ESCUELA TÉCNICA SUPERIOR DE INGENIEROS INDUSTRIALES Y DE TELECOMUNICACIÓN

UNIVERSIDAD DE CANTABRIA

Trabajo Fin de Grado

Monitorización y estudio de redes celulares en explotación a través de dispositivos USRP

(Monitoring and study of cellular networks in operation through USRP devices)

Para acceder al Titulo de

Graduado en Ingeniería de Tecnologías de Telecomunicación

Autor: Alejandro González Valle

07 - 2018

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

GRADUADO EN INGENIERÍA DE TECNOLOGÍAS DE TELECOMUNICACIÓN

CALIFICACIÓN DEL TRABAJO FIN DE GRADO

Realizado por: Alejandro González Valle
Director del TFG: Ramón Agüero Calvo
Título: "Monitorización y estudio de redes celulares en explotación a través de dispositivos USRP"
Title: "Monitoring and study of cellular networks in operation through USRP devices"

Presentado a examen el día: 20 de Julio de 2018

para acceder al Título de

GRADUADO EN INGENIERÍA DE TECNOLOGÍAS DE TELECOMUNICACIÓN

Composición del Tribunal:
Presidente (Apellidos, Nombre): Artal Latorre, Eduardo
Secretario (Apellidos, Nombre): Agüero Calvo, Ramón
Vocal (Apellidos, Nombre): Lanza Calderón, Jorge

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)

Monitorización y estudio de redes celulares en explotación a través de dispositivos USRP

Grupo de Ingeniería Telemática (GIT)

Resumen

La tecnología LTE se implementó comercialmente por primera vez a finales de 2009. Desde entonces, el número de redes comerciales ha ido creciendo considerablemente en todo el mundo hasta convertirse en la tecnología celular predominante para el envío de datos. Al igual que otras tecnologías celulares, LTE requiere del desarrollo de mejoras que permitan dar soporte a la creciente demanda de datos y densidad de dispositivos. A diferencia de lo que ocurre con otro tipo de tecnologías, tales como WiFi, las implementaciones de tecnologías celulares han estado tradicionalmente disponibles sólo para fabricantes, mientras que la comunidad investigadora ha tenido que hacer uso de otras técnicas para estudiar estas tecnologías.

La solución más extendida para el estudio de tecnologías celulares ha sido la simulación, en sus diferentes vertientes (nivel de enlace, sistema y simulación de redes). En estos casos, aunque su aproximación, según la solución seleccionada, pudiera llegar a ser realista, nunca se podría llegar a reproducir con exactitud un entorno real.

Recientemente, el desarrollo de soluciones Software Defined Radio (SDR) ha permitido disponer de implementaciones de tecnologías celulares capaces de interactuar con redes reales. En concreto, en este trabajo se ha hecho uso de una solución SDR para monitorizar un canal de control LTE haciendo uso de dispositivos comerciales (USRP) y, ya que dicha información es trasmitida en claro, permite realizar un análisis de la red LTE, así como alcanzar una mejor catarterización y comprensión de esta tecnología. Para llevar a cabo tal efecto, se han realizado dos monitorizaciones en distintos escenarios (urbano y suburbano) con diversas condiciones propias del emplazamiento (dispositivos activos, infraestructura, etc), y se han realizado mediciones tanto en el enlace ascendente como descendente, proporcionando información del nivel de uso de la red, tal como la distribución de la carga de una celda a lo largo de la semana o las conexiones de trafico que se realizan cada día.

Asimismo, dado que la solución SDR permite implementar tanto una estación base como un dispositivo de usuario, se ha evaluado la posibilidad de desplegar un sistema completo con la solución SDR seleccionada.

Monitoring and study of cellular networks in operation through USRP devices

Telematics Engineering Group (GIT)

Abstract

The LTE technology was commercially introduced for the first time at the end of 2009. From then on, the number of commercial networks has been growing around the world to become the predominant cellular technology for data transmission. As other cellular technologies, LTE requires the development of improvements to support the growing demand for data and devices density. As opposed to happen with other types of technologies, such as WiFi, implementations of cellular technologies have traditionally been available only to operators, while the research community has had to use other techniques to study these technologies.

The most spread out solution for the study of cellular technologies has been simulation, in different aspects (link level, system and network simulation). In these cases, although their approximations, according to the selected solution, could become realistic, a real environment could never be accuretly reproduced.

Recently, the development of Software Defined Radio (SDR) has allowed implementations of cellular technologies capable of interacting with real networks. Specifically, in this project a SDR solution has been used to monitor a LTE control channel by commercial devices (USRP) and how this information is transmitted unencrypted, allowing the analysis of the LTE network. In order to carry out this effect, two monitoring sessions have been conducted in different scenes (urban and suburban) with various conditions from the environment (active devices, infrastructure, etc.), and the uplink and downlink have been analysed, providing information about the level of use of the network, such as the distribution of the load of a cell throughout the week or the traffic connections that are made every day.

Also, how the SDR solution allows to implement a base station and a user device, it has been evaluated the possibility of deploying a complete system with the selected SDR solution.

Agradecimientos

En primer lugar, quisiera mostrar mi agradecimiento a Ramón Agüero y Luis Francisco Díez, por la oportunidad que me brindaron al ofrecerme este proyecto. Mi más sincero reconocimiento para ellos por su dedicación y comprensión durante todo este tiempo, intentando que esto saliera adelante de la mejor manera posible. No quisiera desperdiciar la oportunidad de hacer una mención especial a Luis por aportarme las herramientas que necesitaba para emprender este camino: orientación, destreza y conocimiento. Has sido una pieza imprescindible de este proyecto.

A mis compañeros y, sobre todo, a aquellos que un día dejaron de serlo para convertirse en amigos. Gracias por hacer el camino más ameno.

A mi familia, por ayudarme siempre que lo he necesitado. Habéis estado en las buenas, pero también en las malas y es con lo que me quedo. En especial agradecer a mis padres, por haberme dado los medios necesarios para formarme personal y académicamente.

Y a Carmen, el motor de mi vida. Me has acompañado en cada momento de toda esta etapa aportando tu paciencia, comprensión, y sobre todo cariño. Gracias por ser como eres.

A todos, MUCHAS GRACIAS.

Índice general

Índice general **I**

Lista de figuras **III**

Índice de tablas **V**

Acronimos **IX**

1. Introducción **1**
1.1. Motivación 1
1.2. Objetivos 1
1.3. Estructura del documento 2

2. Conceptos Previos **3**
2.1. Parámetros *Long Term Evolution* 4
2.2. Arquitectura de *Long Term Evolution* 4
2.2.1. Equipo de Usuario 5
2.2.2. Red de Acceso 5
2.2.3. *Evolved Packet Core* (EPC) 6
2.3. Interfaz radio 7
2.3.1. Plano de usuario 7
2.3.2. Plano de control 8
2.3.3. Protocolo de Convergencia de Datos de Paquetes 9
2.3.4. Control de Enlace de Radio 10
2.3.5. Control de Acceso al Medio 10
2.4. Tipos de Canales 11
2.4.1. Canales físicos 11
2.4.2. Canales de transporte 13
2.4.3. Canales lógicos 13
2.5. *Radio Network Temporary Identifier* 13
2.6. Categoría de los usuarios 14

3. Soluciones SDR existentes **16**
3.1. OpenAirInterface 16
3.2. Solución srsLTE 17

3.3. Proyecto IMDEA-OWL 19
3.3.1. $cell_search -b < *banda* > 20
3.3.2. $imdea_cc_decoder_rotate -f < *freq* > 20
3.4. Elección de la solución SDR 21

4. Resultados **22**
4.1. Estructura del código 24
4.1.1. OwlSearchCell 24
4.1.2. OwlCommonStats 25
4.2. Monitorización 27
4.2.1. Operadores en España 27
4.2.2. Búsqueda de la celda 29
4.2.3. Carga de las celdas 30
4.2.4. Eficiencia de las comunicaciones 33
4.2.5. Análisis de tráfico 35
4.2.6. Sesiones 41
4.2.7. Categoría de los usuarios 43
4.3. Implementación práctica de una estación base y un equipo de usuario 45

5. Conclusiones y líneas futuras **47**
5.1. Conclusiones 47
5.2. Líneas futuras 48

Bibliografía **49**

Índice de figuras

2.1. Evolución de las tecnologías celulares 3
2.2. Arquitectura LTE de alto nivel 4
2.3. Arquitectura E-UTRAN 5
2.4. Arquitectura EPC 7
2.5. División funcional entre E-UTRAN y EPC 7
2.6. Ejemplo de tráfico de enlace ascendente "tunelizado" 8
2.7. Pila de protocolos del plano usuario 8
2.8. Pila de protocolos del plano control 9
2.9. Paquetes en cada capa del E-UTRAN 10
2.10. Mapeo de los canales LTE 11
2.11. *Throughput* de cada categoría de UE 15

3.1. Arquitectura de la plataforma srsLTE 18

4.1. Máxima potencia de los procesadores 22
4.2. Emplazamiento Suburbano 23
4.3. Estructura del Proyecto 24
4.4. Estructura del código `OwlSearhCell` 25
4.5. Estructura del código `OwlCommonStats` 26
4.6. Servicio de Comunicaciones Electrónicas por bandas en España (Fuente: Registro Público de concesiones - Gobierno de España) 28
4.7. Penetración de LTE por operador en función del área de análisis: a la izquierda se muestran los resultados en entorno suburbano, y a la derecha en entorno urbano. Como se puede observar, únicamente se han encontrado celdas pertenecientes a los tres principales operadores en España. 29
4.8. Resumen de tiempo/frecuencia de la estructura de recursos LTE (ref: QoS aware schedulers for multi-users on OFDMA downlink: Optimal and heuristic - Scientific Figure on ResearchGate) 31
4.9. CDF de la cantidad de recursos asignados en la celda suburbana 32
4.10. CDF de la cantidad de recursos asignados en la celda urbana 32
4.11. Nivel medio de carga de los recursos asignados en el tiempo 33
4.12. CDF del valor de MCS en la celda suburbana 34
4.13. CDF del valor de MCS en la celda urbana 35
4.14. Proceso de acceso a contienda del RAP 36
4.15. Tiempo de la respuesta de la ventana RAR 37

4.16. Línea de tiempo de los RAP 38
4.17. Ejemplo de traspaso: *contention-free* (RAP) 39
4.18. Línea de tiempo de los traspasos 39
4.19. Línea de tiempo de la señalización 40
4.20. Línea de tiempo del tráfico 41
4.21. CDF de la longitud de las sesiones 42
4.22. Número de sesiones en cada emplazamiento 42
4.23. Evolución de RNTI 43
4.24. Porcentaje de categorías del UE 43
4.25. Velocidad de descarga de las categorias de UE 44
4.26. Esquema de la implementación práctica de eNB y UE 45
4.27. Captura *Wireshark* de la estación base 46

5.1. Ejemplo del proceso basado en contienda (RAP). Parte 1 50
5.2. Ejemplo del proceso basado en contienda (RAP). Parte 2 51
5.3. Ejemplo del proceso basado en contienda (RAP). Parte 3 52

Índice de Tablas

2.1. Parámetros LTE vs 3G 4
2.2. Valores de RNTI 14
2.3. Canales de RNTI 14
2.4. Categorias de UE 15

4.1. Caracteristicas Estacion Movil (Fuente:InfoAntenas) 22
4.2. Frequencia monitorizada del emplazamiento 24
4.3. Valores RNTI por clases 27
4.4. Mejores celdas encontradas por Banda y SNR 29
4.5. Relación entre PRB, ancho de banda y velocidad pico 31
4.6. Lista de valores del indice MCS 34
4.7. Porcentaje de uso del ancho de banda disponible 41
4.8. Especificaciones de UEs (Fuente:Gsmarena) 44

Acrónimos

ACK Reconocimiento

AES Advanced Encryption Standard

APN Access Point Name

AS Access Stratum

AM Modo Confirmado

BCH Broadcast CHannel

BCCH Broadcast Control CHannel

BPSK Binary Phase Shift Keying

BSR Buffer Status Reports

C-RNTI Cell Radio Network Temporary Identifier

CC-RNTI Common Control RNTI

CCCH Common Control CHannel

CFI Control Format Indicator

CP Cyclic Prefix

DAB Digital Audio Broadcasting

DCCH Dedicated Control CHannel

DCI Downlink Control Information

DL Enlace Descendente

DL-SCH DownLink Shared CHannel

DTCH Dedicated Traffic CHannel

eNB evolved NodeB

EPC Evolved Packet Core

EPS Evolved Packet System

E-UTRAN Red de Acceso

FDD Frequency Division Duplex

GPP General Purpose Processor

GPRS General Packet Radio Service

GSM Global System for Mobile communications

GTP GPRS Tunneling Protocol

HARQ Hybrid Automatic Repeat reQuest

HPSK Hybrid Phase Shift Keying

HSS Servidor de Abonado

IoT Internet of Things

LTE Long Term Evolution

M-RNTI MBMS Radio Network Temporary Identifier

MAC Control de Acceso al Medio

MCCH Multicast Control CHannel

MCH Multicast CHannel

MCS Esquemas de Modulación y Codificación

MIB Master Information Block

MIMO Entrada Múltiple - Salida Múltiple

MME Entidad de gestión de movilidad

MMSE Error Medio Mínimo Cuadrado

MT Mobile Termination

MTCH Multicast Traffic CHannel

NACK Reconocimiento Negativo

NAS Non Access Stratum

NCCE Unidad de Asignación de Recursos Básicos para PDCCH

OAI OpenAirInterface

OFDM Orthogonal Frequency Division Multiplexing

OFDMA Orthogonal Frequency Division Multiplexing Access

PBCH Physical Broadcast CHannel

PCCH Paging Control CHannel

PCEF Función de Control de Políticas

PCH Paging CHannel

PCFICH Physical Control Format Indicator CHannel

PCRF Control de políticas y reglas de cobro de funciones

PDCCH Physical Downlink Control CHannel

PDCP Protocolo de Convergencia de Datos de Paquetes

PDSCH Physical Downlink Shared CHannel

PDU Unidad de Datos de Protocolo

PDN Packet Data Network

P-GW PDN GateWay

P-RNTI Paging RNTI

PHICH Physical Hybrid ARQ Indicator CHannel

PRACH Physical Random Access CHannel

PRB Número de Recursos Asignados

PSS Señal de Sincronización Primaria

PUCCH Physical Uplink Control CHannel

PUSCH Physical Uplink Shared CHannel

QoS Calidad del Servicio

QAM Quadrature Amplitude Modulation

QPSK Quadrature Phase Shift Keying

RA-RNTI Random Access Radio Network Temporary Identifier

RACH Random Access CHannel

RAP Procedimiento de Acceso Aleatorio

RAR Respuesta de Acceso Aleatorio

RB Recursos Asignados

RE Elemento de Recurso

RLC Control de Enlace de Radio

RNTI Radio Network Temporary Identifier

RRC Control de Recursos de Radio

RS Reference Signal

S1AP S1 Application Protocol

SDM Multiplexación por División Espacial

SDR Software Defined Radio

SDU Unidad de Datos de Servicio

SFI Sub-Frame Index

SFN System Frame Number

S-GW Serving GateWay

SAP Service Access Point

SC-RNTI Single Cell RNTI

SC-MCCH Single Cell-MCCH

SC-PTM Single Cell Point-to-Multipoint

SC-N-RNTI Single Cell Notification RNTI

SI-RNTI System Information Radio Network Temporary Identifier

SIM Subscriber Identification Module

SISO Entrada Unica - Salida Unica

SNR Relación Señal/Ruido

SR Solicitud de Programación

SRS Software Radio Rystems (www.softwareradiosystems.com)

SSS Señal de Sincronización Secundaria

TB Bloque de Transporte en Bits

TDD Time Division Duplex

TE Terminal Equipment

TEID Tunnel Endpoint Identifier

TTI Intervalo de Tiempo de Transmisión

TM Modo Transparente

UE Equipo de Usuario

UHD Controlador de Hardware Universal

UL Enlace Ascendente

UL-SCH UpLink Shared CHannel

UICC Universal Integrated Circuit Card

UM Modo no Reconocido

UMTS Universal Mobile Telecommunications System

USIM Universal Subscriber Identity Module

USRP Universal Software Radio Peripheral

3GPP Third Generation Partnership Project

Capítulo 1

Introducción

1.1. Motivación

Los sistemas celulares se encuentran entre las últimas industrias, se espera que converjan a plataformas Hardware/Software de bajo coste o abiertas. En la actualidad, por la complejidad de la red móvil, construir un banco de pruebas con dispositivos comerciales o usar un emulador comercial es costoso. Por lo tanto, los desarrollos abiertos parecen la opción más apropiada para que las comunidades académicas puedan construir y evaluar un ecosistema celular abierto y, de esta manera, puedan fomentar innovaciones en el mundo inalámbrico como ya se produjo en Android para los sistemas operativos móviles. Generalmente hay tres formas de obtener entornos de prueba: la primera es que el generador comercial de telecomunicaciones proporcione acceso a una red. Sin embargo, al tratarse de una red pública el control es limitado. Otro método es que los vendedores de equipos de comunicación móvil implementen sus propios productos de emulado, lo que es generalmente muy costoso. Por último, una opción que está generando popularidad es la de usar desarrollos abiertos que proporcionan implementaciones realistas de los enlaces ascendente y descendente en entornos multicelulares, multiusuario y con conectividad IP de extremo a extremo. La ventaja respecto a los costes hace que esta última opción sea la elección más adecuada para estudios sobre red celular. En este trabajo se hace uso de un desarrollo de Software Defined Radio (SDR) para monitorizar y analizar el uso real de sistemas comerciales Long Term Evolution (LTE). Sus utilidades son muy amplias, por ejemplo se puede utilizar para construir y personalizar una estación base LTE y una red central en un ordenador para conectar un Equipo de Usuario (UE) comercial y probar diferentes configuraciones de red. Otro uso posible es llevar a cabo una monitorización de la red y el dispositivo móvil en tiempo real.

1.2. Objetivos

El objetivo principal de este proyecto es la caracterización y estudio del nivel de uso de redes celulares comerciales, en concreto de la tecnología LTE. Para ello se va a hacer uso de soluciones abiertas SDR. Como objetivo secundario aparece la necesidad de estudiar la tecnología LTE tanto desde un punto de vista de arquitectura como de gestión de recursos. Asimismo, se hace necesario el análisis de las diferentes soluciones SDR que permiten llevar a cabo dicha caracterización.

1.3. Estructura del documento

A continuación, se detalla la estructura y el contenido de cada uno de los capítulos que forman este trabajo para dar una visión general del documento:

- **Capítulo 2: Conceptos previos**

  En el segundo capítulo, se presentan los conceptos previos y teóricos de LTE necesarios para desarrollar y comprender este trabajo.

- **Capítulo 3: Soluciones SDR existentes**

  En el tercer capítulo, se narra el estudio realizado acerca de las diferentes soluciones SDR existentes para determinar con qué solución cimentar este proyecto. A continuación, se describe el proyecto seleccionado detalladamente, el cual servirá de base para la solución implementada en este trabajo.

- **Capítulo 4: Resultados**

  En el cuarto capítulo, se describe la implementación llevada a cabo y se muestran los resultados obtenidos.

- **Capítulo 5: Conclusiones**

  En el quinto y último capítulo, se recogen las ideas obtenidas a lo largo de este trabajo, así como las lineas futuras que surgen de su realización.

Capítulo 2

Conceptos Previos

LTE se inició como un proyecto en el año 2004 por el organismo de telecomunicaciones conocido como Third Generation Partnership Project (3GPP). Evolucionó a partir de un sistema anteriormente conocido como Universal Mobile Telecommunications System (UMTS), que a su vez evolucionó a partir de Global System for Mobile communications (GSM). Un rápido aumento del uso de datos móviles y la aparición de nuevas aplicaciones tales como *Multimedia Online Gaming*, TV móvil, Web 2.0 o *streaming* de contenidos, hicieron necesaria la definición de la 4ª generación de comunicaciones móviles. El principal objetivo de LTE es proporcionar una alta velocidad de datos, baja latencia y optimizar la tecnología de acceso radioeléctrico. Al mismo tiempo, su arquitectura de red se ha diseñado con el objetivo de apoyar el tráfico de paquetes conmutados con movilidad transparente y alta calidad de servicio.

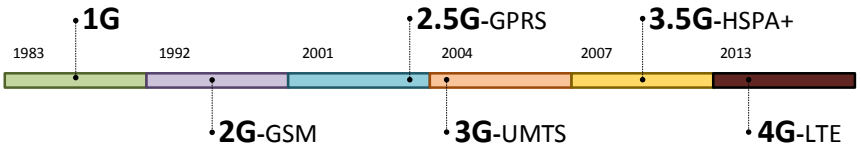


Figura 2.1: Evolución de las tecnologías celulares

Para facilitar la comprensión del documento, en este capítulo se describen algunos conceptos básicos de la tecnología empleada a lo largo de este trabajo. [6] [5]

Primeramente, en la sección 2.1 se dan algunas características técnicas generales acerca de estas redes. Por su parte, la sección 2.2 presenta la arquitectura general de la red, ofreciendo una descripción de las funciones proporcionadas. Seguidamente, en la sección 2.3, se explica la pila de protocolos a través de las diferentes interfaces, junto con una descripción genérica de las funciones provistas por las diferentes capas de protocolo. Además, se ilustra el flujo y empaquetado de datos que sucede en las capas. A continuación, en la sección 2.4 se engloba la estructura detallada de los canales usados en LTE, los cuales, están diseñados para hacer un uso eficiente de los recursos, y para apoyar la multiplexación efectiva entre los datos y la señalización de control. Por último, en la sección 2.5 se explica un parámetro fundamental en el desarrollo de este trabajo, el Radio Network Temporary Identifier (RNTI).

2.1. Parámetros *Long Term Evolution*

En esta sección, se destacan las principales métricas de rendimiento utilizadas en la definición de los requisitos de LTE. La Tabla 2.1 engloba los principales parámetros, en los cuales se puede observar que representan un paso significativo de la capacidad y la experiencia del usuario ofrecidas por los sistemas de comunicaciones móviles de tercera generación que se estaban implementando hasta el momento. Esto es debido a que las redes LTE evitan las restricciones de la compatibilidad con versiones anteriores, permitiendo la inclusión de esquemas Entrada Múltiple - Salida Múltiple (MIMO) avanzados en el diseño del sistema, y un uso del espectro altamente flexible basado en nuevos esquemas de acceso múltiple.

Tabla 2.1: Parámetros LTE vs 3G

Parámetros	**LTE**	**3G**
Codificación de canal	Turbo código	Turbo código
Ancho de Banda del Canal (MHz)	100	100
Esquema de modulación (UL)	QPSK, 16QAM, 64QAM	QPSK
Esquema de modulación (DL)	QPSK, 16QAM, 64QAM	HPSK
Latencia de conexión (ms)	< 100	100–500
Vel. de transmisión máxima (Mbps)	300	2

2.2. Arquitectura de *Long Term Evolution*

Todas estas características son compatibles a través de varios elementos de red de la Evolved Packet System (EPS) con diferentes roles. La Figura 2.2 muestra la arquitectura general de la red, incluyendo los elementos de red y las interfaces estandarizadas. A alto nivel, la red está compuesta por la EPC y la red de acceso, es decir, E-UTRAN. Mientras que la EPC consta de varios nodos lógicos, la red de acceso se compone de un solo nodo, la estación base o, evolved NodeB (eNB), que se conecta a los UE. Cada uno de estos elementos de red está interconectados por medio de interfaces que están estandarizadas para permitir la interoperabilidad entre múltiples proveedores.

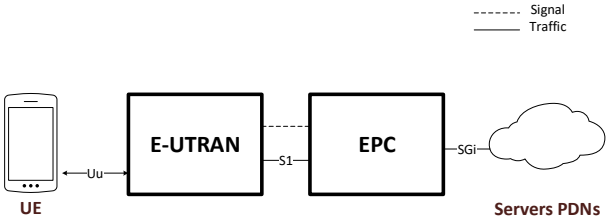


Figura 2.2: Arquitectura LTE de alto nivel

A continuación, se presentan las características principales de cada uno de los componentes.

2.2.1. Equipo de Usuario

La arquitectura interna del Equipo de Usuario (UE) empleada en esta tecnología es idéntica a la utilizada por UMTS y GSM. Se compone de los siguientes módulos:

- **Mobile Termination (MT)**: se encarga de todas las funciones de comunicación.
- **Terminal Equipment (TE)**: pone fin a los flujos de datos.
- **Universal Integrated Circuit Card (UICC)**: más conocida como la tarjeta SIM, en ella se ejecuta una aplicación conocida como Universal Subscriber Identity Module (USIM). Esta aplicación almacena datos específicos del usuario muy similares a la tarjeta SIM como por ejemplo, mantener la información sobre el número de teléfono del usuario, la identidad de la red doméstica y claves de seguridad.

2.2.2. Red de Acceso

Este segmento de red se ocupa de las comunicaciones radio entre el móvil y las estaciones base, eNBs. Además de las comunicaciones con los dispositivos, esta red de acceso radio permite comunicación entre estaciones base, tal como se muestra en la Figura 2.3. Los protocolos que se ejecutan entre las eNBs y los UEs se conocen como los protocolos de Access Stratum (AS). Sus principales funcionalidades son:

- Gestión de recursos de radio, la eNB envía y recibe las transmisiones de radio para todos los UEs que utilizan las funciones de procesamiento de señales digitales.
- Compresión de encabezado, esto ayuda a garantizar el uso eficiente de la interfaz radio.
- Seguridad, ya que todos los datos enviados a través de la interfaz radio están encriptados.
- Posicionamiento, ayuda a encontrar la posición del UE.
- Y por último, conectividad al EPC, la eNB controla el funcionamiento a bajo nivel de todos sus UEs, mediante el envío de mensajes de señalización hacia el MME y la comunicación de datos de usuario hacia el S-GW, que se detallan más adelante.

Como se aprecia en la Figura 2.3, cada eNB se conecta con el EPC a través de la interfaz S1. Por otro lado, se puede conectar a las estaciones base cercanas a través de la interfaz X2, que se utiliza principalmente para la señalización y el reenvío de paquetes durante traspasos.

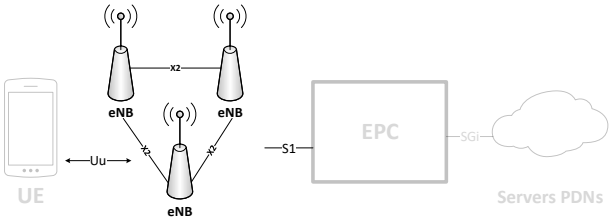


Figura 2.3: Arquitectura E-UTRAN

2.2.3. *Evolved Packet Core* (EPC)

Este componente de la arquitectura comprende el núcleo de la red, es el elemento responsable del control general de los UEs y del establecimiento de las portadoras de datos. Los principales nodos lógicos se detallan a continuación con una breve descripción de cada uno de ellos y la relación que tienen entre sí mediante la Figura 2.4.

- **Entidad de gestión de movilidad (MME)**: es el nodo de control que procesa, la señalización entre el UE y la Red de Acceso (E-UTRAN), y los mecanismos de localización de los UEs. Los protocolos que se ejecutan se conocen como los protocolos del Non Access Stratum (NAS). Sus funciones principales están relacionadas con la gestión de portadoras de tráfico, gestión de conexiones y con la integración con otras redes.

- **Servidor de Abonado (HSS)**: aparece también en UMTS y GSM. Es una base de datos central que contiene información acerca de todos los abonados del operador de red, tales como el perfil de Calidad del Servicio (QoS) suscrito y cualquier restricción de acceso para el *roaming*. Además, contiene información dinámica, como la identidad de la MME a la que el usuario está conectado o registrado actualmente.

- **Serving GateWay (S-GW)**: actúa como un enrutador y reenvía los datos entre la estación base y la pasarela Packet Data Network (PDN) o P-GW que se describe a continuación, es decir, todos los paquetes IP de usuario se transfieren a través del S-GW, que sirve como anclaje de movilidad local para las portadoras de datos cuando el UE se mueve entre eNBs. Además, realiza algunas funciones administrativas en la red visitada, como la recopilación de información para cobrar (por ejemplo, el volumen de datos enviados o recibidos por el usuario) y la interceptación legal. También sirve como anclaje de movilidad para interactuar con otras tecnologías 3GPP, como GPRS y UMTS.

- **PDN GateWay (P-GW)**: es responsable de la asignación de la dirección IP para el UE, así como la aplicación de la QoS y la carga basada en el flujo de acuerdo con las reglas de la PCRF por lo que enlaza con la PDN para comunicarse con el mundo exterior, para ello utiliza la interfaz de SGi. Cada red de paquetes de datos se identifica por un Access Point Name (APN).

- **Control de políticas y reglas de cobro de funciones (PCRF)**: este componente no se muestra en el Figura 2.4, pero es responsable de controlar la factorización en base a políticas definidas, Función de Control de Políticas (PCEF), que reside en el P-GW. La PCRF proporciona el control de QoS, que decide cómo se tratará un determinado flujo de datos en la PCEF y garantiza que esto esté de acuerdo con el perfil de suscripción del usuario.

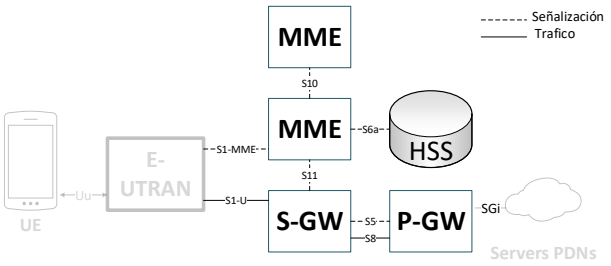


Figura 2.4: Arquitectura EPC

Después de ver las diferentes partes de los elementos de red Evolved Packet Core (EPC) y E-UTRAN, la Figura 2.5 muestra la división funcional entre ellos.

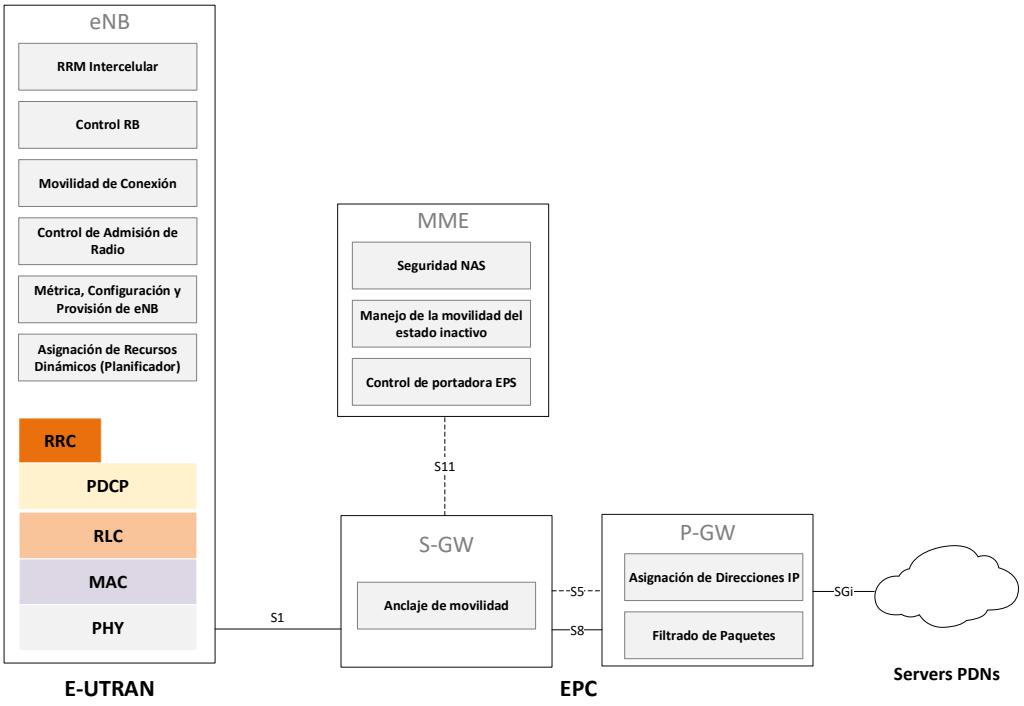


Figura 2.5: División funcional entre E-UTRAN y EPC

2.3. Interfaz radio

En la interfaz radio se utiliza una pila de protocolos específica que se puede dividir en un plano de usuario y un plano de control. A continuación, se detalla cada plano y las capas que tienen en común.

2.3.1. Plano de usuario

El plano de usuario se encarga de todos los protocolos que realizan transferencia de datos de usuario. En esta sección se muestra un ejemplo de cómo un usuario se comunica con un

servidor para el acceso, por ejemplo, a Internet. Un paquete IP sale del UE y se encapsula en un protocolo específico de EPC para ser "tunelizado" entre el P-GW y la eNB. Existen diferentes protocolos de túnel en diferentes interfaces, en el ejemplo mostrado, en la Figura 2.6 usa GPRS Tunneling Protocol (GTP).

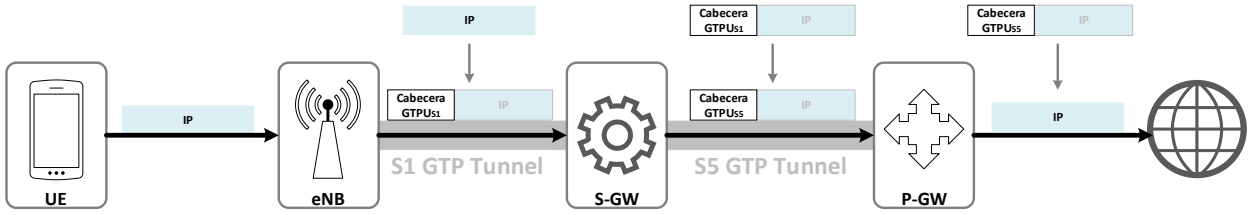


Figura 2.6: Ejemplo de tráfico de enlace ascendente "tunelizado"

En la Figura 2.7 se muestra la pila de protocolos del plano de usuario E-UTRAN, destacar las subcapas PDCP, RLC y MAC que terminan en la eNB en el lado red.

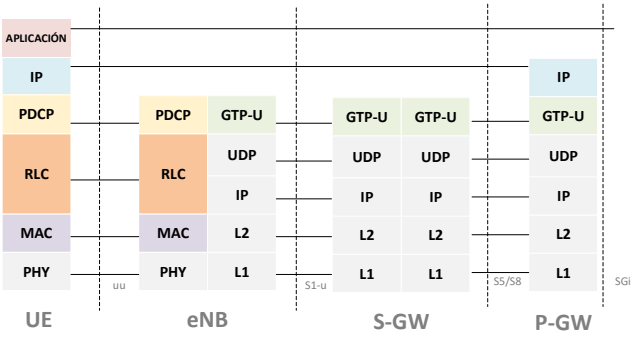


Figura 2.7: Pila de protocolos del plano usuario

Con el fin de reducir los requisitos de procesamiento de la pila de protocolos del plano de usuario en LTE, las cabeceras creadas por cada uno de los protocolos antes mencionados están alineadas por byte. Esto implica que a veces se necesitan bits de relleno no utilizados en las cabeceras y, por lo tanto, el costo de diseño para un procesamiento eficiente es que se desperdicia una pequeña cantidad de capacidad potencialmente disponible.

2.3.2. Plano de control

Este plano se encarga de gestionar la transferencia de datos en el plano de usuario. Además es responsable de las conexiones de los UEs con la E-UTRAN como se muestra en la Figura 2.8. Las capas inferiores realizan las mismas funciones que para el plano de usuario, con la excepción de que no existe una función de compresión de encabezado para el plano de control. El protocolo de Control de Recursos de Radio (RRC), conocido como "Capa 3" en la pila de protocolos AS, se encarga de gestionar las entradas del plano de usuario.

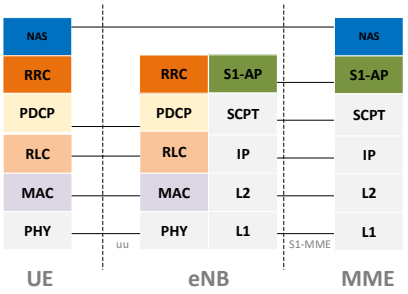


Figura 2.8: Pila de protocolos del plano control

Sus principales funciones son establecer las portadoras radio y configurar todas las capas inferiores usando la señalización RRC entre la eNB y el UE, para ello se establecen túneles GTP, como se vio anteriormente, mediante los siguientes pasos:

1. S-GW asigna un Tunnel Endpoint Identifier (TEID) para el tráfico de enlace ascendente.
2. La estación base, eNB, asigna un TEID para el tráfico de enlace descendente.
3. Los valores TEID se intercambian entre la eNB y el S-GW a través del MME mediante mensajes S1 Application Protocol (S1AP) y GTP-C.

A continuación, se entra en detalle en la capa de enlace que engloba las capas comunes antes mencionadas en las Figuras 2.7 y 2.8. Su principal cometido es, junto a la capa física, sustentar el envió de paquetes IP.

2.3.3. Protocolo de Convergencia de Datos de Paquetes

La capa de Protocolo de Convergencia de Datos de Paquetes (PDCP) está presente tanto en el plano usuario como en el plano de control y realiza las siguientes funciones:

- Compresión y descompresión de cabeceras para datos de plano de usuario.
- Funciones de seguridad como cifrar y descifrar para el plano de usuario y plano de control, y protección y verificación de la integridad para los datos del plano de control.
- Funciones de soporte de traspaso, por ejemplo, entrega y reordenamiento en secuencia de PDU y transferencia sin pérdida para los datos del plano de usuario mapeados en el modo de confirmación del RLC.
- Por último, descarta datos del plano de usuario debido al tiempo de espera.

En este punto es importante dejar claro la diferencia entre SDU y PDU para la compresión de este trabajo.

- Los paquetes recibidos por una capa se conocen como **Unidad de Datos de Servicio (SDU)**.
- Los paquetes de salida de una capa se conoce como **Unidad de Datos de Protocolo (PDU)**.

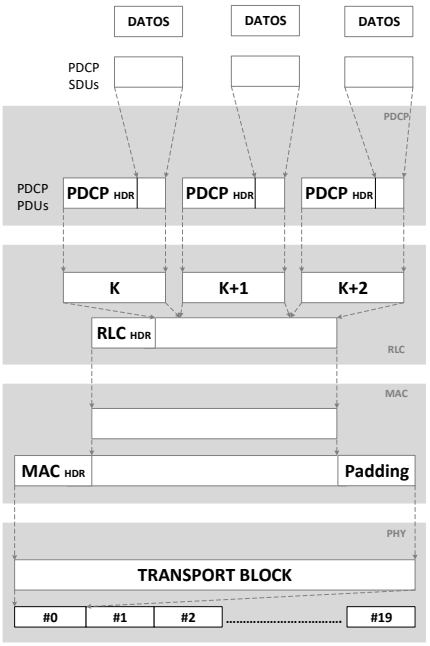


Figura 2.9: Paquetes en cada capa del E-UTRAN

2.3.4. Control de Enlace de Radio

La capa Control de Enlace de Radio (RLC) es la capa intermedia entre la capa PDCP, la capa "superior", y la capa MAC, la capa "inferior". Se comunica con la capa PDCP a través de un Service Access Point (SAP) y con la capa MAC a través de canales lógicos. Una de sus labores, en el lado de transmisión, es segmentar y/o concatenar las PDU recibidas de PDCP para enviarlas a la capa MAC. Por otro lado, en la recepción, realiza el reensamblaje de la PDU de RLC para enviarla a la capa PDCP. Además, la entidad RLC reordena las PDU de RLC si se reciben fuera de secuencia debido a la operación Hybrid Automatic Repeat reQuest (HARQ) realizada en la capa MAC. Esta es la diferencia clave de LTE respecto a UMTS, donde la reordenación HARQ se realiza en la capa MAC.

Las funciones mencionadas son realizadas por "entidades RLC" que se configuran en tres modos diferente con distintos niveles de fiabilidad.: Modo Transparente (TM), Modo no Reconocido (UM) y Modo Confirmado (AM). El modo TM se usa para señalización y no aplica ninguna de las funciones definidas en RLC. Por otro lado, los modos AM y UM se usan para el tráfico de datos en función de los requisitos de QoS. La principal diferencia entre los modos AM y UM es que el primero realiza confirmaciones y reenvíos en caso de que algún PDU de RLC se haya perdido.

2.3.5. Control de Acceso al Medio

La capa Control de Acceso al Medio (MAC) es la capa más baja de la pila de protocolos radio LTE. La conexión a la capa física se realiza a través de canales de transporte, y la conexión a la capa RLC se realiza a través de canales lógicos, en la Sección 2.4 se verán más en detalle. Por lo tanto, la capa MAC realiza multiplexación y demultiplexación entre canales lógicos y canales de transporte.

2.4. Tipos de Canales

Hay tres categorías en las que se pueden agrupar los diversos canales de datos.

- **Canales físicos:** son canales de transmisión que transportan, datos de usuario y canales lógicos (Verdes en la Figura 2.10). Los canales físicos se definen sobre los recursos radio usados por la capa física. y son el primer nivel de diferenciación de tráfico.
- **Canales de transporte:** transportan tráfico hacia la capa física ofreciendo transferencia de información al control de acceso al medio y capas superiores (Naranjas).
- **Canales lógicos:** proporcionan servicios para la capa de control de acceso al medio dentro de la estructura del protocolo LTE (Azules).

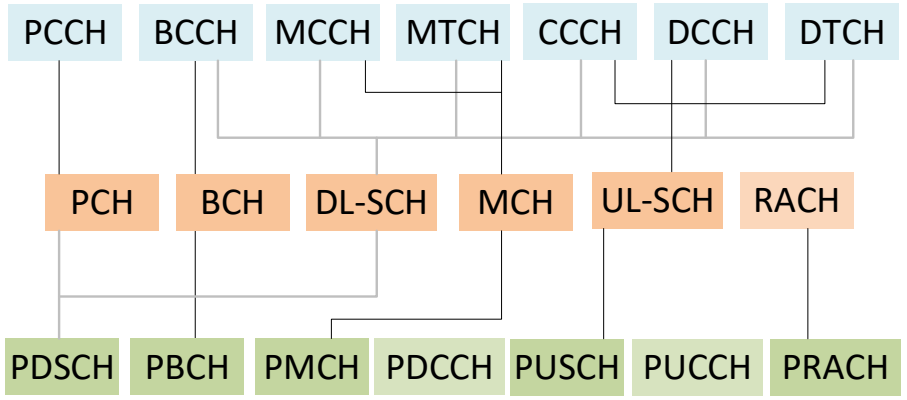


Figura 2.10: Mapeo de los canales LTE

A continuación se enumeran los principales canales definidos en LTE.

2.4.1. Canales físicos

- **Physical Broadcast CHannel (PBCH).** Este canal, transporta información del sistema para los UEs que requieren acceder a la red. Solo lleva lo que se denomina mensajes de Master Information Block (MIB). El esquema de modulación es siempre Quadrature Phase Shift Keying (QPSK) y los bits de información están codificados. El mensaje MIB en el PBCH se mapea en las 72 subportadoras centrales o 6 bloques de recursos centrales, independientemente del ancho de banda general del sistema. Se repite un mensaje PBCH cada 40 ms, es decir, un Intervalo de Tiempo de Transmisión (TTI) de PBCH incluye cuatro tramas de radio.
- **Physical Control Format Indicator CHannel (PCFICH).** Como su nombre indica, el PCFICH informa al UE sobre el formato de la señal que se recibe. Indica el número de símbolos Orthogonal Frequency Division Multiplexing (OFDM) utilizados para los PDCCH, ya sea 1, 2 o 3. La información dentro del PCFICH es esencial porque el UE no tiene información previa.

Un PCFICH se transmite en el primer símbolo de cada subtrama y lleva un campo de Control Format Indicator (CFI). El CFI contiene una palabra de código de 32 bits que representa 1, 2, 3 o 4 (este último esta reservado para un posible uso en el futuro).

Se utiliza una codificación de bloques de 2/32 que da como resultado una velocidad de codificación de 1/16, y siempre utiliza la modulación QPSK para garantizar una recepción robusta.

- **Physical Downlink Control CHannel (PDCCH).** El objetivo principal de este canal físico es llevar información de gestión de diferentes tipos: gestión de recursos de enlace descendente, instrucciones de control de potencia del enlace ascendente, propuesta de recursos de enlace ascendente, indicación para paginación o información del sistema.

  El PDCCH contiene un mensaje conocido como Downlink Control Information (DCI) que transporta la información de control para un UE particular o grupo de UEs. El formato DCI tiene varios tipos diferentes que se definen con diferentes tamaños: tipo 0, 1, 1A, 1B, 1C, 1D, 2, 2A, 2B, 2C, 3, 3A y 4.

- **Physical Hybrid ARQ Indicator CHannel (PHICH).** Como su nombre indica, este canal se utiliza para informar el estado de HARQ. Lleva la señal ACK/NACK para indicar si un bloque de transporte se ha recibido o no correctamente.

  El PHICH se transmite dentro de la región de control de la subtrama y típicamente hace uso del primer símbolo. Si el enlace radio es débil, entonces se extiende a un número de símbolos para dar mayor robustez.

- **Physical Uplink Control CHannel (PUCCH)**. Este canal, proporciona los diversas funcionalidades de señalización de control. Hay varios formatos diferentes definidos para permitir que el canal transmita la información requerida en el formato más eficiente para el escenario particular encontrado. Incluye la capacidad de transportar Solicitud de Programación (SR).

- **Physical Downlink Shared CHannel (PDSCH).** Es el canal principal de enlace descendente que lleva datos en LTE. Se utiliza para todos los datos de usuario, así como para la información del sistema de difusión que no se transmite en el PBCH, y para mensajes de búsqueda de personas.

- **Physical Uplink Shared CHannel (PUSCH).** Este canal físico, es el par de PDSCH en el enlace ascendente.

- **Physical Random Access CHannel (PRACH).** Este canal físico de enlace ascendente, se usa para funciones de acceso aleatorio. Esta es la única transmisión no sincronizada que el UE puede hacer dentro de LTE. Los retardos de propagación de enlace descendente y enlace ascendente son desconocidos cuando se utiliza PRACH y, por lo tanto surge el problema.

2.4.2. Canales de transporte

- **Broadcast CHannel (BCH).** Se asigna al BCCH.
- **DownLink Shared CHannel (DL-SCH).** Es el canal principal para la transferencia de datos de enlace descendente. Es utilizado por muchos canales lógicos.
- **Paging CHannel (PCH).** Se utiliza para transmitir el PCCH.
- **Multicast CHannel (MCH).** Se usa para transmitir información de MCCH y configurar transmisiones de multidifusión.
- **UpLink Shared CHannel (UL-SCH).** Es el canal principal para la transferencia de datos de enlace ascendente. Es utilizado por muchos canales lógicos.
- **Random Access CHannel (RACH).** Se usa para requisitos de acceso aleatorio.

2.4.3. Canales lógicos

- **Broadcast Control CHannel (BCCH).** Proporciona información del sistema a todos los terminales móviles conectados al eNB.
- **Paging Control CHannel (PCCH).** Se utiliza para buscar información cuando se quiere localizar una unidad en una red.
- **Common Control CHannel (CCCH).** Este canal se usa para obtener información de acceso aleatorio, por ejemplo, para acciones que incluyen la configuración de una conexión.
- **Multicast Control CHannel (MCCH).** Se utiliza para la recepción necesaria de multidifusión.
- **Dedicated Control CHannel (DCCH).** Se usa para transportar información de control específica del usuario, por ejemplo, controlar acciones que incluyen control de potencia, traspaso, etc.
- **Dedicated Traffic CHannel (DTCH).** Se utiliza para la transmisión de datos de usuario.
- **Multicast Traffic CHannel (MTCH).** Este canal se utiliza para la transmisión de datos de multidifusión.

2.5. *Radio Network Temporary Identifier*

Un parámetro que aparece con frecuencia cuando se habla de LTE, es el Radio Network Temporary Identifier (RNTI)[1], y como su propio nombre indica, se utiliza principalmente para identificar un canal radio específico. Además, también se usa para diferenciar a un usuario de otro. Hay diferentes tipos que se especifican en la Tabla 2.2, cada RNTI se trasmite en unos canales concretos que se pueden ver en la Tabla 2.3.

Este parámetro se usará posteriormente para realizar el análisis de uso de redes comerciales LTE.

Tabla 2.2: Valores de RNTI

Valor (Hexadecimal)	**RNTI**	**Uso**
0000	N/A	
0001-003C	RA-RNTI	RAR (apéndice I)
003D-FFF3	C-RNTI	Transmisión
FFF4-FFF9	Reservado	
FFFA	SC-N-RNTI	Notificación SC-MCCH
FFFB	SC-RNTI	Información de control SC-PTM
FFFC	CC-RNTI	Información de control PDCCH
FFFD	M-RNTI	Notificación MCCH
FFFE	P-RNTI	Notificación de sistema
FFFF	SI-RNTI	Emisión de información del sistema

Tabla 2.3: Canales de RNTI

RNTI	**Canal de Transporte**	**Canal lógico**
RA-RNTI	DL-SCH	N/A
C-RNTI	DL-SCH, UL-SCH	DCCH, DTCH, CCCH
SC-N-RNTI	N/A	N/A
SC-RNTI	DL-SCH	SC-MCCH
CC-RNTI	N/A	N/A
M-RNTI	N/A	N/A
P-RNTI	PCH	PCCH
SI-RNTI	DL-SCH	BCCH

2.6. Categoría de los usuarios

La información de categoría se usa para permitir que la eNB se comunique apropiadamente con todos los UEs conectados a ella. Dicha categoría define una capacidad combinada de enlace ascendente y enlace descendente por TTI como se especifica en 3GPP TS36.306. Al transmitir la información de la categoría a la estación base, esta es capaz de determinar el rendimiento del UE y comunicarse con él en consecuencia. Por lo tanto, la eNB no se comunicará más allá del rendimiento potencial del UE.

Tabla 2.4: Categorias de UE

Cat.	TB (DL-SCH)	TB (UL-SCH)	Cat.	TB (DL-SCH)	TB (UL-SCH)
1	10296	5160	12	603008	102048
2	51024	25456	13	391632	150752
3	102048	51024	14	3916560	9585664
4	150752	51024	15	798800	226128
5	299552	75376	16	1051360	105528
6	301504	51024	17	25065984	2119360
7	301504	102048	18	1206016	211056
8	2998560	1497760	19	1658272	13563904
9	452256	51024	20	2019360	316584
10	452256	102048	21	1413120	301504
11	603008	51024			

Una manera más práctica de ver la Tabla 2.4 es comparar cada categoría en función del tráfico o "throughput" que permite alcanzar. Aunque la Figura 2.11 muestre su máximo en 1,5 Gbps hay ciertas categorias que lo superan. Como curiosidad señalar que la categoría 0, la cual tiene una velocidad muy baja, es usada para dispositivos pertenecientes a Internet of Things (IoT). El factor más importante de estos es el consumo de energía.

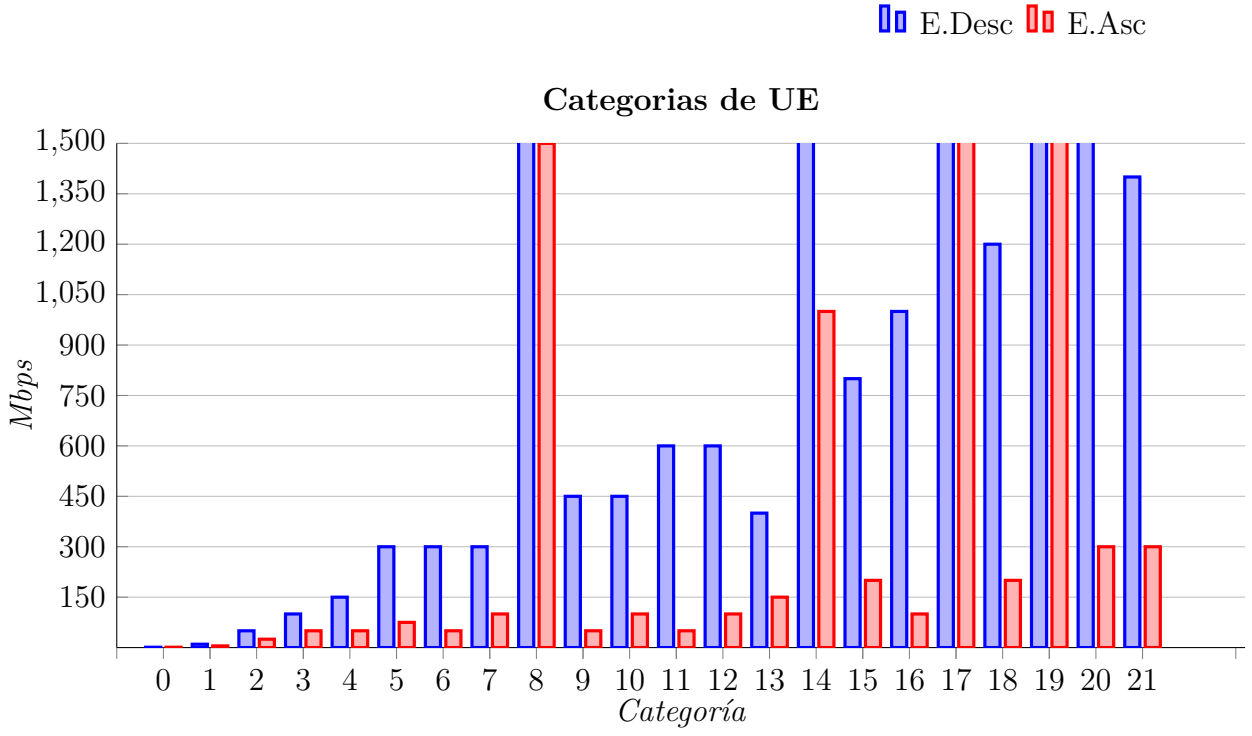


Figura 2.11: *Throughput* de cada categoría de UE

Capítulo 3

Soluciones SDR existentes

En este capítulo se ha realizado un estudio de las principales soluciones SDR abiertas existentes. El objetivo es comparar cada una de las soluciones encontradas, analizando las ventajas que se pueden obtener para el desarrollo e implementación de este trabajo. Todo ello sin perder el punto de vista didáctico, ya que es el fin a conseguir.

3.1. OpenAirInterface

La solución OpenAirInterface (OAI)[4] es una implementación de software completa de sistemas celulares móviles de cuarta generación que cumplen con los estándares 3GPP en el *lenguaje C* bajo LINUX para una arquitectura x86. En la capa física se pueden ver varias características relevante:

- Dispone de compatibilidad en todos los canales, tanto para el enlace descendente como para el ascendente.
- Soporta HARQ.
- Cuenta con un procesamiento de banda base altamente optimizado, incluido el decodificador turbo.
- Es compatible con la versión 8.6 de LTE.
- Permite configuraciones Frequency Division Duplex (FDD) y Time Division Duplex (TDD) en un cierto rango de ancho de banda: 5, 10 y 20 MHz.
- Además, tiene dos capacidades de trasmisión: Entrada Unica - Salida Unica (SISO) y MIMO.

Esta herramienta dota de inteligencia a la red de acceso, E-UTRAN. Tiene la capacidad de implementar las capas MAC, RLC, PDCP y RRC, además da un valor añadido a la capa MAC, ya que tiene un gestor de recursos radio basado en prioridades con selección dinámica de Esquemas de Modulación y Codificación (MCS). Todas estas capas de protocolos son reconfigurables, lo que hace que esta herramienta pueda ser atractiva desde el punto de vista de la investigación. Otro aspecto resañable es la verificación de integridad y encriptación usando algoritmos como Advanced Encryption Standard (AES). Por último, muestra interfaces en la capa S1AP y GTP-U.

OAI se puede utilizar en el contexto de un entorno de desarrollo de software como LINUX y da un sinfín de capacidades que se enumeran a continuación: herramientas de control y monitoreo, analizador de mensaje y tiempo, sistema de registro de bajo nivel, generador de tráfico. También proporciona herramientas para la validación de protocolos, evaluación del rendimiento y prueba del sistema previo al despliegue.

Para posteriores pruebas del desarrollo se dan varios dispositivos móviles comerciales que la herramienta ha verificado: Huawei E392, E398u-1, Bandrich 500, así como con prototipos comerciales EPC de terceros. La plataforma OAI se puede usar en varias configuraciones diferentes que involucran componentes comerciales en diversos grados:

- OAI UE ↔ OAI eNB + OAI EPC
- OAI UE ↔ OAI eNB + EPC comercial
- OAI UE ↔ eNB comercial + OAI EPC
- OAI UE ↔ eNB comercial + EPC comercial
- UE comercial ↔ eNB comercial + OAI EPC
- UE comercial ↔ OAI eNB + EPC comercial
- UE comercial ↔ OAI eNB + OAI EPC

3.2. Solución srsLTE

La solución srsLTE[3] es una plataforma de código abierto para la experimentación LTE diseñada para la máxima modularidad y la reutilización de código desarrollado por Software Radio Rystems (www.softwareradiosystems.com) (SRS). Entre sus características destaca que extiende el código base para permitir transmisiones LTE en las bandas sin licencia. Además, muestra cómo diferentes mecanismos específicos pueden afectar a la coexistencia. El código de esta biblioteca está escrito en *lenguaje C*, así como la solución anteriormente expuesta. En términos de hardware, la librería se ocupa de los búffers en la memoria del sistema, labor muy importante para la correcta sincronización. Actualmente proporciona interfaces para el Controlador de Hardware Universal (UHD), dando soporte a la familia de dispositivos Ettus Research™. El objetivo de la biblioteca es proporcionar las herramientas para construir aplicaciones basadas en LTE.

Esta plataforma tiene las siguientes propiedades: es compatible con la versión LTE *Release* 8 y permite una configuración solamente FDD, en un rango amplio de anchos de banda: 1.4, 3, 5, 10 y 20 MHz. Tiene la posibilidad de trasmitir con una antena simple o con dos antenas. Admite todos los canales tanto del enlace ascendente, como descendente. Cuenta con un decodificador turbo altamente optimizado disponible en Intel SSE4.1/AVX (+100 Mbps) y estándar C (+25 Mbps) y con un reloj avanzado para aprovechar el paralelismo de datos e instrucciones. El turbo decodificador, el estimador, el ecualizador de canal, el demodulador y el decodificador de Viterbi se utilizan para las partes más compleja del receptor. Y, por último, cabe destacar que se apoya en *VOLK*, una librería que contiene *kernels* de código SIMD escrito para diferentes arquitecturas, incluyendo una general escrita en *C*. En ejecución, *VOLK* seleccionará el núcleo correcto para obtener el máximo rendimiento.

Otra funcionalidad que da esta plataforma es la implementación del UE cuyo código cubre todas las capas de la pila, desde la capa física hasta la de red, como se observa en la Figura 3.1. Sus características son las siguientes: contiene archivo de configuración de entrada detallado, para un control total de la simulación, por ejemplo se tiene control sobre la frecuencia de portadora de enlace descendente o las opciones de registro. Otra característica es que la capa MAC permite captura paquetes para luego ser analizados, por ejemplo con *Wireshark*, y facilitar la comprensión de los conocimientos teóricos.

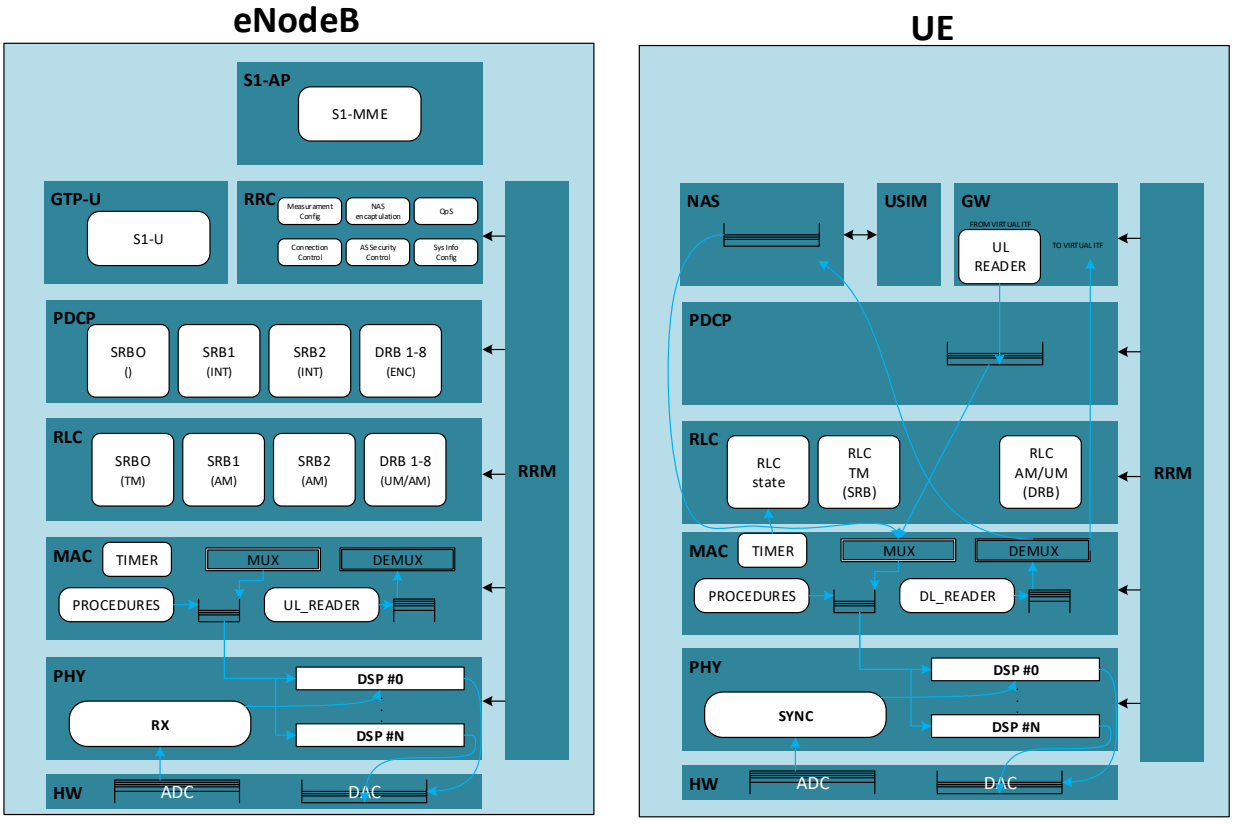


Figura 3.1: Arquitectura de la plataforma srsLTE

A continuación, se explican más en detalle algunos elementos de la Figura 3.1.

- **PHY DSP:** Estos hilos (en azul) realizan todo el procesamiento asociado a una subtrama, incluyendo: demodulación OFDM, búsqueda PDCCH, decodificación PDSCH, codificación PUSCH/PUCCH, generación de señal de enlace ascendente y transmisión al convertidor digital. Una vez finalizado el procesamiento, el hilo vuelve al estado inactivo.
- **PHY SYNC:** Recibe 1 subtrama, realiza la sincronización de tiempo y frecuencia, copia la trama alineada en un hilo *PHY DSP* inactivo y activa su ejecución. (en la parte del UE)
- **MAC PROCEDURES:** Gestiona procedimientos MAC, incluyendo acceso aleatorio, solicitud de programación y HARQ de enlace ascendente/descendente.

- **MAC TIMER:** Proporciona servicios de temporizador a las capas superiores. Todos los temporizadores en LTE tienen una resolución de 1 ms, por lo tanto se implementan con contadores simples sincronizados a la recepción de subtrama en lugar de usar relojes de sistema.
- **MAC DL READER:** Lee los bloques de transporte del enlace descendente desde un búfer, procesa la PDU y empuja el paquete desde la pila hasta el GW.
- **GW UL READER:** Lee desde la interfaz de red virtual y lo almacena en el búfer PDCP.

3.3. Proyecto IMDEA-OWL

El proyecto IMDEA-OWL [2], es un decodificador del canal de control LTE libre y de código abierto desarrollado por IMDEA Networks Institute™ y basado en la solución srsLTE. Las siglas OWL significan Visor Online de LTE y proporciona decodificación a ciegas (ajena a la identidad del terminal) de los mensajes DCI en LTE sobre el canal **PDCCH**. Al igual que srsLTE está escrito completamente en *C*. A continuación, se detallan sus principales características:

- Ofrece un decodificador gráfico que muestra el espectógrafo en línea y los recursos usados de enlace descendente promedio. Además, de la velocidad de datos.
- Obtiene los valores del Cell Radio Network Temporary Identifier (C-RNTI) de PRACH y utiliza la verificación de descodificación a ciegas.
- Mantiene una lista de C-RNTI activos para mayor robustez y velocidad de decodificación.
- Proporciona medios para el análisis de potencia del canal de control (sin decodificación real).

Esta solución también hereda funciones del proyecto srsLTE como cumplir con LTE versión 8, configuración FDD, dos modos de transmisión, antena simple y diversidad de transmisión, procedimiento de búsqueda y sincronización celular para UE, etc.

En lo que se refiere al hardware, la biblioteca actualmente es compatible con el dispositivo UHD de Ettus Research™ y el controlador bladeRF. No hay conversión de frecuencia de muestreo, por lo tanto, el hardware debe admitir un reloj de 30.72 MHz para funcionar correctamente con frecuencias de muestreo LTE y decodificar señales de estaciones base activas.

Por último, dentro de todos los comandos existentes en el proyecto IMDEA-OWL, es conveniente destacar dos que facilitan el uso para un desarrollo de monitorización.

3.3.1. $cell_search -b < *banda* >

Descripción	Escanea eNBs en una banda LTE dada. Se ha modificado para que guarde los parámetros de salida en un archivo.
Parámetros de entrada	**-b** < *banda* > = Número de banda - EARFCN (para limitar la búsqueda)
Parámetros de salida	**1.** Frecuencia **2.** EARFCN en el enlace descendente **3.** Identificador de celda **4.** PRB **5.** SNR **6.** Banda escaneada

3.3.2. $imdea_cc_decoder_rotate -f < *freq* >

Descripción	Este comando ha sido creado basándose en $**./imdea_cc_decoder** para crear ficheros de salida por cada hora, donde el canal de control PDCCH es decodificado.
Parámetros de entrada	**-f** < *freq* > = frecuencia en Hz
Parámetros de salida	**1.** SFN **2.** SFI **3.** RNTI **4.** Dirección **5.** MCS **6.** PRB **7.** Tamaño TB **8.** Tamaño TB (palabra de código 0), -1 si n/a **9.** Tamaño TB (palabra de código 1), -1 si n/a **10.** Tipo de mensaje DCI. Esta versión sólo escanea para 0 (formato 0), 2 (formato 1a), 6 (formato 2a) **11.** Nuevo indicador para la palabra de código 0 **12.** Nuevo indicador para la palabra de código 1 **13.** ID del proceso de HARQ **14.** NCCE ubicación del mensaje DCI **15.** Nivel de agregación del mensaje DCI **16.** CFI **17.** Verificación de la DCI

3.4. Elección de la solución SDR

Se ha decidido basar este proyecto en la solución srsLTE debido a que cuenta con una gran comunidad de usuarios y una programación clara y estructurada, lo que resulta más sencillo de modificar respecto a la solución OAI. Además, está solución permite implementar tanto la parte eNB, como UE, probado y verificado contra redes comerciales LTE en España mediante Telefónica.

Para la parte de monitorización se ha decidido elegir la solución IMDEA-OWL debido a que su implementación se puede realizar a un bajo coste, pues no requiere de altos cálculos de computación. Añadir su gran fiabilidad, cuentan con un índice de decodificación exitoso del 85 %.

Capítulo 4

Resultados

Una vez seleccionada la herramienta que se va a utilizar, en este capítulo se presentan los resultados de monitorización de redes comerciales que se han obtenido.

Para la realización de este trabajo se ha utilizado un ordenador con un microprocesador i7 quad-core, 8Gb de RAM y el sistema operativo Ubuntu 16.04. Es importante disponer de una conexión USB 3.0 para conectar el modelo hardware USRP B210, ya que se requiere alta velocidad de comunicaciones a fin de mantener la sincronización. Por este motivo, se ha configurado el microprocesador para que opere a la máxima velocidad de manera ininterrumpida, deshabilitando el escalado de frecuencia configurado por defecto, con los comandos mostrados en la Figura 4.1.

```
$ sudo nano /etc/default/cpufrequtils
$ sudo update-rc.d ondemand disable
$ sudo apt-get install
```

Figura 4.1: Máxima potencia de los procesadores

- En primer lugar, se ha optado por una zona suburbana situada en Ceceñas. Es una localidad del municipio de Medio Cudeyo (Cantabria, España). En el año 2011 contaba con una población de 520 habitantes (INE[1]). La localidad se encuentra a 30 metros de altitud sobre el nivel del mar, y a 19,6 kilómetros de Santander.

Tabla 4.1: Caracteristicas Estacion Movil (Fuente:InfoAntenas)

Código	**Banda Asignada (MHz)**	**Banda**
VODAFONE ESPAÑA, S.A.	949.90 - 959.90	8 ↓
	949.90 - 959.90	8 ↓
	842.00 - 852.00	20 ↑
XFERA MÓVILES SA	1845.10 - 1855.10	3 ↓
	1915.00 - 1920.00	33 y 34 ↓
	2110.00 - 2125.00	1 ↓

[1]http://www.ine.es/jaxi/Tabla.htm?path=/t20/e244/avance/p02/l0/&file=1mun00.px&L=0

Código	Banda Asignada (MHz)	Banda
TELEFONICA MOVILES ESPAÑA, S.A.U.	939.70 - 944.70	8 ↓
	852.00 - 862.00	20 ↑
	1910.00 - 1915.00	33 y 34 ↓
	2155.00 - 2170.00	1 ↓
	935.10 - 949.90	8 ↓
ORANGE ESPAGNE, SAU	1900.00 - 1905.00	33 y 34 ↓
	2125.00 - 2140.00	1 ↓
	925.10 - 935.10	8 ↓
	925.10 - 935.10	8 ↓
	1859.90 - 1879.90	3 ↓

Figura 4.2: Emplazamiento Suburbano

- En segundo lugar, se ha optado por una zona urbana situada en Santander. En el año 2016 contaba con 172.656 habitantes. El municipio limita al norte con el mar Cantábrico, al Este con la bahía de mismo nombre, que lo rodea también por el sur junto al municipio de Camargo. Al oeste limita con el municipio de Santa Cruz de Bezana.

El siguiente paso ha sido definir dos emplazamientos con características diferentes para un estudio más completo. En el caso del núcleo suburbano se ha realizado una estimación para saber cuál es la estación base que se está monitorizando debido a que, en principio, según la información consultada en InfoAntenas [2] es la estación base más próxima. La Tabla 4.1 muestra las bandas disponibles para establecer una conexión y en la Figura 4.2 se muestra un mapa de la localización de la estación base y desde donde se realiza la monitorización.

Se decidió que el tiempo de monitorización en ambos lugares seria de una semana, con el fin de poder analizar tanto lo que ocurre en días laborables como en fines de semana.

Lo primero que se ha de definir es la frecuencia que se monitoriza en cada emplazamiento. Esto se ha elegido teniendo en consideración ciertos parámetros que se explican más adelante en la clase `OwlSearchCell` (Sección 4.1.1) y queda plasmado en la tabla 4.2.

[2] https://geoportal.minetur.gob.es/VCTEL/vcne.do

Zona	Frecuencia (MHz)	Num. Recursos
Suburbana	806	50
Urbana	796	50

Tabla 4.2: Frequencia monitorizada del emplazamiento

A lo largo de este capítulo se detalla, en primer lugar, la estructura del código desarrollado para automatizar el proceso de recogida y tratamiento de datos. A continuación, se presentan los resultados obtenidos de la monitorización realizada en base a la solución IMDEA-OWL. Y finalmente, se expone el análisis funcional llevado a cabo que permite saber hasta que punto la herramienta srsLTE es apta para desplegar un sistema LTE entero. Este análisis se comentará al final del presente capítulo.

4.1. Estructura del código

A partir de las funcionalidades provistas por la herramienta IMDEA-OWL, se ha acometido un desarrollo en el *lenguaje C++* que permite automatizar la monitorización y la extracción de métricas. Tal como se muestra en la Figura 4.3, a partir de la funcionalidad básica de generación de estadísticas provista por IMDEA-OWL, se han desarrollado clases específicas encargadas de generar cada una de las métricas. A continuación, se detallan las funcionalidades de la herramienta de monitorización resultante.

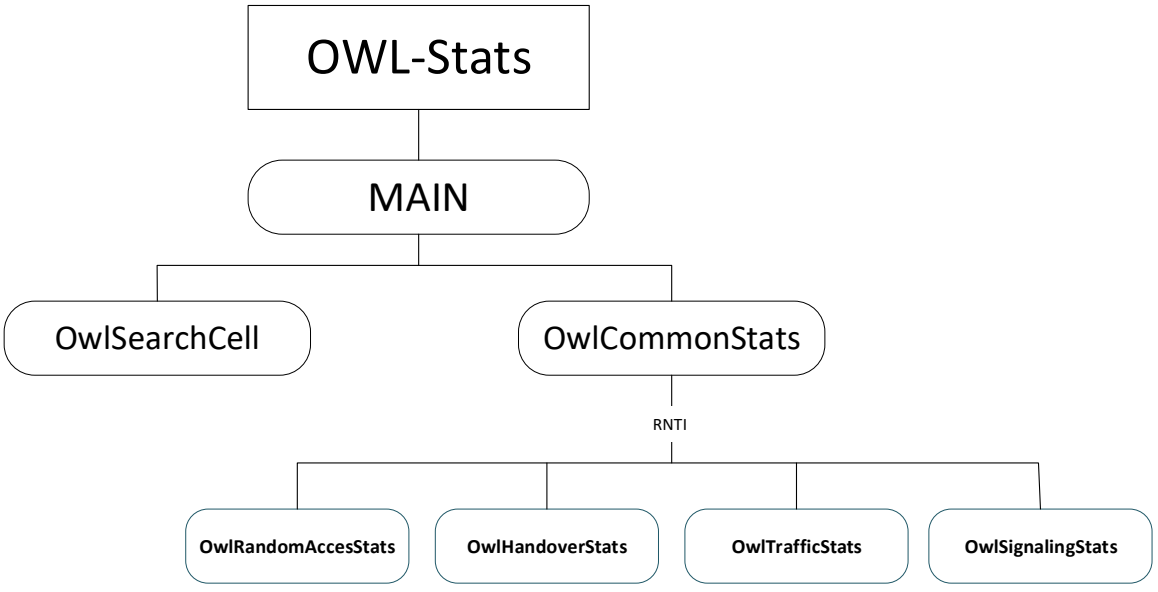


Figura 4.3: Estructura del Proyecto

4.1.1. OwlSearchCell

El principal objetivo de esta clase es analizar el escenario en el que se va a realizar la monitorización, a fin de seleccionar la mejor estación base de la que extraer resultados.

Para ello, se ha creado un archivo ejecutable en *bash*, el cual, hace llamadas al comando perteneciente del proyecto IMDEA-OWL explicado en la Sección 3.4, concretamente a *cell_search*. Como se comentaba en el capítulo anterior, este comando se ha modificado para que, a la vez que muestra por pantalla el resultado, lo escriba en un fichero (`Cell_Found.in`). Cada fila es una nueva celda encontrada en la banda que esta escaneando, y cada columna se rige por los parámetros de salida que indica.

Entrando más en detalle en la clase, está toma como parámetros de entrada el citado fichero (`Cell_Found.in`) y devuelve por un lado un fichero llamado `operators.tr`, con los operadores móviles correspondientes a cada celda encontrada, y, por otro lado, uno llamado `Freq_Found.tr`, con las celdas de las que se recibe mayor potencia encontradas en cada banda, y diferenciada por operador.

Figura 4.4: Estructura del código `OwlSearhCell`

Para conseguir el fichero `operators.tr`, se ha implementado una función basada en la figura 4.6 que se vera más adelante. El gobierno de España es el encargado de administrar el espectro radioeléctrico, en el que cada banda corresponde a un determinado rangos de frecuencias. Dicha entidad licita varios rango de frecuencias, dentro del rango global comentado anteriormente, y cada operador puja por él. Cada línea del fichero `Cell_Found.in` contiene, entre otros parámetros, la banda y la frecuencia central en la que ha sido encontrada cada nueva celda. De esta manera es posible obtener su operador.

Por otro lado para conseguir el fichero `Freq_Found.tr`, primero se ha creado un mapa, "m_sessOper", usando como índice la frecuencia de trabajo, que es única para cada celda. Además, de cada una de las celdas se almacena el ancho de banda que usa, así como el operador al que pertenece. Después, se ha creado un segundo mapa "m_sessCell" que es realmente el de interés. En él, como clave actúa la banda y se almacena el operador asignado y la SNR. A continuación, por cada entrada en "m_sessOper" se comprueba que existe la banda en el mapa "m_sessCell", cuando esto ocurre, se comprueba el operador asignado con el que se tiene en el mapa, así se obtienen las distintas bandas y en cada una de ellas los distintos operadores que se hayan encontrado. Ya solo queda comparar si la SNR de la nueva entrada es mayor que la SNR que se tiene guardada en el mapa, cuando esta premisa se cumple se actualizan los datos con la nueva celda con mejores características.

4.1.2. OwlCommonStats

El cometido de esta clase, es analizar los datos recogidos de ejecutar el comando *imdea_cc_decoder_rotate* que como anteriormente se explica en la Sección 3.4 es una modificación del ejemplo *imdea_cc_decoder* perteneciente al proyecto IMDEA-OWL. Dicho comando genera varios archivos con extensión *.out* y agrupa los datos recogidos cada 24 horas en un único archivo comprimido. Cada columna de dichos archivos equivale a los 17 parámetros de salida indicados en la Sección 3.4. A lo largo del documento, se van a ir explicando algunas

de los parámetros más relevantes, los cuales se han empleado para la caracterización que se ha realizado, y que han sido objeto de este trabajo. En la Figura 4.5, se puede observar el flujo explicado.

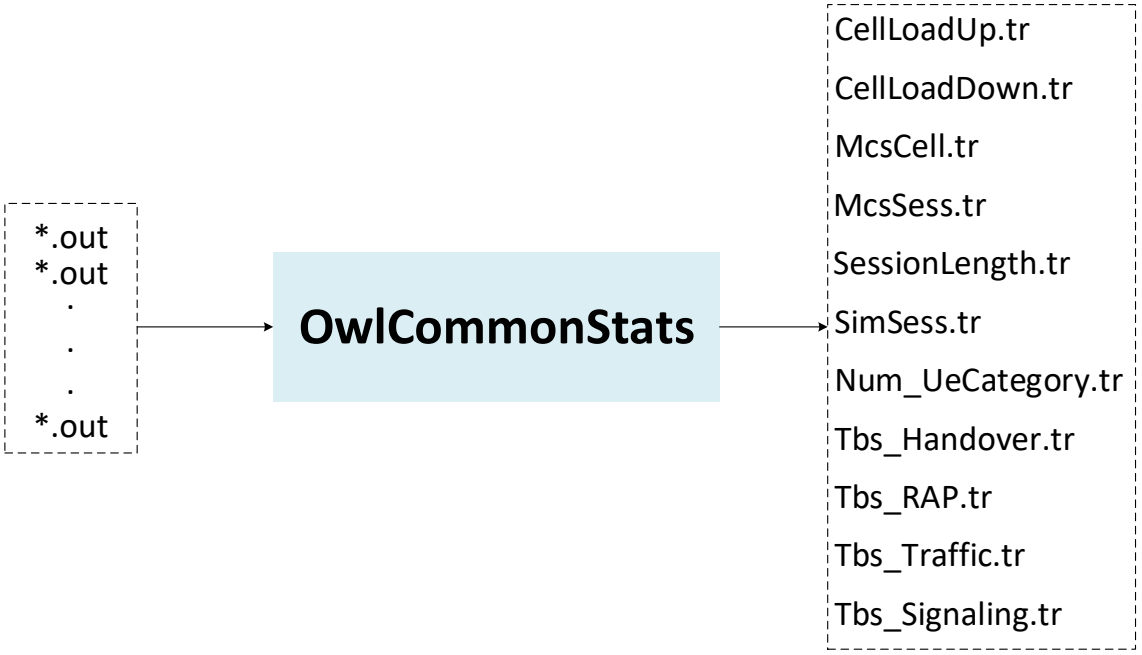


Figura 4.5: Estructura del código `OwlCommonStats`

En primer lugar se detallan los dos primeros parámetros. La columna 1, System Frame Number (SFN), indica el número de trama LTE (cada trama tiene una duración de 10 ms). Este parámetro está comprendido entre 0 y 1023, cuando el número de SFN alcanza el valor máximo (es decir, 1023), regresa a 0. La columna 2, Sub-Frame Index (SFI), es el otro tic-tac del intervalo. Está comprendido entre 0 y 9; cuando el número de subtrama alcanza el valor máximo (es decir, 9), vuelve a 0 y el número de SFN aumenta en 1. Estos dos parámetros son utilizados para calcular el tiempo en cada momento de la monitorización y se basan en la siguiente fórmula:

$$\text{Time (ms)} = SFN * 10 + SFI \tag{4.1}$$

El tercer parámetro que se ha utilizado es el RNTI, introducido previamente el el Capítulo 2. Este valor se usa como filtro para diferenciar entre tipos de tráfico cursados en la estación base. En resumen, los valores bajos de RNTI están reservados a procedimientos de acceso, los valores medios a tráfico de dato, y, finalmente, los valores más altos se usan para indicar tráfico de señalización. En la Tabla 4.3 se indica qué rangos de valores de RNTI son usados por cada una de las clases que generan estadísticas de uso.

Tabla 4.3: Valores RNTI por clases

Clase	Valor RNTI
OwlRandomAccesStats	1 - 10
OwlHandoverStats:	11 - 60
OwlTrafficStats:	61 - 65524
OwlSignalingStats:	65530 - 65535

- **OwlRandomAccesStats:** Esta clase, acumula el tráfico cuando se trata de un acceso antes de realizar la asignación de usuario, de acuerdo a los valores de RNTI indicados en la Tabla 4.3.
- **OwlHandoverStats:** Acumula el tráfico cuando se trata de un traspaso de usuario entre estaciones base.
- **OwlTrafficStats:** Esta clase, acumula el tráfico cuando se trata de un usuario ya establecido.

  Cabe destacar que, dado que el rango de valores de RNTI es finito, estos se pueden repetir para diferentes usuarios. A fin de diferenciar entre usuarios, se ha estimado que usar el rango entero de valores de RNTI de tráfico de datos requiere más de 10 segundos. De este modo, si un valor de RNTI no se utiliza durante más de 10 segundos, se asume que una nueva sesión se ha iniciado en su siguiente uso.

  Además, esta clase lleva a cabo otras funciones como, sesiones simultáneas, promedio de tráfico y MCS por sesión y una estimación de las categorias de los usuarios.
- **OwlSignalingStats:** Por último, esta clase acumula la información relativa a la señalización entre la estación base y los usuarios.

Finalmente, también se ha usado la información proporcionada por las trazas de IMDEA-OWL que indica el sentido del tráfico. Este valor permite separar las métricas para un mejor tratamiento y compresión de los datos. El valor que se obtiene es un un “0” cuando la dirección es en el enlace ascendente, UE $\Longrightarrow$ eNB, y “1” cuando se refiera al enlace descendente, es decir UE $\Longleftarrow$ eNB.

4.2. Monitorización

En esta sección se va a comentar cada uno de los análisis llevados a cabo.

4.2.1. Operadores en España

Antes de obtener los resultados propios del canal de control, se analizó la presencia de los diferentes operadores de telefonía en la región, así como las tecnologías que se despliegan en cada banda, tal como se indica en la Figura 4.6, las frecuencias de telefonía móvil o bandas de telefonía móvil utilizadas en España a día de hoy son las siguientes:

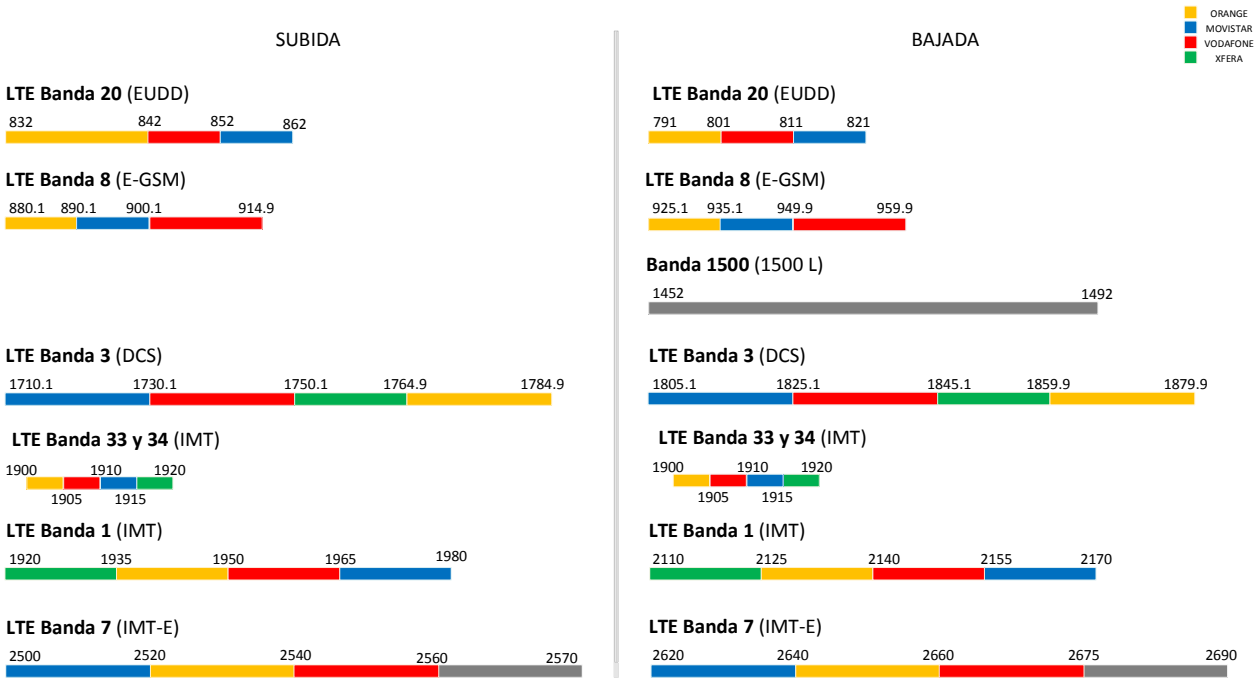


Figura 4.6: Servicio de Comunicaciones Electrónicas por bandas en España (Fuente: Registro Público de concesiones - Gobierno de España)

- **Banda 20:** es conocida como dividendo digital y hasta el 31 de marzo de 2015 se utilizó para servicios de radiodifusión de televisión. Una vez se trasladaron los canales de la TDT a frecuencias más bajas, se utiliza para telefonía de cuarta generación LTE.
- **Banda 8:** se utiliza por la telefonía móvil GSM desde sus inicios, desde septiembre de 2011 también se utiliza para ofrecer 3G por sus buenas cualidades de propagación.
- **Banda 1500:** las frecuencias que hasta mayo de 2015 estaban destinadas a la radiodifusión Digital Audio Broadcasting (DAB), pasarán a manos de las operadoras de telecomunicaciones como complemento para dar servicios 4G, de hasta 500 Mbps, únicamente en sentido descendente (DL). Paises como Alemania ya han licitado esta frecuencia, pero lo cierto es que en España no se tienen muchas noticias sobre ello.
- **Banda 3:** fue utilizada inicialmente para tecnología GSM, desde julio de 2013 se utiliza también para telefonía de cuarta generación LTE.
- **Banda 1:** se utiliza para telefonía 3G.
- **Banda 33 y 34:** ocupa las mismas bandas de frecuencia que la banda 1 pero es tecnología TDD.
- **Banda 7:** es utilizada para tecnología móvil de cuarta generación LTE en aquellos lugares donde la banda 3 no es suficiente por estar muy saturada (lugares con gran afluencia de público, por lo general).
- **Banda 38:** ocupan las mismas bandas de frecuencia que la banda 7, pero es usada para las coberturas de operadores autonómicos con tecnología TDD.

- **Banda 42:** se utiliza en accesos a Internet vía WiMAX, especialmente en zonas rurales.

4.2.2. Búsqueda de la celda

En primer lugar se han escaneado cada banda comentada anteriormente donde los operadores españoles legalmente pueden emitir. La Figura 4.7 muestra la presencia de los distintos operadores, calculado como el porcentaje de celdas encontradas en las bandas gestionadas por cada uno de ellos.

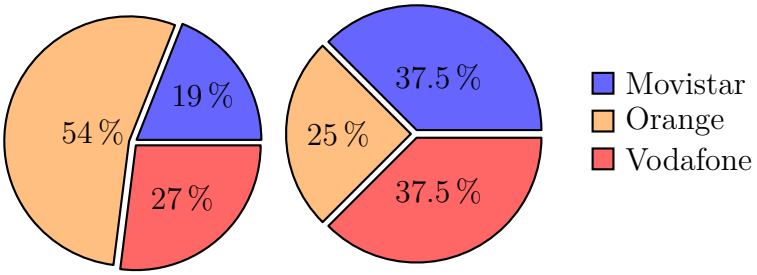


Figura 4.7: Penetración de LTE por operador en función del área de análisis: a la izquierda se muestran los resultados en entorno suburbano, y a la derecha en entorno urbano. Como se puede observar, únicamente se han encontrado celdas pertenecientes a los tres principales operadores en España.

En segundo lugar, se han recogido datos que permiten ver las celdas encontradas y así poder visualizar cuales son más óptimas para llevar a cabo la monitorización. Este primer filtro permite caracterizar las celdas en función del operador, cantidad de recursos que gestionan y valor de Relación Señal/Ruido (SNR) medido desde el punto de monitorización.

Tabla 4.4: Mejores celdas encontradas por Banda y SNR

	Frecuencia	**Id**	**PRB**	**SNR**(dB)	**Banda**	**OPERADOR**
Suburbano						
	816.5	**2**	**6**	**-13.8**	**20**	**MOVISTAR**
	805.7	0	25	-5.4	20	VODAFONE
	805.5	0	25	-15.1	20	VODAFONE
	806	**381**	**50**	**-6**	**20**	**VODAFONE**
	816	**92**	**50**	**-13.8**	**20**	**MOVISTAR**
	805.7	0	75	-10	20	VODAFONE
	1852.4	**1**	**75**	**-20.1**	**3**	**ORANGE**
	1852.5	223	75	-15.8	3	ORANGE
	1869.9	**181**	**100**	**-19.3**	**3**	**ORANGE**
	806.2	0	125	-11.5	20	VODAFONE
	806.6	0	125	-17.7	20	VODAFONE

	Frecuencia	**Id**	**PRB**	**SNR**(dB)	**Banda**	**OPERADOR**
Urbano						
	796	**336**	**50**	**-19.9**	**20**	**ORANGE**
	806	30	50	-11.7	20	VODAFONE
	806	**451**	**50**	**-14.4**	**20**	**VODAFONE**
	1814.8	0	50	-23.3	3	MOVISTAR
	796.2	**411**	**75**	**-24.7**	**20**	**ORANGE**
	805.8	**1**	**75**	**-14.7**	**20**	**VODAFONE**
	1815.1	**279**	**100**	**-21.9**	**3**	**MOVISTAR**
	1815.1	188	100	-19.6	3	MOVISTAR

A la vista de la Tabla 4.4 se ha aplicado la clase `OwlSearchCell` y se ha optado por monitorizar las bandas que se mencionaron anteriormente (Tabla 4.2)

Llama la atención que de todas las bandas disponibles escaneadas solo se encuentran celdas en la banda 20 y, en menor medida, en la banda 3. Esto puede ser debido a que cuanto mayor sea la frecuencia mayor será el coste, por lo que parece ser que la banda 20 es la ideal y la preferida por los operadores. Además, en ningún emplazamiento se han encontrado estaciones base LTE pertenecientes al operador Xfera (Yoigo), que también tiene recursos frecuenciales.

Cabe destacar que al comparar las celdas obtenidas en el emplazamiento suburbano en este estudio con la información pública recogida en la Tabla 4.1, no se han podido corroborar todas las frecuencias. Esto puede ser debido o bien a que la información de la página InfoAntenas (gestionada por el Ministerio de Economía y Empresa) no está actualizada, o a que los operadores no están haciendo uso de todos las bandas.

4.2.3. Carga de las celdas

Retomando la descripción que se comentaba en la Sección 4.1.2 y que tiene que ver con la disección del resultado al ejecutar el comando *imdea_cc_decoder_rotate* explicado en el Capítulo 3. El 6º parámetro de la traza de IMDEA-OWL, como se ha indicado en la Sección 3.3.2, muestra el Número de Recursos Asignados (PRB) en cada momento. Este parámetro está relacionado directamente con el ancho de banda.

Para entender dicho parámetro hay que recordar que las transmisiones de enlace descendente LTE desde la eNB consisten en datos de planos de control y plano de usuario de las capas superiores en la pila de protocolos (como se describe en el capítulo 2, en la sección 2.3) multiplexados con señalización de capa física para soportar la transmisión de datos. La multiplexación de estos datos se hace mediante Orthogonal Frequency Division Multiplexing Access (OFDMA), que permite dividirlos en recursos de tiempo y frecuencia.

Los recursos de transmisión de enlace descendente en LTE poseen dimensiones de tiempo, frecuencia y espacio. La dimensión espacial, medida en “capas”, se accede por medio de múltiples “puertos de antena” en la eNB; para cada puerto de antena, se proporciona una Reference Signal (RS) para permitir que el UE calcule el canal de radio. Por otro lado, los recursos de frecuencia de tiempo para cada puerto de antena de transmisión se subdividen según la siguiente estructura: la unidad de tiempo más grande es la trama de radio de 10 ms, que se subdivide a su vez, en diez subtramas de 1 ms, cada una de las cuales se divide en dos ranuras de 0,5 ms. Cada ranura comprende 7 símbolos OFDM en el caso

de la longitud del Cyclic Prefix (CP) normal. En el dominio de frecuencia, los recursos se agrupan en unidades de 12 subportadoras (ocupando así un total de 180 kHz con un espaciamiento de subportadora de 15 kHz), cada unidad de 12 subportadoras se denomina Recursos Asignados (RB). Por último, la unidad de recurso más pequeña es el Elemento de Recurso (RE), que consiste en una subportadora para una duración de un símbolo OFDM.

A continuación, la figura 4.8 detalla visualmente la estructura de recursos para la longitud del CP normal.

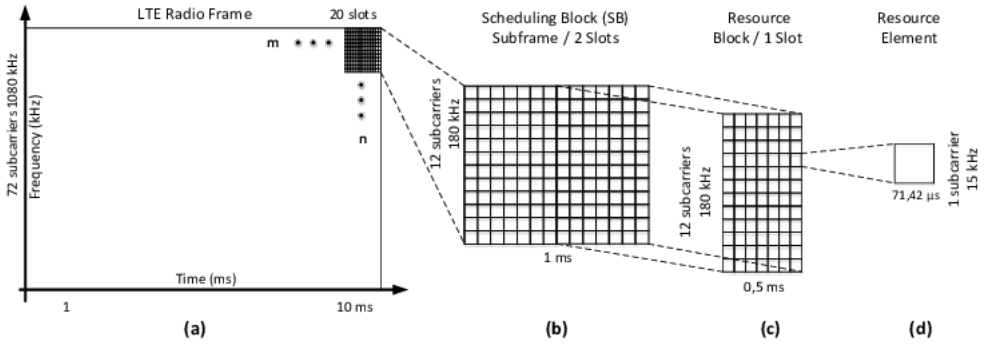


Figura 4.8: Resumen de tiempo/frecuencia de la estructura de recursos LTE (ref: QoS aware schedulers for multi-users on OFDMA downlink: Optimal and heuristic - Scientific Figure on ResearchGate)

Como se menciona anteriormente, por cada recurso asignado se establecen 12 subportadoras, cada una de ellas equivale a 15 KHz, en total 180 KHz. Si en este caso se tienen 50, el ancho de banda es aproximadamente de 10 MHz. Siguiendo este proceso para cada número de recursos posible se obtiene sus anchos de banda, tal como se muestra en la Tabla 4.5.

Por otro lado, a partir de las 12 subportadoras y los 7 símbolos por cada una se tiene en total 84 recursos disponibles en donde ubicar los símbolos de la modulación. Suponiendo que utilizamos la modulación de mayor eficiencia espectral, es decir 64 QAM, que transmite 6 bits/símbolo, se puede llegar a trasmitir hasta 504 bits en un PRB cada 0.5 ms, incluyendo datos codificados de usuario (equivalen un 75 %) y canales de control y señalización propia de la capa física del sistema (equivalen el 25 % restante). Esto proporciona una velocidad bruta de transmisión de pico de aproximadamente 1 Mbps (504bits/0.5 ms) considerando un sistema sin multiplexado espacial (SISO), ya que utilizando un sistema MIMO se multiplicaría dicha velocidad. A modo de resumen, la Tabla 4.5 muestra la capacidad bruta de transmisión para diferentes anchos de banda.

Tabla 4.5: Relación entre PRB, ancho de banda y velocidad pico

Nº RB	6	15	25	50	75	100
BW (MHz)	1.4	3	5	10	15	20
Vpico Datos Usuario (Mbps) SISO	4.5	11.25	18.75	37.5	56.25	75
Vpico Datos Usuario (Mbps) MIMO	18	45	75	150	225	300

En primer lugar se ha calculado la distribución de los recursos asignados en cada estación base a los largo de los periodos de monitorización, tal como se muestra en las Figura 4.9 y 4.10

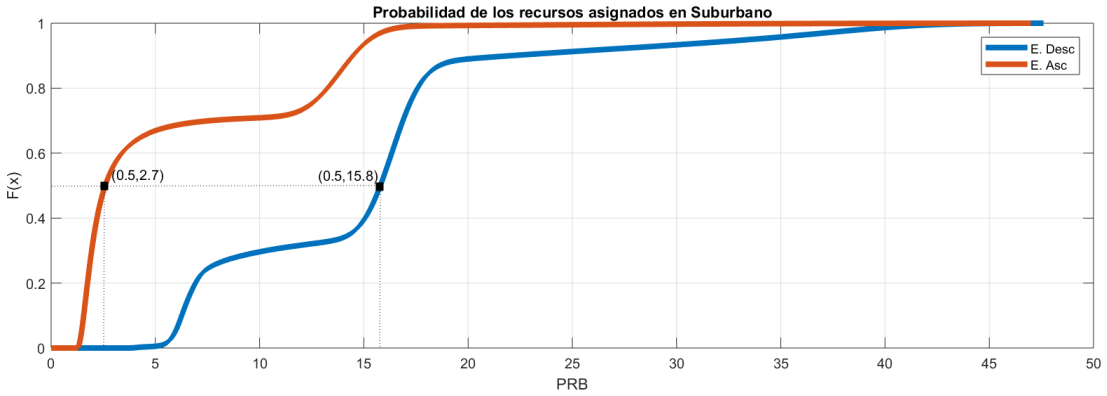


Figura 4.9: CDF de la cantidad de recursos asignados en la celda suburbana

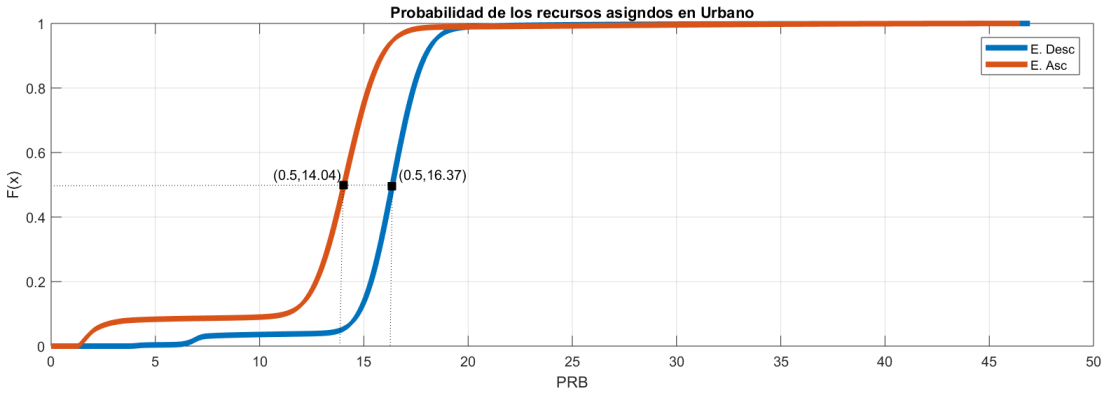


Figura 4.10: CDF de la cantidad de recursos asignados en la celda urbana

Como se observa, el número de recursos asignados se distribuyen con más probabilidad en sus valores más bajos incluso por debajo de la media de su rango. Otro resultado que aparece, es que siempre esta más cargado el enlace descendente como cabe esperar ya que el peso del tráfico se sitúa en el envió de la estación base hacia el usuario. Finalmente, si comparamos las Figuras 4.9 y 4.10, podemos observar que la forma de las distribuciones es muy diferente en los entornos urbano y suburbano. En concreto, la carga de tráfico en el enlace ascendente es notablemente mayor en el urbano.

A continuación, la Figura 4.11 muestra la carga media bruta para ambos enlaces ascendente y descendente, así como el valor medio, para cada una de las celdas seleccionadas y para diferentes días de la semana.

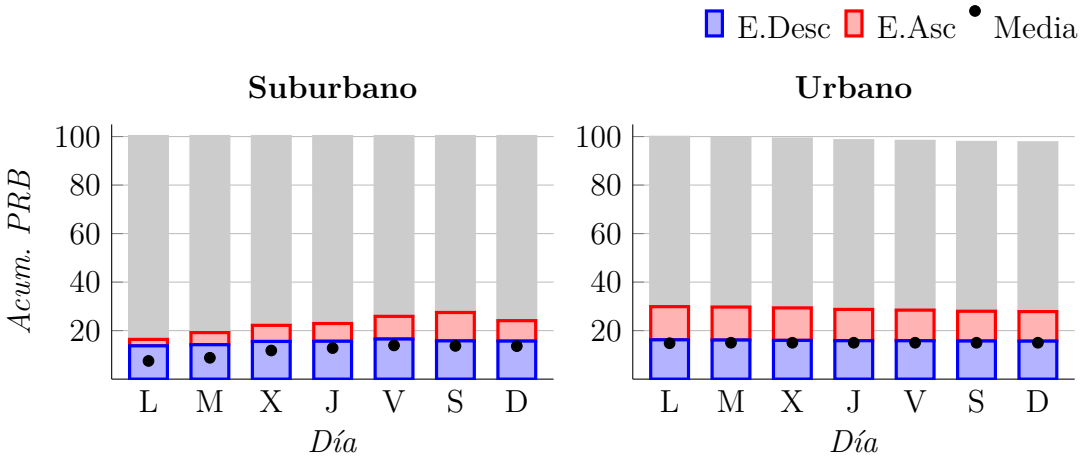


Figura 4.11: Nivel medio de carga de los recursos asignados en el tiempo

La máxima carga en la celda, teniendo en cuenta el enlace ascendente y descendente, es de 100 PRBs en este caso, pero como se observa en la Figura 4.11, la carga media total en la celda esta por debajo de la mitad disponible, lo que refleja una infrautilización de los recursos.

Otro aspecto que se hace evidente es que la carga se reparte de manera diferente en los dos emplazamientos, siendo en el núcleo suburbano más dominante el enlace descendente y estando prácticamente igualado en el núcleo urbano.

4.2.4. Eficiencia de las comunicaciones

En esta sección se analiza el nivel de eficiencia de los recursos utilizados estudiando el nivel de Esquemas de Modulación y Codificación (MCS) asignado por las celdas. MCS, indica el tipo de modulación y velocidad de codificación, su rango está comprendido entre 0 y 31, tal como se muestra en la Tabla 4.6. En la práctica se comienza utilizando un valor de MCS bajo para permitir un margen de desvanecimiento adecuado en el enlace, dicho valor alcanzable depende de un gran número de variables que se describen a continuación:

- **Flujos espaciales**: se utiliza una técnica llamada Multiplexación por División Espacial (SDM) para las transmisiones inalámbricas que permite conseguir varios flujos de información sobre el mismo rango de frecuencias.
- **Modulación**: es el proceso por el cual generamos una señal que se adapta al medio de transmisión. La modulación más básica es la Binary Phase Shift Keying (BPSK) y la más avanzada es la 64-Quadrature Amplitude Modulation (QAM).
- **Tasa de codificación**: se suele especificar con dos cifras. La primera indica el número de bits de información por símbolo (unidad mínima de señal modulada que contiene información) y la segunda indica el número total de bits enviados en un símbolo. Estos bits extra del segundo parámetro son bits de redundancia para la detección de errores.

Tabla 4.6: Lista de valores del indice MCS

MCS	Spatial streams	MCS	Spatial streams	Modulación
0	1	16	3	BPSK
1	1	17	3	QPSK
2	1	18	3	QPSK
3	1	19	3	16-QAM
4	1	20	3	16-QAM
5	1	21	3	64-QAM
6	1	22	3	64-QAM
7	1	23	3	64-QAM
8	2	24	4	BPSK
9	2	25	4	QPSK
10	2	26	4	QPSK
11	2	27	4	16-QAM
12	2	28	4	16-QAM
13	2	29	4	64-QAM
14	2	30	4	64-QAM
15	2	31	4	64-QAM

A continuación en las Figuras 4.12 y 4.13, se muestran las distribuciones de los MCS a lo largo de los siete días de la monitorización, tanto en los dos emplazamientos como en los dos enlaces.

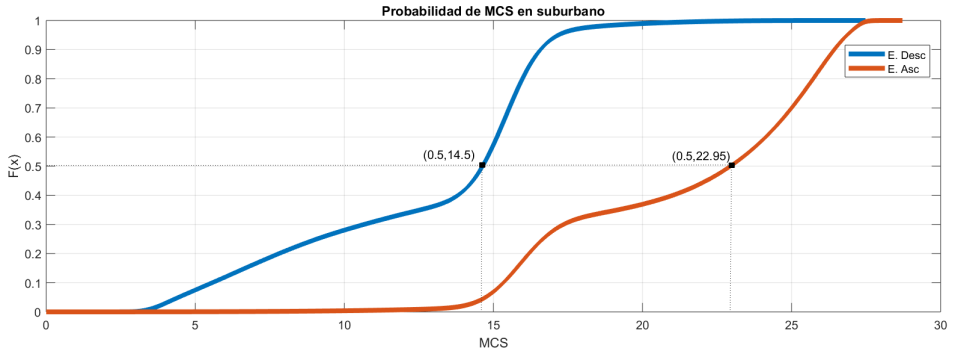


Figura 4.12: CDF del valor de MCS en la celda suburbana

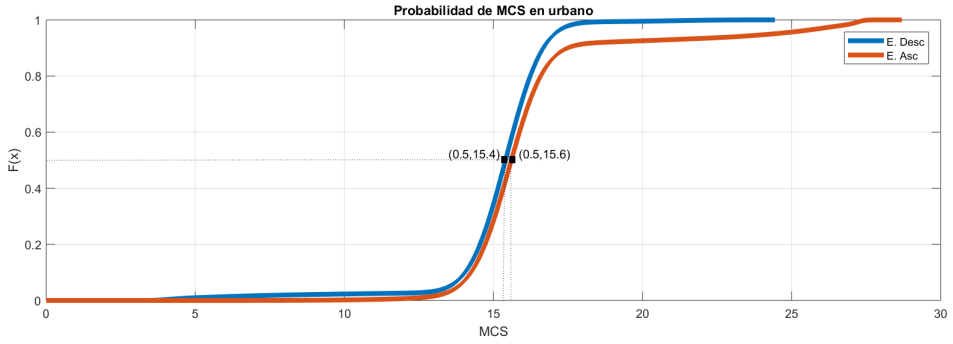


Figura 4.13: CDF del valor de MCS en la celda urbana

Lo primero que llama la atención es que en la monitorización llevada a cabo en el núcleo urbano sigue una distribución normal o gaussiana tanto en el enlace descendente como en el enlace ascendente e indica que se usan valores de MCS altos, aproximadamente a partir del índice 16. Si esto se compara con la Tabla 4.6 se puede deducir que para este emplazamiento en casi su totalidad se esta usando un sistema MIMO.

Por el contrario, los resultados obtenidos en la zona suburbana reflejan que los enlaces no se distribuyen de la misma manera. En el caso del enlace ascendente se usan indices elevados, lo que puede ser debido a que la estación base pretende preservar la batería de los usuarios y que el envió de datos sea lo más corto posible en el tiempo. Por otro lado, el enlace descendente usa indices de MCS más bajo, lo que puede ser consecuencia de la baja carga de las celdas. En este caso, dado que hay recursos suficientes, el operador puede dar prioridad a la robustez de la comunicación aún a expensas de un mayor uso de recursos.

Un análisis de mayor alcance, involucrando más puntos de medida, permitiría corroborar estas hipótesis.

4.2.5. Análisis de tráfico

Tras analizar el uso que se hace de los recursos, se ha estudiado el tráfico gestionado por la celda. Esto se ha llevado a cabo analizando el parámetro Bloque de Transporte en Bits (TB) proporcionado por las trazas de IMDEA-OWL. Desde el punto de vista teórico los TBs depende de dos parámetros explicados en las anteriores secciones, MCS (Sección 4.2.4) y PRB (Sección 4.2.3).

La solución IMDEA-OWL proporciona el tamaño del bloque de transporte real en bits/ms. El esquema de monitorización implementado se encarga de agregar esta información, de forma que se obtienen valores medios por segundo. Las cuatro clases comentadas en la Sección 4.1.2 tienen esta función en común. Finalmente, el resultado obtenido es el *througput* de cada situación que se observa en las figuras que se recogen a continuación.

Tráfico Procedimiento de Acceso Aleatorio (RAP)

En primer lugar se muestra la propuesta de tráfico referente al proceso de acceso aleatorio, es decir, se monitoriza las peticiones y el intercambio de datos que ocurre antes de establecer la conexión entre el UE y la eNB, esto se conoce como RAP y se realiza en un proceso basado en contienda.

En este procedimiento, el UE selecciona aleatoriamente una firma de preámbulo de acceso aleatorio, que puede dar como resultado que más de un UE transmita simultáneamente la misma firma, lo que conduce a la necesidad de realizar un proceso de resolución.

Consiste en 4 pasos como podemos ver en la figura 4.14:

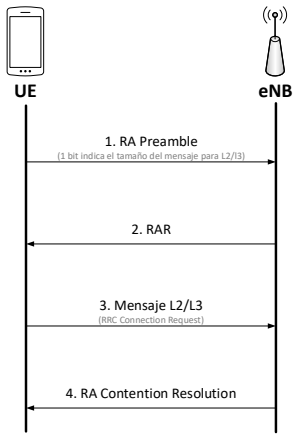


Figura 4.14: Proceso de acceso a contienda del RAP

1. **Transmisión del preámbulo**:

   El UE selecciona una de las firmas $64 - N_{cf}$ disponible en el PRACH, donde N_{cf} es el número de firmas reservadas por la eNB para otro tipo de procedimientos de acceso.

   Su valor se deriva de la ecuación 4.2 donde t_{id} es el índice de la primera subtrama $(0 \leq t_{id} < 10)$, y f_{id} es el índice dentro de esa subtrama $(0 \leq f_{id} < 6)$.

   $$\text{RA-RNTI} = 1 + t_{id} + 10 * f_{id} \tag{4.2}$$

   Para el caso de FDD, f_{id} toma el valor de 0. Por consiguiente:

   $$\text{RA-RNTI} = 1 + t_{id} \tag{4.3}$$

   De lo que se obtiene que el rango de RA-RNTI para nuevos accesos va de 1 a 10, en valor decimal, comprendido entre el rango teórico que se observaba en la Tabla 2.2.

2. **Respuesta de acceso aleatorio**:

   La Respuesta de Acceso Aleatorio (RAR) es enviada por la eNB en el PDSCH, y dirigida con el Random Access Radio Network Temporary Identifier (RA-RNTI), que identifica la ranura de tiempo-frecuencia en la que la petición fue detectada.

   El RAR transmite los siguientes parámetro:

   - La identidad del preámbulo detectado.
   - Una instrucción de alineación de temporización para sincronizar transmisiones de enlace ascendente posteriores.
   - Una concesión de recursos de enlace ascendente inicial para la transmisión del mensaje del paso 3 y una asignación de un C-RNTI (que puede o no ser permanente como resultado de la resolución de disputas).

   El mensaje RAR también puede incluir un indicador de espera que la eNB puede configurar para ordenar al UE que espere durante un período de tiempo antes de reintentar el acceso aleatorio.

El UE espera recibir el RAR dentro de una ventana de tiempo, cuyo inicio y fin también son configurados por la eNB. El proceso que se sigue se puede ver en la Figura 4.15, donde G es el mensaje de asignación de recursos de transmisión del enlace descendente en el PDCCH.

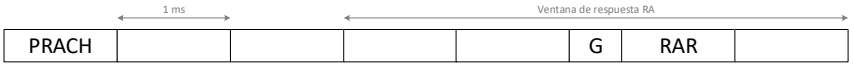


Figura 4.15: Tiempo de la respuesta de la ventana RAR

Si el UE no recibe un RAR dentro de la ventana de tiempo configurada, selecciona una nueva firma y transmite de nuevo. El tiempo des espera mínimo para un nuevo intento es de 3 ms.

Si el UE recibe el RAR pero no puede decodificarlo satisfactoriamente el mensaje, el retardo mínimo aumenta a 4 ms.

3. **Mensaje de Capa 2/Capa 3**:

   Este mensaje es la primera transmisión de enlace ascendente programada en PUSCH y utiliza HARQ. Se transmite el mensaje de procedimiento de acceso aleatorio ya sea: como una solicitud de conexión RRC, como una actualización del área de seguimiento o como una solicitud de programación.

   Este mensaje va dirigido al RA-RNTI y transporta el C-RNTI. En caso de que se haya producido una colisión de preámbulo en el paso 1, los UEs colisionantes recibirán el mismo RA-RNTI y colisionarán también cuando transmitan sus mensajes en este paso, dando como resultado que no se pueda decodificar. Por consiguiente, los UEs reiniciarán el procedimiento de acceso aleatorio después de alcanzar el número máximo de retransmisiones HARQ. Por otra parte, si el mensajes desde un UE se decodifica con éxito, el proceso permanece sin resolver para los otros UEs.

   El siguiente mensaje de enlace descendente (en el Paso 4) permite una resolución rápida de este caso.

4. **Mensaje de resolución**:

   Este mensaje se dirige al C-RNTI (si se indica en el mensaje Capa 2/Capa 3) o al RA-RNTI y, en este último caso, hace eco de la identidad UE asignada en el mensaje Capa 2/Capa 3.

   En caso de una colisión seguida de una decodificación exitosa del mensaje Capa 2/Capa 3, la realimentación HARQ se transmite solo por el UE que detecta su C-RNTI, mientras que otros UEs comprenden que hubo una colisión y pueden salir rápidamente del procedimiento de acceso aleatorio actual para comenzar otro.

   El comportamiento del UE al recibir el mensaje de resolución tiene tres maneras diferentes:

   - El UE decodifica correctamente el mensaje y detecta su C-RNTI: devuelve un acuse de recibo positivo, Reconocimiento (ACK).

- El UE decodifica correctamente el mensaje y descubre que contiene la C-RNTI de otro UE: no envía nada.
- El UE no decodifica el mensaje o pierde la concesión Enlace Descendente (DL): no envía nada.

En el anexo I se puede ver un ejemplo del proceso explicado (Figuras 5.1, 5.2 y 5.3). Teniendo en cuenta la definición del proceso de RAP, se ha estimado la cantidad de tráfico enviado en dicho proceso. En este sentido, la Figura 4.16 muestra el *throughput* medio de este tipo de tráfico en cada una de las celdas, y para diferentes días de la semana.

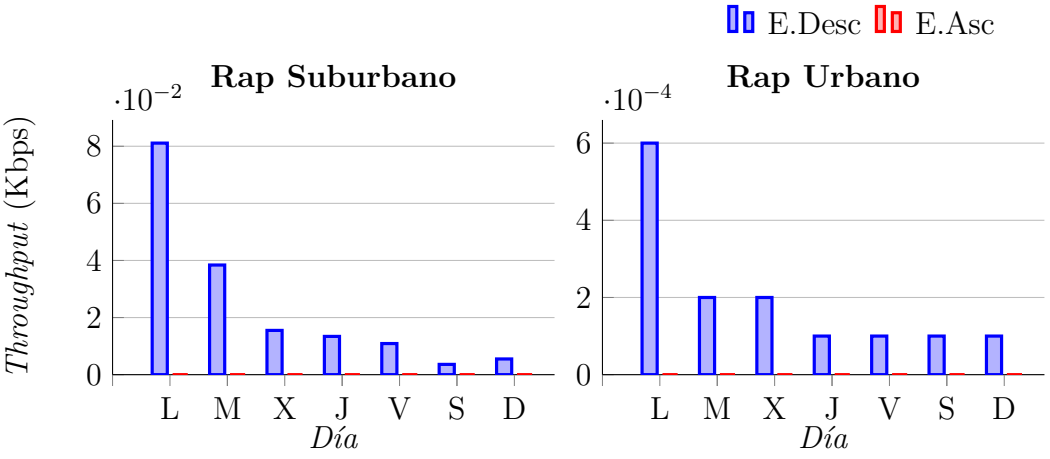


Figura 4.16: Línea de tiempo de los RAP

Como es lógico esperar, el tráfico en el enlace ascendente por el canal PDCCH que se está monitorizando es nulo. Centrándonos en el resultado para la zona suburbana, se detecta que los accesos van descendiendo con el paso del tiempo. Esto podría ser debido a que en entornos rurales pueden existir con más frecuencia dispositivos router inalámbrico de LTE, aunque para asegurar esta premisa haría falta una monitorización más duradera en el tiempo. Por el contrario, se observa que en la zona urbana el tráfico debido al RAP se encuentra dos magnitudes por debajo del de la zona suburbana, aunque, como se verá posteriormente, el tráfico de datos es notablemente mayor.

Cabe comentar que en primera instancia se implementó otra función para la clase `Owl-RandomAccesStats` en la que se quería analizar cómo se producía el acceso de nuevos RNTI (RAP) en las celdas, apoyándose en los conceptos teóricos explicados anteriormente. Al llevar a cabo la implementación apareció un problema imposible de solventar, ya que como se ve en la Figura 5.2 del anexo I, las respuesta que la eNB manda al UE van por el canal DL-SCH que no se monitorizan en la solución escogido, por lo que finalmente se desestimo esta estudio.

Tráfico Traspasos

Además del proceso explicado anteriormente, existe otro procedimiento RAP llamado *contention-free*, que permite realizar el estudio de los traspasos entre celdas y usuarios.

La latencia ligeramente impredecible del RAP se puede eludir para algunos casos de uso en los que se requiere baja latencia, como el traspaso y la reanudación del tráfico del enlace

descendente para un UE, asignando una firma dedicada. En este caso, el procedimiento se simplifica como se muestra en la Figura 4.17.

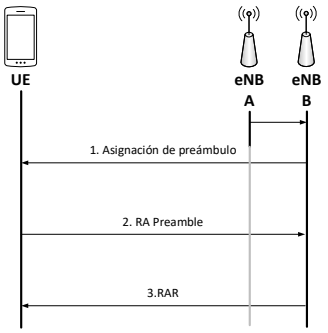


Figura 4.17: Ejemplo de traspaso: *contention-free* (RAP)

El valor de RA-RNTI es el restante del usado para el proceso de acceso a contienda, es decir, su rango para los traspasos comprende desde 11 hasta 60, en valor decimal, tal como se indicó en la Tabla 2.2.

De manera similar al estudio anterior, la Figura 4.18 muestra el *throughput* medio debido a los traspasos en ambos entornos (urbano y suburbano) y para diferentes días de la semana. La premisa al estudiar este tipo de tráfico, como se comentó anteriormente, es que en el emplazamiento urbano las magnitudes sean mayores respecto al emplazamiento suburbano debido a que las celdas puedan estar más cargadas y se produzca un mayor número de traspasos.

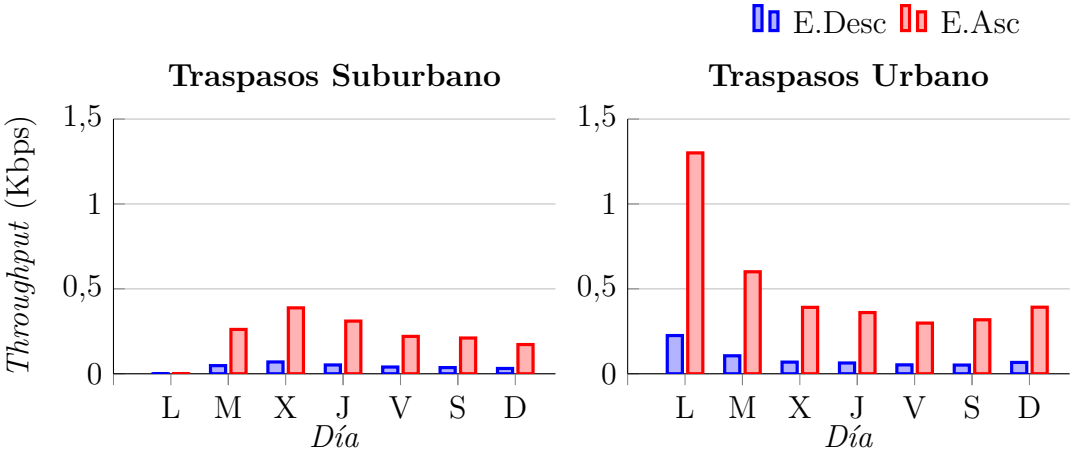


Figura 4.18: Línea de tiempo de los traspasos

Como se puede observar en la Figura 4.18, efectivamente, se comprueba que el tráfico debido a los traspasos es mayor en la celda urbana. Además, otro resultado a esperar, y que también se cumple, es que el enlace ascendente lleve más propuestas de tráfico que el enlace descendente, ya que los traspasos son mayores entre el usuario y la estación base, aunque puede aparecer tráfico entre estaciones bases como se vio en la Figura 2.3.

Tráfico Señalización

En LTE, la baja latencia de señalización proporcionada por la corta duración de subtrama de 1 ms, junto con la ortogonalidad del esquema de acceso múltiple de enlace ascendente que requiere una asignación centralizada de recursos, hace que la eNB deba tener un conocimiento total del estado de los enlaces, tanto ascendente (estimado por la propia estación base) como descendente (indicado por los UEs). Mientras que el tráfico de señalización en el enlace descendente requiere la asignación de recursos concretos a fin de que los UEs puedan decodificar dicha información, en el enlace ascendente no se requiere asignar recursos para señalización, pues la información se incluye en los reconocimientos enviados por los UEs al tráfico de datos. A continuación, la Figura 4.19 muestra el *throughput* medio debido a tráfico de señalización. Como era de esperar, únicamente existe tráfico de este tipo en el enlace descendente.

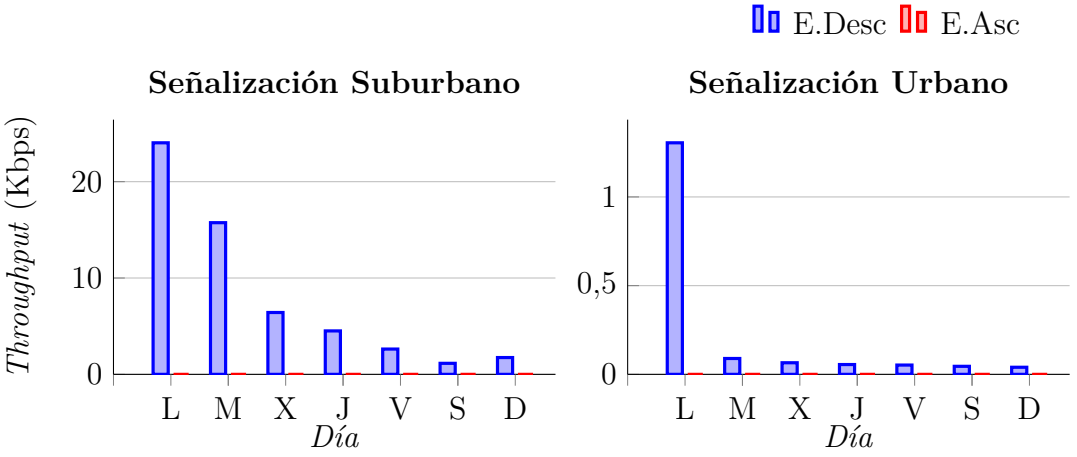


Figura 4.19: Línea de tiempo de la señalización

Llama la atención la gran diferencia en la magnitud de este tipo de tráfico en ambas zonas analizadas. Estos resultados han sido inesperados, ya que se supuso que en entornos urbanos habría más señalización debido a una mayor densidad de usuarios. Se precisaría un análisis más extenso con un mayor número de celdas para poder sacar algún tipo de conclusión.

Tráfico Usuario

Por último, la Figura 4.20 muestra la estimación de tráfico de datos de usuario, tanto en el enlace ascendente como descendente, para ambas celdas y para cada día de la semana.

Como se puede observar, el volumen de datos es mayor en el núcleo urbano, algo que no sorprende ya que se espera que en dicha zona la afluencia de dispositivos sean notablemente mayor. Llegados a este punto llama la atención la manera que tiene de distribuirse la zona urbana, descendiendo a medida que pasa el tiempo de monitorización. Esto lleva a realizar un nuevo análisis de los datos que se comentara más adelante.

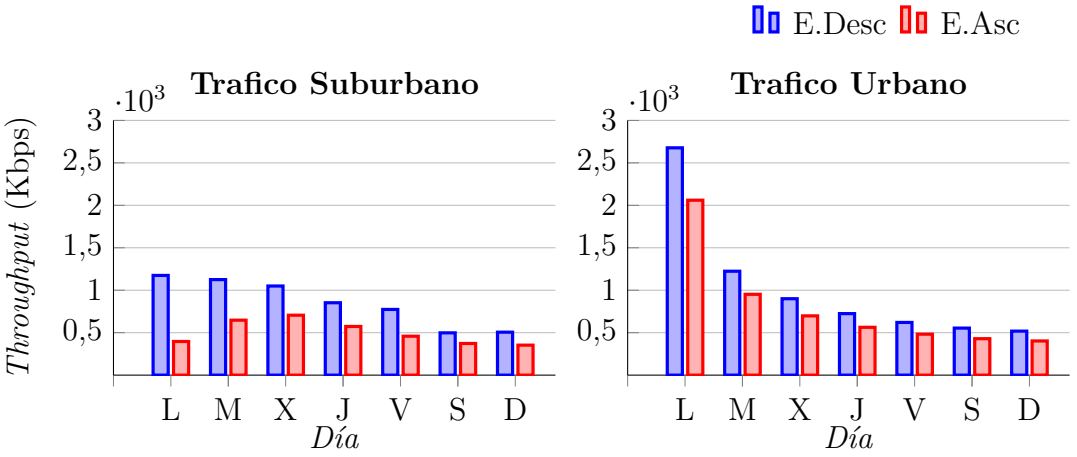


Figura 4.20: Línea de tiempo del tráfico

A modo de resumen, la Tabla 4.7 refleja los valores medios de todas las métricas referidas al uso y eficiencia de recursos, así como a valores de tráfico. Para ello se han utilizado las conclusiones obtenidas anteriormente en combinación con las especificaciones técnicas que marca 3GPP (ETSI TS 136 213 V10.1.0). EL proceso es el siguiente: primero con los valores de MCS se consulta la Tabla 7.1.7.1-1 de 3GPP y se obtiene el índice de TBs. A continuación, con este índice y el valor de PRB se consulta la tabla 7.1.7.2.1-1 de 3GPP para, finalmente, obtener el tamaño de TBs teórico.

Tabla 4.7: Porcentaje de uso del ancho de banda disponible

	Suburbano		**Urbano**	
	E. Desc	E. Asc	E. Desc	E. Asc
MCS	14	23	16	16
Itbs	13	21	15	15
PRB	16	3	14	16
TBs teórico	4136	1480	4264	4968
Throughput (Mbps)	4.1	1.5	4.3	5
***Throughput* Real** (Mbps)	0.8	0.5	1	0.8
Porcentaje de uso	19 %	33 %	23 %	16 %

Como se comprueba el uso real que se va a tener está muy por debajo de lo que se podría alcanzar. Además, cabe destacar que la baja utilización no se debe a un único parámetro, ya que las velocidades reales alcanzadas por un usuario dependen de muchos factores, tales como la calidad del canal radio, el número de usuarios simultáneos en la celda, el tipo de despliegue realizado por el operador, el tipo de servicio considerado y la calidad (QoS) asociada, la capacidad del terminal móvil etc.

4.2.6. Sesiones

Esta sección, se centra en analizar lo que ocurre con los usuarios en el enlace ascendente. Como se explicó en la Sección 4.1.2, no se puede asociar una RNTI a un usuario concreto por lo que el análisis se hace sobre la estimación de las sesiones.

En primer lugar, se estudia el tiempo de vida que tiene cada sesión, tal como se muestra en la Figura 4.21, para cada uno de los entornos.

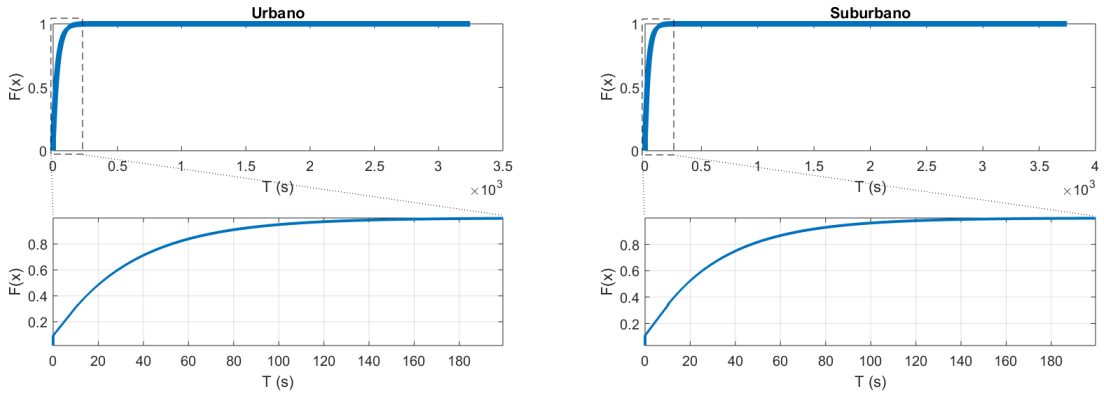


Figura 4.21: CDF de la longitud de las sesiones

Como se esperaba, la distribución tiende rápidamente a 1, debido a que las conexiones que se realizan en LTE suelen ser cortas; según este estudio aproximadamente de 30 segundos. Por ejemplo, mandar un mensaje en cualquier servicio de mensajería instantánea (Whatsapp, Facebook, etc) o hacer una petición a una pagina web, es algo sumamente rápido.

A continuación, en la Figura 4.22 se muestra la estimación del número medio de sesiones en ambos entornos.

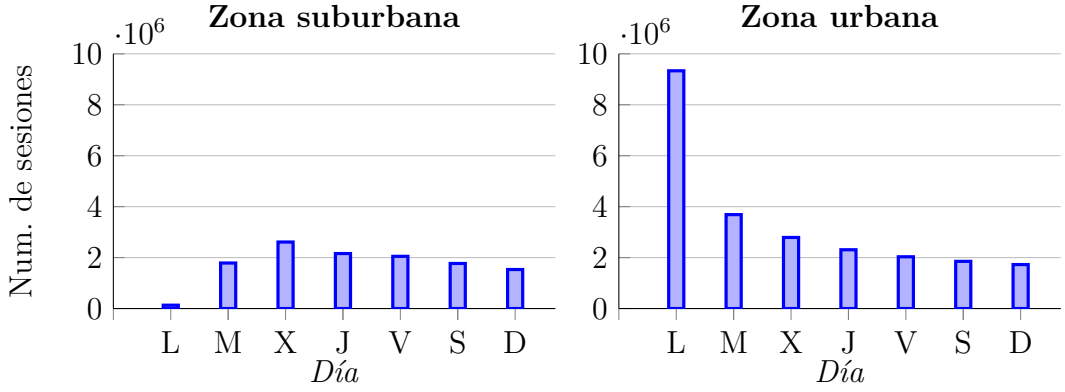


Figura 4.22: Número de sesiones en cada emplazamiento

A la vista de los resultados se comprueba que el número de sesiones es coherente con las métricas de tráfico obtenidas, y que sigue una tendencia en función del día de la semana. Se requeriría una campaña de medida más extensa para sacar resultados concluyentes respecto a este comportamiento.

Por último, la Figura 4.23 analiza la vida útil que tienen varios RNTI en un intervalo de tiempo de aproximadamente 1 minuto, tomando valor 0 cuando no se esta trasmitiendo y 1 cuando se envían datos.

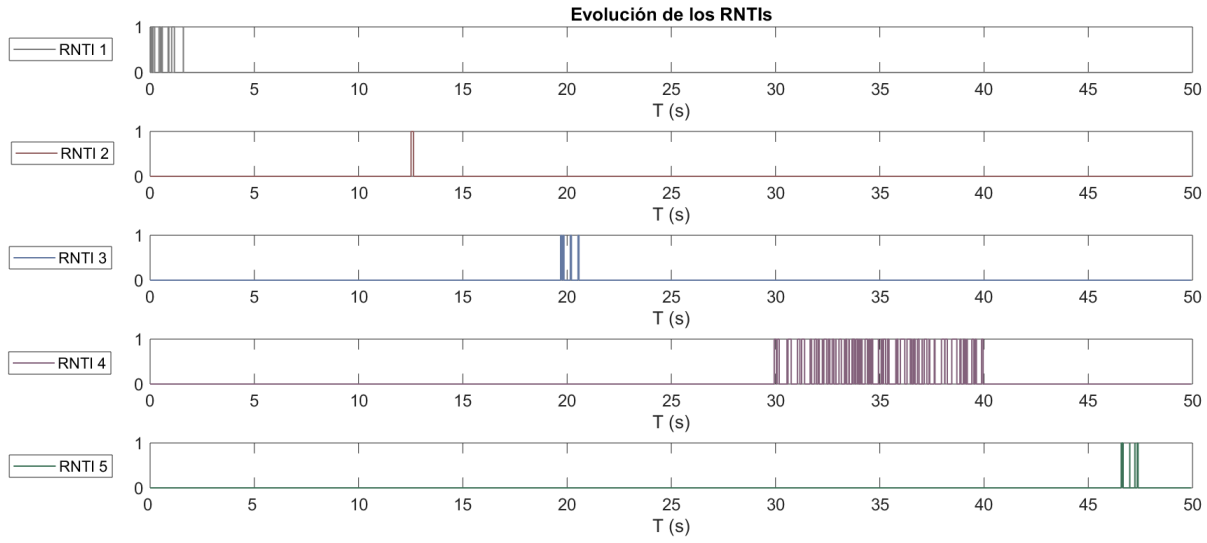


Figura 4.23: Evolución de RNTI

Como se ha comentado a lo largo de esta sección el tiempo de vida de cada RNTI es de apenas segundos, y como muestra la figura se vuelve a corroborar, siendo la ventana de tiempo más grande que se observa de 10 segundos en este caso.

4.2.7. Categoría de los usuarios

Por último, se ha realizado una estima de la categoría de UE requerida para los niveles de tráfico analizados, y se ha comparado con las capacidades proporcionados por terminales comerciales, basándonos en los datos proporcionados en la Tabla 2.4.

Un problema que se ha encontrado es que el canal que se monitoriza en esta plataforma solo nos proporciona información sobre la cantidad de bits de datos en el enlace descendente, por lo que no podemos diferenciar las categorías 6 de la 7, 9 de la 10 y 11 de la 12. Para obtener la estima de categoría de UE se ha acumulado el valor de TBs por cada sesión. A partir de este valor, la Figura 4.24 muestra la categoría de UE que serían necesarias para hacer frente a tráfico medido.

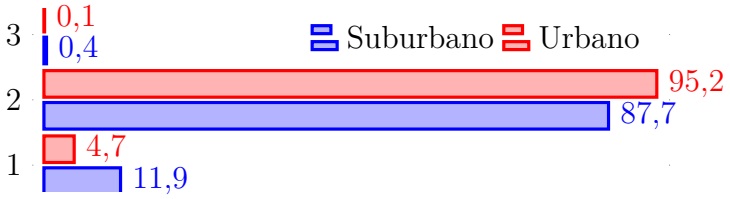


Figura 4.24: Porcentaje de categorías del UE

Con el objetivo de darle un punto de vista más real y práctico a estos resultados se ha buscado las categorias de los diez móviles más vendidos (Fuente: El país) y de los móviles insignia de las dos grandes compañías de telefonía móvil.

Dispositivo	**Bandas LTE** (1, 3, 7, 8, 20, 33 y 34)	**Categoría**
1. Samsung galaxy J5	✓	4
2. Samsung galaxy J3	✓	4
3. Huawei P8 Lite	✓	4
4. Samsung galaxy J7	✓	6
5. Apple Iphone 7	✓	9
6. Samsung galaxy S7	✓	9
7. Huawei P9 Lite	✓	4
8. Xiaomi Redmi Note 4	✓	6
9. BQ Aquaris U2	✓	6
10. Samsung galaxy A5	✓	6
* Apple Iphome X	✓	12
* Samsung galaxy S9	✓	18

Tabla 4.8: Especificaciones de UEs (Fuente:Gsmarena)

A continuación, en la Figura 4.24 se comparan la cantidad de datos que se podrían procesar utilizando cada una de las categorías más populares. Como refleja la Tabla 4.5, la velocidad alcanzable, para un sistema de 50 PRBs utilizando un sistema MIMO es de 150 Mbps, lo cual es superado en gran medida en la mayoría de las categorias.

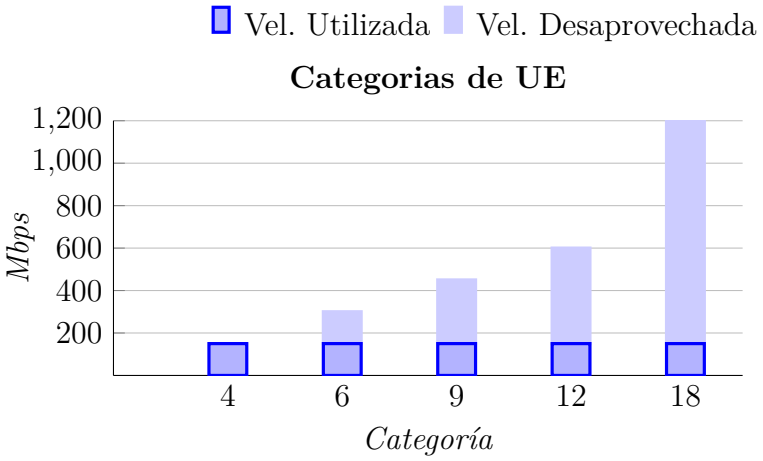


Figura 4.25: Velocidad de descarga de las categorias de UE

A la luz de los resultados, se puede concluir que las capacidades de los dispositivos comerciales se encuentran notablemente por encima de las necesidades de los usuarios.

4.3. Implementación práctica de una estación base y un equipo de usuario

Para concluir este capítulo, debido a la gran modularidad que ofrece en sus características el proyecto srsLTE, se decidió reproducir la conexión entre una eNB y un UE. Para ello se hizo uso de dos USRP B210 que implementan el UE y la eNB, tal como se muestra en la Figura 3.1.

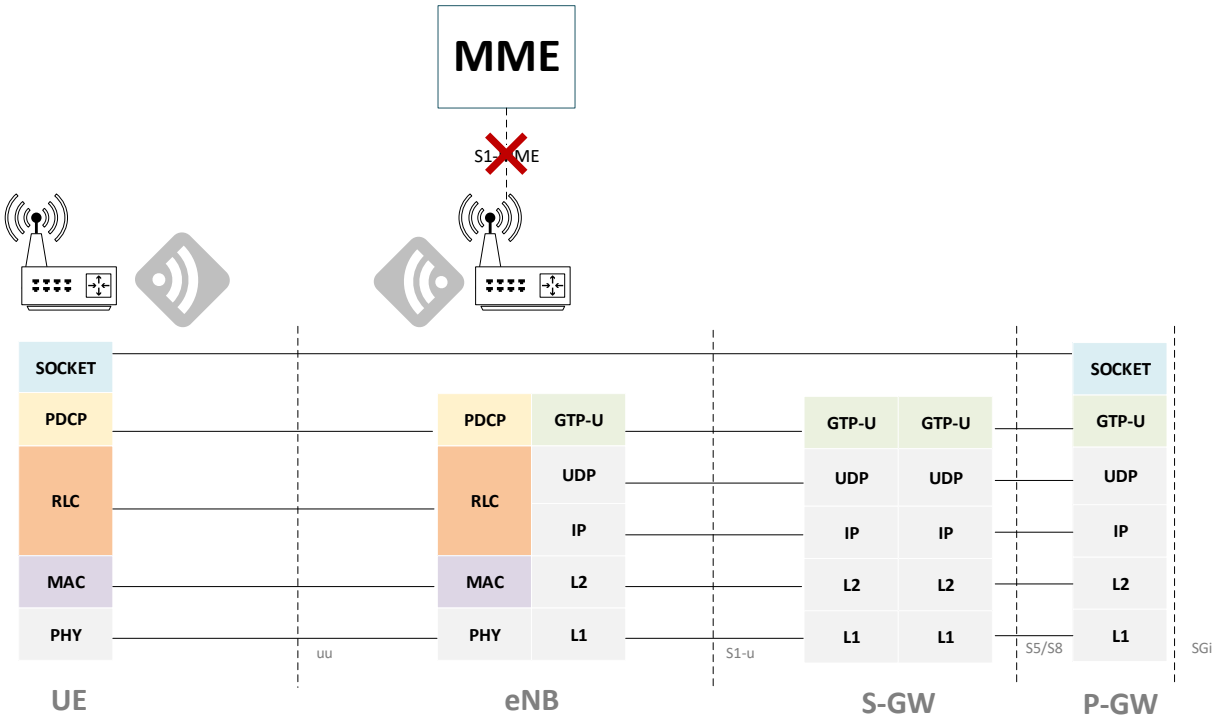


Figura 4.26: Esquema de la implementación práctica de eNB y UE

Dado que no se disponía de soluciones que implementaran el núcleo de la red, se propuso prescindir de la conexión al MME y limitarnos a hacer una conexión a nivel PDCP, y emular la existencia del MME mediante un agente vacío. A continuación, se desarrollaron unos *gateway* (S-GW y P-GW) propietarios que mediante un *socket* se conectan a nivel IP y deberían poder intercambiarse datos.

Para validar la integración se hizo uso del programa *Wireshark*, cuya captura se muestra en la Figura 4.27, donde se puede observar:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
2	0.010027			LTE RRC UL_CCCH	22	RRCConnectionRequest
3	0.016002			LTE RRC DL_CCCH	62	RRCConnectionSetup
4	0.055891			LTE RRC UL_DCCH/NAS-EPS	100	RRCConnectionSetupComplete, Attach request, PDN connectivity request
5	0.064996			MAC-LTE	47	UL-SCH: (SFN=0 , SF=8) UEId=0 (Short BSR) (Padding:remainder)
6	0.072817			MAC-LTE	47	UL-SCH: (SFN=0 , SF=6) UEId=0 (Short BSR) (Padding:remainder)
7	0.416110			MAC-LTE	548	UL-SCH: (SFN=0 , SF=9) UEId=0 (Short BSR) (Power Headroom Report) (Padding:remainder)
8	0.756075			MAC-LTE	532	UL-SCH: (SFN=0 , SF=9) UEId=0 (Short BSR) (Power Headroom Report) (Padding:remainder)
9	2.369759			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
10	2.399938			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
11	2.429185			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
12	2.458823			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
13	2.489008			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
14	2.518798			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
15	2.548979			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
16	2.589791			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
17	2.619974			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
18	2.649787			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
19	2.678840			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
20	2.699799			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
21	2.728906			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
22	2.759772			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
23	2.789929			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
24	2.819731			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
25	2.848833			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)
26	2.879009			MAC-LTE	15	RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)

Figura 4.27: Captura *Wireshark* de la estación base

1. El UE manda un preámbulo RACH como se explica en la Figura 5.1 del anexo I.

2. A continuación, el UE también manda una petición RRC en la que se realiza una propuesta de una serie de parámetros MAC, como el tipo de radio que se va a utilizar,FDD, el valor del C-RNTI, 3, y el valor decimal de RNTI, 70.

3. Ahora se produce la respuesta de la eNB que transporta por un lado una aceptación de los parámetros MAC que se van a utilizar y por otro lado un *RRCConnectionSetup* para indicar al UE los parámetros RRC que se van a usar.

4. La última trama a nivel RRC es mandada por el UE y consta de un mensaje *RRCConnectionSetupComplete* en modo de reconocimiento, ACK. Además, el UE aprovecha para mandar datos de señalización a nivel PDCP, más concretamente hacia el NAS. Primero con una trama de *Attach request* con el número IMSI. Segundo con información de la capacidad de UE, como por ejemplo la seguridad que soporta EEA0(no usar encriptación), 128-EIA1(SNOW 3G) o 128-EAI2(AES). Y para terminar, el tipo de PDN, IPv4.

5. Por último, el UE envía mensajes (5,6,7,8 de la Figura 4.27) hacia la estación base de tipo Buffer Status Reports (BSR), que indicarían que el UE se encuentra esperando la asignación de recursos.

Lo siguiente que debería ocurrir es que la estación base asignara la cantidad mínima de recursos para PUSCH. Sin embargo, como vemos en la captura esto no ocurre. Como se comentó anteriormente, el elemento MME es el encargado de gestionar el NAS y las portadoras radio, así que a pesar de existir una gran modularidad, suplantar el elemento MME requiere un alto número de modificaciones en varios módulos de la solución srsLTE. Una posible opción era contar con una herramienta comercial que supliera el elemento MME pero fue descartado ya que superaba los limites de este trabajo.

Como el proyecto srsLTE esta en continuo desarrollo, en una actualización posterior se ha visto que la propia solución ahora incorpora el elemento MME, por lo que este problema ha sido resuelto.

Capítulo 5

Conclusiones y líneas futuras

En principal cometido de este proyecto ha sido el análisis del uso de redes LTE comerciales, mediante su monitorización con soluciones SDR. Esto ha permitido enfrentar los conocimientos teóricos y prácticos adquiridos con situaciones reales. A continuación, se van a enumerar las principales conclusiones obtenidas de la elaboración de este proyecto, así como las líneas futuras de investigación y desarrollo que surgen a partir del mismo.

5.1. Conclusiones

Los dos objetivos principales que se han planteado en este proyecto han sido: el desarrollo de una herramienta para automatizar la monitorización de despliegues de red LTE comerciales, y la evaluación de las capacidades de una solución SDR para implementar una red LTE en el que se envía información en claro. De este modo, se ha podido alcanzar una mayor comprensión del comportamiento de sistemas reales y comprobar la validez de algunas de las suposiciones que se hacen normalmente en estudios teóricos. Respecto al segundo objetivo, la implementación de la red LTE se ha realizado de forma parcial, debido a las limitaciones de la solución adoptada.

Para llevar a cabo dichos objetivos se ha desarrollado un proyecto sobre la solución IMDEA-OWL, que a su vez esta implementada sobre la solución SDR. De esta manera, se ha permitido automatizar la monitorización de la red LTE.

A la vista de los resultados comentados a lo largo de este trabajo, convendría hacer hincapié en algunas ideas que han parecido que por su aportación han sido consideradas relevantes:

- En primer lugar, se ha ratificado en el uso diferenciado que se realiza en las celdas dependiendo de su localización.
- En segundo lugar, se ha comprobado que la banda 20 (791-821 MHz) es la preferida por los operadores, algo que parece lógico debido a sus mejores condiciones de propagación.
- También relacionado con el análisis de tráfico, se ha corroborado que el tráfico en el enlace descendente aún se encuentra muy por debajo del relativo al enlace ascendente. Aunque la tendencia sea de un mayor balance de tráfico en ambos enlaces, esa situación aún parece lejana.

- Respecto al tráfico cursado por las redes, los resultados obtenidos muestran que las celdas analizadas se encuentran infrautilizadas, tanto en términos de recursos como de capacidad de transmisión. Esta observación choca con las suposiciones típicamente hechas en estudios teóricos, donde se asumen condiciones de saturación o *full-buffer*.

- En cuarto lugar, en cuanto a la monitorización realizada se refiere remarcar que a pesar de que las compañías de dispositivos móviles dotan a los usuarios de terminales con una capacidad de transmisión de datos de lo más elevadas, el uso que, a efectos prácticos, se les puede dar es muy inferior al que tienen asignado.

- En último lugar señalar que, a pesar de ser cierta la idea de que la solución SDR tiene un gran abanico de posibilidades, durante la realización de este trabajo se ha observado que la solución adoptada estaba limitada y dependía de productos de terceros (típicamente comerciales). Sin embargo, versiones posteriores de esta solución SDR permiten el despliegue de la red de forma íntegra.

5.2. Líneas futuras

A partir del trabajo realizado en este proyecto se han definido dos posibles líneas de investigación y desarrollo:

- A raíz de la última conclusión, la solución SDR se ha actualizado dando la posibilidad de realizar la conexión a todos los niveles sin necesidad de ninguna otra herramienta. Por lo tanto, una aplicación muy interesante, y que ayudaría a entender mejor cómo gestionan los operadores las estaciones base que despliegan, implicaría continuar con la implementación por medio de los dispositivos USRP. Incluyendo además el nuevo elemento MME que suministra la última actualización del proyecto srsLTE. A partir del despliegue completo de una red LTE, se podrían implementar soluciones de red y evaluar sus prestaciones en comunicaciones reales con dispositivos de usuario comerciales.

- En relación a la monitorización de la red, como se ha comentado, los resultados obtenidos podrían ser complementados con campañas de medida adicionales. En concreto, se abordarían las siguientes extensiones:

  - Extender la duración de las campañas de medida.
  - Buscar nuevos emplazamientos con diferentes características.
  - Analizar distintas celdas, con distintos anchos de banda.
  - Monitorizar distintos operadores.
  - Muestrear distintas bandas LTE.

Bibliografía

[1] sharetechnote.com. http://www.sharetechnote.com//html/Handbook_LTE_RNTI.html, 2017.

[2] Bui, N., and Widmer, J. OWL: a Reliable Online Watcher for LTE Control Channel Measurements. In *ACM All Things Cellular (MobiCom Workshop)* (Nov. 2016).

[3] Gomez-Miguelez, I., Garcia-Saavedra, A., Sutton, P. D., Serrano, P., Cano, C., and Leith, D. J. srslte: an open-source platform for lte evolution and experimentation. In *Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization* (2016), ACM, pp. 25–32.

[4] Nikaein, N., Knopp, R., Kaltenberger, F., Gauthier, L., Bonnet, C., Nussbaum, D., and Ghaddab, R. Openairinterface: an open lte network in a pc. In *Proceedings of the 20th annual international conference on Mobile computing and networking* (2014), ACM, pp. 305–308.

[5] Semiconductor, F. Long term evolution protocol overview. *White Paper, Document No. LTEPTCLOVWWP, Rev 0 Oct* (2008).

[6] Sesia, S., Baker, M., and Toufik, I. *LTE-the UMTS long term evolution: from theory to practice*. John Wiley & Sons, 2011.

ANEXO I

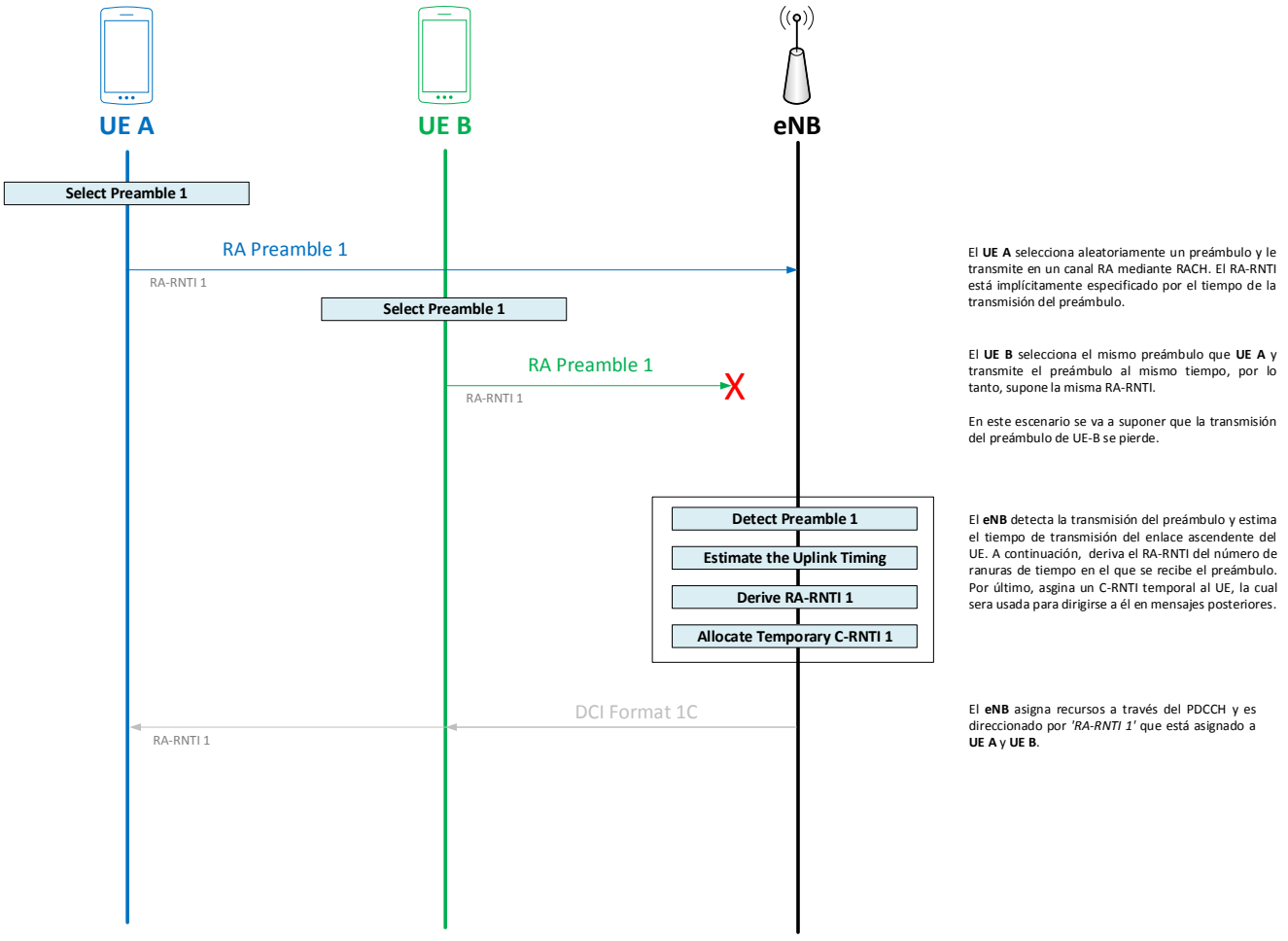
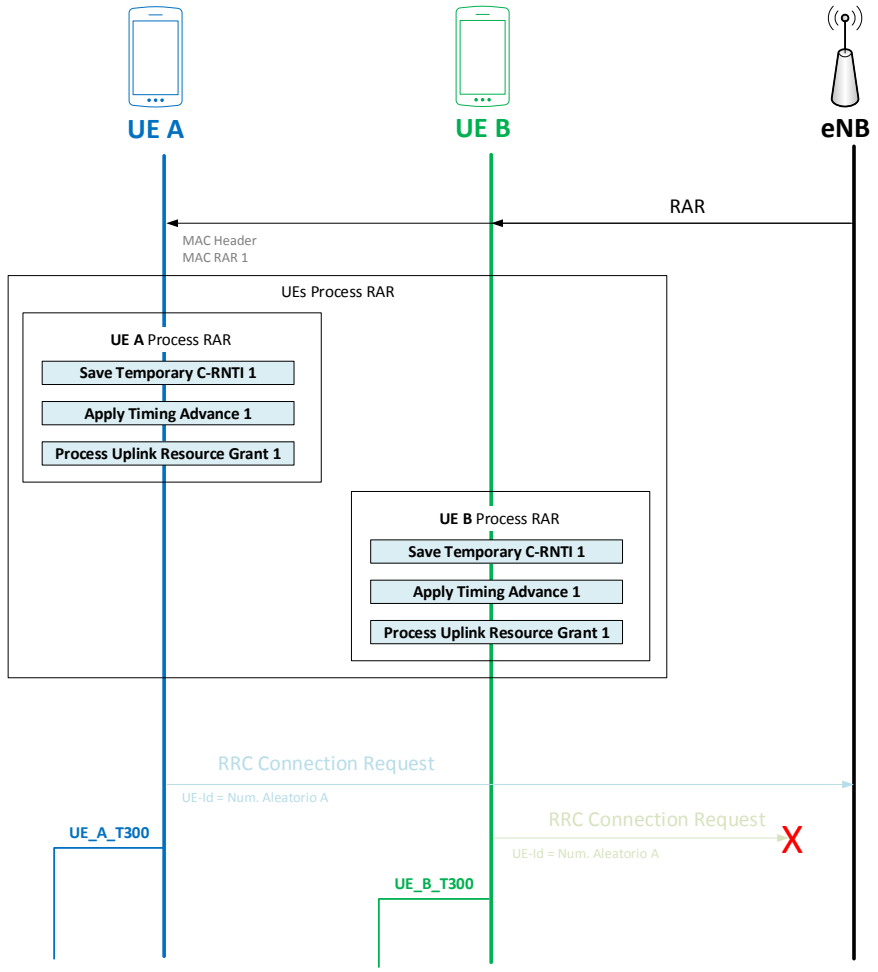


Figura 5.1: Ejemplo del proceso basado en contienda (RAP). Parte 1



El **eNB** transmite la RAR en el canal DL-SCH. El mensaje lleva la asignación de recursos de temporización y enlace ascendente para el Preámbulo 1, también incluye en el encabezado MAC un indicador de retroceso para controlar la duración de la interrupción en el caso de un fallo en el RAP.

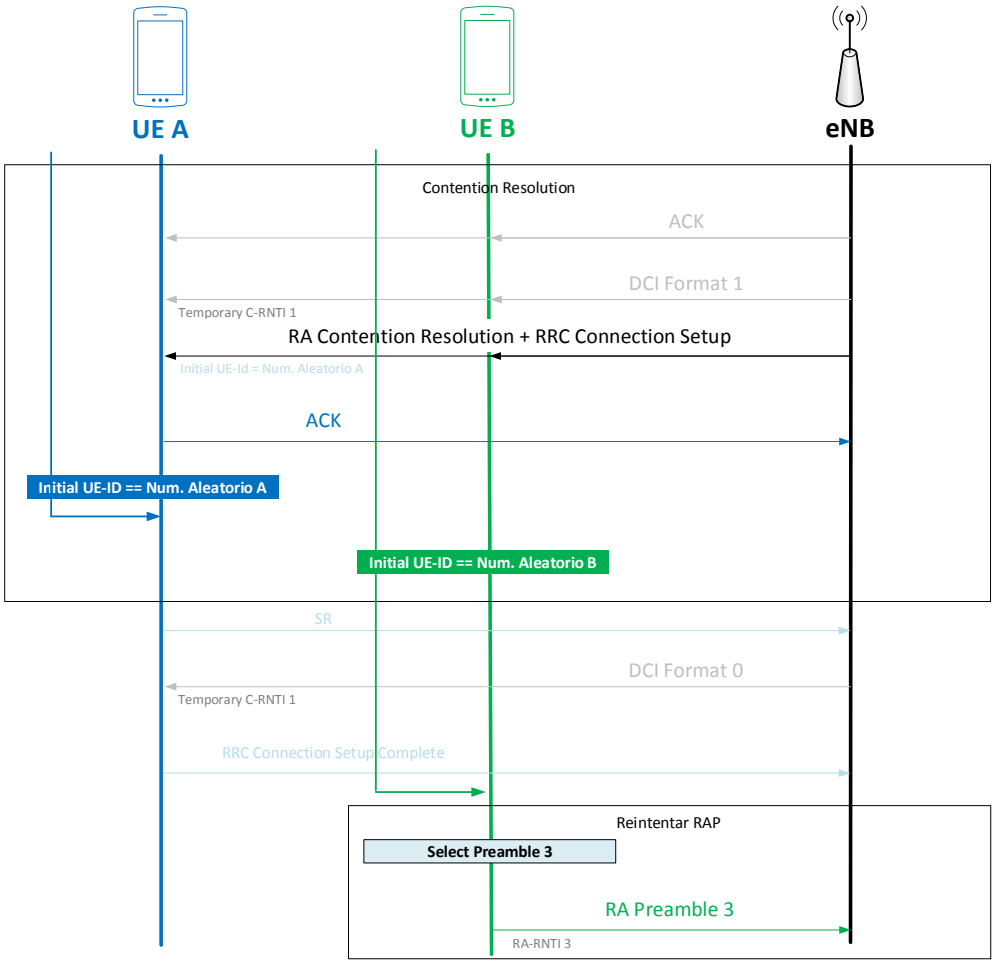
UE A guarda el C-RNTI temporal de los datos MAC para el Preámbulo 1. Después de aplicar la corrección, el **UE A** se sincroniza en la dirección de retorno y puede transmitir ráfagas de datos al **eNB** a través de los recursos de enlace ascendente asignados.

UE B cree erróneamente que la RAR está destinada hacia él ya que el RA-RNTI y el Preámbulo coinciden en el mensaje. Como no tiene forma de saber que el mensaje realmente se refería a **UE-A** continúa con el procedimiento aunque haya sido rechazado.

Esta situación se resolverá después.

UE B transmite por UL-SCH, en la misma asignación y colisiona con la transmisión de **UE A**, por lo que su transmisión no se reciba en el **eNB** ya que está transmitiendo con un avance de temporización que no estaba destinado para él. A su vez, también inicia un temporizador en espera del mensaje de configuración de conexión RRC.

Figura 5.2: Ejemplo del proceso basado en contienda (RAP). Parte 2



El **eNB** acepta la transmisión con un PHICH ACK y señala una asignación de enlace descendente utilizando el C-RNTI temporal 1 a través del PDCCH. Tanto el **UE A** como el **UE B** suponen que la asignación es para ellos, ya que ambos creen que se les ha asignado C-RNTI temporal 1.

UE A y **UE B** reciben el mensaje de configuración de conexión RRC, ya que se dirige con el C-RNTI 1 temporal. El mensaje también contiene **'Número Aleatorio A'** como la identidad inicial.

UE A recibe la transmisión del **eNB**, por lo que reconoce el mensaje con una respuesta HARQ ACK por PUCCH..

El **UE A**, viendo que su propia identidad hizo eco, concluye que el RA fue exitoso y procede con la operación alineada en el tiempo.

La comparación del **UE B** falla, por lo que se da cuenta de que ha perdido a otro UE en la resolución de contienda.

Se acaba el tiempo del **UE B** para el procedimiento de acceso aleatorio ya que no recibió su propia identidad en la resolución de contienda.

UE B vuelve a intentar la solicitud.

UE B reintenta el procedimiento de acceso aleatorio.

Figura 5.3: Ejemplo del proceso basado en contienda (RAP). Parte 3