UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO
INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA
INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

"DISEÑO DE JAMMER PARA TELEFONIA CELULAR"

T E S I S

QUE PARA OBTENER EL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES
P R E S E N T A N :

JOSE MANUEL ROSALES GUZMAN
CARLOS RUBIO CRUZ

ASESOR:

ING. A. MIGUEL ROSAS YACOTU

PACHUCA DE SOTO, HGO., ABRIL DE 2010.

Resumen

Este trabajo aborda la teoría y consideraciones de diseño de un dispositivo inhibidor de señales de radiofrecuencias o *jammer*, el cual tiene como objetivo las redes de telefonía celular ubicadas en la banda *PCS (Personal Communications Services).*

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

Una vez elegidos la técnica de *jamming* y el tipo de *jammer* se muestra el diseño por etapas del dispositivo y su correspondiente simulación. Se explica brevemente el proceso de fabricación y se exponen los resultados obtenidos. Éstos últimos abarcan la parte del espectro cubierta y el área de cobertura efectiva.

El *jammer* descrito atui opera exitosamente a 2 metros a la redonda aproximadamente y toma de 40 a 90 segundos para privar completamente a la unidad móvil de cualquier señal proveniente de la red celular.

Abstract

This thesis presents a theory review and design process for a jammer device on PCS cellular networks. First we describe the basis of radiofrequency theory and jammer design. Topics such as cellular communications and security in communications systems are presented. Also several jamming tehniques are discussed and evaluated.

Design procedure is described using simulation methods. Fabrication process is also described based on final design of jammer device. Several parameters are used to show the performance of jammer considering specific spectrum area. Finally conclusion and future work are presented.

ÍNDICE

Introducción

Durante los últimos años y conforme el empleo de las tecnologías inalámbricas ha ido en aumento, el interés por bloquear ciertos dispositivos en ciertos espacios ha crecido también. Es por eso que el uso de *jammers* y de técnicas de bloqueo e interferencia de señales en la banda de RF ha captado la atención de distintos sectores. Estos dispositivos no son algo nuevo. Sus inicios se remontan a aplicaciones militares durante la Segunda Guerra Mundial. Desde entonces se han fabricado *jammers* para estos y otros propósitos. Debido a su origen militar, países como Estados Unidos, Israel y Japón se colocan como los primeros en el desarrollo de esta tecnología.

El uso de *jammers* encuentra en la telefonía móvil una importante aplicación. Y es que el uso de unidades móviles o teléfonos celulares, como común pero erróneamente se les conoce, ha tenido un incremento considerable en la última década a través de todo el mundo. En México tanto el número de proveedores de servicios de telefonía móvil como el número de usuario ha crecido vertiginosamente[1]. Por ejemplo, mientras que en junio de 1995 tan sólo el 0.7% de la población tenía acceso al servicio de telefonía móvil, en junio del año pasado era un 40.2% el que ya contaba con la posibilidad de recibir este servicio [10].

La Figura 1 muestra como se ha incrementado el número de empresas que proveen servicios de telefonía móvil. De igual manera, se aprecia como ha aumentado el número de usuarios en cada región, arrojando como resultado un cantidad conformada por el 40.2% de la población[2] [11].

Con un acceso tan fácil a la telefonía móvil se vuelve sencillo emplear este servicio de manera incorrecta. Es por eso que surge la necesidad de desarrollar dispositivos capaces de limitar este acceso.

[1] El apéndice A muestra el crecimiento de la telefonía móvil en México [10].
[2] El apéndice B contiene el mapa que muestra la distribución por estados de las distintas regiones [12].

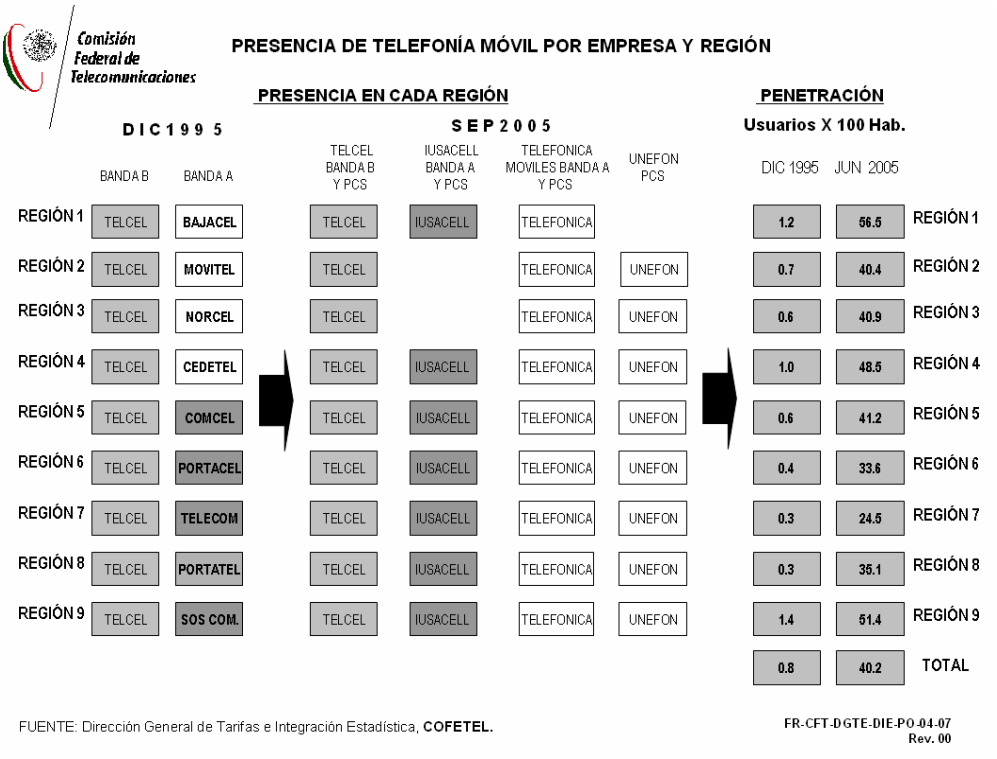

Figura 1 Presencia de Telefonía Móvil por Empresa y Región [11]

El empleo de *jammers* en las redes de la telefonía celular ha abarcado tanto temas de seguridad como de aislamiento acústico. El primero tiene que ver con el empleo de móviles como detonadores o como dispositivos orientados al espionaje. Podrían parecer exagerados los ejemplos antes mencionados pero el uso que se le da a la tecnología es realmente diverso. Existen ejemplos más comunes dentro del campo de seguridad, entre los que destacan el uso de móviles dentro de cárceles y bancos para cometer algún ilícito [7]. Dentro del tema de aislamiento acústico se encuentra el uso de móviles en cines, teatros, bibliotecas o iglesias. En estos casos el uso de *jammers* va ligado a mantener un orden y un espacio en donde se goce de cierta privacidad.

En México el empleo de *jammers* ha causado controversia. Hasta hace unos años la venta de estos dispositivos no era del todo extraña. Sin embargo, debido a la creciente polémica por el uso inadecuado de teléfonos móviles dentro de reclusorios, se ha puesto más atención a lo que dicta la ley referente a estos bloqueadores de señal. Esta ley prohíbe la fabricación y distribución de *jammers*. Es así que la venta de estos dispositivos ha

cesado. En cuestión de diseño y fabriación el único antecedente que se tiene dentro del país proviene del Instituto Politécnico Nacional, donde se fabricó un dispositivo capaz de bloquear la telefonía móvil hace un año.

En el mundo la situación es similar. En países como Francia y Estados Unidos los *jammers* están prohibidos y el argumento es el mismo, la invasión de una frecuencia que es propiedad ajena. Un caso particular es Israel, donde estos bloqueadores son legales. Su situación es única. La guerra ha obligado a crear formas de bloquear las comunicaciones enemigas. Y es debido a esto que los *jammers* comercializados en México provenían de este país. Actualmente en nuestro país su uso es permitido pero solamente en cárceles y bajo ciertas condiciones. Esto se detalla en el apéndice C.

El fácil acceso a la telefonía móvil ha tenido como otra de sus consecuencias la generación de una dependencia a este tipo de tecnología. Tan es así que en el 2004 el "*Lemelson-MIT Program*", una organización que se dedica a la búsqueda de temas sobre inventos e inventores, en su estudio anual llamado "*Invention Index*" publicó una encuesta sobre el invento que se odia más pero sin el cual no se puede vivir. Los resultados ubicaron a los móviles en primer lugar con el 30% de los votos. Al mismo tiempo se realizó otra encuesta sobre si esos mismos inventos tan odiados habían incrementado la productividad. En esta ocasión 95% de los encuestados coincidió en el aumento de su productividad desde que comenzaron a emplear un móvil [9].

El objetivo de este trabajo de tesis es presentar las diferentes técnicas de *jamming* y los distintos tipos de *jammer* con el fin de exponer un análisis comparativo entre ellos y, de esta manera, elegir una técnica y un tipo que permita diseñar y fabricar un *jammer* capaz de bloquear las señales provenientes de las redes celulares TELCEL y MOVISTAR.

Capítulo 1: Conceptos de Radiofrecuencia

1.1 Introducción a la propagación de RF

La comunicación por medio de radio frecuencias tiene lugar cuando una señal, en el rango de 30kHz a 300GHz, se propaga de transmisor a receptor. Entre estos últimos no siempre existe lo que se conoce como línea de vista o *LOS (line-of-sight)* y la señal sufre diversos efectos antes de llegar a su destino.

1.1.1 Comunicación multiruta y sus efectos

Se dice que hay línea de vista cuando no existen obstáculos entre transmisor y receptor en una ruta directa [1, 2, 4]. Al no existir *LOS*, la transmisión es de tipo multiruta. En una transmisión de este tipo la señal sufre efectos como difracción, refracción, reflexión y dispersión, los cuales provocan que la comunicación entre transmisor y receptor se complete por diferentes trayectorias [1, 2, 4].

La difracción ocurre cuando la señal cambia de dirección debido al borde de un obstáculo. A pesar de provocar pérdidas este fenómeno ayuda a la transmisión de la señal cuando no se tiene línea de vista. Por otro lado, la refracción también tiene como consecuencia el cambio de dirección; sin embargo, esta se da cuando la señal pasa de un medio a otro. La refracción se produce siempre y cuando los dos medios tengan un índice de refracción distinto. Siempre que existe refracción se produce otro fenómeno conocido como reflexión. Sin embargo, no siempre existe refracción cuando se da la reflexión. La reflexión de una señal se da cuando la señal choca con un objeto de dimensiones mucho mayores a las de la longitud de onda, lo que provoca que un porcentaje sea transmitido y otro sea reflejado. En el caso de conductores excelentes, la reflexión es total. Es decir, no se refracta la señal y por tanto las pérdidas son menores. La dispersión ocurre cuando la señal choca con objetos de dimensiones pequeñas pero numerosos entre si, como pueden ser arbustos y señalamientos. Al chocar la señal, ésta se refleja en varias direcciones y puede ser que se provoque un cambio en frecuencia y en la polarización de la onda electromagnética. La dispersión solamente se da cuando la señal choca con una superficie rugosa. En el caso de hacerlo con una superficie lisa, el fenómeno que tiene lugar es la

reflexión. Para saber si una superficie es lisa o rugosa se recurre al criterio de Rayleigh [1, 2, 4, 6].

La separación Δh entre dos superficies que reflejan la misma señal indica si la superficie es rugosa o no. Si esta separación es mayor a la existente entre la mayor y menor protuberancia de la superficie en análisis se dice que ésta es lisa, en caso contrario se dice que es rugosa. Para obtener el valor de Δh se utiliza la siguiente ecuación conocida como el límite de Rayleigh [4, 6]:

$$\Delta h = \frac{\lambda}{8 \sin \alpha}$$ **Ecuación 1.1**

donde α es el ángulo con el que choca la señal con el obstáculo, conocido como ángulo de incidencia.

Las diferentes señales provenientes de las distintas rutas no llegan al mismo tiempo y con la misma intensidad. Éstas sufren retrasos y atenuaciones que dependen en general de la longitud de la ruta tomada y del modo de propagación [1, 2, 4, 6].

Además de los efectos antes mencionados, existe otro particular de las modulaciones digitales. Este es la interferencia de símbolos o *ISI* por sus siglas en inglés *intersymbol interference*. Esto ocurre cuando un símbolo anterior al que se está recibiendo interfiere debido a una o más reflexiones. El retraso se debe a que la distancia recorrida por la onda reflejada es mayor que la recorrida por la onda transmitida [5, 6].

Es importante estudiar los efectos que sufre la señal que llega al receptor, ya que estos son los mismos que sufre la señal que recibe el *jammer* [6]. La relación señal-a-ruido *SNR (Signal-to-Noise Ratio)* es la encargada de determinar la calidad con la que llega una señal al receptor [1, 2, 4]. Es esta relación la más importante para determinar los efectos de un *jammer* sobre un sistema de comunicación. El ruido afecta al sistema de comunicación desde el momento que comienza el procesamiento de la señal en el transmisor hasta que

ésta se procesa en el receptor. Los efectos del ruido son de tipo aditivo y logran que decrezca la relación señal-a-ruido. Esto último representa una ventaja para el funcionamiento de un *jammer*, ya que dependiendo de que tan ruidosa sea la comunicación original será el desempeño exigido al *jammer* [6]. Por ejemplo, en caso de que el objetivo del *jammer* sea la generación de ruido aleatorio, la potencia de transmisión de este ruido será menor si la relación señal-a-ruido original no es muy buena.

1.1.2 Parámetros importantes

En el caso de la telefonía móvil es importante la medición de varios parámetros como la relación señal-a-ruido y la relación señal-a-interferencia. Además de las diferentes relaciones entre señales, existen otros puntos que se toman en cuenta para medir el desempeño de un sistema de comunicación inalámbrica. Entre los más importantes están: el *path loss*, el *rms multipath delay spread*, y el *doppler spread* [4, 6].

1.1.2.1 *Path Loss*

El promedio de la potencia P_R con que se recibe una señal, como función de la amplitud de la ruta tomada, está dado por [4, 6]:

$$P_R = \sum_{k=1}^{L} |\beta_k|^2 \quad \textbf{Ecuación 1.2}$$

donde β_k es la magnitud de la trayectoria o ruta y L es el número de trayectorias.

Este promedio es proporcional al inverso de la distancia entre el receptor y el transmisor r_0 elevado a una cierto factor de potencia $(P_R \propto r_0^{-\eta})$. Este factor η es llamado el exponente de *path loss*, el cual al ser multiplicado por diez da como resultado la pérdida de potencia en decibeles por década debido al aumento de la distancia. Valores típicos de η están entre 2 y 4, dependiendo del ambiente. En la propagación por el espacio libre el valor de η es 2. Esto significa que la potencia recibida decae con el inverso del cuadrado de la distancia entre el receptor y el emisor o en otras palabras, 20dB por década de distancia. Una manera sencilla de calcular el *path loss* está definida por la siguiente ecuación:

$$L_p(dB) = P_{TX}(dB) - P_{RX}(dB)$$ **Ecuación 1.2**

donde P_{TX} es la potencia transmitida, P_{RX} es la potencia recibida y L_p son las pérdidas ocasionadas por la trayectoria

Los factores que alteran el valor de las pérdidas por trayectoria en ambientes urbanos incluyen edificios, árboles, lagos, densidad de las construcciones, altura de estas últimas, etc.

1.1.2.2 *Multipath Delay Spread*

El *delay spread* es una medida estadística de los retrasos de tiempo de varias rutas o trayectorias. La potencia normalizada y promediada como función del retraso se conoce como espectro retrasado de potencia [2, 4, 6]. El *delay spread* se puede calcular usando el modelo de Turin para propagación en ambientes urbanos y está dado por [6]:

$$\tau_{rms} = \left[\frac{\sum_{k=1}^{L} (\tau_k - \bar{\tau})^2 \beta_k^2}{\sum_{k=1}^{L} \beta_k^2} \right]^{\frac{1}{2}}$$ **Ecuación 1.3**

donde β_k y τ_k representan a la magnitud y el retraso excesivo de las rutas L respectivamente. $\bar{\tau}$ es el promedio del retraso excesivo y se calcula como [6]:

$$\bar{\tau} = \frac{\sum_{k=1}^{L} \tau_k \beta_k^2}{\sum_{k=1}^{L} \beta_k^2}$$ **Ecuación 1.4**

En ambientes de interiores, el valor *rms* del *delay spread* medido a distancias de 100m está por debajo de los 100ns, mientras que en áreas exteriores es menos de 10μs a distancias de algunos kilómetros [1, 4, 6]. Como se mencionó anteriormente, el efecto

multiruta afecta al promedio de la potencia de la señal recibida, ésta fluctúa a medida que el receptor se acerca y/o aleja del transmisor. Esta fluctuación es causada por un efecto conocido como *shadowing* y se conoce como *shadow fading* [4, 6]. El efecto de *shadowing* ocurre cuando un móvil se coloca detrás de un obstáculo y experimenta una reducción en la potencia de la señal recibida. La diferencia de fase entre las distintas rutas causa que la amplitud de la señal cambie rápida y constantemente. A esta fluctuación se le conoce como *multipath fading* [6].

1.1.2.3 *Doppler Spread*

Cuando una señal es enviada entre un transmisor y un receptor y éste último se está moviendo a una determinada velocidad, existe un cambio en la frecuencia de la señal. Este fenómeno se conoce como *Doppler Shift* [4, 6]. La frecuencia cambia a razón de [6]:

$$f_D = \frac{\nu}{\lambda}\cos(\alpha) \quad \textbf{Ecuación 1.5}$$

donde α es el ángulo de la señal llegando al receptor en relación a la dirección del receptor, ν es la velocidad y λ es la longitud de onda.

El máximo cambio ocurre cuando el receptor está acercando o alejando directamente h del transmisor, es decir, donde α es igual a ± 1. Ese máximo cambio de frecuencia, f_m, está dado por:

$$f_m = \frac{\nu}{c} f_c \quad \textbf{Ecuación 1.6}$$

En la telefonía móvil es común que las señales lleguen al mismo tiempo pero con diferentes ángulos, lo que provoca que la relación entre amplitud y ángulos de fase cambie constantemente. La región en el espectro entre $-f_c - f_m$ y $-f_c + f_m$ es llamada *Doppler Spread*. La densidad *S(f)* de esta parte del espectro se puede calcular como:

$$S(f) = \frac{1}{4\pi f_m} \frac{1}{\sqrt{1 - \frac{(f - f_c)^2}{f_m^2}}}$$ **Ecuación 1.7**

Un efecto relacionado también con el movimiento del receptor es la pérdida de correlación entre fase y amplitud de las distintas rutas. El cambio en la correlación depende de la distancia recorrida. A distancias cortas las señales recibidas están altamente correlacionadas, pero esta correlación decae rápidamente a medida que el receptor se aleja del transmisor [6].

1.2 Modelos de propagación

Para poder predecir todos los efectos durante la transmisión de una señal se han propuesto diversos modelos o expresiones matemáticas. Estos modelos han sido desarrollados para cualquier tipo de ambiente. Desde aquellos donde hay línea de vista *(LOS Line-of-Sight)* hasta aquellos donde las comunicaciones son posibles sin línea de vista *(OLOS Out-of-Line-of-Sight)*. Cuando existe *LOS* las variaciones son modeladas con una distribución de Rician o con una distribución logarítmica normal, mientras que en el caso de *OLOS* las variaciones se modelan con una distribución de Rayleigh. Una tercera distribución es más exacta que las dos anteriores. De hecho incluye ambas. Esta distribución es la Nakagami [1, 2, 4, 6].

Son varios los modelos usados para la telefonía móvil actualmente. Algunos de ellos son el modelo R^n, el modelo de propagación Egli, el modelo de propagación Nicholson y el modelo de propagación Longley-Rice. Sin embargo, los dos modelos clásicos y en los que se basan gran cantidad de modelos actuales son los modelos Okumura-Hata y Walfish-Ikegami [2, 4].

1.2.1 Modelo Okumura-Hata

Basado en el modelo Okumura, es el modelo más ampliamente usado en la planeación de redes de telefonía celular. Este modelo tiene como objetivo predecir los efectos de difracción, reflexión y dispersión ocasionados por las estructuras de la ciudad. Considerando que una ciudad puede ser densamente poblado o no, se consideran cuatro casos: áreas densamente urbanas, áreas urbanas, áreas suburbanas y área rurales [1, 15].

Cuando se habla de ciudades se presentan los dos primeros casos y se emplea la ecuación 1.8 para calcular la atenuación de la onda electromagnética cuando viaja de transmisor a receptor o *path loss* [15].

$$L_p(dB) = C_1 + C_2 \log(f) - 13.82\log(h) - a(h_m) + [44.9 - 6.55\log(h)]\log(d) + C_0 \quad \textbf{Ecuación 1.8}$$

Donde:

f = frecuencia en MHz

d = distancia entre la estación base y el móvil en km

h = altura efectiva de la antena de la estación base

h_m = altura de la antena del móvil

Urbano denso	**Urbano**
$a(h_m) = [1.1\log(f) - 0.7]h_m - [1.56\log(f) - 0.8]$	$a(h_m) = 3.2[\log(11.75h_m)]^2 - 4.97$
$C_0 = 0$	$C_0 = 3$

	150MHz<f<1000MHz	**1500MHz<f<2000MHz**
	$C_1 = 69.55$	$C_1 = 46.33$
	$C_2 = 26.16$	$C_2 = 33.9$

1.2.2 Modelo ITU para interiores

No solamente se toman en cuenta los exteriores al momento de diseñar una red celular. Por ejemplo, al instalar micro o picocélulas al interior de un centro comercial donde el tráfico es elevado es importante modelar el comportamiento de la señal y las pérdidas que puede sufrir. Por esa razón es que existen modelos de propagación para interiores.
Uno de los más usados es el modelo ITU [1, 2].

Este modelo estima el *path loss* dentro de un cuarto o un área cerrada dentro de un edificio delimitado por paredes de cualquier material. Normalmente se aplica a frecuencias alrededor de 2.4GHz y menores; sin embargo, se ha probado con éxito en frecuencias cercanas a los 5.2GHz. La ecuación 1.9 muestra la forma de calcular el *path loss* empleando este modelo [1, 2].

$$L = 20\log f + N\log d + P_f(n) - 28 \quad \textbf{Ecuación 1.9}$$

Donde:

L = path loss

f = es la frecuencia en MHz

d = la distancia entre transmisor y receptor en metros

N = el coeficiente de pérdidas por distancia

n = número de pisos entre transmisor y receptor

$P_f(n)$ = el factor de pérdidas por penetración entre pisos

El coeficiente de pérdidas por distancia se ha obtenido empíricamente y la tabla 1.1 muestra algunos valores.

Tabla 1.1 Coeficiente de pérdidas por distancia

Frecuencia	Área residencial	Área de oficina	Área comercial
900 MHz	N/A	33	20
1.2 GHz	N/A	32	22
1.3 GHz	N/A	32	22
1.8 GHz	28	30	22
4 GHz	N/A	28	22
5.2 GHz	N/A	31	N/A

El factor de pérdidas por penetración entre pisos es una constante empírica dependiente del número de pisos que las ondas necesitan penetrar para llegar a su destino. La tabla 1.2 muestra algunos valores de esta constante.

Tabla 1.2 Constantes por penetración entre pisos

Frecuencia	No. de pesos	Área residencial	Área de oficina	Área comercial
900 MHz	1	N/A	9	N/A
900 MHz	2	N/A	19	N/A
900MHz	3	N/A	24	N/A
1.8 GHz	N	4n	15+4(n-1)	6 + 3(n-1)
2.0 GHz	N	4n	15+4(n-1)	6 + 3(n-1)
5.2 GHz	1	N/A	16	N/A

Es importante destacar que la principal desventaja de este modelo es que no están contemplados todos los casos para obtener los valores de las constantes.

1.3 Introducción a la ingeniería de microondas

Los circuitos de microondas pueden ser divididos en dos grandes grupos; los circuitos activos y los circuitos pasivos. Los circuitos pasivos no agregan potencia a la señal que reciben y los circuitos activos pueden agregar potencia a la señal que reciben. Los circuitos pasivos incluyen desde elementos discretos como resistencias, inductancias y capacitancias hasta circuitos más complejos, tales como: filtros, divisores, acopladores y líneas de transmisión. Dentro de los circuitos que pueden ser tanto activos como pasivos, están las antenas, multiplexores y mezcladores. Los circuitos activos cubren dispositivos tales como: amplificadores, osciladores y moduladores [17].

1.3.1 Líneas de transmisión

Una línea de transmisión se define como un sistema metálico conductor que es usado para transferir energía eléctrica de un punto a otro. Siendo un poco más específicos, podemos decir que una línea de transmisión consiste de dos o más conductores separados por un dieléctrico. La propagación de energía a través de una línea de transmisión se da en forma de ondas electromagnéticas transversales, esto quiere decir que la dirección del desplazamiento es perpendicular a la dirección de propagación. Estas ondas se transmiten

principalmente en el dieléctrico que separa los dos conductores. Es por eso que una onda viaja a través del medio. Algunos tipos de líneas de transmisión son el cable coaxial, las guías de onda, el cable bipolar paralelo, el par trenzado, etc [14, 16, 17].

Cuando la línea de transmisión se usa para transmitir señales de baja frecuencia, su comportamiento es simple y predecible; sin embargo, cuando se usa para transmitir señales de alta frecuencia efectos como la dispersión y la disipación convierten al cable coaxial, al cable bipolar paralelo y al par trenzado en opciones imprácticas. Es por eso que se han construido alternativas para frecuencias por arriba de 500MHz, las líneas de transmisión planas [14, 17].

1.3.1.1 Líneas de transmisión planas

El trabajar con líneas de transmisión en circuito impreso no es algo nuevo. Este tipo de tecnología lleva tiempo siendo usada. Esto se debe a las grandes ventajas que ofrece, entre las que destacan el costo, lo ligero y compacto de los circuitos, el ancho de banda amplio que se puede manejar y las sencillas técnicas de fabricación [14, 17].

Las líneas de transmisión planas se componen de un dieléctrico con metalización en uno o ambos lados. Esta metalización es la que se varía al momento de construir circuitos pasivos, líneas de transmisión y circuitos de acoplamiento. Así mismo, es posible intercalar dispositivos activos. Es por eso que los circuitos complejos son baratos y compactos. Dentro de este tipo de líneas de transmisión la más común es la *microstrip* o microcinta; sin embargo, no es la única. También se encuentran las guías de onda coplanar, la línea de ranura (*slotline*) y la cinta coplanar. La Figura 1.1 muestra una breve descripción de esta familia de líneas de transmisión [14, 17].

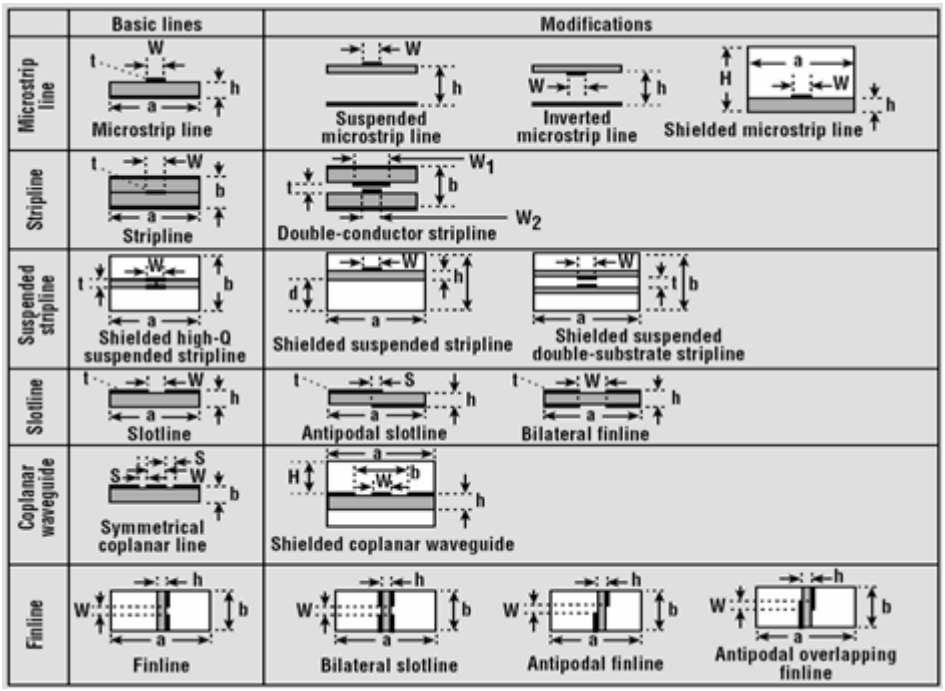

Figura 1.1. Líneas de transmisión planas [17].

Al trabajar con una línea de transmisión de este tipo lo primero que se debe hacer es seleccionar un dieléctrico. Esta selección es importante debido a la constante de permitividad particular de cada material. Las características de la línea estarán controladas por el ancho del conductor y los espacios en el plano dieléctrico [16].

Al diseñar una línea plana se debe determinar la impedancia característica y la permitividad efectiva. Ambas dependen de la frecuencia que se esté manejando [16]. Para hacer esto existen aproximaciones y programas que facilitan la tarea [23].

A pesar de ser similares, no todas las líneas planas son iguales. Existen parámetros que nos permiten comparar unas con otras. Algunos de ellos son el factor Q del circuito, la radiación y la dispersión. La tabla 1.3 muestra una comparación entre las líneas de esta familia.

Tabla 1.3 Comparación entre líneas de transmisión planas [17]

Línea de transmisión	Factor Q	Radiación	Dispersión	Rango de Impedancias	Montaje de chip
Microstrip	250 100 a 150	Baja Alta	Baja	20 a 120	Difícil en paralelo, fácil en serie
Stripline	400	Baja	Ninguna	25 a 250	Pobre
Stripline suspendida	500	Baja	Ninguna	40 a 150	Regular
Slotline	100	Media	Alta	60 a 200	Fácil para paralelo, difícil para serie
Guía de onda coplanar	150	Media	Baja	20 a 250	Fácil para serie y paralelo
Finline	500	Ninguna	Baja	100 a 400	Media

1.3.1.1.1 Línea coplanar

Se trata de una línea de ancho *W* que se encuentra separada del plano de tierra por una distancia *G*. Este tipo de línea tiene la ventaja de conectar componentes pasivos y activos en paralelo con la línea, sin necesidad de taladrar el sustrato. Este tipo de línea puede contener un tercer plano de tierra en la parte inferior del sustrato o puede no hacerlo; sin embargo, es necesario mencionar que en caso de contener el plano de tierra adicional las dimensiones cambiarán si se desea conservar la misma impedancia característica. La Figura 1.2 muestra las dimensiones que se consideran al momento de diseñar una línea coplanar con plano de tierra [17].

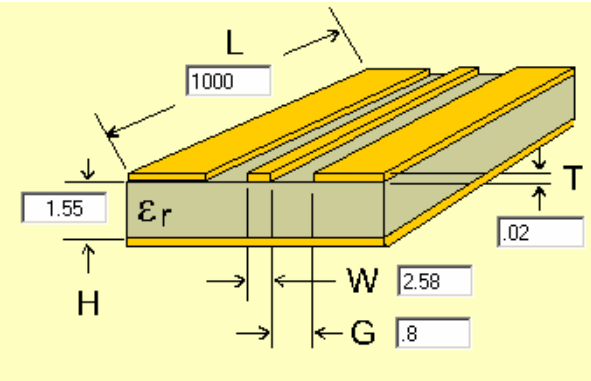

Figura 1.2. Línea coplanar [23]. L = Largo del sustrato, H = Altura del sustrato, T = Espesor del metal, W = Ancho de la línea de transmisión, G = Apertura entre plano de tierra y línea de transmisión

1.3.2 Redes de dos puertos

Cualquier sistema, dispositivo o circuito para el que se puedan definir "n" pares de terminales entre las cuales existe un voltaje se conoce como red de "n" puertos. Es así que un puerto se define como un par de terminales por las que entra o sale una señal [16, 22].

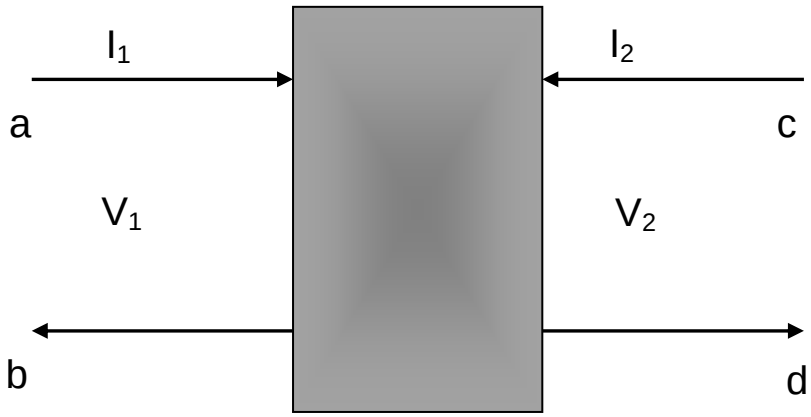

Figura 1.3 Red de dos puertos, donde I_1 es la corriente de entrada, I_2 es la corriente de salida, V_1 es el voltaje de entrada, V_2 es el voltaje de salida, a y b son las terminales en el puerto de entrada, c y d son las terminales en el puerto de salida.

Definir un circuito como una red de dos puertos facilita notablemente su análisis, ya que al conocer un solamente un grupo de parámetros como podrían ser voltajes o corrientes se pueden calcular los restantes. En la Figura 1.3 se muestra el esquema de este tipo de red. Existen distintos tipos de parámetros, destacan los de pequeña señal y los de dispersión o parámetros S. [22]

Entre los parámetros de pequeña señal se encuentran los de impedancia o Z, los de admitancia o Y, los híbridos o H, los de transmisión o T y los de transmisión inversa o ABCD. En la tabla 1.4 se describen brevemente estos parámetros.

Tabla 1.4 Parámetros de pequeña señal

Parámetros	**Componentes**	
Z	$Z_{11} = \left.\frac{V_1}{i_1}\right\|_{i_2=0}$	$Z_{12} = -\left.\frac{V_1}{i_2}\right\|_{i_1=0}$
	$Z_{21} = \left.\frac{V_2}{i_1}\right\|_{i_2=0}$	$Z_{22} = -\left.\frac{V_2}{i_2}\right\|_{i_1=0}$
Y	$Y_{11} = \left.\frac{i_1}{V_1}\right\|_{V_2=0}$	$Y_{12} = \left.\frac{i_1}{V_2}\right\|_{V_1=0}$
	$Y_{21} = -\left.\frac{i_2}{V_1}\right\|_{V_2=0}$	$Y_{22} = -\left.\frac{i_2}{V_2}\right\|_{V_1=0}$
H	$H_{11} = \left.\frac{V_1}{i_1}\right\|_{V_2=0}$	$H_{12} = \left.\frac{V_1}{V_2}\right\|_{i_1=0}$
	$H_{21} = -\left.\frac{i_2}{i_1}\right\|_{V_2=0}$	$H_{22} = -\left.\frac{i_2}{V_2}\right\|_{i_1=0}$
T	$T_{11} = \left.\frac{V_2}{V_1}\right\|_{i_1=0}$	$T_{12} = \left.\frac{V_2}{i_1}\right\|_{v_1=0}$
	$T_{21} = \left.\frac{i_2}{V_1}\right\|_{i_1=0}$	$T_{22} = \left.\frac{i_2}{i_1}\right\|_{v_1=0}$
ABCD	$A = \left.\frac{V_1}{V_2}\right\|_{i_2=0}$	$B = \left.\frac{V_1}{i_2}\right\|_{v_2=0}$
	$C = \left.\frac{i_1}{V_2}\right\|_{i_2=0}$	$D = \left.\frac{i_1}{i_2}\right\|_{v_2=0}$

Estos parámetros necesitan de un cortocircuito o un circuito abierto para poder calcularse. Sin embargo, al trabajar con altas frecuencias no es posible lograr esto. Lo

anterior se debe a que al aumentar la frecuencia de la señal, la condición necesaria para definir cada uno de los parámetros no se pude cumplir por limitaciones de manufactura [16]

Para el análisis de alta frecuencia se emplea lo que se conoce como parámetros de dispersión o parámetros S. Estos parámetros se basan en la reflexión y transmisión medidas en las terminales [16, 22].

Tabla 1.5 Parámetros de dispersión

$$S_{11} = \left.\frac{b_1}{a_1}\right|_{a_2=0} \qquad S_{12} = \left.\frac{b_1}{a_2}\right|_{a_1=0}$$

$$S_{21} = \left.\frac{b_2}{a_1}\right|_{a_2=0} \qquad S_{22} = \left.\frac{b_2}{a_2}\right|_{a_1=0}$$

En la Tabla 1.5 se muestra la manera de calcular estos parámetros. Para entender mejor estos cálculos podemos recurrir a la Figura 1.4, en ella se aprecia el significado de a y b. Se puede ver que las ondas hacia la red están representadas por a y las que salen por b. En otras palabras, a se refiere a la transmisión y b a la reflexión [16].

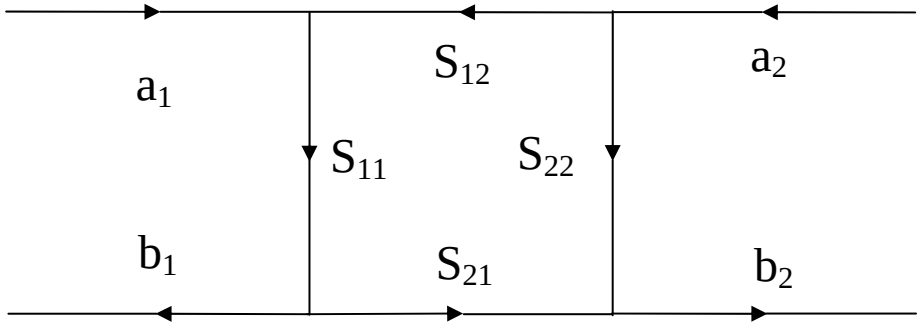

Figura 1.4 Parámetros S, donde a = ondas electromagnéticas que entran a la red, b = ondas electromagnéticas que salen de la red, S_{11} coeficiente de reflexión del voltaje del puerto de entrada, S_{12} = ganancia de voltaje invertida, S_{21} = ganancia del voltaje, S_{22} = coeficiente de reflexión del puerto de salida

Tanto la reflexión como la transmisión dependen de la impedancia característica de la línea y de la impedancia del puerto. El coeficiente de reflexión de la señal, Γ, se puede calcular usando la ecuación 1.10 [16].

$$\Gamma = \frac{Z_i - Z_0}{Z_i + Z_0}$$

Ecuación 1.10 Coeficiente de reflexión

donde Z_i representa la impedancia de la línea y Z_o la del puerto. Se puede ver que el caso ideal, en el que ocurre una transmisión 100% exitosa sin pérdidas de energía es cuando estas dos impedancias son del mismo valor, es decir, cuando las cargas están acopladas.

1.4 Antenas

Una antena es un sistema conductor metálico capaz de radiar y capturar ondas electromagnéticas. Las antenas son usadas como interfaz entre un dispositivo guía y el espacio libre tanto para transmisión como para recepción. Cuando se está transmitiendo, se genera un campo electromagnético al momento de aplicarse un voltaje. En el caso de la recepción el proceso es el inverso; es decir, al momento de captar un campo electromagnético la antena genera como respuesta un voltaje [14, 16, 17, 22].

El tamaño de las antenas es muy importante. Éste está relacionado con la longitud de onda de la señal y es por lo general un submúltipo exacto de ésta. Es por eso que a mayores frecuencias, el tamaño de la antena es menor, es decir, son inversamente proporcionales. Esto se puede ver en la ecuación 1.11. [14, 16, 22]

$$\lambda = \frac{v}{f}$$ **Ecuación 1.11**

donde λ es la longitud de onda, *v* es la velocidad de propagación y *f* es la frecuencia de operación. Una antena se puede representar por medio de su equivalente de Thevenin. Como se puede observar en la Figura 1.5 la fuente es un generador ideal, la línea de transmisión es una línea con impedancia Z_g, y la antena está formada por una carga Z_A ($Z_A = (R_L + R_r) + jX_A$). La resistencia R_L representa las pérdidas en el dieléctrico y la resistencia Rr es la resistencia de radiación. X_A es la parte imaginaria de la impedancia asociada a la radiación de la antena. [22]

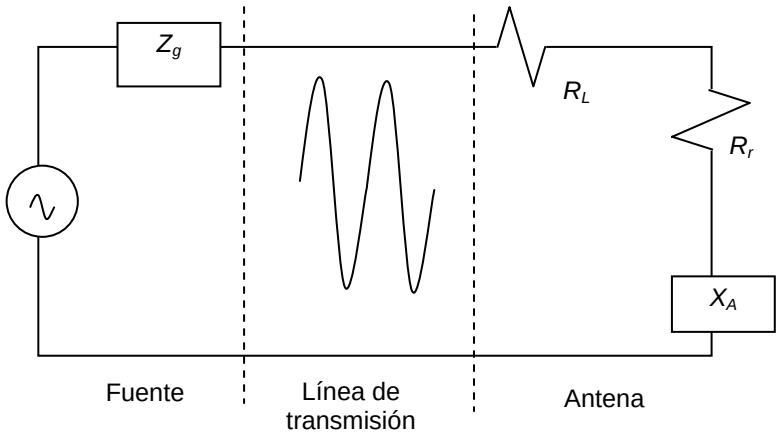

Figura 1.5 Modelo de una antena

1.4.1. Parámetros de antenas

Patrón de radiación, es una representación gráfica de las propiedades de radiación de una antena en función de las coordenadas espaciales [16, 22].

Potencia radiada, P_{rad} se determina con la integral del vector de Poynting en una superficie cerrada que envuelve totalmente a la antena. La ecuación 1.12 muestra el cálculo de la potencia radiada. [16]

$$P_{rad} = \oint S \bullet \mathrm{da} \quad \textbf{Ecuación 1.12}$$

Eficiencia, es una forma de cuantificar las pérdidas de una antena. Se distinguen tres tipos: de reflexión, de conducción y del dieléctrico [14, 16, 22].

Ancho de banda, rango de frecuencias en el que opera correctamente la antena. El límite se determina por la caída a 3dB, es decir, cuando la energía radiada cae aproximadamente a la mitad de su valor máximo [14].

Directividad, se define como la relación entre la potencia radiada en la dirección de máxima radiación y la radiación total de la antena promediada a lo largo del área de la esfera [14, 22].

Ganancia, es la combinación de la eficiencia y la directividad. Una antena es un elemento pasivo por lo que no amplifica señales. La ganancia se expresa en dB [14].

Impedancia de entrada, Z_{in}, este parámetro se obtiene al relacionar inversamente el voltaje de entrada a la antena, E_i, y la corriente, I_i, que se produce en ésta como se observa en la ecuación 1.13 [22].

$$Z_{in} = \frac{E_i}{I_i}$$ **Ecuación 1.13**

El valor de la impedancia es complejo. Es por esto que depende de la frecuencia. Además, depende de la longitud y la resistencia de radiación de la antena.

Resistencia de radiación, es un componente ficticio encargado de representar la potencia radiada [16].

Anchura de haz, es un parámetro de radiación ligado a la ganancia. Es el intervalo angular dentro del cual la potencia relativa radiada por la antena es superior a la mitad de la ganancia [14].

Polarización, se refiere a la dirección de la perturbación. Puede ser elíptica (derecha, izquierda), circular (derecha, izquierda) o lineal (vertical, horizontal) [16].

1.4.2 Tipos de antena

Por su fabricación, las antenas se agrupan en 7 grupos principales [22]:

1. Lineales
2. De lazo
3. Helicoidales
4. De apertura
5. De parche o microstrip
6. De reflexión

7. Arreglos

En los últimos años el avance tecnológico ha volteado la mirada al desarrollo de las antenas de parche o de *microstrip* debido a las ventajas que éstas poseen.

1.4.2.1 Antenas de parche

Una antena de parche está formada por un material conductor que se adhiere sobre un dieléctrico. Las dimensiones y forma del metal determinarán las características de la antena. Pueden ser cuadradas, rectangular, dipolares, etc. Las ventajas y desventajas de este tipo de antenas se pueden ver en la Tabla 1.6 [16].

Tabla 1.6 Ventajas y desventajas de una antena de parche

Ventajas	Desventajas
Integrables al entorno	Factor de calidad alto
Gran número de aplicaciones	Ancho de banda reducido
Robustas	Baja eficiencia
Acoplación sencilla de impedancias	Reducida capacidad de barrido
Tamaño reducido	Pérdidas por ondas superficiales en el dieléctrico

1.4.2.1.1 Antena de parche rectangular

Este tipo de antena consiste en una delgada capa de material conductor adherida a un substrato dieléctrico colocado sobre un plano de tierra. Generalmente su busca un substrato con una permitividad entre 2.2 y 12; entre más bajo sea este valor mayor será eficiencia, el ancho de banda y el tamaño. Las antenas de parche permiten 3 métodos principales de alimentación:

1. Directa, cuando entra en contacto directo con el radiador.

2. Por apertura, una línea de transmisión se encuentra en la parte inferior de dos placas del substrato. En medio de ellas se encuentra el plano de tierra con una ranura que se localiza a una posición, que desemboca a la capa donde se encuentra el radiador. A través de esa ranura, la línea de alimentación se acopla electromagnéticamente al parche radiador.

3. Por proximidad, la línea de alimentación es la que se encuentra en la parte central de dos placas del dieléctrico. La capa inferior es el plano de tierra y la superior es el radiador. Se da también por acoplamiento electromagnético.

1.4.2.1.2 Antena *OMA*

La Figura 1.6 muestra una antena *OMA (Omnidirectional Planar Microstrip Antenna)* de 7 segmentos por sus dos caras. Las antenas *OMA* de *n* segmentos consisten en una serie de parches conectados entre si con el fin de aumentar las características de la antena. Son usadas en aplicaciones de IEEE802.11, donde la frecuencia está alrededor de 2.45GHz. Estas antenas tienen una impedancia muy aproximada de 50Ω y ganancias superiores a los 5dBi. Su construcción y reducido tamaño representan ventajas al momento de elegir una antena. Cada línea de la antena tiene una longitud *L* de la mitad de la longitud de onda. Los planos de tierra tienen un ancho, W_2, *n* veces mayor que el de la línea, W_1. El valor de esta *n* depende de las características propias del sustrato. El objetivo es que en cada segmento la línea de transmisión tenga una impedancia de 50Ω [22].

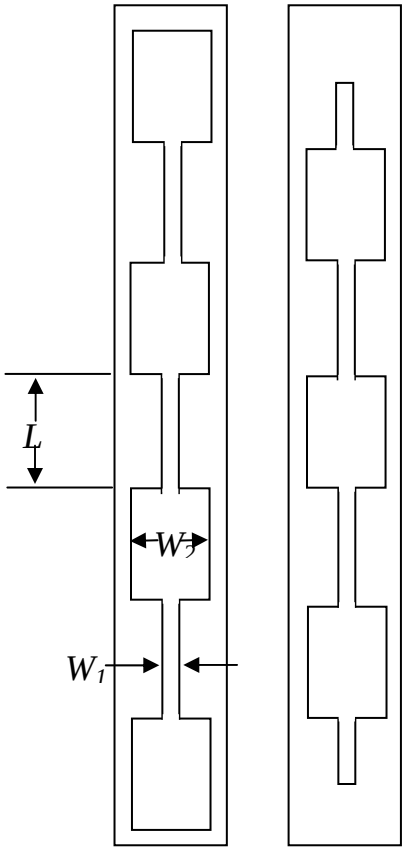

Figura 1.6 Antena *OMA* de 7 segmentos

Capítulo 2: Descripción de la “Guerra Electrónica”

La “Guerra Electrónica” de las comunicaciones o *EW* por sus siglas en inglés “*Electronic Warfare*” es el nombre que se le da a todas aquellas acciones que tienen por objetivo bloquear, interceptar o negar la comunicación de un punto transmisor a otro receptor [5, 6, 7]. Esta llamada “guerra” tiene tres elementos principales [5,6]:

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

2.1 Ataque electrónico

El AE (ataque electrónico) se puede realizar por medio de tres tipos de acciones o técnicas [5, 6, 8]:

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

2.1.1 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 [6, 8]. 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.

2.1.2 Técnica de engaño

La técnica de engaño tiene como objetivo formar una nueva ruta de comunicación [6]. Es así que en lugar de que la información llegue al receptor deseado, ésta sufre un cambio de ruta y es recibida por otro sistema receptor. De igual forma, el engaño puede consistir en la sustitución del sistema transmisor. En este caso el receptor original está recibiendo una

señal que proviene de un segundo sistema transmisor. Cuando el receptor está ocupado no puede recibir la señal emitida por el transmisor original.

2.1.3 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 transmisor y receptor. La potencia emitida debe ser mayor a la que emplea el transmisor del sistema que está sobre ataque [8].

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* [8].

2.2 Apoyo electrónico

El apoyo electrónico funciona como auxiliar del AE. Su función es la medición de parámetros de interés en el sistema de comunicación [6]. Una de las razones principales de hacer esto radica en que si no hay señal que interferir no tiene caso gastar la potencia del *jammer* implementado. Sin embargo, dependiendo de la aplicación será el tipo de *jammer* que se emplee. Es así que se puede mantener en operación un *jammer* por tiempo indefinido o se puede encender siempre y cuando se detecte una comunicación. Todo esto se verá más adelante cuando se analicen los distintos tipos de *jammers* que existen. Entre los parámetros que se encarga de medir el apoyo electrónico se encuentran [6, 8]:

- ***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 [6].

- ***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* [8].

- ***PDR (Packet Delivery Ratio)***

  Compara los paquetes que llegaron al receptor con los que fueron enviados [8].

- ***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 P_e [6].

- ***SER (Symbol Error Rate)***

  Es la probabilidad de que un símbolo sea incorrecto y se llega a escribir como P_s [6].

- ***SIR (Signal-to-Interference Ratio)***

  Relaciona la potencia de la señal deseada con la potencia de la suma de las señales no deseadas [5, 7].

2.3 Protección electrónica

La PE (protección electrónica) consiste en el uso de estrategias para evitar los dos primeros elementos de la llamada “Guerra Electrónica”, es decir, el ataque y el apoyo [6]. La codificación y la modulación entran dentro de este elemento. Con la unión de modulación y codificación nacieron las comunicaciones *AJ* por sus siglas en inglés, *antijam*. Este tipo de comunicaciones tienen como objetivo evitar que un sistema externo pueda dañar, bloquear o interceptar la comunicación de otro sistema.

2.3.1 Tipos de señales *AJ (antijam)*

A pesar de existir varios tipos de señales *AJ*; no es parte de este trabajo mencionar todas. Es por eso que se discutirán las dos principales. Las dos tipos de señales *AJ* a tratar tienen que ver con la telefonía móvil. El primero consiste en la secuencia directa de amplio especto o *DSSS* (*Direct Sequence Spread Spectrum*) [6]. Este tipo de señal es empleado en el estándar de segunda generación de telefonía móvil IS-95A conocida común y erróneamente como *CDMA*. Se debe recordar que *CDMA* (*Code Division Multiple Access*)

es una técnica de acceso múltiple y no un estándar. De igual forma, se emplea en el estándar de 2.5G IS-95B y en el de 3G *Cdma2000*.

El segundo tipo de señal *AJ* es el salto de frecuencia o *FHSS* (*Frequency Hopping Spread Spectrum*) [6]. El estándar de segunda generación de telefonía móvil *GSM* emplea esta técnica para lograr la diversidad de frecuencia.

Para que una señal pueda ser considerada como *AJ* es necesario que el sistema que la transmita sea un sistema *LPD* (*Low Probability of Detection*) y/o *LPI* (*Low Probability of Intercept*) [5, 6].

En un sistema *LPD* el objetivo es lograr que la señal permanezca tan oculta como sea posible. *DSSS* es un ejemplo de sistema *LPD* [5, 6]. En *DSSS* esto se logra al distribuir la señal por todo el espectro disponible, lo que hace que la potencia sea muy baja y parezca ruido. Es así que se vuelve complicado detectar si la señal es de información, o es simplemente ruido.

En un sistema *LPI* (*Low Probability of Intercept*) puede ser que se haya detectado la señal, pero mientras no se intercepte la información, ésta estará protegida [5, 6]. Un ejemplo de estos sistemas es *FHSS*. En *FHSS* la protección se logra cambiando de frecuencia constantemente. Contrario a *DSSS*, donde el ancho de banda requerido es grande, en los sistemas que emplean *FH* la señal ocupa generalmente un ancho de banda angosto que depende del propio sistema, de la aplicación y de la técnica de modulación.

Existen dos tipos de salto de frecuencia. *FFH* (*Fast Frequency Hopping*) y *SFH* (*Slow Frequency Hopping*). La diferencia radica en el número de bits de datos que “saltan”. Cuando el salto es rápido, *FFH*, existen muchos cambios de frecuencia pero se encuentran involucrados pocos bits de datos. En cambio, en *SFH* es mayor la cantidad de datos pero los cambios de frecuencia no son tan numerosos [6, 14].

Capítulo 3: Descripción de *Jamming*

3.1 Estrategias de *jamming*

Existen distintas estrategias que puede emplear un *jammer* para atacar a las diversas aplicaciones. Cada una de estas estrategias tiene sus ventajas y sus desventajas, es por eso que se debe de estudiar el "blanco" para elegir la mejor opción.

Cuando se trata de atacar sistemas que empleen señales *AJ*, el *jammer* debe de emitir una señal portadora en banda base que puede ser modulada por uno o más impulsos o bien por una señal de ruido [5, 6].

3.1.1 *Jamming* por ruido

La portadora emitida por el *jammer* es modulada por una señal aleatoria de ruido [3]. 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. Se divide en *jamming* por ruido de banda-ancha, *jamming* por ruido de banda-parcial y *jamming* por ruido de banda-angosta [5, 6].

3.1.1.1 *Jamming* por ruido de banda-ancha

El ruido de banda ancha o *BBN* (*Broadband noise*) introduce energía a través de todo el ancho del espectro de frecuencias en el que opere la aplicación blanco. A este tipo de *jamming* se le conoce también como *jamming* de banda completa. Este tipo de *jamming* es aplicable a cualquier tipo de señal *AJ* [6].

El nivel de potencia de *jamming* se denomina J_0, y está medido en Watts/Hertz. La principal limitante de este tipo de *jamming* es que tiene un bajo J_0, ya que la potencia es esparcida en una parte amplia del espectro.

El *BBN jamming* funciona elevando el nivel de ruido en el receptor lo que ocasiona un decremento en la relación señal-a-ruido [5, 6, 7]. La eficiencia de este tipo de *jamming* depende del nivel de potencia y por tanto de la distancia entre el *jammer* y el receptor.

3.1.1.2 *Jamming* por ruido de 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 [5, 6].

3.1.1.3 *Jamming* por ruido de banda-angosta

Conocido como *NBN* (*Narrowband noise*), 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 [5, 6].

3.1.2 *Jamming* por tonos

Esta estrategia consiste en colocar uno, *single-tone (ST)*, o varios, *multiple-tone (MT)*, tonos a lo largo del ancho de banda donde se encuentra la señal *AJ* [6]. 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* es posible emplear *single-tone jamming* para modificar el *offset* en los receptores y ocasionar que se sobrepase el nivel máximo de la señal, lo que produce que no se pueda recibir la información. La relación entre la fase del tono emitido por el *jammer* y la fase de

la señal es un parámetro importante. Si se manda un solo tono, éste estará presente ya sea en la frecuencia del cero o del uno. Si se encuentra en la frecuencia del uno entonces la fase representa un problema, ya que si el tono no se encuentra en fase no se podrá bloquear o interferir la transmisión del símbolo. En cambio si el tono se encuentra en la frecuencia del cero, entonces podrá bloquear la transmisión al símbolo siempre y cuando la potencia sea adecuada sin depender de la fase [5, 7].

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 de colocan en canales continuos se conoce a este particular caso de *MT* como *comb jamming* [6].

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

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

3.1.3 *Jamming* por pulsos

Esta estrategia es similar en resultados al *jamming* por ruido de banda-parcial. En este caso el factor a tomar en cuenta no es el ancho del espectro cubierto, sino el tiempo que es *jamme*r está encendido. A pesar de que una de las estrategias se enfoca a frecuencia y la otra a tiempo, la eficiencia es prácticamente la misma. Sin embargo, cuando se analiza el funcionamiento se encuentran similitudes con el *jamming* por ruido de banda-ancha. Esto se debe a que el tiempo que está encendido, el *jammer* que trabaja por pulsos abarca una

parte amplia del espectro. Esta estrategia ahorra de manera considerable la potencia, lo que la hace eficiente si se diseña correctamente el ciclo de trabajo [5, 7].

3.1.4 *Jamming* por barrido

Es un concepto similar al de ruido por banda-ancha o por banda-parcial [6, 8]. De hecho se puede considerar como una estrategia complementaria. 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* [5]. Sin embargo, se tiene que considerar que el barrido debe de ser tan rápido como para identificar la frecuencia en la que se encuentre la señal pero sin llegar a una velocidad tal, que cuando se sitúe sobre el salto se tenga efecto solamente sobre una parte de él. Supongamos que para lograr interferir un sistema de comunicación se debe tener un *BER* de $10^{-1.}$ Un *BER* de 10^{-1} significa que es necesario bloquear la transmisión de un bit de diez, o para un sistema *AJ* que está mandando datos a una velocidad de 20kbps, la transmisión de 2000 bits debe ser bloqueada para alcanzar este *BER*. Si este sistema es de tipo *SHF* y maneja 100 saltos por segundo, cada salto contendrá 200 bits (sin considerar el tiempo entre saltos). De ahí que se necesite aplicar de manera exitosa *jamming* sobre 10 saltos por segundo. Ya que estos saltos pueden estar en todo el espectro asignado, al menos 10 barridos por segundo son necesarios para que el *jammer* sea eficiente.

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

3.1.5 *Jamming* por seguimiento

Esta estrategia se aplica generalmente a sistemas *FHSS*. Consiste en localizar la frecuencia a la cual “saltó” la señal, identificar la señal como el blanco y emplear *jamming* por ruido, tonos o pulsos. Se conoce también como *jamming* de respuesta y *jamming* de repetición [5].

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

Además de esto existen otros problemas. Si se aplica *jamming* al mismo tiempo en más de un canal, la potencia estará distribuida entre estos y probablemente no será suficiente para reducir la relación señal-a-ruido a un nivel donde no puede existir comunicación. Incluso las distintas modulaciones son un escudo ante esta estrategia. Por ejemplo, si se emplea *BFSK* como técnica de modulación el *jammer* no sabe cuál es el canal complementario. En este caso la probabilidad de que el *jammer* sea eficiente se reduce a la mitad. Es por estas razones que a pesar de ser un estrategia eficiente cuando se diseña correctamente, es muy compleja y no representa una opción de sencilla implementación [5, 6].

3.1.6 *Jamming* inteligente

Es común que cuando se aplica alguna estrategia de *jamming* sobre una señal *AJ*, se desperdician recursos y no siempre se elige la opción más adecuada. Cuando se conoce como funciona el sistema que se desea atacar, se pueden optimizar los recursos. Realmente el *jamming* inteligente no es una estrategia como las anteriores, sino que se refiere al estudio del blanco para lograr mejores resultados. Por ejemplo, se puede atacar la señalización en sistemas de telefonía móvil para evitar el uso de móviles [5, 7].

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

Dentro de este tipo de *jamming* se encuentra el *jamming* de engaño. En esta estrategia se envía un mensaje falso para mantener a una de las partes del sistema de comunicación en estado de recepción. De esta manera, se logra que nunca haya confirmación de que se recibió el mensaje y se genera una interrupción en la comunicación. Otra manera de engañar al sistema sobre el cual se aplica *jamming*, es interceptar la señal del transmisor y con ello establecer una ruta de comunicación incorrecta [5, 7].

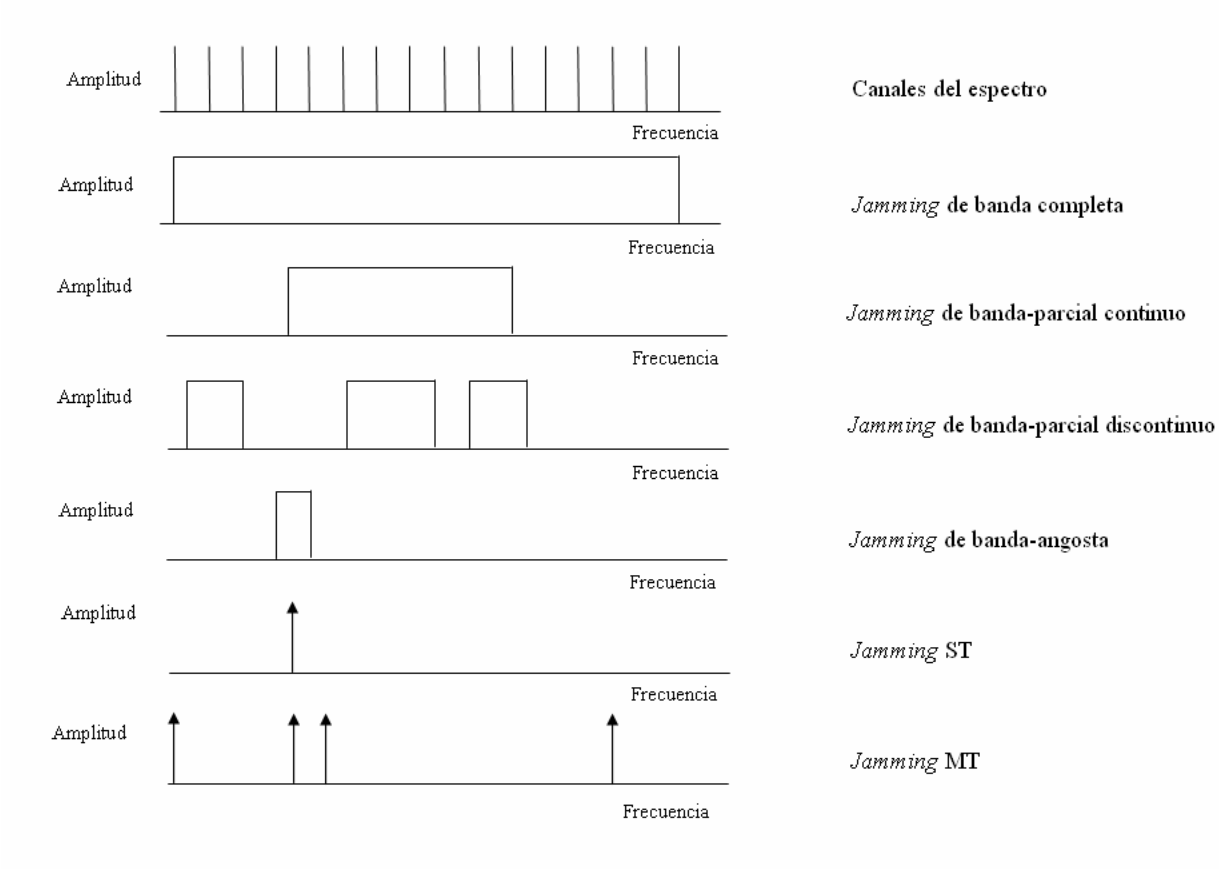

Figura 3.1 Estrategias de j*amming*

3.1.7 Técnicas para incrementar la eficiencia del *jammer*

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

técnicas que involucran el compartir la potencia entre los distintos blancos y el poder encender y apagar el *jammer* por determinado tiempo para dedicarlo a uno o a otro blanco.

3.1.7.1 *Look-Through*

Cuando las señales no son de espectro extendido, esta técnica es empleada para determinar si el blanco ha cambiado de frecuencia o simplemente ha dejado de operar. Esto se hace para no malgastar la potencia y de esta manera emplearla en más de un objetivo o simplemente ahorrarla. Al momento de apagar el *jammer* se mide la actividad en el espectro y se determina si el blanco está en funcionamiento o no. Podría pensarse como solución para sistemas *FH* y como una forma de *jamming* por seguimiento. Sin embargo, debido a la velocidad de salto no se emplea esta técnica para tal propósito. Esta técnica se puede aplicar a sistemas *DSSS* siempre y cuando se pueda detectar su actividad [5, 7].

3.1.7.2 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 [5].

3.1.7.3 Tiempo compartido

Otra técnica para cubrir más de un blanco es orientar la máxima potencia del *jammer* hacia cada blanco pero en momentos distintos. Cuando se aplica *jamming* a una señal digital no se tiene que estar todo el tiempo introduciendo ruido. Basta con incrementar el *BER* hasta cierto nivel. En el caso de las comunicaciones de voz el nivel necesario para cortar la transmisión es más alto que en el caso de datos. En el caso de las comunicaciones de voz analógicas es necesario bloquear o interferir solamente un 30% de la transmisión para que no entienda el mensaje. De ahí que el *jammer* pueda estar orientado a distintos blancos en diferentes momentos [5].

3.2 Clasificación general de *jammers*

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

3.2.1 *Jammer* constante

Este tipo de *jammer* emplea la estrategia de ruido y la de barrido. Su principal ventaja es la relativa facilidad de implementarse. Sin embargo, en aplicaciones donde se desea que el *jamming* pase desapercibido no es recomendable emplear un *jammer* constante [8]. Esto se debe a que al momento de analizar la transmisión de la información se detectará ruido que excede los niveles comunes. Una vez detectado el ruido es posible encontrar la fuente que lo genera. Además de esta desventaja, es necesario considerar que la potencia requerida es grande.

3.2.2 *Jammer* de engaño

Emplea la técnica de engaño que pertenece al *jamming* inteligente. En este caso se envían señales que parecen ser legítimas, pero no se incluye una separación entre ellas. Esto ocasiona que se mantenga el estado de recepción y no haya confirmación de haber recibido información alguna [8]. Este tipo de *jammer* logra mayor invisibilidad que el constante. Sin embargo, aún es posible detectarse. La potencia requerida también es grande.

3.2.3 *Jammer* aleatorio

Este tipo de *jammer* funciona por determinado tiempo y deja de hacerlo por otro [8]. Los tiempos son programados y se debe hacer conocer la aplicación para obtener resultados positivos. Se puede utilizar *jamming* por ruido, por pulsos, por tonos e incluso por barrido [6]. La potencia es menor debido a que no se encuentra en operación todo el tiempo. La detección es posible al realizar un análisis de la actividad de la red.

3.2.4 *Jammer* reactivo

Este tipo es el más complejo pero es el que ofrece una menor posibilidad de ser detectado. Consiste en sensar la actividad de la red para saber en que momento debe de actuar el *jammer* [8]. 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.

Capitulo 4: La telefonía móvil

4.1 Historia de la telefonía móvil

La telefonía móvil se forma básicamente por dos elementos: la red de comunicaciones y las terminales. En su versión análoga, fue presentada por primera vez en los Estados Unidos en 1946. En ese año el servicio se brindaba en 25 grandes ciudades y cada ciudad tenía una estación base que consistía en un transmisor de alta potencia y un receptor colocados en lo alto de una montaña o torre. Este servicio tenía una cobertura de aproximadamente 30 millas a la redonda. A este primer estándar de telefonía móvil se le conoció como *MTS (Mobile Telephone System)*, y funcionaba con una comunicación de tipo *half-duplex*. Tiempo después, a principio de los 50 la *FCC* duplicó el número de canales destinados a la telefonía móvil, reduciéndolos de 120kHz a 60kHz, con lo que se logró una comunicación *full-duplex*. Esto último fue la gran ventaja de *IMTS (Improved Mobile Telephone System)* en comparación con su antecesor [14, 15].

En 1960 *AT&T* presentó la marcación directa. Es necesario mencionar que antes una operadora era la que enlazaba las llamadas y que esto representó un gran avance. Tiempo después, la misma compañía propuso el concepto celular a la *FCC*. A mediados de los 70 este concepto fue desarrollado en conjunto con minicircuitos integrados capaces de manejar los complejos algoritmos necesarios para la conmutación y el control de los canales de comunicación. El ancho de banda se redujo de nuevamente de 60kHz a 30kHz [14, 15].

En 1974 la *FCC* destinó 40MHz extras del espectro para la telefonía móvil. Un año después la *FCC* otorgó a *AT&T* la primera licencia para operar una telefonía celular en desarrollo en la ciudad de Chicago. Al otro año, fue *ARTS (American Radio Telephone Service)* la que recibió autorización para operar en Baltimore [14, 15].

Sin embargo, fue hasta 1983 cuando la telefonía celular comenzó a crecer exponencialmente. Ese año *AMPS (Advanced Mobile Phone System)* se convirtió en el primer estándar de telefonía celular. Este estándar originalmente ocupaba 40MHz de ancho de banda en la banda de los 800MHz, pero en 1989 se le otorgaron 166 canales *half-duplex*

adicionales. Fue en este año que la telefonía celular incursionó en México por medio de dos empresas: Iusacell y Telcel [14, 15].

En 1991 se comenzaron a brindar los primeros servicios digitales en la mayor parte de los Estados Unidos, logrando usar el espectro de una manera más eficiente. La mayor ventaja de los servicios digitales consistió en la comprensión de voz, lo que dejó espacio en el ancho de banda asignado para nuevas aplicaciones [14].

En ese momento de la historia de la telefonía móvil se formaron dos caminos. La diferencia entre éstos radicaba en la técnica de acceso múltiple empleada, fuera *TDMA (Time Division Multiple Access)* o *CDMA (Code Divison Multiple Access)*. En comparación con la técnica empleada por AMPS u otros estándares de primera generación, *FDMA (Frequency Division Multiple Access)*, las dos ofrecían grandes ventajas. Por ejemplo, la capacidad especificada en *USDC (U.S. Digital Cellular)* o IS-54 equivale a tres veces la capacidad de *AMPS* [14].

En esta segunda generación de telefonía móvil surgieron diferentes estándares, entre los que destacan: IS-54, IS-95, *GSM*, *iDEN* y *PDC*. Con el tiempo fue *GSM* el que logró mayor aceptación a nivel mundial, a pesar de que en sus inicios se concentró en el continente Europeo. La mayoría de estos estándares evolucionaron en un paso intermedio conocido como 2.5G [14].

2.5G es utilizado para denominar a los estándares que implementaron conmutación de paquetes en sus redes en conjunto con la conmutación de circuitos. Mientras que los términos 2G y 3G son reconocidos oficialmente, 2.5G no lo es. Este término fue inventado simplemente con fines publicitarios y de ventas [14, 15].

Un ejemplo de lo que es considerado un servicio de 2.5G es *GPRS (General Packet Switching Service)* implementado en las redes *GSM*. *GPRS* emplea conmutación de paquetes para la comunicación de datos, y es por esto que se dice que 2.5G ofrece algunos servicios de 3G. Otro caso particular de las redes *GSM* como ejemplo de proveedora de

servicios similares a los de 3G es *EDGE (Enhanced Data Rates for GSM Evolution)*, el cual es una tecnología que permite aumentar la tasa de transmisión de datos y su confiabilidad hasta 236.8 kbit/s [14].

En los primeros años de esta década la telefonía móvil evolucionó hacia otra generación, 3G. Esta tercera generación ofrece servicios de videoconferencia e Internet de alta velocidad. A diferencia de 2.5G, 3G no consiste en mejoras a las redes 2G y no opera en el mismo espectro de frecuencia. Es por eso necesario construir nuevas redes y adquirir nuevas concesiones de frecuencias. El primer país que ofreció 3G fue Japón. En 2005, 40% de los suscriptores emplean solamente redes de tercera generación. Es así que en 2006 la transición entre generaciones se completó. Incluso ya se habla de mejoras bajo el nombre de 3.5G. Estas mejoras incrementaran la máxima velocidad de 2Mbit/s a 3Mbit/s [14].

4.2 Concepto Celular

Cuando la telefonía móvil dejó de tener una sola estación base por red para migrar a la telefonía celular se corrigieron muchos problemas. Las claves de este concepto fueron develadas en 1947 por investigadores de los laboratorios *Bell* y otras compañías de telecomunicaciones alrededor del mundo. Se determinó que si se subdividía un área geográfica relativamente grande, llamada zona de cobertura, en secciones más pequeñas, llamadas células, el concepto de reuso de frecuencias podrías ser empleado para incrementar considerablemente la capacidad del canal [15].

4.2.1 Célula

Una célula es una zona geográfica de cobertura proporcionada por una estación base. Idealmente se representa por un hexágono que se une con otros para formar un patrón tipo enjambre. La forma hexagonal fue elegida porque provee la transmisión más efectiva al aproximarla con una forma circular y permite unirse a otras sin dejar huecos, lo cual no hubiera sido posible al elegir un círculo. Una célula se define por su tamaño físico, pero más importantemente por la cantidad de tráfico y población que existe en ella. El número de células por sistema no está especificado y depende del proveedor del servicio y de los patrones de tráfico que observe en su red. El tamaño de la célula varía dependiendo de la

densidad de usuarios. Por ejemplo, en una zona rural se coloca una macrocélula. Este tipo de célula tiene una cobertura de entre 1 y 15 millas a la redonda con una potencia que varía de 1 a 20 watts. Por el contrario, las microcélulas radian de 1 a varios cientos de pies con potencias de 0.1 a 1 watt. Este tipo de células son frecuentemente usadas en ciudades.

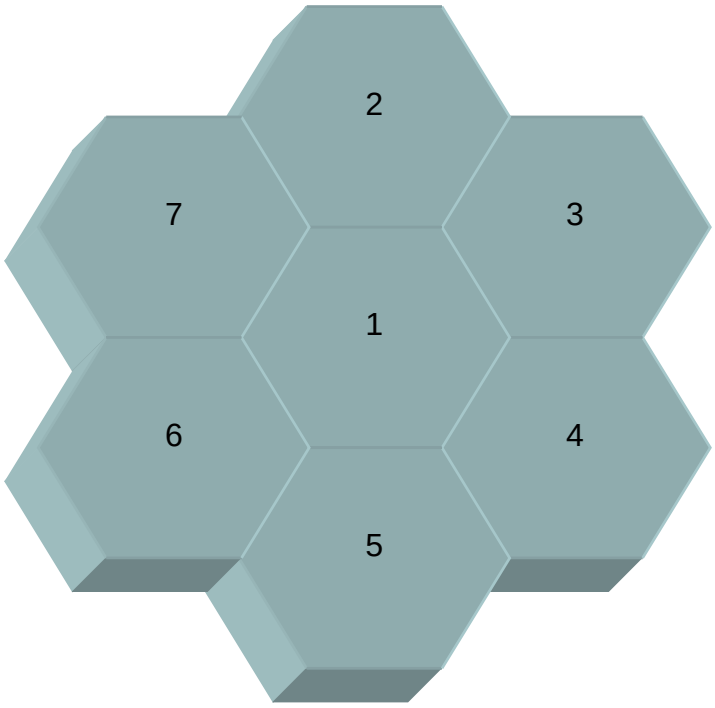

Figura 4.1 Células de la telefonía móvil

En la Figura 4.1 se puede observar la forma ideal de las células y como están colocadas adyacentemente. Sin embargo, la forma real de las células no tiene forma. Esto se debe a los obstáculos que encuentra la señal en el camino, lo que depende de cada zona. Las células ideales se emplean para planificar y dimensionar un sistema considerando un nivel de potencia idéntico para toda el área de cobertura. Esta planificación se vuelve más precisa al emplear herramientas de cómputo que consideran la estructura de la ciudad con edificios, parques, etc. Un concepto importante al hablar de células es el de *hand-off* o *hand-over*. Este proceso ocurre cuando el usuario cambia de una célula a otra y el móvil obtiene un canal sin perder la comunicación. Para saber cuando debe ocurrir el *hand-off* se define un umbral de potencia que generalmente es de -95dBm. Al momento de registrar una señal a esta potencia el móvil busca otra señal con mejor potencia en la célula a la que está entrando [14, 15].

4.2.2 Reuso de frecuencias

Básicamente el reuso de frecuencias permite que un gran número de usuarios puedan compartir un número limitado de canales disponibles en la región. Esto se logra asignando el mismo grupo de frecuencias a más de una célula. La condición para que esto se pueda hacer es la distancia entre ellas, de no hacerlo la interferencia sería alta. A cada estación base se le asigna un grupo de canales que son diferentes de los de las células vecinas, y las antenas de las estaciones base son elegidas para lograr un patrón de cobertura dentro de la célula por medio de la modificación de parámetros como ganancia y directividad [15].

Cuando se diseña un sistema usando células hexagonales, los transmisores de la estación base se colocan en el centro de la célula *(center-excited cells)* o en tres de los seis vértices *(corner-excited cells)*. Normalmente se usan antenas omnidireccionales para el primer caso y antenas sectorizadas para el segundo. Esta sectorización es una forma de subdividir la célula y lograr mayor capacidad. Comúnmente esta división se hace en 3 sectores. Al hacer esto no todo son ventajas. Entre las principales desventajas destacan el aumento de equipo de propagación en la estación base, el cambio constante de canales en la unidad móvil y la disminución en truncamiento por la división de canales dentro de la célula. Aún así es muy común sectorizar la célula, sobretodo en lugares donde la densidad de población es alta [14].

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

$$F = GN \quad \textbf{Ecuación 4.1}$$

donde F es el número de canales *full-duplex* disponibles en un cluster, G es el número de canales en una célula y N el número de canales en el *cluster* o factor de reuso de frecuencia. Se denomina *cluster* a las células que colectivamente usan un conjunto de canales disponibles. Es necesario decir que no es posible darle cualquier valor a N por la geometría de las células. Algunos valores posibles son 3, 4, 7, 12, 13, 19 y 27. Los más comunes son el 3 y el 7 [14].

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

$$C = mGN \quad \textbf{Ecuación 4.2}$$

donde *C* representa la capacidad del canal y *m* el número de clusters. Se puede apreciar que la capacidad del canal es directamente proporcional al número de veces que un *cluster* es multiplicado [14].

4.3 *GSM (Global System for Mobile Communications)*

El servicio de *GSM* empezó en 1991 y en 1993 operaba en 22 países. Actualmente se tienen este tipo de redes en más de 80 países. *GSM* es un sistema de telefonía celular perteneciente a la segunda generación que se desarrolló para solucionar los problemas de compatibilidad existentes en la primera generación, sobretodo en Europa donde se creó el estándar. Fue el primer sistema completamente digital y con casi 50 millones de usuarios en el mundo se ha convertido en el estándar más popular [14, 15].

4.3.1. Servicios y arquitectura

Los servicios de *GSM* se clasifican en tres tipos: *bearer services*, teleservicios y servicios suplementarios. Los primeros ofrecen la capacidad de transmitir señales entre puntos de acceso, los segundos permiten comunicarse con otros suscriptores y los últimos complementan los teleservicios [15].

La arquitectura de una red *GSM* se muestra en la Figura 4.2. Consiste de tres subsistemas conectados entre si y con los abonados. Estos sistemas son:

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

El *BSS* a veces se conoce como subsistema de radio porque provee y maneja las rutas de transmisión de radiofrecuencia entre las unidades móviles y el *MSC (Mobile Switching Center)*. El *BSS* también maneja la interfaz de radio entre las estaciones móviles y los otros subsistemas. Cada *BSS* consiste de varios *BSC (Base Station Controllers)* que son usados para conectar la estación móvil o *BTS (Base Transceiver Station)* con el *NSS* a través de uno o varios *MSC (Mobile Switching Center)*. El *NSS* maneja las funciones de conmutación y permite al *MSC* comunicarse con otras redes. El *OSS* apoya la operación y mantenimiento del sistema. Permite monitorear, diagnosticar y resolver problemas dentro de la red *GSM* [15].

GSM fue originalmente diseñada para 200 canales *full-duplex* por célula con frecuencias de transmisión en la banda de 900MHz. Sin embargo, tiempo después se asignaron frecuencias en la banda de 1800MHz. Un segundo sistema, llamado *DSC 1800 (Digital Cellular System 1800)* fue establecido con las mismas características que tiene *GSM*. De igual manera, *PCS 1900 (Personal Communication Services 1900)* se deriva de *GSM* y es utilizado ampliamente en Norteamérica. Estos tres sistemas admiten el uso de un módulo de identidad de suscriptor conocido como *SIM (Subscriber Identity Module)*, lo que permite que un usuario pueda acceder a los servicios sin tener siempre la misma unidad móvil y en cualquier parte del mundo donde exista una red *GSM* [14].

En México, *GSM* trabaja de 1850MHz a 1910MHz para el enlace de móvil a estación base o *uplink* y de 1930MHz a 1990MHz para el enlace de estación base a móvil o *downlink* [20]. *GSM* emplea una combinación de *FDMA* y *TDMA* como técnica de acceso múltiple para proveer a las estaciones base acceso simultáneo a varias unidades móviles. Las bandas disponibles se dividen en canales de 200kHz y éstos son compartidos por 8 usuarios. Cada usuario ocupa una ranura tiempo por medio de *TDMA*. La tasa de transmisión en ambas direcciones es de 270.833kps para todo el canal y de 33.833kbps para cada usuario, esto se logra por medio de modulación *GMSK (Gaussian minimum shift keying)* [14].

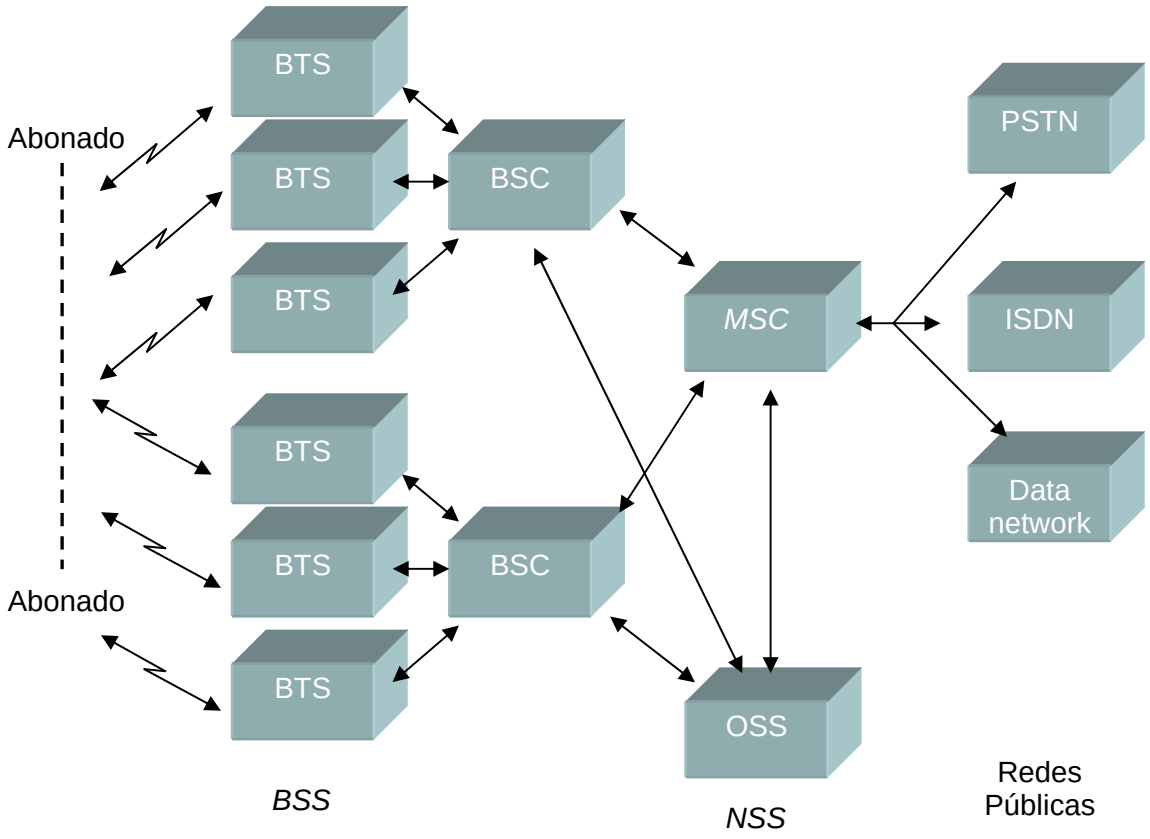

Figura 4.2 Arquitectura *GSM*, donde *BTS = Base Transceiver Station, BSC = Base Station Controller, MSC = Mobile Switching Center, OSS = Operational Support Subsystem, PSTN = Public Switched Telephony Network, ISDN = Integrated Services Digital Network, BSS = Base Station Subsystem, NSS = Network and Switching Subsystem*

4.3.2 Salto en frecuencia

En la propagación de radio frecuencia el canal presenta desvanecimiento de frecuencia selectiva. Esto quiere decir que las condiciones o características para la transmisión varían dependiendo de la frecuencia individual que se maneje. Así mismo, la propagación de la señal es multiruta. Esto ocasiona efectos indeseables en la comunicación. Como alternativa para solucionar estos dos problemas, *GSM* utiliza salto de frecuencia. Existen dos tipos de salto de frecuencia. *FFH* (*Fast Frequency Hopping*) y *SFH* (*Slow Frequency Hopping*) [6]. La diferencia radica en el número de bits de datos que "saltan". Cuando el salto es rápido, *FFH*, existen muchos cambios de frecuencia pero se encuentran involucrados pocos bits de

datos. En cambio, en *SFH* es mayor la cantidad de datos pero los cambios de frecuencia no son tan numerosos.

GSM emplea *SFH* para:

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

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

Capítulo 5: Diseño del *jammer*

El objetivo del *jammer* diseñado es bloquear la comunicación de equipos móviles en el mayor rango posible de la banda *PCS (Personal Communications Services)* y a una corta distancia. La Figura 5.1 muestra la asignación de frecuencias para la región 8 de México, es decir, Veracruz, Puebla, Oaxaca y Tlaxcala [20]. El apéndice B muestra una gráfica sobre la distribución de la banda *PCS* en nuestro país.

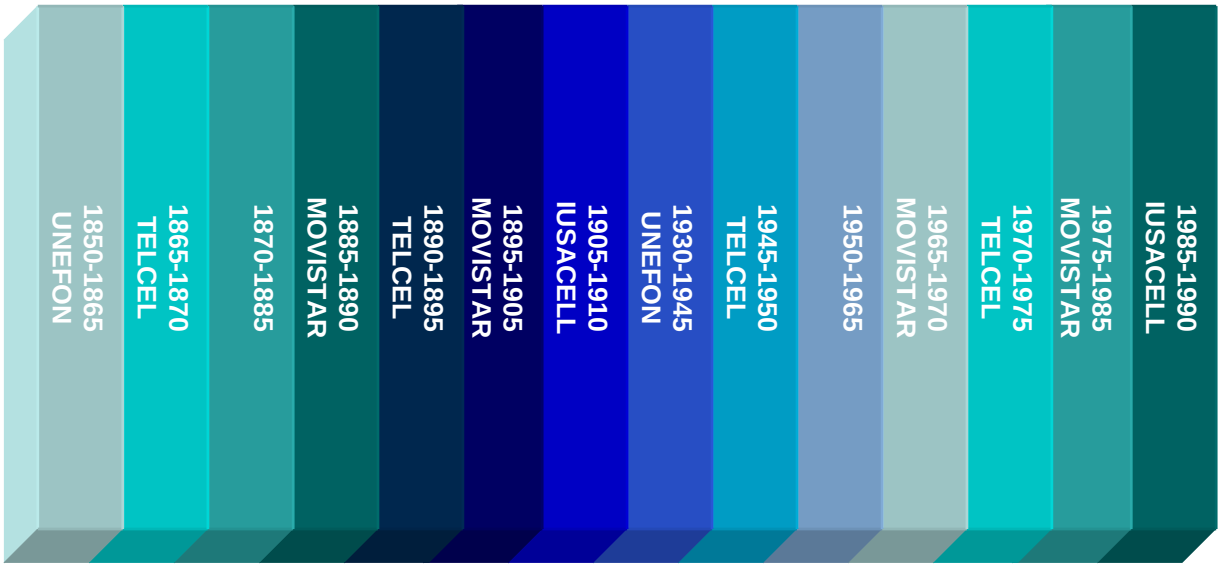

Figura 5.1 Asignación de la banda PCS para la región 8 de México. Las frecuencias están en MHz [20].

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

Al analizar las distintas técnicas y estrategias de *jamming* presentadas en este trabajo de tesis mediante una comparación del factor complejidad-beneficio se ha llegado a la conclusión de que la estrategia de barrido es la ideal. Las demás se descartaron por las siguientes razones:

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

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

- ✓ La estrategia de tonos no es efectiva ante sistemas que empleen *Frequency Hopping*.

- ✓ El *jamming* por pulsos no sería efectivo porque el *jammer* enciende y apaga y se requiere que esté encendido en todo momento. Esto para simplificar el diseño. En este caso el ahorro de potencia no es tan importante como si se tratase de un *jammer* portátil.

- ✓ El *jamming* por seguimiento no se eligió por la complejidad que representa su diseño. El tiempo no sería suficiente para depurar toda la implementación.

Se eligió el *jammer* por barrido porque se pretende utilizar toda la potencia disponible en cada parte del espectro y por momentos distintos. La potencia es importante pero no demasiado porque, como se ha dicho, no se trata de un *jammer* portátil. 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.

Respecto al tipo de *jammer* se ha elegido el de tipo constante. Una vez más el tema del *jammer* no portátil y la potencia surgen. Los demás no se eligieron porque el reactivo y el de engaño son muy complejos y se pretende sencillez, el aleatorio no se eligió porque se desea que el *jammer* trabaje en todo momento.

5.2 Descripción del circuito

Para que un *jammer* utilice como estrategia el barrido funcione se debe implementar el circuito de la Figura 5.2.

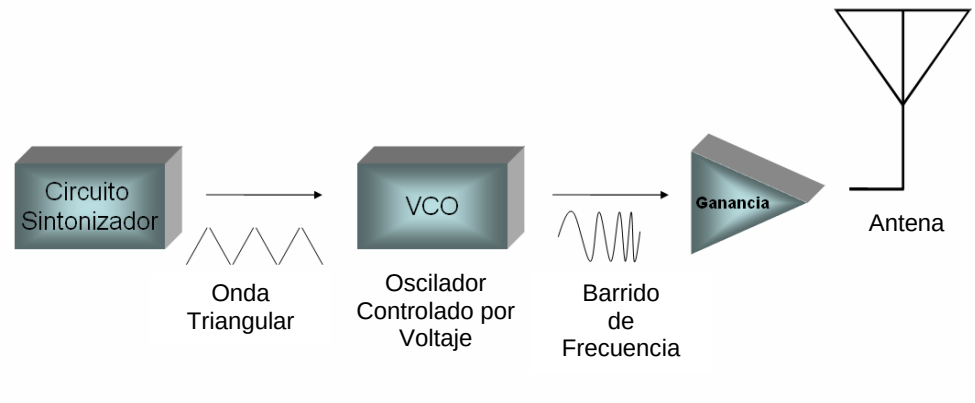

Figura 5.2 Diagrama a bloques del *jammer*

5.2.1 Oscilador controlado por voltaje

El centro medular del *jammer* es el oscilador controlado por voltaje. Al principio se tenían dos opciones, comprarlo o hacerlo. Debido a que las frecuencias a las que se va a trabaja son del orden de gigahertz, la fabricación del VCO es complicada. La dificultad radica en la depuración, ya que a esas frecuencias cualquier componente puede funcionar como antena. Es por eso que se optó por comprar el VCO. Se eligió el modelo JTOS-2000 de *Minicircuits*®. Teóricamente este VCO hace un barrido de 1370 a 2000MHz. Este rango incluye cualquier operadora de telefonía móvil que trabaje sobre la banda PCS. El voltaje que se debe suministrar para el barrido en frecuencia va de 1 a 22 V como se puede ver en la Tabla 6.1. En la misma tabla se puede ver que el barrido debe ser de 14V a 18V para garantizar la cobertura de la banda *PCS*.

Tabla 5.1 Relación entre el voltaje sintonizador y la frecuencia de salida para el JTOS-2000

Voltaje de entrada (V)	Frecuencia (MHz)
1.00	1266.03
3.00	1364.13
5.00	1446.30
7.00	1530.72
9.00	1621.98
11.00	1715.81
13.00	1807.46
15.00	1890.65
17.00	1958.16
19.00	2015.46
21.00	2060.55
22.00	2081.16

5.2.2 Sintonizador

El circuito sintonizador tiene la tarea de suministrar el voltaje de entrada al VCO. Esto se puede hacer mediante una onda de diente de sierra o una triangular. Para esta parte del *jammer* se ha optado por el XR-2206 de *EXAR*®. Este integrado es un generador de funciones del que se pueden obtener señales senoidales, cuadradas y triangulares con frecuencias superiores a 1MHz y voltajes máximos cercanos a los 20V. El aspecto de la frecuencia es muy importante debido a que *GSM* es un sistema que emplea *SFH,* y de esta forma puede ser que los saltos en frecuencias protejan a la comunicación de la interferencia generada por el *jammer*. Lo anterior presenta dos escenarios: Si la variación del voltaje sintonizador es muy lenta no se alcanzará a barrer una parte amplia del espectro de manera que se intercepten los saltos en frecuencia; si la variación es muy rápida no será suficiente el tiempo que la señal del *jammer* interfiera con la señal original para imposibilitar la comunicación. La Figura 5.3 muestra las conexiones para el XR2206 con sus componentes externos.

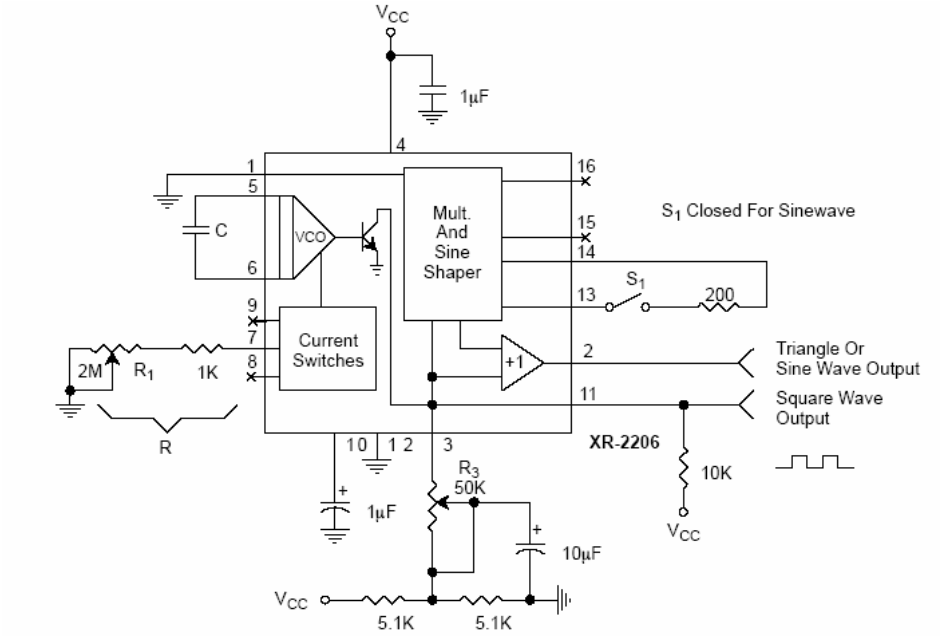

Figura 5.3 Conexiones para el generador XR-2206

La frecuencia se puede variar mediante el capacitor, C, en las terminales 5 y 6 y el potenciómetro conectado en serie con la resistencia de la terminal 7, R_1, mediante la ecuación 5.1.

$$f = \frac{1}{RC}$$ **Ecuación 5.1**

El valor máximo del capacitor, C, es de 100µF y la resistencia, R_1, puede llegar hasta 2MΩ. El valor de C para este *jammer* es de 100pF y la resistencia es variable. La amplitud varía por medio del potenciómetro R_3, y aumenta a razón de 160mV/kΩ para la onda triangular y de 60mV/kΩ para la onda senoidal.

5.2.3 Acondicionamiento de la señal

El acondicionamiento de la señal referente al *offset* corre a cargo de un transistor BJT 2N2222 y de un conjunto de resistencias, una de las cuales es variable. Tanto la amplitud como la frecuencia pueden ser modificadas por medio de dispositivos externos al generador de funciones.

Es así que el circuito posee tres potenciómetros multivueltas con valores de 500kΩ (frecuencia), 50kΩ (amplitud) y 500Ω (offset). Los ajustes son necesarios porque la realidad difiere de la teoría, y al presentarse estas variaciones es necesario acondicionar la señal que alimenta al VCO. Además, al afectarse la frecuencia se altera la amplitud y el *offset* debido a características propias del integrado. La amplitud debe estar entre 14V y 18V, el *offset* debe tener el valor requerido para que el voltaje mínimo sea de 14V y la frecuencia un valor entre 1.5 GHz y 1.8GHz para garantizar la interrupción de la comunicación entre radiobase y unidad móvil. El valor exacto y óptimo se obtiene mediante prueba y error debido a la inexistencia de un método.

5.2.4 Línea de transmisión y antena

La línea de transmisión es de tipo coplanar porque el JTOS-2000 es de montaje superficial y gran número de sus terminales van conectadas al plano de tierra. Las dimensiones de la línea para lograr un acoplamiento a 50Ω se muestran en la Figura 5.4.

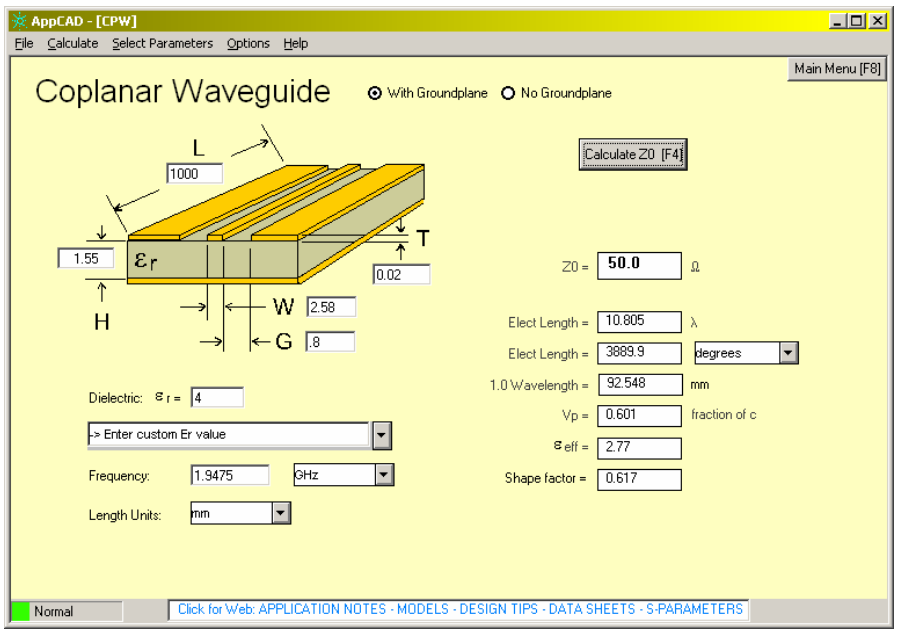

Figura 5.4 Dimensiones de la línea coplanar [23]

El dieléctrico empleado para la placa del circuito es fibra de vidrio fabricada en México. Se eligió este material por su disponibilidad y precio. La caracterización de este material fue realizada en el INAOE y arrojó los siguientes resultados [22]:

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

En la Figura 5.4 se puede ver que la frecuencia, la constante dieléctrica y las alturas del dieléctrico y del metal son parámetros importantes para obtener las dimensiones que garanticen la transferencia de energía.

Por último, la antena con la que trabaja el *jammer* es una *OMA* de 7 segmentos desarrollada en la Universidad de las Américas Puebla [22]. Se eligió esta antena porque presenta un ancho de banda ideal para este proyecto y porque tiene una buena ganancia, es decir, no presenta pérdidas considerables entre la señal con que se alimenta y la radiación que produce. Sus características se pueden ver en la tabla 6.2. La conexión entre la antena y la línea de transmisión se hace por medio de conectores *SMA (SubMiniature version A)*. Este tipo de conectores están acoplados a 50Ω y garantizan la transferencia de energía a frecuencias hasta de 18GHz.

Tabla 5.2 Características de la antena OMA de 7 segmentos [22]

Punto mínimo de S11	-14.007 dB a 1.948 GHz
Ancho de banda (-8dB)	1.5535 – 2.016 GHz: 23.742 %
Ancho de banda (-10dB)	1.6235 – 1.9944 GHz 19.04%
Potencia transmitida	5dBm
Potencia recibida (pol. dir.)	-27dBm
Potencia recibida (pol. cruz.)	-35 dBm
Ganancia	5dBd = 7.15 dBi

La ganancia proporcionada por la antena es suficiente para cubrir un área de aproximadamente 4 metros a la redonda. No es el propósito de este prototipo cubrir zonas más grandes porque, como se ha explicado en el capítulo sobre el marco legal, se estaría incurriendo en una falta.

5.2.5 Alimentación

La alimentación del circuito se toma de la línea de 120. Para rectificar esta señal se usa un transformador a 18V, un puente rectificador de diodos AM154 y un capacitor de 470uF para garantizar la eliminación del rizo. Una vez rectificada la línea se obtienen las salidas necesarias para alimentar al generador, al BJT y al VCO. Los dos primeros requieren voltajes de alimentación de 24V, mientras que el VCO requiere 8V para su funcionamiento. Estas salidas se logran por medio de reguladores de voltaje MA7824, con 24V de salida, y MA7808 con 8 V de salida. Para evitar ruido por parte de la fuente de alimentación, la impresión de esa parte del circuito está en otra placa impresa. Con el mismo fin, se colocan capacitores de acoplamiento. En este caso se utilizaron juegos de 3, 1 de 1μF y 2 de 0.47μF, para los voltajes de 24 V y 8 V. Para los integrados XR-2206 y JTOS-2000 se emplearon capacitores de 1μF para cada uno.

El apéndice D muestra los diagramas para el *jammer* y para la fuente de alimentación; la fabricación del *jammer* se muestra en el apéndice E.

Capítulo 6: Simulación del *jammer*

Las etapas del circuito simuladas fueron dos: el ajuste del *offset* y el acoplamiento de la línea de transmisión.

6.1 Simulación del *Offset*

Para la simulación del *offset* se utilizó *Orcad Capture 9.2.3.p006* y *Pspice 9.2.3*. Para esta simulación y debido a que no se cuenta con el integrado XR-2206 en *Orcad Capture*, se utilizaron valores reales que fueron obtenidos del circuito mostrado en la Figura 6.3. Los valores arrojados por este circuito fueron:

- Voltaje mínimo: 10 V
- Voltaje máximo: 13.72 V
- Frecuencia: 1.712 GHz

La Figura 6.1 muestra el circuito encargado de modificar el *offset*. Se basa en un transistor BJT 2N2222. El objetivo del acondicionamiento es una señal triangular de aproximadamente 14 V a 18 V.

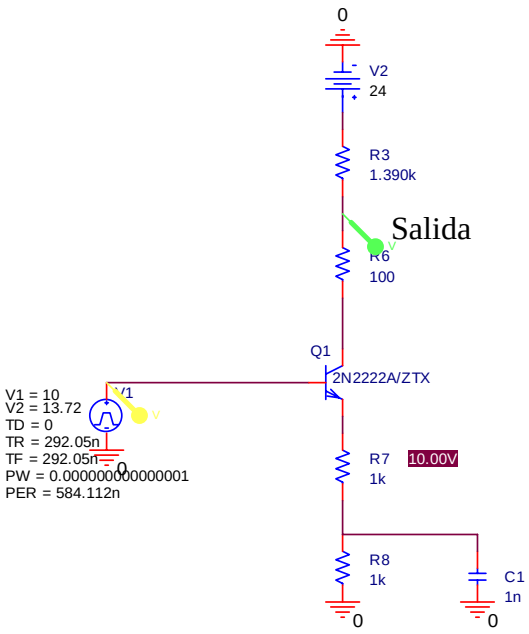

Figura 6.1 Circuito encargado del *offset*[26]

La Figura 6.2 muestra el resultado de esta simulación. Se puede ver que el valor máximo es de 18.737 V y el mínimo de 13.867 V. En el circuito R_3 se sustituye por un potenciómetro de 500 Ω para ajustar el nivel de *offset*.

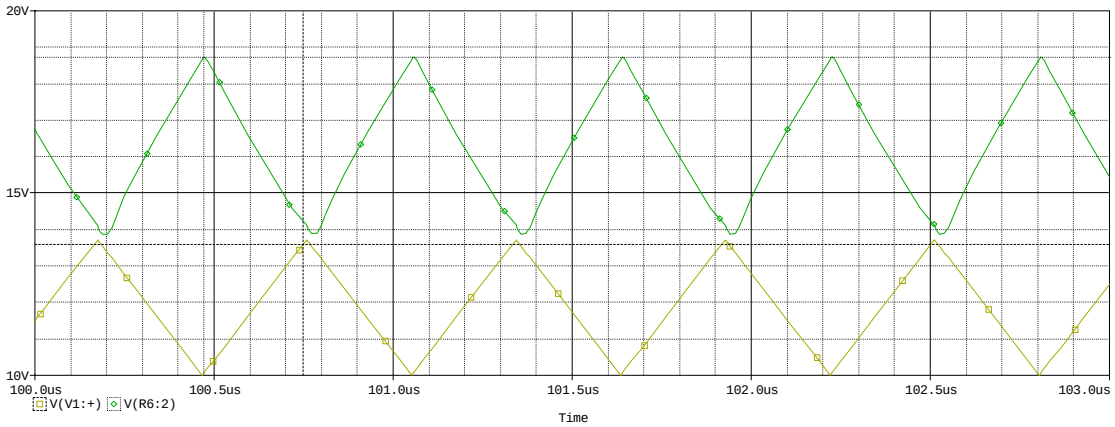

Figura 6.2 Entrada (parte baja) y salida (parte alta) del BJT[27]

6.2 Simulación de la línea de transmisión

Para simular la transferencia de energía en la línea planar se utilizó un simulador electromagnético de onda completa. La Figura 6.3 muestra el dibujo de la línea de transmisión. [24]

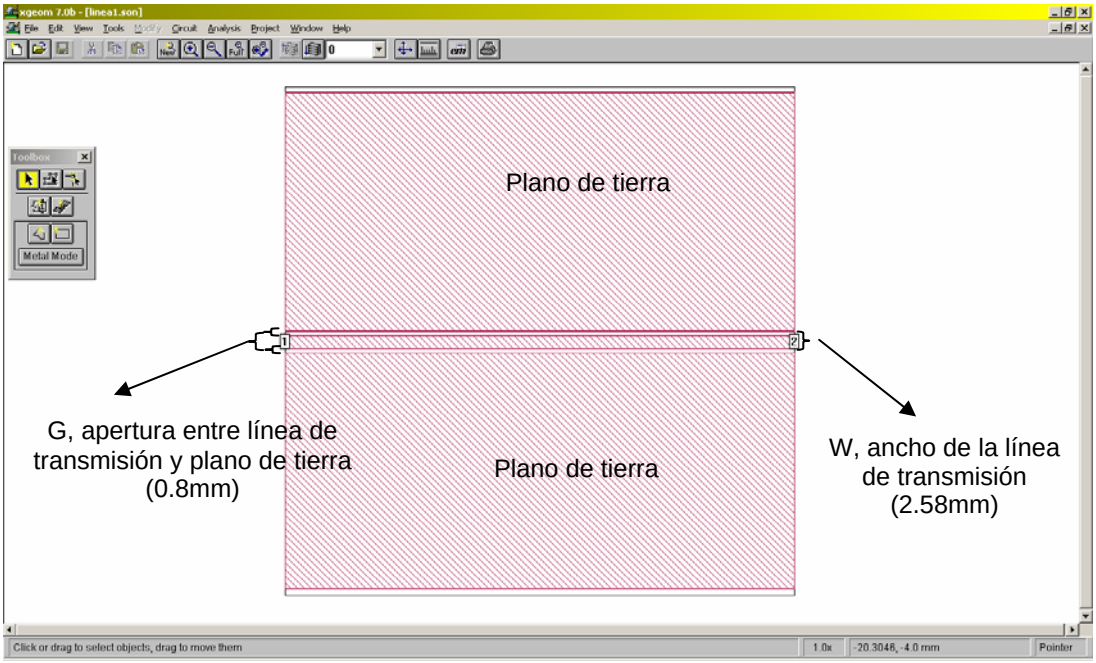

Figura 6.3 Línea de transmisión coplanar [24]

En el simulador se pueden introducir parámetros como el grueso del dieléctrico, su constante, su pérdida tangencial y el tipo de metal que se está utilizando [24]. Las dimensiones de la línea fueron obtenidas con ayuda de software [23]. La caja en la que se encuentra la línea debe ser definida para poder simular [24]. Para este caso se eligió una altura de 10cm para representar el espacio que existe sobre la placa de impresión.

Después de simular la línea se obtiene la Figura 6.4. En ella se pueden ver los parámetros S_{12} y S_{11}. Al analizar la gráfica se concluye que no existe reflexión y que la transferencia de energía es exitosa. Los niveles de magnitud, expresados en dB, reflejan que esto último.

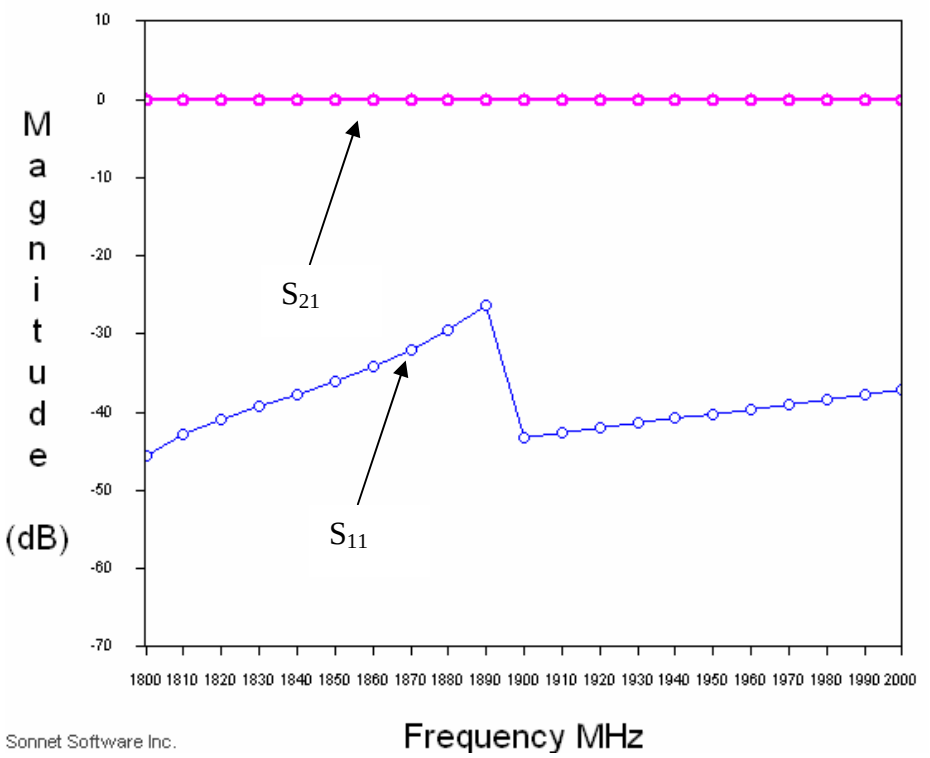

Figura 6.4 Parámetros S_{11} y S_{21}, donde S_{11} es el coeficiente de reflexión en las terminales de entrada y S_{21} es la ganancia de la tensión en directa [24]

6.3 Predicción de la potencia

Para conocer el área de cobertura del *jammer* se utilizaron modelos de propagación tanto para la radiobase como para el dispositivo construido. Para el primer caso se recurrió al modelo Okumura-Hata y se fijó la potencia en 20W [15].

Tabla 6.1 Modelo Okumura-Hata

d(km)	L_p(dB)	P_{rx}(dBm)|P_{tx}=20W
0.03	86.7872052	-43.77690524
0.035	89.1453963	-46.13509625
0.04	91.1881542	-48.17785422
0.045	92.9899944	-49.97969445
0.05	94.6017955	-51.59149545
0.055	96.0598468	-53.04954682
0.06	97.3909434	-54.38064342
0.065	98.6154336	-55.6051336
0.07	99.7491344	-56.73883443
0.075	100.804585	-57.79428466
0.08	101.791892	-58.7815924
0.085	102.719325	-59.70902547
0.09	103.593733	-60.58343263
0.095	104.420851	-61.41055084
0.1	105.205534	-62.19523363
0.2	115.809272	-72.79897182
0.3	122.012061	-79.00176102
0.4	126.41301	-83.40271
0.5	129.826651	-86.81635123
0.6	132.615799	-89.60549921
0.7	134.97399	-91.96369022
0.8	137.016748	-94.00644818
0.9	138.818588	-95.80828841
1	140.430389	-97.42008942
2	151.034128	-108.0238276
3	157.236917	-114.2266168
4	161.637866	-118.6275658
5	165.051507	-122.041207
6	167.840655	-124.830355
7	170.198846	-127.188546
8	172.241604	-129.231304
9	174.043444	-131.0331442
10	175.655245	-132.6449452

La Tabla 6.1 muestra los valores para la Figura 6.5 del modelo Okumura-Hata. Se puede ver como a mayor distancia la señal se va atenuando más.

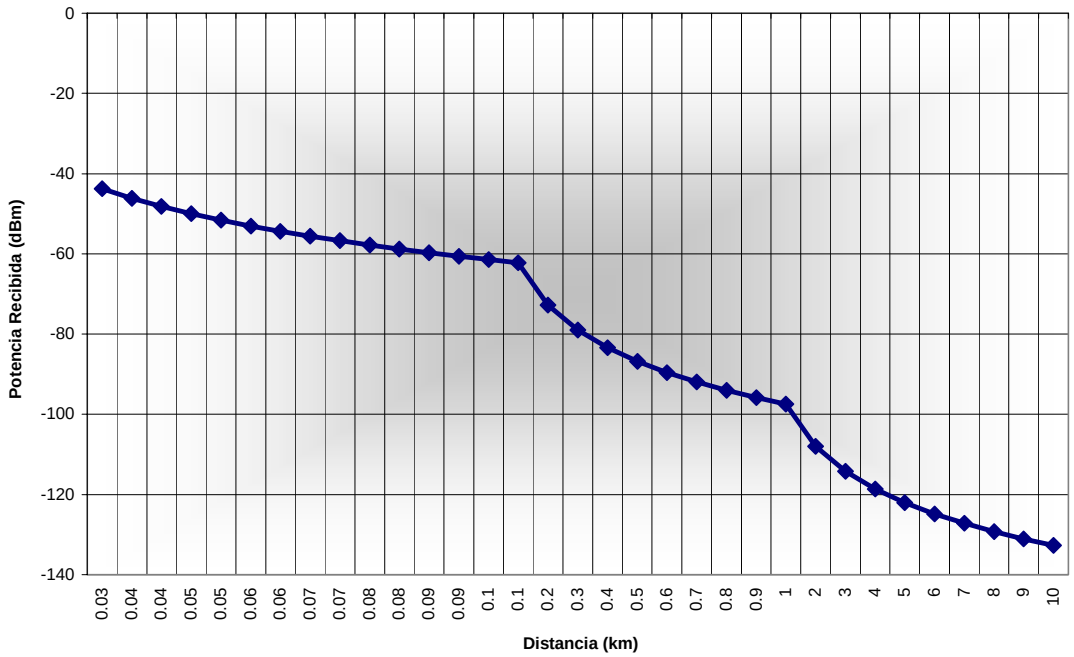

Figura 6.5 Gráfica del modelo Okumura-Hata

Para predecir el comportamiento del *jammer* se utilizó el modelo ITU para interiores. La Tabla 6.2 muestra los valores de la Figura 6.6.

Tabla 6.2 Modelo ITU para interiores

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

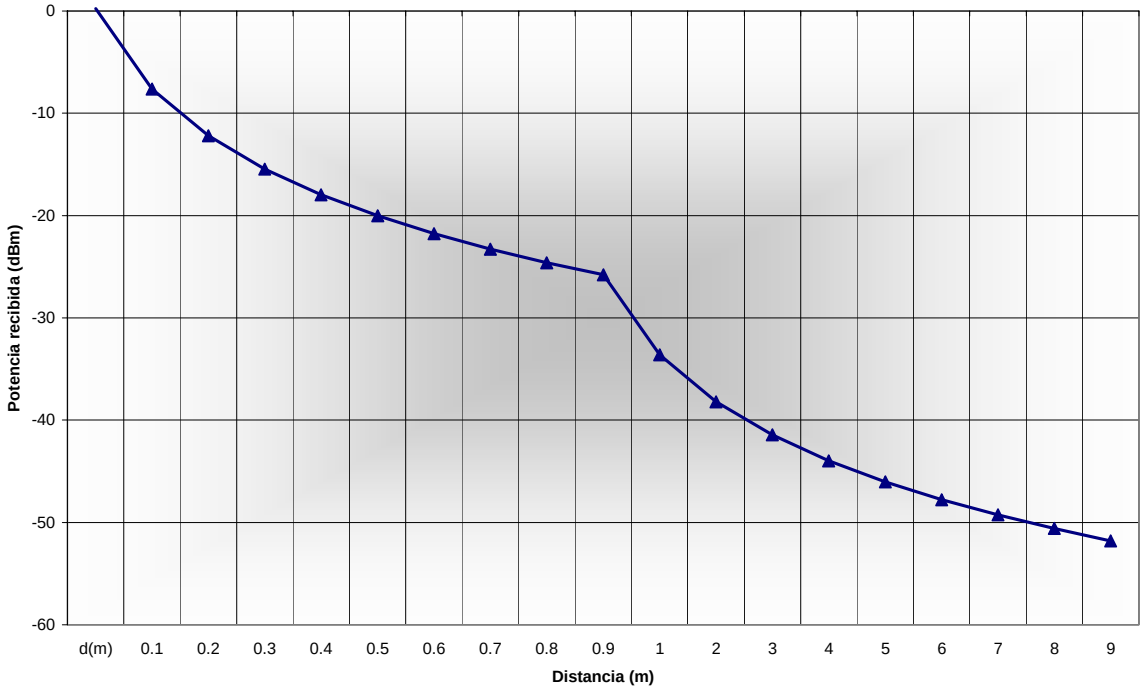

Figura 6.6 Gráfica del modelo ITU para interiores

Al igual que en modelo anterior se observa que a mayor distancia mayor atenuación. La comparación entre estas predicciones es importante porque determinan, en teoría, hasta donde puede operar el *jammer*.

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

Capítulo 7: Conclusiones y Trabajo Futuro

De acuerdo a los resultados arrojados por el *jammer* construido se pueden obtener distintas conclusiones y comentarios.

7.1 Conclusiones

Lo primero que se nota al analizar estos resultados es el área de cobertura. Esta es de aproximadamente 1.70 metros a la redonda, mientras que el área esperada era de 4 metros. Las variaciones entre éstas dos se deben a varios factores:

- El primero de ellos es el modelo de propagación con el que se calcularon las pérdidas. Se debe recordar que los modelos no son exactos y simplemente hacen el mejor esfuerzo para aproximarse a situaciones reales. No se puede modelar cada ambiente y lugar de manera 100% precisa ya que cada objeto tiene un efecto sobre la señal transmitida.
- El segundo factor es el circuito receptor de la unidad móvil; éste no ha sido considerado al momento de los cálculos. Cada unidad móvil posee un circuito con diferente sensibilidad.
- El tercer factor son las tolerancias del proceso de fabricación. A pesar de no haber alcanzado el área teórica el resultado es muy bueno. La interrupción de la señal es total tomando de 40 a 90 segundos para que el móvil no detecte a la estación base y el mismo tiempo para que se recupere la señal una vez que se ha salido del área de cobertura del *jammer*, lo que denota un comportamiento exitoso.

7.2 Trabajo Futuro

El circuito puede ser mejorado en varios aspectos. Con el fin de lograr una mayor integración y portabilidad se podría reducir el tamaño de las placas, ya que éstas se fabricaron más grandes para facilitar la soldadura de los componentes; de igual manera, y con el mismo objetivo, el acoplamiento de la antena podría ser de tipo electromagnético.

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

Un punto importante sobre el tema es lo relacionado al marco legal, razón por la cual no se considera la ganancia para lograr una mayor cobertura. La ley prohíbe la fabricación, distribución y comercialización de *jammers*. Es por eso que se debe mencionar que cualquier persona que emplee este trabajo con el fin de evitar la comunicación en una red de telefonía celular estará incurriendo en una actividad severamente penada.

Referencias

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

[2] Doble, John. Introduction to Radio Propagation for Fixed and Mobile Communications. Norwood: Artech House, 1996.

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

[4] Parsons, J.D. The Mobile Radio Propagation Channel. New York; Toronto: Halsted Press, 1992.

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

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

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

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

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

[10] "Penetración de la Telefonía Móvil por Región 1995-2005 (Semestral)". Comisión Federal de Telecomunicaciones. 23 junio 2005. 20 marzo 2006.

[11] "Presencia de Telefonía Móvil por Empresa y Región 1995-2005(Semestral)". Comisión Federal de Telecomunicaciones. 19 octubre 2005. 20 marzo 2006.

[12] "Regiones de Telefonía Móvil (Anual)". Comisión Federal de Telecomunicaciones. 23 junio 2005. 20 marzo 2006.

[13] Grote, Walter H., Ricardo Olivares. Radiación de Estación Base PCS-GSM. 2001.

[14] Tomasi, Wayne. Electronic Communications Systems. New Jersey: Prentice

Hall, 2001.

[15] Guerrero, Luis G. Apuntes de la clase: Tópicos Avanzados de Comunicaciones. Universidad de las Américas – Puebla. Otoño 2006.

[16] Murphy, Roberto S. Apuntes de la clase: Líneas de Transmisión y Antenas. Universidad de las Américas – Puebla. Primavera 2006.

[17] "Técnicas de RF y Microondas". Universidad Autónoma de Ciudad Juárez, Scientific Atlanta. 31 octubre 2006.

[18] "Gaceta Parlamentaria, año IX, número 1977". Cámara de Diputados LX Legislatura. 29 marzo 2006. 2 noviembre 2006.

[19] Min, Jonathan. Analysis and Design of a Frequency-Hopped Spread Spectrum Transceiver for Wireless Personal Communications. Enero 1996. 20 octubre 2006.