PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DESARROLLO DE UN DISPOSITIVO *JAMMER* PARA EL BLOQUEO DE SEÑAL GSM

Tesis para optar el Título de Ingeniero de Telecomunicaciones, que presenta el bachiller:

Kristiam Eduardo Torres Ascencio

ASESOR: Dr. Manuel Yarlequé

Lima, junio del 2014

FACULTAD DE
CIENCIAS E INGENIERÍA

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO DE LAS TELECOMUNICACIONES

Título : Desarrollo de un dispositivo "jammer" para el bloqueo de señal móvil GSM

Área : Radio Frecuencia # 265

Asesor : Dr. Manuel Yarlequé

Alumno : Kristiam Eduardo Torres Ascencio

Código : 20062239

Fecha : 21/04/2014

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
Facultad de Ciencias e Ingeniería
23 JUN. 2014
DANIEL TORREALVA DAVILA
DECANO

Descripción y Objetivos:

La presente tesis tiene como finalidad el desarrollo de un dispositivo capaz de interferir las señales de los operadores móviles en lugares donde no se tiene permitido el uso de teléfonos móviles, puesto que en la actualidad no se tiene un óptimo control del uso de estos equipos en ambientes restringidos.

Este dispositivo está formado por un transmisor y una antena, el cual tiene por función generar señales interferentes en la banda de frecuencias de la señal móvil (banda de 850 MHz), con lo cual se llega a ocupar la banda de frecuencias destinadas a estos servicios.

La implementación de este dispositivo será de una manera práctica y eficiente, posibilitando el bloqueo en distinto tipos de locaciones como por ejemplo centros penitenciarios, zonas de seguridad, áreas de prueba, etc.

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
Especialidad de Ingeniería de las Telecomunicaciones
Ing. LUIS ANGELO VELARDE CRIADO
Coordinador

RESUMEN

La presente tesis consiste en el desarrollo de un dispositivo electrónico capaz de interferir las señales de los operadores móviles en lugares donde no se tiene permitido el uso de teléfonos móviles que operan en la banda GSM.

Después de presentar los conceptos teóricos concernientes a la radiofrecuencia, se presenta un análisis entre las diversas técnicas de *jamming* y los diferentes tipos de *jammer* con el fin de elegir la mejor opción para el desarrollo del dispositivo.

Posteriormente, se realiza el diseño por etapas del dispositivo y su correspondiente simulación de operación. Además se explica brevemente el proceso del desarrollo de la aplicación y se exponen los resultados obtenidos. Con ello se abarcan la parte del generador de funciones y el área de cobertura efectiva del bloqueador.

El dispositivo *jammer* desarrollado opera exitosamente de 0.5 a 1.7 metros a la redonda aproximadamente y toma de 30 a 35 segundos para bloquear completamente al teléfono móvil de cualquier interacción con la red celular GSM.

DEDICATORIA

Dedico está tesis a quienes desde mi niñez me han educado, cuidado y aconsejado para que cada día pueda ser una mejor persona, es decir mis padres Tula y Félix, el esfuerzo que han realizado, su apoyo, su dedicación del día a día, que han dejado en mi semillas de responsabilidad y madurez.

También dedico este trabajo a dos personas muy especiales, mis hermanos Paul y Sandy, espero que este proyecto sea de inspiración y ejemplo de que un sueño se puede cumplir con el esfuerzo propio y consejos de quienes te aman.

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, a la Pontificia Universidad Católica del Perú por brindarme los conocimientos necesarios y el equipo para el desarrollo de la tesis.

A mis dos asesores, al Dr. Manuel Yarlequé y al Ing. Luis Centeno, gracias por confiar y creer en mí, ya que sin su ayuda no hubiera sido posible el término de este proyecto final y lograr todos mis objetivos.

GRACIAS A TODOS.

INDICE GENERAL

ÍNDICE DE FIGURAS

CAPÍTULO 1 MARCO PROBLEMÁTICO Y FUNDAMENTOS BÁSICOS

CAPÍTULO 2 ESTADO DEL ARTE DE LOS CIRCUITOS DE BLOQUEO

CAPÍTULO 3 DISEÑO Y SIMULACIÓN DEL CIRCUITO DE BLOQUEO

ÍNDICE DE TABLAS

GLOSARIO

Acrónimo	Descripción
AE	Apoyo Electrónico
AJ	*Anti-jam*
AMPS	*Advanced Mobile Phone System*
ARTS	*American Radio Telephone Service*
BBN	*BroadBand Noise*
BER	*Bit Error Rate*
BSC	*Base Station Controllers*
BSS	*Base Station Subsystem*
BTS	*Base Transceiver Station*
CDMA	*Code Division Multiple Access*
CDMA	*Code Division Multiple Access*
DSSS	*Direct Sequence Spread Spectrum*
EA	*Enhanced Data Rates for GSM Evolution*
EP	*Electronic Protection*
ES	*Electronic Support*
EW	*Electronic Warfare*
FCC	*Federal Communications Commission*
FDMA	*Frequency Division Multiple Access*
FFH	*Fast Frequency Hopping*
FH	*Frequency Hopping*
FHSS	*Frequency Hopping Spread Spectrum*
GMSK	*Gaussian Minimum Shift Keying*
GPRS	*General Packet Switching Service*
GSM	*Global System for Mobile Communications*
iDEN	*Integrated Digital Enhanced Network*
IEEE	*Institute of Electrical and Electronics Engineers*
IMTS	*Improved Mobile Telephone System*
ISI	*Inter symbol linterferente*
ITU	*International Telecommunication Union*

JSR	*Jam-to-Signal Ratio*
LOS	*Line of Sight*
LPD	*Low Probability of Detection*
LPI	*Low Probability of Intercept*
MSC	*Mobile Switching Center*
MT	*Multiple-Tone*
MTS	*Mobile Telephone System*
NBN	*Narrow-Band Noise*
NSS	*Network and Switching Subsystem*
OLOS	*Out-of-Line-of-Sight*
OSS	*Operational Support Subsystem*
PBN	*Partial-Band Noise*
PDC	*Personal Digital Communications*
PDR	*Packet Delivery Ratio*
PSR	*Packet Send Ratio*
RF	Radiofrecuencia
SER	*Symbol Error Rate*
SFH	*Slow Frequency Hopping*
SIM	*Subscriber Identity Module*
SNR	*Signal-to-Noise Ratio*
ST	*Single-Tone*
TDMA	*Time Division Multiple Access*
USDC	*U.S. Digital Cellular*
VCO	*Voltage Controlled Oscilator*

INTRODUCCIÓN

GENERALIDADES

En el ámbito de los sistemas de telecomunicaciones, una onda electromagnética tiene como objetivo principal, facilitar la comunicación entre dos lugares distantes. No obstante, cuando se habla de una comunicación cuyo medio de transmisión es el aire, dicho fin puede verse distorsionado, puesto que estas ondas tienen la singularidad de que, una vez transmitidas, pueden llegar a ser interceptadas, bloqueadas o distorsionadas. Con este principio se da origen a la *Guerra Electrónica*.

La guerra electrónica tiene sus raíces en la segunda guerra mundial. Desde entonces se han fabricado dispositivos con eso propósitos. Debido a su origen militar, países como Estados Unidos, Israel y Japón se colocan primeros en el desarrollo de esta tecnología.

Hoy en día, debido a que el empleo de las tecnologías inalámbricas ha ido en crecimiento, el acceso a estas tecnologías se ha vuelto más fácil, y esto conlleva que se vuelva más fácil emplear dichas tecnologías de forma incorrecta. Por ende, en réplica a este mal uso de la tecnología, el interés por bloquear o interferir algunos dispositivos ha crecido también. En otras palabras, la guerra electrónica ha dejado de ser exclusivamente de dominio militar.

Uno de los principales dispositivos de tecnología inalámbrica usados en el ámbito civil, son los teléfonos celulares. Los cuales, están siendo usados por individuos inescrupulosos quienes atentan contra la seguridad y tranquilidad de los ciudadanos comunes. Es por eso que surge la necesidad de desarrollar dispositivos capaces de limitar el acceso a este medio. A estos dispositivos se les conoce como *jammers.*

Los *jammers* son equipos diseñados para bloquear la interacción de los teléfonos celulares mediante la emisión de una señal que interrumpe el proceso de comunicación entre el teléfono móvil y la estación base.

ANTECEDENTES

En la mayoría de los países el uso del dispositivo *jammer* sigue causando cierto debate. Debido que al bloquear las señales de telefonía celular, los *jammers* están interfiriendo con frecuencias que son propiedad ajena. Es decir, se interfiere a las frecuencias cuyas licencias pertenecen a operadoras de telefonía celular, y las cuales pagaron el derecho de utilizarlas.

No obstante, en algunos países como en los casos de Israel y Japón donde los dispositivos bloqueadores son completamente legales, existen otros que aún siguen siendo ilegales. Además de prohibida su venta y distribución.

En el caso de Perú, los *jammers* son completamente legales en algunos lugares como son en el caso de los reclusorios y/u otras entidades del estado. Ya que esto no significa que no viene a ser una invasión a la propiedad. Salvo este caso donde se tuvo que crear el Decreto Supremo N^0 012-2012-MTC. El cual establece lo siguiente:

“Regular la operación de equipos bloqueadores o inhibidores de señales radioeléctricas de los servicios de telecomunicaciones en los establecimientos penitenciarios que conforman el Sistema Nacional Penitenciario y en los Centros Juveniles de Diagnóstico y Rehabilitación y cautela el derecho de las personas a usar y prestar servicios de telecomunicaciones en los exteriores de estos establecimientos, de conformidad con las disposiciones emitidas en la presente norma”

OBJETIVOS

Para el desarrollo de la presente tesis. Se ha planteado como objetivo general y específico lo siguiente:

Objetivo general

Desarrollo de un dispositivo *Jammer* para el bloqueo de telefonía móvil GSM.

Objetivo específico

Registrar el comportamiento de un teléfono celular LTE dentro de una zona de bloqueo GSM.

Registrar el tiempo que le toma al dispositivo interferente en bloquear totalmente al teléfono móvil dentro de su área de cobertura.

Para cumplir con dichos objetivos, en primer lugar se deberá realizar una investigación de las características de los sistemas. En específico, se analizará la banda de frecuencias donde opera la señal GSM (dando énfasis a la banda de 850 MHz), para el caso de las señales móviles y la técnica de acceso múltiple que usan dichos sistemas.

Una vez que se haya recopilado toda la información acerca de los sistemas de telefonía móvil y dispositivos de acceso a la red, resultará importante el estudio y análisis de las técnicas de bloqueo o técnicas *jamming*, para adecuar dichas técnicas al presente asunto de estudio. Esto se logrará eligiendo una técnica *jamming* para realizar el diseño del dispositivo o *jammer* que empleará dicha técnica. Además, se realizará un exhaustivo estudio de los diferentes componentes electrónicos que nos servirán para llevar a cabo el desarrollo del circuito físico del dispositivo.

CAPÍTULO 1

MARCO PROBLEMÁTICO Y FUNDAMENTOS BÁSICOS

LA TELEFONÍA CELULAR

1.1 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 a cada usuario. Esto se realiza para poder transmitir información de manera correcta y eficaz; obteniendo así que ninguna asignación de tiempo o frecuencia no se desperdicie; de una manera que los recursos que se tiene se puedan compartir de manera equitativa.

Para la 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)

1.1.1 Acceso Múltiple por División de Frecuencia

Es una técnica de multiplexación usada en múltiples protocolos de comunicaciones, tanto en digitales como en analógicas, principalmente en radiofrecuencia y entre ellos en los teléfonos móviles de redes GSM. Además se basa en la división del ancho de banda de una línea entre varios canales, donde cada uno de los canales ocupa una porción del ancho de banda del total de la frecuencia. Adoptando las bandas de guarda como zonas de buffer para reducir la interferencia entre los canales vecinos y por la imposibilidad de realizar filtros ideales [1; 2]. (Ver figura 1.1).

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

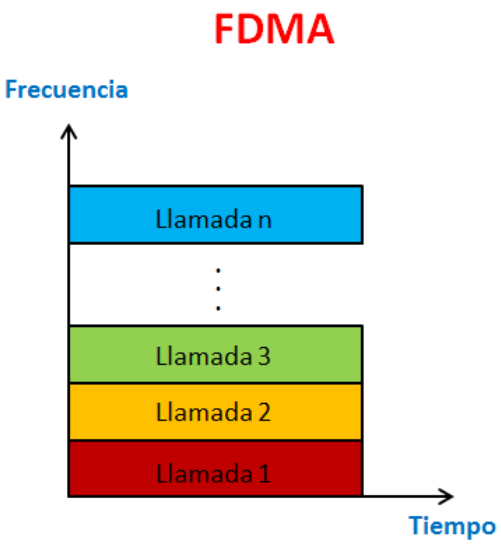

Figura 1. 1 Acceso múltiple por división de frecuencia [Fuente: Elaboración propia]

1.1.2 Acceso Múltiple por División de Tiempo

Es el método principal de acceso múltiple que se usa en la actualidad. Nos proporciona la forma más eficiente para transmitir portadoras moduladas digitalmente (PSK). En TDMA los usuarios comparten la misma frecuencia, pero transmiten en intervalos de tiempo disjuntos. De esta manera los usuarios son ortogonales en la dimensión temporal, y para separar la señal de interés de un usuario concreto basta escuchar el canal en el periodo de tiempo que está transmitiendo dicho usuario y omitir el resto del tiempo. Así, se define una trama como el periodo en el cual todos los usuarios del sistema han tenido la oportunidad de transmitir información, y las ranuras como los intervalos asignados a cada usuario.

También se define como la técnica que realiza una división en 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 a cada ranura de tiempo un espacio de guarda para evitar el traslape entre canales. (Ver figura 1.2) [1; 2].

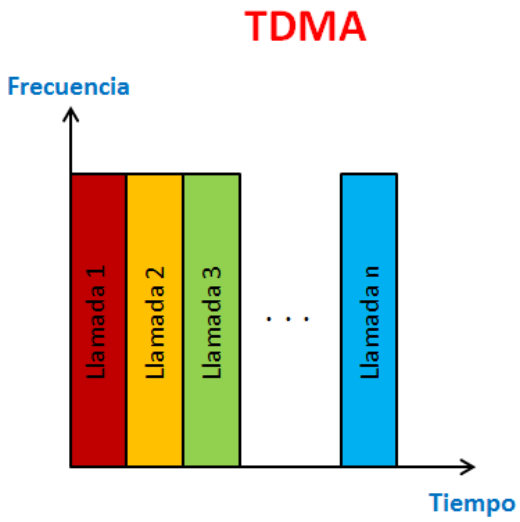

Figura 1. 2 Acceso múltiple por división de tiempo [Fuente: Elaboración propia]

1.1.3 Acceso Múltiple por División de Código

Es una técnica que 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 diferentes señales fuentes sean transmitidas al mismo tiempo, sobre la misma banda de frecuencia, además el uso de códigos permite que el receptor y el transmisor lleven a cabo una comunicación más eficiente y sin interrupciones o interferencias, por usuarios no deseados. [1, 2, 3]

CDMA permite acomodar una gran cantidad de usuarios en un periodo corto de tiempo. La figura 1.3 muestra el agrupamiento de N canales sobre un mismo intervalo de tiempo y frecuencia.

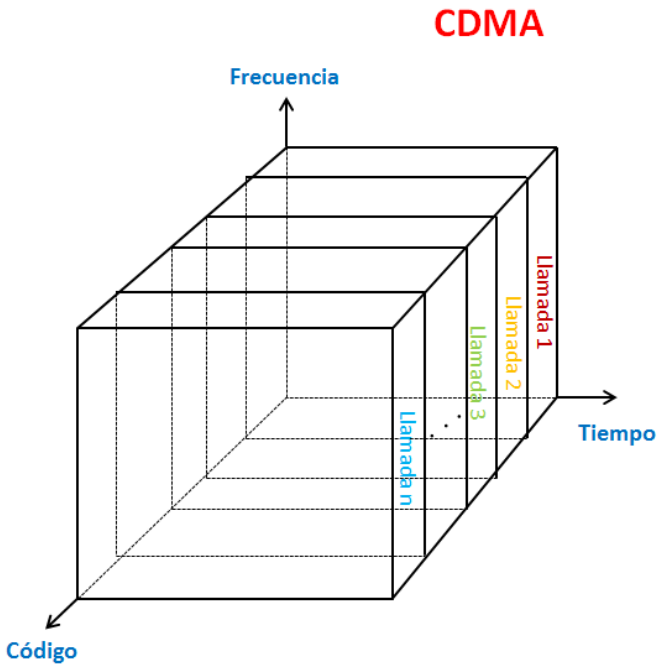

Figura 1. 3 Acceso múltiple por división de código [Fuente: Elaboración propia]

1.2 Espectro disperso

Es 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 este objetivo, que en un principio fueron desarrolladas para sistemas militares por su resistencia ante señales de interferencia y la baja probabilidad de detección. Los métodos son los siguientes:

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

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

- DSSS (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.

Para las redes móviles de 2G se hace utiliza FHSS y 3G por su parte utiliza DSSS, por lo cual se hará hincapié en estas dos formas de espectro disperso.

1.2.1 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 a otro de frecuencia. Durante el intervalo de tiempo Th, la señal portada permanecerá en una frecuencia específica, pasado este intervalo hará un salto a otra frecuencia portadora (ver figura 1.4). Los códigos de dispersión usados para estos cambios son llamados hopping code (códigos de saltos), estos códigos deciden los saltos en el rango de frecuencia. Estos rangos de frecuencia son llamados hop set. [4]

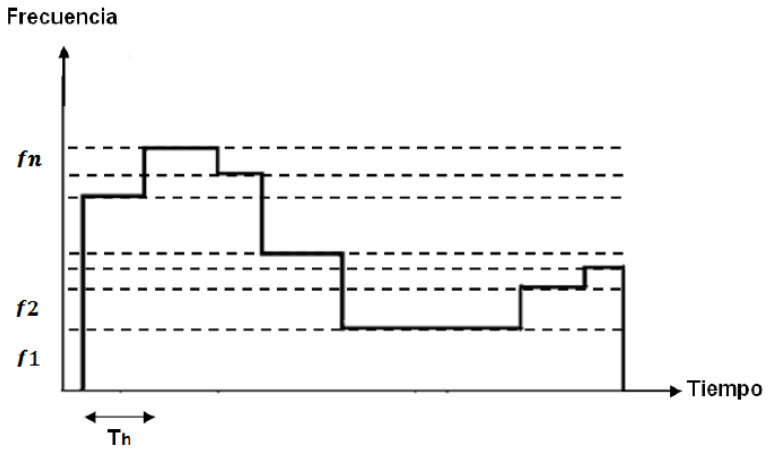

Figura 1. 4 Espectro disperso por saltos de frecuencia [20]

La velocidad a la cual la señal de portadora va a cambiar de frecuencia va a depender de la velocidad de símbolos con lo cual se tendrán un FHSS de dos tipos: F-FH (Fast Frecuency Hopping) y S-FH (Slow Frecuency Hopping).

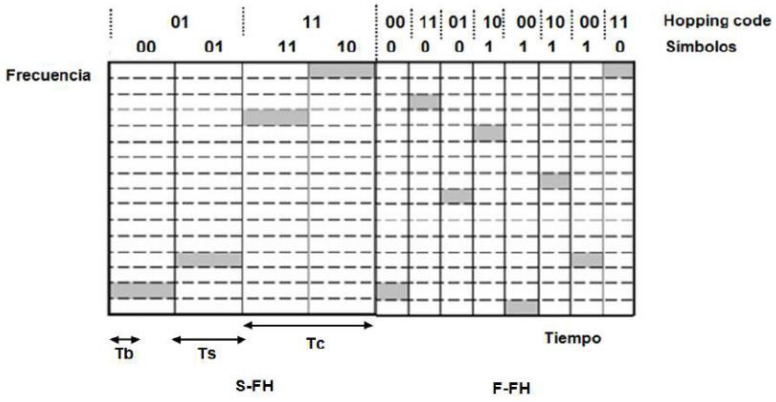

Figura 1. 5 FHSS Lento y FHSS Rápido [20]

En la figura 1.5 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 serán transmitido por dos portadoras diferentes. Por último, en la parte del receptor se contará con un sincronizador que en conjunto con el generador de código local permitirán que la señal se reciba

correctamente. En la figura 1.6 se muestra un diagrama de bloques de un sistema de FHSS [4].

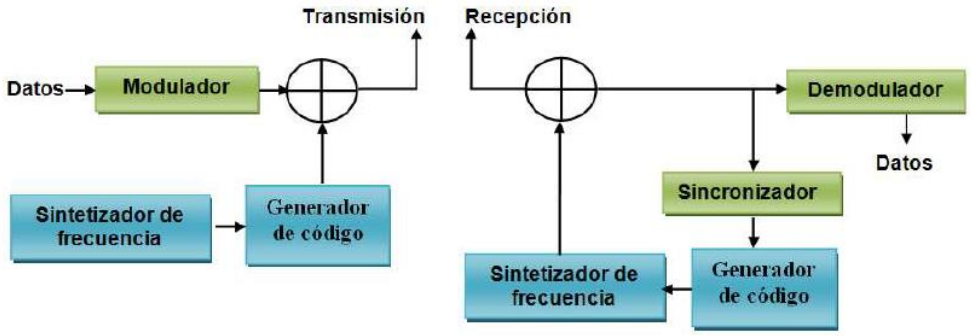

Figura 1. 6 Diagrama de bloques de un transmisor y receptor FHSS [3]

1.2.2 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 una velocidad de bit 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. Ver figura 1.7

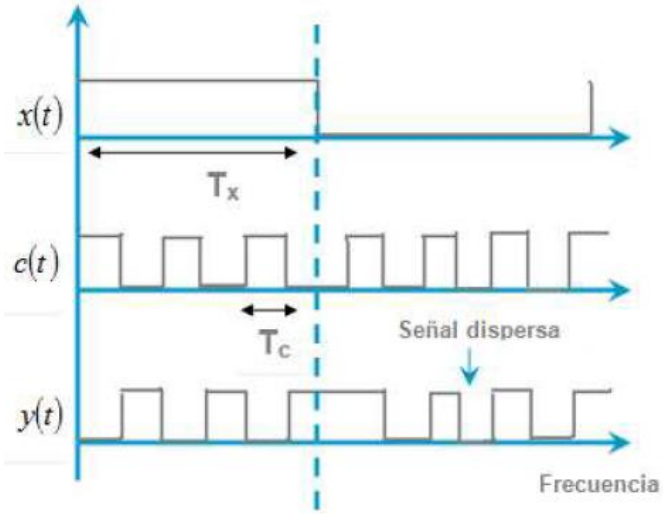

Figura 1. 7 Dispersión de una señal portadora [3]

En la figura 1.7 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.

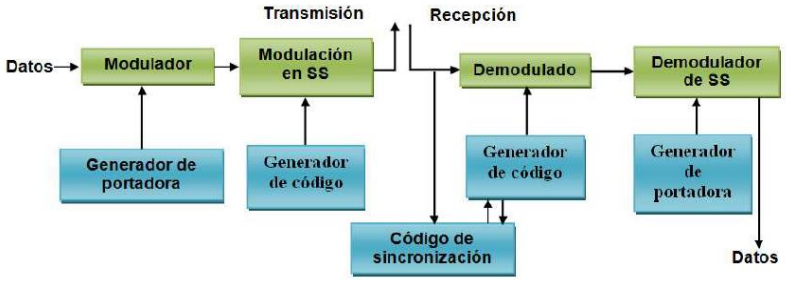

Figura 1. 8 Diagrama de bloques de un sistema DSSS [3]

1.3 Modos de transferencia

Existen dos modos de transferencia que son un requerimiento para las redes 2G y 3G las cuales son: Duplexaje por Division de Tiempo (TDD: Time Division Duplex) y Duplexaje por División de Frecuencia (FDD: Frecuency Division Duplex). En el TDD, las transmisiones de los enlaces ascendentes y descendentes son multiplexados en tiempo por la misma portadora en contraste al FDD en el cual las

transmisiones realizadas en los enlaces ascendente y descendente ocurren en frecuencias de bandas separadas.

En el modo de transferencia FDD hace uso de diferentes bandas de frecuencia entre el transmisor y el receptor, con esto se permite obtener grandes distancias entre el móvil y la BTS. En una red con cobertura nacional, esto es necesario para lograr requerimientos aceptables de cobertura mientra que el modo TDD solo es usada para distancias pequeñas; sin embargo, esto permite una mayor velocidad de transmision y flexibilidad para un tráfico asimétrico, tal como el uso de internet. Ver figura 1.9 [3].

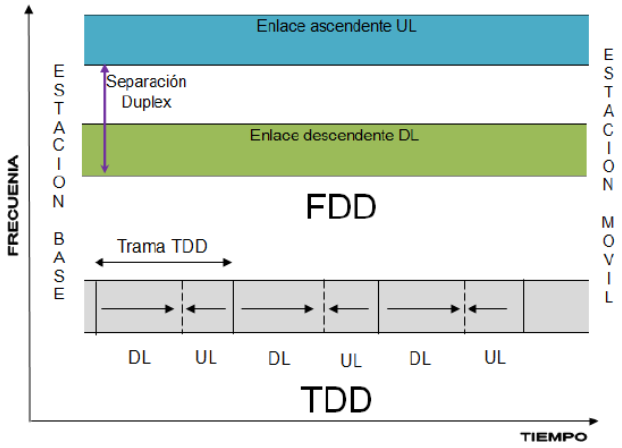

Figura 1. 9 Principio de TDD y FDD [3]

1.4 Evolución de la telefonía móvil

Un sistema de telefonía móvil se define como una red de comunicaciones a través de ondas de radio, que tiene la principal característica, permitir la movilidad contínua tanto el emisor como el 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 móvil en 1979, las comunicaciones móviles sin duda alguna han experimentado un gran crecimiento, desarrollando una diversidad de tecnologías y sistemas para brindar servicios de comunicación móvil. En general el desarrollo de los sistemas celulares en sus diferentes generaciones se ha dado como se indica en la figura 1.10.

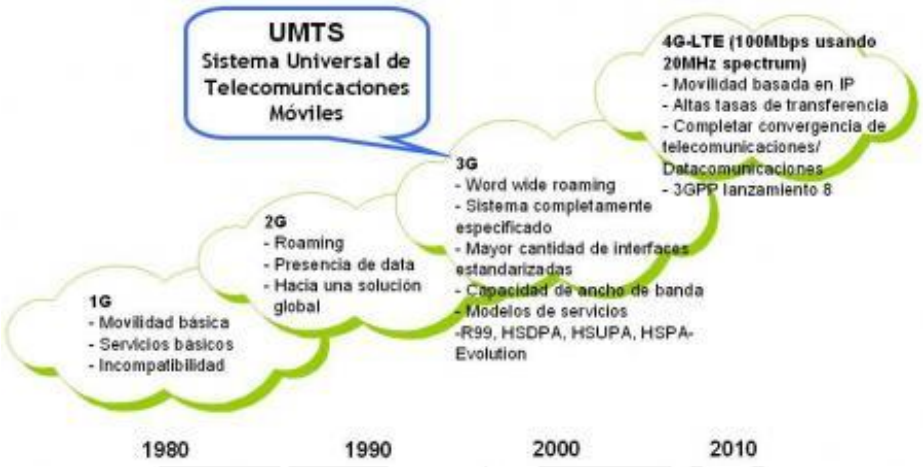

Figura 1. 10 Evolución en telefonía celular [16]

1.4.1 Primera generación

Los sistemas móviles de primera generación se caracterizaron por realizar trnasmisiones de tipo analógico de servicios de voz con niveles de baja calidad, utilizando para su funcionamiento la técnica FDMA o Acceso Múltiple por División de Frecuencia, lo que hacía a estos sistemas limitados en relación al número de usuarios a los que podía dar servicio. La seguridad no existía en estos sistemas.

La tecnología predominante de esta generación es AMPS (Advanced Mobile Phone System), desarrollada por los laboratorios Bell [5].

1.4.2 Segunda generación

La segunda generación se caracteriza especialmente por ser digital, lo que trajo consigo la reducción de tamaño, costo y consumo de potencia en los

dispositivos móviles, además de transmitir voz y datos digitales de volúmenes bajos.

Con los sistemas de telefonía celular de 2G se logró incrementar las velocidades de transmisión de información. Adicionalmente, con los sistemas 2G se logró avances significativos en cuanto a seguridad, calidad de voz y roaming.

Dentro del 2G se puede destacar los sistemas TDMA, GSM y CDMA.

TDMA: La multiplexación por división de tiempo es una técnica que permite la transmisión de señales digitales y cuya idea consiste en ocupar un canal de transmisión a partir de distintas fuentes, de esta manera se logra un mejor aprovechamiento del medio de transmisión.

GSM: Sistema global para las telecomunicaciones móviles. El Group Special Mobile fue el organismo que se encargó de la configuración técnica de una norma de transmisión y recepción para la telefonía europea. El estándar GSM fue desarrollado a partir de 1982, pero no fue hasta 1992 que las primeras redes europeas de GSM-900 iniciaron su actividad, y el mismo año fueron introducidos al mercado los primeros teléfonos celulares GSM, siendo el primero el Nokia 1011 en noviembre de ese año. Los sistemas de 2G GSM emplean una combinación de las técnicas de acceso múltiple FDMA y TDMA.

CDMA: En el año de 1992 la compañía Qualcomm desarrolló un sistema celular basado en la técnica de acceso múltiple CDMA, para posteriormente, en el año de 1993 ser modificado y adoptado por la TIA bajo el nombre IS-95, conocido también como CDMA One. En 1995 finalmente se realizó el lanzamiento del primer sistema comercial basado en esta tecnología en Hong Kong por parte del operador Hutchison Telecom [5].

1.4.3 Segunda generación y media

La generación 2.5G corresponde a mejoras tecnológicas en las redes 2G, las cuales se mencionan a continuación:

- HSCSD mejora el mecanismo de transmisión de datos.
- GPRS transmisión por paquetes se puede utilizar servicios WAP.
- EDGE es una evolución de GPRS.

Todas estas modificaciones con tendencia a entregar capacidades 3G con una velocidad que puede llegar hasta los 384 Kbps, ya adecuada para muchas aplicaciones en la transferencia de datos [5].

1.4.4 Tercera generación

Está basada en la familia de estándares de Unión Internacional de Telecomunicaciones (UIT) establecido en la IMT-2000. UMTS (Universal Mobile Telecommunications System) constituye uno de los miembros de esta familia de estándares IMT-2000. Entre los atributos de UMTS se puede destacar: la conectividad virtual a la red todo el tiempo, diferentes formas de tarificación, ancho de banda asimétrico en el enlace ascendente y descendente, configuración de la calidad de servicio (QoS), integración de la tecnología y estándares de redes fijas y móviles, entorno de servicios personalizados y muchos otros [5].

1.4.5 Cuarta generación

La 4G son las siglas de la cuarta generación de tecnologías de telefonía móvil. Es la sucesora de las tecnologías 2G y 3G, y que precede a la próxima generación, la 5G.

La 4G estará basada totalmente en IP siendo un sistema de sistemas y una red, alcanzándose después de la convergencia entre las redes de cables e inalámbricas así como en computadoras, dispositivos eléctricos y en tecnologías de la información, tales como con otras convergencias para proveer velocidades de acceso entre 100 Mbps en movimiento y 1 Gbps en reposo. Manteniendo una calidad de servicio (QoS) de punta a punta de alta seguridad que permitirá ofrecer servicios de cualquier clase en cualquier momento, en cualquier lugar, con el mínimo coste posible. En nuestro país ya existen redes 4G LTE implementadas por los concesionarios de Servicio Móvil [5].

1.5 Fundamentos de un sistema de telefonía celular

Dado que la presente tesis tiene por objetivo desarrollar un dispositivo bloqueador de 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.

1.5.1 Componentes

Un sistema de telefonía móvil, está formado por 4 partes:

- **Estación móvil (MS)**

  Es el equipo terminal (teléfono celular) 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 control durante la comunicación. Una estación base atiende a una o varias estaciones móviles, según el número de estas y el tipo de servicio.

- **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 las 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 1.11 se muestra los componentes mencionados en líneas atrás [15].

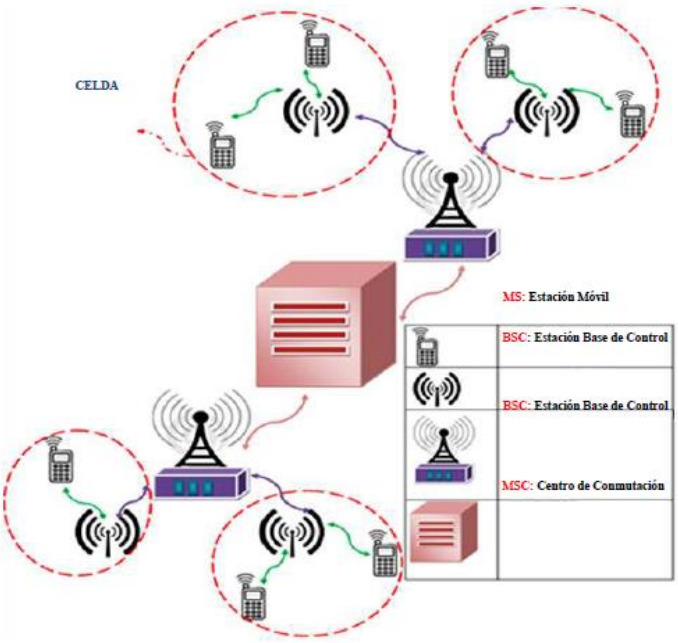

Figura 1. 11 Estructura general de una red de telefonía celular [16].

1.5.2 Elementos

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

1. **Celda**

Es una zona geográfica de cobertura por una estación base. Idealmente se representa por un hexágono que se une con otros para formar un patrón tipo enjambre que vendría hacer el patrón de cobertura total. La forma hexagonal fue elegida porque provee la transmisión más efectiva al aproximarla con una forma circular y permite unirse sin dejar huecos, lo cual hubiera sido posible al elegir el círculo. Una celda se define por su tamaño físico, pero más importante por la cantidad de tráfico y población que existe en ella [7].

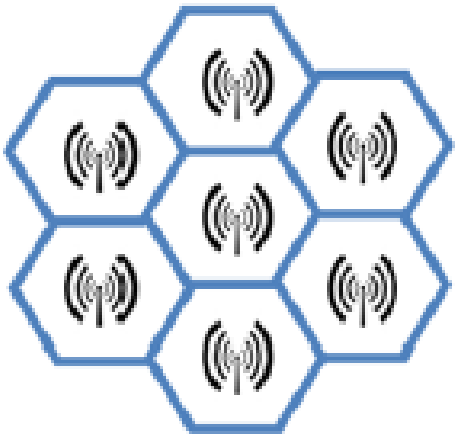

Figura 1. 12 Representación gráfica de una celda [16].

2. **Reúso de frecuencias**

Básicamente el reúso de frecuencias permite que un gran número de usuarios puedan compartir un número limitado de canales disponibles en la región. Esto se logra asignado el

mismo grupo de frecuencias a más de una celda. La condición para que esto se pueda hacer es la distancia entre ellas, de no hacerlo la interferencia seria alta. A cada estación base se le asigna un grupo de canales que son diferentes de los de las celdas vecinas y las antenas de las estaciones base son elegidas para lograr un patrón de cobertura dentro de la celda por medio de la modificación de ganancia y directividad [7].

3. 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 1.1 muestra los tamaños de las divisiones de las celdas [7].

Tabla 1. 1 Tipos de celdas y áreas de cobertura [5]

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

4. Transferencia de llamadas (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 1.2 se muestra los niveles de BER y la clase a la que pertenecen. La calidad de la voz es buena cuando el BER es menor a 1 y mala cuando es mayor a 3.

Tabla 1. 2 Márgenes de interferencia [5]

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	0.8 < BER

El proceso de Handover se lleva a cabo cuando el móvil mide los niveles de recepción de las estaciones bases 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 celdas adyacentes [7].

CAPÍTULO 2

ESTADO DEL ARTE DE LOS CIRCUITOS DE BLOQUEO

FUNDAMENTOS DE BLOQUEO

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 en el año de 1935, con los ingleses Arnold Wilkins, Percival Rowe y el escoces Robert Watson; los cuales realizarían la primera prueba de lo que hoy en día conocemos como radar.

Para el año de 1942, durante la Segunda Guerra Mundial, los alemanes implementaron un sistema receptor de radio dentro de sus submarinos, con lo que pudieron darse cuenta de cuando eran detectados por los radares del enemigo; posteriormente, este sofisticado equipo electrónico fue integrado en los aviones de combate, también se usó para la navegación en los bombarderos y detección de submarinos, así como otra gran cantidad de aplicaciones. Esto marcaría el inicio de la Guerra Electrónica [14].

2.1 Guerra electrónica

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

Hoy en día nuevas tecnologías se están expandiendo más allá del espectro de frecuencias de radio tradicional en las cuales se incluyen las 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) [14].

2.2 Ataque electrónico

El ataque electrónico, se puede realizar por medio de tres tipos de acciones o técnicas [6]:

1. Interferencia (*Jamming*)
2. Engaño
3. Radiación directa de energía

2.2.1 Técnica de *jamming*

El término *jamming* no posee una traducción acertada que englobe todo el concepto. En su más puro significado, *jamming* se define como aquella actividad que afecta la línea de tiempo en alguna comunicación [8; 10]. Es decir, logra que la información no llegue al receptor en el momento que debía de hacerlo. Al afectar esto, se afecta también la relevancia de la información. Esto se debe a que la información solamente es útil en determinado instante. No es útil si se recibe antes o después del tiempo establecido.

2.2.2 Técnica de engaño

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

2.2.3 Técnica de radiación directa de energía

La radiación directa de energía es la manera más fácil de atacar a un sistema de comunicación. Sin embargo, es la más fácil de detectar y poder evitar. Consiste en enviar una determinada señal con determinada potencia para dañar o destruir completamente la comunicación entre el receptor y el transmisor. La potencia emitida debe ser mayor a la que emplea el transmisor del sistema que está siendo atacado [10].

Un dispositivo capaz de emplear cualquiera de las tres técnicas o una combinación de ellas para interferir, dañar o destruir la transmisión de información dentro de un sistema electrónico de comunicaciones es llamado *jammer* [10].

De esta manera, el dispositivo que se encargue de seguir los tres puntos anteriores, se llamará dispositivo *jammer.* Sin embargo, los dispositivos *jammer* con el tiempo también surgieron como una alternativa a la prevención de ataques, como se verá más adelante.

2.3 Apoyo electrónico

El apoyo electrónico funciona como auxiliar. Su función es la medición de parámetros de interés en el sistema de comunicación [8]. Una de las razones principales de hacer esto radica en que si no hay señal que interferir no tiene caso gastar la potencia del *jammer* implementado. Sin embargo, dependiendo de la

aplicación será el tipo de *jammer* que se emplee. Es así que se puede mantener en operación un *jammer* por tiempo indefinido o se puede encender siempre y cuando se detecte una comunicación. Todo esto se verá más adelante cuando se analicen los distintos tipos de *jammers* que existen. Entre los parámetros que se encarga de medir el apoyo electrónico se encuentra [8; 10]:

- SNR (Signal to Noise Ratio). Determina la calidad con la que llega la señal al receptor después de recorrer la ruta del sistema de comunicación e ir contaminándose por ruido.

- JSR (Jam to Signal Ratio). Determina si la potencia con que transmite el *jammer* es mayor o menor que aquella que emplea el transmisor original del sistema [8].

- PSR (Packet Send Ratio). Relaciona los paquetes que fueron enviados correctamente por una ruta de tráfico con los paquetes que trataron de ser enviados fuera de la capa MAC [10].

- PDR (Packet Delivery Ratio). Compara los paquetes que llegaron al receptor con los que fueron enviados [10].

- BER (Bit Error Rate). Indica la fracción de bits que contiene o pudiera contener errores. Es decir, es la probabilidad de que un bit sea incorrecto. El BER se puede escribir también como Pc [8].

- SER (Symbol Error Rate). Es la probabilidad de que un símbolo sea incorrecto y se llega a escribir como Ps [8].

- SIR (Signal to Interference Ratio). Relaciona la potencia de la señal deseada con la potencia de la suma de la señales no deseadas [6; 9].

2.4 Protección electrónica

La protección electrónica consiste en el uso de estrategias para evitar los dos primeros elementos de la llamada “Guerra Electrónica”, es decir el ataque y el

apoyo. La codificación y la modulación entran dentro de este elemento [8]. Con la unión de modulación y codificación nacieron las comunicaciones *antijam* por sus siglas en inglés, *antijam*. Este tipo de comunicaciones tienen como objetivo evitar que un sistema externo pueda dañar, bloquear o interceptar la comunicación de otro sistema.

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 periodo 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 de los algoritmos de cifrado es la clave para lograr que esta técnica sea práctica y efectiva [11; 12].

2.5 Probabilidad de detección e intercepción

Estos términos se aplican a las muchas formas de procesamiento de señales con el fin de hacer lo más difícil posible el conocimiento de que la señal se encuentra presente o no sobre el rango de frecuencias a operar.

Para este tema de tesis se basará en las tecnologías de celulares móviles que abarque la señal GSM haciendo un hincapié en la banda de 850 MHz, las cuales

podrían interferir con el proceso de la antena construída, por lo que se tendrán en cuenta dos tipos de señales:

- Direct Sequence Spread Spectrum: Es un método de ensanchamiento del espectro, de tal manera que se pueda tener un ancho de banda mayor para una señal receptora. Es utiliza en los estándares de IS-95, y en nuestro país es usada por las nuevas tecnologías como UMTS.

- Frecuency Hopping Sprean Spectrum: Es un estándar que se utiliza para crear saltos de frecuencias, de manera que no se quede en un determinado rango de ellas todo el tiempo. Esta tecnología es usada por distintos tipos de telefonía, como GSM, además de ser la preferida para ocultar la frecuencia de transmisión y recepción. Existen dos tipos de saltos de frecuencia, las de alta y baja velocidad.

Después, para que un sistema sea considerado *Antijamin,* deben tener por lo menos una de las dos funciones a continuación:

- Baja probabilidad de detección (LPD - Low Probability of Detection): Donde el objetivo es lograr que la señal este lo más oculta posible. De esta manera, se puede usar DSSS para distribuir toda la señal en un rango determinado de espectro, de tal manera que la potencia es bastante más baja y se parezca al ruido. De esta manera, la detección de las señales será complicada o pasara desapercibida

- Baja probabilidad de interceptación (LPI - Low Probability of Intercept): En donde es posible detectar la señal, pero esta tendrá algún mecanismo de protección. Es aquí donde se usa el FHSS, pues logra la protección se logra cambiando de frecuencia constantemente.[12]

2.6 Estrategias de *Jamming*

Independiente, 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.

Hay varios tipos de estrategias para utilizar un ataque mediante una antena *jammer*, con lo cual solo se deberá elegir el objetivo a querer ser perjudicado. De esta manera, este tema de tesis solo se basará en las estrategias que se utilizará.

Lo que sí es un factor genérico en todas es sobre el tipo de señales que utilizan las antenas *jammer*. Estas deberán emitir una señal portadora en banda base que puede ser modulada por uno o más impulsos o bien por una señal de ruido [8].

Se tienen distintos tipos de técnicas:

2.6.1 *Jamming* por ruido

La portadora emitida por el *jammer* es modulada por una señal aleatoria de ruido [13]. El ruido que se introduce puede ocupar ya sea todo el ancho de banda empleado por la señal AJ, o simplemente una parte de él. Los efectos serán distintos pero se debe de considerar que no siempre se necesita atacar todo el ancho de banda para interrumpir de manera eficiente la comunicación. Estos tipos de ruido son:

- **Por banda completa**

  El ruido de banda ancha o BBN (Broadband noise) introduce energía a través de todo el ancho del espectro de frecuencias en el que opere la aplicación blanco. Su funcionamiento es elevando el nivel de ruido en el receptor lo que ocasiona un decremento en la relación SNR [8]. La eficiencia de este tipo de *jamming* depende del nivel de potencia y por tanto de la distancia entre el *jammer* y el receptor.

- **Por banda-parcial**

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

- **Por de banda-angosta**

Esta manera de generar *jamming* introduce energía en solamente un canal. El ancho de banda de esta energía podría abarcar todo el canal o simplemente una parte de él. Una vez más la diferencia radica en la potencia empleada y el espectro cubierto. La eficiencia de esta forma de *jamming* dependerá en parte del conocimiento de la aplicación blanco, esto es porque se debe de atacar el lugar exacto en el espectro en donde se encuentren los canales de interés. La potencia se puede canalizar toda a una pequeña parte del espectro, lo que representa una ventaja [8].

- **Por banda Parcial continua**

Este método introduce energía en dos anchos de bandas distintos. Puede tener funciones de querer interferir en dos o más sistemas distintos para su uso propio. Este tipo de inserción de ruido necesita una arquitectura más completa en el diseño de la antena *jammer* [12].

2.6.2 *Jamming* por tonos

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

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

El que se produzca una correcta interferencia dependerá en primer lugar de que el tono se coloque en una parte del espectro en donde exista un tono que represente un símbolo, en ese caso la JSR debe ser lo suficientemente alta; en un segundo lugar dependerá de que una vez que el tono del *jammer* esté en la frecuencia del tono del símbolo, la fase entre ellos sea igual. Este tipo de *jamming* es muy poco eficiente contra sistemas FH debido a que depende de que la señal salte a la frecuencia en la cual se ha colocado en tono emitido por el *jammer.*

Es por eso que si se utilizan tonos estos deben estar barriendo una parte del espectro y no estar en una frecuencia específica. Este es el caso de una estrategia de *jamming* posterior.

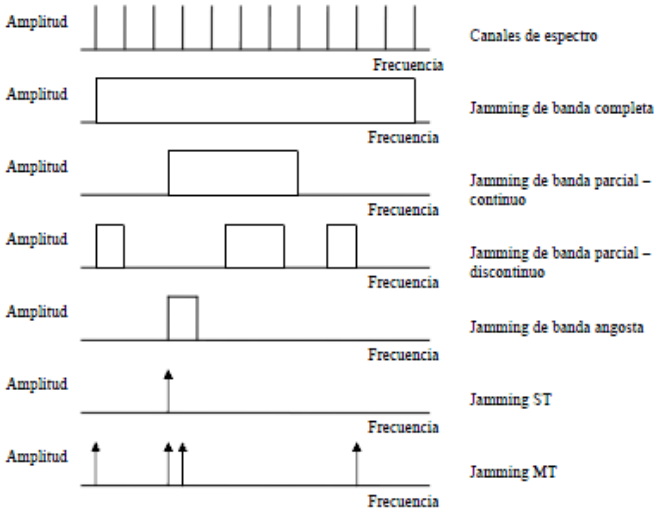

Figura 2. 1 Estrategias de *jamming* [8]

2.6.3 *Jamming* por pulsos

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

2.6.4 *Jamming* por barrido

Consiste en introducir ruido en un pequeña parte del espectro; y una vez colocada está señal, se realiza un barrido por todo el ancho de banda que ocupe la señal AJ. Esta estrategia se puede emplear en un sistema FHSS [7]. Sin embargo, un punto importante es que el barrido debe ser más rápido como para identificar la frecuencia en la que se encuentre la señal pero no lo suficiente como cuando se sitúe sobre el salto se tenga efecto leve, como parte de una señal con interferencia pequeña.

Para dar una idea de lo que involucra el barrido, se puede tomar el ejemplo del BER hipotético de 10^{-1}, lo cual querrá decir que se debería bloquear la transmisión de un bit de diez. Si la trasmisión la hace un sistema que está transmitiendo datos a una velocidad de 64 Kbps, la transmisión de 6400 bits debe ser bloqueada para alcanzar este BER. Si este sistema es de tipo SHF y maneja 100 saltos por segundo, cada salto contendrá 640 bits (sin considerar el tiempo entre saltos). De ahí que se necesite aplicar de manera exitosa sobre 10 saltos por segundo. Ya que estos saltos pueden estar en todo el espectro asignado, al menos 64 barridos por segundo son necesarios para que el *jammer* funcione.

Tiene una ventaja de potencia cuando no trabaja con sistemas de banda ancha, debido a que solo localizaría la frecuencia de transmisión y haría un barrido sobre esta. De esta manera habría un considerable ahorro de potencia [12].

2.6.5 *Jamming* por seguimiento

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

Sus principales limitantes al usarlo contra sistemas FH fueron determinadas por Torieri [26]. Estas limitantes están relacionadas con el tiempo de procesado del *jammer*. Esto se debe a que el proceso de *jamming* en este

caso comienza por conocer la frecuencia a la que ha saltado la señal. Esto se hace midiendo la energía en un punto se podría concluir que esa es la nueva frecuencia, aunque esto no es siempre cierto. Debido a la velocidad del salto de frecuencias es difícil averiguar el nuevo blanco.

Además de esto existen otros problemas. Si se aplica *jamming* al mismo tiempo en más de un canal, la potencia estará distribuida entre estos y probablemente no será suficiente para reducir la relación señal a ruido a un nivel donde no puede existir comunicación. Incluso las distintas modulaciones son un escudo ante esta estrategia [6; 8].

2.6.6 *Jamming* inteligente

Es común que cuando se aplica alguna estrategia de *jamming* sobre una señal *antijam*, se desperdician recursos y no siempre se elige la opción más adecuada. Cuando se conoce como funciona el sistema que se desea atacar, se pueden optimizar los recursos. Realmente el *jamming* inteligente no es una estrategia como las anteriores, sino que se refiere al estudio del blanco para lograr mejores resultados.

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

2.7 Técnica para incrementar la eficiencia del *jammer*

Una manera de incrementar la eficiencia de un *jammer* es incrementar el número de señales que puede bloquear o interferir simultáneamente. Esto es posible mediante algunas técnicas que involucran el compartir la potencia entre los

distintos blancos y el poder encender y apagar el *jammer* por determinado tiempo para dedicarlo a uno o a otro blanco.

2.7.1 Look-Through (Buscar)

Cuando las señales no son de espectro extendido, esta técnica es empleada para determinar si el blanco ha cambiado de frecuencia o simplemente ha dejado de operar. Esto se hace para no malgastar la potencia y de esta manera emplearla en más de un objetivo o simplemente ahorrarla. Al momento de apagar el *jammer* se mide la actividad en el espectro y se determina si el blanco está en funcionamiento o no. Podría pensarse como solución para sistemas FH y como una forma de *jamming* por seguimiento. Sin embargo, debido a la velocidad de salto no se emplea está técnica para tal propósito. Esta técnica se puede aplicar a sistemas DSSS siempre y cuando se pueda detectar su actividad [6].

2.7.2 Potencia compartida

Una manera de compartir la potencia entre dos o más blancos está representada por la estrategia de múltiples tonos. En esta estrategia de *jamming* los tonos se pueden colocar en diferentes partes del espectro sin necesidad de que los canales sean continuos para lograr atacar varios blancos [6].

2.7.3 Tiempo compartido

Otra técnica para cubrir más de un blanco, es orientar la máxima potencia del *jammer* a cada blanco pero en momentos distintos. Cuando se aplica *jamming* a una señal digital se tiene que estar todo el tiempo introduciendo ruido. Basta con incrementar el BER hasta cierto nivel. En el caso de las comunicaciones de voz el nivel necesario para cortar la transmisión es más alto que en el caso de datos. En el caso de las comunicaciones de voz analógicas es necesario bloquear o interferir solamente el 30% de la transmisión para que no entienda el mensaje. De ahí que el *jammer* pueda estar orientado a distintos blancos en diferentes momentos [6].

2.8 Clasificación general de *jammer*

De las estrategias de *jamming* se derivan cuatro tipos principales de *jammer*. La elección del tipo de *jammer* dependerá de la aplicación específica.

2.8.1 *Jammer* constante

Este tipo de *jammer* emplea la estrategia de ruido y la de barrido. Su principal ventaja es la relativa facilidad de implementarse. Sin embargo, en aplicaciones donde se desea que el *jamming* pase desapercibido no es recomendable emplear un *jammer* constante [10]. Esto debido a que excede los niveles de ruido y por tal motivo es fácil su detección, debido a que una vez encontrado el ruido es posible detectar la fuente que lo genera, otro inconveniente es que requiere mucha potencia.

2.8.2 *Jammer* de engaño

Emplea la técnica de engaño que pertenece al *jamming* inteligente. En este caso se envía señales que parecen ser legítimas, pero no se incluye una separación entre ellas. Esto ocasiona que se mantenga el estado de recepción y no haya confirmación de haber recibido información alguna [10]. Siendo una ventaja ser menos propenso a la detección pero aun en este tipo la potencia requerida es grande.

2.8.3 *Jammer* aleatorio

Este tipo de *jammer* funciona por determinado tiempo y deja de hacerlo por otro [10]. El ciclo de trabajo es programado de acuerdo a su aplicación. Se puede utilizar *jamming* por ruido, por pulsos, por tonos e incluso por barrido [8]. Su detección es posible realizando un análisis de la actividad de la red, mientras que la potencia requerida es menor debido a que no se encuentra en funcionamiento todo el tiempo.

2.8.4 *Jammer* reactivo

Este tipo es el más complejo pero es el que ofrece una menor posibilidad de ser detectado. Consiste en censar la actividad de la red para saber en qué momento debe de actuar el *jammer* [10]. Podría pensarse que el consumo de potencia es mínimo. Sin embargo, a pesar de no ser excesivo si se requiere determinada potencia para estar monitoreando la actividad de la red. Una vez que se detecta el envío de la señal, se realiza un *jamming* por ruido, por tonos o por pulsos.

CAPÍTULO 3

DISEÑO Y SIMULACIÓN DEL CIRCUITO DE BLOQUEO

3.1 Elección de la técnica de *jamming* y tipo de *jammer*

Luego de analizar las diferentes técnicas de *jamming* presentadas en este trabajo mediante comparaciones entre complejidad y beneficio se llegó a la conclusión de que la estrategia de barrido es la ideal.

Las demás se descartaron por las siguientes razones:

i. La estrategia de *jamming* por ruido:

- De banda ancha requiere mucha potencia y se tendrían que implementar numerosas etapas de ganancia para la antena. Además de incurrir en problemas legales.
- De banda parcial limitaría a cierta parte del espectro, entre 5 y 10 MHz.

- De banda angosta es fija y no nos ofrece el ancho de banda necesario.

ii. La estrategia de *jamming* por tonos no es efectiva ante sistemas que empleen *Frecuency Hooping* (FH).

iii. La estrategia de *jamming* por pulsos no sería efectivo por su ciclo de trabajo ya que se requiere que esté encendido todo el tiempo. En este caso el ahorro de potencia no es tan importante como si se tratase de un *jammer* portátil.

iv. La estrategia de *jamming* por seguimiento no es práctica por la complejidad en el diseño e implementación además de un largo tiempo para su fabricación.

La técnica de *jamming* por barrido se eligió debido a que se pretende utilizar toda la potencia disponible en cada parte del espectro y por momentos distintos. A pesar de que la velocidad tendrá que ser controlada por los saltos que maneja GSM, esto será posible mediante la definición de parámetros y pruebas constantes.

Para el tipo de *jammer* se eligió el de tipo constante. Se descartó el *jammer* aleatorio porque se desea que trabaje en todo momento, los demás no se eligieron debido a la complejidad que presentan cada uno de ellos, puesto que se pretende sencillez en el diseño.

3.2 Descripción del circuito

Para que un *jammer* utilice como estrategia el barrido, se debe implementar el circuito de la figura 3.1.

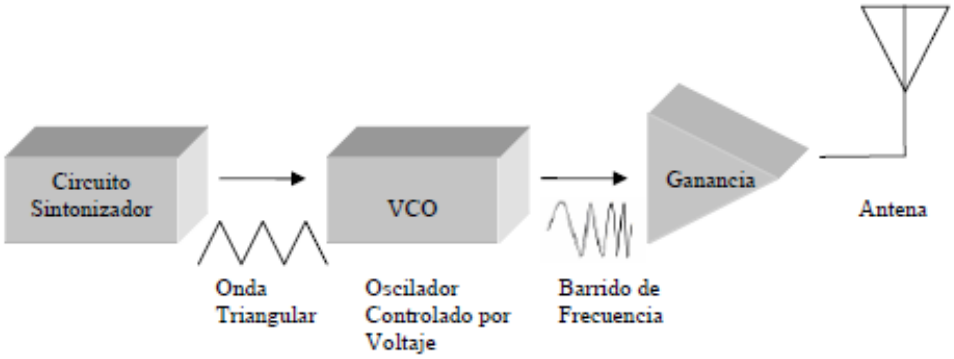

Figura 3. 1 Diagrama de bloques del *jammer* [9]

3.2.1 Generador de la señal triangular

Se optó por utilizar una señal triangular o diente de sierra debido a la sencillez para generarla. Porque simplemente necesitamos una señal que interfiera con la señal proveniente de la estación base (BTS).

Para generar la señal triangular optamos por los circuitos integrados TL0810P (amplificador operacional), el cual con las conexiones mostradas en la figura 3.2 generamos la señal triangular, además con esta serie de conexiones, la señal se puede modificar tanto en amplitud como en frecuencia.

La frecuencia de la señal triangular es muy importante debido a que la tecnología GSM es un sistema que emplea SFH (*Slow Frequency Hopping),* y de esta forma puede ser que con la frecuencia de la señal triangular se proteja a la comunicación de la interferencia generada por nuestro *jammer.*

Nos enfrentamos con dos problemas:

- Si la variación del voltaje sintonizador es muy lenta no se alcanzará a barrer una parte amplia del espectro de manera que se intercepten los saltos en frecuencia.
- Si la variación es muy rápida no será suficiente el tiempo que la señal del *jammer* interfiera con la señal original para imposibilitar la comunicación. Por lo tanto debemos ajustar el voltaje de la señal a un valor promedio.

A consecuencia, tenemos que ajustar la frecuencia en un valor medio para lograr el objetivo, que es bloquear la señal proveniente de la BTS.

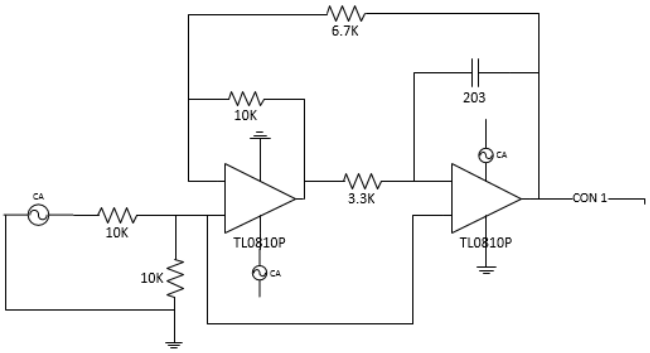

Figura 3. 2 Generador de Señal Triangular [Fuente: Elaboración propia]

3.2.2 Generador de Ruido

Para lograr que la señal interfiera con la señal proveniente de la BTS necesitamos mezclar ruido con la señal triangular, la señal que se obtiene será la que activará el VCO.

Para generar el ruido decidimos ocupar el circuito integrado TL0810P, que es un amplificador de baja tensión, y lo utilizamos para amplificar el ruido, el cual es generado por el diodo zener 1N5335, cuyo voltaje es de 9.4 V. El ruido es de avalancha causado, por el fenómeno de ruptura zener. El arreglo después del diodo zener, su función es acondicionar el ruido antes de ser amplificado. La configuración para obtener el ruido deseado se muestra en la figura 3.3.

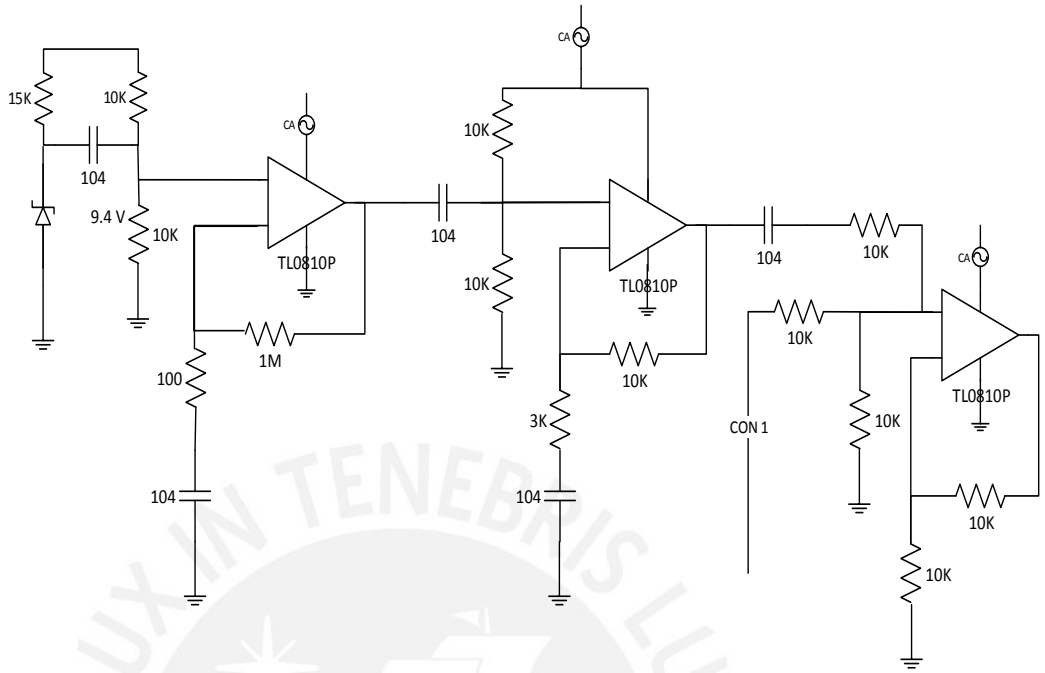

Figura 3. 3 Generador de Ruido [Fuente: Elaboración propia]

3.2.3 Oscilador controlado por voltaje (VCO)

Es el circuito más importante de nuestro proyecto, dado que este circuito es el que realizará el barrido de frecuencia. Decidimos ocupar el circuito integrado VCO JTOS - 1025 ya que con el logramos un barrido de frecuencia desde 650 MHz hasta 1025 MHz. La característica fundamental de este VCO es que está diseñado para aplicaciones de banda ancha. Lo que haremos es ajuste del barrido, a la frecuencia en 850 MHz que es la frecuencia en que los celulares trabajan en el Perú.

Este circuito debe tener una alimentación desde 0 hasta 12 V, y dentro de este rango debemos ajustar la tensión, para poder trabajar en la frecuencia de 850 MHz.

El barrido de frecuencia debe cubrir todas las compañías de telefonía celular, que operan en el Perú. En la siguiente tabla se observan las frecuencias asignadas.

Tabla 3. 1 Frecuencia GSM (Banda 850 MHz) para el Perú [16]

Compañía	Banda de frecuencias		Ancho de banda
	Segmento Inferior	Segmento Superior	
Telefónica Móviles S.A.	824 - 835	869 – 880	22 MHz
	845 – 846,5	890 – 891,5	3 MHz
América Móvil Perú S.A.C.	835 - 845	880 – 890	20 MHz
	846,5 - 849	891,5 - 894	5 MHz

3.2.4 Amplificador RF

Para alcanzar la potencia de salida deseada, etapas de ganancia era necesario, encontrar un amplificador que trabajará dentro de la frecuencia de 850 MHz.

El amplificador RF que se utiliza para esta parte del circuito fue el HMC450QS16G, el cual amplifica la señal saliente del VCO. El arreglo de conexiones que se muestra en la figura 3.4, se hizo para no tener pérdidas causadas por el acoplamiento. A la salida del amplificador va la antena que radiará la interferencia.

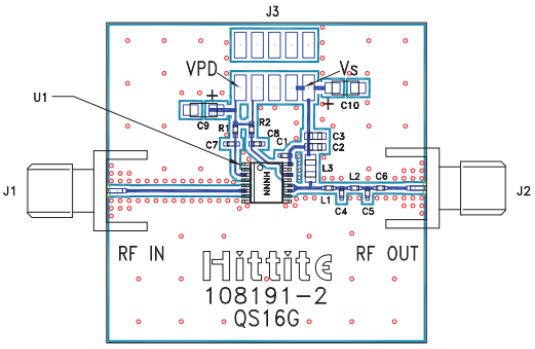

Figura 3. 4 Amplificador RF [24]

3.2.5 Antena

Es la última etapa de nuestro trabajo y para lograr nuestro objetivo decidimos utilizar la antena GSM 800 – 960 MHz, la cual trabaja dentro de la frecuencia de 850 MHz. En la figura 3.5 se observa nuestra antena.

Figura 3. 5 Antena Omnidireccional [21]

Sus principales características son su impedancia de 50 Ω y el rango de frecuencia en el que trabaja que es de 850 y 1900 MHz.

En la figura 3.6 se observa el diagrama, con el cual realizamos nuestro circuito impreso. Dicho diagrama lo realizamos con ayuda del simulador ORCAD versión 9.1.

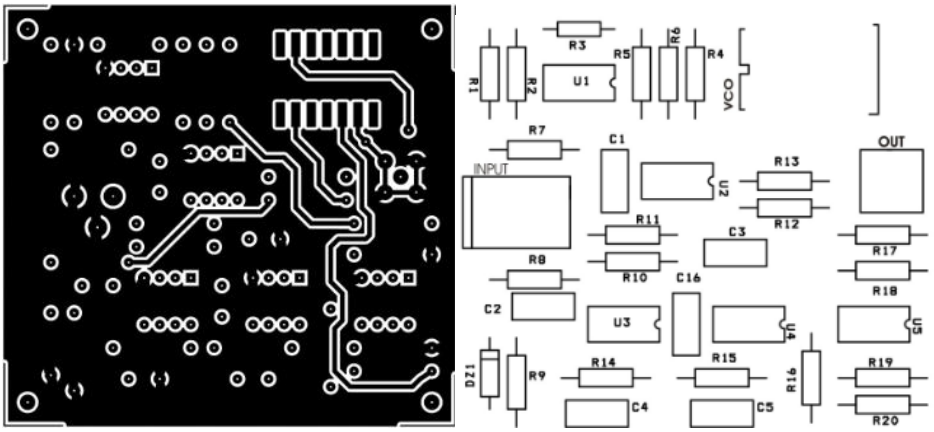

Figura 3. 6 Diagrama del Circuito Impreso del *jammer* [Fuente: Elaboración propia]

3.3 Simulaciones preliminares

3.3.1 Simulación: Sección de Alimentación

Esta simulación se realizó con ayuda de la herramienta de simulación de circuitos denominada SPICE.

Tal como se describió en la parte de diseño, la fuente consta de las etapas correspondientes al transformador y los circuitos de regulación de voltaje. Los resultados obtenidos, de esta simulación, fueron los esperados de acuerdo al diseño. Como se muestra en la figura 3.7

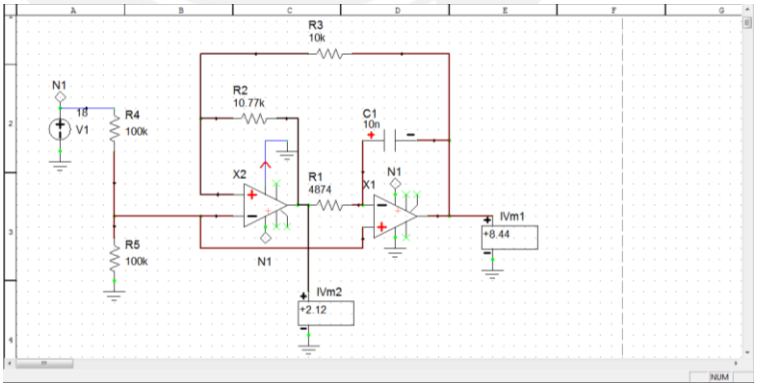

Figura 3. 7 Resultado de simulación de fuente [Fuente: Elaboración propia]

3.3.2 Simulación: Generador de onda triangular

Las pruebas de simulaciones se realizaron en el laboratorio de telecomunicaciones, estas pruebas corresponden a las siguientes partes del circuito generador de onda triangular y generador de ruido. El VCO y el amplificador RF son circuitos que necesitan de equipo especial un equipo especial de medición.

Inicialmente las pruebas las realizamos en una tablilla de pruebas pero nos causaban muchos problemas, como por ejemplo cortos circuitos entre los elementos. Por esa cuestión nos arriesgamos a soldar y de esta forma ver en el osciloscopio los resultados.

En la figura 3.8 observamos la señal triangular la cual es ajustable en amplitud desde 0 a 10 V. En la figura se ve la señal requerida.

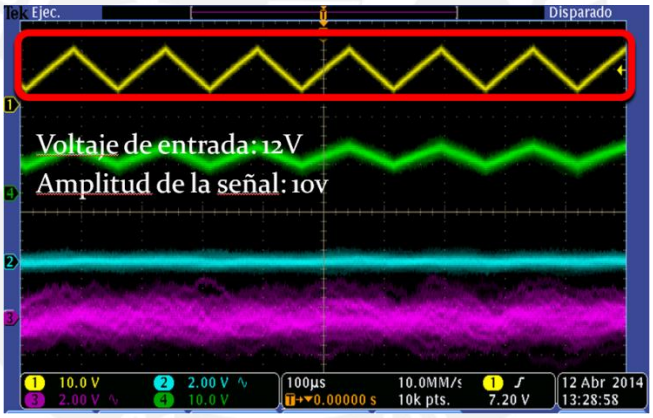

Figura 3. 8 Generador de onda triangular [Fuente: Elaboración propia]

3.3.3 Simulación: Generador de ruido

En la figura 3.9 se observa la señal de ruido generada por el diodo zener, la cual es amplificada por los circuitos TL0810. La señal de ruido también la podemos ajustar en su nivel de amplitud, en la figura se observa en un nivel de amplitud medio.

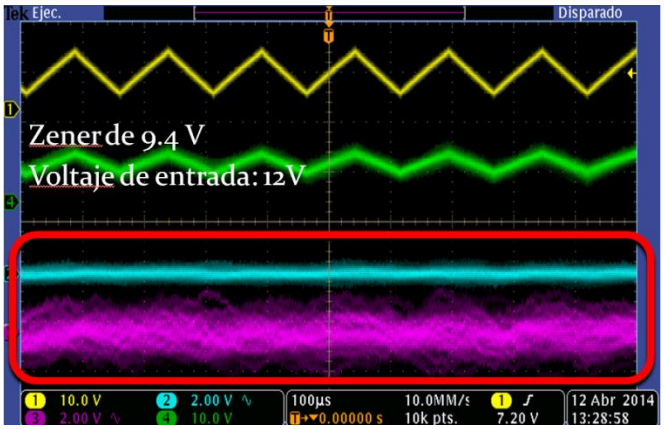

Figura 3. 9 Generador de ruido por el diodo zener [Fuente: Elaboración propia]

3.3.4 Simulación: Onda triangular con ruido

En la figura 3.10 observamos la señal que se obtiene de la mezcla de la señal triangular con el ruido, a señal será la que ponga en funcionamiento el VCO, para obtener el barrido de frecuencia deseado.

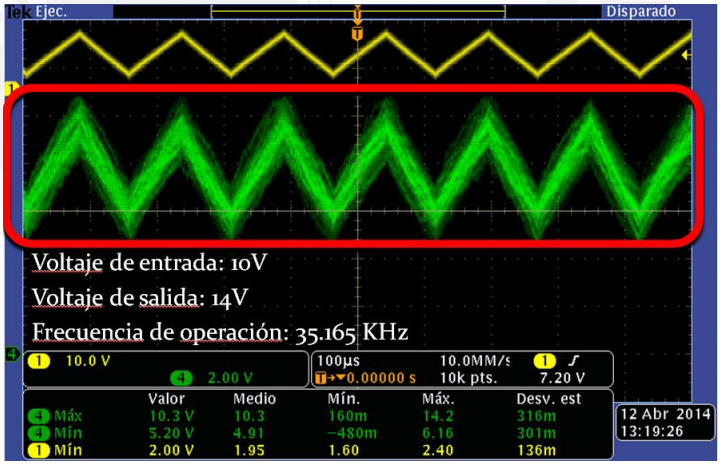

Figura 3. 10 Onda triangular con ruido [Fuente: Elaboración propia]

CAPÍTULO 4

MEDICIONES Y RESULTADOS

4.1 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 layout que se muestra en la figura 4.1.

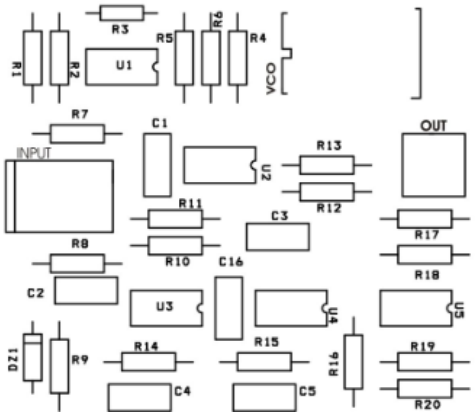

Figura 4. 1 Layout del *jammer* [Fuente: Elaboración propia]

La figura 4.1 nos muestra el PCB utilizado para la implementación física del *jammer*.

Tomando como base el Layout de la figura 4.1, 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 4.2.

Figura 4. 2 Presentación final del *jammer* [Fuente: Elaboración propia]

4.2 Evaluación 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.

- **Sección de oscilación**

Para evaluar la sección de oscilación se utilizó un osciloscopio digital marca Tektronix.

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 la salida del transistor se tenga los resultados esperados, la fuente previamente tiene que suministrar la alimentación adecuada tanto a los TL0810, los que se encargan de generar la señal triangular, como al diodo zener, el cual genera el ruido que sumado con la señal triangular será introducido hacia el VCO, éste último 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 4.3, y resumidos en la tabla 4.1.

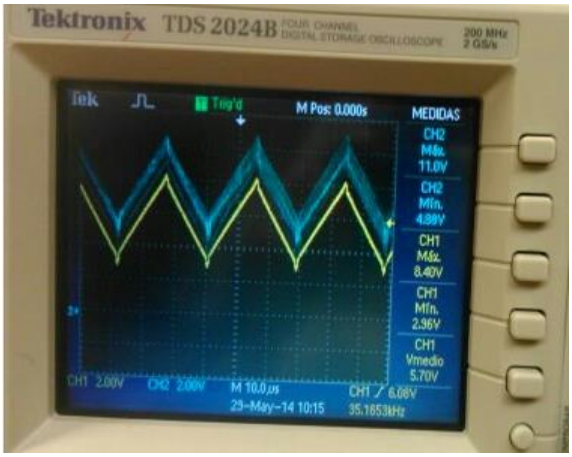

Figura 4. 3 Medida a la entrada del VCO [Fuente: Elaboración propia]

Tabla 4. 1 Resultados de la sección de oscilación [Fuente: Elaboración propia]

Voltaje de entrada			Frecuencia de operación	Voltaje pico-pico
Vmedio	Vmáx.	Vmin.		
7.8 V	11.0 V	4.88 V	35.165 KHz	10 V

- **Sección de RF**

Las mediciones correspondientes a esta sección se realizaron con ayuda de un analizador de espectros marca AGILENT, modelo E4402B. Los resultados obtenidos de dichas mediciones se pueden visualizar en la figura 4.4, así mismo, al igual que en la parte de oscilación, estos son los resultados se resumen en la tabla 4.1.

Figura 4. 4 Medición de la sección RF [Fuente: Elaboración propia]

Tabla 4. 2 Resultados obtenidos de la medición de la sección RF [Fuente: Elaboración propia]

Espectro de frecuencia ocupado		Potencia de salida del circuito
Fmín.	Fmáx.	

776.6 MHz	909.7 MHz	13.4 dBm

La tabla 4.1 nos muestra que el rango del espectro cubierto por el *jammer* es satisfactorio, pues abarca perfectamente toda la banda de los 850 MHz, sobre la cual trabajan los sistemas de 2G y 3G.

Por otra parte, se observa que los valores de voltaje de entrada 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.*

4.3 Presentación de resultados para celulares GSM

Las mediciones realizadas están hechas en función de la distancia de alcance. En la cual se registran 15 mediciones; 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 3.5 m de largo por 5.5 m de ancho y con una altura de 3 m. Se tomaron dos celulares de la misma compañía: Iphone 5S y Sony Xperia (Movistar). El proceso de medición fue el mismo para ambos celulares. Este proceso se describe a continuación:

a. Se colocó el *jammer* en el centro del laboratorio.
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. 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 BTS.

g. Al término de las 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 4.3 y 4.4

Tabla 4. 3 Cobertura del bloqueo del *jammer* [Fuente: Elaboración propia]

Medición	Sony Xperia		Iphone 5S	
	Distancia	Elevación	Distancia	Elevación
1	0.7 m	0.2 m	0.5 m	0.2 m
2	1.0 m	0.2 m	0.8 m	0.2 m
3	1.7 m	0.2 m	1.0 m	0.2 m
4	0.6 m	0.2 m	0.3 m	0.2 m
5	0.3 m	0.2 m	0.6 m	0.2 m

Tabla 4. 4 Tiempos de respuesta [Fuente: Elaboración propia]

Celular	*Jammer* encendido	*Jammer* apagado	Fuera de la cobertura del *jammer*
	Bloqueo	Recuperación de la señal	Recuperación de la señal
Sony	30 s	7 s	7 s

Xperia			
Iphone 5S	32 s	5 s	5 s

En la tabla 4.2 se observa que la distancia lograda por el *jammer* se da a una máxima distancia de 1.70 m.

En cuanto a los tiempos de respuesta del bloqueo. En promedio se registró un tiempo de 31s cuando el dispositivo es encendido, 6s para recuperar la comunicación con la BTS el *jammer* es apagado y 6s de recuperación cuando el móvil sale de la cobertura de bloqueo.

- **Pruebas visuales**

Jammer apagado

A continuación se muestra una imagen del efecto del *jammer* sobre el celular Sony Xperia con tecnología GSM en el cual se mostrara el efecto del dispositivo antes y después de ser encendido.

En la figura 4.5 se muestra el celular que trabaja normalmente con cobertura GSM siendo las 20:37 (en este momento el *jammer* se encuentra apagado), es importante aclarar este punto ya que el efecto del *jammer* difiere un poco de la tecnología con la que trabaje el equipo.

Figura 4. 5 Funcionamiento de los celulares con el *Jammer* apagado
[Fuente: Elaboración propia]

Una vez comprobado el funcionamiento normal del se encendió el *jammer*, al hacer esto inmediatamente se observó cambios en la cobertura del equipo celular Sony Xperia de tecnología GSM y se obtuvo un bloqueo completo como mensajes, llamadas y conexión a internet, ver figura 4.6

***Jammer* encendido**

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

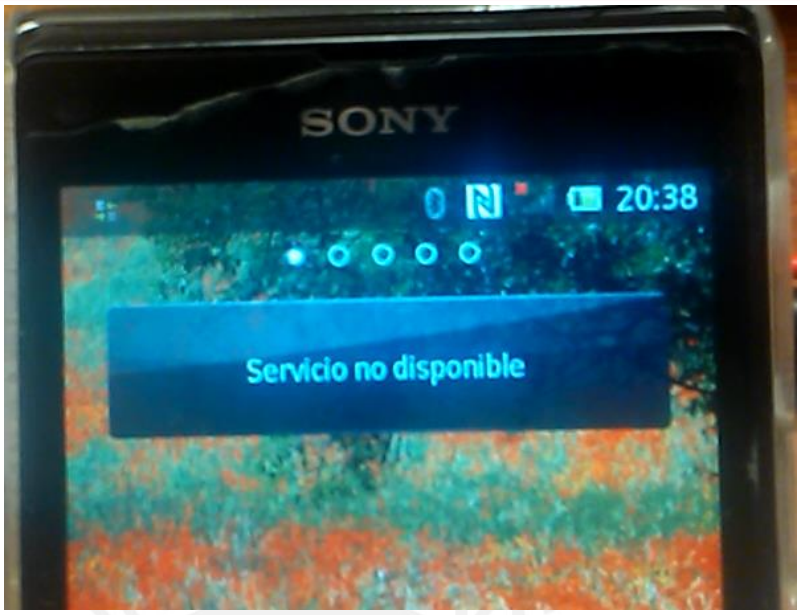

Figura 4. 6 Funcionamiento de los celulares con el *Jammer* encendido
[Fuente: Elaboración propia]

Los resultados de la figura 4.6 muestran que el bloqueo es casi inmediato observándose esto en la hora en la cual se tomaron las imágenes, teniendo que a las 20:37 horas el equipo funciona con normalidad, para cuando el *jammer* es encendido casi un minuto después, 20:38; el equipo muestra una cobertura nula, es decir no se cuenta con ningún tipo de servicio.

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 la introducción, se logró el desarrollo de un dispositivo capaz de bloquear toda operación de teléfonos móviles con tecnología GSM.

- Con el objetivo particular planteado, el cual consistía en registrar el comportamiento de un móvil LTE frente a la operación del *jammer*, se obtuvo que, al monitorear el comportamiento de un teléfono móvil LTE dentro de la zona de cobertura del *jammer*, el efecto de éste último respecto a dicho dispositivo móvil fue prácticamente nulo.

- Respecto al tema del tiempo de respuesta del equipo móvil frente al dispositivo bloqueador, este tiempo es bueno ya que se tuvo como promedio 30 segundos para el bloqueo total del teléfono móvil, comparado con el trabajo anterior que se tiene como referencia, en el cual no se pudo llegar a realizar el bloqueo del teléfono móvil.

- El costo de nuestro dispositivo es bajo, en comparación con las empresas que venden estos equipos interferentes. En el anexo se detalla mejor el costo de los implementos del equipo.

- Por último, cabe mencionar que conforme mejor equipado se encuentre el dispositivo para trabajar con otras bandas alternas, más complicado es el bloqueo. Aparentemente esto se debe a que al salir del área de cobertura de una banda, este intenta conectarse a otra, siempre y cuando el móvil se encuentre también operando en dicha banda. Esto se demuestra en la tabla 4.5 donde se puede

apreciar que el móvil que mayor presentó resistencia fue él que tiene capacidad de soportar la red LTE.

Tabla 4. 5 Tiempos de respuesta respecto a complejidad del dispositivo móvil [22; 23]

Celular	Tiempo de Bloqueo	Bandas de operación
Sony Xperia	30 s	850, 900, 1700, 1800, 1900, 2100
Iphone 5S	38 s	850, 900, 1700, 1800, 1900, 2100, AWS

Recomendaciones

El circuito se podría mejorar en varios aspectos:

- Se podría reducir el tamaño del circuito en la placa con el fin de lograr una mayor integración y portabilidad, al igual que el acoplamiento a la antena.

- Incrementar la banda de frecuencia para poder bloquear otras señales celulares. Esto se lograría, agregándole un circuito VCO paralelo con otro rango de frecuencia y un dispositivo selector, que permita seleccionar que señal se va a bloquear.

- La ley prohíbe la fabricación, distribución y comercialización de un *jammer*, por lo que cualquier persona que use este trabajo para evitar la comunicación de una red celular, está incurriendo en una actividad severamente penada. Por esta razón no se podría incrementar la potencia del *jammer* diseñado.

- Para una mejor interferencia de la comunicación entre la BTS y el teléfono móvil sería incrementar la frecuencia de barrido para que no exista la posibilidad de que el celular pueda ocupar un canal de comunicación.

- Implementar un circuito que realice el control de potencia, para que el área de cobertura sea igual en cualquier sitio donde se desee utilizar el *jammer*. El dispositivo debe monitorear la señal que se va a bloquear, determinar su nivel de potencia y así saber cuánta potencia debe de aplicar el *jammer* para interferir la señal.

Bibliografía

1. Oriol Sallent Roig, José Luis Valenzuela González, Ramón Agustí Comes, *Principios de comunicaciones móviles*, Univ. Politécnica de Catalunya, 2003.
2. Tomasi, Wayne, Electronic *Communication System*, New Jersey: Prentice Hall 2001.
3. Bernad Sklar, *Digital Communication: Fundamentals and Applications*; Prentice Hall; Second Edition.
4. Tero Ojanpera and Ramjee Prasad; *Wideband CDMA for Third Generation mobile Communications*; Artech House.
5. http://www.supertel.gob.ec/index.php?option=com_content&view=article&id=1158: evolucion-de-la-telefonia-movil-en-ecuador&catid=44:principales&Itemid=344 Consulta 10 de junio del 2013.
6. Poisel, Richard. *Introduction to Communication Electronic Warfare System*. Norwood: Artech House, 2004
7. Cuevas León Miriam; *Materia: Redes convergentes*; Instituto Politécnico Nacional, México, 2010
8. Poisel, Rchard. *Modern Communication Jamming Principles and Techniques.* Norwood: Artech House, 2004
9. Schleher, Curtis. *Electronic Warfare in the Information Age.* Norwood: Artech House, 1999
10. Xu, Wenyuan; Wade Trappe; Yanyong Zhang and Tmothy Word. *The Feasibility of Launching and Detecting Jamming Attacks in Wireless Network.* 25 de mayo de 2005. 28 de enero de 2006. http://www.winlab.rutgers.edu/pub/docs/research/JamDetect_Mobihoc.pdf
11. *Electronic Warfare in Operations;* FM 3-36 http://www.fas.org/irp/doddir/army/fm3-36.pdf
12. Richard Poisel; *Introduction to Communication Electronic Warfare Systems;* Artech House.
13. Fried, Limor, *Social Defense Mechanisms: Tools for Reclaiming Our Personal Space,* 28 de enero del 2005, http://www.mit.edu/~ladyada.thesis.pdf Consulta 10 de junio del 2013
14. Doble, John, *Introduction to Radio Propagation for Fixel and Mobile Communicatiosn,* Norwood: Artech House, 2004

15. M. Huidoro José, *Manual de Telecomunicaciones,* Alfa Omega.
16. Valera, Pedro, *Telefonía celular en el Perú.* http://blog.pucp.edu.pe/item/29253/la-telefonia-celular-en-el-peru Consulta 10 de junio del 2013
17. Normales legales, Ministerio de Transporte y comunicaciones. Diario "El Peruano". http://www.mtc.gob.pe/portal/comunicacion/politicas/normaslegales/DDECRETO%20SUPREMO%20N%20012%202012%20MTC.pdf Consulta 10 de junio del 2013
18. Alison Chen and Allen Wan, *FDMA vs TDMA vs CDMA: What`s the difference?* https://www.clear.rice.edu/elec301/Projects01/cdma/compare.html Consulta 10 de junio del 2013
19. Ing. Mshari Albdulkarim, *CDMA (Code Division Multiple Access).* http://www.ustudy.in/node/4793 Consulta 10 de junio del 2013
20. Data Communucations, *Lecture #22 – Wireless Networking.* http://ironbark.xtelco.com.au/subjects/DC/lectures/22/ Consulta 10 de junio del 2013
21. Especificaciones técnicas para antena GSM omnidireccional, http://www.demon-multimedia.com/productos/productos.asp?id=2010&ampliada=Si Consulta 10 de junio del 2013
22. Especificaciones técnicas del celular IPHONE 5, http://catalogo.movistar.com.pe/apple-iphone-5s-16gb?cp=caja-home#/especificaciones Consulta 10 de junio del 2013
23. Especificaciones técnicas del celular SONY XPERIA, http://catalogo.movistar.com.pe/sony-xperia-l-c2104#/especificaciones Consulta 10 de junio del 2013
24. Especificaciones del amplificador RF HMC450QS16G https://www.hittite.com/content/documents/data_sheet/hmc450qs16g.pdf Consulta 01 de junio del 2014
25. Jing Zhang, Yu-xi Liu, *Quantum internet using code division multiple Access;* 17 de julio del 2013, http://www.nature.com/srep/2013/130717/srep02211/full/srep02211.html Consulta 20 de junio del 2014
26. D. J. Torieri. "Statistical Theory of Passive Location Systems" IEEE Transactions on Aerospace Electronic System vol 20, 1984