



**UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO**

**FACULTAD DE ESTUDIOS SUPERIORES
CUAUTITLÁN**

**Localización de un teléfono móvil basado en la red
celular**

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO MECÁNICO ELECTRICISTA

P R E S E N T A :

JOSÉ ANTONIO ZAMORA RODRÍGUEZ

A S E S O R :

ING. GILBERTO CHAVARRÍA ORTIZ

CUAUTITLÁN IZCALLI, ESTADO DE MÉXICO, 2019



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.



UNIVERSIDAD NACIONAL
AUTÓNOMA DE
MÉXICO

**FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN
SECRETARÍA GENERAL
DEPARTAMENTO DE EXÁMENES PROFESIONALES**

U. N. A. M.
ASUNTO: **VOTO APROBATORIO**

**M. en C. JORGE ALFREDO CUÉLLAR ORDAZ
DIRECTOR DE LA FES CUAUTITLÁN
PRESENTE**

**ATN: I.A. LAURA MARGARITA CORTAZAR FIGUEROA
Jefa del Departamento de Exámenes Profesionales
de la FES Cuautitlán.**

Con base en el Reglamento General de Exámenes, y la Dirección de la Facultad, nos permitimos comunicar a usted que revisamos el: **Trabajo de Tesis**

Localización de un teléfono móvil basado en la red celular

Que presenta el pasante: JOSÉ ANTONIO ZAMORA RODRÍGUEZ
Con número de cuenta: 41102831-0 para obtener el Título de la carrera: Ingeniería Mecánica Eléctrica

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el **EXAMEN PROFESIONAL** correspondiente, otorgamos nuestro **VOTO APROBATORIO**.

ATENTAMENTE
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Cuautitlán Izcalli, Méx. a 11 de abril de 2019.

PROFESORES QUE INTEGRAN EL JURADO

	NOMBRE	FIRMA
PRESIDENTE	Ing. Juan González Vega	
VOCAL	Ing. Gilberto Chavarría Ortiz	
SECRETARIO	Ing. Silverio Joel Sánchez Pérez	
1er. SUPLENTE	M. en T.I.C. Alma Alejandra Luna Gómez	
2do. SUPLENTE	Ing. Omar Tequipaneca Escobar	

NOTA: los sinodales suplentes están obligados a presentarse el día y hora del Examen Profesional (art. 127).

LMCF/ntm*

AGRADECIMIENTOS

Al final de esta etapa tan importante para mí y que a pesar de contratiempos y tropiezos estoy concluyendo, quiero dar las gracias a todos aquellos que de forma directa o indirecta me apoyaron para que esto se pudiera realizar.

Primeramente, gracias a mi universidad por permitirme formar parte de sus aulas, sus pasillos, sus jardines y de la cual me llevo grandes momentos, experiencias, conocimientos y muchas anécdotas, recuerdos que definitivamente serán para toda la vida. Gracias a cada uno de mis maestros por formarme como profesional, por compartir conmigo su experiencia y hacer de mí un mejor estudiante y ciudadano, de cada uno de ustedes me llevo los mejores consejos. Gracias de igual forma, a mi asesor de tesis, por el tiempo que me brindó para guiarme, revisar y acompañarme a lo largo de este proyecto.

Muchas gracias a mis amigos y compañeros, gracias por su apoyo, porque con algunos de ustedes empecé esta hermosa aventura académica y que con cada nivel avanzado encontré a más de ustedes, para así, concluir por ahora, mi etapa de estudiante. Agradezco ese compañerismo para juntos salir adelante.

Y por último pero para mí más importante, muchas gracias a mis padres, mis abuelos, mi familia, que de no ser por ustedes jamás hubiera podido pisar esta universidad, gracias a cada uno de ustedes por sus consejos y su apoyo, pero en especial, gracias mamá por tu esfuerzo, tu trabajo y tu responsabilidad para sacarme adelante, gracias abuela y abuelo por criarme y enseñarme a ser alguien de bien. Gracias dios por poner en mi vida a cada uno de ellos.

ÍNDICE

ÍNDICE	4
1 TELEFONÍA FIJA	9
1.1 Telefonía sobre conmutación de circuitos	11
1.2 Telefonía sobre conmutación de paquetes	12
1.2.1 Circuitos virtuales	13
1.2.2 Datagramas	14
1.3 Jerarquización de la red telefónica	14
1.4 Comunicación entre dos abonados	16
2 TELEFONÍA MÓVIL	17
2.1 Elementos del teléfono móvil	17
2.2 Radio bases	23
3 EVOLUCIÓN DE LA TECNOLOGÍA DE COMUNICACIÓN MOVIL	30
3.1 Primera generación 1G	30
3.2 Segunda generación G2	30
3.2.1 Sistema global para comunicaciones móviles (GSM)	31
3.2.2 Arquitectura de la red GSM	31
3.3 Generación 2.5	33
3.3.1 Servicio general de paquetes vía radio (GPRS)	33
3.3.2 Tasas de datos mejoradas para la evolución de GSM (EDGE)	33
3.4 3GPP	34
3.5 Tercera generación 3G	34
3.5.1 Sistema universal de telecomunicaciones móviles (UMTS)	35
3.6 Generación 3.5G Acceso ascendente de paquetes a alta velocidad (HSDPA)	35
3.7 Cuarta generación 4G LTE	35
3.8 Quinta generación	36
4 ARQUITECTURA DE UNA RED GSM	37
4.1 El subsistema de estaciones base BSS	38
4.1.1 La terminal móvil (MS)	39
4.1.1.1 La terminal (ME)	39
4.1.1.2 La tarjeta SIM	40
4.1.2 La estación radio base (BTS)	42
4.1.3 La estación controladora (BSC)	43
4.1.4 La unidad transcodificadora TRAU	44
4.2 El subsistema de conmutación de red (NSS)	44
4.2.1 La central de conmutación móvil (MSC)	46
4.2.2 Registro de datos local (HLR)	46

4.2.3	Registro de datos de visitantes (VLR)	48
4.2.4	Centro de autenticación (AuC)	48
4.2.5	Registro de identidad de equipos (EIR)	49
4.3	El subsistema de operación y mantenimiento (OSS)	49
5	INTERFACES Y PROTOCOLOS USADOS EN GSM.....	52
5.1	Interfaces de la red GSM	52
5.2	Protocolos y señalización en la red GSM	55
5.2.1	Aspectos de red.....	60
5.2.1.1	Gestión de recursos de radio (RR).....	61
5.2.1.1.1	Handover	62
5.2.1.1.2	Tiempo de avance.....	63
5.2.1.1.3	Salto de frecuencia	64
5.2.1.1.4	Transmisión discontinua (DTX).....	64
5.2.1.1.5	Control de potencia.....	65
5.2.1.2	Gestión de movilidad (MM).....	66
5.2.1.2.1	Location update	66
5.2.1.2.2	Autenticación y seguridad.....	67
5.2.1.3	Gestión de las comunicaciones.....	67
6	ESTADOS DEL MÓVIL EN UNA RED GSM.....	69
7	LA INTERFAZ DE RADIO Y CANALIZACIÓN EN LA RED GSM.....	73
7.1	Esquema de acceso	73
7.2	Plan de frecuencias	73
7.3	Canalización GSM.....	74
7.3.1	Canales de señalización	77
7.3.2	Canal de tráfico (TCH)	79
8	POSICIONAMIENTO	81
8.1	Introducción a los métodos de posicionamiento	82
8.1.1	Posicionamiento basado en la cobertura de la célula.....	82
8.1.2	Posicionamiento basado en el tiempo de ida y vuelta.	83
8.1.3	Posicionamiento por la diferencia de tiempos de llegada.	84
8.1.4	Diferencia de tiempos observada mejorada	85
8.1.5	Posicionamiento por el tiempo de llegada	86
8.1.6	Posicionamiento por el ángulo de llegada.....	87
8.1.7	Posicionamiento basado en el nodo de referencia	88
8.1.8	Sistema de posicionamiento global	89
8.1.9	Sistema de navegación por satélite Galileo.....	91
8.2	Precisión del posicionamiento.....	92

8.3	Métodos de posicionamiento especificados para GSM y UMTS	93
8.3.1	Posicionamiento basado en el ID de la Célula	94
8.3.2	Diferencia de tiempos de llegada observados- periodo inactivo en enlace descendente en UMTS.....	95
8.3.3	GPS Asistido	96
8.4	Arquitectura del sistema para los servicios de localización.....	97
8.5	Funciones del LCS en la red central.	100
9	POSICIONAMIENTO CON HLR	102
10	EVOLUCIÓN DEL LOS SERVICIOS DE LOCALIZACIÓN EN LAS NUEVAS TECNOLOGÍAS	107
10.1	HLR y VLR en la arquitectura de las redes UMTS o de tercera generación.	107
10.2	HLR y VLR en la arquitectura de las redes LTE o de cuarta generación....	108
10.3	Gestión de movilidad en LTE	110
10.3.1	Marco de gestión de movilidad	111
10.3.2	Gestión de localización.	112
11	APLICACIÓN DE LA LOCALIZACIÓN DE EQUIPOS MÓVILES CON LA RED MÓVIL.	114
12	CONCLUSIONES	117
12.1	Líneas futuras	118
	BIBLIOGRAFÍA	119
	GLOSARIO Y ACRÓNIMOS	121

INDICE DE TABLAS

Tabla 5.1.	Interfaces y Protocolos de GSM.....	59
Tabla 7.1.	Canales en GSM	79

ÍNDICE DE FIGURAS

Figura 1.1.	Red fija local.....	10
Figura 1.2.	Enlace de telefonía fija Dedicado	11
Figura 1.3.	Formato de una trama.....	12
Figura 1.4.	Jerarquía de la red telefónica fija.....	15
Figura 1.5.	Tonos de información de acuerdo con la UIT-T	16
Figura 2.1.	Partes que conforman un Smartphone	19
Figura 2.2.	Ejemplo de una red celular.....	21
Figura 2.3.	Células de telefonía móvil	21
Figura 2.4.	Plano Aproximado de una radiobase.	24
Figura 2.5.	Estructura tipo torre.....	26
Figura 2.6.	Estructura tipo monopolo.....	27

Figura 2.7. Estación con estructura de tipo móvil	27
Figura 2.8. Equipos de una radio base en azotea.....	28
Figura 2.9. Antenas de microondas montada en torre	29
Figura 3.1. Evolución de la familia GSM.....	36
Figura 4.1. Arquitectura de una red GSM.....	37
Figura 4.2. Sub-sistema BSS.....	38
Figura 4.3. Terminales móviles	40
Figura 4.4. Tarjeta SIM.....	41
Figura 4.5. Contactos según la norma ISO/IEC 7810 para una SIM	42
Figura 4.6. Sub-Sistema NSS en una red GSM.....	45
Figura 4.7. Estructura del número IMSI.....	47
Figura 4.8. Estructura del número MSISDN	48
Figura 4.9. Numero IMEI.....	49
Figura 4.10. Sub-Sistema OSS en una red GSM.....	51
Figura 5.1. Esquema de interfaces en el estándar GSM	53
Figura 5.2. Protocolos GSM	56
Figura 5.3. Protocolos MAP/X.....	60
Figura 5.4. Concepto de Handover.....	63
Figura 5.5. Control de Potencia	65
Figura 6.1. Estados del Móvil en GSM	69
Figura 6.2. Secuencia de mensajes de Attach.....	70
Figura 6.3. Estados del móvil en GPRS	72
Figura 7.1. Estructura del Burst	75
Figura 8.1. Posicionamiento Basado en el Tiempo de Ida y Vuelta.	83
Figura 8.2. Posicionamiento por la diferencia de tiempos de llegada.	85
Figura 8.3. Posicionamiento por el Tiempo de Llegada.....	86
Figura 8.4. Posicionamiento por el Angulo de Llegada.....	88
Figura 8.5. Sistema de Posicionamiento Global.....	90
Figura 8.6. Sistema de Navegación por Satélite Galileo.....	91
Figura 8.7. Comparación de la precisión que ofrecen los diferentes sistemas de posicionamiento	92
Figura 8.8. Arquitectura general de los Servicios de Localización (LCS) en redes UMTS	98
Figura 8.9. Modelo de referencia de los Servicios de Localización en GERAN.	99
Figura 9.1. Precisión con la técnica Cell ID	104
Figura 9.2. Diagrama de radiación.....	105
Figura 9.3. Cell ID con antena sectorizada, Time Advance y E - CGI	105
Figura 10.1. Arquitectura de una red UMTS	108
Figura 10.2. Arquitectura de la red LTE.....	109
Figura 11.1. Monitoreo de datos de bajada Arieso ©	116
Figura 11.2. Triangulación con Arieso ©.....	116

INTRODUCCIÓN

La presente tesis es una investigación que tiene por objetivo explicar la importancia y el funcionamiento de la geolocalización que se lleva a cabo por parte de la red celular para actualizar su Registro de Posición Base o HLR por sus siglas en inglés para llevar a cabo la localización de los abonados y así permitirle a la compañía que brinda el servicio de comunicación, enrutar llamadas, aun cuando constantemente cambie de área de servicio la terminal móvil.

Entre los objetivos de la presente investigación se encuentra detallar como ha ido evolucionando estos sistemas de localización que forman parte de la arquitectura de las diferentes tecnologías que brindan el servicio de comunicación móvil, a partir de su implementación mundial con GSM y que se espera para ellos con las nuevas tecnologías que dejan atrás la conmutación de circuitos y pasan a conmutación de paquetes.

De igual forma se pretende investigar de qué manera se podría ubicar la posición de una terminal móvil de manera más precisa, mediante la información que brinda la base de datos HLR, es decir la información proporcionada exclusivamente por la red de telefonía móvil, con el fin de en dado momento localizar la terminal móvil o a la persona que lo porta, dadas las circunstancias de seguridad que hay en el país.

Para cumplir los objetivos se llevara a cabo por primer parte una reseña histórica de la telefonía móvil, sus inicios y su cambio de analógica a digital, el surgimiento de los elementos a investigar, con los respectivos marcos teóricos, tanto para la telefonía móvil y los métodos de geolocalización que se pretende investigar en el documento.

1 TELEFONÍA FIJA.

El teléfono es un dispositivo de telecomunicación diseñado para transmitir señales acústicas por medio de señales eléctricas a distancia.

Durante mucho tiempo Alexander Graham Bell fue considerado el inventor del teléfono junto con Elisha Gray, sin embargo Bell no fue el inventor de este aparato, sino solamente el primero en patentarlo.

Actualmente la red telefónica pública conmutada PSTN (Public Switching Telephone Network) por sus siglas en inglés, es la de mayor cobertura geográfica volviéndola una red global de conmutación de circuitos tradicional, diseñada principalmente para la transmisión de voz en tiempo real; lo cual en un principio estaba basada únicamente en sistemas analógicos. Actualmente, está compuesta, en su mayoría por una serie de sistemas digitales de conmutación interconectados. En la conmutación de circuitos se establece un canal de comunicaciones dedicado entre dos estaciones, esto es, se realiza la conexión mientras que los recursos de transmisión y conmutación son reservados exclusivamente durante el enlace. Cuando se establece el enlace entre los dispositivos involucrados parece como si estuvieran directamente conectados.

La infraestructura básica de la PSTN es la siguiente, empieza con un bucle local (local loop), también conocido como línea de abonado o línea telefónica, es un circuito de acceso dedicado, que consta de un par de cables de cobre los cuales conectan el teléfono de un usuario con la central telefónica más cercana (Central Office Switch), en donde se encuentran los conmutadores telefónicos. Las centrales telefónicas están conectadas por medio de troncales, los cuales son circuitos conmutados. Aunque hoy la conmutación y la transmisión de datos es digital, la última milla o línea de abonado sigue siendo analógica.

En la figura 1.1 se muestra una red fija local.

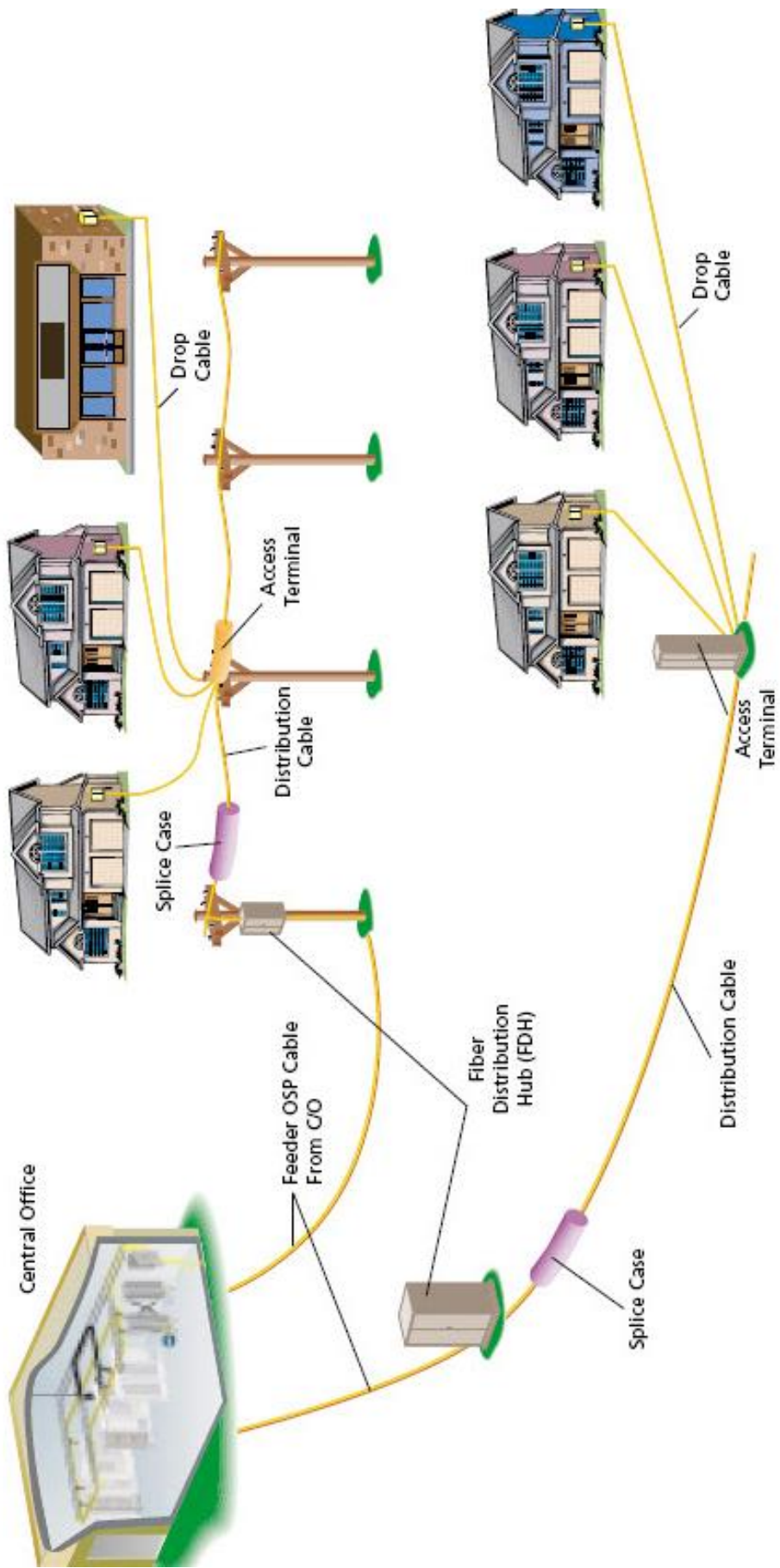


Figura 1.1. Red fija local

1.1 Telefonía sobre conmutación de circuitos

La central telefónica tiene la función principal de identificar, en cualquier número marcado la central, el usuario destino. También debe enrutar la llamada hacia tal central para indicarle al abonado destino, por medio de un tono o timbre de marcado, que alguien quiere comunicarse con él. Cuando la central identifica la ubicación del abonado destino, reserva una trayectoria entre ambos abonados para que, a través de ella se inicie una conversación.

En la conmutación de circuitos es necesario establecer una trayectoria física antes de transferir la información requerida por la comunicación entre un abonado origen y uno destino. Esta trayectoria forma un circuito físico entre el origen y el destino. Una vez que la conexión se establece, y durante toda la comunicación, el uso de este circuito permanece continuo y es exclusivo: la trayectoria se mantiene ocupada para uso único de este enlace, como se muestra en la figura 1.2. En el momento en que termina la comunicación, este circuito es desconectado y los enlaces físicos entre los nodos son liberados; quedan listos para ser utilizados en el establecimiento de otras conexiones.

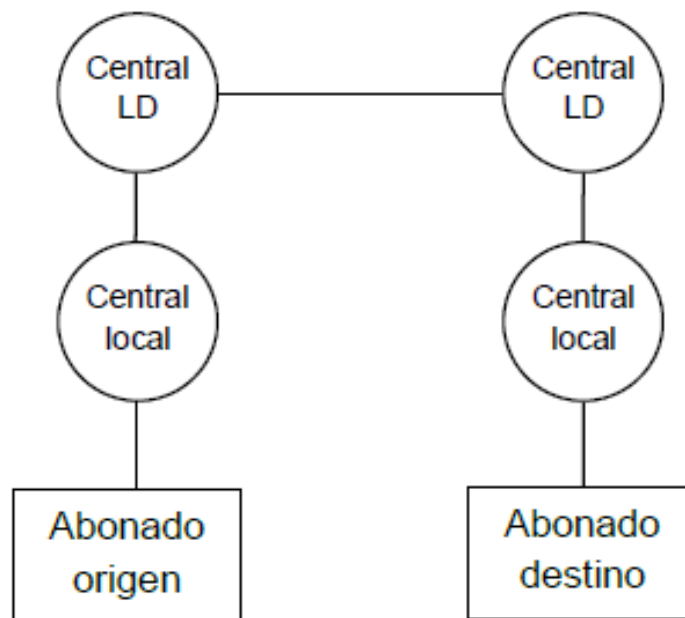


Figura 1.2. Enlace de telefonía fija Dedicado

Esta técnica de conmutación es usada, principalmente, en las redes telefónicas públicas. Sus características primordiales son:

- Comunicación en tiempo real.
- Retardos pequeños y constantes.
- Recursos que son usados de modo ineficiente.
- Establecimiento de la comunicación en un tiempo elevado (del orden de los segundos).

1.2 Telefonía sobre conmutación de paquetes

Esta técnica de conmutación fue creada para utilizar más eficientemente los medios de transmisión; en ella, la información que transmiten diferentes abonados puede compartir una misma trayectoria física.

El proceso es el siguiente: los mensajes se dividen en pequeños pedazos de información llamados “paquetes”. A cada paquete, que es independiente de todos los demás, se le agrega información de control en un encabezado. Éste contiene las direcciones del origen y del destino, el número de secuencia del paquete y una secuencia de *bits* de verificación de errores.

Cada paquete viaja de nodo en nodo, posiblemente en rutas diferentes, se reensambla en el nodo al que está conectado el usuario destino y se entrega.

Un paquete de datos es una secuencia continua de bits de un tamaño determinado que se transmite en una red (puede ser la telefónica), como una unidad de información individual. Los paquetes son construidos en el nodo origen y deben ensamblarse en el nodo destino para obtener la información completa y de manera correcta. En esta técnica, cada paquete debe contener bits adicionales en un encabezado. En la figura 1.3 se muestra el formato de una trama.

Señal de inicio	Direcciones origen y destino	Señal de control	Información	Detección de errores	Fin
-----------------	------------------------------	------------------	-------------	----------------------	-----

Figura 1.3. Formato de una trama

Un sistema de conmutación de paquetes acepta paquetes de un nodo fuente, los almacena internamente en un *buffer* de memoria del conmutador y luego los retransmite a otro conmutador del sistema en el que se repite la secuencia de

almacenaje y retransmisión. El proceso se repite hasta que llegan todos los paquetes al nodo destino.

Principales características de la técnica de conmutación de paquetes:

- Técnica apropiada para el manejo de tráfico interactivo.
- Diversidad de paquetes y destinos que utilizan un mismo medio de transmisión.
- Probabilidad de pérdida de los paquetes transmitidos, en caso de saturación o congestión de los sistemas telefónicos
- Tarificación de los servicios por tráfico, es decir, de acuerdo con el número de paquetes transmitidos.

Es necesario que exista un mensaje de acuse de recibo entre conmutadores contiguos. Éste debe indicar que todos los paquetes llegaron bien. Si el nodo emisor o nodo origen de un paquete no recibe este acuse en un cierto lapso, o si el mismo acuse indica que se detectaron errores, los paquetes deberán ser retransmitidos.

La conmutación de paquetes puede realizarse de dos formas: circuitos virtuales o datagramas.

1.2.1 Circuitos virtuales

Los circuitos virtuales se utilizan en redes cuyo principal servicio está orientado a conexión; la idea básica de este tipo de circuitos es evitar que tengan que hacerse decisiones de enrutamiento para cada uno de los paquetes transmitidos. Esto se logra seleccionando una ruta desde el nodo origen hasta el nodo destino como parte del proceso de conexión, en el momento de establecer una conexión. Esta ruta predeterminada es utilizada para todo el tráfico que circule por la conexión, tal como sucede en los sistemas telefónicos de conmutación de circuitos: cuando se libera la conexión, se libera el circuito virtual.

Cada circuito virtual se comparte por paquetes de diferentes usuarios de la misma red; los paquetes llegan al nodo destino en la misma secuencia en que los mandó el nodo origen.

Los conmutadores deben mantener una tabla para cada circuito virtual establecido; dicho esquema contiene el nodo del que proviene, el número de circuito virtual y el nodo destino al que se desea enviar el paquete. Cada paquete

contiene un encabezado con el número de circuito virtual, el número de secuencia del paquete, un código de redundancia, entre otros datos.

En el momento en que un paquete llega a un conmutador, éste reconoce la línea por la que llegó, así como su circuito virtual. Con estos datos envía el paquete al conmutador siguiente, con esto se identifica la conexión.

1.2.2 Datagramas

Con la conmutación por datagramas no es necesario determinar en forma anticipada alguna ruta, incluso si el servicio está orientado por conexión. Cada uno de los paquetes que se envían se encamina de manera independiente a la de sus predecesores. Los paquetes siguientes pueden seguir rutas distintas.

Este tipo de redes demandan mayor trabajo, pero son más robustas y se adaptan fácilmente a las fallas que pueden presentarse en la comunicación. También manejan de mejor manera la congestión que las redes de circuitos virtuales.

Los conmutadores emplean tablas que contienen la línea de salida que debe utilizarse para cada conmutador o nodo destino; estos esquemas son también utilizados en los circuitos virtuales. En la actualidad ya no se recurre a tablas con líneas para cada uno de los circuitos virtuales establecidos.

1.3 Jerarquización de la red telefónica

La red telefónica está organizada de manera jerárquica. El nivel más bajo está formado por el conjunto de nodos a los cuales están conectados los usuarios. Le siguen los nodos centrales en niveles superiores, enlazados de manera tal que entre mayor sea la jerarquía, de igual manera será la capacidad que los enlaza.

Con esta arquitectura se proporciona a los usuarios diferentes rutas para colocar sus llamadas, que son seleccionadas por los mismos nodos, de acuerdo con criterios preestablecidos, tratando de que una llamada no sea enrutada más que por aquellos nodos y canales estrictamente indispensables para completarla. Se trata de minimizar el número de canales y nodos por los cuales pasa una llamada para mantenerlos desocupados en la manera de lo posible.

Así mismo existen centrales que permiten enrutar una llamada hacia otra localidad, ya sea dentro o fuera del país. Este tipo de centrales se les denomina centrales automáticas de larga distancia. El inicio de una llamada de larga distancia es identificado por la central por medio del primer dígito, y el segundo dígito le indica el tipo de enlace, nacional o internacional; en este último caso, le indica también el país de que se trata.

En la figura 1.4 se muestra una imagen de las jerarquías en una red telefónica fija

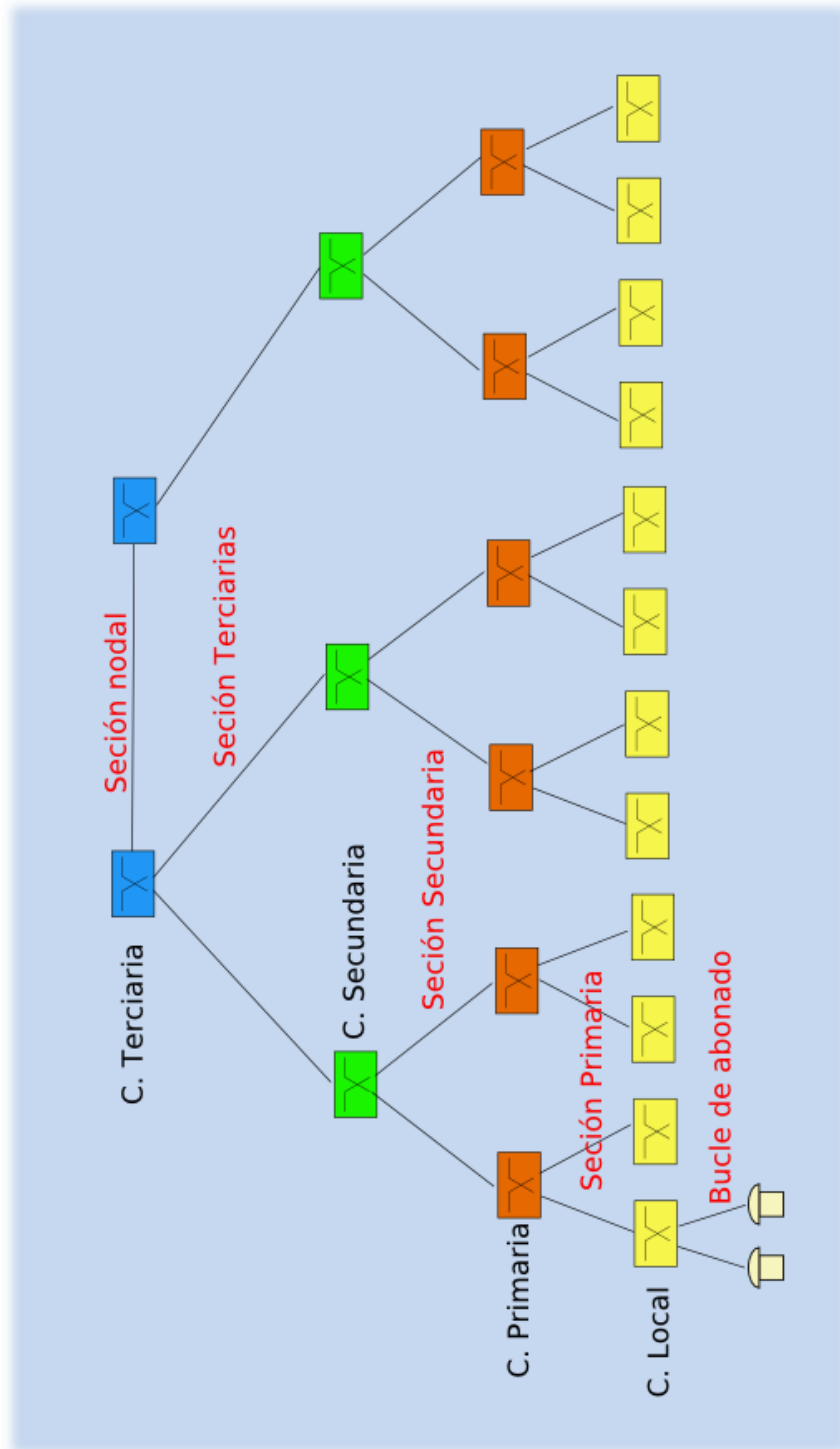


Figura 1.4. Jerarquía de la red telefónica fija

1.4 Comunicación entre dos abonados

Los enlaces entre las centrales locales y los abonados, son normalmente de cables de cobre, pero las centrales pueden comunicarse entre sí por medio de enlaces de cable coaxial, de fibras ópticas, enlaces de microondas o satelitales, dependiendo de las distancias que se desee cubrir.

La comunicación entre dos usuarios en la PSNT se da de la siguiente manera:

1. Cuando un abonado levanta el auricular de su aparato telefónico, la central lo identifica y le envía una "invitación a marcar".
2. La central espera a recibir el número seleccionado, para, a su vez, escoger una ruta del usuario fuente al destino.
3. Si la línea del abonado destino está ocupada, la central lo detecta y le envía al usuario fuente, una señal "tono de ocupado"
4. Si la línea del usuario no está ocupada, la central a la cual está conectado genera una señal para indicarle al destino la presencia de una llamada.
5. Al contestar la llamada el usuario destino, se suspende la generación de dichas señales.
6. al concluir la conversación, las centrales deben desconectar las llamadas y poner los canales a disposición de otro usuario, a partir de ese momento.

En la figura 1.5 se aprecian los tonos de información de acuerdo con la UIT-T.

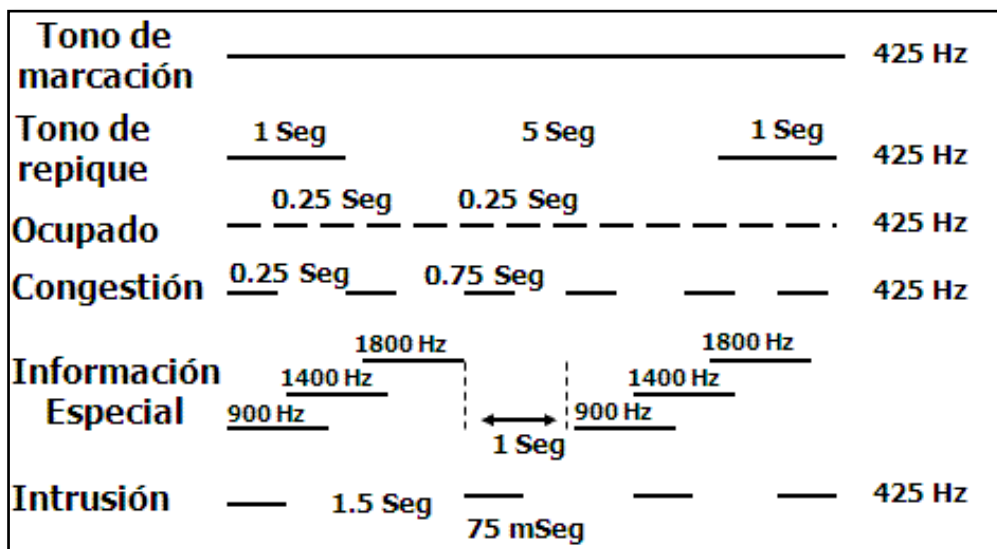


Figura 1.5. Tonos de información de acuerdo con la UIT-T

2 TELEFONÍA MÓVIL.

La radio surgió como una alternativa a la comunicación por cable a finales del siglo XIX. En un primer momento fue utilizada para comunicación marítima, pero a partir de la década de 1920 comenzaron los intentos de aplicarla también a la comunicación móvil en tierra.

El teléfono celular o teléfono móvil es un aparato indispensable en la actualidad; sin embargo su popularización ha sido un fenómeno muy reciente. En un principio el teléfono móvil solo podía ser usado en vehículos por su tamaño, reduciéndose posteriormente a una unidad portátil, y final mente al tamaño de bolsillo que utilizamos hoy. Pero el teléfono en sí, es una pequeña parte de un sistema de telefonía mayor.

En abril de 1973 Martin Cooper directivo de Motorola realizo la primera llamada desde un teléfono móvil desde una calle de Nueva York, precisamente a su mayor rival en el sector de telefonía Joel Engel, de los laboratorios Bell de AT&T.

2.1 Elementos del teléfono móvil

Desde entonces estos dispositivos han evolucionado sin parar y de paso revolucionado la sociedad y la forma de comunicarnos como ningún otro invento. De hecho la conocida revista Time ha reconocido al iPhone y en general a los móviles como el gadget más influyente de todos los tiempos. No en vano un smartphone medio de hoy en día cuenta con más tecnología y potencia que todos los ordenadores de a bordo del Apollo XI, la nave que llevó al hombre a la luna.

De los modelos que ocupaban todo un maletín se pasó a los que podían mandar SMS. Después llegaron las baterías de varios días de autonomía, las conexiones bluetooth. Tras eso aparecieron modelos multipropósito con cámara, con reproductor MP3, con videojuegos y con algo tan imprescindible como el correo electrónico. Todo esto se fue unificando para dar forma al smartphone, que culminó con la sustitución de la botonera por la pantalla táctil y la llegada de internet al móvil.

Desde entonces las novedades ya no sorprenden tanto, pero siguen llegando en forma de aplicaciones para cualquier necesidad.

Algunos de los elementos de los teléfonos Celulares actuales son los siguientes:

- 1.- Cámara trasera y flash. En sí mismo es un dispositivo independiente. El flash, en los mejores modelos, cuenta con dos LED, uno cálido y otro frío.
- 2.- Antena. Elemento que recibe las señales eléctricas de la red celular y las manda al módem para transformarlas en voz y datos.
- 3.- Conexiones. Zona donde se conectan los buses de datos de elementos del dispositivo para ser controlados por la placa base y el procesador.
- 4.- Cámara frontal. La cámara selfi por definición. Suele ser de menor resolución que la principal y con un objetivo de mayor cobertura.
- 5.- Procesador+ RAM. Conocido como el cerebro del sistema, es un microchip similar al de los ordenadores. La memoria RAM almacena los datos.
- 6.- Módem. Establece la comunicación con la red celular, es la parte que hace el trabajo como teléfono en el smartphone. También es responsable de la conexión de datos.
- 7.- Botones. Pese a que la mayoría de smartphones son táctiles, algunos resisten aún. Sus funciones suelen ser de encendido, apagado...
- 8.- Giroscopio y acelerómetro. Estos sensores detectan el movimiento en los tres ejes, así como la magnitud de ese movimiento.
- 9.- SIM. La bandeja para la SIM es uno de los elementos que igual desaparecen con la implantación de la SIM virtual.
- 10.- Altavoz. Miniaturizar un altavoz manteniendo su calidad es siempre difícil, por eso los móviles no suelen sonar demasiado bien.
- 11.- Conexión y 'jack'. Sirve para recargar la batería y funciona como conexión de datos. El jack sirve de salida para conectar unos auriculares.
- 12.- Micrófono. Existen móviles que usan hasta tres micrófonos para obtener mayor fidelidad del sonido en conversaciones o vídeos.
- 13.- Motor háptico. Permite conocer el nivel de presión que se aplica sobre la pantalla y actuar de manera diferente en consecuencia.
- 14.- Batería. El almacén de energía eléctrica que alimenta los circuitos y la pantalla del smartphone. Suelen ser de iones de litio.

15.- Escáner dactilar. Es un elemento de seguridad que permite reconocer la huella y solo da acceso si coincide con alguna de las autorizadas.

16.- Pantalla. Es el elemento más visible del equipo, y su tamaño, entre las 4 y 5,4 pulgadas, y calidad definen la sensación global del conjunto.

En la figura 2.1 se muestran los elementos de un smartphone actual

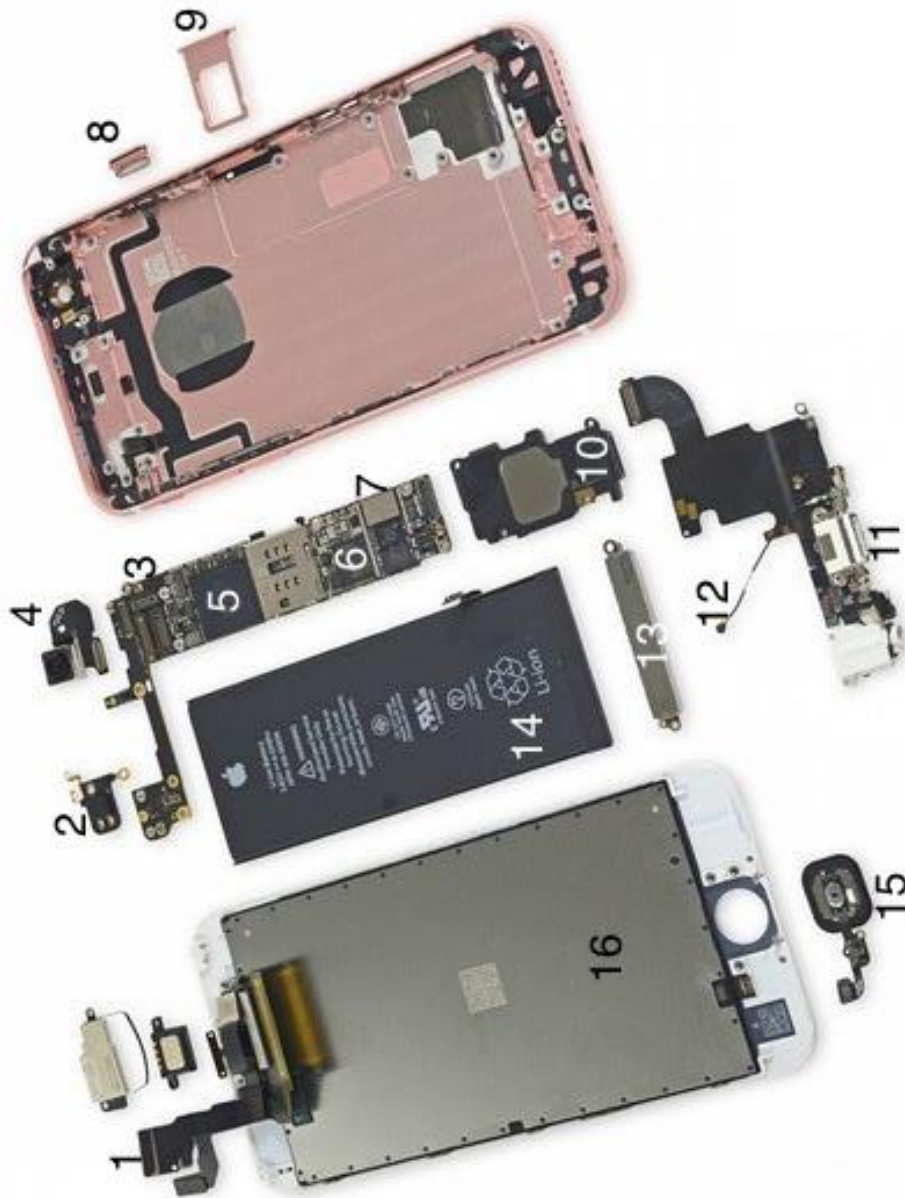


Figura 2.1. Partes que conforman un Smartphone

La telefonía móvil básicamente está formada por dos grandes partes: una red de comunicaciones (o red de telefonía móvil) que está compuesta de antenas

repartidas por la superficie terrestre y de los terminales (teléfonos móviles) que permiten el acceso a dicha red. Tanto las antenas como los terminales son emisores-receptores de ondas electromagnéticas con frecuencias entre 900 y 2000 MHz.

La operadora reparte el área en varios espacios, llamados células, normalmente hexagonales, como en un juego de tablero, creando una inmensa red de hexágonos. De ahí viene el nombre de celular. La forma hexagonal es la forma geométrica que permite ocupar todo el espacio, cosa que no ocurriría si fueran circunferencias. Cada célula es típicamente de un tamaño de 10 millas cuadradas (unos 26Km²).

Sin embargo, el tamaño de las células puede variar mucho dependiendo del lugar en que se encuentre. Las estaciones de base se separan entre 1 a 3 Km. en zonas urbanas, aunque pueden llegar a separarse por más de 35Km en zonas rurales.

En zonas muy densamente pobladas o áreas con muchos obstáculos (como ser edificios altos), las células pueden concentrarse en distancias cada vez menores. Algunas tecnologías, como los PCS (Personal Communication Services), requieren células muy cercanas unas de otras debido a su alta frecuencia y bajo poder en el que operan.

Los edificios pueden, a su vez, interferir con el envío de las señales entre las células que se encuentren más lejanas, por lo que algunos edificios tienen su propia "microcélula." Los subterráneos son típicos escenarios donde una microcélula se hace necesaria. Microcélulas pueden ser usadas para incrementar la capacidad general de la red en zonas densamente pobladas como ser los centros capitalinos.

Debido a que los teléfonos celulares y las estaciones de base utilizan transmisores de bajo poder, las mismas frecuencias pueden ser reutilizadas en células no adyacentes. En la siguiente figura número 2.2, está representada un conjunto de estaciones base en una red celular.

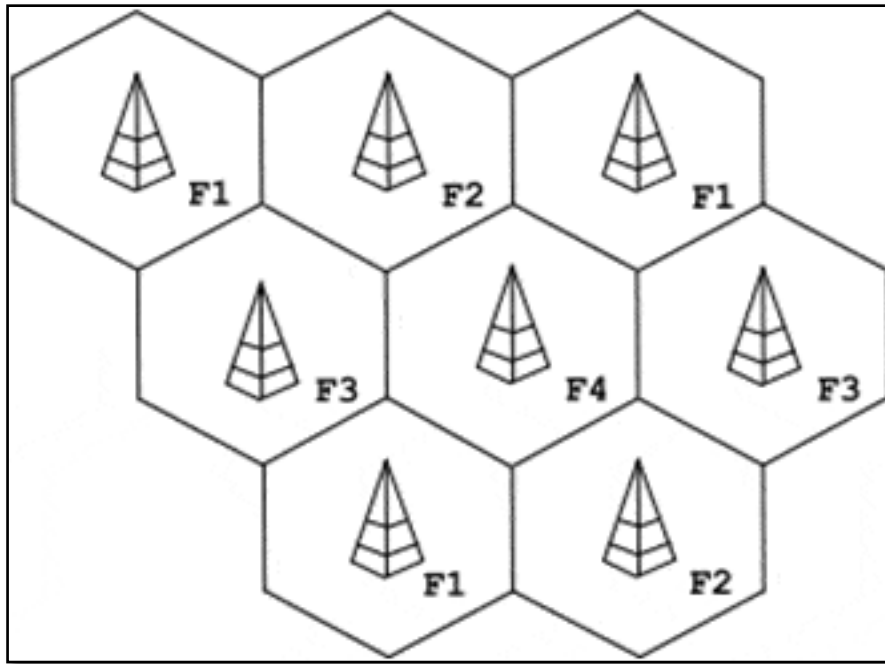


Figura 2.2. Ejemplo de una red celular

En cada célula hay una estación base que será una antena que tiene una amplitud para emitir y recibir en ese hexágono de espacio (célula).

En la figura 2.3 se muestran las celdas, ficticias, ideales y reales de la telefonía celular

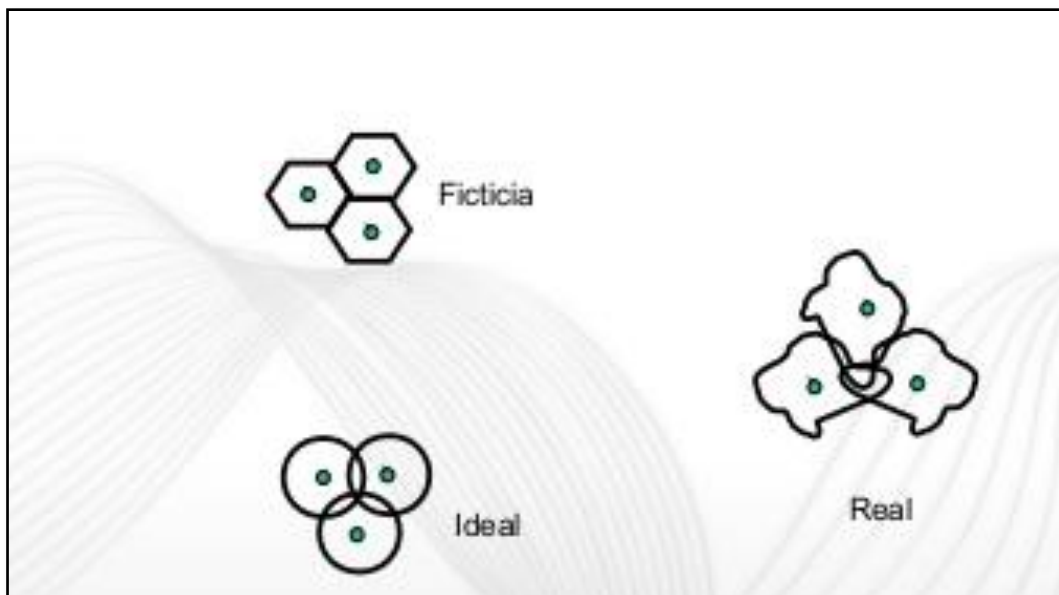


Figura 2.3. Células de telefonía móvil

Cada célula utiliza varias decenas de canales. Un canal es por donde se puede emitir una llamada, es decir que por cada célula se pueden emitir varias decenas de llamadas diferentes simultáneas (una por canal).

Lo que diferencia un canal de otro es su frecuencia. Realmente un canal son las ondas electromagnéticas emitidas y/o recibidas en una comunicación a una frecuencia determinada. Cuando yo me comunico con otra persona con mi teléfono, los dos lo hacemos por la misma frecuencia, la frecuencia del canal por el que nos estamos comunicando (emitimos ondas de la misma frecuencia).

Cada canal emite las señales (ondas electromagnéticas) a una frecuencia diferente, lo que da la posibilidad de que varias decenas de personas puedan comunicarse simultáneamente en cada célula sin interferirse unas con otras.

Una llamada se emite por un canal de la célula a una frecuencia concreta, por eso es única.

Cuando una persona se mueve de una célula para otra, pasa a utilizar y engancharse a una de las frecuencias de la nueva célula (se engancha a un canal de la nueva célula), dejando libre el canal de la célula anterior para ser usada por otra persona.

Durante una llamada ocurre lo siguiente:

Las operadoras de telefonía móvil tienen centrales de conmutación.

La Central de Conmutación es la que permite la conexión entre dos terminales concretos. Hace la conexión entre los 2 teléfonos, conecta a los dos usuarios, el que hace la llamada y el que la recibe. Probablemente al lector le venga a la cabeza la simpática imagen de la operadora conectando dos teléfonos en una llamada mediante clavijas y de forma manual. Hoy en día la conmutación es digital, electrónica y totalmente automatizada.

Cuando un teléfono hace una llamada, se conecta con la central de conmutación de la estación base más cercana y que pertenezca a la red del su operador (movistar, Telcel, AT&T, etc.).

La central de conmutación deriva (busca) al destinatario deseado (identificado por su número de teléfono móvil receptor), en la red de estaciones bases, hasta encontrar dentro de la que está en ese momento y conecta las dos estaciones bases emitiendo una alerta, aviso de llamada, al teléfono receptor.

Si el receptor acepta la llamada los pone en contacto por un canal. La información,

en este caso la voz, se transmite por ondas electromagnéticas de una antena a otra. Los comunicantes están conectados por medio de la red de antenas (estaciones bases) que vimos antes. Las centrales de conmutación suplantaron a las viejas operadoras que unían dos teléfonos mediante clavijas.

Cuando la central de conmutación encuentra la célula a la que pertenece el teléfono receptor, la central de conmutación de la estación base a la que pertenece el móvil receptor, da la frecuencia a la que deben operar los dos móviles para comenzar la transmisión.

Cada estación base informa a su central de conmutación en todo momento de los teléfonos que estén registrados en ella (a su alcance). Es decir cuando un móvil entra en una zona que pertenece a una célula la estación base lo detecta y lo asigna a esta célula registrándolo en la central de conmutación de esa estación base.

Si se mueve a otra zona el móvil pasará a pertenecer a otra célula diferente. Si no encuentra ninguna célula el móvil estará fuera de cobertura.

Muchas veces la comunicación entre una estación base y otra se realiza mediante cable (telefonía convencional=Red de telefonía conmutada).

2.2 Radio bases

En el contexto de la telefonía móvil, una estación base (en inglés: Base Transceiver Station (BTS)) dispone de equipos transmisores/receptores de radio, en la banda de frecuencias de uso (850 / 900 / 1800 / 1900 MHz) en GSM y (1900/2100Mhz) en UMTS que son quienes realizan el enlace con el usuario que efectúa o recibe la llamada(o el mensaje) con un teléfono móvil. Estas frecuencias son reguladas por la UIT (Unión Internacional de Telecomunicaciones). Las antenas utilizadas suelen situarse en lo más alto de la torre (si existe), de edificios o colinas para dar una mejor cobertura y son tipo dipolo. Normalmente, está compuesta por un mástil al cual están unidas tres grupos de una o varias antenas equidistantes. El uso de varias antenas produce una diversidad de caminos radioeléctricos que permite mejorar la recepción de la información.

Además, la Estación Base dispone de algún medio de transmisión, vía radio o cable, para efectuar el enlace con la Central de Conmutación de Telefonía Móvil Automática, que a su vez encamina la llamada hacia el teléfono destino, sea fijo o móvil.

El sistema de telefonía celular está compuesto por los equipos del fabricante (sistema de RF), y un sistema radiante. El sistema radiante está compuesto por la

guía de onda (feeders o fibra óptica)), jumpers (cables conectores flexibles entre guía de onda y equipos y entre guía de onda y antenas) y antenas. La guía de onda y jumpers van sujetos en las estructuras a través de clanes o hangers que lo fijan y sostienen. Las antenas van instaladas en mástiles adecuados al peso y largo de estas por medio de un sistema de herrajes especiales.

A gran escala los equipos de RF (Radio Frecuencia) son el actor principal de una radio base de telefonía celular, pero esta no funciona solo con ellos.

En el plano de la figura 2.4 se destacan aspectos tales como el sistema de energía, tanto fijo (acometida ac y transferencia), como de reserva (planta, tanques de acpm y baterías), además de la estructura física en donde van las antenas y guías de onda, el cuarto de equipos en donde encontramos sistemas de reservas de baterías (Backup de energía), equipos de telefonía celular de diferentes tecnologías (GSM y 3G) y sistemas de microondas (MW). En muchas estaciones, se pueden encontrar dos tecnologías implementadas.

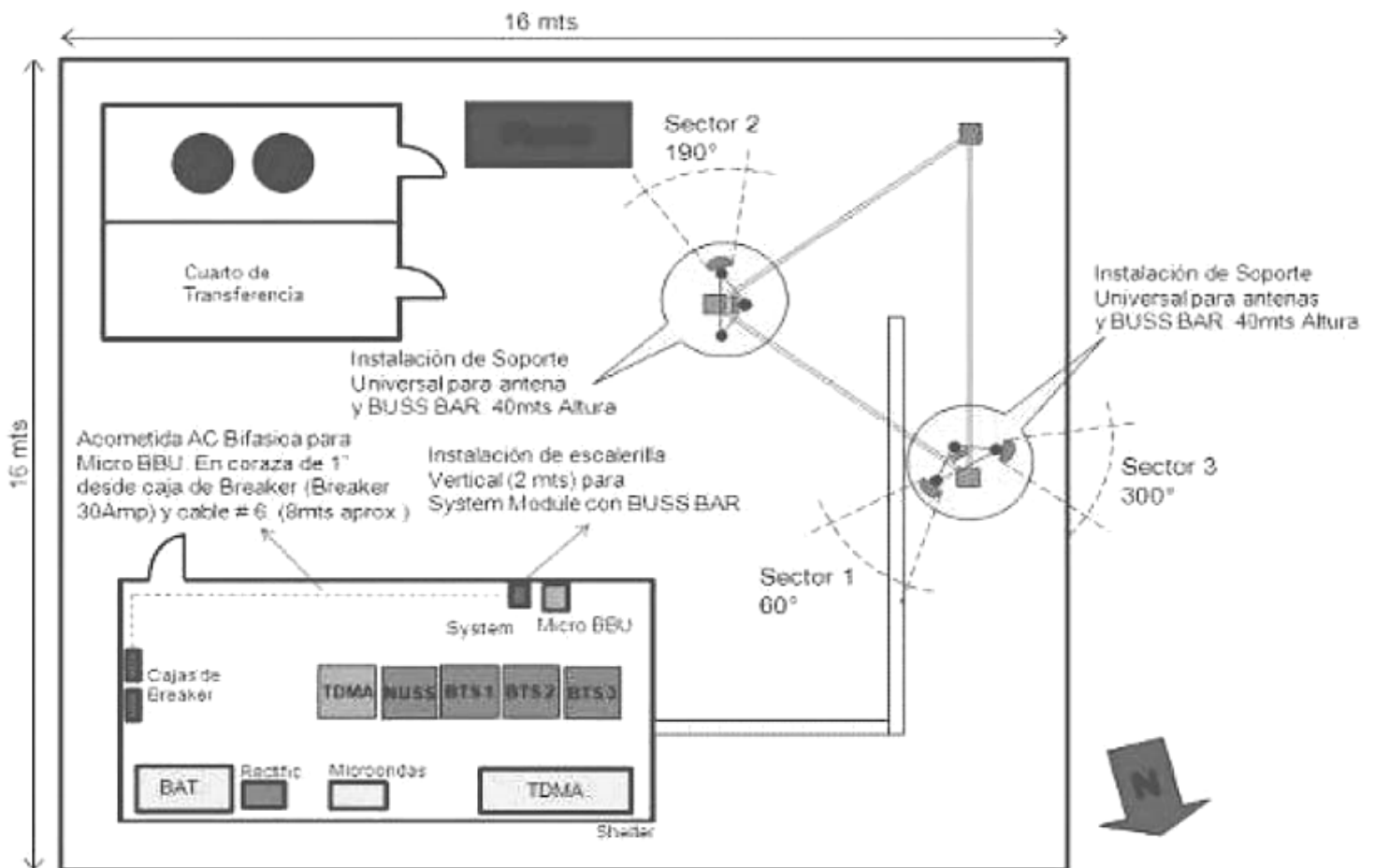


Figura 2.4. Plano Aproximado de una radiobase.

Las unidades de RF por lo general van en piso, en pocas excepciones estas se instalaron en estructuras como torres.

Los equipos que se encuentran pueden ser *outdoor* (externos a la intemperie) o *indoor* (en cuartos cerrados con o sin refrigeración). Estos equipos vienen en gabinetes que facilitan la instalación de cada uno de los módulos y las conexiones entre ellos.

Un aspecto general para todas las tecnologías es el tipo de estructura que se utiliza para el montaje del sistema radiante y equipos si se requiere. Los operadores de telefonía celular tienen definidos cuatro tipos de estructuras opcionales en donde según la necesidad instalan estos equipos.

La primera de estas estructuras en citar son las torres, las cuales son unas de las de mayor costo y son capaces de soportar gran cantidad de carga en equipos, por lo que son bastante útiles. Estas deben ofrecer condiciones de seguridad establecidas como escalerilla de ascenso, guaya para instalación de freno de caída y sus respectivos descansos dependiendo de la altura de la misma. Algunas ofrecen soportes para instalación de antenas y equipos.

En las torres pueden ir ubicados sistemas radiantes de distintas tecnologías e inclusive de distintos operadores, según los convenios que se realicen entre estos.

En la figura 2.5 tenemos la estructura tipo torre.

Los monopolos son otro tipo de estructura utilizada se instalan por lo general en las ciudades. Son de poco tamaño (estructuras de hasta 30 metros o menos) y no soportan tanto peso como las torres, como se observa en la figura 2.6.

Otro tipo de estructura también usada son las encontradas en las estaciones denominadas móviles, las cuales se usan en determinadas ocasiones para eventos, para testear tráfico o en sitios suburbanos. Estas estructuras soportan mucho menos peso que las dos estructuras anteriores. Estas estaciones constan de un tráiler donde se anclan los equipos y posee una torre desplegable que se eleva por medio de un mecanismo electromecánico, que es sujetado por pasos entre la estructura y tensionada con guayas al piso. Se muestra en la figura 2.7.

Otro tipo común de estructuras usada para la instalación del sistema radiante y equipos son las azoteas, proveen un espacio que se adecúa para la implementación del sistema de telefonía celular. En este caso, el sistema va ubicados en las azoteas de edificios, esta se muestra en la figura 2.8.

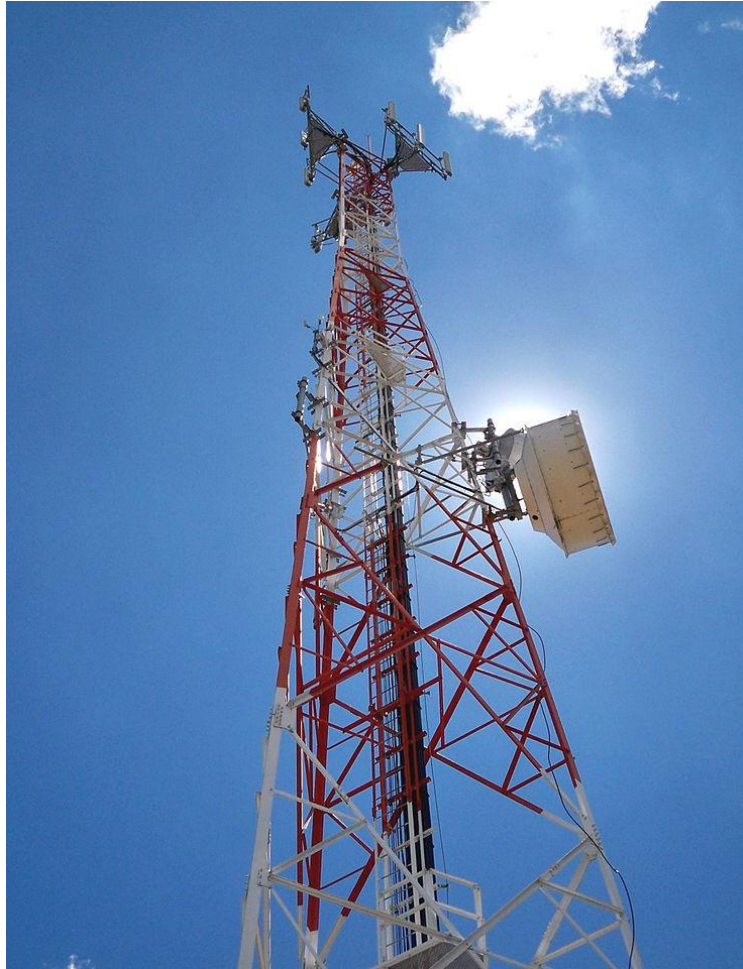


Figura 2.5. Estructura tipo torre

Existe otro tipo de montaje, poco usado que es el correspondiente a los postes; aunque es de poco uso. Los equipos y sistema radiante van sujetos al poste, con adecuaciones. Por lo general proveen un sector de cobertura en especial. Son de poco alcance. Se usan para centros comerciales que demandan mucho tráfico o en zonas donde la señal celular es deficiente.

Todos estos modelos que se ilustran cuentan con un sistema de rectificador de corriente con sistema de banco de baterías. Este sistema es un equipo que es alimentado con energía normal (trifásica, bifásica o monofásica) y el cual se encarga de proveer una energía DC de excelente rectificación.

Los sistemas de alimentación de energía utilizan energía AC comercial y entregan energía DC rectificada (Por lo general 48-54 VDC); cuentan con un sistema de respaldo de baterías interno y un sistema de rectificación de DC, y estos además proveen de alimentación a los equipos indoor de microondas.



Figura 2.6. Estructura tipo monopolo



Figura 2.7. Estación con estructura de tipo móvil



Figura 2.8. Equipos de una radio base en azotea.

Para el sistema de respaldo de energía AC se utilizan plantas eléctricas. En lugares de difícil acceso, en donde es complicada la instalación de energía regulada local de AC, estas plantas pasan a ser el principal proveedor de energía de la radiobase.

Estas plantas funcionan con la energía comercial a través de un sistema de transferencia, el cual se encarga de habilitar en caso de falla comercial el sistema de respaldo de la planta eléctrica AC.

Todas estas tecnologías de telefonía celular necesitan, para comunicarse con otras radiobases o celdas, sistemas de microondas o enlaces, los cuales se encargan de entrelazar celdas y son rutas para la salida o entrada de una llamada.

En una radiobase es común encontrar varios enlaces. La ubicación de estos depende de la estructura física de la radiobase. Algunos operadores optan por la instalación de los equipos de microondas (MW) en gabinetes outdoor, otros poseen cuartos de equipos debidamente acondicionados, con refrigeración, para instalar un rack en donde se montan los equipos indoor de microondas. Los equipos de MW constan en su mayoría de una unidad indoor (IDU) y una unidad

outdoor (ODU). Entre las dos se efectúa una adecuación de frecuencias de transmisión y recepción. La configuración del sistema se realiza a través de la IDU.



Figura 2.9. Antenas de microondas montada en torre

3 EVOLUCIÓN DE LA TECNOLOGÍA DE COMUNICACIÓN MOVIL.

3.1 Primera generación 1G

La primera generación de la telefonía móvil (G1) funcionaba por medio de comunicaciones analógicas y dispositivos portátiles que eran relativamente grandes. Esta generación utilizaba diferentes estándares dependiendo de la región y el país.

- **AMPS** (Advanced Mobile Phone System): se presentó en 1976 en Estados Unidos y fue el primer estándar de las redes celulares. Utilizada principalmente en el continente americano, Rusia y Asia, la primera generación de redes analógicas contaba con un mecanismo de seguridad endeble que permitía hackear las líneas telefónicas.
- **TACS** (Sistema de Comunicación de Acceso Total): Es la versión europea del modelo AMPS. Este sistema fue muy utilizado en Inglaterra, Asia y Japón, utilizaba la banda de frecuencia de 900 MHz.

3.2 Segunda generación G2

La segunda generación de redes móviles (G2) marco un quiebre con la primera generación de teléfonos celulares de pasar de tecnología analógica a digital. En el inicio de los 80 los primeros sistemas de comunicaciones celulares móviles aparecieron en el mundo. Cada nación desarrollaba su propio sistema y un teléfono móvil funcionaba en el país que era comprado, debido a que la tecnología de un país no era compatible con la de otro.

El sistema 2G utiliza protocolos de codificación más sofisticados y son los sistemas de telefonía celular usados en la actualidad. Las tecnologías predominantes son: GSM (Global System for Mobile Communications); IS-136 (conocido también como TIA/EIA-136 o ANSI-136) y CDMA (Code Division Multiple Access) y PDC (Personal Digital Communications), éste último utilizado en Japón.

Los protocolos empleados en los sistemas 2G soportan velocidades de información más altas para voz pero limitados en comunicaciones de datos. Se pueden ofrecer servicios auxiliares tales como datos, fax y SMS (Short Message Service). La mayoría de los protocolos de 2G ofrecen diferentes niveles de encriptación. En los Estados Unidos y otros países se le conoce a 2G como PCS (Personal Communications Services).

La velocidad de transmisión de la 2G se limita a 9.6 kbps, velocidad considerablemente menor que los 56 kbps que permite la telefonía de cable y de la de un megabit del cable modem. Las dos soluciones a estos problemas de ancho de banda las proporcionan las redes móviles 2.5G y 3G.

En 1982, un consorcio de países europeos creó el GSM (Grup Speciale Mobile) para desarrollar una tecnología que proveyera un servicio común de telefonía móvil europea.

El sistema que desarrollaron tuvo una gran acogida y se expandió por varios países del mundo volviéndose una tecnología global. Así las siglas GSM comenzaron a significar "Sistema Global para Comunicaciones Móviles"

3.2.1 Sistema global para comunicaciones móviles (GSM)

Es un sistema de conmutación de circuitos, diseñado originalmente para voz, a la que posteriormente se le adicionaron algunos servicios de datos: servicio de mensajes cortos, un servicio de entrega de mensajes de texto de hasta 160 caracteres y un servicio de datos GSM que permite una tasa de transferencia de 9.6 kbps.

3.2.2 Arquitectura de la red GSM

Una red GSM se encuentra formada por los siguientes componentes:

- La estación móvil (MS: Mobile Station). Es el punto de entrada a la red móvil inalámbrica. Es el equipo físico usado por el usuario GSM.
- El módulo de identidad del abonado (SIM: Subscriber Identity Module). GSM distingue entre la identidad del abonado y la del equipo móvil. El SIM está asociado con el abonado, se trata de un chip que el usuario debe introducir en el terminal GSM.
- La estación transmisora- receptora de base o estación transceptora de base (BTS: Base Transceiver Station). Se encarga de proporcionar, vía radio, la conectividad entre la red y las estaciones móviles.
- El controlador de estación base (BSS: Base Station Subsystem).
- La unidad de transcodificación (TRAU: Transcoding Rate and Adaptation Unit). Se encarga de comprimir la información en el interfaz aéreo cuando se hace necesario. La TRAU forma parte del subsistema BSS. Permite que

tasas de datos GSM (8, 16, 32 kbps) puedan ser enviadas hacia la interfaz RDSI del MSC que solo acepta tasas de 64kbps.

- El centro de conmutación de servicios móviles o centro de conmutación de móviles (MSC: Mobile Services Switching Center). Se encarga de enrutar el tráfico de llamadas entrantes y salientes, y de la asignación de canales de usuario de interfaz entre el MSC y las BSC.
- El registro general de abonados (HLR: Home Location Register). Es una base de datos que contiene y administra la información de los abonados, mantiene y actualiza la posición del móvil y la información de su perfil de servicio.
- El registro de abonados itinerantes (VLR: Visitor Location Register). Diseñado para no sobrecargar el HLR. Guarda localmente la misma información que el HLR, cuando el abonado se encuentra en modo de itinerancia (roaming).
- El centro de autenticación (AuC: Authentication Center). Genera y almacena la información relativa a la seguridad, genera las claves usadas para autenticación y encriptación.
- Registro de identidad de equipos (EIR: Equipment Identity Register). Las terminales móviles tienen un identificador único, el IMEI (International Mobile Equipment Identity), el EIR se utiliza para mantener una relación de las identidades de los equipos abonados; a través del resulta posible identificar aquellos usuarios autorizados.
- El GMSC: Gateway Mobile Services Switching Center. Es el punto hacia el cual es encaminada la terminación de llamada cuando no se tiene conocimiento de la ubicación de la estación móvil. Este componente tiene la responsabilidad por el encaminamiento de la llamada al MSC correcto.
- SMS-G. Este término es usado para describir colectivamente a los dos Gateways que soportan el servicio de mensajería corta (Short Message Services Gateways). El SMS-GMSC (Short Message Services Gateway Mobile Switching Service) encargado de la terminación de los mensajes cortos y el IWMSC (Short Message Services Inter-Working Mobile Switching Center). Encargado de originar los mensajes cortos.

3.3 Generación 2.5

La generación 2.5G brinda características extendidas para ofrecer capacidades adicionales a la de los sistemas 2G, tales como GPRS (General Packet Radio System), HSCSD (High Speed Circuit Switched Data), EDGE (Enhanced Data Rates for Global Evolution), IS-136B, IS-95B, entre otros. La tecnología 2.5G es más rápida y más económica para actualizar a 3G, aunque en algunos países como Japón paso de la segunda generación a la tercera directamente.

3.3.1 Servicio general de paquetes vía radio (GPRS)

General Packet Radio Service (servicio general de paquetes vía radio) y es una extensión mejorada del GSM

Permite la mensajería instantánea, los servicios de mensajes cortos (SMS) y multimedia (MMS) y de correo electrónico.

Otro de los cambios que se introdujeron en la telefonía móvil gracias a la aparición del sistema GPRS fue el uso del protocolo IP. Hasta entonces este solo se encontraba en la red tradicional de los ordenadores, pero con la extensión del GSM cada dispositivo móvil gozaba ya de una identificación propia de IP, lo que permitía que estuviera integrado dentro de Internet.

Proporciona una cobertura inalámbrica completa y velocidades de transferencia de entre 56 a 114 kbps (kilobits por segundo). Por ejemplo, nos permite enviar 30 SMS por minuto, mientras que con GSM podemos mandar entre 6 y 10. Pero no es la más veloz.

3.3.2 Tasas de datos mejoradas para la evolución de GSM (EDGE)

Servicio EDGE o EGPRS, acrónimo en inglés de Enhanced Data Rates for GSM of Evolution (tasas de datos mejoradas para la evolución de GSM) o Enhanced GPRS, es decir, un GPRS mejorado.

Cuando en la pantalla de tu celular aparece la letra E, significa que tu terminal está conectada al servicio EDGE.

Permite alcanzar velocidades de hasta 384 kbps y recibir datos móviles pesados, como grandes archivos adjuntos de correo electrónico o navegar por páginas web complejas a gran velocidad.

La tecnología EDGE actúa como puente entre las redes 2G y 3G y puede funcionar en cualquier red con GPRS y que haya sido actualizada a través de la activación de un software opcional.

3.4 3GPP

El 3GPP (3rd Generation Partnership Project: Proyecto Asociación de Tercera Generación) es una colaboración de grupos de asociaciones de telecomunicaciones, conocidos como miembros organizativos.

El objetivo inicial del 3GPP era asentar las especificaciones de un sistema global de comunicaciones de tercera generación 3G para teléfonos móviles basándose en las especificaciones del sistema evolucionado GSM (Global System for Mobile Communications: sistema global de telecomunicaciones móviles) dentro del marco del proyecto internacional de telecomunicaciones móviles 2000 de la ITU (Unión Internacional de Telecomunicaciones). Más tarde el objetivo se amplió incluyendo el desarrollo y mantenimiento de:

- El GSM incluyendo las tecnologías de radioacceso evolucionadas del GSM (como por ejemplo, GPRS o EDGE).
- Un sistema de tercera generación evolucionado y más allá del sistema móvil basado en las redes de núcleo evolucionadas del 3GPP y las tecnologías de radioacceso apoyadas por los miembros del proyecto.
- Un IMS (Subsistema Multimedia IP) desarrollado en un acceso de manera independiente.

La estandarización 3GPP abarca radio, redes de núcleo y arquitectura de servicio.

El proyecto 3GPP se estableció en diciembre de 1998.

3.5 Tercera generación 3G

La 3G es tipificada por la convergencia de la voz y datos con acceso inalámbrico a Internet, aplicaciones multimedia y altas transmisiones de datos. Los protocolos empleados en los sistemas 3G soportan más altas velocidades de información enfocados para aplicaciones más allá de la voz, tales como audio (MP3), video en movimiento, video conferencia y acceso rápido a Internet, sólo por nombrar algunos.

Los sistemas 3G alcanzan velocidades de hasta 384 Kbps, permitiendo una movilidad total a usuarios viajando a 120 kilómetros por hora en ambientes exteriores, mientras que alcanza una velocidad máxima de 2 Mbps permitiendo una movilidad limitada a usuarios caminando a menos de 10 kilómetros por hora en ambientes estacionarios de corto alcance o en interiores.

Entre las tecnologías contendientes de la tercera generación se encuentran UMTS (Universal Mobile Telephone Service), CDMA2000, IMT-2000, ARIB (3GPP), UWC-136, entre otras.

3.5.1 Sistema universal de telecomunicaciones móviles (UMTS)

El UMTS (Universal Mobile Telecommunications System o Sistema Universal de Telecomunicaciones Móviles) es una tecnología móvil de la llamada tercera generación (3G), sucesora de la tecnología GSM (Global System for Mobile) o 2G.

Esta tecnología permite disponer de una mayor resistencia a interferencias que su predecesora, así como la utilización simultánea de conexiones de voz y datos, con velocidades de descarga que pueden alcanzar los 2 Mbit/s para usuarios con baja movilidad o los 144 Kbit/s para aquellos moviéndose en vehículos a gran velocidad. Estas características han hecho que la tecnología 3G sea una de las más extendidas y utilizadas para el acceso a Internet de banda ancha móvil.

Pero pronto llegarían nuevos avances que permitirían, sobre todo, una velocidad de navegación todavía mayor.

3.6 Generación 3.5G Acceso ascendente de paquetes a alta velocidad (HSDPA)

Red HSDPA o High Speed Downlink Packet Access (Acceso ascendente de paquetes a alta velocidad). Cuando en nuestras pantallas aparece una H, significa que estamos conectados a una red H o HSDPA. Este tipo de conexión también se conoce como 3,5G, 3G+ o Turbo3G y puede llegar a alcanzar velocidades de 14 Mbps en condiciones óptimas.

Es, en definitiva, una optimización de la tecnología UMTS que utiliza la 3G y una evolución de ésta, sin llegar a alcanzar la de mayor velocidad hasta el momento, que sería la 4G.

3.7 Cuarta generación 4G LTE

La tecnología 4G, también llamada LTE, es la más veloz desarrollada hasta la fecha. Pero todavía no es una realidad global y no todos los terminales ni todas las tarjetas SIM son compatibles con ella.

En América Latina, Uruguay es de los países más avanzados, pues la tecnología 4G está disponible en un 84% del territorio, igualando a Singapur. En otras naciones de la región, como Bolivia (67%), Perú (61%) o México (60%) está disponible en la mayor parte del territorio.

Según la Unión Internacional de Comunicaciones (UIT), para que una tecnología pueda etiquetarse como "4G" las velocidades máximas de transmisión de datos deben situarse en 100 megabits en movimiento y 1 gigabit en reposo.

La conexión 4G LTE es la primera arquitectura en transportar todos los datos a través de la conmutación de paquetes, incluida la voz sobre IP.

Las conexiones 4G mantienen una calidad de servicio de alta seguridad que permite ofrecer servicios de cualquier clase en cualquier momento, en cualquier lugar, con el mínimo coste posible.

3.8 Quinta generación

La red 5G es el futuro, pero empresas como Samsung y otros gigantes tecnológicos ya están desarrollándola.

Se espera que alcance velocidades de hasta 1 gigabit por segundo. Y eso la haría nada menos que 100 veces más rápida que la 4G.

Si esto se hace realidad, podremos descargar películas en nuestra computadora en tan sólo un segundo.

Pero para saberlo tendremos que esperar hasta el año 2020.

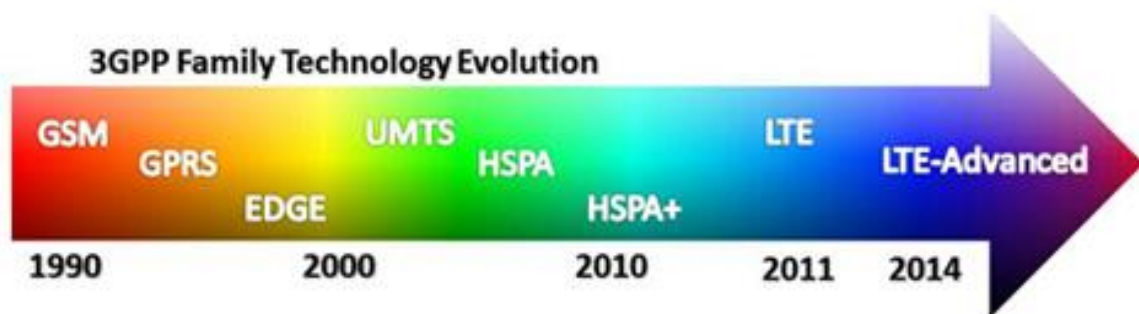


Figura 3.1. Evolución de la familia GSM

4 ARQUITECTURA DE UNA RED GSM

Hay muchas maneras de configurar una red de telecomunicaciones y a lo largo de la historia, se han utilizado muchas versiones de redes que están en funcionamiento y que están planificadas para su uso. Una de estas redes es la red GSM, para la cual se implementa el HLR.

La red GSM se divide en 3 subtemas funcionales como se muestra en la figura 4.1 y son:

- El subsistema de estaciones base (BSS: Base Station Subsystem) trata con la parte de radio de la red, lo que significa recibir y transmitir señal hacia y desde las entidades de usuario.
- El subsistema de conmutación (NSS: Network Switching Subsystem) Aquí es donde se realiza el trabajo principal en la red GSM y también donde se encuentra nuestro HLR. La red GSM se puede conectar a otros tipos de redes, esto se hace aquí.
- El subsistema de operación y mantenimiento (OSS: Operation Subsystem) este es básicamente una interfaz de los operadores a las diferentes unidades de la red GSM. Esto puede incluir actualizar la base de datos HLR, cambiar el enrutamiento en el MSC, es decir la normal operación y configuración de la red.

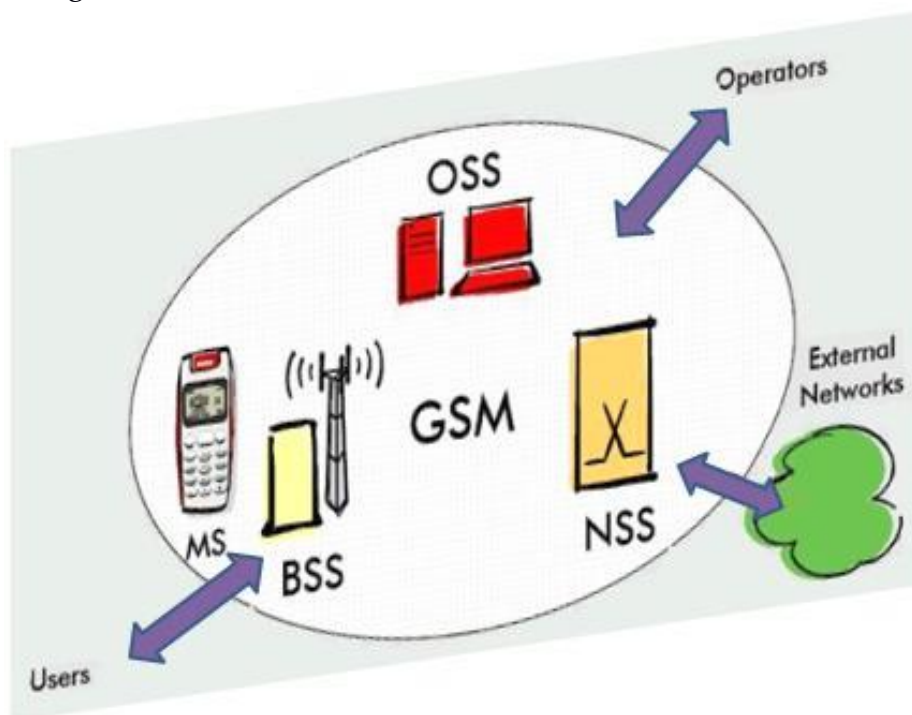


Figura 4.1. Arquitectura de una red GSM

4.1 El subsistema de estaciones base BSS

El subsistema de estaciones base es el que permite el acceso de los móviles a la red GSM, ya que los comunica con el subsistema de conmutación de red.

Este subsistema está compuesto por:

- La terminal móvil (MS: Mobile Station).
- Las estaciones radio base o estaciones base (BTS: Base Transceiver Station)
- La estación controladora (BSC: Base Station Controller)
- La unidad transcodificadora (TRAU: Transcoding and Rate Adaptation Unit).

Como se ilustra en la figura 4.2.

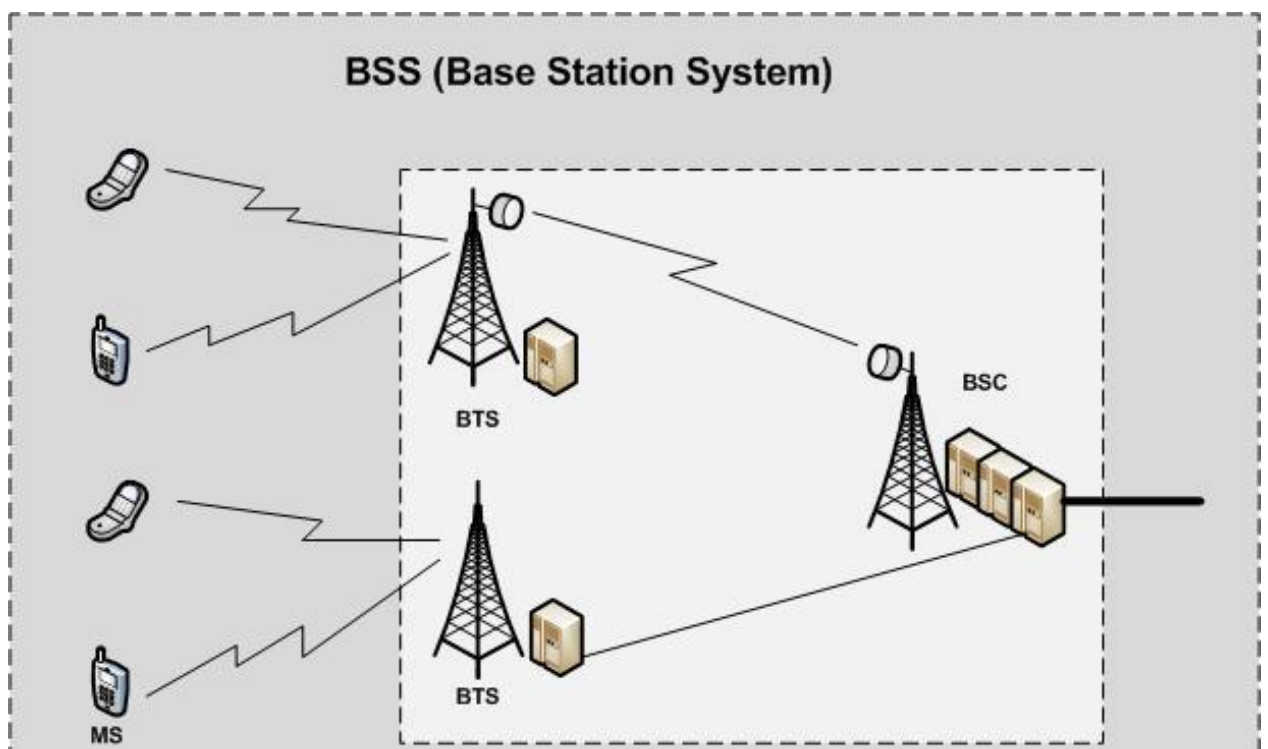


Figura 4.2. Sub-sistema BSS

Existen varias interfaces que conectan las diferentes unidades:

- Interface Um: es la interfaz de radio que comunica el móvil con la estación base.
- Interface Abis: comunica las estaciones base con la estación controladora.
- Interface A: comunica la estación controladora con el subsistema de conmutación NSS.

4.1.1 La terminal móvil (MS)

El móvil o terminal se usa indiscriminadamente. Es el aparato que lleva el suscriptor para realizar llamadas a la red fija o la red móvil. El móvil está compuesto principalmente por dos elementos:

- La terminal.
- La tarjeta SIM

4.1.1.1 La terminal (ME)

Es el equipo físico de comunicaciones con toda la electrónica que conlleva. La terminal puede ser identificado por el número IMEI (International Mobile Equipment Identity) y realiza las siguientes funciones:

- Digitalización y compresión de la voz.
- Seguridad de la información.
- Encriptación para prevenir la interceptación.
- Modulación de la frecuencia de radio.
- Amplificación y transmisión de la señal.
- Gestión de las canales de transmisión.
- Control de flujo de la señalización.
- Adaptación de la velocidad de datos entre el canal de radio y la velocidad del usuario.
- Gestión de movilidad.

Como se vio anteriormente en el documento, la evolución del móvil vive en continuo cambio y mejoras en cuanto a sus funciones y aplicaciones. La potencia de salida máxima que normalmente se usa es de 800mW.

En la figura 4.3 se muestran algunos modelos de equipos móviles.



Figura 4.3. Terminales móviles

4.1.1.2 La tarjeta SIM

La tarjeta de módulo de identificación de abonado (SIM: Subscriber Identity Module) es la que permite la movilidad de la persona, ya que el usuario puede acceder a la red insertando la tarjeta SIM desde cualquier terminal, la red identifica al abonado y le presta los servicios adquiridos.

La tarjeta SIM contiene la siguiente información relativa al abonado:

- Identificación del abonado (IMSI: International Mobile Subscriber Identity y TMSI: Temporary Mobile Subscriber Identity).
- Número de identificación personal (PIN: Personal Identification Number).
- Clave para desbloquear el PIN (PUK: PIN Unblocking Key).

- Algoritmos para identificación y cifrado.
- Claves de autenticación y de cifrado.
- Servicios suscritos.
- Parámetros para procedimientos de seguridad.
- Información de localización.
- Nombre del operador.



Figura 4.4. Tarjeta SIM

El conector tiene ocho pines metálicos visibles y estos están estandarizados, como se muestra en la figura 4.5, que establecen contacto al insertar la tarjeta en la ranura del lector en el terminal móvil. A través de estos contactos, el lector alimenta eléctricamente a la tarjeta y transmite los datos oportunos para operar con ella conforme a los protocolos de conexión.

- | | |
|------------------------|------------------------|
| 1. VCC (Alimentación) | 5. GND (Tierra) |
| 2. RST (Reset) | 6. Vpp |
| 3. CLK (Clock) | 7. I/O (Input/Output) |
| 4. D+ (USB inter-Chip) | 8. D- (USB inter-Chip) |

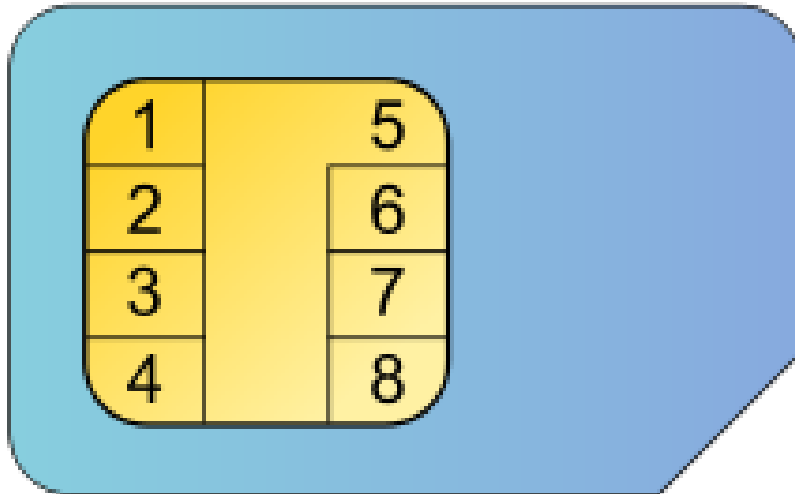


Figura 4.5. Contactos según la norma ISO/IEC 7810 para una SIM

4.1.2 La estación radio base (BTS)

La BTS contiene los transreceptores (transmisores-receptores) y las antenas que definen la celda y manejan el protocolo de enlace de radio con el móvil. La potencia de transmisión del transreceptor define el tamaño de la celda. Cada BTS tiene entre 1 y 16 transreceptores, dependiendo de la densidad de usuarios. La BTS normalmente tiene 3 celdas o sectores, pero muchos operarios confunden el nombre BTS con el de celda. Los transreceptores también son conocidos como transmisores.

El número de BTS en una red es importante, por lo tanto se busca que la BTS tenga el menor procesamiento posible y sea muy sencilla, para que su costo sea bajo y confiabilidad sea alta.

La BTS maneja la interfaz de radio con los móviles y la interfaz Abis con la BSC.

Las funciones principales de la BTS son:

- Codificación del canal: la información es protegida con redundancia y esparcida en el tiempo en diferentes tramas.
- Cifrado: después de la codificación la información es encriptada para prevenir interceptaciones ilegales.
- Formación de la trama: la información es organizada en bloques de 114 bits, enmarcada en un patrón de bits para mejorar la calidad de transmisión y organizada en 8 intervalos de tiempo.
- Modulación: la información modula la frecuencia portadora asignada.

- Control de potencia: las BTS controla la potencia del móvil y de la BTS
- Tiempo de avance (TA: Timing Advance): la BTS calcula la distancia a la cual se encuentra el móvil y le informa con que tiempo de avance debe enviar la información para que no colisione con otro intervalo de tiempo.
- Salto de frecuencia: es una opción para socializar las interferencias, esto es, repartir las interferencias entre todos los abonados que tengan llamadas en una misma celda. En el evento en que la celda tenga varias frecuencias, durante la llamada hace saltos de frecuencia para que la llamada no permanezca todo el tiempo en la frecuencia interferida.
- Sincronización: suministra información a los niveles sobre frecuencia y sincronización.
- Monitoreo y optimización de la calidad de transmisión.

4.1.3 La estación controladora (BSC)

Como la BTS es simple, el procesamiento y toma de decisiones de la parte de radio están centralizados en la BSC. La BSC controla un grupo de BTS y administra los recursos de radio: las frecuencias, potencias, canales de tráfico y señalización y Handover. La BSC se comunica con las terminales a través de las BTS. Las principales funciones de las BSC son:

- Control de un grupo de BTS.
- Conmuta el tráfico entre la MSC y el TRAU
- Asigna y libera los canales de radio.
- Control de Handover dentro de la misma BSC.
- Salto de frecuencia, control de frecuencias y niveles de potencia de las BTS.
- Gestión de configuración y fallas.
- Evaluación de la señalización de la MSC y del móvil.

La BSC está entre las BTS y el TRAU, de tal manera que recoge el tráfico proveniente de muchas BTS a través de interfaces Abis y lo concentra en la menor cantidad de interfaces a entregar al TRAU. La interface entre la BSC y el TRAU

no está estandarizada y recibe varios nombres dados por los fabricantes como Ater y Amux.

4.1.4 La unidad transcodificadora TRAU

El objetivo del TRAU es adaptar la velocidad de las muestras de voz del BSS al NSS y viceversa.

La velocidad del canal de voz en la parte radio es menor a 16 Kbps.

- Full Rate (FR)= 13 Kbps.
- Half Rate (HR)= 5.6 Kbps.
- Full Rate mejorada (EFR: Enhanced Full Rate) = 12.2 Kbps.
- En la interfase A, la Voz es codificada usando la ley de codificación "A". cada muestra de la voz es codificada en 8 bits, los cuales son transmitidos cada 125 μ s. 8 mil muestras son transmitidas en 1 segundo, dando una velocidad total de $8\text{bits} \times 8000 = 64 \text{ Kbps}$.

El TRAU adapta los 64 Kbps de la interface A a los 16 Kbps que se requieren en la interfase Abis. Esto se logra mediante algoritmos de compresión/expansión de los 8 bits de cada muestra contenida en un intervalo de tiempo en la interface A, a 2 bits que requiere la interface Abis.

El TRAU forma parte de la BSS, pero para hacer un uso más eficiente de las enlaces y ahorrar ancho de banda, se coloca lo más cerca posible de la MSC.

4.2 El subsistema de conmutación de red (NSS)

Su principal rol es el de establecer las comunicaciones entre los usuarios móviles y otros abonados móviles o fijos. En el NSS se tienen las bases de datos con información de los abonados y se maneja su movilidad. El NSS conecta la red móvil PLMN (Public Land Mobile Network) con otras redes como la red fija PSTN (Public Switched Telephone Network) y la red de datos PDN (Packet Data Network).

En la figura 4.6 se muestra el subsistema NSS.

Los diferentes componentes del NSS son:

- La central de conmutación móvil (MSC: Mobile Switching Center).
- El registro de datos local (HLR: Home Location Register).
- El registro de datos de visitantes (VLR: Visitor Location Register).
- El centro de autenticación (AuC: Authentication Center).
- El registro de identidad de equipos (EIR: Equipment Identity Register).

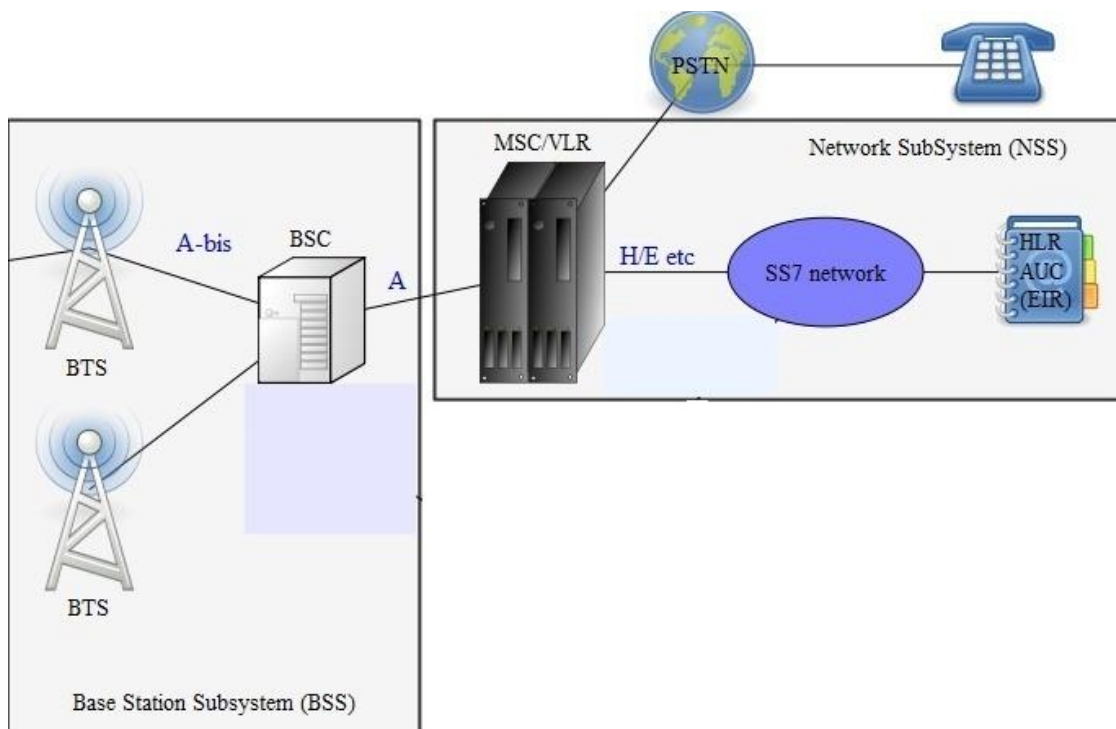


Figura 4.6. Sub-Sistema NSS en una red GSM

Otros equipos opcionales que pertenecen al NSS son:

- Centro de servicios de mensajes cortos (SMS-C: Short Message Service Center).
- Servidor de mensajes de voz.
- Red inteligente (IN: Intelligent Network), para implementar servicios centralizados, ejemplos de estos servicios son por ejemplo, las llamadas por cobrar, el servicio sígueme de Telmex, encuestas telefónicas, portabilidad de número etc.

- La plataforma de prepago, que permite que el operador tenga abonados prepago.

4.2.1 La central de conmutación móvil (MSC)

Es el componente central del NSS. Actual como un nodo de conmutación normal, tal como los usados en la red fija, pero adicionalmente provee todas las funcionalidades necesarias para manejar un abonado móvil, tales como el registro, la autenticación, la ubicación del abonado, los cambios de celda y el enrutamiento de llamadas. La señalización que se usa entre las diferentes entidades funcionales en el subsistema de red es el número 7 (SS7: Signaling System Number 7). La MSC Suministra la conexión con la red fija PSTN vía SS7.

Sus funciones principales son:

- Manejo de llamadas.
- Gestión de movilidad.
- Ejecución del cambio de celda, cuando se cambia del BSC.
- Interfase hacia la PSTN para llamadas terminales.

La MSC que comunica con la PSTN se llama GMSC, donde la G es de Gateway. Es la puerta que une la red fija con la red móvil.

4.2.2 Registro de datos local (HLR)

El HLR es la base de datos en la que se almacena la información de los abonados que pertenecen a una red. Esta base de datos es alimentada por el operador de la red y contiene la siguiente información:

- Identificación del abonado (MS-ISDN e IMSI).
- Servicios suscritos por el abonado.
- Información de localización (VLR donde el móvil está registrado).
- Derechos del Roaming del abonado.

La información de la localización es dinámica y depende de los movimientos del usuario. Cada vez que el usuario se registra en un nuevo MSC/VLR, se actualiza el HLR.

El abonado se conoce en la red por su número IMSI, pero lo que le público conoce es el número MS-ISDN. En el HLR se hace la conversión de un número al otro.

- **IMSI (International Mobile Subscription Identity):** El número IMSI se almacena en la SIM. Podemos conocerlo preguntando a nuestro operador. Tiene un máximo de 15 cifras. Los primeros tres dígitos definen el país y se llaman MCC (Mobile Country Code) o IPM (Indicativo de País para el servicio Móvil). Le sigue el número que indica el operador, es el MNC (Mobile Network Code) o IRM (Indicativo de la Red Móvil), de hasta tres cifras. Los dígitos restantes son el MSIN (Mobile Subscription Identification Number) y se reservan para que el operador los asigne a cada una de las líneas de sus clientes, como se ilustra en la figura 4.7. Es asociado con cada persona que lo compra y es el único identificador del usuario (en el nivel de movilidad de las comunicaciones móviles) que es invariable.

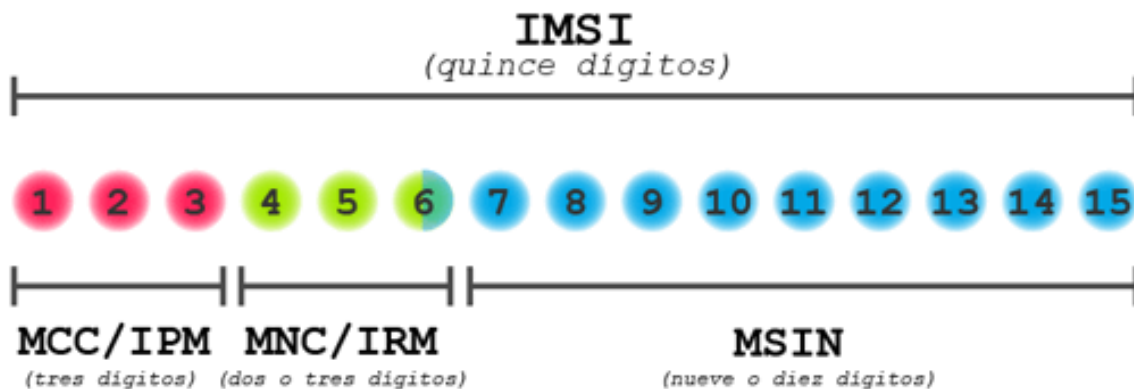


Figura 4.7. Estructura del número IMSI

- El MSISDN (de sus siglas en inglés mobile station integrated services digital network). Con este número nos pueden identificar y es el número que memorizamos y el que proporcionamos a otros abonados, (véase en la figura 4.8). Éste número no está atado al operador y por ello nos permite migrarlo a otro operador. Por extraño que parezca, este número es una entidad lógica y no se guarda en la SIM. El operador dispone de una tabla que enlaza los IMSI con el número de la persona. Por tanto, cuando una persona llama a ese número, el operador primero busca en su tabla a qué IMSI le corresponde. Por tanto, sería posible asociar múltiples MSISDN a

un único IMSI y ese usuario sería localizable desde distintos números de teléfono utilizando una sola SIM.

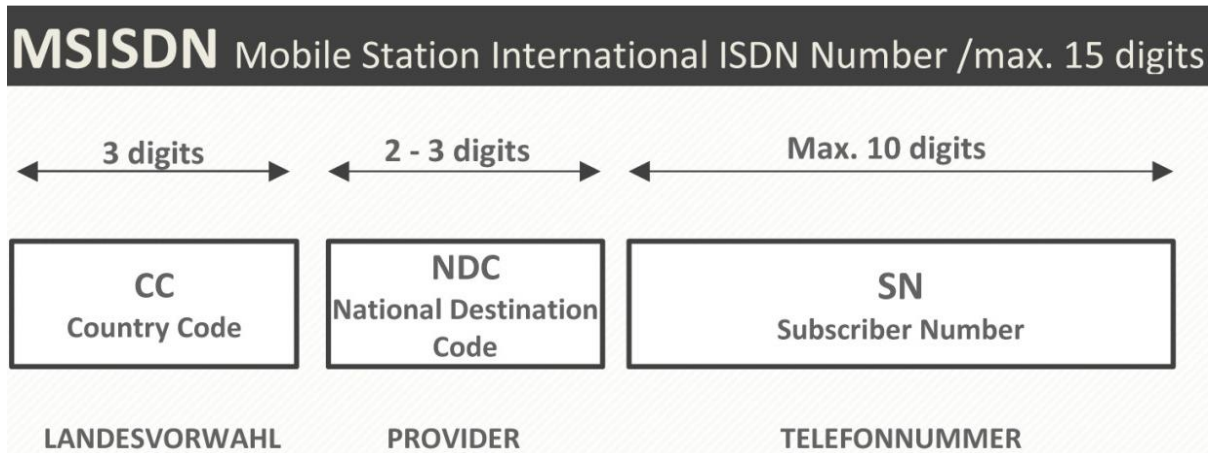


Figura 4.8. Estructura del número MSISDN

4.2.3 Registro de datos de visitantes (VLR)

El VLR es una base de datos dinámica, que varía de acuerdo a los movimientos del terminal. El VLR está asociado a una MSC, por lo cual normalmente se escriben las dos unidades como MSC/VLR, y contiene información de los abonados que actualmente visitan la MSC.

Cuando un abonado entra en el área de cobertura de una nueva MSC, el VLR asociado a esta MSC crea este abonado con los datos consultados al HLR que contiene el abonado. Cuando el abonado deja el área de cobertura de la MSC, el VLR lo borra automáticamente. Esto garantiza que la MSC tiene muy cerca los datos del abonado, y no necesita estar consultando al HLR cada vez que se establezca una comunicación.

La información contenida en el VLR es:

- Identificación del abonado (IMSI, MS-ISDN)
- Información de localización del abonado (LA: Localitation Área).
- Estado del abonado: libre, ocupado, apagado.
- Servicios suscritos por el abonado.

4.2.4 Centro de autenticación (AuC)

El AuC contiene una base de datos, utilizada para autenticar al abonado y para proteger su información contra interceptaciones.

La clave de identificación y los algoritmos de encriptación son almacenados tanto en el AuC como en la tarjeta SIM del usuario.

4.2.5 Registro de identidad de equipos (EIR)

La idea original de este registro fue darle seguridad a los terminales y protegerlos contra robo. El EIR contiene la identificación del terminal IMEI. Esta identificación la puede conocer el usuario digitando en el móvil *#06#.

El procedimiento consistía en que cuando al usuario le robaran el terminal debía llamar al operador y entregar el IMEI para que el operador bloqueara dicho terminal en el EIR. La estrategia no funciono porque en algunas terminales robadas le pueden cambiar el IMEI.

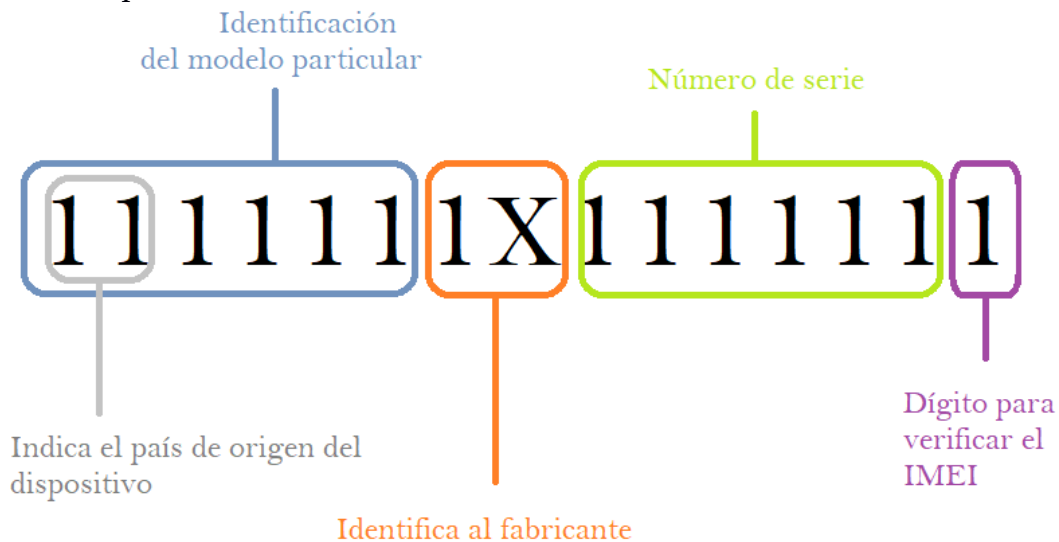


Figura 4.9. Numero IMEI

4.3 El subsistema de operación y mantenimiento (OSS)

El OSS está compuesto por:

- El centro para la operación y mantenimiento de la parte Radio (OMC-R Operation and Maintenance Center for Radio Part).
- El centro para la operación y mantenimiento de la parte de conmutación (OMC-S Operation and Maintenance Center for Switching Part).

El subsistema de operación y mantenimiento se conecta básicamente a la BSC y la MSC para gestionar y monitorear el sistema GSM, como se aprecia en la figura 4.10.

La gestión de una red GSM está basada en el estándar TMN (Telecommunications Management Network).

Cinco funciones de gestión son definidas:

- Gestión de configuración.
- Gestión de fallas.
- Gestión del desempeño.
- Gestión de seguridad.
- Gestión de cuentas.

Los componentes de esta arquitectura funcional son:

- Sistema de operación (OS: Operation System), desde donde se realizan las cinco funciones de gestión de la red previamente definidas.
- Equipos de medición (ME: Mediation Equipment), controlan los elementos de red.
- Elementos de red (NE: Network Elements): son propiamente los equipos a gestionar como las estaciones base.
- Red de comunicación de datos (DCN: Data Communication Network), es la red que une los elementos de red con los equipos de mediación y a estos con los sistemas de operación.

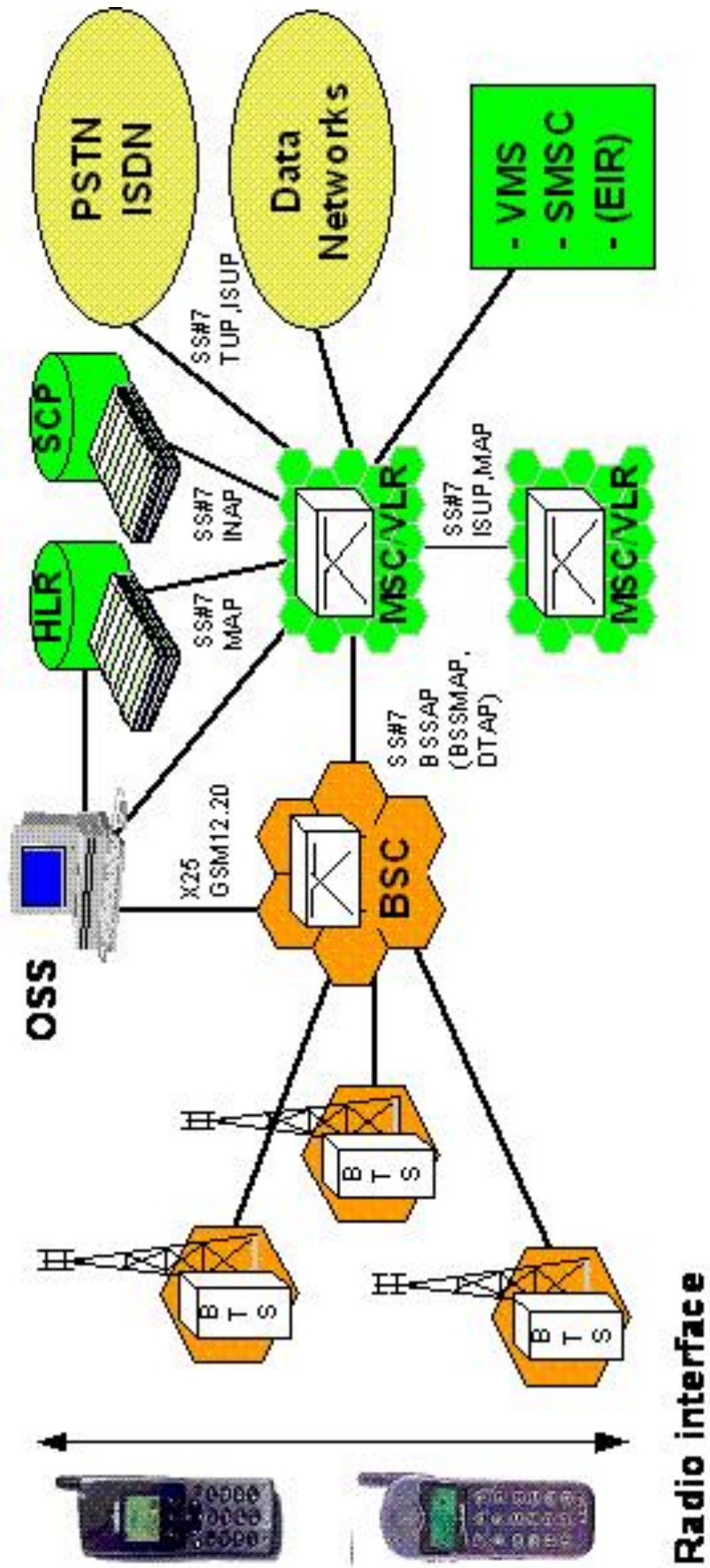


Figura 4.10. Sub-Sistema OSS en una red GSM

5 INTERFACES Y PROTOCOLOS USADOS EN GSM

Los elementos funcionales de la red GSM se interconectan a través de interfaces y protocolos que están estandarizados y cuyo estudio detallado de los mismos no hace parte del alcance de la presente tesis.

Los protocolos están basados en las 7 capas del sistema OSI (Open System Interconnection) que son las capas, física, enlace de datos, red, transporte, sesión, presentación, aplicación y que solo se mencionan en este documento pero no se adentrará en las funciones de cada una de las capas que este modelo posee.

5.1 Interfaces de la red GSM

Se define "interfaz" como la "Conexión o frontera común entre dos aparatos o sistemas independientes".

De esta forma, entre cada entidad de las anteriormente mencionadas que mantengan una comunicación, se define un interfaz que servirá de soporte para los mensajes intercambiados.

En las siguientes figuras se muestran dos esquemas que contienen los nombres de los interfaces que se definen entre cada entidad de red, incluyendo el segundo el interfaz G (interfaz entre dos VLRs pertenecientes a distinta MSC) y H (interfaz entre HLR y AUC).

A continuación se detallan algunos aspectos sobre los interfaces GSM y se ilustran en la figura 5.1:

- Interfaz Um - Interfaz MS-BSS que proporciona servicios de circuito y de paquetes de datos sobre el interfaz aire. Es utilizada por las MS para acceder a todos los servicios de la red GSM a través de la BTS.
- Interfaz Abis - Interfaz BSC-BTS, usualmente tiene una tasa de transferencia de 16 Kbps para señalización y 64 Kbps para voz y datos de usuario. Permite conectar de una forma normalizada estaciones base y controladores de estación base, independientemente de que sean realizadas por un mismo suministrador o por suministradores distintos.

- Interfaz A - Interfaz MSC-BSC. Se utiliza fundamentalmente para el intercambio de información para:

1. Gestión de la BSS
2. Manejo de la llamada
3. Gestión de la movilidad

Soporta canales estándar de 64 Kbps para señalización y tráfico de usuario, sobre una tasa de 2 Mbps. Los principales protocolos de este interfaz son DTAP (Direct Transfer Application Part) y BSSAP (Base Station Subsystem Application Part).

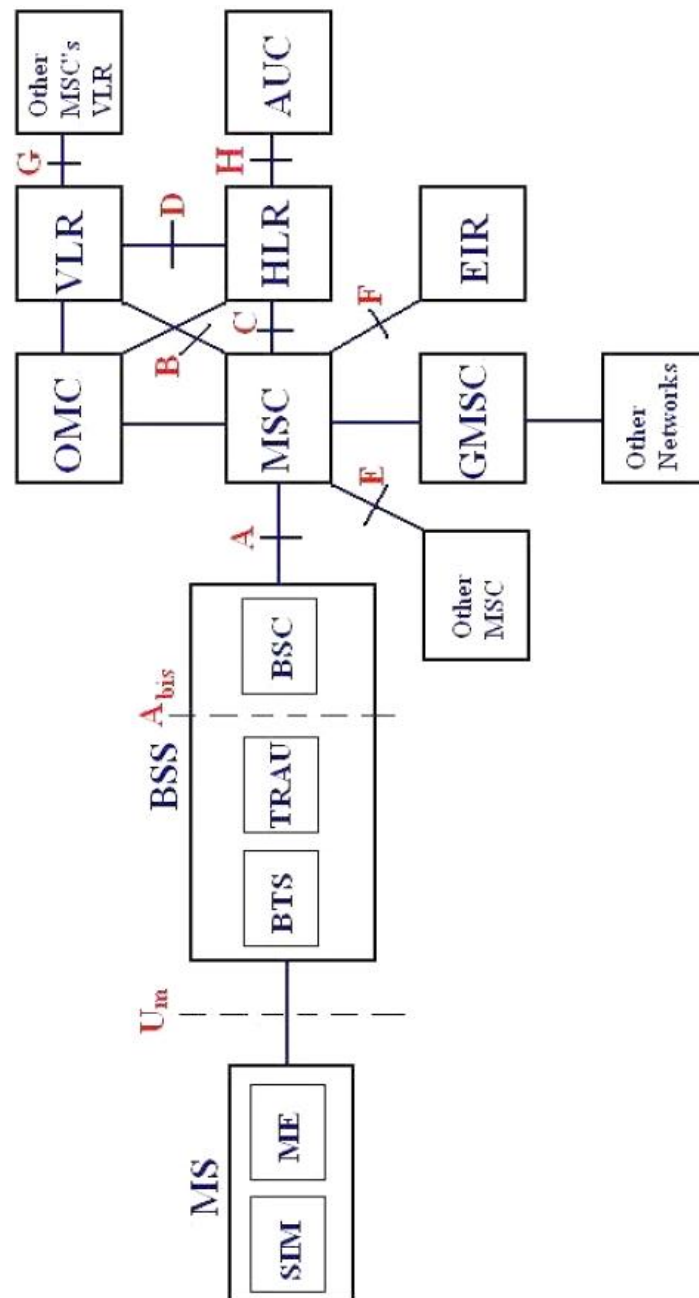


Figura 5.1. Esquema de interfaces en el estándar GSM

DTAP es un protocolo de aplicación para transferir información de señalización entre la MS y la MSC en redes GSM.

BSSAP es un protocolo para transportar información de control de la BSC entre la MSC y la BSS, por ejemplo, para la asignación de canales de tráfico entre la MSC y la BSS.

- Interfaz B - El interfaz MSC-VLR no está normalizada por tratarse normalmente de interfaces internas, dejándose sus especificaciones al criterio del desarrollador del equipo. Cuando un MSC necesite proporcionar información sobre un móvil acudirá a su VLR. Esta interfaz no debe ser externa (dado el volumen de información intercambiado).
- Interfaces C, D, E, F y G - Fueron estandarizadas por el protocolo MAP, protocolo que utiliza los servicios de transacción y transferencia de mensajes del Sistema de Señalización número 7 (SS7). Su funcionalidad se comenta a continuación.
 - Interfaz C: Sobre él se pide la solicitud de información de tarificación por parte de la MSC al HLR, o la localización del terminal necesario para que reciba una llamada de una red externa fundamentalmente.
 - Interfaz D: Esta interfaz se utiliza para intercambiar los datos relacionados con la posición de la estación móvil y los datos de suscripción del usuario. El VLR informa al HLR sobre la posición de una estación móvil, proporcionándole un número de seguimiento a fin de que pueda encaminar las llamadas. En el otro sentido, el HLR envía al VLR de la MS los datos necesarios para soportar los servicios contratados por el usuario. Cuando la estación móvil pasa a estar en el área servida por otro VLR, el HLR envía al primer VLR la orden de que borre el registro de dicha MS.
 - Interfaz E: Cuando una estación se desplaza del área controlada por una MSC al área de otra MSC distinta, es necesario realizar un procedimiento de traspaso para poder continuar la conversación. En este caso las MSC deben intercambiar datos para poder llevar a cabo esta operación.
 - Interfaz F: Utilizada cuando el MSC desea comprobar el IMEI de un equipo.

- Interfaz G: Utilizada para permitir la interconexión entre dos VLRs de diferentes MSCs.
- Interfaz H - Al igual que el interfaz B, el interfaz HLR-AUC suele ser interno, no estando normalizado.
- Interfaz I - En el interfaz MS-MSC se da el intercambio transparente de datos entre la estación móvil y el centro de conmutación móvil.

5.2 Protocolos y señalización en la red GSM

La red GSM debe ser capaz de transmitir la información de usuario a cualquier destino dentro de la propia red o de otra. Para ello también es necesario que proporcione funciones de conmutación y conectividad sobre las redes fijas convencionales, tales como la red RDSI (ISDN - Integrated Services Digital Network) o la red pública conmutada (PSTN - Public Switched Telephone Network). Además de esto, se deben tener en cuenta los aspectos de la señalización derivados de la movilidad de los terminales (localización, continuidad de la llamada en curso etc).

GSM consigue todo esto gracias a un doble esquema de señalización. Por un lado implementa un sistema específico para el interfaz Um, y por otro el sistema Señalización Numero 7, o SS7, para el NSS. Dentro de este último coexistirán varios protocolos para según sobre que interfaz se lleve a cabo la comunicación.

A continuación se comentan los distintos protocolos usados en base a la figura 5.2, teniendo en cuenta los dos diferentes sistemas comentados.

La capa física será la específica de la red GSM en los interfaces Um y Abis, de cuyas características generales se dará una visión en el siguiente apartado. No obstante, para los mensajes de señalización sobre el interfaz A BSS-MSC se utilizan los servicios de la parte de transferencia de mensajes MTP (Message Transfer Part), que proporciona una transmisión fiable y segura.

En el nivel de enlace pueden verse dos protocolos distintos sobre los interfaces Um y Abis. Por un lado LAPD (Link Access Procedure on D channel), y por otro LAPDm, que es una modificación del primero apropiada para el interfaz radio MS-BTS. LAPD (también conocido como ITU Q.921) es un protocolo de control de enlace de datos para los canales tipo D. Tiene dos formas de operación, orientada o no a conexión, y en esencia está diseñado para convertir un enlace físico poco fiable en un enlace de datos fiable. Al igual que para el nivel físico, entre BSS y MSC se utilizara MTP en la comunicación.

GSM Protocol Stacks

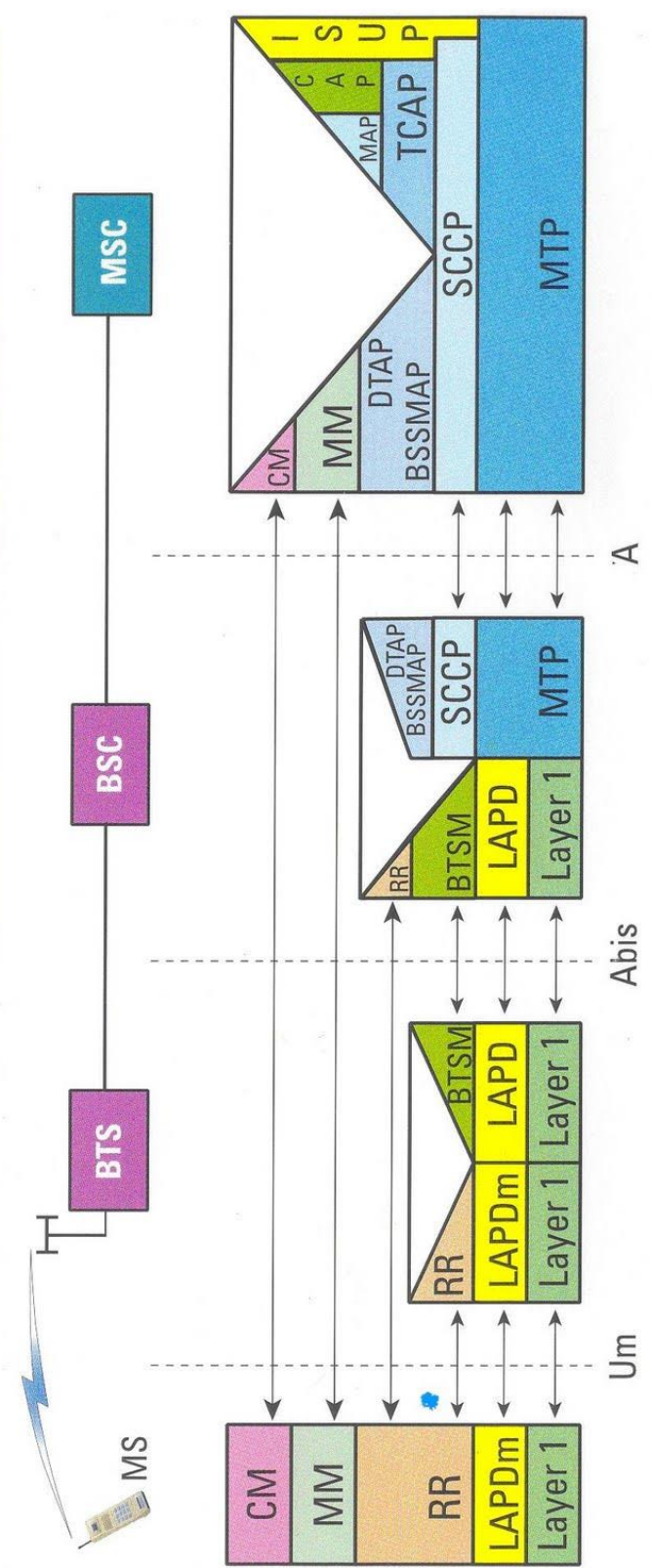


Figura 5.2. Protocolos GSM

El nivel de red se divide a su vez en tres protocolos distintos:

- Gestión de la Conexión (CM - Connection Management). Se encarga de:
 - Control de llamadas. Establece, mantiene y finalmente libera la llamada. CM interactuara con las entidades VLR, GMSC y HLR para la gestión del servicio orientado a la conmutación de circuitos, incluyendo voz y circuito de datos.
 - Servicio suplementario de gestión. Permite a los usuarios tener cierto control sobre su llamada pudiendo variar el servicio básico.
 - Servicio de mensaje corto (SMS). - La transmisión de mensajes cortos requiere establecer una relación de señalización entre la estación móvil y el MSC.
- Gestión de la Movilidad (MM - Mobility Management)
 - Gestiona la base de datos de usuarios, incluyendo la información de localización.
 - Gestiona además las actividades de autenticación SIM, HLR y AuC.
- Gestión de Recursos Radio (RR - Radio Resource Management)
 - Gestiona la transmisión sobre la interfaz radio sobre la que está establecida la conexión MS-BTS. Provee un enlace estable entre la estación móvil y la BSC.
 - Sera la BSS quien realice la mayor parte de las funciones RR.

El protocolo de capa de red BTSM sobre el interfaz Abis gestionara los mensajes RR con la BTS al igual que SCCP hace con BSSAP cobre el interfaz A.

BSSAP es un protocolo para transportar información de control de la BSC entre la MSC y la BSS, por ejemplo, para la asignación de canales de tráfico entre la MSC y la BSS.

CM y MM se implementan en el interfaz A de la MSC, mientras que el RR lo hará sobre la BSC. El protocolo usado para transferir los mensajes CM y MM será BSSAP (Base Station System Application Part), que permite el control directo de la BSS. Por su parte SCCP se encarga del direccionamiento y enrutamiento de las

centrales, ya que ha sido ideado fundamentalmente para posibilitar la transferencia de mensajes entre dos Puntos de Señalización cualesquiera, pertenezcan a la misma red SS7 o a dos distintas.

Para el establecimiento y supervisión de las llamadas establecidas con usuarios de las redes PSTN e ISDN, se utilizan los protocolos TUP e ISUP respectivamente. Para los mensajes de señalización con las entidades HLR, VLR, otras MSC, etc., propias de GSM, se usa el protocolo MAP complementado por TCAP (Transaction Capability Application Part), que proporciona funciones para la comunicación con el extremo remoto de una cadena de señalización y permite el establecimiento de múltiples diálogos.

El TCAP aparte de soportar transacciones entre dos entidades, comprende de dos capas:

- Transacción:
 - Una transacción es un dialogo durante una conexión.
 - Comienza con un mensaje Begin, seguido por varios mensajes, Continue y termina con un mensaje End.
 - Cada entidad identifica la transacción por un número. Los dos números son suministrados al intercambiar mensajes: origen destino.

- Componente:
 - Indica la naturaleza de la operación que se lleva a cabo.
 - Invocación: es un requerimiento de una acción o una información.
 - Resultado: es la respuesta al requerimiento.
 - Error: es un reporte de falla al ejecutar la operación.
 - Rechazo: la operación es rechazada.

TCAP, junto con MAP, constituyen los protocolos más importante de la Core de una red móvil, porque soportan la funcionalidad de Roaming. Encima de MAP están las aplicaciones de los sistemas MSC, HLR, VLR y EIR.

En la tabla 1 se incluye a modo de resumen, las interfaces, los protocolos de la arquitectura GSM, así como le tipo de información que circula por ellos.

Tabla 5.1. Interfaces y Protocolos de GSM

Interfaz	Se encuentra entre	Descripción	Intercambio de información de:	
			Usuario	Señalización
A	MSC-BSC	Permite el intercambio de información sobre la gestión del subsistema BSS, de las llamadas y de la movilidad. A través de ella, se negocian los circuitos que serán utilizados entre el BSS y el MSC.	SI	SS7
Abis	BSC-BTS	Permite el control del equipo de radio.	SI	LAPD
B	VLR-MSC	VLR es la base de datos que contiene toda la información que permite ofrecer el servicio a los clientes que se encuentran en el área de influencia de sus MSC asociados. Por lo tanto, cuando un MSC necesite proporcionar información sobre un móvil acudirá a su VLR. Esta interfaz NO debe ser externa NO (por desempeño, por el volumen de información intercambiado).	NO	MAP/B
C	HLR-GMSC	Es la interfaz utilizada por los Gateways GMSC para enrutar la llamada hacia el MSC destino. La GMSC no necesita contar con un VLR, se trata de un nodo que solo transmite llamadas.	NO	MAP/C
D	HLR-HLR	Permite intercambiar información entre ambas bases de datos, esta información se encuentra relacionada con la posición del móvil y la gestión del servicio contratado por el usuario.	NO	MAP/D
E	MSC-MSC	Permite intercambiar la información necesaria para iniciar y realizar un intercambio Inter MSC cuando el móvil cambia de área de influencia de un MSC a otro.	SI	MAP/E, RDSI e ISUP
F	MSC-EIR	Utilizada cuando el MSC desea comprobar el IMEI de un equipo.	NO	
G	VLR-VLR	Utilizada para permitir la interconexión entre dos VLRs de diferentes MSCs.	NO	MAP/G

H	HRL-AuC	Igual al interfaz B, no suele estar normalizado	SI	MAP/H
I	MSC-MS	Permite el intercambio transparente de datos entre el MSC y el MS a través del BSS.		
Um	BSS-MS	Es la interfaz de radio, se encuentra entre la estación móvil y el BSS.	SI	LAPDm

En la figura 5.3 se muestran los protocolos MAP/X asociados a cada interfaz.

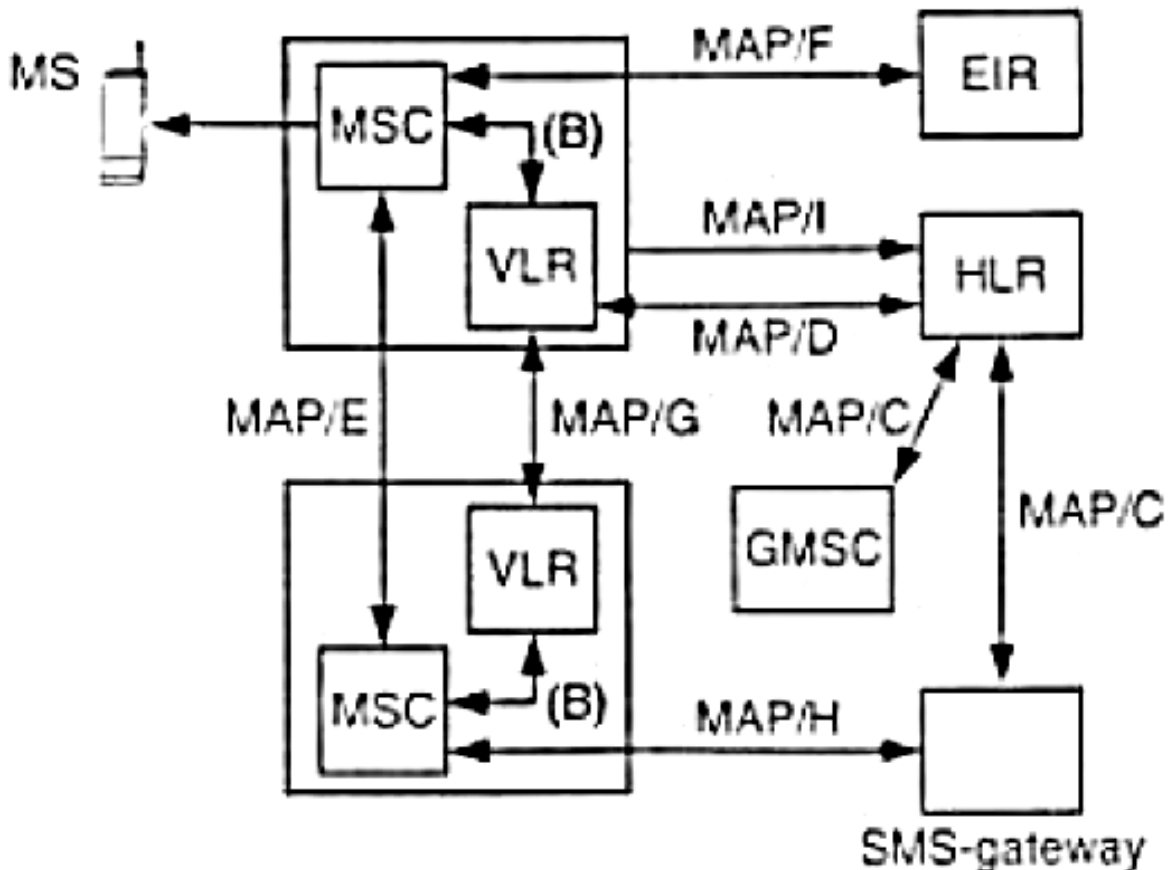


Figura 5.3. Protocolos MAP/X

5.2.1 Aspectos de red

La mayoría de los conceptos que se van a describir en este apartado ya han sido estudiados de manera general en el tema anterior, sin embargo, debido a su importancia y porque incluyen en parte la operación del VLR y HLR se repite ahora con un enfoque diferente.

Las funciones principales definidas en una red GSM son:

- Gestión de Recursos de Radio (RR: Radio Resources Management): Controla el establecimiento, mantenimiento y terminación de los canales de radio, incluyendo el Handover.
- Gestión de Movilidad (MM: Mobility Management): Maneja el Location Update y los procesos de registro, seguridad y autenticación.
- Gestión de las comunicaciones (CM: Communication Management): maneja el control de las llamadas y servicios suplementarios como mensajes cortos.

5.2.1.1 Gestión de recursos de radio (RR)

La función principal del RR es establecer, mantener y liberar las comunicaciones entre el móvil y la MSC. Los elementos involucrados son el móvil y la BTS. Sin embargo, como el RR debe mantener la comunicación aun cuando el móvil cambie de celda, la MSC, que es la encargada del Handover en esos casos, también se involucra.

EL RR también es responsable de la gestión de las frecuencias y cómo reacciona la red frente a los cambios de las condiciones atmosféricas. Algunos de los principales procedimientos del RR son:

- Asignación y liberación del canal.
- Paging.
- Handover.
- Tiempo de avance.
- Salto de frecuencia.
- Transmisión discontinua.
- Control de potencia.

Una sesión de RR es siempre iniciada por el móvil a través del procedimiento de acceso, ya sea para una llamada saliente o entrante.

5.2.1.1.1 Handover

El procedimiento de cambio de una celda a otra, mientras el móvil tiene una comunicación establecida, se llama Handover. Se presenta por el móvil del usuario que se aleja de una celda y se acerca a otra como se observa en la figura 5.4. Se pueden distinguir tres tipos de Handover:

- Handover entre dos celdas que pertenezcan a la misma BSC.
- Handover entre dos celdas de diferente BSC y que pertenecen a la misma MSC/VLR.
- Handover de celdas controladas por diferentes MSC/VLR.

En la mayoría de los casos el Handover es controlado por la BSC, la cual recibe del móvil la potencia y calidad de la señal recibida de la celda que lo está atendiendo y de las celdas vecinas. La BSC aplica el algoritmo necesario para decidir en qué momento hace el Handover. En este caso, la BSC simplemente notifica a la MSC del Handover. El Handover puede ser iniciado por la MSC para balancear el tráfico. También es controlado y decidido por la MSC en el evento de que al cambiar de celda se cambie de BSC. En UMTS, la función de Handover se pasó totalmente a la estación controladora (RNC: Radio Network Controller).

El Handover que se presenta en la red GSM se le conoce ahora como Handover duro, ya que hay cambio de frecuencia y al mismo tiempo que se toman los recursos de la nueva celda, se liberan los recursos de la celda anterior, existiendo una pequeña probabilidad de que la llamada se caiga. En UMTS apareció el Handover suave, que consiste en utilizar los recursos de ambas celdas al mismo tiempo durante el Handover, para evitar este problema.

El móvil recibe el listado de las celdas vecinas por el canal BCCH y mide el nivel de cada señal BCCH de todas las celdas. Esta medida es enviada por el móvil a la BSC por medio del canal SACCH.

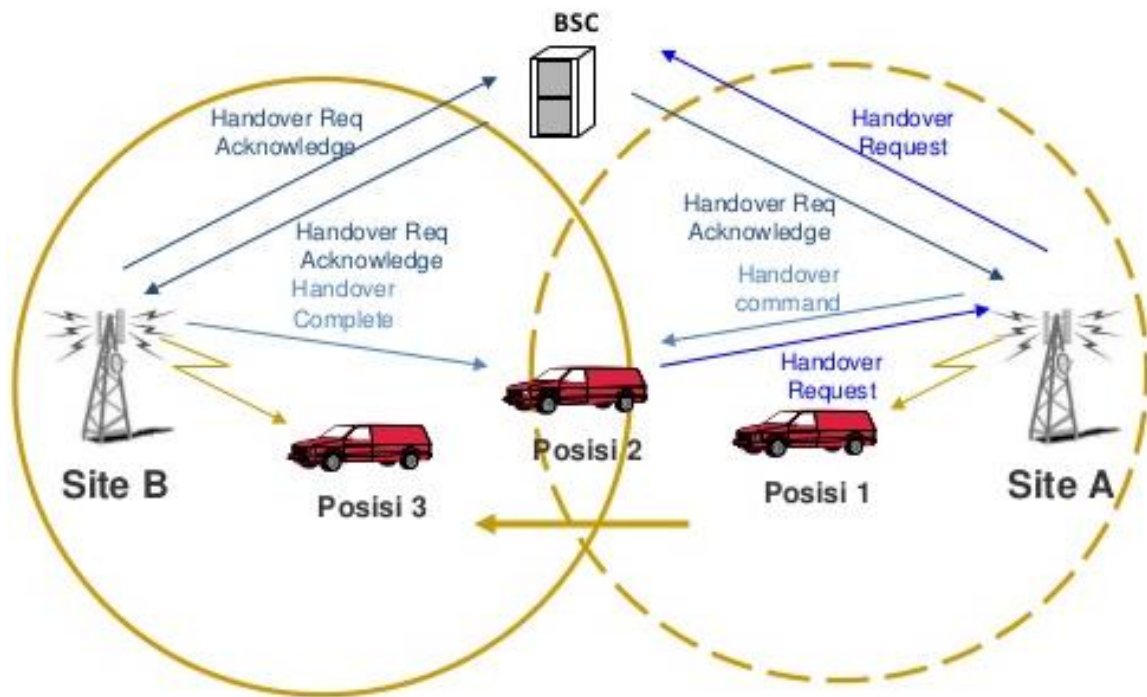


Figura 5.4. Concepto de Handover

Dos algoritmos básicos son usados para decidir el Handover:

- El algoritmo del desempeño aceptable mínimo. Cuando la calidad de la señal decrece, se aumenta el nivel de potencia del móvil (control de potencia). Si al aumentar la potencia la señal no mejora, la alternativa es el Handover.
- El algoritmo del cálculo de potencia, el cual le da precedencia al Handover sobre el control de potencia, intentando mantener la calidad de la señal con la misma potencia haciendo Handover. Esto reduce problemas de interferencias co-canal y evita que cuando llegue a la otra celda, el móvil lleve la máxima potencia.

5.2.1.1.2 Tiempo de avance

El método de acceso de los móviles a la estación base es por medio del acceso múltiple por división de tiempo (TDMA: Time Division Multiple Access). Por tanto, los Bursts transmitidos por estos móviles deben llegar a dicha estación base en un tiempo tal que formen una trama TDMA.

Debido a que los usuarios están a diferente distancia con respecto a la estación base y que el retardo de la señal depende de esta distancia, el sistema debe usar la característica de tiempo de avance para hacer que las señales que vienen de los diferentes móviles lleguen a la estación base en el momento oportuno.

Además, como los usuarios tienen movilidad, la estación base debe estar midiendo constantemente el retardo de las señales recibidas de los móviles, para indicarle a cada móvil con cuánto tiempo de avance debe enviar sus Burst y evitar que sus señales se solapen.

5.2.1.1.3 Salto de frecuencia

Las interferencias y las condiciones de propagación, y por ende el desvanecimiento de la señal y las multitrayectorias, dependen de la frecuencia. Para evitar diferencias de calidad en los canales, se implementa el salto de frecuencia cuando se tienen varias portadoras en la misma celda. El salto de frecuencia cambia la frecuencia en cada trama TDMA, y por tanto socializa el efecto de las interferencias co-canales.

La idea no es evitar las interferencias, sino repartir este efecto en todos los canales. Si una portadora tiene interferencias, la comunicación que utilice dicha portadora tiene problemas de calidad, cuando hace el salto de frecuencia el problema desaparece. Sin embargo, un nuevo canal será asignado a esta frecuencia interferida provocando mala calidad de la comunicación durante el pequeño tiempo que tiene asignada esta portadora.

Existen diferentes algoritmos de salto de frecuencia. El algoritmo seleccionado es informado al móvil por vía del canal BCCH.

5.2.1.1.4 Transmisión discontinua (DTX)

La transmisión discontinua es usada para minimizar las interferencias durante las llamadas de voz y ahorrar batería del móvil. El principio consiste en no transmitir señal durante los silencios (cuando no hay actividad de voz). Un ruido de fondo es reconstruido en el otro extremo para evitar “espacios” que aparezcan como si la llamada se hubiera cortado. Esta característica es muy interesante si tenemos en cuenta que la persona habla menos del 50% durante una conversación.

El control de potencia es obligatorio en los móviles (trayecto Uplink) y opcional en Downlink. Por tanto, el móvil debe cumplir las siguientes características:

- Detección de actividad de voz (VAD: Voice Activity Detection).
- Generación del ruido de fondo cuando reciba en el trama el SID (Silence Descriptor).

5.2.1.1.5 Control de potencia

Su objetivo es transmitir la señal de radio en la interface aérea a la potencia correcta, esto es, no demasiado alto como para minimizar las interferencias con otros móviles, ni demasiado bajo, de tal manera que se pueda recibir una buena calidad de la señal transmitida.

El control de potencias es obligatorio en los móviles (trayecto Uplink). La potencia se puede variar, hacia arriba o hacia abajo, en pasos de 2 dB cada 60 ms. La potencia mínima es de 13 dBm (20 miliwatts) y la máxima es 29 dBm (0.8 watts), lo vemos en la figura 5.5.

El móvil mide la potencia y calidad de la señal recibida, basado en los errores de bit, y envía la información a la BSC cada 480 ms por el SACCH. La BSC decide si debe variar la potencia y envía el comando al móvil por el SACHH.

El control de potencia puede implementarse en la BTS (trayecto Downlink) en pasos de 2 dB.

El control de potencia debe manejarse con cuidado, ya que existe la posibilidad de provocar una inestabilidad si un móvil aumenta su potencia en respuesta a una interferencia co-canal causada por otro móvil que había aumentado su potencia previamente.

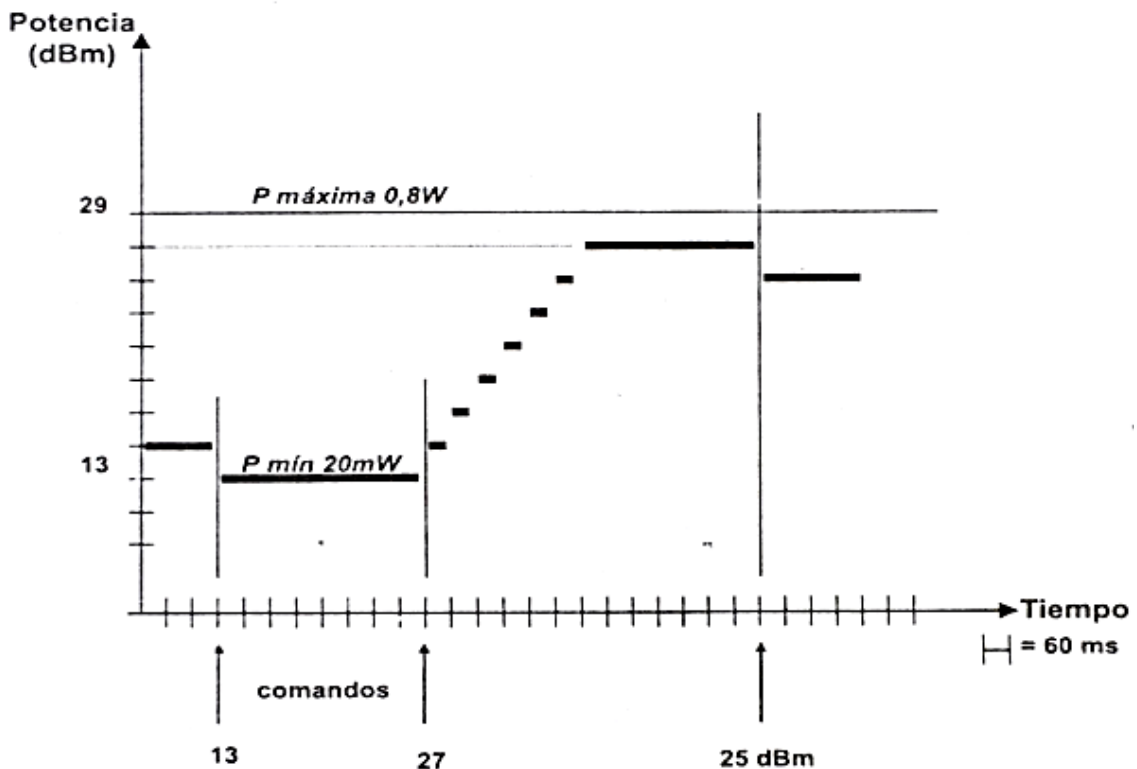


Figura 5.5. Control de Potencia

5.2.1.2 Gestión de movilidad (MM)

La función del MM es la encargada de todos los aspectos relacionados con la movilidad:

- Location Update.
- Autenticación y seguridad.
- Definición de frecuencia.

5.2.1.2.1 Location update

El Location Update consiste en actualizar la ubicación del móvil en la red. El HLR apunta al VLR que está visitando el móvil, el VLR contiene el área de localización del móvil. El área de localización es un número, definido por el operador de la red, que identifica a un conjunto de celdas. Esto significa que la red no conoce con cual celda está el móvil sino en cual área de localización. Cuando la red necesita ubicar al móvil, por ejemplo para indicarle que tiene una llamada, le hace Paging en todas las celdas de localización donde se encuentra el móvil.

El número de área de localización es enviado por todas las celdas por el BCCH. Cuando el móvil cambia de celda bajo la misma área de localización, la red no se entera. Pero cuando el móvil cambia de área de localización realiza el proceso de Location Update. El móvil también actualiza su área de localización en la tarjeta SIM.

El área de localización se utiliza para evitar hacer Location Update con cada cambio de celda del móvil, lo cual consume recursos.

La red tiene un temporizador que tiene una duración estándar de 60 minutos y cada vez que se vence revisa cuales móviles no han tenido actividad de llamadas o no ha hecho Location Update en ese último periodo de tiempo. Los móviles que no han realizado ninguno de estos dos procesos los marca como Dettached, que significa apagados, de tal manera que si uno de estos móviles recibe una nueva llamada, le coloca al llamante el buzón de dicho abonado y no gasta recursos intentando un Paging que no va a ser respondido. Mientras tanto el móvil tiene otro temporizador, con una duración de 50 minutos, cuyo valor lo recibe de la red por el BCCH. Cada vez que se vence este temporizador, si el móvil no ha tenido actividad de llamadas ni ha cambiado de área de localización, el móvil realiza el proceso de Location Update para evitar que la red lo marque Dettached.

Cuando aparecieron las llamadas de paquetes se introdujo el RA (Routing Area)

5.2.1.2.2 Autenticación y seguridad

Una de las funciones importantes que realiza la red se conoce con el nombre de triple A (AAA: Authorization, Authentication and Accounting).

La autorización consiste en verificar si el abonado tiene permiso para acceder al servicio que está solicitando por la red por ejemplo si tiene saldo en el caso de abonados prepago. Dichos servicios se encuentran matriculados en el HLR y VLR.

La autenticación consiste en verificar si el usuario es quien dice ser. Esto es necesario, debido a que el medio de radio puede ser accedido por cualquier persona. La autenticación involucra a la tarjeta SIM y el centro de autenticación (AuC). Como se mencionó anteriormente, cada abonado tiene almacenado una clave y un algoritmo de encriptación tanto en la SIM como en el AuC. Para la autenticación, la red genera un número aleatorio de 128 bits llamado RAND. El móvil aplica el algoritmo, la clave y el RAND para generar la señal SRES de 32 bits. La red hace lo propio utilizando los datos almacenados en el AuC y si el resultado coincide con el SRES recibido del móvil, autentica dicho móvil.

La tarificación hace referencia al costo de la llamada.

5.2.1.3 Gestión de las comunicaciones

La gestión de las comunicaciones es responsable del control de las llamadas y servicios suplementarios:

- Establecer, mantener y liberar la llamada.
- Enrutamiento de la llamada
- Mensajes cortos
- Servicios suplementarios como son el bloqueo de llamadas entrantes y salientes, llamada en espera, identificación del abonado llamante.

Diferente a lo que sucede en la red fija, en donde el terminal está permanentemente cableado a la central, un usuario GSM puede hacer Roaming nacional o internacional.

En una llamada entrante de la red fija, la MSC recibe el MSISDN marcado por el abonado e interroga al HLR para conocer el IMSI del abonado móvil y la información de ruteo. El HLR, a su vez, accede al VLR para conocer el área de

localización donde se encuentra el móvil. El VLR temporalmente asigna un MSRN (Mobile Station Roaming Number), que básicamente contiene el área de localización en donde se encuentra el móvil. Con la información MSRN, la MSC puede ahora enrutar la llamada hacia la nueva MSC. Finalmente, al móvil se hace Paging en el área de localización para averiguar en cual celda se encuentra ubicado.

6 ESTADOS DEL MÓVIL EN UNA RED GSM

El móvil puede estar en uno de estos tres estados mostrados en la figura 6.1:

- Apagado
- Libre
- Conectado

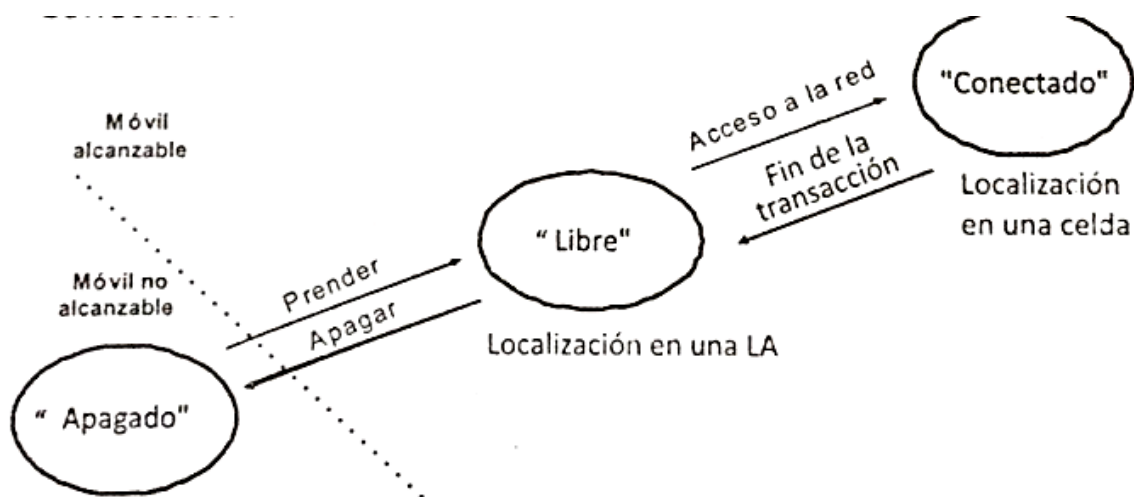


Figura 6.1. Estados del Móvil en GSM

En el estado “apagado” el móvil no puede ser alcanzado por la red. Cuando el usuario prende el móvil, el terminal inicia el procedimiento de “Attach”, que consiste en buscar en la tarjeta SIM el operador preferencial al cual debe conectarse, barrerlas frecuencias en busca de este operador y engancharse con la frecuencia Beacon que recibe con mayor potencia. Al final del procedimiento, el móvil pasa a estado “libre” y en el VLR queda “Attached”.

El móvil también lee de la tarjeta SIM el área de localización LA y la identificación temporal asignada TMSI. La secuencia de mensajes y procedimientos de la red es el siguiente.

- Solicitud de Attach por parte del móvil con los datos de TMSI, MNC, MCC y LA.
- En caso de que le TMSI no pertenezca a la MSC/VLR, esta lo busca en la MSC/VLR que estaba atendiendo a ese abonado anteriormente.
- La MSC/VLR que estaba atendiendo el abonado contesta con la identificación del mismo.

- La MSC solicita identificación al abonado, quien contesta con su IMSI.
- La MSC solicita autenticación al abonado y se valida con el AuC.
- Se solicita el IMEI al abonado y se valida con el EIR.
- La MSC/VLR informa al HLR la nueva ubicación del móvil.
- El HLR envía los datos del abonado a la MSC/VLR.
- Se le envía un nuevo TMSI al abonado y se marca como Attached en el VLR.

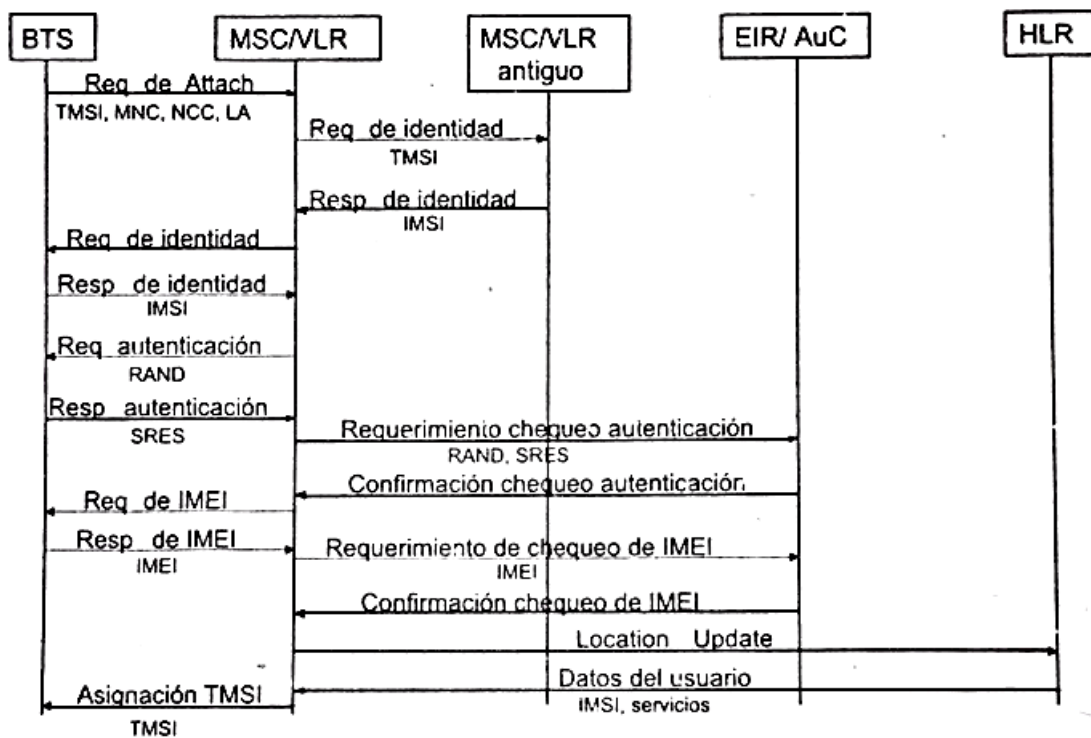


Figura 6.2. Secuencia de mensajes de Attach.

Se observa en la figura 6.2, que en la red se asigna una identificación temporal al móvil llamada TSMI, la cual se almacena en la tarjeta SIM y el VLR. Cada vez que el móvil necesita acceder a la red se identifica con el TSMI. El móvil solamente utiliza el IMSI cuando visita una nueva MSC/VLR. El uso del TMSI le da mayor seguridad al abonado, ya que no está constantemente transmitiendo su identificación IMSI.

La terminal se puede forzar para conectarse a una red particular, en tal caso no toma los datos de la tarjeta SIM, como se ha descrito arriba, sino que busca una

red indicada. Esta operación es utilizada por los ingenieros para realizar pruebas de red.

En el estado libre el móvil escucha únicamente la frecuencia Beacon, se engancha en el intervalo de tiempo 0 y olvida los otros intervalos de tiempo. Por el Beacon recibe las frecuencias de las celdas vecinas. En cualquier momento el móvil puede hacer reelección de celda si recibe la frecuencia Beacon de una celda vecina con mayor potencia que la actual. Al estar en una nueva celda, recibe una nueva lista de celdas (frecuencias) vecinas. Cabe anotar que si el terminal recibe una frecuencia Beacon con mayor potencia que la actual pero que no pertenece a la lista de celdas vecinas, simplemente la ignora.

Si el abonado cambia de celda, teniendo el móvil en estado libre, pero esta nueva celda pertenece a una nueva área de localización, el móvil empieza el proceso de actualización de área (Location Update), que consiste en actualizar la nueva área tanto en el VLR como en la tarjeta SIM. Si la nueva área pertenece a una nueva MSC/VLR, el Location Update consiste, adicionalmente a la anterior, en actualizar el HLR con una nueva ubicación de MSC/VLR del abonado.

Si el abonado apaga el móvil antes de irse a dicho estado, el móvil envía una información a la red para que actualice el VLR con el estado Dettached. Así, las nuevas llamadas son enviadas inmediatamente al correo de voz sin buscar al móvil en la red (Paging). En el evento que el abonado reciba una llamada y no este marcado como Dettached, pero tampoco este en el área de cobertura de la red o su batería este descargada, la red busca dicho abonado en la red haciendo Paging y solamente después de que un temporizador es agotado la llamada se envía hacia el correo de voz.

Al medir las nuevas celdas vecinas el móvil las identifica con el BSIC y el BCCH, ya que el LA y el CI toma demasiada información. La BSC hace la correspondencia BSIC/BCCH con LA/CI, si dos celdas usan el mismo BCCH deben tener diferente color BSIC.

Por el canal BCCH que se estudiara más adelante, la BTS envía información como LA, CA, LAI, BSIC y la lista de celdas vecinas.

Desde el estado libre el móvil puede acceder a la red para cualquier servicio (recibir o iniciar una llamada, realizar el procedimiento de ubicación del abonado, etc.). En cualquier caso, el abonado pasa al estado conectado y la red conocerá la celda en la cual se ubica el abonado.

Cuando el abonado, teniendo el móvil en estado conectado, cambia de celda, se realiza el procedimiento de Handover.

Cuando el móvil está en señalización con la BTS no escucha el Paging de una nueva llamada entrante, por lo tanto la red coloca el buzón a esta nueva llamada.

En GPRS existen tres estados como se muestra en la figura 6.3:

- Libre
- Listo
- Preparado

En el estado libre el móvil puede acceder a la red GSM, pero no está en capacidad de enviar o recibir paquetes. Aparece como no alcanzable ante la red GPRS, sin embargo la red conoce su área de localización y el móvil puede recibir llamadas al detectar un Paging.

Cuando el móvil empieza a recibir o enviar paquetes, el móvil pasa al estado listo. Si el abonado para, la comunicación pasa al estado preparado después de un cierto tiempo.

En el estado preparado se necesita el Paging. Para evitar hacer Paging en muchas celdas se definen las áreas de ruteo (RA: Routing Areas). Las Ra están formadas por un conjunto de celdas, que es a su vez un subconjunto de un área de localización.

El abonado puede permanecer conectado a la red en los estados listo o preparado sin necesidad de hacer ningún Paging para intercambiar datos. Este tiempo que permanece el abonado conectado a la red, llamada Always on, no es cobrado ya que en GPRS se cobra por número de bytes transmitidos o recibidos y no por el tiempo que permanece conectado.

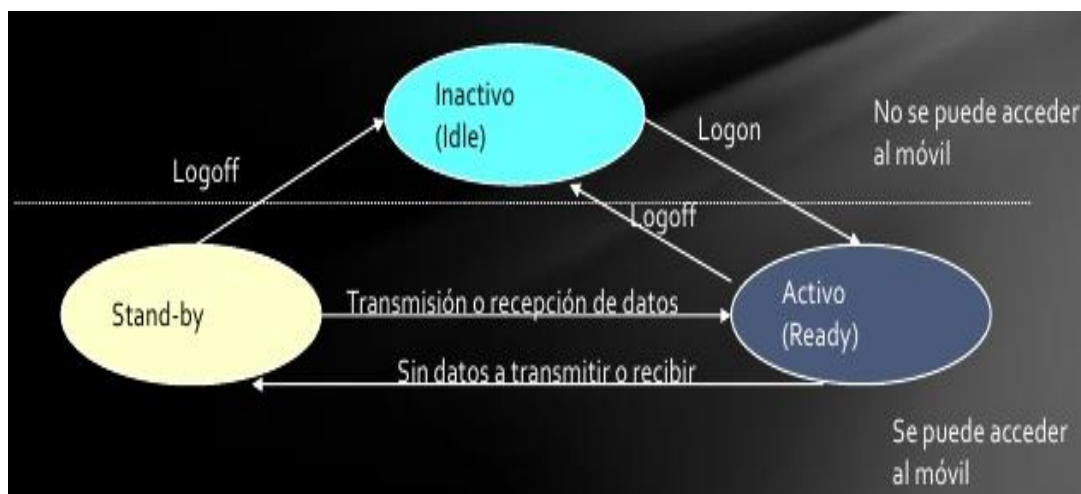


Figura 6.3. Estados del móvil en GPRS

7 LA INTERFAZ DE RADIO Y CANALIZACIÓN EN LA RED GSM

La interfaz de radio es la que permite comunicar el móvil con la BTS. Se considera la interface más importante en un sistema móvil. Para conseguir una absoluta compatibilidad entre los móviles y las redes de los diferentes proveedores y operadores, la interface de radio debe estar completamente definida.

La eficiencia espectral depende la interface de radio en aspectos tales como la capacidad del sistema y las técnicas usadas para disminuir las interferencias y mejorar el esquema del re uso de frecuencias. La especificación de la interface de radio tiene entonces una influencia importante en la eficiencia espectral.

7.1 Esquema de acceso

Debido a que el espectro de radio es un recurso limitado y compartido por los usuarios, un método de acceso a este recurso consiste en dividir el ancho de banda entre todos los usuarios posibles. El método escogido por el sistema GSM fue una combinación del FDMA y con el TDMA.

El ancho de banda asignado a GSM es dividido, usando el esquema FDMA (Frequency Division Multiplex Access), en portadoras de un ancho de banda, cada una de 200 KHz. Después, cada portadora es dividida en tiempo, usando el esquema TDMA (Time Division Multiplex Access) en 8 intervalos de tiempo o TS (Time Slots).

7.2 Plan de frecuencias

La Unión Internacional de Telecomunicaciones (ITU), que recomienda el uso del espectro de radio, colocó el sistema GSM en las siguientes frecuencias: 850, 900, 1800, y 1900 MHz.

La primera banda asignada a GSM fue de 25 MHz, la cual puede proveer hasta 125 portadoras de 200KHz, pero el primer espacio es usado como una banda de guarda entre el sistema GSM y otros servicios que trabajan en frecuencias más bajas. La segunda banda asignada fue de 75 MHz y se utilizan 299 portadoras para dejar guarda con otros servicios.

Los sistemas GPRS y EDGE utilizan el mismo método de acceso FDMA/TDMA con portadoras de 200 KHz para no interferir con el sistema GSM sino permitir su evolución. Debido a que no existen guardas entre portadoras y para evitar interferencias, no se pueden utilizar portadoras con frecuencias seguidas en la misma celda ni en celdas vecinas.

Como la comunicación es bidireccional, se utilizan dos bandas de frecuencias:

- Una banda para la comunicación de la BTS al móvil (Downlink).
- Otra banda para comunicaciones del móvil a la BTS (Uplink).

Debido a que la atenuación de la señal aumenta con la frecuencia, se asignaron las frecuencias bajas al trayecto Uplink, porque el móvil transmite con menor potencia.

Un canal de frecuencias de radio es asociado a una pareja de portadoras (Uplink y Downlink) y es identificado por un número llamado ARFCN (Absolute Radio Frequency Channel Number).

El espacio de frecuencias entre Uplink y Downlink es:

- 45 MHz para 800 y 900 MHz.
- 95 MHz para 1800 MHz.
- 80 MHz para 1900 MHz.

7.3 Canalización GSM

Como se describió anteriormente, cada frecuencia es dividida en 8 intervalos de tiempo, llamados Burst, cada uno con una duración de 577ms. Estos intervalos de tiempo son agrupados en un trama TDMA ($577\text{ms} * 8 = 4.615 \text{ ms.}$), la cual forma la unidad básica para la definición de los canales físicos. Un canal físico es un periodo Burst de la trama TDMA.

El canal está compuesto por un intervalo de tiempo Uplink y otro Downlink, corridos por tres intervalos de tiempo, para que el móvil no requiera transmitir y recibir simultáneamente y haga la electrónica más simple y el terminal más económico.

En la interface de radio, el Burst es usado para transmitir información en cada intervalo de tiempo. Diferentes tipos de Burst son usados. El más común es el mostrado en la figura 7.1. Otros tipos de Burst, llamados cortos, son usados para el monitoreo de frecuencias, la sincronización y el acceso.

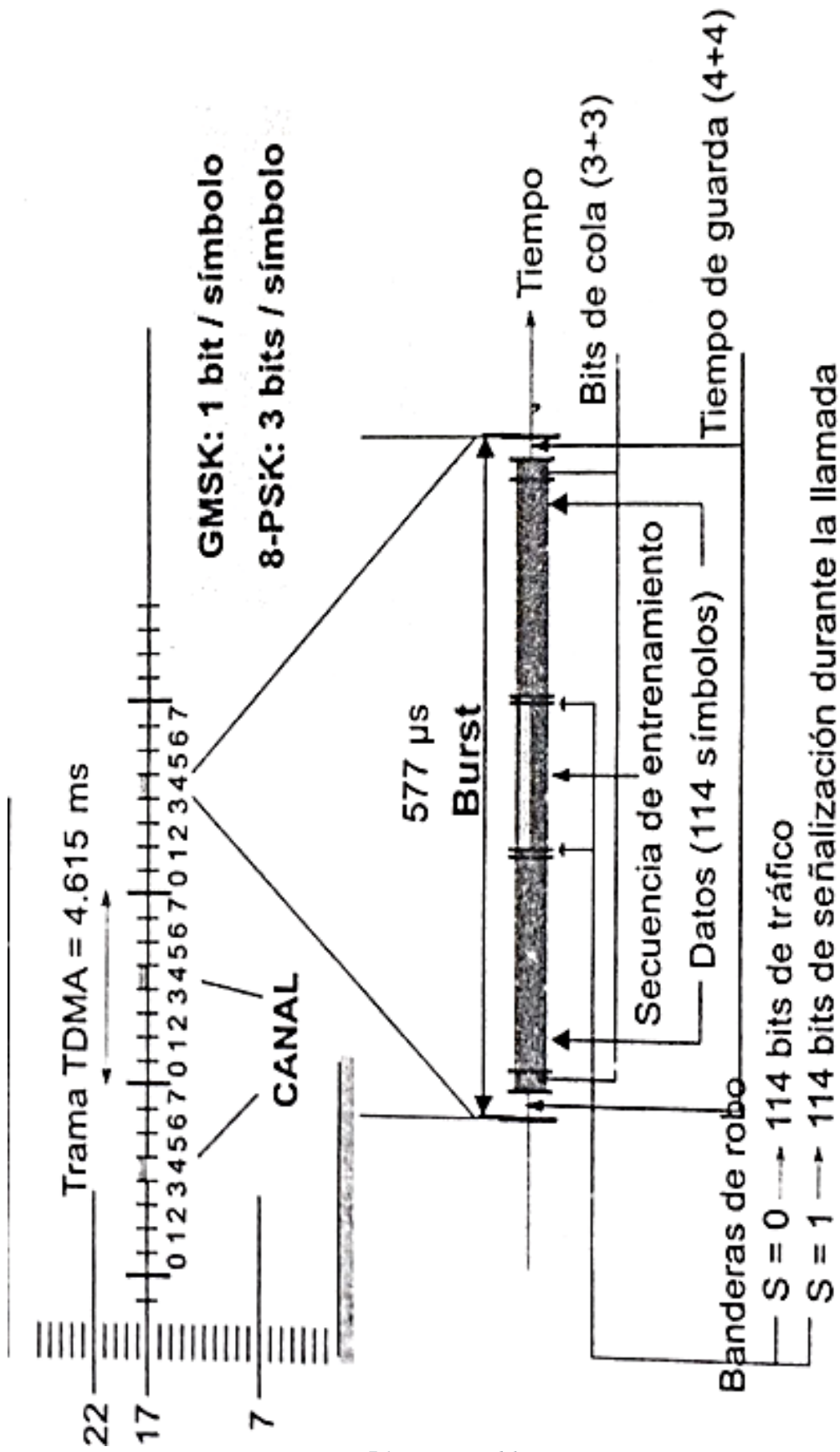


Figura 7.1. Estructura del Burst

El Burst como se observa en la figura 7.1 está compuesto por:

- Una secuencia de entrenamiento en medio del Burst de 26 símbolos.
- 2 bloques de datos de 57 símbolos cada uno, a ambos lados de la secuencia de entrenamiento. Estos datos pueden ser las muestras de voz, datos o señalización.
- 2 símbolos a ambos lados de la secuencia de entrenamiento usados para transmitir señalización en lugar de tráfico durante la llamada, solamente en el caso de modulación GMSK (banderas de robo).
- 4 símbolos adicionales de guarda a ambos lados del Burst, usados para tener en cuenta las posibles variaciones del tiempo para la transmisión de la señal entre el móvil y la BTS cuando el móvil está en movimiento.
- 3 símbolos de encabezamiento y cola a ambos extremos del Burst.

Las ondas de radio se reflejan en los edificios, carros, montañas, etcétera, haciendo que la señal sufra el fenómeno de multipropagación, que se puede ver como una ventaja que permite que la señal llegue a sitios que no tienen línea de vista con la estación base, pero que en muchos casos es una desventaja, debido a que varias señales impactan la antena receptora con diferente fase. Dentro del receptor tanto de la BTS como del móvil, un ecualizador es usado para cubrir los diferentes caminos y decodificar apropiadamente la señal final. La secuencia de entrenamiento es una secuencia de bits, conocida con anticipación, la cual es usada por este ecualizador para mejorar el proceso de demodulación/decodificación de los bits del Burst. Esto es, el receptor es entrenado con una secuencia predeterminada (secuencia de entrenamiento) para mejorar el desempeño del resto del Burst.

El Burst GSM es dividido en 156 símbolos. Un Burst GSM tiene una duración de $3/5200$ segundos ($577\mu\text{s}$). Como en la modulación GMSK un símbolo es equivalente a un bit, el Burst tiene 156 bits. La velocidad de modulación es igual a $(1535.25\text{bits}) / (577\mu\text{s}) = 270 \text{ Kb/s}$

Para EDGE con modulación 8-PSK, un símbolo corresponde a 3 bits.

Velocidad de modulación = $(468.75\text{bits}) / (577\mu\text{s}) = 811 \text{ Kb/s}$

Dos tipos de canales lógicos son definidos por su frecuencia y posición en el Burst de una trama TDMA:

- Los canales de señalización, usados para tareas de mantenimiento y gestión de red.

- Los canales de tráfico, usados para transportar información de muestras de voz o datos.

7.3.1 Canales de señalización

Los canales de señalización o control pueden ser accedidos por el móvil estando en el estado libre o conectado. Estos canales son usados por el móvil en estado libre para intercambiar señalización y pasar al estado conectado. Los móviles en estado conectado monitorean las estaciones base vecinas para realizar Handover y buscar otro tipo de información.

En los canales de control, existen tres categorías:

- BCHs (Broadcast Channels). FCCH, SCH y BCCH.
- CCCHs (Common Control Channel). PCH, AGCH y RACH.
- DCCHs (Dedicated Control Channel). SDCCH, SACCH y FACCH.

Los canales de control pueden a su vez catalogarse en orden a su sentido entre BTS y MS. En función de esta característica podemos catalogarlos como sigue:

- BTS → MS: FCCH, SCH, BCCH, PCH y AGCH.
- MS → BTS: RACH.
- Bidireccional: SDCCH, SACCH y FACCH.

Veamos a continuación la finalidad de estos canales:

- Canal de corrección de frecuencias (FCCH: Frequency Correction Channel). Es el primer canal lógico en la secuencia de control, y gracias a él el MS puede encontrar y sincronizarse con el canal SCH.
- Canal de sincronización (SCH: Synchronization Channel). El canal de sincronización contiene una secuencia de entrenamiento, la misma para todo GSM, que permite sincronización exacta, así como información de BSIC, "Time Advance" (distancia MS-BTS), y número de secuencia dentro de la hipertrama.

- Canal de control Broadcast (BCCH: Broadcast Control Channel). Contiene información útil para emitir/recibir solicitudes de llamada. Esta información es común a todos los MS servidos por una misma BTS (misma célula de cobertura).
- El canal Paging (PCH: Paging Channel). Transmite el IMSI del abonado destino de una llamada entrante a la BTS. Esta información se hace común a todas las MS de la BTS, y se le solicita al receptor la emisión del RACH. Le indica al móvil la presencia de una llamada entrante.
- El canal de requerimiento de acceso (RACH: Random Access Channel). Se forma con los slots de los canales de control en sentido MS → BTS, y será usado por el MS para originar llamadas, enviar mensajes de señalización cuando no esté en una llamada en curso, envío de ACKs a la BTS (a mensajes de Paging, por ejemplo), o registrarse en la red.
- Canal de acceso concedido (AGCH: Access Grant Channel). Contiene información sobre el canal físico en el que debe operar un MS (frecuencia y time slot asignado), así como indicaciones del canal de control dedicado asignado. El AGCH es una respuesta de la BTS ante un RACH de un MS, ya sea RACH en respuesta al PCH o como consecuencia de que el usuario quiere cursar una llamada propia.
- Canal de señalización (SDCCH: Stand alone Dedicated Control Channel). Canal fiable dedicado para el transporte de información de señalización. Garantiza que MS y BTS se mantengan comunicados mientras MSC y BTS verifican la identidad del usuario y se reservan los recursos para la llamada, también interfiere en la actualización de la ubicación del abonado. El SDCCH se concede a través del AGCH y se libera una vez establecida la llamada. Todo SDCCH tiene un canal SACCH asociado.
- Canal de control lento (SACCH: Slow Associated Control Channel), es usado en procedimientos no urgentes tales como el reporte de medidas, monitoreo de la potencia, avance de temporización (TA: Timing Advance), mensajes cortos durante la llamada.
- Canal de control rápido (FACCH: Fast Associated Control Channel). “Robará” tiempo a los canales de voz para dedicárselo a este canal cuando el SACCH no sea lo suficientemente rápido para el proceso de Handover, también sirve para enviar señalización durante el tiempo que una llamada está establecida, como terminación de la misma, llegada de una nueva llamada etc.

7.3.2 Canal de tráfico (TCH)

Un canal de tráfico es usado para llevar la voz y los datos.

Los canales de tráfico pueden llevar voz digitalizada o datos de usuario en dos modos distintos:

- Full Rate. Los datos de usuario tienen asignados una ranura de tiempo o slot en cada trama.
- Half Rate. Se transportan los datos de usuario en una ranura en tramas alternadas (dos usuarios en modo half rate pueden compartir el mismo slot, salvo que en tramas alternas). De esta forma cada trama podrá soportar el doble de llamadas.

En la siguiente tabla se agrupan los canales para GSM

Tabla 7.1. Canales en GSM

Familia	Abrev.	Sentido	Descripción
Broadcast	FCCH	BTS => MS	Corrección de frecuencia: para enganchar al oscilador a la frecuencia exacta.
	SCH	BTS => MS	Sincronización del canal
	BCCH	BTS => MS	Información de la BTS: identificación del operador, frecuencia usada, área de localización, color de la celda, celdas vecinas.
Común	RACH	BTS <= MS	Requerimiento de acceso a la red
	PCH	BTS => MS	Paging al subscriptor
	AGCH	BTS => MS	Confirmación de acceso a la red y asignación de canal SDCCH
	CBCH	BTS => MS	Mensajes cortos Broadcast

Señalización	SDCCH	BTS <=> MS	Señalización: para establecer la llamada, autenticación, encriptación, Location Update, SMS sin llamada, asignación del canal TCH
	SACCH	BTS <=> MS	Señalización: medida de potencia celda actual y vecinas, Timing Advance, SMS dentro de la llamada
	FACCH	BTS <=> MS	Señalización dentro de la llamada
Trafico	TCH	BTS <=> MS	Canal de trafico

8 POSICIONAMIENTO

A través de los años y desde el surgimiento de la telefonía móvil como hemos visto a lo largo de este documento, el posicionamiento siempre ha sido crucial para el funcionamiento de la movilidad en la red, debido a que es necesario conocer en donde se encuentra el abonado para ahí direccionar la llamada y/o los paquetes, dependiendo el caso.

Actualmente la ubicación geográfica de la terminal es de suma importancia para el funcionamiento de la mayoría de los servicios que ofrece la red y las aplicaciones que tenemos en nuestra terminal, como por ejemplo, pueden ser, encontrar rutas para llegar a determinado lugar, compartir nuestra ubicación exacta, información de tráfico vehicular, información del lugar en que nos encontramos, búsquedas personalizadas en relación con nuestra posición geográfica por ejemplo son encontrar servicios como tiendas, cajeros automáticos, restaurantes, museos, o algún otro sitio de interés que se encuentre cercano a el área en la que nos encontramos, también es posible ubicar la terminal en caso de extravío y como un servicio de seguridad para localizar a alguna persona a través del móvil (delincuentes y/o victimas), actualmente aplicaciones como WhatsApp nos permiten compartir la ubicación en tiempo real con algún contacto, lo cual ayuda para monitorear nuestra posición en caso de emergencias. Cabe mencionar que esta información es delicada, ya que se puede prestar para la ejecución de un delito, es por eso que no cualquiera puede acceder a nuestra ubicación sin nuestra autorización.

Como vemos la ubicación es un pilar importante de la telefonía móvil actual, es por ello que en este capítulo hablaremos de cómo podemos llevar a cabo esta ubicación con los servicios que la red nos proporciona y parte de la arquitectura de la misma, en este caso la base de datos que utiliza la red GSM para conocer el área de localización en la que se encuentra el abonado, me refiero al HLR y VLR.

También veremos algunos de los métodos más utilizados para dar el servicio de localización en el mercado, ya que los Servicios de localización pueden evolucionar por dos caminos, por una parte se encuentran los servicios de posición aproximada en función de la cobertura de la célula y, por otra, los servicios que utilicen información de ubicación exacta obtenida con la ayuda de los sistemas de posicionamiento global o utilizando métodos avanzados de cálculo basados en el tiempo en las redes radioeléctricas y datos de ayuda enviados por el móvil

8.1 Introducción a los métodos de posicionamiento

En este apartado se mostraran varios métodos que sirven para determinar la posición geográfica de un teléfono móvil en una red celular y los principios básicos de funcionamiento incluido un breve análisis de la precisión que se puede conseguir con cada uno de ellos. Más adelante se explicaran más a fondo los que están estandarizados por 3GPP.

Entro los más destacados se encuentran:

- Posicionamiento basado en la cobertura de la célula.
- Posicionamiento basado en el Tiempo de Ida y Vuelta (RTT).
- Posicionamiento basado en la Diferencia de Tiempos de Llegada (TDOA).
- Diferencia de Tiempos Observada Mejorada (E-OTD).
- Sistema de Posicionamiento Global (GPS).
- Posicionamiento por el Tiempo de Llegada (TOA).
- Posicionamiento por el Ángulo de Llegada (AOA).
- Posicionamiento Basado en el Nodo de Referencia (RNBP).
- Sistema de posicionamiento Galileo.

8.1.1 Posicionamiento basado en la cobertura de la célula

La posición del terminal puede calcularse averiguando en que célula radioeléctrica se encuentra o ha estado recientemente. La estación base controladora (BDC) o un centro servidor de localización de móviles (SMLC) calcula las coordenadas geográficas aproximadas de la célula indicada y envía el resultado al servidor de localización de la red.

Puesto que el tamaño o la cobertura de una célula varía en función de las características del canal y de la estrategia de planificación de la red radioeléctrica, es posible que el método basado en la cobertura de la célula por sí solo no reúna los requisitos de calidad del posicionamiento necesarios para determinados servicios basados en la ubicación. Por ello, este método se suele combinar con el método de posicionamiento RTT conocido también como método de posicionamiento por avance de tiempo o TA para determinar con mayor precisión las coordenadas del terminal.

8.1.2 Posicionamiento basado en el tiempo de ida y vuelta.

El tiempo de Ida y Vuelta (RTT) de una señal de radio también puede utilizarse para mejorar la precisión de un cálculo de posición. El cálculo de la posición de un terminal puede servirse de las medidas de RTT de las ramas de la señal de varias BS. El RTT es el tiempo de retardo de la propagación de una señal que viaja de un terminal a la BS y vuelve. Por tanto, la distancia entre el terminal y la BS puede obtenerse en función del tiempo, t , y la velocidad, c , de la onda de radio, de modo que:

$$D = \frac{RTT}{2c} + \varepsilon$$

Donde:

- D representa la distancia entre el terminal móvil y la BS.
- C es la velocidad de la onda de radio celular, que equivale a la velocidad de la luz (3×10^8 m/s) en el espacio libre
- RTT es el tiempo de ida y vuelta.
- ε es el error de la medida.

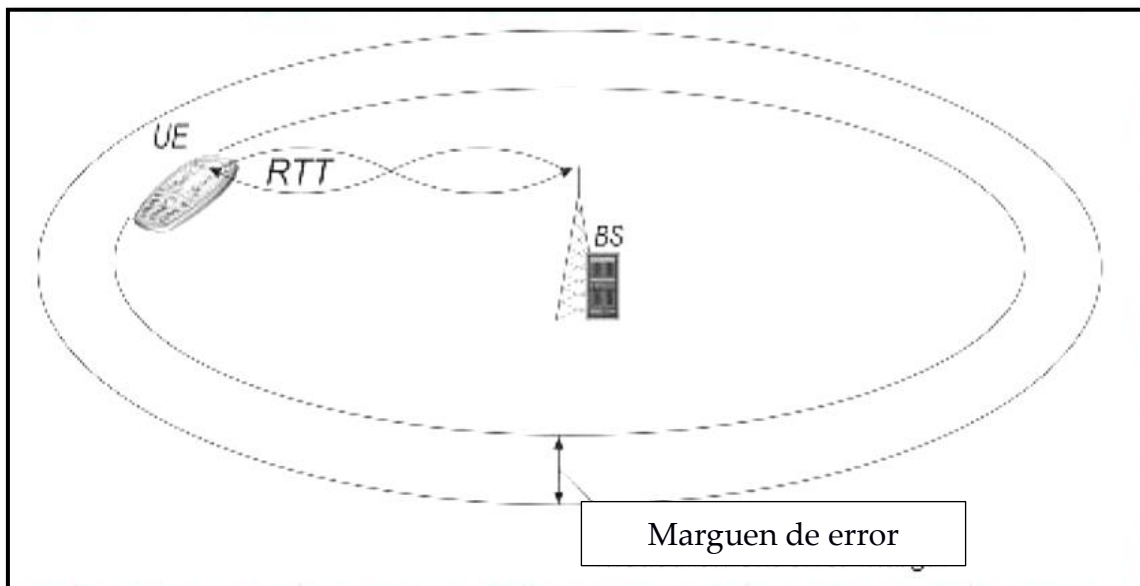


Figura 8.1. Posicionamiento Basado en el Tiempo de Ida y Vuelta.

Se debe tener en cuenta que la distancia D es en realidad el radio del círculo que rodea a la BS. Por tanto, para conseguir apreciaciones más exactas, se podría averiguar la ubicación del terminal móvil utilizando las medidas del RTT de las BS adyacentes, en la medida de lo posible. Entonces, el cálculo de la posición

estará en la intersección de los tres círculos vecinos, con la BS ubicada en el centro de estos círculos. La precisión del cálculo obtenido se determina con los márgenes de error de todas las medidas de RTT. Se ilustra en la figura 8.1.

8.1.3 Posicionamiento por la diferencia de tiempos de llegada.

El principio básico del método de posicionamiento por Diferencia de Tiempos de Llegada (TDOA) es diferente al método (TOA) que está en un apartado más adelante, En el método TDOA, el terminal observa el TDOA de las señales de radio desde las BS vecinas. La posición desconocida del terminal se calcula procesando las medidas de TDOA entre el terminal y, al menos tres BS con coordenadas conocidas. El TDOA observado por el terminal está compuesto por dos elementos:

$$TDOA = RTD + GTD$$

Donde la diferencia de tiempos geométrica (GTD) procede de la geometría (por ejemplo, las diferencias del tiempo de propagación entre el microtelefono y las dos BS). El valor de GTD es la cantidad real que contiene información sobre la posición del microtelefono, puesto que define una hipérbola entre las dos BS. Además en sistemas como el WCDMA, donde las BS no están sincronizadas, es necesario conocer la diferencia de tiempos relativa (RTD). La RTD es la diferencia de transmisión entre las señales de las BS vecinas.

La posición del terminal se calcula en función de la TDOA. Entre la BS de servicio y las BS vecinas, las cuales definen una hipérbola, cuyos focos coinciden con las coordenadas de la antena del transmisor de la BS. La posición del terminal se puede calcular utilizando el método de los mínimos cuadrados de las distancias del terminal a las hipérbolas, cuando haya más de dos valores de TDOA disponibles.

Por lo tanto la idea básica del método TDOA es determinar la posición relativa del terminal examinando la diferencia de tiempo en que la señal llega al objetivo (sea la terminal o la BS), en lugar de considerar el tiempo de llegada absoluto. Por ello, si disponemos de esta diferencia de tiempo entre las BS vecinas y hay visibilidad directa (LOS) entre el terminal y las BS, el terminal móvil está situado en la hipérbola:

$$D_1 - D_2 = c\Delta t = C * GDT = \sqrt{(x_i - x_m)^2 + (Y_i - Y_m)^2 + (Z_i - Z_m)^2}$$

Donde:

- D_1 es la distancia desde el teléfono móvil hasta las BS vecinas

- c es la velocidad de la luz.
- Δt es la TDOA de la señal desde las BS vecinas.
- x_i, y_i, z_i son las coordenadas de las BS vecinas.
- x_m, y_m, z_m son las coordenadas del terminal móvil.

Como se puede ver en la siguiente imagen, midiendo dos TDOA de tres BS diferentes, la posición del terminal se puede calcular en la intersección o intersecciones de las hipérbolas. Sin embargo, para poder obtener un único cálculo, y más preciso, es necesario tener al menos tres medidas de diferencias de tiempo de tres o más BS.

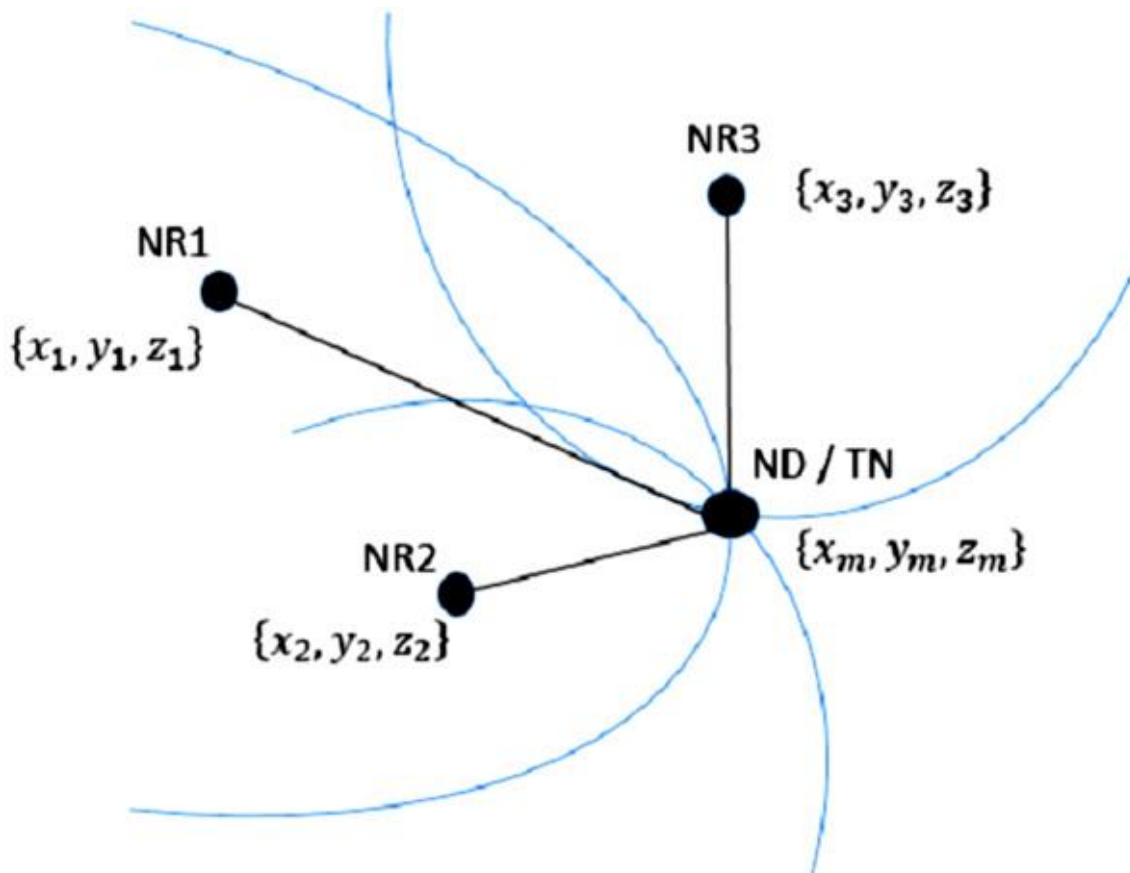


Figura 8.2. Posicionamiento por la diferencia de tiempos de llegada.

8.1.4 Diferencia de tiempos observada mejorada

El principio básico del método de Diferencia de Tiempos Observada Mejorada (E-OTD) es similar al del método TDOA, ambos calculan la posición del dispositivo móvil utilizando las diferencias de tiempo medidas entre varias BS vecinas. Podría parecer que los dos métodos son idénticos, pero en el E-OTD se realizan procedimientos de medida más precisos con la intención de mejorar la precisión del posicionamiento. El método de medida utilizado en E-OTD es el OTD mejorado. En este sentido OTD hace referencia puramente al valor del tiempo

medido, por tanto, no debe confundirse con E-OTD que es el método de posicionamiento propiamente dicho. Existe la necesidad de métodos de medida más precisos (en especial cuando la red no es sincronizada) tanto para los sistemas GSM, como para los de acceso múltiple por división de código banda ancha (WCDMA).

Las medidas de OTD se realizan en las unidades de medida de la ubicación (LMU) y en las estaciones móviles (MS). El BSC, o SMLC, determina una estimación de la ubicación comparando dos series de medidas OTD. Como la notificación de las medidas de OTD ocasiona un aumento en la señalización, las medidas de OTD de las LMU únicamente se enviaran al SMLC cada cierto intervalo. La frecuencia de estos intervalos depende, por un lado, de la disponibilidad de recursos de la BS y por otro, del nivel de precisión que requieran los servicios.

8.1.5 Posicionamiento por el tiempo de llegada

El método de posicionamiento por el Tiempo de Llegada (TOA), en el cálculo de la posición se basa en el tiempo de propagación de la señal de radio desde el dispositivo móvil hasta la BS. Cuando se dispone de un mínimo de tres medidas de TOA, la posición se puede determinar aplicando la técnica de la triangulación, reduciendo al mínimo las distancias del mínimo cuadrado entre el terminal y los círculos de TOA correspondientes. En la imagen siguiente se muestra el principio utilizado para calcular la posición del terminal. El cálculo se realiza midiendo el TOA de tres BS vecinas.

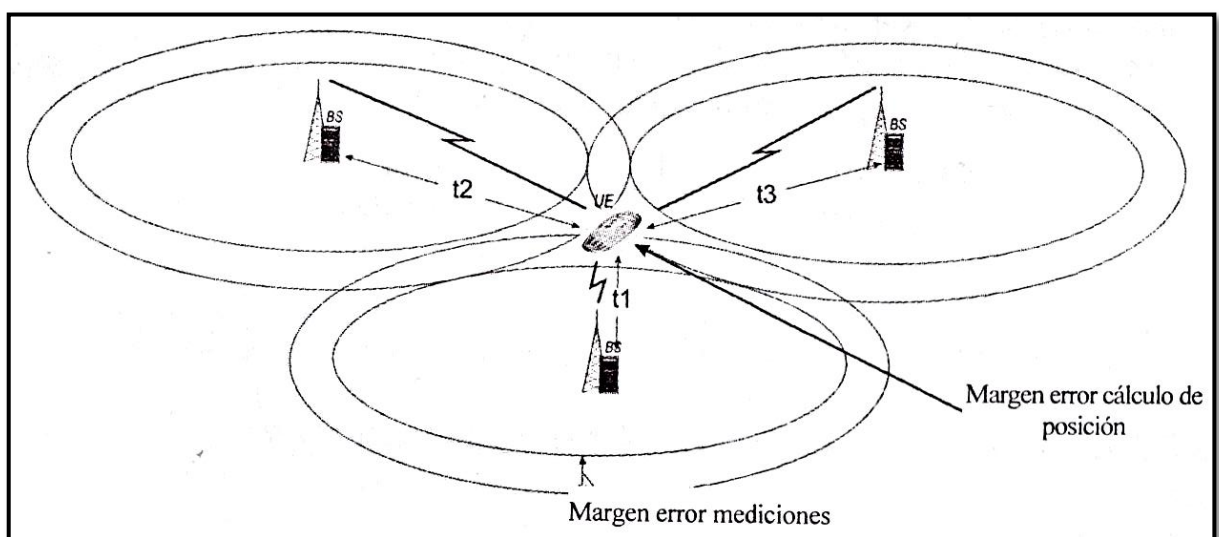


Figura 8.3. Posicionamiento por el Tiempo de Llegada

En el método TOA, la distancia desde el terminal hasta la BS es proporcional al tiempo de propagación, t_i . Por tanto, si hay visibilidad directa (LOS) entre el teléfono y la BS, la distancia que los separa vendrá dada por la siguiente fórmula:

$$D_i = ct_i$$

Donde c es la velocidad de la onda electromagnética y t_i es el tiempo que tarda la señal en viajar de la BS al terminal y viceversa. Sin embargo, en la práctica, siempre surge algún error debido a que no hay visibilidad directa (NLOS), al desvanecimiento de la señal, la reflexión y el ensombrecimiento y, en consecuencia, las variaciones de la cobertura en los límites de la célula. Por ello es necesario introducir un margen de error cuando se calcule la precisión del posicionamiento por TOA.

Como puede observarse en la figura 8.3 anterior, para poder obtener un único cálculo de la posición del terminal móvil, es necesario disponer de las medidas de TOA de al menos tres BS. Entonces, la posición de un teléfono se obtiene calculando la distancia entre el terminal y varias BS (círculos de TOA) con los mínimos cuadrados. Por tanto:

$$D_i = \sqrt{(x_i - x_m)^2 + (Y_i - Y_m)^2 + (Z_i - Z_m)^2 + \varepsilon}$$

Donde:

- x_i, y_i, z_i son las coordenadas de las BS vecinas que participan en el proceso de posicionamiento.
- x_m, y_m, z_m son las coordenadas del terminal móvil que deseamos localizar.

El método TOA requeriría una sincronización muy exacta de la BS y puede suponer algunas dificultades para los sistemas celulares que no estén sincronizados. La entidad que calcula la posición debe poder discernir también la diferencia de tiempo entre la señal transmitida y recibida. La principal cualidad de TOA es que la actualización de la red puede suponer una fuente de problemas por su amplia aceptación de la red móvil.

8.1.6 Posicionamiento por el ángulo de llegada.

La posición del terminal también se puede determinar calculando la intersección de dos líneas que representen las ramas de la señal piloto, cada una de las cuales forman un ángulo con la línea que une a la BS con el terminal móvil. Un solo ángulo forma par de líneas y facilita la posición del teléfono. Entonces, como se puede apreciar en la siguiente figura 8.4, en condiciones de visibilidad directa (LOS) entre el terminal móvil y dos BS y las medidas AOA de dos BS vecinas, se

puede determinar la ubicación del terminal móvil en la intersección de las líneas definidas por las AOA.

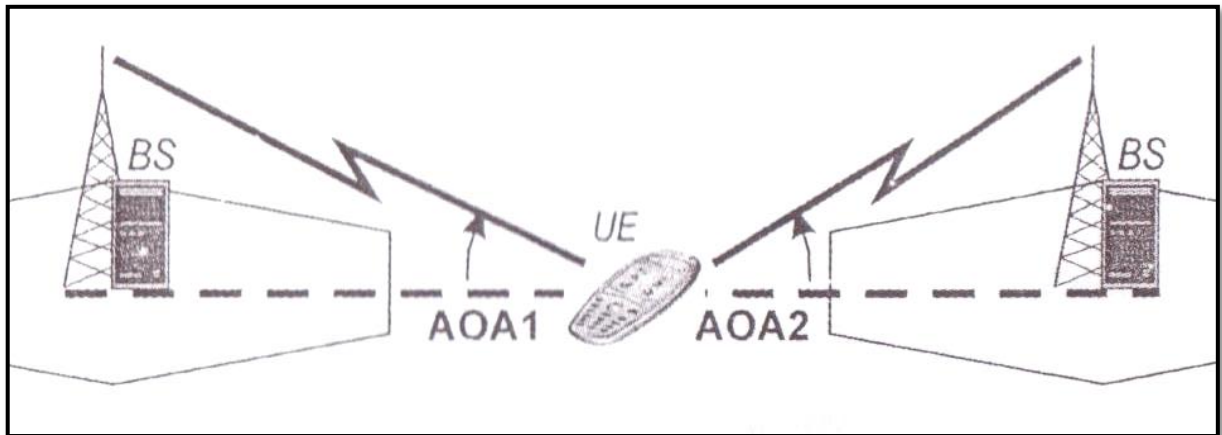


Figura 8.4. Posicionamiento por el Angulo de Llegada

Del mismo modo que ocurre con los métodos TOA y TDOA, se puede mejorar la precisión del método AOA utilizando más medidas, sin embargo, la reflexión y la difracción originan serios errores, especialmente cuando el AOA se emplea en un entorno urbano. Por lo general, el terminal móvil no puede determinar por sí mismo el AOA, de modo que debe medirse en las BS.

El AOA es propenso al desvanecimiento de la señal, por lo que cuando se combine, por ejemplo con, la reutilización de la frecuencia, será necesario considerar meticulosamente el diseño de la red y tener en cuenta que aumenta la exigencia de la planificación de la capacidad de la red. La implementación del método AOA resulta además, complicada y costosa porque requiere varias antenas de grandes proporciones en las unidades de recepción de BS. Si bien es cierto que se podría utilizar con esta finalidad las muchas antenas ya existentes.

8.1.7 Posicionamiento basado en el nodo de referencia

El método de Posicionamiento Basado en el Nodo de Referencia (RNBP), denominado en ocasiones de posicionamiento local o autoposicionamiento, se basa en la elección de un nodo de referencia para que proporcione medidas adicionales de posicionamiento del dispositivo móvil. El nodo de referencia puede ser móvil o fijo y puede tener la funcionalidad de retransmisión o repetición. Puede ser un dispositivo de servicio, un receptor de GSM o cualquier otro dispositivo con una posición conocida que pueda emplearse como punto de referencia para determinar la posición de terminales. En determinadas

circunstancias la información de la posición puede enviarse al móvil desde otro dispositivo cercano con una ubicación geográfica conocida cuando se emplea una tecnología de radio de corto alcance como Bluetooth, una LAN inalámbrica o Banda Ultra Ancha (UWB). El terminal Móvil puede entonces, calcular su propia ubicación midiendo, por ejemplo, la intensidad de la señal recibida o el tiempo de travesía desde los nodos de referencia. Como el número de dispositivos móviles con tecnología de radio de corto alcance está creciendo con rapidez, la viabilidad y precisión del método RNBP mejora notablemente. En concreto, actualmente el método RNBP, no solo se utiliza al aire libre, sino que se utiliza de forma habitual en aplicaciones de interior. Tal es el caso que si en nuestros móviles desactivamos el WIFI y solicitamos la ubicación, de inmediato nos sugiere activar la recepción de WIFI para mejorar la precisión en nuestra ubicación.

Además de tomar medidas tan básicas como la intensidad de la señal y el tiempo de travesía de la señal, el RNBP puede, combinarse con otros métodos de posicionamiento, como le TDOA, TOA o AOA, etc. El motivo más importante es que el RNBP puede mejorar el posicionamiento utilizando dispositivos adicionales de referencia en la red.

8.1.8 Sistema de posicionamiento global

El Sistema de Posicionamiento Global (GPS) se sirve de satélites, los cuales ofrecen en muchos sentidos la mejor ayuda de navegación por radio actualmente disponible. Es el gobierno de Estados Unidos el que opera este sistema y su uso es tanto militar como público.

El GPS puede combinarse con aplicaciones celulares de varios modos. El primer paso es implementar un receptor GPS en el terminal, el cual ofrece las mismas características que cualquier receptor de GPS autónomo. La precisión y la rapidez del receptor GPS puede mejorarse extraordinariamente enviando datos de ayuda GPS al terminal. Gracias a esta característica el GPS resulta muy útil en las redes celulares, porque unos cuantos receptores de referencia GPS pueden generar datos de ayuda y enviarla a los terminales móviles a través de conexiones celulares.

El principio sobre el que se basa GPS es el método TOA, pero su implementación puede resultar complicada a causa del preciso cronometraje que requiere. El satélite GPS transmite una señal de espectro ensanchado con un cronometraje muy exacto a la tierra en la banda L. En el receptor, un reloj de gran precisión mide el retardo de la señal entre los satélites y el receptor, con el resultado se calcula la distancia entre el receptor y cada satélite. Cuando un receptor observa

tres satélites su posición se puede determinar utilizando la triangulación. En la práctica, no es imprescindible que el reloj del receptor sea tan preciso si se compensa con un cuarto satélite que corrija los errores de medición del tiempo. Se puede observar como la señal de radio de un satélite GPS forma una esfera alrededor de él. Esta señal se puede dibujar basándose en el tiempo de travesía de la señal. Habiendo definido tres esferas de tres satélites, la posición del receptor será la intersección de las tres esferas, con coordenadas de longitud, latitud y altitud. En la siguiente figura 8.5, se ilustra el cálculo de la posición con un GPS.

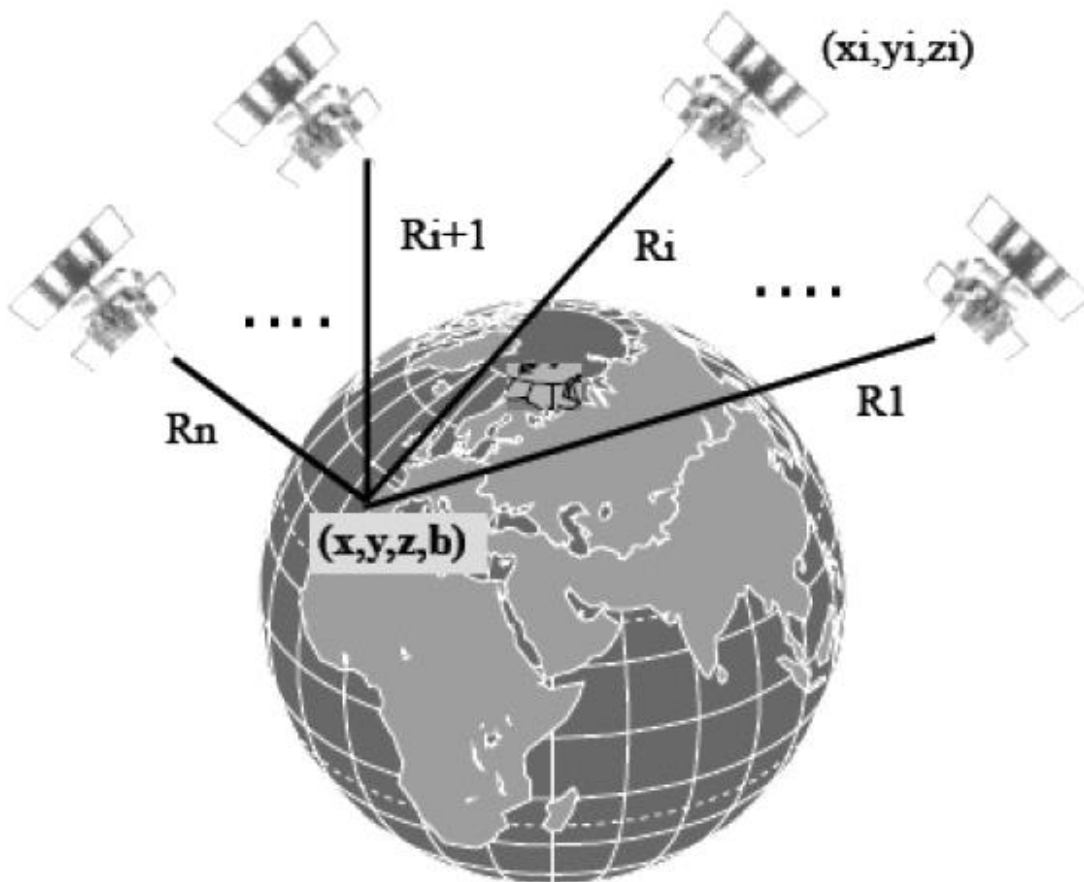


Figura 8.5. Sistema de Posicionamiento Global

El método GPS es uno de los sistemas de posicionamiento más precisos que existen actualmente. No obstante, los receptores GPS necesitan tener visibilidad directa a cuatro satélites y no siempre es posible, como en las aplicaciones de interior. Además, el receptor GPS tiene una antena de satélite exclusiva que puede crear interferencia con el uso del sistema celular. El receptor GPS aumenta los costes de fabricación y el consumo de energía en el móvil. Para superar o al menos, aliviar estos problemas, se ha estandarizado el posicionamiento por GPS y los datos de ayuda de GPS para los sistemas GPS, UMTS y posteriores.

8.1.9 Sistema de navegación por satélite Galileo

El proyecto galileo es una iniciativa conjunta de la UE y de la Agencia Espacial Europea (ESA) que comprenderá de una constelación de 30 satélites en órbita a una altitud de cerca de 24 000 kilómetros y que está operativa a partir del año 2016 con aproximadamente media constelación y se espera que para 2020 tenga su constelación completa como se ve en la figura 8.6.

El proyecto galileo ya está mandando información de navegación a usuarios de todo el mundo y es completamente público a diferencia del GPS que lo controla como vimos la milicia de Estados Unidos.

El principio de operación del Galileo es similar al del GPS. Es decir, se coloca en los satélites un reloj de alta precisión atómico y se indica una señal que transmite la hora exacta. El terminal móvil recibe las señales desde vario satélites y mide el tiempo que ha tardado en llegar la señal. Con los resultados de las mediciones y la hora indicada, el móvil puede calcular su propia posición en función de las distancias hasta los satélites.



Figura 8.6. Sistema de Navegación por Satélite Galileo

8.2 Precisión del posicionamiento

Como hemos descrito anteriormente, los principios básicos de todo método de posicionamiento, con la excepción del método basado en la información de la célula, se sustentan sobre las características de propagación de la señal de radio, las cuales no son fáciles de predecir, la precisión de los métodos de posicionamiento celular depende del entorno, la calidad de la conexión por radio (por ejemplo, la proximidad a la visibilidad directa), las medidas de la señal, las características del receptor y el método de cálculo aplicado.

La precisión en el método basado en el ID de la célula depende principalmente de la estructura y del tamaño de la célula. En una estructura de red con macrocélulas, la precisión de la posición varía entre unos kilómetros y unas cuantas decenas de kilómetros. En una pico o micro célula, el grado de precisión varía entre decenas y centenas de metros.

La precisión del método TOA depende del desvanecimiento de la señal, del ensombrecimiento y del número de medidas de las ramas de la señal disponibles para diferentes BS. Es esencial tener visibilidad directa de varias BS para obtener una estimación precisa de la posición del terminal móvil. Desafortunadamente, este requisito contradice los principios normales de planificación de la red celular, del modo que no será posible lograr una precisión óptima en todos los puntos de la red celular.

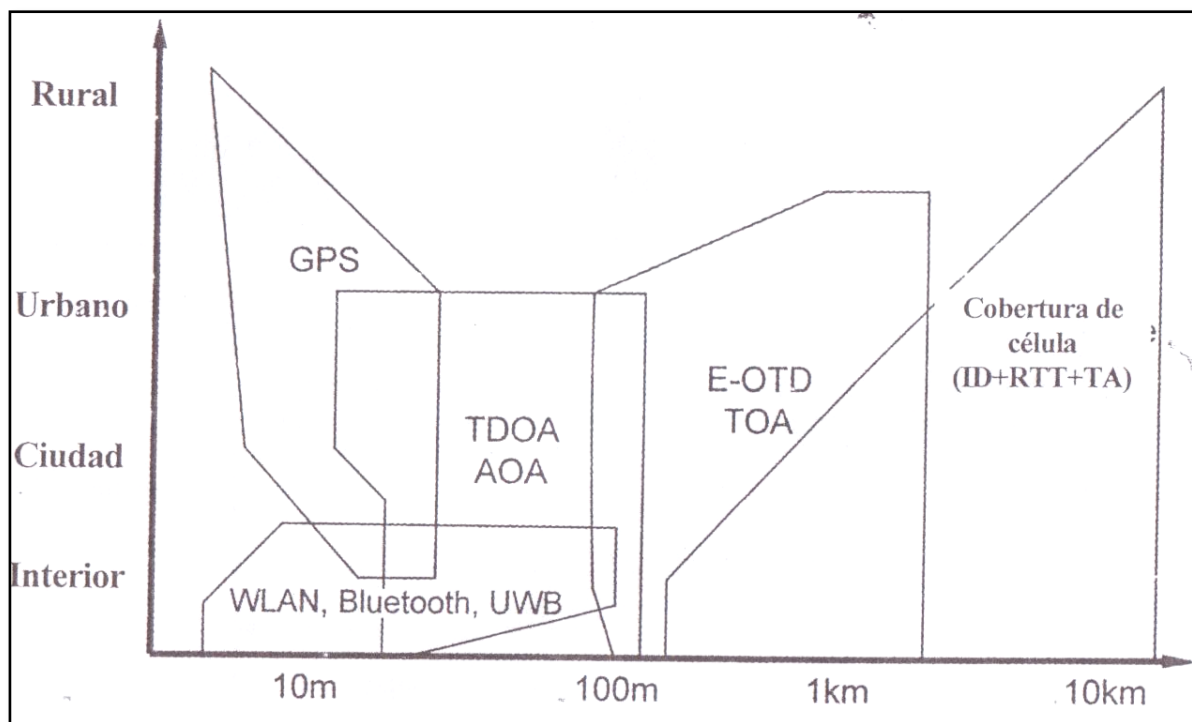


Figura 8.7. Comparación de la precisión que ofrecen los diferentes sistemas de posicionamiento

Como ocurre en el método TOA, la precisión del método TDOA está sujeta a las características inherentes de la señal de radio en el entorno de la red celular y el número de mediciones disponibles, especialmente en los casos en los que no hay visibilidad directa (NLOS). Sin embargo, cuando se emplea un método TDOA, se dan algunos errores comunes en todas las BS y se cancelan entre sí en el proceso de posicionamiento por que únicamente se miden las diferencias de tiempo. Por tanto, los métodos basados en TDOA suelen ofrecer mejores resultados que los basados en TOA en condiciones similares.

Con todo no existe un valor absoluto razonable para generalizar la precisión de los diferentes métodos de posicionamiento. Aunque, el grado de precisión se puede esbozar a grandes rasgos, como se muestra en la figura 8.7. El uso de los métodos más precisos va acompañado de un aumento en los costes, de modo que es más rentable seleccionar un método que ofrezca solo la precisión necesaria para un determinado propósito. Cada tipo de LCS impone unos requisitos de precisión, por este motivo en una red puede utilizarse varios métodos.

8.3 Métodos de posicionamiento especificados para GSM y UMTS

Todos los métodos de posicionamiento que se describieron anteriormente se estudiaron en el 3GPP pensando en la estandarización. El resultado fue la selección de tres métodos para las redes UTRAN:

- El posicionamiento basado en el ID de célula: el ID de la célula corresponde al ID del Area de Servicio (SAI) en las redes UMTS
- El posicionamiento por la diferencia de tiempos de llegada observados (OTDOA) que, como su nombre lo sugiere, se basa en el método TDOA anteriormente mencionado.
- Posicionamiento GPS asistido.

Para las redes GERAN (GSM EDGE Radio Access Network).

- El posicionamiento basado en el ID de célula.
- El posicionamiento por diferencia de Tiempos Observada Mejorada (E-OTD).
- Posicionamiento por GPS asistido.

Estos métodos pueden, en principio, estar basados en la red, en un móvil, basados en la red y asistidos por móvil o basados en móvil y asistidos por la red.

La diferencia entre estas variantes radica en donde se realiza el cálculo, en la red o en el terminal. Otras variantes se definen en función de donde se generan los datos de ayuda y reciben los nombres de asistido por la red o asistido por el móvil, respectivamente. En los siguientes subtemas se repasan un poco más a fondo los métodos de posicionamiento especificados para GSM y también redes de tercera generación como UMTS que heredaron características de su predecesor GSM.

8.3.1 Posicionamiento basado en el ID de la Célula

En el método basado en el ID de célula se asocia el ID de célula al SAI correspondiente. Es posible que se necesiten operaciones adicionales si el móvil se encuentra en estado de traspaso con continuidad o en estado de control de recursos radioeléctricos, donde la célula no está definida.

En estado de traspaso con continuidad, el móvil puede tener diferentes ramas de señales conectadas a diferentes células y, por tanto, estar enviando diferentes ID de célula. En estos casos, el cálculo de posición basado en la cobertura de célula puede mejorarse combinando toda la información disponible.

Por lo general, la selección del ID se basa en los parámetros que definen la calidad de las ramas de señal recibidas. Es decir se selecciona el ID de célula que tenga la rama de señal más intensa como referencia para determinar la posición del móvil. Otra opción es seleccionar como célula el primer ID de célula generado durante el establecimiento de la conexión. Además de estos mecanismos se han especificado otros criterios para determinar el ID de célula durante el traspaso.

El método basado en el ID de la célula debe soportar el posicionamiento del móvil independientemente del estado de la conexión de los recursos de radio.

No es posible obtener el ID de célula si el móvil no se encuentra activo, es decir, si no existe una conexión entre el móvil y al menos una célula. Por ejemplo, se puede facilitar el ID de la célula cuando hay establecida una conexión de recursos de radio entre el móvil y al menos una BS. Por lo tanto, si el móvil está en modo reposo, se fuerza al móvil a entrar en un estado en el que pueda facilitar el identificador de célula. Por ejemplo, en el estado de canal de Paging, es probable que el ID de célula no esté disponible, de modo que fuerza al móvil a entrar en un estado de canal en el que si se tenga el id de célula para poder determinar cuál es. La red también puede evitar que el móvil entre en estado de actualización para recibir las actualizaciones del ID de célula cuando el móvil selecciona una nueva célula. Si el móvil se encuentra en reposo, necesitara recibir un mensaje de Paging para definir su posición.

8.3.2 Diferencia de tiempos de llegada observados- periodo inactivo en enlace descendente en UMTS

El segundo método de posicionamiento es el Diferencia de Tiempos de Llegada Observados- Periodo inactivo en Enlace Descendente (OTDOA-IPLDL), el cual consta de dos partes. En primer lugar, la parte de OTDOA, que es en teoría similar al método TDOA descrito anteriormente, aunque en este concepto se destaca que el móvil mide las diferencias de tiempo observadas entre las BS vecinas para determinar su posición.

Medir la OTDOA no resulta tan evidente en por las siguientes razones:

- En algunos casos es posible que no haya suficientes señales piloto disponibles para que el móvil tome medidas. Esto puede ocurrir cuando el móvil se encuentre tan cerca de la BS de servicio que su receptor se bloquee por la intensidad de las transmisiones de la BS. Este fenómeno se conoce como el efecto de audibilidad.
- Las BS no suelen estar sincronizadas en WCDMA-FDD, de modo que es necesario conocer o medir la diferencia de sincronización entre las BS (la RTD) antes de realizar el cálculo de la posición del terminal.

Con el objetivo de solventar estos problemas, se han estudiado dos posibles soluciones, primero en los organismos de estandarización japoneses y posteriormente en el 3GPP, para dotar a las redes de la capacidad de posicionamiento del móvil.

La primera solución sería aumentar temporalmente la potencia de transmisión de las BS vecinas hasta el punto que el móvil pueda medirlas. El problema es que el WCDMA-FDD, igual que en todas las tecnologías de radio basadas en CDMA, tiene un sistema de limitación de interferencias que imposibilita la estrategia de aumentar la potencia, ya que aumentaría sustancialmente los niveles de interferencia en la red.

La segunda solución sería hacer que la BS en servicio interrumpiera la transmisión durante breves periodos de tiempo y reducir así el problema de audibilidad. Este método se denomina periodo inactivo en enlace descendente (IPDL). Durante un periodo de inactividad de la BS en servicio, el móvil puede medir las señales de la BS vecinas, además durante estos periodos las mediciones de la RTD son más precisas. Las unidades de medida utilizadas para este fin pueden situarse en las BS, o en lugares próximos, cuando se utilice el IPDL.

El empleo del IPDL presenta algunos inconvenientes porque, por lo general, deben conseguirse las mejores condiciones para la conexión y los periodos regulares de inactividad en la transmisión de la BS pueden causar molestias. Otra dificultad en WCDMA es que las células apenas se solapan, por lo que es probable que los móviles no alcancen a recibir y medir un número suficiente de células adyacentes, ni siquiera cuando se utilice la estrategia de IPDL.

8.3.3 GPS Asistido

El 3GPP ha estandarizado los métodos de GPS asistido para su uso en ambos sistemas, SM y UMTS. Existen dos tipos de GPS asistido, el basado en el móvil y el asistido por el móvil. La diferencia radica en donde se realiza realmente el cálculo de la posición. No debemos olvidar que el móvil también puede recibir de la red datos de ayuda de GPS en el caso del método GPS asistido por el móvil.

En la solución de GPS asistido basado en el móvil, el terminal cuenta con un receptor GSM completo y el cálculo de la posición se realiza desde el móvil. Los datos de ayuda de GPS que envía la red al móvil incluyen:

- Datos de ayuda para mediciones, como son la referencia de GPS, la lista de satélites visibles, la señal Doppler de satélite y la ventana de búsqueda de fase de código. Estos datos tienen un periodo de validez de entre dos y 4 horas
- Datos de ayuda para el cálculo de posición, como la hora y la posición de referencia, las efemérides de los satélites y las correcciones del reloj. El periodo de validez de estos datos es de 4 horas.

Cuando se utiliza el sistema de GPS diferencial, también se envían datos de corrección diferencial. Este tipo de datos de ayuda son válidos durante 30 segundos, pero son relevantes para un área bastante extensa. Por tanto, se pueden generar datos de asistencia utilizando un receptor de referencia ubicado en un punto central.

En la solución de GPS basada en la red y asistida por el móvil, el terminal cuenta con un receptor GPS reducido con el que realiza medidas de pseudodistancia y transmite los resultados de las medidas a una unidad de cálculo de la red, desde donde se lleva a cabo el resto de la operación GPS. En esta solución, la red solo envía una cantidad limitada de datos de ayuda al móvil, pero este tiene que enviar todos los resultados de las mediciones en dirección ascendente. También es necesario que la hora de referencia sea más exacta en el modo asistido por el móvil que en el basado en el.

8.4 Arquitectura del sistema para los servicios de localización.

La funcionalidad de los servicios de Localización (LCS) en las redes UMTS se distribuye entre los elementos de red existentes prácticamente del mismo modo que el sistema GSM. Si bien se ha introducido por primera vez en la arquitectura global un importante elemento de red, el Centro de Localización de Móviles de Pasarela (GMLC), para los LCS, tanto en GSM como en UMTS.

En la figura 8.7 se ilustra la arquitectura global de los LCS en UMTS que es la misma para GSM. El equipo y la funcionalidad de los servicios de localización se utilizan en la CN y en la UTRAN. Las entidades UTRAN realizan y recopilan mediciones sobre el posicionamiento y determinan la ubicación del equipo móvil utilizando los métodos anteriormente comentados. En el CN, el GMLC actúa como punto de conexión a través del cual se envían los datos de posicionamiento a otras funcionalidades de servicio o aplicaciones al cliente.

La arquitectura del sistema de localización de UMTS es muy similar a la empleada en GSM como se aprecia en la figura 8.8, pero se han omitido algunas soluciones de red opcionales con la intención de reducir la complejidad. Las redes ULTRAN traen consigo ventajas y desventajas para las aplicaciones de posicionamiento celular si se compara con el de GSM.

En las especificaciones que realizó el 3GPP, se toma un punto de vista más formal de la funcionalidad de los LCS en diferentes elementos de la red y las interfaces correspondientes. En la figura 8.9 se muestra el modelo de referencia de los LCS que definió el 3GPP para GERAN. Las interfaces y las entidades de la red de la figura aparecen definidas en las correspondientes especificaciones de LCS del 3GPP y el LIF-MLP (Interfaz Lógica – Protocolo de Localización de redes Móviles) se especifica en la Alianza Móvil Abierta (OMA). No obstante, la interfaz entre el solicitante mostrado en la Figura y el cliente LCS no ha sido estandarizada. El solicitante es el que origina la solicitud de localización y puede ser otro terminal o un servidor de aplicaciones basadas en ubicación. A menudo, es el propio usuario del terminal objeto de la localización el que realiza la solicitud.

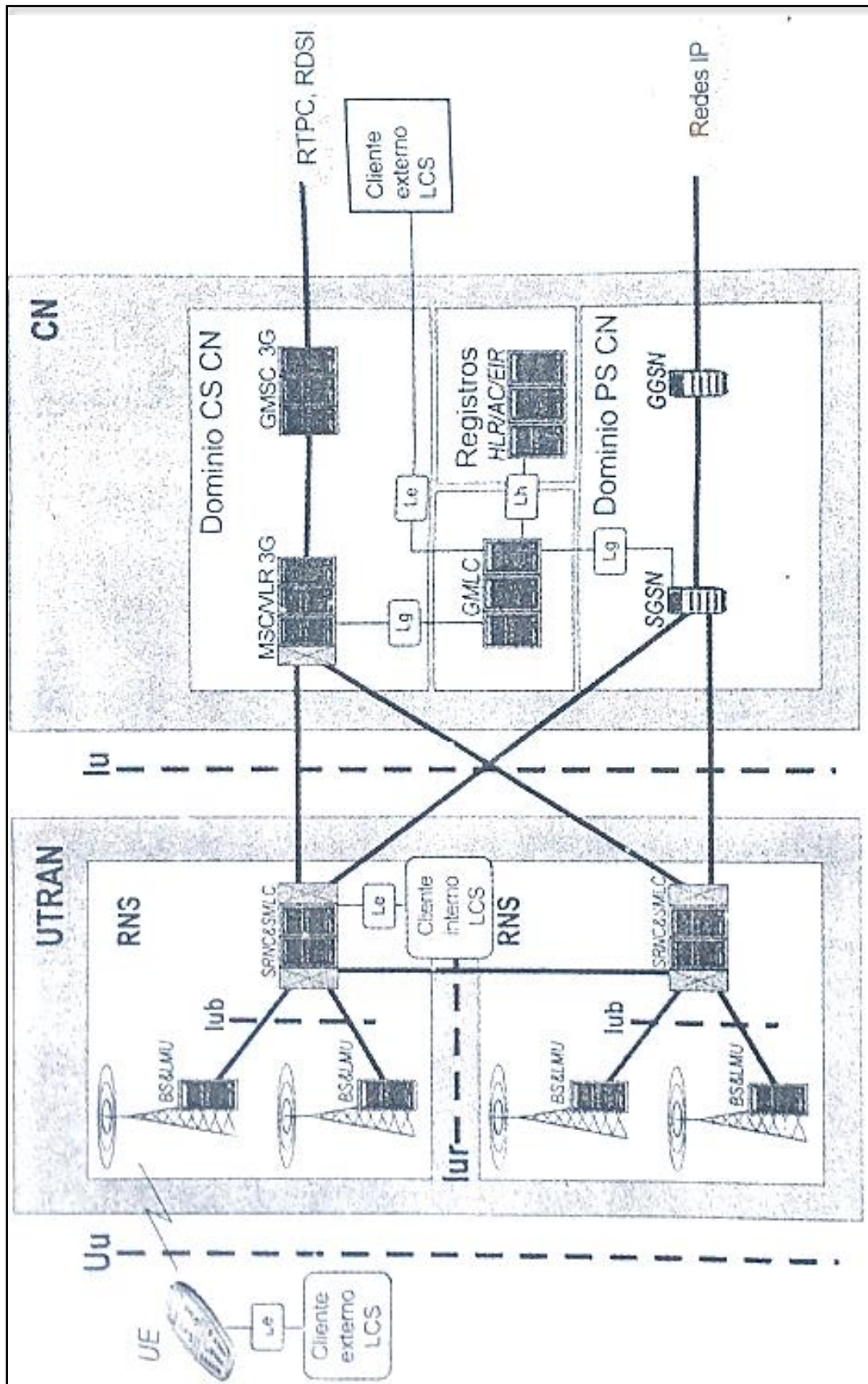


Figura 8.8. Arquitectura general de los Servicios de Localización (LCS) en redes UMTS

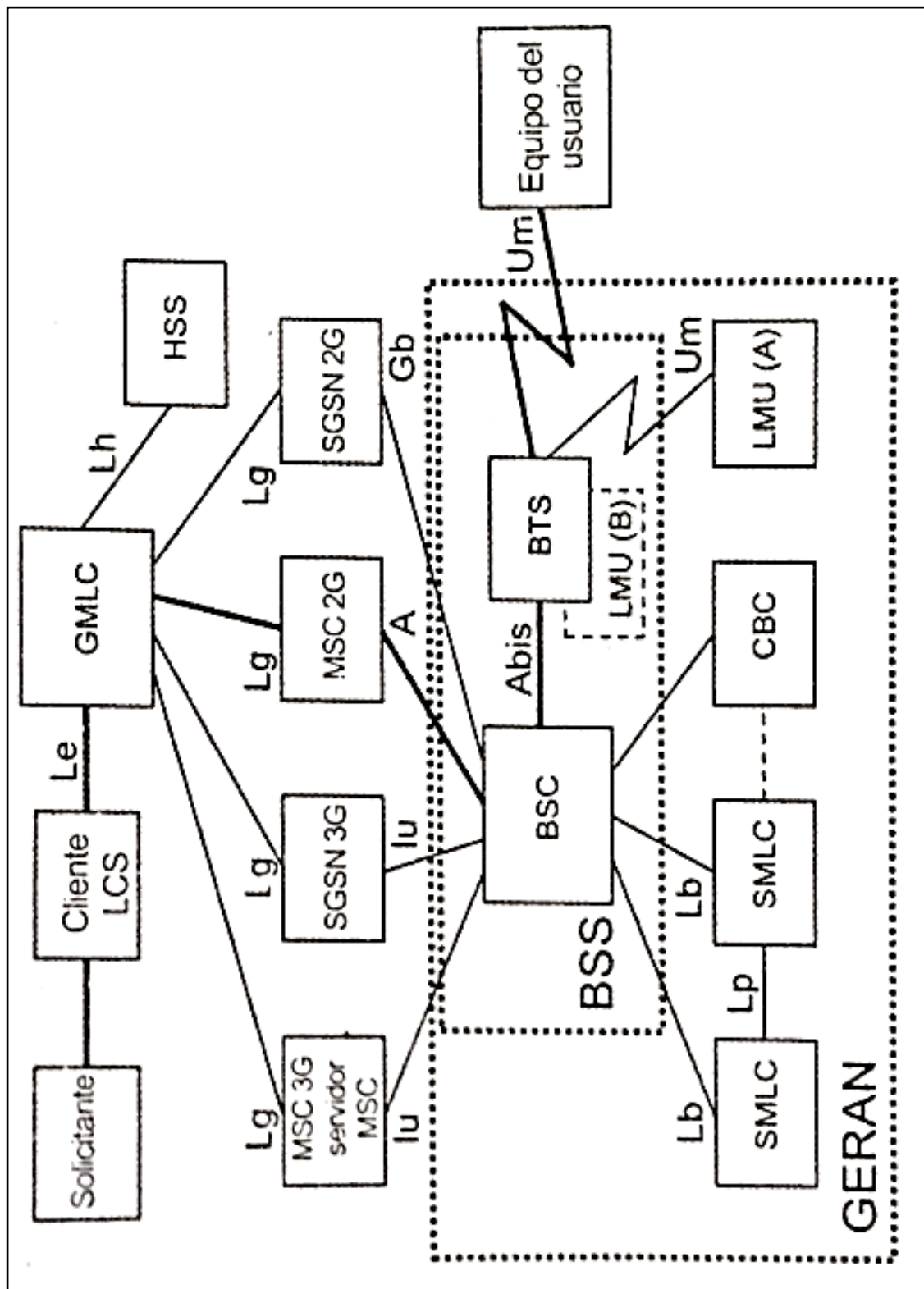


Figura 8.9. Modelo de referencia de los Servicios de Localización en GERAN

8.5 Funciones del LCS en la red central.

La funcionalidad de LCS en la CN corresponde al MSC/VLR, al servidor MSC, al GMLC y al registro de posición base/ registro de abonados residentes (HLR/HSS). El MSC/VLR puede iniciar un mensaje de Paging para los servicios LCS, además de encargarse de la autenticación del móvil, de las solicitudes de posición relacionadas o no con llamadas y de la tarificación.

El usuario puede decidir si se revela o no la posición de su terminal a otros clientes LCS y en caso afirmativo, controlar de qué manera se revela. Estas decisiones se definen en las clases de privacidad incluidas en el perfil de suscripción que se guarda en el HLR. El usuario puede entonces decidir si acepta o rechaza la solicitud del cliente a los terminales habilitados para gestionar y mostrar este tipo de solicitudes. El terminal notifica a la red si está habilitado para ello utilizando las marcas de clase del móvil. El móvil envía la marca de clase 2 es decir a la de CN al MSC indicando si está habilitado para la verificación de privacidad. El móvil también envía la marca de clase 3 al BSC y al MSC indicando los métodos LCS para los que está habilitado.

La entidad MSC se ocupa de la tarificación y la facturación de todo lo relacionado con los servicios de localización. Esto incluye la tarificación y la facturación de clientes y abonados, incluyendo los abonados de la red base y los abonados itinerantes de otras redes móviles terrestres públicas. El MSC también autoriza que se proporcionen servicios de posicionamiento para un móvil concreto, del mismo modo autorizan otros servicios celulares.

El HLR guarda los datos de Suscripción y los perfiles de privacidad para los abonados que utilicen LCS, así como la información sobre el VLR, en el que el móvil se encuentre registrado en ese momento dado. El GMLC solicita información de encaminamiento (es decir en que VLR está registrado el móvil) al HLR a través de la interfaz Lh utilizando la señalización parte de aplicación móvil (MAP).

El GMLC actúa como una pasarela entre los clientes externos de LCS y la red móvil y envía la solicitud de posicionamiento del cliente hasta el MSC/VLR, en función de las indicaciones del HLR. El GMLC autentica al cliente LCS con ayuda del HLR (es decir el GMLC verifica que el cliente LCS tiene permiso para recibir información sobre la posición de un abonado en concreto). El GMLC determina si la estimación de la posición que ha recibido la red satisface los requisitos de QoS o calidad de servicio (Quality of Service) que exige el cliente LCS. Además, el GMLC también controla el flujo de solicitudes de posicionamiento entre solicitudes simultáneas o periódicas y puede convertir la información recibida de la red en coordenadas locales. El 3GPP ha especificado el modo en que el GMLC

debe gestionar las complejas combinaciones de servicios de las llamadas solicitudes de localización diferidas y periódicas. Supongamos que el cliente LCS ha solicitado que se le informe de la activación de un determinado teléfono móvil y que, al mismo tiempo, haya una solicitud de localización periódica pendiente para el mismo abonado.

9 POSICIONAMIENTO CON HLR

Como ya vimos, dado que los aspectos como movilidad y el geo posicionamiento están muy de moda, hablaremos de la viabilidad de la localización usando exclusivamente el HLR, y en su caso, de cómo se podría llevar a cabo con la información de estas bases de datos y los recursos que tiene la red móvil.

La red de telefonía móvil en todo momento y por la arquitectura que tiene, conoce nuestra ubicación, por cuestiones de operatividad de la misma, aunque no de manera exacta, sabe a qué estación célula debe direccionar una llamada o mensaje.

Las antenas de telefonía están configuradas en celdas o células, donde cada célula corresponde al área de servicio, o cobertura de la señal que brinda una radio base.

En cada momento la terminal móvil está negociando el servicio con varias BS, como ya lo vimos en el proceso de señalización, y es la red la que automáticamente escoge que BS es la que le brindara el servicio al teléfono móvil, esto de acuerdo con varios factores como son, los climáticos, y la geografía propia del lugar.

Ya vimos algunos de los métodos más usados para dar con la ubicación de un móvil e incluso los estandarizados por 3GPP, basados en los sistemas propios de la red, y en cada uno de ellos se parte, conociendo la BS o célula de la que está recibiendo el servicio la terminal móvil, y si, para partir de este punto es necesaria la información encontrada en las bases de datos de la red y de la empresa que brinda el servicio. Es por esto que veremos si de alguna forma es posible localizar el terminal exclusivamente con la información de estas bases de datos.

En el apartado de los estados del móvil en una red GSM, vimos como en cuanto un equipo está apagado, la red desconoce el área de localización en la cual se encuentra y por tanto la estación base más cercana, en cuanto el usuario enciende el móvil, ubica el operador de servicio en la SIM, barre las frecuencias buscando en cuál de ellas opera este proveedor, y cuál de estas señales es la más fuerte y en la que se va a enganchar.

En caso de que el móvil haya cambiado de ubicación mientras estaba apagado, y el TMSI no pertenezca a la MSC/VLR actual, esta busca en la MSC/VLR que estaba atendiendo a este abonado anteriormente, se solicita la información del abonado, en este caso su IMSI, se autentica y se valida con el AuC, posteriormente se solicita el IMEI al terminal y se valida con el EIR, con todos estos datos actualizados y validados el MSC/VLR informa al HLR de la nueva ubicación del móvil.

Cabe mencionar que la información no incluye la identificación de la estación base a la que está conectado el móvil, si no el área de localización, que son, el conjunto de estaciones base que están bajo el control de esa MSC/VLR, es hasta cuando la red tiene una solicitud de llamada para el terminal, cuando realiza el Paging que es el proceso iniciado por la red para encontrar la ubicación del terminal y saber así, que estación base es la que le está brindando el servicio.

Dentro de los sistemas de localización mencionados anteriormente, se encuentra el sistema de localización basado en el ID de célula. Este, desde sus características estudiadas, es el que nos permitiría ubicar el móvil con el uso casi exclusivo de la información contenida en el HLR.

Es el método más sencillo y económico, ya que no requiere ningún complemento en la infraestructura de la red, pero igual es el más impreciso.

Su precisión está asociada, al tamaño de la célula, la que puede variar de cerca de 500m a más de 10 Km de rayo, dependiendo del ambiente cubierto (rural, suburbano y urbano).

Algunas mejoras pueden ser obtenidas con la implementación de algunas técnicas, representadas en la figura 9.1.

La introducción de la sectorización de las celdas, usualmente con 120°, delimita el área (el sector) en donde el terminal móvil (usuario) puede ser encontrado.

El GSM posee el método de " Timing Advance ", a través del cual es medido el tiempo de recorrido de un señal entre la BTS/terminal móvil/BTS (Base Transmisión Station). Ese parámetro, originalmente utilizado para sincronización durante el envío de "Bursts" de datos, puede ser utilizado para calcularse la distancia aproximada que un terminal móvil se encuentra de la BTS.

De esa forma, se gana más un nivel de precisión en la localización al reducirse el área (la faja) en donde el terminal puede ser encontrado.

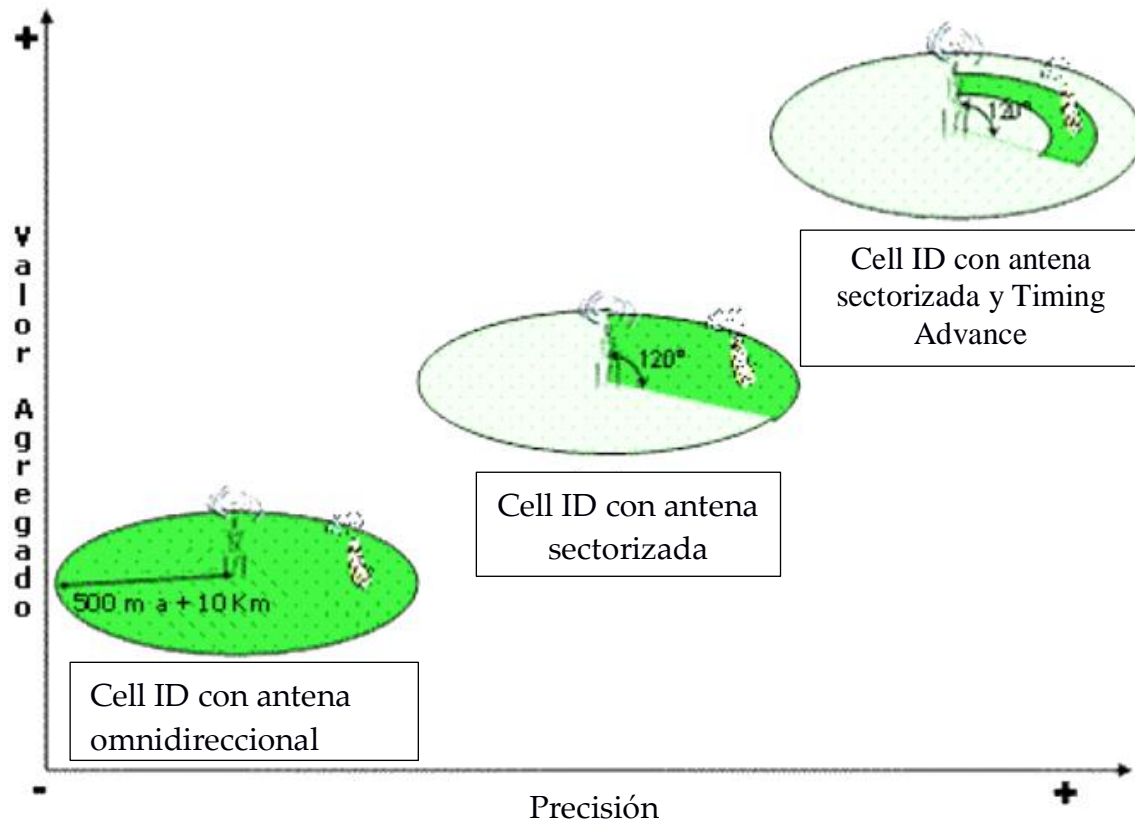


Figura 9.1. Precisión con la técnica Cell ID

Otro recurso que puede ser desarrollado es el E-CGI (Enhanced - Cell Global Identity). En todos los sistemas móviles los terminales celulares realizan mediciones en la interface aérea, que visan el control automático de potencia y, a través del intercambio de esa información con la red, permiten que la red decida sobre la realización de "Handover".

Para mejor entender este recurso, hay que considerar como ocurre la propagación de las señales de radio. Con ese objetivo, es presentado un diagrama de radiación genérico de una antena utilizada en sistemas móviles. Se nota la existencia de un lóbulo principal y de lóbulos secundarios.

Considerándose ahora, el diagrama de radiación estilizado en la figura 9.2, podemos inferir que para una dada potencia de señal (recepción) medida en el teléfono móvil celular, puede ser asociado una ganancia de la antena, que indica el ángulo del móvil en relación al eje central de la antena. De esa forma, a la información anterior de distancia de la BTS (obtenida con el time advance), se suma, entonces el ángulo, lo que restringe la probabilidad de localización del móvil.

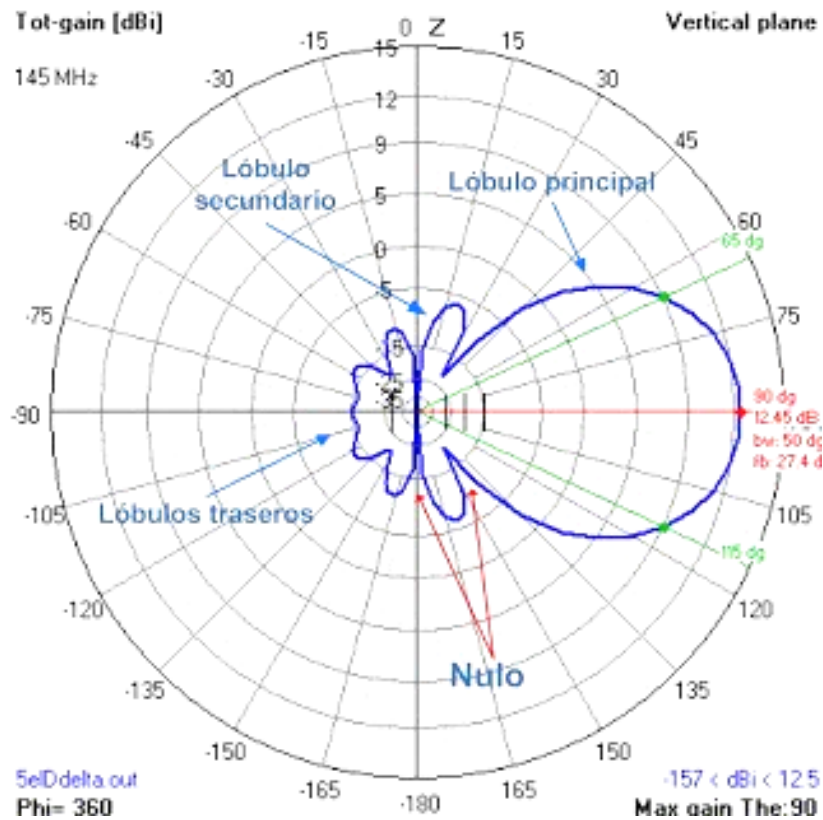


Figura 9.2. Diagrama de radiación.

Como el ángulo proporcionado en un diagrama de radiación o Carta de Smith es aproximadamente simétrico, se puede verificar, con el auxilio de la figura 9.3, que en la realidad el aparato móvil puede estar en dos puntos distintos y simétricos (Y_1 / Y_2) en relación al eje central, excepto cuando el móvil se encuentra en el propio lóbulo principal (Z - ángulo 0°).

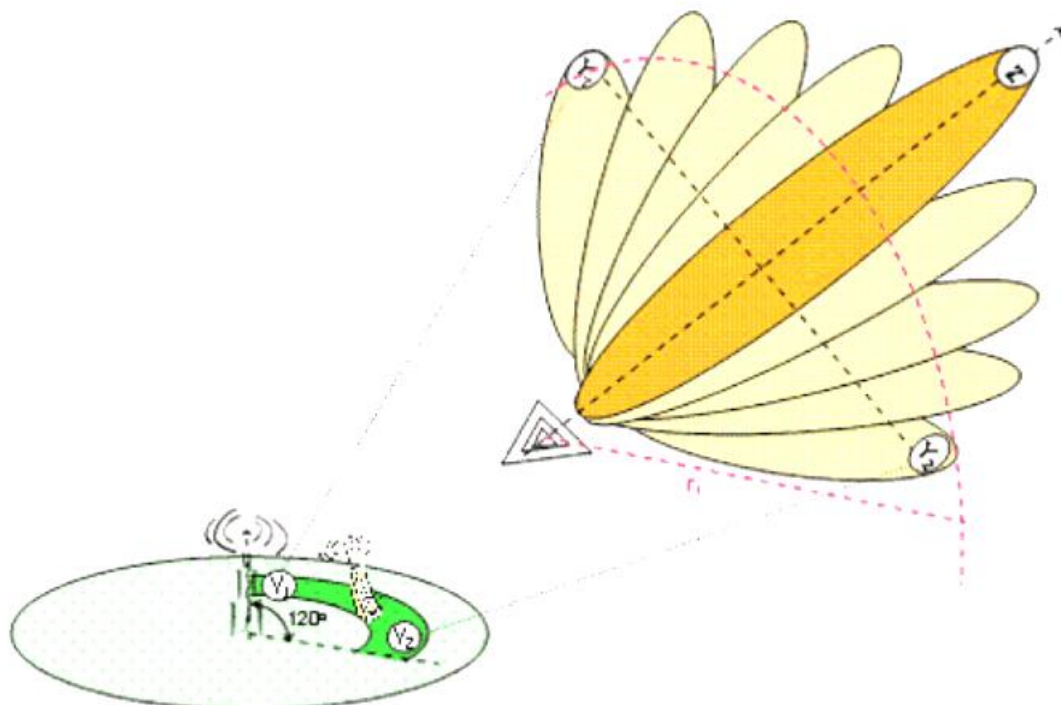


Figura 9.3. Cell ID con antena sectorizada, Time Advance y E - CGI

La única forma de solucionarse el problema de duplicidad de información expuesto arriba, sería que las mediciones fuesen realizadas por más de una BTS, para que, a través de la intersección de las informaciones, se llegase a un único punto.

De manera general, se puede afirmar que todas las soluciones basadas en ID de Célula son extremadamente dependientes de la densidad de las celdas, configuración de la red y ambiente.

Este método como vemos es, usando únicamente lo que la red nos ofrece (Time Advance y control de potencia) y que ya vimos en apartados anteriores, sin ningún complemento, únicamente con algunas técnicas, que por las propiedades de las ondas de radio, podemos implementar para mejorar la aproximación de un teléfono celular.

Existe otro método de localización de un usuario a través del HLR, en la cual se puede hacer una consulta a la red, que te dice en qué país se encuentra un móvil, así como la operadora que brinda el servicio a ese terminal. Eso quiere decir que a nivel de país, cualquier persona puede conocer la ubicación del teléfono, este servicio tiene un costo y es brindado por compañías que piden, esta información a las operadoras, y son un servicio para publicidad principalmente a través de mensajes de texto.

Así vemos, que aunque es posible obtener la ubicación de un abonado con la información que encontramos únicamente en la red de telefonía móvil, en sus bases de datos, HLR y VLR, esta no es precisa y varea dependiendo del tipo de célula en la que nos encontremos y la región así como se geografía.

Toda esta información de ubicación, independientemente del método empleado para obtenerla, está sujeta a los permisos que el usuario del teléfono otorgue a las diferentes aplicaciones que la utilicen, y estas a su vez tienen programas de privacidad de la información, para que no cualquiera tenga acceso a estos datos.

A menos de que sea hackeada la base de datos HLR, permanecerá privada para todo público y solo las Fuerzas de Seguridad tendrán acceso a ella mediante una orden judicial.

10 EVOLUCIÓN DE LOS SERVICIOS DE LOCALIZACIÓN EN LAS NUEVAS TECNOLOGÍAS

La mayoría de los conceptos vistos en los apartados anteriores de las redes GSM son aplicables a las redes de tercera y cuarta generación. Son consideradas como la evolución de GSM y veremos si en estas tecnologías sigue presente el HLR y VLR dentro de las arquitecturas de redes de tercera y cuarta generación.

10.1 HLR y VLR en la arquitectura de las redes UMTS o de tercera generación.

La arquitectura de red UMTS se conforma de dos partes como se muestra en la figura 10.1:

- Red de acceso (ULTRAN: UMTS Terrestrial Radio Access Network).
- Red central (CN: Core Network).

La red de acceso está compuesta por:

- Estaciones base (Node B).
- Estación controladora (RNC: Radio Network Controller).
- El equipo de usuario (UE: User Equipment), compuesto por la terminal móvil y la tarjeta USIM (UMTS Service Identity Module o Universal Subscriber Module).

La red Central está compuesta por:

- La central de conmutación MSC/VLR, o el servidor de llamadas (Call Server). Vemos que aquí aparece el MSC/VLR de igual forma que en las redes GSM.
- La base de datos de usuario HLR/AuC.
- El nodo de servicios SGSN.
- El nodo de Soporte de datos GGSN.

Vemos que dentro de la arquitectura de las redes de tercera generación, siguen apareciendo los sistemas de HLR y VLR, los cuales siguen monitoreando la

ubicación y la información del suscriptor para estas redes. Básicamente la misma función que en las redes GSM.

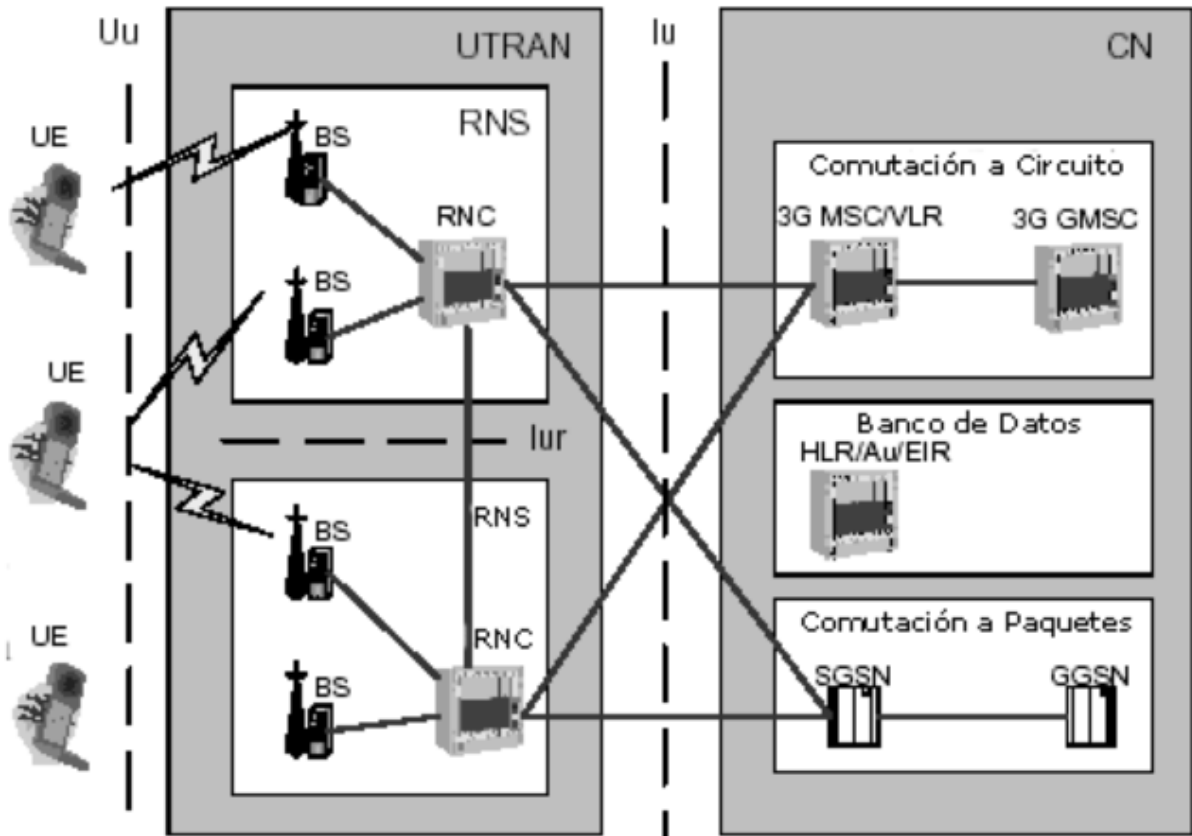


Figura 10.1. Arquitectura de una red UMTS

10.2 HLR y VLR en la arquitectura de las redes LTE o de cuarta generación.

La red LTE se divide en dos, como se muestra en la figura 10.2:

- El corazón de la red, que se conoce como EPC (Enhanced Packet Core).
- La red de acceso, llamada E-UTRAN (Evolved UMTS Terrestrial Radio Access Network).

Se observa una simplificación de ambas redes, tanto del acceso como en el Core. Desaparece la controladora de estaciones base, que se tenía en redes 2G y 3G.

La red E-UTRAN está constituida básicamente por estaciones base, llamadas nodos B evolucionados eNB, que atienden las terminales de usuarios. El eNB se comunica con el S-GW por el plano de usuario y con el MME por el plano de control. El eNB termina el plano de control y de usuario del terminal. Los eNB se comunican entre ellos, razón por la cual los datos de usuario no necesitan subir hasta el Core como lo hacían en redes 2G/3G. Algunas de las principales

funciones de los eNB son, la comunicación con las terminales, el manejo de los recursos de radio, medidas y reportes de la movilidad del terminal.

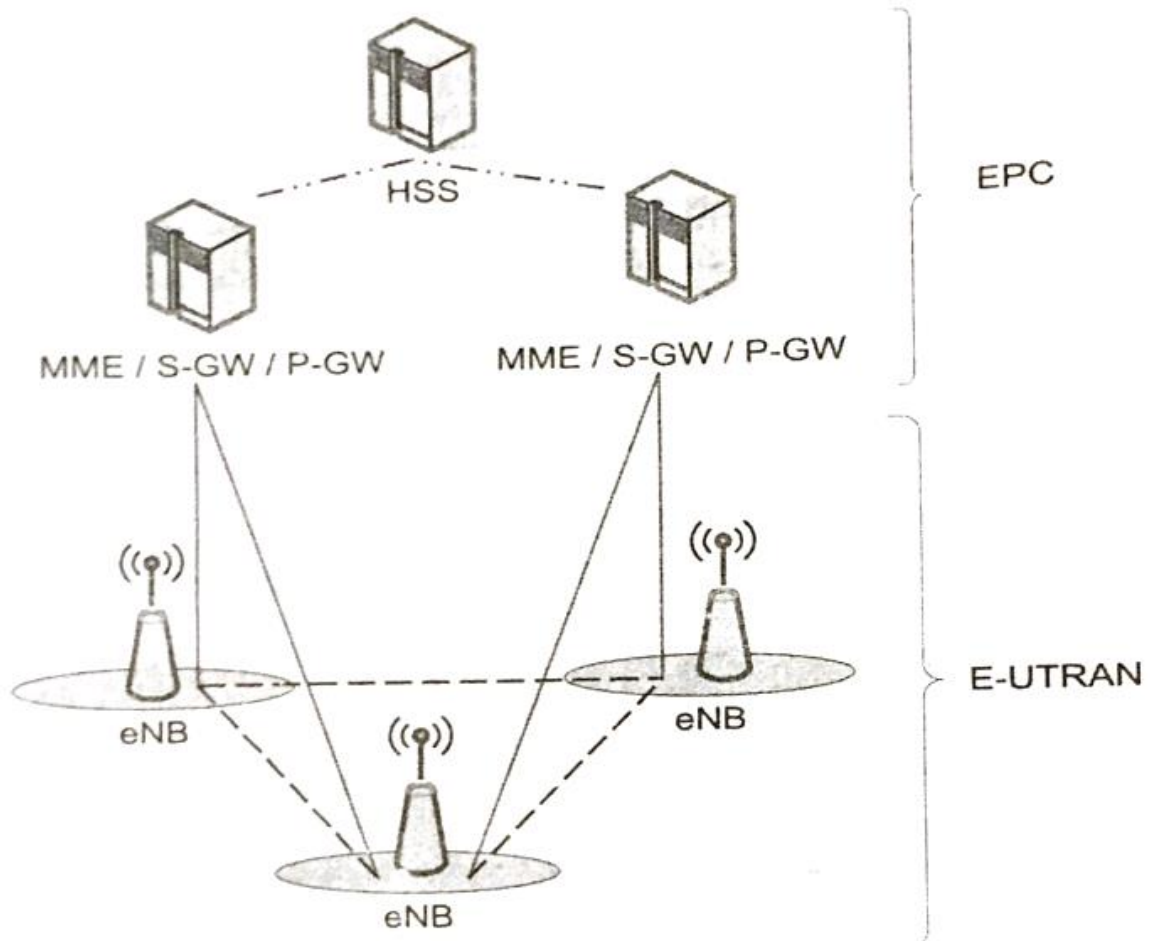


Figura 10.2. Arquitectura de la red LTE

El MME (Mobility Management Entity) es el nodo de control para la red de acceso. Tiene las siguientes funciones:

- Maneja el control de señalización para la movilidad.
- Es el responsable de seguir al terminal cuando está en modo Idle que es el modo en que un terminal está conectado a la red pero no tiene tráfico de datos.
- Hace Paging al terminal para llamada entrante.
- Hace autenticación de usuario consultando el HSS.
- Provee funciones del plano de control, cuando se necesita hacer un paso de una red LTE a una red 2G/3G.

El S-GW (Serving Gateway) enruta los paquetes de datos del usuario. Durante el Handover ayuda a la movilidad del usuario. Es el responsable del Handover para dar la movilidad hacia otras tecnologías. Es el Gateway con otras redes.

P-GW (Packet Data Network Gateway) suministra conectividad al terminal con redes externas de paquetes de datos, siendo el punto de entrada y salida del tráfico del terminal.

El HSS (Home Subscriber Service) fue introducido y contiene la información del Usuario (HLR y AuC).

Como vemos en la red de cuarta generación, desaparece lo que es el MSC/VLR y en su lugar aparece el MME, S-GW y el P-GW, donde se realizan las funciones que realizaba el MSC/VLR además de que se tiene que tener un Gateway, para la conectividad con redes de generaciones anteriores, y el tráfico de datos con redes que no son las móviles.

El HLR y AuC son los que se mantienen, pero como vimos en la descripción anterior, ya solo se utilizan para obtener la información del abonado, no tanto para su gestión de movilidad.

10.3 Gestión de movilidad en LTE

Una de las piezas clave para la telefonía móvil es la gestión de movilidad. Es un requisito básico que deben satisfacer estos sistemas es permitir que los usuarios puedan acceder y recibir sus servicios desde cualquier ubicación geográfica donde el sistema cuente con cobertura, dejando a un lado posibles limitaciones operativas o restricciones derivadas de las propias condiciones del uso del servicio.

Por un lado, este requisito implica que el sistema de comunicaciones móviles tiene que albergar mecanismos que le permitan avisar a los usuarios de la activación de servicios originados desde la red dondequiera que se encuentren. Dada la gran extensión geográfica que llega a abarcar la red celular, el envío de avisos como Paging a los terminales debe hacerse de forma selectiva por así decirlo, a través únicamente de aquellas estaciones base donde exista una cierta probabilidad de encontrar al usuario. Por esto, el sistema debe hacer un seguimiento del terminal móvil que le permita acotar la ubicación de usuarios dentro de la zona de servicio de la red. A esta funcionalidad le llaman gestión de localización.

Por otro lado, cuando los usuarios se encuentran conectados al sistema a través de una determinada estación base, se requiere que el sistema sea capaz de

mantener las conexiones activas aun cuando el móvil se encuentre desplazándose y resulte necesario realizar en el transcurso de una conexión activa un cambio BS que le proporcione el acceso a la red, es decir el Handover, del que ya hemos hablado en las tecnologías anteriores.

De esta forma, la gestión de movilidad en un sistema de comunicaciones móviles abarca tanto la gestión de la localización como la del Handover.

En los siguientes subtemas veremos el marco de gestión de movilidad considerado en los sistemas LTE.

10.3.1 Marco de gestión de movilidad

En el sistema LTE se especifica un modelo de movilidad denominado modelo EMM (EPS Mobility Management) con dos posibles estados que representan dos situaciones de accesibilidad en las que puede encontrarse un usuario del sistema. Los dos estados de EMM son:

- Estado No Registrado (EMM-Deregistered). En este estado el usuario no se encuentra visible en el sistema LTE, y por tanto, no tiene acceso a los servicios del sistema. LTE no dispone de ninguna información relativa la localización del abonado.
- Estado Registrado (EMM-Registered). En este caso el sistema está operativo en el sistema LTE y por tanto, tiene acceso a sus servicios en el móvil. La red LTE dispone de información de localización del móvil con la resolución de al menos, una lista de áreas de seguimiento.

Junto con los estados de movilidad el sistema LTE también define un modelo de estados para indicar la existencia o no de un plano de control activo entre el UE, y el nodo MME de la red, donde se encuentra registrado. Dicho modelo de estados se denomina modelo ECM (EPS Connection Management) y se estructura también en dos posibles estados.

- Estado Desconectado (ECM-Idle). En este estado el UE no tiene establecida una conexión de señalización con ninguna entidad MME. La existencia de este estado es básicamente por la necesidad de disponer de un modo de operación de bajo consumo que permita conseguir un modelo de funcionamiento always on, con la posibilidad de conmutar rápidamente entre este estado y el estado conectado en el que el terminal podrá recibir y envía datos.

- Estado Conectado (ECM-Connected). En este estado el UE tiene establecida una conexión de señalización con una entidad MME de la red troncal. El envío y recepción de datos de señalización o usuario, siempre se realizan en este estado.

10.3.2 Gestión de localización.

Tal como se ha hablado en apartados anteriores acerca de la importancia de conocer en un determinado nivel la ubicación de lo UE que se encuentren registrados (EMM-Registered) pero que no tengan establecida una conexión con ninguna estación base (estado ECM-Idle).

Por esto, LTE se define el concepto Área de Seguimiento (TA, Tracking Area) para gestionar la información de localización. Un TA agrupa un conjunto de eNBs de forma que la información de localización disponible en la red troncal EPC de un determinado UE solamente se conecte en base a la resolución proporcionada por tales agrupaciones. La identidad de un TA se denomina TAI (tracking Area Identifier) y se difunde a través de los mensajes de información de sistemas enviados en los canales de Broadcast de los eNBs que integran un TA. Un eNB solo puede pertenecer a una TA de una red troncal EPC, es decir, no puede haber solapes entre las Tas. El UE a partir del identificador TAI recibido, es el encargado de comunicar a la red en que TA se encuentra accesible mediante los mecanismos de Network Attach y de Area Update, de esta forma cuando la red necesita contactar con el móvil, el mensaje de aviso Paging se difunde a través de todas las estaciones base que integran el TA en que se encuentra localizado el terminal.

La gestión de localización mediante Áreas de seguimiento es un planteamiento que ya vimos que se utiliza en UMTS y GSM. En dichas redes, la localización de terminales registrados en el dominio de circuitos se realiza mediante el concepto de área de localización LA y mediante la definición de áreas de rutado RA en el dominio de paquetes, igual que las TA de LTE no presentan solapes. Sin embargo la modificación importante que introduce LTE es la posibilidad de que un terminal se encuentre registrado en múltiples TAs a la vez, entendiéndose en una lista de TAs. Esta modificación es debido a la necesidad de disponer de mecanismos que ayuden a minimizar la señalización debida a las actualizaciones de localización en las zonas limítrofes entre las TAs. En estas zonas, algunos patrones de movilidad de UEs pueden originar un número de TAs elevado si el móvil va conmutando sucesivamente entre eNBs de diferentes TAs. Por ello mediante el registro de múltiples TAs en móvil únicamente actualiza su localización en el caso de que se mueva fuera de la cobertura del grupo de TAs que integra la lista. Nótese que mediante una gestión apropiada de TAs por UE, la red LTE puede confeccionar de forma dinámica áreas de localización

personalizadas, dicho de alguna manera, que conduzcan a una reducción de la señalización asociada con los procedimientos de TAU y Paging.

Es importante señalar que la gestión de movilidad en LTE ha sufrido importantes simplificaciones respecto a la movilidad que gestiona UMTS donde la red de acceso UTRAN también participa en la gestión de la localización mediante la definición de áreas de rutado propias y de un conjunto de estados asociados a la gestión de movilidad en la capa RRC (FACH, PCH, etc.) En cambio en el sistema LTE, la gestión de localización sustenta íntegramente en la red troncal EPC.

11 APLICACIÓN DE LA LOCALIZACIÓN DE EQUIPOS MÓVILES CON LA RED MÓVIL.

En los últimos años el crecimiento de la telefonía móvil ha ido aumentando de manera increíble e inesperada, tanto en lo que se refiere a la red propia de telefonía móvil, como a los equipos de telefonía celular, los cuales han venido a desplazar a muchos otros productos, ya que a estos se les ha ido incorporando muchas funciones en un mismo producto, como son las cámaras fotográficas y de video, reproductores de música y video, radio, GPS, PCs, chips NFC para realizar pagos entre muchas otras. Y para muchos de estos casos el acceso a internet que permiten estos dispositivos y la red móvil, ha jugado un papel muy importante para el día a día del usuario.

El número de usuarios únicos de telefonía móvil alcanzó los 5.000 millones al finalizar 2017, lo que supone un grado de penetración del 66%, aunque el número de tarjetas SIM usadas por personas (excluyendo las que usan máquinas entre sí) se elevó a 7.800 millones, el 103% de los habitantes del planeta, superando así por primera vez la población mundial (7.600 millones de personas). Son datos del informe anual Mobile Economy de la GSMA, la asociación que organiza el Mobile World Congress (MWC) que se celebra en Barcelona.

El estudio prevé que se añadirán casi mil millones de usuarios de telefonía móvil en 2025, alcanzando los 5.900 millones de suscriptores, lo que equivale al 71% de la población mundial prevista para ese momento. El crecimiento de los suscriptores durante este período estará impulsado por los países en desarrollo, particularmente Bangladesh, China, India, Indonesia y Pakistán, así como por los mercados de África Subsahariana y América Latina. Además, para 2025, se espera que 5.000 millones de suscriptores utilicen sus teléfonos móviles para acceder a Internet, frente a los 3.300 millones en 2017.

Es por todo esto que muchos de los servicios que se ofertan a nivel mundial y de muchas de las nuevas empresas que gracias a la tecnología de las redes móviles y el teléfono, son capaces de dar servicios a domicilio o en el punto en el que se encuentre el usuario, por conocer la ubicación del terminal, gracias a los sistemas de localización que se proporciona al usuario. Los hay desde para servicio de transporte, comida, tráfico y movilidad, búsquedas relacionadas a la ubicación del móvil, de echo las comunicaciones móviles han incluso llegado a empezar a ganarle terreno a la telefonía fija con la llegada de módems WiFi para el hogar, inalámbricos, es decir no necesitan cables a la red de telefonía fija para el acceso a internet, sino que, cuentan con una SIM y se conecta a la red de telefonía móvil para proporcionar el acceso internet, estos sistemas están diseñados para no

poder cambiarlos de domicilio ya que mediante la ubicación del modem a través de la red móvil, cancela el servicio en caso de que detecte un cambio en la ubicación de este, es así de importante la gestión de la información de la ubicación de los terminales móviles para los servicios adquiridos por los usuarios.

Como ya vimos el principal servicio de ubicación es el GPS pero este tiene sus limitantes, y por eso surgió el GPS asistido, donde gracias a la información proporcionada por la red se obtiene una mejor precisión a la hora de dar la ubicación del móvil, y es de vital importancia para el funcionamiento de las redes móviles conocer esta información.

En cuestiones de seguridad, gracias a que se puede acceder a esta información con una orden dictada por un juez, las compañías proveedoras de telecomunicaciones, pueden proporcionar la ubicación aproximada de un UE en caso de robo o para ubicar al usuario en dado caso de que sea un delincuente o una persona desaparecida y/o privada de su libertad.

La ventaja de este servicio es que a diferencia del GPS que se puede desactivar, la red móvil puede conocer la ubicación aproximada del UE en cuanto este es encendido y accede a la red de la compañía con la cual trabaja la SIM. Para dar un mejor resultado se han implementado en las estaciones base los LMU abreviación de Location Measurement Unit. Elementos de la red que actúan como balizas de referencia con el objetivo de estimar el offset en el tiempo de transmisión entre dos estaciones bases, es decir, la sincronización entre dos Nodos B y así triangular de manera más eficiente el móvil, con la información recolectada de tres o más estaciones base.

Para realizar esto hay diferentes plataformas que facilitan la interfaz con el OSS, como por ejemplo Arieso[®], que monitorea en tiempo real la información de la red, los Handover, transmisión de datos, áreas de cobertura entre otras, y con esto se puede obtener la información de ubicación del UE.

En la figura 11.1 se muestra el monitoreo en tiempo real el volumen de datos de bajada en cierta área con Arieso[®], el mapa es generado por la ubicación de cada usuario y su actividad en la red celular.

En la figura 11.2 se muestra la aplicación de geolocalización que proporciona Arieso[®] y la información de la red que maneja.

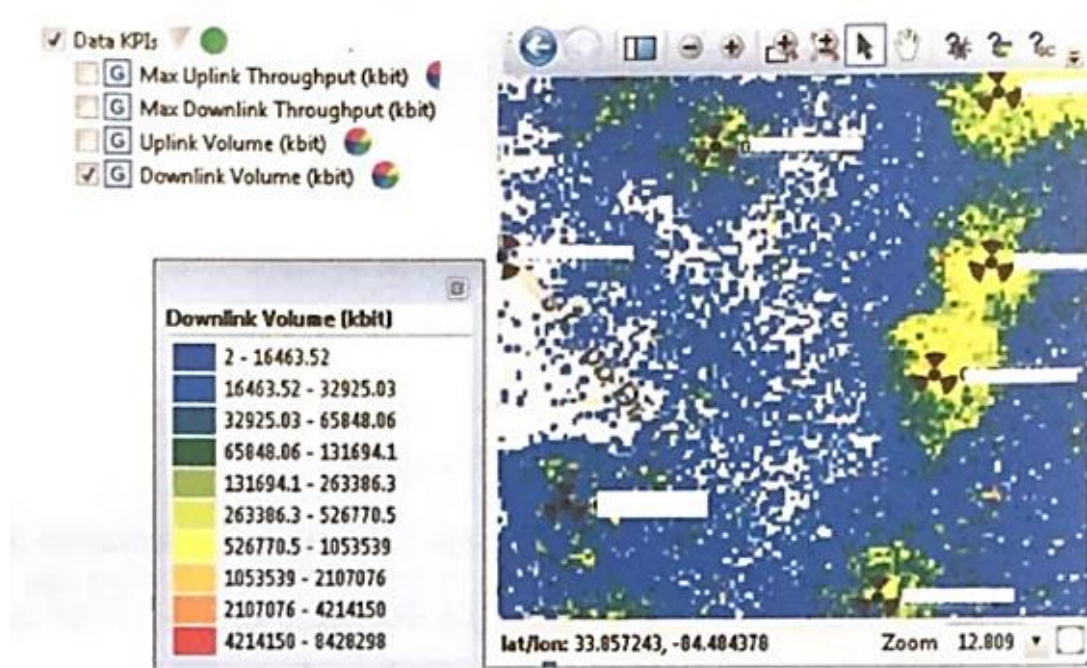


Figura 11.1. Monitoreo de datos de bajada Arieso ©

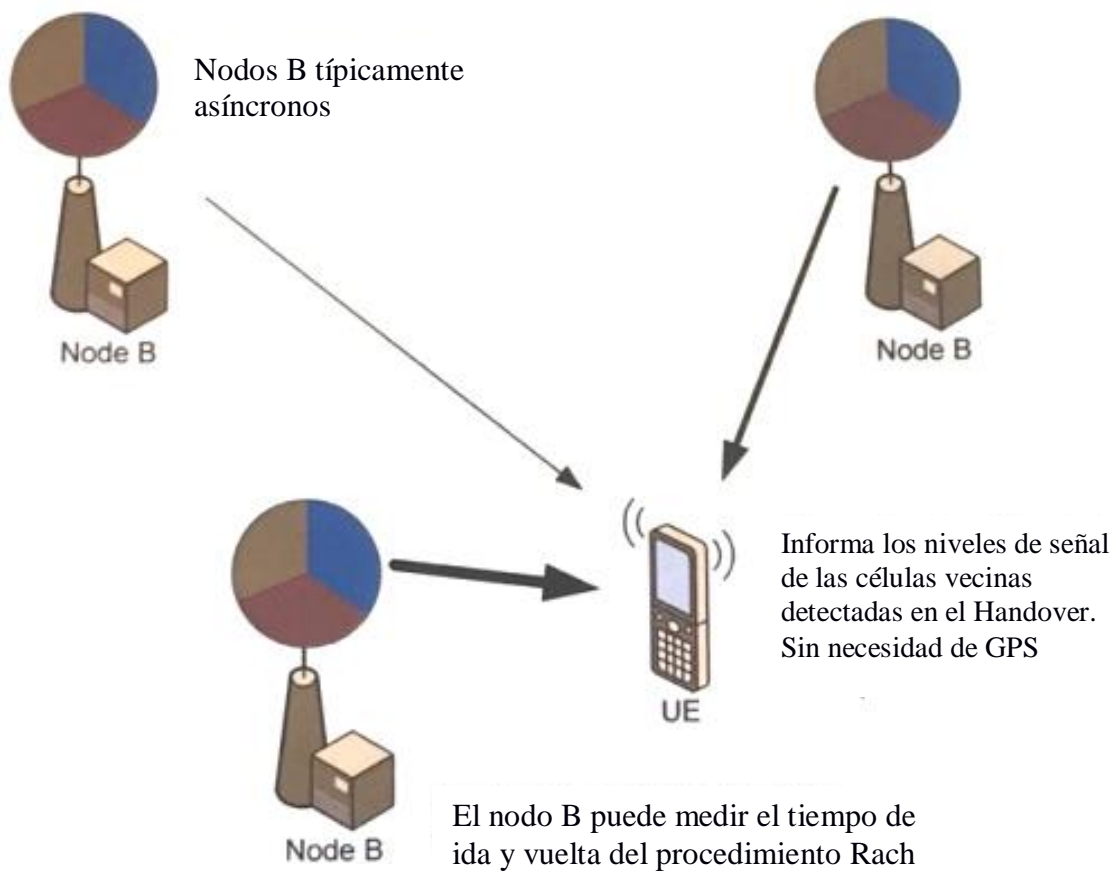


Figura 11.2. Triangulación con Arieso ©

12 CONCLUSIONES

A lo largo de los últimos años el crecimiento de los usuarios de telefonía móvil ha crecido de manera muy importante en nuestro país, y más aun con las reformas en materia de Telecomunicaciones que se aprobaron en el sexenio anterior, abriendo la puerta a la competencia y mejora de precios hacia el usuario y acceso a internet por medio del móvil.

Esto mismo ha traído como consecuencia la entrada de muchos servicios que benefician y dan comodidad a los usuarios, como se mencionó en el tema anterior, ya ha sido superado el número de habitantes a nivel mundial por el número de líneas móviles activas, en México se contabilizaron 119.5 millones de líneas activas con un crecimiento de 5.7 por ciento anual, el mayor en los últimos 5 años, para finales del 2018. La competencia como dije a aumentado y por ello, la mejora de precios en paquetes ha mejorado en el país, esto hace también que cada una de las operadoras, trate de dar el mejor servicio a los usuarios por un buen precio, mejor que el de la competencia para crecer en sus números de suscriptores, invirtiendo en tecnologías e infraestructura para mejorar.

Para conseguir su objetivo es indispensable que las operadoras tengan un buen control y detección de problemas, optimización y monitoreo en su red. La información tiene que estar actualizada y conocer en que celdas se encuentra algún problema, que número de usuarios hay, en que sectores se encuentran, cual es la máxima cobertura que posee cada célula de su red y, en qué lugares les conviene manejar más células, para mejorar su servicio, por todo esto es importante conocer la ubicación del terminal móvil y así identificar las zonas geográficas donde se presentan problemas y/o se requiere instalación de nueva infraestructura, por el número de usuarios que hay en determinada región. Los mapas geo localizados son una de las principales herramientas para ver de manera visual lo que acontece dentro de una red móvil de manera rápida y entendible, estos se crean a partir del uso que los suscriptores hacen de la red, generando así, el área en la que se encuentran y la calidad en cuanto a los servicios obtenidos, como dije, esta información es muy importante para la calidad del servicio proporcionado, y es por eso que entre mejor sea la precisión de la geolocalización del móvil, la información será más eficaz a la hora de compararla con el mapa real de la zona y conocida la información.

A lo largo de esta tesis se ha hablado de los diferentes métodos de localización de móviles, con uso principal de la red móvil de telefonía para conseguirla, y como ha ido evolucionando los sistemas de localización, en las diferentes tecnologías que hay en cuanto a la telefonía móvil. Vemos que este servicio es importante que mejore tanto para las operadoras de servicios de comunicaciones, como para el usuario, mejorando la calidad de servicio por un lado y por otro, la información puede ayudar mucho en las lamentables condiciones de inseguridad

que se viven actualmente en el país, ayudando estos sistemas, a dar con personas desaparecidas, o involucradas en hechos ilícitos, para su pronta localización por parte de las fuerzas de seguridad.

12.1 Líneas futuras

Las líneas futuras para este trabajo, son variadas y se pueden realizar diferentes avances en cuanto a los métodos de geolocalización que hace la red, para brindar sus servicios, aquí ya se habló de los cambios que sufrió a través de las diferentes generaciones que hay, hasta la actual, LTE, se espera la llegada de la 5ta Generación de tecnologías de telecomunicaciones, que está en su fase de pruebas en algunos países, y aunque aún no se empieza a desplegar, ya empiezan a llegar al mercado, equipos que soportan la 5G, con nuevos procesadores para tal motivo. Se espera que en 2020 empiece de manera seria el despliegue de la 5G y veremos qué cambios se añaden a la arquitectura de la red, protocolos y demás para mejorar la eficiencia, el gasto de energía regulando mejor la potencia del equipo, haciendo un mapeo de donde hay más handovers.

Todas estas acciones se pueden mejorar conociendo de manera más precisa la ubicación de los terminales y así conocer cómo se lleva a cabo su desplazamiento o si son fijos o casi fijos, desde donde acceden al servicio.

Es importante ya que se espera que para el 2025 el 72% de las personas con acceso a internet, tendrán acceso a esta a través de teléfonos móviles.

Con la llegada de la 5G se espera que llegue el auge del internet de las cosas (IoT) y con ello varios millones de conexiones industriales nuevas por medio de la red móvil.

Y todo esto se está desarrollando aun cuando en nuestro país aún no se llega a un despliegue completo de la 4G. ¿Qué maravillas tecnológicas nos esperan? ¿Qué beneficios y que desventajas traerá la dependencia tecnológica a la sociedad? Y sobre todo, ¿Qué consecuencias abra cuando todos los dispositivos cotidianos estén interconectados con el internet y este falle o sean hackeados?

BIBLIOGRAFÍA

Agudo de Carlos. Aurora. (2009), *Sistema de localización de dispositivos móviles basados en Wireless LAN (Tesis de Ingeniería)*, Universidad Carlos III de Madrid, Madrid, España.

Agusti Comes. R., (2010), *LTE: Nuevas tendencias en comunicaciones móviles*, España: Edit. Fundación Vodafone España.

AriesoGEO. Arieso. (Online). Disponible: <http://www.arieso.com/>

Campos Polo, H., (2009), *Redes móviles celulares*, Bogotá, Colombia: Edit. Universidad Santo Tomas.

Cuáles son las diferencias entre E, GPRS, 3G, 4G, 5G y esas otras redes a las que se conecta tu celular (y cómo te afectan tu conexión a internet). BBC. (Online). Disponible: <https://www.bbc.com/mundo/noticias-37247130>.

Diseño, integración y optimización de estaciones base de segunda generación. E-Reading. (Online). Disponible: <http://bibing.us.es/proyectos/abreproy/11980/direccion/CAP%C3%8DTULO+1+-+INTRODUCCI%C3%93N+Y+OBJETIVOS%252F>

Escobar Cristiani, J.M. (2012), *Telefonía y Conmutación*, Tlalnepantla. Edo. De México, Editorial Red tercer milenio S.C.

Frecuencias en las que operan las compañías de celular en México. Whistleout. (Online). Disponible: <https://www.whistleout.com.mx/CellPhones/Guides/telefonía-celular-mexico>

Gibson D., J. (Ed.), (1999), *The Mobile Communications Handbook*, Estados Unidos de América: Edit. CRS Press LLC.

Hernando Rábanos, J.M. / Mendo Tomas, L / Riera Salís. J.M., (2015), *Comunicaciones móviles*, España: Edit. Centro de estudios Ramón Areces S.A.

Huidobro, J.M. / Luque Ordóñez, J., (2014), *Comunicaciones Por Radio*, D.F., México: Edit. Alfaomega.

Jiménez Moya, M.T. / Reig Paswal, J. / Rubio Arjona, L., (2006), *Problemas de comunicaciones móviles*, Valencia, España: Editorial de la UPV.

Joskowicz, J. (2015), *Conceptos Básicos de Telefonía (Temario)*, Universidad de la Republica, Montevideo, Uruguay.

Kaaranen, H. / Ahtiainen, A. / Laitinen, L. / Naghian, S. / Niemi, V., (2006), *Redes UMTS Arquitectura, Movilidad y Servicios*, D.F., México: Edit. Alfaomega.

Lara Rodriguez, D. / Muñoz Rodriguez, D / Rosas Garcia, S., (1992), *Sistemas de comunicación móvil*, D.F., México: Alfaomega.

Métodos de localización. Teleco. (Online). Disponible: http://www.teleco.com.br/es/tutoriais/es_tutoriallbs/pagina_1.asp.

Rastreo de ubicación (geolocalización). Myshadow. (Online). Disponible: <https://myshadow.org/es/location-tracking>.

Telefonía celular: un vistazo a una radiobase. Researchgate. (Online). Disponible: https://www.researchgate.net/publication/282612178_TELEFONIA_CELULAR_UN_VISTAZO_A_UNA_RADIOBASE_EN_COLOMBIA_CELULAR_TELEPHONY_AN_OVERVIEW_A_RADIOBASE_STATION_ON_COLOMBIA

Telefonía móvil celular: origen, evolución, perspectivas. Redalyc. (Online). Disponible: <https://www.redalyc.org/html/1815/181517913002/>

Telefonía móvil. Areatecnologia. (Online). Disponible: <https://www.areatecnologia.com/telefonía-movil.htm>

Telefonía Móvil. Monografías. (Online). Disponible: <https://www.monografias.com/trabajos34/telefonía-celular/telefonía-celular.shtml>

Telefonía Móvil. Slideshare. (Online). Disponible: <https://es.slideshare.net/leobarflo/telefonía-movil-2g-final>

Tendencias Mundiales en Telefonía Móvil. ¿Qué está impulsando la industria móvil? Universo Abierto. (Online). Disponible: <https://universoabierto.org/2018/10/04/tendencias-mundiales-en-telefonía-movil-que-esta-impulsando-la-industria-movil/>.

Triangulación y geolocalización de llamadas. Erbol. (Online). Disponible: https://erbol.com.bo/opinion/al_punto/triangulación_y_geolocalización_de_llamadas.

GLOSARIO Y ACRÓNIMOS

1G	Primera Generación de comunicaciones móviles.
2G	Segunda Generación de comunicaciones móviles.
3G	Tercera Generación de comunicaciones móviles.
3GPP	(3rd Generation Partnership Project). Proyecto Asociación de Tercera Generación: es una colaboración de grupos de asociaciones de telecomunicaciones, conocidos como miembros organizativos.
4G	Cuarta Generación de comunicaciones móviles.
A	Interfaz que comunica la estación controladora con el subsistema de conmutación NSS.
AAA	(Authorization, Authentication and Accounting). Autorización, Autenticación y Contabilidad.
Abis	Interfaz que comunica las estaciones base con la estación controladora.
AC	(Alternating current) Corriente alterna.
AGCH	(Access Grant Channel) Canal de acceso concedido.
A-GPS	(Assisted-GPS) GPS Asistido.
AMPS	(Advanced Mobile Phone System) Sistema telefónico móvil avanzado.
AOA	(Angle Of Arrival) Posicionamiento por el Ángulo de Llegada.
ARFCN	(Absolute Radio Frequency Channel Number) Número de canal de radiofrecuencia absoluto.
Attach	Este procedimiento se produce cuando un móvil se conecta a una red GSM y consiste en un intercambio de mensajes entre la estación base y el móvil en los que se envía información de autenticación para comprobar que el móvil tiene acceso a la red.
AuC	(Authentication Center) Centro de Autenticación.
BCCH	(Broadcast control channel) Canal de control de emisión: es un canal punto a multipunto, unidireccional (enlace descendente) que se usa en la interfaz Um del estándar celular GSM.
BCCH	(Broadcast Control Channel). Canal de control Broadcast.
Beacon Frequency	Frecuencia piloto: se dedica obligatoriamente durante el slot de tiempo cero (y opcionalmente en los 2, 4 6) a la emisión y recepción de canales de control.
BSC	(Base Station Controller) Estación Base Controladora.
BSS	(Base Station Subsystem) Subsistema de Estaciones Base.
BSSAP	(BSS Application Part) Parte de Aplicación de la BSS.
BTS	(Base Transceiver Station) Estaciones de Radio Base.
BTSM	(Base Transceiver Station Management) Gestión de estaciones transceptoras base: es responsable por la transferencia de información de nivel RR al BSC.

Burst	Es un intervalo de tiempo en el que se divide una frecuencia, normalmente en 8 partes. Estos intervalos de tiempo son agrupados en un trama TDMA ($577\text{ms} * 8 = 4.615 \text{ ms.}$), la cual forma la unidad básica para la definición de los canales físicos. Un canal físico es un periodo Burst de la trama TDMA.
CDMA	(Code Division Multiple Access) Acceso múltiple por división de código.
CLK	(Clock) Reloj.
CM	(Connection Management) Gestión de la Conexión.
CN	(Core Network) Red central.
DC	(Direct current) Corriente directa.
DCN	(Data Communication Network) Red de comunicación de datos.
DL	(DownLink) enlace o conexión de bajada) es el término utilizado para representar el enlace entre una BTS y el móvil.
DTAP	(Direct Transfer Application Part) Parte de Aplicación de Transferencia Directa.
ECM	(EPS Connection Management) Gestión de conexión EPS.
EDGE	(Enhanced Data rates for GSM Evolution) Tasas de Datos Mejoradas para la Evolución del GSM.
EIR	(Equipment Identity Register) Registro de Identidad de Equipos.
EMM	(EPS Mobility Management) Gestión de Movilidad EPS.
eNB	(evolved Node B) Estaciones base evolucionada.
E-OTD	(Enhanced Observed Time Difference) Diferencia de Tiempos Observada Mejorada.
EPC	(Enhanced Packet Core) Núcleo de paquetes mejorado.
E-UTRAN	(Evolved UMTS Terrestrial Radio Access Network) Red de acceso de radio terrestre UMTS evolucionada.
FCCH	(Frequency Correction Channel) Canal de corrección de frecuencias.
FDMA	(Frequency Division Multiplex Access) Acceso Múltiple por División de Frecuencia.
Full Rate	Canal de velocidad completa.
GERAN	(GSM EDGE Radio Access Network) Red de acceso de radio GSM EDGE.
GGSN	(Gateway GPRS Support Node) Nodo de Soporte de datos.
GMSC	(Gateway Mobile Switching Center) Compuerta de la Central de Conmutación Móvil.
GMSK	(Gaussian minimum shift keying) Modulación por desplazamiento mínimo gaussiano.
GND	(Ground) Tierra.
GPRS	(General Packet Radio Service) Servicio general de paquetes vía radio.
GPS	(Global Positioning System) Sistema de Posicionamiento Global.

GSM	(Global System for Mobile Communications) Sistema Global para las comunicaciones móviles.
Half Rate	Canal de media velocidad.
Handover	traspaso (también handoff o transferencia) al sistema utilizado en comunicaciones móviles celulares con el objetivo de transferir el servicio de una estación base a otra cuando la calidad del enlace es insuficiente en una de las estaciones.
HLR	(Home localitation registrer) Registro local de abonados.
HSDPA	(High Speed Downlink Packet Access) Acceso ascendente de paquetes a alta velocidad.
HSS	(Home Subscriber Service) Servicio de suscriptor local.
IDU	(Indoor unity) Unidad interior.
IMEI	(International Mobile Equipment Identity) Identidad Internacional de Equipo Móvil.
IMS	(IP Multimedia Subsystem) Subsistema Multimedia IP.
IMSI	(International Mobile Subscription Identity) Identidad Internacional del Abonado Móvil.
IN	(Intelligent Network) Red inteligente.
IoT	(Internet of Things) Internet de las cosas. Es un concepto que se refiere a la interconexión de objetos cotidianos a través de internet. Es decir, son todas esas cosas con las que convivimos a diario y que antes no estaban conectadas a la red: vehículos, electrodomésticos, máquinas, ropa, etc.
IP	(Internet Protocol) Protocolo de internet.
ISDN Integrados.	(Integrated Services Digital Network) Red Digital de Servicios Integrados.
ISUP	Es un protocolo de circuitos conmutados, usado para configurar, manejar y gestionar llamadas de voz y datos sobre PSTN. ISUP también vincula la red celular y PCS a la PSTN.
ITU	(International Telecommunications Union) Unión Internacional de Telecomunicaciones.
LAPD	(Link Access Procedure on D channel) Protocolo de Control de Enlace de Datos para los canales tipo D
LCS	Servicios de Localización.
LIF-MLP	Interfaz Lógica – Protocolo de Localización de redes Móviles.
LMU	Abreviación de Location Measurement Unit. Elementos de la red que actúan como balizas de referencia con el objetivo de estimar el offset en el tiempo de transmisión entre dos estaciones bases, es decir, la sincronización entre dos Nodos B.
Location Update	Actualización de la ubicación.
LTE	(Long Term Evolution) Evolución a Largo Plazo: hace referencia a la tecnología de banda ancha inalámbrica que sirve para la

	transmisión de datos con la finalidad de dar acceso a Internet a los dispositivos móviles.
MAP	(Mobile Application Part) Parte de aplicación móvil: se utiliza para compartir información sobre los abonados celulares entre distintas redes.
MBPS	Megabytes por segundo.
ME	(Mediation Equipment) Equipos de medición.
ME	(Mobile Equipment) Equipo Móvil.
MM	(Mobility Management) Gestión de la Movilidad.
MME	(Mobility Management Entity) Entidad de Gestión de la Movilidad.
MMS	(Multimedia Messaging Service) Servicio de mensajería multimedia.
MS	(Mobile Station) Estación móvil.
MS	(Mobile Station) Terminal Móvil.
MSC	(Mobile Switching Center) Central de Conmutación Móvil.
MSISDN	(Mobile Station Integrated Services Digital Network) Estación Móvil de la Red Digital de Servicios Integrados.
MTP	(Message Transfer Part) Parte de Transferencia de Mensajes.
MW	(Microwave) Microonda.
NE	(Network Elements) Elementos de red.
Node B	Estaciones base.
NSS	(Network Switching Subsystem) Subsistema de Conmutación.
ODU	(outdoor unity) Unidad exterior.
OMA	(Open Mobile Alliance) Alianza Móvil Abierta
OMC-R	(Operation and Maintenance Center for Radio Part). Centro para la Operación y Mantenimiento de la parte Radio
OMC-S	(Operation and Maintenance Center for Switching Part) Centro para la Operación y Mantenimiento de la parte de Conmutación.
OS	(Operation System), Sistema de operación.
OSI	(Open System Interconnection) Sistema Abierto de Interconexión.
OSS	(Operation Subsystem) Subsistema de Operación y Mantenimiento.
Overlaid	son las celdas cubiertas por una celda más grande.
Paging	Proceso iniciado por la red para encontrar la ubicación del terminal.
PCH	(Paging Channel) Canal Paging.
PCS	(Personal Communications Services) Servicios de comunicación personal.
PDC	(Personal Digital Cellular/Communications) Celular/Comunicación Digital Personal
P-GW	(Packet Data Network Gateway) Puerta de enlace de red de datos en paquetes.
PIN	(Personal Identification Number). Número de identificación personal.

PSTN	(Public Switching Telephone Network) Red telefónica pública conmutada.
PUK	(PIN Unblocking Key). Clave para desbloquear el PIN.
RACH	(Random Access Channel) Canal de requerimiento de acceso.
RAND	(Random Number) Numero aleatorio: es un numero aleatorio de 128 bits generado por el Registro de ubicación local HLR.
RF	Radio Frecuencia.
RNBP	(Reference Node-Based Positioning) Posicionamiento Basado en el Nodo de Referencia.
RNC	(Radio Network Controller) Estación controladora.
Roaming	Itineracia: es un concepto utilizado en telecomunicaciones para referirse a la posibilidad de un dispositivo inalámbrico de utilizar una cobertura de red distinta de la principal.
RR	(Radio Resource Management) Gestión de Recursos Radio.
RST	(Reset) Reiniciar.
RTT	(Round-Trip Time) Posicionamiento basado en el Tiempo de Ida y Vuelta.
SCCP	(Signalling Connection Control Part) parte de control de conexión de señalización: Forma parte del sistema de señalización 7 (SS7).
SCH	(Synchronization Channel) Canal de sincronización.
SDCCH	(Stand alone Dedicated Control Channel) Canal de señalización.
SGSN	(Serving GPRS Support Node) Nodo de servicios.
S-GW	(Serving Gateway) Puerta de enlace de servicio.
SIM	(Subscriber Identity Module) Módulo de identidad del abonado.
SMS	(Short Message Service) Servicio de mensajes cortos.
SRES	Es la respuesta firmada de 32 bits generada por la estación móvil y el centro de conmutación de servicios móviles.
SS7	(Signaling System Number 7) Sistema de Señalización número 7.
TA	(Timing Advance) Tiempo de avance.
TA	(Tracking Area) Area de Seguimiento.
TACS	(Total Access Communications System) Sistema de Comunicación de Acceso Total, es la versión europea del AMPS.
TAI	(Tracking Area Identifier) Identificador de Área de Seguimiento.
TCAP	(Transaction Capability Application Part) Parte de aplicación de capacidad de transacción: que proporciona funciones para la comunicación con el extremo remoto de una cadena de señalización y permite el establecimiento de múltiples diálogos.
TCH	(Trafic Channel) Canal de tráfico.
TDMA	(Time Division Multiplex Access) Acceso Multiplexado por División de Tiempo.
TDOA	(Time Difference Of Arrival) Posicionamiento basado en la Diferencia de Tiempos de Llegada.

TMN	(Telecommunications Management Network) Red de Gestión de Telecomunicaciones.
TMSI	(Temporary Mobile Subscriber Identity) Identificación Temporal del Abonado.
TOA	(Time Of Arrival) Posicionamiento por el Tiempo de Llegada.
TRAU	(Transcoding and Rate Adaptation Unit) Unidad Transcodificadora.
TUP	Teléfono usuario pieza: es un protocolo analógico que realiza llamadas telefónicas de base de conexión y desconexión.
UE	(User Equipment) Equipo de Usuario.
UL	(UpLink) enlace o conexión de subida, es el término utilizado en un enlace de comunicación para la transmisión de señales de radio (RF) desde el móvil.
Um	Es la interfaz de radio que comunica el móvil con la estación base.
UMTS	(Universal Mobile Telephone Service) Sistema universal de telecomunicaciones móviles.
UTRAN	(<i>UMTS Terrestrial Radio Access Network</i>) Red de acceso de radio terrestre UMTS.
VAD	(Voice Activity Detection) Detección de actividad de voz.
VDC	(Voltage of Continuous Current) Voltaje de corriente continua.
VLR	(Visitor localisation register) Registro Local de visitantes.