ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE UN JAMMER CAPAZ DE BLOQUEAR LA SEÑAL CELULAR DE ALEGRO

CHRISTIAN MAURICIO GUALOTO RAMÍREZ

Sangolquí - Ecuador
2009

CERTIFICACIÓN

Certificamos que el presente proyecto de grado fue realizado en su totalidad por el Sr. Christian Mauricio Gualoto Ramírez bajo nuestra dirección.

Ing. Gonzalo Olmedo	Ing. Julio Larco
DIRECTOR	**CODIRECTOR**

RESUMEN

Este trabajo consiste en el diseño y fabricación de un dispositivo inhibidor de señales de radiofrecuencia o jammer que tiene como objetivo la red de telefonía celular de la operadora ALEGRO.

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 jammers con el fin de elegir la mejor opción para la aplicación.

Una vez elegidos la técnica de jamming y el tipo de jammer se muestra el diseño por etapas del dispositivo y su correspondiente simulación. Se explica brevemente el proceso de fabricación y se expone los resultados obtenidos, éstos últimos abarcan la parte del generador de funciones y el área de cobertura efectiva para la operadora ALEGRO.

El jammer construido opera exitosamente de 1 a 2 metros a la redonda aproximadamente y toma de 10 a 20 segundos para privar completamente a la unidad móvil de la señal proveniente de la red celular de ALEGRO.

DEDICATORIA

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

También dedico este trabajo a dos personas muy especiales, mi esposa María Teresa e hijo Benjamín, espero que este proyecto sea de inspiración y ejemplo de que un sueño se puede cumplir con esfuerzo propio y consejos de quienes te aman.

AGRADECIMIENTO

Quiero agradecer a Dios por bendecirme con una gran familia cuyos padres me han apoyado en mis estudios con mucho sacrificio para que no me falte nada y pueda estudiar sin ninguna preocupación. Agradezco a mi esposa por su incondicional apoyo y consejos en la elaboración de este proyecto, a mi hijo que ha sido una fuente de inspiración y fuerza, agradezco también la ayuda de mis padrinos a conseguir un dispositivo necesario en este proyecto y a mis amigos de trabajo por sus consejos y tiempo prestado.

Finalmente a la Escuela Politécnica del Ejército porque ha sabido incentivarme mediante sus programas de becas y así lograr éxitos académicos.

PRÓLOGO

Por el considerable uso de los teléfonos celulares sin limitación en todos los lugares y que ha pesar de que existan leyes que prohíban la inhibición de las frecuencias celulares, también existen excepciones donde su uso es restringido; ya sea por seguridad (como en Centros Penitenciarios, Organismos de Estado, Organismos Políticos), o por respeto (como en Hospitales, Salas de reunión, Bibliotecas, Iglesias, Museos, Escuelas, etc). Por este motivo el presente trabajo pretende aplicar distintas tecnologías modernas para el desarrollo de un dispositivo electrónico que sea capaz eliminar la frecuencia celular para una pequeña área, además se tomará en consideración la ley que prohíbe la invasión de una frecuencia ajena y por tal motivo el diseño solo se ajustará a una pequeña área de cobertura y la eliminación de la frecuencia celular de una sola operadora, ALEGRO.

El presente trabajo está organizado en 6 capítulos, en los cuales se tratan todos los aspectos referentes al proyecto, desde una mirada rápida a los conceptos básicos de telefonía, hasta las especificaciones técnicas del dispositivo implementado.

En el Capítulo 1, se hace una introducción a los conceptos básicos de telefonía móvil y su historia, además se muestran las diferentes fuentes de transmisión de una señal a altas frecuencias, y finalmente se presentan los principales sistemas de radiación de ondas electromagnéticas, que son las antenas.

En el Capítulo 2, se presenta el marco teórico referente al *jammer*, es decir sus acciones y elementos principales.

En el Capítulo 3, se presenta una descripción de *jamming,* sus estrategias, técnicas de eficiencia y tipos de jammer, indicando su funcionamiento y comparación entre ellas.

En el Capítulo 4, se muestra el análisis comparativo para el diseño del *jammer,* un diagrama en bloques del circuito a implementar y el funcionamiento de cada bloque con su respectiva justificación por la elección de cada dispositivo y proceso de fabricación.

En el Capítulo 5, se exponen las pruebas realizadas al dispositivo diseñado así como también los ajustes necesarios que debieron efectuarse para su correcto funcionamiento.

Finalmente en el Capítulo 6 se encuentran las conclusiones y recomendaciones que han sido producto del presente trabajo.

Además en la sección anexos se muestra información técnica relevante de los circuitos electrónicos utilizados.

INDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURAS

GLOSARIO

TÉRMINO	SIGNIFICADO
RF	Radiofrecuencia
LOS	*Line of Sight*
ISI	*Intersymbol interferente*
SNR	*Signal-to-Line-of-Sight*
OLOS	*Out-of-Line-of-Sight*
ITU	*International Telecommunication Union*
IEEE	*Institute of Electrical and Electronics Engineers*
OMA	*Omnidirectional Planar Microstrip Antenna*
DSSS	*Direct Sequence Spread Spectrum*
CDMA	*Code Division Multiple Access*
FHSS	*Frequency Hopping Spread Spectrum*
GSM	*Global System for Mobile Communications*
LPD	*Low Probability of Detection*
LPI	*Low Probability of Intercept*

FH	*Frequency Hopping*
FFH	*Fast Frequency Hopping*
BBN	*BroadBand Noise*
MTS	*Mobile Telephone System*
IMTS	*Improved Mobile Telephone System*
FCC	*Federal Communications Commission*
ARTS	*American Radio Telephone Service*
AMPS	*Advanced Mobile Phone System*
TDMA	*Time Division Multiple Access*
CDMA	*Code Division Multiple Access*
FDMA	*Frequency Dision Multiple Access*
USDC	*U.S. Digital Cellular*
SIM	*Subscriber Indentity Module*
VCO	*Voltage Controlled Oscilator*

CAPÍTULO 1

CONCEPTOS DE RADIO FRECUENCIA Y TELEFONÍA MÓVIL

1.1 INTRODUCCIÓN A PROPAGACIÓN DE RF

La comunicación por medio de radio frecuencias entre una antena transmisora y una receptora se da en el rango de 30 kHz a 300GHz. Entre ellos puede existir línea de vista o *Line Of Sight* (LOS) como no lo puede haber, y es en esa circunstancia en la cual la señal sufre diversos efectos antes de llegar a su destino.

1.1.1 Comunicación multiruta y sus efectos

Existe línea de vista entre el transmisor y receptor cuando la señal se propaga en el espacio directamente. Al no existir LOS la comunicación es de tipo multiruta, donde la señal sufre efectos como refracción, reflexión, difracción y dispersión los cuales provocan que la señal receptora se complete por diferentes trayectorias.

La refracción se produce cuando la señal pasa de un medio a otro siempre y cuando los dos medios tengan un índice de refracción distinto, además al existir este efecto se produce otra forma de propagación que es la reflexión, que se da cuando la señal choca con un objeto de dimensiones mayores a las de la longitud de onda, provocando que un porcentaje sea transmitido y el otro reflejado. Para el caso de un buen conductor, la refracción es nula y la reflexión es total, en consecuencia las pérdidas son mínimas. La difracción es otra forma de propagación que ocurre cuando la señal cambia de dirección debido a que en su trayecto encuentra bordes muy agudos de un obstáculo, esta forma de propagación es muy útil cuando no existe línea de vista. La dispersión sucede cuando la señal choca con un obstáculo rugoso de longitud menor a la longitud de onda pero numerosos entre sí.

Las diferentes señales provenientes de las distintas rutas no llegan al mismo tiempo, y tampoco con la misma intensidad. Éstas sufren retrasos y atenuaciones que dependen en general de la longitud de la onda y del modo de propagación [7].

Otro efecto que se produce en la señal es la Interferencia Intersímbolo (ISI), que ocurre cuando un símbolo anterior al que se esta recibiendo interfiere debido a una a más reflexiones. El retraso se debe a que la distancia recorrida por la onda reflejada es mayor que la recorrida por la onda transmitida [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 [7]. La relación señal a ruido ó *Signal to Noise Ratio* (SNR) es la encargada de determinar la calidad con la que llega una señal al receptor. Este parámetro es el más importante para determinar los efectos que produce el jammer en un sistema de comunicación. El ruido afecta al sistema de comunicación, desde el momento en que la señal es procesada en el transmisor hasta que se procesa en el receptor. El ruido es de tipo aditivo y por esta razón decrece a la relación señal a ruido. Es así que si la relación señal a ruido tiene un valor bajo la comunicación es ruidosa con lo cual el jammer presentara una ventaja puesto que su funcionamiento no será muy exigido.

1.1.2 Parámetros importantes

Para la telefonía móvil los parámetros que se toman en cuenta son la relación señal a ruido y la relación señal a interferencia. A más de las diferentes relaciones entre las señales, existes otros puntos que se deben tomar en cuenta para medir el desempeño de los sistemas de comunicación inalámbrica como lo son: el *Path loss,* el *rms multipath delay Spreads,* y el *doppler spreads*.

- **Path Loss**

El *Path Loss* es la pérdida de potencia causada por la trayectoria de la señal, este se puede medir con la siguiente formula:

$$L_P(dB) = P_{Tx}(dB) - P_{Rx}(dB) \quad (1)$$

donde: P_{Tx} = potencia transmitida; P_{Rx} = potencia recibida.

Varios factores alteran las pérdidas de potencia por trayectoria en un ambiente urbano como son los árboles, edificios lagos, etc.

- **Multipath Delay Spread**

El *delay spread* es una medida estadística de los retrasos de tiempo de varias trayectorias, se calcula usando el modelo de Turin para propagación en ambientes urbanos [7].

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

donde: β_k = magnitud de la ruta L; τ_k = retraso excesivo de la ruta L; $\bar{\tau}$ = promedio del retraso excesivo y se calcula:

$$\bar{\tau} = \frac{\sum_{k=1}^{L} \tau_k \beta_k^2}{\sum_{k=1}^{L} \beta_k^2} \tag{3}$$

En ambiente de interiores, el valor de rms del *delay spread* medido a distancias de $100m$ está por debajo de los $100ns$, mientras que en áreas de exteriores es menos de $10\mu s$ a distancia de algunos kilómetros [7].

- **Doppler Spread**

Existe una variación de frecuencia de la señal cuando el receptor se encuentra en movimiento al momento de la comunicación entre transmisor y receptor, este efecto se conoce como *Doppler Shift* [7]. La frecuencia cambia a razón de:

$$f_D = \frac{v}{\lambda} \cos(\alpha) \tag{4}$$

La máxima variación ocurre cuando el receptor se acerca o aleja directamente.

$$f_m = \frac{v}{\lambda} f_c \tag{5}$$

Es común que en la telefonía móvil la señal llegue al receptor al mismo tiempo pero con diferentes ángulos, por este motivo varia constantemente la relación entre la amplitud y ángulo de fase.

La región en el espectro entre $-f_c - f_m$ y $-f_c + f_m$ es llamada *Doppler Spread*.

Otro efecto que se produce por el movimiento del receptor es la pérdida de correlación entre la fase y amplitud de las distintas rutas. Dicha correlación depende de la distancia de trayectoria, a medida que la distancia se acorta entre el transmisor y el receptor las señales recibidas son altamente correlacionadas, pero a mayor distancia de separación de estas, la correlación decae rápidamente [7].

1.2 MODELOS DE PROPAGACIÓN

La señal se atenúa durante la transmisión y por esta razón se han propuesto modelos y expresiones matemáticas para poder predecir estos efectos. Los modelos se encuentran clasificados como: analíticos, empíricos y semi-empíricos. Estos modelos se han desarrollado para cualquier tipo de ambiente; sea en transmisiones donde exista línea de vista (LOS) y las variaciones son modeladas con distribuciones logarítmicas normales, o en transmisiones donde no exista línea de vista (OLOS) para los cuales se modelan con distribuciones de Rayleigh. Sin embargo los dos modelos más utilizados en la propagación de la señal en una comunicación móvil son: el modelo Okumura – Hata y Walfish – Ikegami [7].

1.2.1 Modelo Okumura – Hata

Este modelo tiene como objetivo predecir los efectos ocasionados por las estructuras de la ciudad como son la reflexión, difracción y dispersión. Clasificando a la ciudad por su estructura tenemos zonas densamente urbanas, zonas urbanas, zonas suburbanas, zonas rurales.

Al referirse a ciudades se toma en cuenta los dos primeros casos y se emplea la siguiente ecuación para calcular el *path loss* o atenuación de la onda electromagnética que viaja de transmisor a receptor [5].

$$L_P(dB) = C_1 + C_2 \log(f) - 13{,}82\log(h) - a(h_m) + [44{,}9 - 6{,}55\log(h)]\log(d) + C_0 \quad (6)$$

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

$$a(h_m) = [1{,}1\log(f) - 0{,}7]h_m - [1{,}56\log(f) - 0{,}8] \quad (7)$$

$$150MHz < f < 1000MHz$$

$C_1 = 69{,}55$; $C_2 = 26{,}16$; $C_0 = 0$ para urbano denso

Urbano

$$a(h_m) = 3{,}2[\log(11{,}75h_m)]^2 - 4{,}97 \quad (8)$$

$$1500MHz < f < 2000MHz$$

$C_1 = 46{,}33$; $C_2 = 33{,}9$; $C_0 = 3$ para urbano

1.2.2 Modelo ITU para interiores

La propagación en entornos de interiores es muy compleja. Dentro de edificios o centros comerciales es importante modelar el comportamiento de la señal y las perdidas que puede producir debido a que la señal generalmente es bloqueado por paredes, suelos mamparas u otros objetos. Para lo cual se instalan micro o picocélulas.

Este modelo estima el *path loss* 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 muestra la forma de calcular el *path loss* empleando este modelo [5].

$$L = 20\log f + N\log d + P_f(n) - 28 \quad (9)$$

donde: f = frecuencia en MHz; d = distancia entre Tx y Rx en metros; N = coeficiente de pérdidas por distancia; n = número de pisos entre Tx y Rx; $P_f(n)$= factor de pérdidas por penetración entre pisos.

Los valores de N y $P_f(n)$ se encuentran dadas en tablas.

1.3 INTRODUCCIÓN A LA INGENIERÍA DE MICROONDAS

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

1.3.1 Línea 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. En términos más específicos 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 [6, 7].

En la transmisión de señales de baja frecuencia el comportamiento de la señal es simple y predecible al usar una línea de transmisión; sin embargo, para señales de alta frecuencia sufre efectos como dispersión y la disipación, lo que convierte al cable coaxial, cable bipolar paralelo y par trenzado en conductores no óptimos para la transmisión de energía. Es por tal motivo que se han construido alternativas para frecuencias por arriba de 500 MHz, las líneas de transmisión plana [6, 7].

- **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 lo compacto de los circuitos, el ancho de banda amplio que se puede manejar y las sencillas técnicas de fabricación [6, 7].

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 muestra una breve descripción de esta familia de líneas de transmisión.

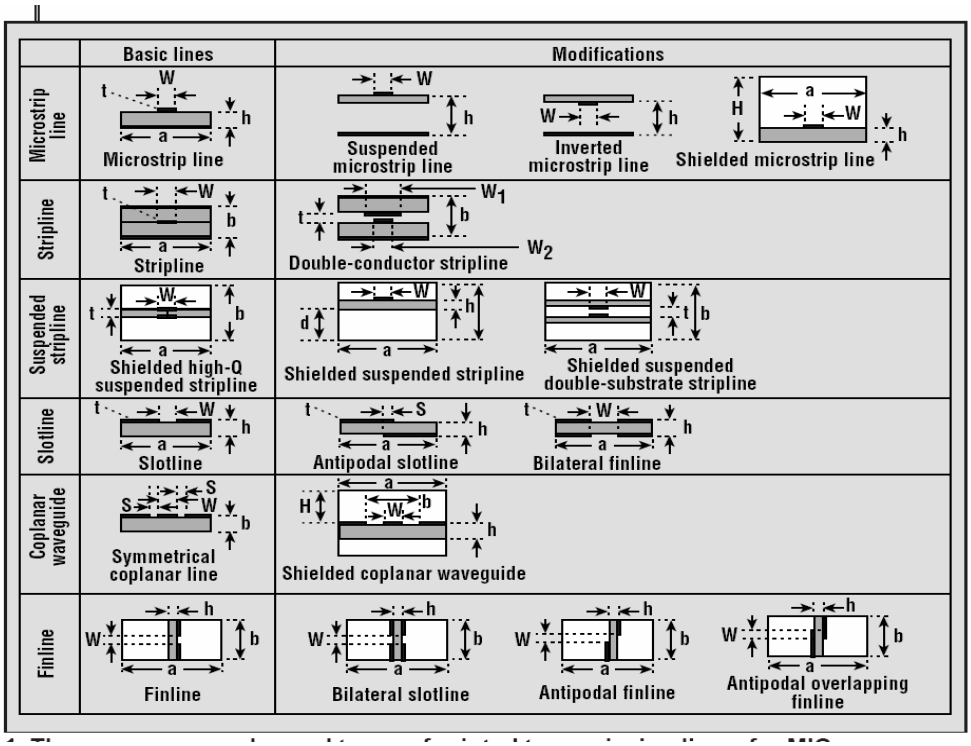


Figura 1. Líneas de transmisión planas [3].

Al trabajar con una línea de transmisión de este tipo lo primero que se debe seleccionar es un dieléctrico debido a la constante de permitividad de cada material. Las características de la línea serán controladas por el ancho del conductor y los espacios en el plano dieléctrico.

Al diseñar una línea plana se debe tomar en cuenta la impedancia característica y la permitividad efectiva. Ambas dependen de la frecuencia que se este manejando. Para hacer esto existen aproximaciones y programas que facilitan esto [13].

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 muestra una comparación entre las líneas de esta familia.

Tabla 1. Comparación de varios tipos de líneas planas [3].

Línea de Transmisión	Factor Q	Radiación	Dispersión	Rango de impedancias	Montaje de chip
Microstrip	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

- **Línea Coplanar**

La línea coplanar se compone de una línea de transmisión de ancho *W* separada del plano tierra por una distancia G. La ventaja que tiene esta línea es la de conectar componentes pasivos y activos en paralelo con la línea, sin la necesidad de taladrar al sustrato. Este tipo de línea puede contener un tercer plano de tierra en la parte inferior del sustrato; sin embargo, la impedancia característica cambiará, por lo que se deberá ajustar las dimensiones para conservar la impedancia requerida. La Figura 2 muestra las dimensiones que se consideran al momento de diseñar una línea coplanar con plano de tierra [3].

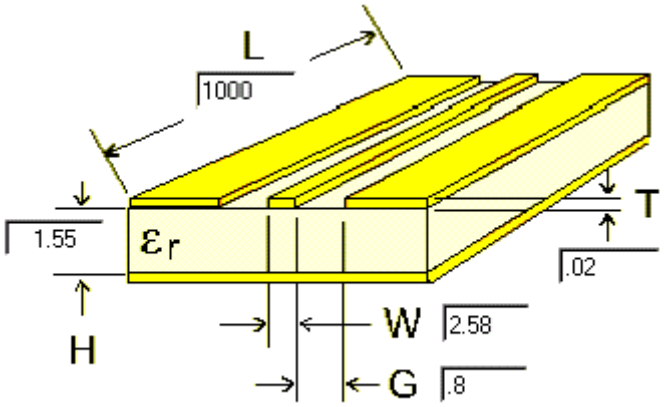


Figura 2. Línea coplanar [13].

donde: *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 la 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.

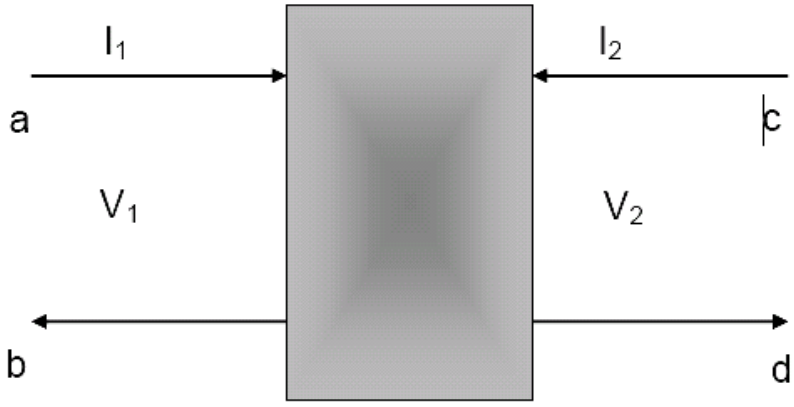


Figura 3. Red de dos puertos

donde: I_1 = corriente de entrada; I_2 = corriente de salida, V_1 = voltaje de entrada; V_2 = voltaje de salida; *a* y *b* = terminales en el puerto de entrada; *c* y *d* = terminales en el puerto de salida

A partir de los datos de voltaje y corriente se pueden encontrar los parámetros restantes como son:

Los parámetros de pequeña señal, en los que se encuentra la impedancia *Z*, admitancia *Y*, los híbridos *H*, los de transmisión *T* y los de transmisión inversa *ABCD* y

Los parámetros de dispersión o parámetros *S*.

1.4 ANTENAS

Una antena es un sistema 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 aplicarse un voltaje, en caso de la recepción el proceso es inverso [6, 7].

El tamaño de las antenas es muy importante porque está relacionado con la longitud de onda de la señal λ y es por lo general un submúltiplo exacto de ésta. Es por eso que a mayores frecuencias el tamaño de la antena es menor, es decir, son inversamente proporcionales [1].

$$\lambda = \frac{v}{f} \tag{10}$$

donde: λ = longitud de onda; v = velocidad de propagación; f = frecuencia de operación.

1.4.1 Parámetros de la antena

- Patrón de radiación.- Es una representación gráfica de las propiedades de radiación de una antena en función de las coordenadas espaciales.
- Potencia radiada.- P_{rad} se determina con la integral del vector de Poynting en una superficie cerrada que envuelve totalmente a la antena.
- Eficiencia.- Es una forma de cuantificar las pérdidas de una antena. Se distinguen tres tipos: de reflexión, de conducción y del dieléctrico [6, 9].
- 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 [6, 9].
- 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 [6, 9].
- 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 [1].
- 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 (11).

$$Z_{in} = \frac{E_i}{I_i} \tag{11}$$

- El valor de la impedancia es complejo. Es por eso que depende de la frecuencia. Además, depende de la longitud y la resistencia de radiación de la antena [1].
- Resistencia de radiación.- Es un componente ficticio encargado de representar la potencia radiada.

- 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 [6, 9].
- Polarización.- Se refiere a la dirección de la perturbación. Puede ser elíptica, circular o lineal.

1.4.2 Tipos de antena

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

- Lineal
- De lazo
- Helicoidales
- De apertura
- De parche o microstrip
- De reflexión
- Arreglos

El avance tecnológico se ha desarrollado a las antenas de parche o *microstrip,* debido a sus ventajas.

- **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, rectangulares, bipolares, etc. Las ventajas y desventajas se detallan a continuación:

Ventajas	**Desventajas**
Integrables al entorno	Factor de calidad
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

- **Antena de parche rectangular**

Este tipo de antena consiste en una delgada capa de material conductor adherida a un sustrato dieléctrico colocado sobre un plano de tierra. Generalmente se busca un sustrato con permitividad entre 2,2 y 12; entre más bajo sea este valor mayor será la eficiencia, el ancho de banda y el tamaño. Las antenas de parche permiten 3 métodos principales de alimentación:

→ Directa.- Cuando entra en contacto directo con el radiador.

→ Por apertura.- Una línea de transmisión se encuentra en la parte inferior de dos placas de 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.

→ 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.

- **Antena OMA**

La *Figura 4* muestra una antena *Omnidirectional Planar Microstrip Antenna* (*OMA*) de 7 segmentos por sus dos caras. Las antenas OMA de *n* segmentos consiste en una serie de parches conectados entre si con el fin de aumentar las características de la antena. Son usadas en aplicaciones de IEEE 802,11, 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 la onda λ, y 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 cada segmento la línea de transmisión tenga una impedancia de 50Ω.

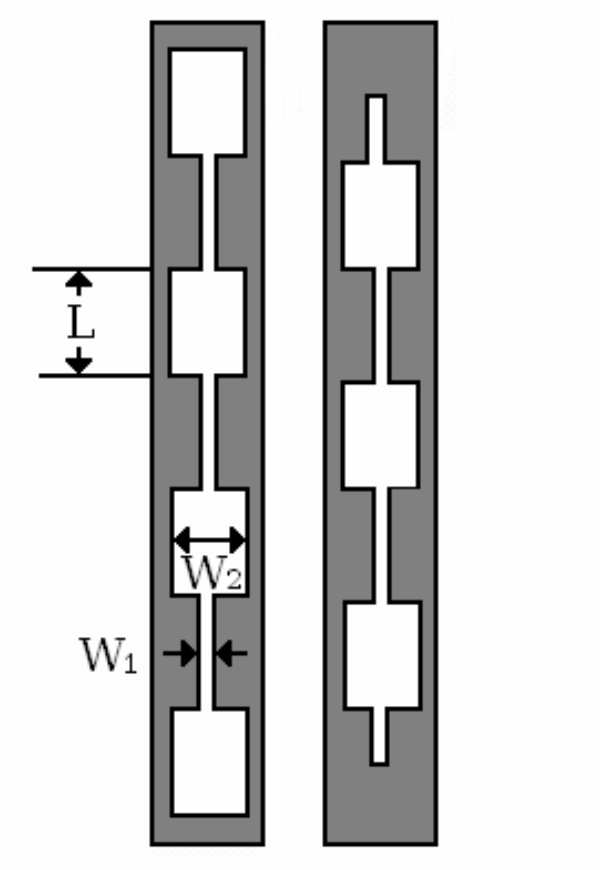


Figura 4. Antena OMA de 7 segmentos

1.5 TELEFONÍA MÓVIL

1.5.1 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 *Mobile Telephone System* (MTS), 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 de gran ventaja de *Improved Mobile Telephone System* (IMTS) en comparación con su antecesor [1].

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 nuevamente de 60kHz a 30kHz [1].

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 *American Radio Telephone Service* (ARTS) la que recibió autorización para operar en Baltimore [1].

Sin embargo, fue hasta 1983 cuando la telefonía celular comenzó a crecer exponencialmente. Ese año *Advanced Mobile Phone System* (AMPS) 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 [1].

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 [1].

En ese momento de la historia de la telefonía móvil se formaron dos caminos. La diferencia entre estos radicaba en la técnica de acceso múltiple empleada, fuera *Time Division Multiple Access* (TDMA) o *Code Division Multiple Access* (CDMA). En comparación con la técnica empleada por AMPS u otros estándares de primera generación, *Frequency Dision Multiple Access* (FDMA), las dos ofrecían grandes ventajas. Por ejemplo, la capacidad específica en *U.S. Digital Cellular* (USDC) o IS-54 equivale a veces la capacidad de AMPS [1].

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 en sus inicios se concentro en el continente Europeo. La mayoría de estos estándares evolucionaron en un paso intermedio conocido como 2,5G [1].

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 recocidos oficialmente, 2,5G no lo es. Este término fue inventado simplemente con fines publicitarios y de ventas [1].

Un ejemplo de lo que es considerado un servicio de 2,5G es *General Packet Switching Service* (GPRS) 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 redes GSM como ejemplo de proveedora de servicios similares a los de 3G es *Enhanced Data Rates for GSM Evolution* (EDGE), el cual es una tecnología que permite aumentar la taza de transmisión de datos y su confiabilidad hasta 236,8 kbits/s [1].

En los primeros años de esta década la telefonía móvil evolucionó hacia otra generación, 3G. Esta tercera generación ofrece servicios de video conferencia e Internet de alta velocidad. A diferencia de 2,5G, 3G no consiste en mejoras a la red de 2G y no opera en el mismo espectro de frecuencia. Es por eso necesario construir nuevas redes y adquirir nuevas concesiones de frecuencia. El primer país que ofreció 3G fue Japón. El 2005, 40% de los suscriptores emplean solamente redes de tercera generación. Es así que en el 2006 la trasmisión entre generaciones se completó. Incluso ya se habla de mejoras bajo el nombre de 3,5G. Estas mejoras incrementarán la máxima velocidad de 2Mbits/s a 3Mbits/s [1].

1.5.2 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 subdividía un área geográfica relativamente grande, llamada zona de cobertura, en secciones más pequeñas, llamadas células, el concepto de reuso de frecuencias podría ser empleado para incrementar considerablemente la capacidad del canal.

- **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 importante 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 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.

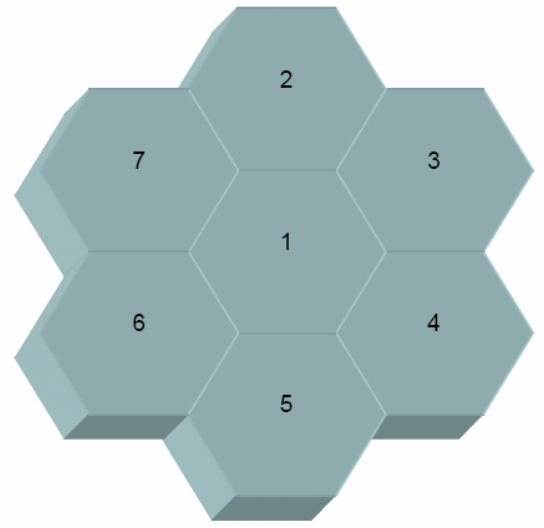


Figura 5. Células de la telefonía celular

En la Figura 5 se puede observar la forma ideal de las células y como están colocados 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 *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 [1].

1.5.3 *Code Divison Multiple Access* (CDMA)

El sistema CDMA es una forma de acceso que permite la trasmisión de telefonía y datos. Una ventaja de CDMA radica en la posibilidad de reutilización de frecuencias entre celdas y sectores contiguos con el correspondiente incremento de la eficiencia espectral. Cada uno de los sectores del área de cobertura dispone de varias portadoras FDMA (cerca de 10) y canales CDMA (cerca de 40) [10].

- **Control de potencia**

En CDMA la potencia transmitida se fija para que SNR sea el valor medio mínimo requerido para una buena recepción. Se trata de controlar permanentemente la emisión del móvil para mantener el mínimo de potencia [10]. Para un usuario dado, los demás usuarios equivalen a ruido aleatorio, por lo tanto, la potencia de cada usuario debe ser cuidadosamente controlada para no provocar interferencia con los demás [10]. Esto se hace con el fin de que un móvil que esté muy cerca de la base no presente una señal tan potente que interfiera demasiado con la señal proveniente de equipos remotos. Dicho en otras palabras, la potencia de transmisión del móvil se debe gestionar de manera tal que en la base todos los móviles se reciban con igual intensidad. Esto trae como ventaja adicional mayor economía en la alimentación de los equipos móviles y una mayor duración de las baterías [11].

CAPÍTULO 2

DESCRIPCIÓN DE LA "GUERRA ELECTRÓNICA"

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

- El ataque electrónico
- El apoyo electrónico
- La protección electrónica

2.1 ATAQUE ELECTRÓNICO

El ataque electrónico se puede realizar por medio de tres tipos de acciones o técnicas [5, 6].

- Jamming
- Engaño
- 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 [7]. 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 [7]. 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 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 trasmisión 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 comunicaciones [7]. 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 [7].

- 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 el ruido.
- JSR (Jam-to-Signal Ratio)
- Determina si la potencia con que trasmite el jammer es mayor o menor que aquella que emplea el transmisor original del sistema [7].
- 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 el número de paquetes recibidos con el número de paquetes generados.
- BER (Bit Error Rate) P_e
- Es la probabilidad de que un bit sea incorrecto.
- SER (Symbol Error Rate) P_s
- Es la probabilidad de que un símbolo sea incorrecto.
- SIR (Signal-to-Interference Ratio)
- Es la relación entre la potencia de la señal deseada y la suma de las potencias de las señales no deseadas.

2.3 PROTECCIÓN ELECTRÓNICA

La Protección Electrónica consiste en el uso de estrategias para evitar los dos primeros elementos de la llamada "Guerra Electrónica", es decir, el ataque y el apoyo [7]. La codificación y al modulación entran dentro de este elemento. Con la unión de la modulación y codificación nacieron las comunicaciones *AJ* por sus siglas en inglés, *antijam*. Este tipo de comunicaciones tiene como objetivo evitar que un sistema externo pueda dañar, bloquear o interceptar la comunicación de otro sistema.

2.3.1 Tipos de señales *Antijam (AJ)*

Las dos principales señales *AJ* tienen que ver con la telefonía móvil son: La secuencia directa de amplio espectro o *Direct Sequence Spread Spectrum* (DSSS) y el salto de frecuencia o *Frecuency Hopping Spread Spectrum* (FHSS).

Para que una señal pueda ser considerada como *AJ* es necesario que el sistema que la trasmita sea un sistema *Low Probability of Detection* (LPD) y/o *Low Probability Intercep* (LPI) [7].

El objetivo de LPD es lograr que la señal permanezca tan oculta como sea posible. DSSS es un ejemplo del sistema LPD [7], por que logra que la señal sea distribuida por todo el espectro disponible lo que provoca que la potencia sea muy baja y parezca ruido para así dificultar su detección.

En un sistema LPI la señal puede ser detectada, pero si la información no es interceptada, ésta señal estará protegida. Un ejemplo es el sistema FHSS [7], donde la protección se logra cambiando constantemente la frecuencia. Ya sea con saltos rápidos pero pocos bits involucrados *Fast Frequency Hopping* (FFH) ó mayor cantidad de datos pero menores cambios de frecuencia *Slow Frequency Hopping* (SFH).

CAPÍTULO 3

DESCRIPCIÓN DE JAMMING

3.1 ESTRATEGIAS DE JAMMING

El jammer tiene distintas estrategias para atacar a diversas aplicaciones. Cada una tiene sus ventajas y desventajas, por esta razón se estudia cada una de estas para elegir la mejor opción que sea acorde con esta aplicación.

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 [7].

3.1.1 *Jamming* por ruido

La portadora emitida por el jammer es modulada por una señal aleatoria de ruido [4]. 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 [7].

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

El ruido de banda ancha o *Broadband Boise* (BBN) introduce energía a través de todo el ancho del espectro de frecuencias en el que opere la aplicación [7]. El BBN jamming funciona elevando el nivel de ruido en el receptor lo que ocasiona un decremento en la relación señal a ruido [7]. Su limitante es que tiene un bajo nivel de potencia jamming

$J_0[Watts/Hertz]$, ya que la potencia es esparcida en una parte amplia del espectro. En cuanto a la eficiencia, depende del nivel de potencia y por tanto de la distancia entre el jammer y el receptor. Este tipo de jamming se le conoce también como jamming de banda completa.

- ***Jamming* por ruido parcial**

Se conoce también como *Partial band Boise* (PBN). 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 de banda del espectro. Al no haber sincronización la comunicación no llega a ser exitosa [7].

- ***Jamming* por ruido de banda angosta**

Conocido como *Narrowband Boise* (NBN), esta manera de generar jamming introduce energía 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, 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 a una pequeña parte del espectro, lo que representa una ventaja [7].

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 encuentre la señal *AJ* [7]. La eficiencia de esta técnica depende completamente del lugar en el espectro donde se coloque los pulsos. 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.

En un caso de *MT* si los tonos se colocan en canales continuos, el desempeño del *jammer* será teóricamente igual al desempeño de *jamming* por ruido de banda parcial. Debido a que los tonos se colocan en canales continuos se conoce a este particular caso de *MT* como *comb jamming* [7].

3.1.3 *Jamming* por pulsos

En este caso el factor a tomar en cuenta no es el ancho del espectro cubierto, sino el tiempo que el jammer está encendido. Al analizar el funcionamiento se encuentra similitudes con el jamming por ruido de banda ancha ya que al estar encendido el jammer trabaja con pulsos que cubren una parte amplia del espectro, ésta estrategia es similar en resultados al jamming por ruido de banda parcial además presenta la ventaja de ahorrar gran cantidad de potencia si se diseña correctamente el ciclo de trabajo.

3.1.4 *Jamming* por barrido

Es un concepto similar al de ruido por banda ancha o por banda parcial [7]. De hecho se puede considerar como una estrategia complementaria. Consiste en introducir ruido en una pequeña parte del espectro; y una vez colocada ésta señal, se realiza un barrido por todo el ancho de banda que ocupe la señal AJ. Esta estrategia se puede emplear en un sistema FHSS [7]. Sin embargo, 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 trasmisión 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 el 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 se optimiza el uso de la potencia. Esto se debe a que la potencia no se esparce 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

Se conoce también como jamming de respuesta y jamming de repetición. Esta estrategia consiste en localizar la frecuencia a la cual "saltó" la señal, identificar la señal como blanco y emplear jamming por ruido, tonos o pulsos. Se aplica generalmente a sistemas FHSS. Sus limitantes están relacionadas con el tiempo de procesado del jammer, la aplicación en más de un canal ya que la potencia se distribuirá entre estos, e incluso las distintas modulaciones son un escudo ante esta estrategia. Por estas razones y a pesar de ser una estrategia eficiente cuando se diseña correctamente, es muy compleja y no representa una opción sencilla de implementación [7].

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 puede 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.

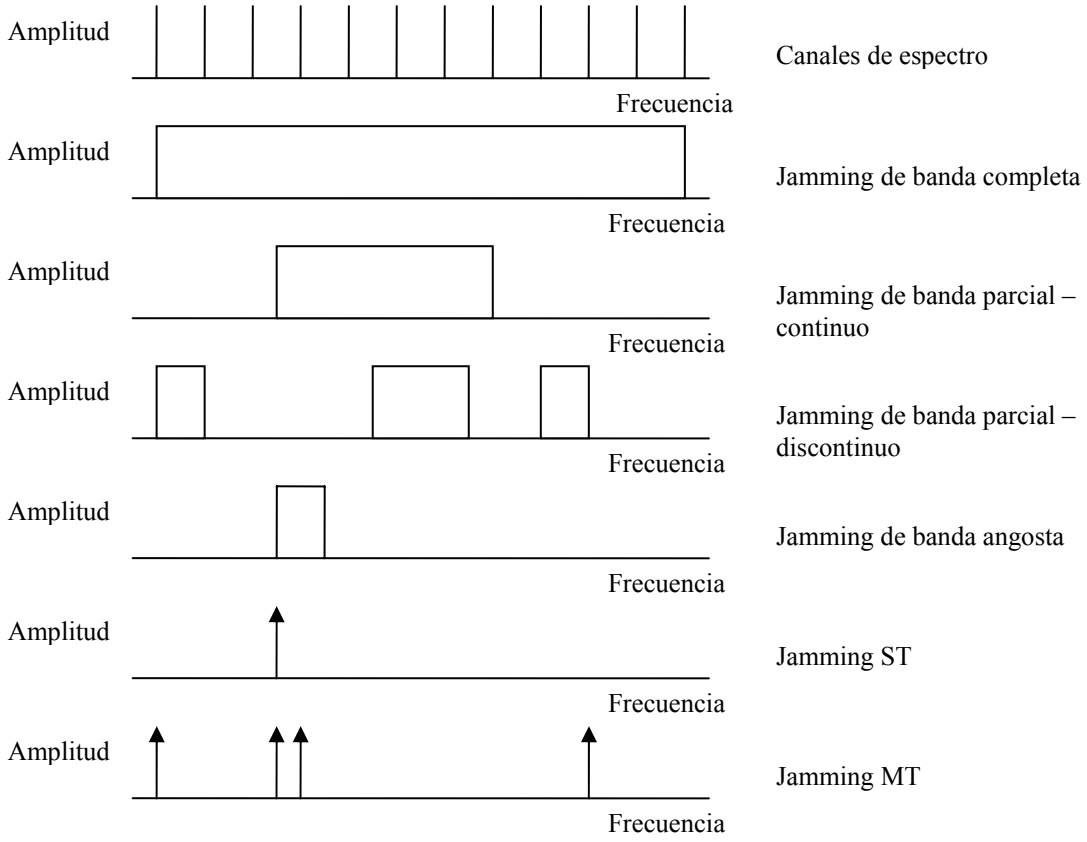


Figura 6. Estrategias de Jamming

3.1.7 Técnica para incrementar la eficiencia del *jammer*

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

- **Look Through**

Cuando las señales no son de espectro extendido, esta técnica es empleada para determinar si el blanco ha cambiado de frecuencia o simplemente ha dejado de operar. Esto se hace para no malgastar la potencia y de esta manera emplearla en más de un objetivo o simplemente ahorrarla. Al momento de apagar el jammer se mide la actividad en el espectro y se determina si el blanco está en funcionamiento o no. Podría pensarse como

solución para sistemas FH y como una forma de jamming por seguimiento. Sin embargo, debido a la velocidad de salto no se emplea esta técnica para tal propósito. Esta técnica se puede aplicar a sistemas DSSS siempre y cuando se pueda detectar su actividad [6].

- **Potencia compartida**

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

- **Tiempo compartido**

Otra técnica para cubrir más de un blanco, es orientar la máxima potencia del jammer a cada blanco pero en momentos distintos. Cuando se aplica jamming a una señal digital 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 [6].

3.2 CLASIFICACIÓN GENERAL DE JAMMERS

De las distintas estrategias de jamming se derivan cuatro tipos principales de jammers. 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 debido a que excede los niveles de ruido y por tal motivo es fácil su detección, debido a que una vez encontrado el ruido es posible detectar la fuente que lo genera, otro inconveniente es que requiere de mucha potencia.

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]. Siendo su ventaja ser menos propenso a la detección pero aun en este tipo la potencia requerida es grande.

3.2.3 *Jammer* aleatorio

Este tipo de jammer funciona por determinado tiempo y deja de hacerlo por otro [8]. El ciclo de trabajo es programado de acuerdo a su aplicación. Se puede utilizar jamming por ruido, por pulsos, por tonos e incluso por barrido [7]. Su detección es posible realizando un análisis de la actividad de la red, mientras que la potencia requerida es menor debido a que no se encuentra en funcionamiento todo el tiempo.

3.2.4 *Jammer* reactivo

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

CAPÍTULO 4

DISEÑO DEL JAMMER

4.1 ELECCIÓN DE LA TÉCNICA DE JAMMING Y TIPO DE JAMMER

Después de analizar las distintas técnicas de jamming, tipos de Jammer y una comparación entre la complejidad y el beneficio, se optó por elegir:

La técnica de Jamming por Barrido y el tipo de Jammer Constante.

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

Las demás se descartaron por las siguientes razones:

i. La estrategia de *jamming* por ruido:
   - De *banda ancha,* requiere mucha potencia y se tendrían que implementar numerosas etapas de ganancia para la antena. Además de incurrir en problemas legales.
   - De *banda parcial,* limitaría a cierta parte del espectro, entre 5 y 10MHz.
   - De *banda angosta,* no ofrece el ancho de banda necesario por ser fija.

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

iii. La estrategia de *jamming* por pulsos no sería efectivo por su ciclo de trabajo ya que se requiere que esté encendido todo el tiempo.

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

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

4.2 DESCRIPCIÓN DEL CIRCUITO

Para que un jammer utilice como estrategia el barrido, se debe implementar el circuito de la Figura 7.

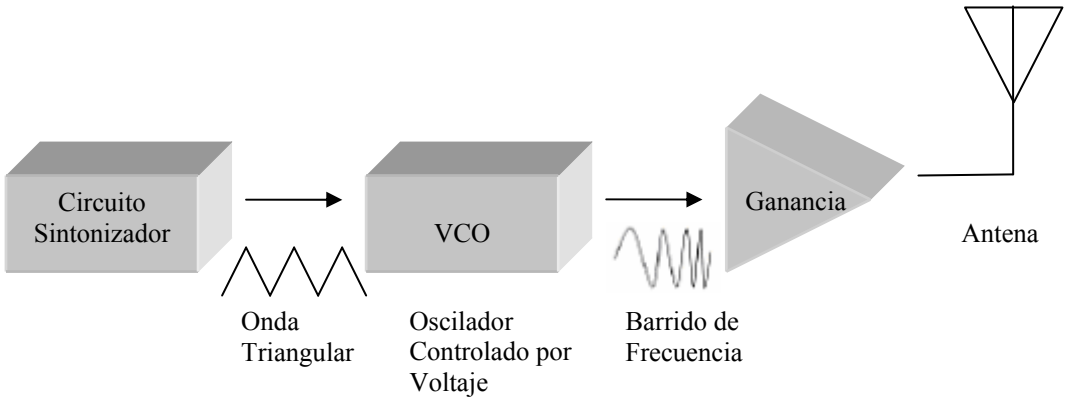


Figura 7. Diagrama de bloques del jammer

4.2.1 Oscilador controlado por voltaje VCO

La función del VCO es la más importante del jammer. Su fabricación es complicada debido a que las frecuencias con las que se va ha trabajar son a nivel de los gigahertz. Además la depuración del VCO es importante, ya que a esas frecuencias cualquier componente puede funcionar como antena. Por este motivo se optó por comprar el VCO modelo JTOS-2000 de Minicircuits®. Este dispositivo hace un barrido de 1370 a 2000MHz, rango que incluye cualquier operadora que trabaje sobre una banda PCS. El voltaje que se debe suministrar para el barrido de frecuencia es de 1 a 22 V. En la Tabla 2

se puede observar que el rango de voltaje que debe ser suministrado va desde 15V a 17V para garantizar la cobertura de la operadora celular ALEGRO.

Tabla 2. Relación entre voltaje sintonizador y la frecuencia de salida

Voltaje	Frecuencia
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

4.2.2 Sintonizador

El circuito sintonizador es el encargado de suministrar el voltaje de entrada al VCO. Se la puede realizar mediante una onda de diente de sierra o triangular. Por esta razón se optó por el integrado XR-2206, el cual es un generador de funciones del cual se pueden obtener señales senoidales, cuadradas y triangulares con frecuencias superiores a 1MHz y voltajes cercanos a los 20V. Se debe tomar muy en cuenta la frecuencia, debido a que GSM es un sistema que emplea SFH y de esta manera los saltos de frecuencia pueden proteger la comunicación de la interferencia producida por el jammer.

Para este inconveniente habría dos causas:

- Si la variación de voltaje del sintonizador es muy lenta el VCO no alcanzará a barrer varios lapsos del espectro provocando que no intercepte los saltos de frecuencia, y
- Si la variación de voltaje del sintonizador es muy rápida el tiempo no será suficiente para que el jammer logre interferir con la señal.

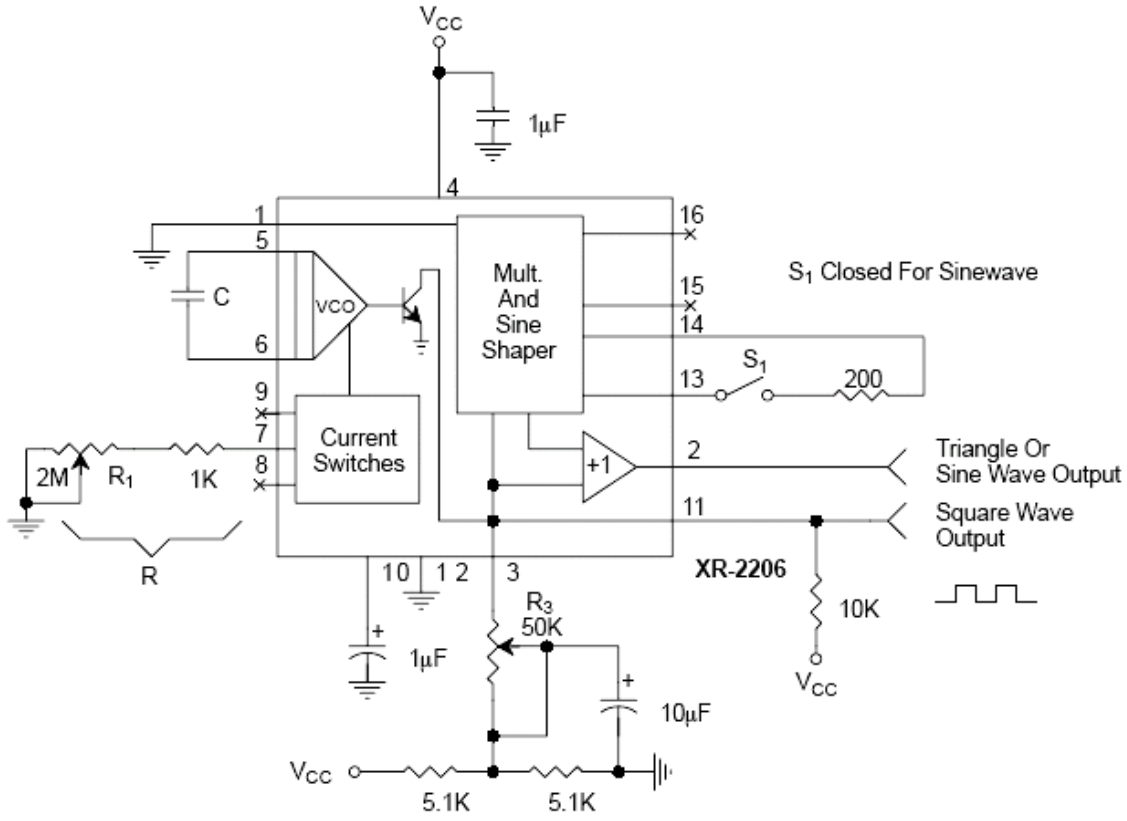


Figura 8. Circuito de generador XR-2206

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, R1, mediante la siguiente ecuación:

$$f = \frac{1}{RC} \tag{13}$$

El valor máximo del capacitor C, es de $100\mu F$ y la resistencia R_1, puede llegar hasta $2M\Omega$. El valor de C para este *jammer* es de $100\rho F$ y la resistencia R_1 es variable. La amplitud varía por medio del potenciómetro R_3, y aumenta a razón de $160\,mV/k\Omega$ para la onda triangular y de $60\,mV/k\Omega$ para la onda senoidal.

4.2.3 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 $2M\Omega$ (frecuencia), $50k\Omega$ (amplitud) y $500k\Omega$ (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 $15[V]$ y $17[V]$, el Offset debe tener el valor requerido para que el voltaje mínimo sea de $15[V]$ y la frecuencia un valor entre $1{,}85GHz$ y $1{,}95GHz$ para garantizar la interrupción de la comunicación entre radiobase y unidad móvil. El valor exacto y óptimo se obtiene mediante prueba y error a la inexistencia de un método.

4.2.4 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 conectados al plano tierra. Las dimensiones de la línea para lograr un acoplamiento a 50Ω se muestra en Figura 9.

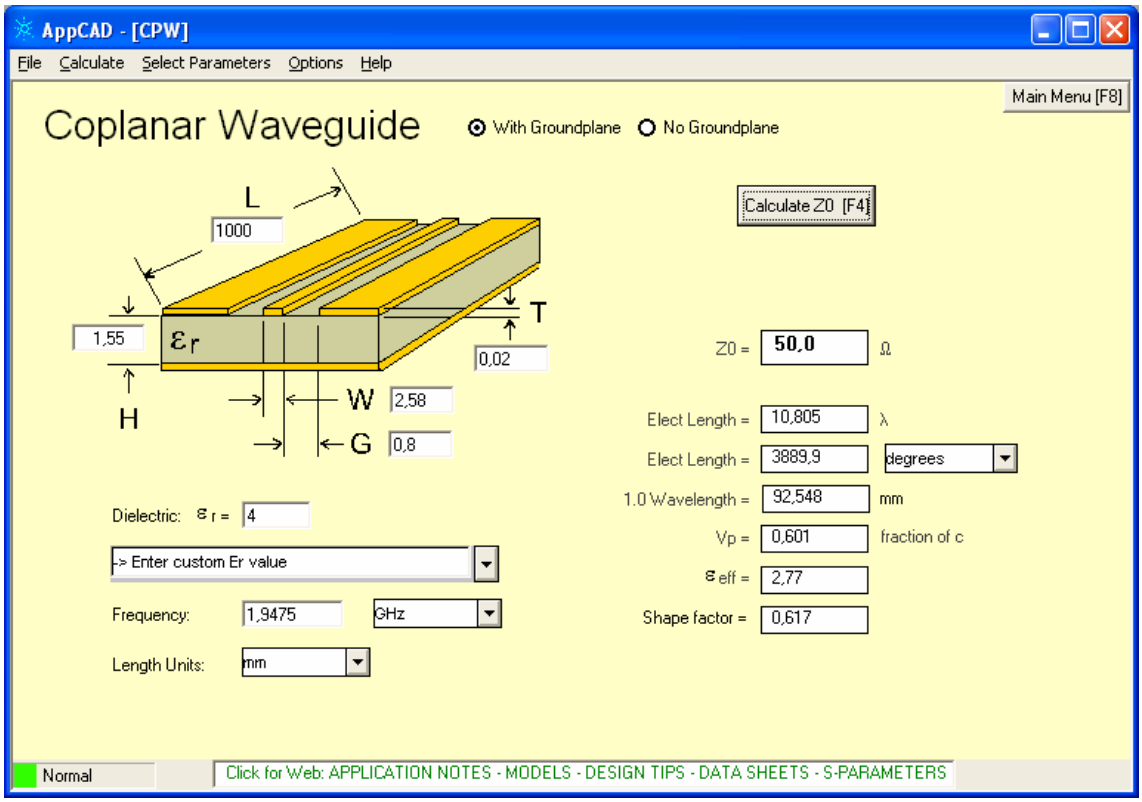


Figura 9. Dimensiones de la línea coplanar [13].

El dieléctrico empleado para la placa del circuito es fibra de vidrio. Las características de dicho material son las siguientes:

- Permitividad relativa de 4
- Pérdida tangente de 0,026
- Altura de 1,55mm.
- Impedancia característica de 50Ω.

En la Figura 9 se puede ver que la frecuencia, la constante dieléctrica y la altura del dieléctrico del material son parámetros importantes para obtener las dimensiones de *W* y *G* que garanticen la transferencia de energía.

El funcionamiento de programa AppCAD consiste en:

- Ingresar los parámetros que son fijos como: *H* = altura del dieléctrico, *T* = altura del conductor, *L* = ancho de la línea de transmisión (imponerse un

valor), ε_r = constante dieléctrica del material y la frecuencia a la cual se va ha trabajar.

- Dar valores a *W* y *G* hasta obtener una impedancia de 50Ω.

Hay que tomar en cuenta que, los valores de *W* y *G* nos son iguales si se utiliza en uno ó ambos lados del dieléctrico, el plano tierra.

Por último, la antena con la que trabaja el jammer es una OMA de 7 segmentos. 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. La conexión entre la antena y la línea de transmisión se hace por medio de conectores *Subminiature version A* (SMA). Este tipo de conectores están acoplados a 50Ω y garantizan la transferencia de energía a frecuencias hasta de 18GHz. Los valores de *L, W_1* y *W_2 son* [9]:

$L = 37mm$, $W_1 = 2mm$, $W_2 = 16mm$

4.2.5 Alimentación

La alimentación del circuito se toma de la línea de 120V. Para rectificar esta señal se usa un transformador a 18V, un puente rectificador de diodos AM154 y un capacitor de $470\mu F$ para garantizar la eliminación del rizo. Una vez rectificada la línea, se obtiene 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 8V de salida. Para evitar ruido por parte de la fuente de alimentación, la impresión de esta parte del circuito estará en otra placa impresa. Con el mismo fin, se colocan capacitares de $1\mu F$ para cada uno.

CAPÍTULO 5

SIMULACIÓN Y RESULTADOS DEL JAMMER

5.1 SIMULACIÓN DEL OFFSET

La simulación del Offset se la realizó en un solo bloque, debido a que el simulador utilizado no cuenta con el integrado XR-2206, por esta razón, se usaron valores reales que fueron obtenidos del circuito. Los valores dados por el circuito fueron:

- ➔ Voltaje mínimo: 9,2 V
- ➔ Voltaje máximo: 14,4 V
- ➔ Frecuencia: 2,17 MHz

La Figura 10 muestra el circuito encargado de modificar el Offset. Consta de un transistor BJT 2N2222 y una fuente de señal triangular de aproximadamente 15V a 17V.

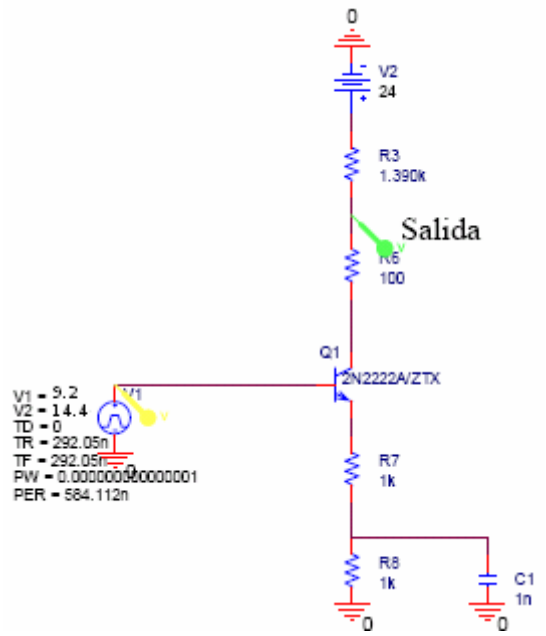


Figura 10. Circuito encargado del Offset [12]

La Figura 11, muestra el resultado de la simulación del Offset. Se puede observar que el valor máximo es de 18,737V y el valor mínimo es de 13,867V.

En el circuito real el valor de R_3 se sustituye por un potenciómetro de precisión de 500Ω, el cual ajustara el valor del Offset.

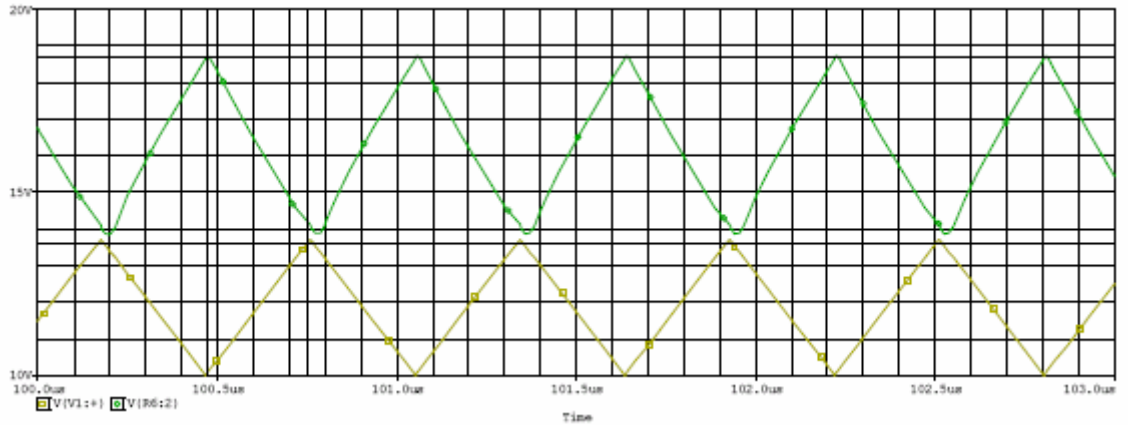


Figura 11. Entrada (parte baja) y salida (parte alta) del BJT.

5.2 PREDICCIÓN DE LA POTENCIA

Se pudo predecir el área de cobertura del jammer, utilizando los modelos de propagación mencionados anteriormente. Para predecir el área de cobertura de la Estación Base (Antena de la operadora ALEGRO) se utilizó el modelo Okumura – Hata y se fijó una potencia de 20W.

Tabla 3. Modelo Okumura – Hata

d(Km)	Lp(dB)	Prx(dBm)/Ptx=20W
0,03	**86,7872052**	**-43,77690524**
0,035	89,1453963	-46,13509634
0,04	91,1881542	-48,17785424
0,045	92,9899944	-49,97969444
0,05	94,6017955	-51,59149554
0,055	96,0598468	-53,04954684
0,06	97,3909434	-54,38064344
0,065	98,6154336	-55,60513364
0,07	99,7491344	-56,73883444
0,075	100,804585	-57,79428504
0,08	101,791892	-58,78159204
0,085	102,719325	-59,70902504

0,09	103,593733	-60,58343304
0,095	104,420851	-61,41055104
0,1	105,205534	-62,19523404
0,2	115,809272	-72,79897204
0,3	122,012061	-79,00176104
0,4	126,41301	-83,40271004
0,5	129,826651	-86,81635104
0,6	132,615799	-89,60549904
0,7	134,97399	-91,96369004
0,8	137,016748	-94,00644804
0,9	138,818588	-95,80828804
1	140,430389	-97,42008904
2	151,034128	-108,023828
3	157,236917	-114,226617
4	161,637866	-118,627566
5	165,051507	-122,041207
6	167,840655	-124,830355
7	170,198846	-127,188546
8	172,241604	-129,231304
9	174,043444	-131,033144
10	175,655245	-132,644945

En Figura 12 se puede observar que a mayor distancia, la señal se va atenuando.

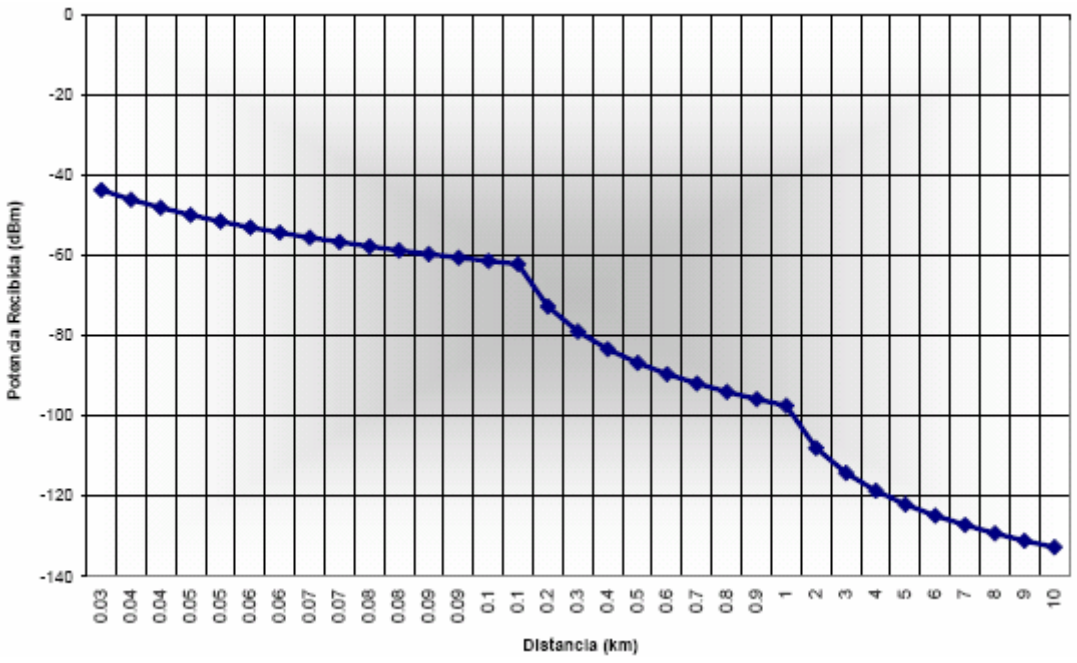


Figura 12. Gráfica del modelo Okumura – Hata.

Para predecir el área de cobertura el jammer, se utilizó el modelo ITU para interiores, la siguiente tabla muestra los valores obtenidos.

Tabla 4. Modelo ITU para interiores

d(m)	Lp(dBm)	Prx(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	-33,61633292
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

Al igual que el modelo anterior, se puede observar a mayor distancia mayor atenuación.

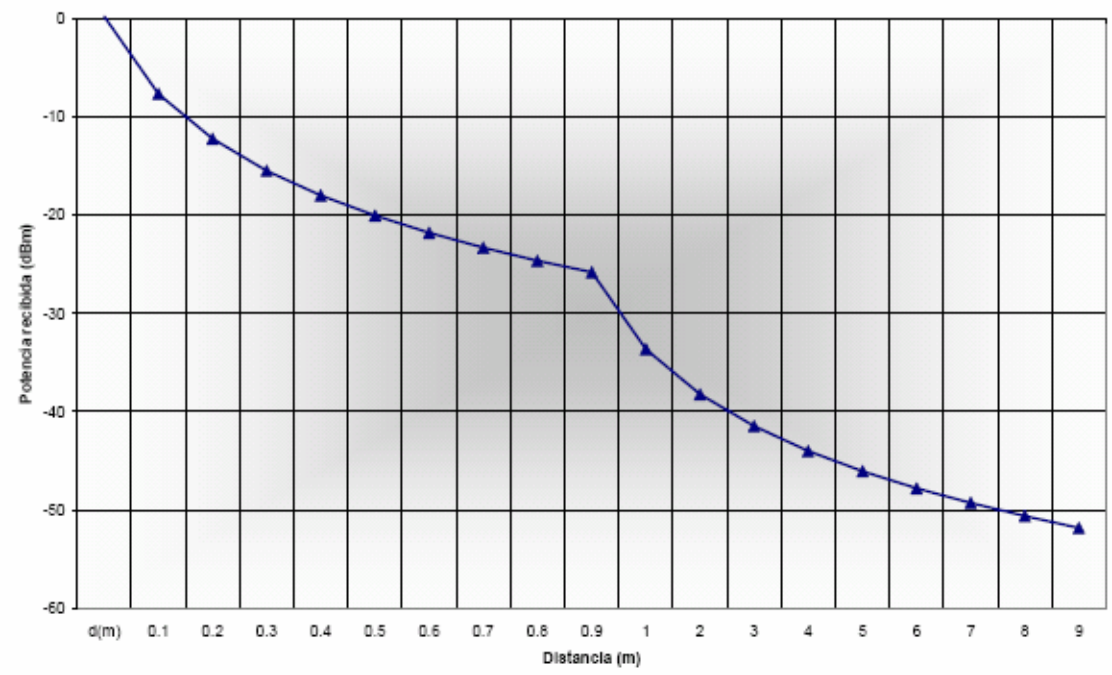


Figura 13. Gráfica del modelo ITU para interiores

Para determinar la cobertura del jammer, se realiza la comparación entre estas predicciones. Se puede observar que en el caso extremo donde la estación base se encuentre a 30m, el jammer podrá operar hasta 4 metros a la redonda, se deduce de la comparación de la potencia de recepción hacia la antena de la unidad móvil (-41,44 > -43,77). Es necesario señalar que este valor depende también de la sensibilidad y ganancia de cada unidad móvil.

5.3 ÁREA DE COBERTURA

Las pruebas realizadas al jammer fueron referentes al área de cobertura. Estas pruebas se realizaron en el aula 210-B de la ESPE. Cabe mencionar que se hay dos ventanas en una de las paredes del aula.

El proceso fue el siguiente:

- Se colocó el jammer aproximadamente en el centro del cuarto.
- Se ubicó al teléfono a una distancia de 4 metros y a 0° con respecto del jammer.
- Se fue acercando el teléfono muy lentamente para ver en que momento la señal sufría alteraciones.
- Al encontrar la distancia máxima se registro para esa dirección.
- Se esperó a que el móvil recuperara la señal alejándolo del jammer.
- Se realizó el mismo proceso pero ahora en móvil colocado a 45° aproximadamente del jammer.

Estas mediciones se realizaron con un teléfono de marca Nokia modelo 2270. La Figura 14 muestra el área de cobertura del jammer, además se puede observar que el jammer está colocado en el centro y la unidad móvil se va moviendo alrededor de él. Además se puede apreciar una brújula que indica la dirección de las mediciones.

Mediante esta la Figura 14, se puede concluir que el jammer trabaja exitosamente a casi 1,10 metros a la redonda, dependiendo de la colocación de la radiobase de la operadora celular.

Esta prueba se realizó en dos ubicaciones diferentes, en los lugares:

- Sangolqui - Capelo, Urb. Las Retamas, donde el área de cobertura llegó a 2 metros a la redonda, y

- Sector el Inca, donde el área de cobertura llegó hasta los 3,5 metros.

Dados estos resultados se puede deducir que el rango de operación o área de cobertura del jammer, dependerá de la ubicación de la radiobase de la operadora celular ALEGRO.

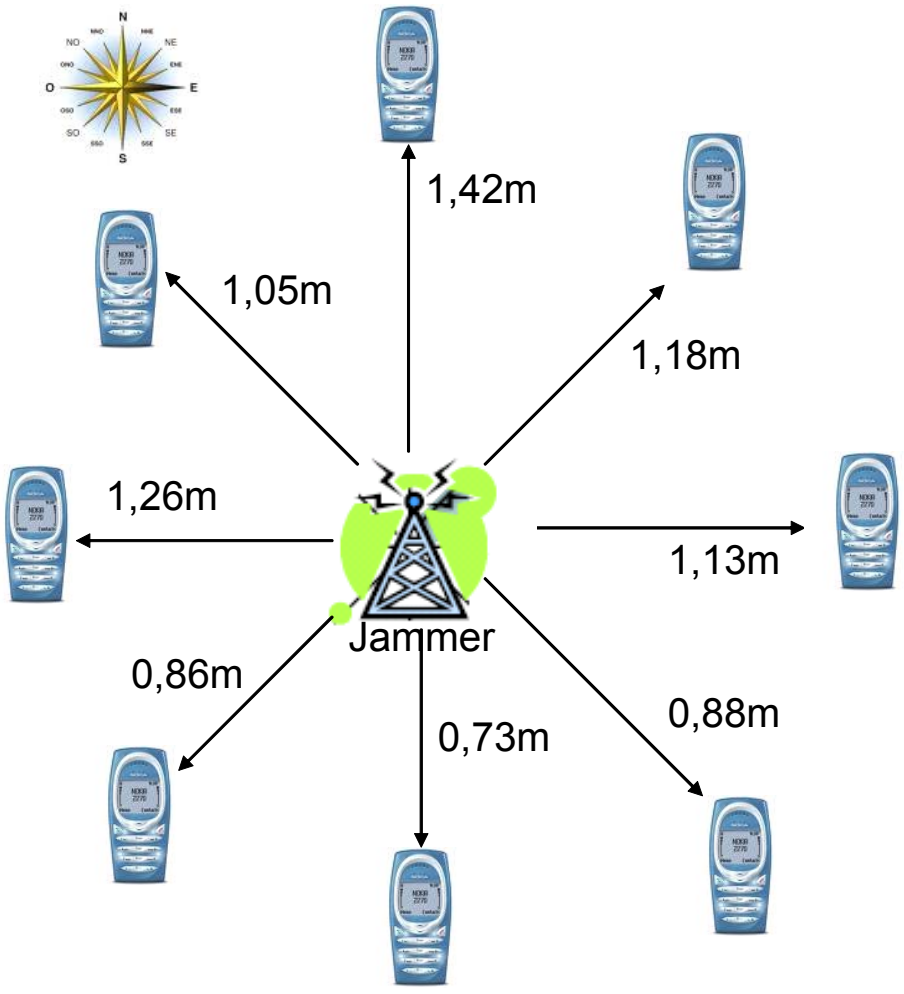


Figura 14. Área de cobertura del jammer en el aula 210B de la ESPE

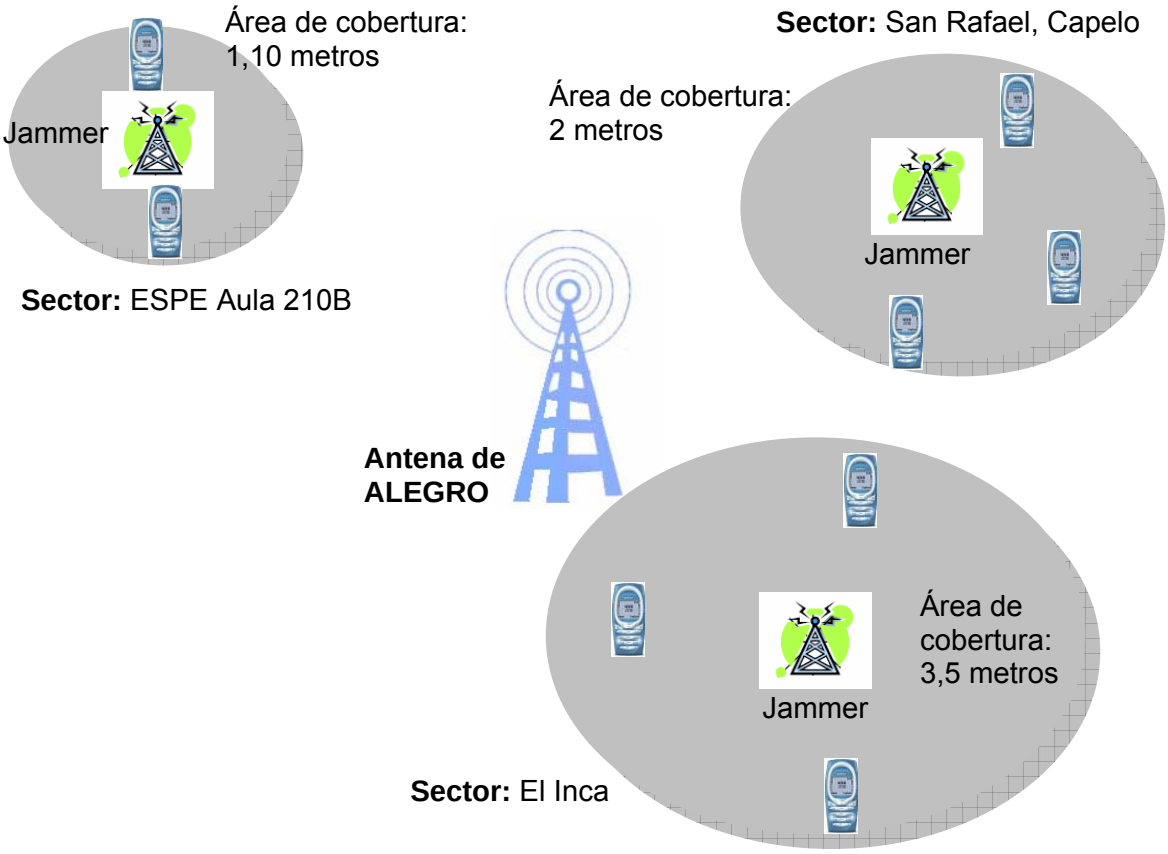


Figura 15. Área de cobertura en 3 puntos distintos

CAPÍTULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

Lo primero que se nota al analizar estos resultados es el área de cobertura, que es de aproximadamente 1,10 metros a la redonda, mientras que el área que se esperaba era de 4 metros. Las variaciones se deben a varios factores:

- Los modelos de propagación para calcular las pérdidas no son exactos, tratan de aproximarse a realidad pero no se puede moldear cada ambiente y lugar de una manera precisa.

- El circuito receptor de la unidad móvil no fue considerado en los cálculos, cada unidad móvil posee distinta sensibilidad de recepción.

- El factor de tolerancia de cada dispositivo del circuito.

Después de realizar varias pruebas en distintos lugares y obtener datos superiores de cobertura comparada con los datos arrojados en el aula 210-B, se analizó que:

- En el diseño no se tomó en consideración el control de potencia que debe poseer el circuito, debido al comportamiento de la transmisión con tecnología CDMA, por esta razón los valores de cobertura son diferentes en distintos sitios.

Si el proyecto se hubiera enfocado a eliminar la señal celular para la tecnología GSM, el área de cobertura sería igual en cualquier lugar.

A pesar de no haber alcanzado el área de cobertura teórica, el resultado es muy bueno. La interrupción de la señal toma de 10 a 20 segundos, tiempo en que demora la

señal del jammer entrar en resonancia con la señal de la operadora celular, el mismo tiempo le toma al móvil para recuperar la señal una vez salido de la cobertura del jammer.

Esto indica que el comportamiento del jammer es efectivo.

6.2 RECOMENDACIONES

El circuito se podría mejorar en varios aspectos:

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

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

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

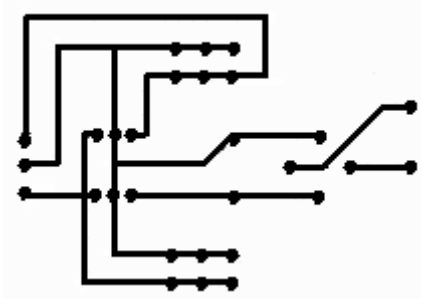
- Implementar un circuito que realice el control de potencia, para que el área de cobertura sea igual en cualquier sitio donde se desee utilizar el jammer. El dispositivo debe monitorear la señal que se va a bloquear, determinar su nivel de potencia y así saber cuanta potencia debe de aplicar el Jammer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

ANEXOS

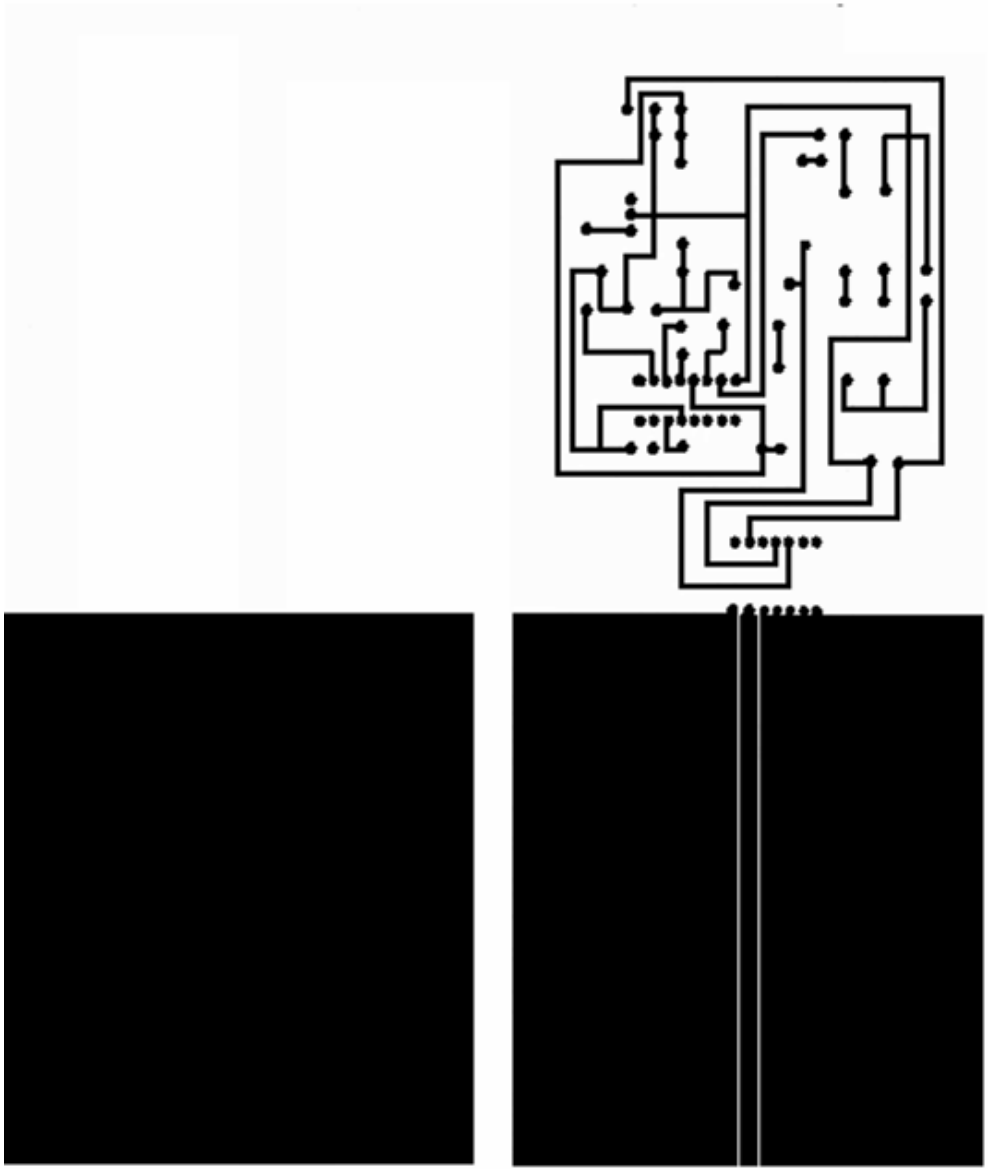
ANEXO 1

CIRCUITO IMPRESO (RUTEO DE PISTAS)

Pista de la fuente de alimentación



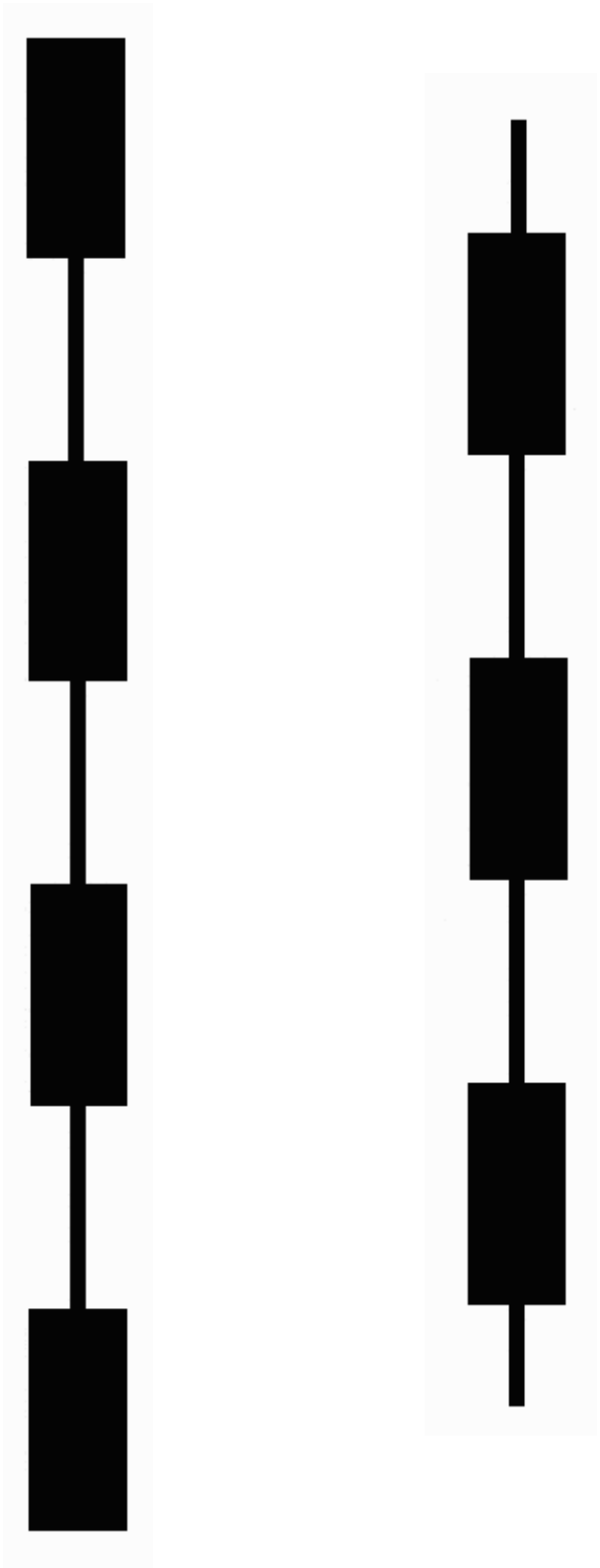
Vista superior **Vista inferior**



ANEXO 2

PISTA DE LA ANTENA

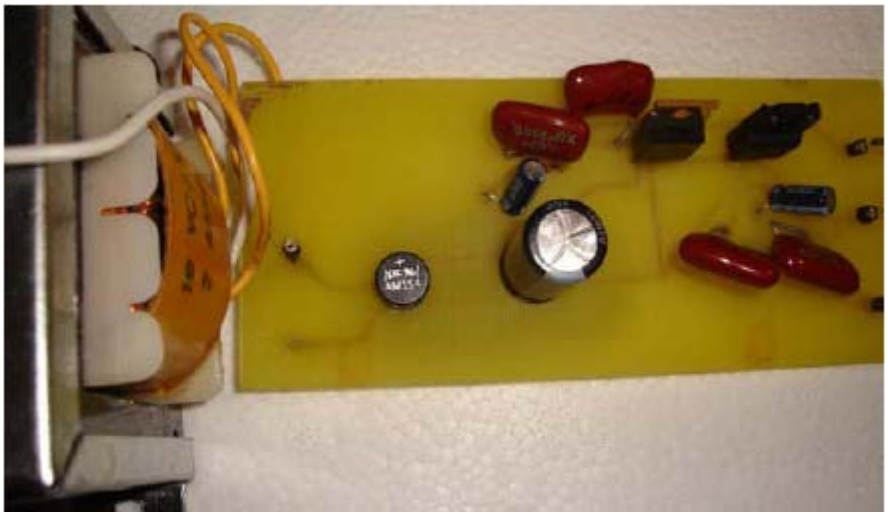
Vista superior **Vista inferior**



ANEXO 3

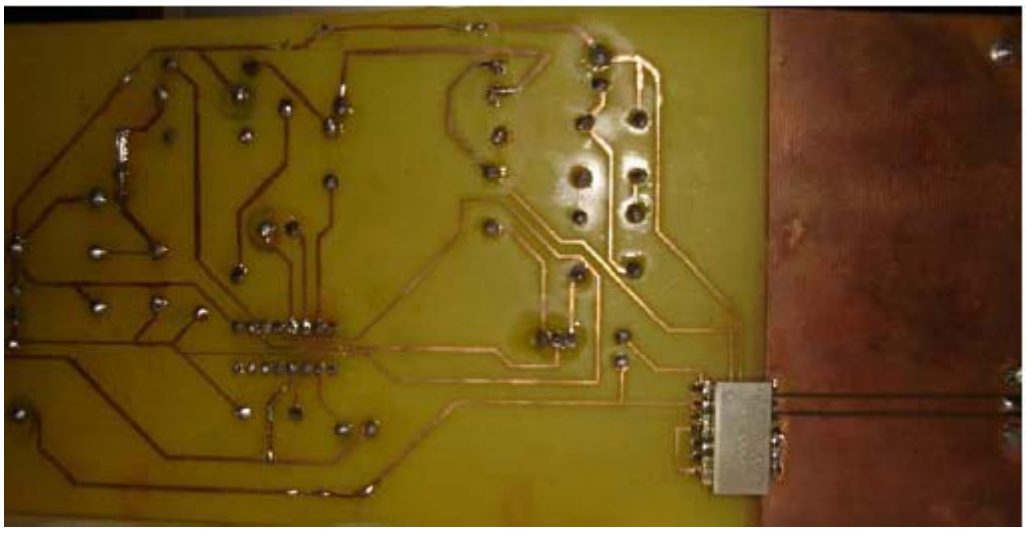
FOTOGRAFÍAS DEL DISPOSITIVO

Placa de Alimentación y transformador

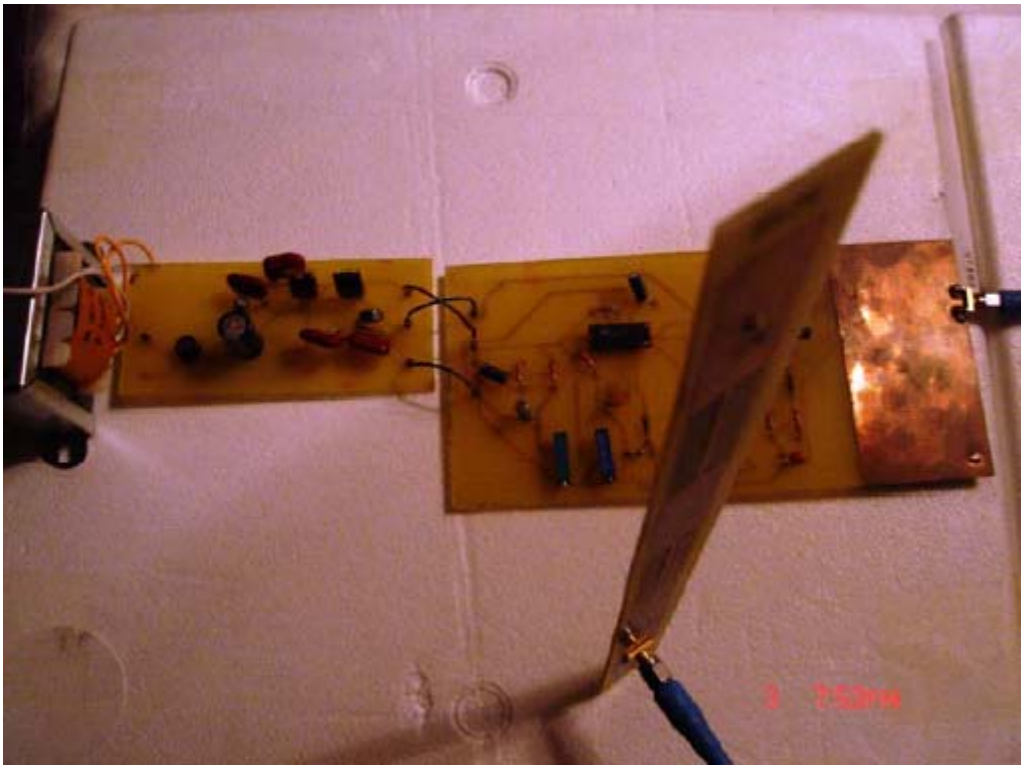


Placa del Jammer

Placa Inferior del Jammer



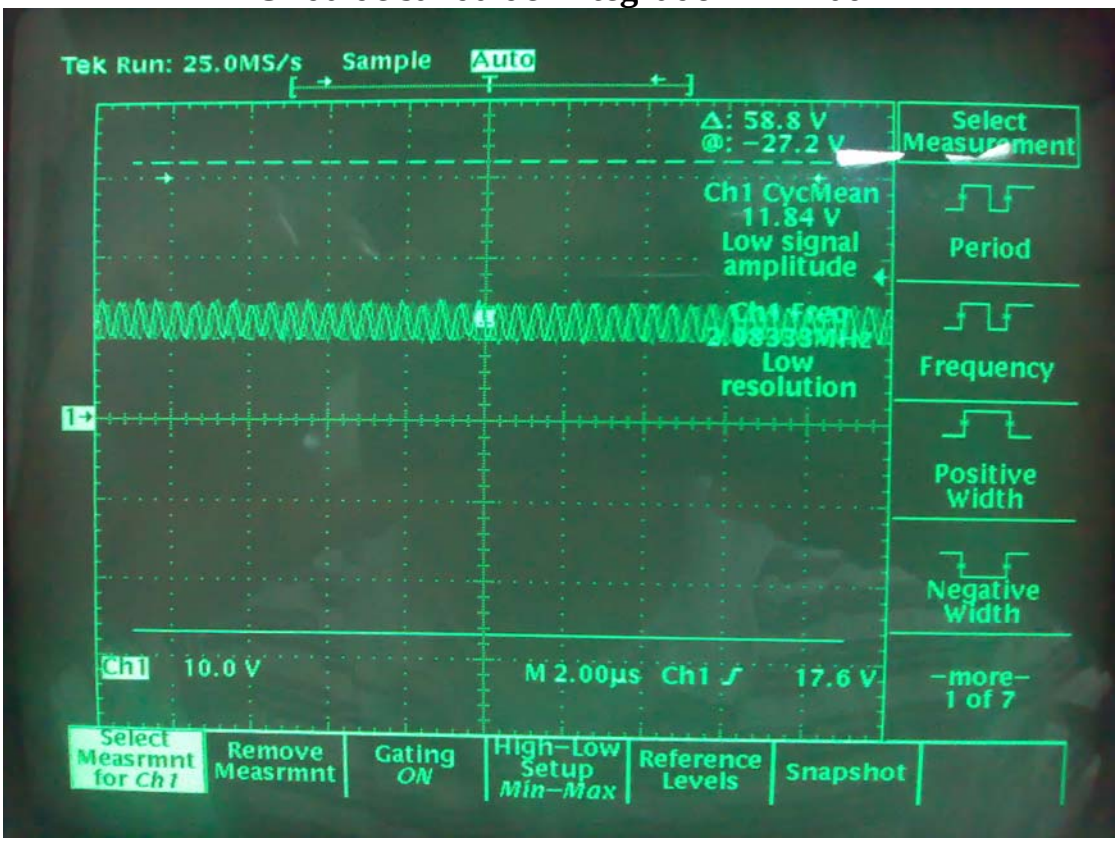
Circuito completo



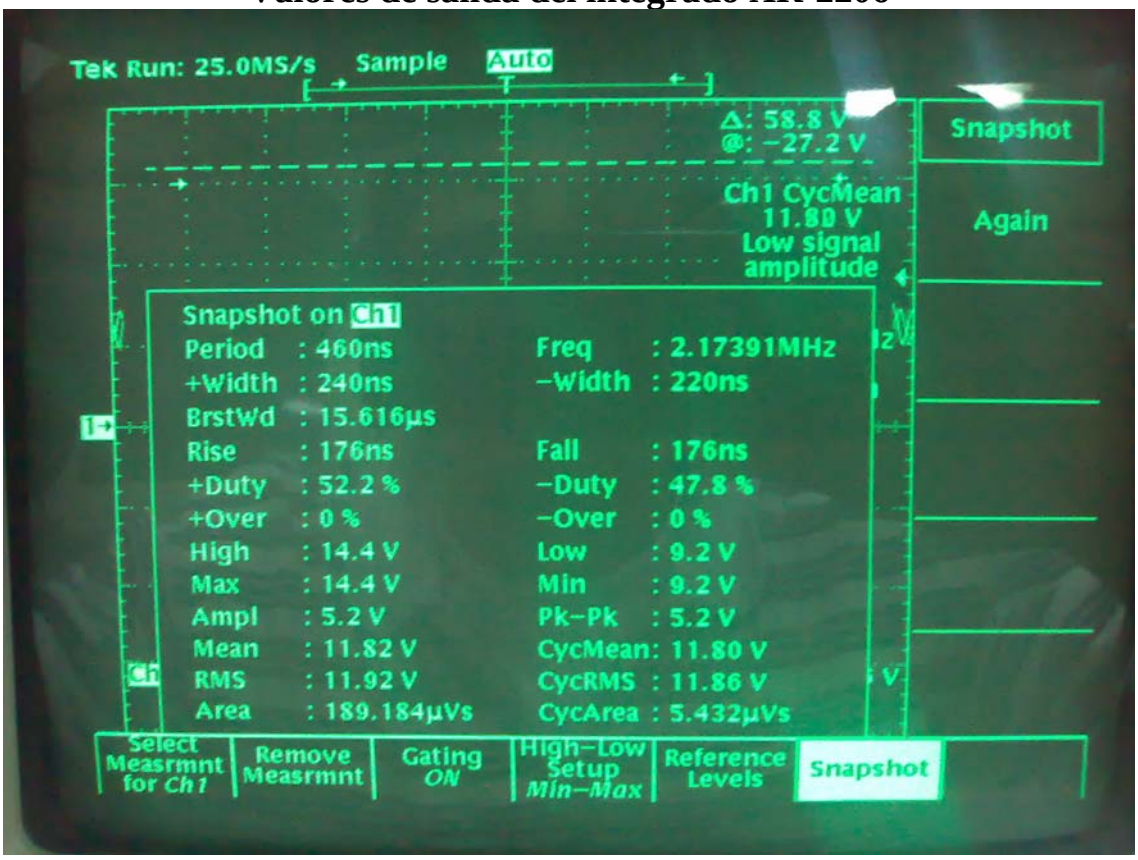
ANEXO 4

DATOS OBTENIDOS DEL OSCILADOR HP

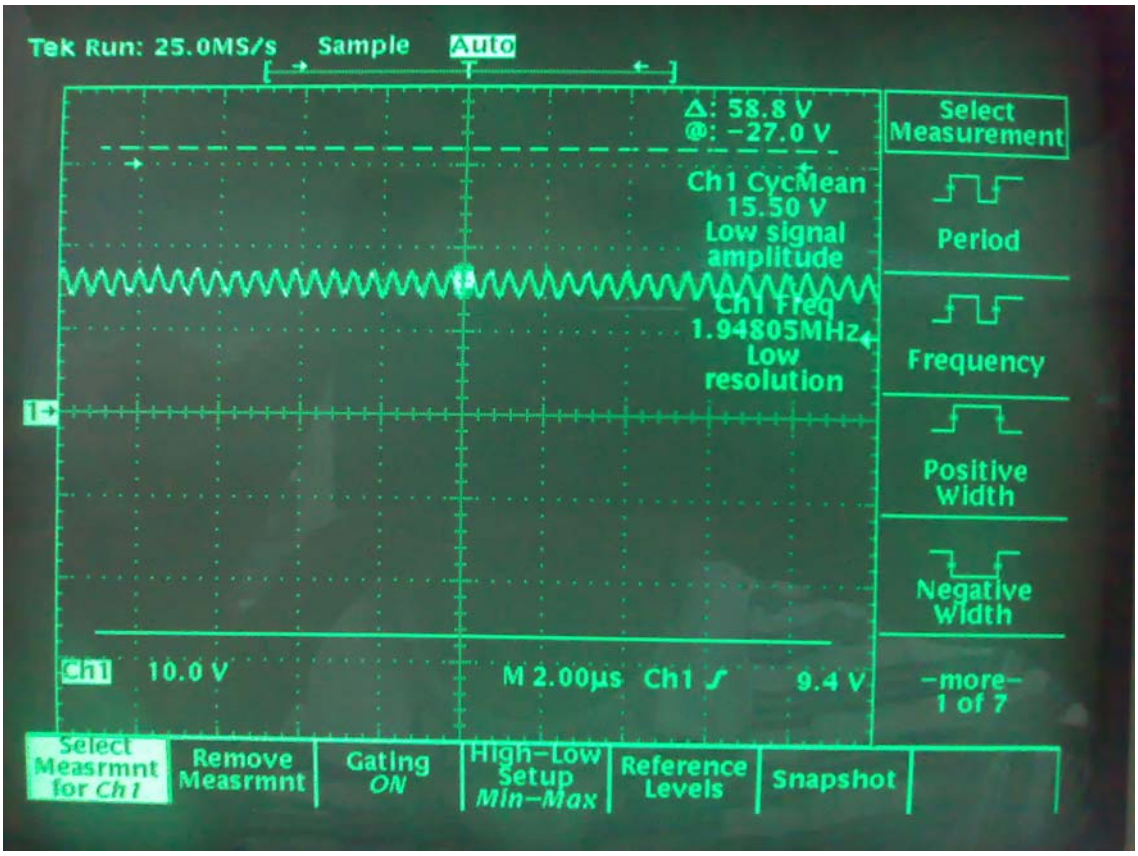
Onda de salida del integrado XR-2206



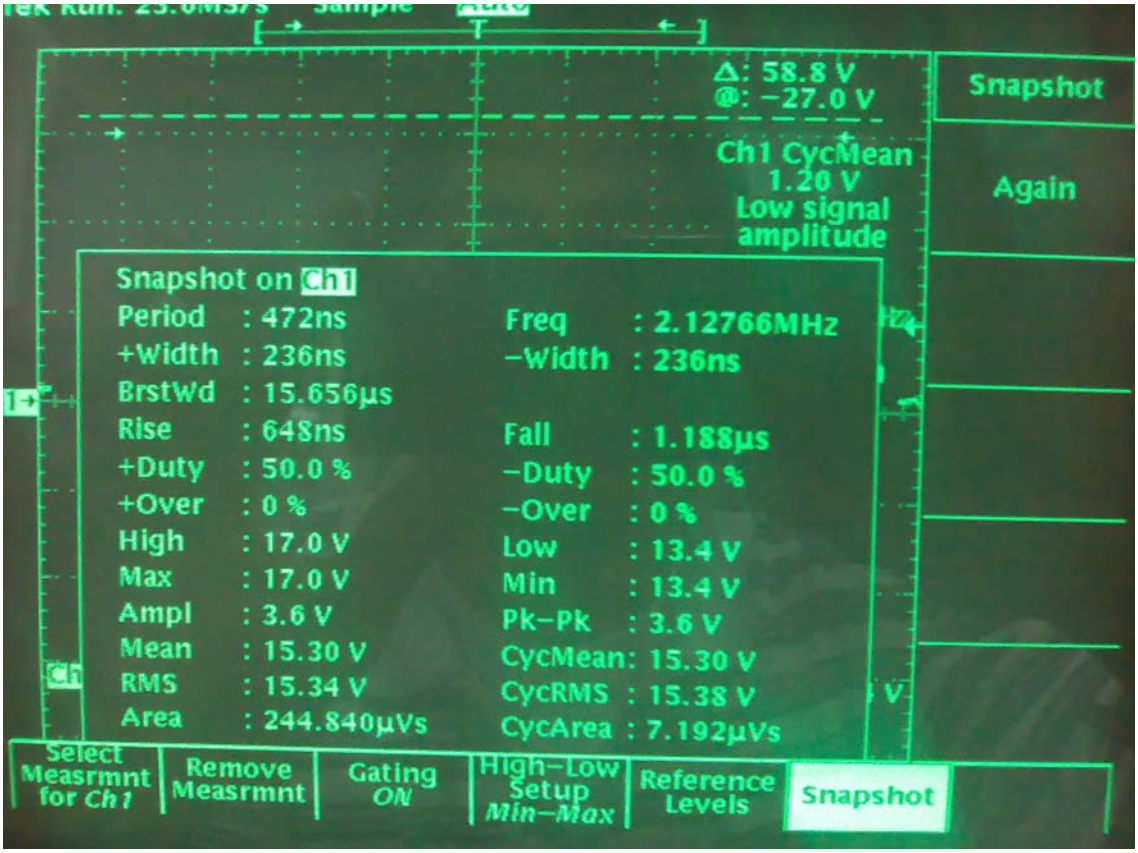
Valores de salida del integrado XR-2206



Onda de salida del BJT 2N2222



Valores de salida del BJT 2N2222



ANEXO 5

LISTADO DE MATERIALES

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL
JTOS-2000 de *Minicircuits*®	1	24,90	24,90
Freight Charges	JTOS-2000	33,50	33,50
Aduana	JTOS-2000	12,50	12,50
XR-2206	1	6,16	6,16
BJT-2N2222	1	0,67	0,67
Potenciómetro de precisión 50kΩ	1	1,90	1,90
Potenciómetro de precisión 500kΩ	1	1,90	1,90
Potenciómetro de precisión 2MΩ	1	1,25	1,25
LM7824	1	1,10	1,10
LM7808	1	0,60	0,60
Puente de diodos AM154	1	0,50	0,50
Transformador de 18V [0,5 A]	1	3,50	3,50
Capacitor cerámico 0,47 uF	4	1,10	4,40
Capacitor cerámico 1 nF	1	0,15	0,15
Capacitor cerámico 100 pF	1	0,15	0,15
Capacitor 1uF	5	0,05	0,25
Capacitor 10uF	1	0,10	0,10
Capacitor 470uF	1	0,25	0,25
Zócalo 16P	1	0,09	0,09
Resistencia 5,1kΩ	2	0,03	0,06
Resistencia 1kΩ	2	0,03	0,06
Resistencia 10kΩ	1	0,03	0,03
Resistencia 100Ω	1	0,03	0,03
Resistencia 270Ω	2	0,03	0,06
Resistencia 820Ω	2	0,03	0,06
Resistencia 1,5kΩ	1	0,03	0,03
Cable SMA 1 metro	1	3,57	3,57
Conectores SMA hembra	2	2,95	5,90
Conectores SMA macho	2	3,60	7,20
Hoja de transferencia térmica	2	0,78	1,56
Cloruro Férrico	4	0,40	1,60
Fibra doble lado	1	9,50	9,50
TOTAL			**$ 123,53**

ANEXO 6

HOJA TÉCNICA DEL VCO

Surface Mount

Voltage Controlled Oscillator

JTOS-2000+
JTOS-2000

Wide Band 1370 to 2000 MHz

Features
- wide frequency range, 1370 to 2000 MHz
- linear tuning characteristics
- low phase noise, -135 dBc/Hz at 1MHz offset
- aqueous washable

Applications
- instrumentation
- PCS/DCS
- communication systems

CASE STYLE: BK377
PRICE: $19.95 ea. QTY (5-49)

+ RoHS compliant in accordance with EU Directive (2002/95/EC)

The + suffix identifies RoHS Compliance. See our web site for RoHS Compliance methodologies and qualifications.

Electrical Specifications

MODEL NO.	FREQ. (MHz)		POWER OUTPUT (dBm)	TUNING VOLTAGE (V)		PHASE NOISE dBc/Hz SSB at offset frequencies: Typ.				PULLING pk-pk @ 12 dBr (MHz)	PUSHING (MHz/V)	TUNING SENSI-TIVITY (MHz/V)	HARMONICS (dBc)		3 dB MODULATION BANDWIDTH (MHz)	DC OPERATING POWER Vcc (Volts)	DC OPERATING POWER Current (mA) Max.
	Min.	Max.	Typ.	Min.	Max.	1 kHz	10 kHz	100 kHz	1 MHz	Typ.	Typ.	Typ.	Typ.	Max.	Typ.		
JTOS-2000	1370	2000	+12.0	1.0	22	-70	-95	-115	-135	40	1.5	30-50	-11	-8	1.0	8	30

Pin Connections

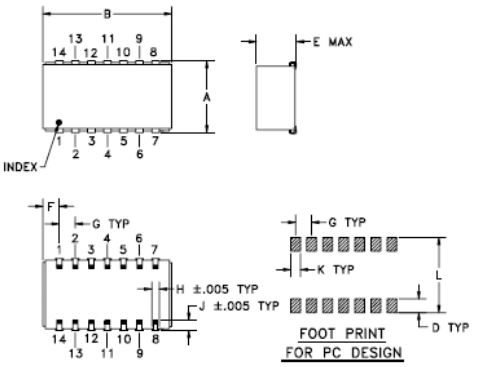
RF OUT	13
VCC	2
V-TUNE	5
GROUND	1,3,4,6,7,8,9,10,11,12,14

Maximum Ratings

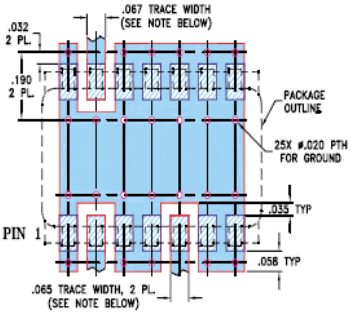
Operating Temperature	-55°C to 85°C
Storage Temperature	-55°C to 100°C
Absolute Max. Supply Voltage (Vcc)	+10V
Absolute Max. Tuning Voltage (Vtune)	+25V

all specifications: 50 ohm system

Outline Drawing



Demo Board MCL P/N: TB-04
Suggested PCB Layout (PL-005)



NOTES: 1. TRACE WIDTH IS SHOWN FOR ROGERS RO4350B WITH DIELECTRIC THICKNESS .030" ± .002"; COPPER: 1/2 OZ. EACH SIDE. FOR OTHER MATERIALS TRACE WIDTH MAY NEED TO BE MODIFIED.
2. BOTTOM SIDE OF THE BOTTOM IS CONTINUOUS GROUND PLANE.

DENOTES PCB COPPER LAYOUT WITH SMOBC (SOLDER MASK OVER BARE COPPER)

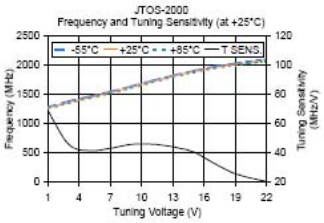
DENOTES COPPER LAND PATTERN FREE OF SOLDER MASK

Outline Dimensions (inch / mm)

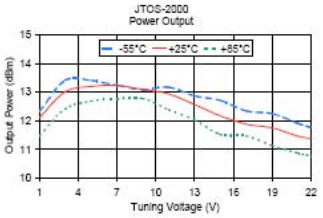
A	B	C	D	E	F	G	H	J	K	L	wt
.505	.800	–	.100	.250	.100	.100	.047	.065	.065	.525	grams
12.83	20.32	--	2.54	6.35	2.54	2.54	1.19	1.65	1.65	13.34	3.0

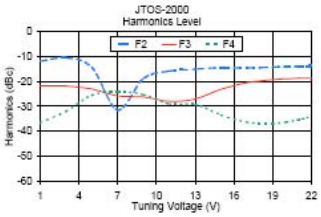
JTOS-2000+
JTOS-2000

Performance Curves

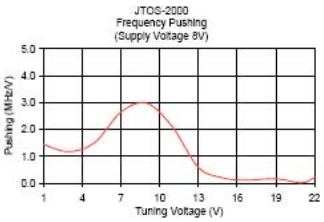


V TUNE	TUNING SENS. (MHz/V)	FREQUENCY (MHz) -55°C	+25°C	+85°C	POWER OUTPUT (dBm) -55°C	+25°C	+85°C
1.00	69.23	1284.71	1266.03	1250.18	12.32	12.11	11.47
3.00	46.00	1384.20	1364.13	1346.86	13.41	13.01	12.41
5.00	41.55	1464.49	1446.30	1429.90	13.41	13.20	12.69
7.00	43.22	1547.52	1530.72	1514.72	13.24	13.24	12.77
9.00	45.84	1640.53	1621.98	1604.43	13.09	13.10	12.78
11.00	46.00	1733.86	1715.81	1699.63	13.17	12.94	12.39
13.00	44.21	1823.35	1807.46	1791.67	12.87	12.57	12.03
15.00	40.65	1905.18	1890.65	1875.57	12.71	12.17	11.52
17.00	32.90	1974.74	1958.16	1941.17	12.34	11.88	11.47
19.00	25.83	2030.28	2015.46	1999.05	12.25	11.75	11.13
21.00	22.06	2078.26	2060.56	2041.93	11.91	11.46	10.87
22.00	20.61	2099.05	2081.16	2061.53	11.76	11.38	10.76





V TUNE	HARMONICS (dBc) F2	F3	F4	FREQ. PUSHING (MHz/V)
1.00	-11.92	-21.75	-36.75	1.43
3.00	-10.52	-21.85	-32.02	1.17
5.00	-14.40	-23.07	-25.57	1.53
7.00	-31.46	-25.80	-24.13	2.65
9.00	-18.84	-26.27	-25.34	2.97
11.00	-15.84	-28.01	-29.01	2.08
13.00	-15.06	-27.06	-29.23	0.59
15.00	-14.49	-23.16	-33.49	0.18
17.00	-14.56	-20.56	-36.39	0.12
19.00	-14.32	-19.32	-36.98	0.16
21.00	-13.93	-18.76	-35.43	0.02
22.00	-13.80	-18.80	-33.96	0.20



ANEXO 7

HOJA TÉCNICA DEL XR-2206

EXAR ...the analog plus company™

XR-2206

Monolithic
Function Generator

June 1997-3

FEATURES

- Low-Sine Wave Distortion, 0.5%, Typical
- Excellent Temperature Stability, 20ppm/°C, Typ.
- Wide Sweep Range, 2000:1, Typical
- Low-Supply Sensitivity, 0.01%V, Typ.
- Linear Amplitude Modulation
- TTL Compatible FSK Controls
- Wide Supply Range, 10V to 26V
- Adjustable Duty Cycle, 1% TO 99%

APPLICATIONS

- Waveform Generation
- Sweep Generation
- AM/FM Generation
- V/F Conversion
- FSK Generation
- Phase-Locked Loops (VCO)

GENERAL DESCRIPTION

The XR-2206 is a monolithic function generator integrated circuit capable of producing high quality sine, square, triangle, ramp, and pulse waveforms of high-stability and accuracy. The output waveforms can be both amplitude and frequency modulated by an external voltage. Frequency of operation can be selected externally over a range of 0.01Hz to more than 1MHz.

The circuit is ideally suited for communications, instrumentation, and function generator applications requiring sinusoidal tone, AM, FM, or FSK generation. It has a typical drift specification of 20ppm/°C. The oscillator frequency can be linearly swept over a 2000:1 frequency range with an external control voltage, while maintaining low distortion.

ORDERING INFORMATION

Part No.	Package	Operating Temperature Range
XR-2206M	16 Lead 300 Mil CDIP	-55°C to +125°C
XR-2206P	16 Lead 300 Mil PDIP	–40°C to +85°C
XR-2206CP	16 Lead 300 Mil PDIP	0°C to +70°C
XR-2206D	16 Lead 300 Mil JEDEC SOIC	0°C to +70°C

EXAR Corporation, 48720 Kato Road, Fremont, CA 94538 ◆ (510) 668-7000 ◆ (510) 668-7017

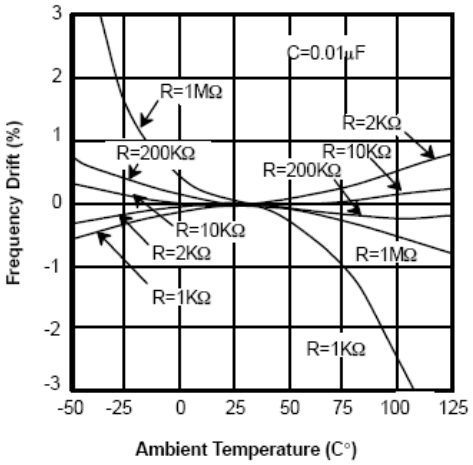


Figure 9. Frequency Drift versus Temperature.

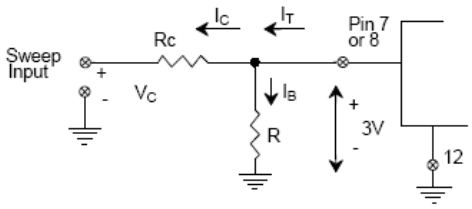


Figure 10. Circuit Connection for Frequency Sweep.

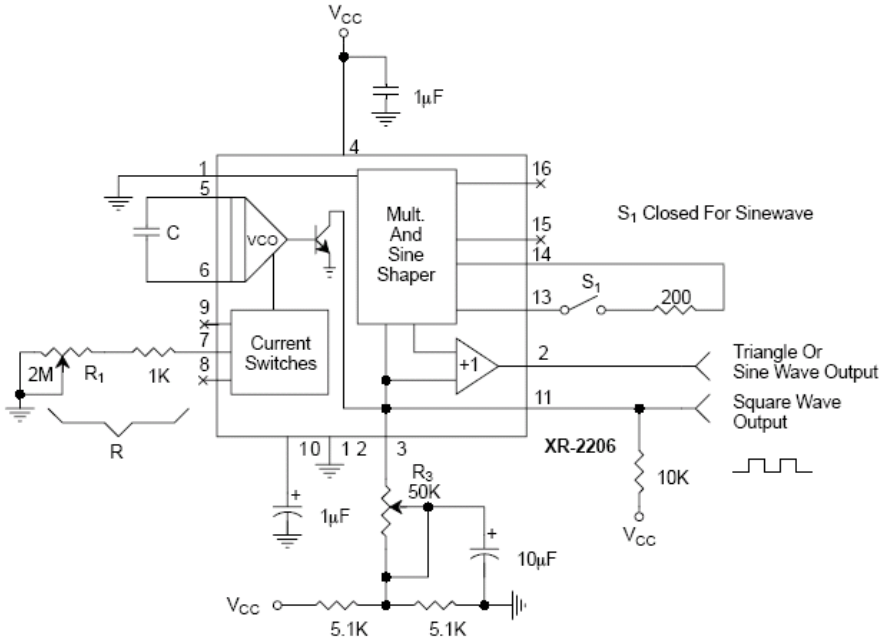


Figure 11. Circuit tor Sine Wave Generation without External Adjustment. (See *Figure 3* for Choice of R_3)

ANEXO 8

HOJA TÉCNICA DEL BJT-2N2222

NPN switching transistors 2N2222; 2N2222A

FEATURES

- High current (max. 800 mA)
- Low voltage (max. 40 V).

APPLICATIONS

- Linear amplification and switching.

DESCRIPTION

NPN switching transistor in a TO-18 metal package.
PNP complement: 2N2907A.

PINNING

PIN	DESCRIPTION
1	emitter
2	base
3	collector, connected to case

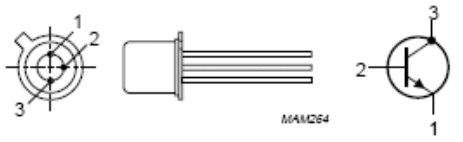


Fig.1 Simplified outline (TO-18) and symbol.

QUICK REFERENCE DATA

SYMBOL	PARAMETER	CONDITIONS	MIN.	MAX.	UNIT
V_{CBO}	collector-base voltage	open emitter			
	2N2222		–	60	V
	2N2222A		–	75	V
V_{CEO}	collector-emitter voltage	open base			
	2N2222		–	30	V
	2N2222A		–	40	V
I_C	collector current (DC)		–	800	mA
P_{tot}	total power dissipation	$T_{amb} \leq 25$ °C	–	500	mW
h_{FE}	DC current gain	I_C = 10 mA; V_{CE} = 10 V	75	–	
f_T	transition frequency	I_C = 20 mA; V_{CE} = 20 V; f = 100 MHz			
	2N2222		250	–	MHz
	2N2222A		300	–	MHz
t_{off}	turn-off time	I_{Con} = 150 mA; I_{Bon} = 15 mA; I_{Boff} = –15 mA	–	250	ns

NPN switching transistors 2N2222; 2N2222A

LIMITING VALUES

In accordance with the Absolute Maximum Rating System (IEC 134).

SYMBOL	PARAMETER	CONDITIONS	MIN.	MAX.	UNIT
V_{CBO}	collector-base voltage	open emitter			
	2N2222		–	60	V
	2N2222A		–	75	V
V_{CEO}	collector-emitter voltage	open base			
	2N2222		–	30	V
	2N2222A		–	40	V
V_{EBO}	emitter-base voltage	open collector			
	2N2222		–	5	V
	2N2222A		–	6	V
I_C	collector current (DC)		–	800	mA
I_{CM}	peak collector current		–	800	mA
I_{BM}	peak base current		–	200	mA
P_{tot}	total power dissipation	$T_{amb} \leq 25$ °C	–	500	mW
		$T_{case} \leq 25$ °C	–	1.2	W
T_{stg}	storage temperature		–65	+150	°C
T_j	junction temperature		–	200	°C
T_{amb}	operating ambient temperature		–65	+150	°C

THERMAL CHARACTERISTICS

SYMBOL	PARAMETER	CONDITIONS	VALUE	UNIT
$R_{th\ j\text{-}a}$	thermal resistance from junction to ambient	in free air	350	K/W
$R_{th\ j\text{-}c}$	thermal resistance from junction to case		146	K/W

REFERENCIAS BIBLIOGRÁFICAS

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

[2] "Jammer PCS", http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/sanchez_i_d/, consultado el 10 de Junio del 2008.

[3] "Técnicas de RF y Microonda", http://docentes.uacj.mx/vhinostr/cursos/tecnicas_rt/capitulo_IV.doc, Consultado el 12 de agosto de 2008.

[4] Fried, Limor, *Social Defense Mechanisms: Tools for Reclaiming Our Personal Space*, 28 enero 2005, http://www.mit.edu/~ladyada.thesis.pdf, consultado el 5 de Noviembre del 2008.

[5] Doble, John, *Introduction to Radio Propagation for Fixel and Mobile Communications*, Norwood: Artech House, 1996.

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

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

[8] The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks, http://www.winlab.rutgers.edu/pub/docs/research/JamDetect_Mobihoc.pdf, consultado el 15 de enero de 2009.

[9] "Omnidirectional planar Antennas for PCS-Band Applications using Fiberglass Substrates", http://ieeexplore.ieee.org/Xplore/login.jsp?url=http%3A%2F%2Fieeexplore

.ieee.org%2Fiel5%2F4470492%2F4470493%2F04470501.pdf%3Farnumber%3D4470501&authDecision=-203, consultado el 15 de Abril del 2009.

[10] http://www.scribd.com/doc/7353218/05-Sistemas-Movilcelular-Cdma, consultado el 8 de Mayo de 2009.

[11] http://www.monografias.com/trabajos13/modu/modu.shtml#cd, consultado el 8 de Mayo de 2009.

[12] Orcad Capture 9.2.3. Cadense Design Systems, Inc. 2002.

[13] AppcCAD for Windows 3.0.2. Agilent Technologies. 2002.

FECHA DE ENTREGA

El proyecto fue entregado al Departamento de Eléctrica y Electrónica y reposa en la Escuela Politécnica del Ejército desde:

Sangolquí, a _____ del 2009.

ELABORADO POR:

_____

CHRISTIAN MAURICIO GUALOTO RAMÍREZ

171841502-7

AUTORIDAD:

_____

Ing. GONZALO OLMEDO

COORDINADOR DE LA CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

_____

Abg. JORGE CARVAJAL

SECRETARIO ACADÉMICO