ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA ELECTRONICA EN TELECOMUNICACIONES

ASPECTOS TÉCNICOS Y LEGALES PARA LA APLICACIÓN DE SISTEMAS DE INTERFERENCIA PARA TELÉFONOS CELULARES CON TECNOLOGÍA GSM EN EL ECUADOR

DIEGO HERNÁN TAPIA PAREDES

Sangolquí – Ecuador

2009

CERTIFICACIÓN

Certificamos que el presente proyecto de grado titulado "ASPECTOS TÉCNICOS Y LEGALES PARA LA APLICACIÓN DE SISTEMAS DE INTERFERENCIA PARA TELÉFONOS CELULARES CON TECNOLOGÍA GSM EN EL ECUADOR", ha sido desarrollado en su totalidad por el Sr. Diego Hernán Tapia Paredes con C.I. 171118677-3, como previo requisito para la obtención del título de Ingeniero Electrónico, bajo nuestra dirección.

Ing. Carlos Romero	Ing. Gonzalo Olmedo
DIRECTOR	CODIRECTOR

RESUMEN

El presente trabajo estudia los dispositivos inhibidores de señales de radiofrecuencias o también llamados jammers, que tiene como objetivo atacar las redes de la telefonía celular ubicadas en la banda PCS (Personal Communications Services).

Después de presentar una breve historia acerca de la telefonía móvil y conceptos teóricos globales concernientes a la radiofrecuencia y la tecnología GSM, se realiza un análisis entre las distintas técnicas de jamming y los diferentes tipos de jammers, con el fin de elegir la mejor opción para la aplicación.

Una vez elegidos la técnica de jamming y el tipo de jammer se muestra el diseño por etapas del dispositivo y su correspondiente simulación. Se explica brevemente el funcionamiento y los resultados obtenidos.

Por último se estudia la legalidad que existe para la instalación de estos dispositivos; y al no tener ninguna ley que contemple el uso, se propondrá hacer una modificación en el reglamento actual, para legalizar la utilización de los mismos.

DEDICATORIA

Este trabajo esta dedicado especialmente a Dios por protegerme y guiarme todos los días de mi vida.

A mi Ita, aquella viejecita que con sus bendiciones, caricias y bondad, me ha enseñado a ser noble y humilde, agachar la cabeza solo ante Dios y ha levantarla ante todos los mortales.

A mi Papi Hernán, hombre sabio, amigo y apoyo; que con sus consejos, palmadas, abrazos y cuidados, hacen de mi un hombre de principios y de luchas.

A mi Mami la señora Marcelita, por dedicarme lo mejor de sus días, por creer siempre en mi, por regalarme con su mirada fe y esperanza, y revelarme que los sueños son alcanzable si se pone corazón en ellos.

A mi hermana Nena, que son sus locuras, carácter y fuerzas, me ha enseñado a ver la vida de una forma diferente.

A mi ángel de la guarda Santiago, amigo incondicional, que me demostró que la verdadera felicidad no está en la cima de la montaña, sino en el camino a ella.

A mi hermana Sol, que con su juventud y palabras de aliento, me enseña que no estoy envejecido sino madurando.

A mi casi hija Dome, que esta ahí cuando más la necesito, que con sus travesuras me recuerda cada día que llevo un niño dentro.

A mi compañera sentimental, por regalarme lo mejor de sus sentimientos y por ese apoyo incondicional en mis locuras y sueños.

AGRADECIMIENTO

Agradezco a Dios, por darme la fuerza, el carácter y la paciencia para saber elegir con sabiduría la carrera universitaria que escogí.

A mi universidad, por acogerme durante todo este tiempo en sus aulas, así como por enseñarme que no solo basta con tener los conocimientos teóricos sino no van acompañados de buenos valores.

A profesores y en especial a mi Director y Codirector del proyecto de grado, por haberme brindado todos sus conocimientos y de esta manera cumplir con uno de mis sueños y objetivos que tengo en la vida.

A mis amigos y compañeros, que con su apoyo supe salir adelante y vencer obstáculos que se presentaban en el camino.

PRÓLOGO

La telefonía móvil se ha convertido en la forma de comunicación más importante para los seres humanos. Tal es así que el celular es el invento con el cual no se puede vivir según una encuesta realizada el 28 de abril del 2008 por la empresa Bloq psicofxp. Este aparato es fácil de adquirir y se halla al alcance de todos, ya que en el mercado se puede encontrar de diferentes precios, marcas y tamaños.

El uso que se les dé a los mismos, depende directamente de los propietarios, no siempre los celulares son utilizados para beneficios personales; tal es así que en la actualidad la delincuencia utiliza estos aparatos para tener comunicación desde el interior y exterior de los lugares donde van a delinquir. Por tal motivo desde hace algún tiempo se prohíbe el uso de celulares en determinados lugares, como bancos, cárceles e instituciones gubernamentales, pero solo con letreros o advertencias por parte de la gente que labora en esos lugares.

Algunas empresas e instituciones se han visto obligadas a diseñar e implementar sistemas bloqueadores de señales celulares (jammers), para proporcionar mayor seguridad; por tal razón deben ser motivos de análisis y estudio para conocer el funcionamiento, aplicaciones y usos que se les puede dar a los mismos.

Por otra parte, se halla la legalidad en el uso de estos dispositivos, ya que es prohibido interferir cualquier frecuencia según las actuales leyes y reglamentos de telecomunicaciones, pero a su vez se encuentra de por medio la seguridad que se debe brindar a la ciudadanía, como contempla la actual constitución ecuatoriana, siendo así este un tema de discusión, y por tal motivo de análisis sobre el uso de jammers.

ÍNDICE DE CONTENIDO

CAPÍTULO I:
INTRODUCCIÓN

CAPÍTULO II:
DESCRIPCIÓN DE JAMMER

CAPÍTULO III:

SIMULACIÓN DEL FUNCIONAMIENTO DE LAS DIFERENTES ETAPAS DEL JAMMER Y PRESENTACIÓN DE RESULTADOS

CAPÍTULO IV:

MARCO REGULATORIO RESPECTO A LA RESTRICCIÓN DEL SERVICIO CELULAR EN SITIOS DE SEGURIDAD

CAPÍTULO V:

CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE TABLAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

ÍNDICE DE FIGURAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

GLOSARIO DE TÉRMINOS

RF.- Radiofrecuencia

LOS.- Line of Sight

ISI.- Intersymbol interferente

SNR.- Signal-to-Noise Ratio

OLOS.- Out-of-Line-of-Sight

ITU.- International Telecommunication Union

IEEE.- Institute of Electrical and Electronics Engineers

EW.- Electronic Warfare

EA.- Electronic Attack

ES.- Electronic Support

EP.- Electronic Protection

AE.- Apoyo Electronico

JSR.- Jam-to-Signal Ratio

PSR.- Packet Delivery Ratio

PDR.- Packet Delivery Ratio

BER.- Bit Error Rate

SER.- Symbol Error Rate

SIR.- Signal-to-Interference Ratio

PE.- Protección Electrónica

AJ.- Antijam

DSSS.- Direct Sequence Spread Spectrum

CDMA.- Code Division Multiple Access

FHSS.- Frequency Hopping Spread Spectrum

GSM.- Global System for Mobile Communications

LPD.- Low Probability of Detection

LPI.- Low Probability of Intercept

FH.- Frequency Hopping

FFH.- Fast Frequency Hopping

SFH.- Slow Frequency Hopping

BBN.- Broad Band Noise

PBN.- Partial-Band Noise

NBN.- Narrow-Band Noise

ST.- Single-Tone

MT.- Multiple-Tone

MTS.- Mobile Telephone System

IMTS.- Improved Mobile Telephone System

FCC.- Federal Communications Commission

ARTS.- American Radio Telephone Service

AMPS.- Advanced Mobile Phone System

TDMA.- Time Division Multiple Access

CDMA.- Code Division Multiple Access

FDMA.- Frequency Division Multiple Access

USDC.- U.S. Digital Cellular

IDEN.- Integrated Digital Enhanced Network

PDC.- Personal Digital Communications

GPRS.- General Packet Switching Service

EDGE.- Enhanced Data Rates for GSM Evolution

BSS.- Base Station Subsystem

NSS.- Network and Switching Subsystem

OSS.- Operational Support Subsystem

BSC.- Base Station Controllers

BTS.- Base Transceiver Station

MSC.- Mobile Switching Center

SIM.- Subscriber Identity Module

GMSK.- Gaussian Minimum Shift Keying

PCS.- Personal Communications Services

VHF.- Very High Frequency

UHF.- Ultra High Frequency

VCO.- Voltage Controlled Oscilator

MMIC.- Monolithic Microwave Integrated Circuits

CONATEL.- Consejo Nacional de Telecomunicaciones

SENATEL.- Secretaria Nacional de Telecomunicaciones

SUPTEL.- Superintendencia de Telecomunicaciones

CAPÍTULO I

INTRODUCCIÓN

La telefonía celular nace de la necesidad del ser humano por comunicarse; y, en un mundo que cada día evoluciona es menester que la tecnología que avanza a pasos agigantados, brinde mayor agilidad en la comunicación persona a persona, apoyando al ejercicio de la economía mundial que se ve obligada a generar mayores expectativas dentro de un mundo globalizado.

Así el primer sistema de comunicación móvil apareció en 1921, cuando el Departamento de Policía de Detroit – EEUU instaló radios emisores y receptores en sus vehículos. Estos equipos eran grandes, torpes y agotaban las baterías del auto, pero se probaron sus beneficios una y otra vez.

Al paso de los años los avances en el diseño de los equipos electrónicos, ha permitido una evolución de los teléfonos móviles, los cuales se han desarrollado tecnológicamente y se hicieron más fáciles de usar.

El auge de las comunicaciones móviles celulares ha revolucionado el concepto de la telefonía de diversas maneras. Ante todo, gracias a la movilidad de los usuarios, ya no llaman a un sitio sino a una persona. Los pequeños aparatos portátiles han liberado a los usuarios del cordón que ataba los teléfonos a un emplazamiento geográfico y les permiten estar al alcance en todo momento y en cualquier lugar.

1.1. Historia de la telefonía móvil

La telefonía móvil se remonta desde el año de 1947 donde se comienza a desarrollar ideas que permitían el uso de teléfonos móviles usando "células" capaces de identificar un usuario en cualquier punto desde donde se generara la llamada. Sin embargo, la limitada tecnología que existía en ese momento obligó a los científicos a posponer la implementación de dichas ideas [1].

Dos años después fue presentado por primera vez en los Estados Unidos la telefonía móvil en una versión analógica, formada por una estación base de alta potencia y un receptor, los cuales se coloraron en lo alto de montañas y torres. Este servicio tenía una cobertura de aproximadamente 30 millas a la redonda y funcionaba como una comunicación *half-duplex*, convirtiéndose así en el primer estándar de telefonía móvil conocido como *MTS (Mobile Telephone System)*. A principio de los 50 se duplicó el número de canales destinados a la telefonía móvil, reduciendo de 120 Khz. a 60 Khz. logrando una comunicación *full-duplex*; en ese entonces los sistemas de telefonía móvil operaban sólo en el modo manual, un operador del teléfono móvil manejaba cada llamada desde y hacia cada unidad móvil [2].

En 1964, los sistemas selectores de canales automáticos fueron colocados en los sistemas de telefonía móvil, esto eliminó la necesidad de la operación oprimir-para-hablar *(push-to-talk)* y les permitía a los clientes marcar directamente sus llamadas, sin la ayuda de una operadora. El *MTS* (Sistema de Telefonía Móvil) usaba los canales de radio de FM para establecer enlaces de comunicación, entre los teléfonos móviles y los transceptores de estación de base centrales, los cuales se enlazaban al intercambio de móviles local por medio de las líneas telefónicas metálicas normales, y cada canal opera similarmente a una línea compartida. Cada canal se podía asignar a varios suscriptores, pero sólo un suscriptor puede utilizarlo a la vez. Si el canal preasignado está ocupado, el suscriptor debía esperar hasta que se desocupe, antes de hacer o recibir una llamada.

En el año de 1971, la demanda creciente en el espectro de frecuencia de la telefonía móvil

provocó la saturación, obligando a buscar un modo de proporcionar una eficiencia del espectro de mayor frecuencia. En este año, AT&T hizo una propuesta sobre la posibilidad de proporcionar respuesta a lo anterior, comenzando a delinear el principio de la radio celular. En este mismo año en Finlandia se lanza la primera red pública exitosa, de telefonía móvil, llamada la red *ARP (Address Resolution Protocol)*. Dicha red es vista como la Generación 0 (0G), estando apenas por encima de redes propietarias y redes de cobertura local [1].

El Dr. Martín Cooper conocido como "el padre de la telefonía celular" es considerado el inventor del primer teléfono portátil, ya que en el año de 1973 siendo gerente general de sistemas de Motorola realizó una llamada a sus competidores de *AT&T* desde su móvil celular, transformándose en la primera persona en hacerlo.

En el año de 1977 los móviles celulares se hacen públicos, dando así comienzo a las pruebas en el mercado. La ciudad de Chicago fue la primera en comenzar con 2000 clientes. Eventualmente otras líneas de prueba aparecieron en Washington D.C. y Baltimore, si bien los Americanos eran los pioneros en la tecnología, los primeros sistemas comerciales aparecieron en Tokio, Japón por la compañía NTT, en 1979. [1]

Sin embargo, fue hasta 1983 cuando la telefonía celular comenzó a crecer exponencialmente *AMPS (Advanced Mobile Phone System)*, este estándar originalmente ocupaba 40 Mhz de ancho de banda de los 800 Mhz [2] .

La telefonía móvil tuvo gran aceptación, por lo que a los pocos años de implantarse se empezó a saturar el servicio. Por tal motivo hubo la necesidad de desarrollar e implementar otras formas de acceso múltiple al canal, y transformar los sistemas analógicos a digitales, para darle cabida a más usuarios. Para separar una etapa de la otra a la telefonía celular, se ha categorizado por generaciones, a continuación se describen cada una de ellas.

1.1.1 Primera generación 1G

La primera generación correspondió a la telefonía analógica, empleando el concepto de sistemas celular, que dividía el territorio en células y utilizaba una técnica de acceso al medio conocida como FDMA *(Frequency Division Multiple Access)* / FDD *(Frecuency Division Duplex)* que era una técnica de acceso múltiple por división de frecuencia y dos frecuencias portadoras distintas para establecer la comunicación entre el transmisor y el receptor [3].

Se dice que Estados Unidos fue el pionero en cuando a telefonía móvil se refiere, pero en 1978 se desarrolló la primera red celular en Bahrein que estaba constituida por un total de 250 usuarios que se comunicaban en la banda de 400Mhz. Al ver que eso funcionaba, ese mismo año la empresa estadounidense *AT&T* se centro en el estudio de esta tecnología y un año más tarde desarrolló el que sería el primer estándar de la telefonía móvil, *AMPS (Adavanced Phone Mobile System)* [3].

AMPS tiene su principio en los años 70 y no alcanzó su éxito comercial hasta 1983 debido a regulaciones inadecuadas y pólizas industriales. Aunque otros estándares fueron creados a principio de los años 80, *AMPS* ya se había quedado obsoleto para ese entonces. Todo esto se debe a que *AMPS* fue diseñado en 1971 cuando todavía no había switches digitales, los microprocesadores no tenían ninguna propiedad en común e incluso la troncal de los sistemas de telefonía cambió completamente desde el principio de la década hasta. *AMPS* es un sistema con una compleja y cara red arquitectura en el cual toda la inteligencia fue situada en una central de conmutación de sistemas. A pesar de todo esto *AMPS* tuvo un gran éxito comercial [3].

NAMPS (Narrowbadamps) es una variante de *AMPS* desarrollada por Motorola a principios de los 90. El espacio de canal es reducido, lo que incrementa la eficiencia en frecuencia en una factor 3. Este estándar es compatible con *AMPS* así que hace posible que se siga usando las redes existentes y la infraestructura instalada. El uso de *NAMPS* fue limitado porque la reducción del canal incrementó el precio de los terminales. Las redes de

este tipo estaban en uso a finales de 1996 con más de un millón de subscriptores, sin embargo la mayoría de las redes son combinadas *AMPS/NAMPS* en las que solo una pequeña proporción de los canales fueron en realidad convertidos a *NAMPS* [3]. Los servicios que proporcionan los sistemas de primera generación son:

- Transmisión de voz analógica.
- Transmisión de datos, equipando al teléfono móvil con un módem adecuado.
- Servicios suplementarios telefónicos, tales como: contestador automático, llamada en espera, asistencia de operadora, información de tarifación, etc.

1.1.2 Segunda generación 2G

La 2G a diferencia de la primera se caracterizó por ser digital. El sistema 2G utiliza protocolos de codificación más sofisticados y son los sistemas de telefonía celular usados en la actualidad. Las tecnologías predominantes son: TDMA (*Time Division Multiple Access*), GSM (*Global System for Mobile Communications*), IS-136 conocido también como TIA/EIA-136 o ANSI-136, CDMA (*Code Division Multiple Access*) y PDC (*Personal Digital Communications*), éste último utilizado en Japón.

Los protocolos empleados en los sistemas 2G soportan velocidades de información más altas para voz, pero limitados en comunicaciones de datos. Se pueden ofrecer servicios auxiliares tales como datos, fax y SMS (*Short Message Service*). La mayoría de los protocolos de 2G ofrecen diferentes niveles de encriptación. En los Estados Unidos y otros países se le conoce a 2G como PCS (*Personal Communications Services*).

- **Generación 2.5G**

Muchos de los proveedores de servicios de telecomunicaciones (*carriers*) pasaron primero por las redes 2.5G antes de entrar masivamente a 3G. La tecnología 2.5G era más rápida y más económica para actualizar a 3G.

La generación 2.5G ofrecía características extendidas para brindar capacidades adicionales que los sistemas 2G tales como GPRS (*General Packet Radio System*), *HSCSD* (*High Speed Circuit Switched Data*), EDGE (*Enhanced Data Rates for Global Evolution*), IS-136B, IS-95B, entre otros. Los *carriers* europeos y los de Estados Unidos se unieron a 2.5G en el 2001. Mientras que Japón fue directo de 2G a 3G también en el 2001 [4]. En general los sistemas de segunda y media generación operan de acuerdo a las especificaciones de la siguiente tabla:

Tabla 1.1. Bandas de Frecuencias de los Sistemas de Segunda y Media Generación

ESTANDAR	BANDAS DE FRECUENCIAS (MHZ)	VELOCIDADES DE TRANSMISIÓN (kbps)
GPRS / EDGE	800 / 900 / 1800 / 1900	115-384
IS-95B / IS-95C	800 / 1900	115-144

Los principales beneficios que la tecnología 2.5G proporciono de forma más eficiente son:

- Mayor velocidad de transmisión.
- Posibilidad de realizar/recibir llamadas de voz mientras se está conectado o utilizando cualquiera de los servicios disponibles con estas tecnologías.
- Conectividad IP directa, no necesita del establecimiento de llamada.
- Modo de conexión permanente ("*always-on*")
- Utilización más eficiente de los recursos de red al basarse en canales compartidos por varios usuarios y no dedicados (modelo GSM).
- Modo de transmisión asimétrico, más adaptado al tipo de tráfico de navegación HTML39 o WML40 (un terminal GPRS 4+1 tendrá cuatro veces mayor capacidad de transmisión de bajada que de subida).

1.1.2 Tercera generación 3G

La 3G es tipificada por la convergencia de la voz y datos con acceso inalámbrico a Internet, aplicaciones multimedia y altas transmisiones de datos. Los protocolos empleados en los sistemas 3G soportan altas velocidades de información enfocados para aplicaciones mas allá de la voz tales como audio (MP3), video en movimiento, video conferencia y acceso rápido a Internet.

Los sistemas 3G alcanzarán velocidades de hasta 384 Kbps permitiendo una movilidad total a usuarios viajando a 120 kilómetros por hora en ambientes exteriores y alcanzará una velocidad máxima de 2 Mbps permitiendo una movilidad limitada a usuarios caminando a menos de 10 kilómetros por hora en ambientes estacionarios de corto alcance o en interiores. Esta tercera generación está representada principalmente por dos estándares, UMTS (*Universal Mobile Telephone Service*)a nivel europeo e IMT-2000 (*International Mobile Telephone*) a nivel estadounidense.

UMTS evoluciona para integrar todos los servicios ofrecidos por las distintas tecnologías móviles, inalámbricas y satelitales, proporcionando mayor capacidad y altas velocidades de transmisión de datos.

Entre las principales características del sistema UMTS, se tienen:

- Velocidades máximas teóricas de 2 Mbps.
- Para la facturación existen tres categorías dependiendo del tipo de información que se transmita que puede ser: voz, datos o información en tiempo real, las mismas que dependerán de los requerimientos de los servicios de la red UMTS.
- En estos sistemas el ancho de banda disponible para las transmisiones variará de acuerdo al tipo de comunicación móvil utilizado.

El estándar IMT2000 es el nuevo sistema de comunicaciones telefónicas móviles de tercera generación y se caracteriza por suministrar el acceso inalámbrico a la infraestructura global de telecomunicaciones, mediante sistemas terrestres y satelitales, atendiendo usuarios fijos y móviles de las redes públicas y privadas. Otra de las características de IMT-2000 es la alta calidad en las comunicaciones, terminales pequeños con capacidad de ser usados en todo el mundo a través del *roaming* internacional, capacidad de ofrecer servicios multimedia a los usuarios móviles y terminales que los soporten [5].

Los sistemas de tercera generación presentan los siguientes servicios:

- Aplicaciones de audio/video en tiempo real, tales como: videoteléfono, videoconferencias interactivas, audio y música; y aplicaciones comerciales multimedia especializadas, inclusive telemedicina y supervisión remota de seguridad.
- Provisión de capacidad que permita nuevos servicios de voz y datos más avanzados que las tecnologías pre-IMT-2000 (celulares y PCS actuales).
- Disponibilidad para los usuarios móviles de una gama de servicios vocales y no vocales, entre ellos datos por paquetes y servicios multimedios.
- Servicios basados en la movilidad, como búsqueda de establecimientos o recepción de anuncios de acuerdo a la localización del usuario.
- Comercio electrónico, compras en línea desde el teléfono.
- *Roaming* internacional, portabilidad de servicios, tarificación de acuerdo a la zona de uso del móvil, acceso a directorios, etc.

1.1.3 Cuarta generación 4G

Los sistemas de cuarta generación, en esencia son redes inalámbricas ultra rápidas , la cual deberá explorar nuevas bandas de frecuencias en torno a 5 GHz y desarrollar nuevas técnicas de procesamiento de señal para aprovechar más eficientemente el espectro radioeléctrico. Es un sistema capaz de aprovechar todo tipo de tecnologías diferentes como:

- El protocolo IP, como la parte de transporte de la Red Universal Multimedia (probablemente en esta red no se usen más números de abonado, sino direcciones de red).
- La tecnología de antenas adaptivas e inteligentes (que permiten reutilizar más densamente las frecuencias en una red celular).
- La tecnología de modulación/ transmisión inalámbrica de multicanalización en frecuencias con portadoras ortogonales OFDM46 (para lograr un eficiencia espectral óptima).
- La tecnología de radio programable, la cual permite que un terminal pueda hacer *hand off*, desde una celda perteneciente a un tipo de red móvil, hacia otra celda perteneciente a otro tipo de red con tecnología inalámbrica diferente.

Los terminales 4G podrán transmitir datos a 20 Mbps, 2000 veces la velocidad de descarga de los terminales actuales y 10 veces superior a los terminales 3G. Para lograr esto se requiere manejar anchos de banda de al menos 20 MHz por canal, por lo que la tecnología se considera de banda ancha.

Puesto que la potencia necesaria para el transmisor es directamente proporcional al ancho de banda de la señal, el área de cobertura de una estación base para una red de cuarta generación es diámetro reducido, por lo que las estaciones base no serían de gran tamaño [6].

1.2. Concepto celular

El concepto celular permite que un sistema de comunicaciones móviles pueda cubrir un área determinada con una densidad de usuarios variable, normalmente creciente, sin requerir más espectro radioeléctrico que el inicialmente asignado.

El nombre de telefonía celular viene de la idea de dividir una zona geográfica, a la que se desea dar servicio, en áreas pequeñas llamadas células o celdas. El concepto celular se puede resumir en dos aspectos claves: rehúso de frecuencias y división de celdas. La Figura 1 ilustra el concepto celular [2].

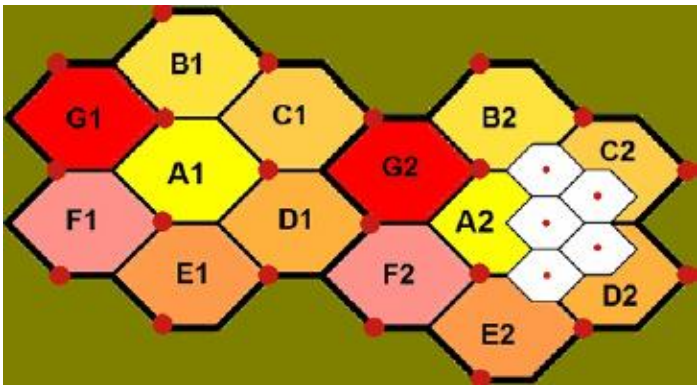

Figura 1.1 Celdas en un sistema de comunicaciones móviles

1.2.1 Célula o Celda

Una célula es una zona geográfica de cobertura proporcionada por una estación base. La forma de las celdas puede ser cualquiera, pero se elige la forma hexagonal porque provee la transmisión más efectiva al aproximarla con una forma circular y permite unirse a otras sin dejar huecos, lo cual no hubiera sido posible al elegir un círculo. Una célula se define por su tamaño físico, pero más importantemente por la cantidad de tráfico y población que existe en ella. El número de células por sistema no está especificado y depende del proveedor del servicio y de los patrones de tráfico que observe en su red. El tamaño de la célula varía dependiendo de la densidad de usuarios, además a las celdas dentro del área de cobertura se las identifica por un número llamado CGI (*Cell Global Identity*).

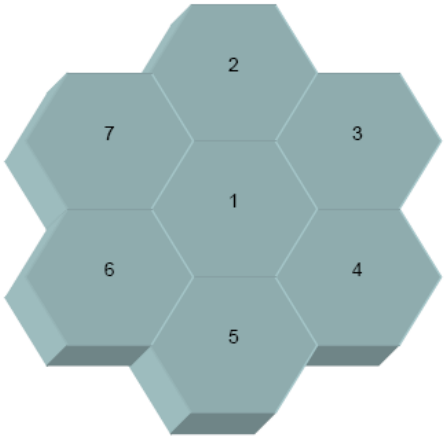

Figura 1.2 Células de la telefonía móvil

En la Figura 1.2 se puede observar la forma ideal de las células y como están colocadas adyacentemente. Las células ideales se emplean para planificar y dimensionar un sistema, considerando un nivel de potencia idéntico para toda el área de cobertura. Esta planificación se vuelve más precisa al emplear herramientas de cómputo que consideran la estructura de la ciudad con edificios, parques, etc.

Un concepto importante al hablar de células es el de *hand-off* o *hand-over,* este proceso ocurre cuando el usuario cambia de una célula a otra y el móvil obtiene un canal sin perder la comunicación. Para saber cuando debe ocurrir el *hand-off* se define un umbral de potencia que generalmente es de -95dBm. Al momento de registrar una señal a esta potencia el móvil busca otra señal con mejor potencia en la célula a la que está entrando [2].

1.2.2 Tipos de celdas

El tipo de celdas a utilizar en un sistema celular depende de la demanda del servicio celular en la población y de parámetros físicos propios del área a la que se dará servicio, así se tienen diferentes tipos de celdas:

- Macro-celdas
- Micro-celdas
- Celdas selectivas
- Celda de paraguas

- **Macro-celdas**

Las macro-celdas son celdas que permiten brindar servicio a áreas geográficas grandes, remotas y escasamente pobladas.

- **Micro-celdas**

Las micro-celdas se usan para cubrir áreas densamente pobladas, o dividir celdas existentes en celdas más pequeñas.

- **Celdas selectivas**

Las celdas selectivas son diseñadas para cubrir zonas con una cobertura menor a los 360 grados.

- **Celdas de paraguas**

La celda de paraguas cubre varias micro-celdas, se la usa con el propósito de disminuir el número de *handovers* que se producen en estaciones móviles que cambian rápidamente de micro-celdas y disminuir el trabajo de la red. El nivel de potencia dentro de la celda de paraguas se incrementa en comparación con el nivel de potencia usado en las micro-celdas.

1.2.3 Cobertura celular

Cobertura es la zona en la cual la estación móvil puede comunicarse con las estaciones transceptores y viceversa. La cobertura se planifica tomando en cuenta las condiciones de transmisión en las que se puede encontrar la estación móvil, las cuales son determinadas por las características particulares del proyecto radioeléctrico. Para implementar un sitio de cobertura se analizan requerimientos tales como: área de servicio o comercialización, tipo de servicio, población y el crecimiento del área proyectada. Únicamente puede hablarse de cobertura en sentido estadístico, esto implica que, las áreas que se representan teóricamente cubiertas, lo están en un determinado porcentaje de tiempo.

1.2.4 Capacidad celular

La capacidad celular es el tráfico total que puede soportar la red celular. La capacidad del sistema es función del número de canales utilizados, ancho de banda disponible, tamaño de las celdas y configuración de los *cluster*. Este último parámetro esta ligado a la relación de interferencia co-canal que el sistema sea capaz de soportar. Al ser un sistema de concentración de canales, la capacidad por cada bloque de canales se calcula mediante la aplicación de la fórmula de Erlang B, es decir, como un sistema de llamadas con pérdidas en donde la llamada entrante es rechazada en caso de congestión del sistema.

La red celular permite soportar gran capacidad de tráfico, mediante el re-uso de frecuencias y sectorización de celdas. El diseño de la capacidad de los sistemas se realiza por zonas, considerando el caso de tráfico más desfavorable, es decir, el tráfico en la hora cargada.

1.2.5 Reuso de frecuencias

Básicamente el reuso de frecuencias permite que un gran número de usuarios puedan compartir un número limitado de canales disponibles en la región. Esto se logra asignando el mismo grupo de frecuencias a más de una célula. La condición para que esto se pueda hacer es la distancia entre ellas, de no hacerlo la interferencia sería alta. A cada estación base se le asigna un grupo de canales que son diferentes de los de las células vecinas, y las antenas de las estaciones base son elegidas para lograr un patrón de cobertura dentro de la célula por medio de la modificación de parámetros como ganancia y directividad [2].

Cuando se diseña un sistema usando células hexagonales, los transmisores de la estación base se colocan en el centro de la célula *(center-excited cells)* o en tres de los seis vértices *(corner-excited cells)*. Normalmente se usan antenas omnidireccionales para el primer caso y antenas sectorizadas para el segundo. Esta sectorización es una forma de subdividir la célula y lograr mayor capacidad. Comúnmente esta división se hace en 3 sectores. Al hacer esto no todo son ventajas. Entre las principales desventajas destacan el aumento de equipo de propagación en la estación base, el cambio constante de canales en la unidad móvil y la disminución en truncamiento por la división de canales dentro de la célula. Aún así es muy común sectorizar la célula, sobretodo en lugares donde la densidad de población es alta [12].

El concepto de reuso de frecuencias puede representarse matemáticamente considerando un sistema con cierto número de canales disponibles.

$$F = GN \quad \textbf{Ecuación 1.1}$$

Donde F es el número de canales *full-duplex* disponibles en un *cluster*, G es el número de canales en una célula y N el número de canales en el *cluster* o factor de reuso de frecuencia. Se denomina *cluster* a las células que colectivamente usan un conjunto de canales disponibles. Es necesario decir que no es posible darle cualquier valor a N por la geometría de las células. Algunos valores posibles son 3, 4, 7, 12, 13, 19 y 27. Los más comunes son el 3 y el 7 [2].

Cuando un *cluster* es multiplicado m veces dentro de un sistema, el número total de canales *full-duplex* puede expresarse como:

$$C = mGN \quad \textbf{Ecuación 1.2}$$

Donde C representa la capacidad del canal y m el número de clusters. Se puede apreciar que la capacidad del canal es directamente proporcional al número de veces que un *cluster* es multiplicado [2].

1.3. GSM *(Global System for Mobile Communications)*

El servicio de GSM empezó en 1991 y en 1993 operaba en 22 países. Actualmente se tienen este tipo de redes en más de 80 países. GSM es un sistema de telefonía celular perteneciente a la segunda generación que se desarrolló para solucionar los problemas de compatibilidad existentes en la primera generación, sobretodo en Europa donde se creó el estándar. Fue el primer sistema completamente digital y con casi 50 millones de usuarios en el mundo se ha convertido en el estándar más popular [2].

GSM emplea una combinación de FDMA y TDMA como técnica de acceso múltiple para proveer a las estaciones base acceso simultáneo a varias unidades móviles. Las bandas disponibles se dividen en canales de 200kHz y éstos son compartidos por 8 usuarios. Cada usuario ocupa una ranura tiempo por medio de TDMA. La tasa de transmisión en ambas direcciones es de 270.833kps para todo el canal y de 33.833kbps para cada usuario, esto se logra por medio de modulación GMSK *(Gaussian minimum shift keying)* [2].

El grupo GSM definió una serie de requisitos básicos para desarrollar este estándar, de los cuales a continuación se mencionan los principales:

- *Roaming* (Itinerancia) Internacional.- Permitir que las estaciones móviles puedan ser utilizadas en todos los países participantes.
- Permitir compatibilidad con otro tipo de servicios, como son los servicios relacionados con la red PSTN (*Public Switched Telephone Network*) y con la red ISDN (*Integrated Services Digital Network*).
- Soportar nuevos servicios.
- No requerir modificación significativa de las redes públicas fijas.
- Usar un sistema de señalización estandarizado internacionalmente para la interconexión de centros de conmutación y registros de localización.
- Usar recomendaciones del CCITT (Comité Consultivo Internacional de Telecomunicaciones) en los planes de identificación y numeración.

1.3.1. Arquitectura de la red GSM

La arquitectura de una red GSM se muestra en la Figura 1.3. Consiste de tres subsistemas conectados entre si y con los abonados. Estos sistemas son:

- BSS *(Base Station Subsystem)*
- NSS *(Network and Switching Subsystem)*
- OSS *(Operational Support Subsystem)*

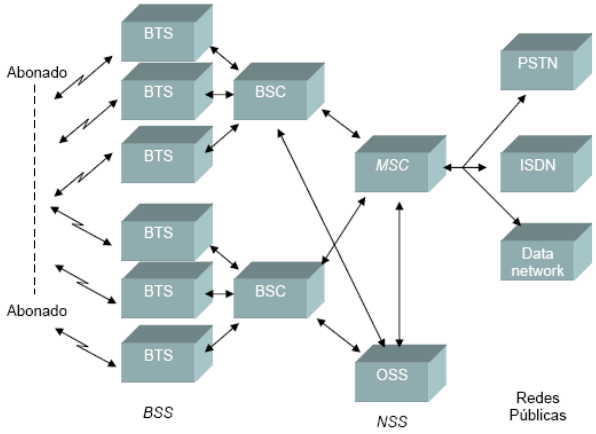

Figura 1.3 Arquitectura GSM, donde BTS = *Base Transceiver Station*, BSC = *Base Station Controller*, MSC = *Mobile Switching Center*, OSS = *Operational Support Subsystem*, PSTN = *Public Switched Telephony Network*, ISDN = *Integrated Services Digital Network*, BSS = *Base Station Subsystem*, NSS = *Network and Switching Subsystem*

- **BSS (Base Station Subsystem)**

Este subsistema constituye la interfaz entre los terminales móviles y el subsistema de red y lo conforman el BSC y sus correspondientes BTS's, como se muestra en la figura 1.4:

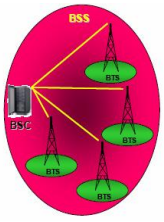

Figura 1.4 Subsistema de Estación Base (BSS)

El Subsistema de Estación Base es una parte de la red que se ocupa de las siguientes funciones:

- Control de la Red de Radio
- Señalización del Interfaz Aire
- Establecimiento de la conexión entre la MS y el NSS
- Gestión de la Movilidad
- Tratamiento y Transcodificación de la Voz
- Recopilación de Material Estadístico

Los elementos que componen el BSS son:

- El BSC (Controlador de Estación Base) es el elemento de red central del BSS y controla la red de radio.
- La BTS (Estación Base) es un elemento de red que mantiene el interfaz Aire. Se ocupa de la señalización y cifrado del interfaz Aire y del procesamiento de la voz.
- El TRX (Transcodificador) es un elemento del BSS que se ocupa de la transcodificación de la voz, es capaz de convertir voz de un formato de codificación digital a otro y viceversa.

La transmisión se considera una parte del BSS debido al hecho de que el BSS es típicamente una entidad geográfica razonablemente grande. La especificación de GSM define sólo los interfaces del equipo; por lo tanto hay una gran cantidad de alternativas para desarrollar una red de transmisión entre elementos del BSS [7].

- **NSS (*Network and Switching Subsystem*)**

El Subsistema de Red es una parte de la red GSM que se ocupa de las siguientes funciones:

- Control de la Llamada
- Interfuncionamiento de redes
- Datos del abonado y Gestión de los Servicios
- Tarificación
- Recogida de Material Estadístico

- Gestión de la Movilidad
- Gestión de la Seguridad
- Señalización del Interfaz A y PSTN
- Control del BSS

Los elementos que la componen son:

El MSC (Centro de Conmutación de Servicios Móviles) es el elemento principal del NSS. Es responsable del control de llamadas, funciones de control del BSS, funciones de interfuncionamiento, tarificación, estadísticas y señalización de los interfaces A y PSTN.

El HLR (Registro de Posición Base) es el lugar donde se almacenan permanentemente todos los datos del abonado. El HLR también da una posición conocida fija, para la información del encaminamiento de variables. Las funciones principales del HLR son los datos del abonado y gestión de servicios, estadísticas y gestión de la movilidad.

El VLR (Registro de Posición Visitante) da memoria local para las variables y funciones necesarias para gestionar llamadas hacia y desde un abonado móvil en el área correspondiente al VLR.

El AuC (Centro de Autenticación) y el EIR (Registro de Identificación del Equipo) son elementos de la red del NSS que se ocupan de los aspectos relacionados con la seguridad. El AuC se ocupa de la información de seguridad de identidad del abonado junto con el VLR. El EIR se ocupa de la información de seguridad del equipo móvil (hardware) junto con el VLR.

En la figura 1.5 se puede observa los elementos que componen el NSS:

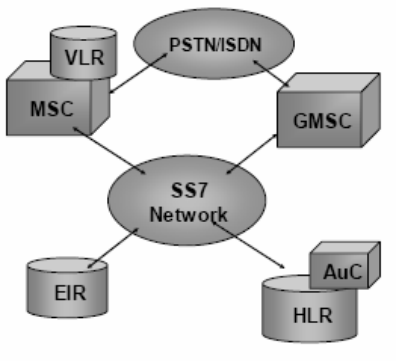

Figura 1.5 Subsistema de Red (NSS)

De la figura 1.5, el elemento de red GMSC (*Gateway Mobile Switching Center*) es un nodo que permite interrogar al HLR para obtener información de encaminamiento para una llamada dirigida a un móvil. Por lo tanto, es el nexo de unión de la red GSM con otras redes externas [7].

- **OSS (*Operational Support Subsystem*)**

El OSS está conformado por el OMC y por el NMC. El OMC (Centro de operación y mantenimiento) es un centro de trabajo donde se encuentra un cierto número de funciones de operación y mantenimiento que típicamente son:

- Modificación de parámetros de servicio en la MSC-VLR, HLR y BSC
- Gestión indirecta de los datos relativos a cada terminal móvil
- Registro de datos de transmisión, de trafico y de alarmas
- Registro de datos estadísticos relativos a las prestaciones de la red
- Configuración de los aparatos de la red
- Registro de los datos de tasación

El NMC (Centro de gestión de la red) junto con el OMC controla y gestiona el funcionamiento de la red.

La MS (Estación Móvil) es una combinación de terminal y abonado. El terminal en sí mismo se llama ME (Equipo Móvil) y los datos del abonado se guardan en un módulo separado llamado SIM (Módulo de Identidad del Abonado). Por tanto, ME + SIM = MS. La SIM es una "tarjeta inteligente" que puede utilizarse con cualquier estación móvil portátil.

El IMSI (Identificador de Terminal Móvil Internacional), memorizado en la tarjeta inteligente, sirve al operador de GSM para identificar al abonado en la red [2].

1.3.1. Servicios y Aplicaciones del GSM

El estándar GSM posee algunos tipos de servicios que pueden ser clasificados en dos grupos:

- Servicios básicos
- Servicios suplementarios

➢ **Servicios Básicos**

Los servicios básicos de telecomunicación que GSM ofrece a los usuarios se dividen en dos categorías principales:

- Teleservicios: son aquellos que permiten al abonado comunicarse con otro abonado.
- Servicios Portadores: permiten al abonado móvil el envío de datos entre dos o más puntos de acceso.

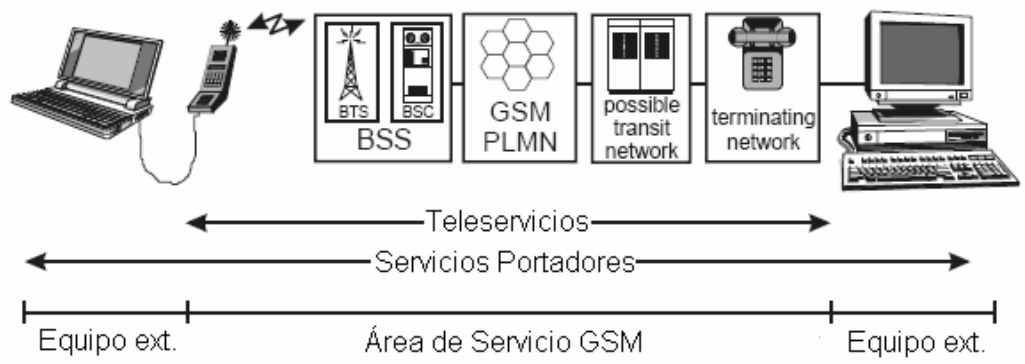

Figura 1.6 Teleservicios y Servicios Portadores

Algunos de los Teleservicios básicos que la red GSM ofrece son:

- **Voz:** capacidad de recibir y de enviar llamadas hacia o desde todo el mundo tanto con abonados fijos como con abonados móviles.
- **Llamadas de emergencia:** posibilita al abonado hacer llamadas de emergencia pulsando un botón aún sin contar con la tarjeta SIM.
- **Servicios de mensajes cortos (SMS):** es posible enviar un mensaje de hasta 160 caracteres desde y hacia un terminal móvil. Si el móvil no está conectado o fuera de cobertura, el mensaje se almacena en la central de mensajes hasta que el abonado se conecte, avisándoles de la existencia de dicho mensaje. Utiliza una modalidad *Store & Forward* (Almacenamiento y envío). El terminal que genera el mensaje se comunica con el terminal que recibe con un retardo temporal introducido por la memorización del mismo en una base de datos, por lo que la entrega del mensaje no es en tiempo real. Utiliza el *signaling path* (ruta de señalización) de la red GSM.
- **Roaming:** la palabra *roaming* significa moverse alrededor de, caminar. Esta palabra fue adoptada para ser usada en telefonía celular para describir el efecto que el abonado móvil pueda moverse de un área de servicio a otra mientras está utilizando el mismo móvil
- **Buzón de voz:** consiste de un contestador incorporado en la red y controlado por el abonado. Las llamadas pueden ser desviadas al buzón del abonado accediendo posteriormente a él con un código personal.
- **Buzón de fax:** permite al usuario recibir mensajes de fax en cualquier máquina a través de su móvil.
- **Voz y fax alternados:** permite que durante una llamada el abonado intercambie entre voz y fax. Se puede conmutar varias veces.

Entre los servicios portadores básicos; que soportan la transmisión de datos síncronos y asíncronos a velocidades de hasta 9.6Kbit/s, se pueden distinguir los siguientes:

- Tráfico hacia la red telefónica (PSTN): para enviar el tráfico de datos hacia la red pública es necesario seleccionar un módem.
- Tráfico hacia la Red Digital de Servicios Integrados (ISDN).
- Acceso a otras redes de datos asíncronos: soporta tráfico hacia las redes públicas de conmutación de paquetes y conmutación de circuitos, necesitando un interfaz en función de cada propósito.

- Transmisión de información a distintas velocidades – comunicación de datos dúplex con conmutación de circuitos síncrona y asíncrona, 300 a 9600 bps.
- Acceso a funciones de PAD (*Packet Assembler/Disassembler*) para comunicación asíncrona, 300 a 9600 bps.
- Acceso de redes públicas de datos, protocolo X.25, servicio de conmutación de paquetes para comunicación de datos dúplex, 200 a 9600 bps.
- Transmisión de voz y datos durante una llamada (*Speech & Data Swapping*), envío alterno de voz y datos.
- Selección de módem, selección de servicios de audio de 3.1 KHz cuando se conecte a la ISDN.
- Soporte de Solicitud Automática de Retransmisión (ARQ, *Automatic Request for Retransmisión*) para mejorar la tasa de errores, modo transparente (Con ARQ) y modo no transparente (No ARQ).

➢ **Servicios Suplementarios**

Estos servicios modifican o complementan los servicios básicos de telecomunicaciones. Se ofrecen junto con o asociados con los servicios básicos de telecomunicaciones y se clasifican en los siguientes tipos de servicios:

- **Servicios de Identificación de números**
  Soporta CNIP (*Calling Number Identification Presentation*): muestra en pantalla el número del abonado que llama.
- **Servicios de completamiento de llamadas**
  CW (*Call Waiting*): llamada en espera.
  CH (*Call Holding*): permite a una unidad móvil GSM recibir una segunda llamada mientras está en curso otra, el abonado puede conmutar a la segunda llamada mientras deja a la primera llamada en espera.
- **Servicios de Transferencia Adicional de Información**
  UUS (*User-to-User Signaling*): permite a un móvil enviar datos a otra unidad móvil o a un número de ISDN.
- **USSD (*Unstructured Supplementary Services Data*)**
  Es un medio de transmitir información o instrucciones por una red GSM. USSD tiene algunas similitudes con el SMS (ambos utilizan el *signaling path* de la red

GSM). Como diferencia, el USSD no es un servicio de almacenamiento y envío, es una sesión-orientada tal que cuando un usuario accede a algún servicio USSD.

1.3.2. Salto de frecuencias

En la propagación de radio frecuencia el canal presenta desvanecimiento de frecuencia selectiva. Esto quiere decir que las condiciones o características para la transmisión varían dependiendo de la frecuencia individual que se maneje. Así mismo, la propagación de la señal es multiruta. Esto ocasiona efectos indeseables en la comunicación. Como alternativa para solucionar estos dos problemas, *GSM* utiliza salto de frecuencia. Existen dos tipos de salto de frecuencia. *FFH* (*Fast Frequency Hopping*) y *SFH* (*Slow Frequency Hopping*) [8]. La diferencia radica en el número de bits de datos que "saltan". Cuando el salto es rápido, *FFH*, existen muchos cambios de frecuencia pero se encuentran involucrados pocos bits de datos. En cambio, en *SFH* es mayor la cantidad de datos pero los cambios de frecuencia no son tan numerosos.

GSM emplea *SFH* para:

- Protegerse ante ataques electrónicos
- Reducir los efectos de la propagación multiruta, lo que aumenta la calidad de la señal
- Lograr diversidad de frecuencia
- Optimizar el uso del espectro

La diversidad de frecuencia significa que manda la información usando diferentes frecuencias, con lo que se incrementa la probabilidad de que los datos lleguen al destino. La tasa de saltos es de 216.7 por segundo. Este valor equivale a la duración de una trama o *frame*. Es así que el móvil transmite a una frecuencia durante una ranura de tiempo y a otra frecuencia distinta durante la siguiente ranura de tiempo.

1.3.3. Bandas de Frecuencias de los Sistemas GSM

GSM-900

Tiene 124 canales en dos sub-bandas de 25 MHz c/u en los rangos 890 MHz-915 MHz y 935 MHz-960 MHz, con BW (Ancho de banda) por canal de 200 KHz. Cada portadora se divide en *frames* (tramas) donde cada trama tiene 8 *time spots* (intervalos de tiempo), con una duración de trama de 4.6 ms. Separación entre la portadora del *Down Link* (enlace de bajada) y del *Up Link* (enlace de subida): 45 MHz. En la figura 1.7 se muestra la distribución de frecuencia en GSM-900 tanto para el *uplink* como para el *downlink* [10].

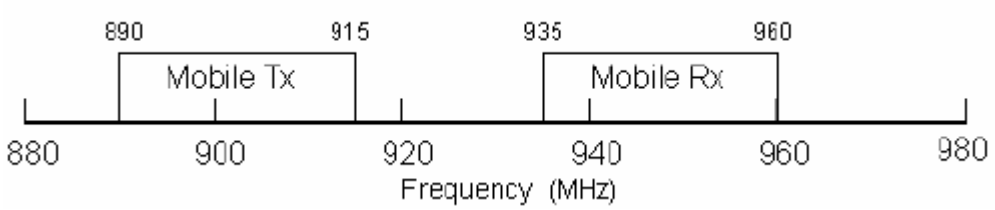

Figura 1.7 Banda de frecuencia GSM 900 MHz

DCS-1800

Tiene 374 canales en dos sub-bandas de 75 MHz c/u en los rangos 1710Mhz-1785 MHz y 1805 MHz – 1880 MHz, con BW por canal de 200 KHz. Separación entre la portadora del *Down Link* y del *Up Link*: 75 MHz. En la figura 1.8 se muestra la distribución de frecuencia en DCS-1800 tanto para el *uplink* como para el *downlink* [9]

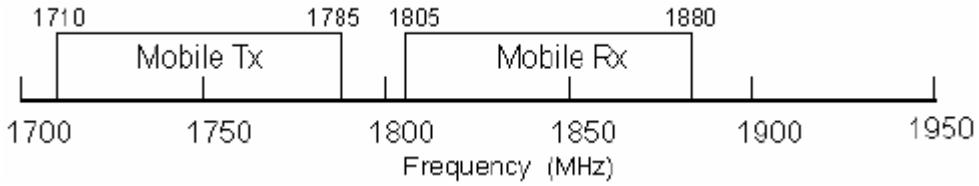

Figura 1.8 Banda de frecuencia DCS 1800 MHz

PCS-1900

Tiene 374 canales en dos sub-bandas de 75 MHz c/u en los rangos 1850MHz-1925 MHz y 1930 MHz – 2005 MHz, con BW por canal de 200 Khz. Separación entre la portadora del *Down Link* y del *Up Link*: 75 MHz. En USA se asignó parte del rango de la banda de 1800

MHz a aplicaciones de comunicaciones punto a punto. En la figura 1.9 se muestra la distribución de frecuencia para PCS-1900 tanto para el *uplink* como para el *downlink* [9].

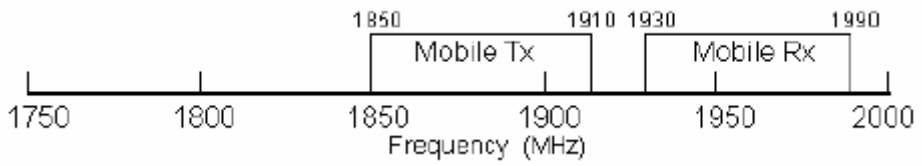

Figura 1.9 Banda de frecuencia PCS 1900 MHz

1.4. Descripción guerras electrónicas

La "Guerra Electrónica" de las comunicaciones o *EW* por sus siglas en inglés "*Electronic Warfare*" es el nombre que se le da a todas aquellas acciones que tienen por objetivo bloquear, interceptar o negar la comunicación de un punto transmisor a otro receptor. Esta llamada "guerra" tiene tres elementos principales [8,11,12]:

- El ataque electrónico (*EA, Electronic Attack*)
- El apoyo electrónico (*ES, Electronic Support*)
- La protección electrónica (*EP, Electronic Protect*)

1.4.1. Ataque electrónico

El AE (ataque electrónico) se puede realizar por medio de tres tipos de acciones o técnicas [8, 12, 13]:

1) *Jamming*
2) Engaño
3) Radiación directa de energía

- **Técnica *Jammer***

El término *jamming* no posee una traducción acertada que englobe todo el concepto. En su más puro significado, *Hamming* se define como aquella actividad que afecta la línea de tiempo en alguna comunicación [8, 13]. Es decir, logra que la información no llegue al

receptor en el momento que debía de hacerlo. Al afectar esto, se afecta también la relevancia de la información. Esto se debe a que la información solamente es útil en determinado instante. No es útil si se recibe antes o después del tiempo establecido.

- **Técnica de engaño**

La técnica de engaño tiene como objetivo formar una nueva ruta de comunicación [8]. Es así que en lugar de que la información llegue al receptor deseado, ésta sufre un cambio de ruta y es recibida por otro sistema receptor. De igual forma, el engaño puede consistir en la sustitución del sistema transmisor. En este caso el receptor original está recibiendo una señal que proviene de un segundo sistema transmisor. Cuando el receptor está ocupado no puede recibir la señal emitida por el transmisor original.

- **Técnica de radiación directa de energía**

La radiación directa de energía es la manera más fácil de atacar a un sistema de comunicación. Sin embargo, es la más fácil de detectar y poder evitar. Consiste en enviar una determinada señal con determinada potencia para dañar o destruir completamente la comunicación entre transmisor y receptor. La potencia emitida debe ser mayor a la que emplea el transmisor del sistema que está sobre ataque [13].

Un dispositivo capaz de emplear cualquiera de las tres técnicas o una combinación de ellas para interferir, dañar o destruir la transmisión de información dentro de un sistema electrónico de comunicaciones es llamado *jammer* [13].

1.4.2. Apoyo electrónico

El apoyo electrónico funciona como auxiliar del AE. Su función es la medición de parámetros de interés en el sistema de comunicación [8]. Una de las razones principales de hacer esto radica en que si no hay señal que interferir no tiene caso gastar la potencia del *jammer* implementado. Sin embargo, dependiendo de la aplicación será el tipo de *jammer* que se emplee. Es así que se puede mantener en operación un *jammer* por tiempo indefinido o se puede encender siempre y cuando se detecte una comunicación. Todo esto se verá más

adelante cuando se analicen los distintos tipos de *jammers* que existen. Entre los parámetros que se encarga de medir el apoyo electrónico se encuentran [8, 13]:

SNR (Signal-to-Noise Ratio)

Determina la calidad con la que llega la señal al receptor después de recorrer la ruta del sistema de comunicación e ir contaminándose por ruido.

JSR (Jam-to-Signal Ratio)

Determina si la potencia con que transmite el *jammer* es mayor o menor que aquella que emplea el transmisor original del sistema [8].

PSR (Packet Send Ratio)

Relaciona los paquetes que fueron enviados correctamente por una ruta de tráfico con los paquetes que trataron de ser enviados fuera de la capa *MAC* [13].

PDR (Packet Delivery Ratio)

Compara los paquetes que llegaron al receptor con los que fueron enviados [13].

BER (Bit Error Rate)

Indica la fracción de bits que contiene o pudiera contener errores. Es decir, es la probabilidad de que un bit sea incorrecto. El *BER* se puede escribir también como *Pe* [8].

SER (Symbol Error Rate)

Es la probabilidad de que un símbolo sea incorrecto y se llega a escribir como *Ps* [8].

SIR (Signal-to-Interference Ratio)

Relaciona la potencia de la señal deseada con la potencia de la suma de las señales no

deseadas [12, 14].

.

1.4.3. Protección electrónica

La PE (protección electrónica) consiste en el uso de estrategias para evitar los dos primeros elementos de la llamada "Guerra Electrónica", es decir, el ataque y el apoyo [8]. La codificación y la modulación entran dentro de este elemento. Con la unión de modulación y codificación nacieron las comunicaciones *AJ* por sus siglas en inglés, *antijam*. Este tipo de comunicaciones tienen como objetivo evitar que un sistema externo pueda dañar, bloquear o interceptar la comunicación de otro sistema.

1.4.4. Tipos de señales anti *jammer*

A pesar de existir varios tipos de señales AJ; no es parte de este proyecto mencionar todas. Es por eso que se discutirán las dos principales. Las dos tipos de señales AJ a tratar tienen que ver con la telefonía móvil. El primero consiste en la secuencia directa de amplio especto o *D*SSS (*Direct Sequence Spread Spectrum*) [8]. Este tipo de señal es empleado en el estándar de segunda generación de telefonía móvil IS-95A conocida común y erróneamente como CDMA. Se debe recordar que CDMA (*Code Division Multiple Access*) es una técnica de acceso múltiple y no un estándar. De igual forma, se emplea en el estándar de 2.5G IS-95B y en el de 3G Cdma2000.

El segundo tipo de señal AJ es el salto de frecuencia o FHSS(*Frequency Hopping Spread Spectrum*) [8]. El estándar de segunda generación de telefonía móvil *GSM* emplea esta técnica para lograr la diversidad de frecuencia.

Para que una señal pueda ser considerada como AJ es necesario que el sistema que la transmita sea un sistema LPD (*Low Probability of Detection*) y/o LPI (*Low Probability of Intercept*) [8, 12]. En un sistema LPD el objetivo es lograr que la señal permanezca tan oculta como sea posible. *DSSS* es un ejemplo de sistema *LPD* [8, 12].

En *DSSS* esto se logra al distribuir la señal por todo el espectro disponible, lo que hace que la potencia sea muy baja y parezca ruido. Es así que se vuelve complicado detectar si la señal es de información, o es simplemente ruido.

En un sistema LPI (*Low Probability of Intercept*) puede ser que se haya detectado la señal, pero mientras no se intercepte la información, ésta estará protegida [8, 12]. Un ejemplo de estos sistemas es FHSS. En FHSS la protección se logra cambiando de frecuencia constantemente. Contrario a DSSS, donde el ancho de banda requerido es grande, en los sistemas que emplean FH la señal ocupa generalmente un ancho de banda angosto que depende del propio sistema, de la aplicación y de la técnica de modulación.

Existen dos tipos de salto de frecuencia. FFH (*Fast Frequency Hopping*) y SFH (*Slow Frequency Hopping*). La diferencia radica en el número de bits de datos que "saltan". Cuando el salto es rápido, FFH, existen muchos cambios de frecuencia pero se encuentran involucrados pocos bits de datos. En cambio, en SFH es mayor la cantidad de datos pero los cambios de frecuencia no son tan numerosos [2, 8].

CAPÍTULO II

DESCRIPCIÓN DE JAMMER

2.1 Estrategias de *Jamming*

La estrategia que emplea un *jammer* depende directamente de la aplicación a la que se desea atacar, por tal motivo se debe estudiar el "blanco" para elegir la mejor opción.

Cuando se trata de atacar sistemas que empleen señales AJ, el *jammer* debe de emitir una señal portadora en banda base que puede ser modulada por uno o más impulsos o bien por una señal de ruido [8, 12]. El nivel de potencia de *jamming* se expresa en J_0 y está medido en Watts/Hertz.

2.1.1 *Jamming* por ruido

La portadora emitida por el *jammer* es modulada por una señal aleatoria de ruido [15]. El ruido que se introduce puede ocupar ya sea todo el ancho de banda empleado por la señal AJ, o simplemente una parte de él. Los resultados serán diferentes considerando que no siempre se necesita atacar todo el ancho de banda para interrumpir de manera eficiente la comunicación.

Dependiendo de el ancho de banda que se ataque se dividen en:

- *Jamming* por ruido de banda-ancha
- *Jamming* por ruido de banda-parcial
- *Jamming* por ruido de banda-angosta [8, 12].

- ***Jamming* por ruido de banda-ancha**

El ruido de banda ancha o BBN (*Broadband noise*) introduce energía a través de todo el ancho del espectro de frecuencias en que opera el blanco que va hacer atacado. A este tipo de *jamming* se le conoce también como *jamming* de banda completa, y es aplicable a cualquier tipo de señal AJ [8]. El principal limitante de este tipo de *jamming* es que tiene un bajo J_0, ya que la potencia es esparcida en una parte amplia del espectro.

El *BBN jamming* eleva el nivel de ruido en el receptor, lo que ocasiona un decremento en la relación señal-a-ruido [8, 12, 14]. La eficiencia de este tipo de *jamming* depende directamente del nivel de potencia y de la distancia entre el *jammer* y el receptor.

- ***Jamming* por ruido de banda-parcial**

Conocido también como *PBN(Partial-band noise).* En este caso la energía se introduce por una parte específica del espectro, cubriendo solamente algunos canales, dichos canales pueden ser o no continuos. Este tipo de *jamming* no desperdicia tanta potencia como el anterior . Dependiendo de la aplicación, en muchos casos no es necesario introducir ruido en todo el espectro, sino simplemente en los lugares donde importa. Por ejemplo, si se conoce la parte del espectro en donde se encuentran los canales de sincronización será mejor introducir ruido en esta parte que en todo el ancho del espectro. Al no haber sincronización la comunicación no llega a ser exitosa [8, 12].

2.1.1.3 *Jamming* por ruido de banda-angosta

Conocido como NBN (*Narrowband noise*). Este tipo de *jamming* introduce energía solamente en un canal. El ancho de banda de esta energía podría abarcar todo el canal o simplemente una parte de él. La eficiencia de esta forma de *jamming* dependerá en parte del conocimiento del blanco, esto es porque se debe de atacar el lugar exacto en el espectro en donde se encuentren los canales de interés. La potencia se puede canalizar toda a una pequeña parte del espectro, lo que representa una ventaja. Una vez más la diferencia entre estos tipos de *jamming*, radica en la potencia empleada y el espectro cubierto [8, 12].

2.1.2 *Jamming* por tonos

Esta estrategia consiste en colocar un tono ST (*single-tone*) o varios tonos MT (*multiple-tone*), a lo largo del ancho de banda donde se encuentra la señal AJ [8]. La eficiencia de esta técnica depende completamente del lugar en el espectro donde se coloquen los pulsos. Es por eso que se requiere estudiar la señal del blanco cuidadosa. En un sistema DSSS es posible emplear *single-tone jamming* para modificar el *offset* en los receptores y ocasionar que se sobrepase el nivel máximo de la señal, lo que produce que no se pueda recibir la información. La relación entre la fase del tono emitido por el jammer y la fase de la señal es un parámetro importante. Si se envía un solo tono, éste estará presente ya sea en la frecuencia del cero o del uno. Si se encuentra en la frecuencia del uno entonces la fase representa un problema, ya que si el tono no se encuentra en fase no se podrá bloquear o interferir la transmisión del símbolo. En cambio si el tono se encuentra en la frecuencia del cero, entonces podrá bloquear la transmisión al símbolo siempre y cuando la potencia sea adecuada sin depender de la fase [12, 14].

En un caso de MT si los tonos se colocan en canales continuos, el desempeño del jammer será teóricamente igual al desempeño de *jamming* por ruido de banda-parcial, debido a que los tonos se colocan en canales continuos. En este caso particular al MT se le conoce como *comb jamming* [8].

El que se produzca una correcta interferencia dependerá en primer lugar de que el tono se coloque en una parte del espectro en donde exista un tono que represente un símbolo, en ese caso el JSR debe ser lo suficientemente alto; en segundo lugar dependerá de que una vez que el tono del *jammer* esté en la frecuencia del tono del símbolo, la fase entre ellos sea igual.

Este tipo de j*amming* es muy poco eficiente contra sistemas FH debido a que depende de que la señal salte a la frecuencia en la cual se ha colocado el tono emitido por el *jammer*. Es por eso que si se utilizan tonos estos deben estar barriendo una parte del espectro y no estar en una frecuencia específica. Este es el caso de una estrategia de *jamming* posterior.

2.1.3 *Jamming* por pulsos

Esta estrategia es similar en resultados al *jamming* por ruido de banda-parcial. En este caso el factor a tomar en cuenta no es el ancho del espectro cubierto, sino el tiempo que el *jammer* está encendido. A pesar de que una de las estrategias se enfoca a frecuencia y la otra a tiempo, la eficiencia es prácticamente la misma. Sin embargo, cuando se analiza el funcionamiento se encuentran similitudes con el *jamming* por ruido de banda-ancha. Esto se debe a que el tiempo que está encendido, el *jammer* que trabaja por pulsos abarca una parte amplia del espectro. Esta estrategia ahorra de manera considerable la potencia, lo que la hace eficiente si se diseña correctamente el ciclo de trabajo [12, 14].

2.1.4 *Jamming* por barrido

Es un concepto similar al de ruido por banda-ancha o por banda-parcial [8, 13]. De hecho se puede considerar como una estrategia complementaria. Consiste en introducir ruido en una pequeña parte del espectro; y una vez colocada está señal, se realiza un barrido por todo el ancho de banda que ocupe la señal AJ. Esta estrategia se puede emplear en un sistema FHSS [12]. Sin embargo, se tiene que considerar que el barrido debe de ser tan rápido como para identificar la frecuencia en la que se encuentre la señal pero sin llegar a una velocidad tal, que cuando se sitúe sobre el salto se tenga efecto solamente sobre una parte de él. Supongamos que para lograr interferir un sistema de comunicación se debe tener un BER de 10^{-1}. Un BER de 10^{-1} significa que es necesario bloquear la transmisión de un bit de diez, o para un sistema AJ que está mandando datos a una velocidad de 20kbps, la transmisión de 2000 bits debe ser bloqueada para alcanzar este BER. Si este sistema es de tipo SHF y maneja 100 saltos por segundo, cada salto contendrá 200 bits (sin considerar el tiempo entre saltos). De ahí que se necesite aplicar de manera exitosa *jamming* sobre 10 saltos por segundo. Ya que estos saltos pueden estar en todo el espectro asignado, al menos 10 barridos por segundo son necesarios para que el *jammer* sea eficiente.

A pesar de que el concepto es parecido al de *jamming* por ruido de banda-ancha, en este caso de optimiza el uso de la potencia. Esto se debe a que no se debe esparcir la potencia por todo el ancho del espectro, sino que se utiliza la máxima potencia en determinado lugar y en determinado momento.

2.1.5 *Jamming* por seguimiento

Esta estrategia se aplica generalmente a sistemas FHSS. Consiste en localizar la frecuencia a la cual "saltó" la señal, identificar la señal como el blanco y emplear *jamming* por ruido, tonos o pulsos. Se conoce también como *jamming* de respuesta y *jamming* de repetición [12].

Sus principales limitantes al usarlo contra sistemas FH fueron determinadas por Torieri. Estas limitantes están relacionadas con el tiempo de procesado del *jammer*. Esto se debe a que el proceso de *jamming* en este caso comienza por conocer la frecuencia a la que ha saltado la señal. Esto se hace midiendo la energía del espectro para saber si ha habido ganancias o pérdidas. Si se detecta mayor energía en un punto se podría concluir que esa es la nueva frecuencia, aunque esto no es siempre cierto. Debido a la velocidad del salto de frecuencias es difícil averiguar el nuevo blanco.

Además de esto existen otros problemas. Si se aplica *jamming* al mismo tiempo en más de un canal, la potencia estará distribuida entre estos y probablemente no será suficiente para reducir la relación señal-a-ruido a un nivel donde no puede existir comunicación. Incluso las distintas modulaciones son un escudo ante esta estrategia. Por ejemplo, si se emplea BFSK como técnica de modulación el *jammer* no sabe cuál es el canal complementario. En este caso la probabilidad de que el *jammer* sea eficiente se reduce a la mitad. Es por estas razones que a pesar de ser una estrategia eficiente cuando se diseña correctamente, es muy compleja y no representa una opción de sencilla implementación [8, 12].

2.1.6 Jamming inteligente

Es común que cuando se aplica alguna estrategia de *jamming* sobre una señal AJ, se desperdician recursos y no siempre se elige la opción más adecuada. Cuando se conoce como funciona el sistema que se desea atacar, se pueden optimizar los recursos. Realmente el *jamming* inteligente no es una estrategia como las anteriores, sino que se refiere al estudio del blanco para lograr mejores resultados. Por ejemplo, se puede atacar la señalización en sistemas de telefonía móvil para evitar el uso de móviles [12, 14].

Por ejemplo, en los sistemas de telefonía móvil es común encontrar canales de sincronización. En el caso de IS-95 se usa un canal codificado por código Walsh que se encarga de la sincronización. Si se identifica a este canal y se aplica alguna estrategia de *jamming* sobre él, será posible interrumpir de manera eficiente toda la comunicación.

Dentro de este tipo de *jamming* se encuentra el *jamming* de engaño. En esta estrategia se envía un mensaje falso para mantener a una de las partes del sistema de comunicación en estado de recepción. De esta manera, se logra que nunca haya confirmación de que se recibió el mensaje y se genera una interrupción en la comunicación. Otra manera de engañar al sistema sobre el cual se aplica *jamming*, es interceptar la señal del transmisor y con ello establecer una ruta de comunicación incorrecta [12, 14].

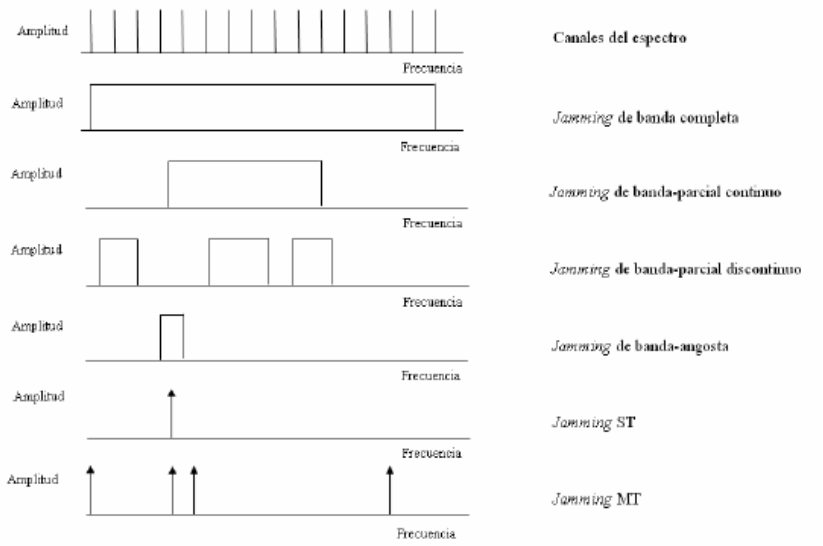

Figura 2.1 Estrategias de jamming

2.1.7 Técnicas para incrementar la eficiencia del jammer

Una manera de incrementar la eficiencia de un jammer es incrementar el número de señales que puede bloquear o interferir simultáneamente. Esto es posible mediante algunas técnicas que involucran el compartir la potencia entre los distintos blancos y el poder encender y apagar el jammer por determinado tiempo para dedicarlo a uno o a otro blanco.

- **Look-Through**

Cuando las señales no son de espectro extendido, esta técnica es empleada para determinar si el blanco ha cambiado de frecuencia o simplemente ha dejado de operar. Esto se hace para no malgastar la potencia y de esta manera emplearla en más de un objetivo o simplemente ahorrarla. Al momento de apagar el jammer se mide la actividad en el espectro y se determina si el blanco está en funcionamiento o no. Podría pensarse como solución para sistemas FH y como una forma de jamming por seguimiento. Sin embargo, debido a la velocidad de salto no se emplea esta técnica para tal propósito. Esta técnica se puede aplicar a sistemas DSSS siempre y cuando se pueda detectar su actividad [12, 14].

- **Potencia compartida**

Una manera de compartir la potencia entre dos o más blancos está representada por la estrategia de múltiples tonos. En esta estrategia de jamming los tonos se pueden colocar en diferentes partes del espectro sin necesidad de que los canales sean continuos para lograr atacar varios blancos [12].

- **Tiempo compartido**

Otra técnica para cubrir más de un blanco es orientar la máxima potencia del jammer hacia cada blanco pero en momentos distintos. Cuando se aplica jamming a una señal digital no se tiene que estar todo el tiempo introduciendo ruido. Basta con incrementar el BER hasta cierto nivel. En el caso de las comunicaciones de voz el nivel necesario para cortar la transmisión es más alto que en el caso de datos. En el caso de las comunicaciones de voz analógicas es necesario bloquear o interferir solamente un 30% de la transmisión para que no entienda el mensaje. De ahí que el jammer pueda estar orientado a distintos blancos en diferentes momentos [12].

2.2 Tipos y clasificación de jammer

De las distintas estrategias de jamming se derivan cuatro tipos principales de jammers. La elección del tipo de jammer dependerá de la aplicación a la que se vaya atacar.

2.2.1 Jammer constante

Este tipo de jammer emplea la estrategia de ruido y la de barrido. Su principal ventaja es la relativa facilidad de implementarse. Sin embargo, en aplicaciones donde se desea que el jamming pase desapercibido no es recomendable emplear un jammer constante [13]. Esto se debe a que al momento de analizar la transmisión de la información se detectará ruido que excede los niveles comunes. Una vez detectado el ruido es posible encontrar la fuente que lo genera. Además de esta desventaja, es necesario considerar que la potencia requerida es grande.

2.2.2 Jammer de engaño

Emplea la técnica de engaño que pertenece al jamming inteligente. En este caso se envían señales que parecen ser legítimas, pero no se incluye una separación entre ellas. Esto ocasiona que se mantenga el estado de recepción y no haya confirmación de haber recibido información alguna [13]. Este tipo de jammer logra mayor invisibilidad que el constante. Sin embargo, aún es posible detectarse. La potencia requerida también es grande.

2.2.3 Jammer aleatorio

Este tipo de jammer funciona por determinado tiempo y deja de hacerlo por otro [13]. Los tiempos son programados y se debe hacer conocer la aplicación para obtener resultados positivos. Se puede utilizar jamming por ruido, por pulsos, por tonos e incluso por barrido [6]. 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.

2.2.4 Jammer reactivo

Este tipo es el más complejo pero es el que ofrece una menor posibilidad de ser detectado. Consiste en censar la actividad de la red para saber en que momento debe de actuar el jammer [13]. Podría pensarse que el consumo de potencia es mínimo. Sin embargo, a pesar de no ser excesivo si se requiere determinada potencia para estar monitoreando la actividad de la red. Una vez que se detecta el envío de la señal, se realiza un jamming por ruido, por tonos o por pulsos.

2.3 Elección de técnica y tipo de jammer

El objetivo del jammer es bloquear la comunicación de equipos móviles en el mayor rango posible de la banda PCS (Personal Communications Services) y a una corta distancia. En la Tabla 2.1 se muestra la asignación de frecuencias para las diferentes operadoras de telefonía móvil que presta su servicio en el Ecuador.

Tabla 2.1 Asignación de frecuencias para telefonía móvil en Ecuador [16].

OPERADOR	DENOMINACIÓN	BANDAS DE FRECUENCIAS EN MHz	
CONACEL S.A. (Porta)	Banda de los 850 MHz	824 - 835	869 - 880
		845 - 846.5	890 – 891.5
	Banda de los 1900 MHz	1885 - 1890	1965 - 1970
OTECEL (Movistar)	Banda de los 850	835 - 845	880 - 890
		846.5 - 849	891.5 - 894
	Banda de los 1900 MHz	1865 - 1870	1945 - 1950
TELECSA S.A. (Alegro)	Banda de los 1900 MHz	1895 - 1910	1975 - 1990

Después de haber descrito y analizado las distintas técnicas y estrategias de *jamming* presentadas en este proyecto de tesis, se llegó a la conclusión que la estrategia de barrido es la ideal para un sistema de telefonía móvil con tecnología GSM puesto que es apropiado para sistemas FHSS, y además se pretende utilizar toda la potencia disponible en cada parte del espectro. A pesar de que la velocidad tendrá que ser controlada por los saltos que maneja GSM, esto será posible mediante la definición de parámetros y pruebas constantes. El tipo de *jammer* adecuado para este sistema es de tipo constante; puesto que el ahorro de potencia es dispensable ya que el *jammer* no es portátil.

La técnica y tipo de *jammer* que se eligió son también los apropiados desde el punto de vista de complejidad, debido a su sencilla implementación.

Los otros tipos y técnicas de *jammer* se descartaron por los siguientes motivos:

- Los de tipo reactivo y de engaño son muy complejos y lo que se pretende es sencillez y optimización, además no se desea que pase desapercibido, puesto que este no es el propósito del *jammer* que está siendo objeto de estudio.
- El de tipo aleatorio no es el apropiado, ya que la interferencia que se realiza debe ser en todo instante de tiempo.
- Las técnicas de ruido debido a que:
    - La de banda-ancha requiere mucha potencia y se tendrían que implementar numerosas etapas de ganancia para la antena. Además de incurrir en problemas legales.
    - La de banda-parcial nos limitaría a cierta parte del espectro, entre 5 y 10MHz.
    - La de banda-angosta es fija y no ofrece el ancho de banda necesario.
- La estrategia de tonos no es efectiva ante sistemas que empleen salto de frecuencia (*Frequency Hopping*).
- El *jamming* por pulsos no sería efectivo porque el *jammer* enciende y apaga, y para este caso se necesita que esté encendido en todo momento. Esta técnica se utiliza más cuando se desea ahorrar de potencia.
- El *jamming* por seguimiento no se eligió por la complejidad que representa su diseño.

2.4 Descripción del circuito

Para que un *jammer* utilice como estrategia el barrido, se debe implementar el diagrama de la Figura 2.2

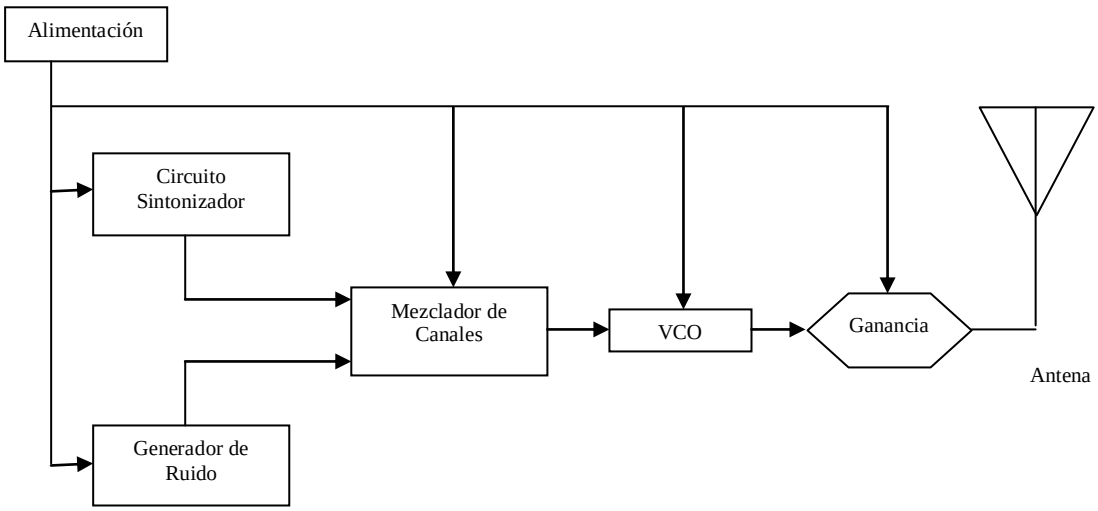

Figura 2.2 Diagrama a bloques del *jammer*

2.4.1 Alimentación

El equipo electrónico en su totalidad se alimenta con voltaje continuo (DC), este se puede obtener de una batería o una fuente de poder. La energía eléctrica se genera y se distribuye con una forma de onda senoidal, la forma de onda de una señal de DC es un nivel constante, por lo tanto se requiere una conversión en la forma de onda de la señal (AC a DC).

- **Transformador**

La alimentación del circuito se toma de la línea de 120V; para reducir el nivel de la corriente alterna se utilizará un transformador (Figura 2.3), el cual es un dispositivo eléctrico que consta de una bobina de cable situada junto a una o varias bobinas, y que se utiliza para unir dos o más circuitos de corriente alterna aprovechando el efecto de inducción entre las bobinas. La bobina conectada a la fuente de energía se llama bobina primaria y las otras bobinas reciben el nombre de bobinas secundarias. Para esta aplicación en particular se utiliza un transformador reductor de 24V.

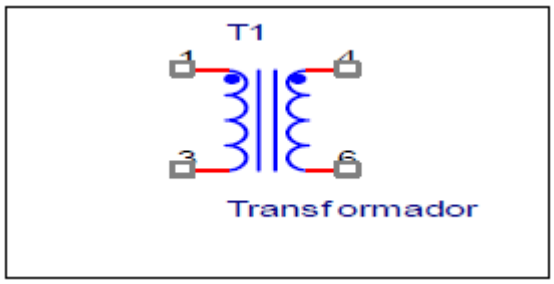

Figura 2.3 transformador

- **Puente Rectificador**

Se puede utilizar el componente 3N255 que es un arreglo de 4 diodos que permite la rectificación en onda completa (figura 2.4), se identifican cuatro puntos de conexión, dos iguales en los cuales coincide un ánodo y un cátodo y estos son los puntos de entrada para la señal de C.A., en otro punto coinciden los cátodos, esta es la salida positiva del rectificador, en el punto donde coinciden los ánodos corresponde a la terminal negativa del rectificador.

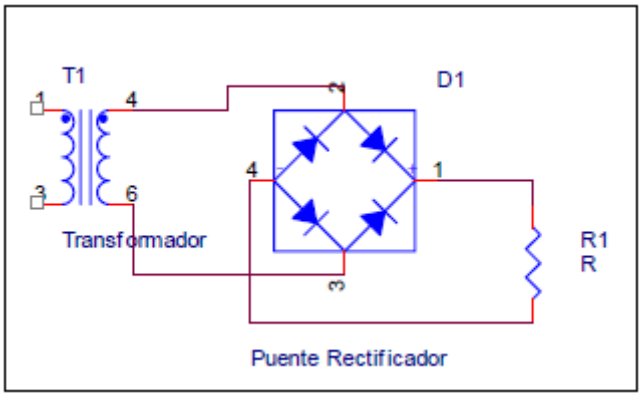

Figura 2.4 Circuito rectificador de onda completa

- **Capacitor electrolítico**

Elimina las pulsaciones de la señal rectificada, el tamaño del capacitor es directamente proporcional a la corriente que debe entregar la fuente, e inversamente proporcional a la frecuencia de la señal a filtrar, por este motivo el capacitor que se utiliza es de 220 nF. Ante la presencia de carga en la fuente, el capacitor comienza a entregar corriente, esto reduce su voltaje, al llegar la parte alta de un nuevo ciclo, se recarga el capacitor, el proceso de carga y descarga forma un rizo en la señal de C.C., el rizo formado es

indeseable en la operación de equipo electrónico. La eliminación del rizo en la señal se logra con una etapa de regulación.

Los reguladores disipativos logran su propósito recortando la parte superior de la señal, eliminando así el rizo, por ello reciben un voltaje mayor al que deben entregar. La energía de la parte recortada es disipada en el regulador. La figura 2.5 muestra el circuito completo para una fuente lineal regulada. Debido a que los componentes del circuito se alimentan con voltajes de +24V, -24V y 9V, se utilizan los siguientes reguladores de voltaje: LM7824CT, LM7924CT y LM7809CT.

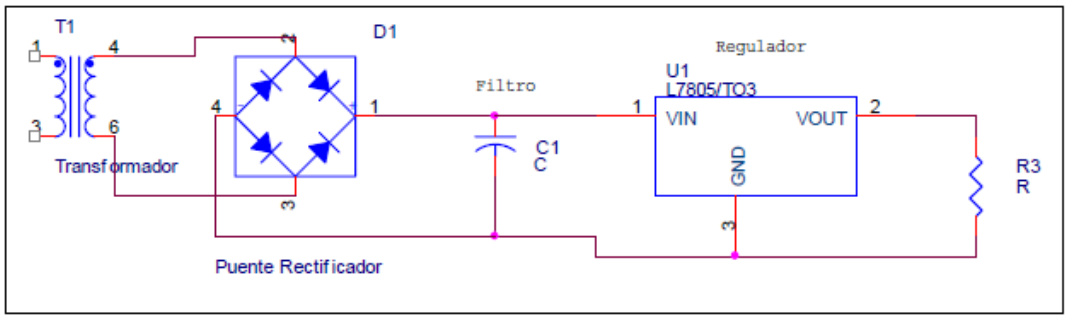

Figura 2.5 Fuente Lineal Regulada

A continuación se muestra el diagrama completo de la fuente de alimentación.

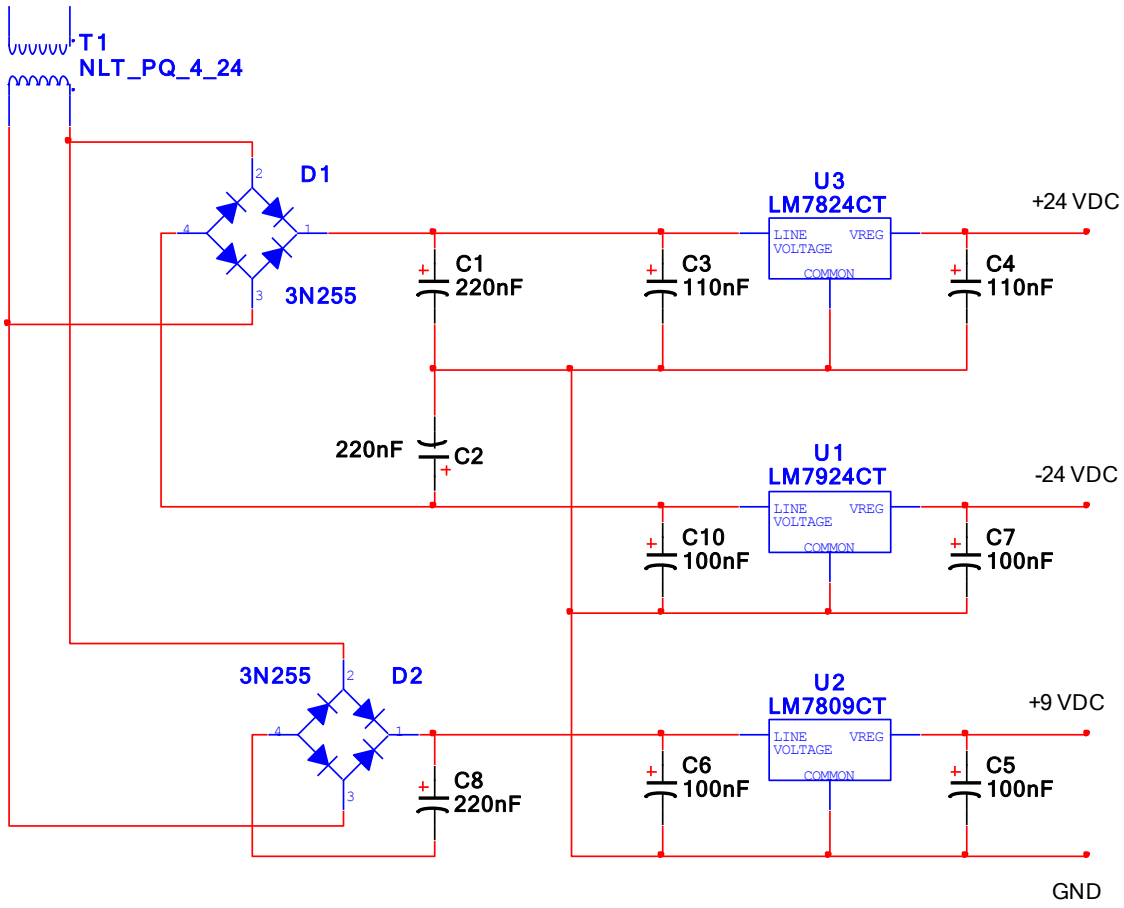

Figura 2.6 Circuito de fuente de alimentación para el *jammer*

Para evitar ruido por parte de la fuente de alimentación, se colocan capacitores de acoplamiento en los reguladores de voltajes como se muestra en la figura 2.6. En este caso se utiliza juegos de 2 capacitores de 100nF.

2.4.2 Sintonizador

El circuito sintonizador tiene la tarea de suministrar el voltaje de entrada al VCO. Esto se puede hacer mediante una onda de diente de sierra o una triangular. Para esta parte del *jammer* se opta por diseñar un circuito que genere una onda triangular con frecuencia variable, y un voltaje que oscile entre de 0.5V y 20V, debido a que el VCO que se va a utilizar trabaja entre estos valores. El aspecto de la frecuencia es muy importante debido a que GSM es un sistema que emplea SFH, y de esta forma puede ser que los saltos en

frecuencias protejan a la comunicación de la interferencia generada por el *jammer*. Lo anterior presenta dos escenarios: Si la variación del voltaje sintonizador es muy lenta no se alcanzará a barrer una parte amplia del espectro de manera que se intercepten los saltos en frecuencia; si la variación es muy rápida no será suficiente el tiempo que la señal del *jammer* interfiera con la señal original para imposibilitar la comunicación. La Figura 2.7 muestra el circuito generador de onda triangular unipolar.

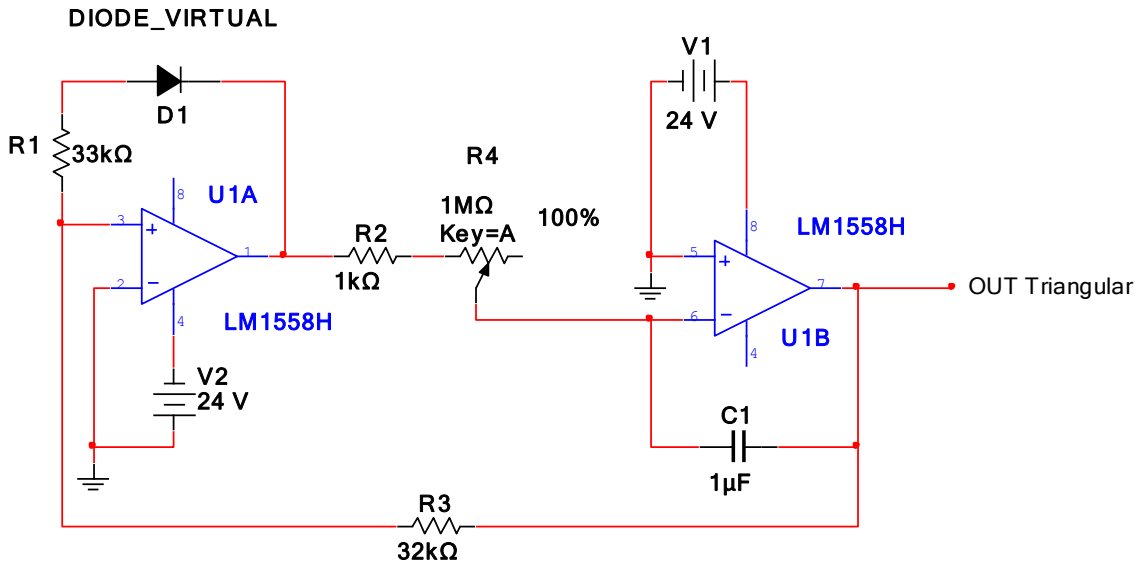

Figura 2.7 Generador de Onda Triangular unipolar

El circuito de la figura 2.7 es capaz de generar simultáneamente una señal de onda triangular y una de onda cuadrada, para lograr esto, se usa 2 operacionales uno que trabaja como comparador U1A y otro como integrador inversor U1B.

Para comprender como funciona el circuito, se supone que a la salida del comparador U1A está en nivel alto en el valor $+V_{sat}$. En estas condiciones se provoca el flujo de una corriente constante ($V_{sat}/R2+R4$) a través del condensador C1 (de izquierda a derecha), volviendo el voltaje del inversor U1B negativo, que pasa de V_{ut} a V_{lt}. Cuando el voltaje de salida de U1B llega a este valor la conexión 3 del comparador se vuelva negativa y el voltaje de salida de U1B cambia simultáneamente al valor $-V_{sat}$.

Cuando el valor de voltaje de la salida de U1A es $-V_{sat}$, se produce un flujo de corriente constante (de derecha a izquierda) a través de C_1, convirtiendo al voltaje de U1A en positivo, desde el valor V_{lt} hasta V_{ut}. En cuanto el voltaje de salida de U1A alcanza el valor V_{ut} la conexión 3 del comparador se vuelve positiva y el voltaje de salida de U1B cambia súbitamente a $+V_{sat}$, lo anterior da lugar al inicio del siguiente ciclo de oscilación. Todo lo anteriormente mencionado ocurre cuando no se encuentra el diodo D_1.

Para producir una onda triangular unipolar, basta con conectar un diodo en serie con R_1. Cuando el valor del voltaje de salida de U1A es de $+V_{sat}$, el diodo interrumpe el flujo de corrientes a través de R_1 y define V_{lt} a 0V. Cuando el voltaje de salida de U1A es $-V_{sat}$, el diodo permite el flujo de corriente por R_1 y define el valor de V_{ut}.

Los valores pico de la onda triangular se calculan a partir de la relación que existe entre las resistencias R_1, R_3 y los voltajes de saturación, todo ellos se calcula de la siguiente manera:

$$V_{UT} = \frac{-(-V_{sat} + 0.6V)}{P} \quad \textbf{Ecuación 2.1}$$

Donde

$$P = \frac{R_3}{R_1} \quad \textbf{Ecuación 2.2}$$

La frecuencia de operación se calcula aproximadamente por:

$$f \approx \frac{P}{2(R_2 + R_4)C_1} \quad \textbf{Ecuación 2.3}$$

Para la construcción del generador de onda triangular unipolar de +20V pico y con una frecuencia variable, se utilizará las ecuaciones descritas anteriormente.

$$V_{UT} = \frac{-(-V_{sat} + 0.6V)}{P}$$
$$20V = \frac{-(-20 + 0.6)}{P}$$
$$P = 0.97$$

Si se toma un valor de R3= 32KΩ entonces:

$$0.97 = \frac{32k}{R_1} \Rightarrow R_1 = 33K\Omega$$

Para el cálculo de la frecuencia, se toma una resistencia R2 de 1KΩ y un potenciómetro R4 de 1MΩ con el cual se puede variar las frecuencia, el valor del capacitor C1 será de 1uF.

Valor máximo de frecuencia:

$$f \approx \frac{P}{2(R_2 + R_4)C_1}$$
$$f \approx \frac{0.97}{2(1000 + 0)1*10^{-6}}$$
$$f \approx 485Hz$$

Valor mimo de frecuencia:

$$f \approx \frac{P}{2(R_2 + R_4)C_1}$$
$$f \approx \frac{0.97}{2(1000 + 1000000)1*10^{-6}}$$
$$f \approx 0.485Hz$$

Para los amplificadores operacionales su puede utilizar el integrado LM 1558, debido a que este posee dos amplificadores operaciones y la salida de voltaje puede variar entre ± 30V.

2.4.3 Generador de ruido Blanco

El ruido blanco se define como la presencia de todas las frecuencias audibles, es semejante a la luz, que contiene todo el espectro de los colores. Se escucha como un sssssssss**,** tal como se escucha en un receptor de radio en frecuencia modulada cuando no se modula la portadora o no hay una emisora sintonizada.

Si se utiliza el ruido como fuente de señal para analizar un circuito, el mismo debe tener una amplitud constante en la banda del espectro considerada. Esta es justamente la característica que define lo que se denomina "ruido blanco". Se trata de un tipo de señal que no posee frecuencia fija, pero sí se extiende por una amplia banda del espectro; en esta banda, en cada porción que se toma al azar, la señal tendrá la misma amplitud. El circuito que se va a describir produce una señal con estas características. Para entender el funcionamiento del circuito, se recordará que una de las fuentes de ruido de un circuito electrónico es la propia agitación de sus moléculas en función de la temperatura. Cualquier cuerpo que esté en una temperatura por encima del cero absoluto (-273ºC) produce ruidos debido a la agitación de sus átomos. En un semiconductor, esta agitación puede causar la liberación de portadores de cargas y en consecuencia la aparición de una cierta corriente de fuga.

Si se polariza un transistor inversamente, de modo que su juntura no conduzca ninguna corriente, aún así notaremos la circulación de una pequeña cantidad de portadores de cargas que se debe a la agitación térmica. No es preciso decir que esta corriente depende de la temperatura, pero es importante que los portadores sean liberados aleatoriamente, generando así una corriente no continua, pero sí pulsante de frecuencia que se extiende por todo el espectro (esta configuración se puede observar en Q1 del circuito del generador que se muestra en la figura 2.8). Los diodos de silicio, o la juntura entre el colector y la base de un transistor, son pues excelentes "generadores" de ruido blanco. Está claro que esta señal es muy débil, pues corresponde a portadores de cargas prácticamente aislados (electrones o lagunas), por lo que necesita de una buena amplificación.

Así, usando un transistor común polarizado inversamente, tenemos el generador de ruido, y con dos más tenemos las etapas de amplificación. Un potenciómetro nos permite hacer una cierta "ecualización" de este ruido, cortando componentes en la extremidad superior del espectro, donde un amplificador puede presentar una ganancia mayor (en el generador, el potenciómetro es R7). Los transistores pueden ser cualquier NPN de uso general de silicio. Como equivalentes a los BC548 tenemos los BC237, BC238, BC547, etc. Las resistencias son todas de 1/8 ó 1/4W con 5 ó 10% de tolerancia y los capacitores pueden ser de poliéster o de cerámica. La alimentación se hace con una fuente de 9V. La salida tiene una

señal de baja intensidad, alrededor de 100mV, que puede ser aplicada a la entrada de cualquier amplificador de audio. R7 es un potenciómetro lineal. Para probar el generador bastará conectar la salida a la entrada de cualquier buen amplificador de audio y después accionar. La señal debe ser reproducida claramente en el amplificador de audio. Ajuste R7 para modificar esta señal.

El capacitor C2 puede ser alterado para hacer más aguda la señal de este generador. Con su reducción, podemos aumentar la intensidad de la señal en la parte más alta del espectro.

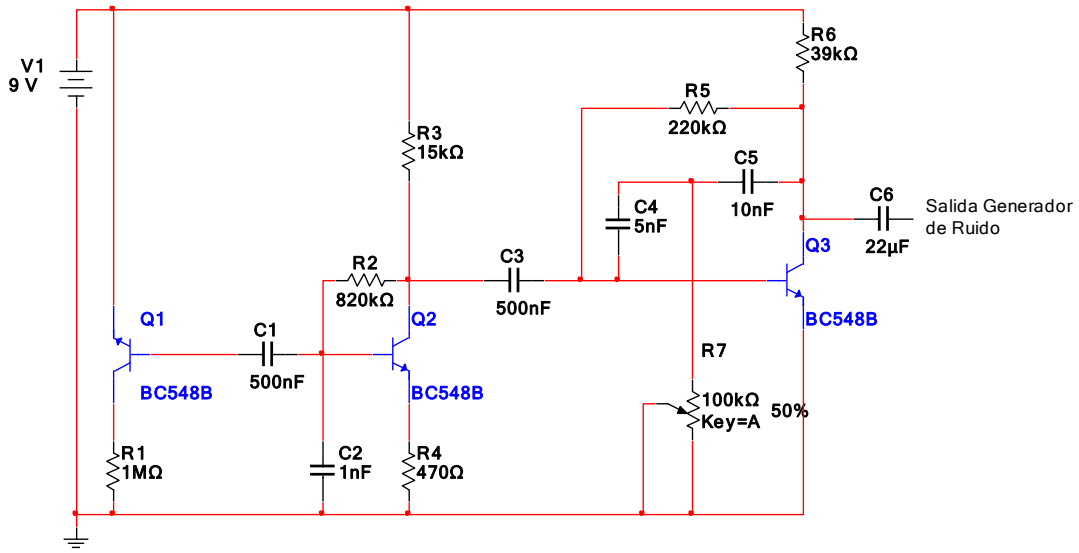

Figura 2.8 Generador de ruido Blanco

2.4.4 Mezclador de dos canales

El mezclador de canales servirá para sumar la señal triangular (Sintonizador) con la señal de ruido. Se diseñara un sencillo mezclador de dos canales con amplificadores operacionales y potenciómetros, que se utiliza para dar más peso a un canal que al otro en el momento de mezcla [17].

Lo primero que se considera es como se hace una mezcla o suma de voltajes con un amplificador operacional genérico (741, 358, 324, etc) , la entrada diferencial constituida por los pines + y - constituyen una tierra virtual y después de algunos cálculos llegamos a la expresión general siguiente :

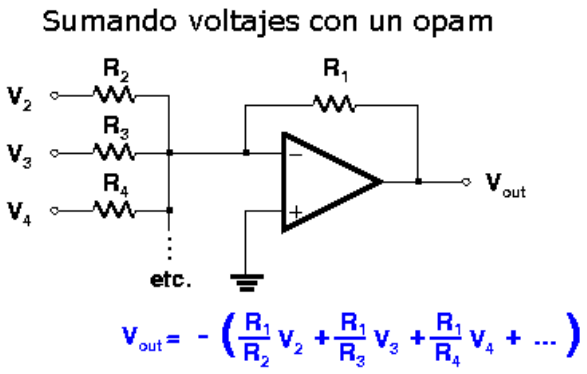

Figura. 2.9 Sumador de voltajes

Donde V1, V2; V3..... son los voltajes de entrada en el caso de la figura 2.9 voltajes continuos y también alternos que se suman de acuerdo a un "peso" dado por el cociente de la resistencia de realimentación y la propia resistencia de entrada, esta resistencia puede ser variada cambiando su valor como en la figura o sacándola desde un potenciómetro, cuanto más grande sea la resistencia de entrada a la sumadora la amplificación es menor, si todas las resistencias son iguales la salida será la suma de los voltajes de entrada multiplicados por un factor -Rf/Rin el signo menos indica que la señal sale invertida o desfasada 180 grados. Para este caso se tiene 2 entradas, las mismas que se van a sumar como se indico en la figura 2.9, el factor de amplificación será de 1 por tanto los potenciómetros darán el mismo "peso" para cada señal sumada. Esta primera salida está invertida, como se desea que la señal no sea inversa se volverá a invertir con un segundo amplificador operacional.

Debido a que todos los amplificadores operacionales tendrán la misma impedancia o resistencia de salida (muy baja) se usa resistencias altas como de 100KΩ

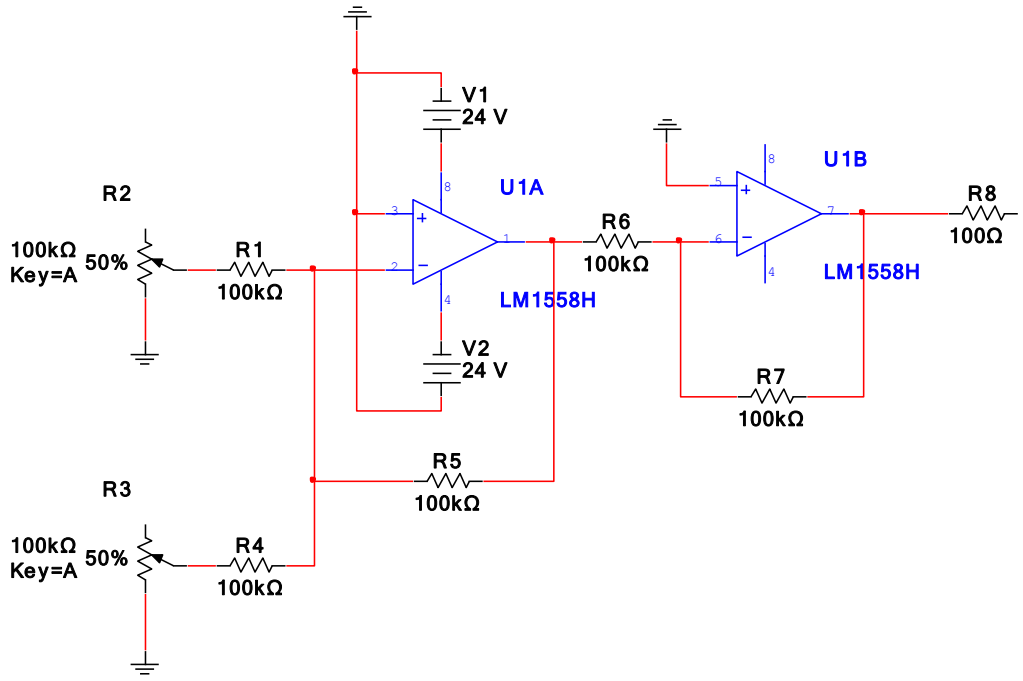

Figura 2.10 Mezclador de dos canales

Para este circuito también se utilizo el integrado LM1558, puesto que tiene dos amplificadores operaciones y trabaja a ± 24V.

2.4.5 Oscilador controlador por voltaje

El centro medular del jammer es el oscilador controlado por voltaje. Un Oscilador controlado por tensión o VCO (*Voltage-controlled oscillator*) es un dispositivo electrónico que usa amplificación, realimentación y circuitos resonantes que da a su salida una señal eléctrica de frecuencia proporcional a la tensión de entrada. Típicamente esa salida es una señal sinusoidal, aunque en VCOs digitales es una señal cuadrada.

Cuando la entrada es 0V, el VCO tiene una señal con una frecuencia llamada frecuencia libre de oscilación y ante variaciones de la entrada, sube o baja la frecuencia de su salida de forma proporcional.

Una aplicación típica de los VCO es generar señales moduladas en frecuencia (FM). También son usados como parte de Bucles de enganche de fase. Suelen emplearse en aplicaciones electrónicas de comunicaciones. En su construcción pueden emplearse distintos dispositivos, siendo los más habituales los diodos varicap y los cristales de cuarzo.

Este tipo de osciladores suele presentar problemas debido a que los cambios de temperatura (humedad) afectan a la afinación del mismo. Se tiene dos opciones, buscar un integrado que realice esta función o diseñar. Debido a que las frecuencias a las que se va a trabaja son del orden de gigahertz, la fabricación del VCO es complicada. La dificultad radica en la depuración, ya que a esas frecuencias cualquier componente puede funcionar como antena. Es por eso que se opta por buscar un integrado VCO.

Se eligió el modelo DCMO80210-10 de SINERGY ® (figura 2.11) porque teóricamente este VCO hace un barrido de 660 a 2100MHz como se puede ver en la Tabla 2.2 y en la figura 2.12.

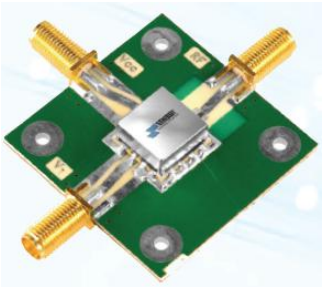

Figura 2.11 VCO DCMO80210-10

Tabla 2.2 Relación entre el voltaje sintonizador y la frecuencia de salida para el DCMO80210-10 [17]

Voltaje de entrada (V)	Frecuencia (MHZ)
0.5	800
5	900
8	1150
12	1450
15	1700
18	1850
24	2100

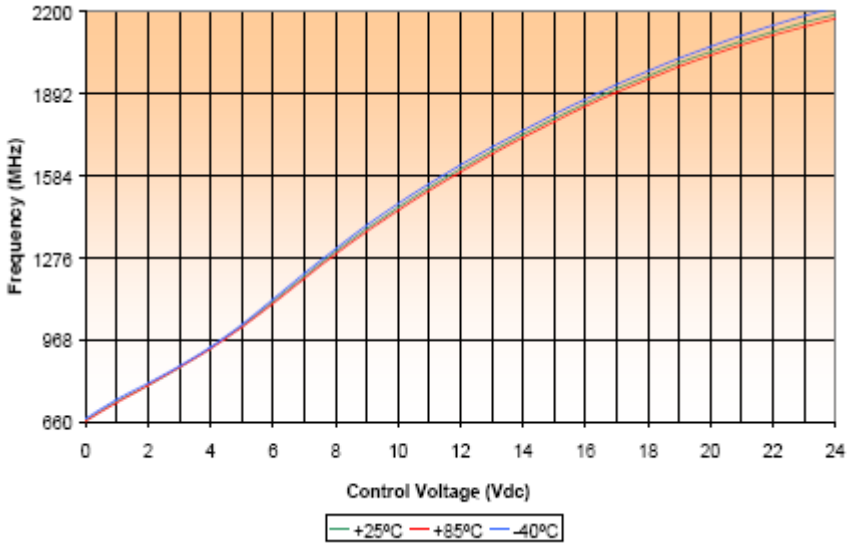

Figura 2.12 VDC vs Frecuencia DCMO80210-10 [17]

El voltaje que se va a suministrar para el barrido en frecuencia es de 0 a 20 V, con lo que se consigue frecuencia de salida desde 660 MHz hasta 2050Mhz, garantizando así una cobertura en las bandas deseadas; hay que tomar en cuenta que al realizar este barrido de frecuencias se van a ver afectadas bandas intermedias, en la tabla 2.3 se muestran las asignaciones otorgadas en estas frecuencias. Después de analizar esta tabla se concluye que las bandas afectadas no son utilizadas en los sitios donde se pretende anular la comunicación telefónica móvil; mas adelante en este proyecto de tesis se va determinar en qué dependencias sería útil y legal suspender este servicio.

Frecuencia	Asignación
614- 806	Radio fusión
806-890	Móvil
890-902	Móvil aeronáutico, radio localización
902-928	Fijo
928-942	Móvil aeronáutico
942-960	Móvil
960-1164	Radio navegación aeronáutica, móvil aeronáutica (R)
1164-1215	Radio navegación aeronáutica, radio navegación por satélite (espacio – tierra)
1215-1300	Exploración de la tierra por satélite, radio localización, radio navegación por satélite (espacio - tierra), investigación espacial
1300-1350	Navegación aeronáutica, radio localización, radionavegación por satélite (tierra – espacio)
1350-1400	Radio localización
1400-1427	Exploración de la tierra por satélite, radio astronomía, investigación espacial
1427-1518	fijo
1518-1559	Móvil por satélite (espacio – tierra)
1559- 1610	Radio navegación aeronáutica
1610- 1660.5	Móvil por satélite (tierra – espacio)
1660.5- 1668	Radio astronomía, investigación espacial
1668- 1668.4	Móvil por satélite (tierra – espacio)
1668.4- 1670	Ayuda a la meteorología, móvil por satélite
1670- 1690	Fijo
1690- 1700	Ayuda meteorológica por satélite
1700- 1710	Meteorología por satélite (espacio - tierra)
1710- 2025	Móvil

Tabla 2.3 Asignación de frecuencias (Plan nacional de frecuencias CONATEL)

2.4.6 Amplificación RF

El amplificador de potencia (PA) es la última etapa del emisor. Tiene la misión de amplificar la potencia de la señal (de este dependerá el área de cobertura) y transmitirla a la antena con la máxima eficiencia. A continuación se mencionan algunas características de un PA para equipos de comunicaciones móviles y sus valores típicos:

- Potencia de salida, s_o +20 a +30 dBm
- Eficiencia, η 30% a 60%
- Ganancia, G_P 20 a 30 dB
- Distorsión, IMR –30 dB (*)
- Control de potencia ON – OFF

(*) Para cada armónico se define IMR = s_o(armónico)/s_o(útil) cuando la entrada es la suma de dos tonos con el mismo nivel, aquel que hace s_o(útil) = $s_{o,\,max}$ – 6 dB [19].

Justamente las armas inteligentes, guerras electrónicas o radas, indujeron a la creación y desarrollo de amplificadores miniatura de bajo ruido, que proporcionan buena linealidad y bajo consumo de corriente en aplicaciones de banda ancha en VHF-UHF donde la potencia de la señal puede variar, tal es así que se crean amplificadores de potencia MMIC (*Monolithic Microwave Integrated Circuits*), que son un tipo de circuitos integrados que operan en frecuencias de microondas, es decir, entre 300 MHz y 300 GHz. La técnica de fabricación de los circuitos MMIC se basa en la utilización de líneas de transmisión planares, y se realiza con combinados de semiconductores compuestos, tales como el arsenurio de galio (GaAS), nitrato de galio (GaN) y el germanio de silicio (SiGe).

Los amplificadores MMIC de potencia son redes de dos puertas internamente formados por la combinación de sucesivas etapas de transistores en paralelo (etapas de amplificación). Estos constan por tanto de:

- Elementos activos para amplificar la señal de radiofrecuencia.
- Circuitos de microondas (redes de combinación, acopladores, líneas de transmisión, estructuras filtrantes…..) para obtener la respuesta en radio frecuencia deseada.
- Elementos como pistas, bobinas, condensadores, resistencia, etc., necesarios para proporcionar la polarización adecuada a cada uno de los transistores que los integran.
- Accesos metalizados para poder inyectar al dispositivo y extraer de él tanto la señal de radiofrecuencia como las señales de polarización e incluso control que pudieran existir.

- Otros elementos destinados a la protección del amplificador, a su estabilidad en la banda de frecuencias de trabajo y a la de gestión de la potencia disipada en el mismo.

En la figura 2.13 se muestra la configuración para un amplificador MMIC de potencia [20].

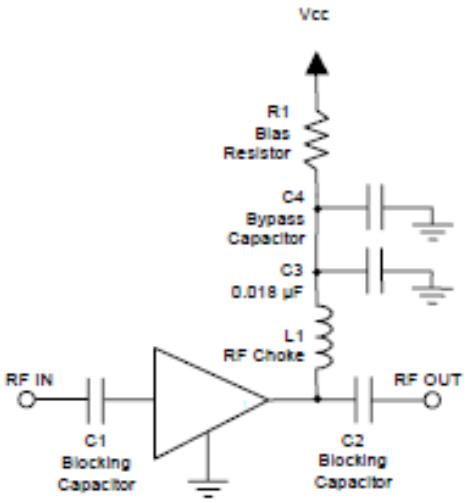

Figura 2.13 Configuración básica de un amplificador MMIC de potencia.

El cálculo de C1, C2, C4 y L1 para el amplificador de potencia se los puede obtener mediante el programa AppCad versión 3.0.2, este programa nos permite ingresar datos como:

- Frecuencias en las que va a operar el amplificador
- Impedancia de entrada y salida
- Ganancia

Los valores de los capacitores y del inductor se muestran en la figura 2.14, y el de R1 está dado de acuerdo al MMIC que se utilice.

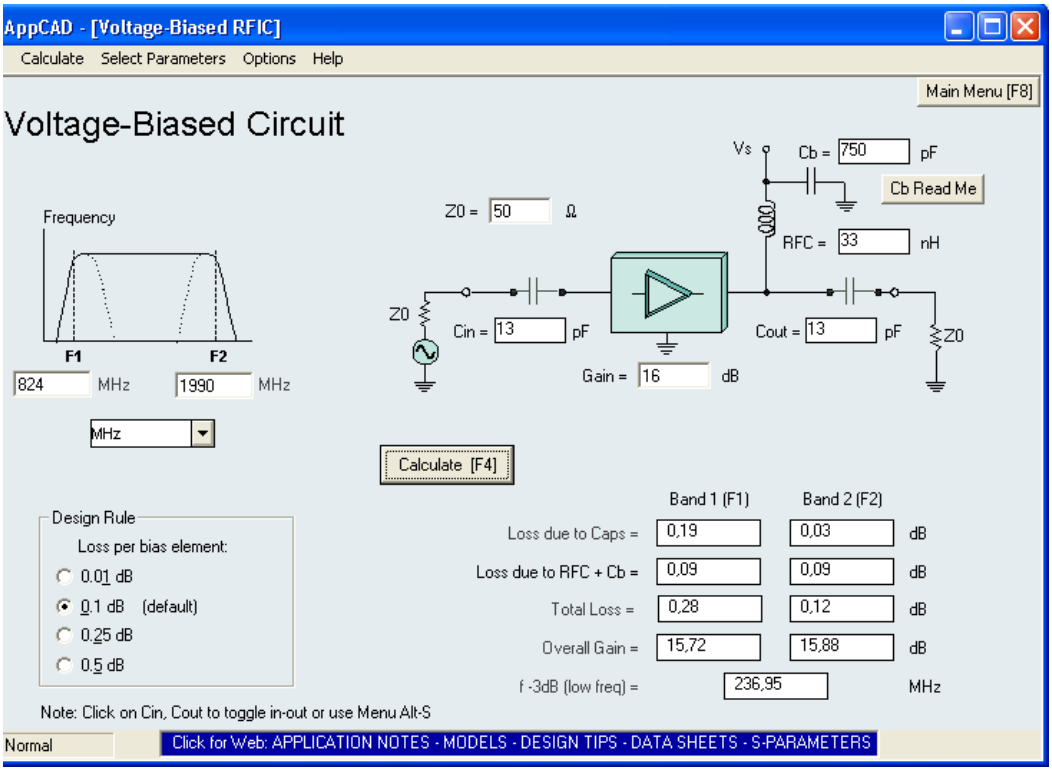

Figura 2.14 Valores para los componentes del amplificador MMIC de potencia (Appcad)

La elección del MMIC dependerá esencialmente:

- De las frecuencias de operación
- Ganancia
- Tecnología a las que se vaya aplicar
- Voltaje de alimentación
- Disponibilidad en el mercado

Para este caso se utilizará el MMIC AG603-83, puesto que cumple con todos los parámetros requeridos; El valor de R1 es de 51Ω, puesto que se alimentara con un voltaje de 9V (Datasheet AG603-86).

2.4.7 Acondicionamiento de la señal

El acondicionamiento de la señal para las diferentes etapas del circuito se puede modificar por medio de dispositivos externos.

Es así que el circuito posee cinco potenciómetros de precisión con valores de 100MΩ (frecuencia de la señal triangular), 33kΩ (amplitud de la señal triangular), 100KΩ (frecuencia de la señal de ruido) y dos de 15KΩ (mezclador de dos canales). Los ajustes son necesarios porque la realidad difiere de la teoría, y al presentarse estas variaciones es necesario acondicionar la señal que alimenta al VCO. Además, al afectarse la frecuencia se altera la amplitud debido a características propias de los diferentes integrados. La amplitud debe estar entre 0V y 20V y a la frecuencia adecuada para garantizar la interrupción de la comunicación entre radiobase y unidad móvil. El valor exacto y óptimo se obtiene mediante prueba debido a la inexistencia de un método. A parte de estos potenciómetros se utiliza una perlita de ferrita 43 para la entrada del amplificador RF evitando así que las señales de alta frecuencia lleguen al circuito electrónico.

2.4.8 Línea de transmisión y antena

La línea de transmisión es cualquier sistema de conductores, semiconductores, o la combinación de ambos, que puede emplearse para transmitir información, en la forma de energía eléctrica o electromagnética entre dos puntos [20].

Las características de una línea de transmisión se determinan por sus propiedades eléctricas, como la conductancia de los cables y la constante dieléctrica del aislante, y sus propiedades físicas, como el diámetro del cable y los espacios del conductor.

Para una máxima transferencia de potencia, desde la fuente a la carga (no hay energía reflejada), una línea de transmisión debe terminarse en una carga puramente resistiva igual a la impedancia característica de la línea.

La impedancia característica (Zo), de una línea de transmisión es una cantidad compleja que se expresa en Ohms, que idealmente es independiente de la longitud de la línea, y que no puede medirse.

La impedancia característica (resistencia a descarga) se define como la impedancia que se ve desde una línea infinitamente larga o la impedancia que se ve desde el largo finito de una línea que se determina en una carga totalmente resistiva igual a la impedancia característica de la línea.

Una línea de transmisión almacena energía en su inductancia y capacitancia distribuida. Las líneas de transmisión frecuentemente se consideran totalmente sin perdidas. Sin embargo, en realidad, hay varias formas en que la potencia se pierde en la línea de transmisión, estas son:

- Pérdida del conductor,
- Pérdida por radiación por el calentamiento del dieléctrico,
- Pérdida por acoplamiento,
- y descarga luminosa (efecto corona).

Las líneas de transmisión de conductores paralelos son apropiadas para las aplicaciones de baja frecuencia. Sin embargo, en las frecuencias altas, sus pérdidas por radiación y pérdidas dieléctricas, así como su susceptibilidad a la interferencia externa son excesivas.

Los conductores coaxiales se utilizan extensamente, para aplicaciones de alta frecuencia, para reducir las pérdidas y para aislar las trayectorias de transmisión. El cable coaxial básico consiste de un conductor central rodeado por un conductor exterior concéntrico (distancia uniforme del centro).

A frecuencias de operación relativamente altas, el conductor coaxial externo proporciona una excelente protección, el uso de la protección no es costeable. Además el conductor externo de un cable coaxial generalmente está unido a tierra, lo que limita su uso a las aplicaciones desbalanceadas.

Esencialmente, hay dos tipos de cables coaxiales: líneas rígidas llena de aire y líneas sólidas flexibles, En una línea coaxial rígida de aire, el conductor central está rodeado de forma coaxial por un conductor externo tubular y el material aislante es el aire. El conductor externo físicamente está aislado y separado del conductor central por un espaciador, que generalmente está hecho de Pirex, poliestireno, o algún otro material no conductivo.

En un cable coaxial sólido flexible, el conductor externo estará trenzado, es flexible y coaxial al conductor central. El material aislante es un material de poliestireno sólido no conductivo que proporciona soporte, así como aislamiento eléctrico entre el conductor interno y externo. El conductor interno es un cable de cobre flexible que puede ser sólido o hueco. Los cables coaxiales rígidos llenos de aire son relativamente caros en su fabricación, y el aislante de aire debe de estar relativamente libre de humedad para minimizar las pérdidas, por tal motivo se utiliza cable coaxial sólido flexible.

Los cables coaxiales son relativamente inmunes a la radiación externa, ellos en sí irradian muy poca, y pueden operar a frecuencias más altas que sus contrapartes de cables paralelos. Otro razón por la que se utiliza cable coaxial es que al no ser un par de cables balanceados, no se elimina el ruido que se está trasmitiendo, recordemos que los cables balanceados tiene la ventaja que la mayoría de la interferencia por ruido (voltaje de modo común) se induce igual mente en ambos cables, produciendo corrientes longitudinales que se cancelan en las carga [22].

El cable coaxial apropiado es el RG-8/U, puesto que posee una impedancia de 50 ohmios, alta precisión y ofrecen unas características excelentes de bajas pérdidas y mínimo ruido debido a la tecnología exclusiva en su pantalla [23].

El dieléctrico que se debe emplear para la placa del circuito es fibra de vidrio, debido a este material por su disponibilidad y precio es el apropiado para este circuito. Las características son las siguientes:

- Permitividad relativa de 4
- Pérdida tangente de 0.026
- Altura de 1.55mm.
- Impedancia característica de 50Ω.

Por último, la antena servirá para transmitir la onda guiada por la línea de transmisión (el cable o guía de onda) en ondas electromagnéticas por el espacio libre. La antena debe de dotar a la onda radiada con un aspecto de dirección. Es decir, deben acentuar un solo aspecto de dirección y anular o mermar los demás. Esto es necesario ya que solo nos interesa radiar hacia una dirección determinada.

La antena que se elija dependerá de algunos factores como son:

- Ancho de banda
- Ganancia (este parámetro es importante ya que influye en el área de cobertura)
- Perdida
- Potencia de transmisión
- Impedancia

Después de tomar en cuenta estos parámetros, Se elige La antena OMNI-A0085, La tecnología empleada en su diseño asegura que el rendimiento de la antena es consistente en todas las bandas de frecuencia (GSM 800, 900MHz, 1800MHz a UMTS 2100MHZ). La antena está polarizada verticalmente. Esta antena puede ser fijada directamente a cualquier equipo GSM. La base giratoria de la antena permite múltiples ángulos de despliegue para acomodar la orientación del equipo [24].

Características:

- Antena de perfil bajo.
- Plano de tierra no requerido.
- Antena giratoria para permitir múltiples ángulos de despliegue
- Código de Producto OMNI-A0085
- Frecuencia de operación:
    - 824 - 894 MHz
    - 880 - 970 MHz
    - 1710 - 1880 MHz
    - 1950 - 2200 MHz
- Ganancia 0 - 2 dBi
- Polarización Lineal

La conexión entre la antena y la línea de transmisión se hace por medio de conectores SMA (SubMiniature versión A). Este tipo de conectores están acoplados a 50 y garantizan la transferencia de energía a frecuencias hasta de 18GHz.

CAPÍTULO III

SIMULACIÓN DEL FUNCIONAMIENTO DE LAS DIFERENTES ETAPAS DEL JAMMER Y PRESENTACIÓN DE RESULTADOS

Antes de armar cualquier esquema, es conveniente probar el funcionamiento individual de cada componente, asegurándose así el correcto funcionamiento de las diferentes etapas del circuito, para una futura implementación.

Las etapas del circuito simuladas fueron cuatro: alimentación del circuito, el ajuste del sintonizador, generador de ruido y mezclador de canales. Para estas simulaciones se utilizó el programa Multisim V.10.

3.1 Simulación de la fuente de alimentación

La primera etapa a probar y analizar es la alimentación del circuito. Tal como se mencionó en el capítulo II la alimentación utiliza un transformador de 24V, 2 puentes de diodos 3N255, 3 capacitores electrolíticos de 220nF, 6 capacitores electrolíticos de 100nF y los reguladores de voltaje LM7824, LM7924 y LM7809 para obtener salidas de +24 V, -24V y +9 V.

Para verificar el comportamiento, se efectuó una simulación. En la figura 3.1 se muestra el esquema utilizado para las mediciones de la fuente de alimentación, y en la figura 3.2 se observa los resultados obtenidos.

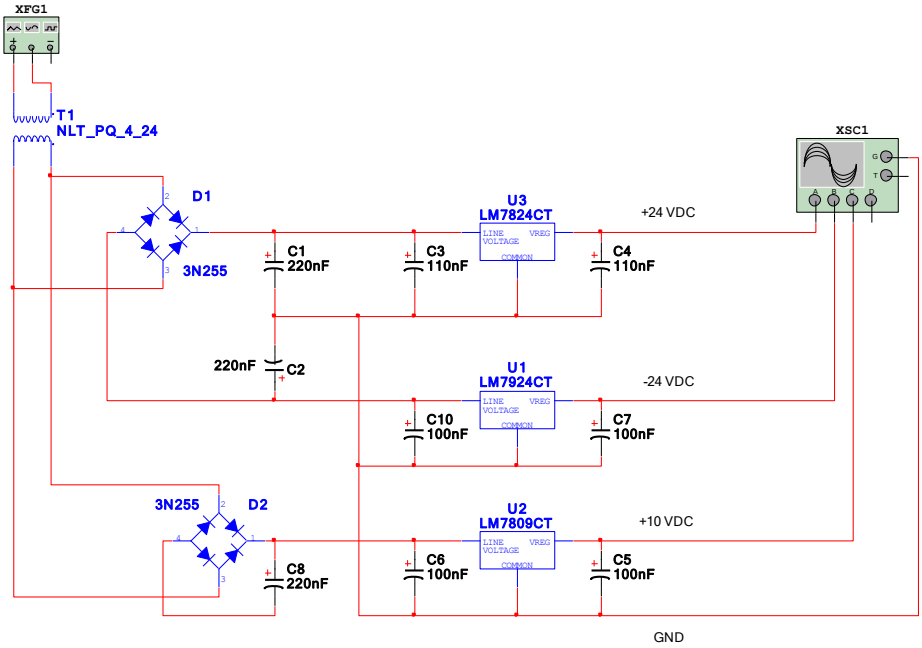

Figura 3.1 Circuito de la fuente de alimentación

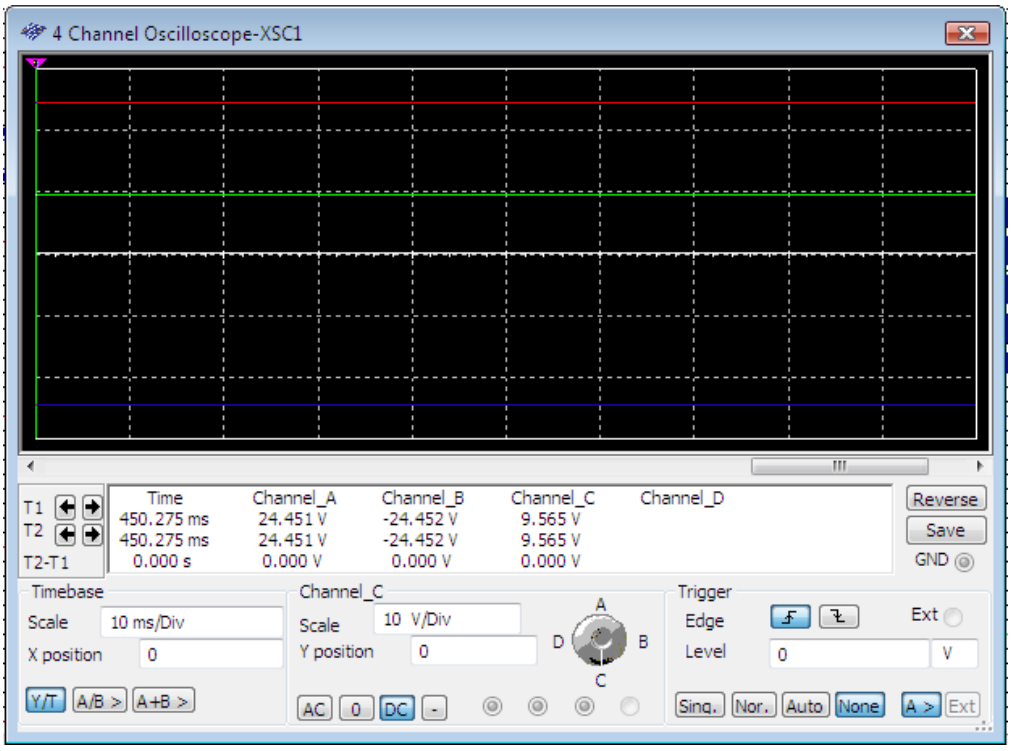

Figura3.2 Salidas de los reguladores de voltajes LM7824CT, LM7924CT y LM7809CT

Los valores obtenidos fueron de 24.451 V, -24.452 y 9.565 V, lo cual es aceptable en todo el rango que se permite para un buen funcionamiento del resto de componentes que van hacer alimentados.

3.2 Simulación del sintonizador

Para la simulación del sintonizador se utilizó valores que fueron calculados en el anterior capítulo. En la Figura 3.3 se muestra el circuito encargado de generar la onda triangular, para el cual se utilizó tres resistencias una de 33KΩ, otra de 32KΩ y una de 1KΩ, además un potenciómetro de 1MΩ, un capacitor de 1uF y el integrado LM1558.

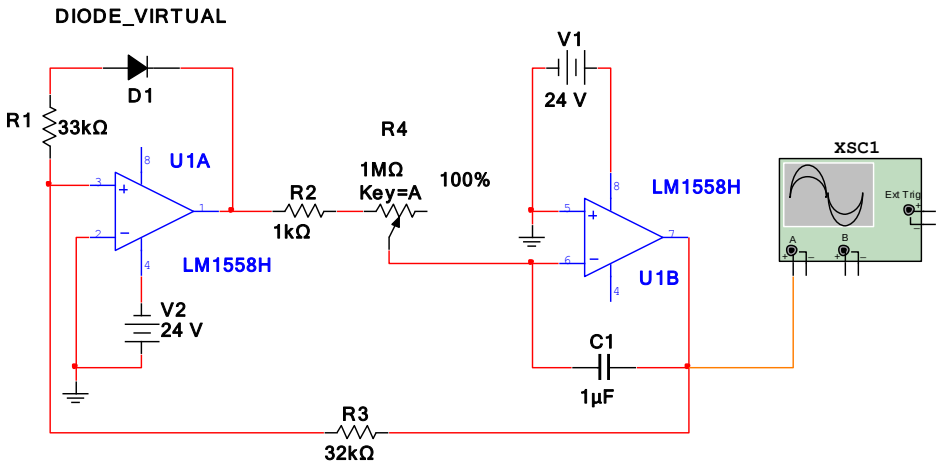

Figura 3.3 Circuito generador de onda triangular

La Figura 3.4 muestra el resultado de esta simulación. Se puede ver que el valor máximo es de 20.351 V y el mínimo de -224.050 mV. El valor de la frecuencia esta dado por el potenciómetro R_4 el cual se encarga de variar.

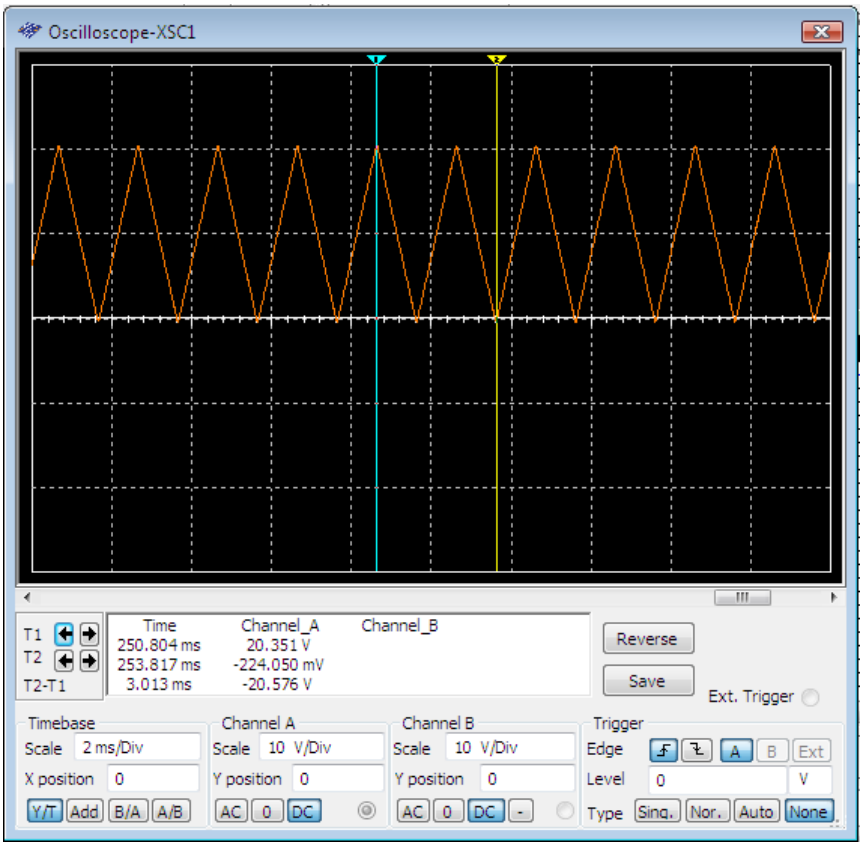

Figura 3.4 Salida del generador de onda triangular

3.3 Simulación del generador de ruido

Para visualizar el comportamiento del circuito generador de ruido blanco figura 3.5, se ha realizado la simulación del mismo utilizando un analizador de señal, puesto que la salida de este generador presenta un voltaje pequeño que no se puede observar en un osciloscopio normal. El generador de ruido blanco utiliza 6 resistencias (1MΩ, 820kΩ, 220KΩ, 39KΩ, 15KΩ y 470Ω), un potenciómetro de 100KΩ, 6 capacitores (2 de 500nF, 1nF, 5nF, 10nF y 22uF) y 3 transistores BC548B.

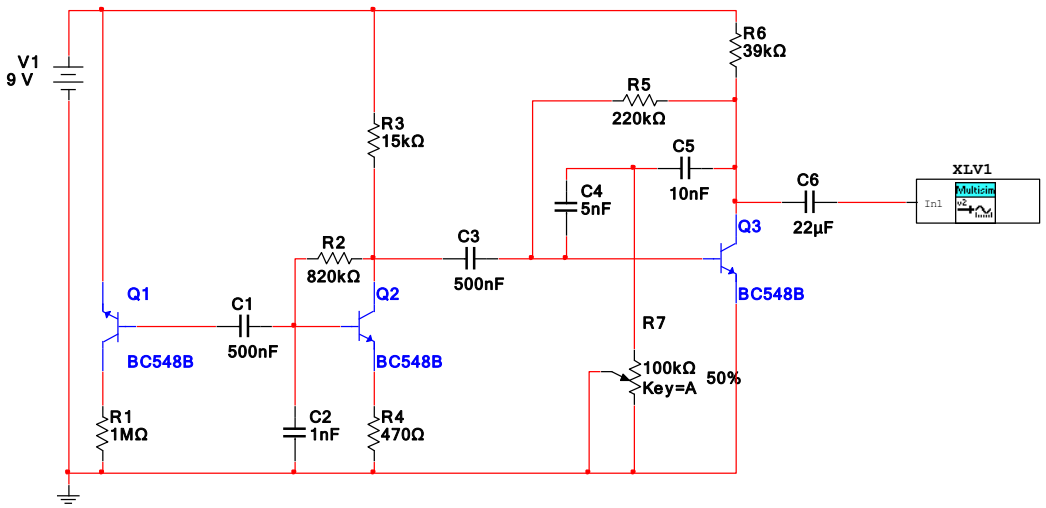

Figura 3.5 Generador de ruido

Si se observa la figura 3.5 la señal no posee una frecuencia fija, y la amplitud sufre mínimas variaciones, presentando así un valor máximos de 2^{-9} V y un mínimo de aproximado de 1^{-9}.

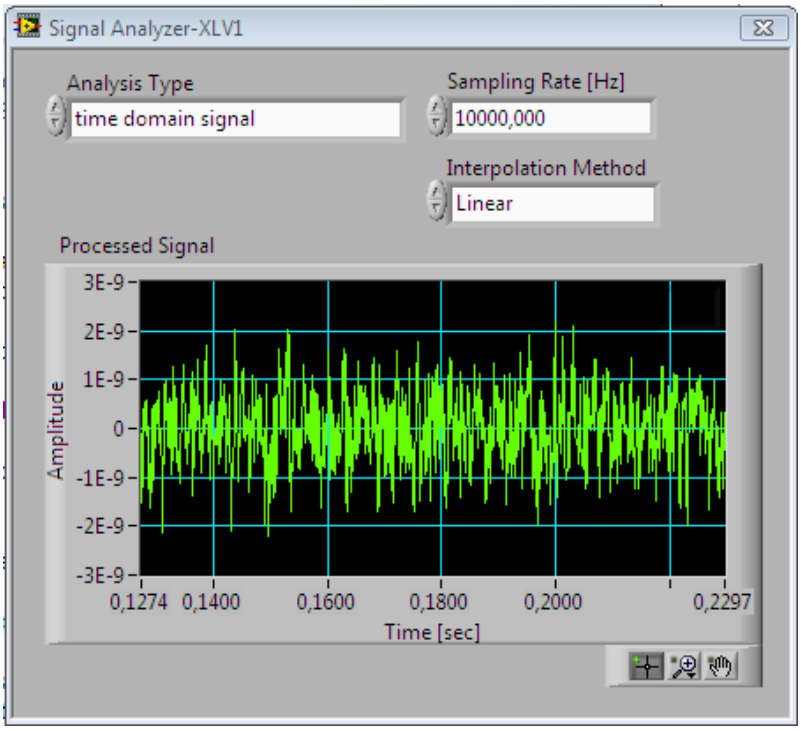

Figura 3.6 Salida de generador de ruido

3.4 Simulación del mezclador de dos canales

Antes de aplicar la señal triangular al VCO, es necesario combinar esta señal con el ruido blanco anteriormente generado, para lo cual se diseño un mezclador de dos canales con ganancia 1, mismo que se observa en la figura 3.7 y que utiliza 2 potenciómetros de 100KΩ, 5 resistencias de 100ΩK, una resistencia de 100Ω y el un integrado LM1558.

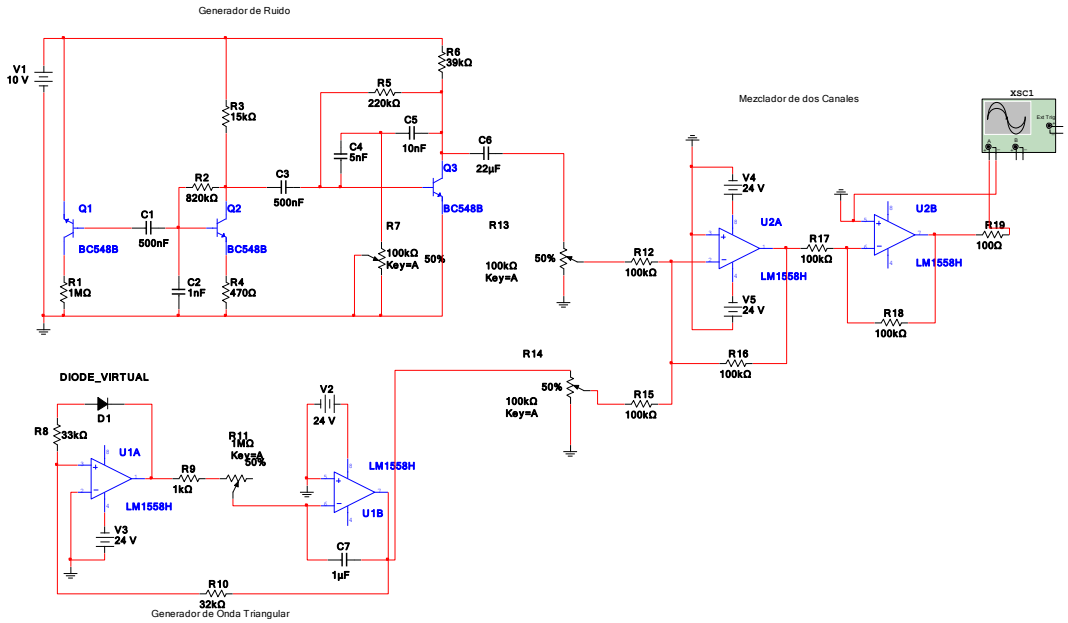

Figura 3.7 Circuito mezclador de dos canales

En la figura 3.8 se muestra el resultado obtenido de la simulación del circuito mezclador de canales, teniendo como resultado un voltaje máximo de 21.100 V y un mínimo de 437.971 mV.

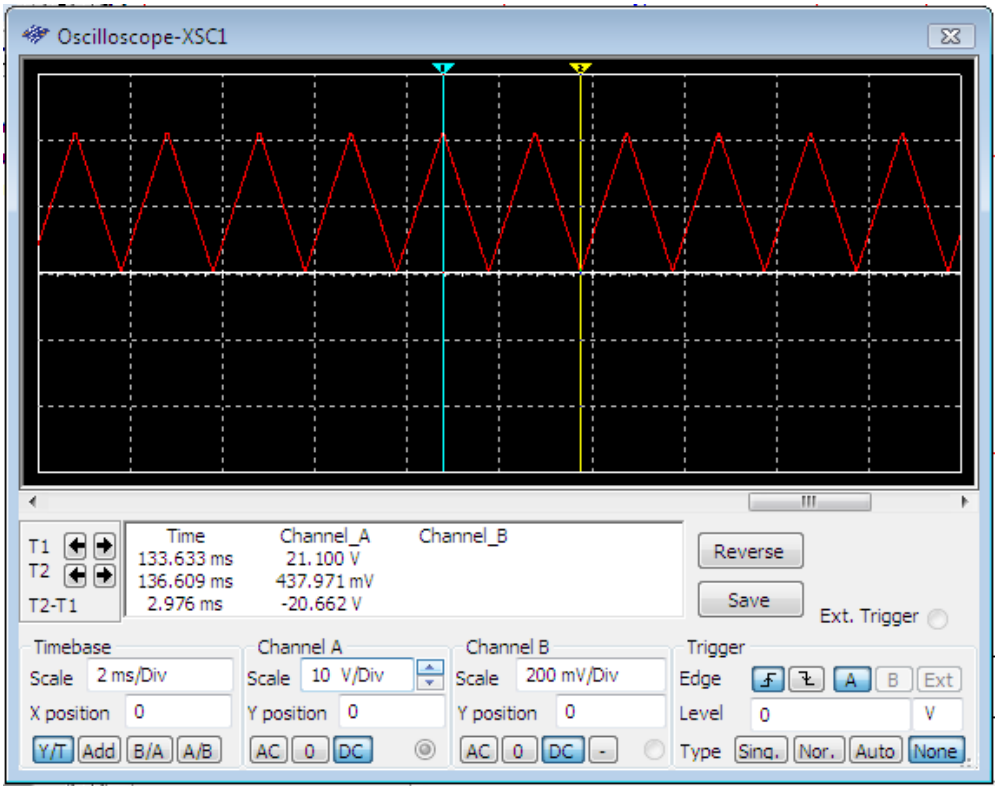

Figura 3.8 Salida del mezclador

3.5 Preedición de potencia

El área de cobertura del jammer, depende esencialmente de cuatro factores:

- Banda de operación del jammer.
- Ganancia del amplificador RF de potencia.
- Ganancia de la antena del jammer.
- La distancia a la que se encuentre el jammer respecto a la radiobase.

Para realizar el cálculo del área de cobertura se pueden utilizar modelos de propagación, tanto para la radiobase como para el jammer. Para el primer caso se recurrió al modelo Okumura-Hata, donde la ecuación de pérdida es:

$$L(dB) = 69.55 + 26.16 \log f_c - 13.82 \log h_{te} - a(h_{re}) + (44.9 - 6.55 \log d)$$ **Ecuación 3.1**

Donde:

f_c: Frecuencia de la portadora en Mhz

h_{te}: Altura de la antena transmisora en metros para un rango de 3 a 300 metros.

h_{re}: altura de la antena receptora en el rango de 1 a 10 metros.

$a(h_{re})$: factor de corrección por la altura efectiva del móvil que es función del tipo de área de servicio.

d: Distancia entre el transmisor y el receptor en kilómetros.

Los valores de $a(h_{re})$ se pueden definir para diferentes ambientes de propagación. Tal es así que se tiene [25].

- Ciudades pequeñas y medianas:
  $a(h_{re}) = (1.11\log f_c - 0.7)\, a(h_{re}) - (1.56\log f_c - 0.8)$ **Ecuación 3.2**
- En ambientes suburbanos:
  $a(h_{re}) = L(\text{urbano}) - 2(\log(f_{c/28}))^2 - 5.4$ **Ecuación 3.3**
- En areas rurales:
  $a(h_{re}) = L(\text{urbano}) - 4.78(\log f_c)^2 + 18.33\log f_c - 40.94$ **Ecuación 3.4**
- Para ciudades grandes con frecuencias menores a 300Mhz
  $a(h_{re}) = 8.29L(\log 1.54\, h_{re})^2 - 1.1$ **Ecuación 3.5**

Para el cálculo de la potencia transmitida se utiliza la siguiente fórmula:

$$P_L/P_T = -L + G_T + G_r \quad (\text{dB})$$ **Ecuación 3.6**

En este caso se tomo valores: para la potencia transmitida de 20W, altura de la antena 30m, frecuencia de 850Mhz y la ganancia de la antena receptora de 0dB, con lo que se obtuvo valores que se muestran en la tabla 3.1.

d(km)	L_p(dB)	P_{rx}(dBm)|P_{tx}=20W
0.03	86.7872052	-43.77690524
0.035	89.1453963	-46.13509625
0.04	91.1881542	-48.17785422
0.045	92.9899944	-49.97969445
0.05	94.6017955	-51.59149545
0.055	96.0598468	-53.04954682
0.06	97.3909434	-54.38064342
0.065	98.6154336	-55.6051336
0.07	99.7491344	-56.73883443
0.075	100.804585	-57.79428466
0.08	101.791892	-58.7815924
0.085	102.719325	-59.70902547
0.09	103.593733	-60.58343263
0.095	104.420851	-61.41055084
0.1	105.205534	-62.19523363
0.2	115.809272	-72.79897182
0.3	122.012061	-79.00176102
0.4	126.41301	-83.40271
0.5	129.826651	-86.81635123
0.6	132.615799	-89.60549921
0.7	134.97399	-91.96369022
0.8	137.016748	-94.00644818
0.9	138.818588	-95.80828841

Tabla 3.1 Modelo Okumura-Hata (Se puede ver como a mayor distancia la señal se va atenuando más)

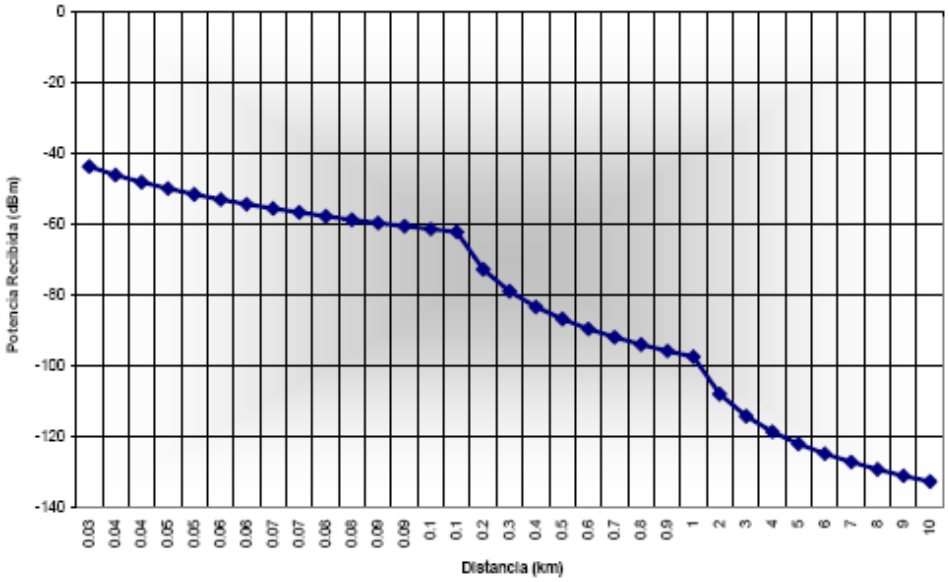

Figura 3.10 Gráfica del modelo Okumura-Hata

Para predecir el comportamiento del jammer se utilizó el modelo ITU para interiores, puesto que es el más estable debido a la utilización de variables que pueden conocerse sin necesidad de mediciones, con lo que se puede determinar en parte que este modelo es mitad teórico y mitad experimental.

$$L_T = 20 \log f_c + 10\ n \log r + L_f(n_f) - 28$$ **Ecuación 3.7**

Donde:

f_c es la frecuencia de transmisión en Ghz.

n es el factor de pérdidas por atenuación exponencial.

r es la distancia en metros dentro del edifico entre el transmisor y el receptor.

$L_f(n_f)$ es el factor de perdidas por penetración en pisos.

El factor de pérdidas por atenuación exponencial (n) depende de la frecuencia de utilización y del ambiente en el que se propaga la señal, los valores para este se pueden tomar de la tabla 3.2.

Frecuencia	**Tipo de ambiente**		
	Residencial	*Oficina*	*Comercial*
0.9 Ghz	----------	3.3	2.0
1.2-1.3 Ghz	----------	3.2	2.2
1.8-2.0 Ghz	2.8	3.0	2.2
4.0 Ghz	----------	2.8	2.2
60.0 Ghz	----------	2.2	1.7

Tabla 3.2 Diferentes valores para la atenuación exponencial.

Los valores de las pérdidas por penetración en pisos, a partir del valor n_f, que es el número de pisos penetrados se puede tomar de la tabla 3.3 [26]

Frecuencia	**Tipo de ambiente**		
	Residencial	*Oficina*	*Comercial*
0.9 Ghz		9 para un piso 19 para dos pisos 24 para tres pisos	
1.8- 2.0 Ghz	$4\ n_f$	$15 + 4\ (n_f - 1)$	$6 + 3\ (n_f - 1)^{26}$

Tabla 3.3 Valores para el factor de penetración en edificios $L_f(n_f)$.

La Tabla 3.4 y la figura 3.11 muestra los valores obtenidos a partir de las formulas del modelo ITU, según nuestras condiciones.

d(m)	L_p(dBm)	P_{rx}(dBm)
0.1	11.7895493	0.21045067
0.2	19.6163292	-7.61632921
0.3	24.1947019	-12.1947019
0.4	27.4431091	-15.4431091
0.5	29.9627694	-17.9627694
0.6	32.0214818	-20.0214818
0.7	33.7620984	-21.7620984
0.8	35.269889	-23.269889
0.9	36.5998546	-24.5998546
1	37.7895493	-25.7895493
2	45.6163292	-33.6163292
3	50.1947019	-38.1947019
4	53.4431091	-41.4431091
5	55.9627694	-43.9627694
6	58.0214818	-46.0214818
7	59.7620984	-47.7620984
8	61.269889	-49.269889
9	62.5998546	-50.5998546
10	63.7895493	-51.7895493

Tabla 3.4 Modelo ITU para interiores

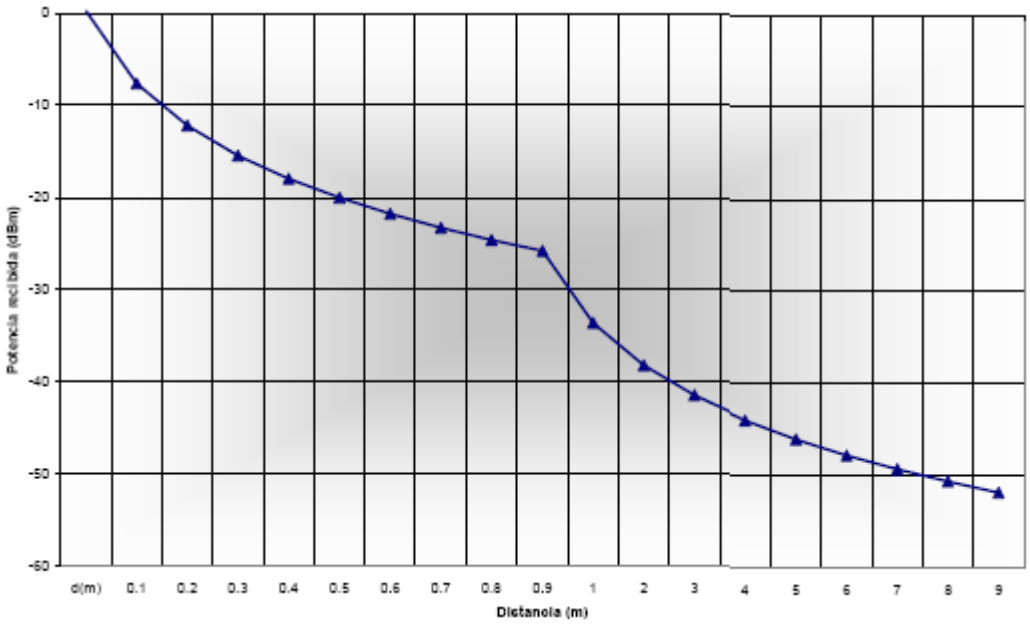

Figura 3.11 Gráfica del modelo ITU para interiores

La comparación entre estas predicciones es importante porque determinan, en teoría, hasta donde puede operar el jammer.

Se puede ver que en el caso extremo donde la radio base esté a 30m el jammer podrá operar a 4 metros a la redonda (-41.44>-43.77). Es necesario mencionar que este valor depende también de la sensibilidad y ganancia de cada unidad móvil.

3.6 Análisis de resultados

3.6.1 Oscilador y generador

Los valores de la onda triangular van a depender directamente del VCO que se utilice, para nuestro caso el voltaje mínimo que debe tener la onda triangular es de 0.5V para obtener una frecuencia de 800 Mhz y un voltaje máximo de 20V para una frecuencia de 2050 Mhz.

Según la simulación que se realizó para la onda triangular, esta oscila entre –224.050 mV y 20.351V, con estos valores se lograra un barrido de frecuencias desde 660Mhz a 2050Mhz aproximadamente, con lo que se consigue bloquear las frecuencias deseadas. Como se explicó en el capitulo II, el que se ataque también a las frecuencias que se encuentran fuera del rango no presentan ningún tipo de problema. Un factor importante es la velocidad de barrido de frecuencia, esto solo se logra en la práctica, debido a que no existe un algoritmo matemático que pueda ayudar al calculo del mismo, es por este motivo que se monto un potenciómetro en el generador de onda triangular para varia la frecuencia y de esta forma conseguir la velocidad apropiada.

3.6.2 Amplificador RF de potencia y Antena

El amplificador RF de potencia y la antena juegan un rol importante para determinar el área de cobertura del jammer, sin dejar a un lado la distancia que exista entre el jammer y la radio base mas cercada. El cálculo de este se lo puede realizar a partir de la predicción de potencia.

Para lograr una área de cobertura propuesta, se debe conocer algunos factores externos, como son: la distancia que existe desde la radio base al jammer, la altura a la que se encuentra la antena de transmisión y su ganancia. Con dichos parámetros y utilizando los modelos de propagación adecuados, se puede calcular la potencia necesaria que debe entregar el jammer, y de esta forma se conoce el valor del amplificador RF de potencia .

CAPÍTULO IV

MARCO REGULATORIO RESPECTO A LA RESTRICCIÓN DEL SERVICIO CELULAR EN SITIOS DE SEGURIDAD

4.1 Organismos de regulación y control en el Ecuador

En el mes de octubre de 1972 el Gobierno Nacional de ese entonces, impulsó el marco regulatorio de las telecomunicaciones, creando así el Instituto Ecuatoriano de Telecomunicaciones (IETEL) como resultado de la necesidad de desconcentrar las funciones del Estado, teniendo como objetivos principales la regulación, planificación y operación de las mismas.

Debido a los cambios vertiginosos que sufría las telecomunicaciones en el mundo, el sistema estatal del Ecuador requirió de un giro hacia un nuevo esquema acorde a los cambios que en ese entonces se daban. Es así que a partir del 10 de agosto de 1992, se reestructuró el sector de telecomunicaciones ecuatoriano con la aprobación de la Ley Especial de Telecomunicaciones, en la que se mantuvieron los servicios básicos de telecomunicaciones a cargo del Estado, mediante la transformación del IETEL en Empresa Estatal de Telecomunicaciones (EMETEL).

Un aspecto importante de esta Ley radica en la creación de la Superintendencia de Telecomunicaciones (SUPTEL) como ente de regulación y control, sujeto a la vigilancia del Congreso Nacional.

Posteriormente, surge la necesidad de modificar la mencionada Ley, debido a que existía la concentración de funciones en un solo organismo público la Superintendencia de Telecomunicaciones, el mismo que ejercía simultáneamente atribuciones de regulación y de control en el sector de telecomunicaciones. Esta razón, sumada a la queja de los usuarios por la falta de apoyo e interés gubernamental para el crecimiento y desarrollo del sector, constituyeron el impulsó para reformar a la Ley Especial de Telecomunicaciones promulgada el 30 de agosto de 1995 (R.O. 770), así como la aprobación de la Ley de Radiodifusión y Televisión.

Lo mas destacado de la reforma de esa ley fue la independencia de funciones otorgadas a los organismos creados, esto es: el Consejo Nacional de Telecomunicaciones (CONATEL), como ente de administración y regulación de las telecomunicaciones en el Ecuador, incluyendo el espectro radioeléctrico; como el Administrador de las Telecomunicaciones en el Ecuador ante la Unión Internacional de las Telecomunicaciones (UIT); y, con facultades para ejercer la representación a nombre del Estado; la Secretaría Nacional de Telecomunicaciones (SNT), como ente encargado de la ejecución e implementación de las políticas y regulación de telecomunicaciones emanadas del CONATEL, incluyendo el Plan Nacional de Frecuencias aprobado por el CONATEL (excepto las bandas de radio y televisión de competencia del CONARTEL y las de servicio móvil marítimo administrados por la Armada Nacional); y, la Superintendencia de Telecomunicaciones (SUPTEL) como el organismo de control y monitoreo del espectro radioeléctrico, así como de supervisión y control de operadores y concesionarios.

Con la Ley para la Transformación Económica promulgada en marzo del 2000, se reorganiza la política para el sector de telecomunicaciones, hacia un régimen de libre competencia, plasmada en la reforma del artículo 38 de la Ley Especial de Telecomunicaciones, delegando así al CONATEL la elaboración y promulgación de un apropiado marco regulatorio para propiciar el mercado en condiciones de libre competencia.

Para afrontar el nuevo reto, desde el año 2000 hasta la presente fecha, tanto el CONATEL como la SENATEL, vienen trabajado conjuntamente por el fortalecimiento del sector de las telecomunicaciones, dirigiendo sus esfuerzos hacia la consolidación de un mercado en apertura, con alto nivel competitivo, dentro de un marco regulatorio con garantías y seguridad jurídica [27].

4.1.1 CONATEL

El CONATEL (Consejo Nacional de Telecomunicaciones) es el organismo que se encarga de la regulación, administración y creación de políticas, que promuevan el acceso de por lo menos un servicio de telecomunicaciones a todos los ciudadanos en el Ecuador. Además el de establecer un escenario de leal competencia entre los actores del sector de las telecomunicaciones, para que desarrollen sus actividades y servicios en condiciones óptimas.

Los principales objetivos que se ha trazado el CONATEL son:

- Administrar de manera técnica el espectro radioeléctrico que es un recurso natural, para que todos los operadores del sector de las telecomunicaciones operen en condiciones de máxima eficiencia.
- Dictar las normas que corresponden para impedir las prácticas que impidan la leal competencia, y determinar las obligaciones que los operadores deban cumplir en el marco que determinan la Ley y reglamentos respectivos.
- Defender los derechos de los ciudadanos en todo momento para que satisfagan su necesidad de comunicarse.

El CONATEL tiene como políticas:

1. Velar por el estricto cumplimiento y respeto a los derechos de los usuarios en materia de servicios de telecomunicaciones.

2. Consolidar la apertura del mercado de las telecomunicaciones en el país que elimine las distorsiones existentes y que atraiga la inversión.
3. Incentivar la participación del sector privado en el desarrollo de infraestructura y prestación de servicios de telecomunicaciones en un marco de seguridad jurídica y de libre y leal competencia.
4. Incentivar la participación del sector privado en el desarrollo de infraestructura y prestación de servicios de telecomunicaciones en un marco de seguridad jurídica y de libre y leal competencia.
5. Fortalecer la presencia del Ecuador en la esfera subregional, regional y mundial en materia de telecomunicaciones.
6. Promover un cambio del marco legal acorde a los avances tecnológicos y libre mercado.
7. Propender a que la sociedad ecuatoriana obtenga el acceso y servicio universal de telecomunicaciones en forma ágil, oportuna, con calidad adecuada y a precios justos.
8. Promover el uso de las Tecnologías de Información y Comunicación (TICs) para garantizar el acceso de todos los ecuatorianos a la Sociedad de la Información.
9. Fomentar el acceso y uso de Internet, así como sus aplicaciones en el ámbito social como educación y salud.
10. Promover la generación de capital humano especializado para el sector de telecomunicaciones.

El directorio del Consejo Nacional de Telecomunicaciones (CONATEL), está integrado por:

- Un representante del Presidente de la República, quien lo presidirá.
- El representante de la Oficina de Planificación de la Presidencia de la República.
- El Jefe del Comando Conjunto de las Fuerzas Armadas.
- Un representante designado conjuntamente por las Cámaras de Producción.
- Un representante del Comité Central Único Nacional de los Trabajadores de Emetel (Conautel).
- El Secretario Nacional de Telecomunicaciones.
- El Superintendente de Telecomunicaciones [28].

4.1.2 SENATEL

La SENATEL (Secretaria Nacional de Telecomunicaciones) se encarga de administrar, regular y desarrollar los recursos asignados para el progreso y mejora de las tecnologías de información y comunicación en el Ecuador.

Su principal objetivo es el de ejecutar una política de telecomunicaciones con transparencia, efectividad y eficiencia en beneficio del desarrollo del sector y del país.

La SENATEL tiene como políticas:

1. El formular un marco regulatorio adecuado, para el desarrollo de las telecomunicaciones.
2. Brindar servicios eficientes y de calidad a los usuarios de la institución.
3. Coadyuvar al Desarrollo Nacional a través de proyectos de universalización de los servicios de Telecomunicaciones.
4. Administrar los recursos con eficacia, eficiencia y efectividad.
5. Fortalecer el Recurso Humano a base del desarrollo de sus competencias.
6. Mejorar los servicios en las Direcciones Regionales [29].

4.1.3 SUPTEL

Según la Constitución de la República del Ecuador establece que: “Las superintendencias serán organismos técnicos con autonomía administrativa, económica y financiera y personería jurídica de derecho público, encargados de controlar instituciones públicas y privadas, a fin de que las actividades económicas y los servicios que presten, se sujeten a la Ley y atiendan el interés general. La Ley determinará las áreas de actividad que requieran de control y vigilancia, y el ámbito de acción de cada Superintendencia”.

La Ley Especial de Telecomunicaciones publicada en el Registro Oficial del 10 de agosto de 1992 creó la SUPTEL (Superintendencia de Telecomunicaciones). Luego, en la Ley Reformatoria a la ley Especial de Telecomunicaciones publicada en el Registro Oficial N° 770 de 30 de agosto de 1995, establece que la Superintendencia es el único ente autónomo encargado del control de las telecomunicaciones del país, en defensa de los intereses del Estado y del pueblo, usuario de los servicios de telecomunicaciones.

Las principales obligaciones de la SUPETEL son:

- Proporcionar información técnica, contractual, administrativa y financiera que resultare del control y de la investigación a las operadoras y prestadoras del servicio de telecomunicaciones y de radio y televisión, a fin de que inicien los procesos investigativos a nivel preprocesal y procesal penal.
- Brindará capacitación y asesoría técnica al personal especializado en esta área.
- Ofrecer apoyo técnico y logístico, para el cumplimiento de diligencias que se evacuen dentro de los procesos investigativos y en las Audiencias de Juicio, y, dotará de espacios físicos en sus dependencias de las ciudades de Quito, Guayaquil y Cuenca, para que funcionen estas Unidades.

Las funciones de la Superintendencia son:

SEGÚN LA LEY REFORMATORIA A LA LEY ESPECIAL DE TELECOMUNICACIONES

1. Controlar y monitorear el uso del espectro radioeléctrico.
2. Controlar las actividades técnicas de los operadores de los servicios de telecomunicaciones.
3. Controlar la correcta aplicación de los pliegos tarifarios aprobados por el CONATEL.
4. Supervisar el cumplimiento de las concesiones y permisos otorgados para la explotación del servicio de telecomunicaciones.
5. Supervisar el cumplimiento de las normas de homologación y normalización aprobadas por el CONATEL.

6. Cumplir y hacer cumplir las resoluciones del CONATEL.
7. Aplicar las normas de protección del mercado y estimular la libre competencia; y,
8. Juzgar a las personas naturales y jurídicas que incurran en las infracciones señaladas en la Ley y aplicar las sanciones en los casos que corresponda.

SEGÚN LA LEY REFORMATORIA A LA LEY DE RADIODIFUSIÓN Y TELEVISIÓN

1. Administrar y controlar las bandas del espectro radioeléctrico destinadas por el Estado para radiodifusión y televisión.
2. Someter a consideración del CONARTEL los proyectos de reglamentos, del plan nacional de distribución de frecuencias para radiodifusión y televisión, del presupuesto del Consejo, de tarifas, de convenios o de resoluciones en general con sujeción a esta Ley.
3. Tramitar todos los asuntos relativos a las funciones del CONARTEL y someterlos a su consideración con el respectivo informe.
4. Realizar el control técnico y administrativo de las estaciones de radiodifusión y televisión.
5. Mantener con los organismos nacionales o internacionales de radiodifusión y televisión públicos o privados, las relaciones que corresponda al país como miembro de ellos, de acuerdo con las políticas que fije el CONARTEL.
6. Imponer las sanciones que le faculte esta ley y los reglamentos.
7. Ejecutar las resoluciones del CONARTEL.
8. Suscribir contratos de concesión de frecuencia para estación de radiodifusión o televisión o de transferencia de la concesión, previa aprobación del CONARTEL.

4.2 Marco Regulatorio para la telefonía móvil celular y avanzados en el Ecuador

En el Ecuador lamentablemente no existe una regulación que contemple el funcionamiento de un Sistema de Interferencia para teléfonos celulares con tecnología GSM, por lo que se analizará las regulaciones existentes en el ámbito de las telecomunicaciones y se

profundizará en el estudio de una figura creada para hacer legal el funcionamiento de la misma. Las telecomunicaciones en el Ecuador están normadas por:

- La Ley Especial de Telecomunicaciones Reformada
- Reglamento General a la Ley Especial de Telecomunicaciones Reformada

Y para el sector de la telefonía móvil se tienen los siguientes reglamentos afines:

- Reglamento para el Servicio de Telefonía Móvil Celular
- Reglamento para la Prestación del Servicio Móvil Avanzado

Observando cada una de estas leyes y reglamentos se trata de entender un poco el entorno regulatorio de las telecomunicaciones en el Ecuador, para luego buscar todo lo que pueda relacionarse con nuestro tema, es decir algo que pueda ayudar al uso de Sistemas de Interferencia para teléfonos celulares en determinados lugares, y de esta forma pueda entrar en funcionamiento en el Ecuador.

4.2.1 Ley Especial de Telecomunicaciones Reformada

Es un instrumento legal que compromete al Estado atribuciones privativas y de responsabilidad para:

- Dirigir, regular y controlar todas las actividades de telecomunicaciones, las cuales constituyen un servicio de necesidad, utilidad y seguridad pública, objetando en el Artículo 1:"...normar en el territorio nacional la instalación, operación, utilización y desarrollo de toda transmisión, emisión o recepción de signos, señales, imágenes, sonidos e información de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos".
- Brindar en régimen de libre competencia, evitando los monopolios, prácticas restrictivas o de abuso de posición dominante, y la competencia desleal, garantizando la seguridad nacional, y promoviendo la eficiencia, universalidad, accesibilidad, continuidad y la calidad del servicio.
- Establecer servicios abiertos a la correspondencia pública divididos en servicios finales y servicios portadores sin describir y/o regular los servicios específicos. Definidos en el Artículo 8 como:

"Servicios finales de telecomunicaciones, son aquellos servicios de telecomunicación que proporcionan la capacidad completa para la comunicación entre usuarios, incluidas las funciones del equipo terminal y que generalmente requieren elementos de conmutación. Forman parte de estos servicios: telefónico rural, urbano, interurbano e internacional; videotelefónico; telefax; burofax; datafax; videotex, telefónico móvil automático, telefónico móvil marítimo o aeronáutico de correspondencia pública; telegráfico; radiotelegráfico; de télex y de teletextos". Incluyendo los que sean definidos por los organismos internacionales competentes, para ser prestados con carácter universal.

"Servicios portadores son los servicios de telecomunicación que proporcionan la capacidad necesaria para la transmisión de señales entre puntos de terminación de red definidos".

Este tipo de servicio se sujeta a normas de servicios que utilizan redes de telecomunicaciones conmutadas para enlazar los puntos de terminación y servicios que utilizan redes de telecomunicación no conmutadas.

Para brindar este servicio se necesita contar con una capacidad de espectro radioeléctrico, y es el Estado, según los artículos 4 y 13 quien administra y se encarga de la regulación de este en el Ecuador. El espectro radioeléctrico es un recurso escaso por lo que al gobierno más que a nadie le conviene aprovecharlo de la mejor forma.

La normativa ecuatoriana regula la prohibición a la interferencia de señales mediante los siguientes artículos:

"Art. 10.- Intercomunicaciones internas.- No será necesaria autorización alguna para el establecimiento o utilización de instalaciones destinadas a intercomunicaciones dentro de residencias, edificaciones e inmuebles públicos o privados, siempre que para el efecto no se intercepten o interfieran los sistemas de telecomunicaciones públicos....."

"Art. 14.- Derecho al secreto de las telecomunicaciones.- El Estado garantiza el derecho al secreto y a la privacidad de las telecomunicaciones. Es prohibido a terceras personas interceptar, interferir, publicar o divulgar sin consentimiento de las partes la información cursada mediante los servicios de telecomunicaciones."

"Art. 17.- Protección contra interferencias.- INECEL, las Empresas Eléctricas y cualquier otra persona natural o jurídica que establezcan líneas de transmisión o de distribución de energía eléctrica o instalaciones radioeléctricas de cualquier tipo, están obligadas a evitar, a su costo, cualquier interferencia que pudiera producirse por efecto de dichas instalaciones sobre el sistema de telecomunicaciones, ya sea adoptando normas apropiadas para el trazado y construcción de las mismas o instalando los implementos o equipos necesarios para el efecto."

En el capítulo IV de la Ley Especial de Telecomunicaciones Reformada se encuentra un artículo que garantiza el derecho que todos los ecuatorianos tienen a comunicarse.

"Art.25.- Derecho al servicio.- Todas las personas naturales o jurídicas, ecuatorianas o extranjeras, tienen derecho a utilizar los servicios públicos de telecomunicaciones condicionado a las normas establecidas en los reglamentes y al pago de las tasas y tarifas respectivas.

Las empresas legalmente autorizadas establecerán los mecanismos necesarios para garantizar el ejercicio de los derechos de los usuarios"

En el capítulo V de las Sanciones se menciona artículos que penan a la interferencia de señales:

"Art. 28.- Infracciones.- Constituyen infracciones a la presente Ley, las siguientes:

a) *El ejercicio de actividades o la prestación de servicios sin la correspondiente concesión o autorización, así como la utilización de frecuencias radioeléctricas sin permiso o en forma distinta de la permitida;*
b) *El ejercicio de actividades o la prestación de servicios que no correspondan al objeto o al contenido de las concesiones o autorizaciones;*

c) La conexión de otras redes a la red de telecomunicaciones sin autorización o en forma distinta a la autorizada o a lo previsto en esta Ley y sus Reglamentos;

d) La instalación, la utilización o la conexión a la red de telecomunicaciones de equipos que no se ajusten a las normas correspondientes;

e) La producción de daños a la red de telecomunicaciones como consecuencia de conexiones o instalaciones no autorizadas;

f) La importación, fabricación, distribución, venta o exposición para la venta de equipos o aparatos que no dispongan de los certificados de homologación y de cumplimiento de las especificaciones técnicas que se establezcan en los Reglamentos;

Se consideran infracciones graves las siguientes:

1) La conducta culposa o negligente que ocasione daños, interferencias o perturbaciones en la red de telecomunicaciones en cualquiera de sus elementos o en su funcionamiento;

2) La alteración o manipulación de las características técnicas de los equipos, aparatos o de terminales homologados o la de sus marcas, etiquetas o signos de identificación;

3) La producción deliberada de interferencias definidas como perjudiciales en el Convenio Internacional de Telecomunicaciones; y, La violación a la prohibición constante en el artículo 14 de la presente Ley."

"Art. 29.- Sanciones.- La persona natural o jurídica que incurra en cualquiera de las infracciones señaladas en el artículo anterior sin perjuicio de la reparación de los daños ocasionados será sancionada por las autoridades indicadas en el artículo 30 con una de las siguientes sanciones según la gravedad de la falta, el daño producido y la reincidencia en su comisión:

a. Amonestación escrita;

b. Sanción pecuniaria de uno hasta cincuenta salarios mínimos vitales generales;

c. Suspensión temporal de los servicios;

d. Suspensión definitiva de los servicios; y,

e. Cancelación de la concesión o autorización y negativa al otorgamiento de nuevas."

"Art. 30.- Juzgamiento.- Corresponde al Superintendente de Telecomunicaciones juzgar al presunto infractor, graduando la aplicación de la sanción según las circunstancias, mediante resolución motivada y notificada al infractor."

"Art. 31.- Notificación.- La notificación de la presunta infracción se hará por una boleta, en el domicilio mercantil o civil del infractor o por correo certificado."

4.2.2 Reglamento General a la Ley Especial de Telecomunicaciones Reformada

Este reglamento tiene como finalidad establecer las normas y procedimientos generales aplicables a las funciones de planificación, regulación, gestión y control de la prestación de servicios de telecomunicaciones y la operación, instalación y explotación de toda transmisión, emisión o recepción de signos, señales, imágenes, datos y sonidos por cualquier medio; y el uso del espectro radioeléctrico.

Los artículos que tienen relación con la interferencia de señales y prestación de servicios de telecomunicaciones son:

"Art. 5.- Para la prestación de un servicio de telecomunicaciones, se requiere un título habilitante, que habilite específicamente la ejecución de la actividad que realice."

"Art. 22.- Denomínase Servicio Universal a la obligación de extender el acceso de un conjunto definido de servicios de telecomunicaciones aprobados por el CONATEL a todos los habitantes del territorio nacional, sin perjuicio de su condición económica, social o su localización geográfica, a precio asequible y con la calidad debida."

"Art. 37.- La interconexión y conexión se permitirán en condiciones de igualdad, no-discriminación, neutralidad, y libre y leal competencia, a cambio de la debida retribución.

Los concesionarios que tengan redes públicas de telecomunicaciones estarán obligados a prestar la conexión o interconexión siempre que se cumplan las siguientes condiciones:

a) Que exista compatibilidad técnica entre sus redes;

b) Que no ocasione daño ni ponga en peligro la vida de las personas o la salud pública; y,....."

"Art. 47.- El espectro radioeléctrico es un recurso natural limitado perteneciente al dominio público del Estado; en consecuencia es inalienable e imprescriptible. La planificación, administración y control de su uso corresponde al Estado a través del CONATEL, la Secretaría y la Superintendencia en los términos de la Ley Especial de Telecomunicaciones, sus reformas y este reglamento y observando las normas y recomendaciones de la Unión Internacional de Telecomunicaciones."

"Art. 51.- El uso del espectro radioeléctrico para telecomunicaciones podrá consistir en uso privativo, uso compartido, uso experimental, o uso reservado y su asignación, siempre requerirá de una concesión. Uso privativo es la utilización de una frecuencia o bandas de frecuencias del espectro, para un servicio de telecomunicaciones específico que, por razones técnicas, no puede ser utilizada sino por un solo concesionario. El Estado garantizará que su uso esté libre de interferencias perjudiciales. Uso compartido es la utilización de una frecuencia o bandas de frecuencias del espectro para un servicio de telecomunicaciones simultáneo por varios concesionarios. Uso experimental es la utilización de una frecuencia o bandas de frecuencias del espectro con propósitos académicos o de investigación y desarrollo. Uso reservado consiste en la utilización, por parte del Estado, de unas frecuencias o bandas de frecuencia del espectro radioeléctrico para fines de utilidad pública o por motivos de seguridad interna y externa."

"Art. 53.- Todas las solicitudes de títulos habilitantes de uso del espectro radioeléctrico que presenten los interesados a la Secretaría para obtener su concesión contendrán como mínimo, la siguiente información:

a) Identificación del solicitante;

b) Estudio de ingeniería correspondiente;

c) Servicios que se ofrecerán; y,

d) En casos especiales que involucren la seguridad nacional, el CONATEL podrá pedir la información adicional que considere necesario."

"Art. 57.- El uso de frecuencias del espectro radioeléctrico requiere de un título habilitante, aprobada por el CONATEL y otorgada por la Secretaría, para lo cual se pagarán los valores que corresponda. El pago por el otorgamiento de frecuencias cuando no haya procesos públicos competitivos, será fijado por el CONATEL sobre la base de un estudio técnico y económico que contemple entre otros aspectos: el ancho de banda solicitado y el área de cobertura prevista en el título habilitante, todo bajo el principio de tratamiento igualitario. La ampliación, extensión, renovación, o modificación de las condiciones fijadas en el título habilitante requerirá de una nueva."

"Art. 78.- El permiso es un título habilitante mediante el cual la Secretaría, previa decisión del CONATEL, autoriza a una persona natural o jurídica para operar una red privada o prestar servicios de valor agregado."

4.2.3 Reglamento para el Servicio de Telefonía Móvil Celular

El presente Reglamento tiene por *"...objeto regular, normar, supervisar y permitir la explotación de los Servicios de Telefonía Móvil Celular (STMC) a través de Redes Públicas de Telefonía Móvil (RPTM)".*

Según lo definido en el Artículo 12, contempla que el área geográfica de cobertura del servicio será todo el territorio nacional; la Operadora debe presentar a la Secretaria Nacional de Telecomunicaciones un plan de expansión para lograr dicha cobertura.

Las empresas OTECEL S.A. (Movistar) y CONECEL S.A. (Porta) fueron quienes brindaron el Servicio de Telefonía Móvil Celular hasta fines del año 2008.

El título habilitante para este servicio es una Concesión que se la obtiene en un proceso de subastas públicas de frecuencias, pero en el caso de OTECEL S.A. y CONECEL S.A. se

firmó este nuevo contrato como si se tratara de una renovación del anterior que era completamente diferente al actual, esta concesión tiene una duración de 15 años, pagando un derecho de concesión de acuerdo con la propuesta de los participantes en la subasta. Otros títulos necesarios para la prestación de este servicio dependen del medio de transmisión del sistema utilizado, esto es:

1. Medio de transmisión alámbrico: registro de redes físicas
2. Medio de transmisión inalámbrico: título habilitante para el uso del espectro radioeléctrico además de una concesión para el uso de frecuencias no esenciales.

Este servicio tenía dos reglamentos expedidos en los años de 1996 y 1998 respectivamente, con el segundo de ellos se tuvo inconvenientes con las operadoras por su negativa para acogerse totalmente a este nuevo reglamento, creando un vacío legal al tener dos reglamentos, es decir que las operadoras se amparaban a cualquiera de los dos según su conveniencia, al respecto se recurrió al Procurador General de la Nación, el mismo que se pronunció en dos ocasiones, estableciendo el acogimiento de las empresas OTECEL S.A. o Movistar (antes Bellsouth) y CONECEL S.A. o Porta al reglamento de 1996.

Las frecuencias otorgadas inicialmente a estos dos prestadores de Servicio de Telefonía Móvil se encuentran en la banda de los 850 MHz, son las bandas nombradas A y B, la banda A se la otorgó a CONECEL S.A. (Porta) y la banda B a OTECEL (Movistar, en ese entonces Bellsouth) el espectro asignado fue de 25 MHz para cada operador.

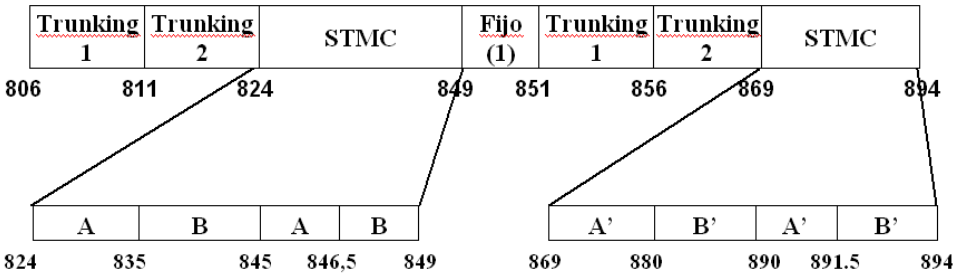

Figura 4.1 Frecuencias otorgadas inicialmente a CONACEL S.A. y OTECEL

Luego las empresas OTECEL y CONECEL pidieron se les conceda un sección de espectro en la banda de 1900 MHz, y se les dio 10 MHz a cada una.

Operador	Bandas de frecuencias en MHz		Denominación
CONECEL	1885-1890	1965-1970	Banda E-E'
OTECEL	1865-1870	1945-1950	Banda D-D'

Tabla 4.1 Asignación de Frecuencias para STMC en banda PCS (Tabla realizada en base a información proporcionada por la SENATEL)

Los servicios que se brindaban en STMC eran los siguientes:

Servicio de Telefonía Móvil

- Servicio orientado a la transmisión de voz.

- **Servicio Suplementario:**
  - Servicios de Mensajes Cortos SMS

- **Servicios Especiales**
  -Transferencia de llamada
  - Llamada en espera
  - Conferencia
  - Llamadas salientes
  - Llamadas entrantes
  - Facturación detallada
  - Roamers básico diario
  - Roamers minuto al aire
  - Marcación abreviada.

Los servicios adicionales que se podían prestar en STMC tienen que ver con un permiso de Valor Agregado que tenían los concesionarios para prestar servicios de Internet sobre la red celular y son:

- Puntos de venta móviles y remotos.
- Acceso móvil a redes corporativas.
- Acceso móvil a Internet.

- Correo electrónico inalámbrico.
- Localización vehicular.
- Telemetría (La telemetría está definida como un servicio de valor agregado que permite transmitir información de sensores o transductores desde sitios remotos a una estación central a través de servicios portadores o finales).
- Servicio de Internet
- Servicio a clientes corporativos y propietarios de redes LAN

4.2.4 Reglamento para la Prestación del Servicio Móvil Avanzado

El presente reglamento tiene por objeto *"...regular la prestación del Servicio Móvil Avanzado (SMA)*."

Definiendo al Servicio Móvil Avanzado como *"...un servicio final de telecomunicaciones del servicio móvil terrestre, que permite toda transmisión, emisión y recepción de signos, señales, escritos, imágenes, sonidos, voz, datos o información de cualquier naturaleza."*

El SMA se prestará en régimen de libre competencia, con cobertura nacional y la prestación del SMA en áreas rurales y urbano marginales se efectuará atendiendo al régimen de servicio universal. Al igual que la telefonía móvil, la prestación y explotación del SMA es una concesión otorgada por la Secretaría Nacional de Telecomunicaciones, previa autorización del CONATEL.

El 03 de Noviembre de 1993 se celebra entre la Secretaría nacional de Telecomunicaciones y TELECSA S.A. el contrato de concesión del Servicio Móvil Avanzado, telefonía de larga distancia internacional a sus propios abonados y la concesión para el uso frecuencias esenciales en la Banda C-C' (1895 – 1910 MHz y 1975 – 1990 MHz), también se le otorgó 10 MHz en la Banda F-F'. Su concesión fue para un tiempo de 15 años con cobertura a nivel nacional, además que se le dio una exclusividad que consistía en que durante 3 años el Consejo Nacional de Telecomunicaciones debía abstenerse de autorizar a otro operador una solicitud para brindar servicios de telecomunicaciones móviles.

A finales del año 2008 las empresas OTECEL S.A. (Movistar) y CONECEL S.A. (Porta) pasan a brindar el servio de telefonía móvil avanzada.

Además a partir del 26 de agosto del 2008 CONECEL S.A. empezó a prestar el servicio de Servicio Móvil Avanzado, terminándose controversialmente su concesión para la prestación del Servicio de Telefonía Móvil Celular al encontrarse incongruencias en la declaración de ingresos de esta empresa, ya que siendo la clara dominante en el mercado reportó más de un año pérdida, esto unido a una serie de negligencias con el mantenimiento de su red, lo que provocó que el Presidente negocie un millonario contrato con CONECEL, pagando muchísimo más de lo que pagaría OTECEL por motivo de la misma concesión.

OTECEL S.A. también firmó su contrato para prestar un Servicio Móvil Avanzado el 30 de noviembre del 2008, en el caso de esta operadora se presentaron más facilidades en el acuerdo de las negociaciones con el CONATEL, además por su concesión, como ya se dijo, pagaron mucho menos de lo que pagó CONECEL S.A., tal vez debido a la sociedad que existió con TELECSA S.A. para que esta prestara el servicio de telefonía celular a través de la red del sistema GSM de OTECEL S.A.

Los servicios que se brindan en SMA son:

- **Servicio Móvil Avanzado -**
  Servicio orientado a la transmisión de datos (voz, imagen, video, etc.)
- **Servicios Adicionales.-**
  - Marcación Abreviada
  - Transferencia de llamadas
  - Casillero de Voz
  - Llamada en espera
  - Conferencia
  - Facturación detallada
  - Cambio de Número
  - Activación Roaming Internacional

4.3 Legalidad de interferencias de señales

En el Ecuador, al momento la Ley Especial de Telecomunicaciones Reformada, y la mayoría de Reglamentos Generales existentes, fueron creados con objetivos muy diferentes en cuanto al servicio de las telecomunicaciones, existiendo reglamentos específicos de la telefonía móvil y la telefonía móvil avanzada.

Tal es así que en la actualidad, el Ecuador cuenta con un conjunto de leyes y reglamentos que impiden la interferencia de servicios de telecomunicaciones. A continuación se señala los leyes y reglamentos que sustentan lo indicado anteriormente, y que servirá de análisis para lo posterior.

En la Ley de Especial de Telecomunicaciones Reformada los artículos 14, 17 , 18 y 28 literal 3 señalan:

"Art. 14.- Derecho al secreto de las telecomunicaciones.- El Estado garantiza el derecho al secreto y a la privacidad de las telecomunicaciones. Es prohibido a terceras personas interceptar, interferir, publicar o divulgar sin consentimiento de las partes la información cursada mediante los servicios de telecomunicaciones."

"Art. 17.- Protección contra interferencias.- INECEL, las Empresas Eléctricas y cualquier otra persona natural o jurídica que establezcan líneas de transmisión o de distribución de energía eléctrica o instalaciones radioeléctricas de cualquier tipo, están obligadas a evitar, a su costo, cualquier interferencia que pudiera producirse por efecto de dichas instalaciones sobre el sistema de telecomunicaciones, ya sea adoptando normas apropiadas para el trazado y construcción de las mismas o instalando los implementos o equipos necesarios para el efecto."

"Art. 18.- Daños a instalaciones.- Cuando las instalaciones de telecomunicaciones pertenecientes a la red pública o las instalaciones de radio comunicaciones que forman parte del servicio público, sufran interferencias, daños o deterioros causados por el uso de

equipos eléctricos, vehículos, construcciones o cualquier otra causa, corresponderá al causante del daño pagar los costos de las modificaciones o reparaciones necesarias, inclusive por la vía coactiva."

"Art. 28.- Infracciones.- Constituyen infracciones a la presente Ley.....

1. *La producción deliberada de interferencias definidas como perjudiciales en el Convenio Internacional de Telecomunicaciones....."*

En el Reglamento General a la Ley Especial de Telecomunicaciones Reformada se encuentra los artículos: 49, 127 y 147, que mencionan:

"Art. 49.- El CONATEL establecerá el Plan Nacional de Frecuencias, incluyendo la atribución de bandas a los distintos servicios y su forma de uso, la asignación de frecuencias y el control de su uso. Todos los usuarios del espectro radioeléctrico deberán cooperar para eliminar cualquier interferencia perjudicial."

"Art. 127.- Se prohíbe cualquier interferencia o intercepción no justificadas a la integridad de los servicios de telecomunicaciones. Se entiende como atentado a la integridad de las telecomunicaciones cualquier interferencia, obstrucción, o alteración a las mismas, así como la interrupción de cualquier servicio de telecomunicaciones, tales como el corte de líneas o cables, o la interrupción de las transmisiones mediante cualquier medio, salvo las excepciones que establezcan las leyes, los reglamentos y los títulos habilitantes."

"Art. 147.- Los usuarios de servicios de telecomunicaciones no podrán usar ningún tipo de equipo terminal que pueda impedir o interrumpir el servicio, degradar su calidad, causar daño a otros usuarios o a otras redes públicas o privadas, ni a empleados de las operadoras de dichas redes. El suministro, instalación, mantenimiento y reparación de los equipos terminales serán responsabilidad del propietario del equipo."

En el Reglamento para telefonía móvil el articulo 37 indica:

"*Art. 37.- Interferencias.- La Operadora será la única responsable por las interferencias radioeléctricas que las estaciones de su sistema puedan causar a otros sistemas de radiocomunicaciones, previamente autorizados, o por daños que puedan causar sus instalaciones a terceros, y estará obligada a solucionar a su costo y a reconocer daños y perjuicios.*

En caso de que las frecuencias asignadas a la Operadora de STMC sufrieren interferencias por terceros, la Superintendencia de Telecomunicaciones procederá, en el término de diez (10) días a determinar la interferencia. El causante de la interferencia se someterá a lo establecido en el Reglamento de Radiocomunicaciones."

En el Reglamento para la Prestación del Servicio Móvil Avanzado el artículo 22 literal 1, mencionan:

"Art. 22.- Son derechos de los prestadores del SMA, los siguientes:

1. *Denunciar ante la Superintendencia de Telecomunicaciones las prácticas de competencia desleal, interferencias y demás infracciones establecidas en la Ley Especial de Telecomunicaciones Reformada....."*

Por todos los artículos expuestos anteriormente, se puede concluir que es ilegal el interferir o bloquear un servicio de telecomunicaciones por cualquier forma que se lo haga, ya que incluso se encuentra penado por la ley ecuatoriana actual.

Existe un único antecedente en el que se procede a suspender el servicio celular en el Centro de Rehabilitación Social de Pascuales, por pedido del Juez Sexto de lo Penal del Guayas el día 30 de octubre de 2002, mediante oficio GJYR-1476-2002 y por la Ingeniera Verónica Yerovi Directora General de servicios de Telecomunicaciones el 8 de julio de 2004 con memorando No. DJR-2004-1111. Tal petición fue acogida por las operadoras PORTA y BELLSOUTH.

4.4 Propuesta para uso de *jammers* en determinados lugares

La comunicación celular ha ampliado considerablemente el campo de los negocios pero también permite a la delincuencia estar en contacto permanente muy fácilmente, por este y otros motivos, se propondrá anular la señal celular en entidades financieras, centros de rehabilitación social y destacamentos militares y policiales, por medio de bloqueadores de señal que eviten o impidan de forma automática en rangos controlables de espacio el uso del celular.

4.4.1 Problema

En los últimos años la telefonía móvil se a convertido en una de las herramientas más importantes para la comunicación del hombre, si bien el uso, la utilidad y el manejo que se le de al teléfono celular depende directamente del cliente, se debe controlar el uso indebido que se le de a este, por los motivos que se mencionan a continuación:

- La planeación y realización de actos delictivos en bancos, cajeros automáticos, lugares de pago y manejo de valores.
- La fácil comunicación que puede tener la población carcelaria desde el interior de los centros de reclusión con amigos, para cometer extorsiones, planear posibles fugas y amotinamientos dentro de las prisiones.
- Al infiltrarse personal no autorizado a dependencias militares y policiales, estos pueden informar datos confidenciales desde el interior, por medio de llamadas o mensaje, poniendo así en riesgo al estado y a la ciudadanía.

4.4.2 Justificación

Con la finalidad de evitar y restringir el uso de teléfonos móviles por motivos de seguridad, es necesario crear una ley que contemple el uso legal de bloqueadores de señales celulares en determinados lugares, considerando de que antes de instalarse en cualquier zona este dispositivo, se tiene que realizar un análisis de campo, para evaluar el funcionamiento adecuado del mismo, evitando así la anulación de la señal fuera de los limites del área que se desea restringir.

Los lugares en los que se pretende anular la señal celular son: Entidades financieras, Centros de rehabilitación social y Destacamentos militares y policiales.

Se debe restringir la señal celular en entidades financieras para evitar el posible contacto que pueden tener los cómplices desde el interior de estas sedes con la delincuencia, ya que pueden proporcionar información fundamental para realizar actos delictivos con mayor facilidad; debido a que los letreros y advertencias colocados en estos sitios no aseguran que los clientes no hagan uso de sus teléfonos celulares.

Al existir la posible infiltración de personas no autorizadas o mal intencionadas a destacamentos militares y policiales, se corre el riesgo de difundir información confidencial. Una de las formas para evitar esta transmisión de información, es limitando la señal celular, para impedir el contacto que pueden tener estas personas por medio de teléfonos celulares con individuos que deseen tener esta información, para causar daño a la sociedad.

Hay que tomar en cuenta que el estado ecuatoriano, mediante la Constitución de la Republica del Ecuador del 2008 menciona que :

"*Art. 3.- son deberes primordiales del Estado:*

1.- Garantizar sin discriminación alguna el efectivo goce de los derechos establecidos en la Constitución y en los instrumentos internacionales, en particular la educación, la salud, la alimentación, la seguridad social y el agua para sus habitantes."

Analizando lo anteriormente citado se podría justificar el uso de bloqueador de señales celulares en entidades financieras y dependencias militares y policiales, por motivos de seguridad social.

Desde el interior de los centros de reclusión social (se denominan centros de reclusión social a las penitenciarias y cárceles existentes, y las que se crearen para el cumplimiento

del régimen penitenciario que establece esta ley. Según el artículo 19 del Código de Ejecución de Penas y de Rehabilitación Social del Ecuador) la población carcelaria hace uso de teléfonos celulares, a pesar de que el uso de estos aparatos se encuentran prohibidos como se señala en el artículo 17 del Reglamento de Evaluación de la Conducta y Disciplina de los internos imputados, acusados y sentenciados en los centros de rehabilitación social del país del 19 de julio del 2007, en el que expone *"Son faltas graves, literal 9.- ingresar artefactos de comunicación o eléctricos no permitidos"*. Los teléfonos celulares son utilizados para realizar extorsiones a las personas que los delataron o acusaron en algún crimen que cometieron, dirigir y organizando a cómplices y amigos para que sigan delinquiendo y fortalecientes sus grupos delictivos. Los teléfonos son proporcionados por familiares, amigos e inclusive por trabajadores de los centros de rehabilitación. Es difícil mantener un control en el uso de teléfonos celulares dentro de las cárceles, por tal razón es necesario implementar sistemas de interferencias para estos aparatos.

Por todo lo expuesto anteriormente y lo que sostienen los artículos 393 de la Constitución de la Republica del Ecuador del 2008 y el artículo 11 de la Ley Especial de Telecomunicaciones Reformada en los que se mencionan:

"Art. 393.- El estado garantizará la seguridad humana a través de políticas y acciones integradas, para asegurar la convivencia pacífica de las personas, promover una cultura de paz y prevenir las formas de violencia y discriminación y la comisión de infracciones y delitos. La planificación y aplicación de estas políticas se encargaran a órganos especializados en los diferentes niveles de gobierno."

"Art. 11.- Uso prohibido.- Es prohibido usar los medios de telecomunicación contra la seguridad del Estado, el orden público, la moral y las buenas costumbres. La contravención a esta disposición será sancionada de conformidad con el Código Penal y más leyes pertinentes."

El Consejo Nacional de Telecomunicaciones CONATEL, puede regular el uso de bloqueadores o sistemas de interferencia para teléfonos celulares en determinados lugares.

4.4.3 Propuesta de reforma

CONSEJO NACIONAL DE TELECOMUNICACIONES
CONATEL

CONSIDERANDO:

Que el CONATEL es el ente de administración y regulación de las telecomunicaciones de la República del Ecuador, y tiene la representación del Estado para ejercer, a su nombre, las funciones de administración y regulación de los servicios de telecomunicaciones y es el Administrador de Telecomunicaciones del Ecuador ante la Unión Internacional de Telecomunicaciones.

Que es de suma importancia para los intereses de la sociedad ecuatoriana crear políticas de seguridad para contribuir con el cumplimiento, con lo dispuesto en los Art. 393 de la Constitución de la República del Ecuador y el Art. 11 de la Ley Especial de Telecomunicaciones Reformada.

Que se debe considerar el uso de bloqueadores o sistemas de interferencia para teléfonos celulares bajo cierto criterios sociales y técnicos.

Resuelve:

EXPEDIR LA SIGUIENTE REFORMA AL REGLAMENTO GENERAL A LA LEY ESPECIAL DE TELECOMUNICACIONES REFORMADA

Art. 1 Agregase luego del Art. 127 el siguiente contenido: Únicamente podrán usarse bloqueadores o sistemas de interferencia para teléfonos móviles sin autorización previa por parte de las operadoras en: entidades financiera, centros de rehabilitación social y destacamentos militares y policiales en rangos controlables de espacio, para lo cual se deberá realizar el correspondiente análisis de campo, para evaluar el funcionamiento adecuado del mismo, evitando así anular la señal fuera de las áreas permitidas.

Art. 2 Sustitúyase el contenido del artículo 147 por lo siguiente: Los usuarios de servicios de telecomunicaciones no podrán usar ningún tipo de equipo terminal que pueda impedir o interrumpir el servicio, excepto bloqueadores o sistemas de interferencia de señal celular bajo las circunstancias que se indica en el Art. 127 de este reglamente, degradar su calidad, causar daño a otros usuarios o a otras redes públicas o privadas, ni a empleados de las operadoras de dichas redes. El suministro, instalación, mantenimiento y reparación de los equipos terminales serán responsabilidad del propietario del equipo.

La presente resolución entrara en vigencia a partir de su publicación en el Registro Oficial.

Dado en Quito, ...

PRESIDENTE DEL CONATEL

SECRETARIO DEL CONATEL

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Después de haber analizados los distintos tipos de jamming, se llegó a la conclusión que la estrategia de barrido es la ideal para un sistema de telefonía móvil con tecnología GSM puesto que es apropiado para sistemas FHSS, y además se pretende utilizar toda la potencia disponible en cada parte del espectro.

- El jamming por barrido se compone de seis etapas: el sintonizador, generador de ruido, mezclador de dos canales, VCO, amplificación RF de potencia y la antena.

- El centro medular del jammer es el VCO ya que este se encarga de proporcionar las frecuencias que van a ser bloqueadas, dependiendo de la tensión de entrada que se le suministre.

- Un aspecto importante a tomar en cuenta en el diseño del jammer, es la etapa de amplificación de potencia y la ganancia de la antena, ya que estos ayudarán a cubrir el área que se desea bloquear la señal celular; para la etapa de amplificación se puede utilizar circuitos integrados que con solo modificar los valores de los componentes pasivos de entrada al mismo, se puede variar la ganancia y por ende el área de cobertura.

- El tipo de *jammer* adecuado para este sistema es de tipo constante, debido a que el ahorro de potencia no es importante, puesto que el *jammer* no es portátil y además se desea que la interferencia de la señal se efectué en todo instante de tiempo.

- Técnicamente lo que realizar el bloqueador de señal celular, es generar una señal que realiza un barrido en toda la banda, esta señal es capaz de posesionarse momentáneamente en cada uno de los canales sean de control o de voz, confundiendo de esta manera la información que llega a los celulares, evitando así se proceda una llamada. El efectuar de esta manera el bloqueo hace que el sistema sea independiente de la tecnología a la que pretenda bloquear.

- Los modelos de propagación con el que se calcularon las pérdidas no son exactos y simplemente hacen el mejor esfuerzo para aproximarse a situaciones reales, ya que no se puede modelar el ambiente y el lugar donde se va a instalar el jammer, lo que podría presentar variaciones en la cobertura, al momento de implementar el mismo.

- Los acondicionamientos de las señales que se dé a cada etapa son importantes, puesto que estos servirán para afinar la señal transmitida, ya que el circuito receptor de la unidad móvil no ha sido considerado al momento de los cálculos, y por tal motivo se deba realizar ajustes a dicha señal.

- En radio frecuencias un parámetro muy importante a considerar es el acoplamiento de impedancias entre cada una de las etapas, este hecho hace necesario que se garantice impedancias características de 50 ohmios en cada uno de los componentes de la etapa de radiofrecuencia.

- Cabe mencionar que mientras más cerca esté el equipo bloquear de una radio base, el nivel de señal que emita la antena de esta radio base será mucho mayor que

cuando esté mas lejos; dando como consecuencias que en cercanías a estas radio bases el equipo de bloqueo alcance coberturas muy reducidas.

- La actual ley de telecomunicaciones y los reglamentos de telefonía móvil no contemplan el uso de bloqueadores de señal celular, por tal motivo, desde el punto de vista de seguridad, es necesario legalizar el uso de estos dispositivos en determinados lugares, con lo cual se contribuye con la seguridad ciudadana.

5.2 Recomendaciones para trabajos Futuros

- El dispositivo podría modificarse agregándole un selector para poder bloquear solamente la red celular deseada (Movistar, Porta o Alegro). Una opción sería implementarlo en el generador de funciones y por medio de resistencias de distintos valores variar la amplitud de la onda triangular generada. Al poder elegir con cual resistencia operar, se variaría la entrada al VCO y por consecuencia la salida de este. Otra opción sería utilizar más de un VCO; ya sea por hardware o por programación en un dispositivo FPGA (*Field Programmable Gate Array*).

- Es recomendable tener en cuenta la línea de transmisión que se elija, puesto que no debe presentar perdidas de transmisión considerables para tener una mayor eficiencia del bloqueador de señal celular, a su vez hay que tomar en cuenta las impedancia de salía, para poder adaptar a la antena que se elija.

- Se recomienda que al diseñar este dispositivo, primero se consulte si los componentes que se van a utilizar existen en el mercado, puesto que si a último momento se cambia de componente por no existir este en el mercado, podría variar los resultados y esto llevaría a modificar las demás etapas del circuito.

- Es recomendable que para diseñar equipos electrónicos se considere siempre el peor de los casos, de tal forma que la operatividad del equipo sea óptimo.

- Un punto importante sobre el tema es lo relacionado al marco legal, puesto que la ley prohíbe la interferencia de señales. Es por eso que se debe mencionar que cualquier persona que emplee este trabajo con el fin de evitar la comunicación en una red de telefonía celular estará incurriendo en una actividad severamente penada por la ley ecuatoriana.

BIBLIOGRAFÍA

[1] Blaunstein, Nathan. Radio Propagation in Cellular Networks. Norwood: Artech House, 1999

[2] Tomasi, Wayne. Electronic Communications Systems. New Jersey: Prentice Hall, 2001

[3] www.eveliux.com/.../la-evolucion-de-la-telefonia-movil.php

[4] http://www.cibertele.com/publicaciones/UMTS.pdf

[5] GARCIA, Santiago, "Técnico en Telecomunicaciones", tomo 3, Editorial Cultural S. A.

[6] http://www.expansiondirecto.com/tecnologia/informes/telefonia/4g.html

[7] http://www.aircom.com.uk

[8] Poisel, Richard. Modern Communication *Jamming* Principles and Techniques Norwood: Artech House, 2004

[9] http://www.rcp.net.pe/rcp/_soporte/rrisco/gsm

[10] Lemelson-MIT Program. Lemelson-MIT Invention Index. Massachussets Lemelson-MIT Program, 2004

[11] www.milspec.ca/jammers/jammers.html

[12] Poisel, Richard. Introduction to Communication Electronic Warfare Systems Norwood: Artech House, 2004

[13] Xu, Wenyuan, Wade Trappe, Yanyong Zhang, and Timothy Word. The Feasibility of Launching and Detecting *Jamming* Attacks in Wireless Networks 25 mayo 2005. 28 enero 2006

[14] Schleher, Curtis. Electronic Warfare in the Information Age. Norwood: Artech House, 1999

[15] Fried, Limor. Social Defense Mechanisms: Tools for Reclaiming Our Personal Space. 28 enero 2005. 28 enero 2006.

[16] Información proporcionada por la SENATEL

[17]http://books.google.com.ec/books?id=vGqE52oO2BQC&pg=PA52&lpg=PA53&ots=117KpU9RNv&dq=circuito+mezclador+de+audio+de+dos+canales#v=onepage&q=circuito%20mezclador%20de%20audio%20de%20dos%20canales&f=false
[18] Datasheet DCMO80210-10

[19] Apuntes Sek

[20] http://oa.upm.es/263/1/09200439.pdf pagina del mmic

[21]http://www.elprisma.com/apuntes/ingenieria_electrica_y_electronica/lineasdetransmision/default2.asp

[22] http://proton.ucting.udg.mx/temas/comunicaciones/lineas/anel.htm

[23] http://www.foentel.com/productos.php?cat=195

[24] http://www.demon-multimedia.com/productos/productos.asp?id=976&ampliada=Si

[25] http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/soriano_m_jc/capitulo2.pdf

[26] http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/campos_v_da/capitulo4.pdf

[27]http://www.conatel.gov.ec/site_conatel/index.php?option=com_content&view=article&catid=25%3Ainformacion-corporativa&id=20%3Ahistoria-de-las-telecomunicaciones-en-el-ecuador&Itemid=78

[28]http://www.conatel.gov.ec/site_conatel/index.php?option=com_content&view=article&id=51&Itemid=28

[29]http://www.conatel.gov.ec/site_conatel/index.php?option=com_content&view=article&id=51&Itemid=28

[30] Hora GMT: 30/Mayo/2006 - 05:00 Fuente**:** Diario HOY Ciudad Quito Autor: Por Bernardo Acosta .

[31] www.actapress.com/Abstract.aspx?paperId=23682

Fecha de entrega de la Tesis: 11 de Diciembre del 2009

Diego Hernán Tapia Paredes	Ing. Gonzalo Olmedo
Autor	Director de Carrera