INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD PROFESIONAL ADOLFO LOPEZ MATEOS

“BLOQUEO DE TELEFONIA CELULAR PARA 2G Y 2.5G”

TESIS

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMUNICACIONES Y ELECTRÓNICA

PRESENTAN:

Machorro Arvizu Carlos Fernando

Ventura Baxin Jesús

ASESORES:

Ing. Fernando Cruz Martínez

M. en C. Javier Herrera Espinosa

MÉXICO D.F. 2011

AGRADECIMIENTOS

Les brindo mi sincero agradecimiento a todas las personas que con su apoyo hicieron posible la culminación de la presente tesis, a mi familia por su incondicional apoyo y aprecio, a mis amigos y compañeros que aportaron momentos de alegría indispensables para un excelente trabajo, al Instituto Politécnico Nacional por brindarme los conocimientos necesarios y el equipo para el desarrollo de la tesis.

A mis dos asesores, Javier Herrera Espinosa y Fernando Cruz Martínez, gracias por confiar y creer en nosotros, ya que sin su ayuda no hubiera sido posible el termino de este proyecto final. Al M. en C. Rubén Flores Leal y al profesor Heriberto Gonzales Jaimes por habernos apoyado con sus conocimientos.

Y a ti amigo Jesús Ventura Baxin “Bax” por acompañarme desde el inicio y fin. Compartiendo momentos de alegría, cansancio y gratitud, por no desistir y seguir siempre adelante.

GRACIAS A TODOS.

Carlos Fernando Machorro Arvizu

AGRADECIMIENTOS

Por la presente tesis y en general, por su aliento durante estos últimos años de estudio:

A mis familiares, por brindarme lo indispensable para salir adelante en la vida, por enseñarme a valerme por mi mismo y por inculcarme los valores que me distinguen y que han forjado mi persona. Y sobre todo, porque jamás dudaron de mí y en todo momento me alentaron a seguir adelante.

A mi amigo y compañero, Carlos Fernando Machorro Arvizu. Por compartir conmigo esta travesía tan importante, por cada momento. Y sobre todo por demostrar siempre mucha responsabilidad y trabajo continúo.

A los profesores Javier Herrera Espinosa y Fernando Cruz Martines, nuestros directores de Tesis, por jamás permitirnos caer durante este trayecto. Por haber depositado su confianza en nosotros, por su apoyo incondicional y sobre todo, gracias por brindarnos su tiempo.

Al IPN, por ser la Institución que me vio crecer y me instruyó como ingeniero, por brindarme las herramientas y conocimientos necesarios para servir a mí patria. Y sobre todo, por darme la oportunidad de pertenecer a esta gran institución.

GRACIAS.

Jesús Ventura Baxin

Resumen. El espectro electromagnético, hoy en día, es uno de los recursos mas explotados por los seres humanos, el cual tiene como objetivo el transporte de informacion para realizar una comunicación a distancia; sin embargo, cuando este recurso es utilizado de forma negativa, será necesario, realizar un bloqueo de su uso ya sea por cuestiones de confidencialidad o seguridad. El propósito de la presente tesis, es implementar un equipo que sea capaz de bloquear toda comunicación con equipos celulares móviles que trabajen con tecnologías de 2G y 2.5G. Los resultados obtenidos jugaran un papel preponderante en la reflexión, guía y desarrollo de proyectos a futuro, que estén basados en el bloqueo del espectro electromagnético para equipos de telefonía celular.

INDICE GENERAL

AGRADECIMIENTOS……..…I

RESUMEN……III

ÍNDICE DE FIGURAS……..……..VII

ÍNDICE DE TABLAS……..IX

GLOSARIO……..……X

CAPÍTULO 1. INTRODUCCIÓN

1.1 Generalidades……..1

1.2 Antecedentes……2

1.3 Objetivos……..……...4

1.4 Justificación……..……5

1.5 Estructura de Tesis ……..……..8

CAPÍTULO 2. TELEFONIA CELULAR

2.1 Acceso Múltiple……..9

2.1.1 Acceso Múltiple por División de Frecuencia……9

2.1.2 Acceso Múltiple por División de Tiempo……..10

2.1.3 Acceso Múltiple por División de Código……...11

2.2 Espectro Disperso……..12

2.2.1 Espectro Disperso por Saltos de Frecuencia (FHSS)……..…..13

2.2.2 Espectro Disperso por Secuencia Directa…. (DSSS)……...16

2.2.3 Códigos de Dispersión……18

2.3 Modos de Transferencia……21

2.4 Evolución de la Telefonía Celular……22

2.4.1 Primera Generación……23

2.4.2 Segunda Generación……24

2.4.3 Evolución GSM hacia 3G……26

2.4.4 Evolución CDMA ONE hacia 3G……26

2.4.5 Tercera Generación……27

2.4.6 Redes 3G……27

2.5 Fundamentos de un Sistema de Telefonía Celular……28

2.5.1 Componentes……28

2,5.2 Elementos……31

2.6 UMTS como Red de 3G……34

2.6.1 Arquitectura de UMTS……35

2.6.2 WCDMA: Interfaz de UMTS……38

CAPÍTULO 3. FUNDAMENTOS DE BLOQUEO

3.1 Guerra Electrónica……39

3.2 Principios de la EW……41

3.3 Protección Electrónica……42

3.4 Soporte Electrónico……43

3.5 Ataque Electrónico……44

3.6 Probabilidad de Detección e Intercepción……44

3.7 Jammer……45

3.7.1 Jamming por Ruido ……47

3.7.2 Jamming por Barrido……49

3.6.3 Jamming por Seguimiento……51

CAPÍTULO 4. CIRCUITO DE BLOQUEO: DISEÑO Y SIMULACIONES

4.1 Requerimientos del Jammer……52

4.2 Diseño del Jammer……54

4.2.1 Sección de Alimentación……54

4.2.2 Sección de Oscilación……55

4.2.3 Sección RF……62

4.3 Simulación del Jammer……70

4.3.1 Simulación: Sección de Alimentación……70

4.3.2 Simulación: Sección de Oscilación……71

4.3.3 Simulación: Sección RF……72

CAPÍTULO 5. EVALUACION: MEDICIONES Y RESULTADOS

5.1 Circuito de Bloqueo (Jammer)……75

5.2 Evaluación del Dispositivo……76

5.3 Presentación de Resultados para Celulares 2G y 2.5G……79

5.4 Presentación de Resultados para Celulares 3G……85

CAPÍTULO 6. CONCLUSIONES Y TRABAJO A FUTURO

6.1 Conclusiones……86

6.2 Trabajo a Futuro……88

APENDICE A. LEGISLACION DE JAMMER EN MEXICO……92

APENDICE B. DISEÑO PCB DE JAMMER……97

REFERENCIAS……100

INDICE DE FIGURAS

Capitulo 2 Introducción a la Telefonía Celular

Figura 2.1 Acceso múltiple por división de frecuencia. 10
Figura 2.2 Acceso múltiple por división de tiempo. 11
Figura 2.3 Acceso múltiple por división de código. 12
Figura 2.4 Espectro disperso por saltos de frecuencia. 14
Figura 2.5 FHSS Lento y FHSS Rápido. 15
Figura 2.6 Diagrama a bloques de un transmisor y receptor FHSS. 15
Figura 2.7 Dispersión de una señal portadora. 16
Figura 2.8 Diagrama a bloques de un sistema DSSS. 18
Figura 2.9 Principio de TDD y FDD. 22
Figura 2.10 Evolución en telefonía celular. 23
Figura 2.11 Estructura general de una red de telefonía celular. 30
Figura 2.12 Representación grafica de una celda. 31
Figura 2.13 Arquitectura de UMTS. 35
Figura 2.14 Arquitectura completa de UMTS. 38
Figura 2.15 Reutilización total de frecuencias en WCDMA. 38

Capitulo 3 Fundamentos de Bloqueo

Figura 3.1 puntos de ataque dentro del espectro electromagnético. 40
Figura 3.2 Componentes de la Guerra Electrónica. 41
Figura 3.3 Bloqueo de canales del espectro usando Jamming por ruido 48

Capitulo 4 Circuito de Bloqueo: Diseño y Simulaciones

Figura 4.1 Diagrama a bloques del Jammer. 53
Figura 4.2 Diagrama a bloques de la fuente de alimentación 54
Figura 4.3 Comparación en linealidad de señales 56
Figura 4.4 Señales con diferentes niveles de referencia en DC 56
Figura 4.5 Configuración para generar una señal triangular 57
Figura 4.6 Relación Vpp vs R_3 58

Figura 4.7 Configuración en emisor común 60
Figura 4.8 Recta de carga 61
Figura 4.9 Recta de carga resultante 62
Figura 4.10 Diagrama a bloques de la sección RF 63
Figura 4.11 Tipos de línea planar 64
Figura 4.12 Medición de la capacitancia de la placa 66
Figura 4.13 Conector 132136 RP-SMA de montaje superficial 68
Figura 4.14 Patrón de radiación omnidireccional de la antena 68
Figura 4.15 Pasos para la fabricación de extensión con conectores SMA 69
Figura 4.16 Resultados de simulación de la fuente 70
Figura 4.17 Ajuste de parámetros en señal triangular 71
Figura 4.18 Resultados en simulación del 2N2222 72
Figura 4.19 Parámetros de la línea de transmisión 73
Figura 4.20 Imagen 3D de la línea de transmisión 74
Figura 4.21 Posibles pérdidas de potencia 74

Capitulo 5 Evaluación: mediciones y resultados

Figura 5.1 PCB del Jammer 75
Figura 5.2 Presentación final del Jammer 76
Figura 5.3 Medición a la salida del transistor 2N2222 77
Figura 5.4 Medición de la sección RF 78
Figura 5.5 Patrón de radiación del Jammer y máximos resultados obtenidos 82
Figura 5.6 Funcionamiento de los Celulares con el jammer apagado 83
Figura 5.7 Funcionamiento de los Celulares con el jammer encendido 84

Apéndice B Diagrama eléctrico del circuito

Figura B.1 Software de simulación 97
Figura B.2 Software de diseño PCB 97
Figura B.3 Diagrama eléctrico del Jammer 98
Figura B.4 PCB final del Jammer 99
Figura B.5 PCB en 3D 99

INDICE DE TABLAS

Capitulo 2 Introducción a la telefonía celular

Tabla 2.1 Familia de códigos PN. 20
Tabla 2.2 Sistemas de telefonía móvil de primera generación. 24
Tabla 2.3 Tipos de celdas y aéreas de cobertura. 32
Tabla 2.4 Márgenes de interferencia. 33

Capitulo 4 Circuito de bloqueo: diseño y simulaciones

Tabla 4.1 Características eléctricas del XR-2206 para una señal triangular 58
Tabla 4.2 Frecuencia de Salida en función del voltaje de entrada 59
Tabla 4.3 Características eléctricas del 2N2222 60
Tabla 4.4 Especificaciones eléctricas del VCO JTOS-2000 63
Tabla 4.5 Resultados de la medición de la capacitancia de la placa 67
Tabla 4.6 Datos y resultado de ϵ_r 67
Tabla 4.7 Cortes del cable para una extensión SMA 69
Tabla 4.8 Especificaciones del RG-58/U 69
Tabla 4.9 Parámetros teóricos del XR2206 71

Capitulo 5 Evaluación: mediciones y resultados

Tabla 5.1 Resultados de la sección de oscilación. 78
Tabla 5.2 Resultados obtenidos de la medición de la sección RF 78
Tabla 5.3 Cobertura de bloqueo del Jammer 80
Tabla 5.4 Tiempos de respuesta 81

Capitulo 6 Conclusiones y trabajo a futuro

Tabla 6.1 Tiempos de respuesta respecto a complejidad del Dispositivo Móvil 88

Apéndice A Legislación de Jammer en México

Tabla A.1 Nivele típicos de transmisión de potencia 96

GLOSARIO

2G	Segunda generación de telefonía móvil
3G	Tercera generación de telefonía móvil
AMPS	Sistema de telefonía móvil avanzado (Advanced Mobile Phone System)
ASK	Modulación por desplazamiento de amplitud (Amplitude-shift keying)
BS	Estación Base (Base Station)
BSC	Estación Base de Control (Base Station control)
CDMA	Acceso múltiple por división de código (Code Division Multiple Access)
CN	Red Central (Central Network)
DAMPS	Sistema de telefonía digital móvil avanzado (Digital-Advanced Movil Phone System)
DL	Enlace de bajada (Down Link)
DSSS	Espectro disperso por secuencia directa (Direct Sequence Spread Spectrum)
EA	Ataque electrónico (Electronic Atack)
EDGE	Tasas de datos mejoradas para la evolución de GSM (Enhanced Data-rates for GSM Evolution)
EMCOM	Control de emisiones (Emission Control)
ES	Soporte electrónico (Electronic Support)
EW	Guerra electrónica (Electronic Wafare)
F-FH	Saltos de frecuencia rápida (Fast frecuency Hopping)
FDD	Duplexaje por división de frecuencia (Frequency Division Duplex)
FDMA	Acceso múltiple por división de frecuencias

FHSS	Espectro disperso por saltos de frecuencia (Frequency Hopping Spread Spectrum)
FSK	Modulación por desplazamiento de Frecuencia (Frequency-shift keying)
GPRS	Servicio general de paquetes por radio (General Packet Radio Service)
GSM	Sistema global para las comunicaciones móviles (Global System for Mobile communications)
IMT-2000	Telecomunicaciones móviles internacionales (International Movil telecomunications 2000)
IP	Protocolo de internet (Internet Protocol)
ISDN	Red digital de servicios integrados (Integrated Services Digital Network)
ITU	Unión internacional de telecomunicaciones (International Telecomunication Union)
LPD	Baja probabilidad de detección (Low Probability of Detection)
LPI	Baja probabilidad de intercepción (Low Probability of intercept)
MAC	Capa de control de acceso al medio (Medium Access Control)
MS	Estación Móvil (Mobile Station)
MSC	Centro de Conmutación (Mobile Switching Center)
NMT	Teléfonos móviles nórdicos (Nordic Mobile Telephones)
NTT	Teléfonos y telégrafos de Japón (Nippon Telephone and telegraph)
PN	Códigos pseudo ruido (Pseudo Noise)
PSK	Modulación por desplazamiento de fase (Phase-shift keying)
PSTN	Red pública conmutada (public switched telephone network)
QPSK	Modulación por cuadratura de fase (Quadrature Phase Shift Keying)
RLC	Capa de control de radio enlace (Radio Link Control)
S-FH	Saltos de frecuencia lenta (Slow Frecuency Hopping).

SS	Espectro disperso (Spread Spectrum)
SGSN	Nodo de soporte para los servicios de GPRS (Serving GPRS Support Node)
SMS	Servicio de mensajes cortos (Short Message Service)
TACS	Sistema de comunicaciones de acceso total (Total Access Communication System)
TDD	Duplexaje por división de tiempo (Time Division Duplex)
TDMA	Acceso múltiple por división de tiempo (Time Division Multiple Access)
THSS	Espectro disperso por saltos de tiempo (Time Hopping Spread Spectrum)
UE	Equipo de Usuario (User Equipment)
UL	Enlace de subida (Up Link)
UMTS	Sistema universal para las telecomunicaciones móviles (Universal Mobile Telecommunications System)
UTRAN	Red de Acceso de Radio (UMTS Terrestrial Radio Access Network)
WCDMA	CDMA de banda ancha (Wideband CDMA)

CAPÍTULO 1
INTRODUCCIÓN

1.1 GENERALIDADES

En términos de telecomunicaciones, una onda electromagnética tiene como principal objetivo, permitir la comunicación entre dos puntos distantes. Sin embargo, cuando se habla de una comunicación cuyo medio de transmisión es el aire, dicho objetivo puede verse distorsionado, ya que estas ondas tienen la particularidad de que, una vez transmitidas, pueden llegar a ser interceptadas, distorsionadas o bloqueadas. Este principio de origen, precisa la naturaleza de la *Guerra Electrónica*.

El concepto de guerra electrónica tiene sus orígenes en la segunda guerra mundial. Comenzando todo con la invención del radar. Ya que, después de su invención, este dispositivo fue implementado en los cazas nocturnos, navegación en los bombarderos, detección de submarinos y otra gran cantidad de aplicaciones.

Hoy en día, debido a que el empleo de las tecnologías inalámbricas ha ido en aumento, el acceso a dichas tecnologías se ha vuelto más fácil, y con ello también se vuelve más fácil emplear estas tecnologías de manera incorrecta. Por tanto, en respuesta a este mal uso de la tecnología, el interés por bloquear algunos dispositivos ha crecido también. Es decir, la guerra electrónica ha dejado de ser exclusivamente militar.

Uno de los principales dispositivos de tecnología inalámbrica usados ampliamente en el ámbito civil, son los teléfonos móviles o teléfonos celulares. Los cuales,

están siendo utilizados para fines no benéficos. Es por eso que surgió la necesidad de desarrollar dispositivos capaces de limitar su uso en ciertas áreas o bajo ciertas condiciones. A estos dispositivos capaces de limitar el uso de teléfonos celulares se les ha dado el nombre de *jammers*.

Los Jammers son equipos diseñados para bloquear la operación de teléfonos celulares mediante la emisión de una señal que interrumpe el proceso de comunicación entre el móvil y la estación base.

1.2 ANTECEDENTES

En la mayoría de los países el uso del jammer aún sigue causando cierto debate respecto a su uso. Debido a que al bloquear las señales de telefonía celular, los jammers están invadiendo e interfiriendo con frecuencias que son propiedad ajena. Es decir, se invade frecuencias cuyas licencias pertenecen a ciertas compañías de telefonía celular, y para las cuales pagaron el derecho a usarla. Además de que existe una posible exposición de personas a altos niveles de radiación electromagnética lo cual puede repercutir en la salud. Además, con el uso de un Jammer se impide la recepción de posibles llamadas o datos que pueden ser de crucial importancia.

Salvo algunos países como es el caso de Israel y Japón donde los bloqueadores son completamente legales, en la mayoría de los países aún siguen siendo ilegales y está prohibida su venta y distribución.

En el caso de México, los jammers aún no son completamente legales. Sin embargo se han presentado casos de su uso en bancos, templos y recientemente en reclusorios. Aunque esto no significa que deje de ser una invasión a la propiedad. Salvo este último caso donde incluso se tuvo que adicionar un artículo (75) a la ley Federal de Telecomunicaciones. El cual dice:

“Tratándose de centros penitenciarios y de readaptación social, tanto de máxima como de mínima peligrosidad, la señal para la recepción y transmisión de llamadas, desde y hacia el interior de la prisión por medio de telefonía celular, queda totalmente restringida por razones de seguridad” [A].

Por otra parte, como antecedentes de diseño e implementación de bloqueadores en México se tienen:

El en año 2003 se tiene el primer antecedente de un jammer desarrollado en el Instituto Politécnico Nacional (IPN), específicamente llevado a cabo por alumnas de la Unidad Profesional Interdisciplinaria de Ingeniería y Tecnologías Avandas (UPIITA). Este Jammer fue desarrollado para Bloquear las señales de teléfonos celulares basados en el sistema DAMPS. El cual constituye junto con GSM y CDMA ONE, uno de los sistemas de Segunda generación (2G) [B].

El segundo antecedente es del año 2006, y se trata de un jammer desarrollado en la Universidad de las Américas Puebla (UDLAP), desarrollado por un alumno de la Escuela de Ingeniería y Ciencias. Este Jammer fue desarrollado para Bloquear las señales de teléfonos celulares basados en el sistema GSM [C].

Puede verse que ambos trabajos de tesis fueron enfocados al bloqueo de telefonía celular de segunda generación (2G), ambos sistemas trabajan haciendo uso de las tecnologías FDMA/TDMA. Sin embargo DAMPS utiliza portadoras de 30 KHz divididos en 3 ranuras de tiempo. Y GSM utiliza portadoras de 200 KHz divididos en 8 ranuras de tiempo.

1.3 OBJETIVOS

Debido a la gran cantidad de nuevos usuarios de telefonía móvil que están demandando dispositivos tecnológicamente equipados para acceder a redes de mayor velocidad (Es decir, Dispositivos con tecnología 2.5G y 3G). Y tomando también en cuenta que, en nuestro país aun existe otra gran cantidad de usuarios que continúan haciendo uso de dispositivos con tecnología 2G. Se ha planteado como objetivo general y particular los siguientes:

1.3.1 Objetivo general

Diseño e implementación de un Jammer que funcione para telefonía celular con tecnología 2G y 2.5G.

1.3.2 Objetivo particular

Registrar el comportamiento de un teléfono móvil de 3G dentro de una zona de bloqueo de 2G.

Para cumplir con dichos objetivos, primero se deberá realizar una investigación de las características de los sistemas de 2G. En específico, sobre la banda de frecuencias a la que operan y, la técnica de acceso múltiple que utilizan dichos sistemas.

Posteriormente se investigará acerca de las diferencias entre una generación y otra, haciendo énfasis en los accesos al medio, ya que los sistemas de 2G como los de 3G utilizan diferentes formas de acceso. Debido a la incertidumbre que existe acerca de cuál es la banda de frecuencias a la que los sistemas de 3G están operando en México, se deberá realizar también la investigación correspondiente.

Una vez que se haya recopilado toda la información acerca de los sistemas de telefonía celular, resultará imprescindible el estudio y análisis de las técnicas de bloqueo o técnicas de jamming, para adecuar una de dichas técnicas al presente proyecto. Esto se lograra eligiendo una técnica de jamming para realizar el diseño del dispositivo o Jammer que empleara dicha técnica. Además, será también indispensable realizar el estudio de los diferentes componentes electrónicos que nos servirán para llevar a cabo el desarrollo del circuito físico.

1.4 JUSTIFICACIÓN

El gran avance que hoy en día se está viviendo con las tecnologías inalámbricas ha marcado un paso muy importante para la humanidad. Dicho avance continúa en aumento, al grado de que su uso e implementación está ahora al alcance de cualquier persona. Sin embargo, este fácil acceso a la tecnología se ha convertido en un problema. Principalmente cuando hablamos de telefonía móvil, ya que su uso se está empleando con fines diferentes a los que fueron propuestos originalmente.

Solo por citar algunos ejemplos tenemos:

- Activación de explosivos en actividades terroristas vía remota por medio de teléfonos móviles.

- Fuga de información empresarial altamente confidencial. Debido a que los Smartphone (Teléfonos inteligentes) modernos ya pueden funcionar como punto de acceso a internet por banda ancha usando la red celular.

- Rastreo satelital. Aunque, la ubicación geográfica se obtiene por un dispositivo GPS colocado en el objeto o sujeto del cual se desea saber la ubicación, la transmisión hacia el centro de monitoreo suele realizarse

desde este dispositivo hacia el centro de monitoreo por medio de llamada programada a celular.

- Comunicaciones peligrosas en reclusorios. Los reos se han encargado de introducir furtivamente teléfonos celulares para realizar llamadas anónimas de extorción, amenazas o engaño.

- Deshonestidad en exámenes universitarios o empleos. Se tienen registros de varias universidades en las cuales se ha detectado que el personal usa mensajes SMS para recibir respuestas de algunas de sus preguntas.

- El simple hecho de irrumpir en la tranquilidad de ciertos lugares como: cines, iglesias, hospitales, teatros, etc.

Toda esta problemática se intentará resolver mediante el diseño de un inhibidor de señales electromagnéticas, que opere bajo las frecuencias a las cuales operan las redes de telefonía móvil. Es decir, mediante un Jammer de Telefonía celular.

Como profesionales e Ingenieros en Comunicaciones y Electrónica, esta problemática acerca del mal uso de las tecnologías de comunicación móvil, nos concierne directamente. Ya que si bien, no somos nosotros quienes estamos ocasionando realmente el problemas, si somos los que disponen de las herramientas adecuadas para desarrollar las contramedidas necesarias y de esta manera terminar o disminuir dicho problema.

Primero que nada, con el desarrollo de este trabajo se pretende poner fin a los problemas planteados sobre el uso inadecuado de los teléfonos móviles. Y segundo, se pretende también alentar a los estudiantes de ingeniería a desarrollar más tecnología en nuestro país, innovar ideas y llegar más allá de simplemente lo adquirido en las aulas de clase.

Por último, este trabajo será capaz de brindar beneficios a todas aquellas personas interesadas en preservar la seguridad, tranquilidad y orden. Abarcando por tanto, diferentes sectores de la sociedad. Desde el civil, religioso y militar.

1.5 ESTRUCTURA DE TESIS

- Capítulo 1

En este primer capítulo, se brinda una introducción general acerca de la problemática que ha motivado a la realización del presente trabajo. Se expone la razón de ser de la tesis; además, se explica con qué fines se desarrolla y la manera en que se llevará a cabo.

- Capítulo 2

Todo proyecto consta de un sustento teórico que sirve de base para la realización del mismo. Por ello con este capítulo se empiezan a dar las pautas que servirán para el posterior análisis del problema y el planteamiento de las posibles soluciones.

- Capítulo 3

En este capítulo se exponen los fundamentos y la teoría de bloqueo que permite realizar una descripción de las técnicas de Jamming y plantear una posible solución.

- Capítulo 4

En este capítulo se retoma la solución propuesta y se brindan las herramientas tecnológicas, tanto electrónicas como de comunicaciones que permitirán desarrollar e implementar dicha solución en forma física, realizando una descripción y análisis de cada parte del Jammer.

- Capitulo 5

El capitulo 5 se evaluara el dispositivo con el cual se realizaran mediciones y se registraran los resultados obtenidos para consolidar la elaboración del proyecto. Aquí se visualiza si la solución propuesta realmente da solución al problema planteado. Finalmente, en este apartado del proyecto se realiza un análisis de los resultados obtenidos en comparación con los objetivos planteados inicialmente. Con lo cual se generan diversas conclusiones relacionadas tanto a los objetivos que fueron alcanzados como a los que no. Además, en acuerdo también con dicho análisis, se plantean las posibles mejoras al proyecto y se plantean como trabajo a futuro.

CAPÍTULO 2
TELEFONÍA CELULAR

2.1 ACCESO MÚLTIPLE

El acceso múltiple es una técnica por la cual se organizan o distribuyen de manera eficiente, los recursos de comunicaciones, como el tiempo y el ancho de banda asignados para cada usuario. Esta distribución se realiza para transmitir información de manera correcta y eficaz; logrando así, que ninguna asignación de tiempo o frecuencia, se desperdicie; de tal manera que los recursos se puedan compartir de manera equitativa.

Para telefonía celular, se tienen tres formas diferentes de acceso múltiple las cuales son:

- Acceso Múltiple por División de Frecuencia (FDMA)
- Acceso Múltiple por División de Tiempo (TDMA)
- Acceso Múltiple por División de Código (CDMA)

2.1.1 Acceso Múltiple por División de Frecuencia

Esta técnica de acceso se basa en la división del ancho de banda de una línea entre varios canales, donde cada canal ocupa una parte del ancho de banda de la frecuencia total, adoptando bandas de guarda que funcionan como zonas de separación para reducir la interferencia entre canales vecinos (ver figura 2.1) [1,2].

Esta técnica es de tipo analógico y fue utilizada como acceso al medio para telefonía celular de primera generación tales como AMPS (Advanced Mobile

Phone System) en Estados Unidos, TACS (Total Access Communication System) en Inglaterra, NMT (Nordic Mobile Telephones) en los países nórdicos y NTT (Nippon Telephone and telegraph) en Japón.

FDMA tiene como principales características:

- Ser eficaz, sencilla y de bajo costo.
- Sus canales de frecuencia no requieren sincronización.
- Desperdicia ancho de banda por el uso de bandas de guarda.
- No es apropiada para el manejo de información digital [3].

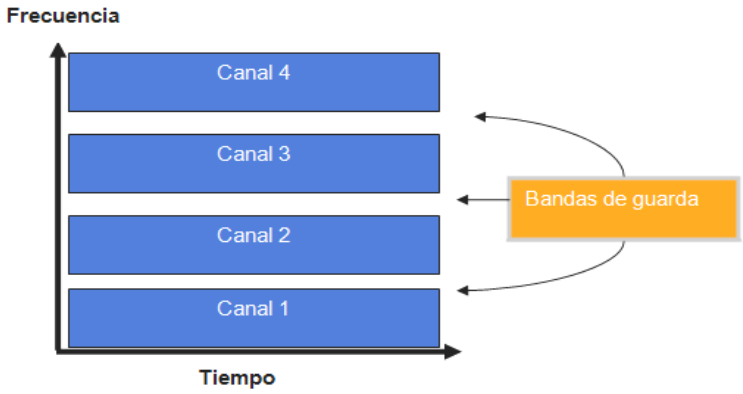

Figura 2.1 Acceso múltiple por división de frecuencia.

2.1.2 Acceso múltiple por división de tiempo

En esta técnica se realiza la división por espacios periódicos o ranuras de tiempo (llamados time-slots) de todo el ancho de banda asignado a un canal de transmisión. Las distintas ranuras de tiempo están repartidas por igual sobre todo el canal, además, como forma de protección, se tiene ligado a cada ranura de tiempo un espacio de guarda para evitar el traslape entre canales. La figura 2.2 muestra un ejemplo de TDMA [1,2].

TDMA trabaja asignando una ranura de tiempo a cada usuario, por lo que el usuario podrá hacer uso de este recurso, durante un periodo corto de tiempo. De esta manera el canal podrá ser compartido por tantos usuarios como ranuras de tiempo existan. Esta tecnología se puso en práctica con la llegada de la segunda era digital con los estándares GSM (Global System for Mobile communications) en Europa, DAMPS (Digital Advanced Movil Phone System) en Estados Unidos y PDC (Personal Digital Cellular) en Japón.

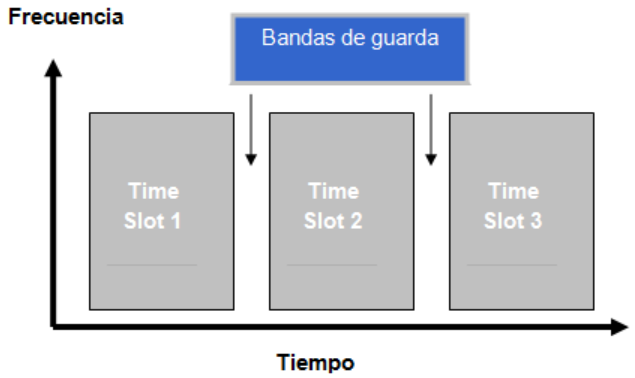

Figura 2.2 Acceso múltiple por división de tiempo.

2.1.3 Acceso múltiple por división de código

Esta técnica se basa en el reconocimiento de códigos los cuales son asignados para cada usuario, este reconocimiento se da tanto en el código generado, transmitido y el recibido, permitiendo que el receptor pueda diferenciar la señal del usuario deseado de entre muchas señales que viajan por el mismo canal. Lo que permite que las señales de diferentes fuentes puedan ser transmitidas al mismo tiempo y sobre la misma banda de frecuencia, además de esto, el uso de códigos permite que el receptor y el transmisor, puedan llevar a cabo una comunicación eficiente y sin interrupciones o interferencias, por usuarios no deseados [1, 2].

CDMA permite acomodar una gran cantidad de usuarios en un periodo corto de tiempo. La figura 2.3 muestra un agrupamiento de tres canales sobre un mismo

canal de tiempo y frecuencia. Esta tecnología de acceso se utiliza para sistemas de segunda generación que trabajan con el estándar IS-95 de Estados Unidos y el cual es completamente digital.

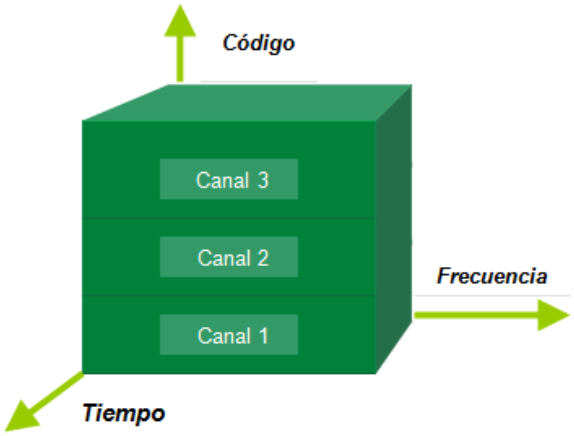

Figura 2.3 Acceso múltiple por división de código.

2.2 ESPECTRO DISPERSO

El uso de la técnica de modulación por espectro disperso (SS: Spread Spectrum) es la forma por la cual se llega a la tan ansiada banda ancha usando para esto *los códigos de dispersión*; existen tres formas básicas de lograr esto, y que en un principio fueron desarrolladas originalmente para sistemas militares por su resistencia ante señales de interferencia y por su baja probabilidad de detección. Los métodos de modulación para generar *Spread Spectrum* son los siguientes:

- **TH**SS (Time Hopping Spread Spectrum), técnica de saltos de tiempo, en la que se combina el intervalo de transmisión dentro de una estructura de trama temporal.

- **FH**SS (Frequency Hopping Spread Spectrum), técnica de saltos de frecuencia, en la que la portadora cambia con el tiempo según sea el patrón establecido.

- **DS**SS (Direct Sequence Spread Spectrum), técnica de secuencia directa en la que la señal de información es multiplicada por una secuencia de chips de mayor velocidad.

Existe una cuarta variante en la cual se hace una combinación de alguna de las tres técnicas antes mencionadas, la cual da como resultado el Hybrid Spread Spectrum, sin embargo para redes móviles de 2G, 2.5G se hace uso de FHSS y 3G por su parte utiliza DSSS, por lo cual solo se profundizará en esta dos formas de espectro disperso [3].

2.2.1 Espectro disperso por saltos de frecuencia (FHSS)

Esta técnica se basa en tomar la señal portadora para después realizar una modulación con códigos de dispersión, los cuales hacen que la señal de información vaya saltando de un rango de frecuencia a otro (posiblemente el mismo). Durante un intervalo de tiempo T_h, la señal portada permanecerá en una frecuencia especifica, pasado ese intervalo T_h hará un salto a otra frecuencia portadora (ver figura 2.4). Los códigos de dispersión usados para estos cambios son llamados hopping code (cogidos de saltos), estos códigos deciden los saltos en el rango de frecuencia. Estos rangos de frecuencia son llamados hop-set [3].

Una señal de espectro disperso por saltos de frecuencia, se representa matemáticamente por la ecuación (2.1), mientras que la probabilidad de que dos o más señales ocupen el mismo hop-set esta dado por la ecuación (2.2) en donde M son los posible canales de salto y K el numero de interferencia entre usuarios [4].

$$c(t) = \sqrt{2}cos2\pi(f_0 + if_1)t \qquad con\ \ iTc \leq t \leq (i+1)T_C \qquad (2.1)$$

$$P_h = 1 - \left(1 - \frac{1}{M}\right)^{K-1} \qquad (2.2)$$

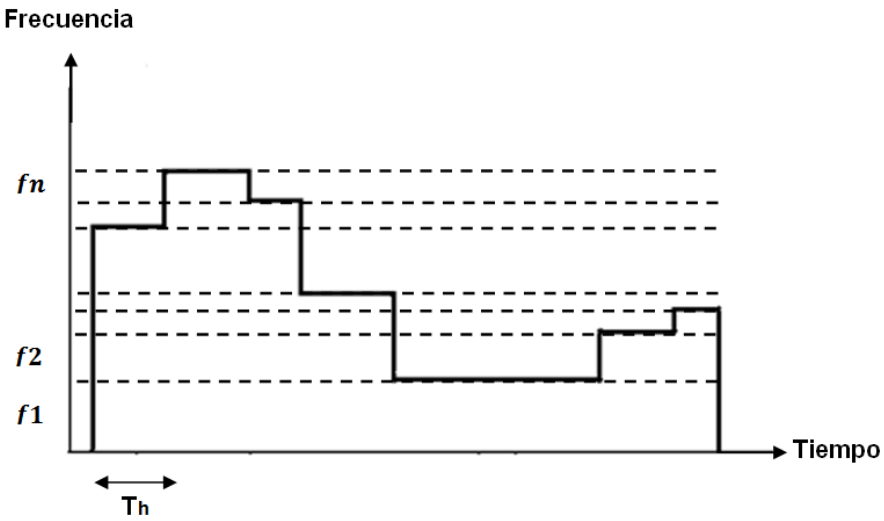

Figura 2.4 Espectro disperso por saltos de frecuencia.

La velocidad a la cual la señal portadora va a cambiar de frecuencia va a depender del simbol rate (taza de símbolos) con lo cual se tendrán un FHSS de dos tipos: F-FH (Fast frecuency Hopping) y S-FH (Slow Frecuency Hopping). En el primero la frecuencia portadora cambiara un número de veces durante la transmisión del símbolo lo cual hará que los bits que conforman este símbolo, sean transportados en diferentes frecuencias portadoras.

En el segundo caso los bits que conforman un símbolo serán transportados en la misma frecuencia portadora. La figura 2.5 muestra un ejemplo de F-FH y S-FH en la cual T_b representa el tiempo de transmisión de un bit, T_S el tiempo de transmisión de un símbolo y T_C el tiempo de transmisión de un chip.

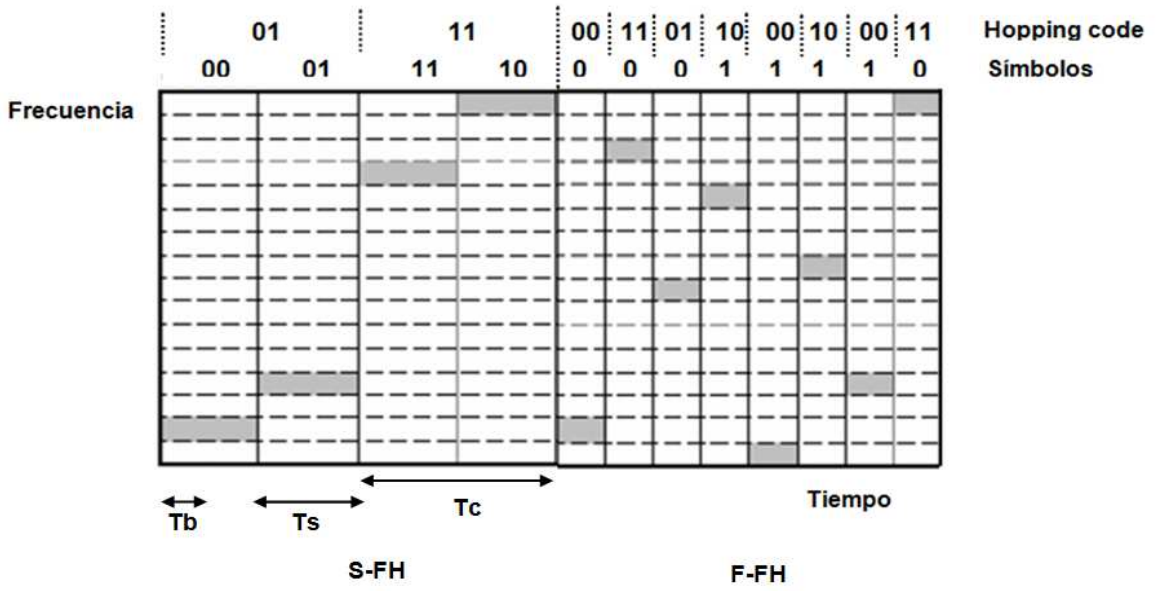

Figura 2.5 FHSS Lento y FHSS Rápido.

En la figura 2.5 se observa que usando S-FH el símbolo conformado por los bits 00 serán transmitidos sobre la misma portadora, mientras que en F-FH el mismo símbolo (00) será transmitido por dos portadoras diferentes. Por último, en la parte del receptor se contara con un sincronizador que en conjunto con el generador de código local permitirán que la señal se reciba correctamente, dado que es preciso conocer el patrón de salto para saber a qué frecuencia se está trabajando en ese momento. En la figura 2.6 se muestra un diagrama a bloques de un sistema de FHSS [3].

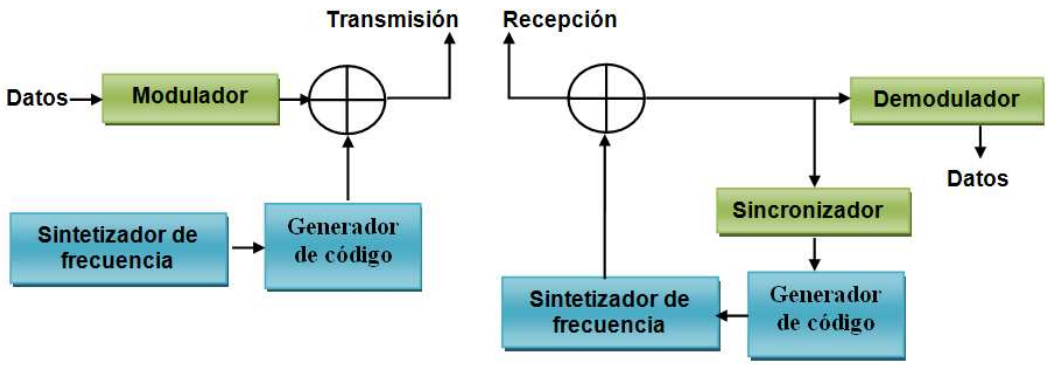

Figura 2.6 Diagrama a bloques de un transmisor y receptor FHSS.

2.2.2 Espectro disperso por secuencia directa (DSSS)

Esta técnica de espectro disperso se basa en la combinación de una señal portadora con un código de dispersión, la cual es independiente de la señal de información y cuenta con un *bit rate* (taza de bits) mayor al de la señal de información. Cada bit de la señal de información será representado por múltiples bits del código de dispersión. La función que tienen los códigos además de representar los bits de la señal de información, consiste en esparcir la señal sobre el ancho de banda mayor al de la señal original. La dispersión de la señal se aplica mediante una suma módulo dos (operación OR exclusiva) en el transmisor. Un ejemplo de esto es la figura 2.7.

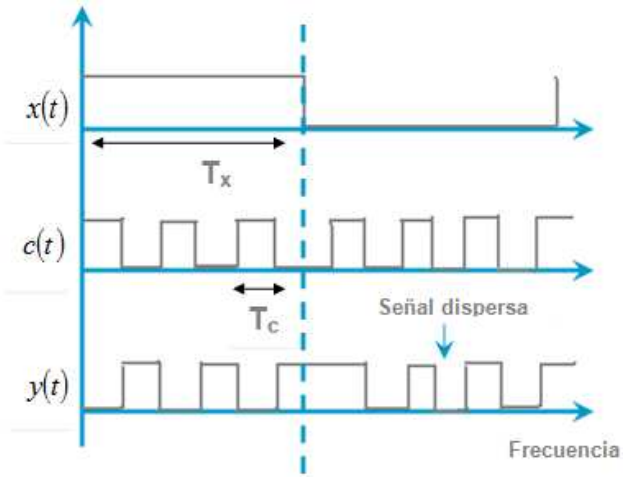

Figura 2.7 Dispersión de una señal portadora.

En la figura 2.7 se muestra una señal banda base $x(t)$, a la cual se le aplica la operación OR exclusiva por un código de dispersión $c(t)$, al realizar esta operación se obtendrá como resultado una señal $y(t)=x(t)\oplus c(t)$. La forma de onda de la señal combinada tendrá un mayor ancho de banda que la señal original. Además se muestran los tiempos de duración de los pulsos, tanto para la señal en banda base como para la secuencia de ensanchamiento, con lo cual se observa que $1/T_c \rangle\rangle 1/T_x$, en donde T_x es el intervalo de bit y T_c es el intervalo de bit del código de dispersión, llamado Chip.

Matemáticamente una señal de espectro disperso por secuencia directa se puede representar por la ecuación (2.3), en la cual A representa la amplitud de la señal, x(t) es la señal portadora, c(t) es el código de dispersión, f_C es la frecuencia de la portadora y θ la fase [4].

$$y(t) = Ax(t)c(t)\cos(2\pi f_C t + \theta) \qquad (2.3)$$

Los códigos de dispersión que están dados por c(t) están representados por la ecuación (2.4), en donde c_i es igual a +1 o -1 y representa el chip de la secuencia de dispersión. La forma de onda del chip $\psi(t)$ se limita idealmente en un intervalo de [0, Tc], esto se hace para prevenir posibles interferencias en el receptor entre chips [4].

$$c(t) = \sum_{i=-\infty}^{\infty} c_i\, \psi(t - iT_C) \qquad (2.4)$$

La razón de Tx entre Tc se le conoce como ganancia de procesamiento y da como resultado un numero entero igual al número de chips en un intervalo de símbolos (un símbolo es un conjunto de chips) y está representado por la formula (2.5) [4].

$$G_p = \frac{T_X}{T_C} \qquad (2.5)$$

Por su parte en el receptor se recibe la señal $y(t)$ a la cual se le aplica un código pseudo aleatorio $c_1(t)$ producido por un generador local en el receptor para poder recuperar la información transmitida $x(t)$ de manera correcta. Es necesario que el receptor se encuentre en sincronía con el transmisor. En la figura 2.8 se muestra un diagrama a bloques completo de un sistema DSSS.

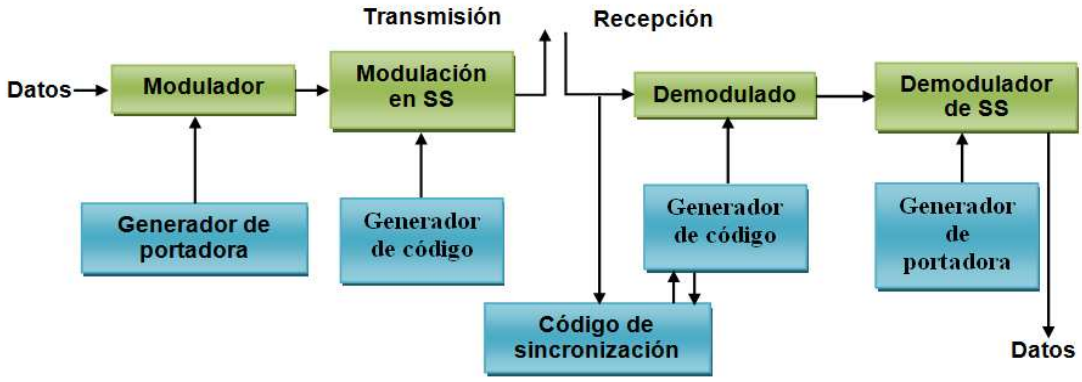

Figura 2.8 Diagrama a bloques de un sistema DSSS.

2.2.3 Códigos de dispersión

Los códigos de dispersión son una secuencia de bits que se utilizan en el transmisor y receptor. Se utilizan para realizar diferentes funciones como el esparcir una señal sobre una ancho de banda mayor o realizar saltos de frecuencia. Estos códigos están compuesto por un número igual de 1's o 0's, pueden ser largos o cortos.

Los códigos cortos abarcan un símbolo por periodo mientras que los códigos largos abarcan varios símbolos por periodo. La correlación (valor que determina que tanta similitud hay entre un conjunto de secuencias con otra) debe ser mínima para evitar una confusión entre un uso de diferentes códigos de dispersión en los receptores, esto evita que no se identifique información de algún usuario no deseado.

Estos códigos permiten que la señal se disperse por debajo del nivel de ruido logrando la nula interferencia entre usuarios y la resistencia a un ambiente con ruido.

Este proceso se realiza tanto en el enlace ascendente (UL: uplink) como en el enlace descendente (DL: downlink). Estos códigos se dividen en dos: códigos Walsh y códigos pseudo aleatorios (PN: Pseudo Noise).

- Códigos pseudo aleatorios

Los códigos pseudo aleatorios, como se menciono antes, son una secuencia de bits, esta secuencia pseudo aleatoria al ser generada deber ser sucesiva, esto significa dentro de un periodo de la secuencia, se tendrán cadenas de unos y ceros, en el cual, el número de cadenas de cada una de estas deben ser iguales.

En cada periodo la mitad de las cadenas del mismo valor tendrá una longitud de 1, para un cuarto del periodo la longitud será de 2, para un octavo la longitud será de 3 y así sucesivamente.

Esta secuencia debe estar balanceada, esto es que la generación del número de unos o ceros binarios en un periodo de la secuencia puede diferir solo en uno, la cantidad de unos y ceros. Su correlación está definida entre un rango de -1 y 1, por ejemplo si el valor de correlación de un par de secuencias es 1 entonces ambas secuencias son iguales, si el valor de la correlación es 0, significa que no hay relación entre el par de secuencias y si el valor de correlación es de -1 significa que una secuencia es espejo de la otra.

Los códigos PN pueden ser de longitud variable, lo cual da lugar a la familia de códigos PN, las cuales se muestran en la tabla 2.1. El periodo máximo de los código estará dado por la formula (2.6) tomando a **n** de la tabla de la familia de los códigos [3].

$$N = 2^n - 1 \qquad (2.6)$$

Tipo	Rango	Numero de códigos	Máxima correlación cruzada
Gold	n =1 a 2	$2^n + 1$	$2^{\frac{n+1}{2}} + 1$
Gold	n = 2 a 4	$2^n + 1$	$2^{\frac{n+1}{2}} + 1$
Gold like	n = 0 a 4	2^n	$2^{\frac{n+1}{2}} - 1$
Gold like	n = 0 a 4	$2^n + 1$	$2^{\frac{n+1}{2}} - 1$
S-Kasami	n = 2 a 4	$2^{\frac{n}{2}}$	$2^{\frac{n}{2}} + 1$
L-Kasami	n = 1 a 2 n = 0 a 4	$2^{\frac{n}{2}}(2^n + 1)$ $2^{\frac{n}{2}}(2^n + 1) - 1$	$2^{\frac{n}{2}} + 1$ $2^{\frac{n}{2}} + 1$
VL-Kasami	n = 2 a 4	$2^{\frac{n}{2}}(2^n + 1)^2$	$2^{\frac{n+4}{2}} + 1$
Dual-BCH	n = 0 a 2	$2^{\frac{n}{2}}$	$2^{\frac{n+1}{2}} + 1$
4-phase set A	n > 0	$2^n + 1$	$2^{\frac{n}{2}} + 1$

Tabla 2.1 Familia de códigos PN.

- Códigos Walsh

Los códigos ortogonales son secuencias ortogonales que cuentan con una correlación de cruce de ceros entre ellas. Estos códigos son usados en sistemas de CDMA para esparcir la señal sobre un ancho de banda mayor al de la señal portadora. Los códigos Walsh se generan por medio de matrices Walsh-Hadamard (2.7), las cuales son matrices cuadradas con valores de 1's y 0's con una longitud potencia de 2 y con N secuencias diferentes de longitud M. Cada fila o columna es una secuencia ortogonal. Su representación está dada a continuación:

$$H_0 = 0 \qquad H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & \overline{H}_{n-1} \end{bmatrix} \qquad (2.7)$$

Otra forma de códigos ortogonales son los códigos de triple estructura ortogonal para diferentes factores de dispersión. Un ejemplo de esto se muestra en la figura 2.9.

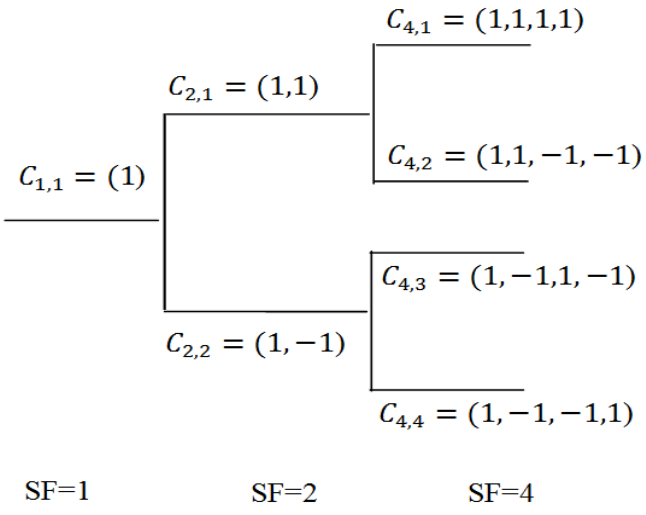

Figura 2.9 Construcción de códigos ortogonales para diferentes factores de dispersión.

La generación de códigos ortogonales de triple estructura está dada por la ecuación (2.8), donde C_{2n} es un código ortogonal de tamaño 2n. Las secuencias pertenecientes a la misma rama forman un conjunto de códigos ortogonales [3].

$$c_{2n} = \begin{pmatrix} c_{2n,1} \\ c_{2n,2} \\ \vdots \\ c_{2n,2n} \end{pmatrix} = \begin{bmatrix} \begin{pmatrix} c_{n,1} & c_{n,1} \\ c_{n,1} & -c_{n,1} \end{pmatrix} \\ \vdots \\ \begin{pmatrix} c_{n,n} & c_{n,n} \\ c_{n,n} & -c_{n,n} \end{pmatrix} \end{bmatrix} \qquad (2.8)$$

2.3 MODOS DE TRANSFERENCIA

Existen dos modos de transferencia que son un requerimiento para las redes 2G y 3G las cuales son: Duplexaje por División de Tiempo (TDD: Time Division Duplex) y Duplexaje por Division de Frecuencia (FDD: Frecuency Division Duplex). En el Duplexaje por División de Tiempo, las transmisiones de los enlaces ascendentes y

descendentes son multiplexados en tiempo por la misma portadora en contraste al Duplexaje por División de Frecuencia en el cual las transmisiones realizadas en los enlaces ascendente y descendente ocurren en frecuencias de bandas separadas.

El modo de transferencia FDD hace uso de diferentes bandas de frecuencia, permitiendo grandes distancias entre móvil y estación base. En una red pública con cobertura nacional, esto es necesario para lograr requerimientos aceptables de cobertura mientras que el modo TDD puede sólo ser usada para pequeñas distancias, sin embargo, esto permite una mayor velocidad de transmisión y flexibilidad para un tráfico asimétrico, tal como el uso de internet. La figura 2.9 ilustra los principios de FDD y TDD [3].

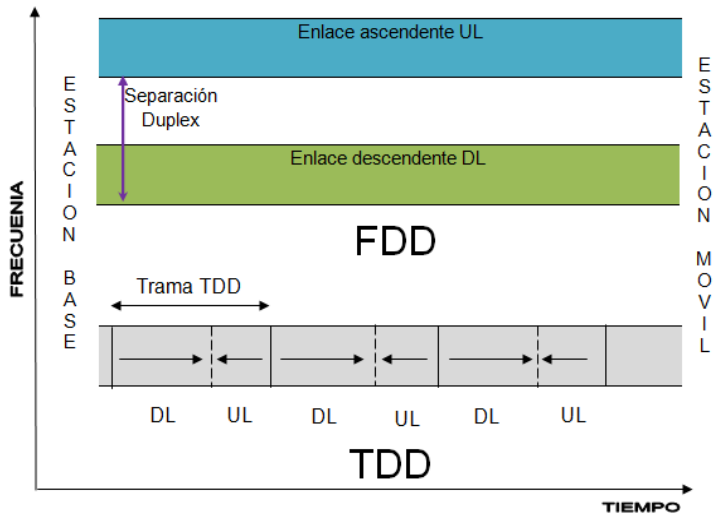

Figura 2.9 Principio de TDD y FDD.

2.4 EVOLUCIÓN DE LA TELEFONÍA CELULAR

Un sistema de telefonía celular se define como una red de comunicaciones vía ondas de radio, que tiene como principal característica, permitir la movilidad continúa tanto del emisor como del receptor. La telefonía móvil ha tenido distintos grados de evolución y a estas etapas se les ha denominado generaciones. Así

desde el comienzo de la era de la telefonía celular en 1979, las comunicaciones móviles sin duda alguna han experimentado un enorme crecimiento, desarrollándose diversas tecnologías y sistemas para brindar servicios de comunicación inalámbrica. En general el desarrollo de los sistemas celulares en sus diferentes generaciones se ha dado como se indica en la figura 2.10.

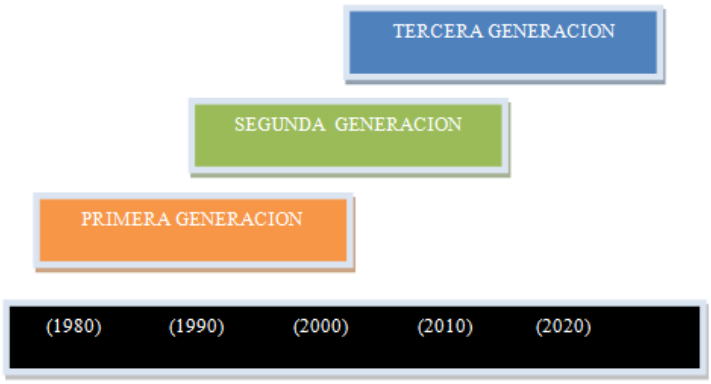

Figura 2.10 Evolución en telefonía celular.

2.4.1 Primera Generación

Los sistema móviles de primera generación se caracterizaban por realizar la transmisión analógica de voz con baja calidad y utilizando para su funcionamiento la técnica de Acceso Múltiple por División de Frecuencia (FDMA: Frecuency Division Multiple Access), lo que producía que los sistema fueran bastante limitados en relación al número de usuarios a los que podía dar servicio, además de contar con una limitada capacidad de roaming (capacidad de moverse y pasar entre diversas aéreas de cobertura sin la interrupción del servicio o perdida de la comunicación).

La tabla 2.2 muestra los sistemas de telefonía móvil de primera generación de mayor relevancia, haciendo mención en la cantidad de canales con que contaban estos sistemas y el ancho de banda que requería cada uno de sus canales [3].

SISTEMA	PAIS	No. CANALES	LONGITUD DE CANAL (Khz)
AMPS	E.U.A	832	30
NMT	ESCANDINAVIA	180	25
NTT	JAPON	2400	6.25
TACS	REINO UNIDO	1000	12.5

Tabla 2.2 Sistemas de telefonía móvil de primera generación.

2.4.2 Segunda Generación (2G)

Ante la limitada cantidad de canales que se podían soportar, con un ancho de banda basado en FDMA en los sistemas de primera generación, se propusieron nuevas alternativas para incrementar la cantidad de usuarios soportados simultáneamente. Surge entonces una segunda generación, caracterizada por ser digital, en lugar de analógica. Aparecieron nuevos métodos de acceso al medio, ya que ahora en lugar de implementar únicamente FDMA, se recurrieron a 2 nuevas tecnologías: Acceso Múltiple por División de Tiempo (TDMA: Time Division Multiple Access) y Acceso Múltiple por División de Códigos (CDMA: Code Division Multiple Access).

De esta manera, el primer sistema de segunda generación apareció en 1993 denominado IS-95, también conocido como CDMAone (Su nombre se debe precisamente a que fue el primer sistema basado en CDMA). De la misma forma, un año más tarde surgió el primer sistema basado en TDMA, al cual se le dio el nombre de IS-136, también conocido con el nombre de DAMPS (Digital-Advanced Movil Phone System), se trata de una evolución del antiguo sistema AMPS de primera generación, pero ahora digital.

La digitalización trajo consigo la reducción de tamaño, costo y consumo de potencia en los dispositivos móviles, así como nuevos servicios tales como:

identificador de llamadas, envío de mensajes cortos (SMS: Short Message Service), mensajes de voz, entre otros. Además, dentro de estos nuevos sistemas de segunda generación se logró soportar una velocidad de información más alta y se tuvo avances significativos en seguridad, calidad de voz y de roaming. Dentro de los sistemas de telefonía celular de segunda generación destacan: CDMAone, DAMPS Y GSM [3].

- GSM

En un inicio, toda Europa utilizaba diferentes sistemas de telefonía celular, siendo incompatibles entre sí, por lo que en 1982 la *Conference Européenne des Postes et Télécommunications* (CEPT) estableció el desarrollo del inicio del estándar GSM conocido en ese entonces como *Groupe Special Mobile* (el cual ahora significa: Global System for Mobile communications), después de algunos años de desarrollo, se llego a un acuerdo en 1988 en donde todos los países europeos firmarían y se comprometerían a cumplir las especificaciones, adoptando el estándar GSM como único. Acuerdo que se cumplió y lo sigue siendo hoy en día. Estos sistemas GSM se caracterizan por utilizar una combinación entre FDMA Y TDMA en un espectro total de 25 MHz. FDMA divide esos 25 MHz en 124 canales portadores de 200 Khz cada uno, y cada canal es entonces dividido en 8 ranuras de tiempo utilizando TDMA [3].

- DAMPS

El ancho de banda de los canales en DAMPS era el mismo que en su predecesor AMPS (30 Khz), solo que ahora, gracias a la tecnología TDMA, cada canal fue dividido en 3 ranuras de tiempo. De este modo, en este sistema se transmiten 3 canales por cada portadora de 30 Khz, incrementando en 3 veces la capacidad con respecto al sistema analógico AMPS [3].

- IS-95 CDMA

A diferencia del ancho de banda de los canales en los sistemas GSM y TDMA, en CDMA se utiliza un ancho de canal de 1.25 MHz, donde cada usuario tiene acceso a él, contando para ello con un código para poderse diferenciar del resto de los usuarios y optimizando de esta forma el uso del espectro. Por lo anterior, con CDMA se incrementa la capacidad del sistema de 10 a 15 veces comparado con AMPS, y más de 3 veces comparado con los sistemas basados en TDMA, como en el caso de DAMPS [3].

2.4.3 Evolución de GSM hacia 3G

En el camino de GSM hacia la tercera generación se desarrollo GPRS (General Packet Radio Service), el cual se caracteriza por añadir conmutación de paquetes a la red GSM, ya que anteriormente se utilizaba la conmutación de circuitos y por lo tanto no se utilizaba eficientemente el ancho de banda.

Con GPRS 8 usuarios pueden compartir una única ranura de tiempo que antes se asignaba a uno solo, logrando de esta forma 115 kbit/s teóricos. Después de GPRS, llega EDGE (Enhanced Data-rates for GSM Evolution), también conocido como GSM 384, ya que alcanza una velocidad de transmisión de 384 kbit/s.

2.4.4 Evolución de CDMA ONE hacia 3G

En el caso de las redes basadas en CDMA, la transición se da con 2 pasos migratorios: IS-95B e IS-95C, que vendría siendo las versiones B y C de CDMAone. La norma IS-95B ofrece una velocidad de 64 kbit/s durante la operación a ráfagas del móvil. Esta velocidad ya es adecuada para acceso a internet y aplicaciones que requieran velocidades medias. En tanto IS-95C también conocida como CDMA2000 1X (CDMA 2000 fase uno) emplea un canal de 1.25 MHz de ancho de banda y ofrece una velocidad de 144 Kbit/s para aplicaciones móviles y estacionarias.

2.4.5 Tercera Generación (3G)

La primera y segunda generación de sistemas de comunicación móvil tuvieron como objetivo primordial, dar soporte a comunicaciones de voz y aunque en la segunda generación se pueden transmitir datos a baja velocidad, no satisfacen los requerimientos de transmisión de grandes volúmenes de información a altas velocidades entre terminales inalámbricas y la red fija. Donde dichos requerimientos son necesarios para aplicaciones como videoconferencias, conexión a internet, audio y video. A ello se añade que en la actualidad, los usuarios buscan un servicio eficiente no solo de telefonía celular para voz y pequeñas transferencias de información, sino además de acceso a servicios multimedia y transferencia de grandes volúmenes de información lo cual ha provocado que se sature la capacidad de los sistemas.

Por lo tanto para dar soporte a los usuarios que requieren cada vez más de los servicios de 3G, se ha ido evolucionando en las tecnologías ya existentes. Por ejemplo, se han realizado importantes mejoras tecnológicas en los sistemas GSM y CDMA ONE, a tal grado que hoy en día se han convertido en sistemas de tercera generación. No obstante, siguen conservando las mismas técnicas de acceso al medio [3].

2.4.5 Redes 3G

Finalmente, la ITU (International Telecomunication Union) formó un grupo de trabajo con el fin de especificar las normas y requisitos para aquellos celulares que estuvieran orientados a brindar servicios de datos y multimedia a alta velocidad, es decir, redes 3G. A dicha iniciativa se le dio el nombre de IMT-2000 (International Movil Telecomunications 2000). Desde entonces IMT-2000 es la norma mundial para comunicaciones inalámbricas 3G y está definida por un conjunto de recomendaciones de la ITU. De esta manera, una vez que se establecieron las normas para los sistemas celulares de tercera generación, los diferentes

organismos se dedicaron a desarrollar propuestas que cumplieran con dichas especificaciones.

Existen diferentes sistemas que fueron propuestos como sistemas de Tercera Generación. Dentro de estos sistemas encontramos dos que son los de mayor importancia y que en la actualidad son considerados como estándares en Sistemas de 3G: UMTS y CDMA 2000. En Europa, la migración hacia 3G, se ha dado a través del sistema UMTS. Además, al igual que ha sucedido con GSM, UMTS es el resultado de estandarizar un único sistema en toda la Unión Europea. Por su parte, en Estados Unidos se busca la evolución de IS-95, mediante el estándar CDMA-2000 para garantizar los requerimientos impuestos por IMT-2000 para sistemas de 3G [3].

2.5 FUNDAMENTOS DE UN SISTEMA DE TELEFONÍA CELULAR

Dado que la presente tesis tiene por objetivo desarrollar un dispositivo que sea capaz de bloquear las señales emitidas o dirigidas hacia un dispositivo móvil, se hace imprescindible conocer la estructura de un sistema de telefonía celular. Motivo por el cual en las siguientes líneas se dan a conocer los componentes y elementos básicos de este sistema.

2.5.1 Componentes

En general, un sistema de telefonía móvil, está compuesto por 4 partes:

1. Estación móvil (MS)
2. Estación base (BS)
3. Estación base de control (BSC)
4. Centro de conmutación (MSC)

- Estación móvil (MS)

Es el equipo terminal (teléfono móvil) que suministran el servicio concreto al usuario en el lugar e instante deseados.

- Estación base (BS)

La estación base se encarga de mantener el enlace entre la estación móvil y la estación base de control durante la comunicación. Una estación base atiende a una o varias estaciones móviles, según el número de estas y el tipo de servicio. Por ejemplo, la reducción de la potencia en las estaciones base permite disminuir las interferencias entre las estaciones móviles asignadas a canales idénticos. Lo que redunda en una mejor calidad del servicio, comodidad de uso y autonomía de la estación móvil.

- Estación base de control (BSC)

Realiza las funciones de gestión y mantenimiento del servicio, además tiene la tarea específica de asignar estaciones base dentro de un área de cobertura a las estaciones móviles que se encuentran dentro de esta. Esto ocurre cuando un usuario se desplaza entre celdas colindantes, la función de conmutación de una comunicación entre estaciones base (handover) permite cambiar el canal ocupado por la estación móvil en la estación base anterior, por otro libre de la estación base próxima, sin interrumpir la comunicación.

- Centro de conmutación (MSC)

Es similar a la central de la red fija. Permiten la conexión entre otras redes públicas y privadas con la red de comunicaciones móviles, así como la conexión entre estaciones móviles localizadas en distintas áreas geográficas de la red

móvil. Estos centros se comportan como los centros de conmutación de cualquier tipo de red. En la figura 2.11 se muestran los componentes antes mencionados [5].

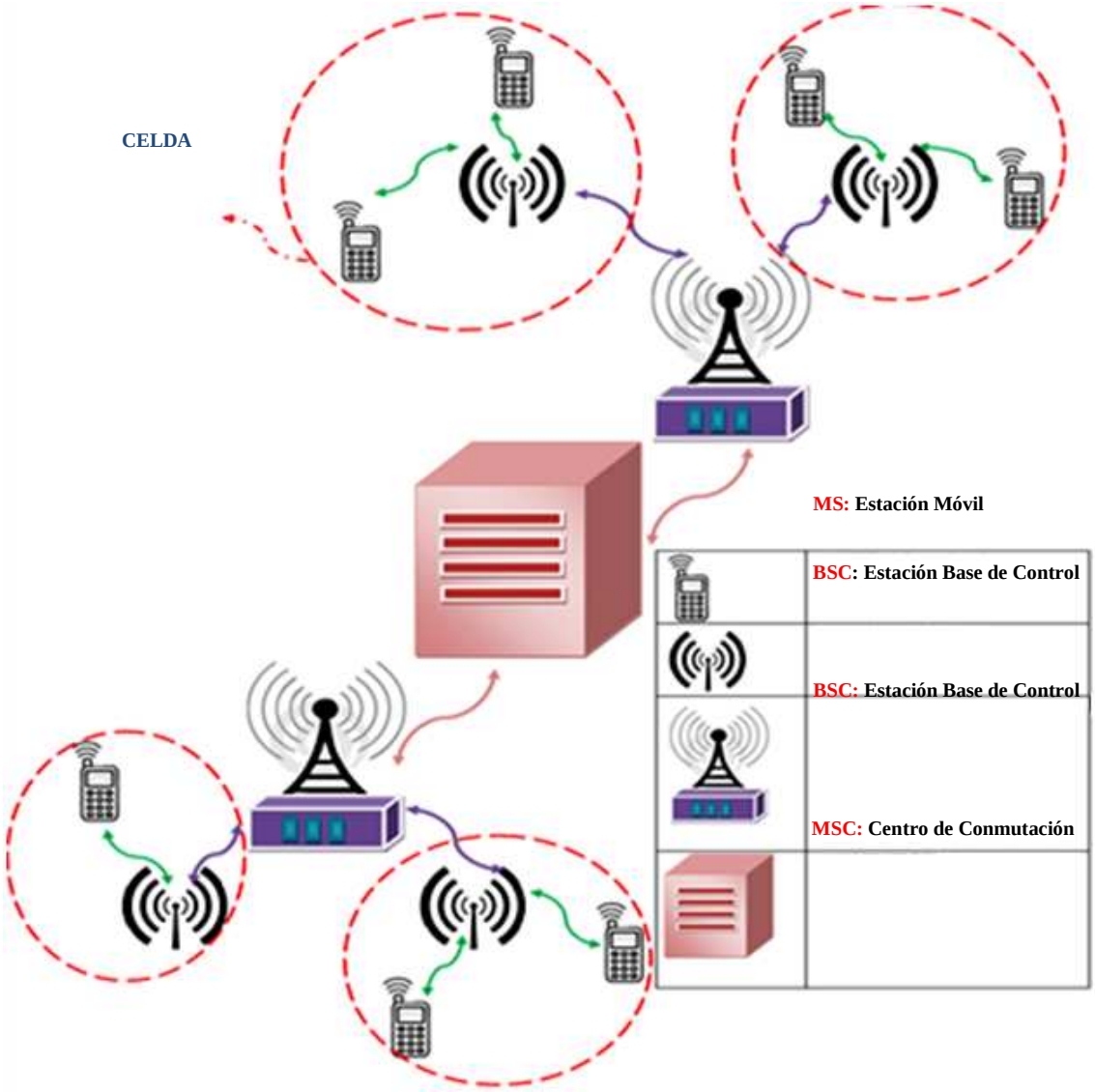

Figura 2.11 Estructura general de una red de telefonía celular.

2.5.2 Elementos

Los elementos que conforman un sistema de telefonía móvil son los siguientes:

1. Celda
2. Reúso de frecuencias
3. División de celdas
4. Transferencia de llamadas (Handover)

- Celda

Es una zona geográfica que permite la cobertura de telefonía móvil proporcionada por una estación base. Idealmente se representa por un hexágono que se une con otros para formar un patrón de cobertura total, ver figura 2.13. La forma hexagonal fue elegida porque provee la transmisión más efectiva al aproximarla con una forma circular y permite unirse a otra sin dejar huecos, lo cual no es posible para una forma circular. El tamaño de la celda depende de la potencia del transmisor, banda de frecuencia utilizada, altura y posición de la antena, el tipo de antena, la topografía del área y la sensibilidad del radio receptor.

Figura 2.12 Representación grafica de una celda.

- Reúso de frecuencias

El reúso de frecuencias es básicamente hacer uso de las mismas frecuencias portadoras para cubrir distintas áreas de cobertura móvil las cuales están

separadas a una distancia tal que evita un interferencia entre canales vecinos. Esto permite reducir la potencia de transmisión así como la altura de elevación de las antenas. La formula (2.9) permite conocer la distancia de separación que debe haber entre las células para permitir el reúso de frecuencias.

$$D = \left[\sqrt{(3)(N)}\right](R) \qquad (2.9)$$

En donde D es la distancia de reúso, N el número de frecuencias por grupo y R es el radio promedio de la celda [6].

- División de celdas

Se utiliza cuando una celda alcanza la capacidad máxima de tráfico, es decir, la demanda de canales alcanza un número límite de canales disponibles en dicha celda. Consiste en formar varias celdas de lo que antes era una sola. Para realizar esta división se consideran los radios mínimos que pueden manejar los diferentes tamaños de las celdas, los cuales se usan para evitar problemas de sobrecarga del sistema, debido a que las transferencias de llamada son más frecuentes. La tabla 2.3 muestra los tamaños de las divisiones de las celdas [6].

Tipo de celda	Radio mínimo	Radio máximo
Picocelda	20 m	400 m
Microcelda	400 m	2 Km
Macrocelda	2 Km	20 Km

Tabla 2.3 Tipos de celdas y áreas de cobertura.

- Transferencia de llamadas (Handover)

El handover es el proceso por el cual se realiza el cambio de estaciones base con el fin de proporcionar mejores recursos de comunicación a una estación móvil. El

Handover está en función del nivel de potencia de la señal y del BER (Bit Error Rate), el cual es una medida que se utiliza para saber la calidad de la llamada. En la tabla 2.4 se muestran los niveles de BER y la clase a la que pertenecen. La categoría del BER definirá la calidad de la voz siendo esta buena cuando: es menor a 1, marginal de 1 a 3 y mala cuando es mayor a 3.

Categoría	BER (%)
0	BER < 0.01
1	0.01<BER <0.1
2	0.1<BER<0.5
3	0.5<BER<1.0
4	1.0<BER<2.0
5	2.0<BER<4.0
6	4.0<BER<8.0
7	BER>8.0

Tabla 2.4 Márgenes de interferencia.

El proceso de handover se lleva a cabo cuando el móvil mide los niveles de recepción de las estaciones base cercanas, después envía esas mediciones a su estación base. La estación base recibe las mediciones de las estaciones base vecinas y envía todos los datos a la estación de control. Se selecciona el canal de voz. Se verifica la presencia del móvil y se ordena el cambio de estación base. Esto ocurre cuando la estación móvil se encuentra en los límites de cobertura y se encuentra entre dos sectores de las células adyacentes [6].

Hard Handover

Este tipo de Handover se le conoce también como transferencia de llamada con interrupción, el cual ocurre cuando las estaciones base que se encuentran en el proceso de transferencia de llamada, manejan diferentes frecuencias portadoras lo que provoca que la señal recibida se interrumpida por un tiempo demasiado corto.

Handover Intersistemas

Cuando se habla de Handover entre sistemas se habla de una transferencia de llamada entre dos sistemas que operan con estándares diferentes, como ejemplo tenemos una transferencia de llamada que ocurre de un sistema de UMTS a GSM los cuales trabajan con diferentes accesos al medio como lo son WCDMA y TDMA respectivamente. Estas transferencias de llamada pueden ser usadas para extender la cobertura o equilibrar la carga de usuarios. Principalmente las transferencias de llamada entre UMTS y GSM son necesarias para proporcionar una cobertura continua, así como también, pueden ser usadas para disminuir la carga en las celdas GSM o UMTS.

Soft Handover

Este tipo de Handover realiza una transferencia de llamada sin interrupción, el cual es el más usado en WCDMA, esto se presenta cuando la estación móvil puede recibir la señales de dos estaciones base o más, realizando esto de forma simultánea, esto será posible solo cuando las estaciones base involucradas trabajan en la misma frecuencia portadora [3].

2.6 UMTS COMO RED DE 3G

UMTS utiliza W-CDMA como técnica de acceso múltiple, establece un estándar mundial para roaming y brinda al usuario velocidades de hasta 2 Mbps, todo esto se plantea usando una dirección IP (Internet Protocol) para cada móvil utilizado y mediante este el acceso a los diferentes servicios.

2.6.1 Arquitectura de UMTS

El sistema UMTS presenta una arquitectura en la cual se destacan principalmente 3 elementos:

- Equipo de Usuario (UE: User Equipment)

- Red de Acceso de Radio (UTRAN: UMTS Terrestrial Radio Access Network)
- Red Central (CN: Central Network)

Estos 3 elementos a su vez, necesitan de alguna interfaz para poderse conectar entre sí. De esta manera, entre el Equipo de Usuario (UE) y la Red de Acceso de Radio (UTRAN), existe una interfaz denominada interfaz Uu, y entre la UTRAN y la Red Central (CN) existe una interfaz denominada interfaz Iu. En base a esto, se tiene una arquitectura general UMTS como se observa en la figura 2.13.

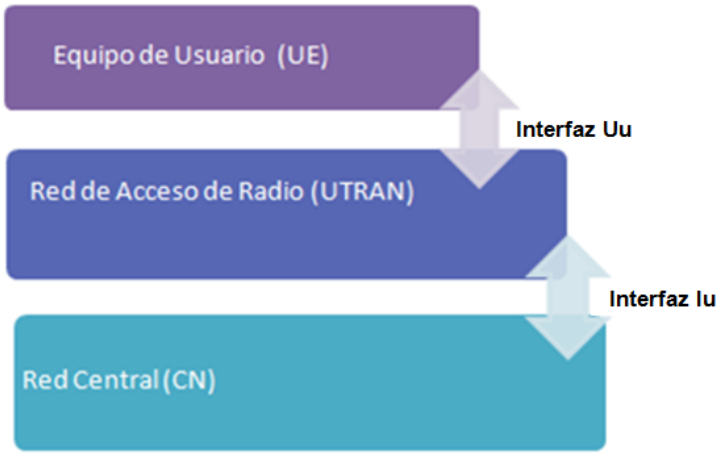

Figura 2.13 Arquitectura de UMTS.

A continuación se explicada con detalle los elementos e interfaces de la arquitectura UMTS.

- Equipo de Usuario (UE)

El Equipo de Usuario es el teléfono móvil que el usuario trae consigo para lograr la comunicación con una estación base en el momento que lo desee y en el lugar donde exista cobertura. Este puede variar en su tamaño y forma, sin embargo debe estar preparado para soportar el estándar y los protocolos para los que fue diseñado.

Por ejemplo, si un móvil trabaja bajo el sistema UMTS, debe ser capaz de acceder a la red UTRAN mediante la interfaz Uu, para lograr la comunicación con otro móvil. O bien, deberá comunicarse con la red pública conmutada (PSTN), la red digital de servicios integrados (ISDN), o un sistema diferente como GSM de 2.5G, tanto para voz como para datos.

- Interfaz Uu (Interfaz de Radio)

La interfaz Uu se encuentra entre el equipo de usuario y la red UTRAN. Esta interfaz no es otra cosa más que la tecnología WCDMA. Dicho en otras palabras, la conexión entre el equipo de usuario y la red de acceso de radio UTRAN es mediante la tecnología WCDMA.

- Interfaz Iu

Es una interfaz abierta que conecta la red principal con la UTRAN. Puede tener dos casos diferentes, Iu-CS *(Circuit Switching)* y Iu-PS *(Packet Switching)*. La Iu-CS conecta la UTRAN a un centro de conmutación móvil, un MSC. La interfaz Iu-PS conecta la UTRAN al SGSN.

- Interfaz Iub

Se sitúa entre el RNC y la estación base en la UTRAN. La interfaz Iub separa la estación base del RNC. Algunas funciones que realiza son: dirigir los recursos de transporte, maneja la información del sistema, manejo del tráfico de los canales comunes, compartidos y especiales.

- Interfaz Iur

Interfaz Iur. Es una interfaz abierta que conecta a dos radio controladores de red, lleva tanto la información de tráfico como de señalización.

- Red de Acceso de Radio (UTRAN)

UTRAN es el nombre de la nueva red de acceso de radio diseñada para el sistema UMTS. Tiene 2 interfaces que la conectan con la red central y en el equipo de usuario: la interfaz lu y la interfaz Uu, respectivamente.

La red UTRAN consiste de varios elementos, entre los que se encuentran los RNC (Radio Network Controller) y los Nodo B (en UTRAN las estación base tienen el nombre de Nodo B). Ambos elementos juntos forman el RNS (Radio Network Subsystem).

- Red Central (CN)

La Red Central, se encuentra formada principalmente por 2 elementos: MSC (pieza central basada en conmutación de circuitos) y el SGSN (pieza central basada en conmutación de paquetes):

o MSC (Mobile Switching Center): como ya se mencionó, el MSC es la pieza central de la red basada en la conmutación de circuitos. El mismo MSC es usado tanto por el sistema GSM como por UMTS. Es decir, GSM y UMTS se pueden conectar con el mismo MSC.

o SGSN (Serving GPRS Support Node): el SGSN es la pieza central basada en la conmutación de paquetes. El SGSN se conecta con UTRAN mediante una interfaz denominada lu-PS y con GSM mediante la interfaz lub.

En base a lo descrito anteriormente, en la figura 2.15 se presenta un esquema general de la arquitectura del sistema UMTS [7,8].

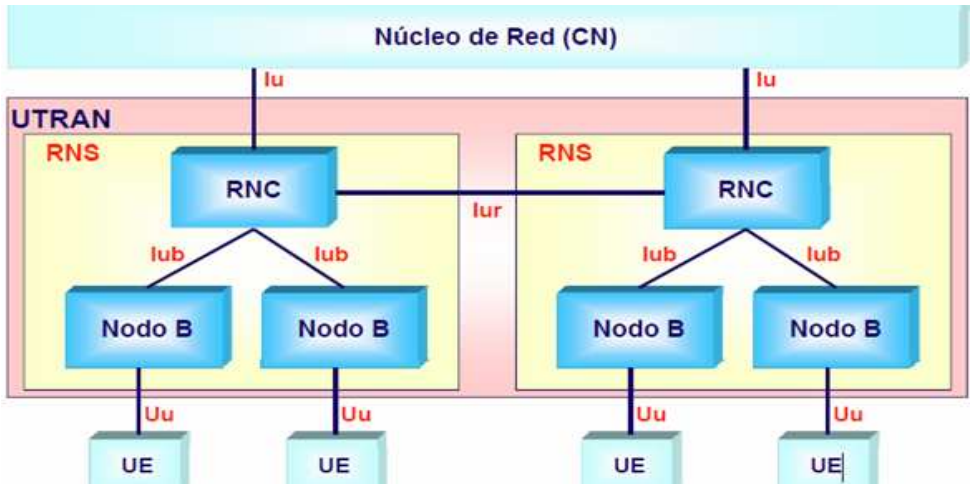

Figura 2.14 Arquitectura completa de UMTS.

2.6.2 WCDMA: Interfaz de UMTS

WCDMA es el acrónimo de Wideband Code Division Multiple Access, es una tecnología de acceso al medio, por el cual las estaciones móviles acceden a las estaciones bases correspondientes, con el objeto de realizar una comunicación, transferencia y recepción de datos. WCDMA se utiliza en redes 3G para llegar a un ancho de banda de 5 MHz para proveer mayores velocidades de transferencia, así como también, grandes volúmenes de usuarios, a diferencia de otras técnicas de acceso utilizadas en 2G que contaban con un ancho de banda de 1.25 MHz. Debido a que WCDMA es un método de acceso por división de código, puede transmitir en cualquier frecuencia sin necesidad de dividirlas. Por lo tanto existe una reutilización total de frecuencias. Comparado con otros sistemas que no se basan en CDMA como lo es FDMA. La figura 2.15 es un ejemplo de esto [3].

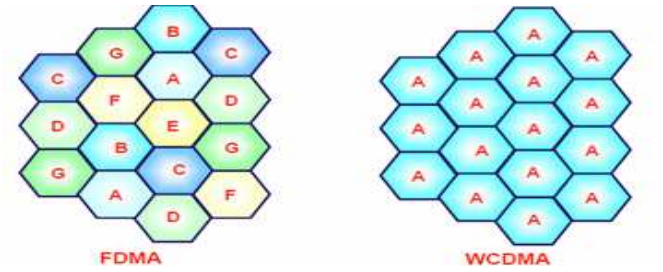

Figura 2.15 Reutilización total de frecuencias en WCDMA.

CAPÍTULO 3
FUNDAMENTOS DE BLOQUEO

Esencialmente, la Segunda Guerra Mundial trajo consigo un gran avance en el desarrollo tecnológico y marcó la pauta principalmente en el uso de la electrónica. Una de estas aplicaciones se dio el 26 de Febrero de 1935, con los ingleses Arnold Wilkins, Percival Rowe y el escocés Robert Watson-Watt; los cuales realizarían la primera prueba de lo que hoy en día conocemos como radar.

Para el año de 1942, en medio de la segunda Guerra Mundial, los alemanes implementaron un sistema receptor de radio dentro de sus submarinos, con el cual pudieron darse cuenta de cuándo eran detectados por los radares ingleses; posteriormente, este sofisticado equipo electrónico fue integrado en los aviones de combate, también se le utilizó para navegación en los bombarderos y detección de submarinos, así como otra gran cantidad de aplicaciones. Esto marcaría el inicio de la llamada *Guerra Electrónica* [9].

3.1 GUERRA ELECTRÓNICA

Durante más de un siglo, el espectro electromagnético se ha utilizado para diversas aplicaciones tanto comerciales como militares.

Hoy en día nuevas tecnologías se están expandiendo más allá del espectro de frecuencias de radio tradicional en las cuales se incluyen los microondas de alta potencia y armas de energía dirigida. Estas nuevas tecnologías son parte de una nueva guerra conocida como Guerra Electrónica (EW: Electronic Warfare).

La guerra electrónica se define como *toda aquella actividad que implica el uso de la energía electromagnética para obtener el control del espectro electromagnético,* con el objetivo de un posterior ataque o protección tanto de información como de equipos.

Existe la amenaza de que un sistema enemigo use el espectro electromagnético a su favor provocando la destrucción parcial o total de nuestra información. La amenaza se ve agravada por el crecimiento de un mundo inalámbrico y el uso cada vez más sofisticado de las tecnologías comerciales disponibles en el mercado. En general las operaciones que desarrolla la EW cuentan con un amplio número de objetivos dentro del espectro electromagnético como se muestra en la figura 3.1

Figura 3.1 Puntos de ataque dentro del espectro electromagnético.

La guerra electrónica se compone de tres divisiones: ataque electrónico (EA: Electronic Attack), protección electrónica (EP: Electronic Proteccion) y soporte electrónico (ES: Electronic Support), las cuales se muestran en la figura 3.2. La

aplicación efectiva de la guerra electrónica tiene como objetivo negar toda capacidad que tenga el adversario sobre toda información, equipo o personal.

Figura 3.2 Componentes de la Guerra Electrónica.

3.2 Principios de la EW

La EW utiliza los principios de explotación, mejora y control para lograr una mayor eficiencia. Los tres principios son empleados por los tres componentes de la EW. La aplicación adecuada de estos componentes produce los efectos de la detección, la negación, la interrupción, el engaño y la destrucción en mayor o menor grado.

- Explotación

La explotación es el principio en el cual se aprovecha al máximo el uso del espectro electromagnético en un beneficio propio. En el cual se puede utilizar la detección, negación, interrupción, engaño y la destrucción en mayor o menor grado. Por ejemplo, al usar un engaño electromagnético (señal de transmisión falsa) para transmitir una información diferente a la verdadera o para el uso de las emisiones electromagnéticas para localizar e identificar al enemigo.

- Mejora

La mejora es el perfeccionamiento de los sistemas para incrementar el uso de la ES como un multiplicador de fuerzas y tiene como fin el detectar, negar, interrumpir, engañar o destruir total o parcialmente la información o sistemas electrónicos a través de un adecuado control y explotación del espectro electromagnético. [10]

- Control

El principio de control es el de dominar el espectro electromagnético, directa o indirectamente, tanto para ataque como protección.

3.3 PROTECCIÓN ELECTRÓNICA

La protección electrónica es una división de la guerra electrónica dentro de la cual se implican las acciones y medidas adoptadas para proteger al personal, instalaciones y equipos de cualquier efecto y uso amigo o enemigo del espectro electromagnético debido al EA o al ES que puedan degradar, neutralizar o destruir la capacidad de combate.

Dentro de la protección electrónica se agrupan diversas técnicas que salvaguardan y evitan la intercepción de la información que se desea transmitir. El control de emisiones o EMCON (EMISSION CONTROL) es quizás una de las formas más simples en la cual, el uso del espacio para las transmisiones es limitado o impedido por un cierto período de tiempo, generalmente en los puntos críticos. El EMCON impide que un adversario pueda interceptar e identificar la frecuencia de funcionamiento de un punto de red de comunicaciones. El manejo adecuado de frecuencia es la clave elemento en la prevención de efectos adversos.

Otra forma de proporcionar dicha protección es mediante el uso de sistemas que utilicen el espectro disperso ya sea por saltos de frecuencia o por secuencia directa las cuales reducen la probabilidad de intercepción de la transmisión. Este tipo de protección incluye medidas tales como la codificación y la modulación.

El cifrado de redes de comunicación, es otra forma de protección electrónica en el cual se evita que un adversario recolecte información una vez que se ha interceptado la transmisión de información. La disponibilidad inmediata de los algoritmos de cifrado es la clave para lograr que esta técnica sea práctica y efectiva. [10, 11]

3.4 SOPORTE ELECTRÓNICO

El soporte electrónico es una componente de la EW que tiene por medidas y acciones el buscar, interceptar, identificar y ubicar las fuentes intencionales y no intencionales de energía electromagnética radiada con el propósito de reconocimiento, orientación, planificación y conducción para un apoyo al Ataque Electrónico.

La parte fundamental del soporte electrónico es obtener la mayor cantidad de información sobre un adversario mediante la intercepción de las transmisiones. Esta energía radiada puede ser emitida por cualquier tipo de transmisor, tales como los transmisores de las redes de comunicación, de los radares o de transmisores de telemetría.

Parte de la información importante se puede extraer de sólo tomar la medición de algunos parámetros de la transmisión tales como su frecuencia de operación, el tipo de modulación, la velocidad de los bits y la ubicación geográfica del transmisor [10, 11].

3.5 ATAQUE ELECTRÓNICO

Ataque electrónico es una división de guerra electrónica que implique el uso de energía electromagnética radiada o dirigida para atacar personal o equipos con la intención de degradar, neutralizar o destruir la capacidad de comunicación y combate. Para llevar a cabo esto, muchas de las veces el ataque electrónico suele auxiliarse del Soporte Electrónico, dependiendo de la finalidad del ataque.

Los tipos más comunes de ataque electrónico son los de interferencia y engaño de los cuales el Jamming por obstrucción y barrido electromagnético es un tipo de EA por interferencia. Mientras que el EA por engaño electromagnético incluye incluyen técnicas como la generación de falsos destinos o duplicado de información.

3.6 PROBABILIDAD DE DETECCION E INTERCEPCION

Estos términos se aplican a las diversas formas de procesamiento electromagnético de señales con el fin de hacer lo más difícil posible el conocimiento de que una señal se encuentre presente o no sobre el rango de frecuencias a operar, así como también, si se da el caso de que sea detectada, la información contenida en ella será difícil de extraer.

La baja probabilidad de detección (LPD: Low Probability of Detection) pretende que las señales presentes sean ocultadas al 100%. Una forma de lograrlo es colocar la señal por debajo del nivel del ruido, de tal manera que la señal no pueda ser diferenciada del ruido que siempre existe en el espectro. Esta técnica se llama Espectro Disperso por Secuencia Directa. Otra forma de ocultar la señal es hacer que la portadora realice una serie de saltos con el fin de que aquellos receptores fijos a una frecuencia no puedan ver esta señal. Esta técnica se conoce como Espectro Disperso por Saltos de Frecuencia, ambas técnicas trabajan por medio de códigos los cuales determinan los saltos de frecuencia o el esparcimiento de la señal además de que solo son conocidos por un único transmisor y receptor.

Si la naturaleza del sistema de comunicación es tal que es difícil establecer LPD por su complejidad, entonces puede ser más deseable ceder el paso a la posibilidad de que la señal pueda ser detectada, pero que una vez que esto suceda, sea difícil extraer la información contenida en ella. La baja probabilidad de intercepción (LPI: Low Probability of Interception) es el término utilizado en este caso.

Una transmisión de señales de banda ancha como estas (DSSS y FHSS) requiere un equipo de recepción que también sea de banda ancha. Por desgracia, es una ley de la física que cuanto mayor sea el ancho de banda de los equipos receptores habrá mucho más ruido de fondo entrando por el receptor, junto con cualquier señal deseada. Este es un factor que pude ser utilizado a favor para que se pueda lograr un bloqueo de la señal de manera eficaz [11].

3.7 JAMMER

Independientemente, de si el Ataque Electrónico se apoya o no en algún método de Soporte Electrónico, se necesita de un dispositivo para llevar a cabo dicho ataque. Este dispositivo recibe el nombre de Jammer, cuya tarea principal consiste en negar la comunicación sobre los enlaces de RF de un adversario.

Para llevar a cabo esta actividad, el jammer recurre a la radiación de energía de una señal “no deseada” hacia los receptores de comunicación del adversario. De esta manera, si el nivel de la señal no deseada es lo suficientemente fuerte, causará que los receptores de comunicación no puedan demodular la señal proveniente del transmisor original. Para llevar a cabo lo anterior, se debe considerar el hecho de que la señal del jammer no es una réplica de la señal que fue transmitida originalmente, ya que esto sólo reforzaría la señal original en lugar de interferirla en forma negativa.

Por otra parte, para realizar lo descrito anteriormente se puede proceder fundamentalmente en 2 formas:

- La primera y más sencilla de llevar a cabo es negarle al adversario la capacidad de comunicarse entre sí. Es decir, obstruyendo al receptor, interfiriéndolo en este caso con niveles de señales no deseadas.

- La segunda forma es empleando un Sistema de Señal Inteligente o SIGINT (Signal Intelligent), conocido también como Sistema de Detección de Comunicación. En este caso primero se estudia al adversario, mediante la medición de ciertos parámetros, los cuales forman parte del Apoyo Electrónico (ES). De esta forma se determina la manera de proceder con el Ataque en cuanto a tiempo y forma de ataque; y una vez realizado lo anterior se procede con la radiación de señales no deseadas hacia el receptor de comunicación. Obteniéndose de esta manera un control del sistema del jammer [11].

Independientemente de la forma en que se desea negar la comunicación ya sea mediante el empleo de señales inteligentes o no, finalmente se radiará energía electromagnética hacia los receptores de comunicación a modo de interferirlos y esto se realiza mediante diferentes técnicas.

A estas técnicas empleadas se les conoce como Técnicas de Jamming. Siendo fundamentalmente:

- Jamming por Ruido (Banda Angosta y Banda Parcial).
- Jamming por Barrido.
- Jamming por Seguimiento.

Ahora, hay que tener en cuenta que se requiere un porcentaje de interrupción de aproximadamente 30% para iniciar una degradación significante en las comunicaciones de voz, haciendo un mensaje casi incomprensible. Sin embargo para una eficaz inteligibilidad del mensaje se requiere de un 70% de interrupción. Además de esto, la eficiencia del bloqueo estará determinada por otros factores que hay que tomar en cuenta como lo son:

- Potencia Efectiva Radiada por el Jammer.
- Potencia Efectiva Radiada por el Transmisor hacia el Receptor.
- Orientación de la Antena Receptora relacionada con la Orientación de la antena del Jammer.
- El terreno.

3.7.1 Jamming por ruido (banda angosta y banda parcial)

Cuando el objetivo es atacar una frecuencia especifica, un jammer por ruido de banda angosta puede ser utilizado. Este tipo de jammer transmite una potente señal de ruido a la frecuencia específica que está usando el adversario.

Este tipo de jammer puede ser útil contra sistemas de comunicación basados en DSSS (Espectro Disperso por Secuencia Directa). Ya que tal como lo especifica el estándar IS-95 de telefonía celular, las sistemas que emplean esta técnica son particularmente sensibles a señales fuertes cerca del receptor. Sin embargo para que esta técnica sea realmente efectiva, se debe tener conocimientos sobre el punto específico que se desea atacar con la señal de ruido.

Por otra parte, puede que no se requiera interferir todo el ancho de una banda de frecuencias, pero tampoco es suficiente interferir un solo canal o frecuencia especifica; sino que tal vez lo que se desea interferir son algunos canales dentro de dicha banda, y no solo uno. Entonces tendríamos que implementar un jammer por ruido de banda parcial.

Este tipo de jammer de banda parcial puede radiar ruido a los diferentes canales al mismo tiempo, utilizando el mismo transmisor y antena. Pero para ello necesita contar con un generador diferente para cada canal a interferir, de tal manera que al mismo tiempo se esté enviando ruido de interferencia a cada canal.

No obstante para este mismo tipo de jammer de banda parcial, existe también la posibilidad de emplear la técnica llamada “de tiempo compartido”, donde no es necesario contar con un generador para cada canal a interferir, sino que a su vez el mismo generador radia ruido a los diferentes canales solo que no al mismo instante, ya que necesita compartir el tiempo con cada canal. Esto es posible ya que como se mencionó anteriormente, no es necesario interferir el 100% de la comunicación, ya que si al menos el 30% de la información es interferida, será suficiente para la inteligibilidad de la información. La figura 3.3 muestra la diferencia de cada bloqueo antes mencionado.

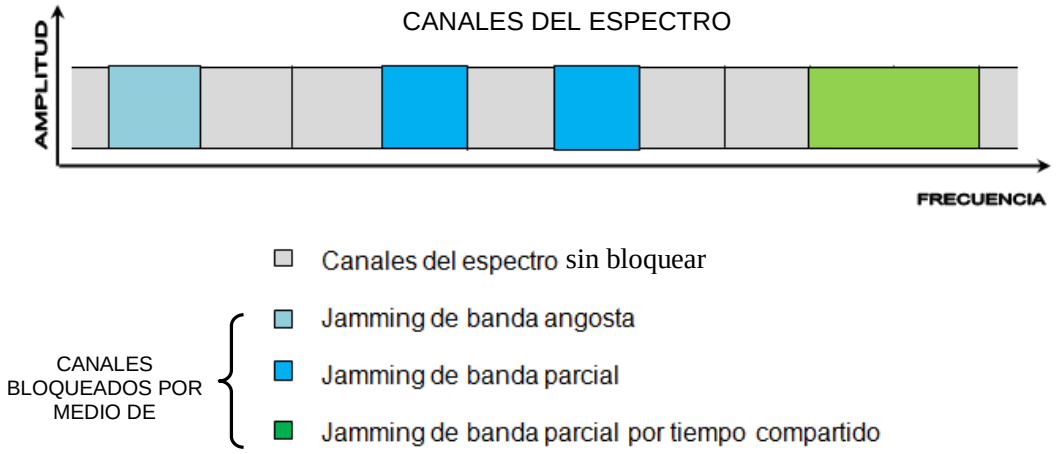

Figura 3.3 Bloqueo de canales del espectro usando Jamming por ruido

Usualmente a esta técnica de tiempo compartido usada por los jammers de banda parcial, también se le conoce como técnica de “Jamming por Pulsos”. Pero como se ve, es llamada por pulsos debido a que, para una frecuencia dada esta presente únicamente en un tiempo determinado, como si fueran pulsos.

Finalmente, cabe mencionar que tanto la Técnica de Jamming por Ruido de Banda Angosta, como la de Banda Parcial, en general, las podemos encontrar como Jamming por Tono Único y Jamming por Tono Múltiple, respectivamente. En Realidad, se podría decir que la única variante es que en estas últimas, no se envía ruido como tal, sino tonos. Pero teóricamente el principio de funcionamiento es el mismo al igual que su eficiencia. Motivo por el cual no se le dará un análisis por separado. [11]

3.7.2 Jamming por barrido

Este tipo de jammer es conveniente tenerlo más cerca del adversario que de los sistemas de comunicaciones amigas, ya que este no se enfoca en unos cuantos canales específicos dentro de la banda completa de frecuencia. Sino que interfiere con todos los canales presentes dentro de una banda de frecuencias. Y puede esencialmente denegar completamente la comunicación dentro de un radio considerable alrededor del jammer. Que aunque su alcance no es lo suficientemente elevado como el que se presenta en los jammers de Banda Angosta o Parcial, si es lo suficiente para negar la comunicación a sus alrededores en una banda ancha de comunicaciones.

Una de las maneras de implementar un jammer como este es generar una señal relativamente estrecha, compuesta por ruido. Seguido, esta señal será trasladada desde una porción del espectro hacia la siguiente, manteniéndose en cada porción durante un periodo de tiempo específico, por ejemplo, 1 ms.

Esta técnica se puede emplear por ejemplo en un sistema basado en FHSS (Espectro Disperso por Saltos de Frecuencia), donde la comunicación se lleva a cabo empleando saltos en frecuencia. Donde a pesar de que dichas frecuencias empleadas están dentro de una banda, no se sabe exactamente a qué frecuencia se transmitirá en el siguiente intervalo de tiempo. Es por ello que un barrido en toda la banda sea útil. Sin embargo, se debe considera un barrido lo

suficientemente rápido como para alcanzar la frecuencia a la cual se está transmitiendo en un momento dado antes de que vuelva a cambiar, pero a su vez también debe ser lo suficientemente lento como para que, cuando este situado sobre la frecuencia actual de transmisión no sea muy corto el tiempo que interfiera con esta, en comparación con el tiempo que dura el enlace a dicha frecuencia.

Como nos habremos dado cuenta el jamming por barrido funciona como si se tratase de una técnica de jamming por Ruido, pero de "Banda Ancha". Y en efecto, existe una técnica que es conocida como *"Jamming por Ruido de Banda Ancha".* Ya que, solo por aclarar, cuando se realiza la técnica de barrido, lo que realmente se está haciendo es introducir ruido en toda la banda de frecuencias, lo cual es en sí, el objetivo de la técnica de de Ruido de banda ancha [11].

3.7.3 Jamming por seguimiento

Para objetivos que emplean señales LPI en particular para aquellos que usan saltos de frecuencia se pueden usar estrategias de Jamming por bombardeo o por banda estrecha sin embargo para que el jammer pueda realizar el bloqueo efectivo el equipo debe ser capaz de seguir el transmisor a medida que cambia la frecuencia. En sí, es una cuestión de identificar la frecuencia a la que el transmisor se trasladado y por último se realizar una verificación de que la nueva señal pertenece a la misma emisora. A dicha técnica de bloqueo se le denomina Jamming por seguimiento. Esta técnica solo bloquea la frecuencia usada por cada salto por lo cual se reducen las interferencias entre canales vecinos.

La frecuencia del transmisor, así como la frecuencia de sintonía del receptor, se cambian rápidamente de manera que el Jammer que opera en una frecuencia fija, tiene un efecto mínimo en toda la transmisión. La complejidad de estos sistemas es bastante alta.

Los saltos de frecuencia son realizados por un proceso pseudoaleatorio por lo que no hay manera de predecir la frecuencia siguiente. Sin embargo, si somos capaces de medir la frecuencia en una pequeña porción del salto, podemos establecer un bloqueo a la nueva frecuencia a la que se ha saltado. Habrá muchas señales presentes, lo más probable es que incluya la señal a bloquear y señales no deseadas. La única manera de identificar una señal en específico es por medio de su ubicación. Así, dos localizadores digitales emisor-receptor deben trabajar juntos para triangular la señal sobre el medio. A continuación tendrá lugar un archivo de computadora con la frecuencia y la ubicación de cada señal de la zona. La emisión del seguidor se ajusta a la frecuencia de la señal de la ubicación del emisor de destino [11, 12].

Los objetivos de ataque para un sistema por saltos de frecuencia dependen de la distancia que haya entre: transmisor / receptor, Jammer / receptor, y Jammer / transmisor. Si el Jammer está demasiado lejos del transmisor en relación con la distancia entre el transmisor y el receptor, la señal llegará Jammer después de que ya ha sido recibido por el receptor. Para lo que el sistema realizara un siguiente salto haciendo de esto un Jamming ineficaz.

El mismo problema se produce si la distancia entre el bloqueador y el receptor en relación con la distancia entre el transmisor y el receptor es demasiado grande. A pesar de que el jammer recibe la señal en el tiempo para comprobar que es el objetivo correcto, la señal emitida por el Jammer debe viajar demasiado lejos para llegar al receptor a tiempo para impedir la comunicación por lo que la aplicación del Jammer será ineficaz, Factor que hay que tomar en cuanta cuando se implementen Jammer de este tipo [11].

CAPÍTULO 4
CIRCUITO DE BLOQUEO: DISEÑO Y SIMULACIONES

4.1 REQUERIMIENTOS DEL JAMMER

Para el diseño del circuito se eligió la técnica de “Jamming por barrido” ya que se desea cancelar a toda operadora que trabaje en el espectro de frecuencias deseado; por lo que las técnicas de Jamming de banda angosta, parcial y tiempo compartido fueron descartadas por su particularidad de cancelar solo ciertos canales del espectro los cuales son fijos.

A su vez, la técnica de Jamming por seguimiento también fue descartada ya que esto involucra una gran complejidad de transporte y diseño en la etapa de rastreo y triangulación de la señal.

Dentro de la elaboración física del circuito se tomaron en cuenta factores como la potencia, la frecuencia y el tipo de la antena.

- Potencia

Se debe de utilizar toda la potencia disponible, suministrada por el circuito, en cada canal del espectro y en distintos intervalos de tiempo y a su vez, teniendo en cuenta esto, no se utilizará demasiada potencia por dos puntos sumamente importantes: el primero de ellos es el problema de la legalidad, ya que está severamente penada por la ley; el segundo punto involucra el implemento de numerosas etapas de ganancia a la salida del circuito, factor que es desfavorable para el diseño [A].

- Frecuencia

Este factor involucra el espectro en el que se desea realizar el bloqueo, en este caso es en la banda de los 1900 MHz, ya que es en esta parte del espectro donde se realiza la comunicación por voz, transferencia de datos y mensajes para 2G y 2.5G. Asi como también se opto por atacar este rango de frecuencia dado que la mayoría de los usuarios de telefonía en México se comunica por medio de GSM, ahora no por esto se deja de lado a 3G ya que como se mencionó en uno de los objetivos de la tesis, se tiene como punto el observar el comportamiento de un sistema de 3G dentro de un rango de bloqueo de 2G [13].

- Tipo de antena

Se optó por utilizar una antena omnidireccional ya que este tipo de antena tiene un excelente patrón de radiación ideal para realizar el bloqueo, patrón con una forma parecida al de una esfera.

La constitución del circuito de bloqueo está dada por los bloques del diagrama de la figura 4.1, los cuales muestran la alimentación, la sección de oscilación y la sección de RF.

Figura 4.1 Diagrama a bloques del Jammer.

En el siguiente apartado se describe con detalle cada uno de los bloques que conforman al jammer.

4.2 DISEÑO DEL JAMMER

4.2.1 Sección de Alimentación

La alimentación de este circuito fue diseñado para usuarios fijos, por lo que se toma la energía eléctrica del contacto de la pared. Dado que la sección de oscilación y la sección de RF necesitan 8 V y 24 V respectivamente, se pasarán de los 127 Vac iniciales a los voltajes necesarios en DC para la alimentación del circuito. Las partes que componen la fuente son: el transformador, el rectificador, el filtro y los reguladores (ver figura 4.2).

Figura 4.2 Diagrama a bloques de la fuente de alimentación.

Al inicio se tendrán 127 Vac del contacto de la pared los cuales deben ser reducidos para la alimentación de los circuitos. Los voltajes de los transformadores se dan en términos de valores rms, por lo que para elegir el transformador adecuado se uso la formula (4.1), en donde E_m es el máximo voltaje instantáneo y E_{rms} es el voltaje en valores rms [20].

$$E_m = (1.4)(E_{rms}) \qquad (4.1)$$

Debido a que la seccion RF necesita un voltaje de alimentacion de 24 V, se necesita que a la salida del rectificador se tenga un voltaje cercano a ese. Por lo que dentro de los valores comerciales de los transformadores, se encontro uno de 18 Vrms, al usar la ecuasion (4.1) se obtuvo un E_m deseado de 25.2 V ac.

$$E_m = (1.4)(\,18\,Vrms) = 25.2\,V\;ac$$

Después de obtener este voltaje a la salida del transformador, a la siguiente etapa, un rectificador de onda completa que pasa los 25.2 V ac a 25.2 V dc.

Al final del rectificador se conecta un capacitor de filtrado para hacer que el voltaje resultante sea los más lineal posible, para esto se coloca un capacitor de 500 μF o más [20].

La parte final de la fuente estará dada por los reguladores LM7824 y LM7808, el primero para alimentar la sección RF que entregara un voltaje regulado de 24 V y el segundo para la sección IF que entregara un voltaje regulado de 8 V.

4.2.2 Sección de Oscilación

Recordemos que un VCO, es un Oscilador Controlado por Voltaje. Es decir, dependiendo del voltaje a su entrada, será la frecuencia de oscilación a su salida. Por tanto, el VCO, necesitará continuamente de un voltaje en la entrada para generar una frecuencia de oscilación en la salida. Sin embargo, si el voltaje de entrada es fijo, en la salida del VCO siempre se verá reflejada una única frecuencia de oscilación.

Entonces, para que el VCO entregue oscilaciones en toda la banda de frecuencia requeridá, se necesitará de un voltaje que varíe automáticamente a cierta velocidad. Por tal motivo se requiere de una previa sección de oscilación.

Esta sección estará determinada por una onda triangular. Debido a que, en este tipo de señales las variaciones de voltaje son más lineales entre sus voltajes picos. Es decir, no hay cambios abruptos de voltaje (ver figura 4.3). De esta manera el barrido que realizará el VCO será más uniforme.

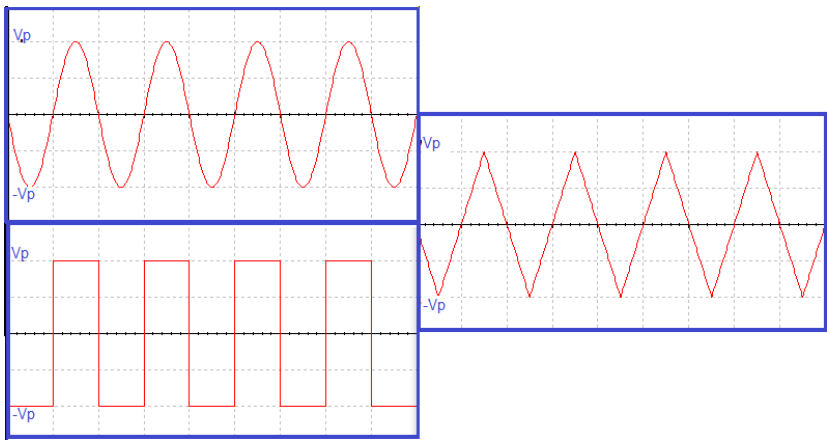

Figura 4.3 Comparación en linealidad de señales.

Por otra parte, de acuerdo a las especificaciones del VCO, el voltaje requerido para barrer la banda deseada, viene dado solo en cierto rango de su voltaje de entrada. Por tanto, será necesario mover el nivel de referencia de la señal triangular para que se ajuste únicamente a los niveles de voltaje requerido. Esto quiere decir que se deberá mover el nivel de DC de ésta señal, como se muestra en la figura 4.4.

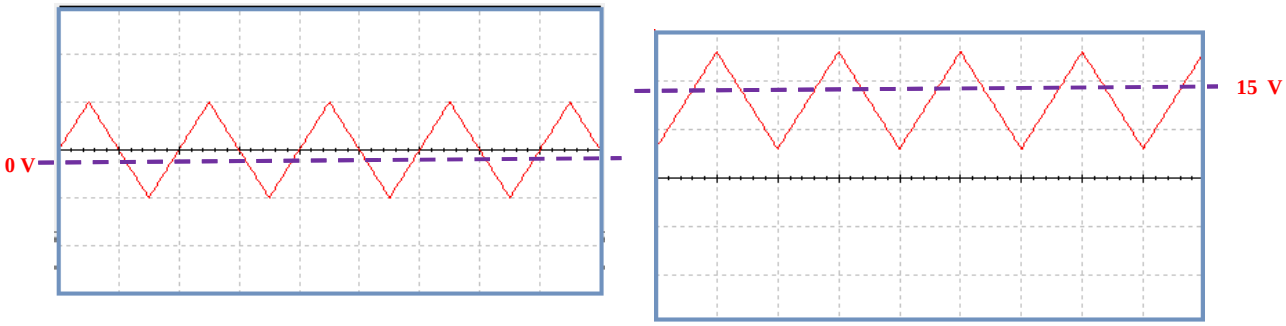

Figura 4.4 Señales con diferentes niveles de referencia en DC.

- OSCILADOR

El oscilador tendrá la función de generar una onda a cierta amplitud y frecuencia tal que, al llegar a la etapa del VCO proporcione el voltaje necesario para que éste último genere el barrido de frecuencia.

El circuito integrado que se usó para realizar esta función es el XR-2206, pues tiene la particularidad de generar ondas de forma triangulares, senoidales y cuadradas con una gran precisión y estabilidad. Además de que este circuito integrado es fácil de conseguir y tiene un costo relativamente bajo.

La configuración utilizada para generar la señal triangular se muestra en la figura 4.5. Con esta configuración se tendrá una frecuencia de 1MHz (Máxima frecuencia de trabajo para este circuito integrado). Como consecuencia, se tendrá una máxima velocidad de barrido. Las características de la señal generada se muestran, a su vez, en la tabla 4.1.

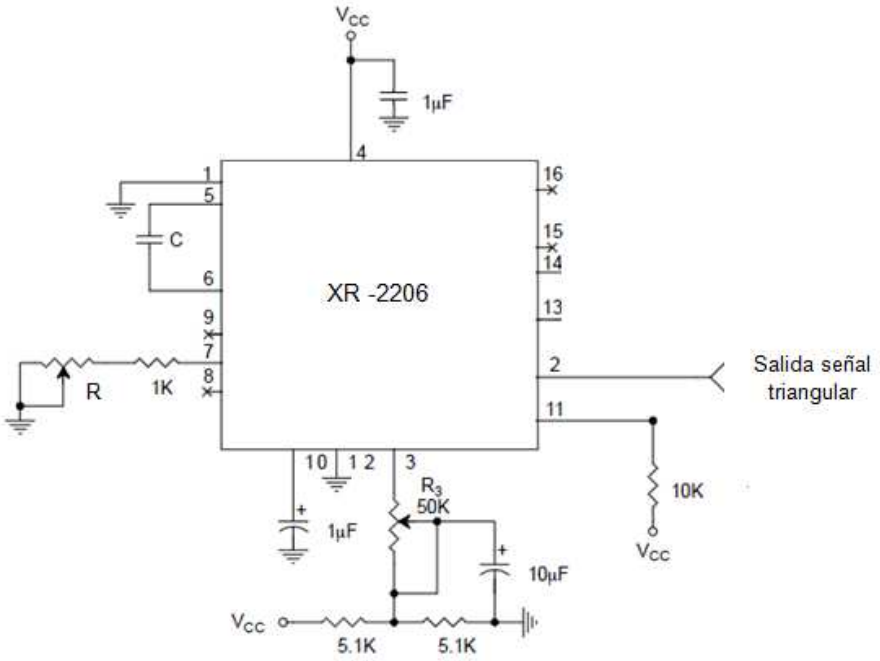

Figura 4.5 Configuración para generar una señal triangular.

El potenciómetro R (Cuyo valor se eligió de 1kΩ, para tener frecuencias comprendidas entre 0.5 MHz y 1 MHz) conectado al pin número 7 del integrado, permitirá el control de la frecuencia de la señal. Determinado por la ecuación:

$$f = \frac{1}{(R_1 C)} \qquad (4.2)$$

Donde: $R_1 = R + 1k\Omega$

$(0 \leq R \leq 1k\Omega)$

Así mismo, el potenciómetro conectado al pin número 3 controlará la amplitud de la señal de salida. De modo que, de acuerdo a las especificaciones del XR2206, para una señal triangular, la amplitud de salida incrementará aproximadamente 160 mV por cada KΩ. Pudiendo obtener como máximo una amplitud de 6 Vpp. Utilizando a su vez un valor máximo resistivo de 50 KΩ, como se muestra en la figura 4.6.

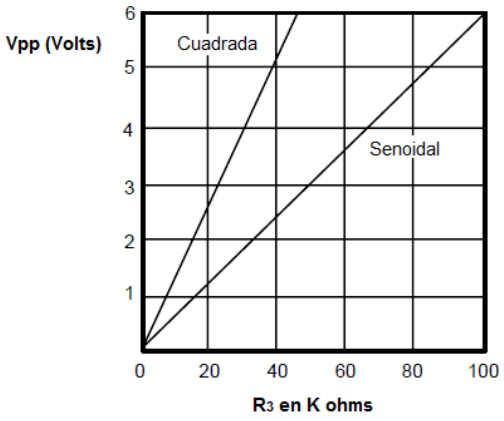

Figura 4.6 Relación Vpp vs R_3 .

Voltaje de alimentación	Frecuencia de operación (MHZ)		Capacitor C	Resistor R	Vpp
(V)	Min	Max	(nF)	(kΩ)	(V)
24	0.5	1	1	1	6

Tabla 4.1 Características eléctricas del XR-2206 para una señal triangular.

Cabe mencionar también que, el divisor de voltaje presente en el pin 3, formado por las 2 resistencias de 5.1 kΩ, tienen la función de introducir un desplazamiento

en DC (offset), propio del XR2206. Dicho divisor fue realizado mediante un arreglo de 2 resistencias en paralelo con valores de 5.6 kΩ y 56 kΩ. Debido a que, a pesar de ser un valor comercial, no fue encontrado como tal.

- SUJETADOR DE NIVEL (OFFSET)

Como se mencionó en párrafos anteriores, el rango de barrido del VCO está en función del voltaje a su entrada. La tabla 4.2 muestra esta relación.

Voltaje de entrada	Frecuencia de Salida	Potencia de salida	Voltaje de entrada	Frecuencia de Salida	Potencia de salida
(V)	(MHz)	(dBm)	(V)	(MHz)	(dBm)
1	1266.0	12.11	13.0	1807.5	12.57
3	1364.1	13.01	15.0	1890.7	12.17
5	1446.3	13.20	17.0	1958.2	11.88
7	1530.7	13.24	19.0	2015.5	11.75
9	1622.0	13.10	21.0	2060.6	11.46
11	1715.8	12.94	22.0	2081.2	11.38

Tabla 4.2 Frecuencia de Salida en función del voltaje de entrada.

Se puede observar que el VCO oscilará en la banda de los 1900 MHz, siempre y cuando tenga a su entrada voltajes comprendidos dentro del rango de 16V a 18V. Por lo cual, fue necesario mover el nivel de referencia (nivel de DC) de la señal triangular, de tal modo que sus límites (Voltajes picos) se encuentre dentro de este rango de voltaje. Esto se llevó a cabo utilizando el transistor 2N2222.

Se trata de un transistor tipo NPN, y se eligió por ser un amplificador de radiofrecuencia que trabaja alrededor de los 300 MHz, con potencias bajas y con una gran capacidad de respuesta. Además de estar familiarizado con su uso.

Algunos de sus parámetros más importantes para fines de este proyecto se muestran en la tabla 4.3. Los cuales fueron obtenidos directamente de su hoja de especificaciones (Datasheet).

V_{CE} (Con Base abierta)	I_C	Frecuencia de trabajo	Potencia de disipación	Tiempo de respuesta
Max.	Max.	Min	Max	Max
30 V	800 mA	300 MHz	500 mW	250 ns

Tabla 4.3 Características eléctricas del 2N2222.

Para realizar esta amplificación y alteración del offset de la señal triangular, se trabajó el transistor en configuración de emisor común, como se muestra en la figura 4.7.

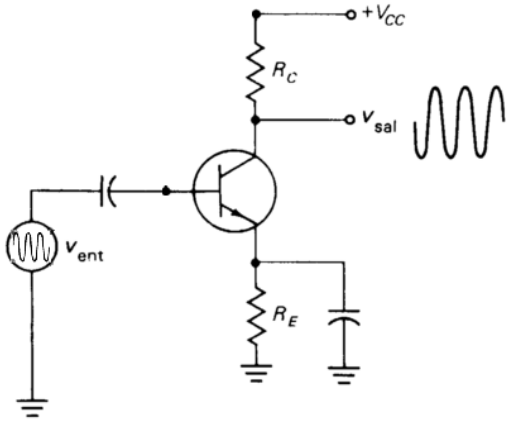

Figura 4.7 Configuración en Emisor común.

Lo que sucede en este tipo de configuración es que, el emisor está acoplado a tierra por medio de un capacitor (de ahí su nombre). Así mismo, se tiene acoplada a la base una pequeña onda (en este caso será triangular), lo cual produce variaciones en la corriente de base. La corriente de colector es una forma de onda igual a la de base, pero amplificada (debido a la ganancia β), conservando la misma frecuencia. Esta corriente de colector, fluye por la resistencia de colector y

produce un voltaje amplificado de salida, lo que da como resultado la formula (4.3).

$$V_{sal} = I_c R_c \qquad (4.3)$$

Por otra parte, debido a las variaciones de CA en la corriente de colector, el voltaje de salida varía proporcionalmente a ésta, en la parte superior e inferior del voltaje de CD (ver figura 4.8). Esta figura muestra también, la línea de carga de CA y el punto Q (Vcc, Ic). El voltaje de CA de entrada produce variaciones de CA en la corriente de base. Esto da origen a variaciones de la forma de onda alrededor del punto Q, como se muestra también en la figura 4.8.

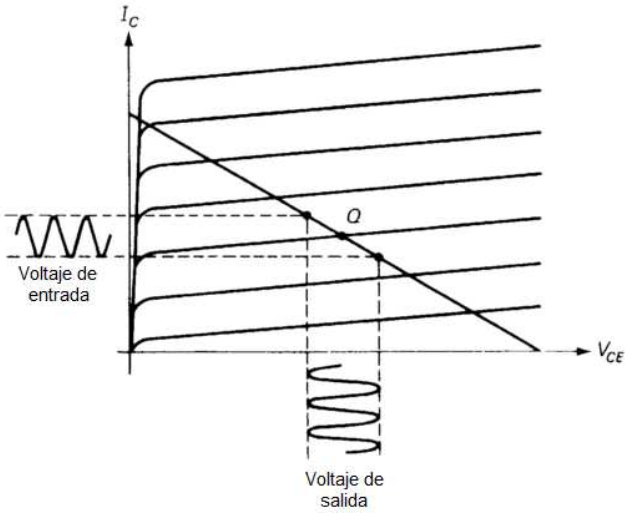

Figura 4.8 Recta de carga.

De esta manera, en el diseño se propusieron los valores resistivos de colector y emisor, de tal manera que no sobrepasaran la región de saturación del transistor. Para esto se utilizaron las siguientes ecuaciones:

$$I_c = \frac{Vcc}{Rc + R_E} \qquad (4.4)$$

$$P_c = (V_{CE})(I_C) \qquad (4.5)$$

Los valores propuestos fueron 2 kΩ y 1.5 kΩ, para emisor y colector, respectivamente. Así mismo, usando las ecuaciones (4-4) y (4-5) se obtuvieron los siguientes valores de corriente de colector y máximo nivel de disipación:

$$I_c = \frac{24\ V}{1.5\ \text{k}\Omega + 2\ \text{k}\Omega} = 6.85\ mA$$

$$P_{C_{Max}} = (24\ V)(6.85\ mA) = 164.4\ mW$$

El resultado obtenido de la potencia de disipación demuestra que la configuración hecha para este transistor, no sobrepasa el máximo nivel de potencia dado por el fabricante, además de que su recta de polarización tampoco llega a un punto de límite de operación como lo muestra la figura 4.9 [18].

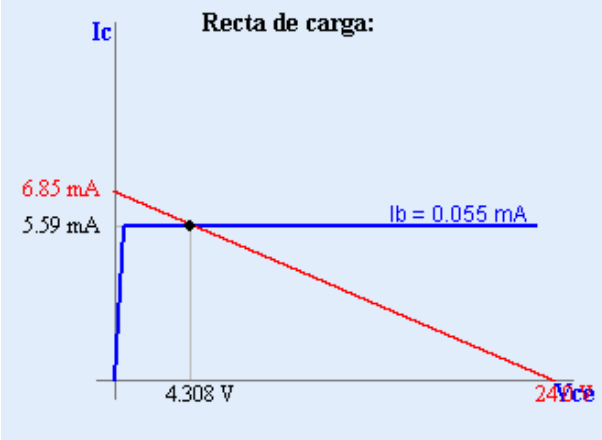

Figura 4.9 Recta de carga resultante.

4.2.3 Sección RF

La sección RF es la parte más importante, ya que será aquí donde finalmente se tendrá la señal a ser radiada por el Jammer. Esta parte está comprendida por un oscilador controlado por voltaje (VCO), una línea de transmisión y una antena.

Además de las interfaces (conectores) comprendidas entre la línea de transmisión y la antena (ver figura 4.10)

Figura 4.10 Diagrama a bloques de la sección RF.

- VCO

El circuito que se eligió fue el JTOS-2000, de montaje superficial, el cual abarca un rango de 1370 a 2000 MHz, resultando óptimo para el objetivo planteado, ya que cubre la banda de los 1900 MHz. Además, cuenta con una buena potencia de salida, la cual como se mencionó antes, no debe ser muy grande, pero a su vez, tampoco demasiado pequeña para aplicar una etapa de amplificación de ser necesario. En la investigación se encontraron dos VCO´s similares que cumplían con un rango de barrido similar, sin embargo el factor que hizo que no fueran elegidos fue la potencia, ya que en un caso era muy pequeña (4 dBm) y en el otro demasiado grande (21 dBm), estos circuitos son: el TRF3721 de Texas Instrument y el VO5180S/01 de SIVERSIMA, respectivamente. En la tabla 4.4 se muestran las características principales del VCO.

Frecuencia (MHz)		Potencia de salida (dBm)	Voltaje de ajuste (V)		Alimentación		Impedancia de salida
Min.	Max.	Típica	Min.	Max.	Vcc (Volts)	Corriente (mA)	(Ohms)
1370	2000	+12.0	1.0	22	8	30	50

Tabla 4.4 Especificaciones eléctricas del VCO JTOS-2000

- LÍNEA DE TRANSMISIÓN

Una línea de transmisión se define como un sistema de conductores, semiconductores o una combinación de ambos con el objeto de transmitir energía eléctrica y señales de un punto a otro; para ser más exactos, desde una fuente hasta una carga. Existen diferentes tipos de líneas de transmisión, sin embargo para la implementación del circuito sólo se consideró la línea de tipo planar ya que además de permitirnos transmitir a éstas altas frecuencias, se adapta perfectamente a un circuito impreso.

Dentro de este tipo de línea se tiene la microcinta (microstrip), la línea de ranura (stripline) y la guía de onda coplanar (coplanar waveguide). La figura 4.11 muestra un ejemplo de las líneas de tipo planar [14, 15].

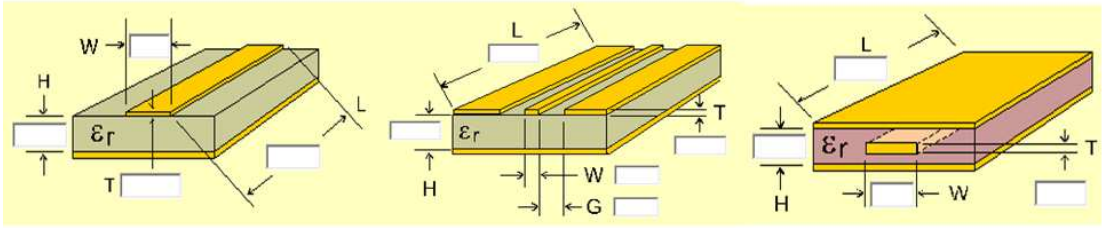

Figura 4.11 Tipos de línea planar.

Como se puede observar en la figura anterior, la guía de onda coplanar es la más idónea para el diseño del circuito por su adecuación al VCO, dado que este es de montaje superficial y la mayoría de sus terminales van conectadas al plano tierra.

Ahora, al trabajar con líneas de transmisión sobre un circuito impreso, se debe tener en cuenta el dieléctrico con el que está hecha la placa, ya que su constante dieléctrica, el ancho de la línea y la separación con el plano tierra, determinan la impedancia característica de la línea, siendo de suma importancia conocer la constante dieléctrica de la placa para poder definir, por medio de software, el ancho y la separación de la línea necesarios para obtener una impedancia deseada.

- Impedancia característica

La impedancia característica de una línea de transmisión se define como una impedancia de entrada que tendría una línea de trasmisión que es infinita; en otras palabras una relación de voltaje y corriente. Dado que nuestra intención es lograr la máxima transmisión de potencia de un punto a otro, se necesita cumplir la condición de que la impedancia de salida del transmisor sea igual a la impedancia de entrada de la carga.

Cuando la impedancia de la carga es diferente a la impedancia de salida del transmisor, se sufrirá una serie de problemas con ondas reflejadas en el proceso de cambio de un punto de la línea al otro, dando como resultado una onda estacionaria. Si este desacoplamiento es demasiado grande, la onda reflejada puede dañar el transmisor.

Si se plantea que una impedancia característica este situada sobre una línea infinita, la onda que se está transmitiendo nunca alcanzará la carga por lo que las condiciones para que ocurra una posible onda estacionaria nunca se darán. Teniendo que acoplar el valor de la impedancia del segundo medio al del valor del primer medio [15].

En este caso se sabe que el VCO trabaja con una impedancia de salida de 50Ω, por lo tanto, la línea de transmisión a elaborar debe cumplir con esa condición a su entrada.

- Caracterización de la placa fenolica

Para realizar el acoplamiento de la línea se realizó una caracterización previa de la placa por medio de un Q-metro para la obtención de su capacitancia y, posteriormente, por medio de la fórmula (4.6) la obtención de su valor de permitividad relativa (ϵ_r). En donde C es la capacitancia, d es la separación entre

las placas [m], S el área [m] y ϵ es la constante dieléctrica la cual está dada por ϵ_r que es la permitividad relativa y ϵ_0 la permitividad del espacio libre [14].

$$C = \frac{\epsilon S}{d} \qquad (4.6)$$

Se hace hincapié que esta forma de obtener ϵ_r no es la más precisa debido al uso de una fórmula y no de un instrumento de medición o en su defecto la fabricación de la placa con la características requeridas; pudiendo verse reflejados sus posibles efectos en el funcionamiento del Jammer. Para empezar la caracterización, el primer paso fue comprar una placa fenolica doble cara de fibra de vidrio de 30x30cm, a la cual se le realizó un pequeño corte de 6.6x3.4 cm; Posteriormente, se colocó sobre una de las terminales de un Q-metro para que esta placa entrara en resonancia con el sistema y así obtener de forma indirecta el valor de su capacitancia. En la figura 4.12 se muestra el Q-metro con la conexión de una pequeña bobina y el corte de la placa para la obtención de su capacitancia; En la tabla 4.5 los valores que se obtuvieron al realizar la medición.

Figura 4.12 Medición de la capacitancia de la placa.

Frecuencia de resonancia	Inductor	Capacitor variable C1	Rango de medición	Factor de calidad	Medición inicial	Medición final	Capacitancia de la placa C2
MHz	μH	ρF	ρF	Q	ρF	ρF l	ρF
25.5	0.33	52	50-150	400	52	120	68

Tabla 4.5 Resultados de la medición de la capacitancia de la placa.

Después de obtener estos resultados se usó la fórmula (4-6) para obtener ϵ_r; Los datos y el valor obtenido se muestran en la tabla 4.6.

C	D	S	ϵ_0	Resultado ϵ_r
ρF	M	M	F/m	
68	1.7×10^{-3}	2.244×10^{-3}	8.8541×10^{-12}	5.8182

Tabla 4.6 Datos y resultado de ϵ_r.

- INTERFACES Y ANTENA

La antena es esencial en un transmisor, ya que es a partir de este punto donde se radia toda señal. Es por ello que se realizó una selección adecuada del tipo de antena para el propósito de este trabajo.

La antena que se eligió fue la COM-830. Esta antena trabaja con un patrón de radiación omnidireccional, con 5 dBi de ganancia, acoplada a 50 Ω, con un VSWR de 1.92 y con pérdidas de retorno de -10dB; además de esto, la antena ya viene equipada con un conector RP-SMA (Reverse Polarity SubMiniature version A).

Este tipo de conector forma parte de la serie SMA, los cuales trabajan a frecuencias superiores a los 18 GHz, están acoplados a 50 Ω y son altamente resistentes y compactos. Debido a esto se eligió un RP-SMA como conector ideal para el montaje superficial del circuito impreso. En la figura 4.13 se muestra el conector usado.

Figura 4.13 Conector 132136 RP-SMA de montaje superficial.

Como se mencionó anteriormente el patrón de radiación de la antena es omnidireccional, mostrado en figura 4.14, donde se observan dos gráficas: la primera para el patrón de elevación y la segunda para el patrón de azimut, las cuales forman el patrón de radiación omnidireccional. Se hace un hincapié en el patrón de elevación de esta antena, ya que puede ir variando de 0° a 90° debido a que esta antena tiene la capacidad de mover su base para lograr una polarización horizontal o vertical.

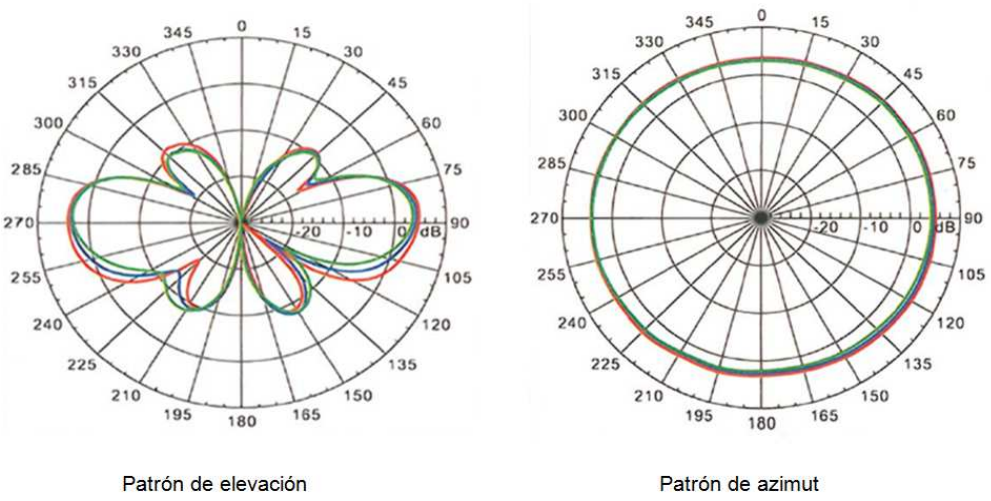

Figura 4.14 Patrón de radiación omnidireccional de la antena.

Por último, se fabricó una extensión con el fin de tomar las mediciones de funcionamiento correspondientes al VCO. Para ello se siguieron ciertas normas y medidas estandarizadas (ver figura 4.15), las cuales permiten que la extensión tenga un mayor rendimiento y pocas pérdidas por acoplamiento. La tabla 4.7 muestra las medidas de cada corte.

Figura 4.15 Pasos para la fabricación de extensión con conectores SMA.

a	B	c
mm	Mm	mm
13.5	5.2	3.5

Tabla 4.7 Cortes del cable para una extensión SMA.

El cable utilizado fue RG-58/U, debido a que los conectores SMA que se encuentran comercialmente sólo trabajan con este tipo de cable. Sus especificaciones se dan en la tabla 4.8

Impedancia característica	Perdidas	Diámetro del conductor	Diámetro del dieléctrico	Diámetro exterior del cable
(Ohms)	(dB/100m)	(mm)	(mm)	(mm)
50	81dB	0.9	2.95	4.95

Tabla 4.8 Especificaciones del RG-58/U.

4.3 SIMULACION DEL JAMMER

4.3.1 Simulación: Sección de Alimentación

Esta simulación se realizó con ayuda de la herramienta de simulación de circuitos denominada NI Multisim (versión 10), de National Instruments.

Tal como se describió en la parte de diseño, la fuente consta de las etapas correspondientes al transformador, el rectificador, el capacitor de filtrado y los circuitos de regulación de voltaje. Los resultados obtenidos, de está simulación, fueron los esperados de acuerdo al diseño. Como se muestra en la figura 4.16.

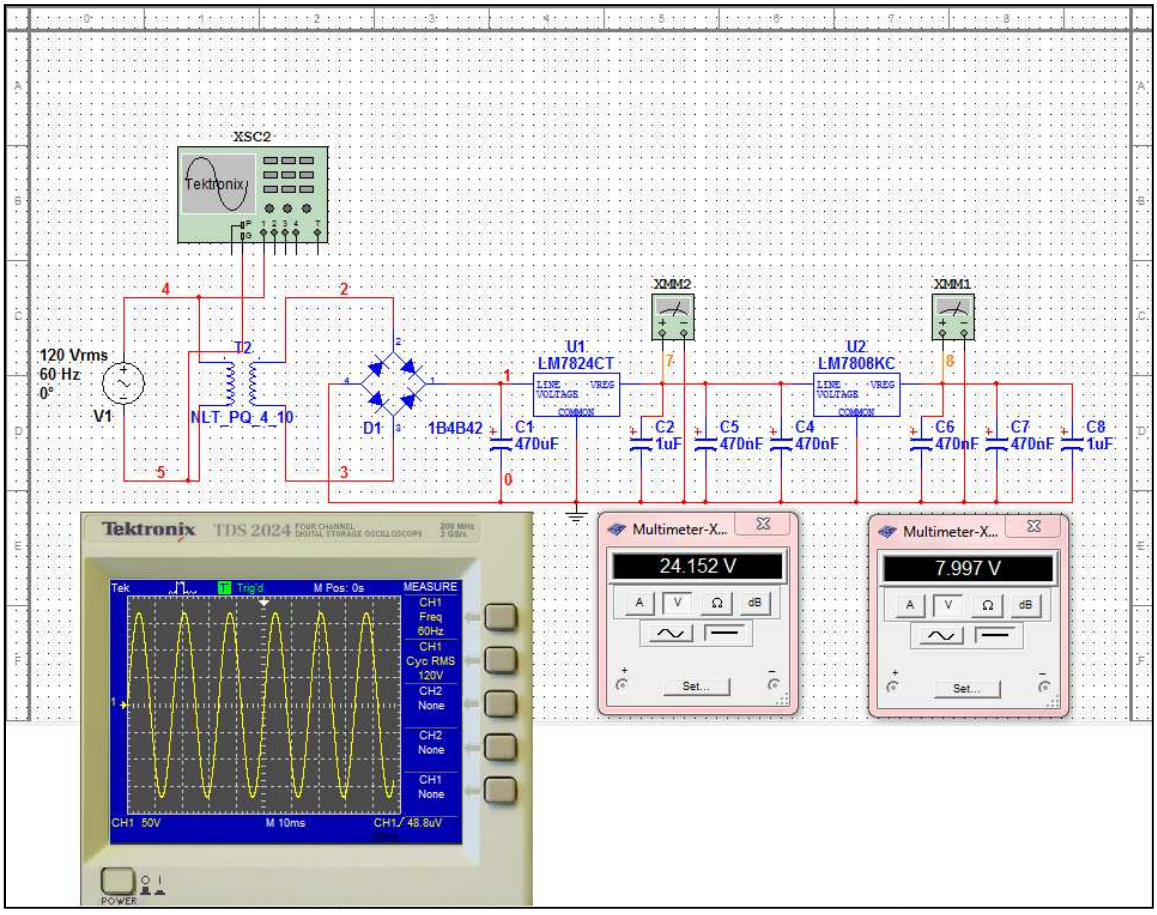

Figura 4.16 Resultado de simulación de fuente.

4.3.2 Simulación: Sección de Oscilación

La señal triangular generada con el circuito XR2206 no fue posible simularla debido a que este componente no se encuentra disponible en el software utilizado. Sin embargo, para que esto no fuera impedimento a la hora de simular el transistor 2N2222, se utilizó en su lugar un generador de funciones en la modalidad de onda triangular. Y únicamente, se establecieron los parámetros que en teoría deberían ser obtenidos del XR2206 (ver figura 4.17). Dichos parámetros son mostrados en la tabla siguiente.

Voltaje de Offset (V)	Vpp (V)	Frecuencia de Trabajo (MHz)	
Max.	Max.	Min.	Max.
12	6	0.5	1

Tabla 4.9 Parámetros teóricos del XR2206.

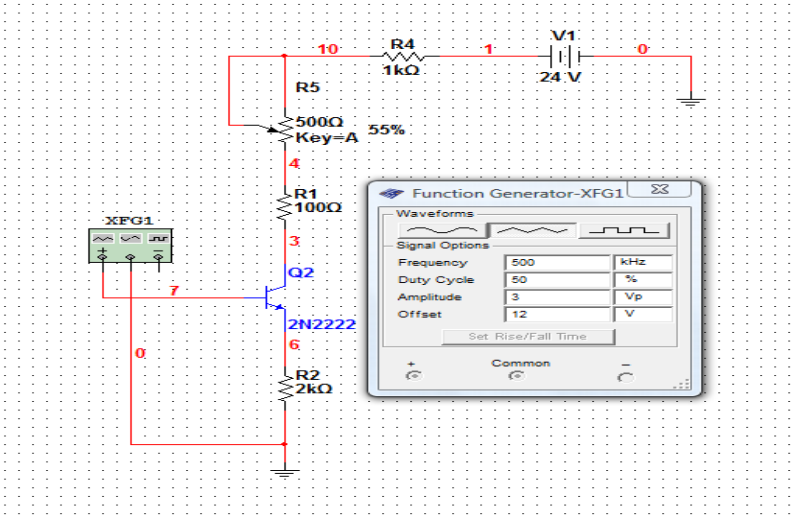

Figura 4.17 Ajuste de parámetros en señal triangular.

La figura 4.17 no sólo muestra los ajustes realizados al generador de funciones para simular la onda triangular, sino que también despliega la configuración utilizada en la simulación del transistor. En la cual, como puede observarse, se

tiene un arreglo resistivo (en serie) en la parte del colector, siendo una de estas resistencias, un potenciómetro. Este potenciómetro es implementado para realizar el desplazamiento en DC de la señal. Y de acuerdo a esto, se obtuvo que la máxima amplitud del potenciómetro, para que la señal llegue a subir sin alterar su simetría, es del 75%.

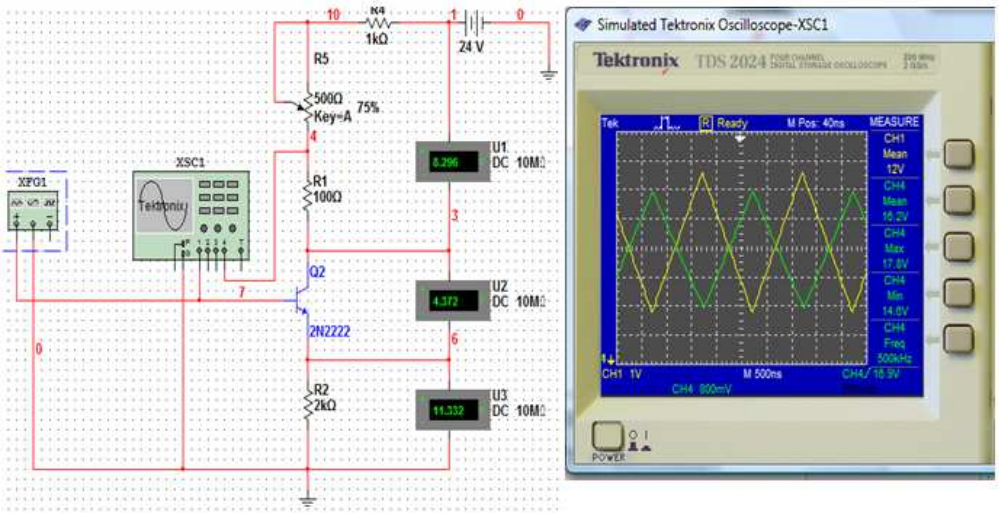

Figura 4.18 Resultados en simulación del 2N2222.

Los resultados de la simulación de la figura 4.18 indican que se tendrá un nivel de DC (offset) máximo en 16.2 V. De igual manera, debido a esta referencia de DC, se tendrá el nivel mínimo de voltaje situado en 14.6 V y un nivel máximo en 17.8 V. De tal manera que, al revisar la tabla 4.2 se observa que los voltajes picos de la señal, debido al offset, quedan comprendidos en el rango deseado para que el VCO pueda realizar un barrido eficiente sobre la banda de los 1900 MHz.

4.3.3 Simulación: Sección RF

La única parte simulada dentro de esta sección fue la correspondiente a la línea de transmisión. Es decir, la parte que se encarga de llevar las señales de radiofrecuencia hacia la antena. Para esto, se utilizó un software denominado TX LINE (versión 2003)

Lo primera que se estableció para la simulación, debido a su importancia en el diseño, fue el acoplamiento a 50Ω. Posteriormente, tomando en cuenta las características físicas de la placa utilizada, se estableció el espesor del conductor (T), la separación de las placas (H) y la permitividad relativa (ϵ_r). Seguido, se propuso el ancho de la línea o conductor (W), así como la separación de ésta con el plano tierra (G). La longitud de la placa (L) ya se había previsto tomando en cuenta el diseño del PCB o layout. Por tanto, se mantuvo en 6 cm [16].

Después de hacer variar principalmente el ancho del conductor (W) y la separación de éste con el plano de tierra (G), sin alterar la impedancia de acoplamiento se obtuvó que, las medidas idóneas (tomando en cuenta las características físicas de las terminales del VCO) son las mostradas en la figura 4.19. Así mismo, una vez establecido los parámetros fisicos de la línea, la misma aplicación nos permite visualizar una imagen en 3D (Figura 4.19).

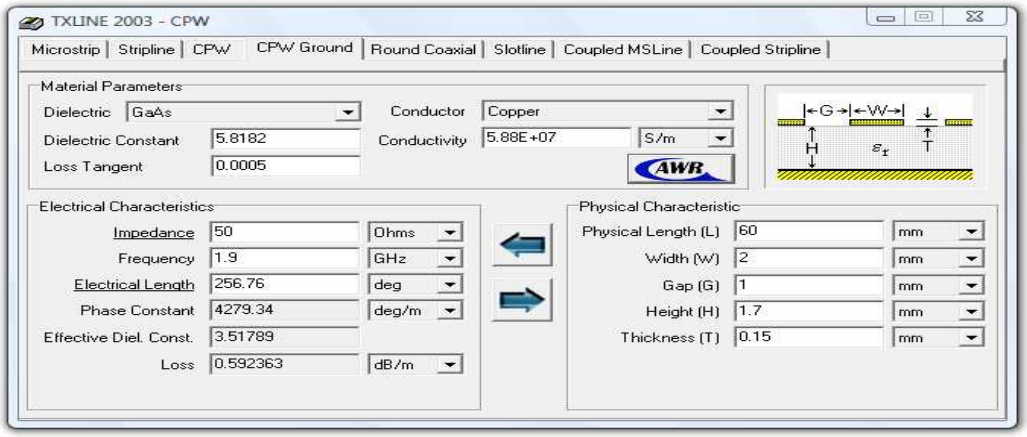

Figura 4.19 Parámetros de la línea de transmisión.

La simulación de la línea permitió conocer un estimado de las posibles pérdidas de potencia que se pudiesen tener por reflexiones a la entrada, parámetro dado por S_{11} (coeficiente de reflexión de puerto de entrada). Para obtenerlo se introdujeron los parámetros de separación de la línea con el plano tierra, ancho de la línea, el tipo de dieléctrico y del conductor. Estas posibles pérdidas están reflejadas en la grafica de la figura 4.20 [17].

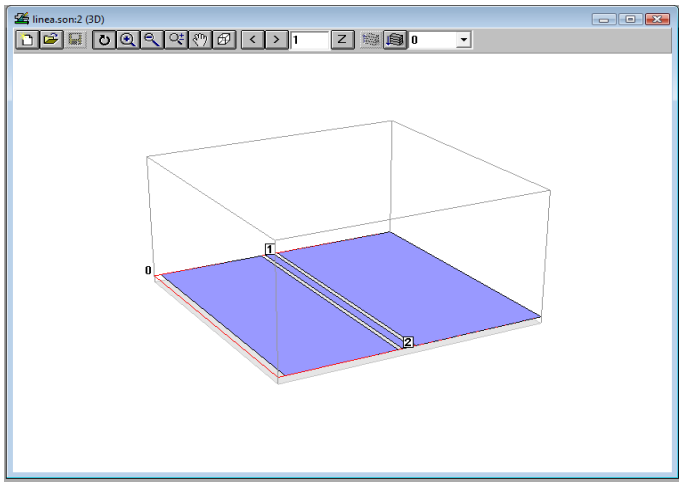

Figura 4.20 Imagen 3D de la línea de transmisión.

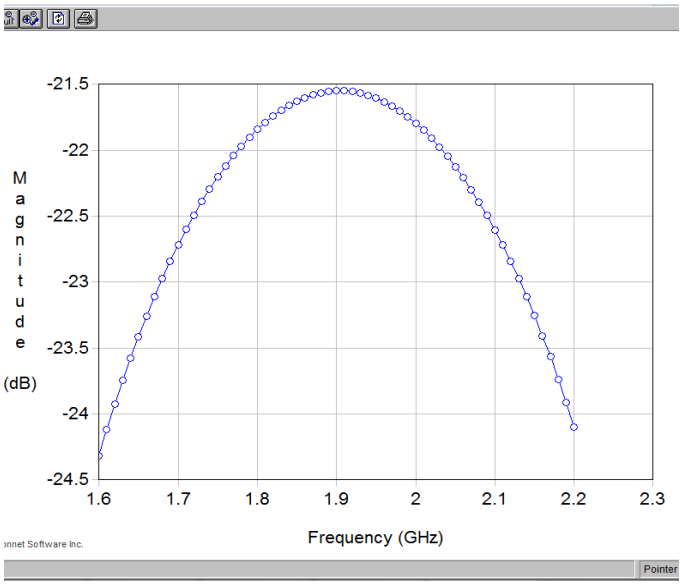

Figura 4.21 Posibles pérdidas de potencia.

En la figura 4.21 se muestra el resultado del parámetro S_{11} sobre el rango de frecuencias que cubre el VCO, por lo que se observa que, para la banda de los 1900 MHz no se tendrán pérdidas considerables de potencia; y por tanto, la transferencia de energía será óptima.

CAPÍTULO 5
EVALUACIÓN: MEDICIONES Y RESULTADOS

5.1 CIRCUITO DE BLOQUEO (JAMMER)

Después de realizar el análisis, diseño y simulaciones correspondientes a cada etapa del Jammer, finalmente se llegó a la implementación física del circuito. el cual está basado en el PCB (Layout) que se muestra en la figura 5.1.

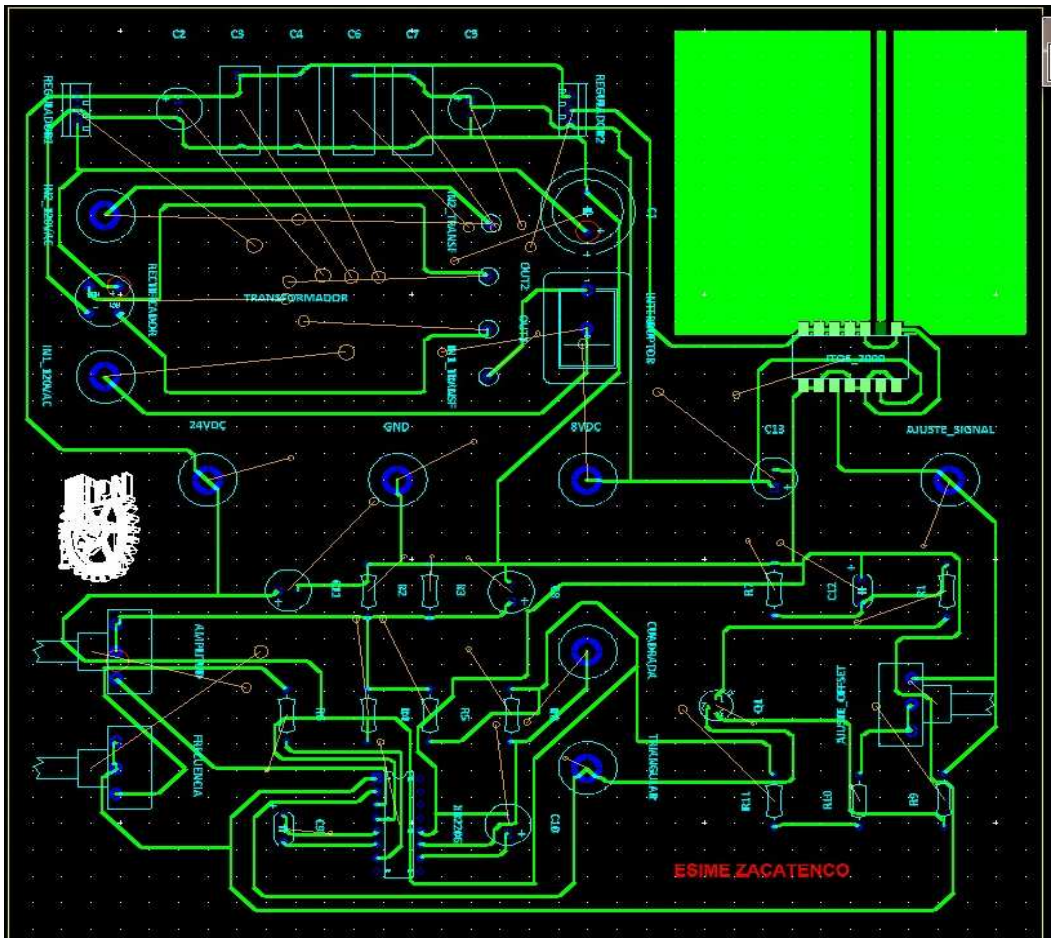

Figura 5.1 PCB del Jammer.

La figura 5.1 nos muestra el PCB utilizado para la implementación física del jammer. Sin embargo en el apéndice B se detalla un poco más el procedimiento de diseño que dio como resultado lo que se muestra en dicha figura.

Tomando como base el Layout de la figura 5.1, y después de realizar todo el proceso correspondiente a la impresión, revelado, perforación, soldado de componentes, adaptación de conectores e inserción de la antena junto con la placa. Se obtuvo finalmente el dispositivo de bloqueo mostrado en la figura 5.2.

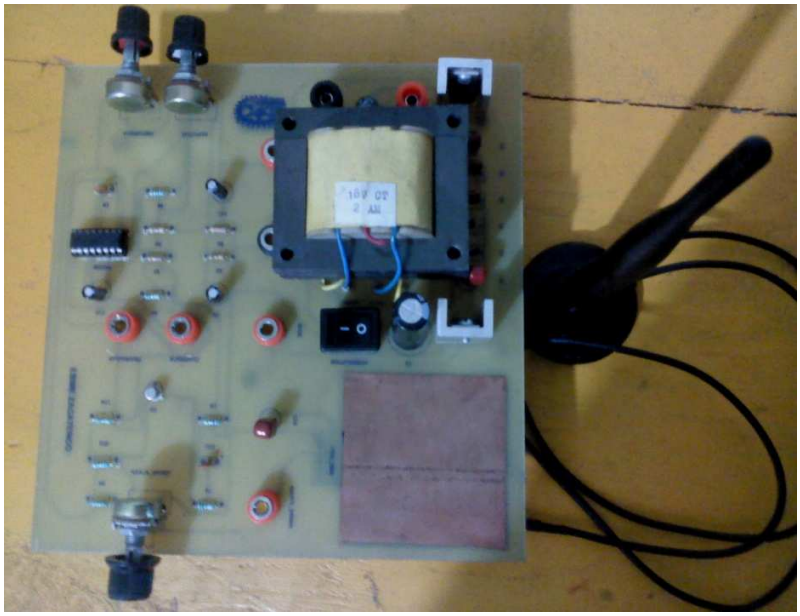

Figura 5.2 Presentación final del Jammer.

5.2 EVALUACION DEL DISPOSITIVO

Para evaluar el funcionamiento del Jammer se realizaron mediciones en dos partes en la cual, se midió primero la parte de oscilación y posteriormente la sección de RF. La sección de alimentación no se evaluó, ya que no representó mayor inconveniente en cuanto a funcionamiento.

- Sección de oscilación

Para evaluar la sección de oscilación se utilizó un osciloscopio digital marca Tektronix, modelo TDS 1002.

Básicamente la medición se realizó a la salida del transistor. Ya que es hasta esta etapa donde se tiene la señal triangular ya acondicionada para proporcionar los niveles de voltaje adecuados para que en consecuencia, el VCO realice su función de barrido.

Cabe mencionar que al evaluar esta sección, se engloban también, las secciones anteriores. Es decir, para que a la salida del transistor se tengan los resultados esperados, la fuente previamente tiene que suministrar la alimentación adecuada tanto al XR2206, el cual se encarga de generar la señal triangular, como al propio transistor, el cual nos dará como resultado la señal ya adecuada para que al introducirla hacia el VCO, éste ultimo realice lo propio, es decir, el barrido en frecuencia. De tal forma que, después de realizar dichas mediciones, se obtuvieron los resultados mostrados en la figura 5.3, y resumidos en la tabla 5.1.

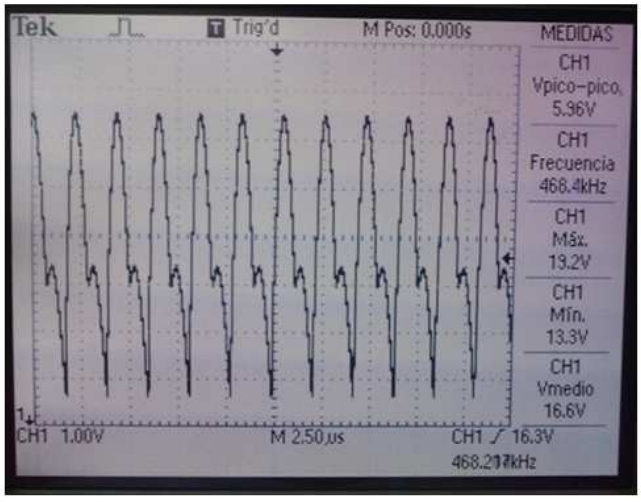

Figura 5.3 Medición a la salida del transistor 2N2222.

Voltajes de offset			Frecuencia de operación	Voltaje pico-pico
Vmedio	Vmáx.	Vmín.		
16.6 V	19.2 V	13.3	468.4 kHz	5.96 V

Tabla 5.1 Resultados de la sección de oscilación.

- Sección de RF

Las mediciones correspondientes a esta sección se realizaron con ayuda de un analizador de espectros marca IRITZU, modelo MS2712E. Los resultados obtenidos de dichas mediciones se pueden visualizar en la figura 5.4. asi mismo, al igual que en la parte de oscilación, éstos mismos resultados se resumen en la tabla 5.2

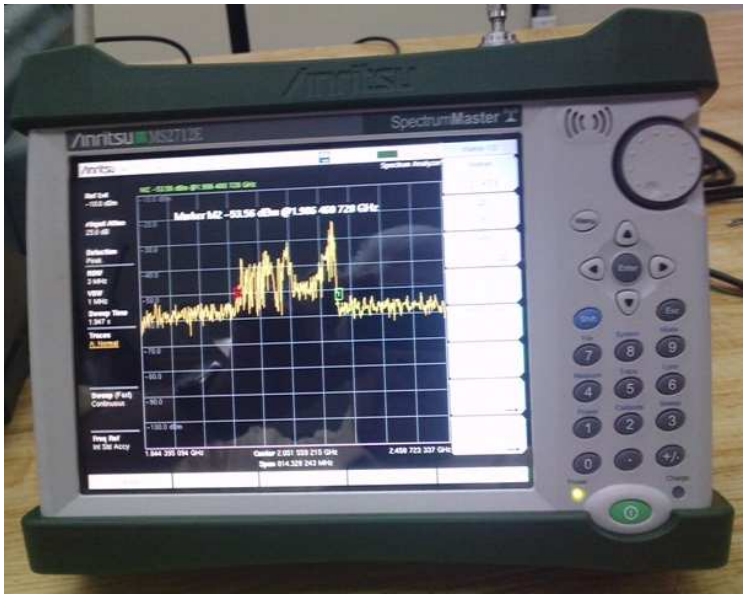

Figura 5.4 Medición de la sección RF.

Espectro de frecuencia ocupado		Potencia de salida del circuito
Fmín.	Fmáx.	
1.9 GHz	2.1 GHz	10 dbm

Tabla 5.2 Resultados obtenidos de la medición de la sección RF

La tabla 5.2 nos muestra que el rango del espectro cubierto por el Jammer es satisfactorio, pues abarca perfectamente toda la banda de los 1900 MHz, sobre la cual trabajan los sistemas de 2G y 2.5G.

Por otra parte, se observa que los valores de voltaje del offset difieren de los valores propuestos en el diseño. Este efecto se debe a cuestiones internas de cada elemento, ya que cada uno cuenta con una tolerancia de trabajo (resistencia, capacitancia y temperatura) que afectan la eficiencia y rendimiento del Jammer.

5.3 PRESENTACIÓN DE RESULTADOS PARA CELULARES 2G Y 2.5G

Las mediciones realizadas están hechas en función del azimut, la elevación (altura) y la distancia. En la cual se registran 15 mediciones con 25° (azimu t) de separación entre cada una de ellas; También se hizo el registro del tiempo de respuesta de los celulares dentro del área de cobertura cuando el Jammer es encendido y cuando es apagado.

- Proceso de medición

Las mediciones se realizaron en un cuarto completamente vacío de 5 m de largo por 4 m de ancho y con una altura de 5 m. Se tomaron tres celulares de diferentes compañías: Nokia 5310 (Telcel), Sony Ericsson Z520a (Movistar), Nokia 2600 (Telcel). El proceso de medición fue el mismo para los tres celulares. Este proceso se describe a continuación:

a. Se colocó el Jammer en el centro del cuarto a nivel de piso.
b. Se colocó el celular al mismo nivel del Jammer en línea recta.
c. Se encendió el Jammer.
d. Se midió el tiempo de respuesta.
e. Una vez hecho el bloqueo, se procedió a tomar la máxima distancia a la cual el Jammer aún ejerce el bloqueo sobre el móvil.
f. Sobre ese mismo punto se tomó la máxima altura de bloqueo.

g. Se realizó una rotación de 25° de azimut y se realizan los pasos **e** y **f**, catorce veces más.
h. Se tomó al celular en el límite de cobertura del Jammer y se salió de esta para registrar el tiempo de respuesta en la cual el celular vuelve a recuperar la señal de la BS.
i. Al término de las 15 mediciones se apagó el Jammer y se tomó el tiempo de respuesta de recuperación de la señal.

- Resultados

Los resultados de estas mediciones se muestran en las tablas 5.3 y 5.4.

Medición	Azimut	Nokia 5310		Sony Ericsson Z520a		Nokia 2600	
		Distancia	Elevación	Distancia	Elevación	Distancia	Elevación
1	0°	1.60 m	2.10 m	1.70 m	2.20 m	1.80 m	2.40 m
2	25°	1.70 m	2.30 m	1.70 m	2.30 m	1.80 m	2.40 m
3	50°	1.80 m	2.30 m	1.80 m	2.00 m	1.90 m	2.50 m
4	75°	1.70 m	2.10 m	1.80 m	2.10 m	2.00 m	2.50 m
5	100°	1.70 m	2.20 m	1.80 m	2.00 m	1.90 m	2.60 m
6	125°	1.70 m	2.10 m	1.80 m	2.00 m	2.00 m	2.60 m
7	150°	1.80 m	2.20 m	1.70 m	2.20 m	1.90 m	2.50 m
8	175°	1.80 m	2.10 m	1.70 m	2.10 m	2.10 m	2.60 m
9	200°	1.60 m	2.20 m	1.70 m	2.30 m	2.00 m	2.60 m
10	225°	1.70 m	2.20 m	1.80 m	2.10 m	2.10 m	2.50 m
11	250°	1.70 m	2.10 m	1.80 m	2.10 m	1.90 m	2.40 m
12	275°	1.60 m	2.20 m	1.70 m	2.30 m	2.00 m	2.50 m
13	300°	1.70 m	2.30 m	1.80 m	2.30 m	1.90 m	2.60 m
14	325°	1.70 m	2.10 m	1.70 m	2.20 m	1.90 m	2.50 m
15	350°	1.70 m	2.20 m	1.80 m	2.10 m	1.80 m	2.40 m

Tabla 5.3 Cobertura de bloqueo del Jammer.

Celular	Jammer encendido	Jammer apagado	Fuera de la cobertura del Jammer
	Bloqueo	Recuperación de la señal	Recuperación de la señal
Nokia 5310	29 s	11 s	9 s
Sony Ericsson Z520a	22 s	8 s	8 s
Nokia 2600	19 s	17 s	12 s

Tabla 5.4 Tiempos de respuesta.

En la tabla 5.3 se observa que la distancia lograda por el Jammer se da a una máxima distancia de 2.10 m. Se puede visualizar también un máximo alcance en elevación 2.60 m.

En cuanto a los tiempos de respuesta del bloqueo. En promedio se registró un tiempo de 23.33 seg cuando el dispositivo es encendido, 12 seg para recuperar la comunicación con la estación base el Jammer es apagado y, 9.66 seg de recuperación cuando el móvil sale de la cobertura de bloqueo.

Por otra parte, tomando en cuenta el tipo de antena empleado por el jammer y el rango de frecuencia real cubierto por éste (de acuerdo con la tabla 5.2), fue posible obtener un patrón de radiación más exacto del dispositivo. Esta grafica del patrón de radiación se obtuvo con ayuda de la herramienta de simulación “Matlab”, pudiéndose a su vez visualizar en la figura 5.5. Esta grafica, si bien, es muy parecida a las mostradas en la figura 4.14, a diferencia de estas últimas, la nueva grafica nos da una perspectiva más real del comportamiento de la energía radiada por el jammer, gracias a que dicho patrón fue graficado basándonos en el rango de frecuencia real, dentro del cual el jammer radia la señal de bloqueo. Además de presentarnos el comportamiento no solo en los planos X y Y, sino también en el Z.

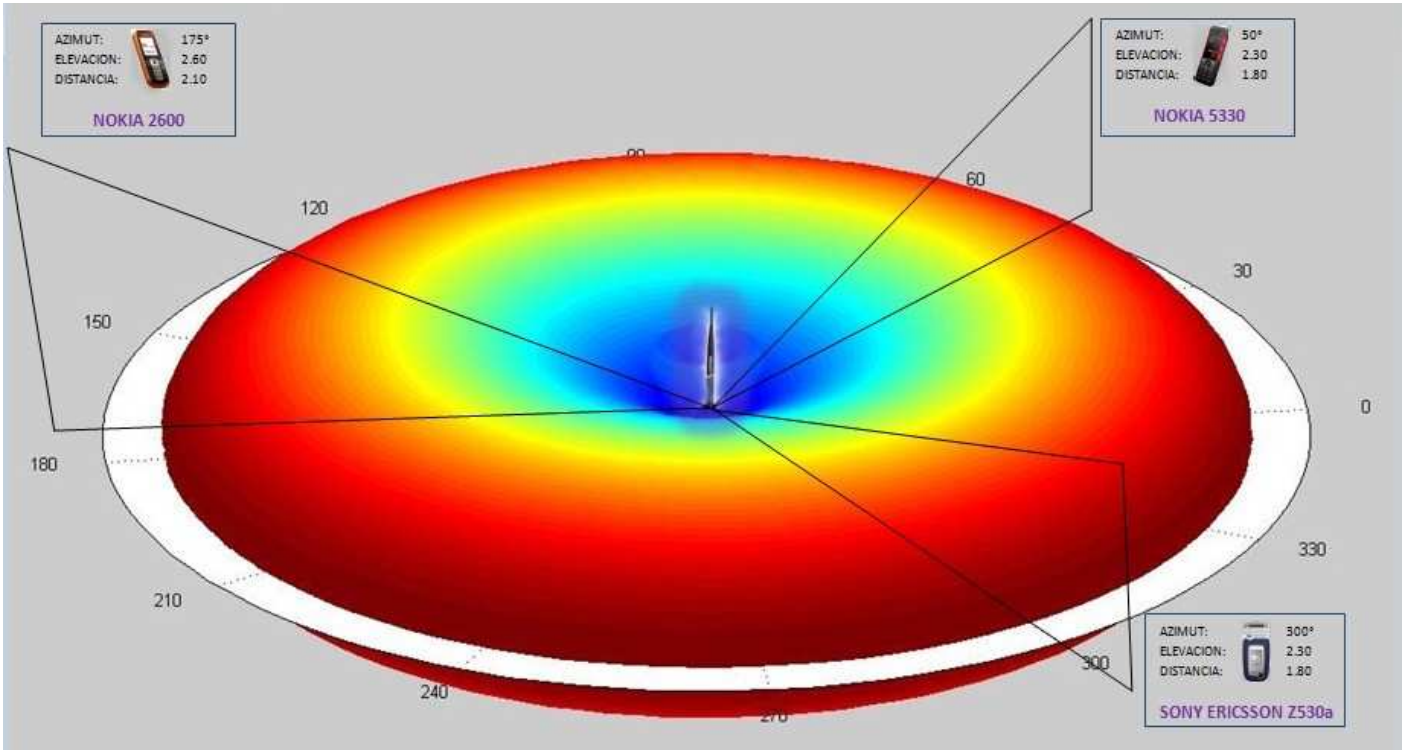

Figura 5.5 Patrón de radiación del Jammer y máximos resultados obtenidos.

La figura 5.5 nos muestra, además del comportamiento de la energía radiada o señal de bloqueo, también los resultados máximos obtenidos por el dispositivo. Midiéndose cada uno de ellos en relación con: El azimut, Elevación y la distancia, de acuerdo con los resultados obtenidos de la tabla 5.3

- **Pruebas visuales**

Jammer off

A continuación se muestran dos imágenes del efecto del Jammer sobre los celulares Nokia 5310 (Telcel) y Nokia 2600 (Telcel) con tecnologías de 2G y 2.5G respectivamente en las cuales se mostrara el efecto del Jammer antes y después de ser encendido

En la figura 5.6 se muestran los dos celulares que trabajan normalmente con cobertura Telcel GSM siendo las 10:36 pm (en este momento el Jammer se encuentra apagado) y vistos de izquierda a derecha se tiene el celular Nokia 2600 y a lado el celular Nokia 5310, es importante aclarar este punto ya que el efecto del Jammer difiere un poco de la tecnología con la que trabaje el equipo.

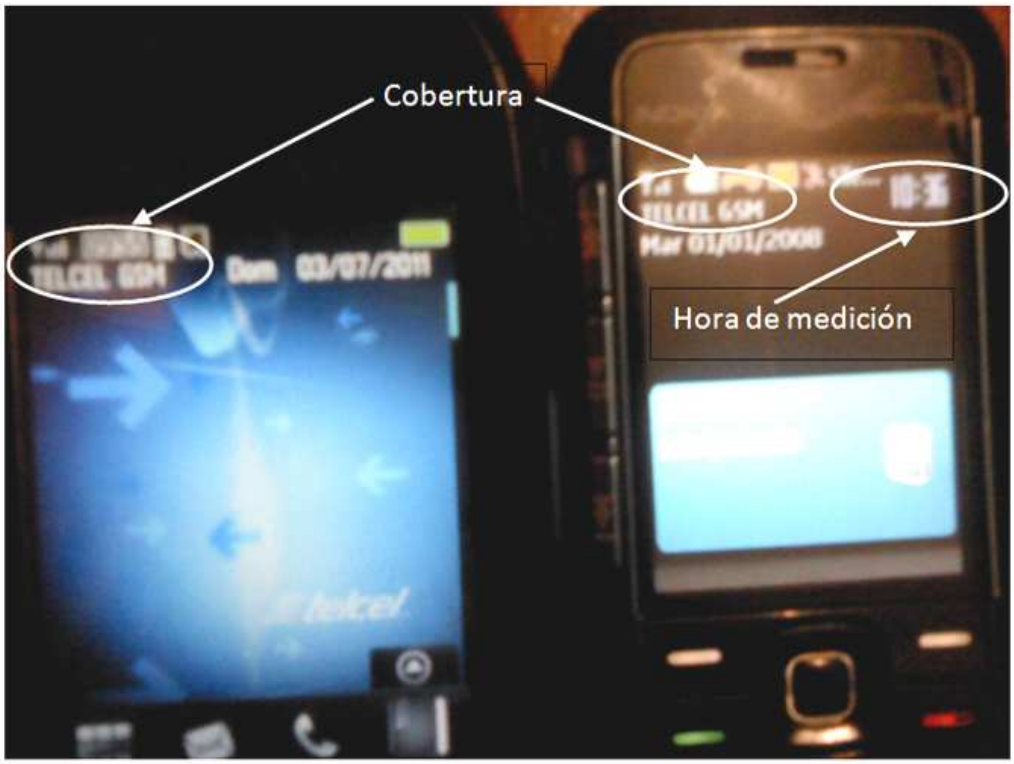

Figura 5.6 Funcionamiento de los celulares con el Jammer apagado.

Una vez comprobado el funcionamiento normal de los equipos se encendió el Jammer, al hacer esto inmediatamente se observaron cambios en la cobertura de los equipos en los cuales para el celular Nokia 5310 de 2G se obtuvo un bloqueo completo mientras que para el celular Nokia 2600 de 2.5G se tuvo un bloqueo de todo servicio que normalmente aporta la compañía como mensajes, llamadas y conexión a internet, desplegando un mensaje de solo emergencias, ver figura 5.7.

Jammer on

El efecto producido por las radiaciones del jammer sobre los teléfonos celulares en el área de cobertura de bloqueo, fue el siguiente:

Figura 5.7 Funcionamiento de los celulares con el Jammer encendido.

Los resultados de la figura 5.7 muestran que el bloqueo es casi inmediato observándose esto en la hora en la cual se tomaron las imágenes, teniendo que a las 10:36 los equipos funcionan con normalidad, para cuando el Jammer es encendido casi un minuto después, 10:37; los equipos muestren una cobertura nula o casi nula, teniendo que para el equipo 2.5G se tiene solo servicios de emergencia, mientras que para un equipo de 2G no se cuenta con ningún tipo de servicio.

5.4 PRESENTACIÓN DE RESULTADOS PARA CELULARES 3G

Las Condiciones de trabajo para realizar las mediciones con un celular 3G (Sony Ericsson 3G J108, Telcel) fueron las mismas que para sistemas de 2G. Se realizaron 15 mediciones inicialmente, sin embargo, dado que el Jammer solo trabaja en la banda de los 1900, los efectos registrados fueron completamente diferentes. No pudiéndose establecer un punto de máxima distancia y elevación de bloqueo, ya que los efectos se daban en forma aleatoria, siempre a nivel de piso y junto a la antena de Jammer. Por tal motivo se realizó en 20 ocasiones sobre un mismo punto la observación. Registrándose los siguientes efectos:

1. En quince ocasiones el celular no registró ningún cambio ante el Jammer.
2. Dos veces el celular no pudo concretar un envió de mensajes con éxito.
3. En dos ocasiones las llamadas telefónicas se registraron con ruido.
4. Y sólo una vez se pudo lograr el bloqueo del teléfono hasta un punto de solo admitir el uso de números de emergencia.

CAPÍTULO 6.

CONCLUSIONES Y TRABAJO A FUTURO

6.1 CONCLUSIONES

Tomando en cuenta los objetivos planteados y los resultados obtenidos, así como los diferentes parámetros, tanto teóricos como prácticos, es posible plantear las siguientes conclusiones.

El objetivo principal fue satisfactoriamente cubierto, ya que de acuerdo con lo planteado en el capítulo 1, se logró el diseño e implementación de un Dispositivo capaz de bloquear toda operación de teléfonos móviles con tecnología 2G y 2.5G.

Por otra parte, con respecto al objetivo particular planteado, el cual consistía en registrar el comportamiento de un móvil de 3G frente a la operación del Jammer, se obtuvo que, al monitorear el comportamiento de un teléfono móvil de 3G dentro de la zona de cobertura del Jammer, el efecto de éste ultimo respecto a dicho dispositivo móvil fue prácticamente nulo.

Los anteriores resultados se deben a que:

- En el primer caso, recordemos que el Jammer fue diseñado para cubrir la banda de los 1900 MHz. Por tal motivo, no se tuvo ningún inconveniente en bloquear teléfonos con tecnología 2G y 2.5G. Ya que, si bien existen diferentes sistemas (CDMA o GSM) operando en distintas bandas del espectro radioeléctrico alrededor del mundo, como son: la banda 800, 900,

1800, 1900 o 2100. En México, para telefonía celular, solo están permitidas utilizar las bandas 800, 1800 y 1900. Y en específico hablando de los sistemas de 2G o 2.5G, estos operan en la banda 1900.

- En el segundo caso, tal como se mencionó, no se tuvo realmente un bloqueo para 3G. Esto se debe a que, a los teléfonos móviles de 3G se les asignó una nueva banda de frecuencia para su operación, diferente a la de 2/2.5G. No obstante, estos teléfonos son capaces de operar tanto en la red 2G como en la red 3G, es decir, pueden operar tanto en una banda de frecuencia como en la otra. De tal manera que originalmente un teléfono de 3G viene pre configurado para identificar la red en la que se encuentra y cambiar automáticamente entre las bandas de 2G y 3G. En base a lo anterior, el Jammer no bloquea los dispositivos con tecnología 3G puesto que solo interfiere en una banda (la banda 1900), dejando disponible la otra banda.

Hablando específicamente de México, la banda adoptada para servicios de 2G es la banda 1900, en tanto para 3G se ha adoptado la banda de los 850 y no la de 2100 MHz como por algún momento se llego a pensar. Esto es a consecuencia de diferentes estudios, los cuales revelaron que la banda 850, en México, representa mejor capacidad de enlace y la mejor percepción de cobertura.

Por otra parte, continuando con el análisis de los resultados de bloqueo en 2/2.5G. Tocamos el tema del tiempo de respuesta. Este tiempo de respuesta es considerablemente bueno, comparado con los 2 trabajos anteriores que se tienen como antecedente, en los cuales los tiempos llegaban a alcanzar hasta 90 segundos (1 ½ minutos). Así mismo, cabe mencionar que conforme mejor equipado esté el dispositivo para trabajar con otras bandas alterna, más complicado es el bloqueo, ya que al salir aparentemente del área de cobertura de una banda, intenta conectarse a otra, siempre y cuando el sistema se encuentre

también operando en esta segunda banda. Esto se demuestra en la tabla 6.1 donde se aprecia que el móvil que mayor presentó resistencia fue el tiene capacidad para soportar la red UMTS (3G).

Celular	Tiempo de Bloqueo	BANDAS DE OPERACIÓN
Nokia 5310	29 s	UMTS / GSM 850/900/1800/1900
Sony Ericsson Z520a	22 s	**GSM 850/900/1800/1900**
Nokia 2600	19 s	**GSM 900/1800**

Tabla 6.1 Tiempos de respuesta respecto a complejidad del Dispositivo Móvil

6.2 TRABAJO A FUTURO

Existen diferentes aspectos en los que este proyecto puede ser mejorado, enfocados principalmente a:

- Económica
- Simplicidad
- Magnitud y Alcance del proyecto

En la parte económica, se tiene por ejemplo que, en vez de utilizar el circuito XR2206 (el cual es un generador de funciones) sería una buena alternativa utilizar en su lugar un integrado que nos brinde únicamente la señal que queremos, ya que a pesar de que el XR2206 presenta algunas otras funciones interesantes, no son realmente relevantes para lo que finalmente se desea, es decir, generar únicamente una onda triangular a cierta frecuencia. Para lo cual serviría bien por

ejemplo el Amplificador Operacional (OPAMP) LM358, el cual es un Circuito integrado doble, justo lo que se necesita para configurarlo en retroalimentación y generar de esta manera una onda triangular. Con lo cual se estaría reduciendo el costo real de un 100% hasta un 7.14%, considerando que el precio del XR2206 es de alrededor de $70.00 y el de un LM358 es de aproximadamente $5.00. Además de que el encapsulado es más compacto y ocupa menos espacio.

Por otra parte, en cuestiones de simplicidad, también en la parte del offset podría trabajarse con un OPAMP, ya que es más fácil sujetar la señal a un nivel de DC, y no solo eso, sino que también se estaría amplificando dicha señal a niveles mayores a los obtenidos con el 2N2222, sin que la señal se vea distorsionada a la salida. Entonces, en cuestión de simplicidad un OPAMP en esta parte sería muy útil, ya que presenta una muy alta ganancia y en consecuencia una excelente amplificación. Así mismo, basta con introducir en una de sus entradas (Inversora o No Inversora) la señal deseada y en la entrada restante un voltaje de DC, el cual representará nuestro offset sin requerir mayor configuración. Dicho en otras palabras, a la señal original se le sumará o restará el nivel de DC presente en la otra entrada. Esto es gracias a que si recordamos, un OPAMP es básicamente un amplificador de diferencia (Es decir, amplifica la diferencia de potencial existente en sus entradas Inversora (-) y No inversora (+)).

Concluyendo los puntos anteriormente expuestos, si se pudiera englobar la parte de oscilación y la de offset, se resumiría todo a un OPAMP cuádruple como el LM324. Con lo cual se englobaría tanto la parte económica como la simplicidad. Además, las dimensiones del circuito físico se reducirían en gran medida.

Por último, en cuanto a las dimensiones y alcance del proyecto. Se especula que puede mejorarse en 3 aspectos principales: las tecnologías que se bloquean, el tiempo de respuesta y el área de cobertura.

En el primer punto, lo primordial es disponer antes que nada, de la información clara y concisa. Ya que, tomando como ejemplo este trabajo, existió desde el inicio mucha incertidumbre al respecto de las frecuencias sobre las cuales están operando las compañías telefónicas en sus redes 3G. Factor que fue determinante en el diseño final del Jammer, y en consecuencia de los objetivos logrados. Ya que tratándose de tecnologías relativamente nuevas en México, no existe un fácil acceso a la información oficial. A tal grado de que se llegó a pensar que las redes estarían operando en la banda de los 2100 MHz, información que fue descartada posteriormente al indagar más a fondo y descubrir que en realidad operan en la banda 850 MHz. Por tanto, si lo que se quiere es bloquear específicamente las redes 3G en México. Se debe de reconfigurar el funcionamiento del Jammer para operar en la banda 850. Para lo cual, el VCO utilizado no sería útil ya que este abarca desde 1370-2000 MHz y la de 850 MHz queda fuera de su rango. Aunque lo ideal sería un Jammer que realice un barrido en frecuencia tanto en la banda 850 (3G), como en la banda 1900 (2G, 2.5G).

Recordemos que los dispositivos móviles de tercera generación ya vienen equipados para trabajar en ambos rangos del espectro y reconocer cualquiera de las 2 bandas ya que funcionan de forma complementaria. Entonces pudiera pensarse en la utilización de un doble VCO en un mismo Jammer, o en dado caso que existiese un Circuito VCO capaz de abarcar tan amplio espectro (lo cual es complicado, ya que la mayoría de estos trabajan en rangos no tan amplios), y hacerlo conmutar en ambas bandas controlado por algún dispositivo microcontrolador compartiéndolo en tiempo o simplemente realizar un barrido en toda la extensión de dicho espectro (nuevamente, en caso de que existiera un VCO con estas características).

En el segundo punto, dentro la magnitud y alcance, se puede mejorar también en los tiempos de respuesta del Jammer. Ya que por ejemplo en México, GSM

trabaja de 1850-1910 MHz para el enlace de móvil a estación base (uplink) y de 1930-1990 MHz para el enlace de estación base a móvil (downlink). Y considerando que el barrido se realizó desde 1900 MHz y no desde los 1850 MHz, entonces en todo momento de la operación del bloqueador influyó únicamente al canal de de bajada (Downlink), aumentando el retardo en el bloqueo. No obstante, dichos tiempos de respuesta también se ven afectados por ciertos parámetros como la frecuencia a la cual opera el VCO, es decir, la velocidad a la cual barre toda la banda, y la cual está determinada por la frecuencia de la onda triangulara que entrega los voltajes al VCO. Además de que también es imprescindible tomar en cuenta las técnicas de acceso que utilizan cada móvil dependiendo de la generación a la cual pertenecen, ya que el comportamiento de dichos móviles depende de si acceden mediante saltos de frecuencia o mediante espectro disperso.

Finalmente, el área de cobertura. Este último punto involucra mucho más análisis. Primero, como se ha venido mencionando ningún civil está autorizado a invadir o impedir la comunicación en frecuencias que están licitadas o autorizadas a terceros, y si a esto le sumamos un área mucho mayor, se tendría que ver justificada y aprobada por las autoridades correspondientes. Además de la parte legal, también involucra una serie de análisis a nivel Ingeniería para implementar etapas de potencia y arreglos de antena, dependiendo de modelos de propagación, atenuación y patrón de radiación requerido.

Una vez expuesto cada uno de los puntos relevantes que se consideran que pueden ser desarrollados para mejora del proyecto, se deja a consideración de quien se encuentre interesado en realizarlo.

APENDICE A
LEGISLACION DE JAMMER EN MEXICO

Comencemos citando, antes que nada, que conforme a la Ley Federal de Telecomunicaciones, en su Capítulo I, Articulo 2.

> En todo momento el estado mantendrá el dominio sobre el espectro radioeléctrico y las posiciones orbitales asignadas al país.

Seguido a esto, es importante saber cuáles son las bandas de frecuencias con las que se está tratando. Lo anterior viene redactado en el Capítulo II, Articulo 10 de dicha ley, y la cual se menciona a continuación:

> Articulo 10. El uso de las bandas de frecuencias del espectro radioeléctrico se clasificara de acuerdo con lo siguiente:
>
> I. Espectro de uso libre: son aquellas bandas de frecuencias que pueden ser utilizadas por el público en general sin necesidad de concesión, permiso o registro.
>
> II. Espectro para usos determinados: son aquellas bandas de frecuencias otorgadas mediante concesión y que pueden ser utilizadas para los servicios que autorice la secretaria en el titulo correspondiente;
>
> III. Espectro para uso oficial: son aquellas bandas de frecuencias destinadas para el uso exclusivo de la administración publica federal, gobiernos estatales y municipales, otorgadas mediante asignación directa.

IV. Espectro para usos experimentales: son aquellas bandas de frecuencias que podrá otorgar la secretaria, mediante concesión directa e intransferible, para comprobar la viabilidad técnica y económica de tecnologías en desarrollo tanto en el país como en el extranjero, para fines científicos o para pruebas temporales.

V. Espectro reservado: son aquellas bandas de frecuencias no asignadas ni concesionadas por la secretaria.

Además, de acuerdo al capítulo III, Artículo 11. En uno de sus puntos se expone que:

> Articulo 11. Se requiere concesión de la secretaria para:
> **Usar, aprovechar o explotar una banda de frecuencias en el territorio nacional, salvo el espectro de uso libre y el de uso oficial.**

Entonces, basados en los puntos anteriormente expuesto. Al hacer uso de un jammer se estaría incurriendo en faltas graves a la ley Federal de Telecomunicaciones. La cual sancionará al/los involucrados de acuerdo a como lo establece en su capítulo IX, el cual consta de los artículos 71, 72, 73 y 74. Los cuales, para fines de esta tesis serán resumidos haciendo mención solo en algunos de sus puntos, como sigue.

> Articulo 71. Las infracciones a lo dispuesto en esta ley, se sancionaran por la secretaria de conformidad con lo siguiente:
>
> A. Con multa de 10,000 a 100,000 salarios mínimos por:
>
> I. Prestar servicios de telecomunicaciones sin contar con concesión por parte de la secretaria.

II. No cumplir con las obligaciones en materia de operación e interconexión de redes públicas de telecomunicaciones;

III. Ejecutar actos que impidan la actuación de otros concesionarios o permisionarios con derecho a ello.

IV. Interceptar información que se transmita por las redes publicas de telecomunicaciones.

Para los efectos del presente capitulo, se entiende por salario mínimo, el salario mínimo general diario vigente en el distrito federal al momento de cometerse la infracción.

Articulo 72. Las personas que presten servicios de telecomunicaciones sin contar con la concesión o el permiso a que se refieren los artículos 11 y 31 de esta ley, o que por cualquier otro medio invadan u obstruyan las vías generales de comunicación respectivas, perderán en beneficio de la nación los bienes, instalaciones y equipos empleados en la comisión de dichas infracciones.

Articulo 73. Las sanciones que se señalan en este capitulo se aplicaran sin perjuicio de la responsabilidad civil o penal que resulte o de que, cuando proceda, la secretaria revoque la concesión o permiso respectivos.

Por otra parte, independientemente de la posible sanción del uso del jammer por incurrir principalmente en el Articulo 71, sección III, y el Articulo 72. También es importante mencionar la incertidumbre que se tiene acerca de los efectos del jammer sobre el cuerpo humano debido a los niveles de potencia radiada por el mismo. Para lo cual se tiene que:

Las potencias emitidas por los teléfonos móviles son miles de veces inferiores a las de las antenas de los tejados pero su intensidad sobre el cuerpo humano es muy superior a la producida por ellas porque la distancia es pequeñísima.

Por otra parte, para ahorrar batería, la potencia emitida por un teléfono móvil se ajusta automáticamente al valor mínimo necesario, de manera que es más pequeña cuanta más cerca se encuentre de una antena receptora. Un móvil que esté cerca de una antena emite una potencia cientos de veces inferior a la suya máxima, la cual sólo se irradia cuando se encuentra a muy larga distancia o con muchos obstáculos físicos intermedios (garajes, habitaciones interiores de las viviendas, etc.) [A].

Pocas actividades humanas han despertado tan grande inquietud social. Debido a ello se han llevado a cabo vastísimos estudios examinando los informes médicos de millones de usuarios de teléfonos móviles. Al día de hoy la comunidad científica mundial está de acuerdo en que el único efecto de consideración sobre el cuerpo humano de las ondas empleadas en la telefonía móvil es térmico, igual al producido por las ondas de los hornos microondas pero en muchísima menor cantidad (un teléfono móvil emitiendo a su máxima potencia ocasiona en la zona cercana del cerebro un aumento de tan sólo 0.1 ℃, cuando el cerebro de manera natural tiene una fluctuación diaria de temperatura mucho mayor).

A continuación se muestra una tabla con los niveles típicos de transmisión de potencia tanto en telefonía. Así como en algunos otros sistemas, únicamente con el fin de realizar una comparación.

NIVEL	POTENCIA	DESCRIPCION
80 dBm	100 KW	Potencia típica de transmisión de una estación de radio FM con un rango de 30-40 millas.
60 dBm	1 KW	Radiación típica combinada de RF de un horno de microondas.
40 dBm	10 W	Potencia entregada a las antenas de telefonía móvil.
33 dBm	2 W	Máxima salida de potencia para un teléfono celular UMTS/3G (Potencia de teléfono clase 1)
30 dBm	1 W	Fuga RF típica de un horno de microondas. Máxima salid de potencia para un teléfono celular GSM 1800/1900.
27 dBm	500 mW	Potencia típica de transmisión de un teléfono celular UMTS/3G (Potencia de teléfono clase 2)
24 dBm	250 mW	Máxima salida de potencia para un teléfono celular UMTS/3G (Potencia de teléfono clase 3)
21 dBm	125 mW	Máxima salida de potencia para un teléfono celular UMTS/3G (Potencia de teléfono clase 4)

Tabla A.1 Niveles típicos de transmisión de potencia

La clase en que entra un móvil en particular se determina por el tipo de teléfono que es y cuanta potencia de transmisión es capaz de producir.

APENDICE B

DISEÑO PCB DE JAMMER

Primero que nada, cabe destacar que el diseño (layout) del PCB fue realizado con ayuda de la herramienta de simulación de circuitos denominada NI Multisim (versión 10), de National Instruments (Figura B.1). Ya que, con esta herramienta se diseñó el diagrama eléctrico completo del circuito del Jammer, y se conectaron todas sus partes, incluyendo las que no son posibles simular pero que físicamente resultan imprescindibles para el funcionamiento del dispositivo. Como por ejemplo el circuito integrado del VCO y del XR2206, los cuales no fue posible simularlos, pero físicamente deben de estar en la placa. Por ello se sustituyó ambos circuitos por algún equivalente con aproximadamente las mismas características físicas. Posteriormente el circuito fue transferido a la herramienta de diseño de PCB denominada NI Ultiboard (versión 10), también de National Instruments (Figura B.2). Mediante esta última, se realizaron las modificaciones necesarias a cada elemento, ya que muchos de ellos, a pesar de que pueden ser simulados, no corresponden con las medidas reales de los elementos físicos.

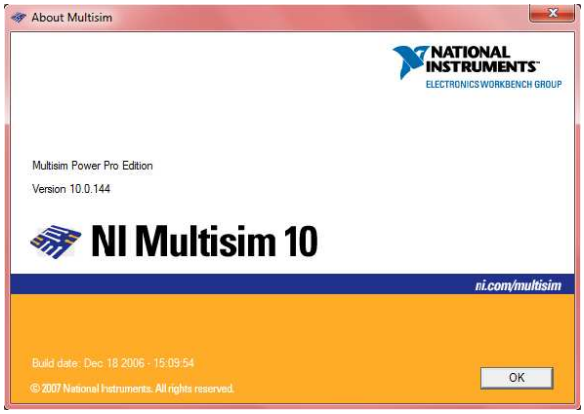

Figura B.1 Software de simulación

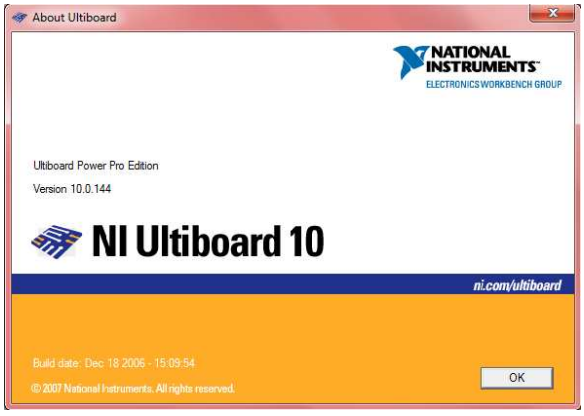

Figura B.2 Software de diseño PCB

- Diagrama eléctrico

Como bien se mencionó en el párrafo anterior, primero se realizó la conexión de todo el circuito del Jammer desde Multisim.

Aunque inicialmente se había propuesto realizarlo por partes, debido a la facilidad en el diseño del PCB, se optó finalmente por diseñarlo de tal modo que todas sus partes (fuente, generador, offset y VCO) quedaran reunidas en un mismo segmento de placa. De manera que, incluso la línea de transmisión coplanar utilizada quedó también impresa en el mismo circuito. Esto debido a que, se consideraron las posibles pérdidas, degradación o distorsión de la señal debido a la introducción de más conectores y acoplamientos.

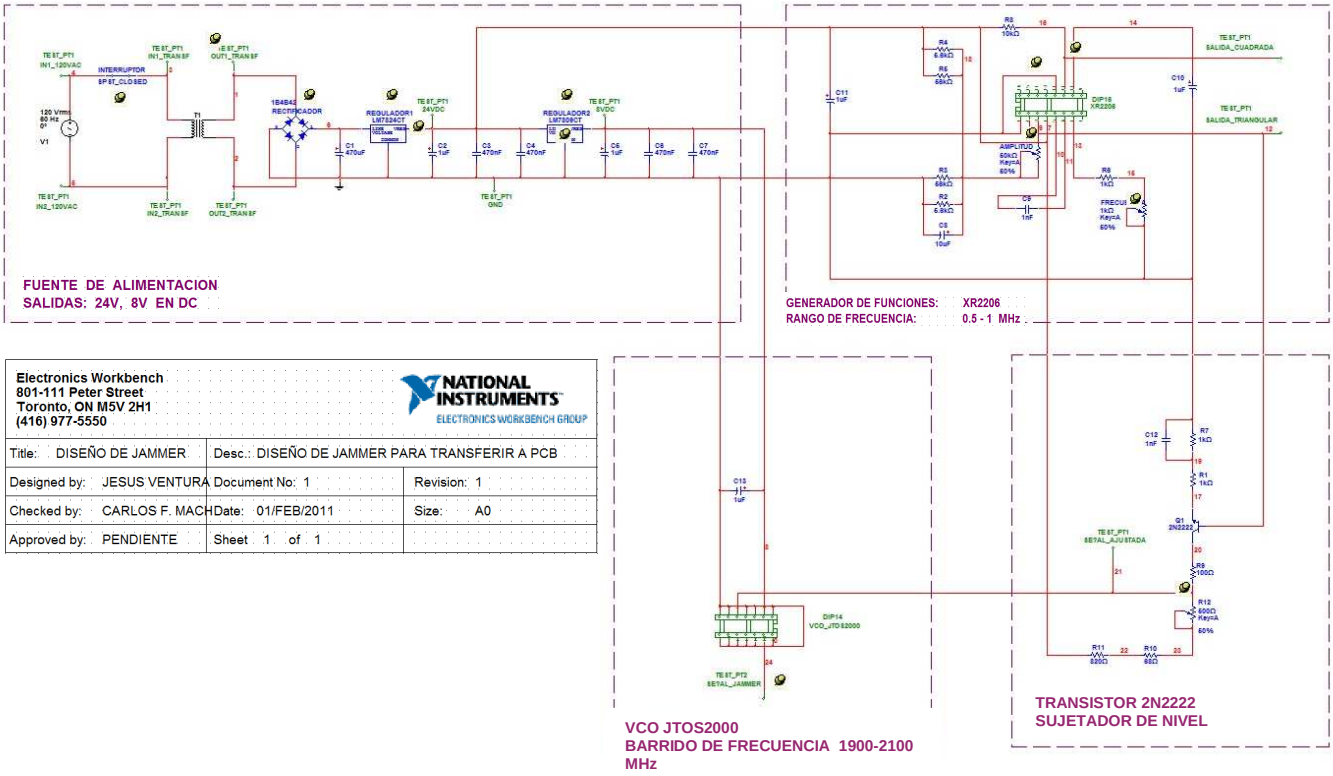

Figura B.3 Diagrama eléctrico del Jammer.

- PCB

Una vez que se finalizó el conexionado de todas las partes del Jammer mediante Multisim. Este fue transferido a Ultiboard desde la misma aplicación.

Realizado lo anterior, en primera instancia todos los componentes del circuito aparecen desordenados dentro de la aplicación de Ultiboard. En ese momento comenzó la segunda etapa, el diseño del PCB. Este diseño quedó finalmente como se muestra a continuación en la figura B.4, y su correspondiente visualización en 3D (Figura B.5).

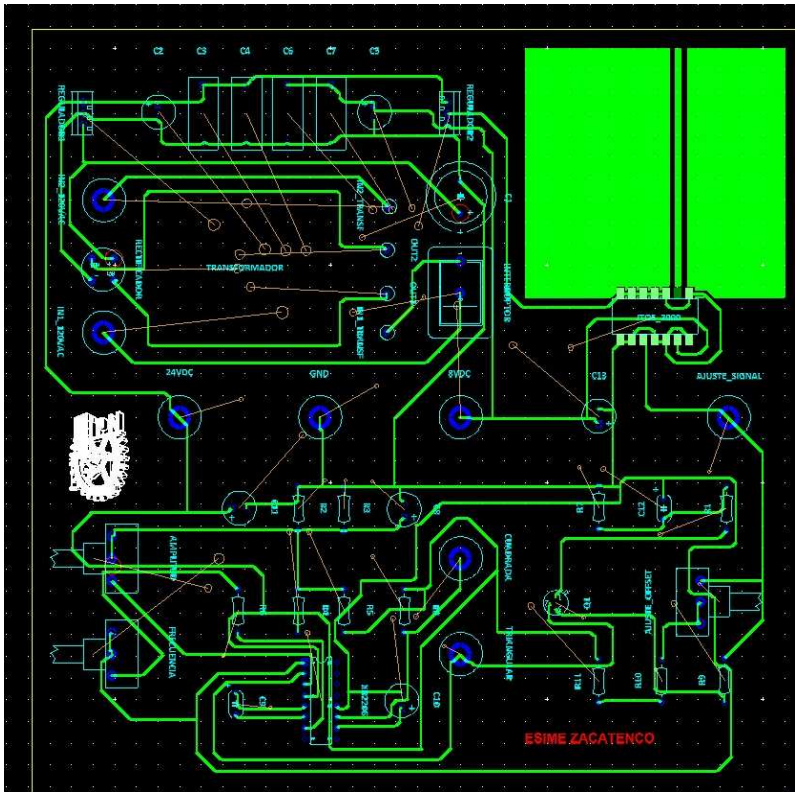

Figura B.4 PCB final del Jammer.

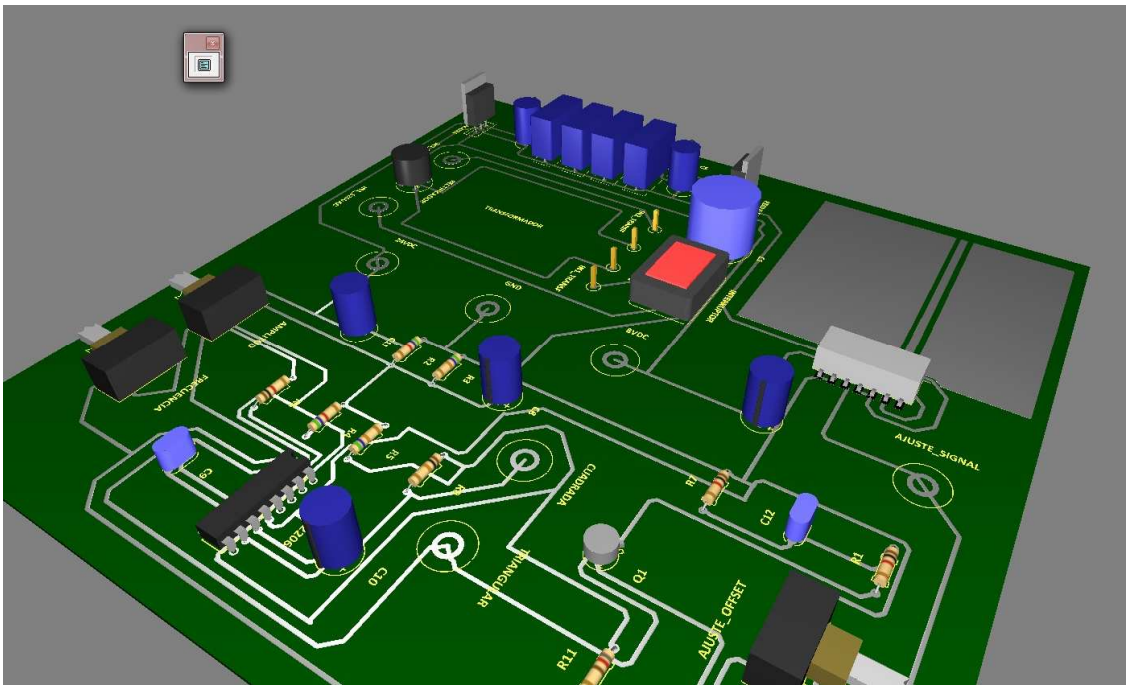

Figura B.5 PCB en 3D.

REFERENCIAS

[1] Tomasi, Wayne, *Electronic Communication Systems*, New Jersey: Prentice Hall 2001.

[2] Bernad Sklar; *Digital Communication: Fundamentals and Applications*; Prentice Hall; Second Edition.

[3] Tero Ojanpera and Ramjee Prasad; *Wideband CDMA for Third Generation mobile Communications*; Artech House.

[4] Theodore S. Rappaport, *Wireless Comunications principie and practice*, Prentice Hall

[5] M. Huidoro Jose, *Manual de Telecomunicaciones*, Alfa Omega.

[6] Cuevas Leon Miriam; *Materia: Redes convergentes*; Instituto Politécnico Nacional, 2010.

[7] Erick Mayoral Palacios; *Redes Inalámbricas de 2G, 2.5G y 3G*; Tesis Profesional;

[8] Miguel A. Valero & Carlos Ramo; *Tecnologia UMTS (parte I)*; Curso 2010
http://asignaturas.diatel.upm.es/ccmm/Documentacion.htm

[9] Jorge Parker Sanfuentes; Radar: *inicios de la electrónica*;
http://www.revistamarina.cl/revistas/2000/1/parker.pdf

[10] *ELECTRONIC WARFARE IN OPERATIONS*; FM 3-36
http://www.fas.org/irp/doddir/army/fm3-36.pdf

[11] Richard Poisel; *Introduction to Communication Electronic Warfare Systems*; Artech House

[12] David L. Adamy; *EW 103, Tactical Battlefield Communications Electronic Warfare*; Artech House

[13] *Cobertura GSM y 3G en Mexico*. http://www.gsmarena.com/network-bands.php3

[14] William H. Hayt, John A. Buck; *Teoria electromagnetic*; Mc Graw Hill.

[15] Rodolfo Neri Vela; *Lineas de transmision*; Mc Graw Hill

[16] *TXLINE 2003*; Microwave office; AWR.

[17] *SONNET,* High Frequency Electromagnetic Software.

[18]Boylestad Nasheslky; *Electrónica: teoría de circuitos y dispositivos electrónicos*; Pearson Prentice Hall.

[19] *Multisim* 10.0; National Instruments.

[20] Coughlin, Frederick, Driscoll, Robert; *Amplificadores Operacionales y Circuitos Integrados Lineales*; Prentice Hall.

[21] *Ultiboard 10.0*; National Instruments, Electronics WorkBench Group.

[A] *Ley Federal de Telecomunicaciones*; Última Reforma DOF 30-11-2010. http://www.diputados.gob.mx/LeyesBiblio/pdf/118.pdf

[B] *Bloqueo para telefonía celular DAMPS*, 2003. UPIITA, IPN; Disponible únicamente como Tesis impresa.

[C] José Manuel Nocedal de la Garza; *RF Jamming*; Universidad de las Américas Puebla; 2006

http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/nocedal_d_jm/index.html