UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN INGENIERÍA
ELECTRICA – TELECOMUNICACIONES

ANÁLISIS DEL DESEMPEÑO DE LA CAPA FÍSICA BASADA EN OPENBTS PARA LAS REDES GSM

TESIS QUE PARA OPTAR POR EL GRADO DE:
MAESTRO EN INGENIERÍA

PRESENTA:
JOSE JESUS CUELLAR RUIZ

TUTOR PRINCIPAL
VICTOR RANGEL LICEA
FACULTAD DE INGENIERIA UNAM

MÉXICO, D. F. ENERO DE 2015

JURADO ASIGNADO:

Presidente:	Dr. Javier Gómez Castellanos
Secretario:	Dr. Víctor Rangel Licea
Vocal:	Dr. Ramón Gutiérrez Castrejón
1 er. Suplente:	Dr. Víctor García Garduño
2 d o. Suplente:	Dr. Miguel Flores Moctezuma

Lugar donde se realizó la tesis: CIUDAD UNIVERSITARIA, UNAM

TUTOR DE TESIS:

Dr. VICTOR RANGEL LICEA

FIRMA

DEDICATORIA

A mis padres Rosario y Margarito por brindarme siempre su apoyo incondicional, cariño y esfuerzos por llevarme siempre por el buen camino.

A mis hermanos Cesar, Jaime, Sergio y Rosa por las experiencias desde pequeños y que continúan hasta ahora.

A mis primos Pedro, Hugo y Aldo quienes desde niño me han enseñado a vivir la vida y a ser una mejor persona.

A todos mis familiares y amigos que me han apoyado y han estado conmigo siempre.

AGRADECIMIENTOS

A PAPIIT por el apoyo recibido para la realización de esta tesis, mediante el proyecto No. 114713, titulado “Diseño y análisis de algoritmos de calendarización en redes LTE y WiMAX”

Al CONACYT, por la beca otorgada a través del proyecto 105279, titulado “Diseño de técnicas de reservación de capacidad de redes de banda ancha móviles”.

Al Dr. Víctor Rangel Licea por sus enseñanzas, paciencia y tolerancia durante el desarrollo de este trabajo de tesis.

A la UNAM y a la facultad de Ingeniería por darme la oportunidad de obtener formación personal y profesional.

RESUMEN

La primera generación de telefonía celular se volvió obsoleta después de la aparición de los sistemas digitales dando paso a las siguientes generaciones que hasta entonces siguen evolucionando.

Las redes inalámbricas se han convertido en la tecnología de hoy en día debido a su alta demanda de nuevos servicios tales como acceso a internet, transferencia de datos, Voz sobre IP, servicios multimedia, redes sociales entre otras, esto ha motivado a la industria de las telecomunicaciones a buscar nuevos sistemas de comunicaciones que puedan soportar estos servicios, para que todos los usuarios tengan acceso a ellos desde cualquier lugar, en cualquier momento y con tarifas accesibles.

La tecnología de acceso inalámbrico especialmente en redes celulares revolucionará la forma de comunicación que actualmente se utiliza para la transmisión de servicios y aplicaciones digitales ya que en algunos lugares el servicio es muy limitado.

Con esta investigación se pretende desplegar una red celular de bajo costo que permita dar servicio a usuarios en lugares donde la cobertura no existe o es muy escasa.

En este trabajo se presenta una tecnología emergente en telefonía celular y lo que la hace importante es poder tener acceso a una interfaz de segunda generación (GSM) mediante hardware de bajo costo y software libre, como lo son los Radios Definidos por Software (SDR) junto con un dispositivo USRP. También en conjunto con GNU Radio, herramienta necesaria para que pueda interactuar el USRP con una computadora personal y se puedan transmitir y recibir las señales.

Capítulo 1

INTRODUCCIÓN

Capítulo 2

ESTADO DEL ARTE

Capítulo 4

DESCRIPCION DEL SISTEMA

Capítulo 5

PRUEBAS Y RESULTADOS OBTENIDOS

Índice de Figuras

ÍNDICE DE TABLAS

CAPITULO I

INTRODUCCION

1.1 ANTECEDENTES

En México el mercado de la telefonía móvil ha crecido de manera cuantiosa. Según la extinta Comisión Federal de Telecomunicaciones (COFETEL) [1], hasta su última actualización, la televisión vía satélite, el tráfico internacional de entrada y el tráfico de minutos cursados en la red de telefonía móvil, son las áreas de mayor importancia. Aumenta 107.3 por ciento el número de suscriptores de banda ancha móvil en un año más del doble. Los operadores de telefonía móvil en México han dirigido sus estrategias comerciales a incrementar su base de usuarios de pospago. La alta demanda que tienen estos usuarios se ve reflejada en la necesidad de las operadoras a mejorar los servicios y lanzar al mercado más y mejores aplicaciones para satisfacer a los suscriptores.

A estas alturas la voz y los mensajes de texto representan un bajo porcentaje del uso de los teléfonos móviles, pero desde hace unos pocos años están creciendo exponencialmente las cifras de tráfico en servicios de datos, especialmente usados para la navegación web, correo electrónico y redes sociales. La introducción primero de la adaptación a GPRS de los sistemas de 2ª generación (2G) y después la aparición de UMTS, con su ampliación específica para datos de alta velocidad HSPA, ha permitido soportar ese incremento durante la primera década de este siglo. Sin embargo, las previsiones de crecimiento actuales hacen que sea necesario el despliegue en muy poco tiempo de nuevas soluciones y nuevas tecnologías.

1.2 DEFINICION DEL PROBLEMA

Hoy en día los servicios de telecomunicaciones que demanda la sociedad son muy altos, enfocándonos en teléfonos celulares mejor conocidos como smartphones ya no se utilizan solamente para realizar llamadas telefónicas o enviar mensajes de texto si no que requieren de una gran diversidad de servicios, debido a que estos ya se encuentran en el mercado actual, la problemática es la velocidad que demanda el usuario para hacer uso de ellos.

Esta problemática se da actualmente en entornos urbanos donde la población es extensa y donde se necesita una mayor cobertura y se pueda ofrecer calidad de servicio para los usuarios.

Alrededor del mundo, se ha estado buscando cómo llegar a la llamada Cuarta Generación (4G) de telefonía móvil, gracias a dicho aumento en la demanda de servicios de telecomunicaciones avanzados que requieren nuevas características, sin embargo los estándares actuales para la tecnología GSM no soportan técnicas sofisticadas para transmisión a altas velocidades.

Estas desventajas de los sistemas actuales de comunicaciones, nos motiva a basar esta investigación en los sistemas inalámbricos que pretenden satisfacer la necesidad de cobertura que hoy en día se requiere, por área de cobertura que en México existen zonas donde no es posible contar con servicio, no solo en las calles, sino también en el hogar, oficinas, escuelas, hospitales, y sobre todo cuando uno se traslada de un lugar a otro y que disponga de una gran cobertura, sin importar la hora, el lugar, ni el tiempo de conexión.

En el último año el Dr. Víctor Rangel ha incorporado las redes GSM basadas en OpenBTS[3] por ser una tecnología para la provisión de servicios digitales y por ser software libre. Y por lo tanto, se cree que la incorporación de los protocolos OpenBTS en esta línea de investigación hará posible realizar investigación de tecnologías digitales como wifi y tecnologías celulares de las generaciones 2G y 2.5G que se pueden poner en funcionamiento a un costo no muy elevado.

1.3 OBJETIVOS

- Poner en funcionamiento la capa física para que opere utilizando la modulación GMSK basado en los sistemas GSM y que considere las diferentes propiedades y características de un medio inalámbrico.

- Estudiar la capa física de GSM mediante el Software Defined Radio (Software definido por radio), para tener una mejor comprensión del estándar y del funcionamiento del sistema.

- Se analizará la importancia que tiene el dispositivo USRP modelo N210 detallando su funcionamiento interno y cómo opera la señal de radio captada por la antena para realizar el procesamiento en el hardware de dicha señal.

- Implementación de un sistema GSM (micro-célula) que proporcione la funcionalidad de realizar llamadas y enviar mensajes de texto y sirva de referencia para realizar posibles mejoras.

1.4 CONTRIBUCIONES

Se realiza una investigación que permita extender el conocimiento actual de las redes GSM. Contribuir al desarrollo de un sistema de comunicaciones de segunda generación viable y económico, sentando las bases de un nuevo sistema que cumpla con las expectativas respecto a este tipo de tecnología.

Por consiguiente, este proyecto forma parte de las tendencias en el estudio de las telecomunicaciones. Se pretende realizar investigación sobre el análisis de nuevas tecnologías GSM.

Este proyecto se enfoca en el proyecto OpenBTS donde se puede montar una red propia micro-célula de cobertura GSM, utilizando hardware no muy costoso y el software libre Asterisk [4] como MSC (Central de conmutación móvil).

Con base a los resultados obtenidos se verifica que este tipo de tecnologías basadas en software libre puede ser útil para brindar cobertura a zonas en donde no se cuenta con ella o en casos de emergencia cuando la red convencional no es funcional.

1.5 ESTRUCTURA DE LA TESIS

En el segundo capítulo se da una descripción del sistema GSM convencional, de manera general se muestra el funcionamiento de la red y partes que la conforman, así como sus características más peculiares y cómo fue su evolución.

En el capítulo tres se realiza una descripción de la capa física de GSM el punto principal de este trabajo de tesis estudiando a detalle como es la señalización, asignación de canales a un usuario y la interfaz de aire por donde viajan las señales que portan la voz y los mensajes de texto.

El capítulo cuatro describe el sistema y la implementación del mismo. Se muestran las etapas y la unión de software y hardware utilizados para obtener la celda celular donde los teléfonos registrados tendrán cobertura.

El capítulo cinco muestra los resultados de los análisis de datos que se obtuvieron de las llamadas de prueba realizadas.

En el capítulo seis se explica en base a los datos que se disponen, las conclusiones del presente trabajo de tesis.

CAPÍTULO 2

ESTADO DEL ARTE

En este capítulo se da una explicación de la importancia del estándar de telefonía GSM, cómo fue su evolución y el porqué de una estandarización que se usaría mundialmente. Aunque su nacimiento no es tan reciente es una tecnología que es usada en todo el mundo hoy en día.

Se presenta un estudio de este tipo de tecnología para evaluar su comportamiento y desempeño para sentar las bases de una tecnología emergente que es una opción atractiva de acceso a comunicaciones móviles de corto alcance. Para lograr lo anterior en este capítulo se describe de manera general el sistema GSM convencional.

Las comunicaciones móviles son actualmente el área de crecimiento más rápido dentro del sector de las telecomunicaciones, especialmente la telefonía móvil celular. Esta investigación se basa en tecnología abierta para tener acceso a una micro-célula GSM.

2.1 ANTECEDENTES [20]

La evolución de los sistemas de telefonía celular empezó a finales de los años setenta con la llamada primera generación (1G) que se basaba en señales analógicas y dispositivos de transmisión relativamente grandes, fue diseñada solamente para transmitir voz donde el enlace era de muy baja calidad y muy lento con una velocidad de 2400 baudios[1] de modo que en un baudio se transmitía un bit, era necesario transmitir más bits por baudio para mejorar la calidad del enlace y brindar servicio a más usuarios.

[1] Baudio: Describe la cantidad de veces que la transmisión cambia de estado (on, off) por segundo. 2400 baudios = 2400 bits por segundo ó bps.

En la década de los ochenta surgió la segunda generación (2G) y reemplazó a la primera generación, el sistema de telefonía celular pasó de analógico a digital. A diferencia del primer sistema (1G) el sistema 2G comienza a transmitir la voz de forma digital y datos empleando protocolos de codificación más sofisticados (GSM) y está basado en los sistemas de telefonía celular actuales.

En general la aparición de una segunda generación de telefonía celular se refiera a una enorme mejora en la tecnología de transmisión utilizada en la primera generación.

GSM son las siglas de *Global System for Mobile Communications* (Actualmente, Sistema Global para las comunicaciones Móviles, aun que originalmente el acrónimo proviene de "*Groupe Spécial Mobile*"), es el sistema de telefonía móvil digital más utilizado y el estándar por defecto para teléfonos móviles.

Definido originalmente como Estándar Europeo Abierto para que una red digital de teléfono móvil soporte voz, datos, mensajes de texto y *roaming* en varios países. GSM es ahora uno de los estándares digitales inalámbricos 2G más importantes del mundo. Según la asociación GSM [5], esta tecnología de segunda generación está presente hasta en 219 países y tiene el 90 por ciento del total del mercado móvil digital.

2.2 TECNOLOGIAS INALAMBRICAS

La comunicación está basada principalmente en la relación entre emisor, mensaje y receptor. Pero la tecnología de hoy en día no solo debe hacer referencia a la transmisión de voz, sino debe intentar abarcar una mayor gama de aplicaciones, llámese la transmisión de datos inalámbricamente.

La popularización de las computadoras personales ha hecho que crezca considerablemente la demanda de sistemas de transmisión de datos por medios inalámbricos que utilizan ondas de radiofrecuencia de baja potencia y una porción del espectro de una banda especifica.

Tipos de Redes Inalámbricas

2.2.1 Redes de Área Local Inalámbrica (Por sus siglas en ingles WLAN, *Wireless Local Area Network*)

Una red LAN se compone por un grupo de computadoras y otros equipos relacionados que comparten un modem inalámbrico (ó una línea de comunicación) y un servidor dentro de un área geográfica por ejemplo un edificio.

2.2.2 Redes de Área Personal Inalámbrica (WPAN, *Wireless Personal Area Network*)

Es una red que conecta todos los teléfonos móviles de la casa y los ordenadores mediante un aparato central vía Bluetooth que cubre un área geográfica pequeña y además conecta dispositivos electrónicos como PDAs, escáner, impresoras, fax, etc.

2.2.3 Redes de Área Extensa Inalámbrica (WWAN, *Wireless Wide Area Network*)

Esta categoría está relacionada con las comunicaciones de voz y datos dentro de una red. La principal característica de estas redes es el área de cobertura. Nos enfocaremos en este tipo de redes que son utilizadas para el servicio de la tecnología móvil.

En el presente estas tecnologías inalámbricas están experimentando mejorías continuamente gracias a los avances en la teoría de las comunicaciones y diseño electrónico.

Desde las décadas de los setenta existen sistemas analógicos de radio para telefonía, pero durante muchos años han tenido un costo elevado para la mayoría de las aplicaciones y un área de cobertura muy escasa. En los últimos años ambos factores han evolucionado de forma drástica, por lo cual hacen posible actualmente considerar los sistemas GSM con Software Libre como una alternativa interesante.

Existen actualmente diversos sistemas de comunicación inalámbrica, todos basados en ondas de radio. La tendencia a la movilidad hace cada vez más sofisticados a estos sistemas y el objetivo es evitar los cables en toda la comunicación no solo en el campo de la telefonía sino también en televisión digital, seguridad, domótica, etc.

La mayoría de los sistemas de comunicación inalámbrica actualmente en uso se basan en el principio de la partición del espacio geográfico en células, de forma que el usuario que se encuentra dentro de una célula se comunica con la estación base correspondiente, cuando el usuario se mueve y pasa a otra célula su comunicación se realiza con la nueva estación base. Para evitar interferencias células contiguas utilizan siempre frecuencias diferentes, pero células no contiguas pueden reutilizar la misma frecuencia. De esta forma es posible cubrir un área más grande utilizando únicamente siete frecuencias.

En realidad cada usuario dentro de una célula ha de utilizar una frecuencia distinta, por lo que lo que no se asignan siete frecuencias sino siete grupos o intervalos de frecuencias.

En este trabajo se tendrá una sola célula, lo relacionado con reutilizar frecuencias no están dentro del alcance de esta tesis.

Parecida a la telefonía convencional, la telefonía celular empezó siendo analógica. Más tarde apareció la telefonía celular digital, que ya ha desplazado prácticamente en su totalidad a la analógica. Entre las ventajas de la telefonía celular digital frente a la analógica podemos destacar las siguientes:

- La calidad de la comunicación es mejor, ya que pueden incorporarse mecanismos de corrección de errores. Si hay cobertura la calidad es buena, si no la hay no es posible interactuar con la red.

- Las conversaciones pueden encriptarse, así se logra privacidad en la comunicación.

- Es posible incluir más conversaciones en un mismo ancho de banda.

- Es posible transmitir por el mismo sistema voz y datos con una velocidad mayor.

Las ondas de radio revelaron desde hace mucho tiempo que son un medio eficaz para establecer comunicaciones con puntos móviles, aunque tiene obstáculos que afectan la fuerza con la que es propagada la señal aun así es muy viable su uso.

2.3 GSM [21]

GSM Sistema Global para Comunicaciones Móviles es un estándar de segunda generación de telefonía celular, lo desarrollo el Instituto Europeo de Normas de Telecomunicaciones (Por sus siglas en Ingles, ETSI, *European Telecommunications Standards Institute*) y ahora propiedad actualmente por el Proyecto Asociación de Tercera Generación (*3GPP, 3rd Generation Partnership Project*), es un sistema digital y es usado en casi todo el mundo, permite su uso en cualquier lugar con cobertura, incluso en áreas internacionales con equipos que sean compatibles con este estándar.

GSM opera en diferentes bandas de frecuencia debido a la diferente disponibilidad del espectro en diferentes países y zonas geográficas. En los 800 MHz (Opera en

Sudamérica y Asia), 900 y 1.800 MHz (Europa y la más extendida) y 1900 MHz (Solo opera en Norteamérica), GSM utiliza modulación digital para mejorar la calidad de la voz, pero los servicios que ofrece la red son limitados, mas delante se describe la modulación GMSK.

Mientras la demanda por los usuarios de celulares aumentaba, los proveedores de 2G continuaban mejorando la calidad de transmisión y la cobertura. Estos también comenzaron a ofrecer servicios adicionales, como fax, mensajes de textos y buzón de voz.

2.4 ARQUITECTURA DE GSM [7]

En este apartado se presentan las entidades e interfaces que constituyen el sistema GSM, describiendo su funcionalidad y las relaciones entre ellas, para poder tener una idea de la estructura física del sistema ya que es la base para diseñar e implementar nuestra propia red GSM.

El sistema GSM se divide en 4 subsistemas:

- Estación Móvil (MS*, Mobile Station*)
- Subsistema de Estación Base (BSS, *Base Station Subsystem*)
- Subsistema de Conmutación y Red (*NSS, Network Subsystem*)
- Subsistema de Soporte y Operación (OMC, *Operation Maintenance Center*)

2.4.1 Estación Móvil

Este subsistema hace referencia a los usuarios de la red (abonados). A su vez la estación móvil consta de 2 partes físicas; el teléfono celular el cual es un elemento de hardware y la tarjeta SIM (Subscriber Identity Module) la cual es un chip inteligente que identifica a un único suscriptor.

El teléfono celular junto con la tarjeta SIM insertada en el mismo permite el acceso a la red a través de la interfaz de radio y realiza las funciones necesarias para soportar el canal físico entre la Estación Móvil y la Estación Base Transceptora (BTS). En general se encarga de la transmisión, control de los canales de radio y codificación/decodificación de la voz.

La tarjeta SIM es la que proporciona la movilidad al suscriptor ya que el usuario puede tener acceso a los servicios de la red que tiene contratados independientemente del terminal. Esta tarjeta contiene toda la información relacionada con el suscriptor, siendo la información más importante; número de serie, IMSI *(International Mobile Subscriber Identity*), clave de algoritmo de autenticación. Sin un SIM el teléfono móvil no es funcional por qué no puede hacer uso de la red.

2.5 SUBSISTEMA DE ESTACION BASE (BSS)

El subsistema de estación base se conforma de los siguientes elementos:

2.5.1 Estación Base Transceptora (BTS, *Base Transceiver Station*)

Una estación base es básicamente la antena emisora/receptora que se encarga de propagar las señales en la interfaz de radio para dar cobertura a los suscriptores.

La interfaz de radio entre la Estación Móvil y la Estación Base es la interfaz Um y es la más importante de la red ya que es utilizada por las Estaciones Móviles para acceder a todos los servicios y utilidades que se tengan disponibles o contratadas en el sistema GSM.

La interfaz que conecta a las estaciones base con su controlador (BSC) se denomina interfaz Abis.

2.5.2 Controlador de Estación Base (BSC, *Base Station Controller*)

Se encarga de gestionar la localización de los canales de tráfico y de la gestión *handover, frequency hopping* (salto en frecuencia) y los controles de las frecuencias de radio de los BTS. Es responsable de asignar y desasignar canales para la transmisión, además mantiene la continuidad y la potencia con que las Estaciones Base transmiten para evitar interferencias.

La interfaz entre el controlador BSC y el conmutador MSC se denomina interfaz A.

2.6 SUBSISTEMA DE RED Y CONMUTACION (NSS)

El subsistema de red y conmutación es el que se encarga de administrar las peticiones de comunicación que se realizan entre un usuario llamante y el usuario llamado es decir se encarga de la gestión de la movilidad, interconexión con otras redes y control del sistema.

Este subsistema consta de varios elementos:

2.6.1 Centro de Conmutación Móvil (MSC, *Mobile Switching Center*)

Es una central de conmutación digital, realiza la función de conmutación telefónica del sistema y controla las llamadas desde y hacia otros teléfonos. Proporciona acceso a los derechos de los suscriptores, se encarga de la gestión de la movilidad de los abonados y en la localización de su ubicación dentro de la red y también en el suministro de los servicios ofrecidos por la red.

2.6.2 Gateway del Centro de Conmutación Móvil (GMSC*, Gateway Mobile Switching Center)*

El Gateway del Conmutador es un dispositivo traductor que se conecta con una red externa y hace la función de puerta de enlace para que los protocolos de comunicaciones que existen en redes diferentes se entiendan y exista la comunicación.

2.6.3 Registro de Localización Local (HLR, *Home Location Register*)

Es una base de datos donde se encuentra la información de los usuarios de la red, tales como el perfil del servicio, la ubicación del usuario, estado de actividad de un abonado. Describe detalladamente el contrato que tiene el suscriptor y los servicios a los que tiene acceso.

Cuando un abonado requiere algún tipo de servicio de red envía la información que contiene en su tarjeta SIM y el HLR reconoce al abonado, de esta forma, le permite al usuario hacer uso de la red.

2.6.4 Registro de Localización de Visitantes (VLR, *Visitor Location Register*)

Es otra base de datos que contiene información de los abonados que están de visita (de paso) por la red, esta información consta de los registros donde se encuentra localizado el usuario. Esta información es transferida desde el HLR cuando un abonado accede a una red visitada mediante un procedimiento de actualización de ubicación y es necesaria para poder tener servicio de Roaming[2].

2.6.5 Centro de Autenticación (AUc, *Authentication center*)

Es un proceso de comprobación de identidad para suscriptores que se efectúa al solicitar algún tipo de servicio ofrecido por la red GSM. En primera instancia la red solicita al abonado proporcione su identidad y cuando el sistema valida al abonado el terminal móvil queda registrado en la red y se le permite el acceso a los servicios solicitados.

2.6.6 Registro de Identidad de Equipo (EIR, *Equipment Identity Register*)

Es una base de datos que se encarga de permitir a terminales móviles hacer uso de la red. Es una medida de seguridad para restringir el acceso a la red a terminales no autorizadas o robadas. Este elemento del subsistema controla el acceso a la red.

2.7 SUBSISTEMA DE SOPORTE Y OPERACIÓN (OMC)

Este subsistema es el responsable del mantenimiento, operación y la explotación de la red, también se encarga de la gestión de los equipos móviles y de la gestión y cobro de las tarifas.

[2] Roaming es cuando un abonado utiliza un teléfono móvil a través de una red de comunicaciones de un país extranjero.

Cada uno de los subsistemas de la red tiene sus operaciones en las cuales se realizan todas las funciones que el sistema GSM proporciona. Las funciones relacionadas con el proceso de llamadas y abonados se encuentran implementadas en el sistema de conmutación MSC, mientras que las funciones relacionadas con la parte radio se encuentran en el sistema de estaciones base BSS, todo ello esta supervisado por el sistema de operación y mantenimiento OMC véase figura 2.1.

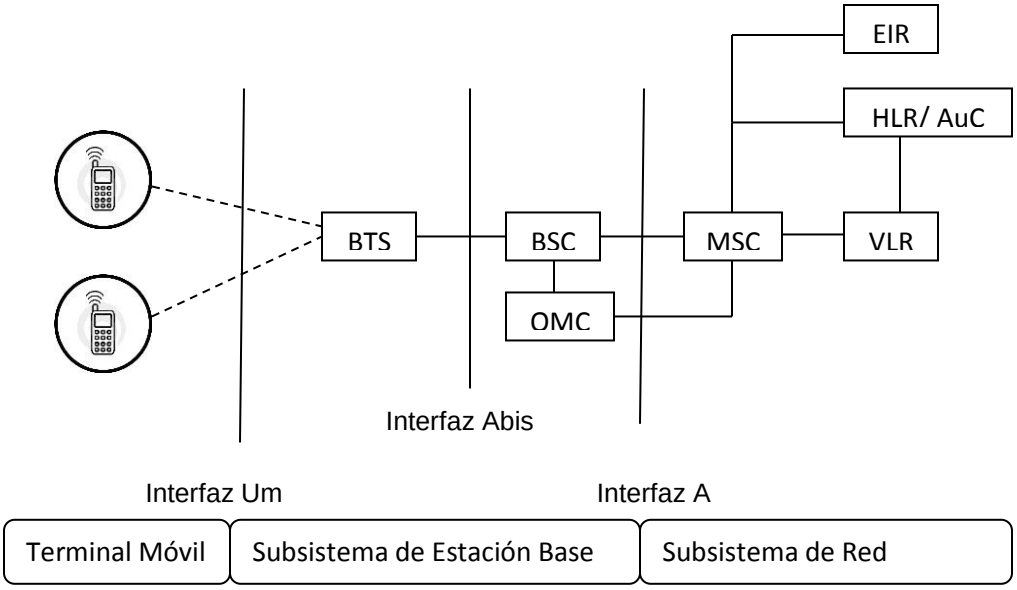


Figura 2.1 Arquitectura Básica de la red GSM.

CAPITULO 3

CAPA FISICA DE GSM

INTRODUCCION

En este capítulo se describe la capa física de radio, la técnica de modulación y de acceso GSM, cómo se organiza en términos de canales, etc.

La capa física es la que define los mecanismos y las características físicas del medio para hacer posible la comunicación en un canal de radio desde una estación móvil hasta su estación base y viceversa.

Estos mecanismos incluyen la modulación, el control de potencia, la codificación y administra el establecimiento y mantenimiento del radio canal. Además soporta todas las funciones necesarias para la transmisión de una secuencia de bits sobre un canal de radio en un medio físico de transmisión.

3.1 Capa Física GSM

Los flujos de bits en la interfaz de radio se transfieren en canales de tráfico, en forma de paquetes de datos y canales de control definidos, la transmisión de estos flujos de bits en el medio físico se describe en la recomendación GSM 04.03 [6].

El sistema GSM utiliza 2 métodos de acceso, Acceso Múltiple por División de Tiempo (TDMA, *Time Division Multiple Access*) y Acceso Múltiple por División de Frecuencia (FDMA, *Frequency Division Multiple Access*). Las frecuencias se usan como canales divididos en ranuras de tiempo llamadas TS (*Time Slots*). A un grupo de estas ranuras

(slots) se le denomina *Frame*. Estos frames a su vez son agrupados para formar multiframes, superframes e hyperframes.

Este arreglo de frames es la base de la estructura física. Los frames son enumerados, esta numeración va desde 1 hasta N frames y entonces la secuencia vuelve a iniciar desde 1. Los números que identifican a un frame con un número de slot de tiempo forman una identidad física. Para realizar esto, la estación móvil (MS) necesita saber el número de frame y el número de slot de tiempo, esto se realiza mediante la transmisión de todos los bits cero “0” (o puede ser conocida una secuencia de bits) en una de las ranuras de tiempo de un frame, esto es una especie de marcador. Los bits cero significan patrón constante modulado y así ayudan a la Estación Móvil a identificar la frecuencia correcta. Hablando en términos utilizados para GSM, la frecuencia correcta es llamada “Canal de Corrección de Frecuencia” (más adelante se explican los canales principales que usa GSM para la transmisión).

3.1.1 Interfaz Um

En esta interfaz (que es la más importante de la red) el multiplexado en la frecuencia divide en 373 canales cada uno de 200 kHz de ancho de banda (canales numerados desde 512 hasta 885), también separa dos bandas de frecuencia desde 1710 hasta 1784 MHz (Transmisión de terminal móvil a estación base, transmisión llamada uplink) y de 1805 a 1879 MHz (Transmisión de estacón base a terminal, transmisión llamada downlink).

El multiplexado en el tiempo hace que un canal de transmisión tenga 8 comunicaciones diferentes.

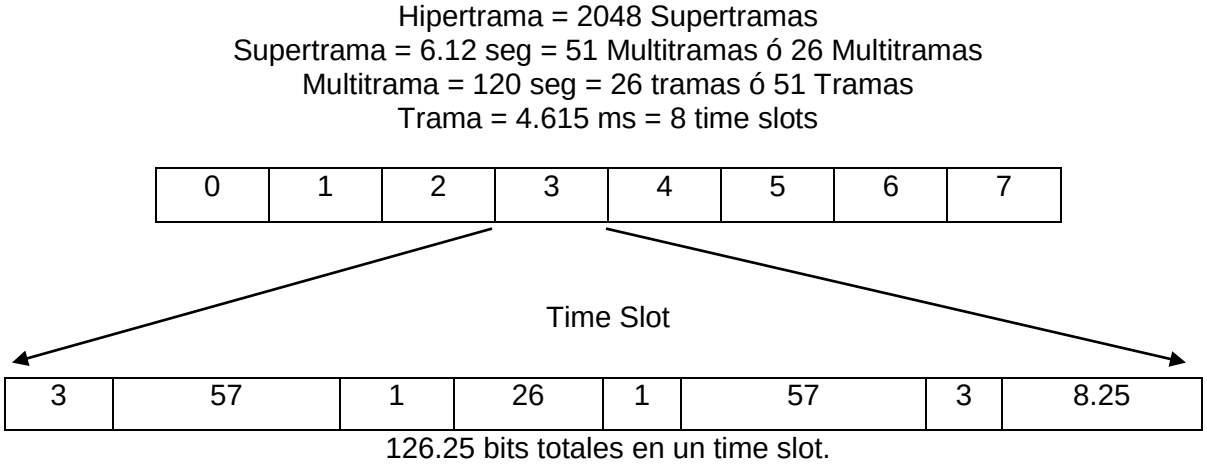
Un frame se divide en 8 intervalos de tiempo con una duración de 577 µs. Cada intervalo constituye un radio canal de comunicación en el cual se transmiten paquetes (conjunto estructurado de bits de forma que se puedan transmitir en el aire) periódicamente. Una trama frame dura 4.615 ms, de esta forma el multiplexado en el tiempo optimiza la utilización de la capacidad de un radio canal.

3.2 Estructura del frame (trama)

En GSM gracias al multiplexado en el tiempo los usuarios comparten un mismo canal mediante la asignación de Slots de Tiempo (time slots) cada uno tiene una duración de 577 µs cada usuario puede volver a utilizar el canal después de 8 slots, es decir mientras ya haya transmitido su información, después de 4.615 ms.

Ocho de los intervalos de tiempo se agrupan para formar una trama que dura aproximadamente 4.615 ms y forma la unidad básica para la definición de los canales lógicos.

Estas tramas TDMA se agrupan en 26 o 51 unidades para formar una multitrama. La multitrama-26 se utiliza básicamente para transmitir los canales de trafico TCH, mientras que la multitrama-51 se usa para los canales de control BCCH, CCCH, SDCCH y SACCH. Estas multitramas a su vez se agrupan para formar supertramas (1326 tramas que dura 6.12 segundos) e hipertramas (2048 supertramas que dura 3 horas, 38 minutos 53 segundos y 760 milisegundos).



3: Cabecera	1: Bits de control
57: Bits de datos	57: Bits de datos
1: Bits de control	3: Fin de trama
26: Secuencia de entrenamiento	8.25: Bits de guarda

Figura 3.2.1 Estructura del Frame GSM [7].

3.3 Radio Canal de Frecuencia

GSM utiliza FDD y la combinación TDMA y FDMA detalles de estas características se especifican en [13] para proporcionar a los terminales y las estaciones base un acceso múltiple. Las bandas de frecuencia se dividen en canales de 200 kHz llamados ARFCN *(Absolute Radio Frecuency Channel Number,* Numero de canal de radiofrecuencia absoluto). EL ARFCN define un par de canales *uplink* y *downlink* separados por 95 MHz y cada canal es compartido en el tiempo por hasta 8 usuarios usando TDMA. Cada uno de los 8 usuarios utiliza el mismo ARFCN y ocupa un único slot de tiempo por trama.

Se denomina canal físico a cada uno de los ocho intervalos temporales en que se divide un radiocanal de 200 KHz. Si una estación base tiene N radiocanales (N frecuencias portadoras), puede ofrecer 8xN canales físicos.

Un canal físico se puede dividir a su vez en diferentes bloques lógicos que se utilizan con fines distintos. Cada una de estas divisiones es un canal lógico. Los canales lógicos pueden ser de dos tipos: de tráfico (transportan datos de usuario) o de señalización y su contenido (información) es el que se inserta sobre los canales físicos

En la siguiente sección se listan todos los tipos de canales y se describe la función que tiene cada uno.

3.4 Tipos de Canales.

GSM define una serie de canales lógicos que están disponibles ya sea en un modo de acceso aleatorio no asignado o en un modo dedicado asignado a un usuario específico. Los canales lógicos se dividen en dos categorías (Figura 3.4.1.1) canales de tráfico y canales de señalización (o de control).

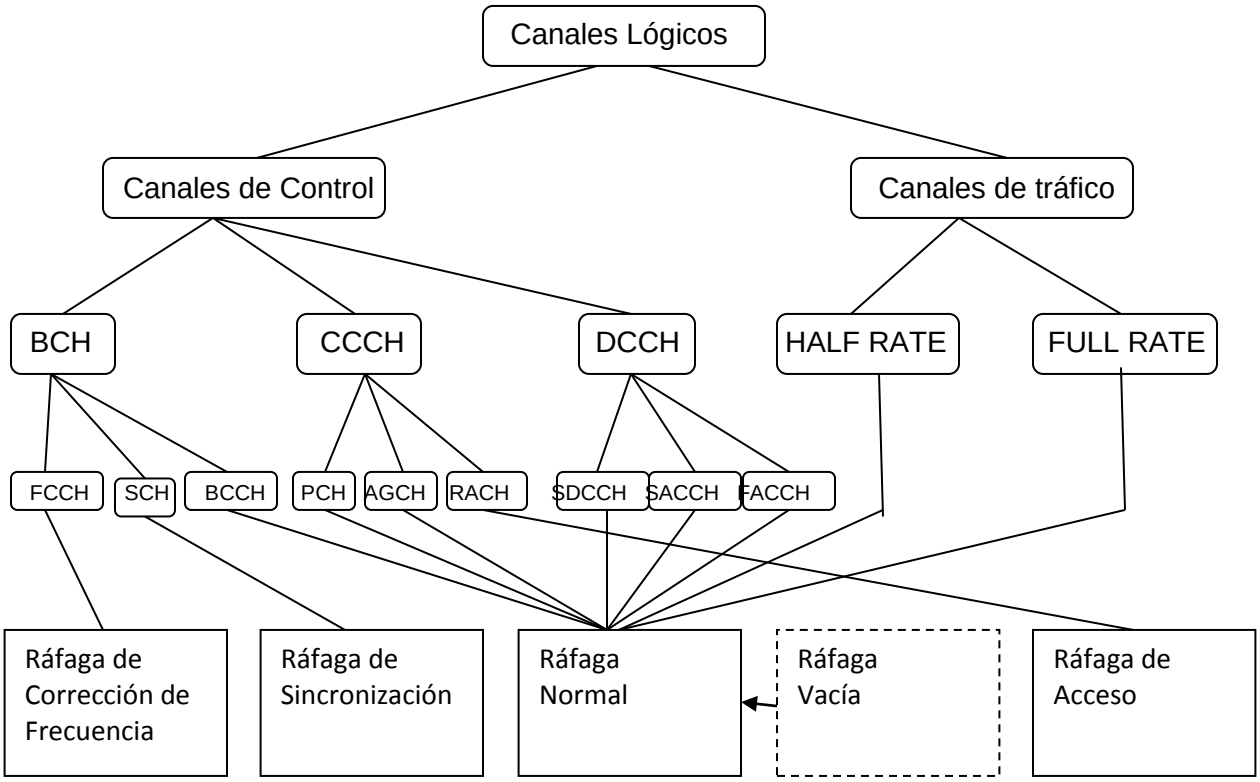


Figura 3.4.1.1 Categorías de los Canales Lógicos [8].

3.4.1 Canales de Difusión (BCH, *Broadcast Channels*)

Estos canales se utilizan para enviar información general desde la estación base hacia todas las estaciones móviles dentro de una célula.

Canal de Corrección de Frecuencia (FCCH, *Frequency Correction Channel*)
Canal de adquisición de frecuencia para detección de la portadora de difusión.

Canal de Sincronización (SCH, *Synchronization Channel)*
Permite que el terminal móvil adquiera la trama que le corresponde.

Canal de Control de Difusión (BCCH, *Broadcast Control Channel*)
Difunde información en el enlace descendente (downlink) para que las estaciones móviles conozcan los parámetros de la estación base y puedan operar.

3.4.2 Canales de Control Común (CCCH, *Common Control Channels*)

Sirven para comunicar una estación móvil con la red en cuanto a intercambio de información, solicitud de un canal dedicado y confirmación del canal asignado por la red.

Canal de Búsqueda (PCH, *Paging Channel*)
Se encarga de localizar móviles y alertarlos de llamadas entrantes y llegada de mensajes SMS.

Canal de Acceso Aleatorio (RACH, *Random Access Channel)*
Este canal es empleado por los móviles cuando necesitan acceder a la red.

Canal de Concesión de Acceso (AGCH: *Access Grant Channel)*
Concede acceso a los móviles que quieren establecer una comunicación

3.4.3 Canales de Control Dedicado (DCCH, *Dedicated Control Channels*)

Son canales bidireccionales de señalización que son asignados a las estaciones móviles para que el móvil pueda establecer y liberar una llamada.

Canal de Control Dedicado Independiente. (SDCCH, *Stand Alone Dedicated Control Channel)*
Intercambia información de la estación móvil con la estación base: Encendido apagado del móvil, actualización de posición señalización para establecimiento de llamada, envió y recepción de mensajes cortos SMS.

Canal de Control Lento Asociado
(SACCH, *Slow Associated Control Channel)*
*T*ransmite información para cuestión de la movilidad y recursos de radio, medidas de calidad.

Canal de Control Asociado Rápido
(FACCH, *Fast Associated Control Channel)*
Utiliza el modo robado, se roba bits de las tramas de tráfico y se utiliza para hacer un traspaso (handover).

Canal de Difusión de célula (CBCH, *Cell Broadcast Channel*)
Se usa para transportar el servicio de difusión de mensajes cortos.

3.4.4 Canales de Tráfico (TCH, *Traffic Channels*)

Se usan para transportar la voz y los datos.

Un canal de tráfico de tasa completa (TCH/F*: Full rate*) ocupa un slot por trama a una velocidad de transmisión de 22.8 kbps

Un canal de tráfico de tasa media (TCH/H: *Half rate*) ocupa aproximadamente un slot cada 2 tramas a 11.4 kbps.

3.5 Tipos de Ráfagas (burst)

Una ráfaga es la secuencia de bits que se transmiten en un periodo de tiempo (time slot). Esta ráfaga corresponde a una duración de 156.25 bits. La ráfaga se compone de varios campos compuestos de parte útil, que es la que transporta la voz o datos y una parte de guarda que permite que no se solapen los datos de las ráfagas adyacentes.

Existen 5 tipos de ráfagas según el tipo de canal al que pertenezca.

- Ráfaga Normal

Este tipo de ráfaga es la más utilizada y sirve para transportar la información en canales de control en los respectivos canales TCH y DCCH tanto para el uplink y downlink.

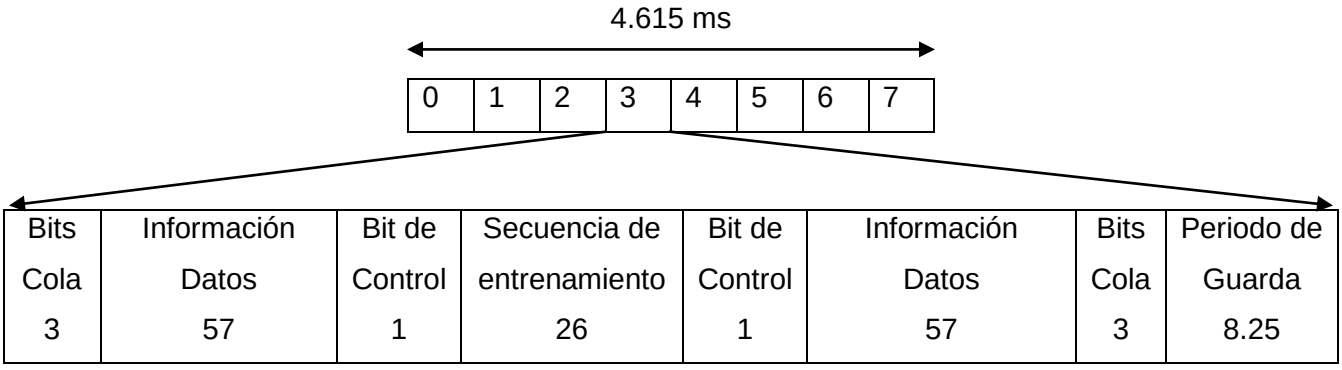


Figura 3.5.1 Ráfaga Normal.

- Ráfaga de Corrección de Frecuencia

Se usa en el enlace descendente (downlink) para la sincronización de frecuencia en el móvil y permite encontrar el canal de difusión BCH.

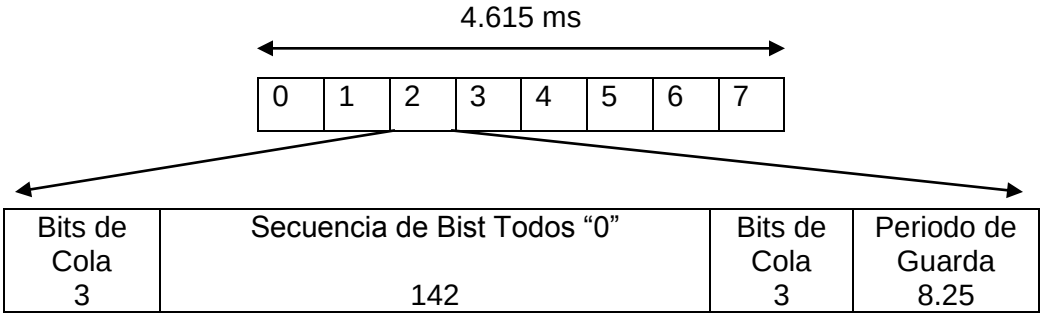


Figura 3.5.2 Ráfaga de Corrección de Frecuencia.

- Ráfaga de Sincronización

Se utiliza para la sincronización temporal del móvil con la estación base, se utiliza en el downlink y es necesaria para poder recibir información.

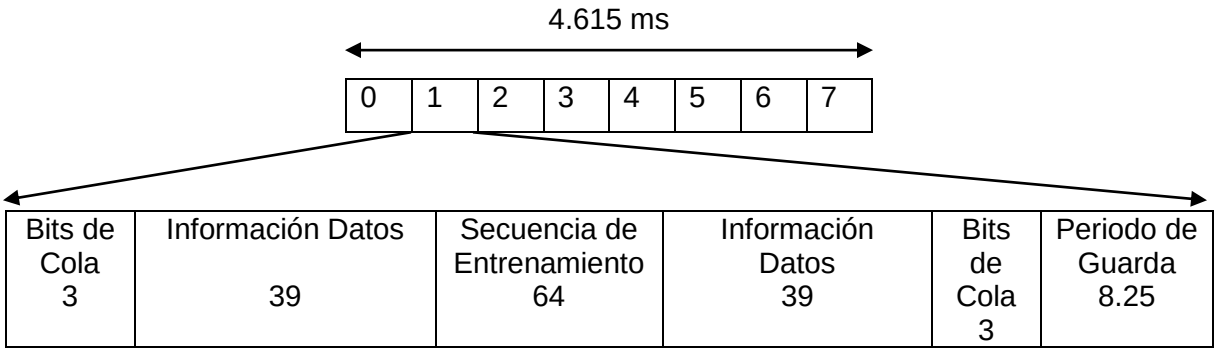


Figura 3.5.3 Ráfaga de Sincronización

- Ráfaga de Acceso

Es más corta de las demás ráfagas y es usada por el móvil para acceder al sistema solo en el enlace uplink.

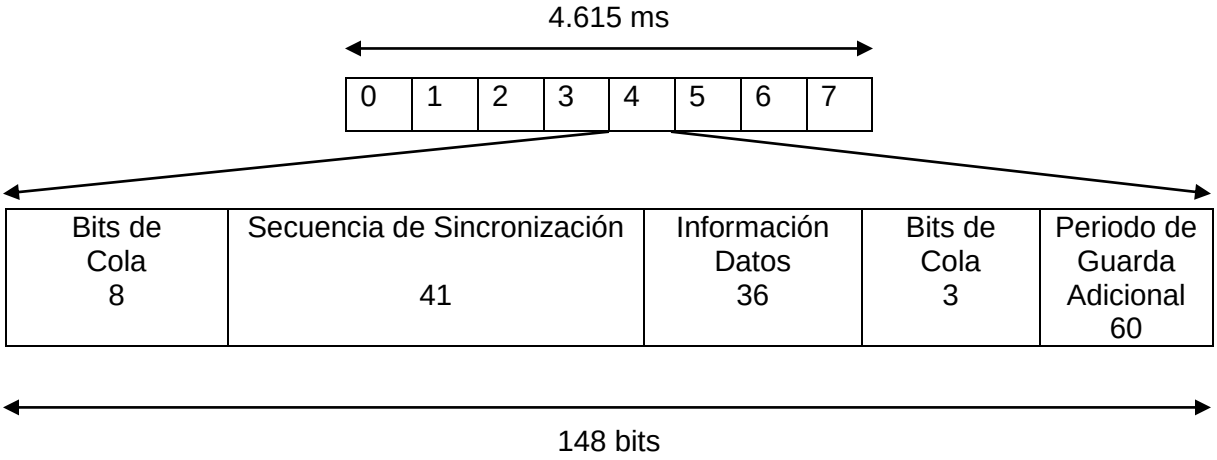


Figura 3.5.4 Ráfaga de Acceso

- Ráfaga de Relleno

Se envía cuando no hay información a ser transmitida

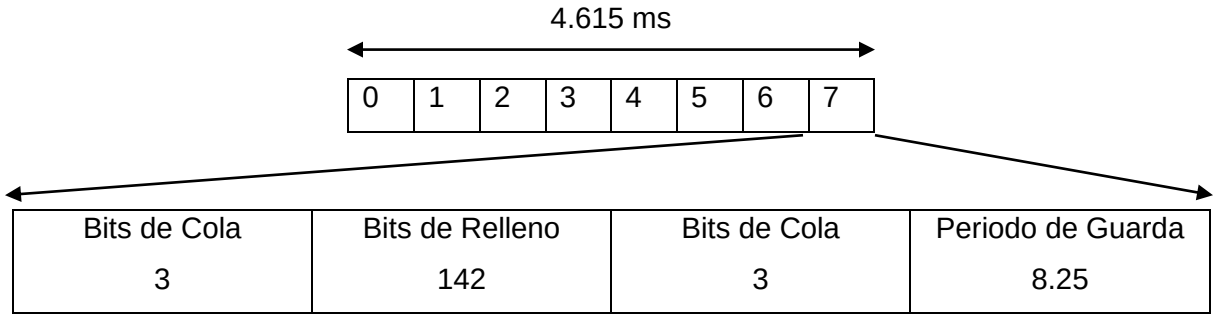


Figura 3.5.5 Ráfaga de Relleno

3.6 Modulación GMSK

La señal empleada en GSM se modula digitalmente utilizando la modulación GMSK (*Gaussian Minimum Shift Keying*, Modulación por desplazamiento mínimo gaussiano). Se trata de una modulación de fase, en la que la señal moduladora se filtra con un filtro gaussiano. De este modo se consigue que la mayor parte de la señal modulada quepa en menos de 200 KHz. Gracias a esto, la canalización en GSM se realiza en radiocanales de 200 KHz de ancho de banda.

La ventaja de esta modulación es que minimiza las transiciones de fase de la señal durante la transmisión y así reduce el ancho de banda necesario. Sin embargo la duración del pulso a la salida del filtro gaussiano es mayor que el tiempo de un bit lo que ocasiona interferencia entre símbolos.

Las transmisiones de radio se hacen a una velocidad de 270.833 kbps usando modulación digital binaria GMSK con BT=0.3. El BT es el producto del ancho de banda del filtro por el periodo de bit de transmisión. Por lo tanto la duración de un bit es de 3.692 µs, y la velocidad efectiva de transmisión de cada usuario es de 33.854 kbps (270.833 kbps/8 usuarios, aproximadamente). Con el estándar GSM, los datos se envían actualmente a una velocidad máxima de 24.7 kbps. Cada Time Slot tiene un tamaño equivalente en un canal de radio de 156.25 bits, y una duración de 576.92 µs y una trama TDMA simple en GSM dura 4.615 ms como se vio al principio de este capítulo. El número de total de

canales disponibles dentro de las bandas (uplink y downlink) de 75 MHz es de 374 (de 200 KHz de ancho de banda cada una) asumiendo que no hay ninguna banda de guarda. Este es un dato teórico y en la práctica el número de canales de tráfico es menor ya que son necesarias bandas de guarda y de control para que el sistema ofrezca un buen servicio.

3.7 Señalización en GSM

La señalización en GSM describe las comunicaciones entre el teléfono móvil y la red. La señalización tiene que ser llevada a través de la red mediante la interfaz de aire al móvil. Diferentes protocolos son usados a través de diferentes interfaces.

Toda la señalización de GSM está basada en el modelo de referencia OSI (*Open System Interconnection*, Interconexión de Sistemas Abiertos). Este modelo esta reducido a 3 capas como se muestra en la figura 3.7.1.

En este caso solo se estudia la señalización en la inetrfaz Um ya que es la utilizada por OpenBTS para llevar a cabo la comunicación mediante la interfaz de aire que despliega el sistema.

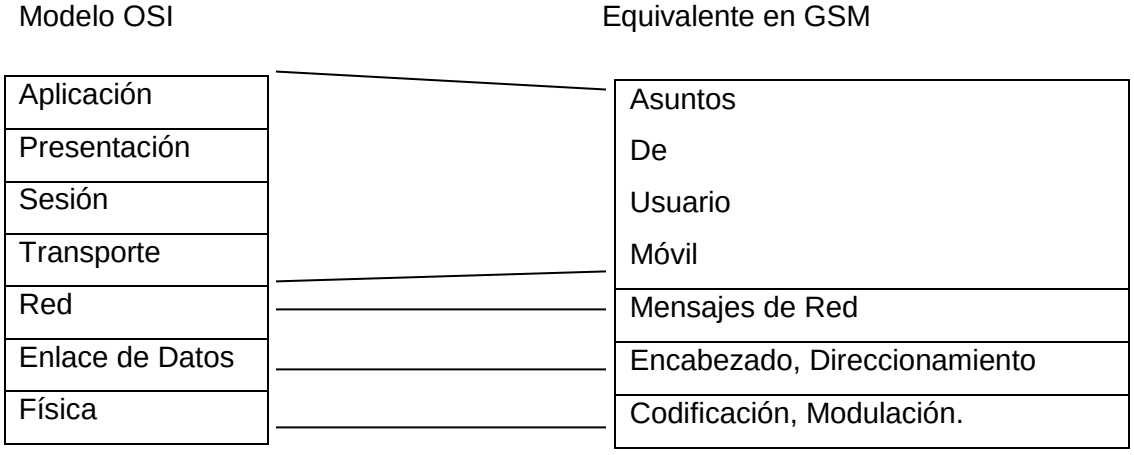


Figura 3.7.1 Relación del Modelo OSI en Capas de GSM.

3.8 Flujo de la información y protocolo stack de GSM.

Capa 3, Lleva los mensajes de señalización, para hacer llegar el mensaje a su destino. Proporciona conexión orientada (enlace de señalización dedicado) o servicios sin

conexión (tipo de paquetes de señalización). Ejemplo: mensaje de Recursos de Radio enviado desde el Centro de Conmutación Móvil, MSC al Controlador de Estación Base, BSC.

Capa 2, Transfiere frames libres de errores entre nodos. Considerando la detección de errores, encabezados, retransmisiones. Ejemplo: Protocolo LAPD en A-bis entre el Controlador de Estación Base, BSC y la Estación base Transceptora, BTS.

Capa 1, Transmite toda la información a través del medio físico. Especifica el medio físico utilizado: mecánicas, eléctricas, funcionales y características de procedimiento. Ejemplo: La modulación GMSK, en RF la antena pone en la interfaz de aire la señal a transmitir entre la Estación Base Transceptora, BTS y la Estación Móvil, MS.

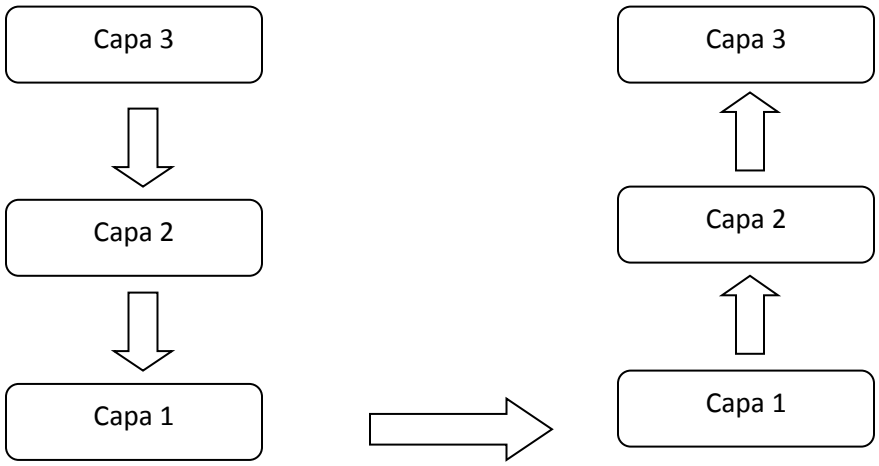


Figura 3.8.1 Flujo de Información por Capas en GSM.

Capa 1: Realiza funciones requeridas para transferir el flujo de bits en los canales físicos TDMA/FDMA.

Capa 2: Proporciona un enlace de señalización segura entre el teléfono móvil y la red. El protocolo está basado en LAPDm de ISDN.

Capa 3: Cuida el control principal de los procesos del teléfono móvil en la red. Se divide en 3 subcapas:

Administración de los recursos de radio. *RR Radio Resource Management.*

- Enruta los mensajes a los canales correctos.
- Establece y mantiene conexiones físicas para los canales de control y de tráfico.

Administración de la movilidad. *MM Mobility Management*.

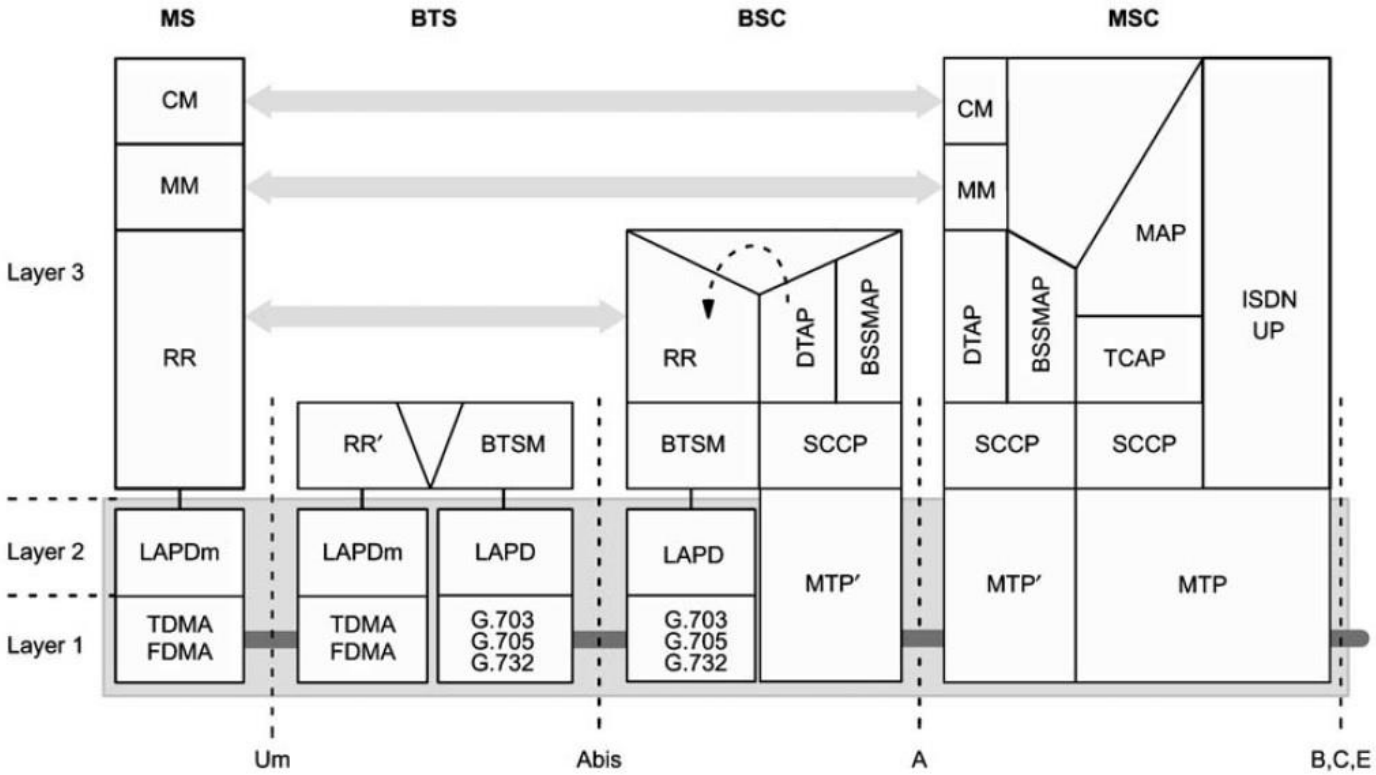
- Controla la autenticación y administración de la seguridad
- Proporciona servicios para la capa administración de conexión.

Administración de conexión. *CM Connection Management.*

- Control de llamada (*Call Control*) es el control responsable de establecer, mantener y liberar llamadas.
- Servicios suplementarios (*SS Supplementary Services*) datos, usuario ocupado, buzón de voz.
- SMS: Short Message Servicios, servicio de mensajería corta.

Capa 1	Capa 2	Capa 3
Cifrado	Encabezados	Administración de recursos de radio.
Configuración de sincronización	Direccionamiento	Administración de movilidad
Codificación de canal	Corrección de errores	Administración de conexión.
Mapeo de los canales lógicos en canales físicos		

La figura 3.8.2 muestra las entidades esenciales de la pila de protocolos de señalización en GSM. Se observan las conexiones con las distintas interfaces que componen la arquitectura convencional de GSM. Más adelante se analizara la parte que nos interesa que es la pila de protocolos de la interfaz Um, los protocolos más importantes se mencionaron anteriormente, los protocolos restantes son definidos en software que vienen junto con la instalación de OpenBTS.



CM	*Connection Management*
MM	*Mobility management*
RR	*Radio Resources management*
LAPDm	*Link Protocol*
BTS Base	*Transceiving Station Management*
BSSMAP	*Base Station System management Application Part*
DTAP	*Direct Transfer Application Part*
SCCP	*Signaling Connection Control Part*
TCAP	*Transaction Capabilities Application Part*
MTP	*Message Transfer Part*
MAP	*Mobile Application Part*
UP	*User Part*

Figura 3.8.2 Pila de Protocolos de GSM para Señalización Extraído de [8].

CAPITULO 4

DESCRIPCION DEL SISTEMA

INTRODUCCION

En este capítulo se presenta la descripción general del sistema, cómo es que se seleccionaron los recursos de software para usarlos en una computadora personal y en conjunto con los recursos de hardware para implementar el sistema y poder desplegar una interfaz de radio (interfaz Um) GSM.

4.1 Radio Definido por Software SDR

Es una técnica en la cual todo el procesamiento se hace en software. Este procesamiento se refiere a la mezcla de frecuencias, filtrado, modulación, demodulación…

Es una tecnología emergente que tuvo sus inicios hace una década. Su nombre *Software Defined Radio* es usado para diseñar radios que son implementados en gran parte basados en software. Esos radios son reconfigurables a través de actualizaciones que se tengan disponibles en los repositorios.

El software puede ser usado para implementar diferentes esquemas de modulación y diferentes estándares pueden ser implementados en el mismo dispositivo. En este caso se está trabajando con GSM. Y otros temas que se desarrollan que emplean SDR están abordando el estándar wifi.

El software es actualizado, por tal razón el dispositivo no se vuelve obsoleto con el tiempo.

El hardware de radio separa los dispositivos, antenas, transceptores. Mientras que el SDR se transforma en un solo dispositivo para muchas funciones.

Hardware necesario: Antena y USRP (*motherboards y daughterboards*).

Herramientas de SDR

GNU Radio: Proporciona bloques para procesamiento de señales para implementar radios por software. La filosofía de GNU Radio es conectar bloques de procesamiento de señales a través de gráficos. El núcleo del software GNU Radio está escrito en C ++, pero el gráfico se describe en Python, un lenguaje de script[3].

4.2 *Hardware Ettus Research USRP-N210*

USRP (*Universal Software Radio Peripheral*, Software Universal de Radio Periférica) es un dispositivo desarrollado por *Ettus Research LLC* [2]. El cual tiene como propósito convertir una computadora en plataformas flexibles de SDR. Ofrece ancho de banda suficiente para soportar transmisiones en banda base digital. Proporciona un canal digital con toda la modulación y demodulación en software en una computadora personal.

El USRP, Software Universal de Radio Periférica es montado sobre un equipo de hardware que genera varios tipos de señales de radio. Este dispositivo junto con OpenBTS se emplean para enviar y recibir las transmisiones entre la estación base y el teléfono móvil.

[3]Un script es un lenguaje que no necesita ser compilado, una maquina servidor puede interpretar el código fuente y ejecutarlo.

Los beneficios de este dispositivo abarcan: usuario, fabricante, sistemas de acceso inalámbrico, interoperabilidad, consideración de espacio, consideración de potencia.

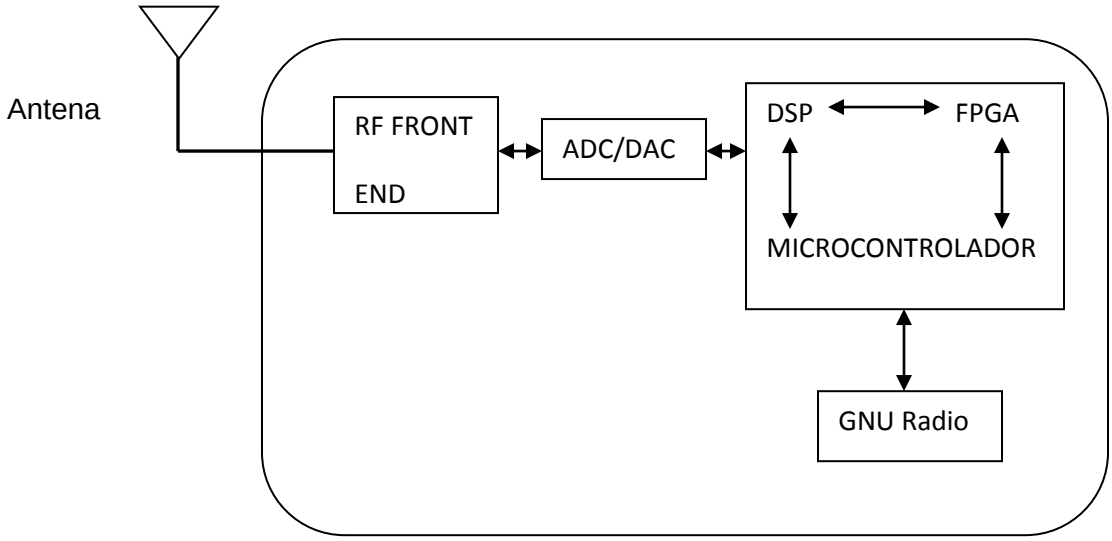


Figura 4.2.1 Diagrama de Bloques USRP [10]

Principales características del modelo USRP N210 [2]:

- 50 MHz de ancho de banda con muestras de 8 bits
- 25 MHz de ancho de banda con muestras de 16 bits
- Conectividad Gigabit Ethernet
- Soporta conexión MIMO – Requiere 2 o más dispositivos USRP N210.
- Procesamiento FPGA en la misma tarjeta madre
- FPGA: Xilinx Spartan XC3SD3400A
- Convertidores Analógico-Digital/Digital-Analógico 14-bits 100 MS/s
- Capaz de conectar un reloj externo de 5 o 10 MHz de referencia
- TCXO Frecuencia de Referencia
- Opcional GPS interno.

4.2.1 *Motherboard (*Tarjeta Madre)

El corazón del Hardware USRP es la tarjeta madre (motherboard) que contiene convertidores analógico-digital (ADC), convertidores digital-analógico (DAC) y antenas. La motherboard está basada en FPGA (Field Programable Gate Array) que permite realizar diferentes configuraciones de hardware, y tarjetas auxiliares o hijas (*daughterboards*) que son las encargadas del manejo de radiofrecuencia con un rango de operación que va desde DC hasta 6 GHz.

4.2.2 *Daughterboards* (tarjetas hijas)

Existen diversos tipos de tarjetas secundarias que se encuentran actualmente en el mercado. A continuación se mencionan algunas de ellas y las principales características de aquellas placas que fueron elegidas para este trabajo por su rendimiento y servicios que ofrecen.

En muchos casos, para la selección de una placa hija (daughterboard) RF se deben tomar en cuenta los requisitos de la aplicación para la cobertura de frecuencia que se desee. En este caso de la aplicación GSM como OpenBTS se suelen utilizar las frecuencias de 900 MHz y 1900 MHz bandas de telefonía celular. Para cubrir estas bandas, tanto las placas WBX, SBX, RF1800 son buenas opciones.

La posible gama de frecuencias de funcionamiento es muy modular (desde DC a 5,9 GHz), dependiendo de las tarjetas hijas disponibles de la siguiente lista:

- BasicRX: 1-250 MHz Receptor
- BasicTX: 1-250 MHz Transmisor
- LFRX: DC to 30 MHz Receptor
- LFTX: DC - 30 MHz Transmisor
- WBX: 50 - 2.2 GHz Transceptor
- SBX: 400 – 4400 MHz Transceptor
- RFX900: 750-1050 MHz Transceptor
- RFX1200: 1150-1450 MHz Transceptor
- RFX1800: 1.5-2.1 GHz Transceptor
- RFX2400: 2.3-2.9 GHz Transceptor
- XCVR2450: 2.4-2.5 GHz and 4.9-5.9 GHz dual-band Transceptor

El equipo de trabajo con el que se despliega la interfaz de aire es un dispositivo Ettus Research N210 y se eligió una tarjeta hija RFX1800.

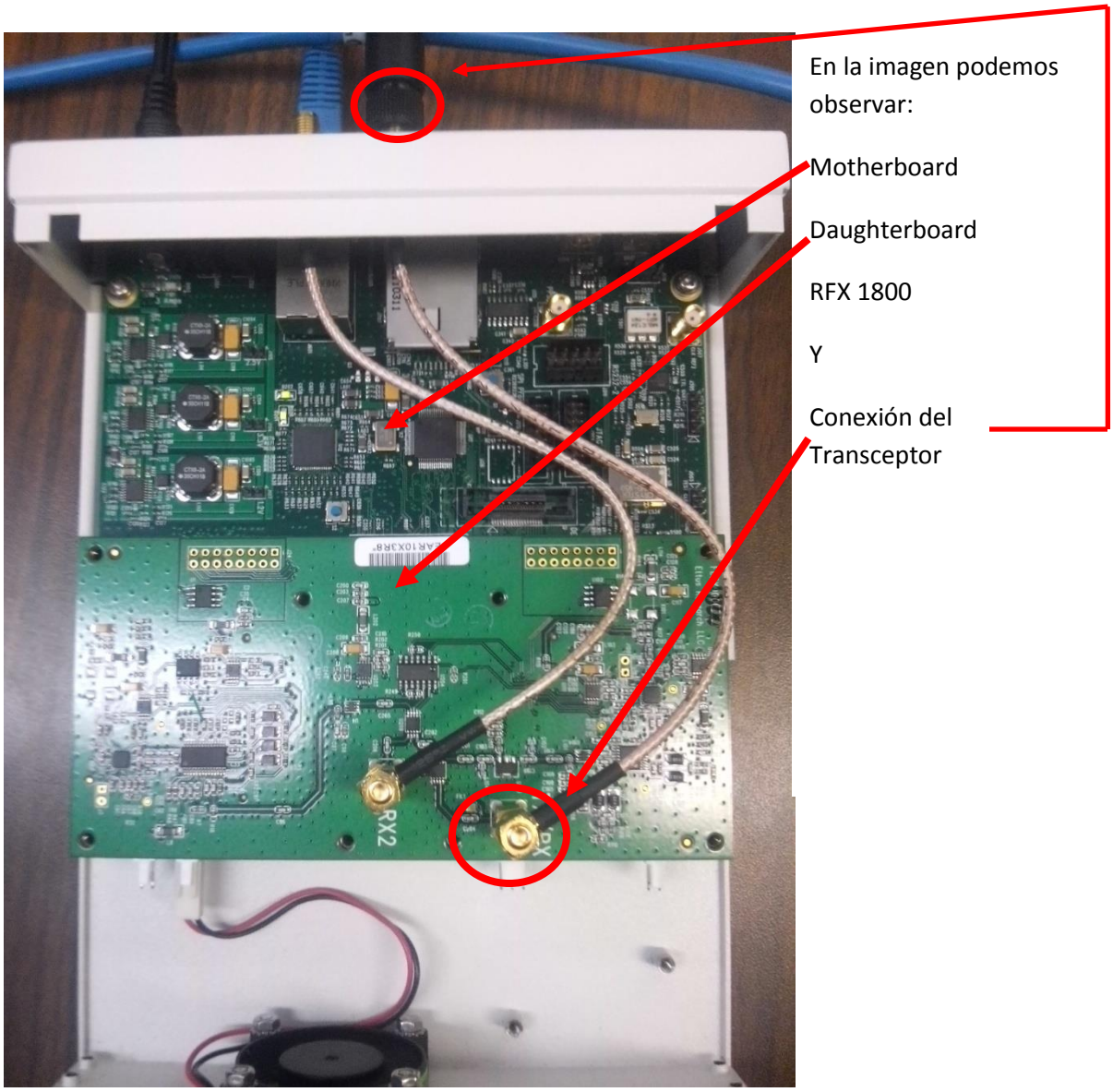


Figura 4.2.2 Vista interna del dispositivo USRP N210

La tarjeta RFX1800 es un transceptor diseñado para trabajar en 1900 y 1800 MHz. Con una potencia típica de 100 mW y una figura de ruido de 8 dB. Una aplicación importante y la que nos importa en este trabajo, estaciones base de telefonía celular, en especial red GSM.

Para poder desplegar la interfaz de aire Um en el aire se selecciona la banda de operación que queremos utilizar, el dispositivo USRP N210 está diseñado para operar en las bandas comerciales de GSM 900, 1800 y 1900 MHz.

Debido a que las bandas de 850 MHz, 900 MHz y 1900 MHz están dedicadas a telefonía celular, bajo las regulaciones del espectro en México se causa interferencia entre ellas.

Haciendo uso de un analizador de espectros se puede observar lo anterior.

Banda de 1900 MHz

Figura 4.2.3 Espectro de la banda de 1900 Mhz.

En la figura 4.2.3 se observa que la banda de 1900 MHz está siendo ocupada (por operadoras telefónicas u otros servicios).

La banda de 1800 Mhz es la más usada en Europa, Asia, Oceanía y Sudamérica. En México la mayoría de las operadoras de telefonía móvil cubren las bandas de 850 MHz, 900 MHz y 1900 MHz.

Con el analizador de espectros podemos observar que la banda de 1800 MHz está disponible y con muy pocas transmisiones lo que favorece a poder realizar las llamadas de prueba. Véase figura 4.2.4.

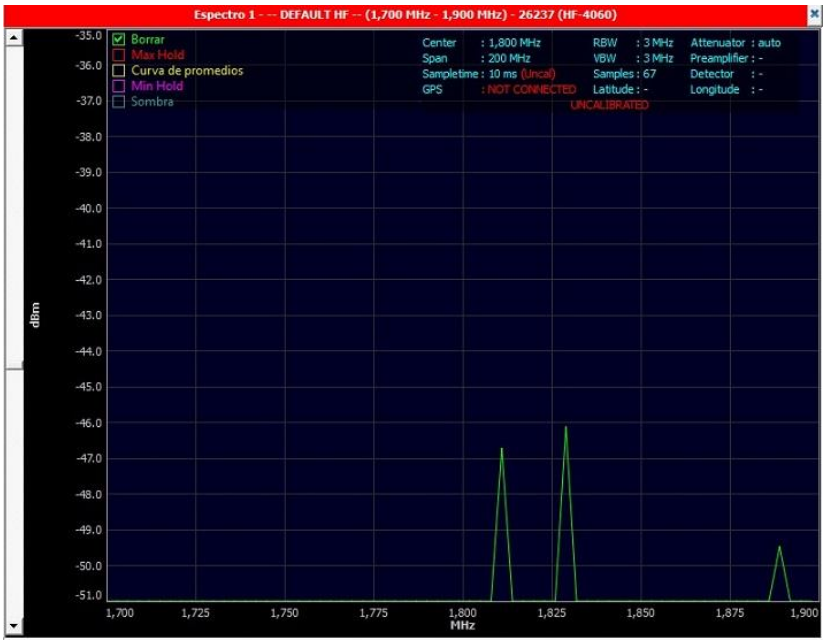


Figura 4.2.4 Espectro de la banda de 1800 Mhz

En figura 4.2.4 se muestra el espectro de la banda de 1800 MHz y no hay muchas transmisiones lo que nos permite poder desplegar nuestra interfaz Um en este rango.

Para que la tarjeta hija pueda enviar y recibir las señales se conecta una antena VERT900 al dispositivo. Las principales características de esta antena son:

VERT900

Rango de frecuencias de 824 a 960 MHz y 1710 a 1990 MHz (bandas celulares) este rango está dentro de los requerimientos, por tal razón se seleccionó esta antena como transceptor.

Figura 4.2.5 Antena, Omni-direccional con 3dBi de Ganancia.

En la figura 4.2.6 se muestra el panel frontal de conexiones en el USRP N210 con antena VERT900.

Figura 4.2.6 Vista Exterior del Dispositivo Ettus Research N210.

4.3 UHD USRP Hardware Driver, Controlador de Hardware USRP

El USRP Hardware Driver es el controlador de hardware para cualquier dispositivo de la familia USRP. Su principal función es ofrecer un controlador al host y una interfaz de programación de aplicaciones API[4], que proporciona acceso a diversas funciones del USRP como sincronización, muestreo, configuración. Este software recurre a otro software como GNU Radio para un correcto funcionamiento.

4.4 Software Asterisk

Asterisk es un programa de software libre (bajo licencia GPL[5]) que proporciona funcionalidades de una central telefónica (PBX). Como cualquier PBX, se puede conectar un número determinado de teléfonos para hacer llamadas entre sí e incluso conectar a un proveedor de VoIP.

[4] API es un grupo de rutinas (conformando una interfaz) que provee un sistema operativo, una aplicación o una biblioteca, que definen cómo invocar desde un programa un servicio que éstos prestan. En otras palabras, una API representa un interfaz de comunicación entre componentes software.

[5] GPL: Licencia Pública General, puede ser usada por cualquiera, ya que su finalidad es usar, compartir, estudiar y modificar el software libre.

4.4.1 VoIP

La telefonía IP (por sus siglas en inglés *Voice Over IP,* Voz Sobre el Protocolo de Internet) es un tipo de telefonía desarrollado para realizar comunicaciones de voz mediante el protocolo de internet. La voz se digitaliza luego viaja en forma de paquetes como cualquier otro dato. En este protocolo la voz viaja en la red de internet en un tramo, hasta este punto es donde hace uso de un Gateway[6] elemento importante en estas redes para poder interconectar con las redes públicas convencionales y otras redes móviles para que los paquetes lleguen a su destino.

4.4.2 PBX

PBX es la abreviatura de Private Branch Exchange, Red Privada de Telefonía, es cualquier central telefónica conectada directamente a la red pública de telefonía para gestionar además de las llamadas internas, las entrantes y salientes con autonomía sobre cualquier otra central telefónica. Este dispositivo generalmente pertenece a la empresa que lo tiene instalado y no a la compañía telefónica, de aquí el adjetivo Privado.

4.4.3 Protocolo SIP

El Protocolo SIP (Protocolo de Iniciación de Sesión, Session Initiation Protocol) define una arquitectura de señalización y control para VoIP [14]. Es un protocolo de señalización a nivel de aplicación para establecimiento y gestión de sesiones con múltiples participantes, está basado en arquitectura cliente/servidor similar al HTTP[7], sigue una estructura de petición-respuesta, estas peticiones son generadas por un cliente y enviadas a un servidor, que las procesa y devuelve la respuesta al cliente. El par petición-respuesta recibe el nombre de transacción. SIP proporciona un conjunto de solicitudes y respuestas basadas en códigos.

[6] Gateway VoIP es un dispositivo de red que convierte las llamadas de voz, en tiempo real, entre una red VoIP y la red telefónica pública conmutada o su centralita digital.

[7] HTTP El protocolo HTTP funciona a través de solicitudes y respuestas entre un cliente (por ejemplo un navegador de Internet) y un servidor (por ejemplo la computadora donde residen páginas web). A una secuencia de estas solicitudes se le conoce como sesión de HTTP.

4.5 Software OpenBTS

OpenBTS [3] (Open Base Transceiver Station, Estación base Transceptora Libre) es una aplicación Unix de software libre que usa el Software Universal Radio Peripheral USRP para proporcionar la interfaz de aire de GSM para la comunicación de los móviles GSM con la red y asigna recursos (time slots, portadora, potencia). Gracias a esto, el terminal puede ser activado en la red mediante la selección de ésta manualmente.

En su núcleo OpenBTS es software de código abierto que crea una interfaz para teléfonos móviles para conectarse a la red. El software se instala en un ordenador con sistema operativo Linux. Un dispositivo de código abierto, Universal Software Radio Peripheral (USRP), se conecta a la computadora. Juntos, crean una señal igual a cualquier señal de los teléfonos GSM.

El software más las herramientas de hardware USRP se conectan a una PBX de código abierto, Asterisk. La central, con una central privada, es un servidor que actúa como una centralita telefónica para realizar llamadas. OpenBTS utiliza Asterisk no solamente para manejar las llamadas de voz sobre IP sino también para autentificar los usuarios. Cada usuario debe ser registrado en el fichero sip.conf con su correspondiente IMSI como se verá más adelante.

La figura 4.5.1 muestra como está conformado el software openBTS con cada una de las dependencias que requiere para ser implementado en software y hardware.

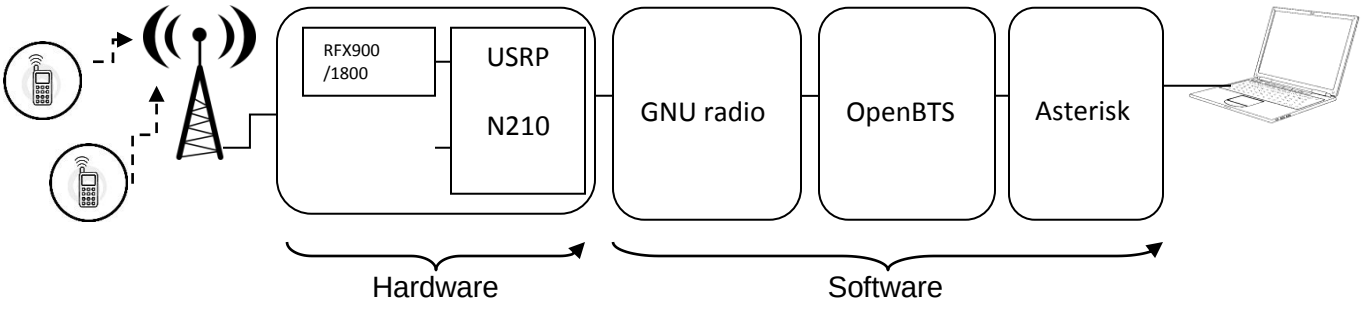


Figura 4.5 Módulos de OpenBTS.

4.5.1 Arquitectura de OpenBTS

OpenBTS reemplaza la infraestructura tradicional del Subsistema de Conmutación de Red del operador de GSM como se muestra en la figura 4.5.1.1. En vez de reenviar el tráfico de la llamada a través del Centro de Conmutación Móvil (MSC) del operador, las llamadas son terminadas en la misma caja reenviando los datos sobre la PBX Asterisk vía Session Initiation Protocol (SIP) y Voz sobre IP (VoIP).

La interfaz de aire Um utiliza una radio definida por software (SDR) encima de la tarjeta USB del Universal Software Radio Peripheral (USRP). Se puede ajustar el USRP para proporcionar varios tipos de señales de radio. En este caso se ejecuta la red OpenBTS para enviar y recibir llamadas entre la estación base y el teléfono celular del usuario.

Una gran ventaja de este sistema es que reemplaza gran parte de la infraestructura física de la red central con software VoIP, con el programa de código abierto Asterisk.

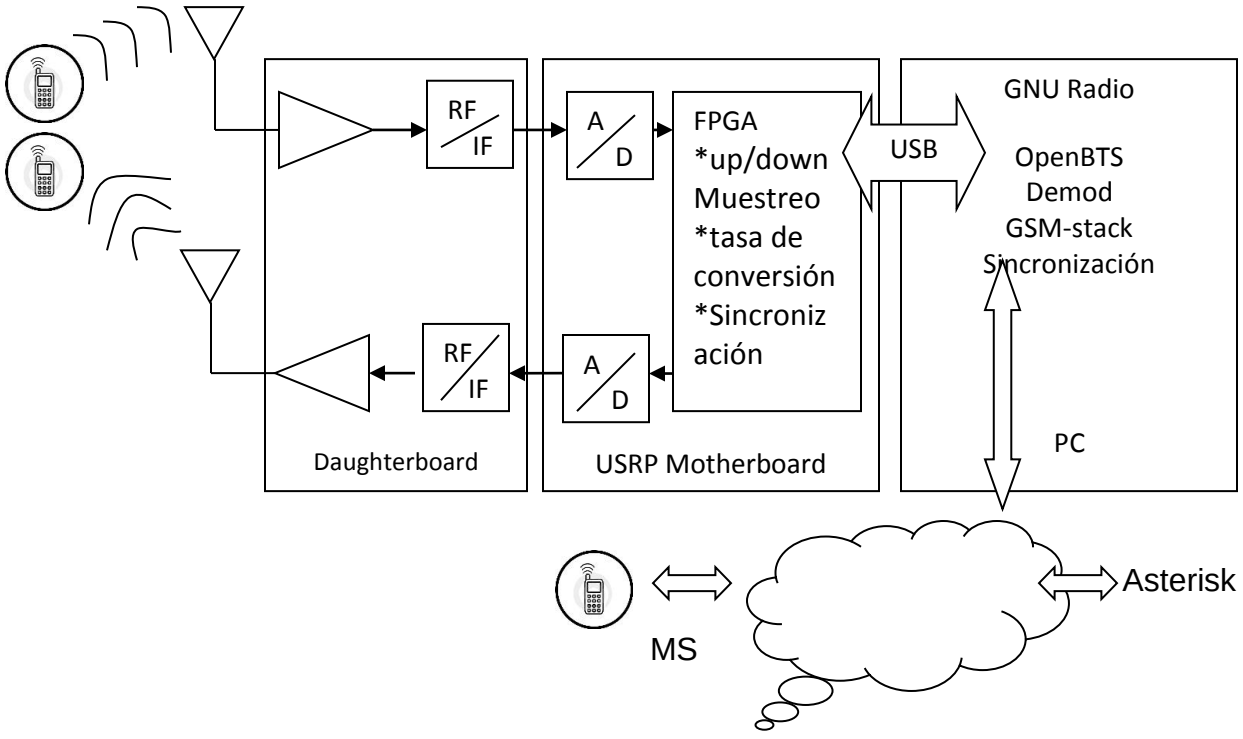


Figura 4.5.1.1 Arquitectura del Sistema OpenBTS [11].

El sistema también requiere de algunas dependencias que son necesarias para operar. Estas dependencias son bases de datos manipulables por el usuario, a continuación se da una breve descripción de cada uno.

4.5.2 *Smqueue*

Es el servicio de almacenamiento y transmisión de mensajes cortos y se obtiene junto con OpenBTS. Esta librería no afecta el funcionamiento de la interfaz de radio, si está o no instalada en el software las llamadas se pueden llevar a cabo sin ningún problema dentro de la red.

4.5.3 *sipauthserve*

Este es el servidor de registro y autorización de usuarios, se usa para la prestación de servicios de autenticación SIP y ejecuta las actualizaciones en la base de datos de usuarios (sqlite3.db).

4.5.4 *Subscriber Registry*

Base de datos donde se almacenan los usuarios de la red.

Las dependencias antes mencionadas cumplen ciertas funciones, haciendo la analogía con una red GSM convencional estos elementos se encargan de ciertas funciones:

OpenBTS: Interfaz celular GSM; Interfaz Um.

Sipauthserve: Se encarga de las funciones del Registro de Localización Local (Home Location Register HLR).

Smqueue: Funciona como el Centro de Servicios de Mensajes Cortos (Short Message Service Center SMSC).

PBX: Central de Conmutación o MSC, en el sistema Asterisk se encarga de estas funciones. PBX Asterisk vía Session Initiation Protocol (SIP) y Voz sobre IP (VoIP).

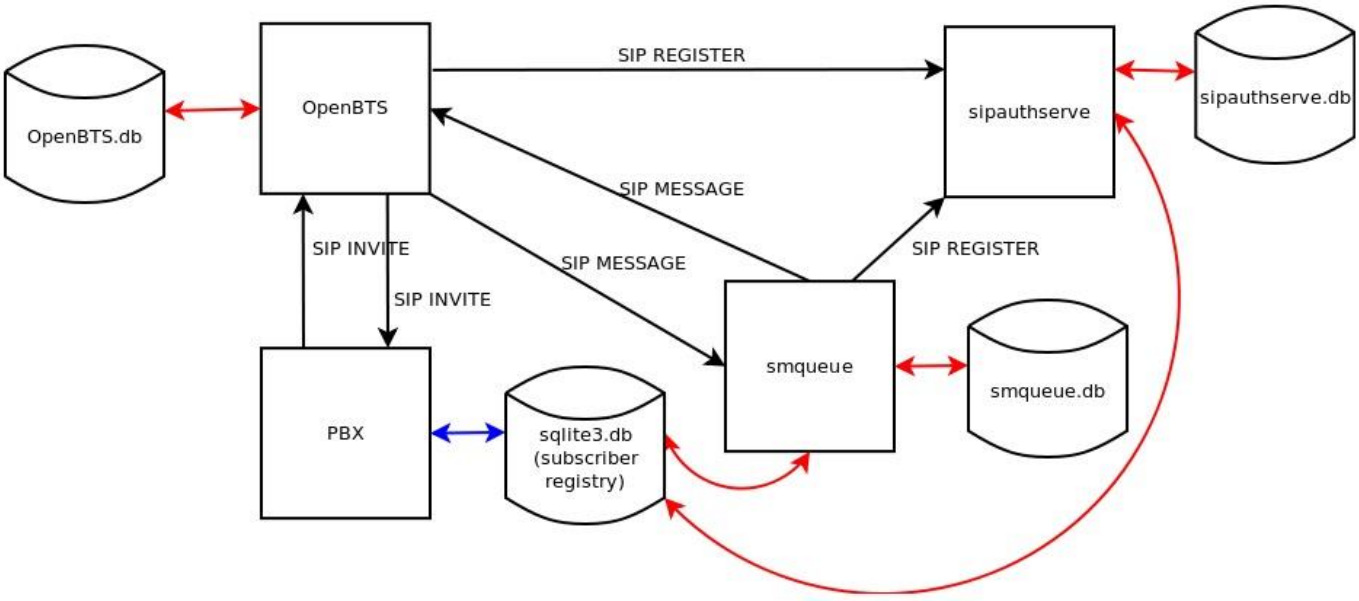


Figura 4.5.1.2 Diagrama de conexiones de OpenBTS extraído de [17].

En la figura 4.5.1.2 se tiene el diagrama de conexiones que realiza OpenBTS, los enlaces de color negro son conexiones SIP (conexiones de red). Los enlaces de color rojo son las conexiones del sistema de archivo (búsquedas SQLite3). Los enlaces de color azul son ODBC (Red / búsquedas locales DB). ODCB Open DataBase Connectivity. Conectividad abierta de bases de datos ODBC, asegura una conexión continua desde un cliente, servidor. ODBC provee una solución completa e independiente para el acceso a datos, porque define estándares para el proceso y acceso físico a las bases de datos.

4.6 Implementación del Sistema

En este apartado se presenta el procedimiento a seguir para desplegar la interfaz GSM con los elementos de hardware y software con los que contamos. La elección de la implementación de una Estación Base Transceptora GSM, como se mencionó anteriormente es impulsada por 2 amplias ventajas, primero, poner en práctica un sistema TDMA, FDMA y FDD mediante software y hardware libre, segunda, los costos en comparación con un sistema convencional son mucho menores.

Para la implementación de la Estación Base se utilizaron los siguientes elementos de hardware:

- 1 *Motherboard Ettus Research, Universal Software Radio Peripheral N210*

- 1 *Daughterboard* RFX18001.5-2.1 GHz Rx/Tx, Antena VERT900
- 2 teléfonos celulares compatibles con la banda de 1800 MHz
- 1 Computadora Personal con OpenBTS versión 2.8 instalada

La placa utilizada para implementar la BTS GSM es una placa base (*Motherboard*) que soporta una placa secundaria (*Daughterboard*). Se conecta a una computadora a través de un puerto Gigabit Ethernet, y es capaz de utilizar el ancho de banda de frecuencia de radio de 50 MHz en ambas direcciones por ello se logra una conexión full dúplex.

A continuación se listan los elementos de Software necesarios para la implementación (junto con las librerías que les corresponden para su funcionamiento descritas en el anexo) en el Sistema Operativo Ubuntu 12.04 LTS:

- GNU Radio Linux; GNU C++ versión 4.6.3
- OpenBTS 2.8
- *Asterisk* versión 11.6

Los siguientes conceptos son algunos que debemos conocer acerca de la red GSM

MCC*: Mobile Country Code* (Código Móvil del País), Se usa para identificar al país por medio de un numero de 3 dígitos.

MNC*: Mobile Network Code* (Código de Red Móvil), Es el identificador de los operadores móviles. Lo representan 2 o 3 dígitos.

Ambos códigos corresponden a los primeros 5 o 6 dígitos del total de 15 dígitos que conforman el código IMSI, International Mobile Subscriber Identity (Identidad Internacional del Abonado a un Móvil). Los dígitos restantes representan el Número de Identificación de Suscripción de Móvil (MSIN, Mobile Subscription Identification Number).

En este caso se utilizaron los valores de prueba para MCC y MNC que vienen por default en OpenBTS para no confundir con algún país u operadora de telefonía celular, estos valores son 001 para MCC y 01 para MNC. La red también puede ser identificada por un nombre, en este caso se le asignó el nombre de Range, tal y como la detectan los celulares.

Como se mencionó anteriormente el USRP N210 cuenta con 2 tipos de tarjetas y una serie de elementos con lo que se procesa la señal como se muestran en la figura 4.6.1.

La tarjeta principal o motherboard contiene elementos importantes como el FPGA, los convertidores Digital-Analógico (DAC) y Analógico-Digital (ADC), la alimentación y la conexión vía GB Ethernet. La daughterboard transceptora transmite y recibe a la vez y se encarga de transformar la señal de banda base o IF hasta la banda RF deseada y viceversa.

Cuenta con convertidores Analógico-Digital de 14 bits por muestra y una tasa de muestreo de 100 MS/s (100,000,000 muestras por segundo). También cuenta con convertidores Digital-Analógico de 16 bits por muestra y con una tasa de muestreo de 400 MS/s (400,000,000 muestras por segundo).

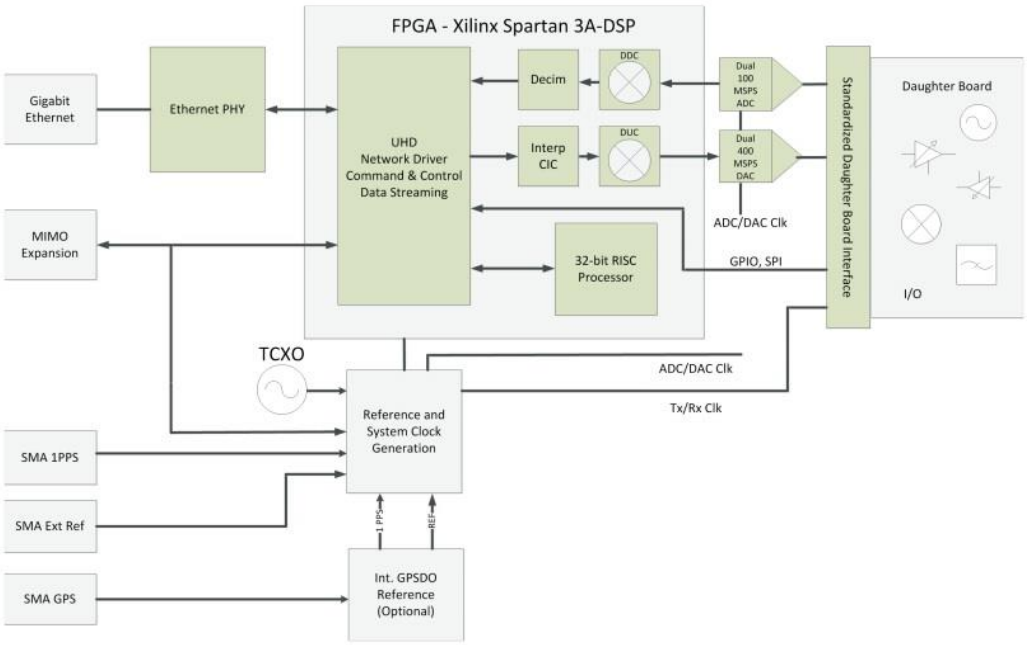


Figura 4.6.1. Arquitectura Interna USRP N210 [12].

El procesador que utiliza el USRP es un FPGA que está conectado a los convertidores ADC y DAC. Este FPGA se encarga del procesado de las señales en la banda que se desee para reducir las tasas de muestreo de datos en la interfaz GB Ethernet, a este proceso se le llama diezmado[8]. Para llevar a cabo el diezmado el FPGA cuenta con convertidores digitales de bajada (DDC, *Digital Down Converter)* para disminuir la tasa de muestreo. Lo que hace es reducir el espectro del procesado para poder enviar y transmitir

los datos generados por los convertidores DACs y ADCs a una tasa mínima a través del puerto GB Ethernet.

El DDC permite llevar la señal digital de una frecuencia intermedia a una en banda base.

Para la transmisión el proceso es de forma inversa. Se usa el *Digital Up Converter* DUC que se encarga de pasar de banda base a frecuencia intermedia y enviarla a través de los convertidores Digital Analógico (DACs).

La tarjeta hija o daughterboard se encarga de la sección de RF y realiza las funciones de transmisión y recepción.

La tarjeta madre recibe la señal analógica del aire a través de la tarjeta hija de recepción y esta muestrea la señal con el ADC a una tasa de 100 MS/s. La señal digital resultante que sale del convertidor va hacia el FPGA, la señal va en la banda de IF y se convierte a complejo en dos señales I/Q (componentes de cuadratura). Este conjunto de señales es llamado *QR Quadrature Rate* una vez hecho el diezmado.

RF front end: Un RF front end se encarga de trasladar adecuadamente y amplificar el centro de un rango de frecuencias a otro rango de frecuencias. La frecuencia central del rango de salida se denomina Frecuencia Intermedia (IF)

[8] Diezmar, se toma una referencia para dar a entender que algo ha sido reducido en un porcentaje bastante considerable, en este caso tasas de muestreo en comunicaciones.

Los canales de señalización están integrados en la interfaz de aire como el BCCH, PCH, AGCH, SDCCH, SACCH y FACCH.

En una red convencional GSM cuando un teléfono móvil se enciende los algoritmos de control con los que cuenta empiezan a trabajar realizando en general la siguiente secuencia de señalización para registrarse en la red que le corresponde.

1.- Busca por las frecuencias de GSM.

2.- Encuentra un FCCH y se sincroniza en frecuencia.

3.- Encuentra un SCH y se sincroniza en tiempo.

4.- Escucha por un BCCH y descarga la información acerca del sistema.

5.- Obtiene las señales de radios bases cercanas y hace una lista de mediciones.

6.- Selecciona al mejor servidor y obtiene sus parámetros para registrarse en la red.

7.- Si el usuario quiere hacer una llamada, el móvil tiene que indicar a la red y lo hace mediante el envío de una solicitud de servicio a la red en el RACH.

En implementaciones prácticas, se proporciona una banda de guarda de la parte más alta y más baja de espectro de GSM. La combinación de un número de (time slot) ST y un ARFCN constituyen un canal físico tanto para el “uplink” como para el “downlink”. De este modo se logra la conexión entre el teléfono móvil y la estación base con la que contamos.

Los TCH (canales de tráfico) transportan la voz codificada digitalmente y tienen funciones idénticas y formatos tanto para el “downlink” como para el “uplink”. Los canales de control llevan comandos de señalización y control entre la estación base y la estación móvil. Se definen ciertos tipos de canales de control exclusivos para el uplink o para el downlink. Hay seis clases diferentes de TCHs y un número aún mayor de Canales de Control, estos canales se describieron brevemente en la sección 3.4

CAPITULO 5

PRUEBAS Y RESULTADOS

En este capítulo se presentan las pruebas realizadas con el sistema puesto en funcionamiento. Desde la comunicación de la PC con el dispositivo USRP N210, hasta utilizar la red.

Se muestra el procedimiento que se llevó a cabo para poder desplegar la interfaz Um en el aire.

En los anexos se muestran los elementos de software que deben ser instalados y las dependencias que cada uno necesita para que el sistema funcione correctamente.

5.1 Conexiones entre PC y Dispositivos. Véase figura 5.1.1.

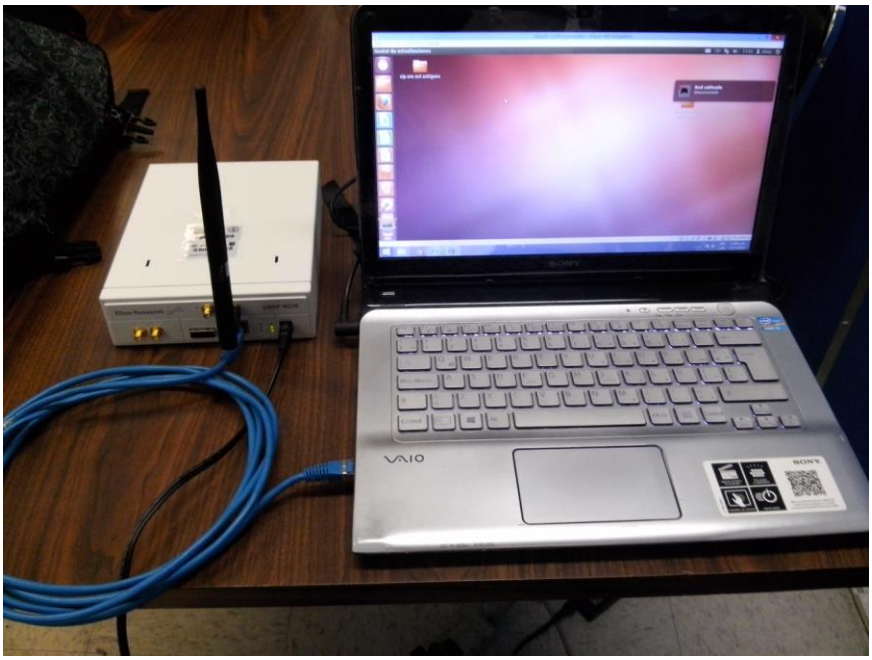


Figura 5.1.1 Conexiones de PC y dispositivo USRP.

El primer paso es verificar que el dispositivo se encuentre bien conectado con el cable Ethernet a la interfaz GB Ethernet de la computadora.

Lo anterior se logra en primera instancia poniendo en la terminal de Ubuntu el comando:

uhd_find_devices, se muestra el dispositivo, dirección IP y serial.

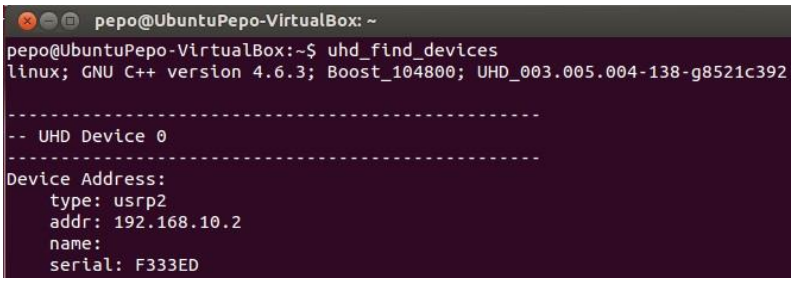


Figura 5.1.2 Dispositivo Conectado Correctamente.

Después con el siguiente comando: uhd_usrp_probe, la terminal de Ubuntu muestra las características del dispositivo conectado, tipo de tarjetas, relojes de sincronización, transmisor, receptor. Véase figura 5.1.3.

Figura 5.1.3 Características del Dispositivo Parte I.

En la figura 5.1.4 se observan las demás características de la tarjeta que tenemos insertada en el dispositivo.

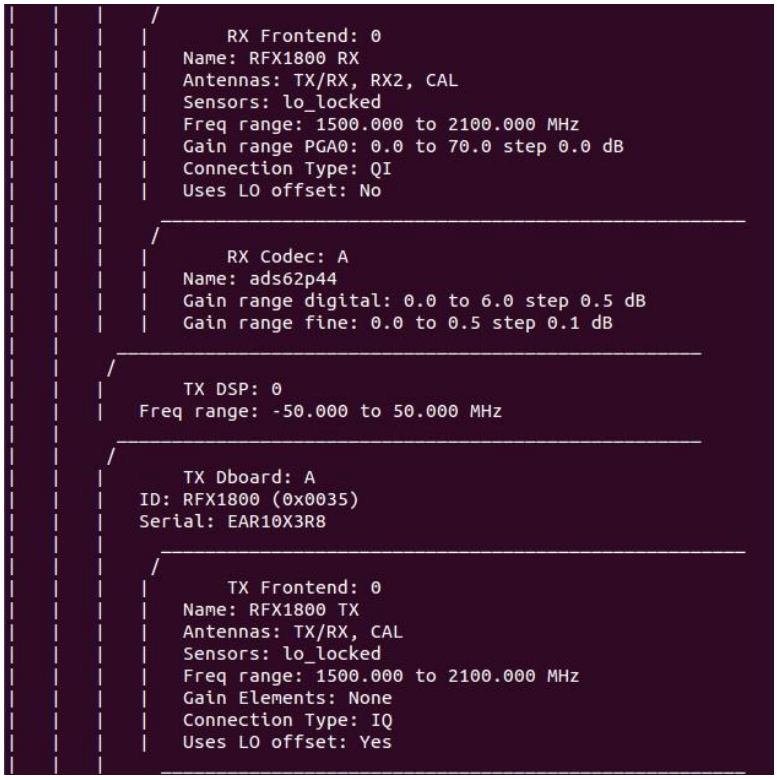


Figura 5.1.4 Características del Dispositivo Parte II.

Una vez que el dispositivo está bien conectada la comunicación con la PC, se dispone a levantar la interfaz de aire Um, que será visible para cualquier teléfono móvil que busque las redes de forma manual con las que dispone a sus alrededores.

El primer paso es levantar cada uno de los elementos que OpenBTS necesita para operar. Estos deben ser ejecutados en una terminal por separado.

Desde el directorio: public/smqueue/trunk/smqueue ejecutar el siguiente comando:

Sudo ./smqueue

Con esto el sistema pone en funcionamiento el centro de mensajería corta, necesaria para poder enviar y recibir Mensajes SMS ver figura 5.5. Es inicializado independientemente de OpenBTS. La interfaz SIP con la que es ejecutada está en el puerto 5063.

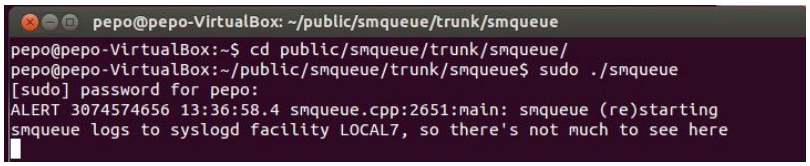


Figura 5.1.5 Encendido del Centro de Mensajería.

Ahora continuamos con sipauthserve, este sistema de archivos es el servidor SIP de registro y autorización de usuarios, se usa para procesar las peticiones de actualización de localización por parte de OpenBTS y realiza los correspondientes cambios en la base de datos del registro de subscriptores. Ver figura 5.1.6. Este elemento SIP se ejecuta en el puerto 5064.

Desde el directorio public/subscriberRegistry/trunk/ ejecutar el siguiente comando:

sudo ./sipauthserve.

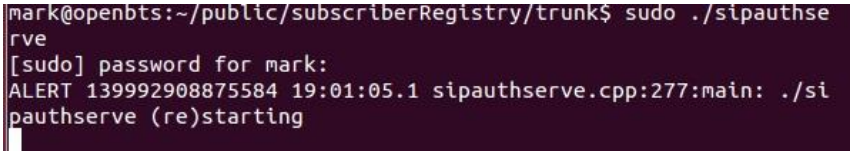


Figura 5.1.6 Registro para Usuarios.

Después tenemos que levantar la central de conmutación. Lo que se está haciendo es poner una interfaz de aire (red celular GSM) sobre una PBX. De este lado de la implementación, la función de este elemento MSC (Centro de Conmutación Móvil) los realiza el servidor de Asterisk como PBX. Ver figura 5.1.7. Esta central PBX conecta las llamadas de voz según las peticiones que envíen los usuarios registrados. Su interfaz SIP está en el puerto 5060. Desde el directorio etc/asterisk ejecutar el siguiente comando sudo ./asterisk –rvvv

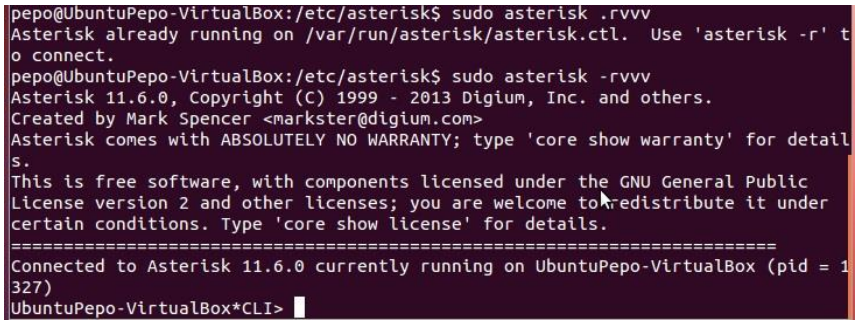


Figura 5.1.7 Asterisk encendido (PBX del sistema).

Casi para terminar y tener nuestro sistema funcionando tenemos que levantar lo más importante, debemos poner la señal en el aire, véase figura 5.1.8. La interfaz SIP del transceptor está en el puerto 5062.

Desde el directorio raíz de OpenBTS public/openbts/trunk/apps ejecutar el siguiente comando: sudo ./OpenBTS

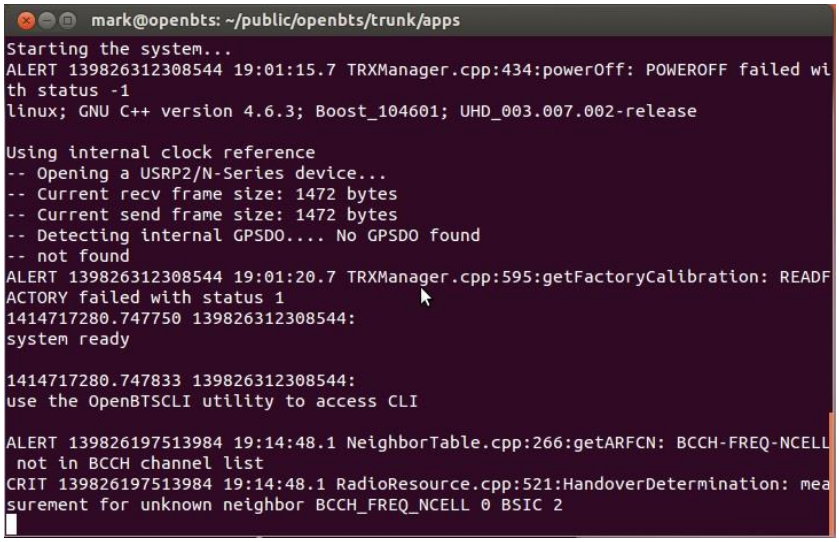


Figura 5.1.8 Interfaz de Aire Um Desplegada en el Aire.

Una vez hecho lo anterior se inicializa el sistema y la interfaz Um ya está desplegada en el aire. La señal será visible por todos los teléfonos celulares que estén dentro de su alcance, siempre y cuando se ponga el teléfono en forma manual a buscar por redes de telefonía celular.

Nuestra interfaz Um es desplegada por la antena transceptora VERT900 que está conectada al dispositivo USRP y los sistemas anteriores ya en funcionamiento.

Por último para que el OMC ó Subsistema de Soporte y Operación administre la red se debe ejecutar desde el directorio /public/openbts/trunk/apps el comando:

Sudo ./OpenBTSCLI

Una vez hecho lo anterior ya está la red desplegada y lista para administrarse véase figura 5.1.9.

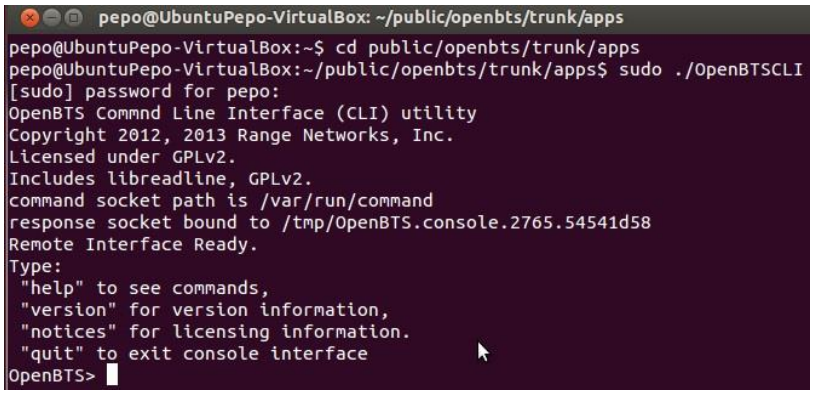


Figura 5.1.9 Consola de OpenBTS.

Lo siguiente es brindar servicio a los usuarios. Para ello se administra la red mediante la interfaz de comandos de OpenBTS.

Primer paso. Con un teléfono celular en forma manual ponemos a buscar las redes que se encuentran disponibles en nuestro entorno. Una vez detectada la red que tiene por nombre “Range” (ó “001 01” que es el nombre por default que proporciona OpenBTS) se solicita acceso a la red. Cuando el teléfono móvil pide ser registrado en la red manda su solicitud a la radio base. Esta última genera un archivo temporal llamado TIMSI ver figura 5.10, por sus siglas en ingles *Temporary Mobile Subscriber Identity*. Hasta este punto el teléfono celular aún no está registrado en la red. Una vez que el administrador de la red detecta que un usuario está intentando registrase debe verificar si le dará servicio o no.

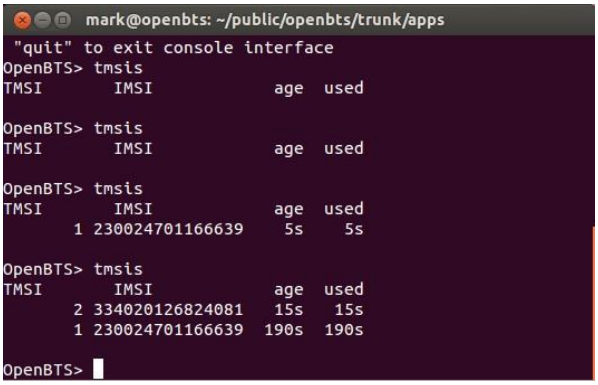


Figura 5.1.10 Solicitudes de Registro a la Radio Base.

En la figura 5.1.10 se muestra la tabla TMSI de nuestra radio base, en las primeras 2 líneas podemos observar que no hay solicitudes para ser registradas. En la tercera línea se observa la primera solicitud de un teléfono que por los primeros 3 dígitos (334)

corresponden a México, se utilizó una SIM telcel con IMSI 334020126824081. La recomendación es utilizar SIM que no sean locales pero aun así son funcionales, siempre y cuando los teléfonos utilizados sean bi-banda o tri-banda. Este número IMSI es de suma importancia para poder permitir al usuario hacer uso de los servicios de la red.

En la cuarta línea se observa que un segundo teléfono solicita ser registrado en la red con IMSI, 230024701166639. Este no es una SIM local, por los primeros 3 dígitos (230) pertenece a la Republica Checa. Esto solo para probar que también con SIM foráneos funciona sin complicaciones siempre y cuando los teléfonos celulares sean compatibles con la banda de 1800 MHz.

Segundo paso. Una vez obtenidos los IMSI de cada uno de los teléfonos celulares que solicitaron ser registrados, se procede a permitirles el acceso a la red.

Esto se hace actualizando los archivos llamados extensions.conf y sip.conf.

A continuación se explica el proceso.

Una vez que la radio base obtiene los IMSI de los teléfonos que solicitan acceso a la red se deben dar de alta en los archivos sip.conf y extensions.conf. Para esto se toma el IMSI de cada teléfono celular y se registra en ambos archivos para que así puedan ser registrados.

A continuación se muestra la parte en donde cada usuario debe ser agregado a la base de datos de la radio base.

Extensions.conf

El archivo extensions.conf es la parte central de toda la configuración, dado que es donde se define el plan de marcado (*dialplan*) de Asterisk. Un dialplan o plan de marcado es el corazón de asterisk. Cada digito que se marque en un terminal recorrerá el dialplan, buscando que instrucciones seguir por lo que de manera básica, se puede decir que el dialplan es como una tabla de enrutado, el usuario marca un número y el dialplan contiene las acciones a realizar para ese número que se ha marcado.

Se compone de 4 partes principales: contextos, extensiones, prioridades y aplicaciones. El dialplan se divide en secciones llamadas contextos, que están rotuladas y contienen un grupo de extensiones.

Una extensión es una instrucción que será seguida por Asterisk, luego de ser solicitada por una llamada entrante, definida en el marco de un contexto. La sintaxis de una extensión es la siguiente: exten => nombre,prioridad,aplicación()

Una extensión puede tener varios pasos, denominados prioridades. Las prioridades comienzan con 1 y se ejecutan en orden numérico. Si no existe la prioridad N+1, Asterisk no salta a la siguiente prioridad (N+2). Cada prioridad ejecuta una única aplicación. Por ejemplo:

exten => 101,1,Answer() ;contestar una llamada

exten => 101,2,Hangup() ; terminar la llamada

Prioridades sin numerar

Asterisk introduce el uso de la prioridad n (next). Cada vez que Asterisk encuentra una prioridad n, toma el número de la prioridad anterior y le suma 1. Simplifica el proceso de escritura del dialplan, evitando tener que volver a numerar las prioridades al insertar una prioridad para la misma exten. Por ejemplo:

exten => 103,1,Answer()

exten => 103,n,hacer algo

exten => 103,n,Hangup()

Nota como el orden numérico (1,2,3) es reemplazado por la letra n.

Aplicaciones

Las aplicaciones realizan una acción determinada en el canal actual, controlando el comportamiento de la llamada y del sistema en sí. Algunos ejemplos son:

answer(): contesta una llamada

hangup(): cuelga una llamada

dial(): realiza una llamada saliente

playback(): reproduce un archivo de sonido

Ciertas aplicaciones requieren del pasaje de parámetros, estos se incluyen dentro de los paréntesis, separados por coma “,”.

A continuación se presenta el contexto utilizado simplificado, únicamente para mostrar que se va contestar una llamada y a colgar sin prioridades.

Configuración del fichero extensions.conf

[default] ;nombre del contexto

exten => 9999,1,Dial(SIP/IMSI230024701166639@127.0.0.1:5062,10) ;lg pepo

exten => 9999,n,Hangup()

Donde

9999 es el número de usuario para identificarlo.

1 prioridad 1, solo se cuenta con 2 (n=2)

Dial es el plan de marcado, (orden de realizar una llamada al IMSI establecido)

SIP protocolo a usar

IMSI identificador Internacional del usuario

127.0.0.1 dirección ip por defecto de asterisk

5062 puerto usado.

;

exten => 8888,1,Dial(SIP/IMSI334020126824081@127.0.0.1:5062,10) ; lg chocolate

exten => 8888,n,Hangup()

Ahora para la configuración de SIP.conf

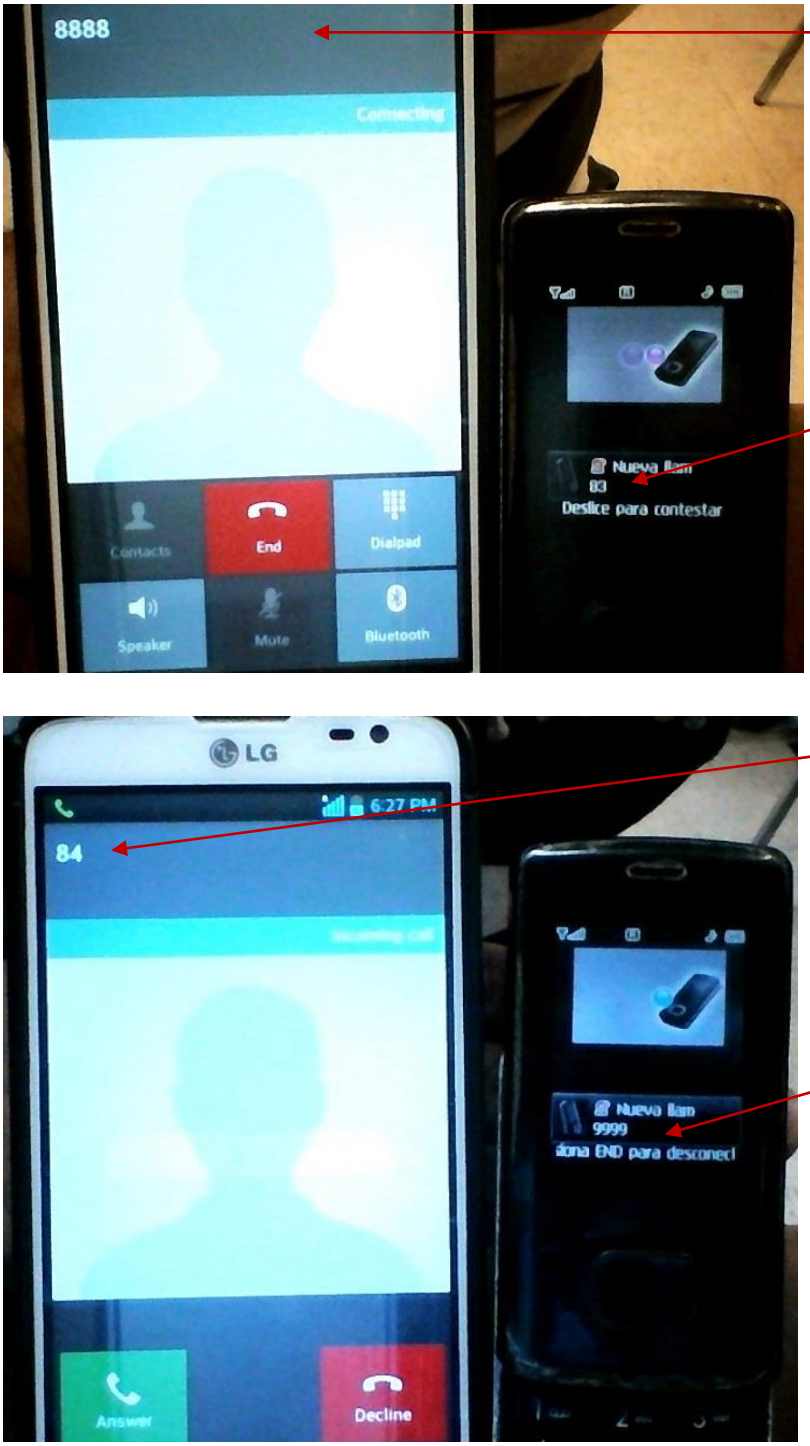
```
[IMSI230024701166639] ; el IMSI es usado como un usuario SIP
type = friend           ;puede recibir y realizar llamadas
host = dynamic          ;el teléfono se puede conectar desde cualquier dirección IP
nat = no                ;deshabilita el soporte de nat.
context = default       ;contexto del que se habló en extensions.conf
qualify = yes           ;determina que el dispositivo puede ser alcanzado
callerid = 83           ; Identificador de llamada
allow=gsm               ; permite codificadores GSM
canreinvite=no          ; se pone no cuando está detrás de un dispositivo que hace nat
[IMSI334020126824081]
type = friend
host = dynamic
nat = no
context = default
qualify = yes
callerid = 84
allow=gsm
canreinvite=no
```

Tercer paso. Una vez hecho lo anterior nos dirigimos a la consola de asterisk y recargamos ambos ficheros extensions.conf y SIP.conf con el comando “reload” para que los usuarios que solicitaron ser registrados ya se encuentren dentro de la base de datos HLR o sipauthserve para que se les permita realizar llamadas y enviar mensajes de texto.

Cuando los archivos son recargados en la consola de Asterisk la radio base le notifica al usuario que ya se encuentra registrado en la base de datos. En figura 5.1.11 se muestra el mensaje enviado por la radio base (101).

Figura 5.1.11 Mensaje de Bienvenida, Usuario Registrado.

5.2 Llamadas entre usuarios. Por último, ya registrados los teléfonos celulares en la radio base se pueden realizar llamadas. En la figura 5.2.1 se muestra como el usuario “9999” con “CallerID” de 83 llama al usuario 8888.



Usuario 9999 llamando a usuario 8888.

Usuario 8888 con llamada entrante del usuario 9999 con CallerID 83 (Identificador de llamada).

Usuario 9999 con llamada entrante del usuario 8888 con CallerID 84 (Identificador de llamada).

Usuario 8888 llamando a usuario 9999.

Figura 5.2.1 Llamadas Entre Usuarios.

En la consola de OpenBTS se puede monitorear el proceso de llamada ver figura 5.2.2.

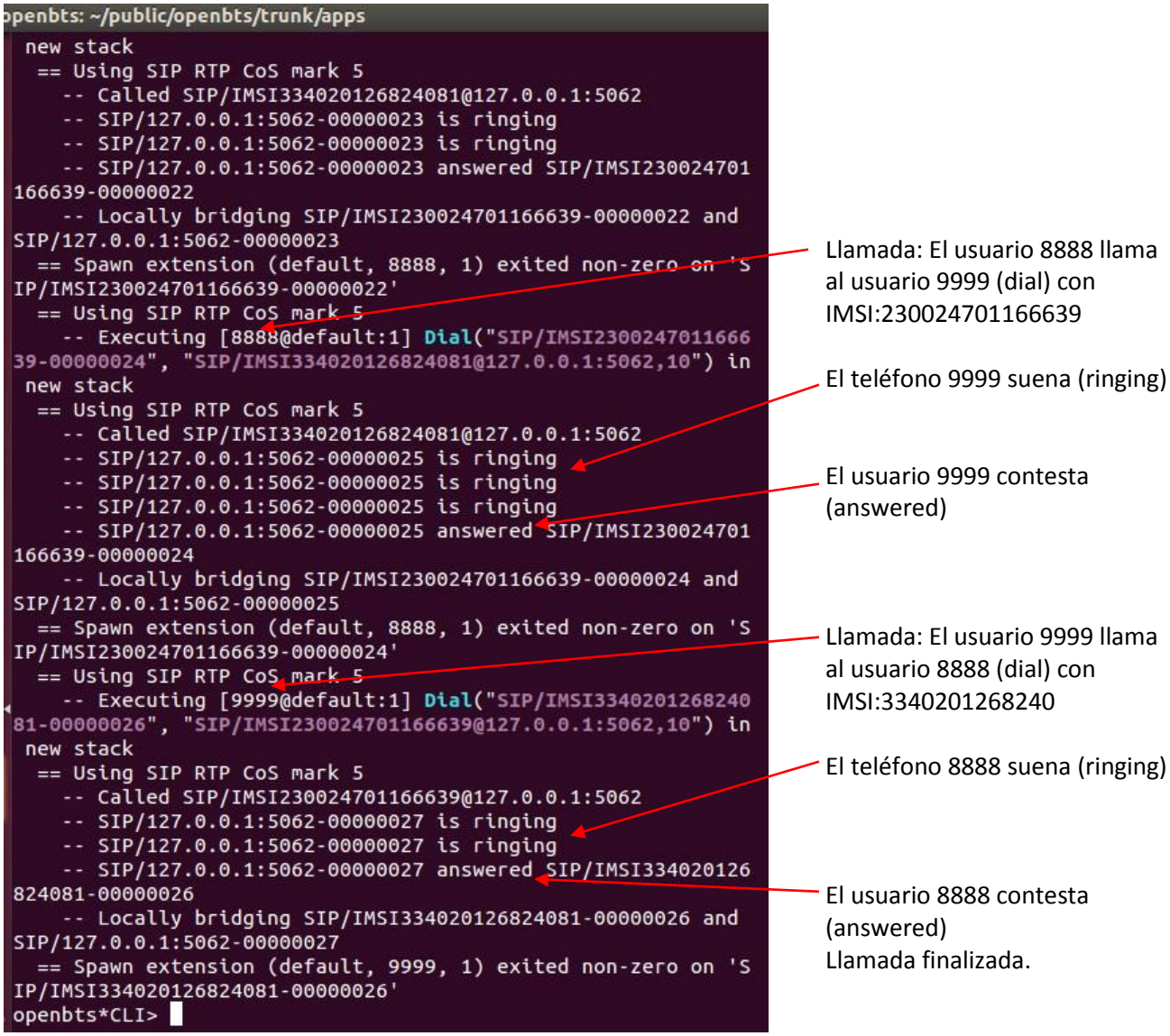


Figura 5.2.2 Proceso de Llamadas en la Consola de OpenBTS.

5.3 RSSI

El RSSI, indicador de fuerza de la señal recibida (*Received Signal Strength Indicator*) es medido en el dispositivo móvil del usuario, este indicador disminuye (se hace más negativo) a medida que el dispositivo se aleja del transceptor debido a las pérdidas de la señal en el espacio libre entre usuario y transceptor. Lo mismo ocurre con las señales que se propagan desde el dispositivo hasta el transceptor.

Para realizar las mediciones de RSSI se utilizó la aplicación en uno de los teléfonos celulares, llamada, GSM *Signal Monitoring* que nos proporciona el nombre del operador el código del país y el código de red.

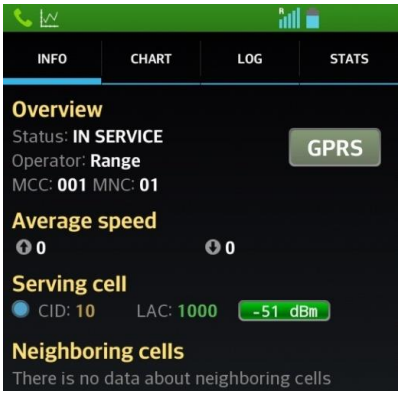


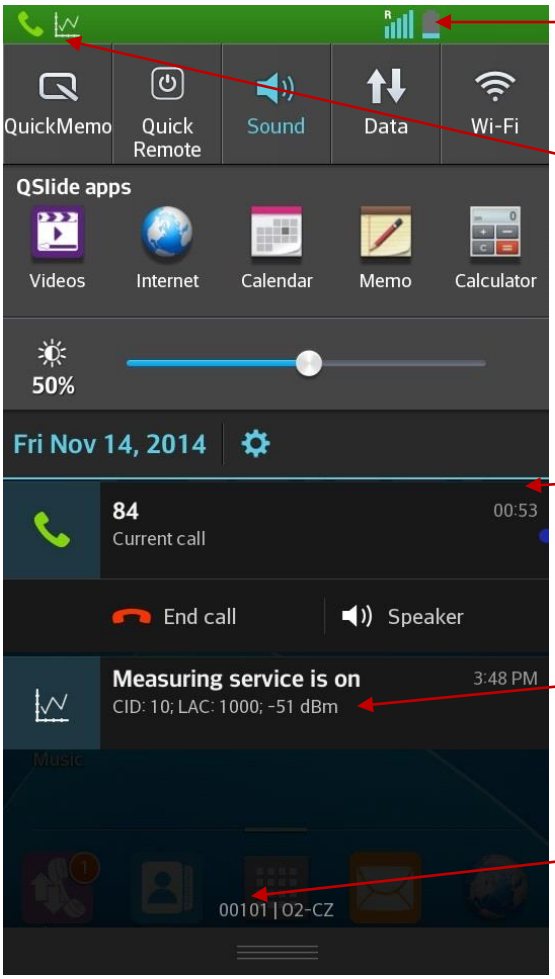
Figura 5.3.1 Pantalla Principal de la Aplicación GSM Signal Monitoring.

En la figura 5.3.1 está la pantalla principal de la aplicación y muestra el nombre del operador y los códigos MCC y MNC y la intensidad de señal recibida RSSI.

En este caso como se mencionó anteriormente nuestros códigos son MCC: 001 y MNC 01. En conjunto el operador es 00101 o “Range” nombre que es proporcionado por default en el sistema.

En las figuras 5.15 y 5.16 se muestran las pantallas de los registros del nivel más alto de RSSI (Mientras más cercano a cero es valor de RSSI es considerado muy bueno) y el nivel más bajo (Mientras el teléfono celular se encuentra en el límite del rango de alcance de la señal).

Valor de RSSI recibido muy cerca de la radio base, RSSI: -51 dBm.



Excelente calidad de señal.

Indica que se tiene establecida una llamada.

Duración de llamada en curso.

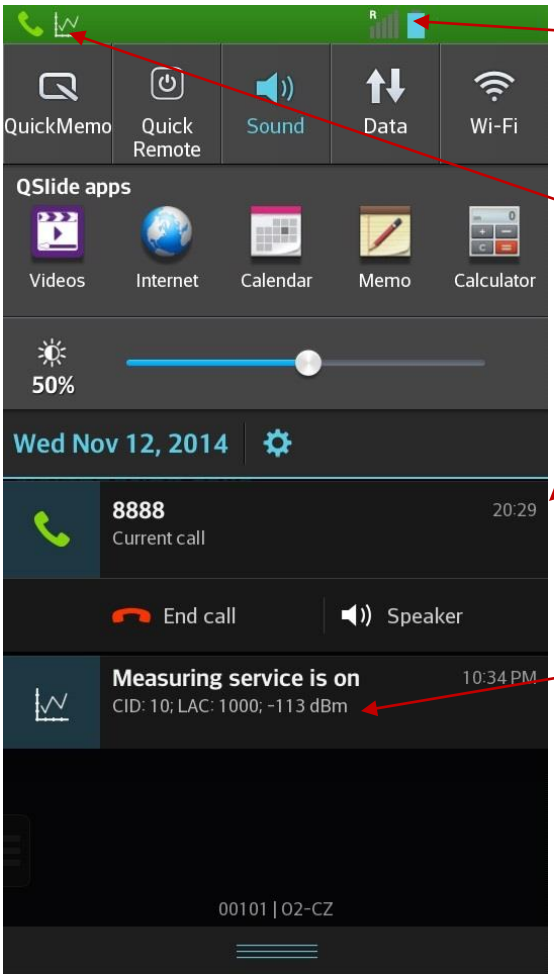
Aplicación ejecutándose y mostrando el valor de RSSI.

(Servicio de medición activado).

Nombre del operador de red.

Figura 5.3.2 Pantalla con Intensidad de Señal RSSI Mayor.

En la figura 5.3.2 se muestra que el teléfono está en los límites del alcance de la antena, con una señal recibida muy débil como para mantener una comunicación. Hasta este punto existe una pérdida de paquetes considerable y prácticamente ya no se puede escuchar lo que se está enviando desde el otro móvil.



En el límite de recepción. La señal recibida es muy débil.

Indica que se tiene establecida una llamada.

Duración de llamada en curso (la duración de llamadas no tiene límite, puede durar el tiempo que se desee).

Aplicación ejecutándose y mostrando el valor de RSSI. (Servicio de medición activado).

Figura 5.3.3 Pantalla con Intensidad de Señal RSSI Menor.

Para corroborar que la antena tiene un alcance de 80-85 metros (valor teórico) utilizamos la ecuación de un radio enlace [19] que involucra el margen de sensibilidad del receptor:

$$EIRP - PathLoss + Gtx = Sr \ldots\ldots\ldots\ldots (1)$$

Donde:

5.4 EIRP: (*Equivalent Isotropically Radiated Power*) o PIRE Potencia Isotrópica Radiada Equivalente. El EIRP es la cantidad aproximada de potencia que la antena isotrópica emite. Y se calcula sumando la potencia del transmisor, más la ganancia de la antena, menos perdidas por el cable de la antena.

$$EIRP = Pout + Gt - Lc \ldots\ldots\ldots\ldots\ldots (2)$$

Donde:

Pout: Potencia de salida del transmisor.

Gt: Ganancia de la antena.

Lc: Perdidas del cable.

Como en este caso no tenemos cable las perdidas solo un conector consideramos una pérdida de 0.25 dB.

$$EIRP = Pout + Gr - 0.25 \text{…….(3)}$$

5.5 PathLoss: Perdidas por trayectoria. En la práctica existen diversos factores que afectan la señal que se transmite por el aire. Estos factores disminuyen la potencia con la que señal es propagada mientras el receptor se aleja de la antena transmisora disminuyendo su alcance. El PathLoss lo calculamos con la siguiente formula [19].

$$PL = 32.44 + 20\log(d) + 20\log(f) \text{……..(4)}$$

Donde:

d: distancia en metros.

f: frecuencia en MHz

Sr: Sensibilidad del receptor.

En ecuación 2, sustituimos.

$$EIRP = 20 \text{ dB} + 3\text{dBi} - 0.25 \;\; ; \;\; EIRP = 22.75 \text{ [dB]} \text{…….(5)}$$

Sustituimos ecuaciones 4 y 5 en 1. Y el valor de la ganancia de la antena de transmisión Gtx = 3dBi y el valor de Sr que de acuerdo a la especificación GSM 05.05 se considera una sensibilidad de -110 dBm [18]. El Sr es el valor mínimo de potencia que el receptor es capaz de recibir.

$$22.75 - (32.44 + 20 \log (d) + 20 \log (1800)) + 3 = -110 \text{…….(6)}$$

De ecuación 6 despejamos d

$$20 \log (d) = 22.75 - 32.44 – 20 \log (1800) + 3 + 110$$

$$20 \log (d) = 38.2045 \text{ …….(7)}$$

Aplicando antilogaritmo a ambos términos:

$$d = 10^{\frac{38.20}{20}}$$

$$d = 81.3 \text{ [m]}$$

Perdidas por Trayectoria (*PathLoss*).

En la Figura 5.4.1 se observa que el indicador de la fuerza de la señal disminuye conforme a una distancia “d” entre emisor y receptor.

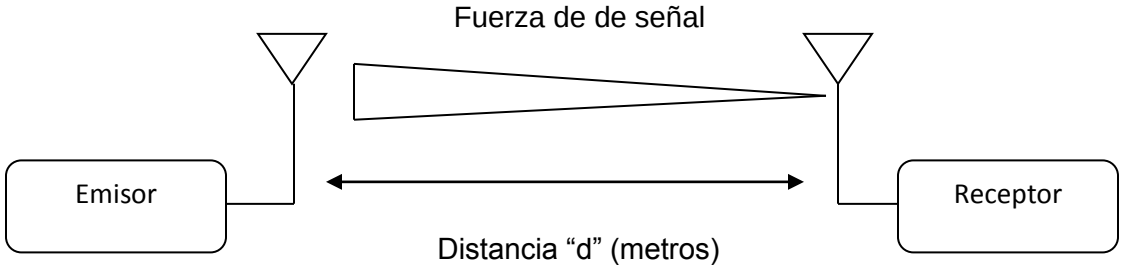


Figura 5.4.1 Emisor y Receptor Separados una Distancia d.

Existen diversas formas de expresar las pérdidas de fuerza de la señal en una transmisión. Existen modelos empíricos y determinísticos que no son alcance de este trabajo. Solo se le dio un enfoque a las perdidas por trayectoria (PathLoss) en el espacio libre.

La mayoría de las comparaciones y mediciones de radio frecuencia se realizan en decibeles [dB]. Esto es más fácil y consistente para comparar los niveles de señal que están presentes en determinados puntos. Es muy conveniente expresar la fórmula de pérdidas por trayectoria en espacio libre FSPL (Free Space Path Loss) en términos de decibeles [19].

$$FSPL \text{ [dB]} = 32.44 + 20 \log (d) + 20 \log (f)$$

Donde

d: distancia en metros

f: frecuencia en MHz

Con lo anterior podemos calcular el Pathloss total con f= 1800 MHz y una distancia de 81.3 metros (distancia teórica obtenida).

$$FSPL = 32.44 + 20 \log (81.3) + 20 \log (1800)$$

$$FSLP = 135.74 \text{ [dB]}$$

Con un Pathloss total de 135.74 [dB] podemos aproximar el valor de RRSI (teórico) con la siguiente formula [19].

$$RSSI_t = EIRP – PL + Gx ;$$

Donde Gx es la ganancia de la antena, de acuerdo a especificaciones del dispositivo utilizado, Gx = 3 dBi.

Sustituimos nuestros valores

$$RSSI_t = 22.75 \text{ [dB]} – 135.74 \text{ [dB]} + 3\text{dBi}$$

$$RSSI = -109 \text{ dBm}$$

A una distancia de 80 metros nuestro valor teórico de RSSI es -109 dBm mientras que el valor RSSI practico de RSSI desde 75-80 metros es RSSI = -113 [dBm].

Tenemos una buena aproximación de nuestro enlace emisor-receptor.

En la figura 5.17 podemos observar la gráfica de las perdidas en nuestro sistema.

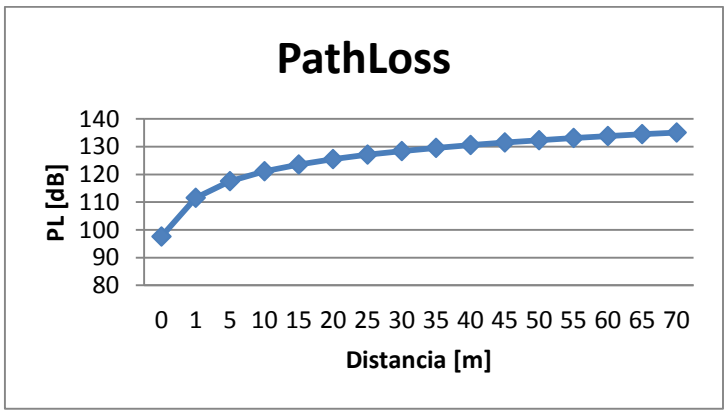


Figura 5.5.1 Gráfica de PathLoss del Sistema.

De forma teórica, se realizaron pruebas al aire libre y con línea de vista entre emisor y receptor.

La tabla 5.1 muestra las medidas tomadas a la distancia mostrada de la aplicación GSM Signal Monitoring desde un teléfono celular.

Distancia [m]	RSSI [dBm]
0	-51
5	-51
10	-55
15	-59
20	-65
25	-69
30	-73
35	-77
40	-79
45	-85
50	-87
55	-95
60	-99
65	-103
70	-107
75	-113
80	Sin señal

Tabla 5.1 Valores de RSSI prácticos.

En la tabla 1 se observan los valores de RSSI. Un valor aceptable de valores está dentro del intervalo [-40 a -80] para una buena calidad de comunicación.

- -80 dBm: es la señal mínima aceptable para establecer la conexión; puede ocurrir caídas de enlace.
- -70 dBm: enlace normal-bajo; es una señal medianamente buena.
- -60 dbm: enlace bueno; se puede lograr una conexión estable al 80%.
- -40a -60 dbm: señal idónea con una conexión estable.

En la Figura 5.6.1 se ve como la intensidad de la señal recibida disminuye conforme el receptor se aleja de la estación base.

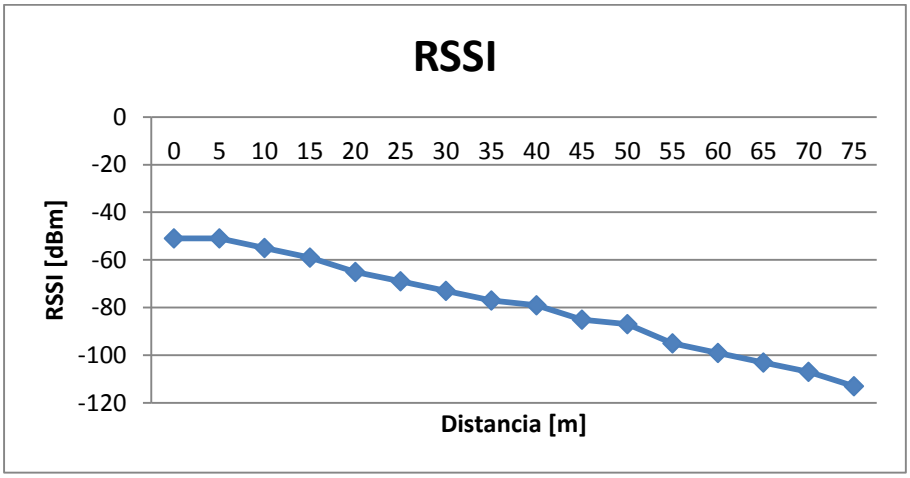


Figura 5.6.1 Gráfica de RSSI (práctico).

Las pruebas se realizaron al aire libre, a una distancia de 50 metros era posible mantener una conversación. Cuando emisor y receptor están alejados más de 50 metros, dentro de un intervalo de [55-70] metros la comunicación comienza a tener perdida de paquetes, señal poco audible y con silencios.

Hasta llegar a los 70 y 75 metros donde prácticamente nos encontramos en el límite del alcance de la antena transceptora. A 80 metros se pierde la señal, con esto se puede tomar como valor aproximado el alcance teórico de 81.3 metros.

Esto es debido a la calidad de la antena que se utilizó. Con un amplificador de potencia se podría contrarrestar este problema de cobertura y alcanzar una célula más grande.

Ahora para realizar la comparación entre RSSI práctico y RSSI teórico se utilizó la siguiente fórmula para poder calcular el RSSI teórico [19]. En la tabla 5.2 se presentan los resultados obtenidos.

$$RSSI = - (10\, n \log10\, (d) + A)$$

Donde:

n: Es el factor de perdida, (en este caso se considera en espacio libre n=2)

d: Distancia en metros.

A: Potencia de una señal recibida a una distancia de 1 metro. (A = -51 dBm)

D	RSSI
0	-
1	-51
5	-64.97940009
10	-71
15	-74.52182518
20	-77.02059991
25	-78.95880017
30	-80.54242509
35	-81.88136089
40	-83.04119983
45	-84.06425028
50	-84.97940009
55	-85.80725379
60	-86.56302501
65	-87.25826713
70	-87.9019608
75	-88.50122527
80	-89.06179974

Tabla 5.2 Valores de RSSI teórico.

5.6 SNR valores prácticos y teóricos.

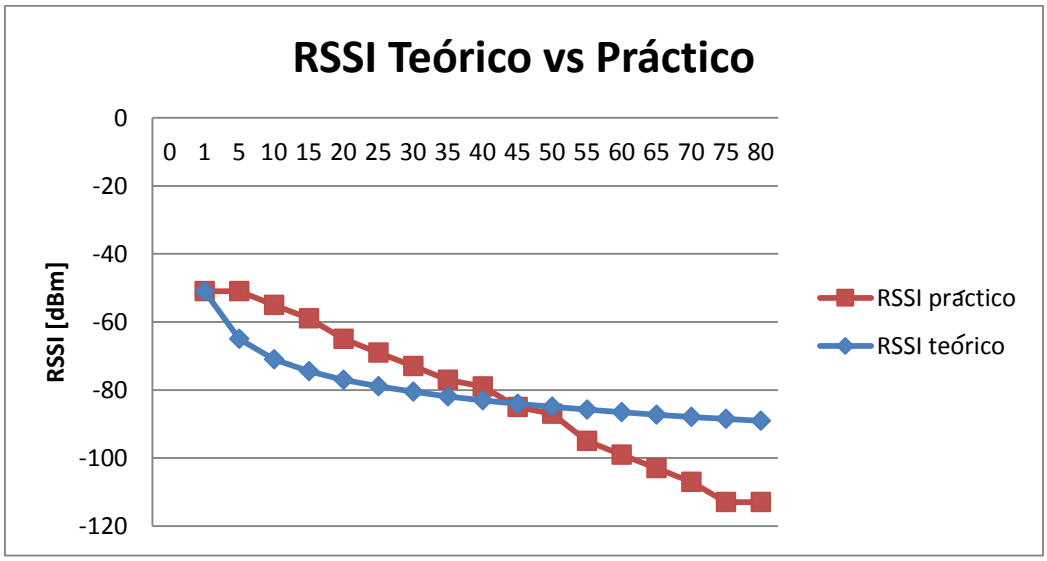


Figura 5.6.2 Gráfica de RSSI Teórico vs Práctico.

El RSSI práctico decae mucho más rápido que el RSSI teórico. En la figura 5.20 el RSSI práctico hasta una distancia de 40-45 metros decae igual que el RSSI teórico. Pasando los 45 metros el RSSI práctico decae más rápido, debido a que la señal va perdiendo cada vez más potencia. Esto es debido a las pérdidas por trayectoria en el espacio libre.

5.7 SNR

El SNR relación señal a ruido *(signal-to-noise ratio*) impacta en el rendimiento de una buena conexión. Un valor de SNR alto significa que la intensidad de la señal es más fuerte en relación a los niveles de ruido, lo que permite mantener una buena comunicación y por lo cual un mejor rendimiento. Al contrario, un SNR menor disminuye el rendimiento.

El ruido (*noise*) se compone de varios factores que degradan la señal al ser transportada hasta su destino. Es una combinación de las fuentes de señal interferentes no deseadas en la recepción, tales como interferencia de radiofrecuencia, distorsión, diafonía, etc. Este valor se mide en dB (decibelios) con valores que van desde 0 a -120. Cuanto más cerca de -120 este el valor significa que hay poca interferencia. Valores típicos oscilan entre -100 y -80. Para calcular el SNR recurrimos a la formula [19].

SNR = RSSI – N

Para calcular la potencia de ruido tenemos la ecuación de potencia de ruido [19].

$$N = 10 \log (T\ BW\ K) + Nf$$

Donde:

N: Potencia de ruido

T: Temperatura de referencia (290 grados Kelvin)

BW: ancho de banda del canal (200 KHz)

K: Constante de Boltzman. K = 1.38×10^{-23} Joule/^{o}K

Nf: Figura de ruido. Nf = 8 dB

$$N = 10 \log (290 * 200000 * 1.38 \times 10^{-23}) + 8 ; \quad N = -147$$

Para tener el ruido en dB, sumamos la cantidad respectiva de 30.

$$N = - 147 + 30$$

$$N = -112 \text{ [dB]}$$

Aplicando el ruido anterior a SNR = RSSI – N. En la tabla 5.3 se muestran los niveles de SNR obtenidos.

Distancia [m]	RSSI [dBm]	SNR [dB]
0	-51	61
5	-51	61
10	-55	57
15	-59	53
20	-65	47
25	-69	43
30	-73	39
35	-77	35
40	-79	33
45	-85	27
50	-87	25
55	-95	17
60	-99	13
65	-103	9
70	-107	5
75	-113	0
80	-113	-

Tabla 5.3 Valores de SNR prácticos.

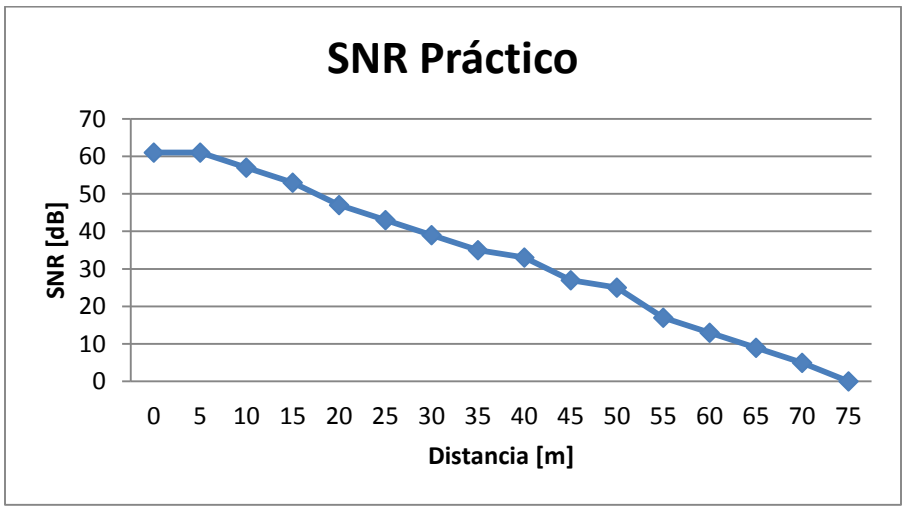


Figura 5.7.1 Gráfica de SNR (práctico).

La figura 5.7.1 muestra la gráfica de SNR práctico. Después de 50 metros la potencia de ruido es mayor a la señal que se está transmitiendo, por tal motivo se empiezan a perder paquetes. Un valor de SNR por encima de los 20 dB se considera bueno.

Ahora aplicamos este mismo ruido a los valores de SNR teóricos (con los valores de RSSI teóricos, que se calcularon anteriormente)

Distancia [m]	SNR [dB]	SNR teórico
0	61	-
5	61	47.0205999
10	57	41
15	53	37.4781748
20	47	34.9794001
25	43	33.0411998
30	39	31.4575749
35	35	30.1186391
40	33	28.9588002
45	27	27.9357497
50	25	27.0205999
55	17	26.1927462
60	13	25.436975
65	9	24.7417329
70	5	24.0980392
75	0	23.4987747
80	-	22.9382003

Tabla 5.4 Valores de SNR teóricos

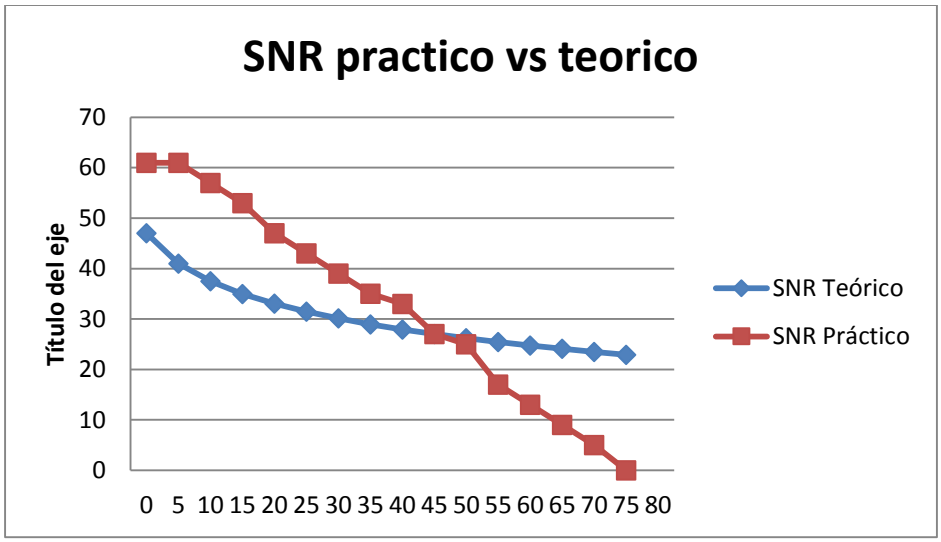


Figura 5.8.1 Gráfica SNR Práctico vs Teórico.

5.8 SNR Práctico vs Teórico.

Al igual que el RSSI, la gráfica de la figura 5.8.1 muestra que al principio tiene un buen registro de SNR, mientras el receptor se aleja de la antena transmisora se va perdiendo la señal y el ruido empieza a afectar en cantidad mayor a la intensidad de señal recibida.

Los componentes en el mundo real son fuentes de ruido adicional que el ruido de interferencia en la señal, así que este valor está sobre los niveles promedio y son más grandes que el ruido calculado teóricamente. Además el receptor agrega su propio ruido por los elementos resistivos en su front end.

CAPITULO 6

CONCLUSIONES

Como se observa en las imágenes del capítulo anterior ya se tiene desplegada una interfaz de aire GSM (interfaz Um), en la cual podemos registrar teléfonos celulares mediante la obtención de su IMSI y como administrador se le puede conceder el acceso o no. La problemática que se abordó fue poder desplegar un servicio de telefonía de segunda generación GSM de bajo costo.

Este proyecto se basó en código abierto y software libre. Los proyectos de código abierto tienen una gran ventaja con respecto a los de código cerrado, y es la innovación y el desarrollo que se deriva de esos proyectos, convirtiéndolos en oportunidades económicas, viables y factibles.

Las llamadas telefónicas se realizaron al aire libre para verificar el alcance de la antena utilizando la banda de 1800 MHz, ya que el hacer uso de bandas comerciales de telefonía celular es complicado y el poder obtener un permiso para hacer uso de esas bandas el costo es elevado. Las condiciones de las pruebas realizadas fueron en línea de vista sin obstáculos y se obtuvo un rendimiento funcional con distancias de entre 45 – 50 metros de la antena para mantener una comunicación estable.

Con las mediciones obtenidas de RSSI se pueden determinar los casos en que la señal recibida es útil a cierta distancia.

La sección de PathLoss representa una gran fuente de pérdidas en el enlace, y existen otros efectos negativos en la propagación que reducen la potencia de la señal.

El software OpenBTS utiliza radio definido por software para presentar la interfaz de aire a los teléfonos móviles de los usuarios. Al mismo tiempo como lo hace asterisk, los dispositivos son presentados como terminales SIP a internet.

Con las pruebas de llamadas realizadas y envió de mensajes, ahora se cuentan con las bases necesarias para seguir desarrollando este tipo de tecnologías que son una alternativa atractiva para tener acceso a comunicaciones móviles.

Los datos obtenidos se alcanzaron gracias a la práctica en espacios exteriores (*outdoors*) y con un sistema de corto alcance (micro-célula) las pérdidas y ganancias son aproximadas ya que en la práctica es difícil de alcanzar la teoría de las comunicaciones.

Por último las principales aplicaciones de está micro-célula son para permitir brindar servicio de comunicaciones de telefonía celular de segunda generación en lugares donde no existe cobertura o es muy escasa, también en casos de emergencia cuando la red convencional no está en funcionamiento. Este es un sistema pequeño que se puede montar en poco tiempo.

TRABAJO FUTURO

En la actualidad, la demanda de los servicios de telefonía celular sigue creciendo exponencialmente. Empresas, negocios, personas requieren de servicios de comunicación móvil cada día.

Lo que hace a este tipo de proyectos un aspecto atractivo es que el software es actualizable y el hardware no se vuelve inservible u obsoleto, esto permite continuar con investigaciones, como por ejemplo para saber la capacidad del sistema, ya que no se pudo completar en este trabajo, debido a que no se cuenta con los teléfonos necesarios (compatibles con la banda de 1800 Mhz) para realizar esta operación. La mayoría de teléfonos en México operan en las bandas de 850-900-1900 MHz.

Este tipo de red inalámbrica luce prometedora para desplegar tecnologías aún más avanzadas. A principios del año 2014 se liberaron códigos para desplegar 2.5G - GSM y GPRS.

También en el mes de Julio del año 2014 se liberó la publicación inicial de 3G – UMTS.

Estos últimos aún siguen en proceso de desarrollo generando oportunidades para continuar con la investigación, lo que hace importante a este tipo de sistemas es que son una opción muy prometedora en la innovación con tecnología emergente y que podría llegar a hacer competencia a las tecnologías que se usan actualmente.

GLOSARIO DE ACRÓNIMOS

AGCH	Access Grant Channel. Canal de Concesión de Acceso
ADC	Analog to Digital Converter. Convertidor Analógico Digital
AuC	Authentication Centre. Centro de Autenticación
BCH	Broadcast Channels. Canales de Difusión
BCCH	Broadcast Control Channel. Canal de Control de Difusión
BSS	Base Station Subsystem. Subsistema de Estación Base
BSC	Base Station Controller. Estación Base de Control
BTS	Base Transceiver Station. Estación Base Tranceptora
CBCH	Cell Broadcast Channel. Canal de Difusión de célula
CCCH	Common Control Channels Canales de Control Común
Cell	Célula
DAC	Digital to Analog Converter. Convertidor Analógico Digital
DCCH	Dedicated Control Channels. Canales de Control Dedicado
DSP	Digital Signal Processor. Procesador digital de señales.
DUC	Digital Up Converter
DDC	Digital Down Converter
DL	Downlink. Enlace descendente.
EIR	Equipment Identity Register. Registro de Identidad del Equipo
ETSI	European Telecommunications Standards Institute
FACCH:	Fast Associated Control Channel. Canal de control Asociado rapido
FCCH	Frequency Correction Channel. Canal de Corrección de Frecuencia.
FDD	Frequency Division Duplex
FDMA	Frequency Division Multiple Access
FPGA	Field Programmable Gate Array
GPRS	General Packet Radio Services
GMSC	Gateway Mobile-services Switching Centre. Centro de Conmutación de Servicios Móviles.
GMSK	Gaussian Minimum Shift Keying
GNU-R	GNU Radio
GSM	Global System for Mobile Communications
HLR	Home Location Register. Regístro de Localización Local
HSPA	High Speed Packet Access
IMSI	International Mobile Subscriber Identity. Identidad Internacional del Suscriptor Móvil
IF	Frecuencia Intermedia
IP	Protocolo de Internet
MCC	Mobile Country Code. Código Móvil de País.
MHz	Mega Hertz
MNC	Mobile Network Code. Código Móvil de Red.
MS	Mobile Station. Estación Móvil

MSC	Mobile-services Switching Centre. Centro de Conmutación Móvil.
MSISDN	Station International ISDN number(s). Numero Internanal ISDN.
NSS	Network Subsystem. Subsistema de Red
OMC	Operation and Maintenance Center
OPENBTS	Estación Base Transceptora Libre.
O&M	Operaton and Management. Operacion Y Mantenimiento
PCH	Paging Channel. Canal de Búsqueda
PLMN	Public Land Mobile Network. Red Móvil Terrestre Publica.
RACH	Random Access Channel. Canal de Acceso Aleatorio
RF	Radio Frecuencia
SACCH	Slow Associated Control Channel
SCH	Synchronization Channel. Canal de Sincronización
SDCCH	Stand alone Dedicated Control Channel. Canal de Control Dedicado Independiente.
SDR	Software Defined Radio. Radio Definido por Software.
SIM	Subscriber Identity Module. Módulo de Identificación del Subscriptor
SMS	Short Message
TCH	Traffic Channels. Canales de Tráfico
TIMSI	Temporary International Mobile Subscriber Identity
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
UL	Uplink. Enlace Ascendente.
UMTS	Universal Mobile Telecommunications System
USRP	Universal Software Radio Peripheral
VLR	Visitor Location Register .Registro de Localización de Visitantes
WLAN	Wireless Local Area Network
WPAN	Wireless Public Area Network
WWAN	Wireless Wide Area Network
1G	1ra Generación de Telefonía Móvil
2G	2da Generación de Telefonía Móvil
3G	3ra Generación de Telefonía Móvil
4G	4ta Generación de Telefonía Móvil

REFERENCIAS

[1] Portal de la Extinta Comisión Federal de Telecomunicaciones
Disponible desde internet en: <http://www.cft.gob.mx:8080/portal/>

[2] Ettus Research a National Instruments Company
Disponible desde internet en: <http://www.ettus.com/home>

[3] OpenBTS Open Source Celullar Infrastructure
Disponible desde internet en: <http://openbts.org/>

[4] Asterisk Project
Disponible desde internet en: <http://www.asterisk.org/>

[5] Asociación GSM, GSMA
Disponible desde internet en:< http://www.gsma.com/aboutus/gsm-technology/gsm>

[6] GSM 04.04 (ETS 300 553): "Digital cellular telecommunications system (Phase 2); layer 1 General requirements".

[7]Huidobro Manuel
Comunicaciones Móviles: Sistemas GSM, UMTS y LTE
Alfaomega Ra-Ma

[8] Jörg Eberspächer, Hans-Jörg Vögel, Christian Bettstetter, Christian Hartmann
GSM - Architecture, Protocols and Services
Third Edition, 2009 John Wiley & Sons

[9] Faúndez Zanuy Marcos. Sistemas de Comunicaciones, Marcombo, p. 86, 87, 88

[10] Arteaga, Arce. Arquitectura de un Sistema de Monitoreo Radioeléctrico usando Software Defined Radio. Revista S&T, 2012, 83-93

[11] Abul Azad, “Open BTS Implementation with Universal Software Radio Peripheral” 2010

[12] Ettus Research, USRP™ N200/N210 Nerworked Series
Features and Product Detalis.
Disponible en:
https://www.ettus.com/content/files/07495_Ettus_N200-210_DS_Flyer_HR_1.pdf

[13] GSM 05.02: \Digital cellular telecommunications system (Phase 2+); Multiplexing and multiple accesson the radio path"

[14] Rughinis, Razvan. Iconaru, Cristian. (2008). A practical Analysis of Asterisk SIP Server Performance.

[15] David A. Burgess, Harvind S. Samra “The Open BTS Project”

Kestrel Signal Processing, Inc.Fairfield, California. August, 2008 p. 15,16

[16] UIT-T Q.921 SECTOR DE NORMALIZACIÓN DE LAS TELECOMUNICACIONES DE LA UIT. SERIE Q: CONMUTACIÓN Y SEÑALIZACIÓN.
Sistema de señalización digital de abonado N.° 1 – Capa de enlace de datos
Interfaz usuario-red de la RDSI – Especificación de la capa de enlace de datos
Disponible en < https://www.itu.int/rec/T-REC-Q.921-199709-I/es>

[17] Range Public, OpenBTS Public Release
Disponible en: <https://wush.net/trac/rangepublic>

[18] GSM 05.05 (3GPP TS) Digital cellular telecommunications system (Phase 2+); Radio Transmission and Reception.

[19] John S. Seybold. Introduction to RF Propagation. John Wiley & Sons p [66-80]

[20] Siegmund H. Redl, Mathias K. Weber, Malcolm W. Oliphant. An Introduction to GSM. Artech House, 1995.

[21] Joachin Tisal, GSM Celullar Radio Telephony. John Wiley & Sons, 1998.

Anexo. Instalación y configuración de OpenBTS

La mejor forma de conseguir OpenBTS es descargando el código directamente del repositorio. Mediante el siguiente comando:

svn co http://wush.net/svn/range/software/public

Una vez obtenido el código, instalar las bibliotecas/utilidades requeridas:

autoconf

libtool

libosip2

libortp

libusb-1.0

g++

sqlite3

libsqlite3-dev (sipauthserve only)

libreadline6-dev

libncurses5-dev

Esto se instala con el siguiente comando.

sudo apt-get install autoconf libtool libosip2-dev libortp-dev libusb-1.0-0-dev g++ sqlite3 libsqlite3-dev erlang libreadline6-dev libboost-all-dev

Además se necesita la librería liba53, que viene incluida con la distribución de OpenBTS descargada. Desde la raíz de openBTS a53/trunk

sudo make install

Para compilar y estructurar OpenBTS desde openbts/trunk ejecutar los siguientes comandos

autoreconf -i

./configure

make

Ahora se debe crear un enlace para el transceptor apropiado para el hardware (Ettus N210)

cd apps

make

ln -s ../TransceiverRAD1/transceiver .

ln -s ../TransceiverRAD1/ezusb.ihx .

ln -s ../TransceiverRAD1/fpga.rbf .

Se crea el directorio llamado OpenBTS donde colocar todo lo relacionado con el sistema OpenBTS ejecutando el siguiente comando.

mkdir OpenBts cd OpenBTS

GNU Radio: para este proyecto se utilizó el Ettus USRP N210, por lo que fue necesario el uso de UHD (dispositivos de hardware universal).

sudo bash -c 'echo "deb

http://files.ettus.com/binaries/uhd_stable/repo/uhd/ubuntu/`lsb_release -cs` `lsb_release -cs` main" > /etc/apt/sources.list.d/ettus.list'

sudo apt-get update

sudo apt-get install -t `lsb_release -cs` uhd

Configuración de OpenBTS

OpenBTS se tiene que configurar para funcionar correctamente. Hay archivos que se deben crear para que esto suceda.

En el directorio /etc/OpenBTS/OpenBTS.db. OpenBTS.db está la base de datos para todas las configuraciones OpenBTS. Debe ser instalado en / etc / OpenBTS.

Así, con el fin de crear este archivo ejecutamos los siguientes comandos desde el directorio OpenBTS.

sudo mkdir /etc/OpenBTS sudo sqlite3 -init ./apps/OpenBTS.example.sql /etc/OpenBTS/OpenBTS.db ".quit

GSM.Radio.Band - en este proyecto se ha seleccionado la banda de 1800 MHz.

GSM.Radio.C0 - este es el ARFCN. Canal 512 fue seleccionado en este trabajo.

Control.LUR.OpenRegistration - poner esto en una expresión regular de números que coinciden con el IMSI de los teléfonos de la prueba. Esto le dice a OpenBTS no rechazar las terminales de prueba sólo porque su servidor de registro no está respondiendo.

Para instalar asterisk ejecutar el comando: sudo apt-get install asterisk

Para editar el archivo OpenBTS.db es recomendable descargar e instalar SQLite Database Browser que permite visualizar la totalidad de la base de datos y sus campos.

sudo apt-get install sqlitebrowser

Entonces es posible ejecutar la Base de datos SQLite llamándolo en el terminal:

sudo sqlitebrowser

Registro de suscriptor y Sipauthserve: OpenBTS depende de la instalación de Sipauthserver el servidor de autorización SIP. Se tiene que instalarlo antes de ejecutar OpenBTS.

cd subscriberRegistry/trunk/configFiles/

sudo mkdir -p /var/lib/asterisk/sqlite3dir

sudo sqlite3 -init subscriberRegistryInit.sql /var/lib/asterisk/sqlite3dir/sqlite3.db

Sipauthserve es un centro de autenticación SIP. La variable de configuración SIP.Proxy.Registration en OpenBTS debe apuntar a su nombre de host y el puerto. Para construir Sipauthserve, debe tener OpenBTS ya ejecutadas. Este es un hack makefile, y se espera que se fije en algún momento en el futuro. Para instalar Sipauthserve (de la raíz svn) ejecutar los siguientes comandos.

cd subscriberRegistry/trunk make

Esto producirá un ejecutable Sipauthserve. Al igual que con OpenBTS, se requiere un archivo de configuración.

/ etc / OpenBTS / desde la raíz subscriberRegister, se ejecutan los siguientes comandos:

sudo sqlite3 -init sipauthserve.example.sql /etc/OpenBTS/sipauthserve.db ".quit"

Smqueue: Smqueue es el servicio de mensajes empaquetado con OpenBTS.

En el directorio smqueue / trunk, se ejecutan los siguientes comandos:

autoreconf -i ./configure make

Después de esto, un ejecutable Smqueue se crea en el directorio Smqueue / trunk / Smqueue.

Configuración Smqueue: Similar a OpenBTS, Smqueue también depende de un archivo de configuración, que se encuentra en /etc/OpenBTS/smqueue.db. Smqueue crea una versión vacía, no funcional de esta base de datos si no está disponible. Se ejecuta el siguiente comando desde el directorio Smqueue.

sudo sqlite3 -init smqueue/smqueue.example.sql /etc/OpenBTS/smqueue.db ".quit"

Correr OpenBTS: Conectar la fuente de alimentación y después los indicadores luminosos de alimentación se encienden, conectar el dispositivo a la computadora a través del cable Gigabit Ethernet. Ahora se siguen estos sencillos pasos para ejecutar todo el sistema.

Asegúrese de que el ordenador reconoce el dispositivo UHD. Para probar si esto funciona puede encontrar el N210 USRP con el comando:

uhd_find_devices

Verificar que los leds indicadores estén activos.

Después de eso ejecutar en una terminal por separado cada uno de los elementos antes mencionados.

sudo asterisk –rvvv

subscriberRegistry/trunk/sipauthserve

Smqueue: este es el directorio para buscar en, ~ OpenBTS / public / Smqueue / trunk / Smqueue /

sudo ./smqueue

OpenBTS: en el directorio, ~OpenBTS/public/openbts/trunk/apps/.

Sudo ./OpenBTS

Esta es la consola de OpenBTS y podemos mover las variables de configuración.

Para entrar a la interfaz de comandos de OpenBTS ejecutar en OpenBTS/public/openbts/trunk/apps/.

Sudo ./OpenBTSCLI

Una vez en la CLI el comando: Config

Mostrará una gran cantidad de opciones de configuraciones, también aquí el usuario puede acceder a toda la configuración y los mandatos de supervisión, es decir, "chans", que muestra el estado del canal de la tabla de canales como RSSI dB señal ascendente RSSI en la BTS, en dB con respecto a la escala completa. Ahora el paquete de software se está ejecutando correctamente y listo para los teléfonos para administrar. También en este punto se recomienda revisar las luces USRP, los LEDs ACEDF en la N210 estos deben ser iluminados y los LED verde y naranja en el puerto Ethernet deben estar también.

Ahora es posible utilizar un teléfono con una tarjeta GSM SIM y compatible con la banda de 1800 MHz. Sería mejor si esta SIM no era de una compañía local; entonces el teléfono no se registrara inmediatamente a una de sus estaciones base en la zona. En la mayoría de los casos, en la mayoría de los teléfonos, hay una manera de seleccionar la red específica que desea seleccionar por el menú del teléfono para escanear las redes disponibles. Para este registro, la red que se debe seleccionar es: 001 01 o una variante por default que es “Range”. Conecte el teléfono a la red. La BTS debe responder con un mensaje de bienvenida, que permite la conexión y enviar de vuelta su IMSI.