El comité de trabajo de grado para la maestría de Física Aplicada certifica que esta es la versión aprobada del siguiente trabajo de grado:

Estudio de sistemas de detección e inhibición para emisores celulares presentes en redes comerciales

---

APROBADO POR:

COMITÉ DE SUPERVISORES:

Asesor: _____

_____

Estudio de sistemas de detección e inhibición para emisores celulares presentes en redes comerciales

Por:

Ing. Augusto Carmona Valencia

Trabajo de grado

Facultad de Ciencias y Humanidades

Universidad EAFIT

En el cumplimiento de los requerimientos para obtener el título de:

M. Sc. Física Aplicada

Universidad EAFIT

Julio, 2013

Agradecimientos

Este trabajo no hubiera sido posible sin el valioso apoyo del profesor Ph. D. José Ignacio Marulanda Bernal, a los recursos humanos y técnicos de Tecnologías MARTE y a la Universidad EAFIT.

Resumen

Estudio de sistemas de detección e inhibición para emisores celulares presentes en redes comerciales

Ing. Augusto Carmona Valencia

Universidad EAFIT, 2013

Asesor: Ph. D. José Ignacio Marulanda Bernal

En el presente trabajo se desarrolló una propuesta metodológica para el proceso de detección e inhibición de móviles celulares en rangos de distancias del orden de los 100m. Se evaluó el desempeño en redes celulares con soporte de tecnología GSM y WCDMA de tercera generación (UMTS). Para la validación del protocolo se usó la potencia proveniente del móvil durante la emisión de la señal de reporte o de actualización de localización del móvil con el fin de evaluar la presencia del celular cuando se encuentra en modo de espera. Para el sistema de prueba se usó filtrado en las señales del *uplink,* un medidor de potencia y un micro-controlador comercial de la serie Arduino. Para la propuesta metodológica del sistema de inhibición se implementaron simulaciones de los procesos de comunicación con base en las normas del proyecto 3GPP™, tanto para GSM como para UMTS. Los resultados de las simulaciones y de la propuesta de medición validaron el tipo de señales propuesto por la normatividad, con lo cual se logró delimitar tanto el hardware como el software requeridos para la implementación de un sistema de detección e inhibición en redes 2G y 3G para ambientes rurales de la geografía colombiana.

Abstract

Study of detection and inhibition systems for mobile phone emitters present in cellular networks

Augusto Carmona Valencia

EAFIT University, 2013

Adviser: Ph. D. José Ignacio Marulanda Bernal

In the present work we developed a methodology for the detection process and inhibition of cell phones in range of distances of the order of 100m. We evaluated the performance in cellular networks with support for GSM and WCDMA (UMTS). To validate the protocol used from the mobile power during the emission of the signal reporting location update or mobile in order to assess the presence of the cell when it is in standby mode. For the test system was used filtering uplink signals, a power meter and commercial microcontroller Arduino series. For methodological proposal inhibition system simulations were implemented communication processes based on 3GPP™ project standards for both GSM and UMTS. The results of the simulations and validated the proposed measure signal type proposed by the regulations, which was achieved delineate both the hardware and software required for the implementation of a system for sensing and inhibition 2G and 3G networks rural environments Colombian geography.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Acrónimos

ADC	Conversor Análogo Digital
BER	Tasa de errores en bits
BLER	Tasa de errores por bloques
BS	Estación base
CDMA	Acceso por división de código
COST	Cooperación Europea en Ciencia y Tecnología
CRC	Comprobación de redundancia cíclica
DOA	Dirección de llegada
DPCCH	Canal de control físico dedicado
DPDCH	Canal de datos físicos dedicado
EDGE	Tasas de datos mejoradas para GSM
FDD	División dúplex por frecuencia
FER	Tasa de errores por trama de datos
FS	Espacio libre
GMSK	Mínimo corrimiento de fase gaussiano
GPRS	Servicio general de paquetes vía radio
GSM	Sistema global para las comunicaciones móviles
HSDPA	Acceso por paquetes de alta velocidad (downlink)
HSPA+	Evolución de la tecnología HSDPA
IEDs	Dispositivos explosivos improvisados
MIMO	Múltiples entradas múltiples salidas
MS	Estación móvil
OSI	Interconexión de sistemas abiertos
PCS	Servicio de comunicación personal

PSK	Modulación por desplazamiento de fase
QAM	Modulación de amplitud en cuadratura
QPSK	Modulación por desplazamiento de fase en cuadratura
RACH	Canal de acceso aleatorio
RCIEDs	Dispositivos explosivos improvisados radio controlados
SNR	Razón señal ruido
TDD	División dúplex por tiempo
TDMA	Acceso por división de tiempo
UMTS	Sistema universal de comunicaciones móviles
UTRA	Red de acceso radio terrestre
WCDMA	Acceso múltiple por división de código de banda ancha

Capítulo I

Introducción

Las comunicaciones celulares han pasado de ser un simple sistema de comunicación a todo un protocolo de posibilidades en el accionar delictivo y, en especial, para la activación de artefactos explosivos improvisados (IEDs, por su sigla en inglés). No sólo en el caso del conflicto colombiano (1) sino alrededor de todo el mundo (2) (3) (4) la activación de IEDs mediante móviles celulares (RCIEDs) ha generado una preocupante problemática, ya que los sistemas de detección e inhibición presentes en el mercado no han generado un ambiente de seguridad en relación a su uso (3) (4) (5) (6). Esto sumado a la amplia cobertura de la redes celulares, hacen de esta tecnología un elemento clave para la activación a distancia de todo tipo de dispositivos improvisados o de control.

Por otro lado, en el mercado existe una amplia gama de dispositivos para el proceso de detección en todas las bandas celulares (7) (8) los cuales, aún en estado de espera, alcanzan a realizar detección del móvil. No obstante, estos dispositivos se caracterizan por su corto alcance y elevados costos para un posible uso en condiciones de conflicto. Por su parte, para el caso de inhibidores de señal las ofertas comerciales son muy variadas (9) (10) (11). Sin embargo, algunas de sus principales especificaciones no son proporcionadas por los fabricantes y, por ende, no permiten dimensionar los márgenes de seguridad en su uso.

Frente a esto surge el interrogante de si es posible detectar o inhibir un emisor celular en determinada región con cierto margen de confianza, utilizando únicamente medidas indirectas de la señal proveniente del móvil en estado de espera (12) (13), sin la necesidad de generar una llamada entrante o un mensaje de texto que finalmente active el sistema. Por ejemplo, observando cambios de potencia en los diferentes enlaces del *uplink* o *downlink* del sistema durante las señales de reporte. Todo ello requiere del conocimiento funcional de los protocolos de comunicación

usados en Colombia y en específico las características geográficas de las zonas de conflicto. Para el caso colombiano, las redes celulares se encuentran principalmente en GSM850 y PCS1900; todas las operadoras ofrecen posibilidades de conexión en GSM, GPRS, HSPA+, HSDPA, UMTS y EDGE. Las frecuencias de operación de las empresas de telefonía celular en Colombia son: Claro en 1900/850 MHz (14), Tigo entre 1900/2100 MHz (15) y Movistar en 1900/850 MHz (16). No obstante, la mayor cobertura del país la posee Claro y en las zonas donde se presentan amenazas con mayor recurrencia los móviles usados sólo soportan, hasta ahora, tecnología 2G y 2.5G.

La tecnología más común en 2G es el protocolo GSM, la cual usa diferentes frecuencias para el establecimiento de la comunicación. El uso de diferentes canales para la transmisión hace bastante difícil detectar toda la señal en el uplink con un analizador de espectro, a menos que se disponga de un ancho de banda mínimo de 80MHz y tiempos de muestreo no inferiores a $2\,\mu s$ (17). Sumado a esto, las señales provenientes de un móvil son de baja potencia (inferiores a -60dBm), por lo cual se hace necesario el uso de procesos de filtrado y amplificadores de muy buena calidad (18) (19) (20). Por otro lado, las redes celulares han evolucionado hacia sistemas cada vez más inmunes a ruidos externos (21) y protocolos de control de potencia cada vez más eficientes (22). Todo lo anterior muestra que el desempeño de los sistemas de detección e inhibición se encuentra estrechamente relacionado con los progresos realizados en los diferentes protocolos de comunicación, lo que hace indispensable el conocimiento funcional de éstos.

En los diseños actuales de redes celulares la potencia de las antenas puede concentrarse, de tal forma que elimine ruidos provenientes por usuarios o agentes externos (tecnología MIMO), lo cual hace que un inhibidor portable (del orden de 25W) con radiación omnidireccional difícilmente logre eliminar las señales de *downlink* a distancias del orden de los cientos de metros. No es de extrañar que por estos motivos se genere gran preocupación para el desarrollo de sistemas de defensa que controlen el uso de la red celular. Aún con el uso de la mejor técnica de inhibición

se cree que es bastante improbable un bloqueo por completo de la señal que pueda detonar un artefacto explosivo (6) (5), lo que hace pensar en soluciones alternativas que generen un uso eficiente de la radiación emitida por el inhibidor. Por ende, si se detecta el móvil y se encuentra la dirección de procedencia de la señal, sería posible mejorar la probabilidad de bloqueo de señal con el uso de potencias direccionales, con lo cual podrían bloquearse zonas de hasta 100 m con el uso de inhibidores portátiles, aumentando el tiempo de uso durante las operaciones.

Los sistemas de detección han mostrado potenciales aplicaciones en lo referente a seguridad (23). Con la proliferación de las redes celulares digitales comenzó también el uso indebido de estos sistemas de comunicación que va desde el control de artefactos explosivos (5) hasta coordinación de operaciones delictivas desde centros de reclusión (24). Algunas de las soluciones a este tipo de problemáticas ha sido el uso de inhibidores, sistemas de seguridad tradicionales y procesos de sensado que permiten detectar la presencia de estos dispositivos en modo activo con bastante precisión, en rangos de algunas decenas de metros (25). Sin embargo, la evolución hacia WCDMA ha mostrado que las comunicaciones son bastante inmunes a diferentes técnicas de inhibición (26). Sólo en los últimos 10 años se han llevado a cabo investigaciones con miras a reducir las interferencias provenientes de inhibidores (27) (28) (29), entre los cuales se sospecha que los de tipo pulso son los más adecuados para evitar comunicaciones que usan WCDMA. Sin embargo, no presentan un sentido muy práctico para uso en anchos de banda tipo 3G. Para este caso, el sensado es aún más crítico ya que requiere mayor sensibilidad. Al incrementarse el ancho de banda, la potencia está mayormente distribuida y por ende la potencia promedio de recepción es inferior.

Una de las opciones más adecuadas para combatir los “saltos en frecuencia” (técnica usada en comunicaciones móviles) es a través de la emisión de una señal de potencia, con el fin de anular la relación señal a ruido tolerable por el protocolo de comunicación (30). Sin embargo, dicha potencia debe ser lo suficientemente alta como para aumentar el ruido sobre las señales de

enlace entre la base y el móvil (6). Dicha técnica es la base de funcionamiento para los inhibidores actuales. Sin embargo, no cuenta con el aval de muchos de sus usuarios, lo cual hace pensar que la concentración de la potencia en una región del espacio pueda ser una solución práctica en relación a portabilidad y consumo de potencia. El uso de una tecnología que integre las técnicas de, detección, dirección de llegada e inhibición concentrada, ha sido propuesto como una solución razonable en términos de rangos de operación y eficiencia en inhibición (28).

El presente trabajo desarrolla una propuesta metodológica para el proceso de detección e inhibición de móviles celulares. Dicha propuesta se encuentra fundamentada en reportes normativos, acercamientos experimentales y teóricos mediante simulaciones. Para obtener las características de las señales procedentes del móvil (proceso de detección y de diseño de dirección de llegada) es fundamental conocer: los estándares desarrollados por el proyecto 3GPP™ (31) para cada uno de los protocolos de comunicación, el canal de comunicación y principalmente las características del hardware usado en el sensado de potencia de la señal electromagnética. Para el caso de inhibición se requiere una cuidadosa lectura de la normatividad y el estudio de las antenas usadas por la estación base durante el proceso de emisión de radiación.

Para el desarrollo de la propuesta metodológica, el siguiente capítulo recoge algunos de los conceptos relacionados con los protocolos de comunicación involucrados, en específico con los protocolos basados en TDMA y WCDMA, los cuales son la base de los sistemas de comunicación GSM y UMTS respectivamente. Posteriormente se retoman algunos conceptos fundamentales de antenas ya que son elementos clave para el proceso de detección y de dirección de llegada. Finalmente, en el siguiente capítulo se recuerdan conceptos relacionados con la teoría de la decisión.

Basados en los conceptos del capítulo II, en el capítulo III se evalúan los protocolos de comunicación a partir de simulaciones desarrolladas en MATLAB®, analizando los niveles de ruido permitidos por el protocolo. Esto permite hallar las características que debe poseer un sis-

tema de inhibición. Con base en estos resultados y teniendo presente las características de las antenas usadas se obtienen los parámetros de radiación mediante el software especializado para dispositivos y sistemas de alta frecuencia CST Microwave Studio®. A partir de dichos resultados se evalúa la posibilidad del diseño de un sistema de detección de la dirección de llegada de una señal emitida por un teléfono celular y se imponen algunos límites de funcionalidad para el proceso de detección.

El capítulo IV presenta el proceso de implementación de un sistema de detección basado en la señal de reporte. Para esto se usa un sistema de filtrado para la franja del *uplink* y el protocolo de adquisición serial mediante Python™ junto con la placa Arduino Mega™. Las señales en frecuencia son tomadas con el analizador de espectro Spectram HF-60105. No obstante, dichas señales son tomadas en modo exploratorio ya que la velocidad de respuesta del analizador no es la adecuada para la totalidad de la señal del *uplink*.

En el capítulo V, para la validación del trabajo desarrollado se usan los resultados de los capítulos III y IV que permiten corroborar que las señales obtenidas mediante el acercamiento experimental son las esperadas por el proceso de actualización del celular móvil y que corresponden a la estructura típica de las ráfagas en GSM y UMTS. Este resultado indica que efectivamente el protocolo de comunicación es una condición limitante para el proceso de detección. De esta forma se enuncian las variables encontradas, las cuales son factores relevantes para el proceso de detección e inhibición. Dichas variables fueron extraídas de diversas fuentes bibliográficas y fueron apoyadas con algunas de las simulaciones desarrolladas en el capítulo III. Finalmente se propone una metodología, la cual usa los métodos de planificación para la construcción de redes, para el desarrollo e implementación de un sistema de detección, inhibición y dirección de llegada que provea un límite no inferior a 150 m.

CAPITULO II

MARCO TEÓRICO

En el presente capítulo se enuncian conceptos asociados a los protocolos de comunicación y procedimientos de medida usados a lo largo del presente trabajo. Algunos detalles se omiten y para ello se presentan opciones bibliográficas donde se explica con mayor claridad y detalle. Se iniciará el capítulo con una breve descripción del proceso de comunicación en redes celulares (2G y 3G para el caso colombiano), particularmente la interfaz de acceso y la capa física de comunicación en los protocolos GSM y WCDMA. Con ello se busca explicar el funcionamiento y algunos parámetros funcionales de los sistemas de emisión y recepción con la influencia del canal de comunicación.

Dentro de la capa física los transceptores son de particular interés para el proceso de detección e inhibición. Para ello se recuerdan algunos conceptos útiles de antenas y su influencia en el proceso final de comunicación. Finalmente, el análisis estadístico del proceso de detección requiere algunos conceptos estadísticos básicos referentes a la teoría de la comunicación y en específico a la detección de señales.

2.1 PROCESO DE COMUNICACIÓN

El proceso de comunicación puede ser visto como la interacción entre tres agentes: el emisor, el receptor y el canal que es el medio que separa ambos usuarios que puede ser desde un cable hasta el espacio vacío (Fig. 2.1). Para el proceso de transmisión y recepción se han desarrollado diferentes "*lenguajes*" que determinan los aspectos de la señal, tipos de codificación, modos de encriptación, modulación, potencia de emisión, sincronización, entre otros factores clave que aseguran la comunicación entre diferentes usuarios. Estas características y factores en conjunto forman el protocolo de comunicación, el cual se encuentra estructurado en diferentes capas o

niveles (modelo OSI (32)). Ya que nuestro interés está centrado en la señal física entre las antenas (detección e inhibición), de todas las capas solo nos interesa la capa 1 del protocolo, denominada la capa física.

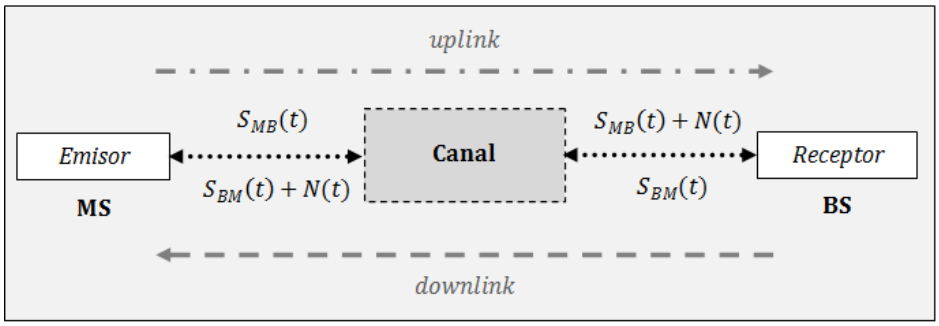


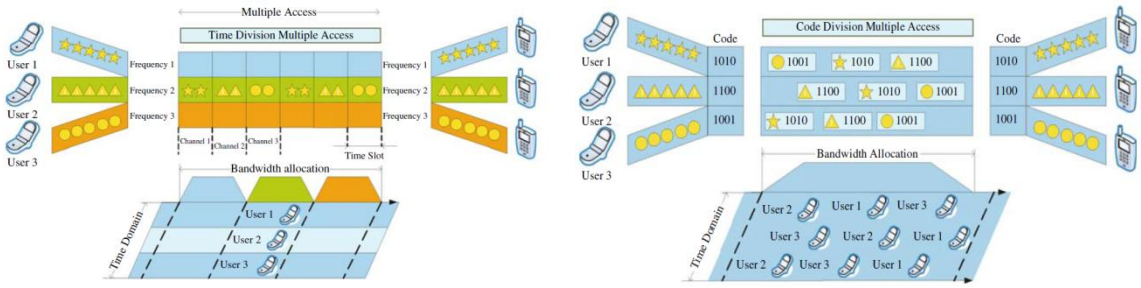
Figura 2.1 Estructura general de un sistema de comunicación

Como muestra la figura 2.1, los dos flujos principales de información en las redes celulares se denominan *uplink* y *downlink*. Adicionalmente se observa que las señales de recepción poseen información recogida en el canal, representado por $N(t)$. Ésta corresponde a fuentes de ruido, sean internas, como las provenientes de la electrónica de detección o externas correspondientes a fenómenos como "fading", interferencia entre canales, ruido en el canal, entre otros factores que finalmente degradan la señal en el receptor. De particular interés para el presente trabajo es determinar si la señal $S_{MB}(t) + N(t)$ realmente proviene de un emisor celular o simplemente corresponde a $N(t)$. En el caso de inhibición, nuestra señal de interés es justamente la opuesta, es decir, la proveniente de la estación base hacia el móvil $S_{BM}(t) + N(t)$.

Cabe sugerir que parte de la robustez de la red celular actual frente a posibles fuentes externas de ruido se debe principalmente a múltiples factores de desarrollo generación tras generación como por ejemplo, procesamientos digitales, algoritmos de corrección, entre otros aspectos (33). Antes de ingresar en la capa física para GSM y WCDMA, se debe mencionar un aspecto clave en el proceso de comunicación celular, referente a la forma cómo los usuarios acceden a la red y cómo dicha red habilita el proceso de comunicación. Para ello existen tres formas principa-

les de acceso múltiple: TDMA, FDMA y CDMA (34). Para el caso de la red celular en Colombia las infraestructuras más usadas son las redes GSM (más particularmente EDGE y GPRS), UMTS/HSDPA (basadas en WCDMA) y para el ingreso de la tecnología 4G en algunas zonas del país se prevé el uso final de redes celulares UMTS 1700 y banda de 2200MHz (35). Sin embargo, cabe aclarar que la infraestructura celular más usada en el ambiente rural colombiano es la asociada a GSM/GPRS y en ocasiones EDGE.

El esquema GSM en el caso Colombiano usa TDMA/FDD como método de acceso. Esto significa que tanto el *uplink* como el *downlink* usan diferentes bandas de frecuencia y los datos son enviados en *slots* de tiempo (Fig. 2a), siempre espaciados 8 slots por paquete y con la posibilidad de usar diferentes frecuencias (36) (34) (37). Por otro lado WCDMA/FDD es la interfaz física para las infraestructuras con UMTS y HSDPA en Colombia, las cuales corresponden a arquitecturas 3G (33). Como puede verse en la figura 2b, la información se envía simultáneamente en todos los canales. Únicamente los usuarios con determinado código pueden recibir determinada información. Ambos tipos de acceso tienen sus ventajas y desventajas (38) (39) (40) (41).



(a) **(b)**

Figura 2.2 Métodos de Acceso a la red (a) TDMA, (b) CDMA (figuras tomadas de **(34)**. p. 44)

2.1.1 Interfaz y capa física para GSM

GSM usa TDMA/FDD como interfaz de acceso. Con base en ello el Instituto Europeo de Normas de Telecomunicaciones ETSI© (42) junto con el proyecto 3GPP™ (31) desarrollaron la normatividad para el protocolo de comunicación. Entre todos los documentos desarrollados, las normas identificadas como TS 45.0xx corresponden particularmente a la capa física del protocolo (43) (44) p. 57. En nuestro caso, aspectos como la codificación del canal (45), la formación de la trama de datos (43), la modulación (46) y la transmisión y recepción (17) son de particular importancia (Fig. 2.3), ya que con base en (47) se pueden obtener los límites permitidos por cada canal, de acuerdo a la normatividad, en términos del BER, FER o BLER, según sea el caso. Además de los niveles de potencia permitidos para el proceso de comunicación.

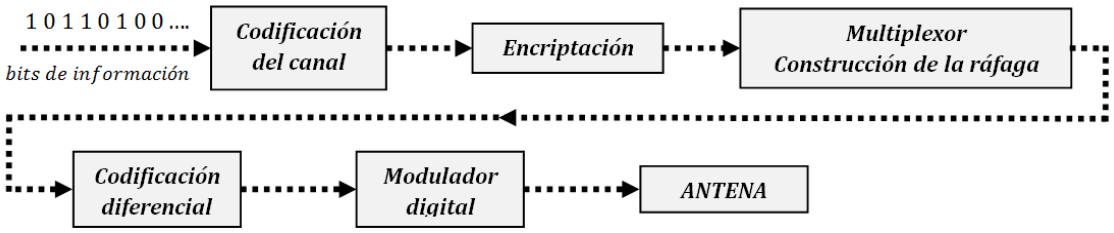


Figura 2.3 Secuencia de envío de información en GSM.

Los canales de comunicación determinan la funcionalidad de cada aspecto del protocolo (43). Éstos físicamente serán las frecuencias de la portadora, los cuales se encuentran espaciados 200kHz; así: GSM850 posee 124 canales, el *uplink* entre 824.2 – 848.8 MHz y una separación de 45MHz para los correspondientes canales del *downlink*; PCS1900 posee 299 canales, el *uplink* entre 1850.2 – 1909.8 MHz y una separación de 80MHz con los correspondientes canales del *downlink* (17).

Como puede verse en la Fig. 2.3, existen varios procedimientos previos a la modulación de la señal (GMSK para GSM o 8PSK para GPRS (36) (48)). Aspectos como la codificación y encriptación hacen del protocolo un sistema robusto frente a fuentes externas de ruido, permitien-

do algoritmos de codificación de errores. Posteriormente, la señal se lleva a la antena y esta será la señal de comunicación entre la estación base y el móvil, es decir la señal en el canal de comunicación. La elección del canal y por consiguiente de la portadora depende del tipo de información a transmitir y en ocasiones de la disponibilidad de uso[1] (43) (37). En general, para todos los canales la información se dispone en ráfagas temporales divididas en 156.25 periodos de símbolo que ocupan 576,9 µs aproximadamente; 8 de dichas ráfagas o *slots* de tiempo conforman la trama principal (≈ 4.62 ms) en TDMA (43) (Fig. 2.4). Dependiendo del tipo de información a transmitir, las ráfagas poseen diferentes características y estructuras (44) de mayor o menor duración (49). Sin embargo, siempre entre cada ráfaga existe un tiempo de guarda (no inferior a 30.46 µs) con el fin de evitar interferencia entre usuarios.

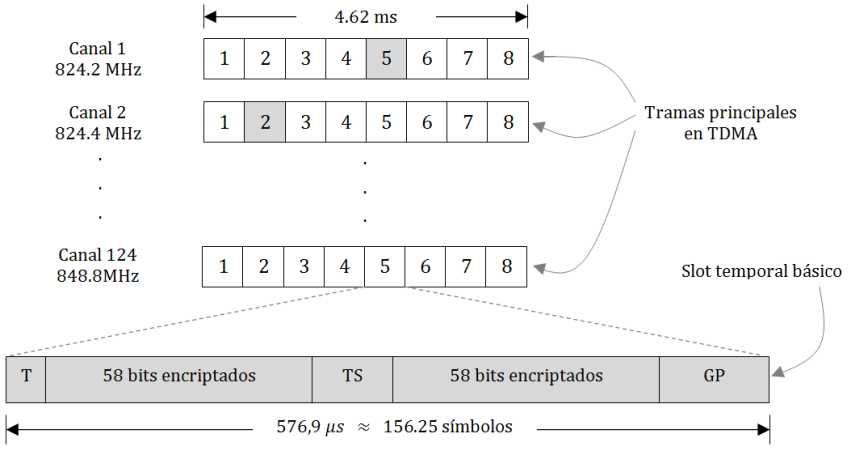
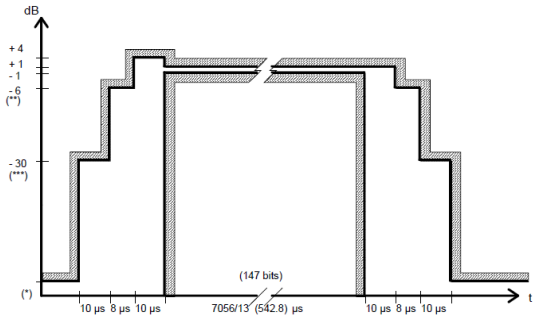


Figura 2.4 Estructura básica en TDMA (para un mayor detalle ver (49) pág. 17)

Finalmente, una de las características que más interesan para los procesos de detección e inhibición es la potencia proveniente tanto del móvil como de la estación base. Para ello (17) contiene las limitaciones básicas del protocolo y las características finales que debe poseer el slot temporal en relación a la potencia de emisión (Fig. 2.5a). Adicionalmente el desempeño del pro-

[1] Finalmente algunos de los canales serán asignados por la estación base

tocolo final dependerá de la calidad del enlace entre la estación base y el móvil. Esto se especifica en los rangos de BER que tolera el sistema (47) (Fig. 2.5b), donde RxEqual representa un parámetro del sistema asociado a la potencia de la señal que recibe el móvil (50).



(a)

RxEQUAL	BER
0	$\text{BER} < 0.2\%$
1	$0.2\% < BER < 0.4\%$
2	$0.4\% < BER < 0.8\%$
3	$0.8\% < BER < 1.6\%$
4	$1.6\% < BER < 3.2\%$
5	$3.2\% < BER < 6.4\%$
6	$6.4\% < BER < 12.8\%$
7	$12.8\% < BER$

(b)

Figura 2.5 Características funcionales y de desempeño para el proceso de comunicación en GSM (a) Potencia transmitida en cada *slot* de tiempo desde el móvil (Tomada del documento 3GPP TS 45.005 **(17)**) (b) Rangos esenciales para el desempeño de la comunicación en el móvil (Tomado del documento 3GPP TS 45.08 **(51)**)

Estos rangos se especifican tanto para el equipo móvil (52) (50) como para la base (47). Cabe resaltar que dichos valores son de vital importancia en lo que resta del presente trabajo ya que representan los límites de trabajo para los procesos de detección e inhibición.

2.1.2 Interfaz y capa física para UMTS

La interfaz de acceso para esta tecnología 3G es WCDMA[2]. Específicamente la más usada es FDD y para el caso colombiano es esta misma. Frente a TDMA permite mayores velocidades de conexión, mejores prestaciones en aspectos funcionales como acceso y sincronización además de poseer algoritmos de control de potencia para la estación base y el móvil (39) (53)

[2] En este caso WCDMA hace referencia al sistema propuesto por ARIB/ETSI

(54). Este protocolo es uno de los estándares (UTRA) del grupo 3GPP™ para sistemas en 3G (31) y dentro de sus normas las asociados a la capa física del protocolo se identifican como TS 25.2xx.

Considerando los casos GSM y UMTS, el presente trabajo únicamente estudia parte de la capa física del protocolo (49) debido a que en ella están contenidas las variables físicas que determinan la funcionalidad del proceso de comunicación. Como muestra la figura 2.6, los aspectos previos al envío de los datos son bastante similares al caso mostrado para GSM (Fig. 2.3). En primera instancia se elige el canal propio para la comunicación (55), posteriormente se codifica (56) y antes de ingresar al proceso de amplificación y envío a la antena se modula (sea QPSK, 16QAM o 64QAM) y expande en frecuencia (57).

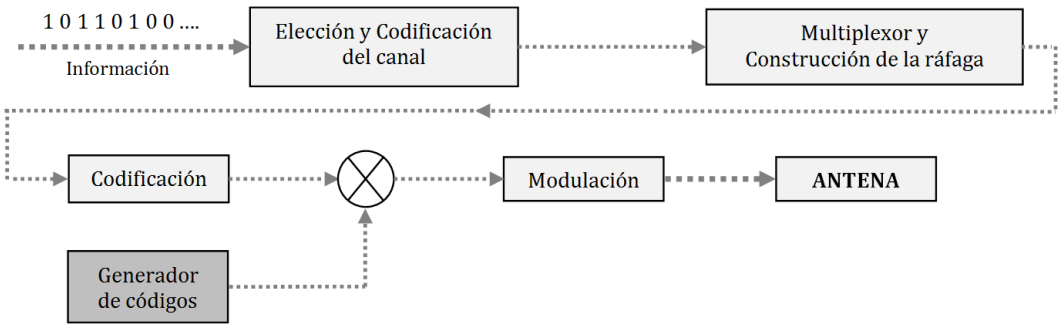


Figura 2.6 Esquema de envío para UMTS en WCDMA

WCDMA hace parte de las técnicas conocidas como de espectro extendido (58). En este caso, el ensanchamiento se obtiene mediante la multiplicación con el generador de códigos (Fig. 2.6). Para el caso específico de UMTS la información queda extendida a lo largo de un canal de 5MHz; la trama principal tiene una duración de 10 ms y está dividida en 15 franjas o slots temporales con 2560 chip/slot (Fig. 2.7); el slot de tiempo es cercano a los 667 μs, en el mismo orden de los 577 μs usados para el caso GSM. La frecuencia mínima corresponde a aquella proveniente del código o chip, es decir, 0.26 µs por periodo de chip, la cual genera casi 4MHz de ensanchamiento. Para reconocer cada uno de los canales, las tramas principales poseen estructuras bien determinadas; al menos uno de los slots posee la información relevante al tipo de canal (control,

datos, aleatorio, entre otros) (55). En el caso de envío de información sea en el *uplink* o *downlink*, se deja un espacio temporal entre los slots para posibles medidas en los canales de frecuencia (56).

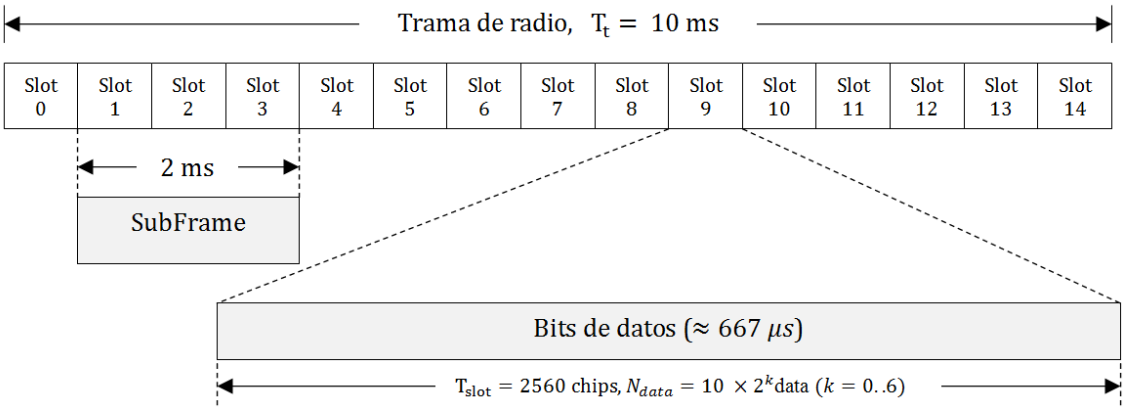


Figura 2.7 Jerarquía temporal para las tramas de datos en UMTS, caso del canal DPDCH (Imagen tomada del documento 3GPP TS 25.211, pág. 10)

Para mantener la compatibilidad, el sistema UMTS permite el uso de bandas similares a las usadas para GSM, aunque con posibilidades de espaciados mayores (5MHz de ancho para cada canal). Así, PCS1900 corresponde a la banda II, entre 1850-1910 MHz para el *uplink* y 1930-1990MHz para el *downlink* y en el caso GSM850 corresponde a la banda XIX con 830-845MHz para el *uplink* y 875-890MHz para el *downlink* (59).

Por último, tanto los niveles de potencia provenientes del emisor celular como la forma de la señal son de particular importancia para el caso de la detección. Para ello (49) describe que la potencia máxima permitida para un móvil no debe superar los 24dBm y la forma final de la señal de potencia es aproximadamente la mostrada en la siguiente figura. Sin embargo, debe recordarse que dicha estructura puede modificarse de acuerdo al tipo de canal en uso.

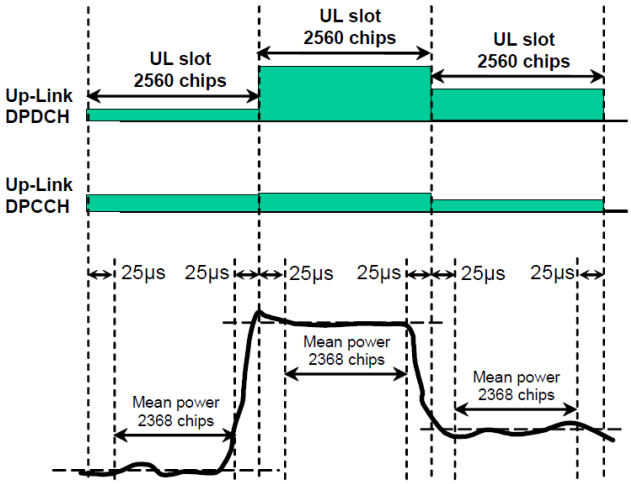


Figura 2.8 Potencia emitida por un móvil celular en UMTS (Imagen tomada del documento 3GPP TS 25.101 pág. 34 (59))

Cabe resaltar que en este caso (Fig. 2.8), el nivel de potencia promedio durante 2368 chips es más o menos constante, pero no es un único valor posible en el envío de datos, lo que no ocurre en GSM donde la potencia siempre será la misma en todas las ráfagas. En este caso código asignado a cada ráfaga no es el mismo y por ende la potencia promedio en cada slot no tiene por qué ser la misma. Por otro lado, la exigencia mayor para UMTS en relación a su desempeño es que en la menor sensibilidad del receptor (-117 dBm), el BER se encuentra entre el 1% e incluso exige 10^{-6} para usos en modulaciones de alta velocidad (49) (60).

2.2- ANTENAS

En este caso el principal interés son características como la directividad, la ganancia, la polarización, los patrones de radiación y los factores de acople de impedancia, ya que estos influyen directamente sobre el desempeño del sistema de comunicación celular. Dentro de la amplia variedad de antenas, las más usadas debido a su alta directividad, ganancia y rangos de frecuencia

para las estaciones base son las tipo sector (61) y para los móviles existe un extenso rango: helicoidales, tipo dipolo, planas invertidas, *microstrip* y tipo serpentín (62) (63) (64) (65).

Otro caso de interés que únicamente será usado para la detección de dirección de llegada (DOA) son los arreglos inteligentes de antenas, que generalmente son usados en sistemas MIMO (33). Dichos sistemas son compatibles con el protocolo UMTS y han mostrado ser una de las soluciones más adecuadas para la implementación de tecnologías 4G. Esto significa que en un futuro cercano la posibilidad de inhibición estará asociada al desempeño final del arreglo de antenas.

Para obtener realmente el desempeño del arreglo es de vital importancia conocer las características físicas de las antenas. Aunque existe una amplia bibliografía alrededor de este tema (65) (66), se recordarán algunos conceptos asociados a las características de las antenas que se retomarán en las próximas secciones del presente trabajo. Algunas características son:

- *Directividad*: Medida en dBi, representa la razón entre la intensidad de radiación de la antena en determinada dirección frente a la intensidad de radiación de una antena isotrópica en esta misma dirección. Para aplicaciones en redes celulares los valores no sobrepasan los 10dBi para la mayoría de los emisores móviles y entre 10dBi y 20dBi para las bases.

- *Ganancia:* Igualmente medida en dBi, se encuentra directamente relacionada con la directividad y representa la eficiencia en la concentración de la radiación en relación a la potencia consumida por la antena. Este valor será menor o igual a la directividad. Puede interpretarse como la directividad, pero tomada sobre toda la potencia disponible para la antena.

- *Área efectiva:* Medida en m^2, representa la disposición de potencia que puede adquirir la antena de la potencia externa incidente. La potencia de salida de la antena receptora sería el producto entre la densidad de flujo S y el área efectiva de la antena.

- *Ancho de banda:* Medida en Hz, determina el rango de frecuencias donde la antena puede usarse eficientemente, es decir, donde las condiciones de reflexión y refracción para las frecuencias son las mejores. Esta condición puede usarse como un posible filtro pasivo de frecuencias.

- *Patrón de radiación:* Es la representación gráfica de la radiación de la antena en cada dirección. Éste es tridimensional, sin embargo dada su potencial simetría se presenta como un corte transversal mostrando un esquema polar en 2D.

- *Parámetros S:* Ya que la antena es un elemento pasivo que posee puertos de entrada y salida, es muy común caracterizarla en términos de sus parámetros de impedancia, admitancia y de transmisión.

En términos de propagación es importante determinar las zonas características donde una antena mantiene un comportamiento más o menos similar y constante en el tiempo. En estos casos suele caracterizarse la antena por un factor geométrico que determina los rangos de distancias (L) donde se sectoriza la antena (Fig. 2.9).

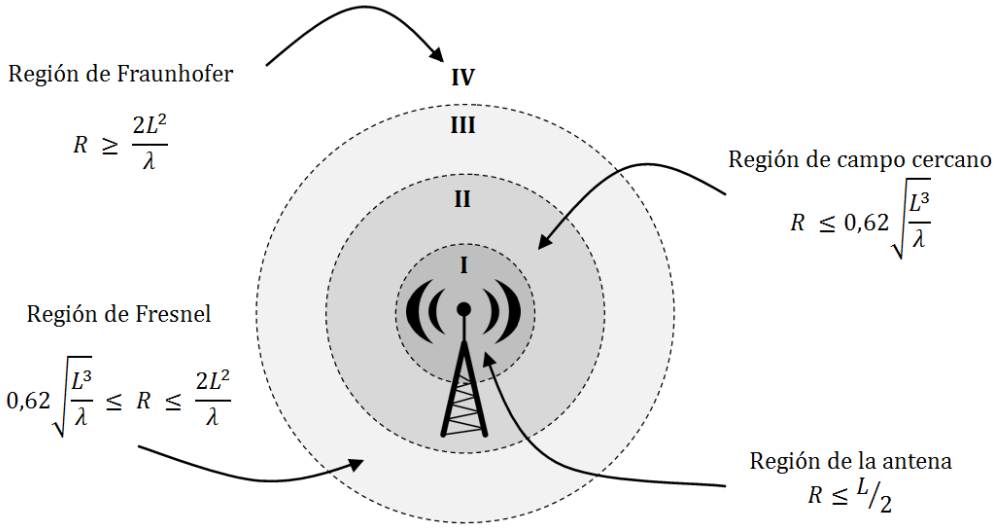


Figura 2.9 Regiones de radiación para una antena

En el presente caso la región sobre la cual las medidas se realizan en la región de Fraunhofer, donde las componentes del campo y por ende la dirección de propagación no cambian con el tiempo.

2.3- ESTADÍSTICA Y TEORÍA DE LA INFORMACIÓN

Debido a la degradación de la señal al viajar del emisor al receptor, la razón señal ruido suele disminuir a medida que la distancia aumenta, degradando la calidad de la señal. Los móviles celulares poseen un detector de *umbral*, el cual finalmente realiza la decisión de la presencia o ausencia de una señal en el canal de comunicación (67), estos elementos usan la teoría de la decisión para continuamente recalibrar el umbral de operación. Esto hace que la teoría de la detección e información sean elementos muy conocidos en la industria de las telecomunicaciones (33).

El teorema de Shannon afirma que la probabilidad de error es inversamente proporcional al nivel SNR de la señal. Por ende, la forma clásica de anular cualquier proceso de comunicación es a partir de la inserción de ruido sobre el receptor (inhibición).

El criterio clásico de detección está asociado a la distribución del ruido presente en el canal y la distribución de la señal en presencia de este mismo ruido. En este sentido, todo el protocolo finalmente se reduce a elegir un *umbral* de trabajo donde el equipo móvil pueda operar o simplemente esperar por un mejor canal de comunicación. Como se observa en la Fig. 2.10, ambas distribuciones comparten una región común. Usualmente se deja el umbral cercano al 10% de probabilidad de ruido

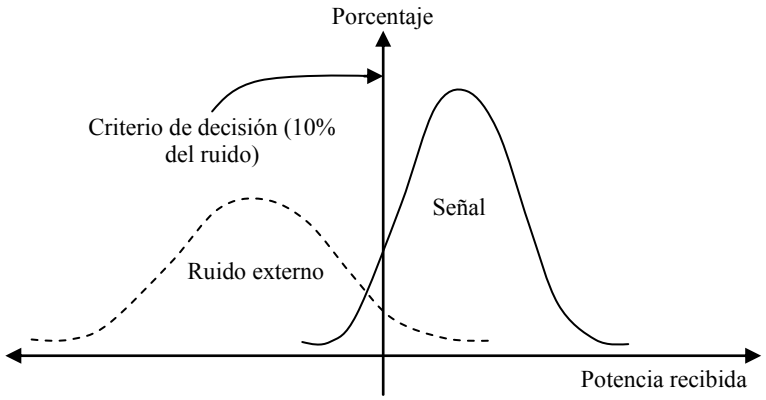


Figura 2.10 Distribuciones clásicas para elaborar un sistema de decisión

Finalmente una de las condiciones teóricas más atractivas es el criterio asociado al teorema de Hartley – Shannon, ya que permite hallar la capacidad máxima del proceso de comunicación frente a las características del canal y la potencia de emisión del emisor. De alguna manera esta condición representa el límite admisible para la existencia de un proceso de inhibición (33).

CAPITULO III

SIMULACIÓN

El presente capítulo desarrolla un acercamiento teórico a partir de la simulación de los protocolos de comunicación en GSM y UMTS. Aunque existe un extensa bibliografía para este tipo de simulaciones (68) (69) (70) (71) y hardware que permite simular el protocolo con conexiones finales (72) (73), el presente trabajo evalúa principalmente las incidencias de las características del canal de comunicación sobre las capacidades de emisión y recepción en el móvil y del canal de comunicación en general, lo cual permite explorar tanto el caso de detección como de inhibición del dispositivo móvil. Los protocolos de comunicación fueron extraídos de los documentos del proyecto 3GPP™, los cuales son de acceso libre. Para las características de emisión y recepción en las antenas celulares se usa CST Microwave Studio® como plataforma de simulación y para los procesos digitales se usa MATLAB®. Como caso específico del proceso de comunicación se usará el proceso de actualización de localización del móvil (12) (13) (74) y como canal el RACH (37) (55). Ambos casos permiten explorar las características de un detector y un inhibidor en el proceso de emisión y recepción de la señal de y hacia el móvil, particularmente señales de control y reporte entre el móvil y la antena base.

3.1 GSM

El protocolo GSM es considerado el caso más exitoso para las redes de telefonía celular 2G (44) (33). El uso de TDMA y GMSK como métodos de acceso y modulación respectivamente, mostraron un balance adecuado entre su eficiencia espectral (cercana a 0.58bps/Hz) y la infraestructura requerida para la capa física de comunicación. La estructura de acceso (TDMA) está compuesta por intervalos temporales (*Frame*) de 4.615 ms de duración, divididos en 8 franjas temporales (*slots*). Sobre cada una de estas franjas es donde se emite la información tanto en el

uplink como en el *downlink*. A continuación se mostrará el proceso desde la digitalización, es decir bit a bit, hasta la recepción en la antena.

3.1.1 Receptor en GSM

En el caso del dispositivo móvil (MS), el proceso previo a la emisión (salida al canal) puede representarse como un proceso de digitalización compuesto por algunos procesos previos a la modulación (Fig. 3.1). Estos procesos intermedios permiten controlar la comunicación frente a posibles fuentes de ruido externos. Dichas codificaciones y modulaciones se especifican en las normas del proyecto 3GPP. Para nuestro caso se simula el proceso de emisión de información en el canal RACH, ya que es el que finalmente usa el MS para iniciar el proceso de reporte o actualización de su localización (13) y finalmente es el que genera el enlace del móvil con la base.

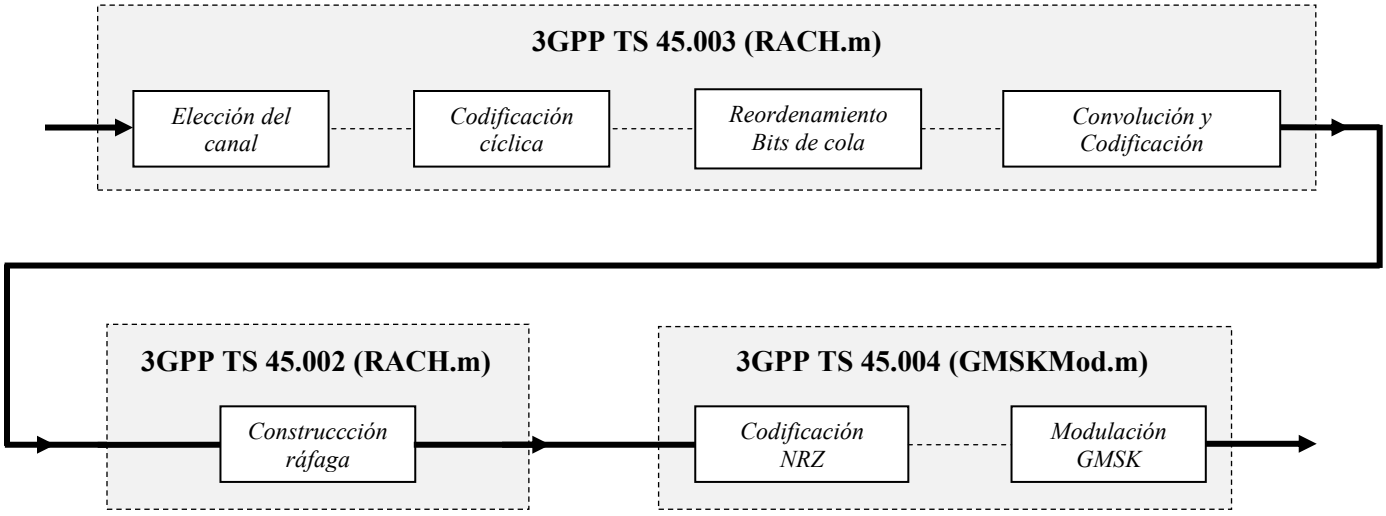


Fig. 3.1 Proceso de emisión para el MS en GSM

Por ende, sin pérdida de generalidad usaremos el proceso de reporte como caso de estudio para el proceso de detección e inhibición. Esto en principio se debe a que la mayoría del tiempo el móvil se encuentra en modo de espera y finalmente la activación del dispositivo móvil podría

activar un dispositivo improvisado. Así una de las formas más adecuadas para la localización del móvil es a partir de la señal de actualización de localización (13). Dicha señal, como se mencionó en el capítulo previo es equivalente al proceso de ingreso a la red y como punto de partida usaremos el modelo mostrado en la figura 3.1 junto con los documentos suministrados en el proyecto 3GPP™ (37) (45) (46) para la capa física en GSM, el uso del canal y el tipo de la trama se especifican en (37).

Se hará usó del canal RACH, con lo cual la estructura de la ráfaga será determinada por este tipo de canal. Podemos adicionalmente usar algunos de los canales lógicos, en particular los de difusión (13) para valorar la efectividad del proceso de inhibición y por tanto las ráfagas normales de comunicación. Sin embargo, la interferencia generada por un inhibidor convencional debe ser la responsable para que la señal de reporte o señales de control procedentes de la base no superen los rangos definidos en la figura 2.5b. Por esta razón en el caso general el uso del RACH puede verse como una buena aproximación tanto para el proceso de detección como de inhibición.

Para obtener la ráfaga de envío completa se implementó un modelo matemático usando MATLAB®, los datos son organizados de acuerdo a (45) (archivo *RACH.m*), antes de ser enviados al canal de comunicación deben ser modulados digitalmente (46) (archivo *GMSKMod.m*). Luego en el canal de comunicación se simulan algunas características del inhibidor y propiedades de atenuación (archivo *Canal.m*), luego debe ser de-modulada la señal (46) y se compara con la ráfaga inicial de emisión. Al final del proceso se obtienen los niveles de FER para el caso específico del canal RACH (archivo *GMSKDemod.m*). En la figura 3.2 se observa el comportamiento del sistema general en relación a su BER (Fig. 3.2a) y para el caso simulado con secuencias de ráfagas de información en el RACH se calculan los niveles de FER que el sistema obtiene bajo diferentes condiciones de ruido (Fig. 3.2b).

Como puede observarse en la gráfica 3.2a el nivel normativo en la mayoría de los protocolos de comunicación es un BER de 0.001, lo cual en el caso general de inhibición requiere como mínimo una señal un poco superior a la de llegada de la estación base. Para el caso específico del canal RACH, el cual bajo condiciones estáticas permite 0.5% en su FER como límite máximo para mantener la comunicación (47), se observa un comportamiento bastante similar. De nuevo la señal de inhibición debe ser del orden de la señal de llegada de la torre.

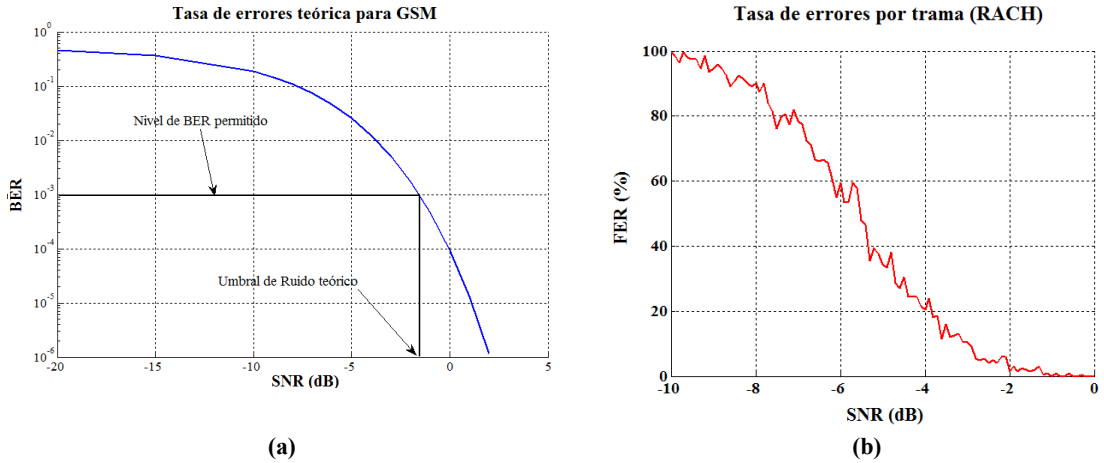


Figura 3.2 BER para GSM en el RACH (a) Caso teórico y (b) Caso simulado con 200 ráfagas de información

En lo referente a 3GPP™ el nivel de ruido que la norma usa como estándar es 9dB para GSM, lo cual está por encima de lo mostrado en la Fig. 3.2, no obstante este límite por encima tiene en cuenta los factores de ruido asociados a la recepción en el móvil y las pérdidas generales antes del proceso de demodulación.

3.2 UMTS

UMTS fue producto del desarrollo en conjunto principalmente entre ETSI© y 3GPP™. Y usa como método de acceso WCDMA y FDD para el caso colombiano. Como se mencionó en la sección 2.1.2, la estructura principal de datos se divide en franjas de 10 ms divididas en 15 slots

de tiempo sobre los cuales se tiene la información codificada. Para el caso del canal RACH se tienen ráfagas iniciales de preámbulo y al menos una franja de radio completa de transmisión (56) (75) junto con sus respectiva señal de control en paralelo.

3.2.1 Receptor en UMTS

Como en el caso evaluado para GSM. Se usará la estructura del canal RACH para el análisis de la información enviada. En este caso la estructura es un poco diferente ya que tenemos procedimientos que aumentan el ancho de banda de la señal emitida (57) (76) (77). Sin embargo, el proceso de actualización mantiene parte de la estructura dada por GSM en relación a algunos de los procesos digitales previos al envío de la información al canal de comunicación. El diagrama de flujo de información para el emisor es el mostrado en la figura 3.3. Para el caso del receptor los procedimientos son justamente los inversos, pero la estructura funcional es bastante similar. En primera instancia se elige el canal propio para la comunicación (55). Posteriormente se codifica y *multiplica* (56) y antes de ingresar al proceso de amplificación y envío a la antena se modula (sea QPSK, 16QAM o 64QAM) y se expande en frecuencia (57).

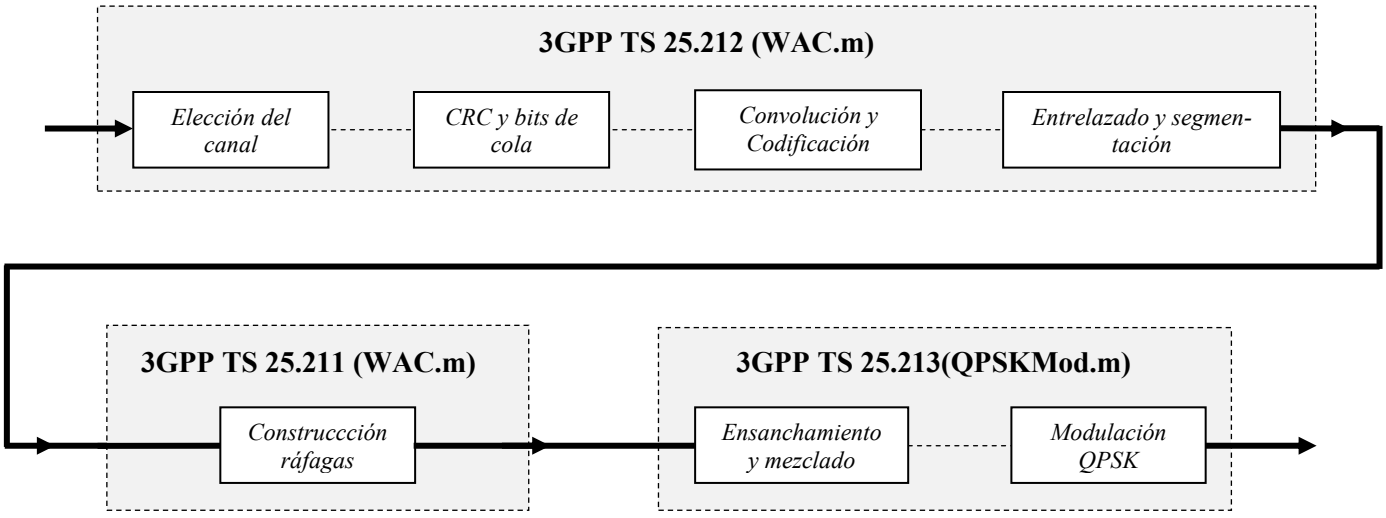


Fig. 3.3 Proceso de emisión para el MS en WCDMA

Se construye la estructura de radio de acuerdo a (55) (56) (75) (archivo *WAC.m*). Posteriormente es modulada (archivo *QPSKMod.m*) y se pasa por un canal de comunicación con fuente de ruido tipo gaussiano (archivo *Canal.m*) sobre el cual se realizan algunos cambios, principalmente el índice de ruido sobre el canal. De esta forma se obtienen los márgenes de amplitud que debe poseer el inhibidor sobre el móvil. Para obtener tanto el BER como el FER del canal RACH se demodula la señal proveniente del canal (archivo *QPSKDemod.m*) y con base en ellos se obtienen las gráficas mostradas para el caso general de transmisión la figura 3.4a y para el caso específico del canal de acceso aleatorio la figura 3.4b. De nuevo como en el caso para GSM los niveles de BER y FER son bastante similares, en este caso la potencia requerida por el inhibidor es 10dB menos que el caso 3.1.1. Sin embargo, aunque para WCDMA sea menor, el ancho de banda es muy superior al caso en GSM. Y por ende la señal de interferencia debe estar en un ancho de banda mayor, lo que requiere igualmente una mayor potencia de emisión.

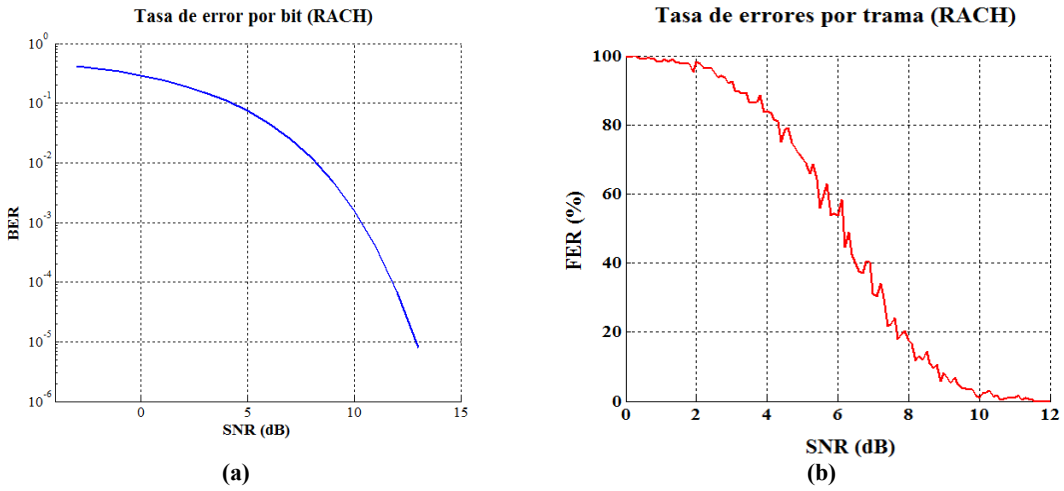
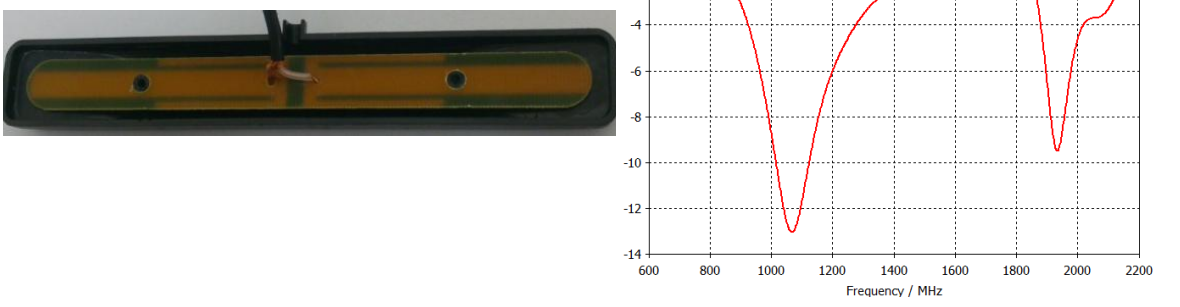


Figura 3.4 BER para WCDMA en el RACH (a) BER en el caso general y (b) FER simulado con 300 ráfagas de información

3.3- ANTENAS

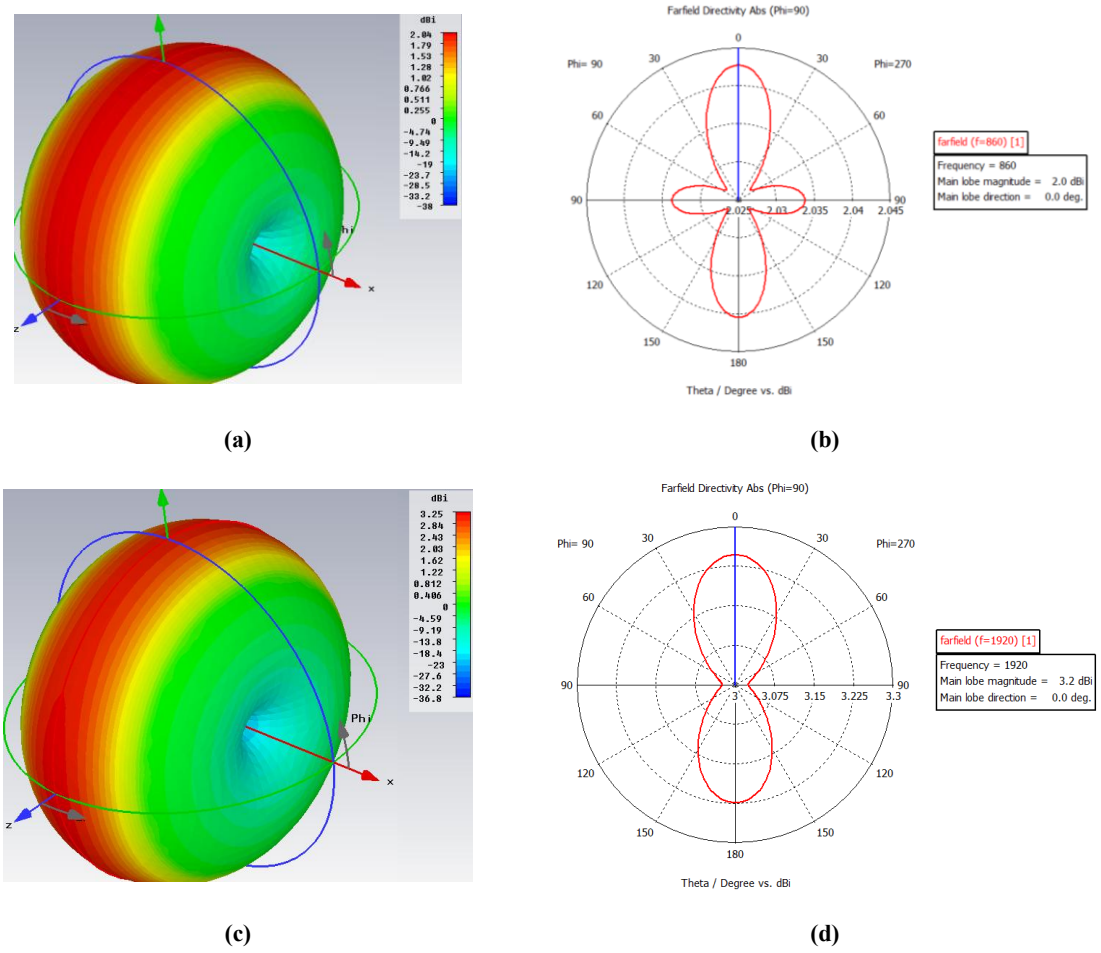
La simulación de antenas es uno de los campos más activos tanto en la industria como en la academia. El diseño actualmente es cada vez más exigente ya que se requieren sistemas con mejores anchos de banda, de menor tamaño y mayor ganancia (65). En el presente caso se elabora el protocolo a partir de un móvil de segunda generación (Nokia 1100b) y una antena tipo dipolo para la recepción de la señal. A partir de sus características físicas se pueden encontrar las características en emisión y recepción en función de su forma mediante CST Microwave Studio®. Cabe recordar que una de las características de dicho software requiere que la región de los puertos de inserción de la señal sea homogéneo en al menos tres líneas de enmallado en la dirección longitudinal. Otra de las características es que permite obtener mejor precisión a medida que el rango de frecuencias es mayor. De hecho se recomiendan anchos de banda entre el 20% y 100% adicionales. Para el caso de la antena usada en el sensado de la señal (78) (Fig. 3.5) se toman las respectivas medidas geométricas y se simula su comportamiento en frecuencia, con particular énfasis sobre variables como la directividad. El índice de confiabilidad de dicha simulación está condicionado por los valores en frecuencia del parámetro S_{11}, lo cual nos asegura de alguna forma que la simulación está acorde con lo ofrecido por el fabricante (Fig. 3.5).



(a) **(b)**

Figura 3.5 Antena de sensado P1-GSM SMA *(a)* Modelo real y *(b)* Modelo simulado

Osérvese de nuevo que la señal está optimizada para las frecuencias en GSM850. No obstante, al no poseer límites apreciables en las demás frecuencias, dicha antena tiene un ancho de banda significativo. Y por ello es necesario el uso de filtros para la detección únicamente en el uplink de la comunicación. El patrón de radiación de esta antena (Fig. 3.6) corresponde efectivamente a un dipolo. Los anchos angulares son bastantes altos y por ende la eficiencia en radiación es cercana a 1. De nuevo en PCS la señal tiene mejor directividad que en GSM.

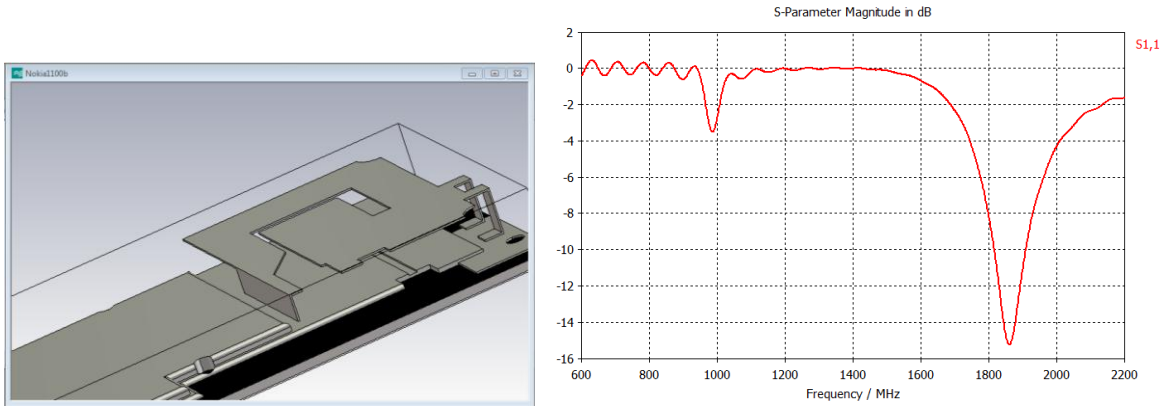


(a) **(b)**

(c) **(d)**

Figura 3.6 Patrones de radiación para la antena usada como sensor del sistema de recepción (a)-(b) Caso GSM850 y (c)-(d) Caso PCS1900

En el caso de la antena del Nokia1100b de igual forma se proceden a medir sus características geométricas y se hacen algunas aproximaciones al tipo de material constitutivo de las partes del móvil. Recuérdese que la implementación de esta simulación es exploratoria ya que no se realiza una retroalimentación experimental que corrobore las gráficas mostradas en las figuras 3.5-3.8. Sin embargo, la simulación sí muestra parte del comportamiento del sistema móvil en relación a los parámetros de radiación, en este caso a la directividad de la antena. El parámetro S_{11} mostrado en la figura 3.7b indica que la antena sólo está bien sintonizada en GSM850. El caso PCS1900 presenta fuertes variaciones en la franja de frecuencias, sin embargo es una zona donde la antena puede resonar bajo ciertas condiciones de los materiales.



(a) **(b)**

Figura 3.7 Antena plana invertida para el Nokia1100b, (a) Modelo de la antena del móvil y (b) Parámetro S para el modelo propuesto

Una de las variables más representativas en los procesos de detección e inhibición es la ganancia de las antenas. En la figura 3.8 se tiene el patrón de radiación para la antena del Nokia1100b, en el que se observa que para el caso GSM850 (Fig. 3.8a-3.8b) la directividad es similar al caso de un elemento dipolar. De hecho, el ancho angular es casi de 72°, debido a que este

tipo de antenas usan el plano de tierra como parte activa de radiación y no como efecto de reflexión. El caso PCS1900 además de poseer un patrón poco uniforme de radiación tiene mayor directividad que en el caso GSM850. Se observa que la señal en PCS1900 produce menos radiación sobre el usuario (caso de una llamada sobre el oído). La forma en que radia el elemento a mayores frecuencias no usa el elemento de tierra como extensión de circuito, emitiendo menos radiación en la dirección del usuario.

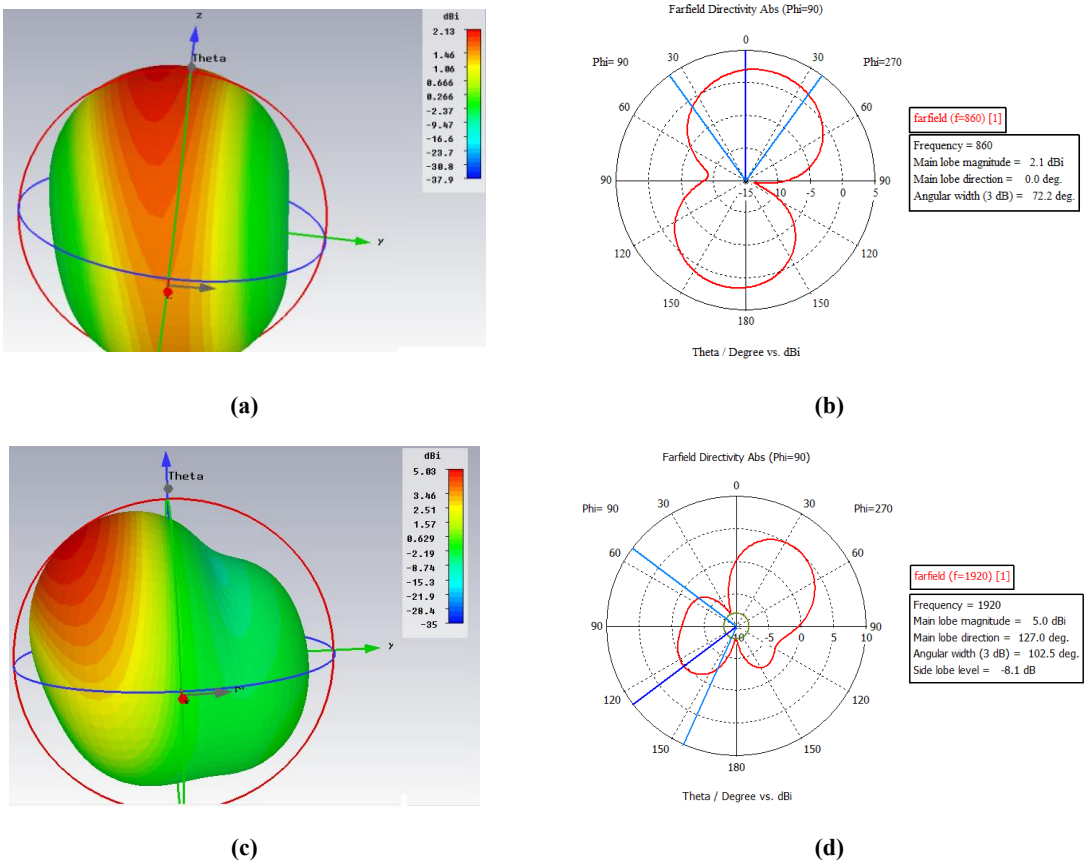


Figura 3.8 Patrones de radiación para la antena del Nokia1100b (a)-(b) Caso GSM850 y (c)-(d) Caso PCS1900

3.4- CANAL DE COMUNICACIÓN

Tanto GSM como UMTS hacen uso del modelo COST-259 dentro de sus especificaciones normativas como modelo de propagación para el canal de comunicación (79). Inicialmente se identificó el COST-231 para redes con GSM1800 y el Okumura-Hata para redes GSM900 (44). Sin embargo 3GPP™ optó por un sistema modular que describe la variedad de condiciones ambientales en función de la distribución del canal y no un extenso número de casos específicos (79). Se sabe que las condiciones de potencia para cada caso presentan algunas diferencias significativas (80). En el caso de áreas abiertas, el modelo de Okumura-Hata se usa para frecuencias inferiores a 1500 MHz y grandes distancias entre el emisor y receptor; el COST 231-Walfish-Ikegami se usa en frecuencias mayores y distancias pequeñas entre la base y el móvil[3]. (81) (82). Para una zona de detección cercana a los 150 m a la redonda, el COST-231 podría ser una elección adecuada para la caracterización de la emisión del móvil en campo cercano frente a las pérdidas por transmisión.

El caso en particular analizado requiere la potencia nominal emitida por un móvil en GSM850 o PCS1900. El proyecto 3GPP limita la potencia de los móviles de acuerdo al tipo de modulación y banda usada (17). En el caso de modulaciones diferentes a GMSK, PCS1900 no debe exceder 2 W (+33dBm) de emisión y GSM850 no debe superar los 6 W (+38 dBm). Para WCDMA la potencia del emisor no debe superar los +24dBm (250 mW). El canal específico analizado es un ambiente rural (RA) en el cual el tamaño de la celda es del orden de 5km (Macrocélula). Sin embargo, para el protocolo se plantea hasta un máximo de 150 m entre el móvil y el sistema de detección. Aunque los modelos enunciados en el párrafo anterior son de amplio uso en la planeación de la infraestructura celular, los resultados mostrados al final del capítulo 5 muestran que una opción bastante ajustable para los datos obtenidos es el uso de un modelo de pérdidas igual al caso del espacio libre. La figura 3.9 muestra el comportamiento de la potencia de

[3] Así como la altura de las antenas y la distancia el emisor

salida de un móvil a diferentes distancias y para la máxima potencia permitida por las especificaciones, el caso WCDMA es el más exigente en relación a la sensibilidad del detector. No obstante, los datos mostrados presentan la potencia que recibiría una antena, cabe recordar que la señal que incide sobre la antena es una señal electromagnética. Y generalmente sólo parte de esta señal puede ser captada la antena (dependiendo del área efectiva de la misma) y ese promedio temporal, llamado el vector de Poynting, es el que finalmente da la potencia promedio de la radiación de llegada.

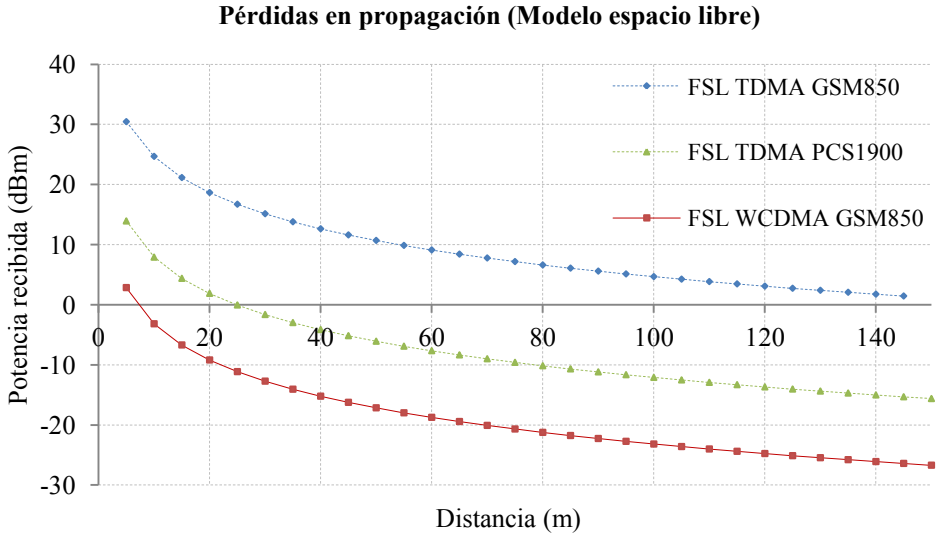


Figura 3.9 Caídas de potencia en función de la distancia de sensado

CAPÍTULO IV

ACERCAMIENTO EXPERIMENTAL

Una de las características generales del envío de información en el canal RACH tanto para GSM como para WCDMA es la no existencia de algoritmo de control para la potencia de la señal. Por ende las ráfagas son enviadas con la mayor potencia disponible de tal manera que puedan ser sensadas en toda la celda (60). Para retroalimentar el proceso de simulación, se implementó un sistema de detección y adquisición basado en la medición de la potencia durante el proceso de ingreso del móvil a la celda. La presente arquitectura experimental sólo usa la potencia de la señal de emisión con el objetivo de detectar el móvil. No obstante, a partir de las simulaciones realizadas y la información del protocolo de comunicación, se tienen algunas propiedades conocidas de las señales para GSM y WCDMA en cuanto a su forma, con lo cual el comportamiento de la potencia en el tiempo es de particular interés para correlacionar estas señales en presencia de bajos niveles de SNR e implementar procesos de filtrado y reconocimiento de múltiples emisores al mismo tiempo.

4.1 SISTEMA IMPLEMENTADO

Una de las razones por las cuales se revisó la normatividad asociada a los protocolos de comunicación fue el hecho de correlacionar dicha información con las señales en el tiempo que deberían provenir del móvil, ya que la estructura de las señales en GSM y UMTS condiciona tanto la velocidad de adquisición como la sensibilidad en el sistema de detección. Como se observa en la figura 4.1, el espectro electromagnético usado para telefonía celular en Colombia tiene dos zonas de operación muy marcadas, GSM850 y PCS1900, cuyas zonas de *downlink* son las más visibles, siendo el caso PCS de mayor amplitud que el caso GSM. Esto se debe a que la mayor atenuación sucede a mayores frecuencias. No obstante cabe recordar que la zona del *uplink* es

la de interés para el caso de detección, por ende un proceso de filtrado es necesario para ambos casos ya que normalmente la señal entre la estación base y el móvil no es constante en el tiempo.

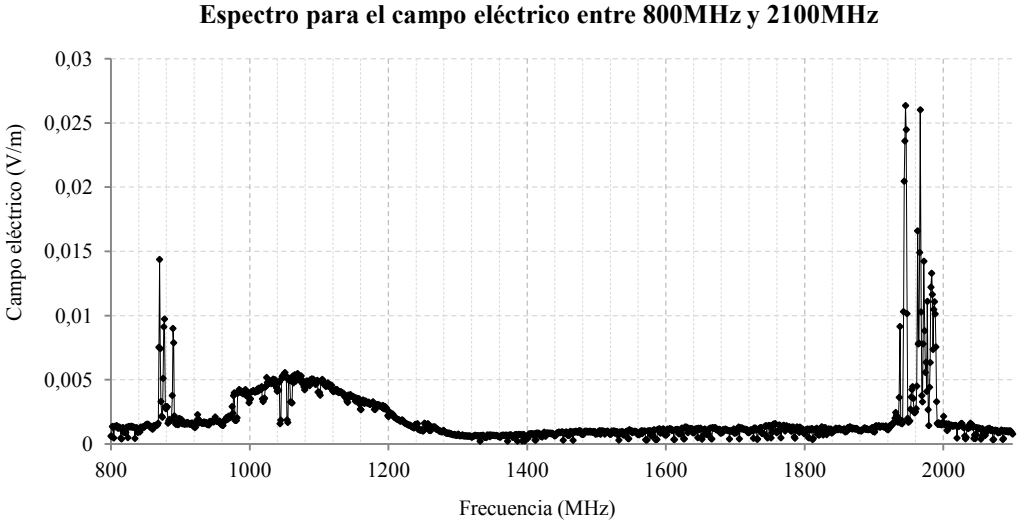


Figura 4.3 Espectro para el campo eléctrico en una red urbana (tomado con el *Spectran HF-60105*)

Para el sistema experimental se usó una antena planar tipo dipolo, con polarización vertical y sensible a las 4 bandas principales de GSM/WCDMA (*uplink* y *downink*). Aunque los datos técnicos de esta antena no son muy precisos para un análisis contundente del sistema (78), la simulación desarrollada en la sección 3.3 permite obtener una buena aproximación de algunas características de esta antenna[4]. Como caso particular de un emisor móvil se usó un Nokia1100B, cuyo soporte únicamente valida GSM y cuya antena en forma de F invertida (PIFA) permite obtener un patrón de radiación, a su vez depende de las frecuencias de operación (sec. 3.3). De nuevo, como en el caso del detector, estos datos son tomados en cuenta más en relación a su forma que a su valor. Para la medición específica del espectro de las señales provenientes del emisor celular se usó el analizador de espectro SPECTRAN HF-60105 (83). Cabe recordar que

[4] Dicha simulación puede considerarse tan solo un acercamiento, ya que las propiedades de los materiales no son conocidos.

dicho medidor tiene velocidades de muestreo inferiores a las requeridas para GSM y WCDMA, por ende los valores obtenidos no son exactamente los reales, pero se obtiene un promedio del espectro en las frecuencias celulares de estudio. Ya que las señales del downlink son de gran amplitud para ambas bandas (Fig. 2), en el caso de detección es indispensable el uso de un filtrado, de tal forma que sólo pase la señal procedente del móvil hacia la estación base.

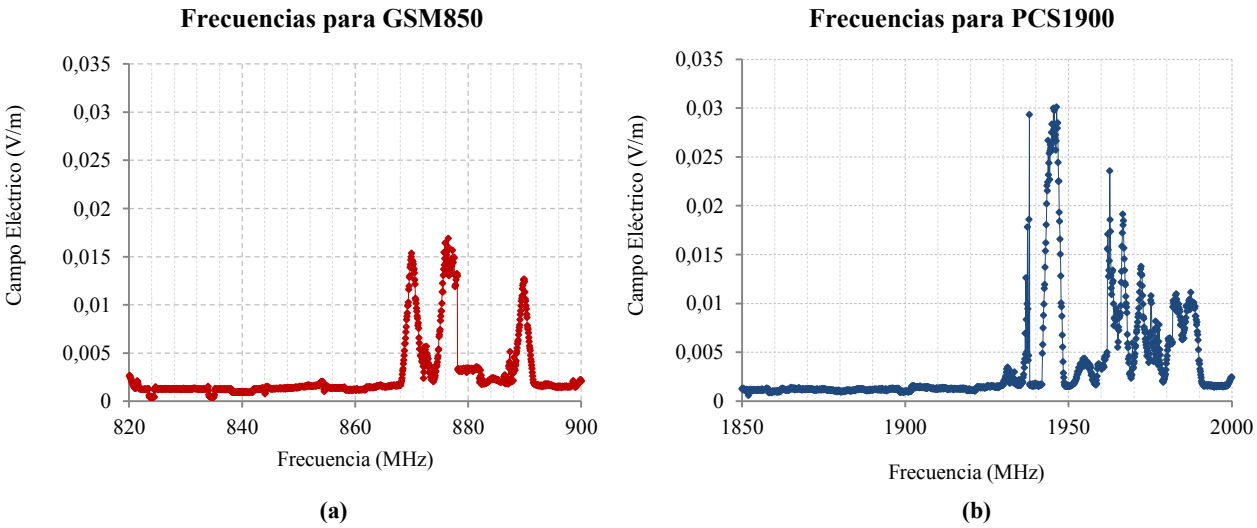
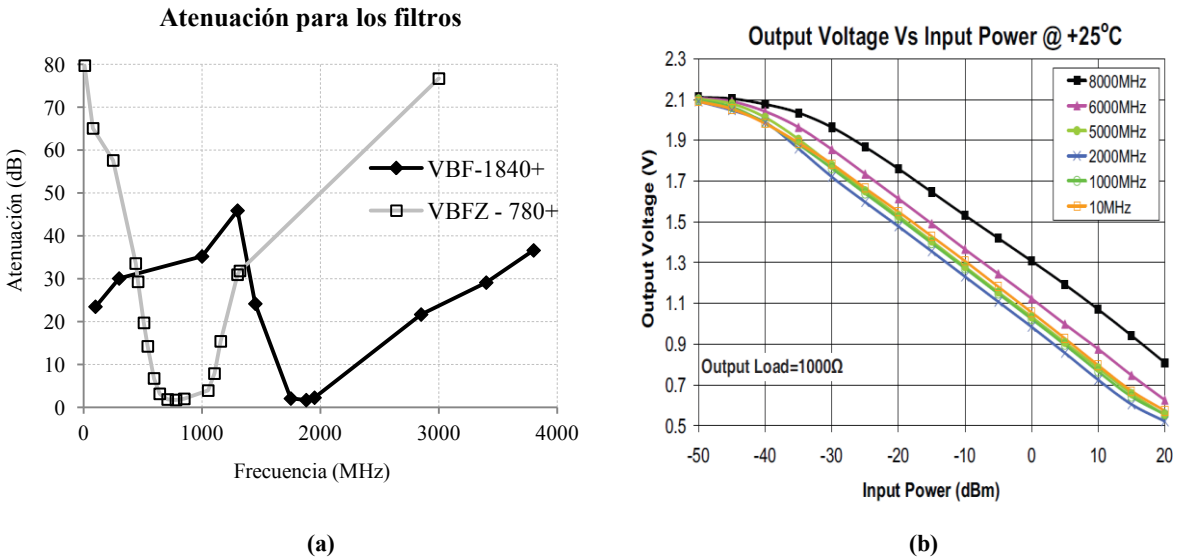


Figura 4.4 Campo eléctrico en las principales bandas celulares *(a)* GSM850 y *(b)* PCS1900, (tomados con el *Spectran HF-60105*)

Para la obtención de la señal de potencia únicamente en las franjas del *uplink* se tienen dos filtros pasabanda tanto en GSM850 (84) como en PCS1900 (85) (Fig. 4.3a) y un detector de potencia logarítmico con un máximo de sensibilidad en -40dBm (86) (Fig. 4.3b). El proceso de adquisición de la señal de salida del medidor de potencia usa la interfaz de comunicación serial en Python 2.7.3 y como hardware de adquisición un microcontrolador Arduino Mega 2560 (87). A partir de su velocidad de procesamiento y su conversor ADC de 10 bits se pueden obtener cambios de hasta 3mV en tiempos de hasta 26µs. Sin embargo, el detector de potencia posee una figura de ruido de 10mVpp lo cual implica que el uso de un conversor con mejor resolución no es

una elección aplicable para extender el uso del sistema a mayores distancias, en cuyo caso una etapa previa de amplificación o un medidor de potencia con mayor sensibilidad podría alcanzar mayores distancias de sensado.



(a) **(b)**

Figura 4.3 Datos técnicos para los filtros y el medidor de potencia (a) filtros de las bandas GSM850 y PCS1900 en el uplink y (b) potencia de recepción del medidor de potencia (ZX47-40+)

El arreglo final usa los elementos específicos de la tabla 4.1. En principio, para emular un sistema de comunicación celular la sensibilidad debe ser del orden de -110dBm, lo cual obliga al sistema el uso de un amplificador de bajo nivel de ruido. Sin embargo para un primer caso exploratorio y como propuesta de un protocolo de detección e inhibición no se usará este elemento. Además el alto costo de dichos elementos triplicaría el precio total del sistema de prueba (88). Por esta razón se omite para este caso, lo cual disminuye la distancia de sensado, pero permite proponer una posible propuesta metodológica para un protocolo de sensado con mayor alcance en distancia y velocidad de procesamiento.

Sistema	Elemento comercial	Figura	Precio
Antena	P1-GSM SMA/MCX R/A		$18 US
Filtro pasa banda	VBF - 1840+ VBFZ - 780+		$34.95 US $39.95 US
Medidor de potencia	ZX47-40+		$89.95 US
ADC	Arduino Mega		$ 60 US
Conectores	SMA, USB, entre otros		$ 30 US
		Total	**$ 272,85**

Tabla 4.1 Elementos usados para el sistema de detección

4.2 DOMINIO DE LA FRECUENCIA

Antes de usar el esquema experimental descrito en la sección anterior, se deberá medir la señal de reporte proveniente del móvil tanto para el caso 2G como 3G. De ese modo confirmamos el uso de las bandas celulares en los operadores y por ende la potencia que deberíamos observar en la salida del medidor de potencia. Aunque el analizador de espectro (83) no posee el muestreo adecuado para todo el rango de frecuencias en el *uplink*, sí permite identificar el uso de ciertas frecuencias durante el envío de la señal de reporte del móvil. Tanto para el caso GSM850 como PCS1900 se obtiene el comportamiento en la frecuencia de la señal justo cuando el móvil ingresa a la red celular (Fig. 4.4). Aunque es posible que algunas frecuencias no sean detectadas durante el barrido del analizador, se observa claramente la presencia de una señal en la banda del *uplink*.

Como caso particular, se tienen potencias mayores y tiempos menores de uso en el espectro para la señal en PCS1900 que para GSM850, lo cual hace pensar que en la práctica la señal en 850MHz requiere mayor procesamiento y sensibilidad que la señal proveniente de emisores en las redes 1900MHz.

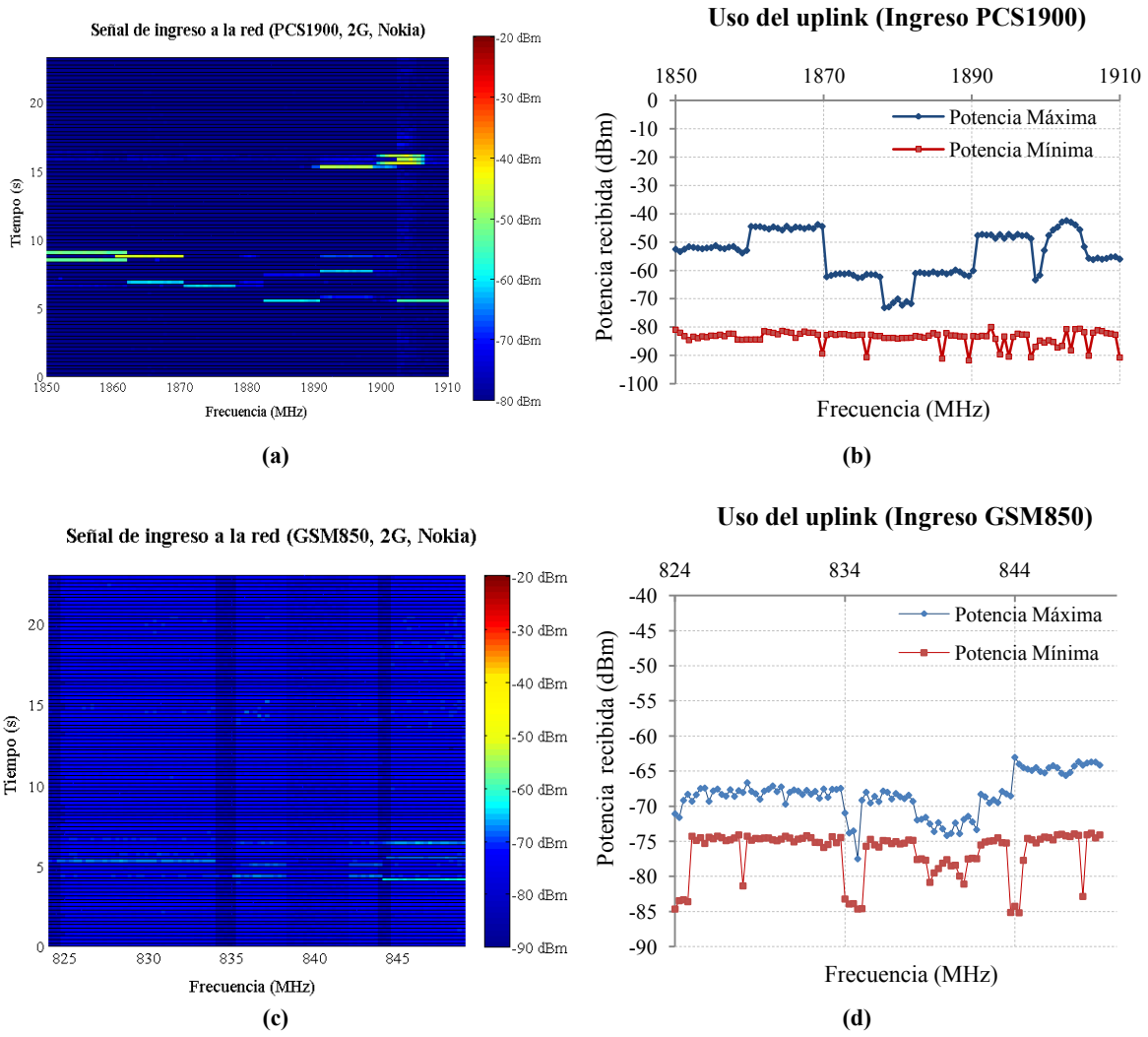


Figura 4.4 Uso de la banda PCS1900 y GSM850 en el uplink durante una señal de reporte en 2G **(a)** Espectro en el tiempo para PCS1900, **(b)** Niveles de potencia máxima y mínima en PCS1900, **(c)** Espectro en el tiempo para GSM850, **(d)** Niveles de potencia máxima y mínima en GSM850

El caso 3G (Fig. 4.5) es bastante distintivo y el Nokia1100b no permite usar dicha tecnología. Por esta razón se usaron dos tipos de celulares que soportan ambas tecnologías; para GSM850 se usó un Samsung SIII y para el caso PCS1900 un Xperia P. Aunque ambos celulares no tienen las mismas características en relación a su hardware, la señal en la frecuencia para am-

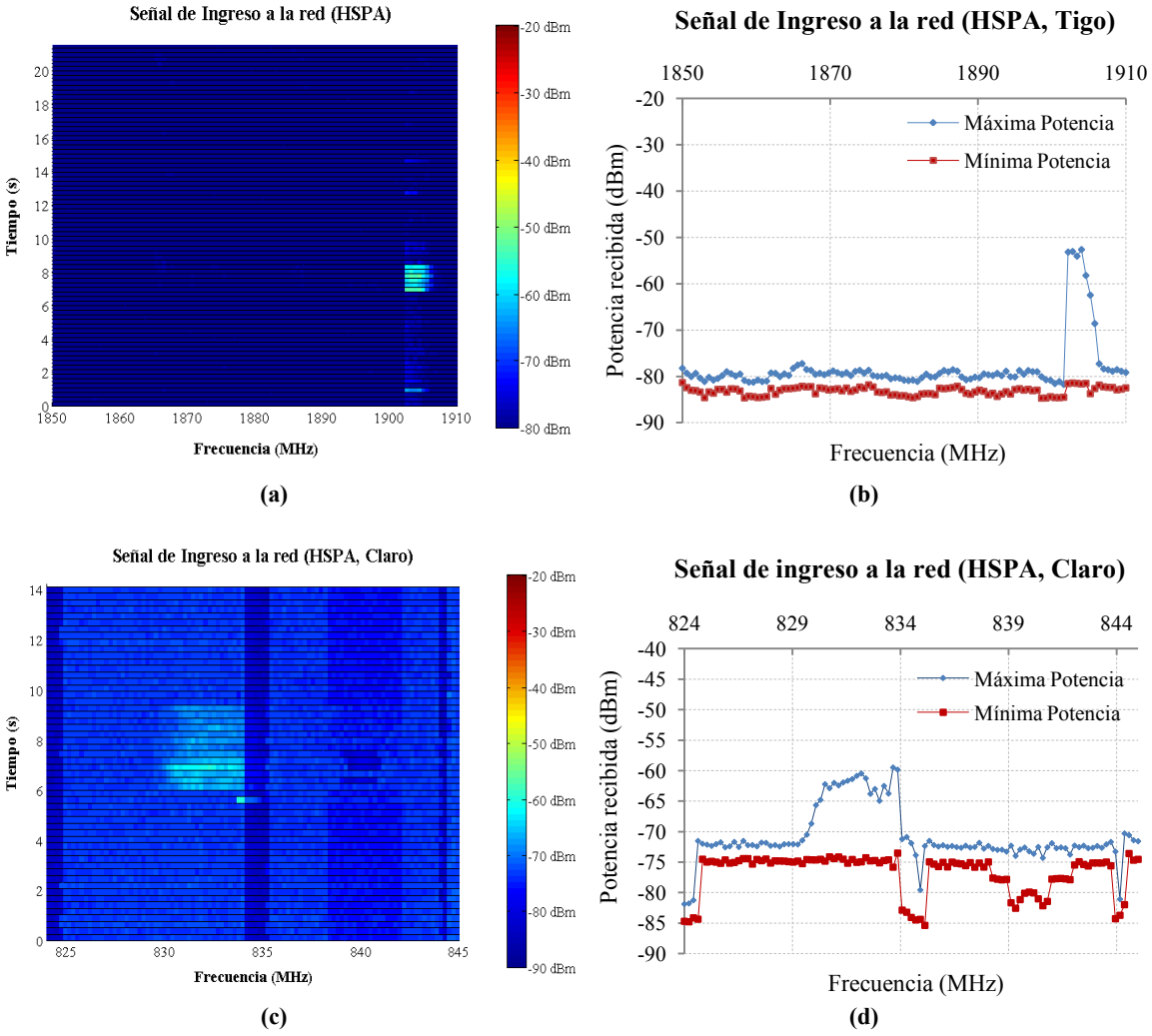


Figura 4.5 Uso de HSPA en el uplink durante una señal de reporte **(a)** Espectro en el tiempo para Tigo, **(b)** Niveles de potencia máxima y mínima en Tigo, **(c)** Espectro en el tiempo para Claro y **(d)** Niveles de potencia máxima y mínima en Claro

bos casos debe poseer similitudes en cuanto a su forma. Como en el caso 2G, se observa un mayor nivel de potencia en la señal de Tigo y usa una única portadora para dicha señal (alrededor de 5 MHz de ancho de banda que corresponde a WCDMA). Claro, aunque usa menos potencia, tiene mayor duración en el tiempo y usa al menos 3 portadoras en tecnología WCDMA. Por ende, en lo referente a la detección de las señales en 3G, se observa en particular que ahora el sistema implementado puede estar limitado en relación a la potencia medida. Aunque la señal de reporte se mantiene como una posible opción, el problema limitante es la sensibilidad, pues ahora la señal está mayormente distribuida en la frecuencia y por ende la potencia promedio disminuye. Así, la detección de móviles está fuertemente condicionada por el tipo de tecnología. Los alcances para 2G y 3G son distintos ya que las tecnologías de acceso son completamente diferentes.

4.3 DOMINIO DEL TIEMPO

Finalmente, los datos mostrados en la sección 4.2 muestran el uso de las bandas en el uplink tanto para las tecnologías 2G como 3G lo cual garantiza el uso del proceso de filtrado. Ahora bien, la medida en el dominio del tiempo de la potencia emitida por el móvil debe ser coherente con la respuesta del medidor de potencia. Para ello se usa un osciloscopio digital *Tektronix MSO 4054* y se proceden a medir las señales de salida del medidor de potencia (86) durante la emisión de la señal de reporte. Las medidas para este caso son tomadas a distancias del orden de centímetros sobre la antena receptora, de tal forma que las señales externas no generen ruidos comparables con la señal proveniente del móvil.

La señal proveniente del móvil es la mostrada en la figura 4.6 (a). Obsérvese que los niveles de potencia son cercanos a los mW para las primeras ráfagas de información, lo cual para el caso de la detección es una ventaja. Adicionalmente se observa un tren de pulsos que alcanza los 4s de duración. Por ende, en términos de potencia y duración, las señales de reporte poseen hue-

llas que pueden seguirse, de tal forma que en presencia de ruido la señal puede compararse tanto en el dominio del tiempo como en el de la frecuencia.

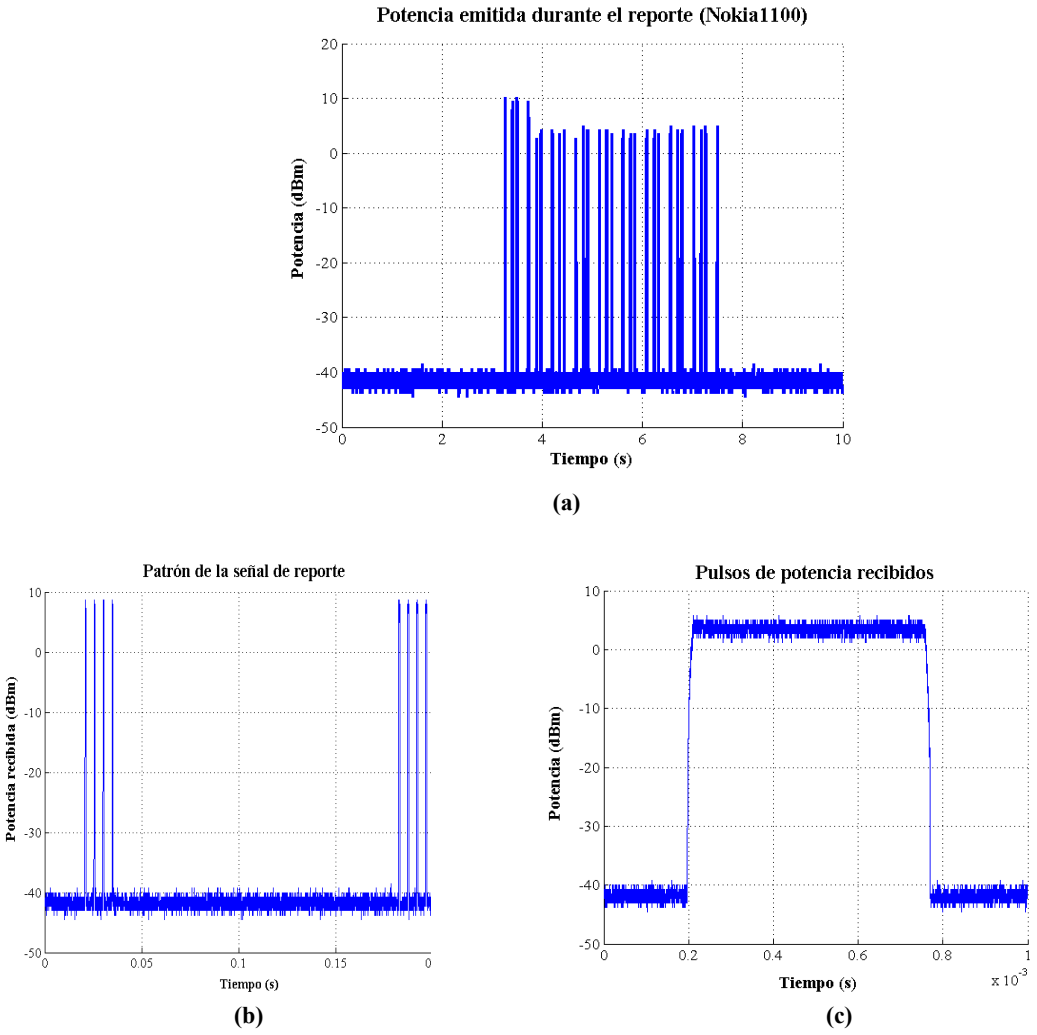


Figura 4.6 Potencia emitida durante la señal de reporte (Nokia 1100) (a) Señal completa, (b) Secuencia de pulsos, (c) Pulso aislado dentro de la señal de reporte

De particular interés son las señales aisladas en la parte (a) de la figura 4.6. Los casos 4.6b y 4.6c muestran cierto comportamiento en el tiempo de la señal de potencia. Dicho comportamiento puede estar asociado a algunas frecuencias particulares y será analizado en la siguiente

sección. La figura 4.6c muestra un pulso de la secuencia 4.6b; obsérvese que la duración de dicho pulso es cercana a los 570 μs, lo que concuerda precisamente con la duración esperada para los pulsos considerados en la sección 2.1.1.

CAPÍTULO V

RESULTADOS Y VALIDACIÓN

Para validar los resultados obtenidos en el acercamiento experimental del capítulo anterior, se evaluaron las medidas de potencia tomadas con el sistema implementado. Las señales en el tiempo mostradas en el capítulo anterior efectivamente son señales provenientes de un emisor celular en tecnología GSM; las medidas de distancia muestran que el modelo de propagación tipo espacio libre (FS) es en este caso el más aproximado para un ambiente rural con cobertura en ambas bandas celulares.

Finalmente, una de las características a buscar en los procesos de emisión de potencia es la estructura de la trama de datos (37). Aunque cada móvil realice la actualización de forma diferente, la forma de las ráfagas de información siempre será la misma. Para GSM existen 5 tipos de ráfagas (44); en RACH las ráfagas de acceso son las más comunes. Sin embargo, el uso de las ráfagas comunes debe ser igualmente tomado en cuenta.

5.1 RESULTADOS

Dada la estructura en el tiempo mostrada por la figura 4.6c, la exigencia en el muestreo sobre el Arduino debe ser de un tiempo inferior a los $250\mu s$ de tal forma que se cumpla el criterio de Nyquist. Luego se programa el micro controlador para el envío de una muestra cada $200\ \mu s$ a través de Python™ hacia el computador. Para el análisis del alcance de la medida usada con el sistema descrito en el capítulo anterior se debe tener presente que el ruido de fondo es un agente importante para la decisión de la presencia o ausencia de la señal. Para ello se tomaron los datos para un ambiente rural (Fig. 5.1) con ausencia de posibles móviles celulares a una distancia tolerable de medición.

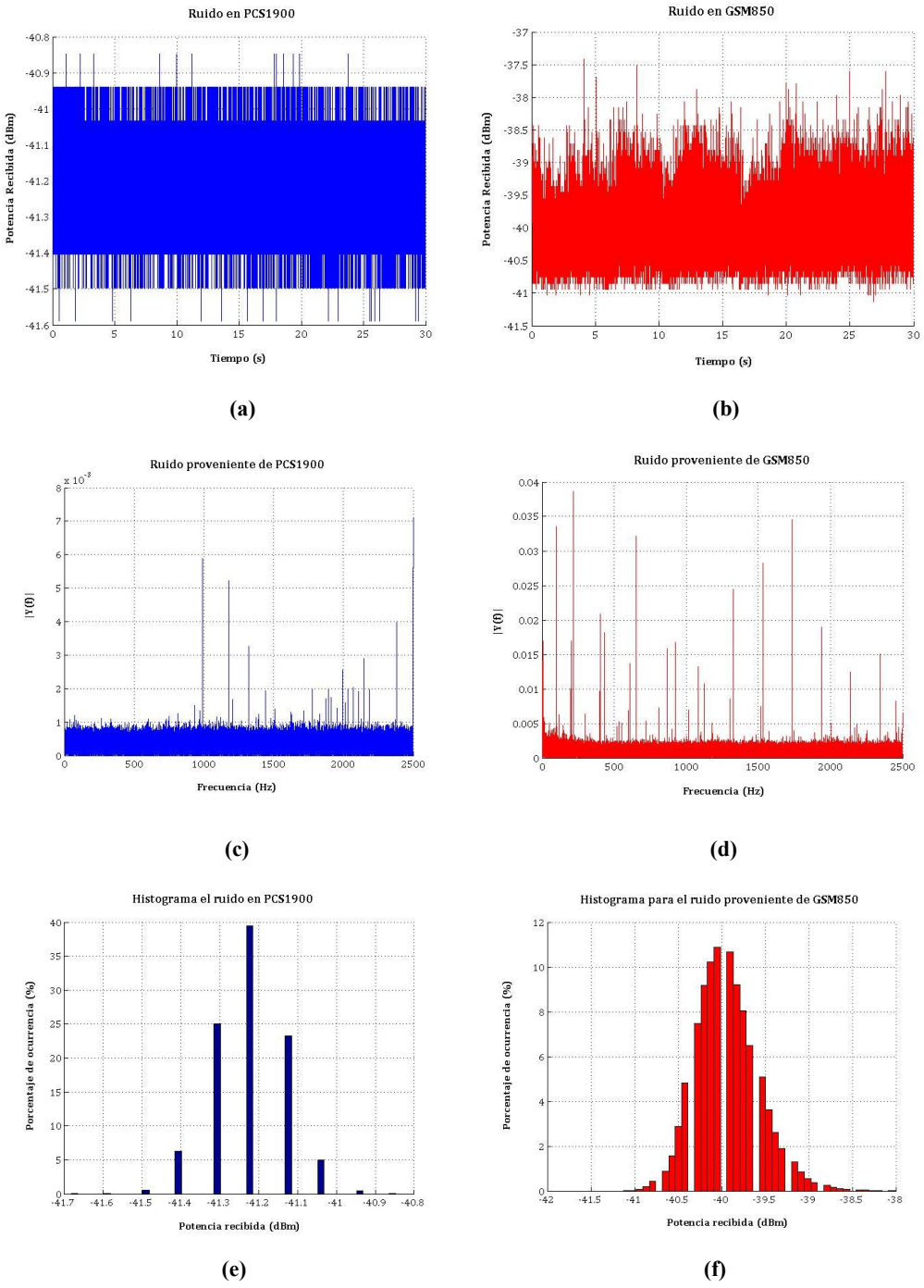


Figura 5.1 Ruido de fondo en GSM850 y PCS1900 en ambientes rurales, *(a)* y *(b)* PCS1900 y GSM850 en el dominio del tiempo, *(c)-(d)* PCS1900 y GSM850 en el dominio de la frecuencia y *(e)-(f)* Perfil porcentual para PCS1900 y GSM850 respectivamente

Se observa con claridad que el perfil de ruido de fondo es un perfil gaussiano (Fig. 5.2e y 5.2f). Sin embargo, el caso GSM850 muestra una distribución para el ruido con una varianza mayor que el caso PCS1900 y un conjunto de frecuencias bastante diferente al caso PCS1900. Dichos aportes pueden deberse a la cercanía de la torre de Claro frente a la distancia de la torre de Tigo para el canal usado experimentalmente. La forma de los histogramas fue evaluada con MATLAB® y en ambos casos se obtiene un perfil tipo gaussiano. Cabe resaltar que dichos perfiles poseen factores no lineales, asociados quizás a la forma mostrada en Fig. 4.3b.

Para el estudio de la señal de reporte se evaluaron dos elementos móviles, un Nokia1100b y un LGA255 (los cuales fueron diseñados para uso exclusivo en tecnologías 2G). El escenario elegido para las pruebas fue una macro celda en ambiente rural donde se trató de evitar al máximo la presencia de celulares y agentes externos que pudieran interferir con la señal de reporte del móvil en específico. Según lo encontrado en la sección 3.3, el patrón de radiación determina una región de mayor intensidad. Por ende, se fija la antena receptora a una altura de $2\ \mathrm{m}$ y para la emisión de la señal de reporte se cambian las distancias del móvil a la antena de recepción, siempre manteniendo la misma dirección de emisión del móvil hacia el receptor. Se genera la señal de salida de la red (apagando el móvil) y luego se ingresa a la red (encendiendo el móvil) y se toman los datos mediante el sistema de adquisición descrito en el capítulo anterior. La figura 5.2 presenta los resultados obtenidos a una distancia de $5\ \mathrm{m}$ para las dos operadores evaluadas, esta vez el caso de Tigo presenta menor potencia de emisión que el caso de la señal de Claro. Sin embargo, para ambos casos se observa un comportamiento similar en el tiempo para la señal de reporte. De nuevo, la componente de ruido proveniente de la red de Claro es bastante superior a la que genera la red de Tigo por casi 2dBm de amplitud, lo cual concuerda con los resultados obtenidos para las señales de ruido mostradas en la figura 5.1. Un caso bastante interesante del comportamiento de la señal de potencia en 2G es que las franjas principales en TDMA tienen una duración de alrededor de $4.615\ \mathrm{ms}$, lo cual concuerda con los espectros mostrados en las figuras 5.2c y 5.2d,

la separación entre los picos de frecuencia de mayor amplitud es alrededor de los 210-220Hz, lo cual se esperaba ya que los pulsos no son señales continuas en el tiempo, por ende el espectro en frecuencia mostrará tanto múltiplos como submúltiplos de dicha cantidad.

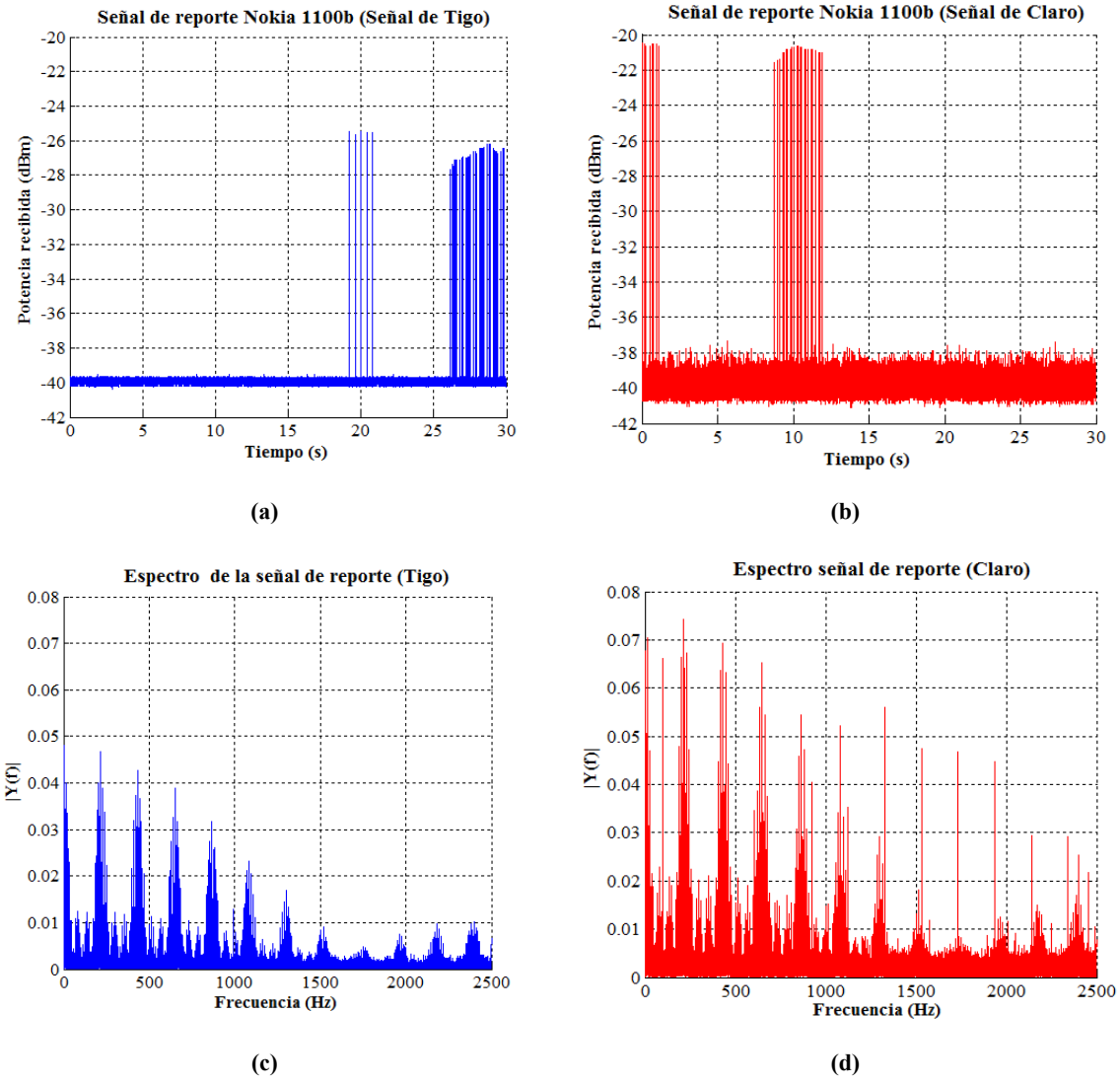


Figura 5.2 Señales salida e ingreso para el Nokia 1100b, a la misma distancia pero para diferentes operadoras (a) Señal de Tigo en el tiempo, (b) Señal de Claro en el tiempo, (c) Señal de Tigo en la frecuencia y (d) Señal de Claro en la frecuencia

La anterior gráfica muestra que efectivamente la señal de reporte está asociada al tipo de tecnología sobre la cual el móvil se encuentra sin importar el tipo de operadora. La señal de potencia proveniente del móvil se caracteriza por el comportamiento mostrado en la figura 5.2 tanto en frecuencia como en tiempo. Antes de relacionar las pérdidas en distancia para cada caso, la figura 5.3 presenta la señal de reporte para el caso del móvil LGA255 tanto en el tiempo como en la frecuencia. Obsérvese de nuevo el comportamiento similar al caso del Nokia1100b; la componente del ruido en GSM850 es mayor que en el caso visto para PCS1900; las componentes en frecuencia concuerdan con los tiempos de duración en TDMA y la arquitectura del proceso de actualización es bastante similar en los tres casos. Esto permite generalizar el protocolo de detección la tecnología asociada a la comunicación (2G y 3G) y las características del móvil determinan finalmente la posibilidad de detección del mismo.

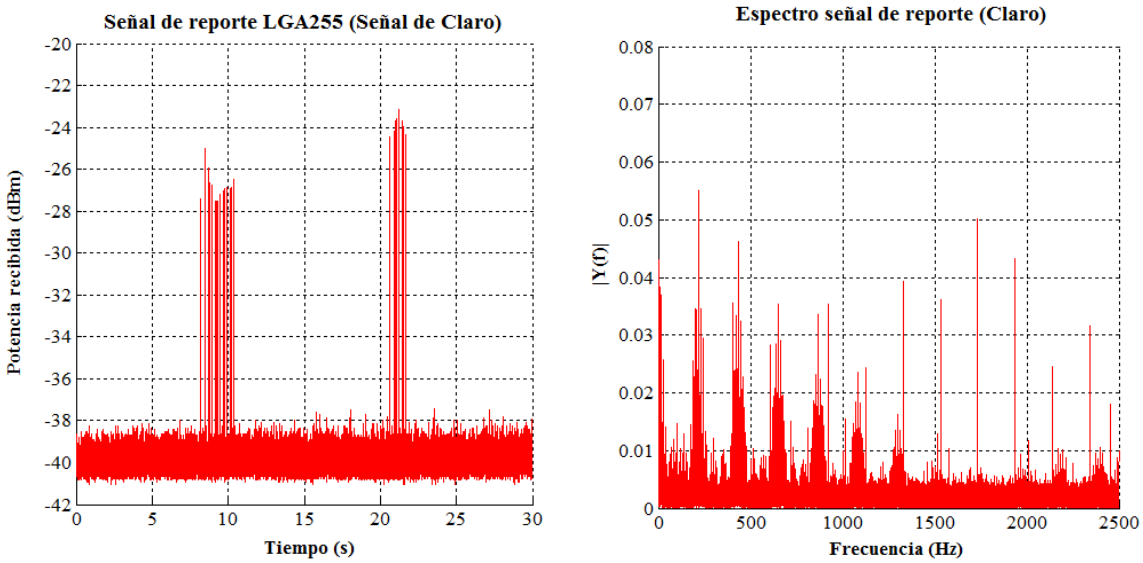


Figura 5.3 Señales ingreso y salida para el celular LGA255 a 5m del sistema de detección, (a) Señal en el tiempo y (b) Espectro de la señal de potencia

Finalmente, para formalizar la metodología de detección en 2G, se comparan las señales de reporte en función a la potencia recibida por el sistema de detección a diferentes distancias. Dichos resultados son mostrados en la Fig. 5.4 y se observa un comportamiento cercano al mostrado por las pérdidas teóricas para el espacio libre (FS). La potencia de la señal fue extraída de la figura 4.6a, la cual muestra una potencia promedio durante la señal de reporte cercana a los 5dBm, las ganancias de ambas antenas fueron las obtenidas en la sección 3.3 y ya que se trató de apuntar en la dirección de mayor potencia de emisión se tomaron valores cercanos a $2 - 3\text{dBi}$, los cuales fueron obtenidos en la sección 3.2

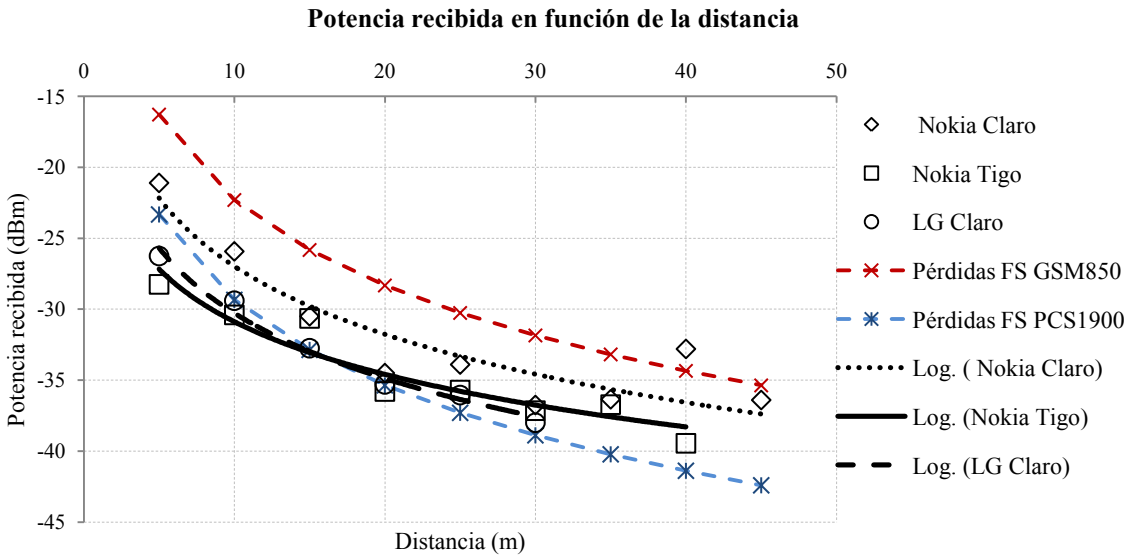


Figura 5.4 Variación de la potencia para la señal de reporte en función de la distancia

5.2 PROPUESTAS METODOLÓGICAS

La figura 5.4 muestra que el canal en consideración puede modelarse como un canal con pérdidas similares al espacio libre, por ende usaremos dicho modelo para el diseño posterior de la metodología tanto para el proceso de detección como de inhibición. Por otro lado, dada la varie-

dad de circunstancias en las cuales el sistema de detección e inhibición puede operar, la propuesta metodológica debe tener en cuenta las variables más importantes en la comunicación celular. Dichas variables fueron extraídas de la documentación encontrada en la normatividad, algunas de ellas reforzadas mediante las simulaciones y por supuesto muchas son de uso constante en el dimensionamiento para la construcción de las redes celulares (89) (90). Básicamente las propuestas metodológicas implementadas hacen uso de los métodos de planeación de redes celulares (91) como protocolo de diseño, esta vez dimensionando el alcance de la señal proveniente del móvil (proceso de detección) y de los niveles SNR sobre la estación fija (proceso de inhibición). Lo anterior tiene mucho sentido desde el punto de vista práctico ya que las redes celulares se dimensionan con dichos sistemas. A continuación se enuncian las variables relevantes en el problema de detección e inhibición y posteriormente se describen las metodologías propuestas para los tres casos; detección, inhibición y el último caso de detección de dirección de llegada plantea el uso de la señal de reporte en términos de su potencia, sin embargo sólo muestra un diseño tentativo del uso de la técnica para una implementación posterior.

5.2.1- Variables físicas determinantes en el proceso de comunicación

Como se mencionó previamente, algunas de las variables fueron extraídas de los documentos normativos del proyecto 3GPP. Otras fueron reforzadas con la simulación del proceso de comunicación y la mayoría de ellas son parte fundamental en el proceso de diseño de las redes de comunicación celular (91). En particular se dan algunas características del sistema de detección implementado. Ello permitirá evaluar si el dimensionamiento propuesto está acorde con lo obtenido en el presente trabajo, es decir, que los márgenes de distancia son del orden de 50m para un detector de potencia cuya sensibilidad máxima es $-40\ \text{dBm}$. Las alturas de las antenas son un caso adicional, sin embargo son de amplio uso en modelados del canal tipo COST-259 (79).

Variable	*Rango de uso*[5]
Tipo de modulación - 2G - 3G	 GMSK QPSK
Limite SNR tolerable - GSM - UMTS	 $x > 9$ dB $x > 7.2$ dB
Potencia del emisor (MS) - GSM850MHz - PCS1900MHz - UMTS	 $0 \text{ dBm} < x < 38\text{dBm}$ $0 \text{ dBm} < x < 33\ dBm$ $0 \text{ dBm} < x < 24 \text{ dBm}$
Potencia de la estación base (92)	40 – 46 dBm
Altura de la estación base	$6 < x < 30\ m$
Sensibilidad del receptor (BS) - GSM - UMTS - Sensado propio	 $-102 \text{ dBm} < x < -15 \text{ dBm}$ $-117\text{dBm} < x < -25 \text{ dBm}$ $-40 \text{ dBm} < x < 20 \text{ dBm}$
Directividad del receptor - Estaciones Base - Estación base usada	 $0 < x < 16$ dBi $0 < x < 3$ dBi
Distancia del móvil al punto de sensado	$0 < x < 150$ m
Distancia de la base al móvil	$50 \text{ m} < x < 5$ km
Distancia del inhibidor al punto del móvil	$10 \text{ m} < x < 150$ m
Pérdidas en los sistemas de medida - Filtro - Medidor de potencia - Cables	 -2 dBm -1 dBm -1 dBm

[5] Rango de uso se refiere no sólo a valores numéricos sino al tipo de información o parámetro usado en la variable del lado izquierdo.

Figura de ruido en el receptor	< 5 dBm
Tiempo de slot principal de emisión - GSM - UMTS	 577 µs 667 µs
Tiempo de la trama - GSM - UMTS	 4.62 ms 10 ms o 2 ms
Tipo de canal de comunicación	Urbano

Tabla 5.1 Principales variables involucradas en el proceso de detección e inhibición

5.2.2- Propuesta metodológica para el sistema de detección

Los resultados discutidos en la sección 4.1 aseguran que las señales de reporte en los casos 2G y 3G son distintas principalmente en potencia, lo cual condiciona la sensibilidad del detector. Las variables mostradas en la tabla anterior establecen que la sensibilidad en el caso GSM disminuye en 9 dBm los requerimientos de sensibilidad frente al caso 3G. El balance mostrado en la Tabla 2 contiene las variables requeridas como diseño metodológico para el proceso de detección y permite obtener la sensibilidad mínima para el caso de máxima separación de 150m entre el objetivo y el dispositivo de medida.

Señal procedente de la estación móvil (Uplink, 2G, 3G)	
Variable	*Pérdidas asociadas (dBm)*
Ganancia de la antena celular Potencia de salida del móvil	3 dBi 33 dBm (24 dBm)
Pérdidas asociadas al canal	- 84,42 dBm
Ganancia de la antena de recepción Figura de ruido en el receptor	3 dBi - 5 dBm
Figura Total de Potencia	- 72,42 dBm
Sensibilidad requerida en detección	**- 52,42 dBm (-61,42 dBm para 3G)**

Tabla 5.2 Balance para el proceso de detección a 150m para un móvil con ganancia de 3dBi

Obsérvese que el canal es el agente de mayor interferencia para el proceso de detección. Adicionalmente no debe pasarse por alto que una de las características con mayor importancia en este proceso es el tiempo mínimo de muestreo; 280 μs para GSM y 330 μs para WCDMA. Finalmente, para probar la temática del proceso de simulación, implementación y propuesta metodológica en el proceso de detección de móviles celulares, es decir, el trabajo desarrollado hasta el presente capítulo, se evalúan las características del sistema experimental implementado y con ello se determina el rango máximo de medición con el cual el sistema permitiría obtener la señal de actualización procedente del celular (Tabla 5.3)

Señal procedente de la estación móvil (Uplink, 2G,3G)	
Variable	**Pérdidas asociadas (dBm)**
Ganancia de la antena celular	3 dBi
Potencia promedio de salida del móvil	33dBm (24 dBm)
Ganancia de la antena de recepción	3 dBi
Figura de ruido en el receptor	- 5 dBm
Sensilidad en el receptor	- 40 dBm
Potencia total disponible	**74 dBm**
Distancia de operación	**45,22 m (16,05 m para 3G)**

Tabla 5.3 Balance para el alcance máximo de detección con un mayor de sensibilidad de -40dBm

La distancia máxima que el protocolo identifica en este caso con un medidor de potencia cuya sensibilidad es -40 dBm para el caso 2G es alrededor de 45 m, lo cual concuerda en muy buena aproximación a lo suministrado por la figura 5.4. Por otro lado el caso en 3G es bastante exigente ya que a tan sólo 20m requiere medidores de potencia de mejor sensibilidad. Este resultado prueba que la tecnología sobre la cual el teléfono móvil se encuentre acampando es de vital importancia para el dimensionamiento y alcance de un sistema de detección. Con esto se concluye que a partir de los datos mostrados en las anteriores tablas, el sistema de detección se encuentra

limitado primeramente por el tipo de tecnología de la red y en segunda instancia por el tipo de canal.

5.2.3- Propuesta metodológica para el sistema de inhibición

En los procesos de inhibición la parte clave de todo el trabajo radica en hacer que las condiciones del canal obliguen al móvil a generar fallos en los procesos de *downlink*. Normalmente esto se logra a partir del aumento de la tasa de errores en las tramas de datos enviados tanto desde el móvil hacia la estación base y viceversa. Particularmente la variable clave en este proceso es la figura de ruido y por ende los rangos permitidos para cada tecnología (GSM y WCDMA). Una de las fuertes amenazas a combatir es la potencia y directividad de la antena en la estación base la cual puede usar hasta tres antenas tipo sector lo cual aumenta la ganancia de la señal proveniente de la torre. El caso general de la relación señal ruido es el dado por la siguiente expresión (93):

$$\mathrm{SNR} = \mathrm{P_{out}} + \mathrm{G_{BS,MS}} - \mathrm{L_s} + 174\,\mathrm{dBm/Hz} - \mathrm{B} - \mathrm{NF} - \mathrm{J_s} \qquad (5.1)$$

Donde P_{out} es la potencia de salida de la antena base, $G_{BS,MS}$ es la suma de las ganancias tanto del móvil como de la antena base, L_s son las pérdidas asociadas al canal, B corresponde a $10\log \mathrm{BW}$(BW es el ancho de banda de la señal), NF es la figura de ruido en el móvil y $\mathrm{J_s}$ es la potencia de la señal de inhibición. Teniendo esto en mente y usando las características de los sistemas de comunicación en GSM y WCDMA tendremos el balance mostrado en la Tabla 5.4 para el caso de un sistema de inhibición. El caso estudiado es un escenario rural con una estación base a 1km del móvil objetivo y un sistema de inhibición a una distancia máxima de $150\mathrm{m}$, como se observa en la tabla. Para ambas tecnologías (2G y 3G) la potencia requerida por un inhibidor omnidireccional es del orden de $100\mathrm{W}$, no obstante el ancho de banda exigido para ambos casos es

diferente (5MHz para WCDMA y 200kHz para GSM). De la misma forma que el caso de detección, la inhibición está ligada al tipo de infraestructura de la red celular. El caso 3G representa uno de los retos mayores ya que el sistema posee procesos de control de potencia lo que paradójicamente fue diseñado para detectar la dirección del usuario y mejorar el canal anulando posibles fuentes de interferencia cercanas al usuario y un control en lazo cerrado para la potencia (60).

Señal a inhibir de la estación base (Uplink, 2G, 3G)	
Variable	**Pérdidas asociadas (dBm)**
Ganancia de la antena base	- 16 dBi
Potencia promedio de salida de la antena	- 46 dBm
Pérdidas asociadas al canal (emisor)	120,9 dBm
Directividad de la antena de inhibición	0 dBi
Pérdidas asociadas al canal (inhibidor)	- 104,42 dBm
Potencia total en el móvil	-54,52 dBm
Figura de ruido buscada (SNR)	- 9 dBm (-7 dBm)
Potencia promedio de inhibición	**54,52 dBm (52,52 dBm)**

Tabla 5.4 Balance de potencia para un proceso de inhibición a 150m de un celular y con una estación base a 1km de distancia

Obsérvese que la ganancia real de todo el sistema de emisión para la estación base es la ganancia de la antena y la directividad de la misma. Esto permite reforzar el concepto de inicio del presente trabajo y es el hecho que el uso de potencias directivas aumenta significativamente la capacidad del sistema de inhibición. En lo referente a la estación base hay un factor cercano a los 60dBm que condiciona el funcionamiento del inhibidor.

5.2.3- Propuesta para el diseño de un sistema de detección de dirección de llegada

La directividad de la señal proveniente de la estación base es un requerimiento actual que es usado hasta en las macro-celdas rurales y es la responsable de los niveles de potencia necesa-

rios para un proceso de inhibición a 150 m de distancia del móvil. Detectar la dirección de llegada de la señal de actualización proveniente del móvil es una de las estrategias más adecuadas para mejorar la probabilidad de inhibición de dispositivos móviles, esto con el fin de combatir los 60dBm de potencia de la estación base (Potencia + Ganancia). En este caso se propone un arreglo lineal de antenas del mismo tipo que se usaron en la implementación anterior (78), esto con el objetivo de unir ambos prototipos de diseño en un único dispositivo que permita la detección de presencia y dirección de la señal.

Ya que la sensibilidad del sistema de detección es la base para los sistemas de sensado de dirección de llegada, la metodología usada para este caso puede hacer uso de los métodos de planeación descritos en la sección 5.2.2, adicionalmente se propone el uso del root-MUSIC (94) como algoritmo de detección y para el sistema de adquisición se usa USRP1 (95) y WBX-USRP (96) como tarjetas de adquisición y sensado para las señales provenientes de las antenas, el diseño final se fundamente en los prototipos desarrollados por (97) y (98), los cuales permiten usar la arquitectura de GNURadio (99) como plataforma de desarrollo y por ende definir algunas de las características tanto del hardware como del software final que son requeridas en el desarrollo e implementación de un sistema de detección de dirección de llegada.

5.3 TRABAJOS FUTUROS

Los resultados presentados en este capítulo avalan adecuadamente el proceso de diseño desarrollado desde las simulaciones, pasando por el acercamiento experimental, hasta la adquisición final de medidas del dispositivo. Se garantiza con cierto margen de operación que el uso de las plataformas de diseño de redes celulares permite evaluar los sistemas de detección e inhibición. Para el caso de aumentar el rango de operación en los sistemas de detección, el uso de detectores logarítmicos de amplio espectro (ADL5513) con rangos dinámicos del orden de -80dB, garantizarían la detección en GSM en distancias geométricas del orden de los 150 m ó sistemas

de amplificación, no necesariamente de bajo ruido, ya que lo que se quiere detectar de la señal de interés es su potencia y no su forma temporal.

El sistema de detección posee un inconveniente y es que su desempeño depende del protocolo de reporte del móvil celular. En principio el envío de potencia por parte del inhibidor garantiza la emisión de dicha señal; luego de suspender la inhibición la solución más adecuada para este caso sería el uso de un sistema de interrogación que emulara una estación base. Dichos sistemas son implementados (y de uso abierto) en plataformas como GNURadio, lo cual hace prever en corto plazo el uso de este tipo de plataformas.

A partir de los resultados de la sección 3.1 y 3.2 se pueden explorar las características de otros tipos de inhibición, de tal forma que los rangos de ruido necesarios para generar FER del orden de 0.5% en el canal RACH sean cada vez más bajos, lo cual permitiría optimizar los recursos del inhibidor.

CONCLUSIONES

Se implementó un sistema de detección de actividad en la banda celular con muy buenos resultados, acordes con lo exigido por las normas para el uso del espectro electromagnético. La instrumentación utilizada es de bajo costo y completamente analógica, lo cual la hace bastante rápida para un posible uso en campo sin el uso de costosos sistemas de procesamiento digital y permite un escalamiento en frecuencia y potencia al ser pensada bajo un esquema modular para tecnologías celulares 2G y 3G, lo que hace pensar en implementaciones futuras. Se establece de paso un comparativo en las exigencias de sensibilidad para la detección en las tecnologías mencionadas.

Como conclusión importante del presente trabajo se identifican requerimientos de potencia para el problema de inhibición, que puede ser integrado al sistema de detección y de esta forma pensar en una metodología inteligente para la problemática asociada al uso de artefactos explosivos improvisados radio controlados (RCIEDs).

El problema de detección e inhibición ha sido mostrado como la composición de distintos elementos que gobiernan principalmente aspectos relacionados con el protocolo de comunicación y el hardware disponible para cada uno de los móviles celulares. Algunos de los resultados más importantes del presente trabajo fueron mostrados en las secciones 4.2, 4.3 y 5.2.3, en estas secciones se corroboró que el proceso de detección e inhibición se encuentra condicionado por el tipo de tecnología, el caso 2G es el caso más simple de detección ya que la potencia de la señal es máxima durante la señal de reporte, el caso 3G presenta serias limitaciones en cuanto a hardware y software ya que las señales son más débiles en potencia y cortas en el tiempo. Por otro lado, la detección tanto en 2G como en 3G presenta variaciones respecto a la sensibilidad requerida por el detector, esto debido al uso de distintas bandas de frecuencia, anchos de banda y en algunos casos al uso de protocolos de control de potencia (WCDMA). Para el caso del sistema de inhibición la metodología propuesta (Sec. 5.2.3) arroja valores parecidos para ambas tecnologías, en este caso

la limitante mostrada es fundamentalmente la directividad asociada a las antenas de las estaciones base, no obstante una de las exigencias para el inhibidor es garantizar los anchos de banda de las señales en 2G y 3G y por ende la velocidad de salto debe ser inferior a la que realiza el protocolo de comunicación.

Como recomendación proveniente de los resultados obtenidos en las medidas se sugiere evitar a toda costa operaciones militares en cercanías a estaciones base celulares, dado que los requerimientos de un sistema de inhibición bajo estas condiciones difícilmente podrían ser alcanzadas.

Los resultados mostrados en frecuencia para la señal de reporte confirman que los móviles usan tecnologías asociadas a los protocolos de comunicación GSM y WCDMA. Para el caso 2G se observan trenes de pulsos de mayor intensidad y duración, en el caso 3G la señal es de mayor ancho de banda pero con una reducción significativa en la potencia de emisión. Por su parte, a partir del comportamiento en el tiempo para las señales en 2G se establece cuáles efectivamente muestran la duración de una ráfaga de información del orden de 570 μs. Esto muestra que el sistema experimental propuesto permite identificar el tipo de tecnología en la cual móvil se encuentra funcionando.

El sistema de recepción puede diseñarse con una variedad de componentes electrónicos de sensado y procesamiento, lo mostrado por la metodología para el desarrollo de un sistema de detección muestra que una de las mayores exigencias para 2G es la sensibilidad del detector de potencia, para el caso 3G el sistema no sólo aumenta en términos de su sensibilidad sino que requiere el uso de sistemas previos de amplificación y quizás de preprocesamiento, esto se debe en gran medida a que las señales en TDMA son de menor ancho de banda y por ende la potencia es mayormente impulsiva, sin embargo en WCDMA la potencia está distribuida en un ancho de banda mayor, por ende los pulsos tienen menor amplitud, lo cual requeriría mayor sensibilidad en el detector.

Las gráficas 5.2 y 5.3 permiten definir claramente que los procedimientos de detección dependen de la tecnología donde el móvil se encuentre operando y no del tipo de operador o móvil del cual sea emitida la señal. Obviamente la potencia de emisión de cada móvil no es la misma y quizás la directivida de las antenas no sea la misma. Sin embargo, en lo relacionado a la señal de potencia en el tiempo su estructura refleja claramente el uso de tecnología 2G. Una de las limitantes en el proceso de detección es la potencia de salida del emisor celular y en algunos casos los patrones de radiación pueden camuflar la señal de reporte y por ende no se podría detectar el móvil.

La estructura de las ráfagas de información en las dos tecnologías (2G y 3G) es claramente de suma importancia en el proceso de detección teléfonos celulares, ya que los tiempos de muestreo de los ADC permiten delimitar las zonas temporales donde el sistema puede sensar los cambios de potencia. La duración en el tiempo de las señales de reporte muestran reiterativamente componentes cercanas a los 220Hz, la cual es bastante cercana a los 216,7 Hz (4.615 ms) correspondientes a la duración de las 8 ráfagas de información según lo establecido por la norma.

BIBLIOGRAFÍA

1. Presidencia de la República . Acción Contra Minas. *Situación Nacional Víctimas de minas antipersonal en Colombia.* [En línea] Progrma Presidencial para la Acción Integral contra Minas Antipersonal, 4 de April de 2013. [Citado el: 13 de June de 2013.] http://www.accioncontraminas.gov.co/Situacion/Paginas/SituacionVictimasMinasAntipersonal.aspx.

2. Higginbotham, Adam. U. S. Military Learns to Fight DEadliest Weapons. *WIRED Magazine.* [En línea] 28 de July de 2010. [Citado el: 18 de June de 2013.] http://www.wired.com/magazine/2010/07/ff_roadside_bombs/all/1.

3. Clay Wilson. Navy Departament Library. *Improvised Explosive Devices (IEDs) in Iraq: Effects and Countermeasures.* [En línea] 6 de February de 2006. [Citado el: 18 de June de 2013.] http://www.history.navy.mil/library/online/ied.htm.

4. Suarez, Ray. Military Grapples with Onslaught of Homemade Bombs in Iraq. *Online newshour.* PBS Newshour, Middle East USA : PBS , 21 de june de 2007.

5. *Cellular Jamming.* Gold, Steve. 8 de 2012, Network Security, págs. 15-18.

6. Poisel, Richard. *Modern Communications Jamming Principles and Techniques.* Norwood : Artech House, 2011.

7. NETLINE. Cell Phone Detector. *Netline Counter Terror Electronic Warfare.* [En línea] [Citado el: 18 de june de 2013.] http://www.netline.co.il/cellular_phone_detector.aspx.

8. ROHDE & SCHWARZ. Rhode and Schwarz Digital HF/VHF/UHF Monitoring Direction Finder. *http://www.rohde-schwarz.com/.* [Online] 2013 йил. [Cited: 2013 3-may.] http://www.rohde-schwarz.com/en/product/ddf0xe-productstartpage_63493-9482.html.

9. Lockheed Martin. Press Releases. *Lockheed Martin Delivers 2000th Symphony Imporvised Explosive Device Jamming System.* [En línea] Lockheed Martin, 5 de June de 2011. [Citado el: 12 de June de 2013.] http://www.lockheedmartin.com/us/news/press-releases/2011/may/symphony.html.

10. Allen Vanguard (R). Electronic Countermeasures. *Scorpion.* [En línea] Allen Vanguard, 2013. [Citado el: 16 de june de 2013.] http://www.allenvanguard.com/en-us/products/electroniccountermeasures/scorpion.aspx.

11. NETLINE. Military RF Jammers. *Portable IED Jammers.* [En línea] NETLINE. [Citado el: 10 de june de 2013.] http://www.netline.co.il/portable_ied_jammers.aspx.

12. 3GPP TM ETSI. *3GPP TS 23.012 UMTS Location management procedures.* Sophia Antipolis - France : European Telecommunications Standards Institute, 2011.

13. —. *3GPP TS 25.304 Functions related to Mobile Station (MS) in idle mode.* Valbonne - France : European Telecommunications Standards Institute, 2007.

14. M2MSupport.net. Carrier Search. *Carrier Claro Colombia.* [En línea] M2MSupport, 2013. [Citado el: 18 de May de 2013.] http://m2msupport.net/m2msupport/claro-columbia-m2m-modules-certification-sim-data-plans/.

15. M2MSupport. Carrier Search. *Carrier Tigo Colombia.* [En línea] 2013. [Citado el: 18 de June de 2013.] http://m2msupport.net/m2msupport/tigo-colombia-m2m-modules-certification-sim-data-plans/.

16. —. Carrier Search. *Carrier Movistar Colombia.* [En línea] 2013. [Citado el: 18 de June de 2013.] http://m2msupport.net/m2msupport/movistar-colombia-m2m-modules-certification-sim-data-plans/.

17. 3GPP TM ETSI. *3GPP TS 45.005 Radio Trasmission and reception.* Sophia Antipolis Cedex - France : European Telecommunications Standards Institute , 2011.

18. Yue, Prof. C. Patrick. ECE 219 - CMOS RFIC Design. *USCB High-Speed Silicon Lab.* [En línea] 2007. [Citado el: 18 de JUne de 2013.] http://www.ece.ucsb.edu/yuegroup/Teaching/ECE219Winter2013/ECE219.html.

19. Häggman, Prof. Sven-Gustav. Radio Receiver Architecture. *Postgraduate Course in Radio Communications.* [En línea] 22 de February de 2005. [Citado el: 18 de June de 2013.] http://www.comlab.hut.fi/opetus/333/2004_2005_slides/Receiver_architectures.pdf.

20. Texas Instruments. Real World Signal Processing TM. *Wireless Terminals Soluton Guide.* [En línea] 2004. [Citado el: 13 de July de 2013.] http://focus.ti.com/pdfs/vf/wireless/ti_wireless_solutions_guide.pdf.

21. Howard Huang, Constantinos B. Papadias and Sivarama Venkatesan. *MIMO Communication for Cellular Networks.* New York - USA : Springer, 2012. e-I SBN 978-0-387-77523-4.

22. *Multi-Carrier Systems & Solutions 2009, Uplink power control performance in UTRAN LTE Networks.* Robert Müllner, Carsten F. Ball, Kolio Ivanov, Johann Lienhart and Peter Hric. Herrsching - Germany : Springer , 2009. ISSN 1876-1100.

23. Daniels, David. *EM Detection of Concealed Targets.* Hoboken, New Jersey : Jhon Wiley & Sons Inc., 2010.

24. Wilkinson, R. *Cellular Detection & Control.* San Francisco : Corrections Technology Association (A forum for collaboration), 2005.

25. Scott, Nicholas W. *Study of cellular phone detection techniques.* Nebraska : Computer and Electronics Engineering, University of Nebraska, 2011.

26. Ipatov, Valery P. *Spread Spectrum and CDMA principles and applications.* Chichester, England : John Wiley & Sons Ltd, 2005.

27. *Beamforming solutions for interference reduction for high altitude airborne CDMA systems.* Syst, Northrop Grumman Inf. 2011, Aerospace Conference, 2011 IEEE, págs. 1-7.

28. *Jammer Suppression in DS-CDMA Arrays Using Independent Component Analysis.* K. Raju, T. Ristaniemi, J. Karhunen, and E. Oja. 2006, IEEE Transactions on Wireless Communications, págs. 1-6.

29. *Suppression of bit-pulsed jammer signals in DS-CDMA array system using independent component analysis.* Karthiksh Raju, Tapani Ristaniemi, Juha Karhunen, A. Oja. 2002, IEEE International Symposium on Circuits and Systems, págs. 189-192.

30. Verdú, Sergio. *Multiuser Detection.* Cambridge, United Kingdon : Cambridge University Press, 2003.

31. 3GPP TM. 3GPP TM. *3GPP TM A global Initiative THE Mobile Broadband Standard.* [En línea] 3GPP TM, 2013. [Citado el: 13 de Marz de 2013.] http://www.3gpp.org/.

32. TelecomHall. Curso Telecomunicaciones. *Las 7 capas del Modelo OSI.* [En línea] 2008. [Citado el: 14 de June de 2013.] http://www.telecomhall.com/es/las-7-capas-del-modelo-osi-.aspx.

33. Swamy, Ke-Lin Du & M. N. S. *Wireless Communication Systems from RF Subsystems to 4G enabling technologies.* Cambridge - United Kingdom : Cambridge University Press, 2010. ISBN 978-0-521-11403-5.

34. Yongwan Park, Fumiyuki Adachi. *Enhanced Radio Access Technologies for next Generation Mobile Communication.* Dordrecht, The Netherlands. : Springer Link, 2007. 978-1-4020-5531-7.

35. MinTIC Colombia. Ministerio de Tecnologias de la Información y las Comunicaciones. *Proceso de Subasta de 4G, Gobierno Adjudica licencias de 4G.* [En línea] 26 de June de 2013. [Citado el: 30 de June de 2013.] http://www.mintic.gov.co/index.php/proceso-subasta-4g-noticias/2290-gobierno-adjudica-licencias-de-4g.

36. Gilley, James E. Digital Phase Modulation. [Online] 2003 йил 7-August. [Cited: 2013 йил 6-May.] http://ok1mjo.com/all/ostatni/Yaesu_Vertex_VX-1700/Transcrypt_Digital_Phase_Modulation.pdf.

37. 3GPP TM ETSI. *3GPP TS 45.002 Radio Access Network Multiplexing and multiple access on the radio path.* Valbonne-France : European Telecommunication Standard Intitute, 2008.

38. *An overview of Air interface multiple access for IMT-2000/UMTS.* Prasad, Tero Ojaperä and Ramjee. 9 p. 82-86, s.l. : IEEE Communications Magazine, 1998, Vol. 36. ISSN : 0163-6804.

39. *A comparison of CDMA and TDMA Systems.* Björn Gudmundson, Johan Sköld and Jon K. Ugland. 1, p. 732-735, Stockholm, Sweden : Vehicular Technology Conference, 1992, Vol. 2. ISSN 1090-3038.

40. *Comparison between CDMA and TDMA air interface for cellular systems.* Hui, Wong Ngee. Nanyang, Singapore : s.n.

41. *An Overview of CDMA Evolution toward wideband CDMA.* Ojanperä, Ramjee Prasad and Tero. 1. p. 2-29, s.l. : IEEE Communications Surveys & Tutorials, 1998, Vol. 1. ISSN: 1553-877X.

42. (C) ETSI. ETSI.org. *ETSI Standards.* [En línea] (C) European Telecommunication Standars Institute, 2012. [Citado el: 13 de Marz de 2013.] http://www.etsi.org/standards.

43. 3GPP TM ETSI. *3GPP TS 45.001 Physical layer on the radio path.* Sophia Antipolis Cedex - France : European Telecommunication Standards Institute, 2011. RTS/TSGG-0145001va00.

44. Jorg Eberspacher, Hans-Jorg Vogel, Christian Bettstetter, Christian Hartmann. *GSM - Architecture, Protocols and Services.* Wiltshire, UK : Jhon Wiley and Sons, 2009. 978-0-470-03070-7.

45. 3GPP TM ETSI. *3GPP TS 45.003 Radio Access Network.* Valbonne - France : European Telecommunications Standard Institute, 2008.

46. —. *3GPP TS 45.004 Radio Access Network Modulation* . Velbonne - France : European Telecommunication Stantards Institute, 2008.

47. 3GPP TM Organizational Partners. *3GPP TS 11.21 Technical Specification Group GSM/EDGE Radio Access Network Base Station System equipment specification.* Velbonne - France : 3GPP TM, 1999.

48. Kikkert, C. J. James Cook University - Communication Systems Principles. *Digital Communication Systems and their Modulation Techniques.* [En línea] August de 2004. [Citado el: 12 de February de 2013.] http://www.ece.jcu.edu.au/subjects/ee3700/lectures/EE3700DigitalCommSystems.pdf.

49. 3GPP TM ETSI. *3GPP TS 25.201 Physical layer - general description.* Sophia Antipolis Cedex - France : European Telecommunications Standards Institute, 2008.

50. —. *3GPP TS 51.010-1 Mobile Station conformance specification, Conformance specification.* Sophia Antipolis Cedex - France : European Telecommunications Standards Institute, 2013.

51. 3GPP TM. *3GPP TS 45.008 Technical Specification Group GSM/EDGE Radio Access Network.* Valbonne - France : 3GPP TM, 2009.

52. —. *3GPP TS 5.08 Technical Specification Group GSM/EDGE Radio Access Network; Radio subsystem link control.* Valbonne - France : 3GPP TM, 2005.

53. 3GPP TM ETSI. *3GPP TS 25.214 Physocal layer procedures (FDD).* Sophia Antipolis Cedex - France : European Telecommunication Standards Institute, 2007.

54. Stüber, Gordon L. Ch 12 CDMA Cellular Systems. *Principles of Mobile Communication.* New York : Springer, 2011.

55. 3GPP TM ETSI. *3GPP TS 25.211 Physical cahnnels and mapping of trasport channels onto physical channels (FDD).* Sophia Antipolis Cedex - France : European Telecommunications Standards Institute , 2010.

56. —. *3GPP TS 25.212 multiplexing and channel coding (FDD).* Sophia Antipolis Cedex - France : European Telecommunication Standards Institute, 2012.

57. —. *3GPP TS 25.213 Spreading and modulation (FDD).* Sophia Antipolis Cedex - France : European Telecommunication Standards Institute, 2000.

58. Torreri, Don. *Principles of Spread-Spectrum Communication Systems.* New York : Springer, 2011. ISBN 978-1-4419-9594-0.

59. 3GPP TM ETSI. *3GPP TS 25.101 User Equipment radio transmission and recepction (UMTS).* Sophia Antipolis Cedex - France : European Telecommunication Standards Institute, 2011.

60. Toskala, Harri Holma and Antti. *WCDMA for UMTS.* New Delhi - India : John Wiley & Sons, Ltd, 2004. ISBN 0-470-87096-6.

61. Andrew (R) . Applications Enginneering Notes. *Commscope Andrew Solutions.* [En línea] 2012. http://docs.commscope.com/Public/applications_engineering_notes.pdf.

62. Elsadek, Hala. *Microstrip Antennas for Mobile Wireless Communication System.* [En línea] 2010. [Citado el: 14 de May de 2013.] http://cdn.intechopen.com/pdfs/8994/InTech-Microstrip_antennas_for_mobile_wireless_communication_systems.pdf. ISBN: 978-953-307-042-1.

63. *Design of Antennas for mobile communications devices: practical aspects.* Vázquez, Marta Martínez. Boston : IEEE & IMTS GmbH, 2011.

64. *Antenna Design for Mobile Devices.* Zhang, Zhijun. Noida - India : Wiley-IEEE Press, 2011. ISBN: 978-0-470-82446-7.

65. Manteuffel, Frank Gustrau and Dirk. *EM Modeling of Antennas and RF Components for Wireless Communication Systems.* Kamp-Lintfort-Germany : Springer, 2006. ISBN-10 3-540-28614-4.

66. S. Drabowitch, A. Papiernik, H. D. Griffiths, J. Encinas and B. L. Smith. *Modern Antennas.* Dordrecht - Netherlands : Springer, 2005. ISBN-IO 1-4020-3216-1.

67. Yang, Samuel C. *CDMA RF System Engineering.* Norwood - United Kingdom : Artech House, 1998. ISBN 0-89006-991-3 p. 30.

68. Parra, Javier. *Simulación de la interfaz de radio para sistemas de comunicaciones móviles GSM/GPRS.* Cali - Colombia : Universidad del Valle, 2005.

69. Mikkelsen, Arne Norre Ekstrøm & Jan H. *GSMsim A MATLAB Implementation of a GSM Simulation Platform.* Aalborg Øst - Denmark : Institute of Electronic Systems, Division of Telecommunications, Aalborg University, 1997.

70. Syed, M. Zafi S. Shah. MATLAB(R) CENTRAL. *UMTS Rel 99 Physical layer Simulation.* [En línea] 2 de Marz de 2008. [Citado el: 10 de April de 2013.] http://www.mathworks.com/matlabcentral/fileexchange/19000-umts-rel-99-physical-layer-simulation.

71. *Bit error rate performace analysis on modulation techniques of wideband code division multiple access.* M. A. Masud, M. Samsuzzaman and M. A. Rahman. 2 p. 22-29, s.l. : Journal of Telecommunications, 2010, Vol. 1.

72. Rohde & Schwarz. Mobile Radio. *Protocol Tester.* [En línea] 2003. [Citado el: 18 de Marz de 2013.] http://cdn.rohde-schwarz.com/dl_downloads/dl_common_library/dl_news_from_rs/178/n178_crtu-g-w.pdf.

73. Agilent Technologies. IO Libraries Suite. *GSM Design Library.* [En línea] September de 2004. [Citado el: 10 de April de 2013.] http://newport.eecs.uci.edu/eceware/ads_docs/pdf/gsm-doc.pdf.

74. ETSI. *Functions related to Mobile Station in idle mode and group receive mode.* Valbonne - France : ETSI TS 3.22 European Telecommunications Standards Institute, 2000.

75. 3GPP TM. *3GPP TR 25.944 Channel coding and multiplexing examples.* Sophia Antipolis Cedex - France : European Telecommunications Standards Institute, 2006.

76. 3GPP TM Organizational Partners . *3GPP TR 25.814 Physical layer aspects for evolved universal terrestrial radio acess.* Velbonne - France : 3GPP TM, 2006.

77. 3GPP TM ETSI. *3GPP TR 25.913 Requeriments for evolved UTRA and evolved UTRAN.* Velbonne - France : European Telecommunications Standards Institute, 2009.

78. Laipac Technology Inc. GSM Antennas . *Antenna Specification.* [En línea] 23 de August de 2010. [Citado el: 12 de May de 2013.] http://www.laipac.com/pdf/p1gsm.pdf.

79. 3GPP TM ETSI. *3GPP TR 25.943 Technical Specification Group Radio Access Networks.* Valbonne-France : European Telecommunication Standards Institute, 2012.

80. Yves R. Hamel et Associés Inc. Broadcast and Telecommunication Consultants. *Analysis of the coverage differences between the cellular (850 MHz) and PCS (1900 MHz) Bands, including a sample deployment study of Highway 401 and Kingston.* Montreal, Québec : s.n., 2033.

81. Swamy, Ke-Lin Du & M. N. *Wireless Communication Systems from RF subsystems to 4G Enabling Technologies.* Cambridge - United Kingdom : Cambridge University Press, 2010. 978-0-521-11403-5 p. 40-46.

82. Molisch, Andreas F. Wireless Communications, 2nd Edition Suplememtary material. *Wiley Ltd.* [En línea] november de 2010. [Citado el: 14 de may de 2013.] http://www.wiley.com/legacy/wileychi/molisch/supp2/appendices/c07_Appendices.pdf.

83. AARONIA AG. Products, Spectrum Analyzers. *HighEnd EMC Spectrum Analyzer up to 9,4GHz with ultra high sensitivity SPECTRAN HF-60100 V4.* [En línea] AARONIA AG, 2013. [Citado el: 12 de February de 2013.] http://www.aaronia.com/products/spectrum-analyzers/hf-60100-v4-emc-spectrum-analyzer/.

84. Mini-Circuits(R) . Coaxial Bandpass Filter. *Dash Board: VBFZ-780-S+.* [En línea] 2013. [Citado el: 14 de May de 2013.] http://www.minicircuits.com/pdfs/VBFZ-780+.pdf.

85. Mini-Circuits(R). Coaxial Bandpass Filter. *Dash Board VBF-1840+.* [En línea] 2013. [Citado el: 15 de April de 2013.] http://www.minicircuits.com/pdfs/VBF-1840+.pdf.

86. —. Power Detectors . *Dash Boaard ZX47-40-S+.* [En línea] 2013. [Citado el: 12 de April de 2013.] http://www.minicircuits.com/pdfs/ZX47-40+.pdf.

87. ATMEL(R). AVR 8-bit and 32-bit Microcontroller. *8-bit Atmel Microcontroller ATmega2560.* [En línea] 2012. [Citado el: 20 de 5 de 2013.] http://www.atmel.com/images/doc2549.pdf.

88. Mini-Circuits. Products - Amplifiers. *Amplifiers - Low Noise - 0.1 to 5400 MHz.* [En línea] Mini-Circuits RF/IF & Microwave Components, 2013. [Citado el: 23 de may de 2013.] http://www.minicircuits.com/products/amplifiers_coax_low_noise.shtml.

89. *Cell Coverage Area and Link Budget Calculations in GSM System.* Singh, Purnima K. Sharma and R. K. 2 pp. 170-176, s.l. : International Journal of Modern Engineering Research, 2012, Vol. 2. ISSN: 2249-6645.

90. *Estimation of Design Parameters for Cellular WCDMA Network.* Mawjoud, S. A. 4, Mosul, Iraq : Al-Rafidain Engineering, 2008, Vol. 16.

91. Manninen, Jukka Lempiäinen and Matti. *Radio Interface System Planing for GSM/GPRS/UMTS.* Boston - Massachusets : Kluwer Academic Pubishers , 2001. ISBN 0-7923-7516-5.

92. 3GPP TM. *3GPP TS 25.141 Base Station (BS) conformance testing (FDD).* VAlbounne - France : 3GPP TM, 2010.

93. *A Quantfication of Link Budget Differences Between the Cellular and PCS bands.* Greenstein, T. -S. Chu and Larry J. 1, s.l. : IEEE Transactions on vehicular technology, 1999, Vol. 48. 0018-9545/99.

94. Zhizhang Chen, Gopal Gokeda and Yiqiang. *Direction of Arrival Estimation.* Norwood - Masachusets : Artech House, 2010. ISBN 978-1-59693-089-6.

95. Ettus Research. Product Categories. *USRP Bus Series.* [En línea] Ettus Research, 2013. [Citado el: 18 de May de 2013.] https://www.ettus.com/product/details/USRPPKG.

96. —. Product Categories. *RF Daughterboards.* [En línea] Ettus Research, 2013. [Citado el: 18 de May de 2013.] https://www.ettus.com/product/details/WBX.

97. Abu-Shaban, Zohair M. *Localisation Testbed using Software-Defined Radio.* London - United Kingdom : Imperial College London, 2010.

98. GNU Radio. GNURadio Wiki. *Hackfest1211.* [En línea] GNURadio, 26 de November de 2012. [Citado el: 14 de Marz de 2013.]

99. Rondeau, Tom. GNU Radio the open source software radio. *GNU Radio the open source software radio.* [En línea] GNU Radio, 23 de march de 2013. [Citado el: 14 de may de 2013.] http://www.trondeau.com/.