ESCUELA TÉCNICA SUPERIOR DE INGENIEROS INDUSTRIALES Y DE TELECOMUNICACIÓN

UNIVERSIDAD DE CANTABRIA

Trabajo Fin de Grado

SOPORTE PARA GESTIÓN REMOTA OTA SOBRE UNA PICOCELDA GSM/GPRS

Over-The-Air management on a GSM/GPRS picocell

Para acceder al Titulo de

Graduado en Ingeniería de Tecnologías de Telecomunicación

Jesús Vega Diaz

Septiembre 2014

E.T.S. DE INGENIEROS INDUSTRIALES Y DE TELECOMUNICACION

GRADUADO EN INGENIERÍA DE TECNOLOGÍAS DE TELECOMUNICACIÓN

CALIFICACIÓN DEL TRABAJO FIN DE GRADO

Realizado por: Jesús Vega Diaz
Director del TFG: Jorge Lanza Calderón
Título: "Soporte para gestión remota OTA sobre una picocelda GSM/GPRS"
Title: "Over-The-Air management on a GSM/GPRS picocell"

Presentado a examen el día: 24 de Septiembre de 2014

para acceder al Título de

GRADUADO EN INGENIERÍA DE TECNOLOGÍAS DE TELECOMUNICACIÓN

Composición del Tribunal:
Presidente (Apellidos, Nombre):
Secretario (Apellidos, Nombre):
Vocal (Apellidos, Nombre):

Este Tribunal ha resuelto otorgar la calificación de: .....

Fdo.: El Presidente

Fdo.: El Secretario

Fdo.: El Vocal

Fdo.: El Director del TFG
(sólo si es distinto del Secretario)

Vº Bº del Subdirector

Trabajo Fin de Grado Nº
(a asignar por Secretaría)

Agradecimientos

Simplemente dar las gracias a todo el que haya contribuido directa o indirectamente en que me convierta en algo parecido a un Ingeniero de Telecomunicaciones.

En primer lugar a mi familia, sin la que por supuesto, nada de esto sería posible, a mi padre por hacerme nacer con un “Macintosh” bajo el brazo, a mi madre y hermano, y también a los que lo vean desde algún lejano lugar.

Mención especial merece Irene, con quien he soportado gran parte de la carga nerviosa que conlleva estudiar esta carrera, gracias por apoyarme en todo momento, por confiar en mí, y sobre todo por cuidarme.

No quiero olvidarme de los compañeros conocidos durante la carrera, que aunque no son muchos, son muy buenos, y sobre todo aquellos que se han convertido en grandes amigos.

A todos los buenos profesores de la Universidad de Cantabria de los que he sido alumno durante esta carrera, a todo el grupo de Ingeniería Telemática, y en especial a Jorge, por brindarme la posibilidad de trabajar en un proyecto atractivo para mí, bonito y sobre todo útil.

Resumen

Si hay un desarrollo tecnológico que tenga una fuerte presencia entre la población de los últimos veinte años, ese es el *Global System for Mobile Communications* (GSM). Todos tenemos un teléfono móvil en nuestro bolsillo, y hacemos uso de los servicios de esta red a diario, siendo ya un elemento imprescindible de nuestros días.

Una de las prestaciones que esta red ofrece es el servicio de mensajes cortos, característica que nos permite enviar mensajes de hasta 140 caracteres entre dos terminales móviles. Dicho servicio tuvo una importante utilización hasta la aparición de las redes de datos móviles y la irrupción de los servicios de mensajería instantánea.

El servicio de mensajería, además de contener texto convencional, ofrece la posibilidad de insertar datos binarios, que serán procesados por las tarjetas inteligentes contenidas en las estaciones móviles, siendo necesaria para esto, la implementación de un centro de mensajería y una entidad remota de gestión *Over-The-Air* (OTA).

Gracias al desarrollo de nuestra propia red a través de una "picocélula" basada en software libre, contaremos con toda la infraestructura de una red móvil de bajo coste, ideal para entornos rurales, interiores, o de investigación, perfecta para estudiar en profundidad la pila de protocolos y todos sus servicios.

Esta picocélula nos abre un gran abanico de posibilidades en cuanto a monitorización y control remoto de dispositivos, ya no sólo terminales móviles, sino cualquier elemento que pudiese portar una tarjeta *Subscriber Identity Module* (SIM), como son muchos de los elementos de una red de sensores, habilitando una red propia para la comunicación entre máquinas (M2M, *Machine-to-machine*).

Mediante el desarrollo de nuestra plataforma *Over-The-Air*, es posible realizar remotamente operaciones de gestión de los subscriptores a la red, la programación vía comandos OTA, insertar aplicaciones en los dispositivos, activar o desactivar servicios, y un largo etcétera de posibilidades.

Así mismo, aprovechando el despliegue realizado, podremos analizar tanto desde fuera como desde dentro de la red, la robustez de su seguridad, y presentaremos algunos posibles ataques a la red.

Abstract

If there is a technological development that has a strong presence among the world population in the last twenty years, that is the Global System for Mobile Communications (GSM). Everyone of us has a mobile phone in our pockets, and we use the services of this network daily, being an essential element of these days.

One of the features this network offers is the Short Message Service (SMS), allowing sending up to 140 characters messages between two or more mobile terminals. The SMS service had a significant use until the appearance of mobile data networks and the release of instant messaging applications.

This messaging service, although mainly used for exchanging text between users, provides the ability of encapsulating binary data, such as for instance commands that will be processed by the smart card contained in the mobile station. The implementation of a SMS Mobile Switching Centre (SMSC) and the request-response pairs of the Short Message Peer-to-peer Protocol (SMPP) is required to support such functionality.

By developing our own network through a "picocell" based on free software, we are able to study in depth the protocol and all its services. This way it will be possible to enable remote monitoring and control of devices, not just typical mobile devices, but anything that could carry a Subscriber Identity Module (SIM) card, as many of the elements of a Wireless Sensor Network (WSN), enabling a dedicated network for communications between machines (M2M).

Moreover, it will also allow analyzing network security using a two way approach, from the perspective of an external user and from the internal administrative point of view.

Indice

1. Introducción y objetivos 1
1.1 Redes Inalámbricas 1
1.2 Objetivo del trabajo 3
1.3 Estructura de la memoria 4
2. Global System for Mobile Communications 6
2.1 Interfaz radio 6
2.1.1 Características físicas 6
2.1.2 Canales lógicos de control 9
2.1.3 Canales lógicos de tráfico 10
2.1.4 Ráfagas GSM 10
2.2 Arquitectura de red 11
2.2.1 Estación móvil 11
2.2.2 Subsistema de estación base 12
2.2.3 Subsistema de red y conmutación 13
2.2.4 Subsistema de operación y mantenimiento 13
2.3 Seguridad 14
2.3.1 Autenticación 14
2.3.2 Confidencialidad 15
2.3.3 Anonimato 15
3. General Packet Radio System (GPRS) 16
3.1 Características físicas 17
3.2 Arquitectura de red 18
3.3 Arquitectura de Protocolos 18
3.3.1 Plano de transmisión 18
3.3.2 Plano de señalización 19
3.4 Gestión de la movilidad 19
3.5 Enrutado de los paquetes 20
3.6 Enhaced Data Rates for GSM Evolution (EDGE) 20
4. Mensajería 21
4.1 Short Message Service (SMS) 21
4.1.1 Repertorio de PDUs 23
4.1.1.1 SMS-SUBMIT (MS → SC) 23
4.1.1.2 SMS-SUBMIT-REPORT 24
4.1.2 SMS-DELIVER (SC → MS) 25

4.1.2.1 SMS-DELIVER-REPORT *25*
4.1.3 User Data Header (UDH) *26*
4.1.4 SIM Toolkit Security Headers *27*
4.2 Short Message Peer-to-peer Protocol (SMPP) 29
5. Evolución de las comunicaciones móviles 31
5.1 Evolución de las Redes móviles en España 31
5.1.1 Operadores Móviles Virtuales (OMV) *34*
5.1.2 Situación del espectro radioeléctrico en España *35*
5.2 Cuarta generación de telefonía móvil: LTE 36
5.3 Plataformas OTA sobre LTE 37
6. Analizador de Redes GSM 40
6.1 OsmocomBB 40
6.1.1 Software en el terminal móvil (Baseband Firmware) *41*
6.1.1.1 RSSI Monitor Firmware *43*
6.1.1.2 Layer1 ..... *43*
6.1.2 Software en el PC (Host Software) *44*
6.2 Procedimiento de uso del analizador GSM 45
6.2.1 Registro en la red (IMSI Atach) *48*
6.2.1.1 Desconexión (IMSI Detach) *50*
6.2.2 Llamada de voz *50*
6.2.3 Envío y recepción de SMS *53*
7. Despliegue de una picocélula GSM/GPRS 55
7.1 OpenBSC 55
7.1.1 ip.access nanoBTS *56*
7.1.1.1 Configuración nanoBTS *57*
7.1.2 osmo-nitb *58*
7.1.3 Operación de la red *60*
7.1.3.1 HLR/VLR *61*
7.1.4 Operaciones de Gestión *62*
7.1.5 Servicios *63*
7.2 Soporte para datos móviles GPRS 64
7.2.1 Configuración *65*
7.2.2 Operación de la red *66*
7.2.3 Evolución de GPRS: EDGE *69*
7.3 Soporte para mensajería SMPP 69
7.4 Plataforma de gestión remota OTA 70
7.4.1 Operación de la plataforma OTA *72*
7.4.2 Caso de uso *73*

7.5 Implicaciones de Seguridad 74
7.5.1 DOS: Denegación de Servicio (Denial of Service) 74
8. Conclusiones y líneas futuras 76
8.1 Conclusiones 76
8.2 Líneas futuras 77
9. Bibliografía 79
10. Acrónimos 82
11. Apéndices 86
11.1 [Apéndice 1] Guía de Instalación OsmocomBB 86
11.2 [Apéndice 2] Comandos OsmocomBB 88
11.3 [Apéndice 3] Guía de Instalación OpenBSC 89
11.4 [Apéndice 4] openbsc.cfg 91
11.5 [Apéndice 5] Comandos Osmo-SGSN 92

Indice de Figuras

Figura 1.1: Conexiones móviles activas 3
Figura 2.1: Bandas de frecuencia GSM en Europa 7
Figura 2.2: Duplexado frecuencial GSM 7
Figura 2.3: Duplexado temporal GSM 7
Figura 2.4: Combinación TDMA/FDMA 8
Figura 2.5: Esquema de partición celular 8
Figura 2.6: Estructura jerárquica TDMA 10
Figura 2.7: Arquitectura de red GSM 11
Figura 2.8: Proceso de Autenticación 15
Figura 3.1: Arquitectura de red GPRS 18
Figura 3.2: Plano de transmisión GPRS 19
Figura 4.1: Arquitectura de red con servicios SMS 22
Figura 4.2: SMS-SUBMIT TPDU 23
Figura 4.3: SMS-SUBMIT-REPORT TPDU 24
Figura 4.4: SMS-DELIVER TPDU 25
Figura 4.5: SMS-DELIVER-REPORT TPDU 26
Figura 4.6: UDH contenida en campo UD de SMS 26
Figura 4.7: Estructura del "command packet" 28
Figura 4.8: Arquitectura de red SMPP 29
Figura 4.9: SMPP PDU 29
Figura 4.10: Ejemplo de sesión SMPP 30
Figura 5.1: Reparto del espectro tras subasta año 2000 33
Figura 5.2: Ganancia líneas móviles por operador 34
Figura 5.3: Prueba de velocidad 4G 37
Figura 5.4: Modelo cliente-servidor en plataformas OTA 39
Figura 6.1: Arquitectura general OsmocomBB 41
Figura 6.2: Canalización Osmocon 42
Figura 6.3: RSSI Monitor Firmware 43
Figura 6.4: Cabecera GSMTAP 44
Figura 6.5: Lectura datos SIM 46
Figura 6.6: Redes disponibles 47

Figura 6.7: Celdas adyacentes....47
Figura 6.8: Tramas dirigidas a otros subscriptores....47
Figura 6.9: Asignación Inmediata de canal....48
Figura 6.10: Proceso de registro en la red....48
Figura 6.11: Location Update Request....49
Figura 6.12: System Information....49
Figura 6.13: Ciphering Mode Command....49
Figura 6.14: Proceso de desconexión....50
Figura 6.15: Procedimiento de llamada saliente....50
Figura 6.16: Service Request (llamada)....51
Figura 6.17: Setup (llamada saliente)....51
Figura 6.18: Connect....51
Figura 6.19: Desconexión de la llamada....52
Figura 6.20: Proceso de llamada entrante....52
Figura 6.21: Setup (llamada entrante)....52
Figura 6.22: Assignment Command....53
Figura 6.23: Service Request (SMS)....53
Figura 6.24: SMS-SUBMIT....54
Figura 6.25: Transmisión de SMS saliente....54
Figura 6.26: Mensaje entrante al analizador....54
Figura 6.27: SMS-DELIVER....54
Figura 7.1: Arquitectura General OpenBSC....56
Figura 7.2: ip.access nanoBTS 1800....57
Figura 7.3: Datagrama UDP ipaccess-find....58
Figura 7.4: Arquitectura OpenBSC "Network-In-The-Box"....59
Figura 7.5: Distribución de timeslots OpenBSC....60
Figura 7.6: Arranque osmo-nitb....60
Figura 7.7: Búsqueda y selección de red....60
Figura 7.8: Terminal asociado con la red....61
Figura 7.9: Interfaz Web HLR....62
Figura 7.10: Llamada y SMS entrantes....63
Figura 7.11: Arquitectura OpenBSC + OpenGGSN....64
Figura 7.12: Distribución de slots OpenBSC+GPRS....64
Figura 7.13: Arranque ggsn....66

Figura 7.14: Arranque osmo-sgsn 67
Figura 7.15: Terminal bajo red GPRS 67
Figura 7.16: Reenvío de paquetes en ggsn 68
Figura 7.17: Proceso de registro GPRS 68
Figura 7.18: PDP Context Request 68
Figura 7.19: Terminal bajo red EDGE 69
Figura 7.20: Arquitectura OpenBSC + SMPP 71
Figura 7.21: Proceso de envío de mensaje SMS vía SMPP 72
Figura 7.22: Encapsulado del mensaje SMPP enviado 72
Figura 7.23: Tabla de servicios SIM 72
Figura 7.24: SMS-DELIVER con comando STK (aleatorio) 73
Figura 7.25: Comando UPDATE contacto 74
Figura 7.26: Segundo octeto del SPI 74
Figura 7.27: Tráfico intercambiado 75
Figura 7.28: SMS-DELIVER-REPORT 75

Indice de Tablas

Tabla 2.1: Códigos contenidos en la tarjeta SIM 12
Tabla 3.1: Canales lógicos GPRS 17
Tabla 4.1: Elementos de la PDU SMS-SUBMIT 23
Tabla 4.2: Elementos de la PDU SMS-SUBMIT-REPORT 24
Tabla 4.3: Elementos de la PDU SMS-DELIVER 25
Tabla 4.4: Elementos de la PDU SMS-DELIVER-REPORT 26
Tabla 4.5: Elementos del command packet 28
Tabla 5.1: Reparto del espectro en España hasta 2030 35
Tabla 6.1: Elementos de la cabecera GSMTAP 45
Tabla 7.1: Configuración empleada para osmo-nitb 59

Capítulo 1

Introducción y objetivos

Las tecnologías de la información forman ya parte de nuestro día a día y prácticamente sin darnos cuenta nos encontramos rodeados de cada vez más mecanismos de comunicación. La capacidad de procesado de los dispositivos empleados para el acceso a la información aumenta a la par que disminuye su tamaño. Todo ello tiene un reflejo directo en el acceso cada vez más global a dispositivos más inteligentes y con capacidades de acceso a la plétora de redes de muy distinta naturaleza que nos rodea.

Estas redes inicialmente diseñadas y empleadas para transportar información entre usuarios y poner a personas en contacto, deben ahora soportar a la creciente demanda de comunicación entre dispositivos. Equipos (sensores, actuadores, etc.), que hasta hace poco actuaban de forma independiente, actualmente presentan necesidades de coordinación y, por tanto, de transferencia de información. Este nuevo paradigma de red se conoce como el Internet de las Cosas (IoT, *Internet of Things*).

Debido a sus requerimientos de movilidad, las comunicaciones inalámbricas juegan un papel esencial a la hora de hacer realidad estas nuevas redes. De forma genérica su operativa se basa en un conjunto de elementos sensores que recopilan datos del entorno; esta información se transmite haciendo uso de otros nodos similares hacia concentradores que publican, a través de redes móviles o Internet, los datos agregados.

Parece claro, que si las redes móviles ya jugaban un papel vital durante la última década, la tendencia muestra un claro incremento en su uso fruto de la aparición de nuevos casos de uso. En este nuevo entorno resulta fundamental mantener un alto nivel de seguridad, más aún cuando se consideran dispositivos conectados permanentemente a redes públicas.

1.1 Redes Inalámbricas

Cualquier enlace de radiocomunicación entre dos terminales, en el cual el receptor, el emisor o ambos están en movimiento, es la base de una red de comunicaciones móviles. El reglamento de radiocomunicaciones de la *International Telecommunication Union* (ITU-R) define el servicio móvil como un servicio de radiocomunicación entre estaciones móviles y estaciones terrestres o entre estaciones móviles únicamente. En función de la situación del terminal móvil, el reglamento diferencia tres tipos de servicios: servicio móvil terrestre, servicio móvil marítimo y servicio móvil aeronáutico. Las comunicaciones móviles también pueden dividirse en sistemas punto a punto y punto-multipunto, siendo éstos últimos el objeto de éste documento.

Desde mediados del siglo XX existen sistemas capaces de transmitir datos por medios radioeléctricos, pero éstos no estaban al alcance de cualquiera, debido a su coste quedaban relegados a uso exclusivo de fuerzas militares de ciertos países.

Actualmente, el servicio más utilizado es sin duda la telefonía móvil, la cual hizo aparición a finales de los años 1950, cuando los primeros sistemas analógicos, también conocidos como de primera generación (1G), comienzan a desplegarse en los países nórdicos. Aparecen así diversos sistemas de comunicaciones móviles en países Europeos, todos ellos incompatibles entre sí. En el año 1982, la Conferencia Europea de Administraciones de Correos y Telecomunicaciones (CEPT, *Conférence européenne des administrations des postes et des télécommunications*) crea el grupo de trabajo *Groupe Spécial Mobile* (GSM), asignándole la tarea de desarrollar un estándar europeo de telefonía móvil digital con el principal propósito de evitar los problemas de las redes analógicas anteriores. En 1990 se finalizan las especificaciones del primer estándar GSM y en 1991 se presentan los primeros terminales móviles GSM. No es hasta 1992 cuando comienza la actividad de las primeras redes de segunda generación (2G), como se denominó a los primeros despliegues de telefonía móvil digital.

La rápida adopción que tuvo el sistema GSM provocó un gran avance de la tecnología, habilitando bajadas de precio y popularizando el acceso tanto al servicio y a los terminales. El éxito comercial de estas redes ha supuesto sin duda alguna uno de los mayores nichos de negocio de nuestros días. A finales del año 2003, había algo más de un billón de subscriptores en redes móviles, lo que significa que una de cada seis personas tenía contratados servicios móviles. Actualmente hay alrededor de 7 billones de tarjetas SIM activas, excluyendo de esta cifra las tarjetas utilizadas para conexiones M2M. La fuerte penetración de estos servicios hace necesario nuevos avances y cambios, que ya demandan los propios consumidores, como la interoperabilidad, y otros que son consecuencia de la saturación de su uso, como la eficiencia espectral.

GSM cumplió los objetivos que le fueron encomendados al grupo de trabajo del CEPT, pero la demanda del mercado de servicios multimedia hizo necesaria la presencia de un servicio de datos de alta velocidad. Este es el germen de las redes de tercera generación (3G). Sin embargo, la tecnología no estaba lo suficientemente madura como para soportar los nuevos requerimientos y se decide desplegar un sistema de transición (2.5G) operando sobre *General Packet Radio System* (GPRS). Se incluyen mensajes multimedia (MMS, *Multimedia Message Service*) y un servicio de conmutación de paquetes vía radio que soporta regímenes binarios entre 56 y 114 kbps. Con la evolución *Enhaced Data Rates for GSM Evolution* (EDGE) se alcanzan los 384 kbps en modo paquete, cumpliendo los requisitos de la ITU para denominarse red 3G. La aparición de novedosos métodos de acceso al medio rádio como *Code Division Multiple Access* (CDMA) hace posible el desarrollo nuevos sistemas móviles, ya sí de 3G, como *Universal Mobile Telecommunications System* (UMTS), que alcanzan velocidades elevadas de entre 144 kbps hasta 7,2 Mbps.

El nuevo crecimiento de las necesidades de datos de los usuarios, sobre todo audio y vídeo, y la fuerte implantación de las redes internet han hecho necesario una nueva evolución hacia las denominadas redes de cuarta generación (4G) operando mediante *Long Term Evolution* (LTE).

Como se ha venido apuntando, la industria móvil está en continuo crecimiento, tanto en subscriptores que, como se puede observar en la Figura 1.1, se estima llegue a los 10 billones en el año 2020, como en tráfico de datos. Adicionalmente juega un papel fundamental en el desarrollo socio-económico de muchos otros sectores industriales.

La alianza GSM (GSMA) señala cuatro áreas clave para que el crecimiento continúe y suponga significantes oportunidades y beneficios:

- Datos personales: el acceso autenticado a un amplio abanico de servicios mediante una identidad digital enlazada con el teléfono móvil
- Comercio digital: los teléfonos como corazón del comercio, con el potencial de realizar operaciones de distinta índole utilizando monederos digitales.
- Vida conectada: las redes inteligentes tienen la oportunidad de revolucionar las vidas de sus usuarios y la productividad de muchas empresas.
- Futuras redes: las redes móviles tendrán un papel clave en la era todo-IP.

Es en éstas áreas donde toma mayor relevancia el uso de la tarjeta SIM como responsable de gran parte de la seguridad del sistema.

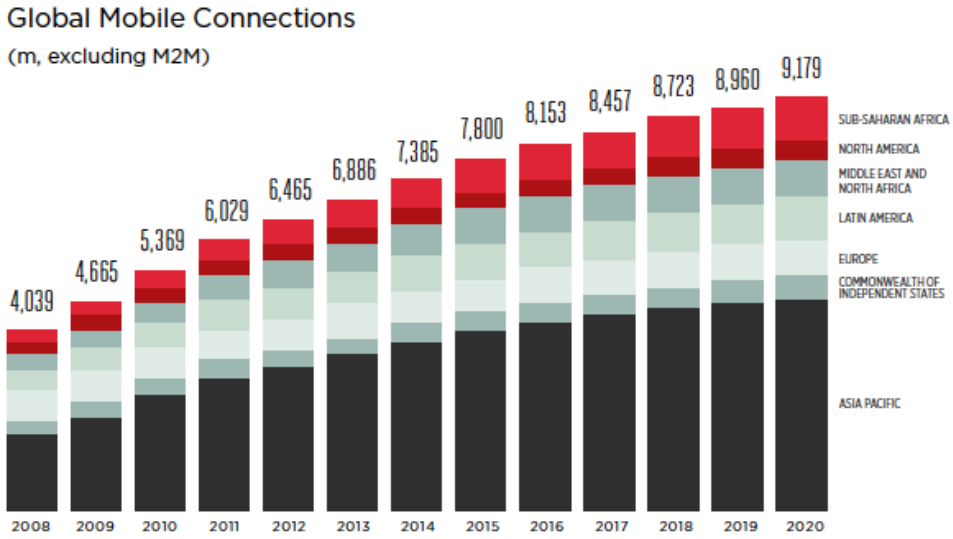


Figura 1.1: Conexiones móviles activas

1.2 Objetivo del trabajo

Con el mencionado crecimiento de las necesidades de los usuarios en términos de disponibilidad y ancho de banda, los operadores se enfrentan continuamente al reto de satisfacer dicha demanda de tráfico, aumentada si cabe por la introducción de un mayor número de dispositivos en la red.

Así mismo, dichas necesidades varían enormemente en función del entorno de despliegue, pudiendo ser grandes en áreas urbanas, y más ligeras en zonas rurales. Es en las zonas rurales, dónde los operadores encuentran mayores dificultades para recuperar la inversión realizada, dado su mayor coste y mantenimiento, y el menor número de subscriptores que harán uso de la infraestructura. La solución aportada durante el trabajo puede tener aplicación en ciertos despliegues, dados sus bajos requerimientos eléctricos y de computación, sería posible servir mediante picoceldas independientes un gran área rural, con una baja inversión económica, allí donde no existen grandes requerimientos de calidad del servicio.

Dejando a un lado el enfoque meramente comercial y centrándose en una perspectiva académica, las redes mantenidas por los operadores tradicionales presentan el gran inconveniente de estar completamente cerradas, sin acceso a ninguno de sus

elementos de red para un posible análisis o estudio. Las diferentes publicaciones en el área se centran en aspectos teóricos de los protocolos empleados, el procesado de la señal transmitida o del diseño y despliegue de redes desde el punto de vista usuario o del administrador del sistema.

En este sentido aunque el estándar GSM es abierto y permitiría el desarrollo de soluciones globales y accesibles, las implementaciones realizadas, principalmente comerciales, de los múltiples elementos de la red realizadas de los diferentes elementos son cerradas y difícilmente accesibles para su evaluación por su elevado coste.

Por esta razón, uno de los objetivos de este trabajo consiste en familiarizarse, desarrollar, configurar y desplegar la infraestructura de red necesaria para operar y mantener una red de comunicaciones móviles con soporte tanto de voz como de datos.

Una vez desplegada, entraremos en uno de los aspectos principales de su operación y mantenimiento, la gestión del comportamiento de los elementos en disposición del usuario, principalmente la tarjeta SIM, y sus capacidades de identificación, almacenamiento de información, roaming y otros datos. Debido a lo que se hará especialmente hincapié dentro del trabajo a la gestión de este elemento, de manera remota empleando lo que se conoce como gestión *Over-the-air*.

Adicionalmente, se aprovechará el despliegue de red realizado con el objeto de estudiar la operativa del estándar GSM desde dentro de la red. Así se plantea el uso de un analizador de red para comprender el flujo de datos, etc., resultado de lo cual se expondrán las posibilidades que ofrece desde un punto de vista educativo.

1.3 Estructura de la memoria

La presente memoria está dividida en ocho capítulos organizados según el orden seguido durante el desarrollo de este proyecto. La primera mitad del trabajo plantea el marco teórico necesario para comprender el posterior desarrollo práctico. En el segundo capítulo se describe el estándar mundial de telefonía móvil GSM presentando sus características principales, así como su arquitectura y mecanismos de seguridad. El siguiente capítulo introduce, dentro el contexto del sistema GSM, el soporte para tráfico de datos con la tecnología GPRS, así como su evolución para una mejora de los regímenes binarios EDGE. A continuación se presentan los protocolos de transferencia de datos y mensajería de los que se hará uso en el proyecto, a destacar el servicio SMS, describiendo su funcionamiento y ampliando sus clásicas características, y el protocolo *Short Message Peer-to-Peer* (SMPP) dada su estrecha relación con la mensajería.

En el capítulo cinco se contextualiza al lector, presentando un resumen de la evolución histórica de las comunicaciones móviles en España hasta la actualidad y mostrando las tendencias de futuro de las comunicaciones móviles con la aparición de las redes de cuarta generación y la importancia de las plataformas OTA en éstas redes.

Tras lo anterior el proyecto se centra en el despliegue, configuración y evaluación de una picocélula GSM. En este sentido, inicialmente en el capítulo seis se describe el

uso de un analizador de redes GSM y se presenta el análisis de los procedimientos más comunes sobre redes GSM.

El capítulo siete muestra el despliegue de una picocélula GSM/GPRS capaz de ofrecer tanto servicios convencionales de voz y mensajería, como de transmisión de datos de usuario. Las capacidades de mensajería SMS disponibles en esta picocélula serán también explotadas con el fin de gestionar de manera remota los dispositivos conectados a ella.

Para terminar se extraen diversas conclusiones derivadas del desarrollo del proyecto. La implementación de una red de comunicaciones móviles propia ofrece múltiples posibilidades, muchas de las cuales no ha podido explotarse en el presente trabajo. Por esta razón, quedan abiertas varias líneas futuras de investigación y desarrollo.

Capítulo 2

Global System for Mobile Communications

El sistema global para las comunicaciones móviles (GSM) constituye el primer sistema estándar de telefonía digital. Originalmente publicado por el *European Telecommunications Standards Institute* (ETSI), actualmente está bajo el desarrollo del *3rd Generation Partnership Project* (3GPP).

El nombre procede de las siglas del grupo llamado "*Group Special Mobile*" formado en 1982 por la CEPT con el propósito de crear un sistema celular digital Europeo que reemplazase los anteriores sistemas incompatibles entre sí. Cuando el servicio GSM empezó a ofrecerse en 1991, se rehusaron las siglas para denominar así al sistema; "*Global System for Mobile Communications*".

Se trata de un sistema de comunicaciones móviles digitales que proporciona numerosas ventajas frente a los sistemas analógicos precedentes como la aparición de la transmisión de datos, la posibilidad de interconexión con redes telefónicas digitales, la implantación de seguridad mediante el uso de criptografía, una significativa mejora de la calidad del servicio, codificación para el control de errores y técnicas de ecualización, una mayor robustez frente a las interferencias. GSM supone también una mejora en cuanto a la capacidad de la red y el uso del espectro radioeléctrico.

Haremos un repaso por las especificaciones del sistema, en primer lugar sus características físicas recogidas en el estándar ETSI/3GPP TS 45.001 [15] y sus canalizaciones bajo el ETSI/3GPP TS 45.002 [16]. Posteriormente describiremos su arquitectura de red, propia del ETSI/3GPP TS 23.002 [12] para finalizar con ciertos aspectos relativos a su seguridad.

2.1 Interfaz radio

Podemos separar las redes GSM en dos partes principalmente en cuanto a su interfaz física. En primer lugar encontramos el interfaz radio dedicado a la utilización eficiente del espectro radioeléctrico y la división del mismo. Por otro, las conexiones troncales entre los elementos de la arquitectura de red GSM, usualmente cableadas.

2.1.1 Características físicas

El interfaz radio GSM emplea la banda de los 900 Mhz, extendiéndose posteriormente a los 1800 Mhz debido a la saturación de la anterior. Su funcionamiento es similar, con diferencias en cuanto a la propagación de la señal, como una peor penetración en interiores. La ITU estandariza las frecuencias a utilizar por estos sistemas, donde las principales bandas de frecuencias en subida y bajada se muestran en la Figura 2.1. En América GSM opera en 824-849 Mhz / 869-894 Mhz, y en 1850-1910 Mhz / 1930-1990 Mhz. En Asia-Pacífico y África se emplean las mismas bandas que en Europa.

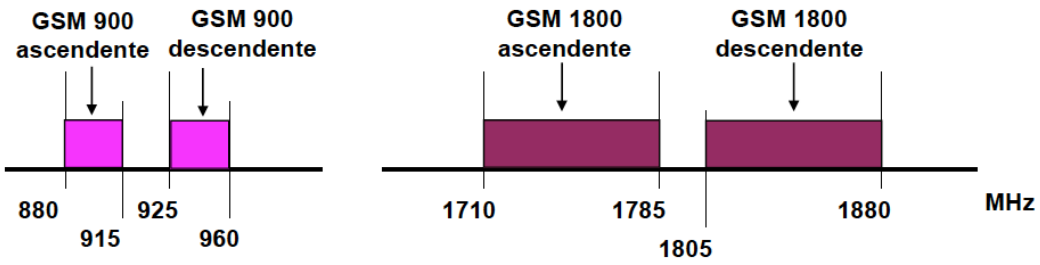


Figura 2.1: Bandas de frecuencia GSM en Europa

Como en toda comunicación inalámbrica, la compartición del medio físico hace necesaria la introducción de técnicas de multiplexación para permitir varias comunicaciones simultáneas y un uso eficiente de las bandas frecuenciales. Son las denominadas técnicas de control de acceso al medio. GSM combina varios esquemas de reparto del espectro radioeléctrico como el duplexado FDD (*Frequency Division Duplex*) o el temporal TDM (*Time Division Multiplex*).

El duplexado en frecuencia FDD separa las bandas de subida y bajada 45 Mhz. Por otro lado el acceso FDMA divide cada banda en canales de 200 kHz llamados *Absolute Radio-Frequency Number* (ARFCN), reservando el canal 0 como banda de guarda con otros sistemas, se presenta en la Figura 2.2 el reparto en los 900 y 1800 Mhz.

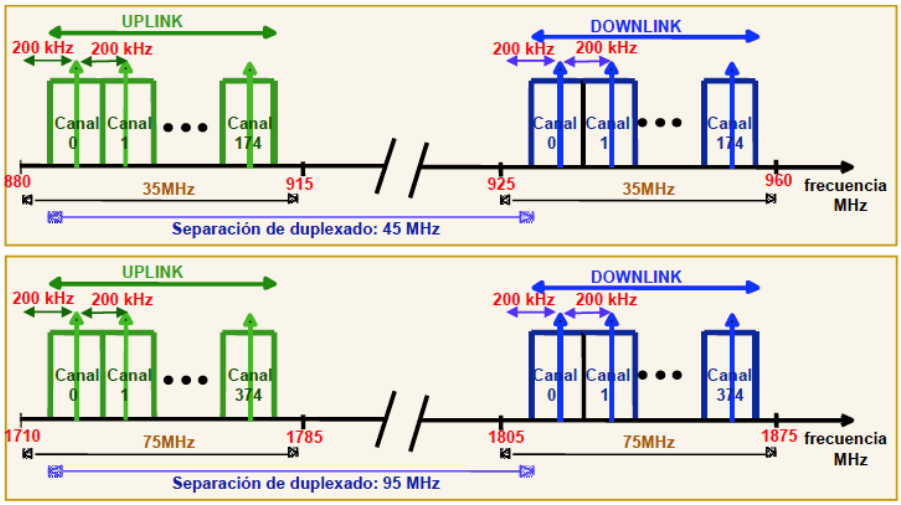


Figura 2.2: Duplexado frecuencial GSM

Cada uno de los canales ARFCN se divide a su vez en ocho ranuras o *slots* temporales TDMA, cada una de las cuales será reservada para un usuario, con un desplazamiento de tres timeslots entre tramas de subida y de bajada. Esta separación temporal es suficiente para permite la sincronización del transceptor y conmutar el comportamiento entre modo transmisión y recepción, gracias a lo cual es posible no tener que usar duplexores en los terminales. La Figura 2.3 y la combinación frecuencial-temporal en la Figura 2.4 representan el comportamiento descrito.

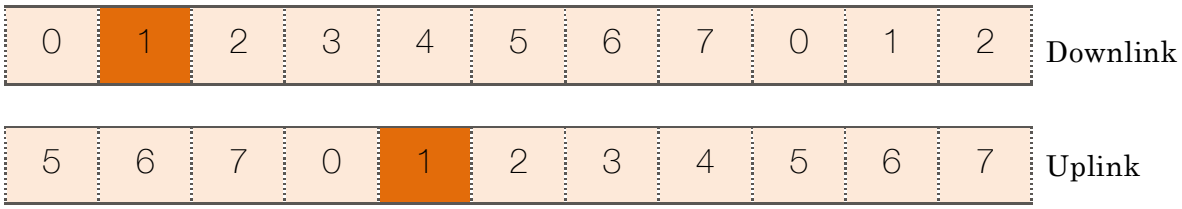


Figura 2.3: Duplexado temporal GSM

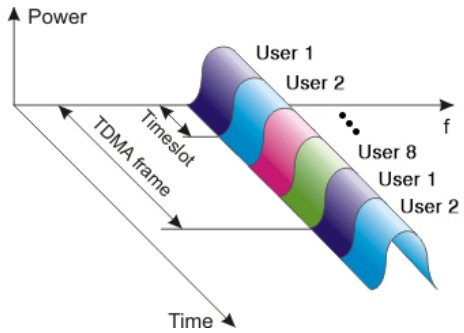


Figura 2.4: Combinación TDMA/FDMA

GSM hereda de la telefonía analógica el esquema de partición celular. Se tesela el territorio en zonas o celdas de tamaño y forma similar (hexagonal por ser la forma que maximiza el reparto repetido de un área), situando la estación base en el centro de ella. A la suficiente distancia, evitando celdas adyacentes, se rehusa el esquema de frecuencias hasta cubrir todo el territorio al que sirva el operador. Cuando existen zonas con una determinada concentración de usuarios, es posible dividir las células en sectores habitualmente de 120º o de 60º con el fin de reducir la relación portadora-interferencia. Se necesitan más antenas por estación base y se incrementa el número de traspasos. En función del tamaño del área de cobertura se pueden definir distintos tipos de células, como se muestra en la Figura 2.5:

- Macrocélula: radios entre 1.5 y 20 km, zonas rurales de poca densidad.
- Minicélula: radios entre 0.5 y 1.5 km, zonas urbanas de densidad media.
- Microcélula: radios entre 0.2 a 0.5 km, zonas urbanas de densidad alta.
- Picocélula: radios menores de 250m, zonas interiores de mucha densidad.
- Femtocélula: radios menores de 100m, zonas interiores; hogares y negocios.

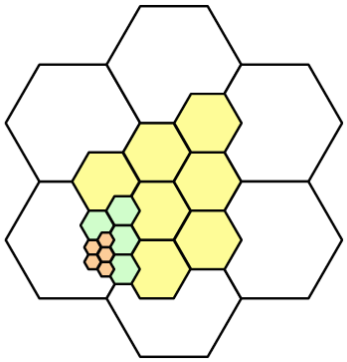


Figura 2.5: Esquema de partición celular

La división espacial en células comentada hace necesario un mecanismo para la transferencia de llamadas en curso cuando se desplaza el móvil. Este traspaso (*hand-over*) puede darse hacia una nueva célula (*inter-cell)* o a otro canal de la misma estación base (*intra-cell*) en función de los parámetros de calidad del servicio.

Cada ARFCN ocupa dispone de un régimen binario de 270,833 kbps utilizando modulación digital *Gaussian Minimum Shift Keying* (GMSK), por lo tanto la velocidad bruta de transmisión para cada usuario es 33,854 kbps (270,833 kbps / 8 u.). No obstante, la velocidad útil baja hasta los 24,7 kbps, debido al overhead de señalización. Agrupando varios canales temporales se forman los canales lógicos. Estos pueden agruparse en dos tipos según el tipo de información que portan en canales lógicos de control y canales lógicos de tráfico

2.1.2 Canales lógicos de control

Cada canal de control consiste en varios canales lógicos distribuidos en el tiempo para proporcionar funciones de control. Los canales de bajada *Broadcast Channels* (BCH) y *Common Control Channels* (CCCH) se implementan en los slots 0 de ciertos ARFCN. Los dedicados *Dedicated Control Channels* (DCCH) se pueden enviar en cualquier slot temporal y en cualquier trama. Veamos dichos canales en profundidad:

- BCH: los canales de difusión operan en el downlink de un ARFCN dado dentro de cada celda. Proporcionan sincronización a los terminales y en ocasiones son monitorizados por los terminales de celdas vecinas para recibir medidas de potencia y tomar decisiones de *handover*. Los otros siete slots de la trama del mismo ARFCN quedan disponibles para datos. Se definen tres tipos de canales BCH:

  - BCCH (*Broadcast Control Channel*): canal de control de broadcast: proporciona identificación y características operativas de la celda y de red.
  - FCCH (*Frequency Correction Channel*): canal corrector de frecuencia: permite sincronizar la frecuencia interna de cada terminal a la de la red.
  - SCH (*Synchronization Channel*): canal de sincronización: identifica a la estación base en servicio portando el código *Base Station Identity Code* BSIC.

- CCCH: los canales de control comunes ocupan el slot 0 de cada trama que no esté ocupada por un BCH o una trama idle. Los CCCH son los canales más frecuentes entre las señales de control y se utilizan para buscar a los terminales, asignar canales de señalización y recibir contestaciones de los móviles. De nuevo se pueden dividir en:

  - PCH (*Paging Channel*): canal de búsqueda; proporciona señales de búsqueda a los terminales bajo una celda y avisa en caso de llamada procedente de la RTC.
  - RACH (*Random Access Channel*): canal de acceso aleatorio; es un canal de subida utilizado por el móvil para confirmar una búsqueda iniciada por un PCH.
  - AGCH (*Access Granted Channel*): canal de acceso garantizado; proporciona el enlace estación base-terminal, es decir, el canal físico (time-slot y ARFCN).

- DCCH (*Dedicated Control Channels*): los canales de control dedicados son bidireccionales, su formato y función es independiente del sentido. Los SDCCH proporcionan señalización bajo demanda de los usuarios y los SACCH y FACCH supervisan las transmisiones de datos durante una llamada.

  - SDCCH (*Slow Dedicated Control Channel*): canal de control dedicado independiente; creado por la estación base justo antes de la conexión con el móvil, asegura el mantenimiento del enlace, verifica y alerta al abonado.
  - SACCH (*Slow Associated Control Channel*): canal de control asociado lento; lleva información general entre terminal y estación base, instrucciones de potencia a transmitir, temporización, calidad del TCH, medidas BCH de celdas vecinas.
  - FACCH (*Fast Associated Control Channel*): canal de control asociado rápido; contiene mensajes urgentes cuando no se ha dedicado un SDCCH para un usuario. Gana tiempo de acceso a un slot robando tramas del canal de tráfico en uso gracias a la activación de los "*stealing bits*" de una ráfaga TCH; al activar dichos bits, el slot contiene datos FACCH en lugar de tráfico en esa trama.

2.1.3 Canales lógicos de tráfico

Los canales de tráfico pueden llevar voz digitalizada o datos de usuario. Se establecen dos velocidades de transmisión, que definen cómo los datos se encapsulan en las diferentes tramas. Así, Cuando se transmite a velocidad completa (*full-rate*), los datos viajan en un slot de la trama, mientras que si transmitimos a velocidad mitad (*half-rate*) el mismo slot temporal se comparte por dos comunicaciones diferentes.

Cada trece tramas *Traffic Channel* (TCH) se envía un SACCH *idle*. Se define una multitrama MF26 como la agrupación de 26 tramas TCH. Así resulta que empleando TCH/F se logran tasas de usuario de hasta 9,6kbps, por los 4,8kbps en modo TCH/H.

2.1.4 Ráfagas GSM

Las ráfagas constituyen la unidad básica de transferencia de información en GSM, pueden tener uno de los siguientes cinco formatos definidos en el estándar. Cada ráfaga es emitida durante el slot temporal asignado. La ráfaga normal se emplea en transmisiones TCH y DCCH en bajada y subida. Las ráfagas de corrección de frecuencia y de sincronización se utilizan en el slot cero de las tramas específicas para enviar mensajes de control de frecuencia y temporización en sentido descendente. La ráfaga de acceso es utilizada por todos los terminales móviles para acceder al servicio y la ráfaga muda rellena los slots inutilizados.

Como se menciona anteriormente, a la agrupación de veintiséis tramas se le denomina multitrama en el caso de canales dedicados de tráfico (MF26) con una duración de 120 ms. En el caso de portar canales de señalización y control, la multitrama (MF51) consta de 51 tramas, valor sin divisor común con las 26 de tráfico, con el fin de que los móviles puedan escuchar los canales SCH y FCCH de las celdas adyacentes, necesarios para realizar traspasos entre celdas. Ambas formaciones de multitramas siguen ciclos en paralelo sobre una estructura superior denominada supertrama. El nivel superior de la jerárquia TDMA lo forma la hipertrama GSM, formada por 51 multitramas de tráfico y 26 de control con una duración aproximada de tres horas y media. En la Figura 2.6 se muestra la estructura jerárquica de organización de envío de la información en GSM, así como la duración temporal de las distintas estructuras.

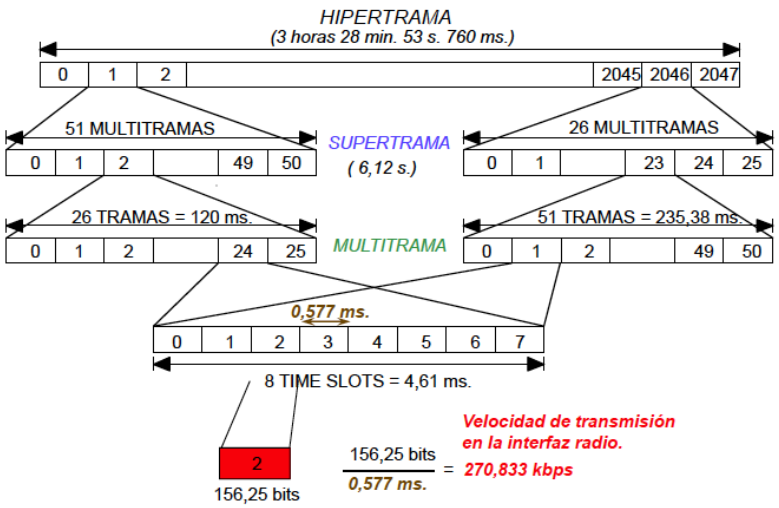


Figura 2.6: Estructura jerárquica TDMA

2.2 Arquitectura de red

La arquitectura de la red GSM, tal y como define el ETSI/3GPP TS 23.002 [12] se puede dividir en cuatro subsistemas con funciones definidas dentro de la red: *Base Station Subsystem* (BSS), *Network Station Subsystem* (NSS), *Operation and Support Subsystem* (OSS) y *Mobile Station* (MS). Cada uno engloba a su vez otros elementos con sus propias funcionalidades como se observa en la Figura 2.7. A continuación se describe cada uno de ellos en mayor detalle.

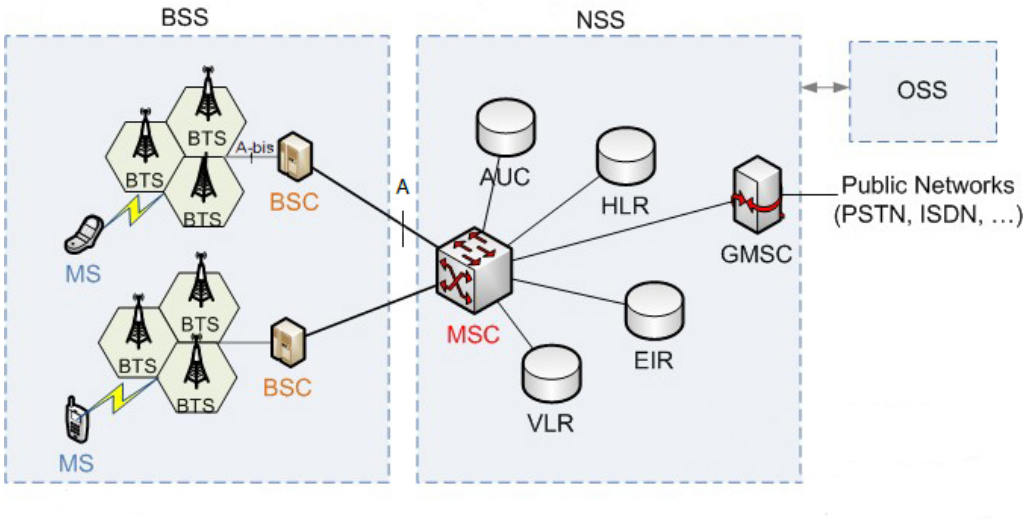


Figura 2.7: Arquitectura de red GSM

2.2.1 Estación móvil

La estación móvil proporciona el acceso del usuario a la red GSM y es anónima hasta que se personaliza con la inserción de una tarjeta inteligente SIM que aloja la información necesaria para identificar al usuario en la red. Esta separación entre terminal y usuario aumenta la movilidad personal, pues en la definición del acceso a los servicios es independiente del terminal que se emplee para acceder a ellos.

La tarjeta SIM contiene, además de la identidad del abonado o *International Mobile Subscriber Identity* (IMSI), los datos de configuración para el acceso a la red, incluyendo las claves y algoritmos criptográficos necesarios para garantizar la autenticación y cifrado de las comunicaciones. Adicionalmente, puede alojar información de los contactos de usuario, sus mensajes SMS, etc. En la Tabla 2.1 se muestran algunos de los códigos que permiten la identificación del usuario y de la red.

Las capacidades de la SIM incluyen la posibilidad de almacenar y ejecutar aplicaciones de diversa índole como veremos más adelante, recogidas en el ETSI/3GPP TS 11.14 [8] referente al uso de la interfaz entre el terminal y la tarjeta SIM. Pudiendo utilizar aplicaciones alejadas del propósito principal de ésta en la red GSM. Así, por ejemplo, puede almacenar aplicaciones de pago, de firma electrónica, etc.

Tabla 2.1: Códigos contenidos en la tarjeta SIM

Código	Nombre	Descripción
PIN	Personal Identification Number	Consta de 4 dígitos que se deben introducir antes de usar el terminal
PUK	PIN Unblocking Key	Desbloquea el terminal en caso de introducir el PIN erróneamente 3 veces, consta de 8 dígitos
IMSI	International mobile Subscriber Identity	Identificador del usuario
Ki	Authentication Key	Código de 16 bits empleado en la autenticación de las tarjetas en la red
MCC	Mobile Country Code	Código del país donde se encuentra la red
MNC	Mobile Network Code	Código del operador que gestiona la red

2.2.2 Subsistema de estación base

Agrupa la infraestructura relativa a los aspectos celulares de GSM. Se encuentra en contacto directo con las estaciones móviles a través de la interfaz radio y por otro lado conectado a los conmutadores del NSS. Se compone de dos partes: las estaciones base o *Base Transceiver Stations* (BTS) y las controladoras de éstas o *Base Station Controller* (BSC). Las interfaces de conexión, como se representa en la Figura 2.7, son por un lado la "Um" que habilita el dialogo de las BTS con los terminales, y por otro la interfaz "A" que conecta el BSC con la MSC. El interfaz entre BSC's y BTS se denomina "Abis", sin tener nada que ver con la interfaz "A".

Las BTS contienen los dispositivos de transmisión y recepción radio, incluyendo las antenas, elementos de conexión, y las instalaciones accesorias como la torre de soporte, pararrayos, tomas de tierra, etc. Se pueden considerar complejos modems radio con funciones como la formación del múltiplex GSM, la realización de medidas de la señal radio procedente del móvil, la gestión de la sincronización temporal *time advance* y es responsable de la operación y el mantenimiento del enlace.

El segundo componente más importante del subsistema de estación base es el controlador BSC, que gestiona y controla por comando remoto las BTS. En esencia se pueden considerar conmutadores con gran capacidad de cómputo, cuyas funciones principales son la asignación de los canales radio a los usuarios, la gestión de los traspasos *handovers*, el control de la potencia y la detección de silencios.

Otro componente importante del BSS, es la *Transcoding and Rate Adaptor Unit* (TRAU), equipo que realiza la codificación de la voz, así como la adaptación de velocidades del interfaz radio GSM (13 kbps) al formato empleado en la *Red Telefónica Conmutada* (RTC) de 64 kbps. Puede estar localizado en la BTS, BSC o MSC.

2.2.3 Subsistema de red y conmutación

El NSS es el encargado de la conmutación en GSM y de la gestión de los datos de usuarios. Gestiona también las comunicaciones entre usuarios de la red GSM, tanto dentro de la propia red de un determinado operador como hacia los pertenecientes a redes de otros operadores. La conexión con redes fijas externas requiere de una pasarela o g*ateway* que posea las funciones de *interworking* o traducción.

Se pueden considerar dos grandes funcionalidades en su operativa. Por un lado las asociadas a la provisión del servicio básico, entre las que estarían la gestión de llamadas, la autenticación de la identidad del usuario, las llamadas de emergencia, los servicios suplementarios, los servicios de mensajería (SMS) y la confidencialidad de los elementos de información de señalización. Por otro lado, se consideran las funciones que habilitan la operación entre celdas, como el registro de posición, los procedimientos mediante los cuales las bases de datos *Home Location Register* (HLR) y *Visitor Location Register* (VLR) guardan de forma actualizada la posición de los terminales, los traspasos y restablecimiento de llamadas. El NSS hace uso del sistema de señalización por canal común del CCITT nº 7 (SS7, *Signalling System N. 7*).

Como se observa en la Figura 2.7, existen dos tipos de centrales de conmutación dentro del subsistema de conmutación, *Mobile Switching Center* (MSC) y *Gateway Mobile Switching Center* (GMSC). La primera es la central de conmutación propia de la subred del operador, que controla varias BSC. Además es la encargada de coordinar el establecimiento y encaminamiento de llamadas hacia o desde el exterior. Por su parte, la GMSC conecta la red del operador con otras redes, sirviendo como puerta de enlace.

Además de los conmutadores MSC y GMSC, el NSS incluye las bases de datos en las que se almacena la información relativa a los usuarios o abonados. La información del abonado relativa al suministro de los servicios contratados se encuentra en el HLR, independientemente de la posición actual del abonado. El HLR cuenta con una subdivisión funcional importante que es el *Authentication Center* (AuC), encargado de la gestión de la seguridad de los abonados. El encargado del almacenamiento temporal de los datos para los usuarios bajo el área de servicio de un determinado MSC es el VLR. Se trata de bases de datos distribuidas repartidas estratégicamente para controlar de forma eficiente la información de los usuarios.

2.2.4 Subsistema de operación y mantenimiento

Engloba los mecanismos y equipos que velan por el correcto funcionamiento de la red y sus servicios. Implementa los procedimientos que permiten modificar parámetros de configuración en tiempo real para prevenir y reparar comportamientos anómalos del sistema. Las redes GSM han crecido mucho desde su implementación y es vital disponer de una plataforma de gestión remota para poder gestionar redes de grandes dimensiones. Existen tres dominios de gestión para cada uno de los equipos gestionados:

- Centro de Operación y mantenimiento: Se trata de la interfaz mediante la cual el humano puede interactuar con el sistema para modificar parámetros, monitorizar los recursos...

- Control de la subscripción: Contempla la gestión de los datos de abonado así como la tarificación. El estándar no es nada específico en este apartado y los operadores pueden decidir su forma de implementación.
- Operación y mantenimiento: Engloba todas las funciones que se pueden realizar sobre la red y su configuración así como la gestión de las estaciones de base y los equipos electrónicos presentes en la infraestructura de red.

2.3 Seguridad

Los conceptos de seguridad para las comunicaciones y terminales móviles son de vital importancia dada su naturaleza inalámbrica. Aunque GSM se desarrolló en la década de los ochenta, se tomaron en cuenta potenciales riesgos de seguridad en vista de dotar al sistema de la robustez necesaria durante varios años. Sin embargo, a pesar de las precauciones tenidas durante la fase de especificación, actualmente, gracias a la evolución tecnológica, han aparecido varias brechas de seguridad en sistemas GSM.

2.3.1 Autenticación

La autenticación es necesaria para evitar que personas no autorizadas sean capaces de hacer uso de los servicios de la red GSM. El proceso de autenticación se lleva a cabo después de que la red tenga conocimiento del IMSI o del *Temporal Mobile Subscriber Identifer* (TMSI) del móvil y antes de que el canal esté cifrado. En GSM la red autentica al terminal móvil, pero dicha autenticación no es mutua, lo que puede dar lugar a posibles ataques con estaciones base falsas.

El flujo de mensajes intercambiados consiste en el envío un número aleatorio *RAND* de 128 bits al terminal, pidiendo la devolución de la respuesta firmada *SRES*, resultado de aplicar el algoritmo "A3" a los parámetros *RAND* y *Ki*. La respuesta firmada también podría ser igual a los primeros 32 bits del algoritmo *COMP128* que se ejecuta en la tarjeta SIM. Cuando el MSC recibe la respuesta de la MS, calcula la respuesta firmada correcta y comprueba que sea igual a la enviada por el terminal, en caso afirmativo, el terminal está autenticado. La robustez de la autenticación reside por tanto en el secreto de la clave *Ki*, siendo imposible derivarla partir de una o varias parejas (*RAND, SRES*).

Como estándar mundial, uno de los requerimientos de GSM era una alta flexibilidad, así puede darse el caso de que una MS necesite autenticarse con una red desconocida, el proveedor de la red no conocerá en ese caso el secreto *Ki* por lo que no sería posible autenticar a la SIM. Para solucionar esto, GSM define las tripletas, con lo que cualquier SIM es capaz de autenticarse ante cualquier red. Una tripleta valida consiste en el reto *RAND*, la respuesta firmada SRES y una clave de sesión *Kc*, el procedimiento es igual al caso anterior, con la única introducción del algoritmo "A8" para el cálculo de *Kc* como podemos observar en la Figura 2.8.

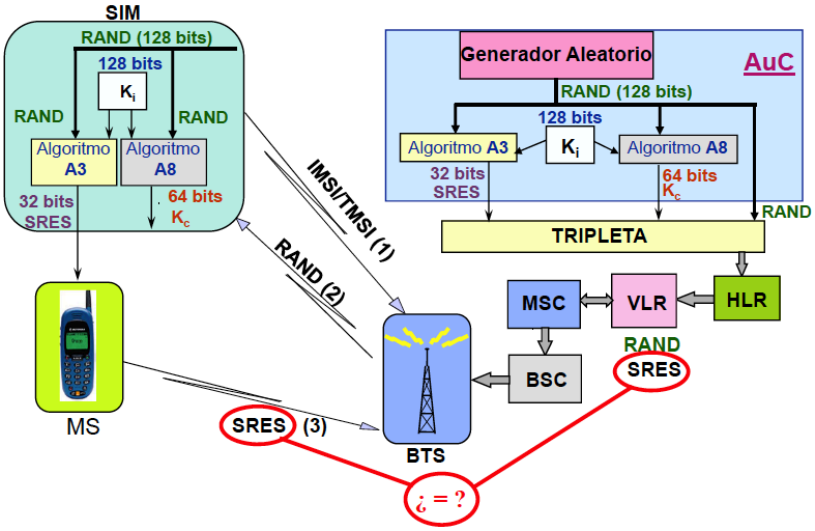


Figura 2.8: Proceso de Autenticación

2.3.2 Confidencialidad

Puesto que la transferencia de datos se realiza a través de un canal de comunicaciones compartido, es necesario cifrar los datos para dotar de confidencialidad a las comunicaciones. GSM define varios algoritmos para ello. El método de cifrado se realiza bit a bit en bloques de 114 bits; es decir, lo que se transmite por la interfaz radio es el resultado de aplicar el algoritmo "A5/X" a la información que se quiere transmitir. En el proceso interviene la clave de cifrado *Kc* y el número de trama *FN*. La X de "A5/X" puede tomar valores de 1 a 7, dando lugar a 7 algoritmos diferentes, de los cuales "A5/1" y "A5/2" son obligatorios. La clave no se transmite directamente por la interfaz radio. Tal como se ha visto, dentro de la red es el AuC el que la calcula utilizando *RAND*, *Ki* y el algoritmo "A8", a la vez que calcula los parámetros necesarios para la autenticación. Los algoritmos "A5/1" y "A5/2" se almacenan en el equipo terminal, no en la SIM. El móvil guarda la clave *Kc* en la SIM hasta que se actualice en la siguiente autenticación. Durante un traspaso la clave *Kc* no cambia.

2.3.3 Anonimato

En la red GSM a veces es necesario pedir al móvil que se identifique, para lo que éste debe enviar determinados parámetros que permitan su identificación, como el IMSI o el IMEI. El procedimiento de identificación es necesario en determinadas ocasiones, pero supone una brecha de seguridad en el sistema al transmitir elementos como el IMSI. Con objeto de evitar que un intruso pueda saber qué móvil está accediendo a la interfaz radio con sólo escuchar la información intercambiada, el IMSI se cifra y se intenta evitar su transmisión en la medida de lo posible. Para ello, se utiliza el TMSI Éste sólo tiene validez dentro de un área de localización, por lo que es necesario que vaya acompañado siempre del *Location Area Identity* (LAI), para evitar ambigüedades. Así, cuando un VLR recibe de un móvil un TMSI y un LAI y ve que el LAI no es de su zona de influencia, le asigna un nuevo TMSI. Cuando el móvil lo recibe, reemplaza al anterior y lo guarda junto con el nuevo LAI en una memoria no volátil (en la SIM) de forma que estos datos no se pierdan al apagar el móvil. Los VLR siempre guardan la relación entre el IMSI y el TMSI que han asignado.

Capítulo 3

General Packet Radio System (GPRS)

Con la aparición de las redes de transmisión de datos y el auge de Internet aparece la necesidad de transmitir datos de manera inalámbrica. De manera paralela se produjo un crecimiento increíble en el número de usuarios tanto de Internet como de las redes móviles GSM, era por tanto inevitable la convergencia de ambas tecnologías. Los usuarios de redes móviles comenzaban por tanto a requerir acceso a la información desde cualquier lugar.

Los servicios de datos que la tecnología GSM proporciona son altamente ineficientes y costosos, dado que se trata de una transmisión mediante conmutación de circuitos donde un usuario ocupa en exclusiva el canal todo el tiempo que la sesión permanece activa. La facturación del servicio se realiza en función de la duración de dicha sesión y no considerando el volumen de datos intercambiado. Además, existen otras limitaciones como la tasas de transferencia de tan sólo 9,6 kbps y tiempos de establecimiento altos de entre 15 y 30 segundos.

La solución pasaba por una transición hacia tecnologías de transmisión que empleasen conmutación de paquetes. El uso de la conmutación de paquetes permite una compartición eficiente de los recursos radio, ya que los usuarios sólo hacen uso de la red cuando estén transmitiendo o recibiendo paquetes, dejando el canal inactivo libre para ser utilizado.

El retraso en el despliegue de redes de tercera generación y la búsqueda de nuevos servicios con los que continuar rentabilizando las redes disponibles favorecieron la aparición de tecnologías de transición basadas en GSM que, con pequeñas modificaciones en la red ya utilizada, permitiesen mejorar los servicios de transmisión de datos. Una primera mejora aparece con las especificaciones del ETSI 3GPP TS 22.034 [13] y 23.034 [14] las cuales definen los requerimientos necesarios para utilizar la tecnología *High Speed Circuit Switched Data* (HSCSD) en redes GSM. HSCSD aumenta la velocidad de transmisión de los datos hasta velocidades de 57,6 kbps aplicando técnicas de agregación de hasta cuatro time-slot para un único usuario. También empleando más bits para información de usuario perdiendo capacidad de corrección de errores. La implementación de esta solución requería únicamente ciertas actualizaciones de software y hardware.

En 1997, a raíz del proceso de mejora de GSM denominado *GSM Phase 2+* se publica el estándar *General Packet Radio System* (GPRS), bajo las especificaciones ETSI EN 301 113 [17] y ETSI EN 301 344 [18]. También es llamado en ocasiones GSM-IP, por su integración con las redes Internet y el uso de la pila TCP/IP en la red troncal. La tecnología GPRS representa un paso más en el uso de los servicios de transferencia de datos. Permite a los usuarios móviles enviar y recibir datos en modo paquete bajo demanda, habilita la tarificación por volumen de datos transferidos y no por tiempo de conexión y puede diferenciar a los distintos usuarios móviles mediante la asignación de diferenciadas calidades de servicio (QoS, *Quality of Service*) en función del caudal medio o pico del enlace, los retardos y la fiabilidad.

GPRS proporciona tasas de transmisión de datos variables gracias al uso de la transmisión multislot y a cuatro nuevas codificaciones de canal: CS-1: 9,05 kbps, CS-2: 13,4 kbps, CS-3: 15,6 kbps, CS-4: 21,4 kbps. Así por ejemplo, usando varios slots de una misma portadora y empleando CS-4 se alcanza una velocidad máxima teórica de 171,2 kbps (21,4 kbps x 8 slots).

3.1 Características físicas

El acceso al canal en GPRS se basa en sesiones de transferencia de datos definidas entre el móvil y la *Packet Control Unit* (PCU) denominados *Temporary Block Flow* (TBF). Los paquetes de un TBF se segmentan, codifican y transforman en bloques *Radio Link Control* (RLC), formados por cuatro ráfagas transmitidas en el timeslot asignado en cuatro tramas sucesivas. Los slots se asignan dinámicamente según las necesidades, pudiendo ser multislot, y por separado para cada sentido, pudiendo establecer conexiones asimétricas idóneas para tráfico web. El canal de bajada utiliza una cola FIFO para los paquetes en espera, mientras que el canal de subida utiliza un esquema de contención similar al Aloha ranurado (Roberts, 1972). Cada TBF se marca con un identificador temporal llamado *Temporal Frame Identity* (TFI), que se usa en recepción para relacionar los datos con el usuario.

En GPRS se define el canal físico sobre el que se trasladarán los canales lógicos como *Packet Data Channel* (PDCH). Un PDCH actúa como mínimo como maestro *Master Packet Data Channel* (MPDCH) pudiendo servir como *Packet Common Control Channel* (PCCCH) encargado de toda la señalización de control necesaria para iniciar la transmisión de paquetes, como señalización dedicada o como datos de usuario. El resto actúan como esclavos *Slave Packet Data Channel* (SPDCH) y son usados para transmitir datos de usuario. El operador es capaz de decidir en tiempo real si dedica algunos PDCH para tráfico GPRS y cambiar el número de PDCHs, introduciendo el concepto de "*Capacity-on-demand*".

Los canales lógicos en GPRS son los mismos que en el sistema GSM con la adición de los canales dedicados. En la Tabla 3.1 se recogen los nuevos canales.

Tabla 3.1: Canales lógicos GPRS

Grupo	Canales	Nombre	Función
PBCCH	PBCCH	Packet Broadcast Control Channel	Broadcast
PCCCH	PRACH	Packet Random Access Channel	Acceso
	PPCH	Packet Paging Channel	Búsqueda
	PAGCH	Packet Access Granted Channel	Conceder acceso
	PNCH	Packet Notification Channel	Notificaciones
PTCH	PDTCH	Packet Data Traffic Channel	Datos
	PACCH	Packet Associated Control Channel	Control
	PTCCH	Packet Timing-Advance Control Channel	Sincronización

3.2 Arquitectura de red

Puesto que GPRS es el resultado de la evolución de GSM, comparte la arquitectura de la red de acceso con dicho sistema. La MS, que desee acceder al sistema deberá soportar esta tecnología. Se introducen dos nuevos nodos en la parte troncal de la red NSS, como comprobamos en la Figura 3.1.

En primer lugar, el *Gateway GPRS Support Node* (GGSN), actuando como interfaz lógico hacia el resto de redes de datos, se encarga de gestionar el mapeado de direcciones necesario para realizar el encaminamiento de los paquetes entre el terminal y las redes externas. El enrutamiento interno dentro de la red GPRS se realiza mediante túneles entre nodos; por una parte se establece un túnel entre el móvil y el *Serving GPRS Support Node* (SGSN) y por otra entre el SGSN y el GGSN que prestan servicio a la comunicación.

El segundo elemento es el SGSN encargado de la entrega y recepción de paquetes al terminal móvil bajo su área de servicio. Sus funciones son el control de acceso al sistema, lo que incluye la seguridad, y la localización de los terminales dentro de la red. A través de la interfaz "*Gbis*" se comunica con el BSS posibilitando el diálogo con el terminal. Cuando éste desea acceder a los servicios GPRS se inicia el procedimiento *GPRS Attach*, que tiene como resultado la creación del contexto entre el SGSN y el terminal, listo para iniciar conexiones y se mantendrá localizado.

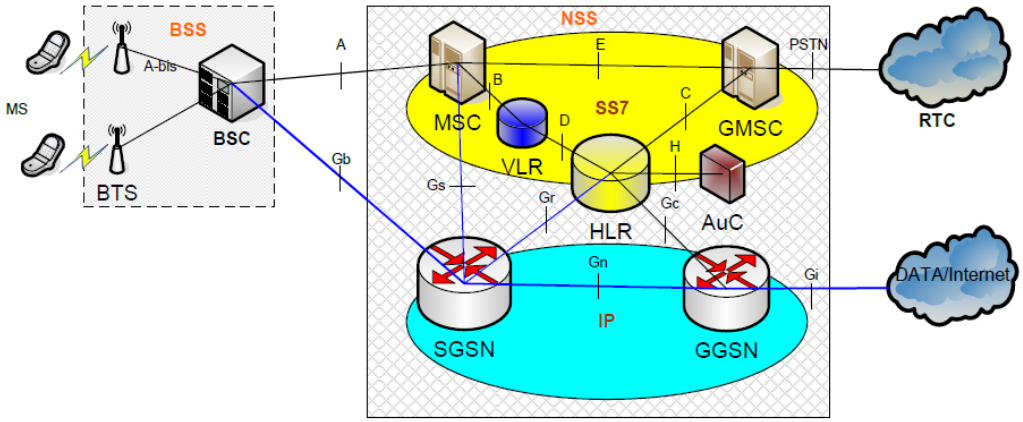


Figura 3.1: Arquitectura de red GPRS

3.3 Arquitectura de Protocolos

El modelo de protocolos de GPRS se divide en dos planos: el de transmisión, mostrado en la Figura 3.2, encargado de la transferencia de los datos de usuario, el control de flujo y de errores de los mismos. Y el de señalización, utilizado para el control y soporte de las funciones del plano de transmisión.

3.3.1 Plano de transmisión

La capa física puede ser dividida en la subcapa de RF, equivalente a la capa radio de GSM, y la subcapa de enlace físico, que representa el propio enlace entre MS y la red. A nivel dos, la capa MAC maneja la asignación de canales y la multiplexación, en unión con la capa RLC, que provee un enlace radio fiable a las capas superiores. Soporta modos de transferencia, reconocidos y no reconocidos.

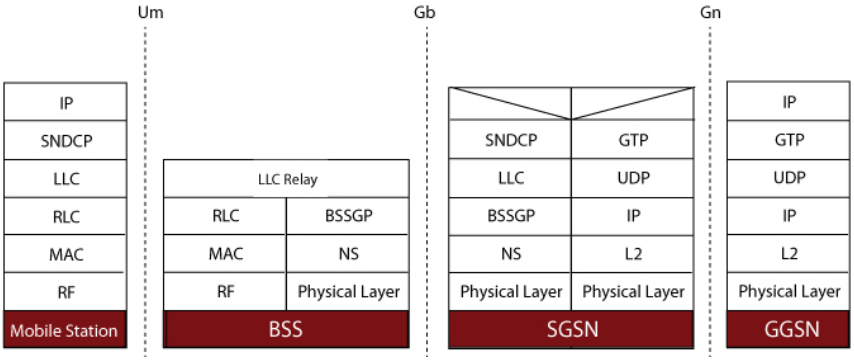


Figura 3.2: Plano de transmisión GPRS

La capa *Logical Link Control* (LLC) ofrece un enlace lógico, seguro y fiable entre el terminal y el SGSN, independientemente de las capas superiores. El protocolo *Subnetwork Dependent Convergence Protocol* (SNDCP) es el encargado de facilitar la entrega de los paquetes, multiplexando conexiones de nivel de red de una gran variedad de protocolos sobre la capa de LLC. También realiza compresión y descompresión de los datos.

El *GPRS Tunneling Protocol* (GTP) es el encargado de transportar paquetes de usuario y las señales de control asociadas a ellos entre los nodos de soporte de la red GPRS, es decir, entre el SGSN y el GGSN, permitiendo al SGSN activar el contexto *Packet Data Protocol* PDP. Los paquetes GTP contienen protocolos de niveles superiores como Internet Protocol IP, y utiliza como protocolo de transporte *User Datagram Protocol* (UDP).

El protocolo *Base Station System GPRS Protocol* (BSSGP), transfiere información de control y señalización entre el BSS y SGSN en la interfaz *Gb*. Su función principal es proveer información sobre la calidad del servicio y enrutamiento entre el BSS y SGSN.

3.3.2 Plano de señalización

En el plano de control, la señalización se transfiere a través de una conexión *Signalling Connection Control Part* (SCCP) en la interfaz "*Iu*". La capa *Radio Resource Control* (RRC) maneja las funciones de establecimiento, mantenimiento y liberación de las conexiones entre los terminales y el BSS, de manera análoga al sistema GSM. Se introduce la capa *GPRS Mobility Management and Session management* (GMM), encargada de la gestión de los registros de terminales en la red GPRS, la seguridad, la activación y desactivación de los contextos PDP, y las actualizaciones de los áreas de enrutamiento (RA, *Routing Areas*)

3.4 Gestión de la movilidad

La gestión de la movilidad la lleva a cabo el SGSN quien asigna el *Packet TMSI* (P-TMSI), cuya función es similar a la del TMSI para las conexiones de voz. También se define el RA como un subconjunto del área de localización (LA). Cada RA es gestionada por un sólo SGSN. Cuando el móvil está en reposo, el SGSN debe conocer en qué RA se encuentra. En este sentido, el HLR conoce sólo el SGSN que sirve al

móvil y no la RA. La gestión de la movilidad incluye los procedimientos de registro o *Attach*, desconexión o *Detach* y actualización de la posición o *Location Update*.

3.5 Enrutado de los paquetes

Las unidades de información, conocidas como paquetes, se conocen como *PDP PDU*. Después de un *GPRS Attach* se establece lo que se denomina un contexto PDP entre el terminal y GGSN, o lo que es lo mismo, una sesión entre ambos donde el terminal está preparado para recibir o enviar datos y el GGSN monitoriza el terminal para que pueda hacerlo. Entre el terminal y el SGSN se utiliza el protocolo GTP para transferir la información a través de túneles, separando de esta forma las comunicaciones de los diferentes servicios. Los elementos SGSN y GGSN, en esencia actúan como routers que reciben paquetes por uno de sus puertos o enlaces y los envían por la salida correspondiente. Si éste reenvío no es posible cuentan además con *buffers* que permiten el almacenamiento de paquetes hasta que puedan ser reenviados.

3.6 Enhaced Data Rates for GSM Evolution (EDGE)

En 1999 se lanza la especificación de una nueva mejora sobre GSM/GPRS, denominada *Enhaced Data Rates for GSM Evolution* (EDGE), con la que proporcionar mayores regímenes binarios. Su bajo coste y facilidad de implementación hace que la mayoría de operadores opte por disponerla en sus estaciones base como mejora de GPRS en zonas con poco tráfico de datos, y como solución de apoyo en otras.

La tecnología EDGE (EGPRS) incluye algunas modificaciones en la interfaz radio de GPRS para aumentar la tasa de transmisión. En cuanto a la modulación, además de GMSK se incluye 8-PSK, lo que permite triplicar la tasa de transmisión bruta en el aire. En total, se definen 9 combinaciones de modulación y codificación de canal (MCS, *Modulation and Coding Scheme*) que se eligen adaptativamente según las condiciones del canal. Dependiendo del MCS seleccionado, se pueden conseguir tasas de transmisión de entre 8,8 y 59,2 kbps por timeslot utilizado (lo que supone un máximo teórico de 473,6 kbps si se utilizan los ocho timeslots de una portadora). Se introducen asimismo nuevos mecanismos de control de errores como ARQ (HARQ: Hybrid ARQ) o FEC (*Forward Error Correction*), este último basado en la transmisión de redundancia incremental (en lugar de retransmitir los paquetes erróneos, se transmiten más bits de redundancia para intentar corregir los errores del paquete transmitido inicialmente). Existen propuestas de mejora de EDGE, como Evolved Edge, que introducen modulaciones 16QAM y 32 QAM, o la posibilidad de que el móvil pueda duplicar la tasa de transmisión mediante el empleo de varias portadoras.

Capítulo 4

Mensajería

Definido como la información que un emisor envía al receptor a través del canal de comunicaciones; el mensaje es en el sentido más general, el objeto de la comunicación entre dos entidades. Cualquier información que pueda representarse de forma binaria, ya sea texto, o un paquete de datos, puede considerarse un mensaje.

Uno de los servicios más extendidos de entre los que ofrece el sistema GSM, es sin duda, el servicio de mensajes cortos (SMS, *Short Message Service*). La popularidad del mismo se vió reducida con la aparición de soluciones de mensajería basadas en el tráfico de datos. Aún con la actual disminución de su uso, continuan siendo importantes para otros casos de uso, como veremos durante el capítulo. También se presentará un protocolo de mensajería, (SMPP, *Short Message Peer-to-peer Protocol)*, muy utilizado sobre clientes de mensajería en la red fija.

4.1 Short Message Service (SMS)

El servicio SMS representa una sencilla vía de comunicación no orientada a conexión entre teléfonos móviles y/o terminales fijos. Los conceptos iniciales fueron desarrollados en 1984, con la idea de transmitir información en los canales de señalización necesarios para GSM. Como las llamadas sólo hacen uso de canales de tráfico, hacer uso de los canales de señalización para transmisión de texto durante la llamada optimiza la utilización del sistema, pues permite recibir un mensaje mientras el usuario realiza una llamada. Bajo estas condiciones, la longitud máxima del mensaje a transmitir es se reduce a 128 caracteres, cifra que posteriormente se extendió hasta los 140, si se emplea un alfabeto de 8 bits, o 160 utilizando el alfabeto de 7 bits.

En 1993 fué implantado comercialmente en Finlandia y lanzado como parte de las especificaciones *GSM phase 2* del ETSI 3GPP TS 03.38 [1] y 03.40 [2]. Una importante ventaja frente a las tecnologías predecesoras; como los mensáfonos, es que el proceso de mensajería es no orientado a conexión. En caso de que el mensaje a transmitir supere la longitud máxima establecida, éste se puede fragmentar siendo recuperados de forma ordenada en recepción con la ayuda del software del teléfono.

El servicio SMS ha sido muy exitoso desde su introducción, siendo reemplazado en la actualidad por las aplicaciones de mensajería instantánea. No obstante, los SMS siguen teniendo un gran interés en ciertas situaciones como:

- Notificaciones: administración, monitorización, buzón de voz, fax, email.
- Pagos electrónicos: servicios “premium”.
- Autenticación en dos pasos: banca online, redes sociales.
- Publicidad.
- Comunicaciones entre máquinas (M2M)
- Programación OTA: configuración remota del terminal.

Existen dos tipos de mensajes, de difusión (SMS-CB, *SMS Cell Broadcast*), dirigidos a todos los terminales existentes en un determinado área, y mensajes punto a punto (SMS-PP, *SMS Point-to-Point*) destinados a un usuario específico. Se centrará el estudio en estos últimos.

Como se puede observar en la Figura 4.1 el único elemento que se introduce en la arquitectura de la red GSM para gestionar el envío y recepción de mensajes de los usuarios es el *Short Message Service Center* (SMSC), también denominado *Service Center* (SC). Cada operador necesita al menos uno en su red, si bien debido a la popularidad del servicio no es extraño contar con varios. El SMSC combina elementos software y hardware con el objetivo de reenviar los mensajes al destino o a otro SMSC, en el caso de cambiar de red. Si el receptor no está disponible, lo guardará hasta que lo esté o hasta que expire un contador. Además cuenta con un servicio de confirmación de recepción de mensajes.

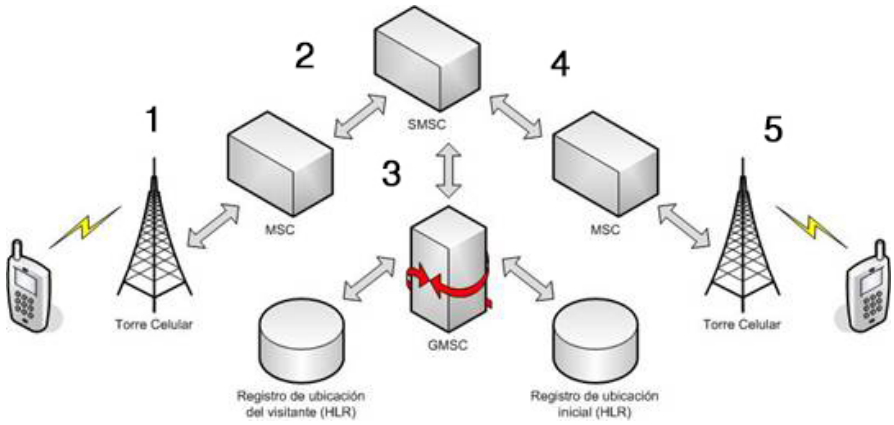


Figura 4.1: Arquitectura de red con servicios SMS

Cuando se envía un mensaje de un móvil hacia otro, éste atraviesa varias entidades antes de ser entregado. El flujo que sigue el mensaje representado en la Figura 4.1 se define en el estándar ETSI TS 03.40 [2], y se describe a continuación.

En primer lugar (1), el mensaje es enviado desde la estación móvil a un MSC a través del BSS, transportando las GSM Data Units hasta el NSS. A continuación (2), el MSC, que recibe las unidades de datos, está conectado a un SMSC, al que entrega el mensaje. Una vez el SMSC recibe el mensaje, identifica el MSC bajo el que se encuentra el usuario receptor accediendo a la información disponible en el HLR (3). Por último, el MSC determina la ubicación exacta para entregar el mensaje interrogando al VLR y envía el mensaje al BSS correspondiente (4). Dicho BSS se encarga por su parte de la entrega final al móvil destinatario (5).

Se pueden enviar y recibir SMS en dos modos: en modo texto clásico, al que estamos acostumbrados o en modo PDU. Los mensajes en modo PDU pueden emplearse para enviar datos en binario, lo que además, con la codificación adecuada, permite transportar más información que en modo texto.

Los SMS también contienen algunos metadatos como información sobre los participantes (número del SMSC o del remitente), información del protocolo, del esquema de codificación de los datos empleado o de sellado de tiempo. El uso de los recursos radio están definidos bajo la especificación del ETSI 3GPP TS 04.11 [4], mientras que los aspectos de nivel de red no están definidos, lo que supone que no exite ninguna restricción para su implementación.

Podemos diferenciar dos tipos de servicio de mensajería punto a punto en función del sentido de la comunicación: los originados por un móvil (SMS-MO, SMS *Mobile Originated*) que serán transportados hasta un SC y los terminados en un móvil (SMS-MT, SMS *Mobile Terminated*). En función del servicio empleado, es decir, del sentido de la comunicación, tendremos diferentes unidades de datos, que pasamos a describir.

4.1.1 Repertorio de PDUs

El protocolo de transferencia de los mensajes especificado en el ETSI TS 03.40 [2] emplea cuatro tipos de unidades de datos (TPDU, *Transport Protocol Data Unit*), dos por cada servicio, una transportando el propio mensaje y otra informando sobre el estado del mismo.

4.1.1.1 SMS-SUBMIT (MS → SC)

Unidad de datos que transporta un mensaje desde la estación móvil hacia el SMSC (SMS-MO). Opcionalmente se puede especificar un periodo de validez para guardar el mensaje en el SMSC hasta que la estación se encuentre disponible. La descripción de las cabeceras que componen la TPDU SMS-SUBMIT, así como el campo de datos, en un color más oscuro, se puede encontrar en la Tabla 4.1 a continuación de la propia PDU de la Figura 4.2.

MTI (f)	RD (f)	VPF (f)	RP (f)	UDHI (o)	SRR (o)	MR (f)	DA (f)	PID (f)	DCS (f)	VP (o)	UDL (f)	UD (o)

*F:FIJO, O:OPCIONAL

Figura 4.2: SMS-SUBMIT TPDU

Tabla 4.1: Elementos de la PDU SMS-SUBMIT

Abreviatura	Nombre	Función
MTI	Message-Type-Indicator	Describe el tipo de mensaje
RD	Reject-Duplicates	Parámetro que indica si el SC debe aceptar un mensaje con un campo MR ya existente
VPF	Validity-Period-Format	Indica si el campo VP está presente
RP	Reply-Path	Ruta de la respuesta
UDHI	User-Data-Header-Indicator	Indica que el campo "User-Data" (UD) contiene una cabecera de usuario
SRR	Status-Report-Request	El terminal solicita reporte de estado al SC
MR	Message-Reference	Parámetro que identifica al mensaje
DA	Destination-Address	Dirección de la entidad destino.

PID	Protocol-Identifier	Identifica el protocolo de la capa subyacente
DCS	Data-Coding-Scheme	Esquema de codificación de los datos usado.
VP	Validity-Period	Tiempo tras el que el mensaje no es válido
UDL	User-Data length	Longitud del campo User-Data
UD	User-Data	Datos

4.1.1.2 SMS-SUBMIT-REPORT

Esta unidad de datos es similar a la TPDU SMS-SUBMIT, como se puede comprobar en la Figura 4.3. Se encarga de informar de errores (en caso de haberlos), y la correspondiente causa del error. También realiza un reconocimiento positivo tras la correcta entrega de un SMS-SUBMIT. Se describen sus elementos en la Tabla 4.2.

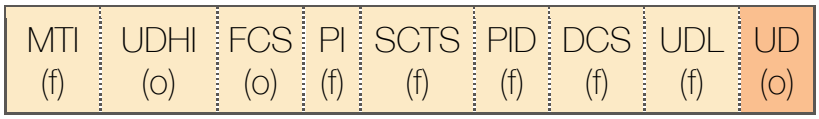


Figura 4.3: SMS-SUBMIT-REPORT TPDU

Tabla 4.2: Elementos de la PDU SMS-SUBMIT-REPORT

Abreviatura	Nombre	Función
MTI	Message-Type-Indicator	Describe el tipo de mensaje
UDHI	User-Data-Header-Indicator	Indica que el campo "User-Data" (UD) contiene una cabecera de usuario
FCS	Failure-Cause	Indica la razón por la que falló el envío del SMS-SUBMIT
PI	Parameter Indicator	Indica la presencia de los parámetros opcionales que le siguen
SCTS	Service-Centre-Time-Stamp	Marca temporal que indica cuando el centro de mensajería recibió el mensaje
PID	Protocol-Identifier	Identifica el protocolo de la capa subyacente
DCS	Data-Coding-Scheme	Esquema de codificación de los datos usado.
UDL	User-Data length	Longitud del campo User-Data
UD	User-Data	Datos

4.1.2 SMS-DELIVER (SC → MS)

Unidad de datos que transporta un mensaje desde el centro de mensajería SC al terminal móvil destinatario. Incluye una marca temporal, *Service Center Time Stamp* SCTS, como se puede ver en la Figura 4.4 usada por el SMSC para informar al receptor del instante en el que el mensaje llegó al centro de mensajería y un parámetro que indica si existen más mensajes esperando en el centro de mensajería para entrega al mismo terminal. Se describen todos sus campos en la Tabla 4.3.

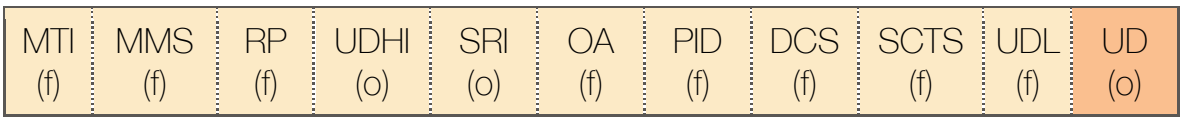


Figura 4.4: SMS-DELIVER TPDU

Tabla 4.3: Elementos de la PDU SMS-DELIVER

Abreviatura	Nombre	Función
MTI	Message-Type-Indicator	Describe el tipo de mensaje
MMS	More-Messages-to-Send	Indica si quedan mensajes en el SMSC para enviar
RP	Reply-Path	Ruta de la respuesta
UDHI	User-Data-Header-Indicator	Indica que el campo "User-Data" (UD) contiene una cabecera de usuario
SRI	Status-Report-Indication	Indica si el SC solicita reporte de estado
OA	Originating-Address	Dirección de la entidad remitente.
PID	Protocol-Identifier	Identifica el protocolo de la capa subyacente
DCS	Data-Coding-Scheme	Esquema de codificación de los datos usado
SCTS	Service-Centre-Time-Stamp	Marca temporal que indica cuando el centro de mensajería recibió el mensaje
UDL	User-Data length	Longitud del campo User-Data
UD	User-Data	Datos

4.1.2.1 SMS-DELIVER-REPORT

Al igual que en el caso anterior, también tenemos informe para la PDU SMS-DELIVER, representado en la Figura 4.5. Se encarga de informar de errores y su causa, además de los reconocimientos. Se describen en la Tabla 4.4 los elementos que la componen.

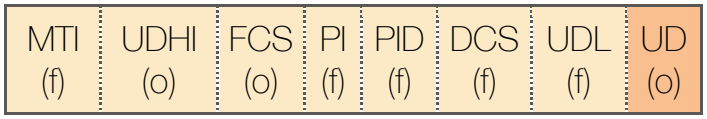


Figura 4.5: SMS-DELIVER-REPORT TPDU

Tabla 4.4: Elementos de la PDU SMS-DELIVER-REPORT

Abreviatura	Nombre	Función
MTI	Message-Type-Indicator	Describe el tipo de mensaje
UDHI	User-Data-Header-Indicator	Indica que el campo "User-Data" (UD) contiene una cabecera de usuario
FCS	Failure-Cause	Indica la razón por la que falló el envío del SMS-SUBMIT
PI	Parameter Indicator	Indica la presencia de parámetros opcionales
PID	Protocol-Identifier	Identifica el protocolo de la capa subyacente
DCS	Data-Coding-Scheme	Esquema de codificación de los datos usado
UDL	User-Data length	Longitud del campo User-Data
UD	User-Data	Datos

En el caso de enviar texto convencional, el parámetro *User Data Header Indicator* (UDHI) estará fijado a cero. Por lo tanto, no habrá cabecera de datos de usuario (*User Data Header*, UDH) en el campo de datos, simplemente se portará el texto codificado según el alfabeto escogido. Es posible ampliar las posibilidades de transporte de datos de la TPDU, haciendo uso de la cabecera de usuario UDH, quedando el campo de datos disponible para otros usos tal y como describe el estándar ETSI TS 03.40 [2].

4.1.3 User Data Header (UDH)

La cabecera de datos de usuario UDH amplía el rango de posibilidades de los SMS, añadiendo una serie de octetos al inicio del campo de datos de usuario (UD) que permiten definir la provisión de servicios de valor añadido, dando como resultado lo que podríamos denominar mensajería inteligente (*smart messaging*).

Cuando el bit UDHI se fija a uno, se está indicando que el campo de datos contiene una cabecera UDH. Tiene que ser incluida en los bytes que queden disponibles de entre los 140 del SMS completo, tal y como se muestra en la Figura 4.6. En este caso, por simplicidad se incluye un sólo elemento de información *Information Element* (A).

Figura 4.6: UDH contenida en campo UD de SMS

Dicho elemento de información, mediante su campo *Information Element Identifiers* (IEI) es un identificador que mapea el contenido con una determinada característica, de entre las definidas en el ETSI TS 03.40 [2]. Cabría destacar la capacidad para enviar tonos de llamada, mensajes concatenados (superiores a 140 Bytes), animaciones de operador, tarjetas de contactos o interactuar con la tarjeta SIM contenida en el terminal.

Para ésta última característica, objeto de nuestro trabajo, el estándar define que el identificador IEI deberá ser 0x70. También se especifica que el valor de la longitud del dato contenido, es decir, el campo *Information Element Data Length* (IEDL), estará presente pero fijado a cero. Esto se debe a que la longitud de los datos estará contenida en otro campo, como veremos más adelante. Como consecuencia, la longitud de la UDH necesaria será 0x02, y la UDH completa 0x027000.

Para interactuar con la tarjeta SIM, además será necesaria la introducción en el campo de datos IED de una nueva cabecera, la denominada *(U)SIM Toolkit Security Header,* recogida en el estándar ETSI/3GPP TS 03.48 [3] y descrita a continuación.

4.1.4 SIM Toolkit Security Headers

Una de las opciones más interesantes de las cabeceras de usuario (UDH) es la de generar paquetes seguros, que sean atendidos por la tarjeta SIM. Haciendo posible una interacción remota a través de mensajes SMS entre el gestor y la tarjeta, sin ningún tipo de procesado por parte del teléfono. Puede ser usado para enviar comandos de configuración para la tarjeta vía SMS, como suele ser el caso de los operadores, que aprovechan esta característica para configurar remotamente aspectos administrativos de los servicios contratados por los abonados. Esto es posible gracias a los mecanismos que define el *toolkit* de la tarjeta SIM (*SIM Application Tootlkit,* SAT), encargado de la gestión de la interfaz entre el terminal y la SIM.

En el documento ETSI 3GPP TS 03.48 [3] se especifica la estructura y codificación de un conjunto de comandos de aplicación que serán transportados sobre el campo de datos de un SMS, previa UDH codificada apropiadamente como ya se ha comentado. Este conjunto de comandos, consisten en unidades de datos *Application Protocol Data Units* (APDU), que son un subconjunto de los estandarizados en el ETSI/3GPP TS 11.11 [7]. Pueden dividirse entre comandos de entrada o de salida, en función del sentido de la comunicación.

Los comandos de entrada, es decir, los que ejecutamos contra la tarjeta SIM son: SELECT, UPDATE BINARY, UPDATE RECORD, SEEK, INCREASE, VERIFY CHV, CHANGE CHV, DISABLE CHV, ENABLE CHV, UNBLOCK CHV, INVALIDATE, REHABILITATE. La tarjeta SIM responderá a dichos comandos de entrada a través de los comandos de salida; READ BINARY, READ RECORD, GET RESPONSE.

Estos comandos, serán cifrados según las claves introducidas, y adjuntados en el campo *Secured Data* bajo la *SIM Toolkit Security Header*, que se muestra en la Figura 4.7. La entidad receptora responderá con paquetes de respuesta similares, conteniendo la información requerida. Se detallan para un mejor entendimiento en la Tabla 4.5 las funciones de los campos de la cabecera SIM Toolkit.

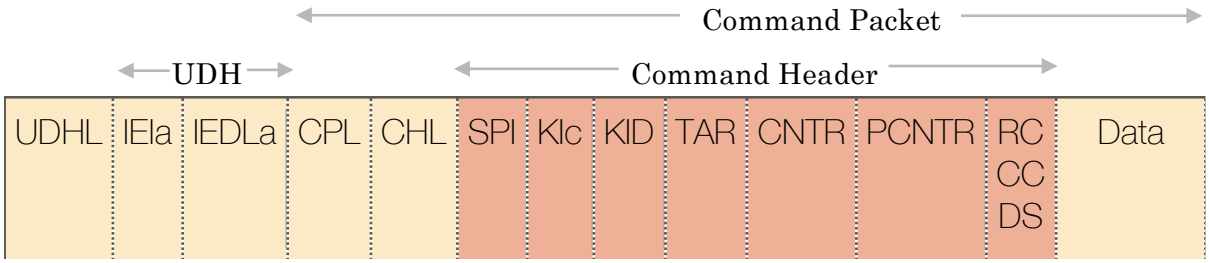


Figura 4.7: Estructura del "command packet"

Tabla 4.5: Elementos del command packet

Abreviatura	Nombre	Función
CPL	Command Packet Length	Número de octetos desde el Command Header hasta el final de los datos seguros
CHL	Command Header Length	Número de octetos desde el SPI hasta el final de RC/CC/DS
SPI	Security Parameter Indicator	Define el nivel de seguridad aplicado al mensaje
KIc	Ciphering Key Identifier	Identificador de la clave y algoritmo empleado para el cifrado
KID	Key Identifier	Identificador de la clave y algoritmo empleado para el RC/CC/DS
TAR	Toolkit App. Reference	Identifica la aplicación de la SIM hacia la que se dirige el comando
CNTR	Counter	Detección de duplicados e integridad del mensaje
PCNTR	Padding Counter	Indica el número de octetos de relleno empleados en el cifrado al final de los datos seguros
RC/CC/DS	Redundancy-Check / Crypto-Checksum / Digital-Signature	Chequeo de errores mediante redundancia, mediante suma de chequeo o firma digital

4.2 Short Message Peer-to-peer Protocol (SMPP)

SMPP [24] es un protocolo abierto diseñado para proveer una comunicación de datos flexible, generalmente a través de mensajes cortos, entre entidades de mensajería (ESME, *External Short Messaging Entities*) y otras entidades finales, generalmente móviles. Típicamente se define como ESME al cliente SMS en la red fija. Como se puede observar en la Figura 4.8, requiere elementos de la red encargados del enrutado *Routing Entities* (RE) y centros de mensajería *Message Centers* (MC), como los SMSC de las redes GSM, red a través de la cuál suele hacerse la entrega final.

SMPP suele utilizarse para permitir a terceros servicios enviar mensajes, habitualmente de difusión y soporta otras tecnologías no-GSM como UMTS o CDMA. Es el protocolo más utilizado para intercambiar mensajes fuera de redes con sistema de señalización por canal común (SS7).

Está basado en intercambios de pares de PDUs petición-respuesta, como la representada en la Figura 4.9, transportadas sobre TCP. Puede operar tanto modo síncrono, donde cada lado espera respuesta a cada PDU enviada, como asíncrono, dónde múltiples envíos pueden realizarse sin esperar reconocimiento, permitiendo el envío de bloques de mensajes.

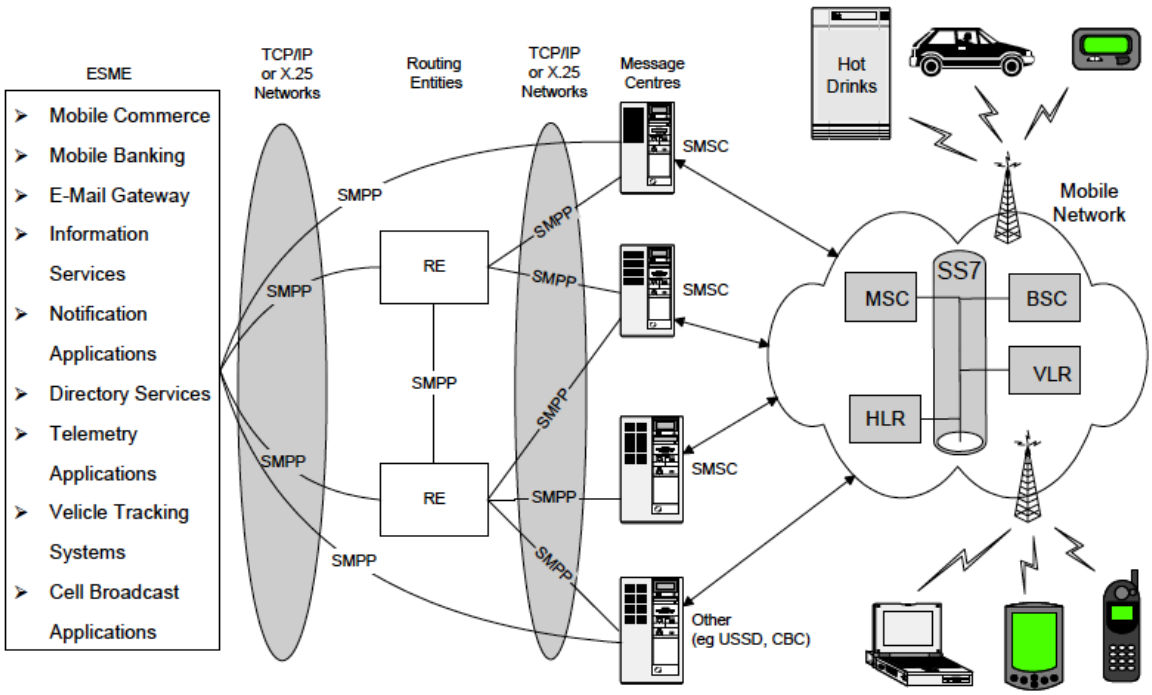


Figura 4.8: Arquitectura de red SMPP

4 B	4 B	4 B	4 B	L B
Command Length	Command ID	Command Status	Sequence ID	PDU Body

Figura 4.9: SMPP PDU

Para hacer uso del protocolo, se debe establecer una sesión SMPP entre la entidad emisora y el centro de mensajería, usualmente iniciada por la entidad ESME. Para ello posee un conjunto definido de operaciones y estados.

El flujo de mensajes presente en la Figura 4.10, consta de un ESME y MC en conexión. Para iniciar la sesión SMPP (estado *open*), se ejecuta la operación *bind_transmitter*, tras lo que si la respuesta es afirmativa, la sesión pasa al estado *bound_tx*. En este punto, la sesión está establecida y lista para recibir la operación que transporta el mensaje *submit_sm*. La respuesta *submit_sm_resp* informará del estado de la recepción del mensaje. La sesión se cierra con la operación *unbind*, que nos lleva al estado *unbound*, y posterior cierre de la conexión.

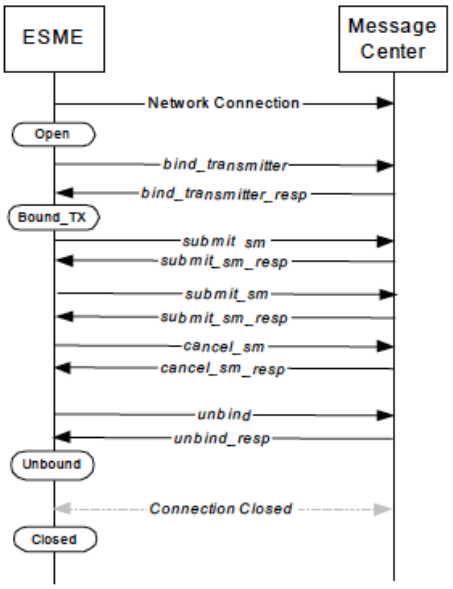


Figura 4.10: Ejemplo de sesión SMPP

Capítulo 5

Evolución de las comunicaciones móviles

El sector más relevante dentro del mercado de las telecomunicaciones es sin duda el de las comunicaciones móviles, sector que ha evolucionado dramáticamente en los últimos tiempos, no sólo en cuanto al desarrollo de la tecnología, sino al modo en que los usuarios hacen uso de ella. Los teléfonos de hoy en día están bastante alejados de los aparatosos terminales con los que operaban las primeras redes GSM, cuyo único propósito era ofrecer llamadas de voz. Gracias a dicha evolución hoy es posible acceder desde prácticamente cualquier lugar a una gran variedad de servicios y aplicaciones. La aparición de nuevos servicios multimedia con un consumo de información en tiempo real y toda una serie de nuevas aplicaciones relacionadas con las redes sociales, los pagos móviles, etc. generan entre los usuarios necesidades de ancho de banda cada vez mayores.

Para soportar este rápido crecimiento de las necesidades de tráfico, ya no sólo terminales móviles, sino de un número cada vez mayor de dispositivos dedicados únicamente al tráfico de datos, los operadores móviles necesitan invertir en mejorar la capacidad de sus redes. LTE, como red de acceso móvil de cuarta generación basada en IP, constituye probablemente la mejor alternativa a largo plazo para los operadores, permitiéndoles aumentar dicha capacidad, con el compromiso de mantener los costes de operación y mantenimiento de la red controlados.

Bajo este contexto, hay una enorme oportunidad para aumentar el papel que juega la tarjeta inteligente contenida en dichos dispositivos. Con el creciente uso de los servicios de banca móvil y las comunicaciones *Near Field Communications* (NFC), hay una innegable necesidad de un método seguro para la identificación del usuario. Las plataformas OTA juegan aquí un papel crucial asegurando a los operadores móviles obtener el máximo rendimiento a la inversión de sus redes LTE.

5.1 Evolución de las Redes móviles en España

El primer servicio de telefonía móvil en aparecer en nuestro país lo ofreció la Compañia Telefónica Nacional de España (CTNE) en el año 1976. El llamado Teléfono Automático en Vehículos (TAV) consistía en un rudimentario sistema que utilizaba las técnicas propias de los equipos de comunicaciones móviles privadas (PMR) de la época [38][39]. El alto precio de los terminales y su escasa capacidad de usuarios frenaron la demanda, quedando limitada prácticamente a personal de la propia CTNE y altos cargos de la administración pública. El servicio era explotado en régimen de monopolio por la compañía al igual que sucedía con el servicio fijo. Esto propició que el mercado de la telefonía móvil se fundamentara en un triple monopolio, es decir, la misma empresa concentraba el suministro de los terminales, la operación de los servicios y era la propietaria de la red.

La aparición comercial en 1981 de los sistemas nórdicos de telefonía móvil (NMT, *Nordic Mobile Telephone*) cambió por completo la situación. El sistema NMT estaba

basado en el concepto de radiocomunicación celular ideado por D.H. Ring en los laboratorios Bell de la empresa AT&T. La CTNE puso en funcionamiento el primer sistema de telefonía móvil celular en nuestro país aprovechando la celebración del Mundial de Fútbol de 1982. El denominado TMA-450 (Telefonía Movil Automática) deriva del estándar nordico, en la banda de los 450 Mhz, con la principal ventaja frente a los sistemas TAV de permitir un sencillo crecimiento de la red gracias al funcionamiento de los sistemas celulares. El sistema tuvo un gran éxito.

Posteriormente a la publicación del Libro Verde de las Telecomunicaciones por parte de la Comisión Europea, las Cortes Generales aprobaron en 1987 la Ley de Ordenación de las Telecomunicaciones (LOT), que obligó a la CTNE a liberalizar la comercialización de los terminales de usuario. En junio de 1988 cambia la denominación social de la CTNE por Telefónica de España S.A. El sistema TMA-450 alcanzó durante 1990 los 54.700 abonados entre las 50 provincias españolas, observándose los primeros síntomas de congestión del espectro radioeléctrico en la banda de 450 Mhz. Telefónica comenzó a estudiar la introducción de un nuevo estándar de telefonía celular ya en funcionamiento desde 1985 en Gran Bretaña; el *Total Access Communication System* (TACS). Bajo su filial TS1, Telefónica lanzó en 1991 el sistema TMA-900 derivado del estándar TACS, en la banda de los 900 Mhz. Comercializado con el nombre de Moviline, se convirtió en el primer acercamiento de la telefonía móvil al ciudadano.

Mientras se produce el despliegue de la telefonía móvil analógica en toda Europa, la CEPT crea el grupo de trabajo GSM con el propósito de desarrollar un estándar de telefonía móvil bajo dos requisitos principales; el empleo de tecnología digital y la interoperabilidad entre los países Europeos. En 1987 los trece operadores más importantes del momento firmaron un Memorando de Entendimiento “GSM MoU”, para lanzarlo en 1991, pero ciertos retrasos en el desarrollo técnico hicieron postponer el lanzamiento hasta el año siguiente. Telefónica desarrolló dos proyectos piloto y el Ministerio de Obras Públicas y Transportes trabajaba en la modificación de la LOT en aras de la ruptura del monopolio de la telefonía móvil. La evolución de la red de Telefónica fue más lenta que en el resto de países Europeos, contando con un número de usuarios menor al esperado, lo que llevo al Gobierno a pensar en la conveniencia de introducir un segundo operador como incentivo al desarrollo del servicio. El 26 de Septiembre de 1994 se aprueba el pliego de cláusulas de explotación y bases de adjudicación del concurso para la concesión de una segunda licencia de telefonía móvil GSM. El consorcio Airtel-Sistelcom-Reditel se hizo con la licencia de la actual Vodafone comenzando a operar en Octubre de 1995 [33].

Tras la creación del “duopolio” tanto en redes móviles (Movistar-Airtel) como en fijas (Telefónica-Retevisión), el siguiente paso fue la privatización de ambas compañías, en primer lugar Telefónica y en segundo Retevisión. Para equilibrar las condiciones del servicio de ambas, se convocó un concurso en 1998 para la concesión de tres licencias en la modalidad *Digital Cellular System 1800* (DCS-1800), sistema similar a GSM en la banda de 1800 Mhz idóneo para entornos microcelulares. El concurso se resolvió en favor de Retevisión Móvil (filial de Retevisión), quien comenzó a prestar servicio bajo la marca de Amena en 1999, licencia que opera actualmente Orange tras la compra de France Telecom. Los dos operadores existentes también obtuvieron licencia para esta banda. La desventaja competitiva que suponía el uso de frecuencias altas, por tener éstas un menor alcance y penetración en interiores, forzó al resto de operadores a

firmar un pacto de provisión de servicio con Amena llamado "Acuerdo de Suministro Provisional de Infraestructura de Red", así como una restricción en el uso de GSM-1800 durante seis meses. La llegada de Amena al mercado supuso un aumento del 16 al 38% de la penetración del móvil en España, dejando claro que la llegada de los dos nuevos operadores aumentó el dinamismo del mercado.

Tras el fortalecimiento de las comunicaciones móviles y la transformación de las costumbres sociales y culturales de la población hacia el modelo de sociedad conocida como "Sociedad de la Información", aparece la necesidad de conformar el binomio "Internet-Móvil". El primer intento fué lanzado por Telefónica con el servicio *Wireless Application Protocol* (WAP) en Octubre de 1999, el cual no resultó exitoso, ya que las características de los terminales de la época no eran adecuadas para ofrecer una buena experiencia de usuario navegando por internet.

La clase política europea decide dar el salto a la tercera generación de telefonía móvil con el ambicioso nombre de *Universal Mobile Telecommunications System* (UMTS), y tras un polémico concurso en el año 2000 se adjudicaron cuatro licencias para la explotación del servicio 3G en la banda de los 2100 Mhz a las empresas Telefónica, Airtel Móvil, Retevisión Móvil y Xfera (actual Yoigo), quedando repartido el espectro radioeléctrico tal como se muestra en la Figura 5.1. La situación durante el año 2001 fué bastante diferente de lo esperado produciéndose varios hechos en Europa y España que hacían hablar de recesión económica en el sector. También en el año 2000 se regula por parte de la "*Comision del Mercado de las Telecomunicaciones*" (CMT) el proceso de portabilidad, mediante el cual un abonado puede cambiar de compañía sin perder su número de teléfono de forma gratuita. El lanzamiento comercial de la tecnología de tercera generación se retrasa hasta 2002, ya que no estaban disponibles ni los terminales ni muchas especificaciones técnicas que ayudasen a la implantación de las nuevas redes. De hecho, las licencias de UMTS se conceden sin realizar ninguna prueba piloto como en el caso de GSM, lo que reforzó el uso temporal del sistema GPRS.

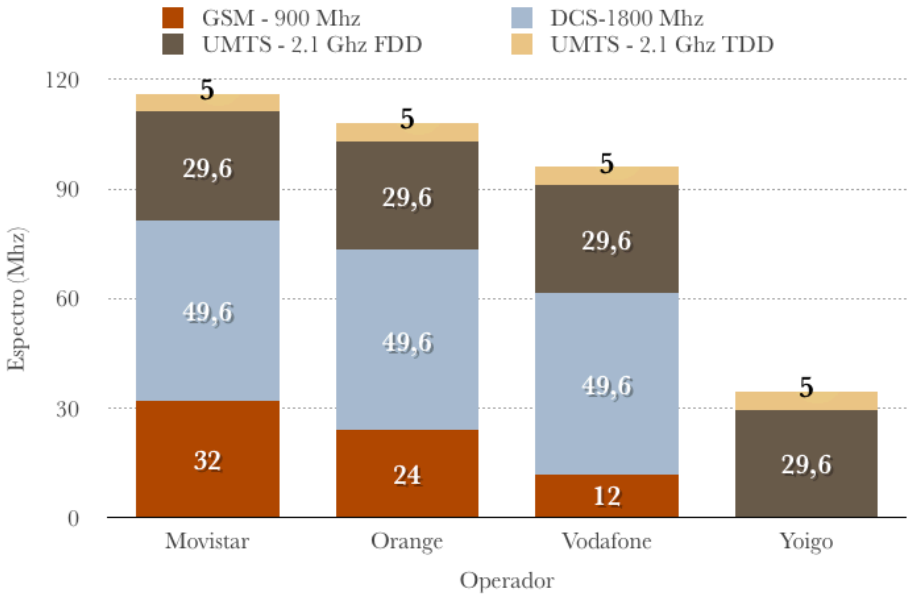


Figura 5.1: Reparto del espectro tras subasta año 2000

5.1.1 Operadores Móviles Virtuales (OMV)

El concepto es similar al que se venía desarrollando en servicios de telefonía fija y banda ancha ADSL, donde el operador predominante (Telefónica) se veía obligado a alquilar su línea hasta el usuario para que un tercero pudiese ofrecer sus servicios.

Los OMVs son operadores que ofrecen servicios de red, sin poseer realmente de la infraestructura necesaria, son simples revendedores de la capacidad sobrante de otras compañías. Algunos OMVs también disponen de elementos de red propios, como es el caso de Yoigo, que alquila a Movistar la infraestructura allá donde la suya no llega.

Se realizan varios intentos por parte del ministerio de Ciencia y Tecnología de aumentar el número de competidores en el mercado como conceder nuevas licencias GSM que se liberan con el cierre de Moviline, pero finalmente no se aprovecharon y las licencias se adjudicaron a Telefónica y Amena.

El segundo intento de aumentar la competencia fue la creación en 2001 de los operadores móviles virtuales (OMV), facilitando a operadores de telefonía existentes convertirse en operadores duales. Sin embargo, la libre negociación de las partes para los precios de interconexión resultó en un retraso hasta el año 2007 al no llegar a acuerdos de roaming nacional. La CMT intensifica sus esfuerzos fijando precios, plazos y aspectos técnicos habilitando la llegada de este tipo de operadores. Hacia el año 2008, Yoigo acuerda con Telefónica el uso de su red, Carrefour hace lo mismo con Orange y Euskaltel con Vodafone.

Actualmente los OMV poseen una cuota de mercado modesta, pero están erosionando notablemente el oligopolio de Movistar, Orange y Vodafone. Su introducción ha sido positiva para el mercado, ya que los operadores tradicionales se han visto obligados a mejorar sus precios para frenar la pérdida de clientes. Como podemos observar en la Figura 5.2, en el último año han ganado cerca de dos millones de clientes, a costa de los operadores tradicionales. Con la excepción de Orange, éstos últimos ven reducir su número de clientes, o lo incrementan levemente como en el caso de Yoigo.

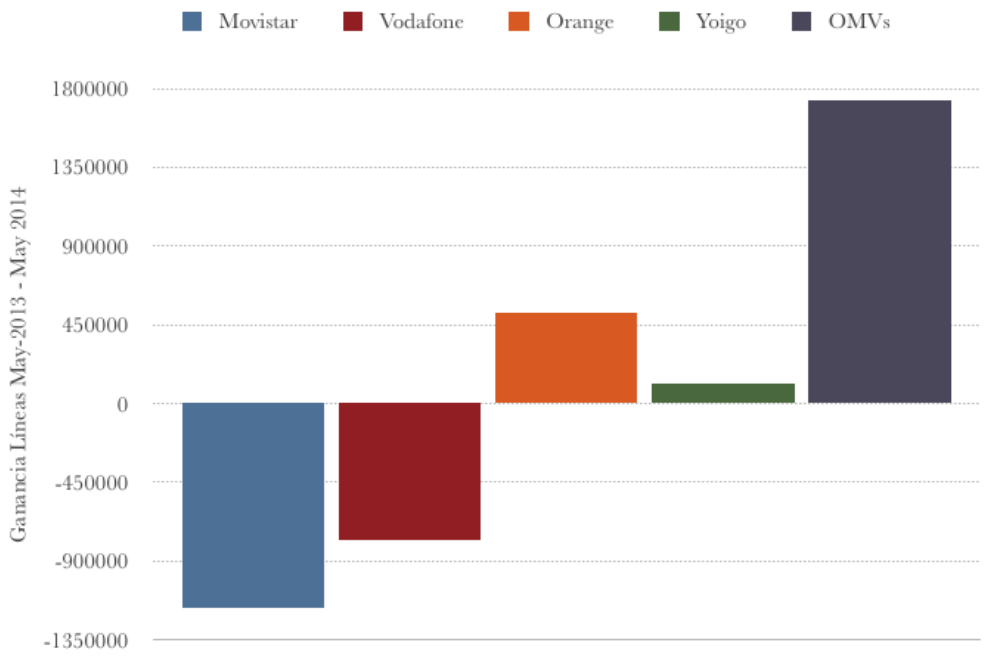


Figura 5.2: Ganancia líneas móviles por operador

5.1.2 Situación del espectro radioeléctrico en España

El 7 de Julio de 2011 se adjudicaron las licencias para la explotación de la tecnología de cuarta generación en la banda de 2,6 Ghz, así como bloques en la banda de 800 Mhz (790-862 Mhz), en ese momento ocupados por la televisión digital terrestre (TDT), pero que se verían liberados mediante el denominado dividendo digital. Este proceso consistiría en la liberación de dichas frecuencias de UHF ocupadas por la TDT, derivadas del apagón de la televisión analógica, para el despliegue de las redes móviles de cuarta generación. El bloque más conflictivo fue adjudicado a Orange, cuyas frecuencias según algunos instaladores, podrían causar interferencias con la señal TDT. Se considera que estas dos bandas de frecuencias deberían satisfacer las demandas de espectro de los operadores para las comunicaciones de banda ancha móvil. El reparto de espectro tras dicha subasta queda bastante equilibrado, como muestra la Tabla 5.1.

Tabla 5.1: Reparto del espectro en España hasta 2030

Operador	800 MHz	900 MHz	1.800 MHz	2.100 MHz	2.600 MHz
Movistar	10 MHz FDD	14,8 MHz FDD	19,8 MHz FDD	15 MHz FDD 5 MHz TDD	20 MHz FDD
Orange	10 MHz FDD	10 MHz FDD	19,8 MHz FDD	15 MHz FDD 5 MHz TDD	20 MHz FDD 10 MHz TDD
Vodafone	10 MHz FDD	10 MHz FDD	19,8 MHz FDD	15 MHz FDD 5 MHz TDD	20 MHz FDD 20 MHz TDD
Yoigo	-	-	15 MHz FDD	15 MHz FDD 5 MHz TDD	-

La liberación de dicha banda ha sufrido varias modificaciones de su fecha, debido a que el Tribunal Supremo dio la razón a algunas cadenas de televisión que recurrieron contra el reparto de canales de la TDT, sentencia que ha tenido como consecuencia el cierre de nueve canales de televisión. Aunque en un principio se habló de tenerla lista para 2014 se retrasa para el inicio de 2015.

A raíz de esta situación, el gobierno español ha elaborado un proyecto de Real Decreto conteniendo el "Plan Técnico Nacional de la TDT" en el que se regula el proceso para llevar a cabo la liberación. Además de reordenar frecuencias, el plan técnico incrementa la oferta actual de canales mediante la convocatoria de un concurso que dará prioridad a los contenidos de alta definición. Como consecuencia de la reordenación de los canales, es posible que sea necesario realizar ciertas adaptaciones en las instalaciones de televisión de los edificios.

Los operadores ya han realizado despliegues de cuarta generación en las bandas de 1800 y 2600 Mhz, pero esperan a los 800 Mhz para darle un verdadero impulso a sus despliegues.

Otro asunto que resuelve el Gobierno en el reparto del espectro del año 2011, es la reutilización (*refarming*) de las frecuencias de 900 y 1800 Mhz (GSM) para ubicar en ellas otras tecnologías con mayor eficiencia espectral como UMTS que ofrezcan

servicios 3G como *High Speed Packet Access* (HSPA) y sus derivados en subida (HSUPA) y bajada (HSDPA). Se permite que los operadores utilicen indistintamente las frecuencias de que disponen para tecnologías de cualquier generación, consiguiendo una mayor eficiencia en el despliegue de sus redes y aumentando la cobertura de tercera generación a costa de despliegues con cobertura de segunda generación existente mediante una renovación de los equipos de red. Se logra así que un alto porcentaje de la población tenga acceso a 1 Mbps como mínimo, ampliando la cobertura 3G en zonas rurales considerablemente y facilitando un posterior paso a la cuarta generación. Además del evidente aumento de capacidad, los usuarios pueden notar con estos cambios un ahorro de la batería en sus terminales al recibir señales de mayor estabilidad y no tener que alternar entre antenas tan frecuentemente.

5.2 Cuarta generación de telefonía móvil: LTE

Las necesidades de los usuarios en términos de calidad y velocidad de transmisión van en aumento. Las redes UMTS de tercera generación soportan las nuevas condiciones de tráfico y muchos de los servicios ofertados presentan una deficiente calidad. El aumento del uso de dichas redes de datos y la aparición de nuevos servicios como la televisión móvil, el vídeo bajo demanda, juegos online, streaming de audio y vídeo, hacen necesaria la aparición de una tecnología que soporte flujos de datos propios de redes de banda ancha, no siendo soportados por las tecnologías 3G. Son estos aspectos los que motivan al 3GPP para el desarrollo del proyecto LTE, especificado nuevamente por el ETSI, bajo los documentos TR 25.913 [19] y TR 25.814 [20].

La principal ventaja de la tecnología LTE es un aumento de las velocidades de transmisión, con latencias por debajo de 50 ms y velocidades teóricas de 150 Mbps en bajada y 75 Mbps en subida, pudiendo alcanzar bajo la especificación LTE-Advanced. actualmente en pruebas, los 300 Mbps[1]. Dicha velocidad vendrá fuertemente condicionada por la cantidad de espectro dedicado por el operador y la banda de frecuencia a la que se opera.La interfaz radio de LTE emplea *Orthogonal Frequency Division Multiple Access* (OFDMA) en el enlace descendente y *Single Carrier Frequency Division Multiple Access* (SC-FDMA) en el *uplink*. Gracias al uso de éstas y otras técnicas como el uso de múltiples antenas (MIMO), se trata de una tecnología con una gran eficiencia espectral, consiguiendo una reducción del consumo energético de los terminales. Evita la fragmentación de los terminales de usuario a nivel mundial por el tipo de duplex, ya que es compatible tanto con FDD como con TDD.

La arquitectura de las redes LTE está basada en el modelo del 3GPP *Evolved Packet System* (EPS), consistente en el empleo de conmutación de paquetes IP en toda la red, y la compatibilidad total con las redes predecesoras de segunda y tercera generación, reduciendo la inversión necesaria para su implementación y los costes de mantenimiento. En este sentido LTE no es considerada por la ITU como un estándar de cuarta generación, sino "casi-4G", pues no cumple los tres requisitos establecidos

[1] Los operadores tradicionales ya han realizado diversas pruebas en nuestro país: http://www.xatakamovil.com/vodafone/vodafone-ya-prueba-la-siguiente-generacion-de-lte-en-espana-llegando-a-los-300-mbps-de-descarga
http://www.xatakamovil.com/conectividad/asistimos-a-pruebas-reales-de-lte-a-de-orange-de-verdad-es-tan-bonita-esta-tecnologia-como-la-pintan

para considerar que un estándar es 4G: el empleo del modelo de red "all-IP", alcanzar velocidades de pico de 1 Gbps en movilidad y de 100 Mbps en alta movilidad, y contar con picos de eficiencia espectral de 15 bits/Hz en bajada y 6,75 bits/Hz en subida.

El despliegue en España se está viendo condicionado como hemos visto a consecuencia al retraso en el dividendo digital, si bien los operadores tradicionales ya poseen despliegues de cuarta generación en los principales núcleos urbanos, éste se encuentra en las bandas de 1.800 Mhz y 2.600 Mhz, con las consecuencias de alcance y penetración en interiores que esto conlleva, y no tiene una expansión territorial muy grande. A continuación se presenta una prueba de velocidad realizada bajo el operador Movistar, alcanzando velocidades en movilidad de unos 20 Mbps, nada despreciables, pero aún lejos de lo que la ITU entiende por 4G, y con el inconveniente de tener un nivel de cobertura no muy alto, -106 dBm.

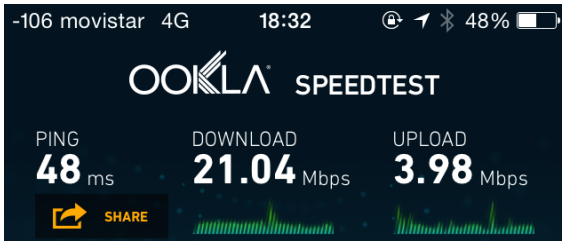


Figura 5.3: Prueba de velocidad 4G

5.3 Plataformas OTA sobre LTE

Como su propio nombre indica, LTE representa la evolución natural de las redes móviles actuales motivada por el rápido desarrollo de los terminales y de las plataformas de aplicación. Como resultado de este desarrollo surgen nuevos modelos de negocio para los operadores como el acceso a servicios en la nube, los mencionados servicios de pago, banca móvil y comunicaciones NFC. La naturaleza personal de la SIM y su capacidad de manejo a través del interfaz radio (Over-the-Air) contribuyen a asegurar la calidad de la experiencia del usuario, independientemente de la tecnología que emplee la red a la que se encuentre conectado.

El surgimiento de nuevas aplicaciones y servicios no sólo afecta a los dispositivos y redes sino también a las tarjetas SIM y a las plataformas de manejo remoto (RFM, *Remote File Management*) a través del aire (OTA) de las mismas. La solución tradicional para el manejo remoto de los terminales es una plataforma OTA basada en SMS y el empleo de las cabeceras de usuario vistas en el apartado 4.1.4, definidas en las especificaciones del ETSI 3GPP TS 03.40 [1] y 03.48 [3].

Con la implantación de las redes LTE, habrá menos tráfico de SMS y en algunos casos incluso no se prestará dicho servicio, como consecuencia del uso de IP, los operadores están obligados a mantener las redes de generaciones anteriores para contar con el servicio de mensajería y voz tradicionales y, aunque están esforzándose en encontrar alternativas como VoLTE, puede darse el caso de que un operador de bajo coste no cuente con dicha infraestructura de red, optando por una arquitectura LTE totalmente IP y VoIP como solución para la voz.

Del mismo modo, para el caso de comunicaciones OTA, aparecen plataformas OTA basadas en sistemas totalmente IP [35]. Las redes LTE pueden asegurar a las plataformas OTA la capacidad de mantener y actualizar las aplicaciones y datos de

manera permanente, beneficiándose de las características de una infraestructura de red IP de gran ancho de banda, escalable, y fiable gracias al empleo del modelo cliente-servidor.

Las tarjetas inteligentes *Universal Integrated Circuit Card* (UICC) no solo sirven para proveer la identidad del usuario en el proceso de acceso a la red. El gran potencial de las tarjetas UICC contenidas en los terminales es sin duda la provisión de esta identidad en procesos de autenticación como cliente ante un servidor OTA remoto. La plataforma OTA a su vez, permite la gestión remota y segura de la información personal como las credenciales del cliente. Pueden usarse con multitud de propósitos como aplicaciones del operador utilizando el "SIM Toolkit", aplicaciones, almacenamiento de datos como contactos, listas de prioridades "*roaming*" o la calidad del servicio relativa al usuario. Pero donde juega un importante papel es en la implementación de aplicaciones seguras, como la banca móvil y los pagos NFC. Varios expertos creen que las aplicaciones NFC poseen un gran potencial en la generación de ingresos mediante el uso de la UICC.

A medida que madure la tecnología LTE, también lo hará la tarjeta UICC, llegando incluso el día de mañana a contar con su propia dirección IP y comunicándose con el teléfono a través de una interfaz de alta velocidad. El actual protocolo empleado en la comunicación entre el teléfono y la tarjeta será reemplazado por interfaces tipo Ethernet. La arquitectura OTA estará basada en una aplicación web "HTTP" cliente-servidor, integrando la gestión remota OTA en el mundo Internet y mejorando las posibilidades de uso que ofrecen las plataformas actuales basadas en mensajería SMS. La integración de IP en la tarjeta UICC permitirá ofrecer mayor capacidad de descarga, comparado con el uso de la comunicación mediante concatenación de SMS actual, así como reducir la tasa de errores. Debido a la cantidad de datos involucrados en ciertos servicios NFC, esto puede ser un requisito para el éxito de la comunicación.

Los operadores móviles usualmente utilizan sus plataformas OTA para la activación y provisión de servicio de los terminales de usuario, configurando parámetros como números *Mobile Station Integrated Services Digital Network* (MSISDN), buzón de voz, el centro de mensajería, listas de prioridades, suscripciones y otros servicios. Esto les permite mantener las tarjetas sin personalizar hasta el momento de la venta y posterior activación, reduciendo costes logísticos. Todo esto será más fácil para el operador bajo la integración LTE-UICC-IP. También se benefician notablemente en el caso de actualizaciones masivas, donde el volumen de los datos es enorme y puede significar una gran carga en la red de señalización, así como una elevada tasa de errores. Gracias el uso de IP, se ofrece una capacidad para manejar este tipo de operaciones mucho mayor [36].

Las tecnologías OTA tradicionales basadas en SMS están ampliamente extendidas y siguen cumpliendo un papel importante en la provisión remota de aplicaciones. Sin embargo, la tecnología *Smart Card Web Server* (SCWS), basada en servidores web ejecutados sobre la SIM está evolucionando. Presenta diversas ventajas como una mejor integración en el terminal, una interfaz de usuario atractiva y accesible, basada en protocolos estándar del mundo Internet en lugar de protocolos específicos de la tarjeta SIM, haciendo más fácil desarrollar servicios para la tarjeta SIM integrados con servicios web típicos de Internet. El uso del modelo cliente-servidor permite configurar relativamente fácil los recursos dedicados a los casos de uso críticos,

manteniendo diversos niveles de QoS. Por ejemplo es posible dedicar hardware y software a las operaciones NFC, haciéndolas independientes de las actualizaciones masivas o las listas de roaming.

Hay tres posibles escenarios en esta comunicación cliente-servidor; *pull*, en el que es el suscriptor quien accede a la información, por ejemplo cuando el usuario consulta su buzón de voz, el caso *push*, en el que la información se envía al dispositivo sin ser solicitada, por ejemplo cuando el operador configura ciertos parámetros del servicio, y la encuesta *poll*, que suele ser el caso de las actualizaciones de firmware comprobadas periódicamente en busca de nuevas versiones.

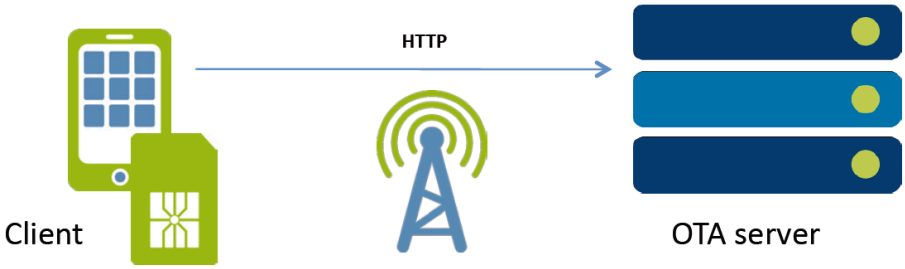


Figura 5.4: Modelo cliente-servidor en plataformas OTA

Capítulo 6

Analizador de Redes GSM

Todo lo que rodea al equipamiento GSM más allá de la estación móvil está celosamente protegido por los operadores móviles o tiene un alto precio que lo hace inaccesible para el usuario. Existen diversos equipos para análisis de redes móviles en el mercado que permiten acceder a medidas de la señal radio sobre redes de cualquier generación, visualizando la fuerza de la señal en tiempo real y otra información relevante de la celda. Modelos como TSMQ de Rohde&Schwarz [51], o Nexus 8630 de nexusTelecom [52], nos permiten incluso un análisis de varias generaciones de redes móviles, ademas de fijas en el caso del segundo.

Suelen ser empleados por los operadores para buscar la mejor ubicación de la antena evitando posibles interferencias con frecuencias adyacentes y para realizar posteriores pruebas de cobertura. También pueden ser útiles para detectar señales inhibidoras.

Otro problema con el que podemos encontrarnos, es que los analizadores convencionales sirven para realizar medidas espectrales, pero no acceden al tráfico del sistema GSM, por lo tanto no permiten un análisis detallado de las tramas intercambiadas.

Como solución a su elevado coste y en ocasiones difícil acceso, aparecen diversas iniciativas desde el ámbito de la investigación que tratan de analizar y estudiar las redes mediante pocos recursos y el uso de software libre. Mediante el uso de *Software-Defined Radio* (SDR), y sintonizadores de TDT, la iniciativa RTL-SDR [53] consigue analizar tráfico GSM gracias a la herramienta Airprobe [54] para Linux. Tomaremos como base de éste trabajo el proyecto Osmocom [40], familia de proyectos centrada en las comunicaciones móviles *open source*. Este tipo de iniciativas por un lado consigue incentivar la investigación e innovación en redes móviles tan generalizadas y, por otro, ayudar a estudiantes o ingenieros interesados en la materia a adquirir un punto de vista práctico que de otra manera sería difícil de conseguir con la lectura de libros.

El proyecto Osmocm incluye desarrollos tanto software como hardware y cuenta con una serie de herramientas capaces de analizar diversas tecnologías móviles, desde las públicas como GSM o GPRS hasta las privadas como *Terrestrial Trunked Radio* (TETRA), la telefonía inalámbrica de corto alcance *Digital Enhaced Cordless Telecommunications* (DECT) o la satelital *GEO-Mobile Radio Interface* (GMR). A continuación se realiza la descripción de los trabajos realizados empleando la utilidad OsmocomBB, con la que se ha llevado a cabo el estudio de las redes GSM a través del analizador de protocolos de código abierto.

6.1 OsmocomBB

El proyecto OsmocomBB comprende todo el software necesario para implementar un analizador de redes GSM para lo que se requiere de un teléfono compatible en el que se instalará un firmware personalizado que permite transferir los mensajes y tramas recibidos al PC a través de una interfaz serie. Cuenta con una aplicación que se

ejecuta en el ordenador encargada de gestionar la carga de firmwares en el teléfono y otra que traduce e interpreta los mensajes recibidos de las capas 2 y 3 de la pila de protocolos GSM.

Osmocom proporciona un conjunto de firmwares ya operativos, entre los que se tiene uno que actúa de forma independiente presentando la información básica de la celda en la que se encuentra el terminal y los niveles de señal y otro que ejerce de intermediario entre la capa más baja de GSM y el software del PC y gracias al cual se puede gestionar el teléfono desde el ordenador manteniendo la operativa básica de un teléfono móvil, al tiempo que se analiza el tráfico. La herramienta *Wireshark* [50] se emplea como analizador de los datos obtenidos desde el programa de control. En la Figura 6.1 se puede observar un esquema general del mencionado conjunto de posibles aplicaciones corriendo tanto en el terminal móvil como en el PC.

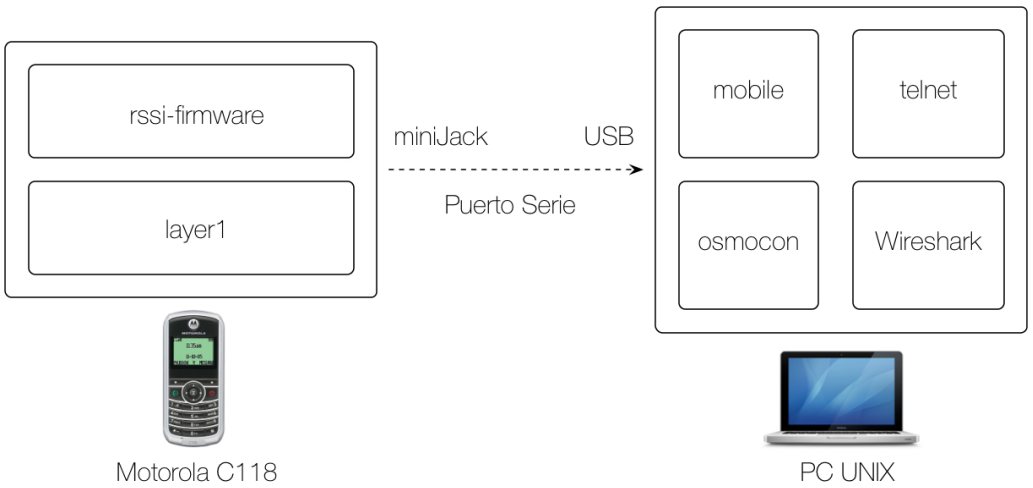


Figura 6.1: Arquitectura general OsmocomBB

Existen diversas guías para la instalación y configuración del sistema que se complementan entre sí. Por esta razón y como resultado del presente trabajo se ha generado una pequeña guía completa que se adjunta en el Apéndice 11.1. Una vez se haya completado el proceso de descarga del código y su compilación, y la instalación y configuración del sistema se puede comenzar a utilizar el analizador de redes.

6.1.1 Software en el terminal móvil (Baseband Firmware)

En aras de mantener una fácil accesibilidad y bajos costes de implementación, el proyecto Osmocom busca para sus desarrollos teléfonos móviles de bajo coste. Los modelos de la serie CXXX de Motorola no sólo cumplen dichas premisas, sino que además cuentan en su interior con el chip de comunicaciones Calypso con arquitectura ARM y conocido por estar presente en una gran multitud de aparatos electrónicos. Dada su amplia documentación y conocimiento entre la comunidad, además de que sus especificaciones y funcionamiento, este tipo de terminales con el chip Calyso se pueden reprogramar para obtener información de las capas inferiores de GSM, aspecto este que con otro equipamiento no sería posible.

El encargado de todo el procesado digital de la señal de la señal GSM es el DSP dentro del chip Calypso. Los usuarios del proyecto Osmocom han desarrollado un driver capaz de manejar el chip Calypso y de interactuar con el DSP mediante un sencillo

API, incluyendo interfaces abiertos para permitir la posterior interacción desde equipos externos.

Como se ha comentado anteriormente, Osmocom proporciona un conjunto de firmwares para realizar las tareas más usuales sobre el sistema, pero es posible el desarrollo de nuevos firmwares o personalizar los ya disponibles. En este sentido, es necesario habilitar un entorno de compilación cruzada, ya que se desea generar un firmware ejecutable en el teléfono móvil, pero dicha compilación se realizará en el PC con una arquitectura Intel, distinta a la del objetivo de la compilación, ARM.

Para la carga de un firmware en el terminal existen dos opciones. La primera consiste en cargar dicho firmware en la memoria flash del teléfono, reemplazando completamente el existente de fábrica y quedando, por tanto, inutilizado como teléfono convencional. La segunda opción, la cual ha sido la seleccionada en este proyecto, consiste en cargarlo en la memoria RAM, de forma que al reiniciar el teléfono el equipo vuelve a su configuración anterior. Esta solución es mucho menos agresiva.

La conexión del teléfono con el ordenador de control se realiza a través de un puerto serie que está habilitado a través del conector de audio del terminal. Para cargar el firmware deseado se ejecuta por medio del *Command Line Interface* (CLI) el programa `osmocon`, con el firmware deseado. Para que comience el proceso, se debe presionar brevemente el boton de encendido del dispositivo, y el firmware comenzará a descargarse en el teléfono.

```
$ ./osmocon -p /dev/ttyUSB0 -m c123xor
../../target/firmware/board/PHONE_TYPE/FIRMWARE.compalram.bin
```

Después de cargar el firmware, como vemos en la Figura 6.2, `osmocon` se convierte en un multiplexor/demultiplexor *High-Level Data Link Control* (HDLC), habilitando una comunicación multicanal con el dispositivo. La consola del teléfono está en uno de esos canales y será redirigida al terminal (`stdout`) en el que se ha ejecutado `osmocon`, mientras que el otro canal se ocupa de la lectura del archivo a cargar. También se abren otros dos canales por medio de los sockets de UNIX, uno para el gestor de arranque "*bootloader*" denominado `osmoload`, y otro para interactuar con los programas de capas superiores que se ejecutarán en el PC, por ejemplo `mobile`.

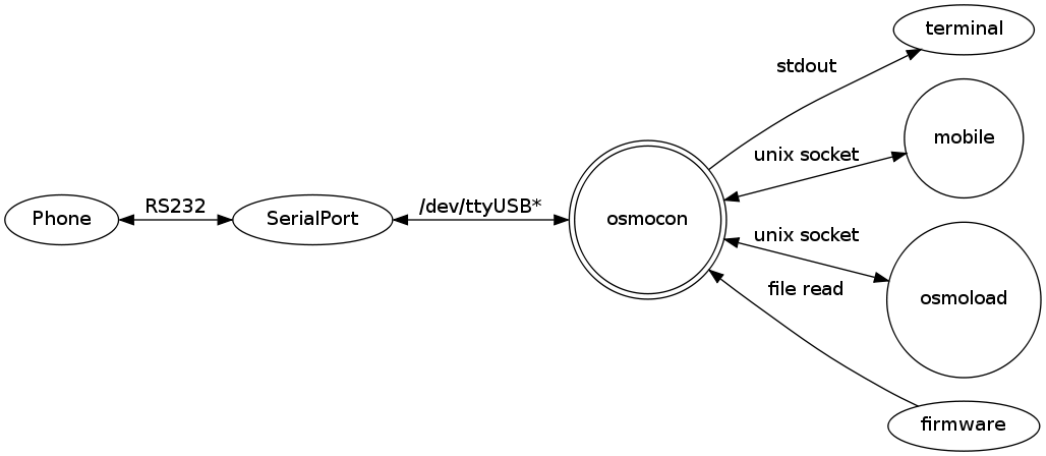


Figura 6.2: Canalización Osmocon

Para comprobar el correcto funcionamiento, cargamos el firmware `hello_world`, el cual muestra en la pantalla del terminal "*hello world*" y los niveles de batería.

```
$ ./osmocon -p /dev/ttyUSB0 -m c123xor
../../target/firmware/board/compal_e88/hello_world.compalram.bin
```

6.1.1.1 RSSI Monitor Firmware

Existen otros firmware disponibles que permiten, de forma independiente, monitorizar las características de la señal recibida (RSSI, *Received Signal Strength Indication*) y cierta información relacionada con el estándar GSM. Así, habilita la selección manual del ARFCN y visualizarlos individualmente o al completo.

Su ejecución en el terminal se realiza de forma análoga al caso anterior mediante el programa `osmocon`, escogiendo en este caso el firmware `rssi`. En la Figura 6.3 se observan dos capturas de las pantallas habilitadas en el teléfono mediante dicho firmwares. La imagen de la izquierda muestra el selector de ARFCN, y la ilustración a la derecha corresponde con las características de la señal seleccionada.

```
$ ./osmocon -p /dev/ttyUSB0 -m c123xor -c
../../target/firmware/board/compal_e88/rssi.highram.bin
../../target/firmware/board/compal_e88/chainload.compalram.bin
```

Figura 6.3: RSSI Monitor Firmware

6.1.1.2 Layer1

Los firmwares anteriores no permiten interactuar desde el PC con el teléfono, simplemente corren y se manejan desde el mismo. Para tener un manejo completo del terminal y sus funciones desde el ordenador, así como para habilitar la captura del tráfico GSM se utiliza el firmware `layer1`. Este firmware actúa de proxy entre el chip ARM y la interfaz a nivel físico de la pila GSM. Combinado con la aplicación `mobile` ejecutada en el "*host*" PC, se lograr controlar todas las funcionalidades GSM desde el equipo y se tiene una implementación GSM totalmente funcional. Al igual que los firmwares anteriores, para su carga se ejecuta `osmocon`.

```
$ ./osmocon -p /dev/ttyUSB0 -m c123xor
../../target/firmware/board/compal_e88/layer1.compalram.bin
```

Para que `layer1` habilite la cadena de transmisión del teléfono hay que editar una línea del fichero de texto que gestiona la compilación de los programas (`…/osmocom-bb/src/target/firmware/layer1/makefile`)

```
# Uncomment this line if you want to enable Tx (Transmit) Support. CFLAGS
+= -DCONFIG_TX_ENABLE
```

6.1.2 Software en el PC (Host Software)

Durante el proceso de carga del firmware en el terminal hemos utilizado la aplicación `osmocon`, que podríamos considerar la primera de las aplicaciones del lado host. Osmocon es una herramienta de consola para la gestión de los firmwares en el teléfono. Como se ha visto anteriormente, entre las aplicaciones ejecutadas en el PC, además se encuentran las encargadas de comunicarse con el teléfono e interactuar con él, entre las que se encuadra `mobile`.

`Mobile` contiene todo el software involucrado en las capas 2 y 3 de la pila de protocolos de GSM y opera siempre en colaboración con la capa 1 del teléfono ejecutándose gracias al firmware `layer1`. Implementa la mayoría de las acciones convencionales de un teléfono GSM, pues desde ella podemos controlar procedimientos como el registro en la red, solicitar una actualización de la posición, seleccionar la celda, realizar llamadas, enviar y recibir mensajes y servicios complementarios como el reenvío de llamadas. Tras su ejecución mediante el comando que se incluye a continuación, genera una terminal virtual a través de la cual acceder a la consola de control del terminal móvil ejecutando `layer1`.

```
$ cd osmocom-bb/src/host/layer23/src/mobile/
$ ./mobile -i 127.0.0.1
      -h --help             Ayuda
      -i --gsmtap-ip        IP destino para GSMTAP.
      -v --vty-port         Puerto de terminal virtual (4247 por defecto)
      -d --debug            Cambiar flags de debug
```

El acceso a la terminal virtual se realiza mediante el protocolo Telnet y para el control de la operación del terminal se definen un conjunto de comandos, que están recogidos en el Apéndice 11.2.

```
$ telnet localhost 4247
```

Adicionalmente, `mobile` habilita otro interfaz a través del cual redirige todas las tramas de tráfico GSM y permite que realizar la captura y análisis de todo el tráfico mediante cualquier aplicación externa o analizador de protocolos como por ejemplo Wireshark.

```
$ nc -u -l -p 4729 > /dev/null & wireshark -k -i lo -f 'port 4729'
```

GSMTAP es el formato en el que la aplicación `mobile` exporta las tramas. Introduce una pseudo-cabecera, adjunta en la Figura 6.4, que no forma parte del protocolo original. Encapsula las tramas GSM de la interfaz aire (Um) en paquetes UDP/IP. En este proyecto se ha hecho uso de Wireshark pues incorpora un disector de protocolos, que permite interpretar las tramas GSM que se recogen. Se describen los campos para un mejor entendimiento bajo la Tabla 6.1.

8 b	8 b	8 b	8 b	16 b	1 b	8 b	8 b	32 b	8 b	8 b	8 b
V	HL	PT	TS	ARFCN	UL	SNR	SL	FN	CT	AN	SS

Figura 6.4: Cabecera GSMTAP

Tabla 6.1: Elementos de la cabecera GSMTAP

Abreviatura	Campo	Descripción
V	Version	Versión GSMTAP
HL	Header length	Longitud de la cabecera en palabras (32 bits)
PT	Payload Type	Tipo de trama GSM
TS	Timeslot	Timeslot asignado
ARFCN	ARFCN	Canal de frecuencia portadora
UL	Uplink	Bandera que indica si es de subida
SNR	SNR	Nivel de relación señal/ruido
SL	Signal level	Nivel de recepción de señal (dBm)
FN	Frame Number	Número de trama en la secuencia GSM
CT	Channel Type	Tipo de canal empleado
AN	Antenna Number	Número de antena
SS	Subslot	Subslot dentro del timeslot

6.2 Procedimiento de uso del analizador GSM

En el apartado se han introducido un conjunto de aplicaciones cuyas funcionalidades hacen posible el análisis de las tramas GSM, `layer1` en el terminal móvil y `mobile` en el PC. Gracias a ambas seremos capaces de obtener información en tiempo real sobre el estado de la red y todas sus características. Se presentará un análisis de algunos de los procedimientos que los usuarios realizan habitualmente sobre las redes GSM. Una vez ejecutado `mobile` se puede interactuar con el teléfono a través de la terminal virtual.

El primer proceso que se ha observado, gracias al analizador, es la lectura de datos referentes al servicio del subscriptor contenidos en la tarjeta SIM, como se observa en la Figura 6.5, haciendo uso de las APDU mencionadas en el apartado 4.1.4. Se utilizan los comandos de selección y lectura de ficheros (SELECT y READ BINARY), de manera que la aplicación obtiene mediante comandos y respuestas toda la información que requiere. Podemos comprobar dichos datos introduciendo el comando **`show subscriber`**, cuya salida se adjunta. Tras su ejecución se muestran los códigos IMSI, TMSI, ICCID, SMS-SC, la red bajo la que se encuentra y la lista de redes preferidas y prohibidas del resto de operadores. También se muestra información sobre la localización de la red (LAI, *Location Area Identity*), los códigos de identificador del país (MCC, *Mobile Country Code*), identificador de la red (MNC, *Mobile Network Code*) e identificador de las estaciones base (CGI, *Cell Global Identifier).*

0.000000	localhost	localhost	GSMTAP	67 GSM SELECT File MF
0.069997	localhost	localhost	GSMTAP	89 GSM GET RESPONSE
0.097345	localhost	localhost	GSMTAP	67 GSM SELECT File EF.ICCID
0.149814	localhost	localhost	GSMTAP	80 GSM GET RESPONSE
0.193225	localhost	localhost	GSMTAP	75 GSM READ BINARY Offset=0
0.221553	localhost	localhost	GSMTAP	67 GSM SELECT File DF.GSM
0.290374	localhost	localhost	GSMTAP	89 GSM GET RESPONSE
0.317938	localhost	localhost	GSMTAP	67 GSM SELECT File EF.IMSI
0.371578	localhost	localhost	GSMTAP	80 GSM GET RESPONSE
0.455879	localhost	localhost	GSMTAP	74 GSM READ BINARY Offset=0
0.510864	localhost	localhost	GSMTAP	67 GSM SELECT File EF.LOCI
0.564190	localhost	localhost	GSMTAP	80 GSM GET RESPONSE
0.608846	localhost	localhost	GSMTAP	76 GSM READ BINARY Offset=0
0.636715	localhost	localhost	GSMTAP	67 GSM SELECT File EF.Kc
0.688975	localhost	localhost	GSMTAP	80 GSM GET RESPONSE
0.730027	localhost	localhost	GSMTAP	74 GSM READ BINARY Offset=0
0.760043	localhost	localhost	GSMTAP	67 GSM SELECT File EF.PLMNsel
0.812810	localhost	localhost	GSMTAP	80 GSM GET RESPONSE
0.919530	localhost	localhost	GSMTAP	113 GSM READ BINARY Offset=0
0.953780	localhost	localhost	GSMTAP	67 GSM SELECT File EF.HPPLMN
1.007215	localhost	localhost	GSMTAP	80 GSM GET RESPONSE
1.034702	localhost	localhost	GSMTAP	66 GSM READ BINARY Offset=0
1.064023	localhost	localhost	GSMTAP	67 GSM SELECT File EF.SPN
1.116686	localhost	localhost	GSMTAP	80 GSM GET RESPONSE
1.197307	localhost	localhost	GSMTAP	82 GSM READ BINARY Offset=0
1.228376	localhost	localhost	GSMTAP	67 GSM SELECT File EF.ACC
1.282550	localhost	localhost	GSMTAP	80 GSM GET RESPONSE
1.311030	localhost	localhost	GSMTAP	67 GSM READ BINARY Offset=0
1.340236	localhost	localhost	GSMTAP	67 GSM SELECT File EF.FPLMN
1.393096	localhost	localhost	GSMTAP	80 GSM GET RESPONSE
1.441012	localhost	localhost	GSMTAP	77 GSM READ BINARY Offset=0
1.469259	localhost	localhost	GSMTAP	67 GSM SELECT File MF
1.536965	localhost	localhost	GSMTAP	89 GSM GET RESPONSE

Figura 6.5: Lectura datos SIM

```
OsmocomBB# show subscriber
Mobile Subscriber of MS 'movil':
 IMSI: 214075500285725
 ICCID: 8934075500001120337
 SMS Service Center Address: +34609090909
 Status: U1_UPDATED  IMSI attached  TMSI 0x600b088c
         LAI: MCC 214  MNC 07  LAC 0x0f78  (Spain, movistar)
 Key: sequence 3  df 86 10 ab 93 50 3b 74
 Registered PLMN: MCC 214  MNC 07  (Spain, movistar)
 Access barred cells: no
 Access classes: C5
 List of preferred PLMNs:
        MCC    |MNC
        -------+-------
        208    |01        (France, Orange)
        208    |20        (France, Bouygues)
        234    |10        (Guernsey, O2)
        268    |06        (Portugal, TMN)
        268    |03        (Portugal, Optimus)
        222    |01        (Italy, TIM)
        262    |07        (Germany, O2)
        204    |08        (Netherlands, KPN)
        604    |00        (Morocco, Moditel)
        232    |03        (Austria, T-Mobile)
        228    |02        (Switzerland, Sunrise)
        272    |02        (Ireland, O2)
        334    |030        (Mexico, 030)
        202    |10        (Greece, Wind)
        226    |10        (Romania, Orange)
        226    |03        (Romania, Cosmote)
 List of forbidden PLMNs:
        MCC    |MNC    |cause
        -------+-------+-------
        214    |01     |#255        (Spain, Vodafone)
        214    |03     |#255        (Spain, Orange)
        214    |04     |#255        (Spain, Yoigo)
```

En este punto también se dispone de información de parámetros que solo se podrían obtener a través de un analizador de red, como información sobre las celdas adyacentes. Gracias a los comandos `show cell` y `show neighbour-cells`, cuya ejecución se adjunta en las Figuras 6.6 y 6.7, se dispone de datos como el nivel de relación señal-ruido mínimo (min-db), la potencia máxima de transmisión (max-pwr), el nivel de señal en recepción (rx-lev), su código de localización (LAC), su identificador de celda (cell ID) y otros parámetros de configuración. Se puede notar en las figuras que en las pruebas iniciales realizadas se emplea una tarjeta SIM del operador Movistar, campeando bajo la celda con ARFCN=7 (891,4 Mhz)[2].

```
OsmocomBB# show cell movil
ARFCN   |MCC    |MNC    |LAC    |cell ID|forb.LA|prio   |min-db |max-pwr|rx-lev
--------+-------+-------+-------+-------+-------+-------+-------+-------+-------
   2    |214    |07     |0x0f42 |0x0afd |n/a    |n/a    |-102   |   5   |-96
   3    |214    |07     |0x0f42 |0x01e1 |n/a    |n/a    |-102   |   5   |-96
   4    |n/a    |n/a    |n/a    |n/a    |n/a    |n/a    |n/a    |n/a    |n/a
   7    |214    |07     |0x0f42 |0x0981 |no     |normal |-102   |   5   |-81
   9    |214    |07     |0x0f42 |0x0000 |n/a    |n/a    |-102   |   5   |-92
  10    |214    |07     |0x0f42 |0x0000 |n/a    |n/a    |-102   |   5   |-95
  13    |214    |07     |0x0f42 |0x09bd |n/a    |n/a    |-102   |   5   |-90
  14    |214    |07     |0x0f42 |0x01e2 |n/a    |n/a    |-102   |   5   |-97
  15    |214    |07     |0x0f42 |0x09bc |n/a    |n/a    |-102   |   5   |-92
  18    |214    |07     |0x0f42 |0x0000 |n/a    |n/a    |-102   |   5   |-95
 114    |214    |01     |0x0fcc |0x6201 |no     |normal |-110   |   5   |-80
 526DCS|214    |07     |0x0f42 |0x01e5 |n/a    |n/a    | -87   |   0   |-105
```

Figura 6.6: Redes disponibles

```
OsmocomBB# show neighbour-cells movil
Serving cell:

ARFCN=7  RLA_C=-80  C1=22  C2=22  LAC=0x0f42

Neighbour cells:

#      |ARFCN  |RLA_C  |C1     |C2     |CRH    |prio   |LAC    |cell ID|usable
-------------------------------------------------------------------------------
 1 last|   4   |   -80 |-      |-      |-      |-      |-      |-      |no
 2     |  10   |   -88 |  14   |  14   |   0   |normal |0x0f42 |0x0000 |yes
 3     |   9   |   -89 |  13   |  13   |   0   |normal |0x0f42 |0x0000 |yes
 4     |  15   |   -90 |  12   |  12   |   0   |normal |0x0f42 |0x09bc |yes
 5     |  18   |   -91 |  11   |  11   |   0   |normal |0x0f42 |0x0000 |yes
 6     |  11   |   -93 |-      |-      |-      |-      |-      |-      |no
--- unmonitored cells: ---
 7     |   3   |   -95 |   7   |   7   |   0   |normal |0x0f42 |0x01e1 |yes
 8     |  14   |   -94 |   6   |   6   |   0   |normal |0x0f42 |0x01e2 |yes
 9     |  16   |   -99 |-      |-      |-      |-      |-      |-      |no
10     | 526   |   -98 |-      |-      |-      |-      |-      |-      |no
11     | 527   |  -107 |-      |-      |-      |-      |-      |-      |no
```

Figura 6.7: Celdas adyacentes

Así mismo, es posible observar durante toda la captura, tramas de tráfico dirigidas hacia otros terminales de la red, como las mostradas en la Figura 6.8. Dichas tramas, transportadas sobre canales comunes de control (CCCH), suelen contener datos para la búsqueda de terminales (*paging*), o información sobre parámetros radio de las celdas.

```
GSMTAP         83 (CCCH) (RR) System Information Type 13
GSMTAP         83 (CCCH) (RR) System Information Type 2
GSMTAP         83 (CCCH) (RR) System Information Type 3
GSMTAP         83 (CCCH) (RR) Paging Request Type 1
GSMTAP         83 (CCCH) (RR) Paging Request Type 1
GSMTAP         83 (CCCH) (RR) System Information Type 4
```

Figura 6.8: Tramas dirigidas a otros subscriptores

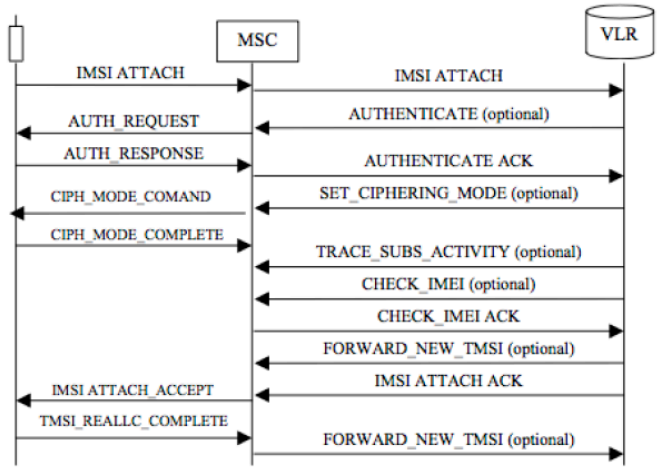
[2] Para la correspondencia entre ARFCN y la frecuencia portadora, se utiliza una fórmula "$f_c = f_0 + 0.2\ x\ n$", variando f_0 y n en función de la banda GSM que se emplea.

6.2.1 Registro en la red (IMSI Atach)

El siguiente paso que todo terminal realiza tras conocer los datos del subscriptor y sensar el entorno radioeléctrico es asociarse con una estación base. Para ello, la estación móvil que desea acceder a la red escucha tramas *broadcast* de las estaciones base colindantes, en busca de una que se ajuste a las características del subscriptor, tras lo que enviará una petición que la estación base contesta con una asignación inmediata como la presente en la Figura 6.9, en la que se incluye información acerca del canal dedicado y las características de la comunicación.

```
GSM CCCH - Immediate Assignment
▷ L2 Pseudo Length
▷ Protocol Discriminator: Radio Resources Management messages
  Message Type: Immediate Assignment
▽ Page Mode
    .... 0000 = Page Mode: Normal paging (0)
▷ Dedicated mode or TBF
▷ Channel Description
▷ Request Reference
▷ Timing Advance
▷ Mobile Allocation
▷ IA Rest Octets
```

Figura 6.9: Asignación Inmediata de canal




```
LAPDm          81 U, func=UI(DTAP) (RR) Measurement Report
LAPDm          81 U P, func=SABM(DTAP) (MM) Location Updating Request
LAPDm          81 U, func=UI(DTAP) (RR) System Information Type 5
LAPDm          81 U, func=UI
LAPDm          81 U F, func=UA(DTAP) (MM) Location Updating Request
LAPDm          81 U, func=UI(DTAP) (RR) System Information Type 6
LAPDm          81 I, N(R)=0, N(S)=0(DTAP) (RR) Ciphering Mode Command
LAPDm          81 S, func=RR, N(R)=1
LAPDm          81 I, N(R)=1, N(S)=0(DTAP) (RR) Ciphering Mode Complete
LAPDm          81 U, func=UI
LAPDm          81 U, func=UI(DTAP) (RR) Measurement Report
LAPDm          81 U, func=UI(DTAP) (RR) System Information Type 5
LAPDm          81 I, N(R)=1, N(S)=1(DTAP) (MM) Location Updating Accept
LAPDm          81 S, func=RR, N(R)=2
LAPDm          81 I, N(R)=1, N(S)=2(DTAP) (RR) Channel Release
LAPDm          81 S, func=RR, N(R)=3
LAPDm          81 U P, func=DISC
LAPDm          81 U, func=UI
```

Figura 6.10: Proceso de registro en la red

El proceso que se observa en la Figura 6.10, comienza con el envío por parte del terminal de una trama informando sobre medidas de la interfaz radio, tales como la potencia con la que transmite, el valor actual del *time advance* y otros parámetros relacionados con los niveles de señal. Junto a este informe se solicita una petición para actualizar la posición del terminal, *Location Updating Request*, mostrado en la Figura 6.11, en la que se incluyen características de la estación móvil que desea acceder al canal.

```
GSM A-I/F DTAP - Location Updating Request
▷ Protocol Discriminator: Mobility Management messages
  00.. .... = Sequence number: 0
  ..00 1000 = DTAP Mobility Management Message Type: Location Updating Request (0x08)
▷ Ciphering Key Sequence Number
▷ Location Updating Type - IMSI attach
▽ Location Area Identification (LAI)
  ▽ Location Area Identification (LAI) - 214/07/3906
       Mobile Country Code (MCC): Spain (214)
       Mobile Network Code (MNC): Telefonica Moviles Espana, SAU (07)
       Location Area Code (LAC): 0x0f42 (3906)
▽ Mobile Station Classmark 1
  ▽ Mobile Station Classmark 1
       0... .... = Spare: 0
       .01. .... = Revision Level: Used by GSM phase 2 mobile stations (1)
       ...0 .... = ES IND: Controlled Early Classmark Sending option is not implemented in the MS
       .... 0... = A5/1 algorithm supported: encryption algorithm A5/1 available
       .... .011 = RF Power Capability: class 4 (3)
▷ Mobile Identity - TMSI/P-TMSI (0xb80cb9da)
```

Figura 6.11: Location Update Request

Al igual que en cualquier protocolo de control del enlace derivado de HDLC, la estación base confirma la recepción de tramas por parte del terminal con el envío de tramas *Unnumbered Information* (UI). A continuación la estación base envía una trama de información, incluida en la Figura 6.12 con una lista de frecuencias (ARFCN) en las que hay portadoras transmitiendo canales de *broadcast* (BCCH), para que el móvil conozca todas las antenas que tiene a su disposición.

```
GSM A-I/F DTAP - System Information Type 5
▷ Protocol Discriminator: Radio Resources Management messages
  DTAP Radio Resources Management Message Type: System Information Type 5 (0x1d)
▽ Neighbour Cell Description - BCCH Frequency List
     ..0. .... = EXT-IND: The information element carries the complete BA (0)
     ...0 .... = BA-IND: 0
     00.. 000. = Format Identifier: bit map 0 (0x00)
     List of ARFCNs = 19 15 14 12 11 7 5 4 3
```

Figura 6.12: System Information

La estación base devuelve la petición de actualización de la posición confirmando que se dispone a realizar el proceso y de nuevo transmite una trama de información, esta vez con parámetros identificativos de la celda que se ofrece a prestar servicio. Posteriormente solicita el cifrado de las comunicaciones mediante el envío del *Ciphering Mode Command,* mostrado en la Figura 6.13, que el móvil confirma mediante el envío de una trama *Receiver Ready* (RR). Si todo es correcto enviará la trama *Ciphering Mode Complete* conteniendo el IMEI que lo identifica y por parte de la red se acepta el registro del terminal con la trama *Location Update Accept*. Se cerrará el canal mediante el envío de una trama *Channel Release*, que el terminal contesta mediante un *Disconnect* (DISC). El terminal continuará enviando informes de medidas de señal periódicamente.

```
GSM A-I/F DTAP - Ciphering Mode Command
▽ Protocol Discriminator: Radio Resources Management messages
     .... 0110 = Protocol discriminator: Radio Resources Management messages (0x06)
     0000 .... = Skip Indicator: No indication of selected PLMN (0)
  DTAP Radio Resources Management Message Type: Ciphering Mode Command (0x35)
▽ Cipher Mode Setting
     .... ...1 = SC: Start ciphering (1)
     .... 000. = Algorithm identifier: Cipher with algorithm A5/1 (0)
▽ Cipher Mode Response
     ...1 .... = CR: IMEISV shall be included (1)
```

Figura 6.13: Ciphering Mode Command

6.2.1.1 Desconexión (IMSI Detach)

De manera análoga se produce la desconexión del terminal de la red. Comienza, como se observa en la Figura 6.14, con el envío hacia la red de la indicación de la solicitud de separación *IMSI Detach Indication y* su correspondiente confirmación vía trama UI. Tras esto se produce el reenvío de dicha trama de solicitud hacia el terminal, al mismo tiempo que la liberación del canal *Channel Release*, que el terminal confirma con la trama RR. La liberación a nivel LAPD se realiza gracias al *Disconnect* (DISC) y dando por concluido el proceso al confirmar la estación base (UI).

```
LAPDm          83 U, func=UI(DTAP) (RR) Measurement Report
LAPDm          83 U P, func=SABM(DTAP) (MM) IMSI Detach Indication
LAPDm          83 U, func=UI
LAPDm          83 U F, func=UA(DTAP) (MM) IMSI Detach Indication
LAPDm          83 I, N(R)=0, N(S)=0(DTAP) (RR) Channel Release
LAPDm          83 S, func=RR, N(R)=1
LAPDm          83 U P, func=DISC
LAPDm          83 U, func=UI
```

Figura 6.14: Proceso de desconexión

6.2.2 Llamada de voz

Una vez conectados a la red de nuestro operador, posiblemente el procedimiento más utilizado sea el de la llamada de voz. Se estudia seguidamente el caso de una llamada saliente, cuya captura se muestra en la Figura 6.15. Desde la terminal virtual de `mobile` ejecutamos el comando `call +NUMBER` con lo que el terminal móvil transmite una primitiva de petición de establecimiento *Service Request* sobre un canal asociado rápido de control (FACCH). Esta primitiva contiene la información relativa a las capacidades del terminal, los algoritmos de cifrado que soporta, y los esquemas de codificación de la voz como se puede ver en la Figura 6.16. Al igual que en el proceso anterior de registro, se negocian las claves de cifrado mediante las primitivas *Ciphering Mode Command/Complete* y se envían reportes de medidas periódicamente.

```
LAPDm          81 U F, func=UA(DTAP) (MM) CM Service Request
LAPDm          81 U, func=UI(DTAP) (RR) System Information Type 6
LAPDm          81 I, N(R)=0, N(S)=0(DTAP) (RR) Ciphering Mode Command
LAPDm          81 S, func=RR, N(R)=1
LAPDm          81 I, N(R)=1, N(S)=0(DTAP) (RR) Ciphering Mode Complete
LAPDm          81 U, func=UI
LAPDm          81 U, func=UI(DTAP) (RR) System Information Type 5
LAPDm          81 U, func=UI(DTAP) (RR) Measurement Report
LAPDm          81 S, func=RR, N(R)=1
LAPDm          81 I, N(R)=1, N(S)=1(DTAP) (CC) Setup
LAPDm/GSM      81 I, N(R)=2, N(S)=1(DTAP) (CC) Call Proceeding (GSM MAP) invoke
LAPDm          81 S, func=RR, N(R)=2
LAPDm          81 U, func=UI(DTAP) (RR) System Information Type 6
LAPDm          81 U, func=UI
LAPDm          81 U, func=UI
LAPDm          81 U, func=UI(DTAP) (RR) System Information Type 5ter
LAPDm          81 U, func=UI(DTAP) (RR) Measurement Report
LAPDm          81 U, func=UI
LAPDm          81 U, func=UI
LAPDm          81 U, func=UI(DTAP) (RR) System Information Type 6
LAPDm          81 U, func=UI
LAPDm          81 U, func=UI
LAPDm          81 U, func=UI(DTAP) (RR) System Information Type 5
LAPDm          81 U, func=UI
LAPDm          81 U, func=UI(DTAP) (RR) Measurement Report
LAPDm          81 U, func=UI
LAPDm          81 U, func=UI(DTAP) (RR) System Information Type 6
LAPDm          81 I, N(R)=2, N(S)=2 (Fragment)
LAPDm          81 S, func=RR, N(R)=3
```

Figura 6.15: Procedimiento de llamada saliente

```
GSM A-I/F DTAP - CM Service Request
▷ Protocol Discriminator: Mobility Management messages
  00.. .... = Sequence number: 0
  ..10 0100 = DTAP Mobility Management Message Type: CM Service Request (0x24)
▷ Ciphering Key Sequence Number
▽ CM Service Type
    .... 0001 = Service Type: (1) Mobile originating call establishment or packet mode connection establishment
▽ Mobile Station Classmark 2
    Length: 3
    0... .... = Spare: 0
    .01. .... = Revision Level: Used by GSM phase 2 mobile stations (1)
    ...0 .... = ES IND: Controlled Early Classmark Sending option is not implemented in the MS
    .... 0... = A5/1 algorithm supported: encryption algorithm A5/1 available
    .... .000 = RF Power Capability: class 1 (0)
    0... .... = Spare: 0
    .0.. .... = PS capability (pseudo-synchronization capability): PS capability not present
    ..01 .... = SS Screening Indicator: Capability of handling of ellipsis notation and phase 2 error handling  (1)
    .... 1... = SM capability (MT SMS pt to pt capability): Mobile station supports mobile terminated point to point SMS
    .... .0.. = VBS notification reception: no VBS capability or no notifications wanted
    .... ..0. = VGCS notification reception: no VGCS capability or no notifications wanted
    .... ...1 = FC Frequency Capability: The MS does support the E-GSM or R-GSM
    0... .... = CM3: The MS does not support any options that are indicated in CM3
    .0.. .... = Spare: 0
    ..0. .... = LCS VA capability (LCS value added location request notification capability): LCS value added location req
    ...0 .... = UCS2 treatment: the ME has a preference for the default alphabet
    .... 0... = SoLSA: The ME does not support SoLSA
    .... .0.. = CMSP: CM Service Prompt: Network initiated MO CM connection request not supported
    .... ..0. = A5/3 algorithm supported: encryption algorithm A5/3 not available
    .... ...1 = A5/2 algorithm supported: encryption algorithm A5/2 available
▷ Mobile Identity - TMSI/P-TMSI (0x2165b139)
```

Figura 6.16: Service Request (llamada)

Con el móvil autenticado en la red, proceso que no se puede observar mediante el analizador por no encontrarse situado en el segmento de red adecuado, y negociadas las claves de sesión, el terminal inicia el establecimiento del canal de comunicaciones mediante la primitiva típica de LAPD *Setup*, que como se presenta en la Figura 6.17 contiene además del número llamado, información sobre las capacidades en términos de la codificación de la voz que ofrece el terminal. A continuación, si todo es correcto y la estación base puede satisfacer las demandas del terminal, se procede a cursar la llamada, informando de esto la primitiva *Call Proceeding*. En este punto, la red tratará de localizar al subscriptor llamado y enviará la trama *Alerting* cuando lo haya encontrado.

```
GSM A-I/F DTAP - Setup
▷ Protocol Discriminator: Call Control; call related SS messages
  01.. .... = Sequence number: 1
  ..00 0101 = DTAP Call Control Message Type: Setup (0x05)
▷ Bearer Capability 1 - (MS supports at least full rate speech version 1 and half rate speech version 1. MS has a greater preference for full rate speech
▷ Called Party BCD Number - (679099055)
▽ Call Control Capabilities
    Element ID: 0x15
    Length: 1
    0000 .... = Maximum number of supported bearers: 1
    .... 0... = MCAT: The mobile station does not support Multimedia CAT
    .... .0.. = ENICM: The mobile station does not support the Enhanced Network-initiated In-Call Modification procedure
    .... ..0. = PCP: the mobile station does not support the Prolonged Clearing Procedure
    .... ...1 = DTMF: the mobile station supports DTMF as specified in subclause 5.5.7 of TS 24.008
```

Figura 6.17: Setup (llamada saliente)

En el momento que el terminal llamado descuelga, se indica al otro extremo mediante la trama *Connect*, a lo que el llamante responderá con un *Connect Acknowledge*, quedando establecido el canal de comunicaciones para la conversación. Se puede comprobar en la Figura 6.18. Dado que la comunicación está cifrada, no tenemos acceso a las tramas de voz que se intercambian, pudiendo observar únicamente los reconocimientos y tramas de control LAPD. En el capítulo siguiente desplegaremos nuestra propia celda GSM. Si analizamos el tráfico en dicha situación, si observaremos las tramas de tráfico, al no emplear cifrado de los datos.

```
LAPDm          83 I, N(R)=2, N(S)=4(DTAP) (CC) Connect
LAPDm          83 S, func=RR, N(R)=5
LAPDm          83 I, N(R)=5, N(S)=2(DTAP) (CC) Connect Acknowledge
LAPDm          83 U, func=UI
```

Figura 6.18: Connect

Para la desconexión de la llamada, la estación base envía la primitiva *Disconnect*, dado que en este caso es el extremo llamado el que desea terminar la comunicación. El otro terminal contestará con una trama *Release*, y si todo es correcto se indica la liberación del canal mediante la trama *Release Complete* y el posterior cierre del canal a nivel LAPD (DISC). Proceso que se adjunta en la Figura 6.19.

```
LAPDm          83 I, N(R)=3, N(S)=5(DTAP) (CC) Disconnect
LAPDm          83 S, func=RR, N(R)=6
LAPDm          83 I, N(R)=6, N(S)=3(DTAP) (CC) Release
LAPDm          83 U, func=UI
LAPDm          83 S, func=RR, N(R)=4
LAPDm          83 U, func=UI(DTAP) (RR) System Information Type 6
LAPDm          83 I, N(R)=4, N(S)=6(DTAP) (CC) Release Complete
LAPDm          83 S, func=RR, N(R)=7
LAPDm          83 U, func=UI
LAPDm          83 I, N(R)=4, N(S)=7(DTAP) (RR) Channel Release
LAPDm          83 S, func=RR, N(R)=0
LAPDm          83 U P, func=DISC
LAPDm          83 U, func=UI
```

Figura 6.19: Desconexión de la llamada

En el caso de contar con una llamada entrante, el proceso es similar, pudiendo responder a la llamada ejecutando el comando `call answer`. La primera diferencia que encontramos en la Figura 6.20, se encuentra en la aparición de la trama *Paging Response*. Se debe a que es la red la que busca al terminal para informarle de que tiene una llamada para él. Esta trama contiene todas las características disponibles de la estación móvil, como en el caso de la llamada saliente la petición de servicio. Se produce la negociación de claves, tras lo que, en este caso, la estación base envía el *Setup*, presente en la Figura 6.21, conteniendo el número llamante. El terminal acepta la llamada transmitiendo la primitiva *Call Confirmed* sin llegar a descolgar, como confirmación a los parámetros de configuración. Seguidamente se produce el Alerting avisando de la llamada, en este caso se recibe en la terminal `Incoming call (from NUMBER)`.

```
LAPDm          81 U F, func=UA(DTAP) (RR) Paging Response
LAPDm          81 I, N(R)=0, N(S)=0(DTAP) (RR) Ciphering Mode Command
LAPDm          81 S, func=RR, N(R)=1
LAPDm          81 I, N(R)=1, N(S)=0(DTAP) (RR) Ciphering Mode Complete
LAPDm          81 U, func=UI(DTAP) (RR) Measurement Report
LAPDm          81 I, N(R)=1, N(S)=1(DTAP) (CC) Setup
LAPDm          81 S, func=RR, N(R)=2
LAPDm          81 I, N(R)=2, N(S)=1(DTAP) (CC) Call Confirmed
LAPDm          81 S, func=RR, N(R)=2
LAPDm          81 I, N(R)=2, N(S)=2(DTAP) (CC) Alerting
LAPDm          81 I P, N(R)=3, N(S)=2 (Fragment)
LAPDm          81 S F, func=RR, N(R)=3
LAPDm          81 I, N(R)=3, N(S)=3(DTAP) (RR) Assignment Command
LAPDm          81 S, func=RR, N(R)=4
LAPDm          81 U, func=UI(DTAP) (RR) Measurement Report
LAPDm          81 U P, func=SABM
LAPDm          81 U, func=UI
LAPDm          81 U F, func=UA
LAPDm          81 I, N(R)=0, N(S)=0(DTAP) (RR) Assignment Complete
LAPDm          81 U, func=UI
```

Figura 6.20: Proceso de llamada entrante

```
GSM A-I/F DTAP - Setup
▷ Protocol Discriminator: Call Control; call related SS messages
  00.. .... = Sequence number: 0
  ..00 0101 = DTAP Call Control Message Type: Setup (0x05)
▷ Bearer Capability 1 - (Full rate support only MS/fullrate speech version 1 supported)
▷ Calling Party BCD Number - (679099055)
```

Figura 6.21: Setup (llamada entrante)

La comunicación no se establece hasta que finaliza el procedimiento de asignación, mediante el cual los dos extremos acuerdan los parámetros de la llamada. El terminal que inició la conexión transmite el comando *Assignment Command*, cuya captura se presenta en la Figura 6.22 y el extremo llamado responde si todo es correcto con un *Assignment Complete*.

```
GSM A-I/F DTAP - Assignment Command
▷ Protocol Discriminator: Radio Resources Management messages
  DTAP Radio Resources Management Message Type: Assignment Command (0x2e)
▽ Channel Description 2 - Description of the First Channel, after time
    0000 1... = TCH/F + FACCH/F and SACCH/F
    .... .011 = Timeslot: 3
    100. .... = Training Sequence: 4
    ...1 .... = Hopping channel: Yes
    Hopping channel: MAIO 0
    Hopping channel: HSN 28
▷ Power Command
▷ Cell Channel Description
▽ Channel Mode - Mode of the First Channel(Channel Set 1)
    Element ID: 0x63
    Channel Mode: speech full rate or half rate version 2(GSM EFR) (33)
▷ Mobile Allocation - Mobile Allocation, after time
```

Figura 6.22: Assignment Command

El proceso de desconexión es igual al comentado en el caso de la llamada saliente, variando únicamente el orden y autoría de las tramas en función de quien finaliza la llamada.

6.2.3 Envío y recepción de SMS

Otra de las acciones más repetidas, al menos hasta hace unos años, entre los usuarios de las redes móviles GSM, es el envío de mensajes cortos SMS. Es posible realizar el envío de un mensaje SMS desde la terminal virtual de `mobile` que controla el teléfono mediante el comando `sms MS_NAME NUMBER MSG`, procedimiento que analizaremos en primer lugar.

Al igual que en los caso anteriores, la estación base asigna un canal dedicado al terminal tras la petición de servicio de este último que, como se observa en la Figura 6.23, en este caso corresponde al servicio de mensajes cortos. Se repite todo el proceso de autenticación, negociación de claves y reportes de medidas de los casos anteriores.

```
GSM A-I/F DTAP - CM Service Request
▷ Protocol Discriminator: Mobility Management messages
  00.. .... = Sequence number: 0
  ..10 0100 = DTAP Mobility Management Message Type: CM Service Request (0x24)
▷ Ciphering Key Sequence Number
▽ CM Service Type
    .... 0100 = Service Type: (4) Short message service
▷ Mobile Station Classmark 2
▷ Mobile Identity - TMSI/P-TMSI (0x2d261033)
```

Figura 6.23: Service Request (SMS)

La estación móvil envía el mensaje hacia el MSC o el SGSN en caso de contar con una red GPRS. Al tratarse de un mensaje *Mobile Originated* irá transportado sobre la unidad de datos SMS-SUBMIT, como se vio en el apartado 4.1.1.1. En dicha unidad de datos viaja la dirección en formato E.164 [21] del centro de mensajería de la red (*Service Center*, SC), o SMSC al que le será entregado el mensaje para la posterior redirección al correspondiente centro de mensajería de la red bajo la que se encuentre el terminal asociado al destinatario. Como se puede ver en la Figura 6.24, en el mensaje viajan dos direcciones, la del SC y la del destinatario.

```
GSM A-I/F RP - RP-DATA (MS to Network)
  Message Type RP-DATA (MS to Network)
▷ RP-Message Reference
▷ RP-Originator Address
▷ RP-Destination Address - (34609090909)
▷ RP-User Data
GSM SMS TPDU (GSM 03.40) SMS-SUBMIT
  0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
  .0.. .... = TP-UDHI: The TP UD field contains only the short message
  ..0. .... = TP-SRR: A status report is not requested
  ...0 0... = TP-VPF: TP-VP field not present (0)
  .... .0.. = TP-RD: Instruct SC to accept duplicates
  .... ..01 = TP-MTI: SMS-SUBMIT (1)
  TP-MR: 132
▷ TP-Destination-Address - (54321)
▷ TP-PID: 0
▷ TP-DCS: 0
  TP-User-Data-Length: (11) depends on Data-Coding-Scheme
▽ TP-User-Data
    SMS text: Hola mundo!
```

Figura 6.24: SMS-SUBMIT

Si el mensaje llega a la estación base correctamente, ésta confirma su recepción mediante el envío de una trama CP-ACK. Cuando el receptor reciba el mensaje, el terminal destinatario devolverá un reconocimiento afirmativo sobre la trama RP-ACK confirmando la entrega. Proceso a continuación recogido en la Figura 6.25.

```
GSM SMS      83 I, N(R)=0, N(S)=4(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
LAPDm        83 I, N(R)=5, N(S)=0(DTAP) (SMS) CP-ACK
LAPDm        83 I, N(R)=5, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-ACK (MS to Network)
```

Figura 6.25: Transmisión de SMS saliente

En el caso de contar con un mensaje entrante al analizador, de forma análoga al proceso de envío visto, únicamente se podrán observar las tramas que se reciban en el terminal que actúa como analizador. El mensaje que se reciba en este caso será del tipo *Mobile Terminated*, por lo que irá sobre una unidad de datos SMS-DELIVER, representada en la Figura 6.27. En la pantalla de la terminal virtual se muestra un mensaje como el de la Figura 6.26 avisando de la llegada de dicho mensaje. Al igual que en el caso del mensaje saliente, la estación base confirma la llegada con una trama CP-ACK y el receptor con la trama RP-ACK, como se observa en la Figura 6.26.

```
% (MS movil)
% SMS from 12345: 'Hola mundo!'
```

Figura 6.26: Mensaje entrante al analizador

```
GSM SMS TPDU (GSM 03.40) SMS-DELIVER
  0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
  .0.. .... = TP-UDHI: The TP UD field contains only the short message
  ..0. .... = TP-SRI: A status report shall not be returned to the SME
  .... .0.. = TP-MMS: More messages are waiting for the MS in this SC
  .... ..00 = TP-MTI: SMS-DELIVER (0)
▷ TP-Originating-Address - (12345)
▷ TP-PID: 0
▷ TP-DCS: 0
▷ TP-Service-Centre-Time-Stamp
  TP-User-Data-Length: (5) depends on Data-Coding-Scheme
▷ TP-User-Data
```

Figura 6.27: SMS-DELIVER

Capítulo 7

Despliegue de una picocélula GSM/GPRS

Si durante el capítulo anterior se menciona la inaccesibilidad que presentan ciertos elementos de la red GSM, el mismo problema se tiene cuando se trata de acceder a elementos que formen parte de la infraestructura de red necesaria para montar una red GSM, celosamente protegidos por la industria de la telefonía móvil. El objetivo de este proyecto será, siguiendo una filosofía similar a la empleada para el caso del analizador de redes GSM, desarrollar una implementación de la arquitectura de red GSM totalmente funcional para terminales comerciales, manteniendo un bajo coste mediante el uso de software libre. La implementación que se realice se restringirá al ámbito investigador y académico, por tanto, empleando una potencia de transmisión muy reducida, para restringir el área de cobertura a distancias inferiores a la decena de metros. De manera que no se produce ninguna intromisión en redes comerciales.

En el mercado existen una gran variedad de estaciones base GSM disponibles cuyos precios varían en función de sus características. Sin embargo el principal escollo lo supone el software necesario para su funcionamiento, ya que éste no suele ser público, su coste es prohibitivo y suele estar limitado a los desarrollos propios de cada operador. Como solución, surgen desde el ámbito investigador ciertas iniciativas, como OpenBTS [41], plataforma que utiliza tecnologías SDR para implementar pilas de protocolos bajo estándares 3GPP como GSM o UMTS. No obstante, en este trabajo se optará por tomar como base el proyecto OpenBSC [40], nuevamente desarrollado desde la comunidad Osmocom.

7.1 OpenBSC

El objetivo del proyecto OpenBSC es proveer toda la infraestructura necesaria para experimentar de un modo práctico con las redes GSM, adquiriendo conocimientos a bajo nivel sobre el equipamiento real e investigar la operativa y la seguridad del estándar desde el lado de la red. Incluye la implementación software de toda la infraestructura de red GSM que se encuentra más allá de la BTS en la interfaz A-bis como son el BSC, MSC, HLR, AuC, VLR y EIR. Constituye así, en unión de una BTS, una red GSM completamente funcional, de acuerdo a los estándares ETSI/3GPP que especifican el sistema GSM 08.51 [5] y 12.21 [6]. Existe la posibilidad de realizar el despliegue de OpenBSC empleando una BTS ad-hoc construida desde cero utilizando la iniciativa “UmTRX” [43], consistente en una plataforma programable de radiofrecuencia basada en tecnología SDR, capaz de operar en cualquier frecuencia en el rango de 0.3-3.8GHz. OpenBSC también permite utilizar BTS comerciales, contando actualmente con soporte para el modelo BS-11 de Siemens, sysmoBTS 1002 de sysmocom [44], UmSITE y UmDESK de fairwaves [45] y los modelos nanoBTS del fabricante ip.access [42]. Partiendo de la implementación de las funcionalidades mínimas que posee una red GSM, como las llamadas de voz o los mensajes de texto, se han ido incluyendo más capacidades hasta lograr dotar a OpenBSC de soporte para tráfico de datos GPRS y otras aplicaciones, como la simulación de ciertos elementos de red, o incluso de tarjetas SIM.

Hay tres modos de uso del software OpenBSC en función del hardware que se disponga y de las características que se desee emplear. La opción denominada *Network-in-the-box* (NITB) se muestra en la Figura 7.1. Concentra todos los elementos de la red como el BSC, MSC, HLR, en un solo lugar, en contraposición con la arquitectura típica de GSM, dónde los elementos se encuentran distribuidos. Éste modo no permite conexión con otras redes. Por lo que si se desea conectar con llamadas desde o hacia otras redes se debe incluir en la arquitectura una centralita de comunicaciones de voz externa, como *Linux Call Router* (LCR) junto a OpenBSC en su modo NITB. La tercera posibilidad es emplear OpenBSC como BSC únicamente y ejecutar por separado el resto de elementos de la red (MSC, VLR, HLR y AuC), ofreciéndo la opción de desarrollar elementos propios para explotar nuevas funcionalidades.

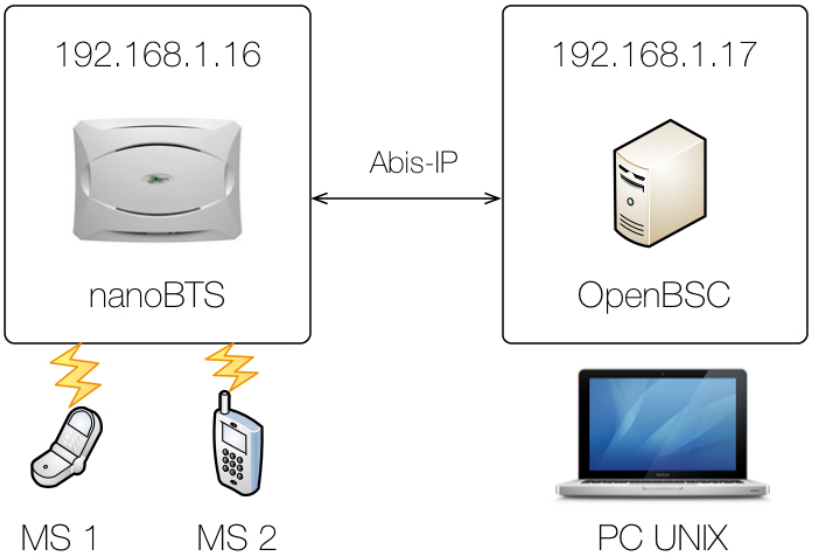


Figura 7.1: Arquitectura General OpenBSC

7.1.1 ip.access nanoBTS

Se trata de una sencilla BTS que cuenta con una interfaz "*A-bis*" sobre IP, utiliza Ethernet 100-Base-Tx en su capa física, llevando tanto la información como el suministro eléctrico necesario mediante *Power over Ethernet* (PoE) por lo que necesitaremos un adaptador *mid-span* para su alimentación y conexionado.

Se ha optado por el modelo nanoBTS 1800, mostrado en la Figura 7.2, del proveedor ip.access para este trabajo entre otros motivos por su bajo coste y consumo eléctrico, su reducido tamaño (poco mayor que el de un punto de acceso WiFi), el soporte para tráfico de datos y su mejor integración con el proyecto OpenBSC. Dichas características la hacen ideal para proveer servicio bajo determinadas circunstancias, como por ejemplo, áreas rurales, siendo posible su alimentación mediante energías renovables, lo que elimina la necesidad de realizar grandes inversiones en acometidas eléctricas. También es interesante su aplicación en entornos embarcados, como aeronaves o barcos, donde las exigencias de consumo también juegan su papel, o simplemente para mejorar la cobertura en interiores de una pequeña o mediana empresa, un centro comercial o un aeropuerto.

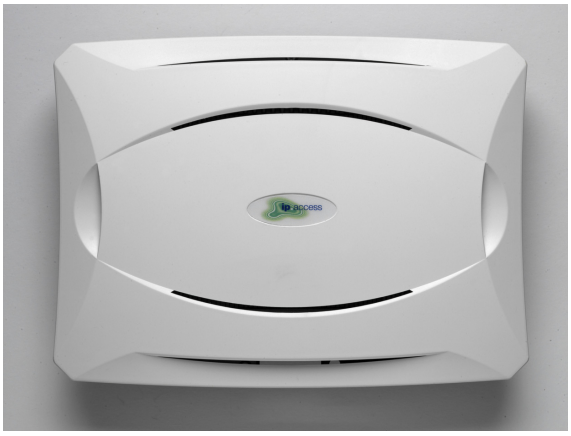


Figura 7.2: ip.access nanoBTS 1800

Al no contar con especificaciones de los protocolos propietarios de ip.access empleados en la nanoBTS, la comunidad de desarrolladores del proyecto OpenBSC se vio obligada a analizar mediante ingeniería inversa las tramas intercambiadas entre una BSC comercial y una nanoBTS. La interfaz "*A-bis*" sobre IP proporciona la conexión con el PC sobre sockets de UNIX. En el nivel de enlace se emplean los protocolos hablados entre la BTS y el BSC en GSM, especificados en los ETSI/3GPP GSM TS 12.21 y 08.58 *Operation and Maintenance Link* (OML) y *Radio Signaling Link* (RSL), a los que se les añade una pequeña cabecera sobre sesiones TCP. El flujo de datos transportado sobre canales de tráfico (TCH) se transporta en segmentos UDP utilizando el protocolo *Real Time Protocol* (RTP), debido a sus requerimientos de retardo. También se provee desde la comunidad OpenBSC de un disector para el analizador de protocolos Wireshark llamado gsm_abis_rsl.

Es posible operar la BTS en un modo denominado *multi-TRX*, donde se configuran varias unidades nanoBTS para funcionar como múltiples antenas de una misma BTS, manejadas desde un solo BSC, en lugar de comportarse como BTS individuales, siendo posible acumular un total de cuatro nanoBTS. Esta configuración puede resultar interesante para despliegues que requieran cubrir grandes áreas de cobertura, por ejemplo en zonas rurales.

7.1.1.1 Configuración nanoBTS

Como se ha mencionado anteriormente, la picocélula nanoBTS se conecta mediante cable Ethernet con la red, a la que deberá estar conectado el PC UNIX, a la vez que se alimenta gracias al adaptador PoE necesario. Una vez realizadas correctamente dichas conexiones, la BTS está configurada de fábrica para obtener una dirección IP automáticamente mediante *Dynamic Host Configuration Protocol* (DHCP). También escucha posibles conexiones entrantes *A-bis-over-IP*, enlace denominado *Secondary OML Link*. Uno de los parámetros que se debe configurar es el identificador de la BTS *Unit ID*, que por defecto tiene con el valor "65535/0/0", y no será válido hasta ser modificado.

Utilizaremos la aplicación `ipaccess-find` para identificar la picocelda dentro de la red y la dirección IP obtenida. Para ello, la aplicación genera paquetes de *broadcast Identity Request* del protocolo *IPA protocol* [42] propietario de ip.access, a los que la BTS responderá en caso de recibirlos. Se muestra a continuación un ejemplo de su ejecución y el paquete de broadcast que es enviado en la Figura 7.3.

```
$ ./ipaccess-find eth0
ipaccess-find (C) 2009 by Harald Welte
This is FREE SOFTWARE with ABSOLUTELY NO WARRANTY
Trying to find ip.access BTS by broadcast UDP...
MAC_Address='00:02:95:00:84:88'  IP_Address='192.168.1.16'
Unit_ID='1800/0/0'  Location_1=''  Location_2='BTS_NBT131G'
Equipment_Version='165g029_79'  Software_Version='168a352_v142b30d0'
Unit_Name='nbts-00-02-95-00-84-88'  Serial_Number='00206269'
```

```
Internet Protocol Version 4, Src: 192.168.1.17 (192.168.1.17), Dst: 255.255.255.255
User Datagram Protocol, Src Port: ii-admin (3006), Dst Port: ii-admin (3006)
IPA protocol ip.access, type: IPA
  DataLen: 19
  Protocol: IPA (0xfe)
GSM over IP ip.access CCM sub-protocol
  MessageType: IDENTITY REQUEST (0x04)
  Tag: MAC Address (0x07)
  Tag: IP Address (0x06)
  Tag: Unit ID (0x08)
  Tag: Location (0x02)
  Tag: Unit Type (0x03)
  Tag: Equipment Version (0x04)
  Tag: Software Version (0x05)
  Tag: Unit Name (0x01)
  Tag: Serial Number (0x00)
```

Figura 7.3: Datagrama UDP ipaccess-find

Una vez identificada, debemos configurar la dirección IP del enlace *Primarly OML IP* y el identificador *Unit ID*. Para ello, ejecutamos el software `ipaccess-config` junto a las opciones `--unit-id`, `--oml-ip`, y `--restart`, acompañados de la dirección IP de la BTS, como se muestra a continuación. Tras dicha ejecucion, si la BTS confirma que todo es correcto, se reiniciará, teniendo la configuración tal y como se presentó en la Figura 7.1 (configuración empleada en este proyecto).

```
$ ./ipaccess-config -u 1234/0/0 -o 192.168.1.17 -r 192.168.1.16
ipaccess-config (C) 2009-2010 by Harald Welte and others
This is FREE SOFTWARE with ABSOLUTELY NO WARRANTY
Trying to connect to ip.access BTS ...
OML link established using TRX 0
setting Unit ID to '1234/0/0'
setting primary OML link IP to '192.168.1.17'
restarting BTS
```

7.1.2 osmo-nitb

Para el despliegue celular de este proyecto se ha optado por emplear el modo *Network-In-The-Box* del proyecto OpenBSC, por su sencillez y compatibilidad con los elementos hardware de los que se disponen. Al igual que en el caso del analizador de redes GSM, se elabora durante el desarrollo del trabajo una pequeña guía de instalación, adjunta en el apéndice 11.3. Por lo tanto a continuación no se profundizará en el proceso de instalación del sistema sino en su empleo. Como se ha mencionado y se puede observar en la Figura 7.4, el modo NITB concentra todos los elementos en un mismo punto, reduciendo considerablemente la carga de tráfico que soporta la red y la capacidad de procesado necesaria para su ejecución.

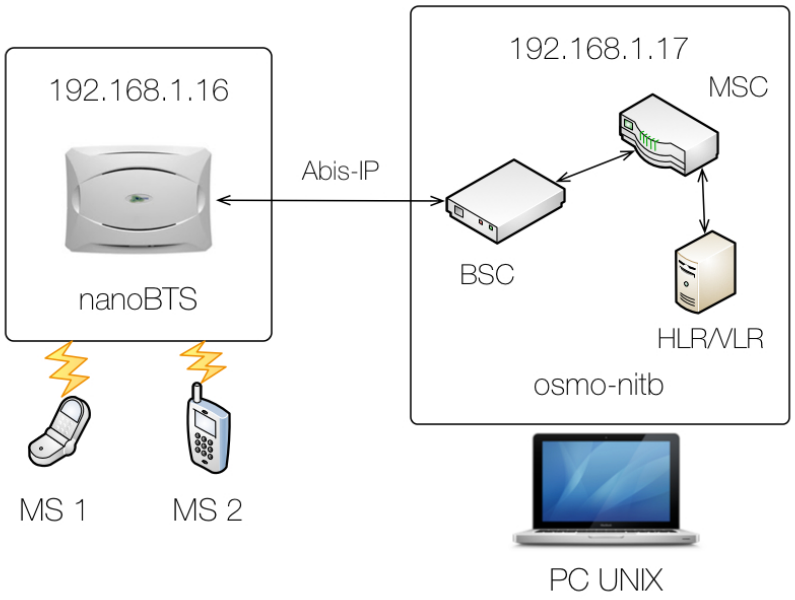


Figura 7.4: Arquitectura OpenBSC "Network-In-The-Box"

La aplicación `osmo-nitb` emplea un archivo de configuración que deberá ser actualizado de acuerdo al despliegue a realizar. Entre otras opciones, es posible definir los canales alojados en los timeslots, optando en nuestro caso por la distribución que se muestra en la Figura 7.4 la frecuencia de operación (ARFCN), el identificador de la red (MCC/MNC) y otros parámetros. Se recogen en la Tabla 7.1 algunos de los más importantes empleados. En el apéndice 11.4 se adjunta la configuración empleada.

La frecuencia de operación ha sido escogida tratando de no interferir con los canales ya ocupados, así como se ha restringido la potencia de transmisión al mínimo posible. Se define el acceso a la red cerrado para evitar que un terminal cercano se registre en la misma incontroladamente.

Tabla 7.1: Configuración empleada para osmo-nitb

Parámetro	Valor	Descripción
mcc	214	Código identificador del país (España)
mnc	25	Código identificador de la red
short/long name	WEGA	Nombre de la red
auth policy	closed	Política de acceso cerrada
type	nanobts	BTS utilizada
band	DCS1800	Banda GSM de operación
arfcn	678	Frecuencia de operación
ip.access unit_id	1234 0	Identificador de la BTS

TS0	TS1	TS2	TS3	TS4	TS5	TS6	TS7
CCCH SDCCH4	SDCCH8	TCH/F	TCH/F	TCH/F	TCH/F	TCH/F	TCH/F

Figura 7.5: Distribución de timeslots OpenBSC

7.1.3 Operación de la red

Una vez realizadas todas las configuraciones oportunas, tanto referentes a la BTS como al resto de la red, se puede iniciar la celda ejecutando la aplicación `osmo-nitb`.

Tras su ejecución, se produce el proceso mostrado en la Figura 7.6 donde se inicializan la base de datos y la cola de mensajes SMS y se establecen los enlaces OML primario y secundario, quedando la célula generada, transmitiendo en el ARFCN indicado y lista para dar servicio a los terminales.

```
<0019> input/ipaccess.c:1007 enabling ipaccess BSC mode
DB: Database initialized.
DB: Database prepared.
<001d> sms_queue.c:220 Attempting to send 20 SMS
<001d> sms_queue.c:280 SMSqueue added 0 messages in 0 rounds
<0019> input/ipa.c:308 accept()ed new link from 192.168.1.16 to port 3002
Failure Event Report Type=communication failure Severity=critical failure Probab
le cause= 03 03 11 Additional Text=
<0019> input/ipa.c:308 accept()ed new link from 192.168.1.16 to port 3003
<0004> bsc_init.c:265 bootstrapping RSL for BTS/TRX (0/0) on ARFCN 678 using MCC
=214 MNC=25 LAC=1 CID=0 BSIC=1 TSC=7
```

Figura 7.6: Arranque osmo-nitb

Al haber configurado una política cerrada de acceso, los terminales no se asocian automáticamente con la red bajo su influencia, sino que se debe ejecutar una búsqueda manual. Puesto que el nombre asociado a la red desplegada no está configurado entre las que se incluyen en las tarjetas SIM, los terminales móviles muestran el identificador configurado (MCC-MNC), como se puede comprobar en la Figura 7.7. El primer intento de acceso será fallido ya que se debe autorizar al subscriptor como se indicará en el siguiente apartado. No obstante, dicho intento servirá para conocer y registrar los datos del subscriptor en nuestro HLR y realizar dicha autorización.

Figura 7.7: Búsqueda y selección de red

7.1.3.1 HLR/VLR

Como se describió en el apartado 2.2.3, el HLR es el elemento de la red encargado de la gestión de los subscriptores, apoyado en el VLR, que lleva un registro de los visitantes actualmente bajo la celda. El proyecto OpenBSC implementa ambos elementos mediante una base de datos SQL, de manera sencilla y accesible en todo momento para el software. Consta de doce tablas, de entre las que cabría destacar la que recoge el equipamiento registrado (`equipment`) y la de subscriptores (`subscribers`).

OpenBSC obtiene el IMEI y el IMSI a partir de las peticiones *Location Updating Request* que escucha y crea una nueva entrada en la tabla correspondiente para el equipamiento y los subscriptores cada vez que sea necesario.

Los valores almacenados en la base de datos son accesible bien a través de un cliente SQL tradicional o a través de la terminal virtual que incluye `osmo-nitb`. A continuación se incluye una de las operaciones habituales en la gestión de la red, como es la autorización del acceso a un subscriptor, en primer lugar desde la terminal virtual y a continuación mediante el envío directo de secuencias SQL. Tras la ejecución de uno de estos dos comandos, el terminal está autorizado para acceder a la red.

```
subscriber imsi 214075500285725 authorized 1
$ sqlite3 hlr.sqlite
update Subscriber set authorized=1 where imsi=214075500285725;
```

El siguiente paso en la gestión de un nuevo usuario es la asignación de un número de teléfono, de manera que sea alcanzable para el resto de terminales bajo la red. Estos dos comandos deben ser repetidos cada vez que se desea registrar un nuevo terminal en nuestra red. La autenticación GSM en este caso no se produce, dado que para ello se deben disponer tarjetas SIM con claves, y en la configuración se ha establecido no utilizarla por sencillez. Se incluye para ilustrar el fin del proceso la Figura 7.8, en la que se puede comprobar el terminal asociado con la red, y un nivel de cobertura de -50 dBm, dada la cercanía con la BTS.

```
subscriber imsi 214075500285725 extension 12345
$ sqlite3 hlr.sqlite
update Subscriber set extension=12345 where imsi=214075500285725;
```

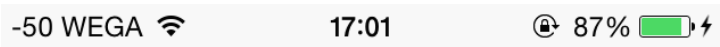


Figura 7.8: Terminal asociado con la red

También desde la comunidad de desarrolladores de OpenBSC se ha escrito en el lenguaje de programación PHP una interfaz web para mejorar el acceso al HLR. Como podemos observar en la Figura 7.9, proporciona una vista general de su estado y permite editar directamente desde el navegador la mayoría de los parámetros contenidos en la base de datos, autorizar subscriptores, fijar números de teléfono, enviar mensajes de difusión, leer los últimos mensajes intercambiados bajo la red o enviar un mensaje a un subscriptor en concreto. También se muestra un resumen de algunas estadísticas de la red.

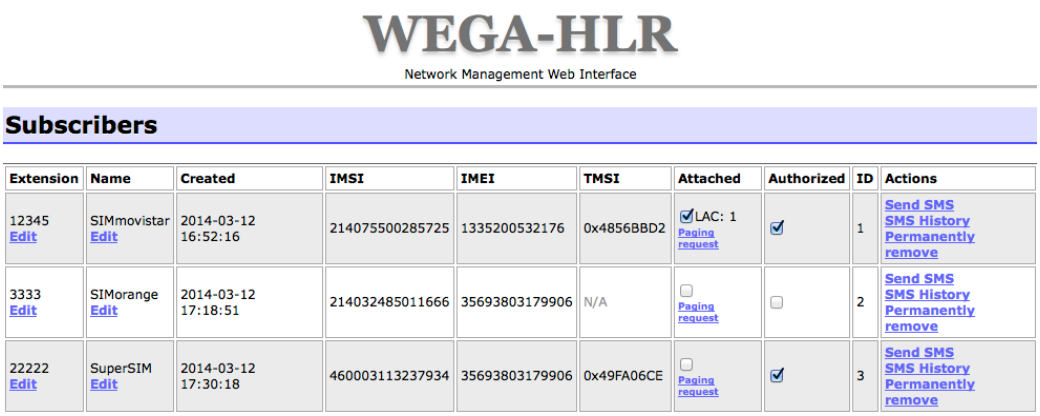


Figura 7.9: Interfaz Web HLR

7.1.4 Operaciones de Gestión

Es posible acceder a multitud de información en tiempo real acerca de la red, como su estado, estadísticas de utilización, parámetros de configuración de la red, las características de la BTS transmitiendo, los subscriptores que se encuentran bajo servicio de la red y otras opciones. Para ello, se puede hacer uso de la terminal virtual tal como se muestra a continuación.

```
OpenBSC# show statistics
Channel Requests         : 10 total, 0 no channel
Channel Failures         : 0 rf_failures, 0 rll failures
Paging                   : 0 attempted, 0 complete, 0 expired
BTS failures             : 0 OML, 0 RSL
Channel Requests         : 2 total, 0 no channel
Location Update          : 3 attach, 1 normal, 0 periodic
IMSI Detach Indications  : 0
Location Update Response: 2 accept, 0 reject
Handover: 0 attempted, 0 no_channel, 0 timeout, 0 completed, 0 failed
SMS MO                   : 10 submitted, 0 no receiver
SMS MT                   : 10 delivered, 0 no memory, 0 other error
MO Calls                 : 2 setup, 1 connect ack
MT Calls                 : 2 setup, 1 connect

OpenBSC# show network
BSC is on Country Code 214, Network Code 25 and has 1 BTS
  Long network name: 'WEGA'
  Short network name: 'WEGA'
  Authentication policy: closed
  Location updating reject cause: 13
  Encryption: A5/0
  NECI (TCH/H): 1
  Use TCH for Paging any: 0
  RRLP Mode: none
  MM Info: On
  Handover: Off
OpenBSC# show bts
BTS 0 is of nanobts type in band DCS1800, has CI 0 LAC 1, BSIC 1, TSC 7
and 1 TRX
Description: (null)
MS Max power: 15 dBm
Minimum Rx Level for Access: -110 dBm
Cell Reselection Hysteresis: 4 dBm
RACH TX-Integer: 9, RACH Max transmissions: 7
```

```
Channel Description Attachment: yes
Channel Description BS-PA-MFRMS: 5
Channel Description BS-AG_BLKS-RES: 1
System Information present: 0x0000087e, static: 0x00000000
  Unit ID: 1234/0/0, OML Stream ID 0xff
  NM State: Oper 'Enabled', Admin 'Unlocked', Avail 'OK'
  Site Mgr NM State: Oper 'Enabled', Admin 'unknown 0x0', Avail 'OK'
  GPRS NSE: Oper 'Enabled', Admin 'Unlocked', Avail 'OK'
  GPRS CELL: Oper 'Enabled', Admin 'Unlocked', Avail 'OK'
Paging: 0 pending requests, 0 free slots
  OML Link state: connected.
  Current Channel Load:
            CCCH+SDCCH4:   0% (0/4)
                  TCH/F:   33% (1/3)
                SDCCH8:   0% (0/8)

OpenBSC# show trx
TRX 0 of BTS 0 is on ARFCN 678
Description: (null)
  RF Nominal Power: 23 dBm, reduced by 20 dB, resulting BS power: 3 dBm
  NM State: Oper 'Enabled', Admin 'Unlocked', Avail 'OK'
  Baseband Transc. NM State: Oper 'Enabled', Admin 'Unlocked', Avail 'OK'
  ip.access stream ID: 0x00

OpenBSC# show subscriber id 1
    ID: 1, Authorized: 1
    Name: 'SIMmovistar'
    Extension: 1234
    LAC: 1/0x1
    IMSI: 214075500285725, TMSI: 07E3C3A2
    Expiration Time: Wed, 12 Mar 2015 19:52:33 +0100
    Pending: 0, Use count: 1
```

7.1.5 Servicios

Llegados a este punto, la red es capaz de ofrecer principalmente dos servicios a los terminales conectados bajo su red, llamadas de voz y mensajes SMS. Para comprobar su correcto funcionamiento, se registran dos terminales en la red y se realiza una llamada y el envío de un mensaje de texto entre ambos, con un resultado satisfactorio como se comprueba en la siguiente Figura 7.10.

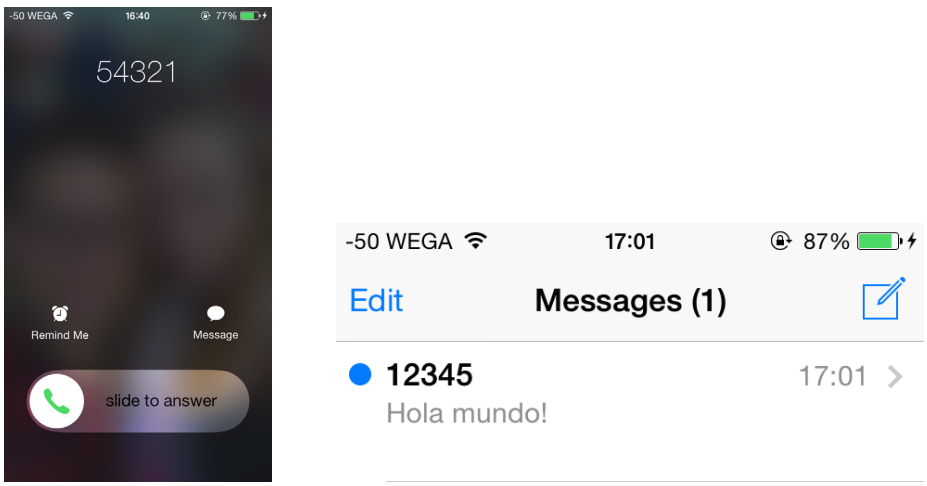


Figura 7.10: Llamada y SMS entrantes

7.2 Soporte para datos móviles GPRS

Como parte del proyecto OpenBSC, surge para cubrir la necesidad de tráfico de datos de los usuarios de la comunidad Osmocom, la ampliación OsmoSGSN. Se trata de una implementación abierta del nodo SGSN contenido en la arquitectura de las redes GPRS y encargado de la gestión de la movilidad y sesiones de los usuarios. Se conecta a través a la interfaz "*Gb*" con el subsistema de la estación base y mediante el protocolo "*GTP*" con el nodo GGSN, como el implementado por OpenGGSN, también desde la comunidad Osmocom. El nodo GGSN es utilizado por los operadores como interfaz entre Internet y el resto de la infraestructura de la red móvil, y ese será también su papel en el escenario que se describe en este proyecto..

Gracias a la extensión OsmoSGSN es posible dotar a la infraestructura anteriormente desplegada de capacidades para tráfico de datos GPRS. Los aspectos de instalación de las aplicaciones involucradas están recogidos en la guía de instalación de OpenBSC, adjunta en el Apéndice 11.3. Tras la instalacion del software necesario, la arquitectura actualizada del despliegue se presenta en la Figura 7.11.

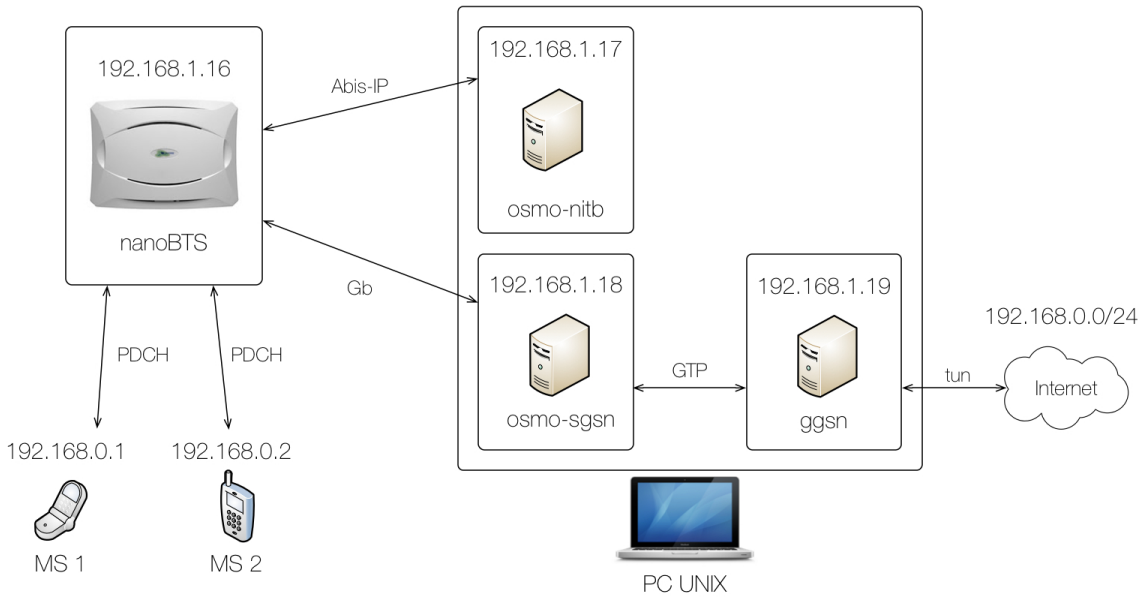


Figura 7.11: Arquitectura OpenBSC + OpenGGSN

Para permitir el tráfico de datos a través de la red, será necesario alojar algunos canales de paquetes de datos (PDCH) en los timeslots de la trama. La asignación de esos slots se realiza a través del fichero de configuración del nodo asociado a la aplicación `osmo-nitb`. Se ha optado por usar una asignación en la que se alterne un canal de datos con un canal de tráfico para mantener los servicios de voz como se muestra en la Figura 7.12.

```
phys_chan_config PDCH
```

TS0	TS1	TS2	TS3	TS4	TS5	TS6	TS7
CCCH SDCCH4	SDCCH8	TCH/F	PDCH	TCH/F	PDCH	TCH/F	PDCH

Figura 7.12: Distribución de slots OpenBSC+GPRS

7.2.1 Configuración

Como se observa en la Figura 7.11, para implementar la nueva arquitectura se necesitan tres máquinas distintas, cada una ejecutando aplicaciones diferentes. En primer lugar, se configura OpenBSC para soportar el tráfico GPRS incluyendo las siguientes opciones en la máquina que ejecute el aplicativo `osmo-nitb`. El parámetro `gprs nsvc 0 remote`, deberá contener la dirección IP y puerto de la máquina que ejecute el nodo SGSN. OpenBSC notificará a la BTS de esta dirección durante la fase de configuración para que se establezca el enlace entre ambos sobre la interfaz "*Gb*".

```
gprs mode gprs                              (Opciones none/gprs/egprs)
gprs routing area 0
gprs cell bvci 2
gprs nsei 101
gprs nsvc 0 nsvci 101
gprs nsvc 0 local udp port 23000            (Puerto UDP del nodo osmo-sgsn)
gprs nsvc 0 remote udp port 23000           (Puerto UDP del nodo ggsn)
gprs nsvc 0 remote ip 192.168.1.18          (IP del nodo osmo-sgsn)
```

El siguiente elemento que aparece en la arquitectura es el nodo SGSN de la red, implementado gracias a la aplicación `osmo-sgsn`, que al igual que en casos anteriores, posee su propio archivo de configuración, `osmo_sgsn.cfg`, que se modificará como sigue. El parámetro `gtp local-ip` contiene la dirección IP del propio SGSN y `ggsn 0 remote-ip` la dirección IP del nodo GGSN. Es posible ejecutar ambos procesos en la misma máquina, caso bajo el que se deberán generar varias direcciones IP para la misma interfaz de red o utilizar la interfaz de loopback. Los parámetros identificados por `encapsulation` deben contener datos que coincidan con los configurados anteriormente para openbsc o osmo-nitb.

```
!
! Osmocom SGSN configuration
!
line vty
no login
!
sgsn
gtp local-ip 192.168.1.18                   (IP del nodo osmo-sgsn)
ggsn 0 remote-ip 192.168.1.19               (IP del nodo ggsn)
ggsn 0 gtp-version 1
!
ns
timer tns-block 3                           (Gestión de los CV)
timer tns-block-retries 3
timer tns-reset 3
timer tns-reset-retries 3
timer tns-test 30
timer tns-alive 3
timer tns-alive-retries 10
encapsulation udp local-ip 192.168.1.18     (IP del nodo osmo-sgsn)
encapsulation udp local-port 23000          (Puerto del nodo osmo-sgsn)
encapsulation framerelay-gre enabled 0
!
bssgp
!
```

Por último, el nodo GGSN, implementado por la aplicación `ggsn`, también posee un archivo de configuración, `ggsn.conf` a modificar. La entrada `listen` especifica la dirección IP del propio nodo, que deberá coincidir con la entrada `ggsn 0 remote-ip` del archivo `osmo_sgsn.cfg`. El parámetro `net` contiene la dirección IP del túnel que se establecerá hacia Internet. Una de las funcionalidades de este nodo es la defiir la subred que se empleará en el despliegue, aspecto este que se configura mediante los parámetros `dynip` que incluye el conjunto de direcciones IP que será asignado a los terminales, `pcodns1` que define la dirección IP del servidor DNS y `timelimit` establece el tiempo que permanece la aplicación abierta.

```
!
! OpenGGSN configuration
!
fg
debug
listen 192.168.1.19
net 192.168.0.0/24
dynip 192.168.0.0/24
pcodns1 192.168.1.1
timelimit 0
```

Además de configurar el sistema asociado a OpenBSC, también hay que realizar las configuraciones pertinentes para adecuar las tablas de rutas del equipo anfitrión de forma que habilite la conectividad del túnel que se genera hacia Internet. Para ello se debe hablitar las opciones de redirección de paquetes (`ip_forward`)y establecer la configuración del equipo para que actue como *Network Address Translation* (NAT), traduzca las direcciones IP origen de la red privada a la dirección pública asociada.

```
$ sudo echo 1 > /proc/sys/net/ipv4/ip_forward
$ sudo iptables -A POSTROUTING -s 192.168.254.0/24 -t nat -o eth0 -j
MASQUERADE
```

7.2.2 Operación de la red

Tras configurar correctamente la infraestructura de la red, se está en condiciones de proceder a su operación y manejo. En primer lugar se ejecuta la aplicación `ggsn` que inicializará la interfaz *GTP*, quedará a la espera de la conexión por parte del nodo SGSN y establecerá el túnel IP hacia Internet.

Figura 7.13: Arranque ggsn

A continuación, se inicia el SGSN, encargado de generar el entorno GPRS, y enlazar a través de la interfaz "*GTP*" con el nodo GGSN, quedando a la espera del inicio de `osmo-nitb` para establecer el enlace en la interfaz "*Gb*" con la BTS. Al igual que `osmo-nitb`, ofrece una terminal virtual accesible mediante telnet que servirá para modificar algunos parámetros en tiempo de ejecución o para acceder a un control sobre el nodo y sus estadísticas. Se adjuntan en el Apéndice 11.5 los principales comandos a utilizar.

Por último, se arranca el programa `osmo-nitb`, al igual que en el escenario anterior. Tras establecer los enlaces primarios y secundarios con la BTS, se abre la conexión entre la BTS y el SGSN sobre la interfaz "*Gb*", como se observa en la Figura 7.14 mediante una conexión virtual *Network Service Virtual Connection* (NS-VC). Dicha conexión virtual provee un enlace extremo a extremo independientemente de la tecnología subyacente. También se genera la entidad *Network Service Entity* (NSE), que agrupa NS-VC, permitiendo que un mismo SGSN sirva a varios BSS. A nivel BSSGP se establece una conexión virtual BSS-SGSN, denominada *BSSGP virtual connection* (BVC), encargada de la señalización de la NSE a la que pertenecen. La asociación BVCI-NSEI identifica a la celda GPRS.

```
root@ubuntu:~/openbsc/openbsc/src/gprs# ./osmo-sgsn -c osmo_sgsn.cfg
<0010> gprs_ns.c:199 NSVCI=65534 Creating NS-VC
<0010> gprs_ns.c:199 NSVCI=65535 Creating NS-VC
<0010> gprs_ns.c:1200 Creating NS-VC for BSS at 192.168.1.16:23000
<0010> gprs_ns.c:774 NSVCI=65535(invalid) Rx NS RESET (NSEI=101, NSVCI=101, caus
e=O&M intervention)
<0010> gprs_ns.c:594 NSEI=101 Tx NS RESET ACK (NSVCI=101)
<0010> gprs_ns.c:512 NSEI=101 Starting timer in mode tns-test (30 seconds)
<0010> gprs_ns.c:512 NSEI=101 Starting timer in mode tns-test (30 seconds)
<0010> gprs_ns.c:1281 NSEI=101 Rx NS UNBLOCK
<0011> gprs_bssgp.c:249 BSSGP BVCI=0 Rx RESET cause=Transmission capacity modifi
ed
<0011> gprs_bssgp.c:249 BSSGP BVCI=2 Rx RESET cause=O&M intervention
<0011> gprs_bssgp.c:272 Cell 214-25-1-0 CI 0 on BVCI 2
<0011> gprs_bssgp.c:344 BSSGP BVCI=2 Rx BVC-UNBLOCK
<0011> gprs_bssgp.c:753 BSSGP BVCI=2 Rx Flow Control BVC
<0011> gprs_bssgp.c:790 BSS instructs us to MS default bucket leak rate != 0, re
starting DL GPRS!
```

Figura 7.14: Arranque osmo-sgsn

Para comprobar el correcto funcionamiento de la red GPRS, se repite el proceso de búsqueda y registro de un terminal. Se repite el proceso *Location Update* visto anteriormente en la red GSM, durante el que el terminal ahora conoce las nuevas capacidades de la red, por lo que solicita un *GPRS attach*. A esta solicitud la red responde asignandole un *P-TMSI*, para después solicitar la activación de un contexto PDP, proceso que se puede visualizar en la terminal de osmo-sgsn durante su ejecución, como la de la Figura 7.14..

Tras el acceso del terminal a la red, ahora se muestra el símbolo GPRS en su pantalla, como se comprueba en la Figura 7.15. Establecidas todas las conexiones, en la terminal de `ggsn` se observa que se reenvian paquetes hacia el túnel IP (Internet), como muestra la Figura 7.16.

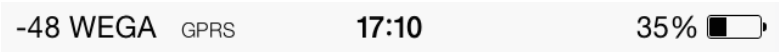


Figura 7.15: Terminal bajo red GPRS

```
Creating tun interface
Setting tun IP address
Received create PDP context request
encaps_tun. Packet received: forwarding to tun
encaps_tun. Packet received: forwarding to tun
encaps_tun. Packet received: forwarding to tun
Received packet from tun!
Received packet from tun!
```

Figura 7.16: Reenvío de paquetes en ggsn

```
<0012> gprs_llc.c:245 LLC RX: unknown TLLI 0x7f1fbe7f, creating LLME on the fly
<0002> gprs_gmm.c:1573 Unknown GSM 04.08 discriminator 0x0e
<0011> gprs_bssgp.c:376 BSSGP TLLI=0x7f1fbe7f Rx UPLINK-UNITDATA
<0012> gprs_llc.c:551 LLC SAPI=1 C   FCS=0x2cd7a8CMD=UI DATA
<0002> gprs_gmm.c:640 -> GMM ATTACH REQUEST MI(214075504677729) type="GPRS attach"
<0002> gprs_gmm.c:444 <- GPRS IDENTITY REQUEST: mi_type=02
<0011> gprs_bssgp.c:841 BSSGP BVCI=2 Rx Flow Control MS
<0011> gprs_bssgp.c:376 BSSGP TLLI=0x7f1fbe7f Rx UPLINK-UNITDATA
<0012> gprs_llc.c:551 LLC SAPI=1 C   FCS=0xf6e21eCMD=UI DATA
<0002> gprs_gmm.c:582 -> GMM IDENTITY RESPONSE: mi_type=0x02 MI(357997056602710)
<0002> gprs_gmm.c:352 <- GPRS ATTACH ACCEPT (new P-TMSI=0x4fc78892)
<0011> gprs_bssgp.c:753 BSSGP BVCI=2 Rx Flow Control BVC
<0011> gprs_bssgp.c:376 BSSGP TLLI=0xcfc78892 Rx UPLINK-UNITDATA
<0012> gprs_llc.c:551 LLC SAPI=1 C   FCS=0xbcd739CMD=UI DATA
<0002> gprs_gmm.c:1052 -> ATTACH COMPLETE
<0011> gprs_bssgp.c:753 BSSGP BVCI=2 Rx Flow Control BVC
<0011> gprs_bssgp.c:841 BSSGP BVCI=2 Rx Flow Control MS
<0011> gprs_bssgp.c:753 BSSGP BVCI=2 Rx Flow Control BVC
<0011> gprs_bssgp.c:841 BSSGP BVCI=2 Rx Flow Control MS
<0011> gprs_bssgp.c:376 BSSGP TLLI=0xcfc78892 Rx UPLINK-UNITDATA
<0012> gprs_llc.c:551 LLC SAPI=1 C   FCS=0x3134a3CMD=UI DATA
<0002> gprs_gmm.c:1319 -> ACTIVATE PDP CONTEXT REQ: SAPI=3 NSAPI=5 IETF IPv4
<000f> sgsn_libgtp.c:126 Create PDP Context
<000f> sgsn_libgtp.c:379 libgtp cb_conf(type=16, cause=128, pdp=0xb738e1a0, cbp=0x8ed9180)
<0002> gprs_gmm.c:1197 <- ACTIVATE PDP CONTEXT ACK
<0011> gprs_bssgp.c:753 BSSGP BVCI=2 Rx Flow Control BVC
<0011> gprs_bssgp.c:376 BSSGP TLLI=0xcfc78892 Rx UPLINK-UNITDATA
<0012> gprs_llc.c:551 LLC SAPI=3 C   FCS=0x2188e4CMD=XID DATA
<0013> gprs_sndcp.c:523 SN-DATA PDU at unitdata_ind() function
<0011> gprs_bssgp.c:376 BSSGP TLLI=0xcfc78892 Rx UPLINK-UNITDATA
<0012> gprs_llc.c:551 LLC SAPI=3 C   FCS=0xc1537cCMD=UI DATA
<000f> sgsn_libgtp.c:434 GTP DATA IND from GGSN, length=156
```

Figura 7.17: Proceso de registro GPRS

Al capturar el tráfico generado generado en el SGSN con la ayuda del analizador de protocolos Wireshark, se obtienen tramas del protocolo GTP intercambiadas, desde la petición de contexto PDP hasta el intercambio de tráfico, entre el SGSN y el GGSN hacia Internet, en este caso sobre protocolos de transporte tanto TCP como UDP. Dicha petición de creación de contexto PDP, incluida en la Figura 7.18, será respondida incluyendo datos como la IP asignada al terminal o el servidor DNS. Con esta configuración se han obtenido tasas binarias máximas de unos 64 kbps en bajada y 20 kbps en subida, utilizando una aplicación web [55], que ejecuta un test de velocidad en el terminal. Estos resultados están muy cerca del máximo teórico.

```
GPRS Tunneling Protocol
▷ Flags: 0x32
  Message Type: Create PDP context request (0x10)
  Length: 140
  TEID: 0x00000000
  Sequence number: 0x0000
  IMSI: 214075504677729
  Recovery: 64
  .... ..01 = Selection mode: MS provided APN, subscription not verified (1)
  TEID Data I: 0x00000001
  TEID Control Plane: 0x00000001
▷ NSAPI: 5
▷ End user address (IETF/IPv4)
▷ Access Point Name: telefonica.es
▽ Protocol configuration options
    Length: 52
    [Link direction: MS to network (0)]
    1... .... = Extension: True
    Configuration Protocol: PPP for use with IP PDP type or IP PDN type (0)
  ▷ Protocol or Container ID: Password Authentication Protocol (0xc023)
  ▷ Protocol or Container ID: Internet Protocol Control Protocol (0x8021)
  ▷ Protocol or Container ID: MS Support of Network Requested Bearer Control indicator (0x0005)
▷ GSN address : 192.168.1.18
▷ GSN address : 192.168.1.18
▷ MS international PSTN/ISDN number
▷ Quality of Service
```

Figura 7.18: PDP Context Request

7.2.3 Evolución de GPRS: EDGE

El proyecto OpenGGSN no solo contempla GPRS en sus desarrollos, sino también su evolución para una mejora de las tasas binarias, EDGE. Gracias al soporte para dicha tecnología con el que cuenta la picocelda nanoBTS escogida, es posible acceder a dicha mejora y disfrutar sus ventajas.

En caso que el terminal se encuentre cerca de la BTS, la calidad de la señal puede ser considerablemente alta, lo que implica que la BTS empleará esquemas de codificación de los datos con altas tasas. La nanoBTS soporta todos los esquemas de codificación EDGE, desde MCS1 hasta el MCS9, con una tasa binaria bruta máxima de 414 kbps, lo que triplica las tasas previstas para GPRS. Además, la BTS monitoriza continuamente el espectro radioeléctrico, adaptando el esquema utilizado en función de las condiciones actuales, haciendo un uso inteligente del espectro disponible.

Dotar al despliegue realizado de capacidades EDGE es realtivamente simple ya que únicamente hay que activar el modo `egprs` en la configuración.

```
gprs mode egprs
```

Nuevamente comprobamos su funcionamiento registrando el terminal en la red, ahora mostrando el símbolo E, correspondiente a la tecnología EDGE. Realizamos un acceso a una página web cualquiera desde el navegador y se confirma su correcta operación.

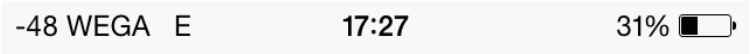


Figura 7.19: Terminal bajo red EDGE

En este nuevo escenario se han logrado tasas binarias de 216 kbps en descarga y 284,8 kbps en subida, utilizando la misma aplicación para comprobar velocidades. Lo que supone un incremento de velocidad de al menos 140 kbps por sentido, y tasas cercanas de nuevo al máximo teórico.

7.3 Soporte para mensajería SMPP

Como se ha mencionado, la aplicación `osmo-nitb` provee a través de su terminal virtual la capacidad para el envío de mensajes SMS hacia los terminales. Sin embargo, su uso queda limitado al envío de mensajes de texto convencionales. Entre los objetivos planteados al inicio de este proyecto, se incluía el envio de mensajes en modo binario, lo que supone adaptar la cabecera de usuario (UDH) e introducir datos binarios a continuación según el formato definido en el ETSI/3GPP TS 03.48 [3].

Una opción habría sido modificar directamente el código asociado a dicha funcionalidad para permitir editar un mayor número de parámetros y manejar mensajes binarios, pero se descartó por su complejidad y riesgo de eliminar la estabilidad que la implementación dispone.

Como alternativa se ha optado por hacer uso del protocolo SMPP. En concreto se ha empleado la implementación abierta del mismo "*C-open-smpp-3.4*" [46], desarrollada por Raul Tremsal y compatible con el entorno desplegado en el proyecto. La librería toma como base parte del código fuente del software Kannel [47] para proporcionar una serie de funciones capaces de empaquetar y desempaquetar estructuras de datos

hacia o desde un buffer. Es decir, la librería incluye todo lo referente al manejo de las PDU de SMPP, independientemente del uso que se haga de la conexión TCP y la sesión SMPP. El objetivo planteado es por tanto integrar un servidor de mensajería con soporte para SMPP en la infraestructura existente de OpenBSC, lo que permitirá desarrollar más adelante un cliente SMPP a medida.

Para integrar la librería en el software OpenBSC en primer lugar hay que instalar la librería bajo el mismo directorio que el resto de librerías del proyecto Osmocom. Posteriormente hay que recompilar OpenBSC, previo a lo cual se realizan algunas modificaciones para habilitar el soporte para el protocolo SMPP.

```
2     DEPENDS = "libdbi libosmocore libosmo-sccp libosmo-abis openggsn
libsmpp34"
13    INC_PR = "r15.${META_TELEPHONY_OSMO_INC}"
16    EXTRA_OECONF += " --enable-nat --enable-osmo-bsc --enable-smpp"
```

Por otro lado, se debe forzar que OpenBSC realice la gestión de mensajes SMS siempre a través de SMPP aún en el caso de que el receptor sea un usuario de la red GSM. Modificaremos el fichero `openbsc/src/libmsc/gsm_04_11.c` tal como se describe.

```
400   //    if (!gsms->receiver) {
415   //    }
```

Tras estas modificaciones se procede a la reinstalación y reconfiguración del sistema, incluyendo las opciones para establecer las sesiones SMPP, el usuario y contraseña que deberán emplear los clientes que deseen conectarse al servidor SMPP, la política de autenticación y la ruta por defecto.

```
smpp
 local-tcp-port 2775
 policy closed
 esme OSMPP
  password OSMPP
  default-route
```

Adicionalmente a estas modificaciones habrá que ejecutar el servidor SMPP que realizará todas las gestiones necesarisas para el envío y recpción de mensajes.

7.4 Plataforma de gestión remota OTA

Tras el despliegue del servidor SMPP con el que se dota al software OpenBSC de soporte para dicho protocolo, el último paso antes de contar con toda la infraestructura necesaria para la gestión *Over-The-Air* de los terminales es el desarrollo de un cliente de mensajería SMPP capaz de elaborar las estructuras de datos deseadas. Dicho cliente será la interfaz a través de la cual el usuario accede a la plataforma para realizar la operación de gestión oportuna. El escenario final se muestra en la siguiente Figura 7.20.

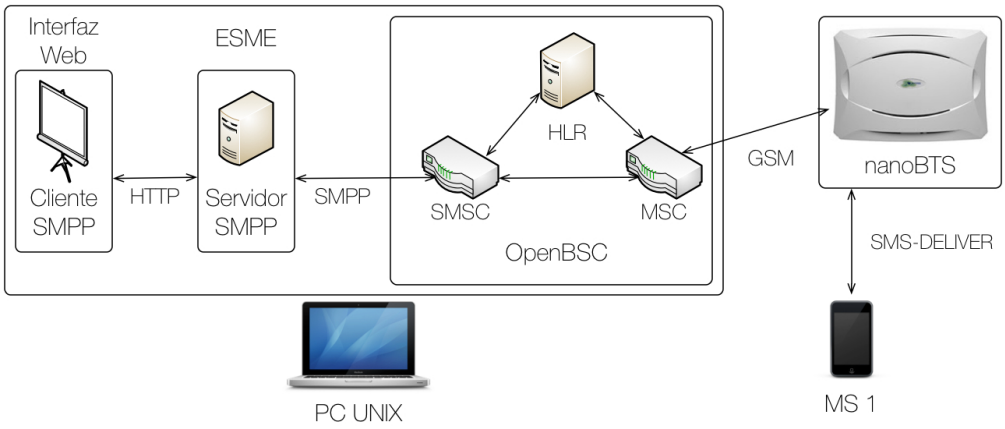


Figura 7.20: Arquitectura OpenBSC + SMPP

Tomando como inicio diversos desarrollos existentes bajo licencia libre, se ha elaborado un script en el lenguaje de programación PHP que implementa un cliente SMPP que cubra todos los requerimientos. Éste consta de una clase PHP encargada de implementar los procedimientos y estructuras de datos del protocolo SMPP y un script que constituye el propio cliente a editar como acceso a la plataforma.

En dicho cliente, se introducen todos los parámetros de nuestro servidor SMPP con el que se establecerá la sesión en la parte inicial del script, dirección, puerto, usuario y contraseña, así como el mensaje a enviar. En el caso de no contar con la infraestructura de red GSM que haga entrega del mensaje, es posible utilizar el cliente SMPP con servidores de mensajería comerciales existentes.

El script en primer lugar se conecta al servidor SMPP, establece la sesión SMPP con él, hace una prueba del enlace y posteriormente envía el mensaje, tras lo que se cierra la sesión. A continuación, cuenta con varias funciones para el envío del mensaje, en función de las características requeridas. Ofrece la posibilidad de enviar mensajes de texto convencionales, de la longitud que se desee. También soporta el envío de mensajes codificados según el estándar Unicode y como destinatarios múltiples receptores para un mismo mensaje. Adicionalmente permite, como se ha comentado, la opción de enviar mensajes binarios. Para ello, se especifica bajo el campo `$udh` la cabecera de usuario a emplear, y en el campo `$binary` los datos oportunos, de acuerdo con el estándar ETSI/3GPP TS 03.48 [3].

El proceso presente en la Figura 7.21 comienza con el establecimiento TCP de la sesión sobre la que se realiza la petición HTTP del recurso, en este caso la clase cliente. Al ejecutar el script PHP, se inicia el procedimiento de transmisión SMPP, que comienza con el establecimiento de la sesión SMPP *bind*, su posterior respuesta afirmativa, y el envío del mensaje *submit_sm*, con su correspondiente confirmación. Finalmente se cierra la sesión SMPP entre el cliente y el servidor; *unbind*.

Tras esto, el mensaje se remite al centro de mensajería, quien extraerá el campo de datos del mensaje SMPP y lo incluye en el campo de datos de usuario "*UD*" de un mensaje SMS, del tipo SMS-DELIVER, para su posterior transferencia al terminal. Será el MSC quien interrogue al HLR por la localización del destinatario y realice la entrega a la correspondiente BTS, que finalmente transmitirá a través del interfaz aire el SMS hacia el móvil. Si la entrega se produce correctamente, el terminal devuelve un reconocimiento RP-ACK sobre la unidad de datos SMS-DELIVER-REPORT.

HTTP	460	GET /PHP/php-smpp-master/prueba.smpp.php HTTP/1.1
SMPP	118	SMPP Bind_transmitter
SMPP	90	SMPP Bind_transmitter - resp: "Ok"
SMPP	116	SMPP Submit_sm
SMPP	107	SMPP Submit_sm - resp: "Ok"
SMPP	84	SMPP Unbind
SMPP	84	SMPP Unbind - resp: "Ok"
HTTP	362	HTTP/1.1 200 OK (text/html)
GSM SMS	104	DATA REQuest (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
GSM SMS	77	DATA INDication (DTAP) (SMS) CP-DATA (RP) RP-ACK (MS to Network)

Figura 7.21: Proceso de envío de mensaje SMS vía SMPP

7.4.1 Operación de la plataforma OTA

Una vez comprobado el funcionamiento del cliente y servidor SMPP mediante la correcta entrega de un SMS convencional de texto, es momento de aprovechar la infraestructura desplegada para realizar la gestión *Over-the-Air* de un terminal a través de mensajes SMS contenedores de comandos binarios. Para un mejor entendimiento del lector se presenta a continuación el encapsulado final que presenta el mensaje SMPP enviado.

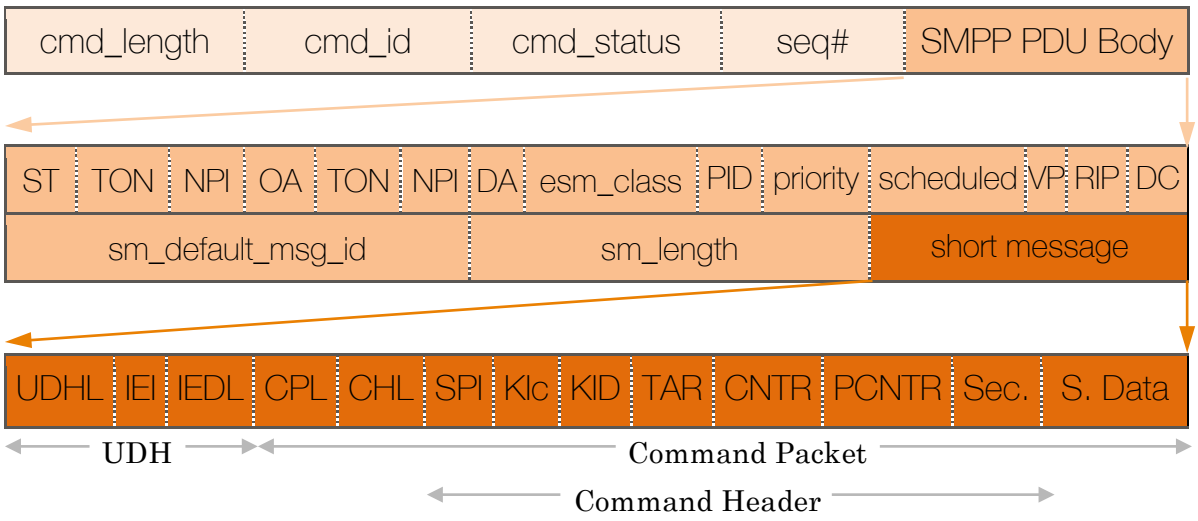


Figura 7.22: Encapsulado del mensaje SMPP enviado

Antes de proceder al envío de un mensaje binario, hay que comprobar que la tarjeta SIM destinataria tiene en su tabla de servicios almacenada en el fichero *SIM service table* (EFsst), alojado y activado el servicio *Data Download via SMS-PP*, al igual que en la Figura 7.23 Para ello se ha utilizado un lector de tarjetas inteligente y el software gratuito para Windows *SimSpy* [48], si bien se puede enviar el conjunto de comandos directamente y realizar una gestión manual.

Service 25:	activated	Data download via SMS-CB
Service 26:	activated	Data download via SMS-PP

Figura 7.23: Tabla de servicios SIM

El estándar ETSI/3GPP TS 11.14 [8] define que el mensaje será enviado directamente a la tarjeta SIM cuando el parámetro PID esté fijado a valor "0x7F", correspondiente con el servicio *(U)SIM Data Download*. Así mismo, el parámetro DCS deberá tener el valor "0xF6", identificando al mensaje como específico de la tarjeta SIM (clase 2). Si el servicio *Data Download via SMS-PP* está alojado y activado en la tabla de servicios de

la SIM, el terminal utilizará el comando ENVELOPE para transmitir el mensaje transparentemente a la SIM y no mostrará el mensaje o aviso alguno en el móvil.

La validación del sistema desplegado para su uso como plataforma de gestión OTA se inicia enviando el mensaje de la **¡Error! No se encuentra el origen de la referencia.**Figura 7.24, el cual contiene una cabecera de usuario UDH y se ha rellenado el campo de datos aleatoriamente. No podemos capturar el proceso que ocurre entre el terminal y la tarjeta SIM, obteniendo únicamente el reconocimiento de la entrega del SMS por parte del terminal, lo que al igual que sucedió durante el envío del mensaje mostrado en la Figura 7.21, supone que el procedimiento es operativo.

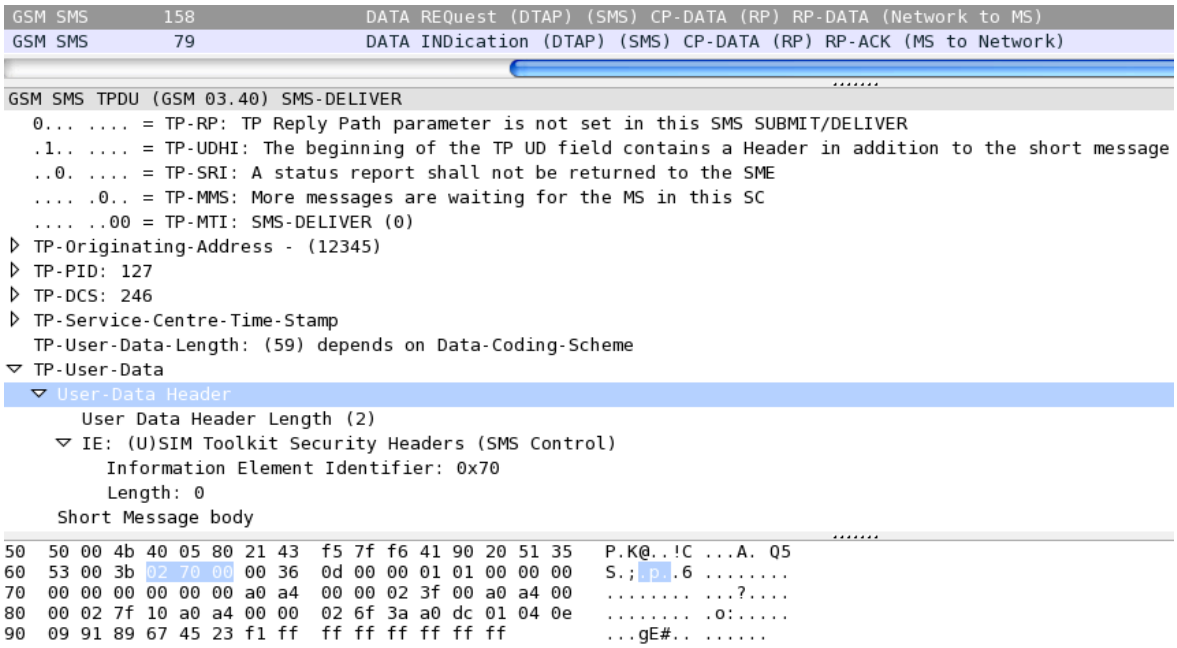


Figura 7.24: SMS-DELIVER con comando STK (aleatorio)

7.4.2 Caso de uso

A continuación se plantea el envio de un mensaje que incluye información válida. No obstante al no contar con los valores de las claves KIc y KID no devolverá un resultado correcto. Para lograr una ejecución correcta del intercambio, se debería contar con tarjetas SIM programables, en las que modificar dichas claves, y posteriormente codificar oportunamente el comando.

Gracias al software *Easy OTA* de Gemalto, se generan de una manera sencilla una serie de mensajes que permitan la modificación de la agenda alojada en la SIM. Para modificar un contacto de la agenda contenida en la tarjeta SIM se realizan cuatro acciones: las tres primeras sirven para navegar entre los directorios de la SIM hasta acceder al registro que contiene la agenda y la última acción realiza la modificación de la entrada indicada. El software se encargará de adjuntar las cabeceras oportunas, de acuerdo con el estándar ETSI/3GPP TS 11.11 [7], la secuencia de comandos necesaria, representada en la Figura 7.25 es:

```
SELECT DFmaster, SELECT DFtelecom, SELECT EFadn, UPDATE RECORD#1
```

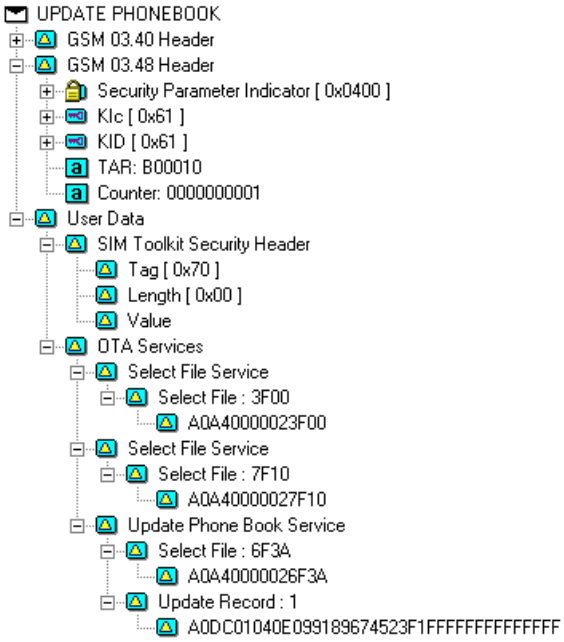


Figura 7.25: Comando UPDATE contacto

El mensaje generado siguiendo los pasos del software *Easy OTA* se introduce en el script PHP tal y como se ha mencionado, por un lado la cabecera UDH, y a continuación los datos binarios, es decir la cabecera 03.48 mostrada en la Figura 7.25.

7.5 Implicaciones de Seguridad

Accidentalmente, durante el desarrollo de la plataforma de gestión remota OTA se observó un comportamiento anómalo al enviar diversos mensajes binarios, algunos de los cuales dejaba la red temporalmente fuera de servicio. Aunque se trató de analizar el comportamiento no se pudo obtener las causas de ello, pudiendo ser debido a la SIM, a la red u otro elemento externo.

No obstante, abrió una línea de trabajo en la que se analizaron diversas grietas de seguridad ya conocidas y fácilmente replicables utilizando la picocélula.

7.5.1 DOS: Denegación de Servicio (*Denial of Service*)

Uno de los componentes de la cabecera de los comandos seguros es el *Security Parameter Indicator* (SPI), de dos octetos de longitud y con la estructura definida en las especificaciones del ETSI 3GPP TS 11.14 [8].

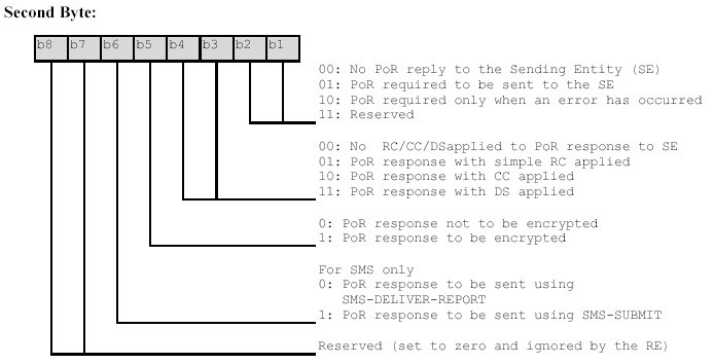


Figura 7.26: Segundo octeto del SPI

La vulnerabilidad se da gracias al segundo byte del campo SPI, en el que se puede fijar como se envía el acuse de recibo *Proof of Receipt* (PoR), bien vía SMS-DELIVER-REPORT o SMS-SUBMIT. Cuando se fija a SMS-SUBMIT el teléfono intentará enviarlo al remitente original. Si lo se fija a SMS-DELIVER-REPORT, el teléfono notificará a la red del estado del mensaje. Como no se habrá formado correctamente el mensaje, al no disponer de las claves Kic y KID, el resultado será erróneo, y el teléfono informará de dicho error. El centro de mensajería creerá que el teléfono no ha recibido el mensaje y tratará de enviarlo de nuevo, poniendo en espera el resto de mensajes de la cola hasta que el tiempo del mensaje inicial expira. Queda inutilizado tanto el terminal como la red, porque se podría encuadrar este ataque entre los denominados de denegación de servicio (DoS). Una implicación importante de este ataque es que funciona independientemente del terminal y de la red móvil (GSM/UMTS). En la Figura 7.27 se muestra el tráfico capturado mediante el analizador de protocolos Wireshark, en el que se observa el mensaje enviado al terminal en la primera línea y el informe de error que devuelve la tarjeta SIM vía SMS-DELIVER-REPORT en la siguiente. También se adjunta dicho mensaje con el informe erróneo en la Figura 7.28, dónde se puede ver como la tarjeta SIM ha informado de un error en la descarga del comando, dado que las claves son erróneas. A continuación se repite el reintento de envío del mensaje por parte del SMSC, y los sucesivos informes de error del terminal, quedando red y terminal inutilizables hasta que expira el tiempo de reintento.

```
DATA REQuest (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
DATA INDication (DTAP) (SMS) CP-DATA (RP) RP-ERROR (MS to Network)
DATA INDication (DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
DATA REQuest (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
DATA INDication (DTAP) (SMS) CP-DATA (RP) RP-ERROR (MS to Network)
DATA REQuest (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
DATA INDication (DTAP) (SMS) CP-DATA (RP) RP-ERROR (MS to Network)
DATA INDication (DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
DATA REQuest (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
DATA INDication (DTAP) (SMS) CP-DATA (RP) RP-ERROR (MS to Network)
DATA REQuest (DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
DATA INDication (DTAP) (SMS) CP-DATA (RP) RP-ERROR (MS to Network)
DATA INDication (DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
DATA INDication (DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
DATA INDication (DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
DATA INDication (DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
DATA INDication (DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
DATA INDication (DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
DATA INDication (DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
DATA INDication (DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
```

Figura 7.27: Tráfico intercambiado

```
GSM SMS TPDU (GSM 03.40) SMS-DELIVER REPORT
  .0.. .... = TP-UDHI: The TP UD field contains only the short message
  .... .0.. = TP-MMS: More messages are waiting for the MS in this SC
  .... ..00 = TP-MTI: SMS-DELIVER REPORT (0)
  TP-Failure-Cause (TP-FCS): (U)SIM data download error (0xd5)
▷ TP-Parameter-Indicator
▷ TP-PID: 127
▷ TP-DCS: 246
  TP-User-Data-Length: (16) depends on Data-Coding-Scheme
▷ TP-User-Data
```

Figura 7.28: SMS-DELIVER-REPORT

Capítulo 8

Conclusiones y líneas futuras

Una vez llegado el final de este trabajo, es momento de extraer conclusiones relevantes sobre su resultado y realización. Se presentan tambien posibles mejoras y líneas de investigación futuras como resultado del trabajo en este Trabajo de Fin de Grado, que podrán ser retomadas en futuros desarrollos.

8.1 Conclusiones

Durante la redacción de este trabajo se ha realizado un pequeño análisis del estado de las comunicaciones móviles, relacionando su evolución temporal con el desarrollo en nuestro país, notando los cambios producidos, y los agentes que intervienen. Resulta interesante tener cierta perspectiva de su evolución y pasado, para comprender su importancia. Se pueden observar claramente los cambios bruscos que sufre la tecnología, el aumento de la competencia y la influencia de los factores regulatorios.

Contar con la posibilidad de analizar el tráfico de las redes GSM, es tremendamente útil como se ha podido comprobar, pudiendo observar todos y cada uno de los detalles de los procesos involucrados en las comunicaciones. Además de cómo aprendizaje, o investigación, posee una gran utilidad a la hora de depurar fallos en el caso de estar desarrollando una red propia, como es el caso de este trabajo.

Durante el despliegue de nuestra infraestructura de red, se nota la tremenda sofisticación de los elementos de la red. Por lo que es de valorar el correcto funcionamiento de las redes comerciales, y la definición del estándar GSM, como tecnología robusta. Una vez más, se comprueban de manera práctica los procedimientos definidos, y se experimenta de cerca con los aspectos más técnicos.

En el caso de la plataforma de gestión remota desarrollada, es importante notar que se consigue eliminar la necesidad de contratar servicios a operadores convencionales, especialmente interesante en el caso de necesitar una gestión y mantenimiento de comunicaciones entre máquinas. Mediante un despliegue como el realizado, es posible servir de total conectividad a una serie de nodos, así como interactuar con ellos gracias a la plataforma de gestión remota OTA. Normalmente, será mas rentable para un proyecto de éstas características desplegar la infraestructura de red necesaria, que contratar dichos servicios, aunque es tarea del gestor valorar su amortización.

Cabe destacar la importante vertiente académica que posee el trabajo, tanto en el caso del analizador de redes GSM, como en el despliegue de nuestra propia red GSM/GPRS a través de la picocelda. Se consigue acceder a varios elementos de red, usualmente protegidos por los operadores, gracias a los que es posible comprobar de manera práctica todos los conceptos teóricos que cabría ver en una asignatura, o que recogen los libros, y afianzar dichos conceptos mediante la realización de prácticas guiadas en el laboratorio.

En lo referente a una investigación profunda sobre este tipo de redes, ya sea en aspectos de seguridad o cualquier otro, parece imprescindible el acercamiento real a la tecnología, haciendo posible todo tipo de pruebas y escenarios, perfectos para corroborar con pruebas de campo cualquier trabajo o investigación que se realice.

8.2 Líneas futuras

No podemos dar por cerrado el trabajo realizado, dadas sus enormes posibilidades y complejidad en ciertas áreas. Las tarjetas inteligentes requieren elevados conocimientos para su correcta utilización, así como sucede con otras tecnologías relacionadas con el proyecto. Por esto, se requiere una mayor profundidad para aumentar las funcionalidades del sistema.

Como se menciona en el capítulo siete, referente al uso de la plataforma de gestión remota, durante la realización del trabajo no se consigue formar correctamente un comando contenido en un SMS que realice una acción determinada, sino que se ha optado por comprobar su correcto envío y recepción. Queda por tanto pendiente, formar correctamente un mensaje contenedor de un comando. Para ello, necesitaremos bien tarjetas SIM de las que conozcamos las claves KIc y KID, o bien tarjetas programables en las que codificar dichas claves a nuestro gusto. Posteriormente, al igual que se describe durante el capítulo, se formaría el comando, en este caso cifrado con las claves idóneas. Su funcionamiento debería ser totalmente correcto, observando cierta respuesta por parte del terminal.

También puede ser interesante capturar el proceso que tiene lugar en la interfaz entre la tarjeta SIM y el terminal, para observar lo ocurrido en caso de producirse errores durante dicho proceso o comprobar su correcto funcionamiento. Desde la comunidad Osmocom, se cuenta con la iniciativa *SIMtrace* [49]. Se trata de una combinación software y hardware capaz de capturar las APDUs intercambiadas entre el terminal y la SIM, gracias a su integración con Wireshark. También es posible emular el comportamiento de un teléfono o de una tarjeta inteligente. Existe una utilidad con funcionamiento similar, denominada *DCT3TAP*, que requiere para su utilización de un teléfono Nokia 3310 o similar y un cable serie específico *Serial/USB FBUS*.

Una vez fuéramos capaces de generar comandos interesantes totalmente funcionales, sería posible recoger varios de estos comandos bajo un servicio web. De esta manera, cualquier usuario no experimentado sería capaz de realizar ciertas tareas cotidianas de gestión, como la consulta del estado de un nodo, sus parámetros y medidas, o ejecutar acciones de mantenimiento.

Aunque de momento parece complicado, desde la comunidad Osmocom se aceptan donaciones de todo tipo de equipamiento UMTS, con el fin de tratar de extender el soporte de OpenBSC a siguientes generaciones como UMTS o LTE. Por el momento es pronto para hablar de desarrollos funcionales, pero sí que se han realizado ciertas capturas de tráfico de datos sobre LTE utilizando Módems USB.

Dado el interés académico del proyecto, cabría ampliar las guías de instalación realizadas hacia guiones de prácticas, con el fin de tutorizar sesiones prácticas de laboratorio sobre la tecnología GSM. Resulta realmente útil ahondar más en los

aspectos de seguridad, tanto en la búsqueda de grietas, como en la propuesta de soluciones de mejora ante dichos problemas.

Los escasos requerimientos que posee la picocelda, como su bajo consumo eléctrico, o la poca capacidad de procesado necesaria para su funcionamiento, la hacen ideal para el despliegue de redes bajo determinadas circunstancias. Se han realizado despliegues totalmente funcionales, alimentando la picocelda mediante placas fotovoltáicas que proporcionan el suministro eléctrico a través de energía solar, y utilizando sencillos ordenadores "*Raspberry Pi*" para la ejecución del software necesario.

Podría plantearse el caso en el que se desea monitorizar cultivos en un área rural sin conectividad, para lo que un despliegue como el realizado resulta ideal, recogiendo los sensores bajo su red, y proporcionando acceso desde el exterior mediante una interfaz hacia Internet. También resulta interesante su despliegue sobre vehículos, sobre los que además de servir de conectividad a dispositivos habituales como el teléfono móvil, podría servir para gestionar los elementos del propio vehículo mediante una integración con el bus de comunicaciones oportuno, como por ejemplo, el CAN-BUS en el caso de los coches.

Capítulo 9

Bibliografía

[1] ETSI/3GPP TS 03.38; "*Alphabets and language-specific information*"

[2] ETSI/3GPP TS 03.40; "*Technical realization of the Short Message Service Point-to-Point*"

[3] ETSI/3GPP TS 03.48; "*Security mechanisms for the SIM application toolkit*"

[4] ETSI/3GPP TS 04.11; "*Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface*"

[5] ETSI/3GPP TS 08.51; "*BSC-BTS Interface, General Aspects*"

[6] ETSI/3GPP TS 12.21; "*Radio Access Network; Network Management procedures and messages on the A-bis interface*"

[7] ETSI/3GPP TS 11.11; "*Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface*"

[8] ETSI/3GPP TS 11.14; "*Specification of the SIM Application Toolkit (SAT) for the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface*"

[9] ETSI/3GPP TS 04.11; "*Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface*"

[10] ETSI/3GPP TS 22.034; "*Technical Specification Group Services and System Aspects; High Speed Circuit Switched Data (HSCSD); Stage 1"*

[11] ETSI/3GPP TS 23.034; "Technical Specification Group Core Network and Terminals; High Speed Circuit Switched Data (HSCSD); Stage 2

[12] ETSI/3GPP TS 23.002; "*Technical Specification Group Services and System Aspects; Network Architecture*"

[13] ETSI/3GPP TS 23.040; "*Technical realization of the Short Message Service*"

[14] ETSI/3GPP TS 23.048; "*Security Mechanisms for the (U)SIM Application Toolkit*"

[15] ETSI/3GPP TS 45.001; "*Physical layer on the radio path; General description*"

[16] ETSI/3GPP TS 45.002; "*Radio Access Network; Multiplexing and multiple access on the radio path"*

[17] ETSI EN 301 113; "*General Packet Radio Service (GPRS); Service description; Stage 1*"

[18] ETSI EN 301 344; "*General Packet Radio Service (GPRS); Service description; Stage 2*"

[19] ETSI TR 25.913 "*Agreed requeriments for the Evolved UTRA & UTRAN*"

[20] ETSI TR 25.814; "*Physical layer aspects of Evolved UTRA*"

[21] ITU-T E.164; "*Plan Internacional de Numeración de Telecomunicaciones Públicas*"

[22] Nico Golde; "*SMS Vulnerability Analysis on Feature Phones*"

[23] Bogdan Alecu; "*SMS Fuzzing - SIM Toolkit Attack*"

[24] SMS-Forum; "*Short Message Peer to Peer Protocol v5.0 Specification*"

[25] Christian Forst; "*Security vulnerabilities in GSM*"

[26] GSMA; "*The Mobile Economy Report 2014*"

[27] GSMA; "*Remote Provisioning Architecture for embedded UICC Technical Specification*"

[28] Zhe Chen, Shize Guo, Kangfeng Zheng and Yixian Yang; "*Modeling of Man-in-the-Middle Attack in the Wireless Networks*"

[29] N.J. Croft, M.S. Olivier; "*A Silent SMS Denial of Service Attack*"

[30] Sharad Kumar Verma, Dr. D.B. Ojha; "*An approach to enhace the mobile SMS Security*"

[31] Lars Lockefeer; "*Encrypted SMS, an analysis of the theoretical necessities and implementation possibilities*"

[32] Arturo Rivas Arias; "*Despliegue de una celda GSM basada en sistemas abiertos*"

[33] Joan Calzada, Alejandro Estruch; "*Telefonía móvil en España: regulación y resultados*"

[34] Steve Perlman, Antonio Forenza; "*Distributed-Input-Distributed-Output (DIDO) Wireless Technology; A New Approach to Multiuser Wireless*"

[35] Giesecke & Devrient; White Paper "*The OTA Platform in the world of LTE*"

[36] SIMalliance; "*UICC in LTE: A guidance from SIMalliance"*

[37] André Egners, Enno Rey, Hendrik Schmidt, Peter Schneider, Sascha Wessel; "*Threat and Risk Analysis for Mobile Communication Networks and Mobile Terminals*"

[38] Romeo, J. M. y Huidobro, J. M.; "*El ímpetu de la telefonía móvil», en Crónicas y testimonios de las telecomunicaciones españolas*"

[39] Sancho, D.; *"La regulación de la telefonía móvil en España: Ideología e instituciones"*

[40] Página web del Proyecto Osmocom; http://osmocom.org

[41] Página web del Proyecto OpenBTS; http://openbts.org

[42] Página web del proveedor ipaccess; http://www.ipaccess.com/en/smallcells

[43] Página web del transceptor UmTRX ; http://umtrx.org

[44] Página web de sysmocom; http://www.sysmocom.de/products/sysmobts

[45] Página web de fairwaves; https://fairwaves.co/wp/equipment/

[46] Página web de la librería C-SMPPv3.4; http://c-open-smpp-34.sourceforge.net

[47] Página web del gateway Kannel; http://www.kannel.org/

[48] Página web del software SimSpy; http://www.nobbi.com/simspy/simspy.html

[49] Página web de SIMtrace; http://bb.osmocom.org/trac/wiki/SIMtrace

[50] Página web de la herramienta Wireshark; https://www.wireshark.org

[51] Página web del analizador R&S TSMQ; http://www.rohde-schwarz.com/en/product/tsmq-productstartpage_63493-7713.html

[52] Página web del analizador Nexus 8630; http://www.nexustelecom.com/products/nexus8630/

[53] Página web de RTL-SDR; http://www.rtl-sdr.com/rtl-sdr-tutorial-analyzing-gsm-with-airprobe-and-wireshark/

[54] Página web de Airprobe; https://srlabs.de/airprobe-how-to/

[55] Página web del Test de Velocidad; http://www.speedtest.net/es/

Capítulo 10

Acrónimos

#

3GPP: 3rd Generation Partnership Project

A

ARFCN: Absolute Radio Frequency Channel Number

ARM: Advanced RISC Machine

ARQ: Automatic Repeat Request

APDU: Application Protocol Data Unit

B

BCCH: Broadcast Control Channel

BER: Bit Error Rate

BSS: Base Station Subsystem

BSSGP: Base Station Subsystem GPRS Protocol

C

CCCH: Common Control Channel

CDMA: Code Division Multiple Access

CEPT: Conférence Européene des Postes et Télécommunications

CLI: Command Line Interface

D

DECT: Digital Enhaced Cordless Telecommunications

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

DOS: Denial of Service

E

EDGE: Enhaced Data Rates for GSM Evolution

ETSI: European Telecommunications Standards Institute

F

FDD: Frequency Division Duplex

FDMA: Frequency Division Multiple Access

FEC: Forward Error Correction

G

GMR: GEO-Mobile Radio Interface

GPRS: General Packet Radio System

GSM: Global System for Mobile Communications (orig.: Groupe Spécial Mobile)

GSMA: GSM Association

GTP: GPRS Tunelling Protocol

H

HDLC: High-Level Data Link Control

HSPA: High Speed Packet Access

HSDPA: High Speed Downlink Packet Access

HSUPA: High Speed Uplink Packet Access

I

IoT: Internet of Things

ITU: International Telecommunication Union

IP: Internet Protocol

L

LTE: Long Term Evolution

M

M2M: Machine to Machine

MITM: Man In The Middle

MMS: Multimedia Message Service

MS: Mobile Station

MSISDN: Mobile Station Integrated Services Digital Network

N

NITB:Network-In-The-Box

NFC: Near Field Communications

NSS: Network Station Subsystem

O

OTA: Over The Air

OMV: Operador Movil Virtual

OSS: Operation and Support Subsystem

P

PDP: Packet Data Protocol

PDU: Protocol Data Unit

PMR: Private Mobile Radio

Q

QoS: Quality of Service

R

RDSI: Red Digital de Servicios Integrados

RFM: Remote File Management

RTC: Red Telefónica Conmutada

RSSI: Received Signal Strength Indication

S

SDR: Software Defined Radio

SIM: Subscriber Identity Module

SMS: Short Message Service

SMSC: Short Message Service Center

SMPP: Short Message Peer-to-peer Protocol

SNDCP: Sub Network Dependent Convergence Protocol

SS7: Signalling System number 7

T

TCP/IP: Transmission Control Protocol / Internet Protocol

TDD: Time Division Duplex

TDMA: Time Division Multiple Access

TETRA: Terrestrial Trunked Radio

U

UART: Universal Asynchronous Receiver-Transmitter

UDH: User Data Header

UICC: Universal Integrated Circuit Card

UNIX: Uniplexed Information and Computing System

UMTS: Universal Mobile Telecommunications System

USB: Universal Serial Bus

USIM: Universal Subscriber Identity Module

V

VoIP: Voice over IP

W

WSN: Wireless Sensor Network

Capítulo 11

Apéndices

11.1 [Apéndice 1] Guía de Instalación OsmocomBB

En primer lugar, necesitaremos el gestor de paquetes **aptitude**, en caso de no tenerlo ya instalado ejecutar el siguiente comando:

```
$ sudo apt-get install aptitude
```

Para compilar osmocom serán necesarios los paquetes **autoconf, automake, libtool, pkg-config, make y GCC**. También utilizaremos el software de gestión de versiones GIT. Ejecutamos para ello el siguiente comando:

```
$ sudo aptitude install libtool shtool autoconf git-core pkg-config make
gcc
```

Además necesitaremos la librería central que utilizan todos los programas del prouecto; **libosmocore**, que se instala por separado. En primer lugar la descargamos desde el git del proyecto, y posteriormente la compilamos (standalone):

```
$ git clone git://git.osmocom.org/libosmocore.git
$ cd libosmocore/
$ autoreconf -i                                                          $
./configure
$ make
$ sudo make install
$ cd ..
```

Para compilar el software que correrá en el teléfono es necesaria una herramienta de programación capaz de generar código para una arquitectura distinta a la del PC, es decir, un compilador cruzado, en nuestro caso utilizaremos "**GNU toolchain for Arm**".
A continuación describiremos los pasos necesarios para compilar nuestra propia "toolchain", que consistirá fundamentalmente en GCC 4.5.2, Binutils 2.21.1 y Newlib 1.19. En primer lugar, creamos el directorio y descargamos gnu-arm-build.2.sh allí. Necesitaremos hacerlo ejecutable:

```
$ chmod +x gnu-arm-build.2.sh
```

También necesitaremos los siguientes paquetes:

```
$ sudo apt-get install build-essential libgmp3-dev libmpfr-dev libx11-6
libx11-dev texinfo flex bison libncurses5 libncurses5-dbg libncurses5-dev
libncursesw5 libncursesw5-dbg libncursesw5-dev zlibc zlib1g-dev libmpfr4
libmpc-dev
```

Abrir un nuevo terminal en el directorio de gnu-arm-build.sh y crear los siguientes directorios:

```
$ mkdir build install src
```

Descargamos las fuentes necesarias en la carpeta src:

```
$ cd src/
$ wget http://ftp.gnu.org/gnu/gcc/gcc-4.5.2/gcc-4.5.2.tar.bz2
$ wget http://ftp.gnu.org/gnu/binutils/binutils-2.21.1a.tar.bz2
$ wget ftp://sources.redhat.com/pub/newlib/newlib-1.19.0.tar.gz
```

Estaremos ahora en condiciones de generar el compilador:

```
$ cd ..
$ ./gnu-arm-build.2.sh
I will build an arm-elf cross-compiler:
  Prefix: <YOURPATH>/install              Sources: <YOURPATH>/src
  Build files: <YOURPATH>/build Press ^C now if you do NOT want to do
this.
```

Pulsamos enter y tras unos instantes si todo va bien recibiremos el siguiente mensaje:

```
Build complete! Add <YOURPATH>/bin to your PATH to make arm-elf-gcc and
friends accessible directly.
```

Para hacerlo accesible al bash, necesitamos exportar el camino con la siguiente línea al archivo ~/.bashrc:

```
export PATH=$PATH:<YOURPATH>/install/bin
Ejemplo: export PATH=$PATH:/home/wega/Documents/built/osmocom-
bb/install/bin
```

El siguiente paso será compilar osmocom-bb, previa descarga desde el git del proyecto:

```
$ git clone git://git.osmocom.org/osmocom-bb.git
$ cd osmocom-bb
$ git pull –rebase
```

Tanto el código que correrá en el teléfono como el que correrá en el host se generan con el siguiente comando, éste asume que “arm-elf-gcc” está dentro de la ruta actual.

```
$ cd src
$ make
```

11.2 [Apéndice 2] Comandos OsmocomBB

Interfaz Control

```
OsmocomBB#
enable
help
  list
  write terminal
  write file
  write memory
  write
  show running-config
  exit
  disable
  configure terminal
  copy running-config
startup-config
  show startup-config
  show version
  show online-help
  terminal length <0-
512>
  terminal no length
  who
  show history
  terminal monitor
  terminal no monitor
  show ms [MS_NAME]
  show subscriber
[MS_NAME]
  show support [MS_NAME]
  show cell MS_NAME
  show cell MS_NAME <0-
1023> [pcs]
  show neighbour-cells
MS_NAME
  show ba MS_NAME [MCC]
[MNC]
  show forbidden
location-area MS_NAME
  show forbidden plmn
MS_NAME
  monitor network
MS_NAME
  no monitor network
MS_NAME
  off
  sim testcard MS_NAME
[MCC] [MNC] [LAC] [TMSI]
  sim testcard MS_NAME
MCC MNC LAC TMSI
attached
  sim reader MS_NAME
  sim remove MS_NAME
  sim pin MS_NAME PIN
  sim disable-pin
MS_NAME PIN
  sim enable-pin MS_NAME
PIN
  sim change-pin MS_NAME
OLD NEW
  sim unblock-pin
MS_NAME PUC NEW
  sim lai MS_NAME MCC
MNC LAC
  network search MS_NAME
  network show MS_NAME
  network select MS_NAME
MCC MNC [force]
  call MS_NAME
(NUMBER|emergency|answer
|hangup|hold)
  call MS_NAME retrieve
[NUMBER]
  call MS_NAME dtmf
DIGITS
  sms MS_NAME NUMBER
.LINE
  service MS_NAME
(*#06#|*#21#|*#67#|*#61#
|*#62#|*#002#|*#004#|*xx
*number#|*xx#|#xx#|##xx#
|STRING|hangup)
  test re-selection NAME
  delete forbidden plmn
NAME MCC MNC
```

Configuración Terminal

```
OsmocomBB# configure
terminal
OsmocomBB(config)#
 help
  list
  write terminal
  write file
  write memory
  write
  show running-config
  exit
  end
  hostname WORD
  no hostname [HOSTNAME]
  password (8|) WORD
  password LINE
  enable password (8|)
WORD
  enable password LINE
  no enable password
  banner motd default
  banner motd file
[FILE]
  no banner motd
  service terminal-
length <0-512>
  no service terminal-
length [<0-512>]
  line vty
  service advanced-vty
  no service advanced-
vty
  show history
  gps device DEVICE
  gps baudrate
(default|4800|9600|19200
|38400|57600|115200)
  gps enable
  no gps enable
  hide-default
  no hide-default
  ms MS_NAME
  ms MS_NAME create
  ms MS_NAME rename
MS_NAME
  no ms MS_NAME
  end
```

Configuración Terminal X

```
OsmocomBB(config)#ms 1
OsmocomBB(ms)#
  help
  list
  write terminal
  write file
  write memory
  write
  show running-config
  exit
  end
  show this
  layer2-socket PATH
  sap-socket PATH
  sim (none|reader|test)
  network-selection-mode
(auto|manual)
  imei IMEI [SV]
  imei-fixed
  imei-random <0-15>
  no emergency-imsi
  emergency-imsi IMSI
  no sms-service-center
  sms-service-center
NUMBER
  call-waiting
  no call-waiting
  auto-answer
  no auto-answer
```

11.3 [Apéndice 3] Guía de Instalación OpenBSC

Para la instalación de OpenBSC resolvemos en primer lugar ciertas dependencias.

```
$ apt-get install libdbi0-dev libdbd-sqlite3 build-essential libtool
autoconf automake git-core pkg-config libortp-dev
```

Si no la tenemos ya instalada, necesitaremos la librería central del proyecto osmocom "**libosmocore**", comprobamos la última versión desde el git del proyecto y ejecutamos el script de autoconfiguración. Posteriormente compilaremos dicha versión.

```
$ git clone git://git.osmocom.org/libosmocore.git
$ cd libosmocore
$ autoreconf -fi
$ ./configure
$ make
$ make install
$ ldconfig
```

El siguiente componente a instalar es la librería "libosmo-abis".

```
$ git clone git://git.osmocom.org/libosmo-abis.git
$ cd libosmo-abis
$ autoreconf -fi
$ ./configure
$ make
$ make install
$ ldconfig
```

Ahora estaremos en condiciones de compilar el propio OpenBSC.

```
$ git clone git://git.osmocom.org/openbsc.git
$ cd openbsc/openbsc
$ autoreconf -i
$ export PKG_CONFIG_PATH=/usr/local/lib/pkgconfig
$ ./configure
$ make
```

Una vez instaladas las librerias necesarias, y configurada la BTS, estamos en condiciones de ejecutar la solución "*Network-In-The-Box*" de OpenBSC, concentrando en una aplicación todos los componentes necesarios de la red GSM. OpenBSC utiliza un archivo de configuración en el directorio de mismo nombre (`openbsc.cfg`)

```
$ ./osmo-nitb -c openbsc.cfg
```

Es posible dotar de capacidades para tráfico de datos a nuestra red GSM gracias a la extensión del proyecto OpenBSC, OpenGGSN. En primer lugar, al igual que en los casos anteriores, descargamos todas las dependencias necesarias:

```
$ apt-get install libdbi0-dev libdbd-sqlite3 libtool autoconf git-core
pkg-config make libortp-dev
```

Descargamos el código fuente de OpenGGSN, y lo compilamos

```
git clone git://git.osmocom.org/openggsn.git
```

```
cd /openggsn
autoreconf; automake --add-missing; autoreconf; autoconf; automake;
./configure --prefix=/usr/local; make -j 2; make install
```

Comprobamos nuevos cambios en las librerias desde el git del proyecto, y compilamos.

```
cd /root
git clone git://git.osmocom.org/libosmocore.git;
git clone git://git.osmocom.org/libosmo-abis.git;
git clone git://git.osmocom.org/openbsc.git
cd /root/libosmocore; autoreconf -fi; ./configure; make; make install;
ldconfig
cd /root/libosmo-abis; autoreconf -fi; ./configure; make; make install;
ldconfig
cd /root/openbsc/openbsc; autoreconf -fi; export
PKG_CONFIG_PATH=/usr/local/lib/pkgconfig; ./configure; make
```

Si todo es correcto, tenemos una copia funcionando de las aplicaciones ggsn, osmo-sgsn y osmo-nitb en nuestra máquina.

11.4 [Apéndice 4] openbsc.cfg

```
!
! OpenBSC Configuration
File
!!
!
line vty
 no login
!
e1_input
 e1_line 0 driver ipa
 e1_line 0 port 0
 no e1_line 0 keepalive
network
 network country code 214
 mobile network code 25
 short name WEGA
 long name WEGA
 auth policy closed
 location updating reject
cause 13
 encryption a5 0
 neci 1
 paging any use tch 0
 rrlp mode none
 mm info 1
 handover 0
 handover window rxlev
averaging 10
 handover window rxqual
averaging 1
 handover window rxlev
neighbor averaging 10
 handover power budget
interval 6
 handover power budget
hysteresis 3
 handover maximum distance
9999
 timer t3101 10
 timer t3103 0
 timer t3105 0
 timer t3107 0
 timer t3109 4
 timer t3111 0
 timer t3113 60
 timer t3115 0
 timer t3117 0
 timer t3119 0
 timer t3122 10
 timer t3141 0
 dtx-used 0
 subscriber-keep-in-ram 1
 bts 0
  type nanobts
  band DCS1800
  cell_identity 0
  location_area_code 1
  base_station_id_code 1
  training_sequence_code 7
   ms max power 15
   cell reselection
hysteresis 4
   rxlev access min 0
   periodic location update
30
   channel allocator
ascending
   rach tx integer 9
   rach max transmission 7
   channel-descrption attach
1
   channel-descrption bs-pa-
mfrms 5
   channel-descrption bs-ag-
blks-res 1
   ip.access unit_id 1234 0
   oml ip.access stream_id
255 line 0
   neighbor-list mode
automatic
   codec-support fr
   gprs mode egprs
   gprs routing area 0
   gprs network-control-
order nc0
   gprs cell bvci 2
   gprs cell timer blocking-
timer 10
   gprs cell timer blocking-
retries 10
   gprs cell timer
unblocking-retries 10
   gprs cell timer reset-
timer 10
   gprs cell timer reset-
retries 10
   gprs cell timer suspend-
timer 10
   gprs cell timer suspend-
retries 10
   gprs cell timer resume-
timer 10
   gprs cell timer resume-
retries 10
   gprs cell timer
capability-update-timer 10
   gprs cell timer
capability-update-retries
10
   gprs nsei 101
   gprs ns timer tns-block 3
   gprs ns timer tns-block-
retries 3
   gprs ns timer tns-reset 3
   gprs ns timer tns-reset-
retries 3
   gprs ns timer tns-test 30
   gprs ns timer tns-alive 3
   gprs ns timer tns-alive-
retries 10
   gprs nsvc 0 nsvci 101
   gprs nsvc 0 local udp
port 23000
   gprs nsvc 0 remote udp
port 23000
   gprs nsvc 0 remote ip
192.168.1.18
   gprs nsvc 1 nsvci 0
   gprs nsvc 1 local udp
port 0
   gprs nsvc 1 remote udp
port 0
   gprs nsvc 1 remote ip
0.0.0.0
   no force-combined-si
   trx 0
    rf_locked 0
    arfcn 678
    nominal power 23
    max_power_red 20
    rsl e1 tei 0
     timeslot 0
      phys_chan_config
CCCH+SDCCH4
      hopping enabled 0
     timeslot 1
      phys_chan_config
SDCCH8
      hopping enabled 0
     timeslot 2
      phys_chan_config PDCH
      hopping enabled 0
     timeslot 3
      phys_chan_config TCH/F
      hopping enabled 0
     timeslot 4
      phys_chan_config PDCH
      hopping enabled 0
     timeslot 5
      phys_chan_config TCH/F
      hopping enabled 0
     timeslot 6
      phys_chan_config PDCH
      hopping enabled 0
     timeslot 7
      phys_chan_config TCH/F
      hopping enabled 0
mncc-int
 default-codec tch-f fr
default-codec tch-h hr
smpp
 local-tcp-port 2775
policy accept-all
 esme OSMPP
  password OSMPP
  default-route
```

11.5 [Apéndice 5] Comandos Osmo-SGSN

Interfaz Control

```
OsmoSGSN#
help
  list
  write terminal
  write file
  write memory
  write
  show running-config
  exit
  disable
  configure terminal
  copy running-config startup-config
  show startup-config
  show version
  show online-help
  terminal length <0-512>
  terminal no length
  who
  show history
  terminal monitor
  terminal no monitor
  logging enable
  logging disable
  logging filter all (0|1)
  logging color (0|1)
  logging timestamp (0|1)
  logging set-log-mask MASK
  logging level
(all|mm|pag|meas|ref|gprs|ns|bssgp|l
lc|sndcp|lglobal|llapd|linp|lmux|lmi
|lmib|lsms)
(everything|debug|info|notice|error|
fatal)
  show logging vty
  show alarms
  show sgsn
  show mm-context imsi IMSI [pdp]
  show mm-context all [pdp]
  show pdp-context all
  show ns
  show ns stats
  show ns (nsei|nsvc) <0-65535>
[stats]
  logging filter nsvc (nsei|nsvci)
<0-65535>
  nsvc (nsei|nsvci) <0-65535>
(block|unblock|reset)
  show bssgp
  show bssgp stats
  show bssgp nsei <0-65535> [stats]
  logging filter bvc nsei <0-65535>
bvci <0-65535>
  show llc
  show sndcp
```

Configuración Terminal

```
OsmoSGSN# configure terminal
OsmoSGSN(config)#
  help
  list
  write terminal
  write file
  write memory
  write
  show running-config
  exit
  end
  hostname WORD
  no hostname [HOSTNAME]
  password (8|) WORD
  password LINE
  enable password (8|) WORD
  enable password LINE
  no enable password
  banner motd default
  banner motd file [FILE]
  no banner motd
  service terminal-length <0-512>
  no service terminal-length [<0-
512>]
  line vty
  service advanced-vty
  no service advanced-vty
  show history
  log stderr
  no log stderr
  log file .FILENAME
  no log file .FILENAME
  log alarms <2-32700>
  no log alarms
  log syslog
(authpriv|cron|daemon|ftp|lpr|mail|n
ews|user|uucp)
  log syslog local <0-7>
  no log syslog
  sgsn
  ns
  bssgp
```