anti-jamming [23].

Estos tipos de dispositivos se encargan de sensar toda actividad de la red para identificar el momento más adecuado para actuar. Otra diferencia importante que posee un jammer reactivo es que su finalidad no es simple hecho de bloquear a fuerza bruta una emisión, si no la de interceptar la información, aprovechando al máximo todas las debilidades que pueda presentar el enlace, en codificación y encriptamiento.

Si se compara el consumo energético, también se puede observar que disminuye al máximo, optimizando la potencia en la transmisión y dedicar más recursos para el monitoreo continuo.

2.2.4 Jamming función específica. Este tipo de jammer se implementa basado en el concepto de operar bajo funciones y configuraciones determinadas, para atacar a un servicio o tecnología en específico [24], empleando las técnicas más efectivas para completar su tarea. Puede ser proactivos o reactivos, utilizar un

canal dedicado o múltiplos canales, se enfoca en el éxito del jamming, independiente del consumo de energía o de recursos físicos que pueda demandar. Posiblemente, sobre esta categoría puede fácilmente ubicarse el S-Jammer, debido a que está inicialmente construido para atacar a servicios específicos como la radiodifusión sonora en FM y posiblemente para aplicaciones en Televisión Digital Terrestre (TDT).

Jammer de seguimiento

El jamming de seguimiento posee a su disposición mayores recursos para la explotación de todos los canales disponibles, realizando un seguimiento por saltos de frecuencias a una alta velocidad y en determinados de tiempos muy cortos, dotándola de la capacidad de ubicar emisiones soportadas en técnicas anti-jamming. Limita el consumo de energía al actuar sobre un único canal al tiempo, y sus saltos pueden ser secuenciales o de tipo aleatorio, al final, el Jammer de seguimiento resulta ser muy efectivos contra servicios que se basan en el salto de frecuencia o *Frequency Hopping*.

Jammer de saltos de canal

El Jammer se especializa en atacar a los sistemas basado en múltiples canales, anulando el éxito de toda transmisión del objetivo. Cuenta con la capacidad de afectar a más de un canal y utiliza un soporte para las fases de descubrimiento y seguimiento, lo que lo convierte en un Jammer silencioso y difícil de detectar. El modo de ataque puede variar según la secuencia pseudoaleatoria seleccionada.

Jammer de ruido pulsado

El Jammer de ruido pulsado opera mediante el cambio de canales y realiza ajuste en el ancho de banda y los periodos de tiempo activo. Posee cualidades similares al Jammer aleatorio, pero con la ventaja de optimizar la energía mediante el encendido y apagado del jamming. Además, otro punto positivo que posee el

Jammer de ruido pulsado a comparación del aleatorio, es la posibilidad de transmitir a diferentes canales en un mismo instante.

2.2.5 Jammers híbridos inteligentes. Se denominan inteligentes debido a su naturaleza eficaz y eficiente al momento de realizar funciones de bloqueo. El objetivo principal de estos jammers es aumentar el efecto de interferencia en la red que pretenden atacar. Además, prima el uso óptimo del consumo de la energía al momento de irradiar.

Se enfocan específicamente en consumir la suficiente energía en el lugar correcto para dificultar el ancho de banda de comunicación para toda la red o una parte importante de la red, en redes muy grandes. Cada uno de estos tipos de Jammer se puede implementar como proactivo y reactivo, brindando un aspecto híbrido.

Como se expondrá a continuación, estos tipos de Jammer tienen como objetivos inhabilitar toda función basada en la capa MAC, a toda red o sistema de comunicación inalámbrica mediante el uso de estrategias como la Denegación del Servicio (Denial of Service DoS), sabotaje informático, hacking de redes, hacking de redes y demás ataques que puedan incluirse en este tipo de jamming.

Jammer de canales de control

Los jammers de canales de control funcionan en redes multicanal dirigiéndose al canal de control o al canal utilizado para coordinar la actividad de la red. Un jammer aleatorio que se dirige al canal de control podría causar una grave degradación del rendimiento de la red, mientras que un jammer continúo dirigido al canal de control podría denegar el acceso a la red por completo. Estos ataques generalmente se logran comprometiendo un nodo en la red. Además, las ubicaciones de los canales de control futuros se pueden obtener a partir de los nodos comprometidos.

Jammers de ataques implícitos

Son aquellos que, además de deshabilitar la funcionalidad del objetivo deseado, provocan un estado de denegación de servicio en otros canales de la red víctima. Este ataque explota el algoritmo de adaptación de velocidad utilizado en redes inalámbricas, donde el Punto de Acceso (*Access Point AP*) atiende al nodo débil al reducir su velocidad. Debido a este proceso, el AP pasa más tiempo comunicándose con este nodo débil que los otros nodos. Por lo tanto, cuando el jammer implícito bloquea un nodo que se está comunicando con el AP, el efecto de adaptación de velocidad aumentará el enfoque del AP en el nodo atascado y causará que otros clientes sufran.

Ataques de jammers de flujo

El uso de múltiples Jammers para actuar en toda la red implica asegurar el atascamiento paquetes para reducir el flujo de tráfico. Estos ataques se inician utilizando información de la capa de red. Este tipo de ataque de interferencia es bueno para los atacantes con recursos limitados. Si hay un control centralizado, entonces se ajusta al mínimo el aporte de cada uno de los Jammers sobre el flujo de paquetes. En un modelo de jammer no centralizado, cada jammer comparte información con jammers vecinos para maximizar la eficiencia. En pocas palabas, los Jammers de flujo opera en conjunto como una red unitaria, donde cada Jammer actúa de manera individual o en conjunto según evalúe la forma más óptima de ataque su núcleo de procesamiento y soporte.

2.3 Análisis comparativo de Jamming

Después de definir cada uno de los diferentes tipos de jamming más importantes en los apartados anteriores del presente capítulo, se procede a resumir en la Tabla 2, aquellos que pueden considerarse entre las categorías de jammers proactivos y reactivos, incluyendo además, si posee la capacidad de optimizar al máximo su consumo energético, y, si requiere o está dimensionado para el uso de

ataques a un canal de frecuencias en específico o por el contrario, puede operar en múltiples canales al mismo tiempo.

Al profundizar mucho más en el tema, cada vez más existe trabajos que pueden resultar interesantes como puede ser [2], al momento de realizar distintas variaciones de los terminales definidos, incluyendo características y capacidades que benefician el jamming al momento de enfrentarse a sistemas tan difíciles de bloquear como el protocolo Wi-Fi, debido a que utiliza múltiples métodos anti-jamming y de reducción de interferencia para evitar ser objeto de ataque de ciertos tipos de jammers básicos y de sistemas que puedan interferir de manera no intencional sobre éstas.

Tabla 2 Resumen comparativo entre los distintos tipos de jammers

Jammer	**Proactivo**	**Reactivo**	**Eficiencia energética**	**Canal individual**	**Canales múltiples**
Constante	x			x	
Falso	x			x	
Aleatorio	x		x	x	
Jammer de seguimiento	x		x	x	
Salto de canal		x		x	x
Ruido pulsado	x			x	x
Canal de control	x	x	x	x	
Implícito	x	x	x	x	
Jammer de flujo	x	x	x	x	x

Otro punto que requiere una revisión en esta sección es la identificación de otros aspectos que no hacen parte del equipo o de las funciones básicas que compone el jammer, pero sí importa al momento de planear estratégicamente las

operaciones de jamming sobre las emisiones establecidas como objetivos, con el único fin de realizar acciones exitosas sobre ellas.

2.3.1 Ubicación del sistema de jamming. La ubicación del jammer resulta ser factor muy importante para garantizar un bloqueo eficaz. Independiente de las características mencionadas, las características del sitio de instalación y la posición del jammer con respecto a los transmisores del enlace víctima, podrían jugar un papel favorable o desfavorable al momento de observas el impacto que genera el jammer. Algunas técnicas requieren situarse cerca de la fuente transmisora, otros, por el contrario, no lo necesitan y solo depende de la potencia de la relación señal a jamming s/j que se ajuste.

2.3.2 Ataques óptimos de interferencia. Emplear estrategias en conjunto al sistema de jamming puede elevar toda posibilidad de inhibición. El conocer perfectamente todas las características técnicas, permite al equipo atacante, ganar cierta ventaja sobre su víctima, explotar al máximo las debilidades expuestas o descuidadas, facilita toda tarea de jamming. Algunos tipos de jammers, aquellos que poseen cierta capacidad de identificación y de adaptación, recurre a soportar sus operaciones mediante el uso de la información, módulos que se encargan de correlacionar variables medidas y predeterminadas, para realizar ataques efectivos. Los que no poseen estos recursos por defecto, pueden ser acoplados a sistemas de soporte que potencialicen sus efectos de jamming.

La forma de distribución de diferentes de jammers sobre un área determinada, realizar seguimiento a redes complementarias que puedan redirigir el tráfico, identificar la ejecución de maniobras anti-jamming, entre otros, aspectos que a la final, optimizan en cierto grado cualquier despliegue de cualquier tipo de jamming.

2.3.3 Bloqueos bajo completa incertidumbre. Si el despliegue del sistema de jamming o el conjunto de jammers, no cuenta con la posibilidad de analizar la información previa de la víctima, y cuenta sólo con una distribución totalmente aleatoria con respecto a la posición real exacta del transmisor objetivo, es necesario realizar ciertos ajustes como el uso de antenas omnidireccionales y equipos amplificadores de mayor potencia, garantizando una mayor cobertura posible de jamming.

Otras situaciones más específicas [7], se requiere que el jammer actúe sobre una ubicación y afecte un área determinada. En estos casos, es necesario limitar la cobertura y trabajar sobre aspectos conocidos, utilizando técnicas básicas como el jamming constante o sus variaciones.

2.3.4 Ataques de bloqueo de rango limitado. Cuando se tiene dispositivos con capacidades limitadas para el uso de jamming, a diferencia de las estrategias anteriores, no existe la posibilidad de extender al máximo los rangos de cobertura y todo efecto de jamming queda simplemente reducido a las prestaciones disponibles. De todas maneras, si se usa estratégicamente al complimiento de objetivos muy concretos, pueden llegar a ser muy útiles por la gran dificultad que tienen los sistemas de detección de jamming, deteriorando en distintos grados la calidad del servicio en general. Se pueden observar en los casos de enlaces punto a punto, en dónde el jammer se sitúa cerca del receptor víctima y no del trasmisor.

2.3.5 Red de Nano Jammers. En la gran mayoría de los casos mencionados anteriormente, casi todos los efectos de jamming están ligados a la potencia de transmisión que posee los equipos de bloqueo, y sus efectos recaen sobre uno o muy pocos dispositivos. En este caso, el uso en red de equipos con prestaciones de energía más bajas, pero operando en colaboración con una cantidad considerada de jammers, se mejoran con el uso de inhibidores basados en

características reactivas. Al distribuir la potencia que consumiría una sola terminal en diferentes dispositivos de bajo consumo, pero distribuidos de tal modo, que puedan ampliar el área de cobertura sin necesidad de elevar los niveles de radiación. Existe una diferencia entre usar en red equipos de alta potencia y baja, la más evidente, el costo de construcción de los jammers. Los nano jammer suelen ser mucho más económicos de construir e implementar que aquellos que usan rangos nominales o establecidos para operar en solitario.

En la siguiente tabla se encuentra resumido el análisis de esta sección. Concluyendo así en resaltar nuevos aspectos que puedan ser tenido en cuenta para las futuras mejoras y versiones del equipo S-Jammer.

Tabla 3 Revisión de las estrategias de jamming

Estrategia de jamming	**Conocimiento de la red**	**Poder de transmisión**	**Número de jammers**	**Nivel de detección**
Ataques óptimos de interferencia	Sí	Controlable	Uno	Difícil
Bloqueos bajo completa incertidumbre	Limitada	Calculado	Varios	Moderado
Ataques de bloqueo de rango limitado	No	Bajo	Varios	Difícil
Red de Nano Jammer	No	Medio	Varios	Muy difícil

CAPÍTULO III

REVISIÓN DEL MARCO LEGAL PARA EL USO DE JAMMERS EN COLOMBIA

Este capítulo tiene como objetivo la revisión del marco legal que envuelve el uso y el despliegue de sistemas Jammers, equipos dedicados para la inhibición o bloqueo de frecuencias. Como trabajo de monografía, resulta de suma importancia el complementar la revisión de la bibliografía técnica en conjunto con la normatividad, que, en la mayoría de las ocasiones, es descuidada o simplemente pasada por alto. Otro punto importante, es identificar todo el proceso necesario para un futuro despliegue de la solución como un servicio con cierto grado de madurez.

3.1 Reglamentación en Colombia

En Colombia existen diferentes entidades reguladoras que protegen y controlan el uso del espectro, partiendo de las asignaciones realizadas a entidades de riesgo como UNGRD, Gestión del riesgo, seccionales de salud, secretarias de gobierno, esquemas de seguridad de gobernaciones y el sector público en general, para luego realizar asignaciones a las entidades privadas, previa presentación de licitación o proceso publico directamente con la ANE.

En la actualidad se observa a nivel nacional que las entidades públicas y privadas cuentan con diferentes sistemas de comunicación como telefonía móvil, radiocomunicación, telefonía satelital, internet, datos móviles, etc., y así mismo diferentes protocolos, estándares y por ende marcas, con un problema generalizado y es el mal servicio, la decadencia de la señal y los limitantes geográficos a nivel nacional, es por esto aspectos anteriores que el estado reglamenta su uso.

A continuación, revisaremos la norma y reglamentación aplicada desde su inicio. La primera vez que se nombra el espectro electromagnético es en la Constitución Política Colombiana, Artículo 75, el cual indica:

> *"Artículo 75 de la Constitución Nacional Colombiana, donde establece que el espectro electromagnético es un bien público inajenable e imprescindible 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."*[8]

De esta manera se inicia la primera versión de gestión del uso del espectro por parte del estado, identificando y definiendo que es un bien común propio del estado Colombiano, por lo tanto debe ser vigilado por el mismo asegurando el buen uso tanto de internos como de externos, es decir salvaguardando el acceso al mismo por todos los colombianos y de manera equitativa, por otra parte también tiene la función de controlar el uso indebido por países vecinos que quieran hacer aprovecharse del espectro.

Seguido a la constitución política de Colombia, vinieron otras resoluciones y leyes como que dieron pie a separaciones, asignaciones, controles, títulos, prohibiciones y obligatoriedades para los diferentes usuarios y proveedores:

La Resolución 2774 del 16 de agosto del 2013 en la que se establecen los mecanismos legales para emplear los inhibidores, bloqueadores y amplificadores

[8] Tomado de: Constitución Política de Colombia Articulo 75 preparada por la Corte Constitucional Consejo Superior de la Judicatura, Sala Administrativa Centro de Documentación Judicial (Cendoj) Biblioteca Enrique Low Murtra-Belm, Título de la colección: Normatividad 5, ISSN: 2344-8997, Editado por: Corte Constitucional
Consejo Superior de la Judicatura, Sala Administrativa – Cendoj, www.corteconstitucional.gov.co

de señales radio eléctricas de manera legal, dejando en claro que solo el Ministerio de las TIC podrá autorizar a quienes los usen.[9]

Esta resolución define los términos y conceptos de amplificadores de señales radioeléctricas, inhibidores de señales radioeléctricas y bloqueadores de señales radioeléctricas en sus dos fases: Primero cuando se traslada en el espacio y Segundo: Cuando no sufre ningún tipo de traslado en el espacio, adicionalmente fija las condiciones para lugares externos e internos.

Además, define el criterio para sanciones cuando una instalación de inhibidores o bloqueadores de señal no esté autorizado por el Ministerio de Tecnologías de la Información y las Comunicaciones. De igual manera define los diferentes escenarios posibles para obtener autorización para instalación de inhibidores o bloqueadores de señal las cuales son: para entidades públicas y el sector financiero, previo análisis de la justificación brindada la cual debe estar homologada y/o avalada por un ingeniero de telecomunicaciones o ramo a fin, en dicha justificación se debe incluir un diseño que incluye: fichas técnicas del equipo a instalar que incluya potencia y bandas de frecuencia, tiempo de uso, coordenadas, nombre del solicitante, planos arquitectónicos para espacios confinados, mapas de cobertura, mancha de propagación y toda la máxima información detallada respectiva.

Una vez aprobada la licencia se podrá instalar el bloqueador o inhibidor de señal y se deberán realizar pruebas de funcionamiento con el fin de no afectar a los usuarios más allá de lo permitido, es decir que a las zonas comunes y publicas no se debe afectar el uso del espectro, para comprobar este efecto nuevamente se deberá enviar a la ANE el respectivo informe de funcionamiento y operación desde el día uno hasta el día del envió del informe.

[9] Tomado de: Resolución 2774 del 16 de agosto del 2013

Existen excepciones en la reglamentación del uso de inhibidores o bloqueadores de señal radioeléctrica, como lo son: el Instituto Nacional Penitenciario y Carcelario INPEC, al igual que las entidades de seguridad pública: Fiscalía, CTI, Policía, Fuerza Aérea, Ejercito Nacional, entre otros.

Por último, abarca el tema de los amplificadores de señal celular que indica que independiente de contar o no con el permiso para el uso del espectro estos dispositivos se deben ajustar a lo señalado en la resolución 2544 de 2009.

Dicha resolución concluye que las únicas entidades de vigilancia y control son la Agencia Nacional del Espectro ANE y la Dirección de Vigilancia y control del Ministerio de Tecnologías de la información y las Comunicaciones MINTIC, aclarando que el MINTIC no cuenta con conceptos técnicos profesionales para el análisis del mismo, sino que esta función la realiza la ANE, apoyados en la dirección de protección a usuarios de servicios de comunicaciones

La Ley 1341 del 2009, "Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones"[10] esta ley es la principal herramienta del Ministerio y abarca todas las políticas públicas y marco legal a nivel nacional incluyendo y sin limitarse a la protección de acceso al medio a los usuarios, la competencia libre y equidad para evitar monopolios, el uso eficiente de las redes y del espectro radioeléctrico para asegurar calidad y eficiencia sin discriminación alguna.

Está fundamentada en principios orientadores que incluyen: 1) Prioridad al acceso y uso de las Tecnologías de la Información y comunicaciones, 2) Libre competencia, 3) Uso eficiente de la infraestructura y de los recursos escasos, 4)

[10] Tomado de: Ley 1341 del 2009 Ministerio de las Tecnologías de La información y las Comunicaciones TIC, http://www.mintic.gov.co/portal/604/w3-article-3707.html

Protección de los derechos de los usuarios, 5) Promoción de la Inversión, 6) Neutralidad Tecnológica, 7) El Derecho a la Comunicación, la Información, y la Educación y los Servicios Básicos de las TIC 8) Masificación del gobierno en Línea

Esta ley específica la importancia de la información en la sociedad para el desarrollo y el conocimiento, es por esto que el estado debe intervenir para proteger a los usuarios, promover acceso y desarrollo de contenidos y aplicaciones, asegurar la pluralidad y competencia equitativa y sobre todo garantizar el uso adecuado del espectro

El Artículo 11 de la misma Ley, señala que el uso del espectro necesita de un permiso especial otorgado por el MINTIC para su operación y uso, con el fin de controlar interferencias sobre otros servicios o usuarios, complementario con el Artículo 64, el cual especifica la infracción que puede con llevar el uso del espectro sin debida autorización, de igual manera aclara que cualquier operador que no cuente con el permiso será considerado como clandestino y las autoridades podrán en cualquier momento suspenderlo y retirarle los equipos

La resolución 3066 del 2011 de la superintendencia de industria y comercio establece el régimen de la protección de los derechos de los usuarios de los servicios de comunicaciones, adoptando la Decisión 638 de 2006 que emitió la Comisión de la Comunidad Andina –CAN, con el fin de brindar armonía a los usuarios en la subregión andina en materia de Comunicaciones.

3.2 Entidades Reguladoras

MINISTERIO DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Se denominó en el artículo 16 de la ley 1341 del 2001 de igual manera creo los objetivos en los que incluía cuatro principales

1. Diseñar, formular, adaptar y promover las políticas, planes, programas y proyectas del sector de TIC, en correspondencia can la Constitución Política y la ley, con el fin de contribuir al desarrollo económico, político y social de la Nación, y elevar el bienestar de los colombianos.

2. Promover el uso y apropiación de las TIC entre las ciudadanas, las empresas, el gobierno y demás instancias nacionales como soporte del desarrollo social, económico y político de la Nación.

3. Impulsar el desarrollo y fortalecimiento del sector de las TIC, promover la investigación e innovación buscando su competitividad y avance tecnológico conforme al entorno nacional e internacional.

4. Definir la política y ejercer la gestión. Planeación y administración del Espectro radioeléctrico y de los servicios postales y relacionados, con excepción de lo dispuesto en artículo 76 de la Constitución Política.[11]

COMISIÓN DE REGULACIÓN DE COMUNICACIONES CRC

Se denominó en el artículo 19 de la ley 1341 del 2001 como apoyo al MINTIC, con independencia administrativa, técnica y patrimonial sin personería jurídica adscrita al MINTIC, es el ente encargado de promover la competencia, evitar el abuso dominante y regular los mercados de las redes y los servicios de las comunicaciones; con el fin que la prestación de los servicios sea económicamente

[11] Tomado de: Ley 1341 del 2009 Ministerio de las Tecnologías de La información y y las Comunicaciones TIC, http://www.mintic.gov.co/portal/604/w3-article-3707.html

efectiva y refleje altos niveles de calidad, inicialmente empieza con las definiciones acorde a lo instaurado por la ITU.

Básicamente la Comisión de Regulación de Comunicaciones CRC, es quien define los conceptos y habilita técnicamente cualquier decisión que se vaya a tomar en el MINTIC, los comisionados de la CRC deben tener la capacidad para establecer el régimen de regulación, libre competencia, acceso al medio, homologaciones, habilitaciones técnicas, permisos de nuevas tecnologías, estándares y certificaciones, aclarar consultas o dudas técnicas, restricciones o controversias de operadores, condiciones de ofertas, recursos y todo lo que concerniente al ámbito técnico de las tecnologías y comunicaciones nacionales.

AGENCIA NACIONAL DEL ESPECTRO (ANE)

En el capítulo II de la ley 1341 del 2009, artículo 25 se reglamenta la creación de la Agencia Nacional del Espectro - ANE - como una Unidad Administrativa Especial del orden nacional, adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones, sin personería jurídica, con autonomía técnica, administrativa y financiera. [12]

Tiene dentro de sus funciones ejercer la vigilancia y control del espectro radioeléctrico, hace parte del apoyo técnico del MINTIC y sus funciones principales incluye asesorar al MINTIC en la planeación de programas y diseños del espectro radioeléctrico, si bien la CRC es el apoyo técnico en temas de terminales, mercados y calidad de servicios y todo lo correspondiente a Tecnologías y Comunicaciones, lo único que no puede gestionar es el espectro radioeléctrico, ya que la ANE es el único ente de vigilancia y control del espectro radioeléctricos incluyendo satelital.

[12] Tomado de: Ley 1341 del 2009 Ministerio de las Tecnologías de La información y y las Comunicaciones TIC, http://www.mintic.gov.co/portal/604/w3-article-3707.html

UNION INTERNACIONAL DE TELECOMUNICACIONES UIT

La UIT es la entidad especializada en Telecomunicaciones y fue establecida para crear, estandarizar, controlar y regular las telecomunicaciones a nivel mundial.

En cumplimiento de su misión: “Comprometida para conectar al mundo” complementa la regulación internacional del espectro con las múltiples actividades de su Sector de Radiocomunicaciones (UIT-R), Normalización y Teleco y sus Comisiones de Estudio; fruto de ellas son las Recomendaciones y Reportes ITU-R, los cuales son referente universal en la materia; así mismo, la publicación de manuales especializados, y otras labores de difusión, promoción, y asistencia técnica en materia de gestión y regulación del espectro.

En sus recomendaciones se enmarca la Recomendación IUT-R SM.1446, con el fin de hacer gestión al espectro y: Definición y medición de los productos de intermodulación en transmisores que utilizan técnicas de modulación de frecuencia, de fase o compleja, RECOMENDACIÓN UIT-T H.246 Enmienda 1 – Correspondencia del nivel de prioridad de usuario y de la red nacional/internacional de origen de llamada entre H.225 y la ISUP

3.3 Disposición técnica para el despliegue de la tecnología en Colombia

Como se describe en el capítulo anterior la COMISIÓN DE REGULACIÓN DE COMUNICACIONES CRC, en el artículo 22 FUNCIONES DE LA COMISION DE REGULACIÓN DE COMUNICACIONES indica:

> Son funciones de la Comisión de Regulación de Comunicaciones las siguientes:
> 1. Establecer el régimen de regulación que maximice el bienestar social de los usuarios.

2. Promover y regular la libre competencia para la provisión de redes y servicios de telecomunicaciones, y prevenir conductas desleales y prácticas comerciales restrictivas, mediante regulaciones de carácter general o medidas particulares, pudiendo proponer reglas de comportamiento diferenciales según la posición de los proveedores, previamente se haya determinado la existencia de una falla en el mercado.

3. Expedir toda la regulación de carácter general y particular en las materias relacionadas con el régimen de competencia, los aspectos técnicos y económicos relacionados con la obligación de interconexión y el acceso y uso de instalaciones esenciales, recursos físicos y soportes lógicos necesarios para la interconexión; así como la remuneración por el acceso

3.4 Aplicaciones tácticas y Servicios para Jamming en Colombia

3.4.1 Aplicaciones Militares. Los bloqueadores e inhibidores de frecuencia están diseñados para afectar la calidad de transmisión o recepción de las señales en un área definida, es por esto por lo que el uso más frecuente es en el sector publico especialmente en el militar representado para sitios de reclutamiento, centros especializados de investigación, cárceles, entre otros, a continuación, revisaremos diferentes ámbitos y múltiples aplicaciones en el mercado colombiano.

A continuación, se presenta una breve reseña de los actores nacionales que, a consideración de la Agencia nacional del Espectro han tenido y/o tienen un papel significativo en Colombia.

Los datos contenidos en este apartado están basados en la información investigada en los diferentes procesos licitatorios públicos y privados enunciados en el SECOP y SECOP II, adicionalmente datos que fueron suministrados por

dichas entidades en respuesta a la petición de información realizada por el Ministerio Nacional de Justicia y Paz MINNJUSTICIA.

Las fuerzas militares son el mayor consumidor de detectores de señal, bloqueadores e inhibidores de frecuencia, dada su alta complejidad en la operación y sobre todo por la discreción y seguridad que conlleva, usando dispositivos de muy alta tecnología con grados de seguridad y encriptada avanzada.

La instalación de bloqueadores de señal por parte del Instituto nacional penitenciario y carcelario INPEC, se sujeta a lo dispuesto en el decreto 4768 de 2011 y las normas que lo complementen. [13]

El inicio de los Bloqueadores de señal en el sistema carcelario se da en mesas de trabajo junto con el MINTIC, Gaula, Policía y Ejército, con el fin de disminuir la intensidad de señal de los operadores móviles, esta finalidad se soportaba en el decreto 4768 de 2011, toda vez que los reclusos estaban obligados a someterse a las normas internas de la institución, por lo cual el derecho al acceso a los medio de comunicación ya no eran permitidos con el mismo trato que una persona el común, de esta manera se decide que los internos no pueden tener elementos de comunicación como teléfonos, fax, gps radios o comunicaciones privadas[14], no solo por dar valor a la condición de recluso sino por controlar los diferentes actos de extorción, amenaza y estafa que principalmente se generaba desde las cárceles.

Por lo anterior el Ministerio de Tecnologías de la Información y las comunicaciones decreta que puede emitir el permiso para el Instituto Carcelario y Penitenciario INPEC, previa radicación de solicitud y justificación de la necesidad siempre y

[13] Tomado de: Resolución 2774 de 5 de agosto del 2015, Articulo 4 autorización de inhibición y bloqueo de señales radioeléctricas en ubicaciones fijas confinadas, parágrafo tercero.
[14] Tomado de: inciso 4° del artículo 111 de la Ley 65 de 1993.

cuando sea operado internamente-insourcing, es decir que no puede ser manejado por externos, tema contrario al suministro, la provisión de sistema de inhibición de señales radioeléctricas deberá tratarse como un proceso publico formal licitatorio, en cualquiera de las modalidades expuestas en la Ley 80 de 1993 y 1150 de 2007 de esta manera se asegurara el principio de pluralidad, equidad e igualdad en las contrataciones evitando detrimentos públicos y vicios de funcionarios.

De esta manera se da continuidad al plan de dotación de amplificadores de señal para las entidades militares con un aporte de $2.800.000 millones de pesos del Ministerio de Defensa para ser usado a nivel nacional, con el cual se adquiere sistema de inhibición para Valledupar, Barranquilla, Curacao, Combita, Cerrojo, un aporte secundario de $3.100.000 millones para Itagüí, $2.800.000 millones para Bellavista y de esta manera se logra cubrir más de 16 centros penitenciarios y carcelarios con el plan CERROJO para cubrir: Cúcuta, Ibague, Barranquilla, Acacias, Bogotá, Palmira, Cali, Bucaramanga, Pereira, Pedregal, Puerto Triunfo, Valledupar, Combita, Barranquilla, La Picota y Medellín Buenavista. El plan ORION tuvo exclusividad con la cárcel de Itagüí y luego fue adheridos los Establecimientos Popayán, Dorada, Valledupar – Mediana, Villavicencio, Itagüí, Quibdó, Cartagena, Barranquilla-, Pasto, Neiva, Jamundí, Girón, Sincelejo, Riohacha, Montería, Florencia y Santa Marta.

Las aplicaciones militares incrementaron su efectividad dado que los planes, organizaciones y órdenes estaban saliendo directamente de las cárceles, de esta manera lograron bajar el índice de extorciones que salían de los centros penitenciarios.

Adicionalmente se han usado sistemas de inhibición de señal radioeléctrica en la Lucha Contra Artefactos Explosivos, en el caso de los dispositivos activados a distancia por radio, la manera de contrarrestar esta amenaza consiste en

perturbar, mediante equipos inhibidores, la banda de frecuencias en la que opera el artefacto, para evitar que éste pueda recibir la señal de activación.

Otro caso a nivel internacional es la Protección de Aeronaves contra Misiles, que utiliza la potencia generada por las Ondas emitidas por microondas para neutralizar o destruir los sistemas electrónicos de guiado de los misiles.

Para finalizar, es importante señalar que la introducción de las armas de energía dirigida de RF en el escenario de operaciones obligará a introducir modificaciones en el diseño de los sistemas electrónicos de las plataformas e instalaciones militares, de tal manera que puedan estar razonablemente protegidas frente a un ataque con dichas armas. Por otro lado, la necesidad de minimizar el impacto de estos ataques sobre las plataformas militares introducirá algunos cambios en la doctrina de utilización de dichas plataformas, de tal manera que se definirán los procedimientos y tácticas adecuadas para reducir la probabilidad de que una plataforma se encuentre dentro del radio de acción de una RF-DEW.

3.4.2 Aplicaciones en Sistemas de Comunicaciones actuales. Hay un sin número de sistemas y tecnologías implicadas en el desarrollo de los sistemas de bloqueadores y/o inhibidores y amplificadores de señal radioeléctrica, por lo que describir todas podría resultar demasiado extenso. Por esta razón, se ha optado por incluir únicamente las que se considera que más van a influir en el futuro desarrollo de nuevos sistemas, Estas tecnologías son:

- *Antenas de tipo Array Activas de Barrido Electrónico (AESA).*

La tecnología tipo Array emplea una dirección guiada electrónicamente sin necesidad de realizar movimientos en el espacio, esto permite tener un desplazamiento de haz mucho más rápido que las que tienen un método mecánico, de esta manera logra hacer seguimiento a varios elementos “aviones,

carros, patrullas, etc.” simultáneamente. Para esto se requiere un alto nivel de potencia y amplificadores de tubos de vacío.

- *Nitruro de Galio (GaN).*

La tecnología Nitruro de Galio permite fabricar dispositivos en banda ancha, lo que significa que se puede usar un rango amplio de frecuencia para inhibir señales de diferentes tipos de aplicaciones, es decir que se podría bloquear con un inhibidor de banda desde 400Mhz a 900Mhz una señal radiocomunicación en UHF y también una señal de operador celular, dado que los radios de comunicación en UHF operan en 400 Mhz a 470 Mhz y la telefonía móvil tiene operación en 800 Mhz a 900 Mhz.

- *Sistemas Digitales.*

La tecnología digital ha abarcado todo el mercado nacional e internacional a puntos donde se fabrican dispositivos en modo mixto análogo/digital gran ancho de banda, esto permite que la inhibición de la señal sea más dinámica y precisa, puesto que los apuntamientos a las señales portadoras son exactos y no interfieren en ningún momento las señales adyacentes. La disminución de la efectividad se refleja dadas las amplitudes, disminuciones de conversores aplicados y formas de transporte de información 0 y 1

CAPÍTULO IV
RECOMENDACIONES TÉCNICAS PARA LA PATENTE DE JAMMING

El capítulo final presentado a continuación, resume unos aspectos técnicos importantes obtenidos a partir de los capítulos anteriores como recomendaciones que aporten al esclarecimiento de las preguntas problematizadoras que soportan el presente trabajo de monografía. Aclarando, que, aunque se describen ciertas recomendaciones, éstas no poseen un gran impacto en aspectos investigativos, no se sustenta sobre hipótesis comprobadas o evaluadas mediante un trabajo exhaustivo sobre la implementación del dispositivo bloqueador de frecuencias S-Jammer, si representa un primer paso, en lo que respecta al análisis del estado del arte y la discusión sobre aspectos que puedan presentar cierto grado de innovación.

Dado que los procesos que se llevan a cabo para concretar una solicitud de patente suelen ser muy largos y en algunos casos, tediosos, siempre se empieza de la misma manera. Identificar si el desarrollo o idea tiene el suficiente grado de invención e innovación que justifique todos estos esfuerzos.

El equipo bloqueador posee hasta el momento características básicas de un equipo de jammer común, revisados con profundidad en el capítulo 2. No obstante, posee la flexibilidad que ofrece todo tipo de aplicación de SDR, lo que amplía las posibilidades de implementar diferentes tipos de jamming, sin realizar ningún cambio a sus recursos de Hardware.

Otra característica para retomar de nuevo en este capítulo es su capacidad de operar en conjunto a otros terminales para utilizar estrategias optimas de jamming, y técnicas mucho más avanzadas.

Con base a lo anterior, se realizó una revisión exhaustiva sobre los diferentes registros de patentes aprobadas en el tema de jamming, con la finalidad de seleccionar la patente o las patentes que más se asemeja a la idea inicial del grupo de investigación.

Dentro de los parámetros de búsqueda se seleccionó el punto más importante, el uso en red de jammer inteligentes. Dentro de las razones que influyeron para tomar esta posición, se encuentra el pobre de desarrollo en la composición del hardware del equipo. No posee aporte alguno, sólo se basa en el uso de los recursos ya disponibles como equipos comerciales y adaptación de elementos existentes. Aun así, si existe grandes esfuerzos en identificar nuevas de formas de emplear más de un inhibidor y explorar nuevos métodos para asegurar el funcionamiento óptimo de la red. Dicho resultado se presenta con más detalle en la siguiente sección del capítulo.

4.1 Análisis de Patente "Metodología y Sistema para la generación de señales de jamming inteligente"

La patente "*METHOD AND SYSTEM FOR INTELLIGENT JAMMING SIGNAL GENERATION"* [25] o su traducción directa al español "Metodología y Sistema para la generación de señales de jamming inteligente", con número de patente US 20140206279A1, publicada en Julio 24 del 2014 por los inventores Chaz Inmendorf, Jungman Yun y Eamon Gormley, fue seleccionada como la invención que más similitudes posee con el concepto que RadioGIS desea explorar. El uso de Jammers inteligente en red.

El registro cuenta con el siguiente Abstract traducido directamente del inglés:

> "*La detección e inhibición de una red inalámbrica mediante el uso de un jammer inteligente que determina si una fuente de señal es una fuente de*

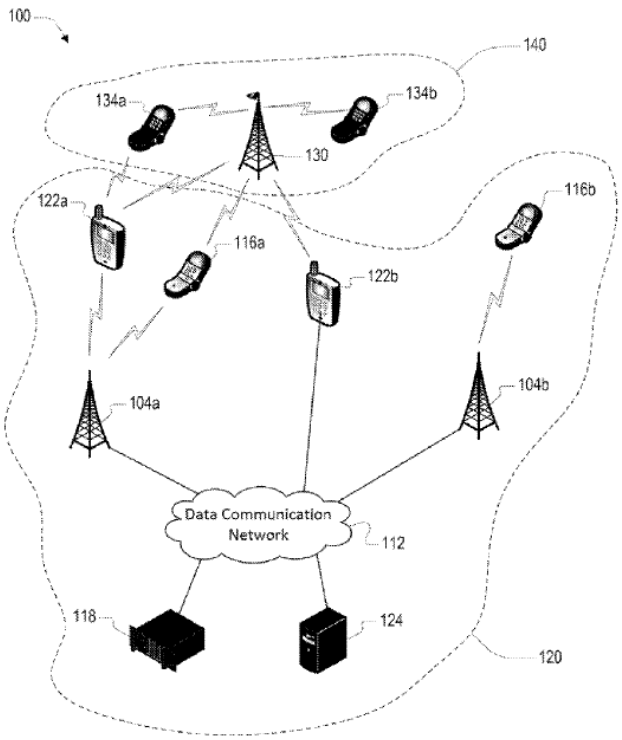
señal ilegal, sincronizando el jammer inteligente con la fuente de señal no autorizada y retransmitiendo una señal de interferencia.

Un sistema para detectar y atascar una red inalámbrica comprende un primer bloqueador inteligente y un servidor inteligente de detección y atasco acoplado al primer bloqueador inteligente."

El invento comprende la forma o metodología que se necesita para realizar el jamming y el sistema que comprende el uso de un servidor, base de datos dónde se registren las emisiones licenciadas, un core encargado del procesamiento y análisis de la emisión, un equipo jammer para la transmisión de la señal de interferencia, incluyendo otro jammer que opera como un equipo que monitorea la emisión no afectada como referencia.

En la siguiente figura tomada de [25] muestra el despliegue del sistema jamming.

Figura 6 Sistema de jamming inteligente[15]

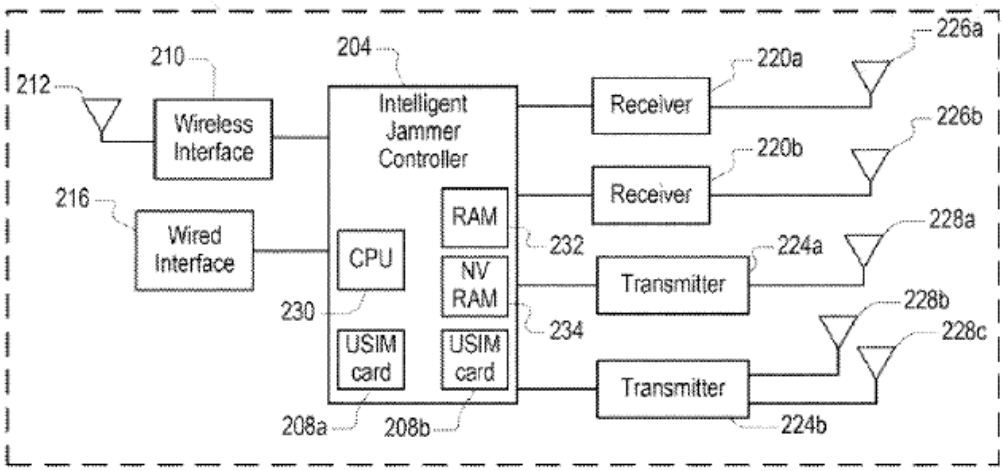


[15] Figura tomada de [25]

En la imagen de la figura 6 se puede identificar que los equipos jammer (122 a-b) que se soporta en las redes móviles o conexión directa por ethernet para acceder a internet y acceder a los equipos de servidores de jamming (124) y al sistema core que controla las operaciones de los jammers (118), el sistema no licenciado (140) y el transmisor de emisiones clandestinas (130). Otros elementos de la imagen resultan ser actores secundarios como usuarios del sistema licenciado y no licenciado.

En la figura 7 muestra los componentes esenciales que hacen parte del dispositivo de bloqueo de frecuencias que utiliza el sistema de jamming. Cuenta con dualidad en interfaces de comunicación inalámbrica y alámbrica para el acceso hacia internet, un equipo compuesto por un sistema embebido para el procesamiento y gestión del jamming, y varios puntos de transmisión y recepción para realizar operaciones de jamming o de monitoreo.

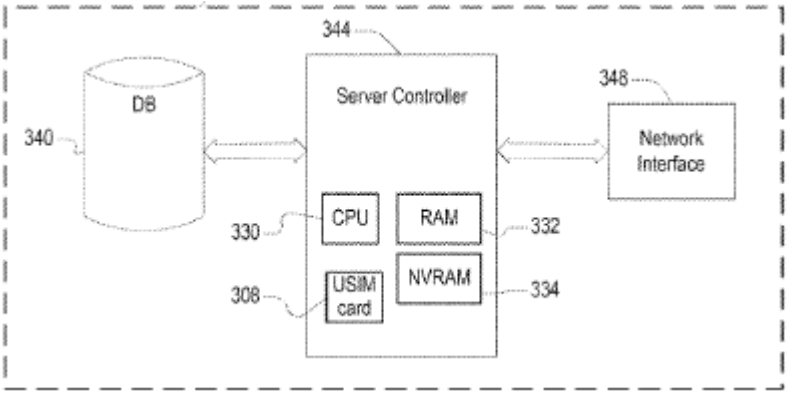
Figura 7 Arquitectura que compone el jammer inteligente patentado[16]



[16] Figura tomada de [25]

La arquitectura que posee la patente y la descrita en la figura 3 del S-Jammer, resultan ser similares en aspectos generales, como la dualidad de transmisor y receptor para múltiples funciones y el sistema embebido propio que brinda más autonomía en el momento de gestionar sus acciones de jamming.

Figura 8 Arquitectura del Servidor para el Jamming Inteligente[17]



El servidor para las operaciones de jamming propone unas características de dualidad en el modo de resolver las peticiones por parte de cada jammer conectado, se puede dimensionar como un recurso físico robusto o de una terminal móvil más ligera y flexible.

En un sentido más general, la Figura 8 nos muestra que el servidor de jamming cuenta con interfaces de red para conexión alámbrica e inalámbrica, usando las redes móviles para el acceso hacia internet del mismo modo que los dispositivos jammer mencionados anteriormente.

[17] Imagen tomada de [25]

Otros aspectos de consideración

La patente contiene además del sistema de jamming, otra componente importante como la metodología necesaria para realizar los ataques de jamming en conjunto al sistema de jamming. La metodología comprende la detección de la señal no licenciada, el método para enviar la información de la señal no licenciada desde el dispositivo jammer que realiza el trabajo de monitoreo hacia el servidor de jamming, los métodos para la configuración en tiempo y frecuencia para la operación del dispositivo jammer, la diversidad de protocolos para la comunicación alámbrica e inalámbrica de todo el sistema, la diversidad de protocolos y modulaciones que pueda tener la señal de la emisión

En sus reivindicaciones, los inventores apelan a que el uso del sistema y su metodología no solo están enfocados en aquellas emisiones ilegales que se soporten en la telefonía móvil, atacando los enlaces de Down Link (DL) y Up Link (UL), si no también cualquier desarrollo de software sobre el servidor que pueda soportar esta arquitectura, sus posibles variaciones, e incluso, el método para realizar el jamming en tiempo y frecuencia.

4.2 Análisis comparativo entre invención de la patente y S-Jammer

En la tabla 4 se muestra un resumen de los aspectos más importantes encontrados entre la patente 20140206279A1 y el S-Jammer de RadioGIS. Aspectos como el uso de más de un dispositivo jammer y la conexión en red, juegan un papel muy importante para las dos soluciones en particular. Debido a la complejidad de las tecnologías de objeto de ataque, es imprescindible el uso de soporte electrónico, mejorando el performance de las técnicas de jamming.

Tabla 4 Análisis técnico entre S-Jammer y patente 20140206279A1

Desarrollo o invención	**Aparato o dispositivo jammer**	**Técnica de jamming**	**Servicios o tecnologías a ser objeto de ataque**	**Configuración y operación en red**	**Nivel de inteligencia en el jamming**
Patente 20140206279A1	2 equipos para realizar bloqueo	Si	LTE, CDMA, GSM	Centralizado en un servidor de jamming	Básica, limitada las técnicas de jamming presentadas
S-Jammer	2 equipos para realizar bloqueo	Básica por el momento	Radiodifusión Sonora y TDT	Requiere definir la arquitectura	Sin definir

Con respecto a las oportunidades que posee S-Jammer, existe una gran barrera en el uso de la distribución centralizada que reivindica los inventores de la patente. Pero existe oportunidades en la diversidad de objetivos de ataque que no están presente en el texto de la patente.

Continuando con los aspectos poco favorables, se incluye toda forma y medio para la ubicación del Jammer y el servidor, incluyendo entre otros, vehículos, globos aerostáticos, drones y otros vehículos no tripulados.

En resumen, para dar respuesta a las preguntas que motivaron la realización de este trabajo se tiene las siguientes apreciaciones y conclusiones:

- Evidentemente existen más técnicas de jamming que pueden ser implementadas para mejorar el prototipo S-Jammer, pero están condicionadas a la complejidad del servicio o tecnología a ser objeto de ataque y qué tan protegidas están contra los ataques de jamming. Para tener éxito en el jamming el uso de tácticas óptimas es fundamental. Se recomienda a los

desarrolladores del bloqueador indagar más sobre los protocolos, las modulaciones, y las vulnerabilidades que presentan para ser aprovechadas al máximo.

- La patente 20140206279A1 es un claro ejemplo de que ya existe un precedente grande en el campo del jamming. Como punto de referencia, los desarrolladores del S-Jammer deben continuar con la revisión del texto [25], para encontrar más aspectos técnicos que no se tuvieron en cuenta en el análisis. No obstante, se recomienda ampliar las referencias con el fin

- Existen muchas oportunidades de patente para RadioGIS según la revisión bibliográfica realizada. Las cuales están descritas en el apartado de recomendaciones técnicas de este capítulo. Se proponen, además, nuevas capacidades a ser tenidas en cuenta para la mejora del equipo S-Jammer.

4.3 Recomendaciones técnicas para patentar

Arquitectura de la Red de jammers

El dispositivo debe contar con una arquitectura descentralizada y operar de manera más flexible. Para esto, los jammers deberán tener la capacidad de operar coordinadamente con jerarquías de maestros y esclavos, de modo matricial, interacciones entre vecinos, entre otros. La finalidad es la de poder transmitir en distintas bandas al mismo tiempo, evitar al máximo el Hopping que presentan las emisiones basadas en Multiplexación por División de Frecuencias Ortogonales (OFDM), especialmente los sistemas de TDT.

Para lo anterior se recomienda analizar a profundidad la patente *“Method and aparathus for distributed signal processing among internetworked wireless integrated network sensors (WINS)*” [26]. La cual expone un método para realizar la distribución en red entre sensores simples para IoT.

Servicios a ser objeto de ataque

Como punto de partida, el dispositivo cuenta con las capacidades para inhibir señales de radiodifusión sonora FM y TDT soportado por OFDM. En el caso de la televisión digital, se cuenta con una diversidad de patentes para la protección de interferencias y técnicas anti-jamming. En tal caso, para realizar jamming más elaborado, se requiere proponer métodos para evitar el Hopping y asegurar la degradación de la recepción de la transmisión.

Se propone también al grupo de investigación, analizar la posibilidad de explotar al máximo la potencialidad que tiene el uso de USRP, para apuntar a servicios de nueva generación como el Acceso Múltiple por División de Bandas (BDMA) y el Acceso Múltiple por División de Tiempo con Saltos Lentos de Frecuencia (SFH-TDMA) [27], las bases para las comunicaciones de Quinta Generación 5G [28].

Diversidad en Técnicas de jamming

El dispositivo bloqueador de frecuencias debe contar con una variedad de técnicas, de las cuales, pueden basarse en los tipos descritos en el capítulo 2 o una variante de ellos.

Usar más de una variedad de jamming deriva en una nueva adaptación de los recursos de hardware disponible. Filtros y arreglos de antenas, así como el rango de frecuencias que pueda soportar el amplificador de potencia, deben presentar una mejora en el diseño. Además, se recomienda adaptar otros modelos y técnicas que puedan ser útiles, para darles un uso más innovador para las tareas de bloqueo de emisiones ilegales.

REFERENCIAS

[1] D. C. Schleher, Electronic Warfare in the Information Age, Artech House,, 1999.

[2] S. S. Bellardo J, «802.11 denial-of-service attacks: Real vulnerabilities and practical solutions,» *Proceedings of the 12th Conference on USENIX Security Symposium,* pp. 15 - 28, 2003.

[3] MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES, Resolución 2774, Bogotá: 2013.

[4] 5G Americas, El bloqueo de señales de servicios móviles en America Latina, 2017.

[5] J. G. C. V. y. A. F. T. C. M. D. Bravo Obando, «Diseño e implementación de un prototipo inhibidor de señales de celular para un salón de clases,» *Revista de Ingeniería y Región,* nº 11, pp. 73-74, 2014.

[6] A. Jisrawi, GSM-900 Mobile JAMMER, Jordan University os Science and Tecnology, Electrical Engineering Department, 2006.

[7] A. C. Valencia, Estudio de sistemas de detección e inhibición para emisores celulares presentes en redes comerciales, Medellín, 2013.

[8] B. M. P. Morales, Diseño, Simulación e Implementación de una predictor de pulsos de radar para Guerra Electrónica, Universidad de Alcalá, 2015.

[9] R. Poisel, Modern communications jamming principles and techniques, Artech House, 2004.

[10] Sistema de Observación y Prospectiva Tecnológica SOPT, La Guerra Electrónica en España, Imprenta del Ministerio de Defensa, 2009.

[11] B. S. Col. István Resperger, «HYBRID WARFARE OR THE EVER CHANGING FACE OF WAR,» *Defense Review,* vol. 144, nº 2016/1, pp. 71 - 89, Enero 2016.

[12] P. Alison Lawlor Russell, «Strategic Anti-Access/Area Denial in Cyberspace,» *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace,* pp. 153-168, Mayo 2015.

[13] L. W. Y. Z. y. M. W. L. Wang, «Radar and Jammer Power Allocation Strategy Based on Matrix,» *Procedia Computer Science,* nº 107, p. 478 { 483, 2017.

[14] A. L. Q. Y. Kanika Grover, «Jamming and anti-jamming techniques in wireless networks: a survey,» *International Journal of Ad Hoc and Ubiquitous Computing ,* vol. 17, nº 4, pp. 197-215, 2014.

[15] Agencia Nacional de Espectro, «Cuadro Nacional de Atribuciones de Bandas de Freuencias,» 2017. [En línea]. Available: http://cnabf.ane.gov.co/cnabf/. [Último acceso: 16 Octubre 2017].

[16] O. H. M. J. P. Santos D. Tania, Caracterización de un sistema de emisiones clandestinas basado en tecnología SDR, Bucaramanga: Universidad Industrial de Santander, 2017.

[17] Shephard Press Ltd, Electronic Warfare Handbook, 2008.

[18] L. GHERMAN, «ELECTRONIC WARFARE IN INFORMATION AGE,» *Review of the Air Force Academy,* vol. 27, nº 3, pp. 27-30, 2014.

[19] USA, DEPARTMENT OF DEFENSE, CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS, USA: USA, DEPARTMENT OF DEFENSE, Abril 2017.

[20] E. E. B. H. J. &. F. C. J. A. Cadena Muñoz, « Gestión del espectro radioeléctrico en Colombia,» *Revista Tecnura,* vol. 19, nº 45, pp. 159-173, 2015.

[21] M. G. Robert Koch, «Blackout and Now? Network Centric Warfare in an Anti-Access Area-Denial Theatre,» *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace,* pp. 169 - 184, Mayo 2015.

[22] J. F. D. Bejarano, APLICACIÓN DE TÉCNICAS ANTI-JAMMING A UN SISTEMA DE COMUNICACIONES CONVENCIONAL PARA SU

EXPLOTACIÓN EN ENTORNOS TÁCTICOS,, Madrid, 2012.

[23] M. I. a. S. V. K. Konstantinos Pelechrinis, «Denial of Service Attacks in Wireless Networks: The Case of Jammers,» *IEEE COMMUNICATIONS SURVEYS & TUTORIALS,* vol. 13, nº 2, pp. 245 - 257, 2011.

[24] C. R. M. d. Sousa, INTERFERIDORES DE GPS: ANÁLISE DO SISTEMA E DE POTENCIAIS FONTES DE INTERFERÊNCIA, Instituto Militar de Engenharia, 2005.

[25] J. Y. y. E. G. Chaz Inmendorf, «METHOD AND SYSTEM FOR INTELLIGENT JAMMING SIGNAL GENERATION». USA Patente US 20140206279A1, 24 July 2014.

[26] L. D. G. W. J. K. F. N. e. a. Davis C. Gelvin, «Method and aparathus for distributed signal processing among internetworked wireless integrated network sensors (WINS)». USA Patente US 6832251B1, 14 December 2004.

[27] T. Y. M. S. E. F. T. Kunihiro, «BDMA testbed-configuration and performance results,» *Vehicular Technology Conference 1999 IEEE 49th,* vol. 3, nº ISSN 1090-3038, pp. 1836-1840, 1999.

[28] K. H. H. S. Y. Kamio, «Adaptive-modulation/SFH/TDMA system for high quality and high capacity microcellular systems,» *Vehicular Technology Conference, 'Mobile Technology for the Human Race', IEEE 46th,* vol. 3, pp. 487-491, January 1996.

BIBLIOGRAFIA

A. L. Q. Y. Kanika Grover, «Jamming and anti-jamming techniques in wireless networks: a survey,» International Journal of Ad Hoc and Ubiquitous Computing , vol. 17, nº 4, pp. 197-215, 2014.

L. GHERMAN, «ELECTRONIC WARFARE IN INFORMATION AGE,» Review of the Air Force Academy, vol. 27, nº 3, pp. 27-30, 2014.

5G Americas, El bloqueo de señales de servicios móviles en America Latina, 2017.

J. Y. y. E. G. Chaz Inmendorf, «METHOD AND SYSTEM FOR INTELLIGENT JAMMING SIGNAL GENERATION». USA Patente US 20140206279A1, 24 July 2014.

M. I. a. S. V. K. Konstantinos Pelechrinis, «Denial of Service Attacks in Wireless Networks: The Case of Jammers,» IEEE COMMUNICATIONS SURVEYS & TUTORIALS, vol. 13, nº 2, pp. 245 - 257, 2011.

USA, DEPARTMENT OF DEFENSE, CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS, USA: USA, DEPARTMENT OF DEFENSE, Abril 2017.