Evaluación de una estación base LTE basado en software

(Software-based LTE Base Station Evaluations)

Ingeniería Superior de Telecomunicaciones

Proyecto Final de Carrera

Autor: Holmes Liu

Director/a: ILKER SEYFETTIN DEMIRKOL

Año: 2016

Resumen

A principios de la década de los 90 se introdujo el estándar GSM en Europa, con una fuerte inversión por parte de las operadoras para ofrecer un servicio digital al usuario doméstico. Entonces no existían la agrupación de funcionalidades que hoy disfrutamos en los terminales. Las funcionalidades de llamadas, cámara, video, GPS, acceso a internet, etc. estaban distribuidas en diferentes dispositivos. Actualmente, la unificación de los aparatos anteriores en el terminal móvil y la introducción de la tecnología a gran parte de la población han implicado un mayor requerimiento en calidad de servicio, ancho de banda y cobertura, lo que obliga a las operadoras a optimizar la explotación de los diferentes servicios con una visión a largo plazo.

Uno de los objetos de estudio de esta evolución tecnológica continuada en el tiempo es la adecuación de la infraestructura para adaptarse a los estándares de la próxima generación, los cuales prometen una mejora en rendimiento y eficiencia. Sin embargo, los equipos operativos que las operadoras poseen actualmente pueden no estar diseñados ni preparados para este fin, y ello implica la necesidad de volver a reemplazarlos. Ante esta necesidad nacen los conceptos de SDR (Software Defined Radio) y C-RAN (Cloud Radio Access Network). El primero es una solución para proporcionar versatilidad al equipo hardware, y el segundo para facilitar el dimensionado de la red y optimizar recursos según demanda.

Este proyecto estudia y evalúa el uso de la plataforma OpenAirInterface, solución basada en SDR para implementar una estación base de telefonía LTE, con la posibilidad de separar las diferentes entidades de la arquitectura (C-RAN). Utilizando para ello dispositivos portátiles de bajo coste.

Abstract

In the early 90s, the GSM standard was introduced in Europe with an important carrier-side investment in order to deliver a digital service to the home user. Back then there was no functionality bundling in contrast to the actual terminals. Call functionality, camera, video, GPS, Internet access, etc. were distributed through different devices. Currently, the prior service integration into a single mobile device, along with the technology diffusion to the overall population, involved a greater requirement on quality of service, bandwidth and coverage, forcing operators to optimize the resource usage with a long-term vision.

One of the study objects within this long haul technological evolution is the infrastructure adaptation to accommodate the next generation of standards, which promise improved performance and efficiency. However, current operator infrastructure may not be designed to, nor prepared for this purpose, suggesting replacing them again. Given this need arise the concepts of SDR (Software Defined Radio) and C-RAN (Cloud Radio Access Network). The former is a versatile solution in the hardware area, while the latter a promising key to aid with network dimensioning and resource optimization.

This project examines and evaluates the use of OpenAirInterface platform, a software solution based on SDR, to implement a LTE base station, with the possibility of splitting the different entities of the architecture (C-RAN), and using for this purpose low-cost portable devices.

Índice de contenido

Lista de figuras

1. Introducción

1.1. Contexto

Ante el aumento de la demanda de servicios de telecomunicaciones, con un perfil de usuario cada vez más exigente en términos de movilidad, disponibilidad, ancho de banda o autonomía, crecen los esfuerzos por parte de las operadoras para diseñar e implementar una infraestructura, capaz de soportar este aumento de nivel de tráfico, a la vez que minimiza los costes para compensar en la medida de lo posible la saturación del *revenue*.

Con la evolución constante de la tecnología, se ha hecho posible llevar a la práctica algunos de los conceptos que se han ido gestando y madurando en los últimos años en el entorno Software Defined Radio (SDR), término acuñado por Joe Mitola en 1991, y que consiste en un dispositivo radio en el cual algunas de sus funciones de nivel físico (o todas) pueden modificarse a través del software, lo que proporciona mayor flexibilidad frente al hardware tradicional, permitiendo por ejemplo que se puedan añadir nuevas capacidades al hardware (o modificar las existentes), sin la necesidad de reemplazarlo constantemente para su actualización, reduciendo de esta forma los costes que ello implica.

Por otro lado, la revolución en la capacidad de computación ha permitido separar físicamente las funcionalidades que corresponde a la interfaz radio de las de procesado digital, distribuyendo la primera en el terreno de cobertura, y ubicar las unidades de procesamiento de forma centralizada, permitiendo asignaciones dinámicas de recursos según demanda. Dicha arquitectura, conocida como *Cloud RAN* o *C-RAN*, es otra forma de optimizar el consumo de recursos, con la consecuente disminución en costes.

1.2. Objetivo y organización de la memoria

Este Proyecto Fin de Carrera se enmarca dentro del ámbito de las tecnologías de la información y las comunicaciones (TIC), con la finalidad de evaluar y mostrar las

posibilidades de una implementación basada en SDR para el despliegue de una estación base LTE (conocido como *evolved Node B, eNodeB o eNB*), mediante un dispositivo de bajo coste USRP (*Universal Software Radio Peripheral*) conectado a un ordenador de propósito general para el procesado en banda base, además de emular al mismo tiempo una red troncal (*Core Network*) que da acceso a la red exterior.

Pretendemos introducir el uso de una plataforma flexible y versátil destinado a ayudar en el desarrollo de la próxima generación de telefonía móvil 5G, así como la mejora en la tecnología actual 4G, sirviendo a su vez de apoyo en el ámbito educativo.

La memoria ha sido estructurada en cinco partes principales: en primer lugar revisaremos brevemente la arquitectura base de la telefonía móvil de próxima generación basado todo en IP, el EPS (Evolved Packet System), el cual se divide en las tecnologías de red de acceso (*Long Term Evolution*, LTE) y de red troncal (*Evolved Packet Core*, EPC). En este mismo capítulo de trasfondo también hablaremos acerca de la implantación de LTE en España y las asignaciones frecuenciales en el mismo territorio. Todo ello son aspectos que nos afectarán de manera directa durante la fase de experimentación.

Seguidamente explicaremos la plataforma que hemos utilizado para realizar el escenario de pruebas, el OpenAirInterface, y los elementos software y hardware que componen el mismo escenario. En el capítulo cuatro definiremos la implementación y las configuraciones que hemos llevado a cabo, mostrando en este mismo capítulo una visión global de la arquitectura del *testbed*.

Posteriormente describiremos los retos a los que hemos enfrentado en la implementación del escenario y la realización de las pruebas. Dichos ‘desafíos’ pueden verse también como fruto de la experimentación con el SDR y tienen el mismo peso que el capítulo siguiente relativo a los resultados. En este último mostraremos las verificaciones y comprobaciones del sistema con diferentes herramientas, así como la presentación los resultados obtenidos.

2. Trasfondo: EPS y estado de la tecnología LTE en España

2.1. Evolved Packet System

El EPS representa el sucesor lógico del estándar 3G/UMTS introducido por el comité de estándares 3GPP (*3rd Generation Partnership Project*). La necesidad de la evolución a largo plazo de la tecnología 3G surgió desde el mismo 3GPP a finales de 2004, con el fin de mantener, para el futuro, una posición competitiva de las tecnologías basadas en UMTS. Por consiguiente, se decidió emprender la evolución de la arquitectura de sistema y de acceso de red, cuyas especificaciones se concluyeron durante el primer trimestre del 2009, quedando reflejado en el Release 8 del 3GPP [1][2].

EPS es conocido también por otros acrónimos, relacionados con sus respectivos objetos de estudio técnicos: LTE (*Long Term Evolution*), el cual se centra en la evolución de la interfaz radio, y SAE (*Service Architecture Evolution*), enfocado a la arquitectura de núcleo de la red de acceso radio. De esta manera se forman dos sistemas independientes pero complementarios.

2.1.1. Long Term Evolution

LTE es el término utilizado por la comunidad 3GPP en sus informes y especificaciones para referirse a la red de acceso E-UTRAN (*Evolved UMTS Terrestrial Radio Access Network*). Se trata del estándar de red de acceso de radio diseñado para reemplazar a las tecnologías UMTS (*Universal Mobile Telecommunications System*) y HSPA (*High Speed Packet Access*). A diferencia de HSPA, se compone de una interfaz aérea totalmente nueva, incompatible con W-CDMA (*Wideband Code Division Multiple Access*). Proporciona mayores velocidades de transferencia de datos, menor latencia, y está optimizado para transferir únicamente paquetes de datos.

Según el estándar, en esta red de acceso, habría que garantizar una latencia reducida, anchos de banda estandarizados de 1.4, 3 , 5, 15 y 20 MHz, se simplifica la arquitectura eliminando el RNC (*Radio Network Controller*) de 3G, que heredó a su vez del BSC (*Base Station Controller*) en 2G. De esta manera, la nueva red de acceso está formada sólo por eNodeBs.

Con esta simplificación se reduce la latencia y tuvo que añadir nuevas funcionalidades en el eNodeB:

- RRC (*Radio Resource Control*): Se refiere a la asignación, modificación y liberación de recursos en la transmisión por la interfaz radio, entre el terminal de usuario y el eNodeB.
- *Radio Mobility management*: procesamiento de mediciones y resolución de handover.
- Protocolo de la capa 2 de la interfaz radio, similar a la capa *Data Link* del modelo OSI, su función es garantizar la transferencia de datos entre entidades de la red, esto implica la detección y posiblemente corrección de errores que puede ocurrir en la capa física.

A nivel físico presenta las siguientes características principales:

- Uso del OFDM (*Orthogonal Frequency Division Multiplexing*), la cual utiliza un esquema de modulación digital multi-portadora, en el que la información se distribuye en un gran número de sub-portadoras ortogonales transportando sub-streams de datos paralelos, y que agregados convenientemente, forman el stream de datos principal. Cada sub-portadora se modula con un esquema de modulación convencional (como QAM) y tiene una tasa de símbolos baja.
- Métodos de acceso de múltiples usuarios: OFDMA en downlink y SC-OFDMA para uplink.
- MIMO (*Multiple-Input Multiple-Output*). Tecnología que hace uso de múltiples antenas para mejorar el rendimiento de las comunicaciones.
- Soporte de FDD y TDD.

- Tramas de radio con una duración de 10 ms (10 subtramas de 1 ms).
- Codificación de símbolos por medio de *turbo coding*.

Se define una nueva interfaz opcional, *X2*, entre eNodeBs, que los conecta en forma de malla, con el fin de minimizar la pérdida de paquetes por la movilidad del usuario. Por ejemplo los paquetes no enviados en la cola del eNodeB origen pueden ser enviados a través de esta interfaz hacia el eNodeB destino.

Con la arquitectura anterior se elimina los procedimientos de *soft-handover* (conocido también por el nombre de macro diversidad), utilizados en las interfaces radio basadas en CDMA y gestionados a nivel de RNC en la interfaz *Iur* de 3G/UTRAN. En el anexo 8.2 encontrarán una explicación más detallada.

La figura 1 es un ejemplo de una arquitectura simplificada de E-UTRAN y EPC, remarcados en contenedores de color gris. También se ilustra su integración con otros sistemas: conexión a IMS (IP Multimedia subsystem)[1] y otras tecnologías de acceso de red, tanto las de tipo *non-3GPP* (WLAN en la figura), como las de tipo 3GPP (UTRAN), así como *fallback* al circuito conmutado a través del IMS.

[1] El IMS es una plataforma genérica que se encarga de provisionar servicios IP multimedia basados en el protocolo SIP de IETF. Provee funciones y procedimientos de control de sesión, de *bearer* (conexión virtual), de política y de facturación.

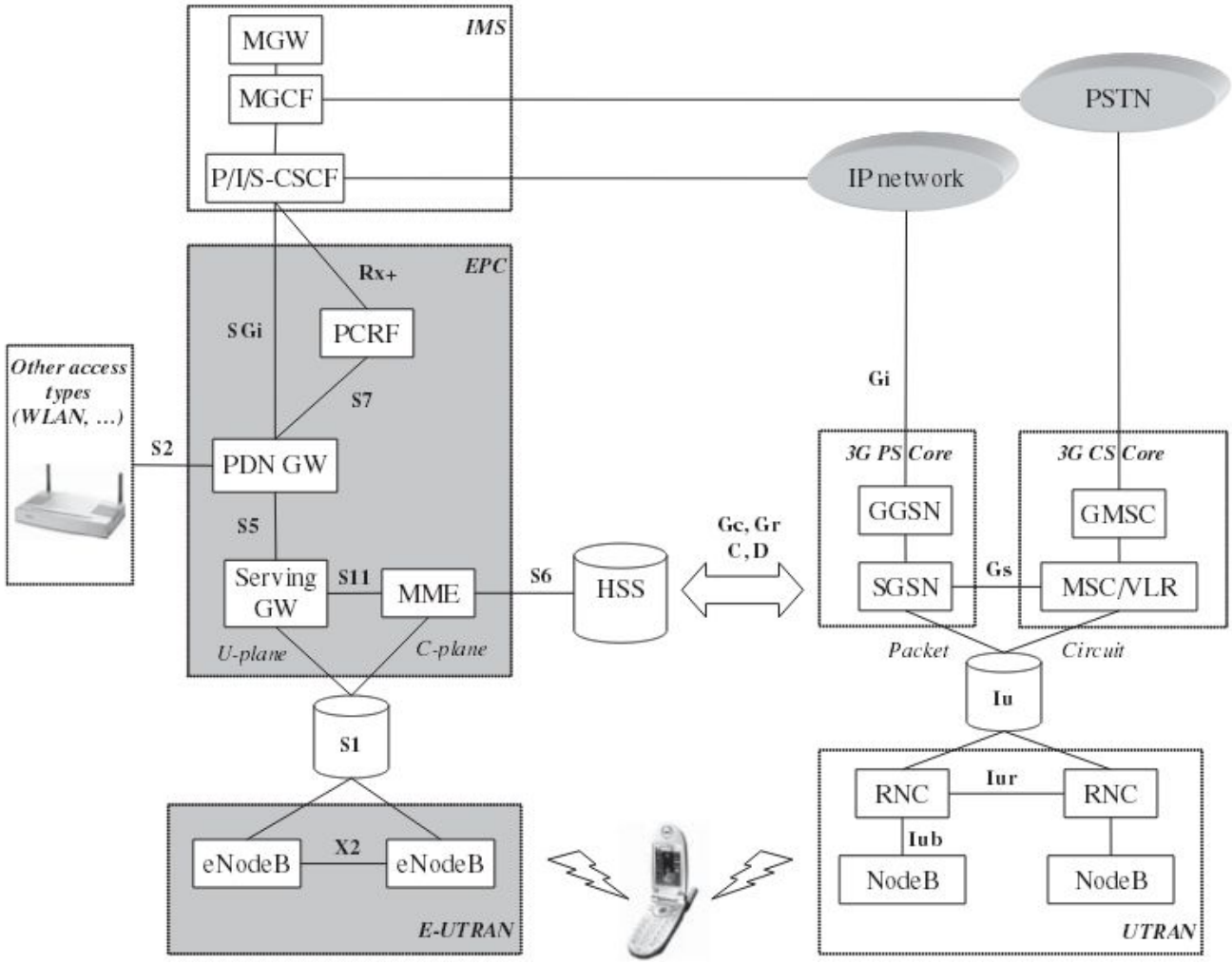


Figura 1: Esquema genérico de la arquitectura EPS [1]

2.1.2. System Architecture Evolution

El SAE core, también conocido como EPC (Evolved Packet Core), es la arquitectura de red troncal de las redes 3GPP LTE y constituyen la evolución y alternativa a las redes core GPRS (General Packet Radio Service)[2].

En GSM, la arquitectura funciona por conmutación de circuitos. Esto es un tipo de conexión que establece un canal de comunicaciones dedicado entre el origen y el destinatario, reservando recursos de transmisión y de conmutación de la red para su

[2] Servicio de datos móvil orientado a paquetes en el sistema de comunicaciones celular 2G y 3G. Se creó como extensión del sistema GSM para complementar al servicio por conmutación de circuitos.

uso exclusivo en el circuito durante la conexión.

En GPRS y UMTS, con la popularización del World Wide Web, se añade al sistema anterior la conmutación por paquetes. Con este método, los datos son transportados en paquetes sin el establecimiento previo del circuito dedicado, ganando así en flexibilidad y eficiencia. Aunque se sigue utilizando el dominio del circuito en los servicios destinados para la voz y el SMS.

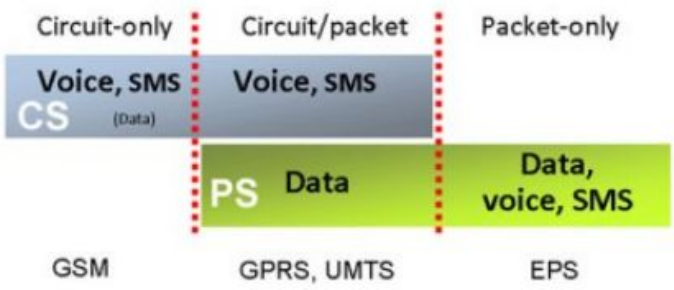


Figura 2: Dominios de circuito y de paquetes en distintas tecnologías [3]

Durante el diseño de la evolución del sistema 3G, la comunidad 3GPP decidió utilizar el IP como protocolo de transporte de todos los servicios. Por lo que se acordó que el EPC no funcionaría en el dominio de conmutación por circuitos, sino que sería una evolución de la conmutación de paquetes del GPRS/UMTS.

La arquitectura del EPC fue introducido en el Release 8 del estándard. El transporte del tráfico es encargado por varios nodos diseñados para ganar eficiencia desde las perspectivas de rendimiento y coste.

Por motivos de escalabilidad, adaptabilidad y ayudar al dimensionamiento de las redes, también se decidió separar los datos del usuario, conocido también como plano de usuario (*user plane*), de los de señalización o plano de control (*control plane*).

Los principales subcomponentes que forman el EPC son los siguientes:

- Home Subscriber Server - HSS: es la base de datos central que contiene la información relativa a los usuarios de la red. Provee soporte a las funciones de gestión de la movilidad, establecimiento de sesión / llamada, autenticación y

autorización de usuarios. Está basado en el HLR (Home Location Register) y AuC (Authentication Centre) del 3GPP Release 4.

- Serving Gateway - SGW: Los gateways (S/P GW) se centran en el plano de usuario (*user plane*), transportando tráfico IP entre UE y las redes externas. Aunque particularmente en el SGW también interviene el plano de control (por su conexión con MME por la interfaz S11). El SGW es el punto que interconecta el lado de la radio con EPC. Sirve a los UEs enrutando los paquetes IP entrantes y salientes. Actúa como punto de control (*anchor*) en operaciones de *handovers* entre eNodeBs y operaciones de *mobility management* entre LTE y otras tecnologías 3GPP. Y se conecta de manera lógica al PGW.

- Packet Data Network Gateway - PGW: punto de interconexión entre el EPC y las redes IP externas, llamadas PDN (Packet Data Network). PGW enruta los paquetes desde / hacia PDNs. Hace cumplir las políticas de seguridad, filtrado de paquetes o interceptación por parte de autoridades. Actúa como punto de control (anchor) para movilidad con tecnologías no 3GPP (p. ej. WiMAX) y 3GPP2 (CDMA1X y EvDO).

- Mobility Management Entity - MME: este nodo trabaja con el *control plane*, se encarga de la señalización relativa a la movilidad y seguridad de acceso a E-UTRAN, mediante la interacción con el HSS. Es el responsable del *tracking, paging* de los UEs en estado *idle*. Es el punto de terminación de la señalización NAS[3], así como su protección de cifrado e integridad [3].

En el anexo 9.1 encontrarán un resumen de las interfaces que conectan los nodos anteriores.

[3] NAS (Non-Access Stratum) es un conjunto de protocolos soportados entre UE y MME, desarrollados por el 3GPP para llevar a cabo la gestión de movilidad de los equipos de usuario (EPS Mobility Management, EMM) y la gestión de las sesiones para el establecimiento de la conectividad entre el UE y P-GW (EPS Session Management, ESM). Consecuentemente son protocolos no relacionados a la interfaz de acceso radio y se ubican en los niveles superiores dentro de la pila de protocolos (nivel 3).

2.2. Implantación de LTE y asignación frecuencial en territorio español.

A pesar de que las tecnología GSM / UMTS son las más utilizadas en las comunicaciones móviles en todo el mundo, presente en la mayoría de los países, lo cierto es que ante el avance incesante de la tecnología y la necesidad cada vez mayor de los usuarios, se han quedado obsoletos en cuanto a prestaciones y seguridad. En consecuencia, las operadoras se apresuran en el despliegue de las tecnologías sucesoras como el LTE, que ofrece mayor calidad de conexión a internet móvil, en términos de latencia y velocidad, seguridad más robusta, arquitectura simplificada con menos componentes con el consecuente abaratamiento en mantenimiento, sentando de esta manera las bases para la llegada del 5G.

El despliegue comercial de LTE en España se retrasó frente a otros países europeos. La banda de 800 MHz, previamente ocupada por la TDT (Televisión Digital Terrestre), se liberó en abril de 2015. Esta reasignación del espectro 790-862 MHz fue una decisión de la Unión Europea para mejorar las comunicaciones móviles logrando aumentar la cobertura y penetración del LTE [4][5]. Dicho retraso de la posibilidad de utilización de la banda para LTE ha facilitado una mayor disponibilidad de terminales. Actualmente, con un alto índice de la población cubierta, LTE se ha convertido ya en un servicio consolidado en en las principales ciudades españoles [6], alcanzando una cobertura del 76.3%[4] en el año 2015 (actualizado con un 90% en 2016) según estudios de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI) del Ministerio de Industria, Energía y Turismo [7].

En este mismo informe de la SETSI en 2015, elaborado a partir de los datos facilitados por 126 operadores, observamos también el dominio casi por completo del UMTS con HSPA, alcanzando un asombroso 99,7% de cobertura en el territorio español (figura 3). La consolidación en el despliegue de estas tecnologías ha representado todo un desafío

[4] Según el estudio, para un nivel de potencia mediana de la señal recibida en exteriores de, al menos, -90 dBm.

a la hora de ubicar un lugar adecuado para la realización de nuestras pruebas, ya que actualmente incluso en interiores es posible recibir señales de las estaciones cercanas con niveles de potencia aceptables. En el capítulo 5. *Retos del entorno real* volveremos a tratar este punto, así como las repercusiones de éste en el proyecto.

2015							
ADLS ≥ 2 Mbps	ADSL ≥ 10 Mbps	VDSL	WiMAX	HFC	FTTH	3,5G (HSPA)	4G (LTE)
89%	69%	11%	57%	48%	45%	99,7%	76%

Figura 3: Comparativa cobertura de banda ancha en España en el año 2015 [9]

El Ministerio de Industria, Energía y Turismo es el encargado de controlar y regular la implementación de servicios de redes móviles en el territorio español. Mediante el Cuadro Nacional de Atribución de Frecuencias, y actualizado a través del BOE, se asigna a los distintos servicios de radiocomunicaciones las diferentes bandas de frecuencias en función de requerimientos técnicos o regulaciones internacionales, y que abarcan desde 8,3 kHz hasta 3000 GHz, aunque por el momento a partir de 275 GHz no están licenciadas [10].

Particularmente, los servicios de telefonía para el entorno civil comprenden desde 790 MHz hasta 2690 MHz, en donde conviven con diferentes servicios de telecomunicaciones[5]. En la siguiente figura (Figura 4) se ilustra la asignación frecuencial de servicios de telefonía en España. En la Figura 5 se desglosa las bandas destinadas al LTE, y las operadoras que intervienen en cada una de ellas.

[5] Por ejemplo, radioastronomía, investigación espacial, radionavegación aeronáutica, banda ISM (Industrial, Scientific and Medical)

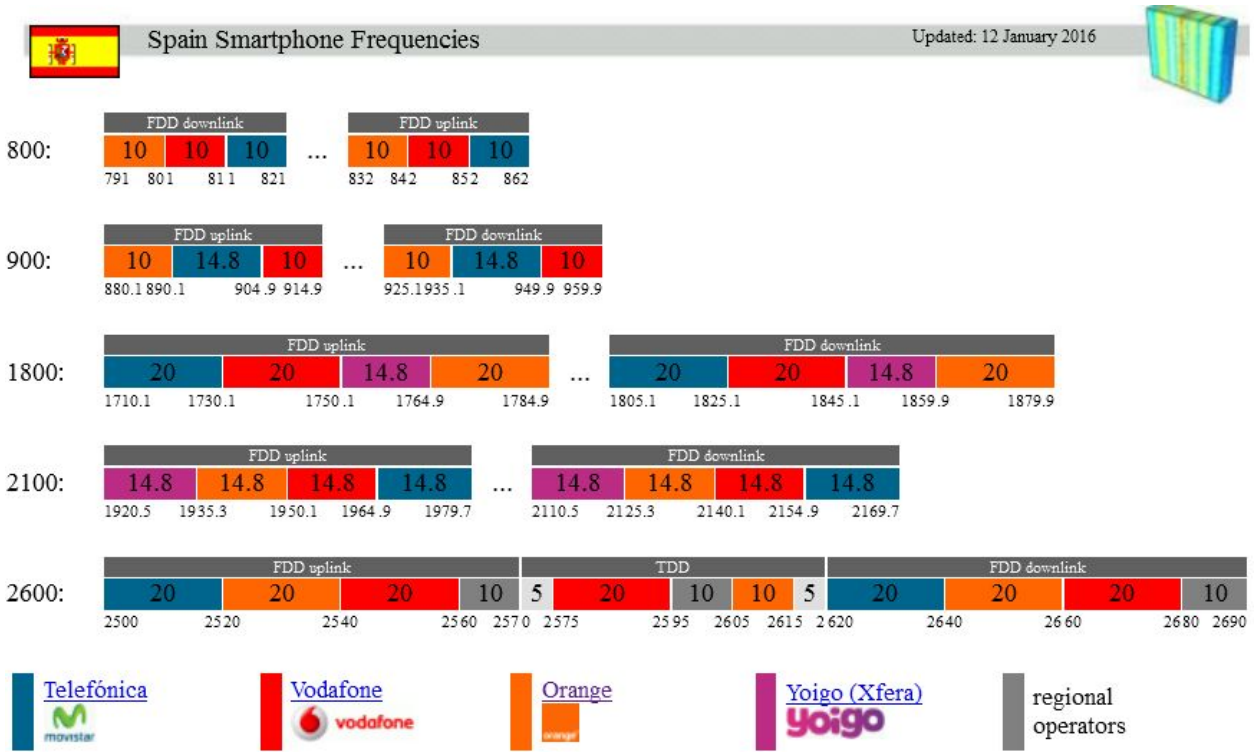


Figura 4: Reparto de frecuencias para el uso comercial [11]

Guiándose por la figura anterior, la banda de 900 MHz da servicio 2G / 3G; La banda 1800 MHz da servicio 2G y 4G; La banda 2100 MHz da servicio 3G.[6]

En el territorio español, son tres las posibles bandas LTE a utilizar, banda 20 (800 MHz), banda 3 (1800 MHz) y banda 7 (2600 MHz).

[6] El Real Decreto 458/2011 introdujo la neutralidad tecnológica en las bandas 900 y 1800 MHz, permitiendo la utilización para 3G y LTE de estas bandas inicialmente restringidas a las tecnologías 2G, y supuso una revalorización de las concesiones otorgadas [46].

Leyenda

Sin uso	En uso	En pruebas

Frecuencias y bandas LTE en España

Frecuencia (MHz)	Banda LTE	Frecuencias subida (MHz)	Frecuencias bajada (MHz)	Uso actual	Operadores
800	20	832-862	791-821	Utilizada para la difusión de televisión hasta el 31 de marzo de 2015 (ver dividendo digital), actualmente se emplea para telefonía móvil 4G/LTE.	Movistar, Orange, Vodafone
1500	32	-	1452-1492	Banda de solo bajada que saldrá a subasta pública próximamente.	-
1800	3	1710-1785	1805-1880	Actualmente se emplea para telefonía móvil 2G/GSM y 4G/LTE.	Movistar, Orange, Vodafone, Yoigo
2600	7	2500-2570	2620-2690	Actualmente se emplea para telefonía móvil 4G/LTE.	Movistar, Orange, Vodafone, varios

Figura 5: Frecuencias y bandas LTE en España [12][46]

A nivel estatal, sin contar las OMVs, existen cuatro operadoras que ofrecen servicio de LTE: Movistar, Orange, Vodafone y Yoigo. Las tres primeras cuentan con espectro en las tres bandas mientras que Yoigo sólo tiene licencia en 1800 MHz, por lo que no puede ofrecer *Carrier Aggregation*. Algunas operadoras regionales, p. ej. Telecable, Euskaltel o R cable, disponen también de concesiones a nivel regional u autonómico, para operar en la parte alta de la banda 2600 MHz. Nosotros hemos aprovechado la ausencia de estas operadoras regionales en Cataluña para los experimentos en el interior (zona cubierta). En el capítulo 5.3 volveremos a hablar sobre el uso de esta banda para las pruebas.

3. Plataforma OpenAirInterface - OAI

Dependiendo de qué estándar estamos interesados, existen varias opciones para implementar una estación base por medio del USRP. Nos encontramos con OpenBTS para GSM; OpenBTS-UMTS para WCDMA; en el caso del LTE, existen OpenLTE, srsLTE, OAI y Amarisoft LTE. Éste último es una solución comercial completamente funcional con altos costes en la implementación, mientras que los tres primeros son de código abierto, siendo OAI el más completo y popular, apoyado por una comunidad creciente, formado por instituciones educativas, operadoras, fabricantes y amateurs.

Bajo el contexto anterior, introducimos OpenAirInterface, un entorno software desarrollado por el consorcio no lucrativo OSA (OpenAirInterface™ Software Alliance) y patrocinado por Eurecom, una institución educativa francesa. Tiene como objetivo el desarrollo de un ecosistema de código abierto para el *core network* y para el acceso a la red E-UTRAN definidos por 3GPP. Proveen herramientas tanto a nivel software como hardware para la experimentación e investigación de tecnologías y nuevas redes futuras como el 5G, cloud-RAN o massive MIMO [13].

La plataforma OAI ofrece una implementación basada en software del sistema LTE, incluyendo toda la pila de protocolos del estándar 3GPP para E-UTRAN y EPC. Mediante esta plataforma podemos emular una estación base LTE (OAI *eNB*) y una red troncal (OAI *CN*), todo en un ordenador o distribuido en varios, conectando dispositivos móviles comerciales para probar diferentes configuraciones y ajustes de la red, a la vez que los monitoreamos en tiempo real. El software está escrito en C para Linux con *low-latency kernel* y optimizados para procesadores Intel x86 y ARM. Esbozaremos la arquitectura del escenario que hemos implementado en los siguientes capítulos, pero de manera resumida, con OAI la funcionalidad del transceptor se encarga el SDR *front-end* conectado a un ordenador host para el procesado, así como la conexión al *core network*. En la figura 6 se ilustra el diagrama del eNode B de nuestro testbed, o lo que es lo mismo, la conexión del USRP con el host PC, así como el rol que juega OAI eNB en relación con los otros componentes del sistema, los cuales se detallarán en las secciones siguientes.

El código fuente de OAI está organizado en diferentes directorios, que se puede condensar en:

- cmake_targets : sistema de configuración y compilación del Openair
- common : código común de todas las capas.
- openair1 : código de la capa física, scheduling y PHY abstraction para OAISIM.
- openair2 : código fuente de la capa 2(MAC, RLC, RRC, PDCP).
- openair3 : código intermedio o *middleware*.
- openair-cn : código de protocolos del core network.
- targets : código específico para ejecutables, contiene principalmente configuraciones y compilaciones antiguas del sistema.[14]

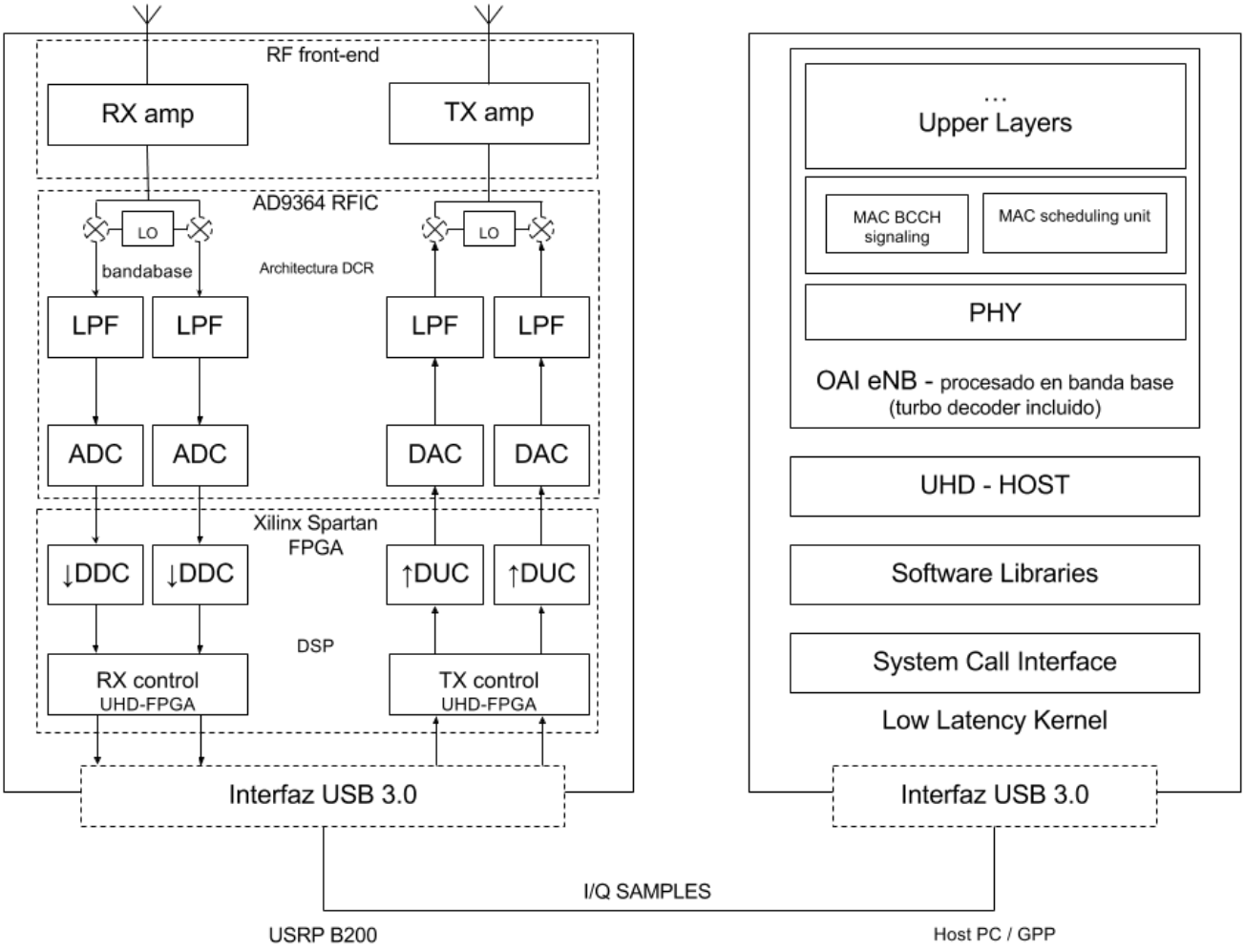


Figura 6: Diagrama del eNB implementado con conexión USRP - Host PC

3.1. Componentes Software que interactúan con OAI

3.1.1. El Kernel de Linux

El procesado de la señal banda base se realiza en software. El componente de software principal es el sistema operativo, el cual ofrece un entorno básico para la ejecución de las aplicaciones SDR, multitarea (multitask scheduling), manejo de interrupciones o gestión de memoria.

En este contexto, el procesado del SDR cobra especial importancia [15], que requiere de unos recursos computacionales que garantizan los estrictos márgenes de tiempo o *deadlines* que existe en LTE, como el TTI[7] de 1 ms que dictan los estándares para mantener una baja latencia [16][17].

Durante la ejecución de un proceso SDR, éste puede ser interrumpido por un cambio de contexto (*context switch*), por lo que es necesario darles mayor prioridad en el *multitask scheduling*.

3.1.2. UHD

El UHD, del inglés USRP Hardware Driver, es el controlador de software gratuito y de código libre destinado para la plataforma de SDR USRP. Ambos componentes (software y hardware) son desarrollados por Ettus Research, principalmente para Linux, aunque soporta los otros dos principales sistemas operativos. Algunos ejemplos de framework e instrumentos software que utilizan UHD son: GNU Radio, OpenBTS, Simulink o Amarisoft [18]. Gracias a los APIs de UHD, escritos en C++, se garantiza una gran adaptabilidad de los softwares anteriormente mencionados a los distintos modelos del hardware USRP.

La plataforma OAI utiliza, para el caso de dispositivos USRP, los APIs de UHD con el fin de establecer comunicación con las capas subyacentes y con el hardware. Estos APIs

[7] Transmission Time Interval, duración de una transmisión en el radio enlace.

controlan una gran cantidad de parámetros de USRP a bajo nivel, como puede ser controles de transporte (sockets UDP o LibUSB), identificación de dispositivos, ganancias, velocidad del reloj, etc. Sin duda es un recurso básico para los desarrolladores de plataformas como el OAI.

Todos los dispositivos USRP se cargan con un *firmware* especial e imágenes para el FPGA [19]. Esta acción se realiza al hacer la primera llamada de UHD, durante la ejecución del OAI. La carga se realiza una sola vez al inicio de los experimentos y permanece en la memoria del dispositivo hasta el apagado.

3.2. Plataforma Hardware

El escenario que implementamos está compuesto por varias piezas hardware, su elección está enfocado hacia la flexibilidad, la escalabilidad y el bajo coste, en comparación con las soluciones comerciales que implementan actualmente las operadoras. A continuación se detallan las principales piezas que componen los escenarios implementados.

3.2.1. Ordenador con procesador de propósito general

Eurecom especifica que para la ejecución del OpenAirInterface se requiere de ordenador con procesador de arquitectura Intel, debido a las funciones optimizadas del DSP, las cuales hacen un uso intensivo de las instrucciones SIMD[8]. Concretamente recomiendan las siguientes familias de procesador [47]:

Generation 3 Intel Core i5,i7
Generation 2 Intel Xeon
Intel Atom Rangely
Generation 4 Intel Core i5,i7

[8] Single Instruction, Multiple Data, técnica empleada para conseguir paralelismo a nivel de datos en computación.

3.2.2. USRP - modelo B200

USRP es una familia de productos SDR diseñados y fabricados por Ettus Research, compañía californiana subsidiaria de National Instruments desde 2010. Se pretende que sea una plataforma de software radio relativamente barata destinado a laboratorios de investigación, universidades y amateurs [21].

En este caso utilizamos el modelo USRP Ettus B200, presentado en la segunda mitad de 2013 para prototipar y experimentar estaciones base GSM mediante el software opensource OpenBTS [22]. Este modelo pertenece a la familia de los *Bus Series*, la cual utiliza una interfaz USB 2.0 o 3.0 para la transferencia de muestras con el host PC. Están diseñados para aplicaciones que no requieren tanto ancho de banda, en comparación con los modelos de la familia *Network Series* que utilizan en su caso conexiones de Gigabit Ethernet [23].

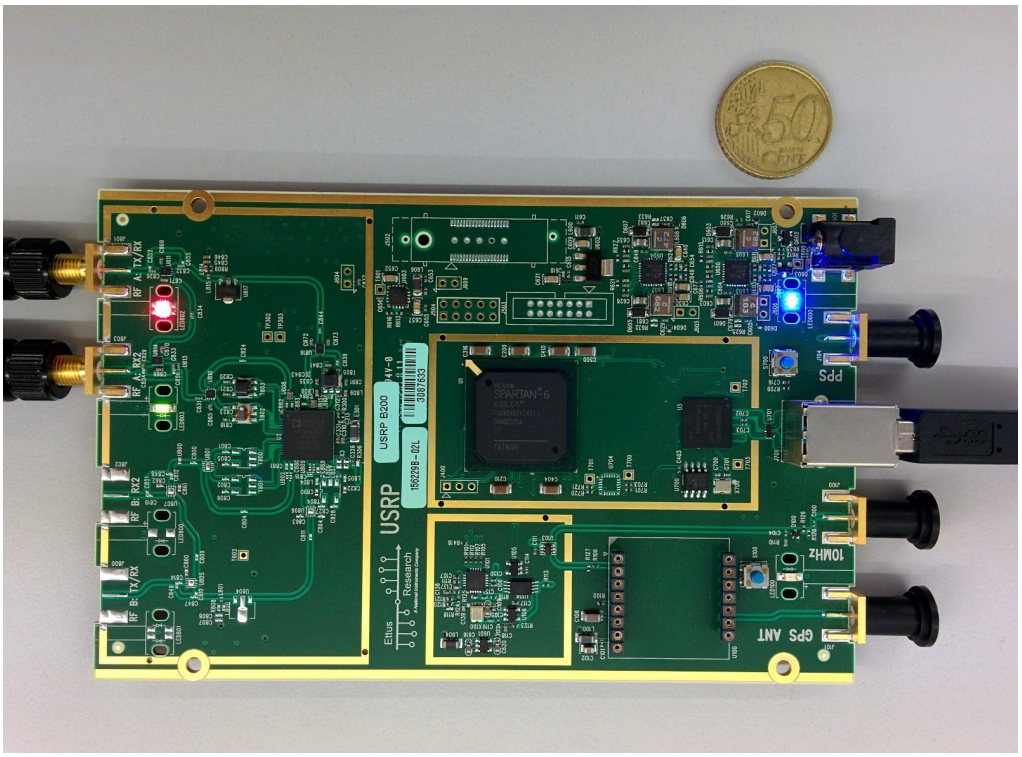


Figura 7: Dispositivo USRP B200

El B200 Consiste en una sola pieza de hardware que cubre un rango amplio de frecuencias, desde 70 MHz a 6 GHz. Contiene un transceiver de conversion directa [24], conocido también como sincrodino o *zero-IF*, que a diferencia de la arquitectura superheterodino, no utiliza una etapa de frecuencia intermedia, sino que la detección de la señal entrante se lleva a cabo mediante un oscilador local que funciona a una frecuencia muy cercana a la portadora. El oscilador que trae consigo tiene una precisión de ±2 ppm y ofrece la posibilidad de incorporar un oscilador externo como referencia.

También forma parte de la placa una FPGA[9] (del inglés Field Programmable Gate Array) modelo Xilinx Spartan-6, y una interfaz USB 3.0 para conectar al host PC y que sirve tanto para la transmisión de datos como alimentación en el caso de no utilizar un oscilador externo.

Como les mostramos en la figura 6, en el caso de utilizar la plataforma OAI con el dispositivo USRP B200, el procesado de la señal banda base no se realiza en el DSP[10] del FPGA, sinó en el host PC. Por otro lado, al tener el B200 una arquitectura de conversión directa, la etapa de DDC/DUC del FPGA no ejerce tampoco su función de traslación frecuencial (frequency shifting). Entre otras funciones, el DSP/FPGA se encarga del diezmado de los datos recibidos a la salida del ADC, e interpolación en la transmisión de éstos en la entrada del DAC.

A diferencia de su hermano mayor B210, que puede operar en 2TX 2RX (MIMO), el B200 funciona en modo 1 TX 1 RX, por lo que solo será posible el sistema SISO.

[9] Un FPGA es un chip de silicio reprogramable. A diferencia de los procesadores que se encuentra en un PC, al programar un FPGA el chip se vuelve a cablear (esto es, reconfigurar la interconexión de los bloques lógicos) para implementar su funcionalidad en lugar de ejecutar una aplicación de software [25].

[10] Del inglés *Digital Signal Processor*, microprocesador con la arquitectura optimizada para operaciones de procesado de señal digital, en especial aquellas operaciones en las que requieren un gran número de cálculos matemáticos de manera repetida y en un tiempo real.

3.2.3. Commercial off-the-shelf UE

UE (User Equipment) es un término heredado de las especificaciones de 3G/UMTS y se refiere al conjunto de equipo de terminal móvil. Está formado principalmente por los siguientes elementos:

- Mobile Equipment (ME): el dispositivo celular físico.
- UICC (Universal Integrated Circuit Card): conocido comúnmente como la tarjeta SIM (en sistemas GSM) y USIM (en sistemas UMTS y LTE), es el módulo de abonado que lleva las aplicaciones de USIM y la información para la provisión de servicio para el usuario final a través de tecnologías 3GPP.

Mediante esta separación entre terminal (ME) y tarjeta se permite que un usuario (identificado a través de la SIM/USIM) pueda utilizar diferentes terminales para acceder a la red. De esta manera también se dispone de dos identificadores diferentes:

- IMEI (International Mobile Equipment Identity): el identificador del equipo móvil.
- IMSI (International Mobile Subscriber Identity): provisionado por la tarjeta SIM, es el identificador del abonado de cara a la red celular. Está compuesto por MCC (Mobile Country Code), MNC (Mobile Network Code) y MSIN (Mobile Subscription Identification Number).

En la arquitectura EPS, el UE se encarga de aquellas funciones relacionadas con la interfaz radio en el lado del usuario, acceso a la red inalámbrica y transmisión de datos en general: gestión de movilidad, de sesión, de identificación y control de llamada. En la E-UTRAN, el UE se comunica directamente con el eNodeB por la interfaz radio Uu.

En este documento, referiremos al UE como sinónimo de ME. En consecuencia, un UE puede ser un ordenador conectado a un adaptador dongle que incorpora un módem y la SIM, o cualquier terminal móvil comercial. A continuación detallamos los aspectos del

equipo móvil utilizado, y en las siguientes secciones encontrarán información acerca de la programación de la SIM.

Hemos probado y trabajado con varios modelos diferentes de UEs comerciales, pero vamos a centrarnos con el Nexus 5 ZNFD821, que no lleva ningún software wrapper de terceros fabricantes (veremos más tarde que este detalle puede entorpecer las pruebas por la modificación de las bandas a escuchar a través del wrapper). Resumimos a continuación las principales características que nos atañe.

Conexiones móviles:

LTE Cat 4 (150/50 Mbit/s)
HSDPA+ (4G) 42.2 Mbit/s
HSUPA 5.76 Mbit/s
UMTS, EDGE, GPRS

Bandas FDD LTE:

800 (banda 20)
850 (banda 5),
900 (banda 8)
1800 (banda 3)
2100 (banda 1)
2600 (banda 7) MHz [26]

3.2.4. Antena

En alguna de las pruebas realizadas hemos utilizado dos antenas VERT900 de Ettus Research LLC, es de tipo omnidireccional y cubre las bandas 824 a 960 MHz y 1710 a 1990 MHz, con una ganancia de 3 dBi. Se recomienda el uso de duplexores para aislar las interferencias del Tx a Rx, necesarios para un rendimiento estable del OAI [50].

4. Implementación del testbed

4.1. Escenarios OAI

La plataforma OAI puede ser utilizado en diferentes configuraciones involucrando componentes comerciales en distintos grados:

UE comercial ↔ eNB comercial + OAI EPC
UE comercial ↔ OAI eNB + EPC comercial
UE comercial ↔ OAI eNB + OAI EPC
OAI UE ↔ OAI eNB + OAI EPC *
*OAI UE ↔ OAI eNB + EPC comercial**
*OAI UE ↔ eNB comercial + OAI EPC **
*OAI UE ↔ eNB comercial + EPC comercial**
*** Escenarios aún en fase de desarrollo por la comunidad* [28].

No disponemos de eNB o EPC comerciales en nuestro laboratorio, en consecuencia hemos tratado con aquellos escenarios en los que no intervienen estos elementos.

Para el caso del *OAI UE ↔ OAI eNB + OAI EPC*, optamos por utilizar dos dispositivos USRP B200, uno para actuar como UE, y el otro como eNB. Ambos están conectados al ordenador con GPP para el procesado. Sin embargo no pudimos establecer la conexión. Posiblemente sea debido a que esté aún en una fase temprana de desarrollo y haya fallos varios a corregir. De todas maneras, para descartar incidencias con el medio de propagación, sea ruido / interferencias, planteamos la posibilidad de conectar las dos placas directamente mediante cables sma-sma y simular así la interfaz *Uu* de LTE. Sin embargo desistimos por riesgo de causar daños en las placas al no disponer de un atenuador, aún bajando las ganancias del TX y RX [29].

El otro escenario que probamos fue UE comercial ↔ OAI eNB + OAI EPC. Conseguimos para este caso rendimientos más o menos aceptables que detallaremos en la sección de tests y resultados.

4.2. Instalación

La instalación de la plataforma OAI varía en función del escenario a implementar y la versión del programa. Explicaremos a continuación los pasos para instalar la versión master de su repositorio, que normalmente es la más estable de las existentes, y enfocado a un escenario de eNodeB y EPC instalados en un solo host-PC.

Tal como habíamos mencionado en el capítulo 3, por motivos de licencia, OAI se divide en OAI eNB y OAI CN. En cada parte existen scripts que automatizan y facilitan el procedimiento de instalación de las librerías y de recursos necesarios.

4.2.1. Requerimientos previos

Para la implementación hemos utilizado un ordenador con procesador de propósito general: Intel i5 de primera generación, cuatro núcleos, modelo 650 @ 3.20GHz. Cabe destacar en este punto que nos encontramos con la necesidad de puertos USB 3.0 de fabricantes específicos por la utilización del USRP B200. Esto es debido a que el USB 3.0 es una interfaz relativamente nueva, algunos controladores no se comportan de manera fiable frente a determinados dispositivos, como pueden ser los SDR, que transmite datos (*I/Q samples*) de manera contínua. En los casos de utilizar controladores no recomendados por el fabricante, muy posiblemente se pueda derivar a errores y comportamientos no esperados durante la ejecución del software, con los cuales difícilmente podemos hacer un diagnóstico adecuado.

Después de varios intentos y de pruebas fracasadas utilizando el controlador que vino de serie con la placa madre de nuestro ordenador, decidimos probar uno nuevo y adquirimos el de NEC Corporation modelo uPD720202, que según Ettus ofrece un rendimiento en el ratio de transferencia de muestras IQ de 39 MS/s, para el caso de 1 TX 1 RX [20]. Con el nuevo modelo solucionamos todos los comportamientos extraños del software y hardware, como el parpadeo intermitente de los LEDs o los mensajes de error como *RX overpowered*.

Como consecuencia del punto 3.1.1, más el hecho de ejecutar en un mismo host-PC todo el software necesario y por razones de compatibilidad, se ha optado por el uso de Ubuntu 64-bit 14.04 LTS, el mismo que utilizan la mayoría de la comunidad de OpenAirInterface, y 3.19.0-031900-lowlatency de kernel.

Para cambiar de kernel, podemos utilizar las siguientes líneas de comandos:

```
wget -r -e robots=off --accept-regex "(.*lowlatency.*amd64)|(all).deb"
http://kernel.ubuntu.com/~kernel-ppa/mainline/v3.19-vivid/
dpkg -i kernel.ubuntu.com/*/*/*/*deb
```

Por los mismos motivos, también procedemos a desactivar todas las características de gestión de energía en la BIOS, como los estados de hibernación o el escalado automático de frecuencia de CPU, dejándolo en modo máximo rendimiento. Para ello instalamos la siguiente utilidad:

```
sudo apt-get install cpufrequtils
```

Editamos el archivo de configuración:

```
sudo nano /etc/default/cpufrequtils
```

Y añadimos

```
GOVERNOR="performance"
```

Deshabilitamos el daemon para evitar el *rollback* de la configuración:

```
sudo update-rc.d ondemand disable
```

Comprobamos que el procesador está funcionando a máxima velocidad con el comando:

```
cpufreq-info
```

4.2.2. Instalación del OAI eNB

Una vez obtenido el código del OAI eNB en el gitlab de Eurecom[11], utilizamos los siguientes comandos para la instalación de los paquetes y librerías requeridos:

[11] https://gitlab.eurecom.fr

```
cd ~/openairinterface
source oaienv
cd cmake_targets
./build_oai -I -g --eNB -x --install-system-files -w USRP  --install-optional-packages
```

-I indica la instalación de paquetes requeridos
-g añade herramientas de debug
--eNB indica la instalación del eNodeB
-x añade la herramienta de software oscilloscope
--install-system-files instala los archivos de sistema requeridos por OAI
-w indica el soporte al hardware que vamos a utilizar
--install-optional-packages instala los paquetes opcionales

Durante la instalación del software adicional, es posible que los scripts descarguen e instalen versiones de UHD incorrectas, de la rama de desarrollo que implican inestabilidades durante la ejecución. Si es el caso, hemos de actualizar a la versión correcta.

Una vez instalados los paquetes necesarios, ejecutamos las siguientes líneas para la compilación:

```
cd ~/openairinterface5g
source oaienv
./cmake_targets/build_oai -w USRP -x -c --eNB
cd cmake_targets/lte_build_oai/build
```

Y ésta para la ejecución:

```
sudo -E ./lte-softmodem -O
$OPENAIR_DIR/targets/PROJECT/GENERIC-LTE-EPC/CONF/archivo_de_configuracion.conf
```

-c elimina los archivos de compilaciones anteriores
-O indica el archivo de configuración. Hablaremos de la configuración de cada entidad en el apartado 4.3 Configuraciones.

4.2.3. Instalación del OAI CN

De manera análoga, obtenemos el código del OAI CN del repositorio y ejecutamos los scripts para la instalación:

```
./build_epc -i
./build_hss -i
```

-i indica la instalación de paquetes requeridos para el CN, solo es necesario ejecutarlos la primera vez.

Posteriormente compilamos y ejecutamos HSS y EPC por separado:

```
cd ~/openair-cn
cd SCRIPTS
./build_epc -c -l
./run_epc
```

```
cd ~/openair-cn
cd SCRIPTS
./build_hss -c -l
./run_hss
```

-l indica que EPC y HSS se encuentran en un mismo host-PC.

La orden de ejecución de las diferentes entidades del EPS es importante en este caso. Primero hemos de arrancar el HSS, seguido de EPC y comprobamos que se establecen la conexión entre ellos. Seguidamente ejecutamos eNodeB. Si está todo correcto deberíamos de ver lo siguiente en la terminal:

```
...
[SCHED][eNB] Started eNB main thread on CPU 1 TID 5273
eNB_thread: mlockall in ...
eNB_thread: mlockall out ...
waiting for sync (eNB_thread)
TYPE <CTRL-C> TO TERMINATE
Entering ITTI signals handler
```

4.3. Configuraciones

Presentamos a continuación la configuración de parámetros y de las preparaciones necesarias para el escenario de UE comercial ↔ OAI eNB + OAI EPC.

OAI eNB y EPC poseen archivos de configuración diferentes en los que se puede regular varios parámetros físicos y de capas superiores.

4.3.1. eNodeB

Se puede encontrar principalmente con los siguientes parámetros:

- De identifiación: eNB_ID, cell_type, eNB_name, tracking_area_code, mobile_country_code, mobile_network_code.
- De la capa física: frame_type (FDD o TDD), eutra_band, downlink_frequency, uplink_frequency_offset, N_RB_DL, nb_antennas_tx/rx, tx/rx_gain.
- SRB: parámetros de tiempo de los *radio bearers* especiales.
- Parámetros de la interfaz de conexión.
- Y otros parámetros secundarios y niveles de log de las diferentes capas.

Detallamos en la siguiente tabla (figura 8) los valores de los parámetros más relevantes para el escenario que hemos implementado:

Parámetros de identificación	
eNB_ID cell_type eNB_name tracking_area_code mobile_country_code mobile_network_code	0xe00 "CELL_MACRO_ENB" "eNB_Eurecom_LTEBox" "1" "208" "93"
Parámetros físicos	
frame_type eutra_band downlink_frequency uplink_frequency_offset N_RB_DL nb_antennas_tx	"FDD" 8 930100000L -45000000 25 1

nb_antennas_rx tx_gain rx_gain pdsch_referenceSignalPower	1 90 125 -29
Parámetros de red	
mme_ip_address ENB_INTERFACE_NAME_FOR_S1_MME ENB_IPV4_ADDRESS_FOR_S1_MME ENB_INTERFACE_NAME_FOR_S1U ENB_IPV4_ADDRESS_FOR_S1U ENB_PORT_FOR_S1U	ipv4 = "192.170.0.1" "eth0:3" “192.170.0.2/24” "eth0:3" “192.170.1.2/24” 2152

Figura 8: Parámetros y valores del eNodeB

En la siguiente figura 9 se ilustra un ejemplo de las diferentes redes móviles que detecta nuestro UE, en función de los parámetros identificativos de la celda: Mobile Country Code y Mobile Network Code. Las operadoras que aparecen en la figura fueron detectadas en el módulo C5, en un entorno no aislado, ante un USRP B200 sin ninguna antena conectada.

En cuanto a parámetros físicos, hemos optado por utilizar FDD a razón de nuestros COTS UE[12], los cuales ninguno opera en modo TDD. El número de antenas en este caso es uno para TX y otro para RX, por la limitación de la propia placa que ya especificamos en el apartado 3.2.2, sólo opera en SISO. Los parámetros de ganancias controlan el atenuador regulable del USRP. Para el modelo que tenemos los valores óptimos fueron calculados por la comunidad OAI.

En otro entorno más aislado probamos de ejecutar el eNodeB con diferentes bandas y resource blocks, los resultados de los cuales se encuentran en los siguientes capítulos, así como la configuración de las interfaces de conexión con MME.

[12] Commercial off-the-shelf User Equipment, término utilizado para referir a los terminales móviles comerciales estándar que se vende para la población general.

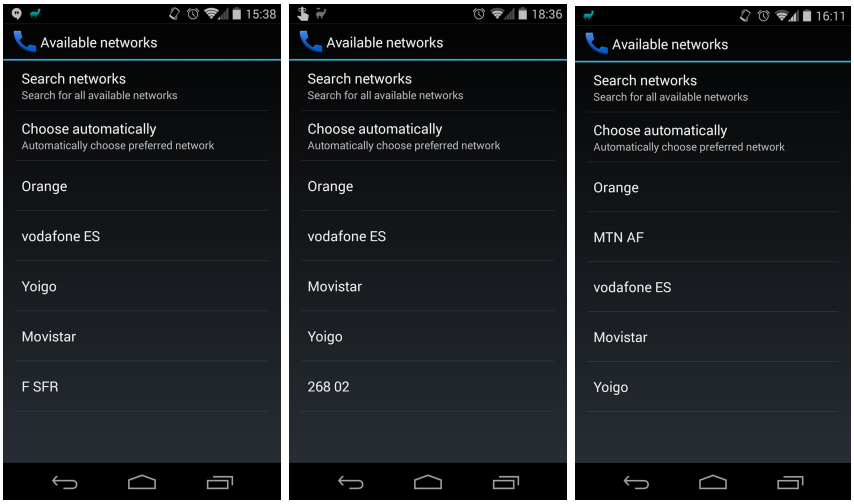


Figura 9: Redes móviles disponibles y detectables por el UE

4.3.2. Core Network - EPC

En el caso del core network, al estar agrupado diferentes partes de la red, el archivo de configuración *epc.conf.in* engloba los parámetros de MME, S-GW y P-GW. En la siguiente tabla se encuentran los principales:

REALM	string	Esfera de operación del protocolo Diameter. Es configurado durante la instalación del MME.
MAXENB	Num/Integer	Número máximo de eNB que puede conectarse a MME.
MAXUE	Num/Integer	Número máximo de UEs que MME puede servir. Para propósitos de depuración.
RELATIVE_CAPACITY	Num/Integer	Actualmente no es utilizado. Tendrá funciones de balanceo de carga de MME.
MME_STATISTIC_TIMER	Num/Integer	Período para mostrar estadísticas en logs.
EMERGENCY_ATTACH_SUPPORTED UNAUTHENTICATED_IMSI_SUPPORTED EPS_NETWORK_FEATURE_SUPPORT_IMS_VOICE_OVER_PS_SESSION_IN_S1 EPS_NETWORK_FEATURE_SUPPORT_EMER GENCY_BEARER_SERVICES_IN_S1_MODE EPS_NETWORK_FEATURE_SUPPORT_LOCATION_SERVICES_VIA_EPC	string	Actualmente solo soporta ‘no’.

EPS_NETWORK_FEATURE_SUPPORT_EXTENDED_SERVICE_REQUEST		
IP_CAPABILITY	string	Actualmente solo soporta IPV4. Posibles valores: IPV4, IPV4V6, IPV4ORV6
MME_CODE MME_GID	Array of Num/Intege	Parámetros de identifiación del MME. GUMMEI
TAI	Array of TAI (PLMN:TAC)	TAI=MCC.MNC:TAC Actualmente puede haber hasta 16 tracking areas identity en la lista. Pero no soportan redes compartidas, por lo que tienen que ser iguales.
S1AP_OUTCOME_TIMER	Num/Integer	Temporizador de abortar el procedimiento en curso y de liberar el UE si no se recibe respuesta de la petición.
S6A_CONF HSS_HOSTNAME	String	Parámetros de configuración para la interfaz S6A. Son configurados durante la instalación del MME.
ORDERED_SUPPORTED_INTEGRITY_ALGORITHM_LIST ORDERED_SUPPORTED_CIPHERING_ALGORITHM_LIST	Array of String	Lista de preferencias en orden decreciente, de los algoritmos de integridad y confidencialidad soportados. Actualmente soportan EEA0, EEA1, EEA2
ITTI_QUEUE_SIZE	Num/Integer	Límite superior del tamaño de la cola de mensajes expresado en bytes. Todos los mensajes intercambiados por las tareas tienen el mismo tamaño.
MME_INTERFACE_NAME_FOR_S1_MME MME_IPV4_ADDRESS_FOR_S1_MME MME_INTERFACE_NAME_FOR_S11_MME MME_IPV4_ADDRESS_FOR_S11_MME	String, CIDR	Direccionamiento del MME en las interfaces S1 y S11
SGW_INTERFACE_NAME_FOR_S11 SGW_IPV4_ADDRESS_FOR_S1 SGW_INTERFACE_NAME_FOR_S1U_S12_S4_UP SGW_IPV4_ADDRESS_FOR_S1U_S12_S4_UP SGW_IPV4_PORT_FOR_S1U_S12_S4_UP SGW_INTERFACE_NAME_FOR_S5_S8_UP SGW_IPV4_ADDRESS_FOR_S5_S8_UP	String, CIDR	Direccionamiento del SGW para diferentes interfaces. Las interfaces S5 y S8 no están implementadas aún.
DEFAULT_DNS_1_IPV4_ADDRESS DEFAULT_DNS_2_IPV4_ADDRESS	String, IPv4 dot decimal	Direcciones DNS IPv4 primario y segundario, que pueden ser requeridos por UEs.
PGW_INTERFACE_NAME_FOR_S5_S8 PGW_IPV4_ADDRESS_FOR_S5_S8 PGW_INTERFACE_NAME_FOR_SGI PGW_IPV4_ADDRESS_FOR_SGI PGW_MASQUERADE_SGI	String, CIDR	Direccionamiento del PGW para la salida a la red externa. Las interfaces S5 y S8 no están implementadas aún.
IPV4_LIST IPV6_LIST	String, CIDR	Pool de direcciones a repartir a los UEs

Figura 10: Parámetros de configuración del OAI EPC

4.3.3. HSS

Para el *home subscriber server* existe un fichero de configuración de nivel superior, *hss.conf.in*, que contiene todos los parámetros y enlaza a otros archivos de configuración. No es necesario ninguna modificación o customización porque el paso de variables se realiza durante la fase de compilación. Dicho fichero contiene las direcciones y logins de la base de datos del usuario.

Por otro lado, la base de datos se puede editar (operaciones SQL) mediante varias vías:

- Con la ayuda de por ejemplo phpMyAdmin.
- Vía línea de comandos *mysql*.

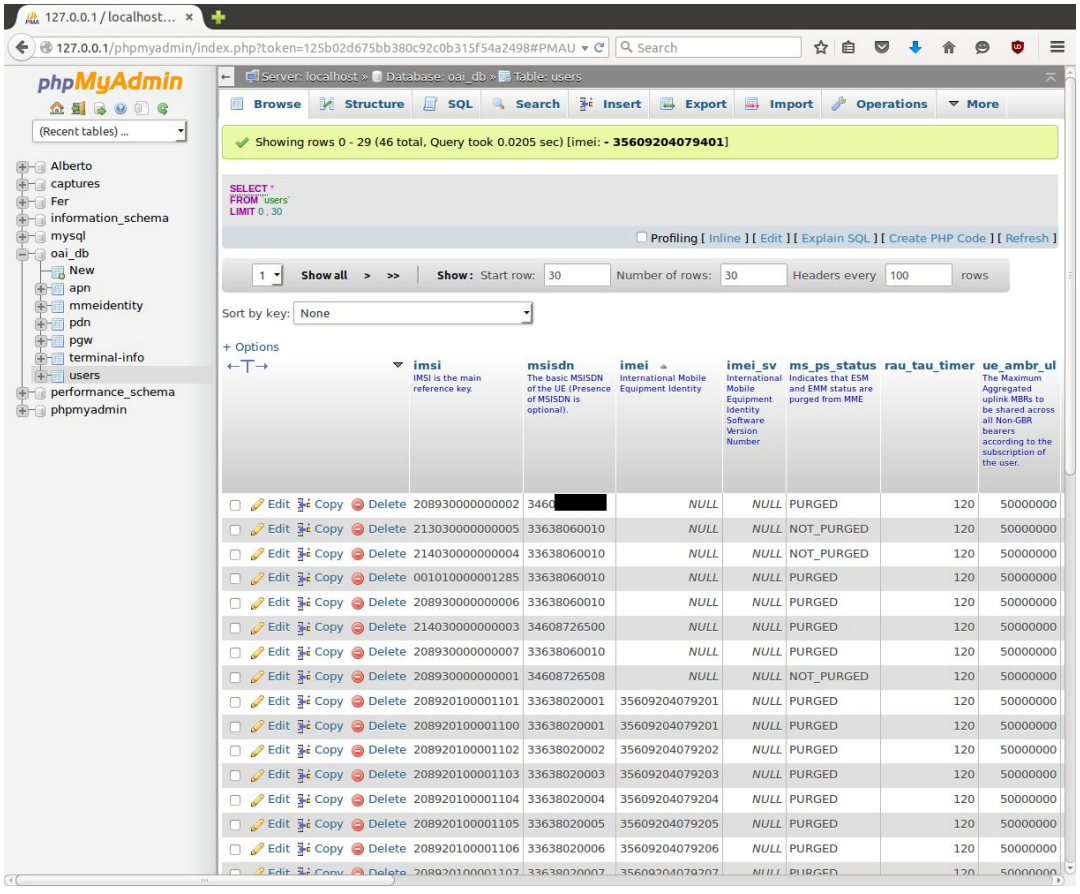


Figura 11: Base de datos para provisionar usuarios desde phpMyAdmin

Mediante phpMyAdmin[13] podemos añadir o modificar los diferentes parámetros de cada usuario de manera cómoda, como el imsi, OPc o K_i . Otros campos como el MSISDN figuran un valor cualquiera pues no implementamos ningún IMS o PSTN, los cuales utilizan estos valores para realizar, por ejemplo, llamadas vía VoLTE o por la conmutación de circuitos.

Si por el contrario optamos por provisionar los usuarios a través de la línea de comandos, podemos utilizar las siguientes instrucciones:

```
shell > mysql -u root -p
mysql > use oai_db;
mysql >

INSERT INTO users (`imsi`, `msisdn`, `imei`, `imei_sv`, `ms_ps_status`,
`rau_tau_timer`, `ue_ambr_ul`, `ue_ambr_dl`, `access_restriction`, `mme_cap`,
`mmeidentity_idmmeidentity`, `key`, `RFSP-Index`, `urrp_mme`, `sqn`, `rand`, `OPc`)
VALUES ('208930000000001',  '34666777888', NULL, NULL, 'PURGED', '120', '50000000',
'100000000', '47', '0000000000', '3', 0x8BAF473F2F8FD09487CCCBD7097C6862, '1', '0', '',
0x00000000000000000000000000000000, '');
```

El OPc se computa automáticamente al ejecutar HSS, a partir de los datos introducidos.

4.3.4. USIM

En el despliegue del testbed LTE que queremos implementar, son necesarias tarjetas SIM para el usuario final. La obtención y programación de estas tarjetas no es trivial gracias a las mejoras de seguridad que ofrece LTE con respecto a tecnologías antecedentes (como la autenticación mutua) y que el proyecto OAI haya respetado el estándar 3GPP. Con las herramientas adecuadas podemos programarlas por nuestra cuenta o bien conseguirlas a través de terceras partes.

Tres elementos son necesarios para su programación [30]:

- Tarjeta USIM programable con soporte a Milenage.

[13] Herramienta gratuita y open source, escrita en PHP, destinada a administrar MySQL mediante el uso de un navegador web.

Muchas de las 'Test SIMs' que hay actualmente en el mercado para el testeo de 3G/4G utilizan el algoritmo XOR o '*dummy*'. El cual es diferente del Milenage, ampliamente utilizado en el despliegue de redes 3G/4G.
Milenage es un algoritmo de autenticación e intercambio de claves basado en AES-128. Reemplaza el deficiente COMP128-1 del 2G[14] [31].
Dependiendo del proyecto, como el OpenBTS (GSM y UMTS), se ofrece e implementa la opción de utilizar tarjetas que soporten A3/A8/comp128 [32]. Pero otros como OAI se requiere del Milenage por su carácter *3GPP compliant*.

De estas tarjetas USIM con soporte Milenage, con el objetivo de aprovisionarse en el HSS es necesario conocer dos claves importantes, el OPc y el K_i . OPc es la clave principal formada a partir de OP[15] y de K_i (Subscriber secret key) utilizando el algoritmo de cifrado RijndaelEncrypt (AES) [33].

- Hardware capaz de realizar lectura y escritura de la tarjeta.
  Para este punto tenemos dos restricciones:
  i. Que tenga soporte APDU, del inglés *Application Protocol Data Unit*, datagrama de comunicación lógica entre un lector de tarjetas inteligentes y una tarjeta inteligente. Dependiendo del tipo, *command / response*, es capaz de transportar hasta 260 / 258 bytes de datos. Su estructura está definida en los estándares ISO/IEC 7816.

  ii. Que sea compatible con la implementación de la especificación para tarjetas inteligentes PC/SC (abreviatura de Personal

[14] Los algoritmos COMP128 son implementaciones de los algoritmos A3 y A8 definidos en el estándar GSM.

[15] OP es el código de la operadora utilizada para la generación de claves en 3G y 4G. Se pasa este valor como input al algoritmo RijndaelEncrypt para generar OPc. Para un atacante con conocimiento de OP, es posible que pueda suplantar a todos los SIMs de la operadora. Si se conoce OPc, único para cada SIM, tan solo puede suplantar a la SIM con el OPc conocido.

Computer/Smart Card)[16], gratuita en Linux con nombre PC/SC Lite.

Bajo estas condiciones y guiándose por las recomendaciones de la comunidad de openLTE, optamos por utilizar el lector Scm Microsystems SCR3310V2 (figura 12).[17]

Figura 12: Lector / Escritor de tarjetas inteligentes Scm Microsystems SCR3310V2

- Software para la programación de las SIMs.

  Al igual que en otros ámbitos, podemos diferenciar dos tipos de software:

  i. Propietarios: como el Card Admin de Gemalto, el cual se requiere de Licencia para su uso, con un coste monetario relativamente elevado.

  ii. Open source, gratuito, compuesto por tres aplicaciones: PySIM, PCSCd, Pyscard. Consiste en módulos y herramientas python que en conjunto dan soporte a PC/SC y permiten la programación de las USIM.

[16] Algunos ejemplos de miembros del grupo de trabajo (workgroup) PC/SC son: Gemalto, NXP, Realtek o Toshiba.

[17] Otros ejemplos los podemos encontrar en esta lista http://pcsclite.alioth.debian.org/ccid/supported.html

Optamos primero por adquirir los USIMs blancos con soporte al algoritmo Milenage a través de un popular portal de vendedores chinos. Sin embargo en el servicio de post-venta nos informan que no dan soporte a las aplicaciones de Linux anteriores y que en principio solo sería compatible con su hardware Bludrive II CCID Smart Card reader/writer y su software particular.

Como sistema de redundancia, pedimos al mismo tiempo tarjetas USIM a la compañía sueca Smartjac, especializada en tarjetas inteligentes. En este caso, con la información de los parámetros que les proporcionamos, personalizaron los SIMs. Sin embargo no todas las tarjetas del pedido funcionaban, tuvimos diferentes problemas con algunos, como bloqueo por códigos PIN y errores en las fases de autenticación en la interfaz S6a [18] (posiblemente debido a algún error en la fase de programación de las tarjetas SIM).

El resultado final es que tenemos 3 USIMs que funcionan, dos con la identificación PLMN 208 93 y uno con la 213 03.

4.3.5. APN

APN es el nombre identificativo del gateway o punto de acceso a la red y determina, para el caso de LTE, el PGW que el UE debe utilizar. También define el túnel conectando el UE al PDN, como puede ser internet [34][35]. La información del APN se mantiene en el HSS, o dicho de otra manera, este último contiene la información de los APN que el usuario puede conectarse.

En nuestro testbed, al haber sólo un PDN, se emplea una etiqueta simple configurado en el HSS. Posteriormente, también lo configuramos en el UE, indicando de manera explícita el APN en cuestión, Bearer LTE y protocolo IPv4.

[18] S6a es la interfaz entre MME y HSS, está basada en el protocolo Diameter, que ofrece servicios AAAS (Authentication, Authorization and Accounting with Secure Transport). [3GPP TS 29.272][RFC 6733]

4.3.6. Sistema operativo del UE

Hemos utilizado Android KitKat 4.4.4 como sistema operativo en el UE, que ofrece un entorno relativamente limpio, sin softwares adicionales de fabricantes específicos que pueda entorpecer de alguna manera a la recepción de señales. Éste último es el caso de algunos terminales que proporcionan determinados proveedores de telecomunicaciones. Por ejemplo hemos aprendido de la comunidad de OAI que los Samsung S4 de AT&T, a pesar de ser móviles libres y desbloqueados, sigue teniendo un software-wrapper, o un firmware modificado con propósitos de eficiencia energética que tiene como consecuencia no escuchar determinadas bandas, pese a que el dispositivo tiene la capacidad de hacerlo [27].

4.4. Diagrama del escenario configurado

La siguiente figura representa el diagrama de bloques de los diferentes componentes del EPS que hemos configurado. Como se observa es una configuración basada en un único host PC, es decir, el eNB y los diferentes módulos del *core network* se encuentran en el mismo equipo host-PC.

En este aspecto OAI ofrece la posibilidad de ejecutar eNB y CN en equipos diferentes, conectados a través de ethernet. De esta manera se reparte el uso de recursos hardware. Esta liberación de recursos repercute principalmente en el procesado de la señal banda base en el eNB, siendo uno de los procesos que más CPU consume. Como *trade-off* o contrapartida para el caso distribuido, estaríamos ganando latencia en la transmisión, una limitación muy restrictiva por los estándares LTE y más aún en el futuro 5G. En nuestro caso hemos utilizado interfaces virtuales para simular la conexión (interfaces S1-MME y S1-U) entre estas entidades en el mismo host. Presentamos en la figura 13 la configuración implementada.

Por otro lado, las conexiones entre entidades que forman el EPC o SAE Core utilizan el sistema de comunicación y sincronización entre tareas (inter-task communication) gestionado por el propio sistema operativo y no pasa por la capa de red. Existen

propuestas en la comunidad OAI de, por ejemplo, separar y ejecutar MME y los GW en servidores separados, pero aún en fase de desarrollo.

Generalmente configuramos las direcciones IP de de la arquitectura anterior mediante los archivos de configuración de OAI eNB y OAI CN. En este último se especifica también el rango de direcciones que tendrán los UEs asociados a la red, así como los servidores DNS que se asignan por defecto, en nuestro caso el DNS de la UPC como primario y el famoso de Google como secundario.

En el lado opuesto, configuramos la interfaz SGi con la IP pública del host PC. Por esta conexión el PDN Gateway se conecta a otras redes, que en nuestro caso sería la red de la UPC / internet.

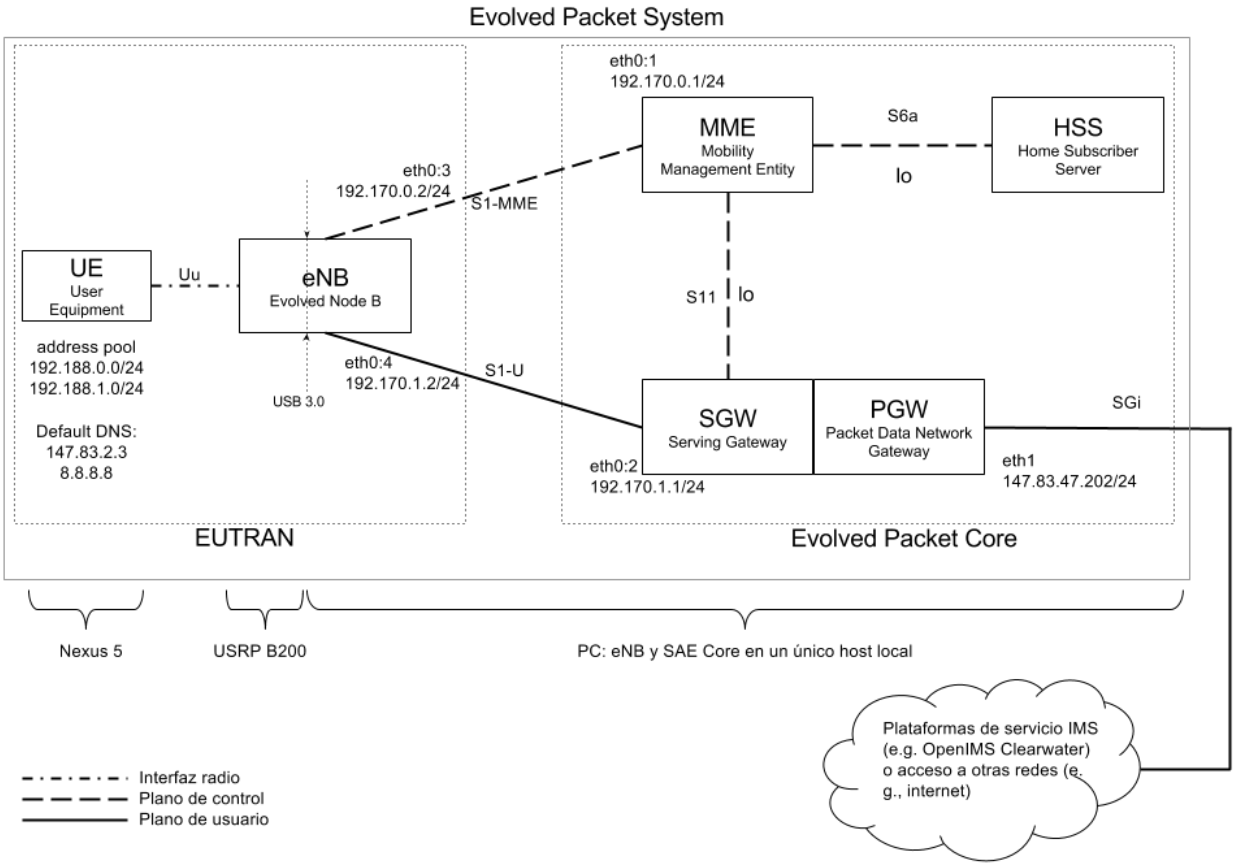


Figura 13: Arquitectura a nivel de IP del escenario implementado [19]

[19] Pueden encontrar un resumen de los stacks de protocolos de los diferentes interfaces S1 en el anexo 8.1.

5. Retos del entorno real

5.1. Uso del espectro para los experimentos

A diferencia de las simulaciones realizadas en un ambiente controlado, hacer pruebas en un entorno real suelen conllevar retos que acarrean situaciones y resultados no esperados por diferentes factores externos y que pueden no ser contemplados en una primera evaluación.

Para poder llevar a cabo los experimentos en este entorno, una de las primeras tareas que intentamos realizar al inicio del proyecto fue la de solicitar el uso frecuencial, con motivo de investigación, al organismo competente, en este caso la SETSI, amparado por el Ministerio de Industria, Energía y Turismo.

La resolución de dicha solicitud, con número 2015-0144753, fue

> *(...) que no existe disponibilidad actual para asignar nuevas frecuencias en las bandas deseadas, por lo que la única alternativa es que contacte con alguno de los operadores actuales con asignación de frecuencias en dichas bandas y sea a través de ellos quienes les proporcionen los recursos frecuenciales con la que poder llevar a cabo las tareas de investigación/docencia. (...)*

Ante la anterior respuesta y la pasividad por parte de las operadoras, consideramos otras opciones para llevar a cabo los experimentos sin incumplir ninguna regulación. Optamos finalmente por realizar las pruebas con antena en el sótano del edificio C3 de Campus Nord, y las pruebas sin antena en el despacho habitual del módulo C5. Destacamos aquí la relativa baja potencia de emisión del USRP B200, 10 dbm (10 mW), frente a, por ejemplo, de los 20 dbm (100 mW) PIRE del estándar IEEE 802.11 en sus enmiendas para la banda del 2,4 GHz.[20]

[20] CNAF, UN - 85 Banda 2400 a 2483,5 MHz

5.2. CPU insuficiente

Aunque no haya sido un punto demasiado crítico para nuestros experimentos, hemos visto que nuestro PC host no ofrecía el rendimiento suficiente en términos de capacidad de cálculo, a pesar de utilizar low latency kernel o habilitar el modo *performance* del CPU. Durante la ejecución del OAI eNB, el proceso mostraba por pantalla flags U y flags L que indican lo siguiente:

U flag, de *underrun* o *underflow*: ocurre cuando el host PC no genera o produce datos / muestras lo suficientemente rápido, dicho de otra forma, el host no puede mantener la demanda de *samples* que requiere el USRP. Cuando el UHD detecta este estado, muestra por stdout "*U*"s. [36]

L flag, de *late packet*: de igual manera, es un indicador que avisa de un paquete / *sample* desincronizado (desfasado / entrega tardía) en el punto de control del USRP (DSP) en donde se decide si se rechaza, descarta o acepta para su transmisión. Esto suele ocurrir cuando hay un desfase en el timestamp de las muestras con el clock del FPGA, fenómeno conocido como *time drifting*, generalmente es causado por la peor calidad del clock del host PC [37].

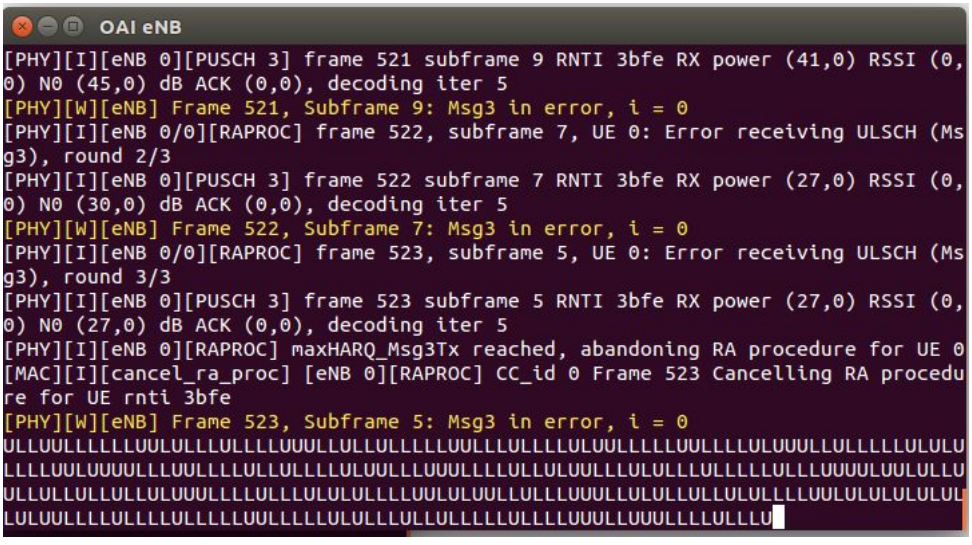


Figura 14: Situación de underrun y late packet

En cualquier caso este descarte de paquetes (*packet dropping*) suele ser significante después de períodos de ejecución contínua (de OAI) muy largos.

5.3. Inestabilidad de la señal de eNB

En nuestras primeras pruebas de la plataforma OAI hemos visto que la señal de la operadora de test no es estable, traducido en apariciones y desapariciones de la señal en el escaneo de operadoras por parte del UE, de manera aleatoria e independiente de las dos localizaciones en donde hemos realizado las pruebas. E incluso, en algunas frecuencias o bandas (especialmente en las bandas altas), el UE no detecta la operadora en ningún momento.

Una primera hipótesis fue que estaríamos ocupando frecuencias comerciales en uso. Por ende nos volvemos a asegurar de estar usando una frecuencia en la que no opera ninguna proveedora de servicios: 2685 MHz[21] (banda 7).

Recurrimos al Servicio de información sobre Instalaciones Radioeléctricas y Niveles de Exposición de la SETSI, de donde obtuvimos información detallada de las estaciones de telefonía móvil que hay alrededor de nuestra localización (figura 15).

[21] Como ya mencionamos en el capítulo 2.2, en esta parte de la banda operan algunas compañías de servicio regionales o autonómicos, fuera de Cataluña.

Figura 15: Estaciones de telefonía móvil que proporciona servicio al Campus Nord [38]

En la siguiente tabla resumimos las emisiones de las estaciones anteriores.

Código y referencias	Dirección / banda asignada (MHz)
VODAFONE ESPAÑA, S.A. - 155695	CL JORDI GIRONA, 1. BARCELONA, BARCELONA
B B -1600014 B B -1600009 B B -1600010 B B -1600012 B B -1600013	949.90 - 959.90 842.00 - 852.00 1825.10 - 1845.10 949.90 - 959.90 1905.00 - 1910.00; 2140.00 - 2155.00
TELEFONICA MOVILES ESPAÑA, S.A.U. - 0800942	PZ EUSEBI GÜELL, 6. BARCELONA, BARCELONA
B B -0900936	1910.00 - 1915.00; 2155.00 - 2170.00
VODAFONE ESPAÑA, S.A. - 011481	AV ESPLUGUES, 92. BARCELONA, BARCELONA
B B -1301505 B B -0430111 B B -0431465	1825.10 - 1845.10 1905.00 - 1910.00; 2140.00 - 2155.00 1825.10 - 1845.10
ORANGE ESPAGNE, SAU - CATR3023B	AV ESPLUGUES, 92. BARCELONA, BARCELONA
B B -0600159 B B -1201674 B B -1201683 B B -1400180 B B -0700568	1900.00 - 1905.00; 2125.00 - 2140.00 925.10 - 935.10 925.10 - 935.10 2640.00 - 2660.00 1859.90 - 1879.90
XFERA MOVILES SA - 1B2B0212	CL SOR EULALIA D'ANZIZU, 11. BARCELONA, BARCELONA

B B -1100515 B B -1200432 B B -1301097	1915.00 - 1920.00; 2110.00 - 2125.00 1845.10 - 1859.90 1845.10 - 1855.10
TELEFONICA MOVILES ESPAÑA, S.A.U. - 0800199	CL DE SOR EULÀLIA D'ANZIZU, 11. BARCELONA, BARCELONA
B B -0431991 B B -0431992 B B -1200005 B B -1400949 B B -0431993	935.10 - 949.90 1805.10 - 1825.10 939.70 - 944.70 1805.10 - 1825.10 1910.00 - 1915.00; 2155.00 - 2170.00
ORANGE ESPAGNE, SAU - CATR0510J	CL DE SOR EULÀLIA D'ANZIZU, 11. BARCELONA, BARCELONA
B B -0430893 B B -1201534 B B -1400051 B B -0432881 B B -1201527	1900.00 - 1905.00; 2125.00 - 2140.00 925.10 - 935.10 2640.00 - 2660.00 1859.90 - 1879.90 925.10 - 935.10

Figura 16: Bandas asignadas de las estaciones de telefonía móvil en la zona de Campus Nord (mayor de 2016)

Como pueden ver, la frecuencia de operación en la que trabajamos, siempre a baja potencia, no coincide con ninguna banda comercial en las cuales operan las estaciones cercanas. Por otro lado, siguiendo los consejos de la comunidad OAI también utilizamos la herramienta *cell_search* de srsLTE[22] y el USRP para hacer un escaneo en la banda 7 de las estaciones comerciales, con el mismo resultado obtenido a través de la administración. En la figura 17 se ilustra el resultado de dichos escaneos, que corresponde a los EARFCN de las estaciones base de Orange, ninguno de los cuales se interponen en la frecuencia 2685 MHz.

Por ello nos hizo dudar de esta hipótesis y continuar con las del siguiente apartado.

[22] srsLTE es una librería de LTE y opensource, destinada a SDR, organizada de manera modular y desarrollada por SoftwareRadioSystems. [39]

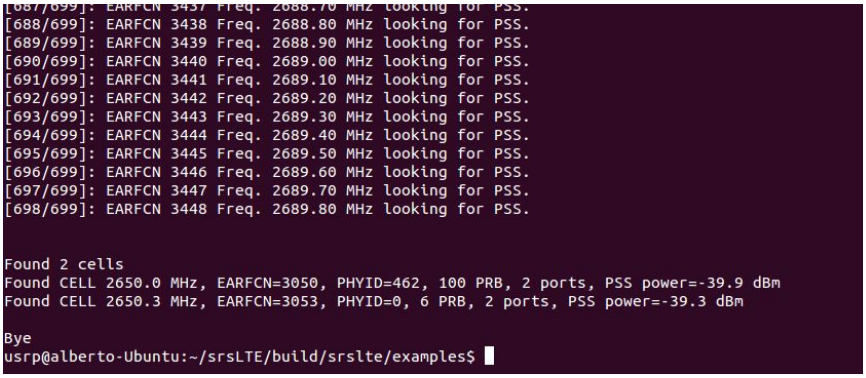


Figura 17: Resultado de los escaneos en la banda 7 mediante el USRP y srsLTE

5.4. Exactitud frecuencial

Del proyecto OpenBTS[23] aprendemos que el problema de la 'visibilidad' entre el UE y la estación base puede ser debido a la exactitud frecuencial [40]. De la misma manera que con GSM, en LTE se utiliza la misma tecnología de osciladores para la sincronización de los dispositivos.

Según el estándar 3GPP TR 36.922 [41] release 10, esto es LTE-A, para aquellos eNodeBs considerados macro celdas, que soportan handovers de hasta 350 km/h, recomiendan una precisión frecuencial de ±0.05 ppm[24]. En el mismo estándar establece que para aquellos eNodeBs destinados a zonas interiores, Home eNodeBs, al limitarse la velocidad máxima que puede alcanzar el UE, también se relaja las restricciones del error frecuencial que puede tolerar. Así pues, para una frecuencia de operación en la banda de los 2600 MHz, se recomienda para el Home eNodeB una precisión de ±0.34 ppm.

[23] En el Anexo 9.3 podrán encontrar una breve explicación anecdótica de la implementación de Node B utilizando el software OpenBTS-UMTS.

[24] La tolerancia en la frecuencia se refiere a la máxima desviación permitida y se expresa en partes por millón (ppm). Un error de 0.05 ppm se traduce a 45 Hz en las bandas bajas (850/900 MHz) y 90 Hz en 1800/1900 MHz, siendo estas cantidades consideradas muy precisas y son típicas de osciladores disciplinados por GPS.

En el lado del equipo móvil, durante el encendido 'en frío' de un UE, sin haberse sincronizado con un reloj externo previamente, el dispositivo hace un escaneo barriendo todo el rango de frecuencias utilizando la variación (*frequency drift*) de su propio reloj hasta encontrar una señal de sincronización (PSS y SSS)[25], y a partir de aquí calcular el PCI (*Physical layer Cell Identity*). Una vez detectado la señal de sincronización, corrige su oscilador local para sincronizarse contra la estación base. A partir de este punto, si se pierde la señal de la operadora, el UE en lugar de escanear todo el rango nuevamente, calcula el *frequency drift* para el peor caso y deja de escanear si encuentra una señal de sincronismo. Podemos clasificar los efectos de la desincronización dependiendo del grado de error en el reloj [40]:

- Efecto de los errores frecuenciales moderados (500 Hz a pocos kHz)

En este caso, el eNodeB de test opera con una precisión frecuencial con la que el UE es capaz de sincronizar, pero difiere de los operadores locales reales por unos pocos cientos hertzios. Como consecuencia el UE muestra primero las operadoras que ha detectado, ya sea las reales o la de test, e ignora el resto.

- Efecto de los errores frecuenciales considerables (varios kHz o más)

Para este punto, el error que induce el eNodeB es tan grande que permanece fuera del rango de frecuencias que puede calcular el UE con los *frequency drifts* de su oscilador local. Por lo que el UE simplemente no encuentra a la operadora de test.

Estos errores provocados por el oscilador del USRP y el UE pueden variar con la edad de los dispositivos y la temperatura, por lo que el comportamiento de los fallos pueden ser diferentes según el aparato y el tiempo de ejecución, por ejemplo a medida que se calientan o enfrían, o que la resincronización de las tramas puede seguir políticas diferentes dependiendo del modelo de UE. Todo ello puede originar síntomas difíciles de diagnosticar.

En nuestro escenario no consideramos el desplazamiento frecuencial por el efecto Doppler (que implica ICI y la pérdida de la ortogonalidad de las subportadoras del

[25] Primary / Secondary Synchronization Signals.

OFDM) pues no hemos realizado las pruebas en movimiento. A pesar de las pruebas en posición estática, la precisión del USRP B200 es de ±2 ppm, y si trabajamos en el 2685 MHz, tendría unos errores máximos de ±5370 Hz. En el peor de los casos esto implicaría que el UE no puede detectar la señal de test independientemente de las operadoras comerciales (punto dos anterior). A medida que bajamos la frecuencia de operación (que supone una disminución del error máximo), parece ser que este efecto se diluye y hay más posibilidades de verse a nuestra señal de eNodeB. No hemos podido demostrar con certeza esta hipótesis sin un entorno totalmente aislado (p.e. cámara anecoica) para el primer punto, o utilizar un oscilador externo de mejor calidad para el segundo punto, aunque los diferentes efectos y resultados que hemos visto apuntan a los fenómenos anteriores.

6. Pruebas y resultados

Después de montar el escenario y de tratar con las incidencias, tanto las de configuración como las del apartado anterior, comprobamos que la red provisiona correctamente el UE una vez establecida la conexión y que efectivamente obtiene acceso a la red exterior. Mediante las siguientes pruebas comprobamos los distintos aspectos de la conexión y analizamos algunos intercambios de paquetes entre las diferentes entidades que forma el EPS.

La figura 18 ilustra el estado RRC_RECONFIGURED[26] del UE en el lado del eNodeB, que indica el correcto establecimiento de los servicios portadores radio de señalización[27].

La figura 19 ilustra una captura de pantalla en el UE cuando se ha realizado correctamente las operaciones de *network attach*, la operadora en este caso es UPC por el SPN (Service Provider Name) especificado en la USIM. Por consiguiente, durante el escaneo de redes en el UE, seguiremos viendo el PLMN[28] que hemos especificado en el archivo de configuración del eNodeB, que en este caso particular es 208 93.

---

[26] Después de que el UE inicie un procedimiento de acceso aleatorio, envía un mensaje de *RRC Connection Request* que incluye el motivo de la petición y una identificación temporal del móvil. Si el eNB acepta la petición de conexión, envía como respuesta un mensaje del tipo *RRC Connection Setup* que incluye los parámetros de configuración inicial de la portadora radio SRB1. Al recibir el mensaje anterior, el UE envía un mensaje, al NAS, de reconocimiento (*RRC Connection Setup Completed*) que incorpora el identificador PLMN del operador móvil seleccionado. Completada esta fase el UE pasa de estado RRC desocupado (*RRC-Idle*) al estado RRC conectado (*RRC-connected*). Y continúa con la fase de activación de los mecanismos de seguridad: eNB envía el mensaje de activación del modo de seguridad (*Security Mode Command*) para solicitar la activación del modo cifrado y de los mecanismos de protección de integridad. Esta fase se completa con el mensaje *Security Mode Completed* enviado por el UE. Entonces la red envía la petición de reconfiguración de la conexión RRC (*RRC-Connection Reconfiguration*), que incluye los parámetros de configuración para establecer el segundo servicio portador radio de señalización (SRB2) y una o más servicios portadores radio de datos (DRB). El terminal móvil completa el procedimiento enviando un mensaje de reconfiguración completada (*RRC-Connection Reconfiguration Complete*). Establecidos los servicios portadores radio de señalización, ya se puede pasar a configurar una o varios servicios portadores radio de datos (DRB). [48]

[27] Los servicios portadores radio (Radio Bearers, RB), son servicios de transferencia entre un eNB y un UE, necesarios para establecer cualquier tipo de transferencia de información entre ellos. Estos servicios han sido diseñados específicamente para soportar tráfico IP. La conexión de control se soporta mediante el protocolo RRC, a través del cual gestionan, entre otros servicios, el establecimiento, modificación y liberación de los servicios portadores radio entre el eNB y UE.

[28] Public Land Mobile Network, compuesto por Mobile Country Code (MCC) y Mobile Network Code (MNC), es el código identificador de la operadora.

```
        </nonCriticalExtension>
    </nonCriticalExtension>
</UE-EUTRA-Capability>
[RRC][I]RRCConnectionReconfiguration Encoded 797 bits (100 bytes)
[RRC][I][eNB 0] Frame 4763, Logical Channel DL-DCCH, Generate RRCConnectionReconfiguration (bytes 100, UE id b075)
[SCTP][I][sctp_send_data] Successfully sent 82 bytes on stream 1 for assoc_id 50
[RLC][I][FRAME 04763][eNB][MOD 00][RNTI b075][SRB AM 01] RLC_AM_DATA_REQ size 105 Bytes,  NB SDU 1 current_sdu_index=5 next_sdu_index=
6 conf 0 mui 2
[RRC][N][eNB 0] Frame 617: received a DCCH 1 message on SRB 0 with Size 2 from UE b075
[RRC][I][FRAME 04765][eNB][MOD 00][RNTI b075] Received on DCCH 1 RRC_DCCH_DATA_IND
[RLC][I][FRAME 04765][eNB][MOD 00][RNTI b075] [DRB 1] rrc_rlc_add_rlc  DRB
[RRC][I][eNB 0] Frame  4765 : Logical Channel UL-DCCH, Received RRCConnectionReconfigurationComplete from UE rnti b075, reconfiguring
DRB 1/LCID 3
[RRC][I][eNB 0] Frame  4765 : Logical Channel UL-DCCH, Received RRCConnectionReconfigurationComplete from UE 0, reconfiguring DRB 1/LC
ID 3
[MAC][I][rrc_mac_config_req] [CONFIG][eNB 0/0] Configuring MAC/PHY for UE 0 (b075)
[PHY][I]phy_config_dedicated_eNB: physicalConfigDedicated=0x7f2208001600
[RRC][I][FRAME 04765][eNB][MOD 00][RNTI b075] UE State = RRC_RECONFIGURED
[SCTP][I][sctp_send_data] Successfully sent 43 bytes on stream 1 for assoc_id 50
[PHY][I][eNB 0] Frame 619: Sent physicalConfigDedicated=0x7f2208001600 for UE 0
[RRC][N][eNB 0] Frame 619: received a DCCH 1 message on SRB 0 with Size 16 from UE b075
[RRC][I][FRAME 04766][eNB][MOD 00][RNTI b075] Received on DCCH 1 RRC_DCCH_DATA_IND
[SCTP][I][sctp_send_data] Successfully sent 64 bytes on stream 1 for assoc_id 50
[SCTP][I][sctp_eNB_flush_sockets] Found data for descriptor 46
```

Figura 18: Mensaje de log del eNB (host PC) indicando RRC_RECONFIGURED

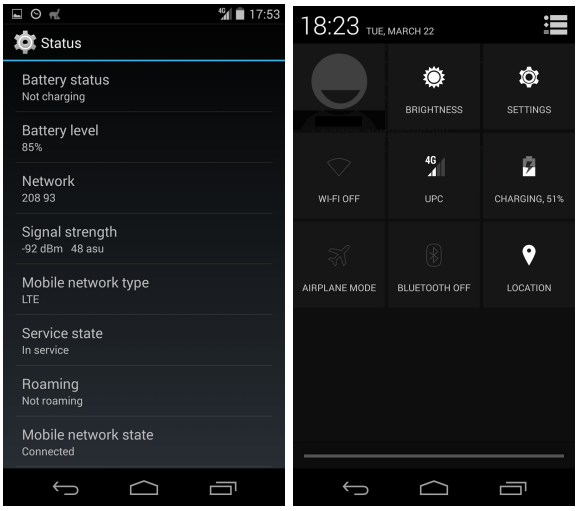


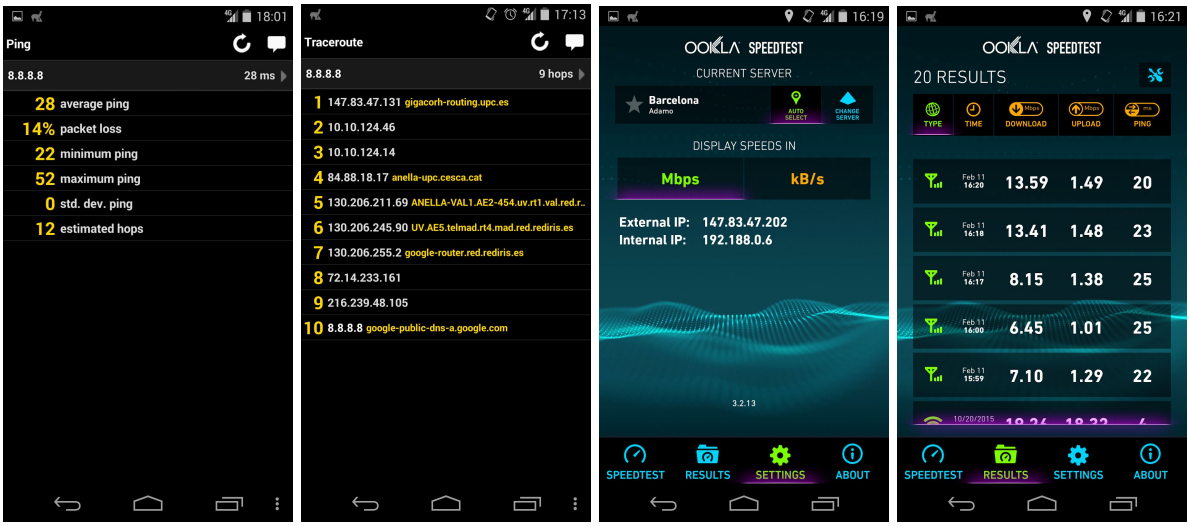
Figura 19: Capturas en el UE una vez establecida la conexión con eNB

6.1. Pruebas de conectividad y de rendimiento

6.1.1. Ping / Traceroute

Las primeras pruebas que realizamos fueron con el comando ping / traceroute para comprobar la conectividad y el tiempo de respuesta de un ICMP Echo Reply.

Existen multitud de aplicaciones que realizan esta función, muchas veces integradas directamente en aplicaciones de medición de velocidad de transporte de datos (*throughput*). A continuación pueden ver algunos ejemplos:



a) *b)* *c)* *d)*

Figura 20: Ejemplos de Ping, Traceroute y Speedtest a redes externas

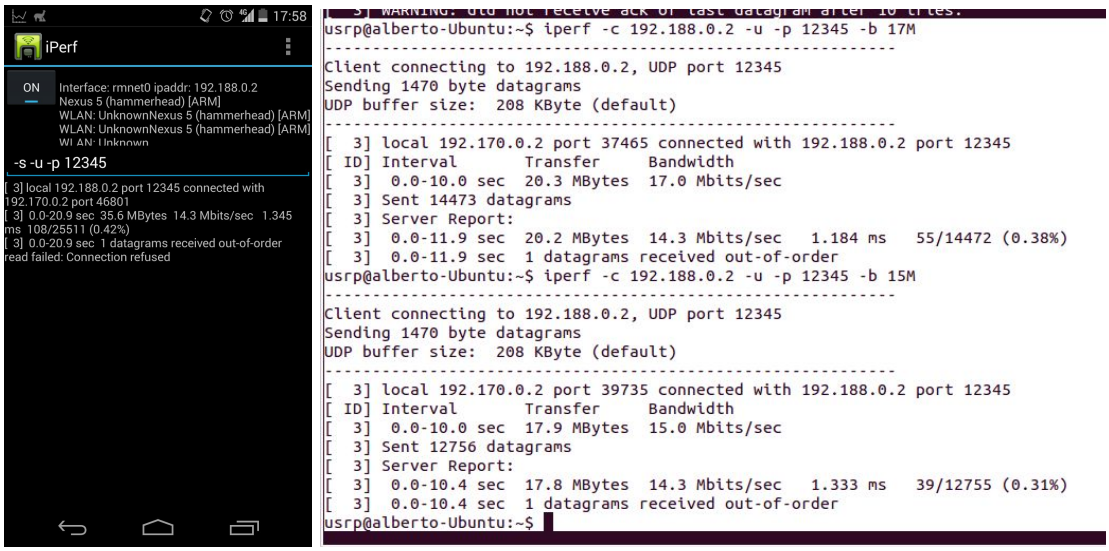
En la figura 20 se muestran capturas de pantalla de diferentes aplicaciones en el lado del UE. Las capturas a) y b) corresponden a las métricas del ping y traceroute para comprobar la conectividad hacia el DNS primario de Google. Observamos que hay un 14% en la pérdida de paquetes, los pings varían entre 22 y 52 ms y el camino seguido es el que seguiría cualquier ordenador del laboratorio, pasando por la red troncal de alta velocidad, *l'Anella Científica*. La pérdida de paquetes se produce, posiblemente, en la interfaz radio Uu. Otra posibilidad es que el host-PC no ha podido cumplir con los requerimientos de tiempo real (*real time constraints*) por sus recursos limitados. En la captura podemos observar la IP interna del UE asignada por el EPC, así como la de la salida a la red exterior, es decir, la IP de la interfaz SGi del P-GW, que corresponde a la IP pública de nuestro host-PC. En la captura d) se ilustra la velocidad del Downlink y Uplink contra un servidor externo (determinado automáticamente por la aplicación según localización), fuera de la red de UPC. La baja velocidad que alcanza en el Uplink es debido a un bug de OAI que se solventó más tarde. También hemos observado que estas velocidades, es decir, el rendimiento de la red, depende en gran medida del consumo de recursos del host PC. Por ejemplo, para un ancho de banda de 5 MHz, sin

ejecutar la función del *software oscilloscope*, se alcanza en Downlink los 16 Mbits/s. Y si activamos esta funcionalidad la velocidad se disminuye hasta la mitad o más.

6.1.2. Iperf

Para independizarse de las fluctuaciones que puede haber en los nodos intermedios de la red exterior y con el objetivo de hacer mediciones en la interfaz *Uu* solamente, utilizamos la herramienta Iperf para medir el Uplink y Downlink.

En el lado del UE, la interfaz de línea de comandos no es accesible a simple vista, por lo que instalamos la aplicación *iPerf for Android*, que ejecuta correctamente los comandos de la aplicación. Elegimos siempre el protocolo UDP para evitar las ventanas de control de congestión del TCP. Para el Downlink el UE actúa como iPerf servidor y el host PC como cliente, con salida por la interfaz virtual eth0:3 (referir a la figura 13: Arquitectura a nivel de IP del escenario implementado). Para el Uplink lo configuramos de manera inversa.



a) *b)*

Figura 21: Test de throughput en el Downlink mediante iPerf

La figura 21 ilustra un ejemplo de medición del throughput en el Downlink, sin antenas conectadas y con el UE al lado del eNodeB. La captura a) corresponde al UE en modo servidor y la captura b) el eNode B como cliente. En la siguiente tabla resumimos los

principales resultados que obtuvimos con diferentes parámetros de eNodeB y calidad de señal.

N_RB_DL	bandwidth MHz	RSSI dBm	RSRP dBm	RSRQ dB	throughput DL (Mb/s)	throughput UL (Mb/s)
6	1.4	too many 'U' and 'L' flags, carrier not visible.				
15	3	[PHY][E]Unsupported N_RB_DL 15				
25	5	-65	-79	-4	16.6	1.7
25	5	-75	-89	-3	16.5	1.69
25	5	-85	-98	-4	12.2	1.69
25	5	-96	-108	-5	5.5	0.91
25	5	-111	-118	-9	3.3	0.309
50	10	-70	-83	-4	10.3	1.62
50	10	-75	-89	-4	10.3	
50	10	-85	-98	-4	7.22	
50	10	-100	-108	-7	7.7	
50	10	-112	-118	-9	5.36	
75	15	bandwidth not supported in band 8				
100	20	bandwidth not supported in band 8				

Figura 22: Resultados de tests de velocidad según ancho de banda, medidas de intensidad y calidad de la señal recibida en el UE

En la tabla anterior se muestran las velocidades que obtuvimos según ancho de banda configurada y calidad de señal (medida con la app TestelDroid del PlayStore de Android) sin conectar ninguna antena. La primera columna corresponde al número máximo de *Resource Blocks*[29] en Downlink, parámetro configurable en el eNodeB y que se relaciona directamente con la canalización (segunda columna). Cada fila corresponde a los diferentes niveles de potencia de señal para un determinado ancho de banda. Estos niveles los obtuvimos alejando y acercando el UE del eNodeB.

[29] PRB (Physical Resource Block) consiste en el mínimo elemento de información que puede ser asignado por el eNB a un UE. Un PRB ocupa 180 KHz de banda equivalente a doce sub-portadoras equiespaciadas 15KHz entre ellas. En función de la longitud de prefijo cíclico utilizada, se transmiten 6 ó 7 símbolos OFDMA en el PRB. La duración de un PRB es igual a 0,5 ms, que equivale a la duración de un slot o ranura temporal.

El RSSI (Received Signal Strength Indicator) es la potencia de portadora LTE observada por el UE, está formada por la potencia recibida de la celda servidora y celdas no servidoras en la misma portadora LTE, la interferencia de canal adyacente y el ruido térmico. El RSRP (Reference Signal Received Power) se mide como el promedio lineal sobre las potencias recibidas de los REs[30] que transportan la *Reference Signal*[31] del eNodeB. Proporciona una estimación de la fuerza de la señal recibida y se puede utilizar para la toma de decisiones en los procedimientos de handover.

Se define RSRQ (Reference Signal Received Quality) como $RSRQ = \frac{N_{PRB} * RSRP}{RSSI}$ Esta medida de la calidad de señal recibida es una estimación de la relación señal a ruido más interferencia observada por el terminal para una determinada celda.

Volviendo a la explicación de la figura 22, observamos que para el ancho de banda 1.4 MHz existen demasiados *Late packet* y *Underrun*, y no es posible la detección de la señal de eNodeB por parte de UE. Actualmente OAI no soporta ejecuciones para el ancho de banda de 3 MHz. Para las bandas de 5 y 10 MHz observamos que evidentemente las velocidades decrecen a medida que empeora la calidad de la señal recibida. El rendimiento del ancho de banda de 10 MHz es inferior al de 5 MHz, posiblemente sea debido a 1) bugs del programa OAI, o bien 2) directamente relacionado con las prestaciones de nuestro equipo. Sólo pudimos medir el Uplink de esta banda para el mejor caso. Porque si forzamos solo un poco las condiciones incrementando la distancia entre ellos, la conexión sufre caídas inmediatamente, debido quizás a un fallo en el *Power loop control*, según uno de los desarrolladores de OAI. Los anchos de banda de 15 y 20 MHz no son soportados para las frecuencia en las que trabajamos sin antena, 942.5 MHz y 930.1 MHz.

Posteriormente tratamos de tomar medidas con el USRP conectado a dos antenas VERT900, en el sótano del módulo C3, donde es más aislado de las operadoras

[30] Resource Element: subportadora OFDM en un determinado símbolo OFDM dentro de un time-slot.

[31] Reference Signal: señales piloto transmitidos en el downlink y utilizados por el UE para realizar estimaciones del canal de downlink. Estas señales son moduladas utilizando QPSK para hacerlas resistente a ruido y errores, y llevan uno de los 504 identidades celulares.

comerciales. A falta de un duplexor para evitar las interferencias del Tx a Rx, realizamos las mediciones con dos disposiciones de antena distintas, y siguiendo el mismo criterio anterior de variar la distancia entre eNodeB y UE para conseguir los diferentes niveles de potencia. El primero en posición ortogonal entre ellas y el segundo en paralelo. Como se observa en la figura 23, se consigue mejor rendimiento para la disposición ortogonal, aunque no alcanza en ningún momento las velocidades máximas del caso anterior. Las casillas en blanco corresponden a casos en los que no pudimos estabilizar el nivel de señal deseado (demasiada variación en un corto período de tiempo con una separación determinada). Así pues, utilizando las antenas, evidentemente ganamos en área de cobertura, aproximadamente la longitud de dos aulas de laboratorio, en comparación con el caso sin antenas, en donde el área de cobertura no se extiende más allá de la mesa de trabajo. Los resultados muestran también que utilizar las antennas en la formación paralela causan más errores en la recepción del eNodeB y como consecuencia obtenemos menor velocidad. Esto es debido a la interferencia del Tx hacia Rx y que muestra la necesidad de un duplexer.

VERT900 in 90º formation						
N_RB_DL	bandwidth MHz	RSSI dBm	RSRP dBm	RSRQ dB	throughput DL (Mb/s)	throughput UL (Mb/s)
25	5	-31	-45	-3	14.3	1.3
25	5	-41	-55	-3	14.3	1.3
25	5	-61	-75	-3	13.3	1.3
25	5	-65	-79			
25	5	-75	-89	-3	13	1.1
25	5	-83	-98	-4	12.5	1
25	5	-96	-109	-5	10.6	0.05
25	5	-111	-118			
VERT900 in parallel setup						
25	5	-35	-48	-3	13.1	1.3
25	5	-41	-55	-3	8.3	1.3
25	5	-61	-75	-3	8.8	1.3
25	5	-65	-79	-3		0.63
25	5	-75	-89	-3	6.07	0.12

25	5	-83	-98	-4	4.6	0.4
25	5	-96	-109	-7	4	0.1
25	5	-111	-118			

Figura 23: Resultados de tests de velocidad con antenas en diferentes distribuciones

6.2. Análisis de procedimientos LTE mediante herramientas de observación y de depuración

En este apartado estudiamos diferentes procedimientos del LTE mediante las herramientas integradas en OAI, que a su vez sirve de apoyo en los procesos de desarrollo, análisis y resolución de incidencias. Debido a los limitados recursos del host PC, hemos visto que el uso de estas herramientas durante la ejecución del software SDR puede empeorar notablemente el rendimiento general del sistema, por lo que no se recomienda su uso para, por ejemplo, las pruebas de *throughput*.

6.2.1. Message Sequence Charts Generator

MSCGEN es un programa que crea estructuras y diagramas de secuencia de mensajes (Message Sequence Charts) a partir del análisis de textos que describen entidades e interacciones durante un período de tiempo concreto [42]. La plataforma OAI utiliza esta herramienta para ofrecer otra visión de los eventos que ocurren durante la ejecución del software, más concretamente los sucesos a partir del nivel de S1-AP[32] del stack de protocolos. A continuación encontrarán el análisis de un ejemplo de los diagramas creados por esta herramienta: el procedimiento de registro (Network Attach)[33] del UE a la red, visto desde el punto de vista del *Core Network*.

Para utilizar esta herramienta, antes hemos de cambiar a 'True' la variable CFLAG MESSAGE_CHART_GENERATOR del archivo OPENAIRCN_DIR/BUILD/EPC/CMakeLists.template. Una vez realizado el cambio

[32] S1-AP (S1 Application Protocol), protocolo de la capa de aplicación entre el eNode B y MME. Se trata de una de las interfaces del plano de control.

[33] La realización del registro en la red LTE es necesaria para que el usuario pueda iniciar o ser contactado para proceder a la activación de un servicio.

anterior, hemos de utilizar el argumento `-m ruta_de_archivos_generados` al ejecutar el Core Network.

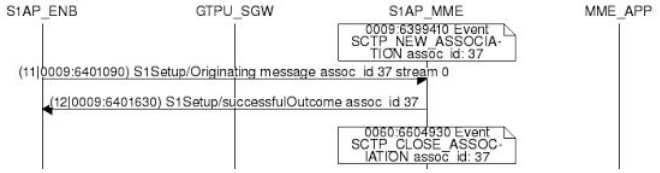


Figura 24: MSCGEN: establecimiento de la conexión eNB - MME

En la figura 24 se ilustra el Message Sequence Chart (MSC) del sincronismo entre eNode B y el MME durante el inicio de la ejecución de ambos procesos. El siguiente texto en plano corresponde a dicho MSC:

```
msc {
        width = "2048";
          S1AP_ENB, GTPU_SGW, S1AP_MME, MME_APP, NAS_MME, NAS_EMM, NAS_ESM,
        SP_GW_MME, S6A, HSS;
          S1AP_MME note S1AP_MME [ label = "0009:6399410
         Event SCTP_NEW_ASSOCIATION assoc_id: 37", textcolour="black" ] ;
          S1AP_MME<=S1AP_ENB [ label = "(11|0009:6401090) S1Setup/Originating message assoc_id 37
        stream 0", linecolour="black" , textcolour="black" ] ;
          S1AP_MME=>S1AP_ENB [ label = "(12|0009:6401630) S1Setup/successfulOutcome assoc_id 37",
        linecolour="black" , textcolour="black" ] ;
          S1AP_MME note S1AP_MME [ label = "0060:6604930
         Event SCTP_CLOSE_ASSOCIATION assoc_id: 37", textcolour="black" ] ;
}
```

Una vez establecida esta conexión del eNB contra el EPC, el UE ya puede iniciar el proceso de *attach*.

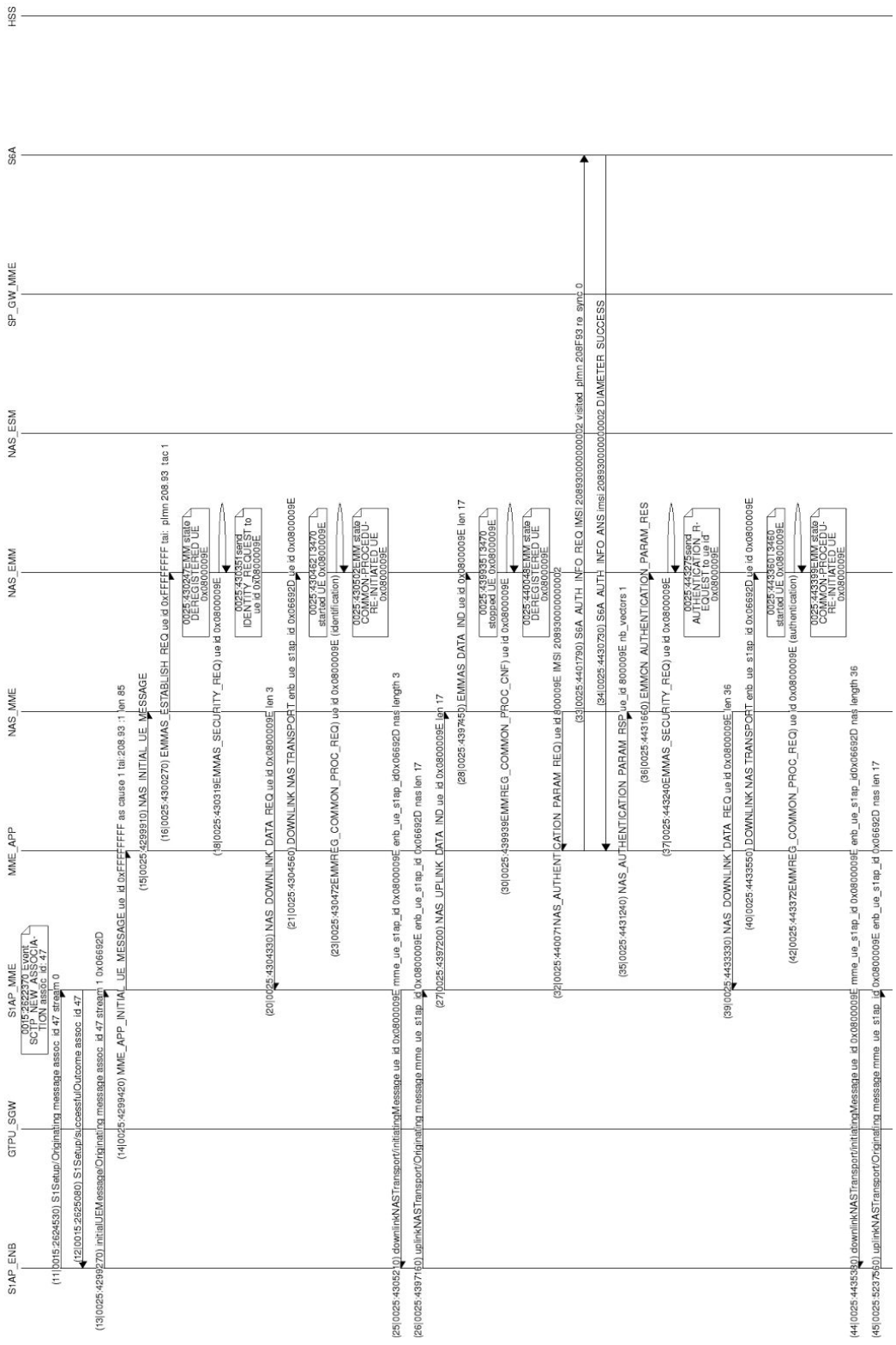


Figura 25: MSCGEN: Inicio del procedimiento de registro (Network Attach) observado desde el CN

La figura anterior es la primera de las tres figuras que ilustran el procedimiento de registro en el CN. Las flechas indican una llamada de función o método. En este caso no se puede observar las interacciones del eNB con UE en la interfaz Uu (protocolo RRC y otros protocolos subyacentes), por lo que las etapas de inicio del procedimiento o las del acceso aleatorio no se muestran mediante MSCGEN. Observamos en la figura 25 que el eNode B recibe el mensaje inicial del UE (tercer evento en la figura) y lo redirige al MME por la interfaz S1AP. El *thread* S1AP_MME a su vez inicia las llamadas de función pertinentes del protocolo NAS, que para este caso concreto de *Network Attach* serían las del protocolo EMM, el cual gestiona la accesibilidad a los servicios de la red LTE de los usuarios.

Posteriormente, hacia la mitad de la misma figura anterior, vemos que se inician los procedimientos que permiten a la red interrogar al equipo terminal para el envío de identificadores como el IMSI (International Mobile Subscriber Identity) y llevar a cabo la autenticación del usuario (EPS Authentication and Key Agreement, AKA), que permite la autenticación mutua entre usuario y red LTE así como el establecimiento de una clave maestra, K_{ASME} , a partir de la cual se derivan las claves de cifrado e integridad [43], la figura 26 ilustra este procedimiento AKA.

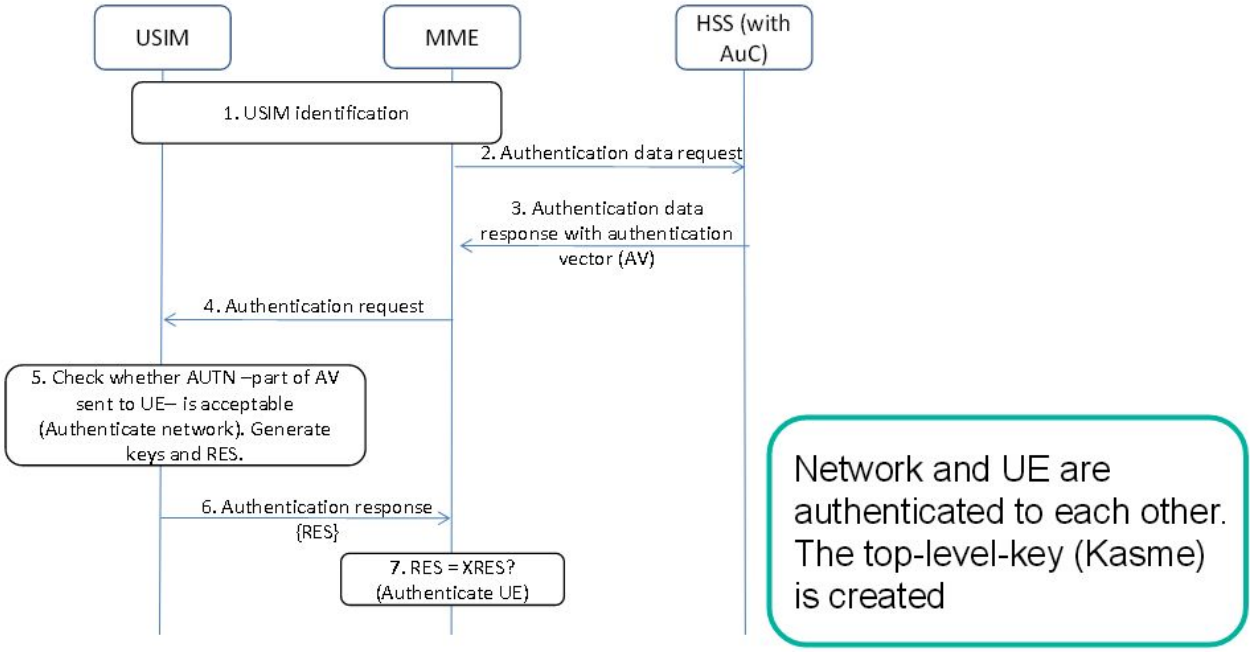


Figura 26: EPS Authentication y Key Agreement (AKA) [44]

El proceso comienza con MME solicitando el vector de autenticación al HSS, que en nuestro caso, en la figura 25, correspondería a la “comunicación” MME_APP con S6A. El HSS computa el *Authentication Vector* a partir de los datos como el tipo de tecnología de acceso, IMSI, PLMN o Sequence Number, y lo distribuye al MME.

Más tarde el MME envía al UE la petición de autenticación de usuario (que puede ser la USIM). Este último realiza las verificaciones necesarias para determinar el estado (*freshness*) y el origen del *Authentication Vector*. Si es todo correcto, el UE genera el parámetro de respuesta, XRES, y otras dos claves, con las cuales obtiene la clave K_{ASME}. Por último el terminal responde con el parámetro XRES proporcionado por la USIM, para la comprobación por parte del MME. Si todo es correcto se considera que el usuario ha autenticado.

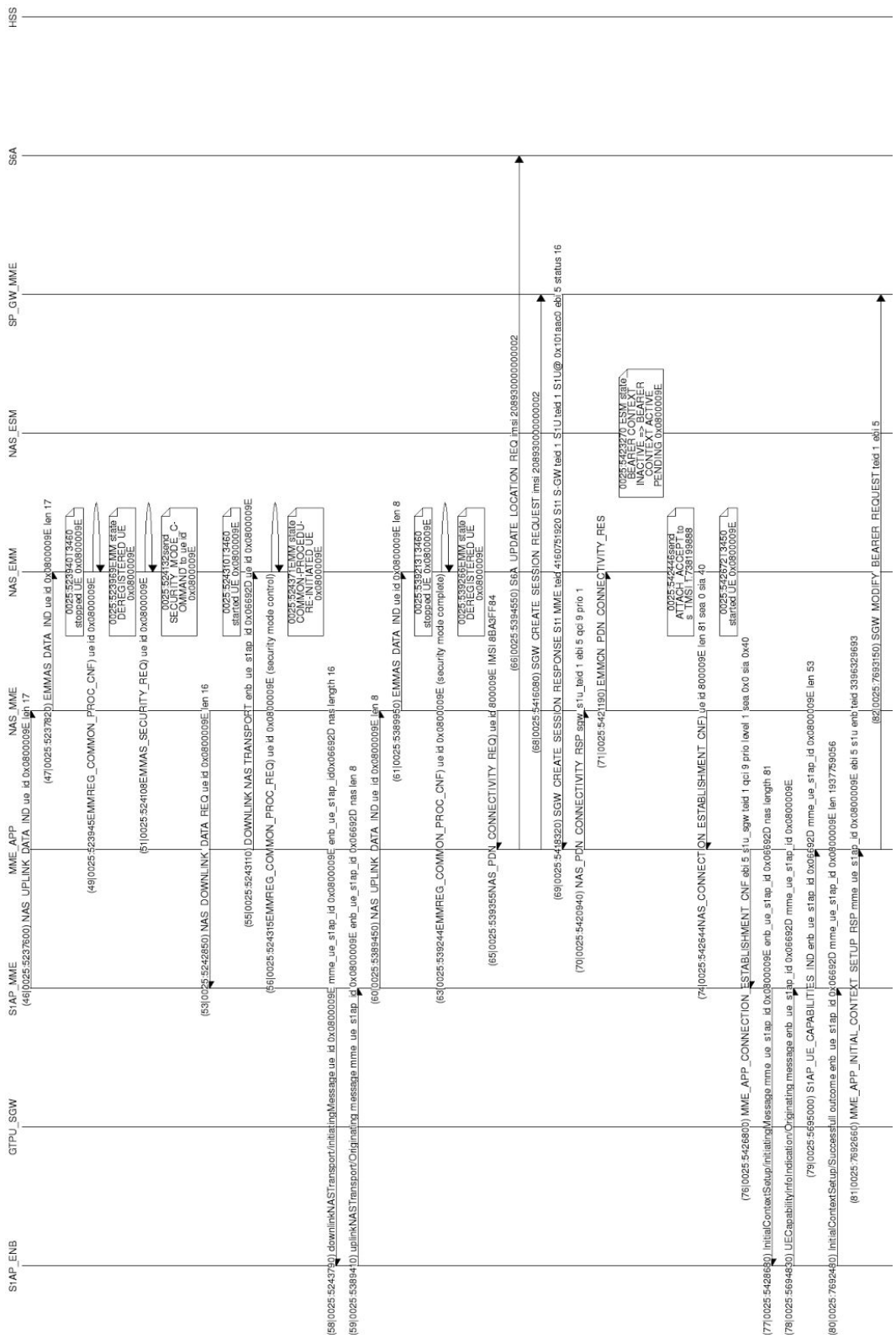


Figura 27: MSCGEN: Proceso Network Attach (continuación) observado desde el CN

A mitad altura de la figura 27, vemos que se completa el proceso de autenticación (*security mode complete*) y comienzan los procesos de solicitud de conexión al PDN (NAS_PDN_CONNECTIVITY_REQ), *location update* hacia el HSS (debido a que es el primer attach y la entidad MME no dispone de la información de subscripción del usuario) y solicitud de creación de sesión al SGW. Por último el estado del Bearer se transforma de *inactive* a *pending* mientras se finaliza el proceso de *attach* y es comunicado al UE, el cual responde con información para actualizar el contexto, por ejemplo la configuración acerca del APN para acabar de configurar el bearer, tal como se ilustra en la figura 28.

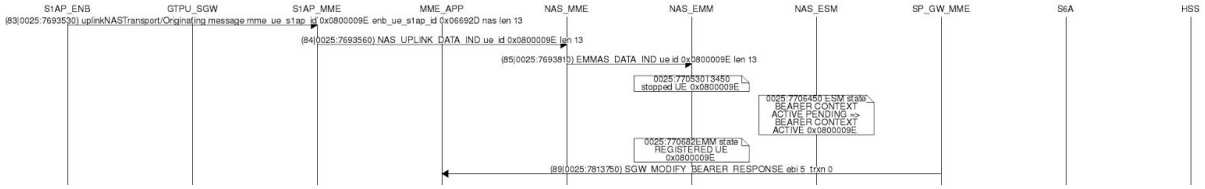


Figura 28: MSCGEN: Finalización del proceso de Network attach

Si ahora simulamos un *detach*, esto es por ejemplo habilitando el modo avión del UE, se inicia el proceso contrario al anterior, eliminando la sesión e inactivando el bearer. En la figura 29 el inicio de este proceso *detach* comienza con el segundo evento de S1AP_ENB, el cual corresponde a la comunicación de las intenciones por parte del UE a la red.

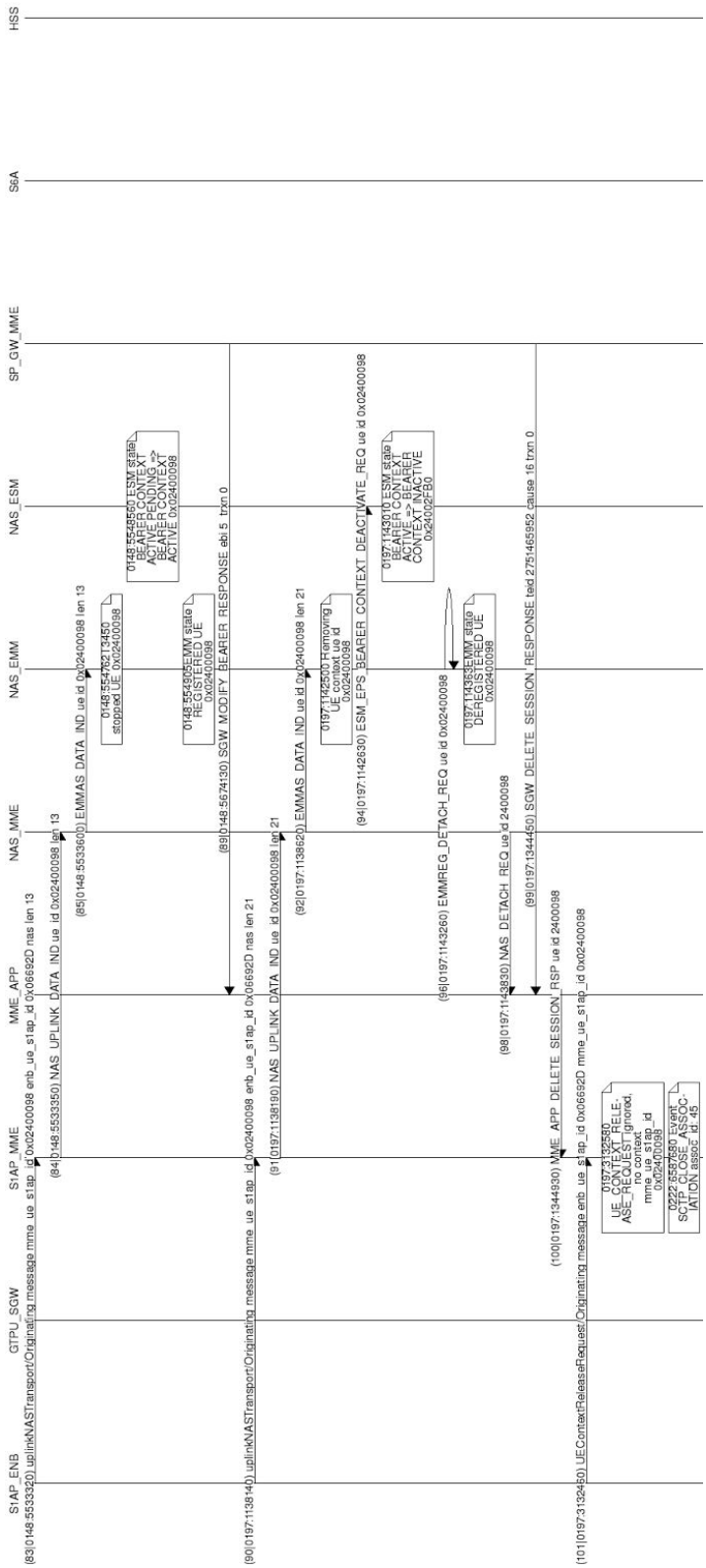


Figura 29: MSCGEN: Proceso de Network Detach

6.2.2. Wireshark

Otra de las herramientas integradas en OAI es el famoso Wireshark. Se trata de una herramienta ampliamente usada para capturar paquetes. Además del análisis de los protocolos de nivel 3, OAI tiene implementado la interfaz de Wireshark para los protocolos de la capa 2 (PDCP, RLC, MAC) utilizando sockets UDP. De esta manera ofrece una visión más transversal y detallada que MSCGEN. Para su utilización, primero hemos habilitado los protocolos anteriores con la opción *over_udp* en el Wireshark (*try heuristics* en las versiones antiguas). A la hora de ejecutar el OAI eNB, añadiremos el argumento "-W" para indicarle que reenvíe la información de las capas inferiores a la interfaz de loopback o "-P /path/archivo.pcap" para almacenar los datos en un archivo.

Las siguientes figuras ilustran algunos ejemplos de paquetes capturados por Wireshark. Los paquetes y tramas de niveles inferiores como el MAC o RLC son capturados en la interfaz de loopback.

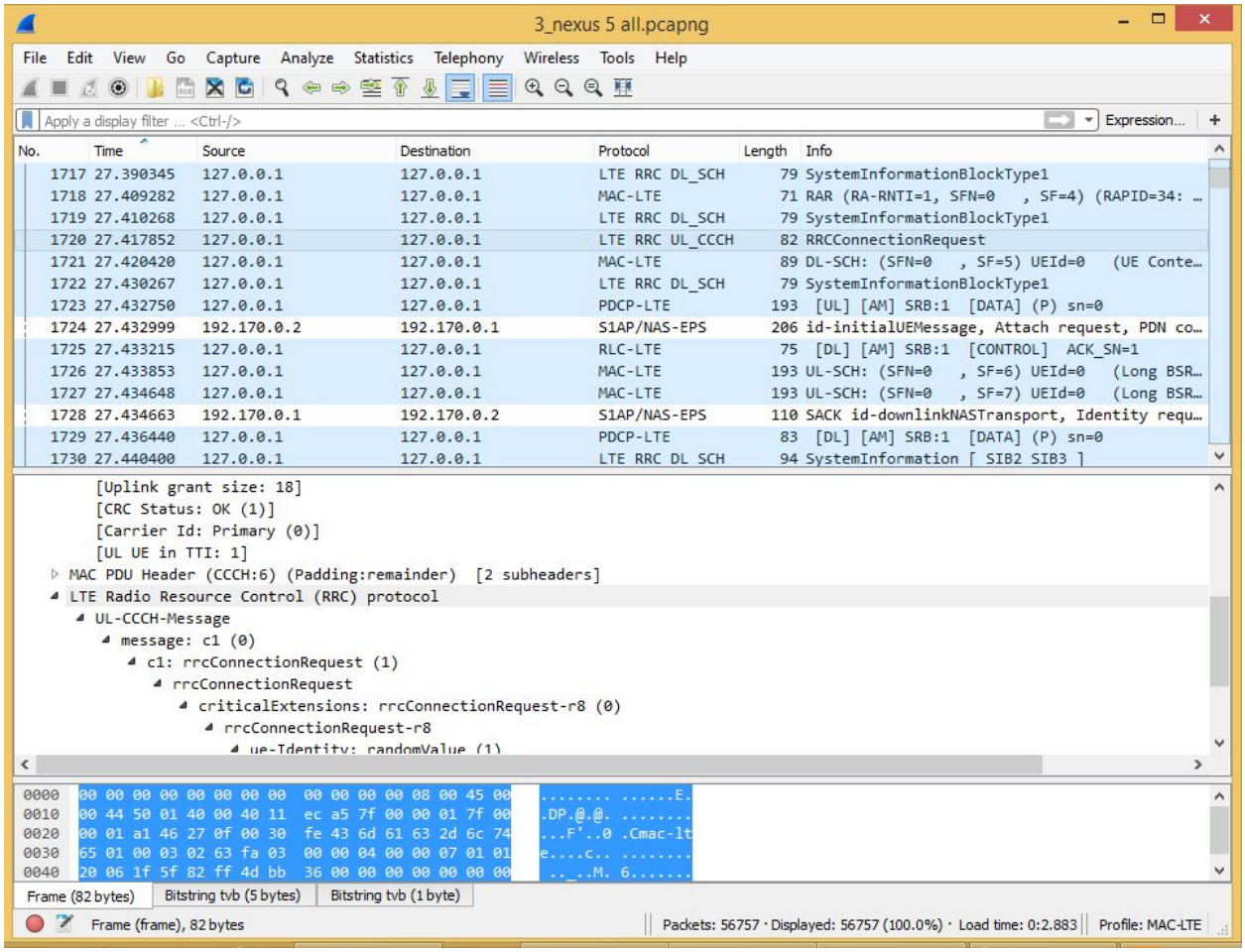


Figura 30: Wireshark: Captura del mensaje RRCConnectionRequest

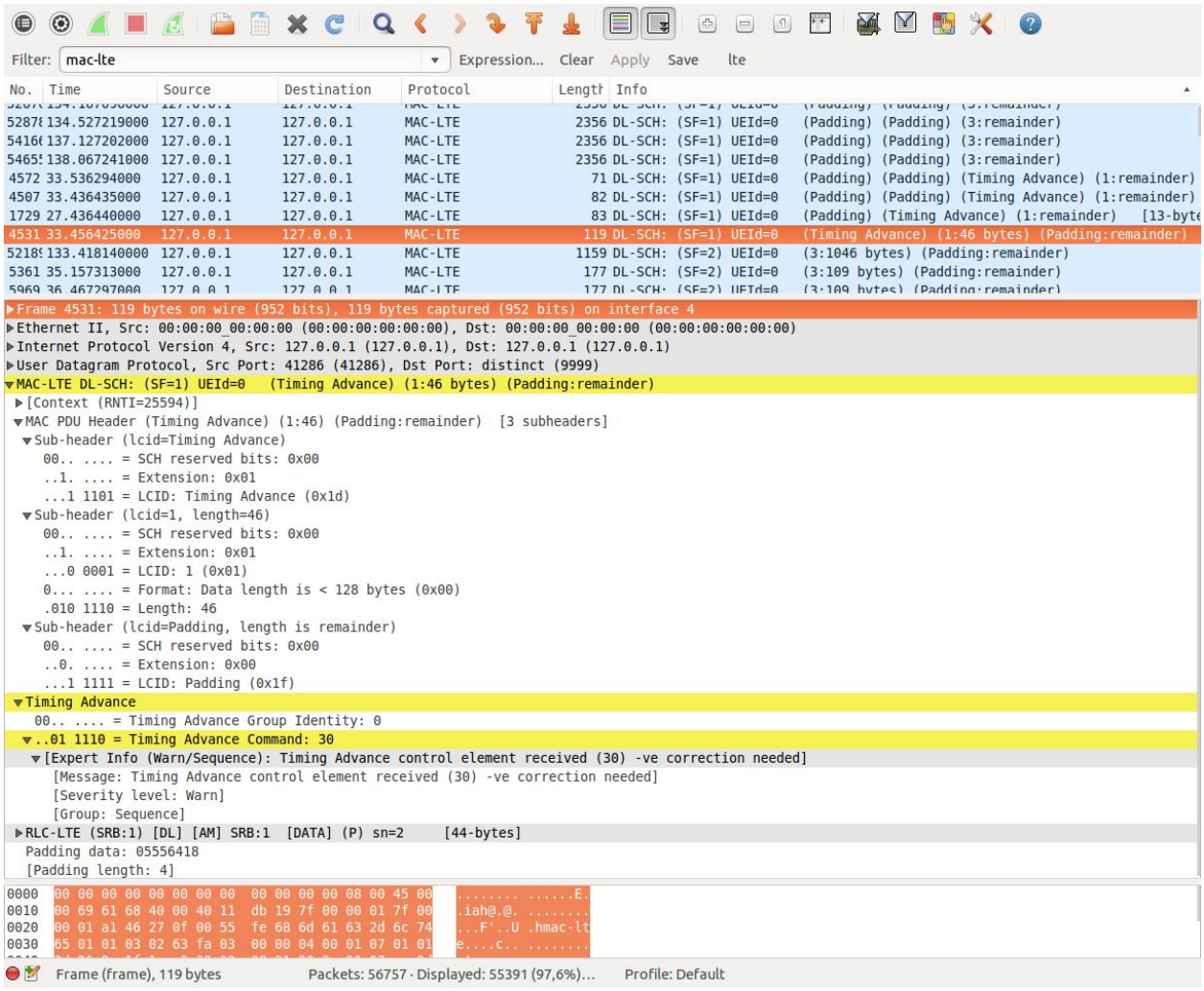


Figura 31: Wireshark: Captura(A) de mensajes relacionados con Timing Advance[34] a nivel de MAC

[34] El avance temporal (Timing Advance) es un mecanismo para garantizar la correcta sincronización de tramas entre el UE y el eNB en el uplink, de manera que los distintos usuarios dentro de una trama no se interfieran entre sí. Este sistema permite compensar los diferentes tiempos de propagación en función de la distancia entre el UE y el eNB, para ello el UE inicia la transmisión en el uplink con un cierto avance temporal, valor proporcionado por el eNB, con respecto al tiempo de inicio teórico. Es necesario ajustar este *offset* contínuamente porque la distancia entre el UE y eNB puede variar (el UE se mueve y cambia de ubicación con respecto al eNB). [49]

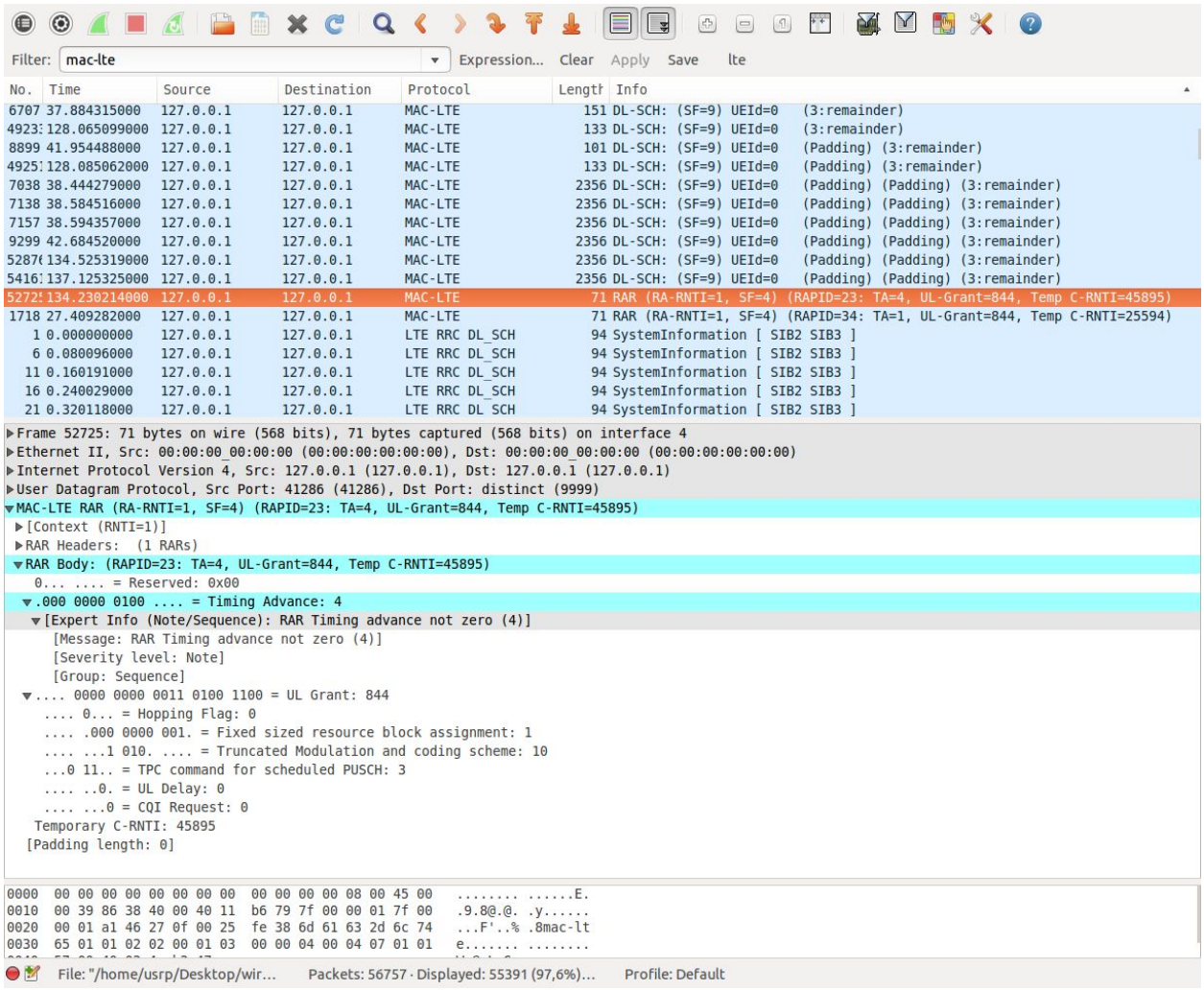


Figura 32: Wireshark: Captura(B) de mensajes relacionados con Timing Advance a nivel de MAC

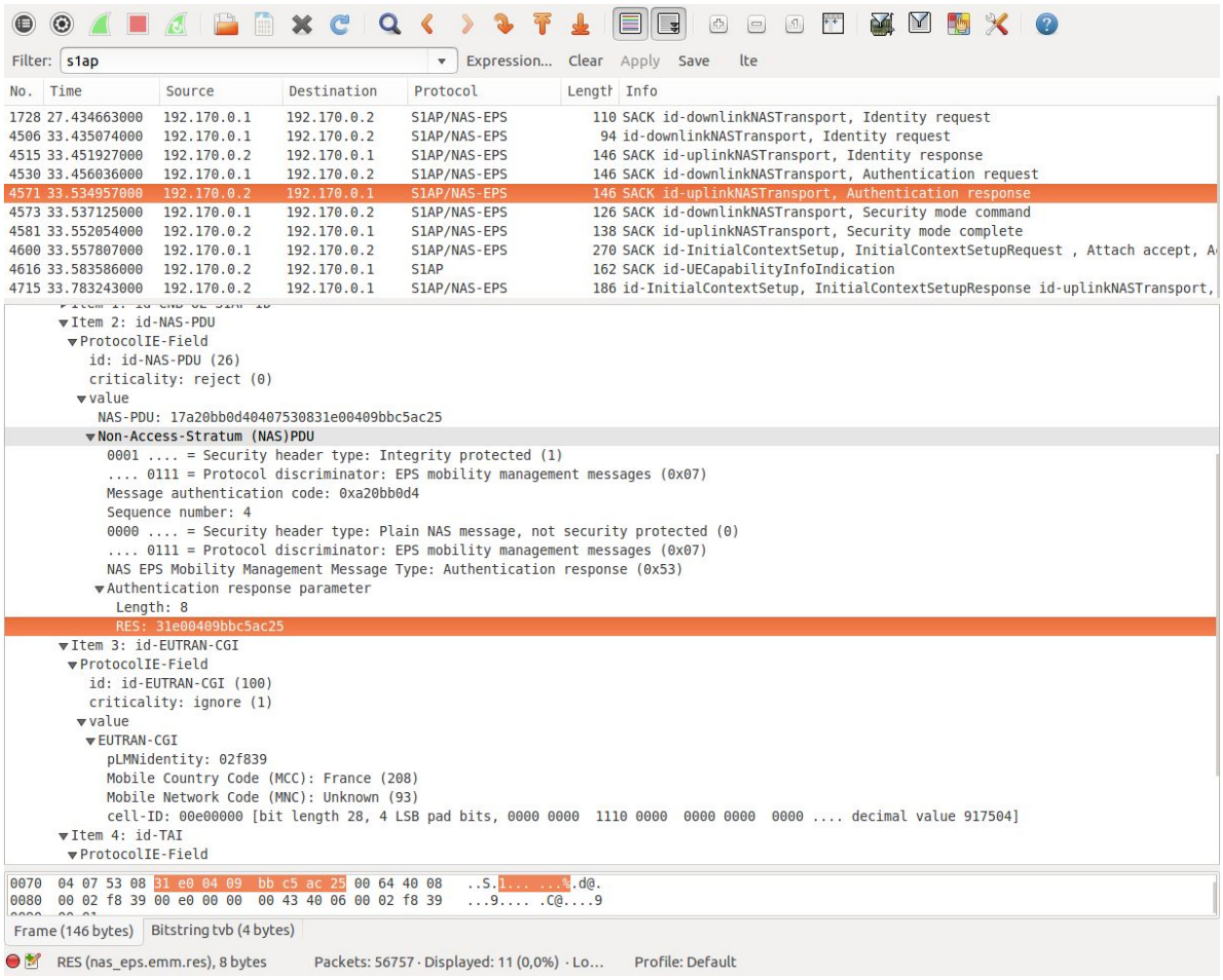


Figura 33: Wireshark: Captura del mensaje RES generado por el UE en Authentication response

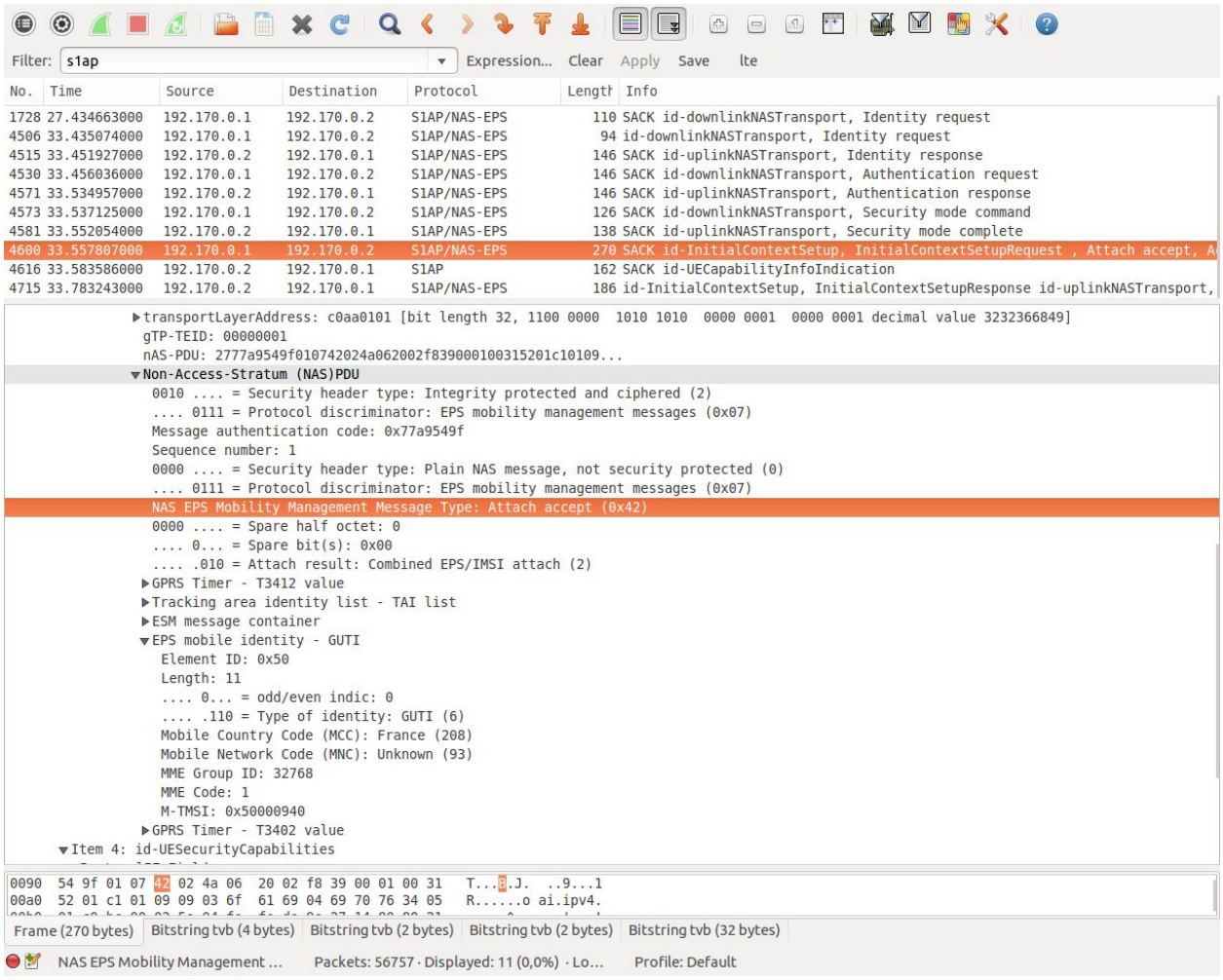


Figura 34: Wireshark: Captura del mensaje Attach accept

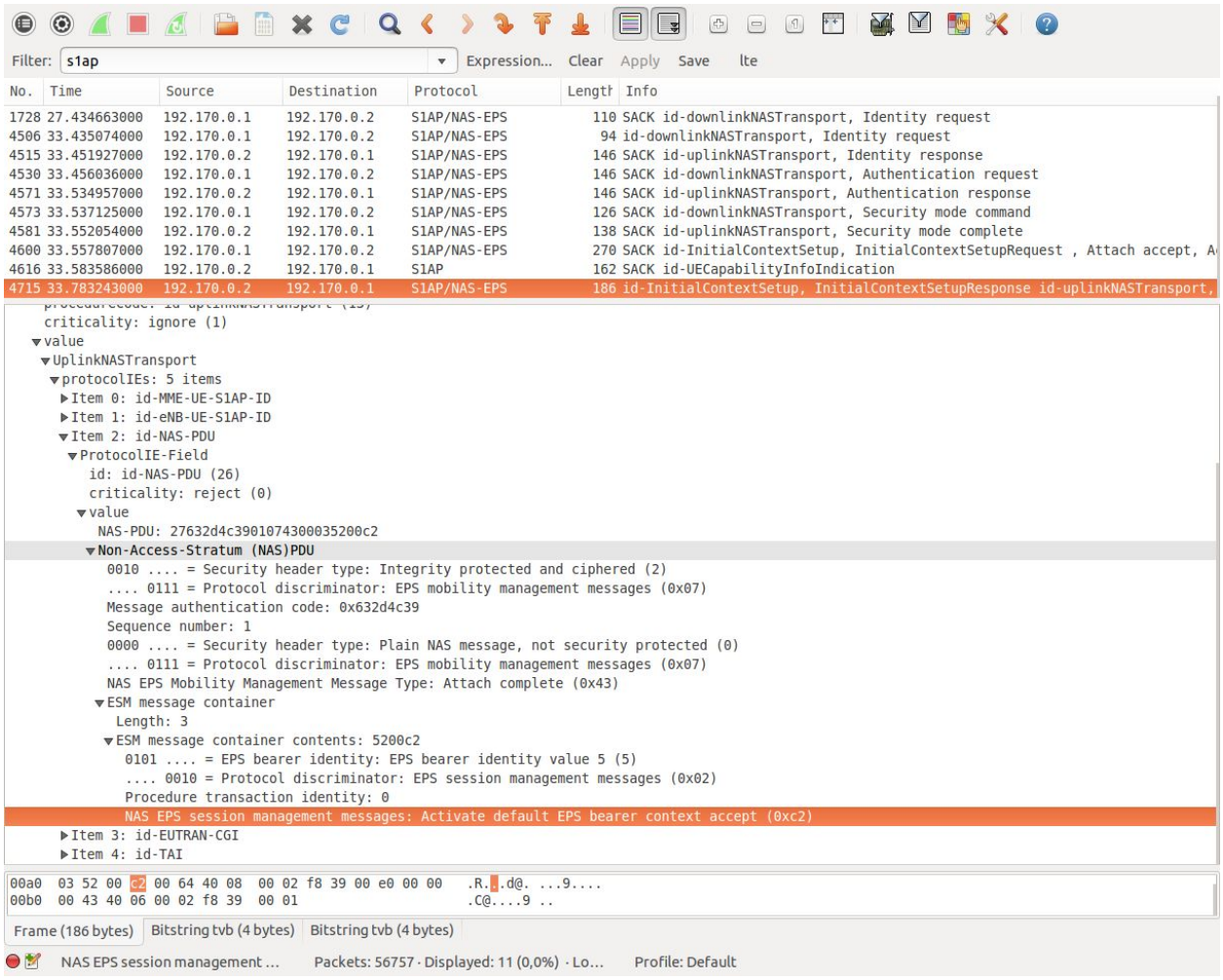


Figura 35: Wireshark: Captura del mensaje Attach complete

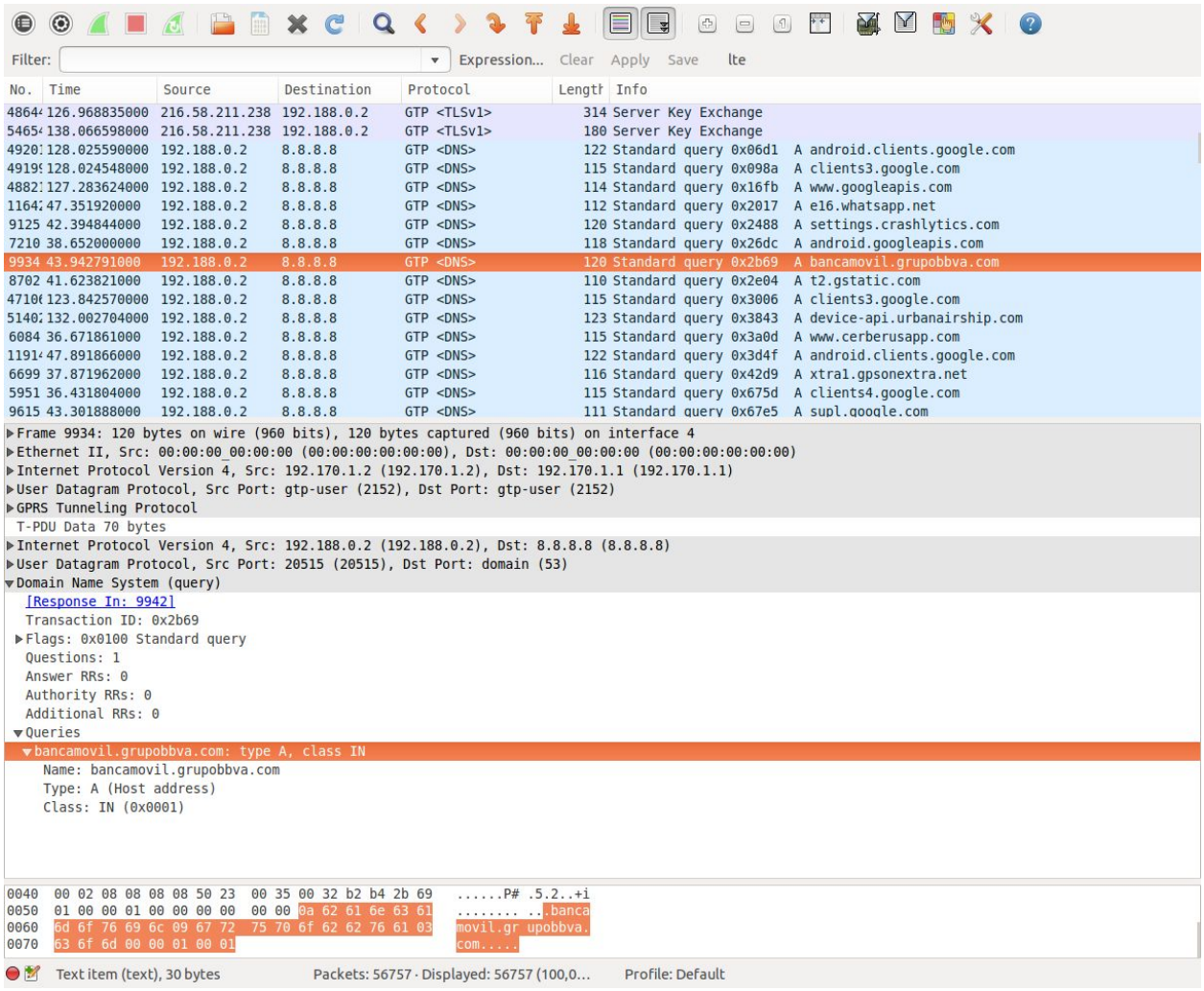


Figura 36: Wireshark: Captura de mensajes de niveles superiores

6.2.3. ITTI Analyzer

Inter-task interface (ITTI) Analyzer es una utilidad (*middleware*) que realiza un volcado de los mensajes intercambiados entre los diferentes procesos de los ejecutables del EPS, y los muestra en un formato más comprensible para el humano. Al igual que Wireshark, es una herramienta para hacer un seguimiento de las trazas y ayudar en la depuración del EPS. Puede tomar como input un archivo XML de los mensajes ITTI intercambiados, o actuar como servidor y escuchar los mensajes en tiempo pseudo-real. El código fuente se encuentra en el directorio de OAI common/utils/itti_analyzer. Al ejecutar las entidades del OAI, incluiremos el argumento `-K` para que se genere los

logs de esta herramienta. Las siguientes figuras ilustran ejemplos de la interfaz gráfica de ITTI Analyzer, así como la captura de algunos mensajes.

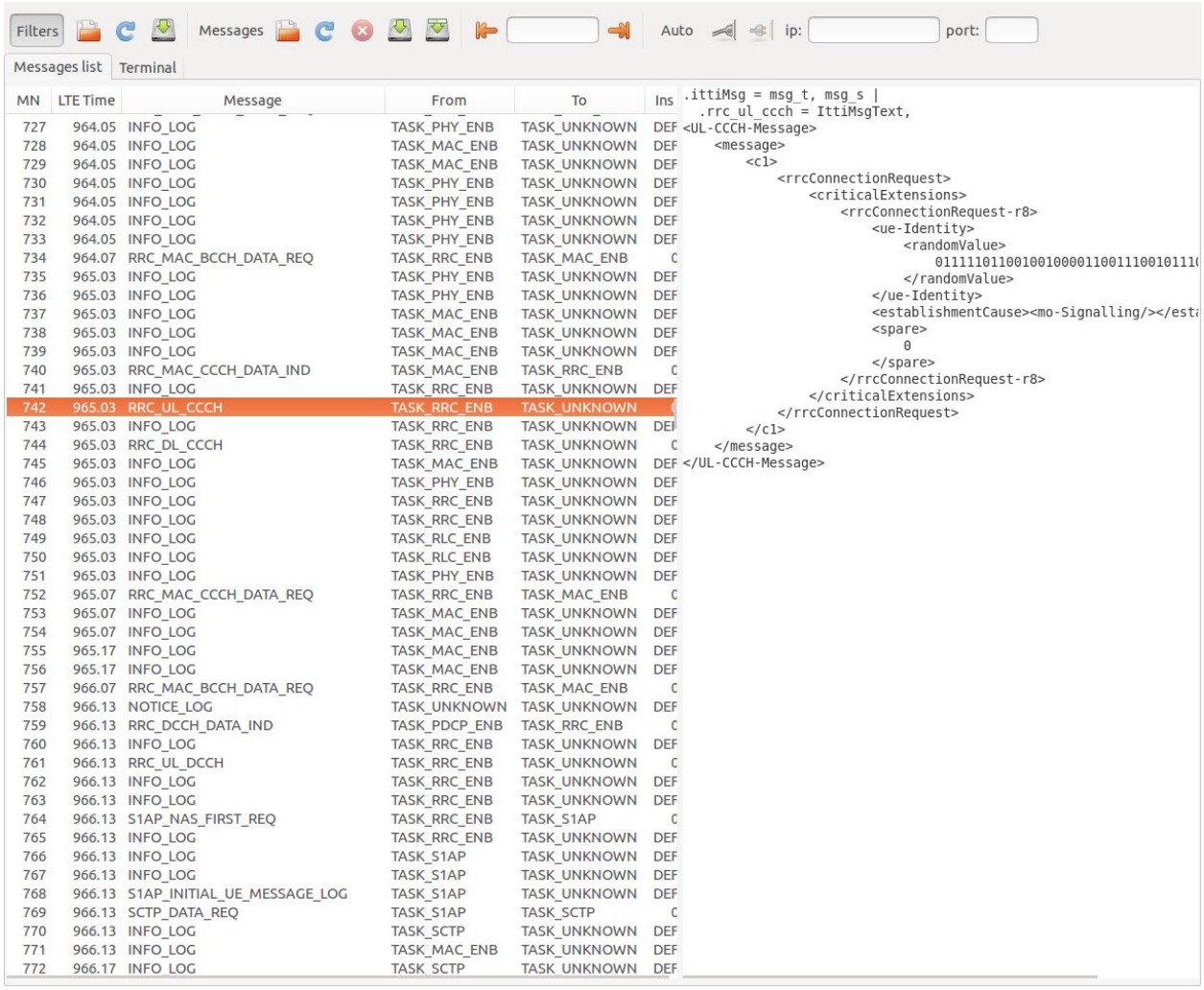


Figura 37: ITTI Analyzer: Captura del mensaje RRCConnectionRequest[35] en el canal lógico[36] CCCH[37] durante el Random Access

[35] Pueden encontrar más información acerca del procedimiento de establecimiento de la conexión a nivel RRC en la nota de pie 26 situado en la página 52.

[36] Los canales lógicos se utilizan para describir el tipo de información que se transmite a través de la interfaz radio. Se clasifican en canales lógicos de tráfico y de control.

[37] CCCH (Common Control Channel) es un canal lógico de control que permite la comunicación entre el eNB y el UE cuando todavía no se ha establecido una conexión a nivel de RRC.

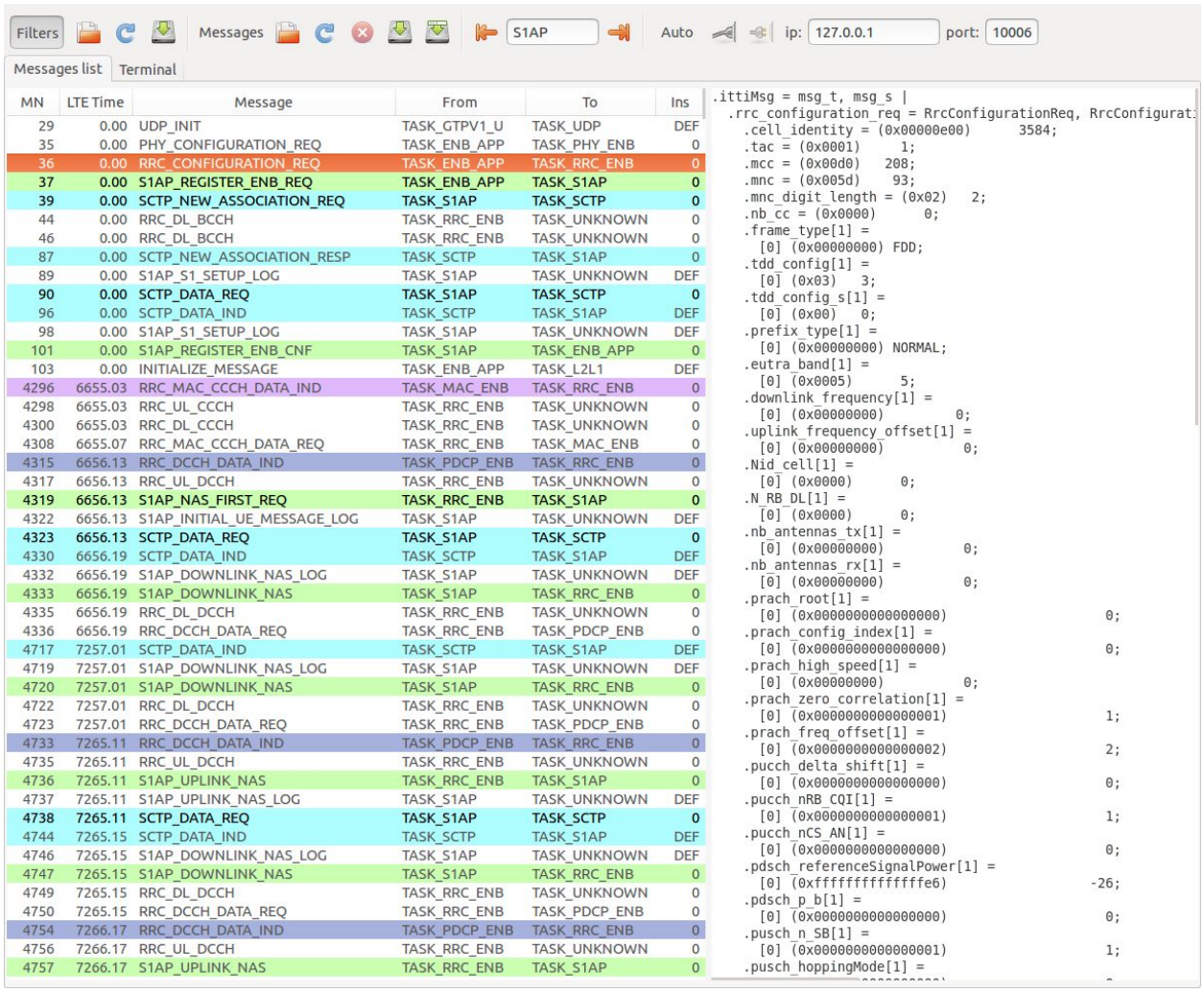


Figura 38: ITTI Analyzer: Captura del mensaje RRCConfigurationRequest entre las tareas ENB_APP y RRC_ENB

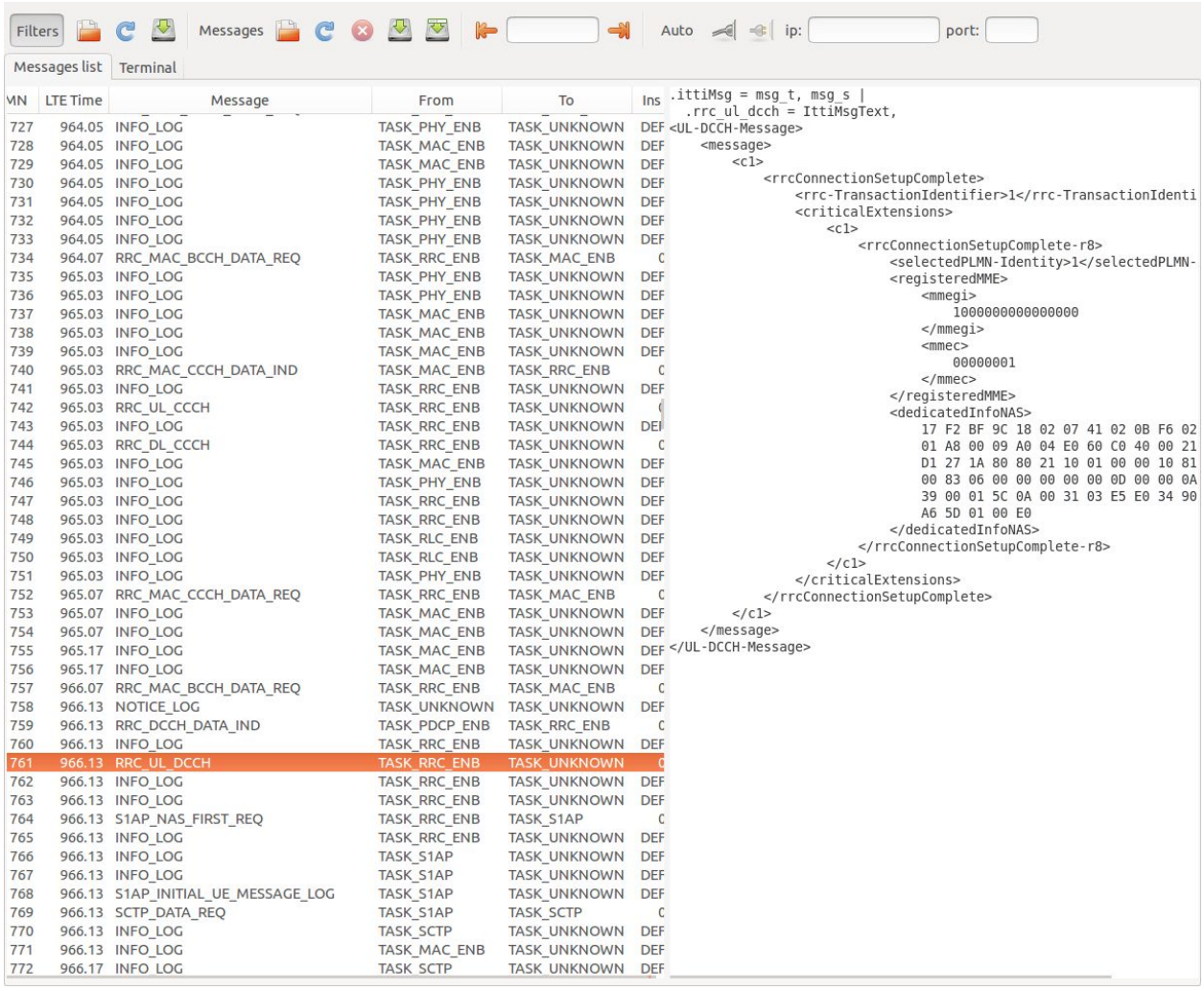


Figura 39: ITTI Analyzer: Captura del mensaje RRCConnectionSetupComplete del canal lógico DCCH[38]

6.2.4. Software Oscilloscope

Por último, el OAI Soft Scope es una herramienta que nos permite monitorear la interfaz física mediante gráficas a tiempo real de la potencia recibida, respuesta frecuencial, throughput, constelaciones, entre otros. Ofrece también diferentes estadísticas como PRBs asignados, CQI, timing advance, etc. En nuestro caso hemos podido observar las

[38] DCCH (Dedicated Control Channel): canal de control punto a punto destinado a transferir información de control entre el eNB y el UE, una vez que se dispone de una conexión a nivel de RRC. Sólo contiene información de control procedente del RRC y señalización a nivel de NAS (power control, handover, ...), no contiene señalización a nivel de aplicación asociada a un flujo de datos de usuario.

estadísticas del Uplink en el lado del eNode B. Para visualizar las estadísticas del Downlink, habría que implementar correctamente el escenario OAI UE ↔ OAI eNB + OAI EPC y ejecutar en el lado de OAI UE la interfaz gráfica del Soft Scope. A continuación encontrarán las capturas con esta herramienta.

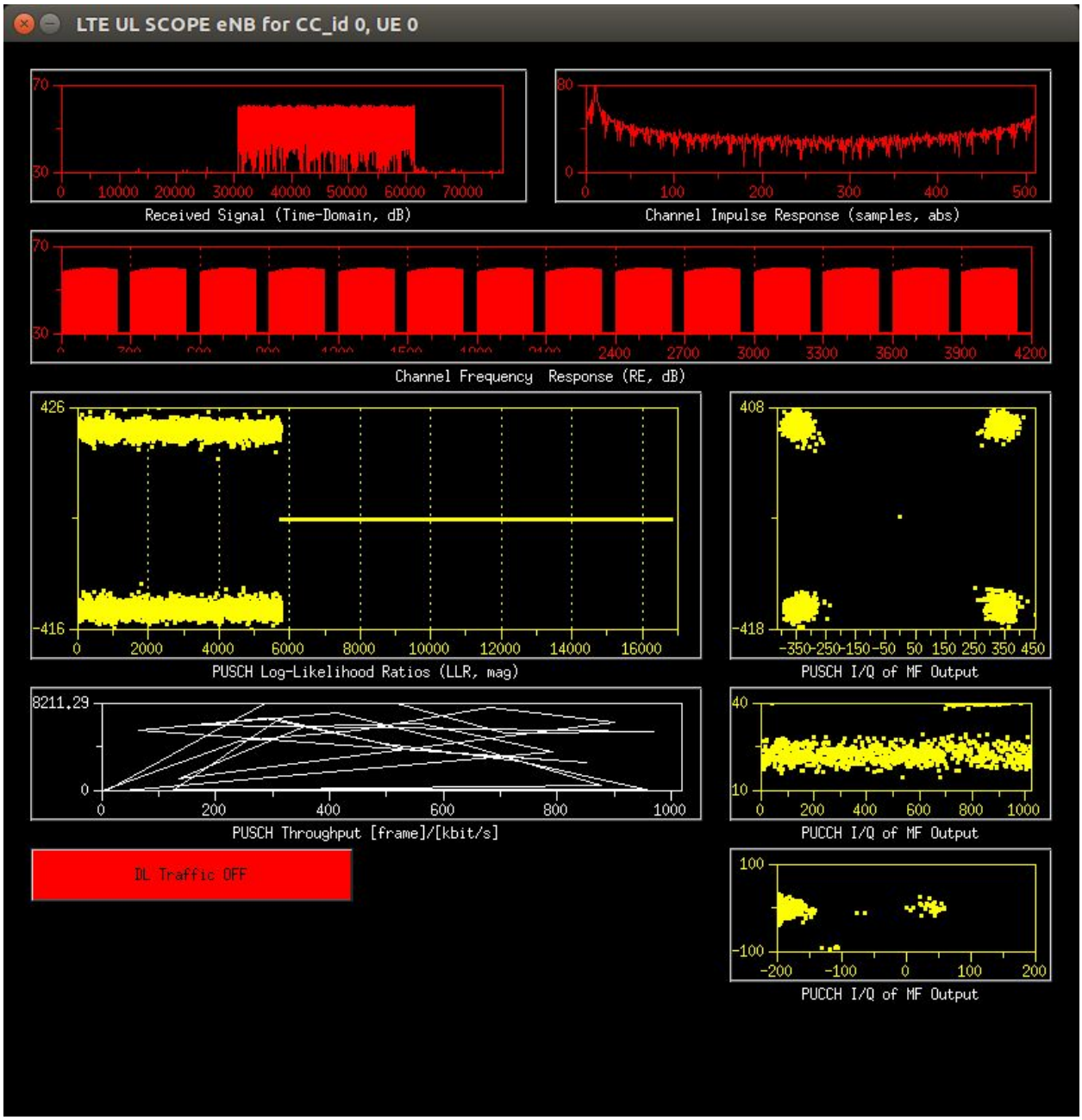


Figura 40: Soft Scope: Diferentes datos del nivel físico, capturados en el eNB, Uplink. Modulación 4-QAM.

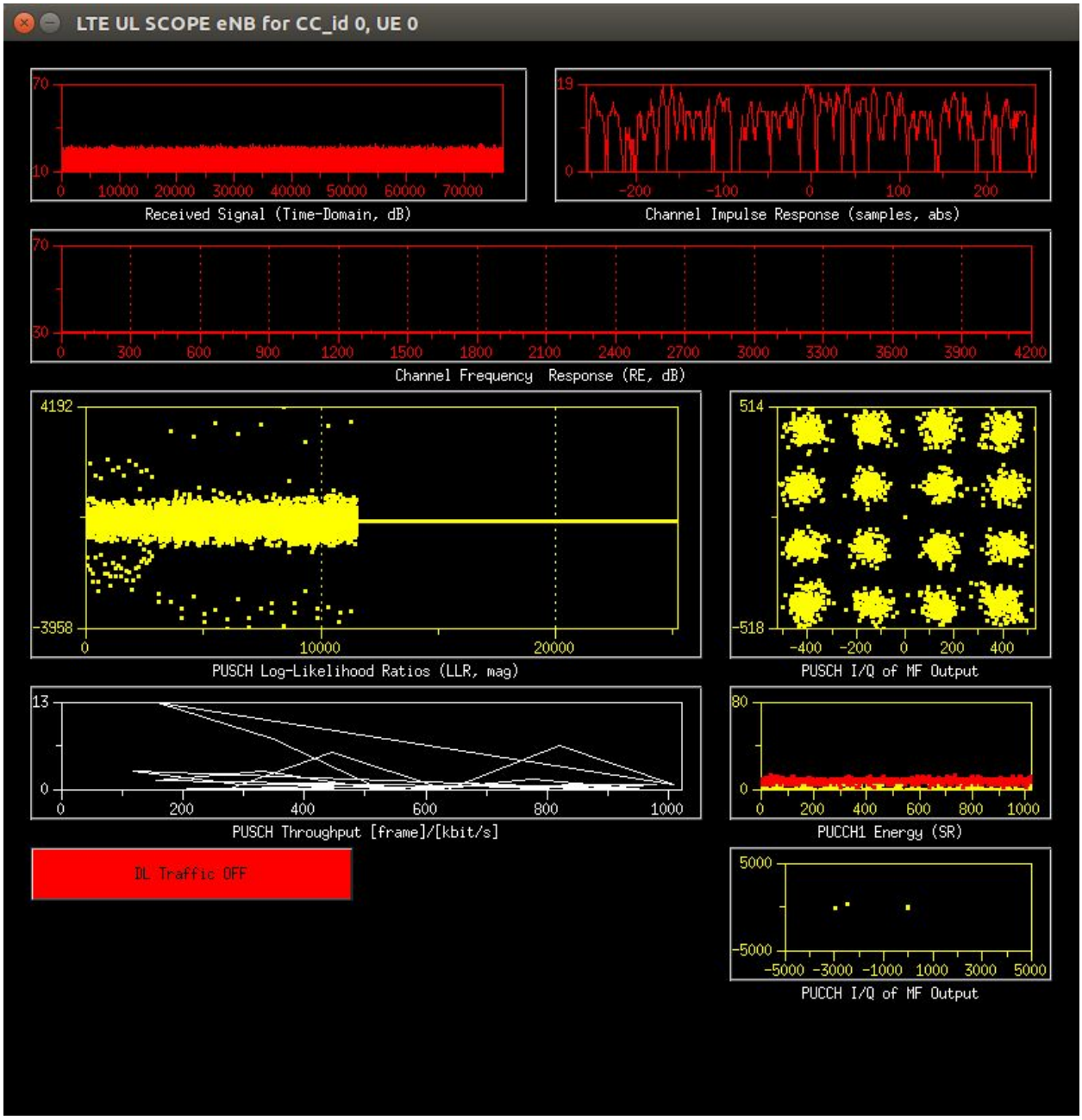


Figura 41: Soft Scope: Modulación 16-QAM en el Uplink

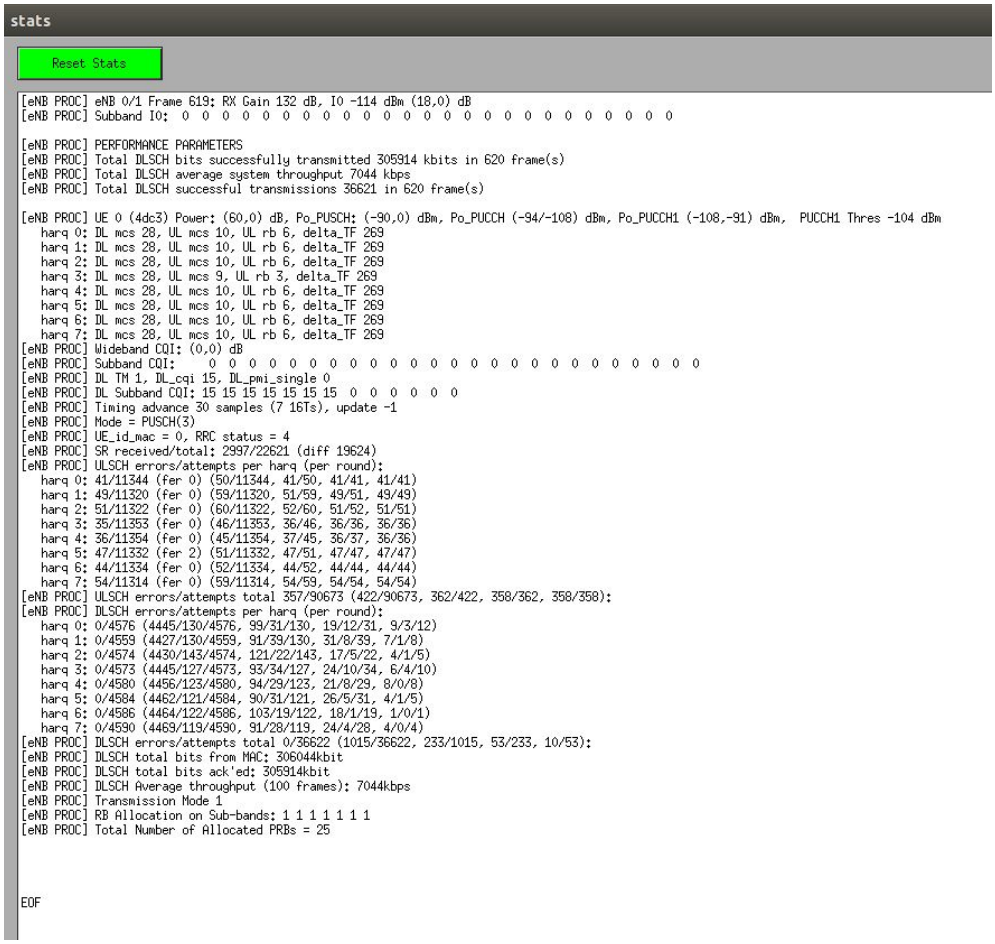


Figura 42: Soft Scope: Estadísticas(A) de la conexión en la interfaz Uu

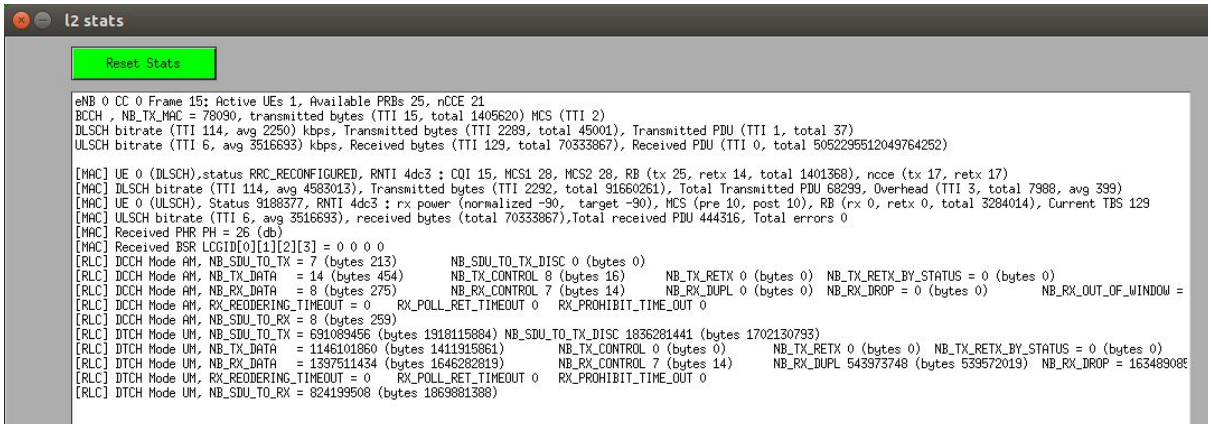


Figura 43: Soft Scope: Estadísticas(B) de la conexión en la interfaz Uu

Las figuras anteriores ilustran diferentes parámetros de rendimiento a nivel físico, como la ganancia en Rx (regulada en el archivo de configuración del eNB), bits transmitidos,

el *throughput* medio, el mcs[39], CQI[40], PRBs asignados o UEs activos. Desgraciadamente no ofrece aún la posibilidad de volcar estos datos en un archivo externo para su posterior análisis y comparación. Al igual que las herramientas anteriores, su uso perjudica el rendimiento general del testbed.

[39] MCS: Modulation and Coding Scheme, es la combinación de codificación de canal y modulación escogido por el mecanismo de adaptación de enlace para conseguir la máxima velocidad de transmisión, dadas unas condiciones de SNR concretas.

[40] CQI: Channel Quality Indicator, es el indicador del estado del canal, informa al eNB del índice máximo de la configuración MCS que permite garantizar una tasa de error (BLER) en el bloque de transporte recibido inferior a 10^{-1} (10%), durante el proceso de adaptación de enlace.

7. Hacia el 5G

Una de las ideas que más fuerza está cobrando entre fabricantes y operadoras para la próxima generación de telefonía móvil[41] es el concepto de C-RAN, del inglés Cloud-RAN o Centralized-RAN. Esta arquitectura reemplaza las estaciones base tradicionales por elementos radio distribuidos (Remote Radio Head, RRH), conectados a un emplazamiento en donde se concentran las unidades de procesamiento (Baseband Unit, BBU) [51].

Este desacoplamiento o división del eNodeB en los elementos anteriores, separados por una distancia considerable mediante por ejemplo, enlaces ópticos[42], tiene dos objetivos principales [52]:

- El procesamiento centralizado reduce la redundancia requerida, mejorando la eficiencia de la red.

- Los RRHs, al ser más simples y reducidos que las estaciones base con procesamiento in situ, permite un dimensionado y despliegue más fácil y económico.

Este sistema abre una puerta hacia la optimización de recursos y de energía, que combinados adecuadamente con otros sistemas, como la virtualización, ofrece la posibilidad de, por ejemplo, balanceo de cargas en el centro de procesamiento según demanda de tráfico, muy común en otros sistemas pero no se había realizado todavía para tecnologías celulares. Por otro lado, dicho frente de estudio se enfrenta también a retos intrínsecos de 4G y 5G, como los ajustados requerimientos temporales que se exige.

[41] El 5G aún no ha sido definido por 3GPP.

[42] Por la necesidad de gran cantidad de tráfico (muestras en fase y cuadratura) que se intercambian entre estas entidades, independientemente del tráfico útil generado.

En el contexto de USRP y de OAI, Eurecom ha publicado, durante el redactado del presente, una propuesta de Cloud-RAN para la plataforma OAI [53], en donde se ha introducido una nueva entidad, RRH GW, que consiste en una extensión del OAI eNB vía ethernet, dicho de otra manera, RRH GW actúa de enlace entre el equipo de radio (USRP) y el OAI eNB, con el fin de ejecutar estos procesos (RRH y eNB) en equipos diferentes.

En nuestro caso hemos adaptado el escenario del *single-host* anterior para dicha implementación, incorporando para este caso un nuevo host-PC. La figura 44 ilustra el diagrama del testbed implementado. Y la figura 45 ilustra la ejecución del OAI RRH, que actúa de servidor escuchando las conexiones entrantes del cliente (BBU).

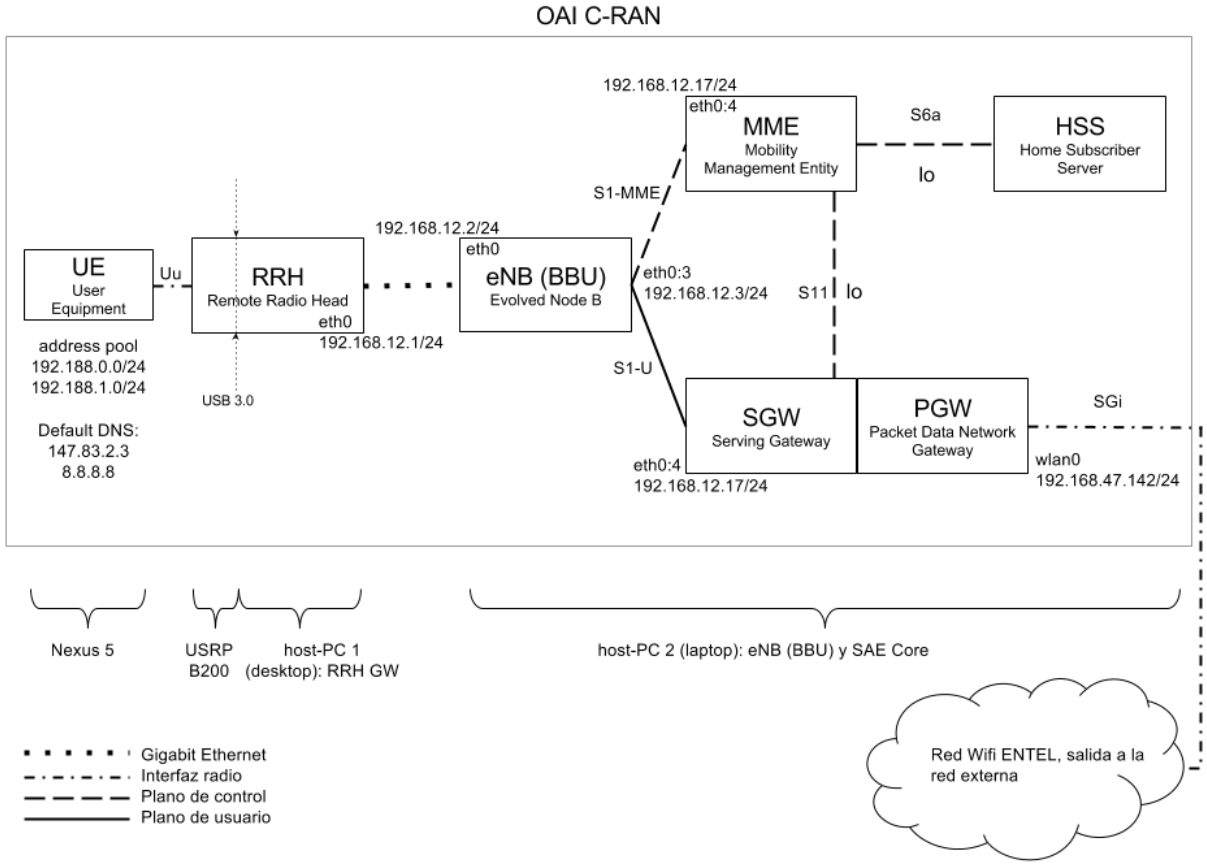


Figura 44: Arquitectura C-RAN implementada

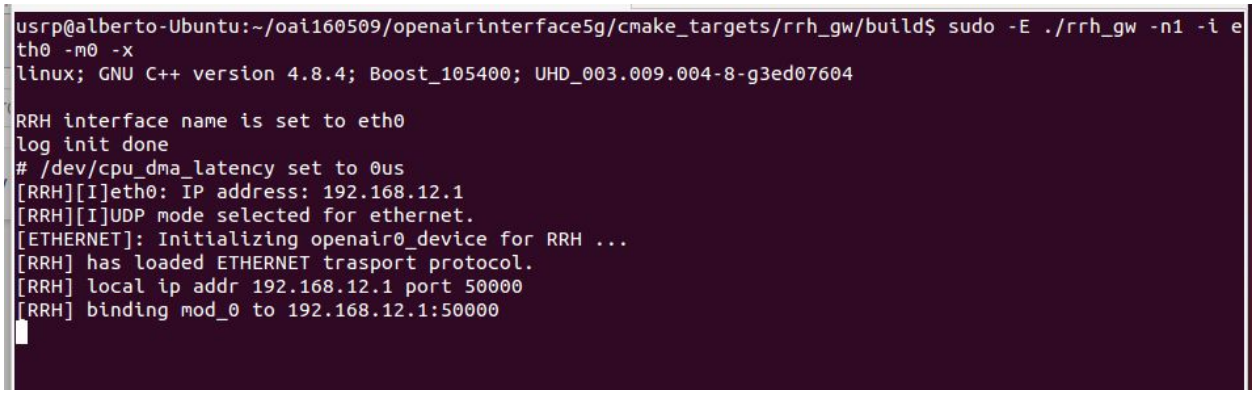


Figura 45: OAI RRH GW

Mediante la herramienta Bmon monitoreamos el ancho de banda del *fronthaul* (interfaz entre BBU y RRH), en donde viajan a una velocidad constante las muestras en fase y cuadratura (I/Q samples): la figura 46 ilustra 30.17 MiB/s para una canalización de 5 MHz (25 RBs). Observamos en la figura 47 que al cabo de unos dos minutos y medio, se han intercambiado una cantidad considerable de información (eNB: 5 GiB en RX y 2 GiB en TX) sin que haya generado apenas tráfico útil.

Si aumentamos la canalización del sistema (parámetro N_RB_DL del archivo de configuración del eNodeB), observamos también más tráfico en esta interfaz, siendo 60.21 MiB/s para 50 RBs y 117.17 MiB/s para 100 RBs (figura 48). Desgraciadamente para anchos de banda tan grandes, el sistema se vuelve muy inestable y el enlace se mantiene entre 10 y 30 segundos.

En cuanto al rendimiento hacia la red exterior, en este escenario de C-RAN obtuvimos throughputs entre 0.5 Mbits/s y 1 Mbits/s para el COTS UE Nexus 5, hacia los servidores exteriores[43].

[43] https://fast.com/

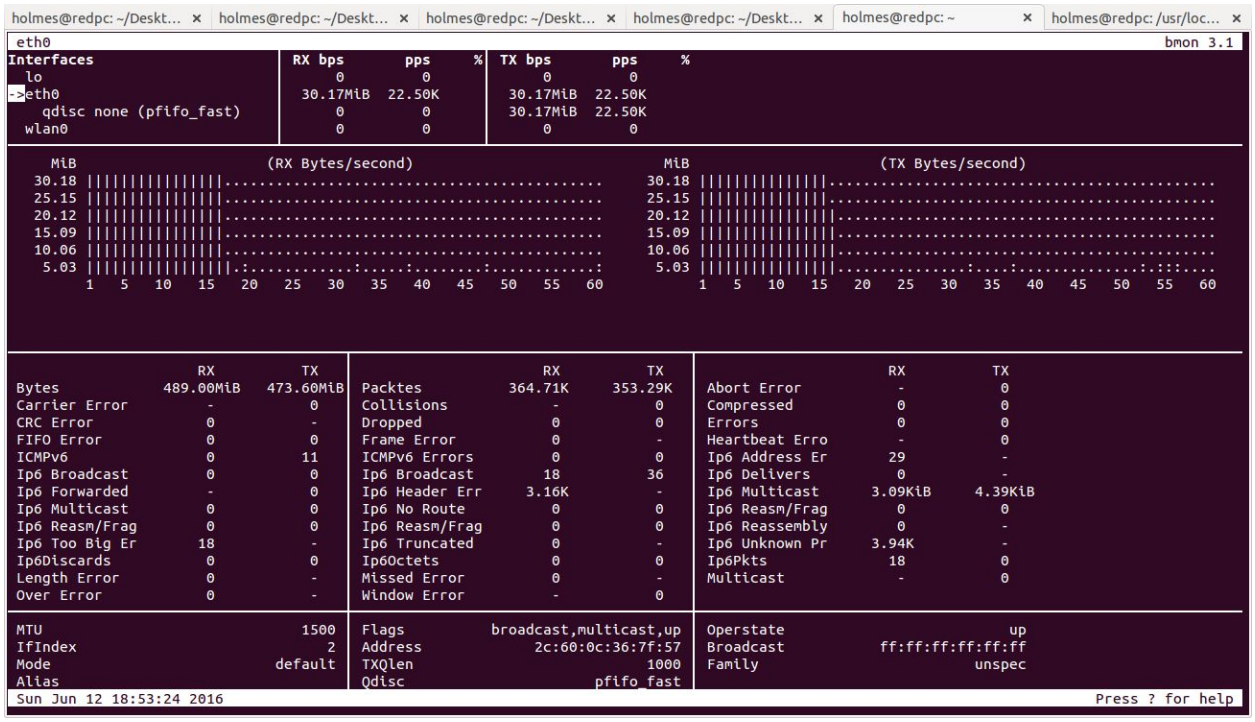


Figura 46: Bmon: monitorización fronthaul en el eNB para RB 25

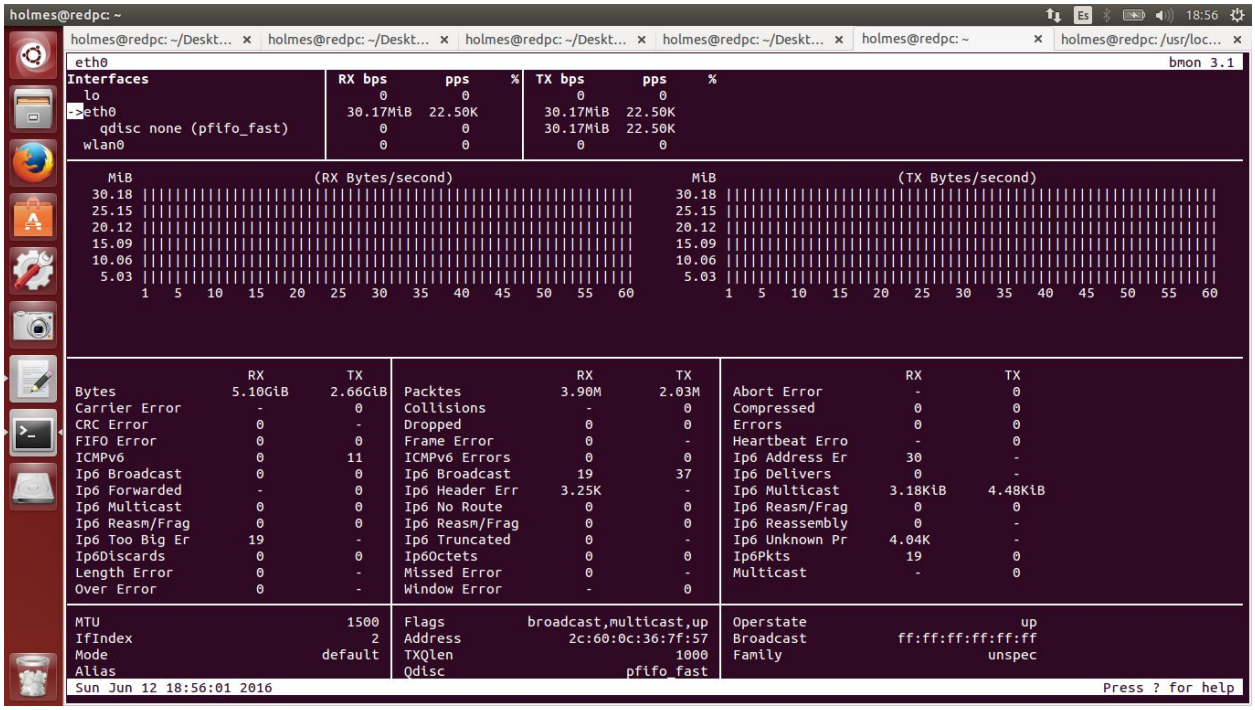


Figura 47: Bmon: captura de la misma monitorización al cabo de 3 minutos

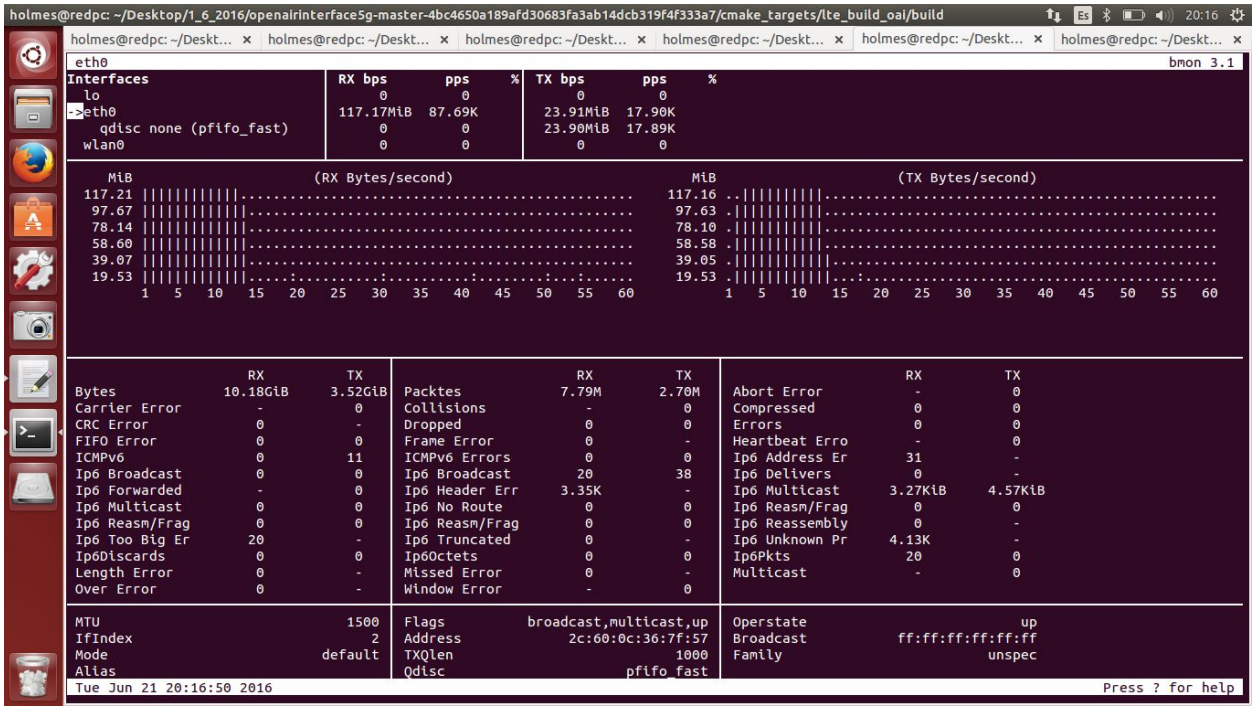


Figura 48: Bmon: monitorización fronthaul en el eNB para RB 100

8. Conclusiones

Hemos visto que la simplificación de la arquitectura de red EPS con respecto a tecnologías anteriores ha facilitado en gran medida el despliegue de soluciones SDR. Particularmente, el *open source* OAI es una de las plataformas de este campo más populares y completas. Destinada a testbeds, ofrece una serie de herramientas muy útiles para el estudio de LTE, como el MSCGEN o la integración con Wireshark. A pesar de ello, sigue siendo incompleto, muchas de sus funciones y prestaciones son todavía inestables o están bajo desarrollo. Además, la estructura de su código es compleja y dificulta en gran medida la customización y modificación por parte de un usuario externo al proyecto, principalmente por la falta de documentación al respecto.

No obstante, es una plataforma aún joven, apoyada por una comunidad sólida y creciente. Asimismo tiene una hoja de ruta bien definida para evolucionar de manera eficiente, como la inclusión de frameworks IMS, igualmente *open source*, a lo largo de este año 2016, como pueden ser los proyectos *OpenIMS* o *ClearWater*.

Por otro lado, también hemos visto las limitaciones que existe, tanto administrativas como técnicas, en el despliegue mediante SDR de testbeds que alojan las últimas tecnologías móviles. Al ser el espectro radioeléctrico un recurso público limitado, actualmente la administración no concede ninguna banda de telefonía móvil para el entorno educativo. Mientras que en la parte técnica nos encontramos con los problemas inherentes en el estudio de estas tecnologías, las cuales se necesita de un procesador potente y amplia memoria por los altos grados de exigencia de los estándares. Esta limitación tiene un considerado efecto que hay que evaluar en los sistemas de bajo coste, que suelen conllevar unos recursos más limitados.

A pesar de las deficiencias y los obstáculos anteriores, la combinación del SDR con los ordenadores personales, se ha traducido en una flexibilidad que tiempo atrás era inviable por la tecnología. Esta versatilidad la hemos percibido, por ejemplo, en los primeros meses del presente proyecto, cuando intentábamos implementar un *Node B* de la tecnología UMTS mediante la plataforma OpenBTS-UMTS, y que más tarde lo

suplimos por la tecnología LTE debido a la falta de soporte del primero por parte de la comunidad, la cual estaba centrada sobretodo en su versión GSM, el OpenBTS.

En definitiva, esperamos que esta evaluación de la plataforma OAI, en conjunto con el dispositivo de Ettus sienta las bases para futuros proyectos, en los que pueden por ejemplo, evaluar diferentes *schedulers* para mejorar el rendimiento en la interfaz radio o separar las distintas entidades del EPS en varios ordenadores personales y así distribuir la carga de trabajo. Son muchas las posibilidades que puede ofrecer el SDR en este campo de estudio, que con toda probabilidad formará parte de la próxima generación de telefonía móvil 5G.

9. Anexo

9.1. Interfaces y protocolos en el EPS

Esta sección mostramos un resumen de las interfaces definidas en la red EPS, especialmente las que afectan a nuestro testbed, así como las pilas de protocolos que intervienen en estos interfaces.

Denominación	Comentarios
E-UTRAN Uu / LTE Uu / interfaz radio	eNB - UE
X2	eNB - eNB, interfaz no implementada en OAI
S1-MME	eNB - red troncal: MME
S1-U	eNB - red troncal: S-GW
SGi	PGW - Redes externas
S6a	MME - HSS
S5/S8	PGW - SGW, interfaz no implementada en OAI
S11	MME - SGW
Señalización NAS	UE - MME

Figura 49: Interfaces EPS del testbed

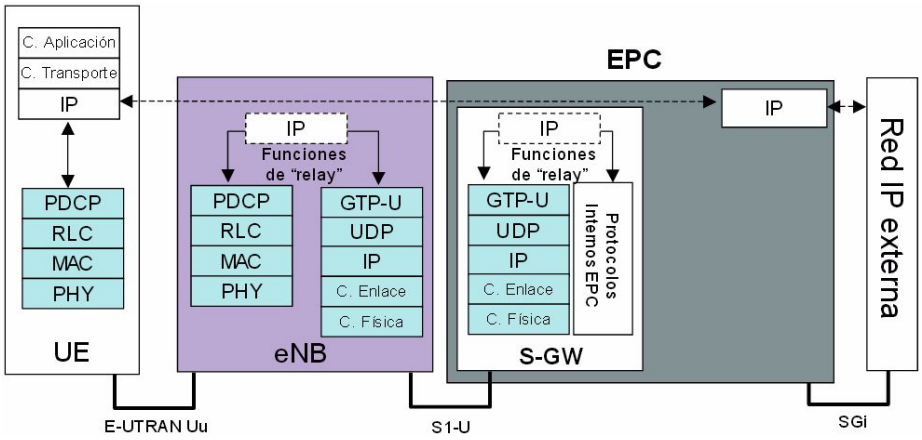


Figura 50: Pilas de protocolos del plano de usuario en E-UTRAN [45]

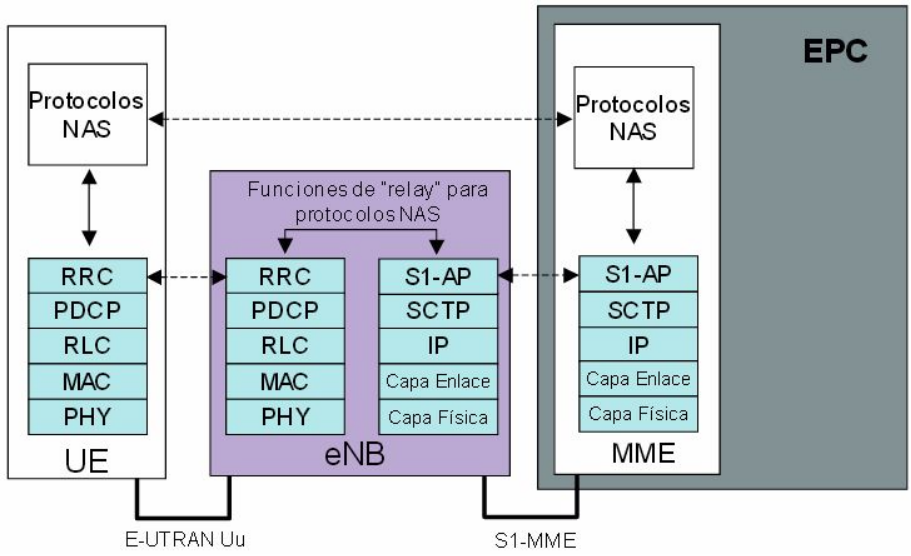


Figura 51: Pilas de protocolos del plano de control en E-UTRAN [45]

GTP-U: interfaz para el transporte de información de plano de usuario entre los diferentes elementos de la red troncal EPC. El S1-U, S5/S8, X2-U son interfaces basados en GTP-U.

GTP-C: interfaz de control que soporta funciones de gestión de sesión y de movilidad. Algunos ejemplos de interfaces basados en GTP-C son: S11, S5/S8.

NAS (Non-Access Stratum): conjunto de protocolos soportados entre UE y MME, se encarga de la gestión de movilidad de los equipos de usuario (EPS Mobility Management, EMM) y la gestión de las sesiones para el establecimiento de la conectividad entre el UE y P-GW (EPS Session Management, ESM).

S1-AP (S1 Application Protocol): Protocolo de nivel de aplicación entre eNodeB y MME.

SCTP (Stream Control Transmission Protocol): Protocolo que garantiza la entrega de mensajes de señalización entre MME y eNodeB.

Diameter: evolución del protocolo RADIUS, sustenta funciones de Autenticación, Autorización, Accounting (AAA) y de otras aplicaciones (extensiones) fuera del ámbito AAA. La interfaz S6a que conecta MME y HSS utiliza este protocolo.

RRC (Radio Resource Control): protocolo encargado de la radiodifusión de la información común procedente de NAS (capa superior), información relativa al modo Idle (parámetros para la reselección de celda, información sobre celdas vecinas, etc.); control de conexión RRC (establecimiento, mantenimiento y cierre de una conexión RRC, paging, establecimiento inicial de los mecanismos de seguridad); configuración de las capas inferiores y de contexto.

PDCP (Packet Dependence Convergence Protocol): protocolo encargado de compresión/descompresión de las cabeceras de los paquetes IP; cifrado de los datos y la señalización; implementación de mecanismos de integridad en mensajes de señalización.

RLC (Radio Link Control): Implementa procedimientos de segmentación/concatenación de los paquetes IP recibidos de capas superiores para adaptar su tamaño a las capacidades de transmisión de la interfaz aire, así como mecanismos de retransmisión de estos paquetes recibidos erróneamente.

MAC (Medium Access Control): implementa mecanismos de corrección de errores mediante procedimientos de retransmisión, Hybrid ARQ, técnica de retransmisión basada en el incremento de redundancia; gestión de prioridades entre canales lógicos utilizando técnicas de *Dynamic Scheduling*; selección del formato de transmisión (tipo de modulación, tamaño del bloque de transporte) de la capa física.

9.2. Otras diferencias entre UTRAN y E-UTRAN

En CDMA cada canal de transmisión se comporta como un interferente para otros canales. Como consecuencia, la gestión de potencia de transmisión es fundamental para preservar la capacidad del sistema CDMA. Especialmente esto es crítico en los bordes de las celdas o zonas con poca cobertura, donde mantener la calidad de transmisión del radio enlace es muchas veces sinónimo de aumentar la potencia de transmisión y añadir ganancia en la diversidad de transmisión. El *soft-handover* es un

mecanismo por el cual un terminal mantiene simultáneamente diferentes radioenlaces de diferentes celdas en una misma sesión o flujo de datos. Posteriormente la información es recombinada desde el receptor, sea en el lado del terminal o de la red. En 3G/UTRAN, soft-handover es aplicado en todos las canales de transmisión dedicadas. No se aplica en HSDPA, el cual utiliza un canal físico compartido.

La consecuencia de esto en la arquitectura del 3G/UTRAN es la obligatoriedad de la interfaz *Iur* entre RNCs para el caso de que los diferentes BTS de un proceso soft-handover no están controlados por el mismo RNC. A partir de aquí se complica la arquitectura de los RNCs, separándolos en SRNC (Serving RNC) y DRNC (Drift RNC). En E-UTRAN no se hace uso de soft handover y se elimina la arquitectura de los RNC, con su respectivo ahorro en costes y simplificación en la arquitectura. X2 es una interfaz opcional que no sustituye a Iur, tiene como objetivo proveer el servicio de transmisión de datos (data-forwarding) en la movilidad entre eNodeBs.

Otra diferencia entre E-UTRAN y UTRAN es el uso de canales compartidos frente a los dedicados. En E-UTRAN la transmisión de datos por la interfaz radio está basado en canales compartidos, para cualquier tipo de servicio o calidad de servicio. Esto limita en mayor medida al *radio scheduler*, ya que el sistema ha de asegurar que todos los datos son transmitidos con el QoS requerido, pero simplifica el diseño y las operaciones de la red, ganando de esta manera en flexibilidad. Ya no es necesario particionar los recursos físicos de la interfaz radio en diferentes conjuntos de canales que compiten entre ellas [1].

9.3. OpenBTS-UMTS

Empezamos este proyecto evaluando la plataforma OpenBTS-UMTS, que es una implementación en 3G del famoso OpenBTS, software open source desarrollado por la empresa Range Networks para implementar un punto de acceso mediante SDR. Al igual que OAI, es una solución de bajo coste para implementar un servicio de telefonía móvil. Sin embargo la conexión que se consigue es muy inestable y apenas existe soporte por

parte de la comunidad, la cual se centra sus esfuerzos sobretodo en el desarrollo y mantenimiento de la versión en GSM, el OpenBTS.

La siguiente figura se ilustra los resultados de un barrido de frecuencias de un terminal Nokia N95, en la que además de las operadoras comerciales, se encuentra la señal de nuestro Node B con códigos identificadores (MCC/MNC) de Mobiland.

Figura 52: Escaneo de operadoras con un Nokia N95

10. Bibliografía

[1] Lescuyer, Pierre and Thierry Lucidarme. *Evolved Packet System (EPS)*. Chichester, West Sussex, England: J. Wiley & Sons, 2008. Print.

[2] "Releases". *3GPP Releases*, 2016. *http://www.3gpp.org/specifications/67-releases*

[3] "The Evolved Packet Core". *3gpp.org*, 2016. *http://www.3gpp.org/the-evolved-packet-core*

[4] "¿Qué es el dividendo digital y en qué consiste su liberación?". *Televisiondigital.gob.es*, 2016. *http://www.televisiondigital.gob.es/DividendoDigital/Paginas/que-es-dividendo-digital.aspx*

[5] "LTE despega en España". *Redestelecom.es*, 2013. *http://www.redestelecom.es/comunicaciones/reportajes/1067797000303/lte-despega-espana.1.html*

[6] "El largo camino de 4G LTE". *Redestelecom.es*, 2015. *http://www.redestelecom.es/infraestructuras/reportajes/1081857001803/largo-camino-4g-lte.1.html*

[7] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO,. "Informe de cobertura de banda ancha de 2015", 2015.

[8] "Cobertura de LTE en España a nivel autonómico". *Minetur.gob.es*, 2015. *http://www.minetur.gob.es/telecomunicaciones/banda-ancha/cobertura/consulta/Paginas/consulta-cobertura-banda-ancha.aspx*

[9] "Información de cobertura banda ancha en España, agregada por operador y desglosada por tecnología.". *Minetur.gob.es*, 2015. *http://www.minetur.gob.es/telecomunicaciones/banda-ancha/cobertura/Paginas/informacion-cobertura.aspx*

[10] Secretaría de estado de telecomunicaciones y para la sociedad de la información,. "Cuadro nacional de atribución de frecuencias (CNAF)", 2016.

[11] Spectrummonitoring,. "Spain Smartphone Frequencies", 2016. *http://www.spectrummonitoring.com/frequencies/*

[12] BandaAncha,. "Frecuencias y bandas LTE en España", 2016. *https://wiki.bandaancha.st/Frecuencias_y_bandas_LTE_en_España*

[13] "About Us". *openairinterface.org*, 2016. *http://www.openairinterface.org/?page_id=72*

[14] *E-UTRAN USER GUIDE*, EURECOM, 2016. *https://gitlab.eurecom.fr/oai/openairinterface5g/*

[15] Tan, Kun; Zhang, Jiansong; Fang, Ji; Liu, He; Ye, Yusheng; Wang, Shen; Zhang, Yongguang; Wu, Haitao; Wang, WeiM. Voelker, Geoffrey. "Sora: High Performance Software Radio Using General Purpose Multi-core Processors".

[16] Nohrborg, Magdalena. "LTE Overview". *3gpp.org* . *http://www.3gpp.org/technologies/keywords-acronyms/98-lte*

[17] Laner, Markus; Svoboda, Philipp; Romirer-Maierhofer, Peter; Nikaein, Navid; Ricciato, FabioRupp, Markus. "A comparison between one-way delays in operating HSPA and LTE networks". *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), 2012 10th International Symposium on*, 2012, pp. 286-292. *http://ieeexplore.ieee.org/iel5/6247524/6260438/06260469.pdf?arnumber=6260469*

[18] "UHD (USRP Hardware Driver™)". *ettus.com*, 2016.
https://www.ettus.com/sdr-software/detail/usrp-hardware-driver
[19] "USRP Hardware Driver and USRP Manual: Firmware and FPGA Images". *ettus.com*, 2016. *http://files.ettus.com/manual/page_images.html*
[20] "USRP B200 and B210 - USB 3.0 Streaming Rate Benchmarks". *ettus.com*, 2016.
https://www.ettus.com/kb/detail/usrp-b200-and-b210-usb-30-streaming-rate-benchmarks
[21] "GNU Radio Opens an Unseen World". *WIRED*, 2016.
http://archive.wired.com/science/discoveries/news/2006/06/70933?currentPage=all
[22] "Announcing the USRP B200 and USRP B210, the first fully integrated USRP devices with continuous RF coverage from 70 MHz –6 GHz". *ettus.com*, 2016.
https://www.ettus.com/news/article/36
[23] "USRP Bandwidth". *ettus.com*, 2016. *https://www.ettus.com/kb/detail/usrp-bandwidth*
[24] "USRP B200 (Board Only)". *ettus.com*, 2016.
https://www.ettus.com/product/details/UB200-KIT
[25] "NI FPGA -National Instruments". *Ni.com*, 2016. *http://www.ni.com/fpga/esa/*
[26] "Google Nexus 5 full specs". *Phone Arena*, 2016.
http://www.phonearena.com/phones/Google-Nexus-5_id8148/fullspecs
[27] "Openair5G User". *Lists.eurecom.fr*, 2016.
https://lists.eurecom.fr/sympa/arc/openair5g-user/2016-04/msg00195.html
[28] "Towards Open Cellular Ecosystem". *Openairinterface.org*, 2016.
http://www.openairinterface.org/?page_id=864
[29] "Openair5G User". *Lists.eurecom.fr*, 2016.
https://lists.eurecom.fr/sympa/arc/openair5g-user/2015-12/msg00122.html
[30] "openLTE / Programming you own USIM card". *Sourceforge.net*, 2016.
https://sourceforge.net/p/openlte/wiki/Programming%20you%20own%20USIM%20card/
[31] "Confidentiality Algorithms". *3gpp.org*, 2016.
http://www.3gpp.org/specifications/60-confidentiality-algorithms
[32] "OpenBTS / Mailing Lists". *Sourceforge.net*, 2016.
https://sourceforge.net/p/openbts/mailman/message/33339542/
[33] *Specification of the MILENAGE Algorithm Set*, 3GPP TR 35.909, 2016.
[34] News, RCR. "APN LTE- What's an APN and How Is It Used in LTE?". *RCR Wireless News*, 2014. *http://www.rcrwireless.com/20140509/evolved-packet-core-epc/apn-lte*
[35] "Overview of APNs - Technical Documentation - Juniper Networks". *Juniper.net*, 2016.
http://www.juniper.net/techpubs/en_US/junos-mobility12.1/topics/concept/gateways-mobility-apn-overview.html
[36] "USRP Hardware Driver and USRP Manual: General Application Notes". *Files.ettus.com*, 2016. *http://files.ettus.com/manual/page_general.html#general_ounotes_underrun*
[37] "Detecting underflows with uhd_usrp_sink". *Lists.ettus.com*, 2016.
http://lists.ettus.com/pipermail/usrp-users_lists.ettus.com/2013-June/006893.html
[38] "Niveles de Exposición". *Geoportal.minetur.gob.es*, 2016.
https://geoportal.minetur.gob.es/VCTEL/vcne.do

[39] Gomez-Miguelez, Ismael; Garcia-Saavedra, Andres; D. Sutton, Paul; Serrano, Pablo; Cano, CristinaJ. Leith, Douglas. "srsLTE: An Open-Source Platform for LTE Evolution and Experimentation", 2016.
[40] "Clocks - OpenBTS". *Openbts.org*, 2016. *http://openbts.org/w/index.php?title=Clocks*
[41] *Evolved Universal Terrestrial Radio Access (E-UTRA); TDD Home eNode B (HeNB) Radio Frequency (RF) requirements analysis*, 3GPP TS 36.922.
[42] "Mscgen: A Message Sequence Chart Renderer". *Mcternan.me.uk*, 2016. *http://www.mcternan.me.uk/mscgen/*
[43] Krishna Prakash and Balachandra,. "AUTHENTICATION AND KEY AGREEMENT IN 3GPP NETWORKS".
[44] *EPS Overview and Security*, NEC Corporation, 2009. *https://niksun.com/presentations/day2/NIKSUN_WWSMC_July26_AnandRPrasad.pdf*
[45] Agustí Comes, Ramon; Bernardo Álvarez, Francisco; Casadevall Palacio, Fernando; Ferrús Ferré, Ramón; Pérez Romero, JordiSallent Roig, Oriol. *LTE*, [Madrid]: Fundación Vodafone España, 2010.
[46] Comisión nacional de los mercados y la competencia,. "ACUERDO POR EL QUE SE APRUEBA LA PROPUESTA SOBRE LA CONVENIENCIA DE MANTENER O FIJAR LÍMITES SUPERIORES EN LA DISPONIBILIDAD DE FRECUENCIAS POR UN MISMO OPERADOR, DE ACUERDO AL ARTÍCULO 8 DEL REAL DECRETO 458/2011, DE 1 DE ABRIL.", 2015.
[47] "Openairsystemrequirements". *Gitlab.eurecom.fr*. N.p., 2016. Web. May 2016.
[48] *Evolved Universal Terrestrial Radio Access (E-UTRA): Radio Resource Control (RRC) Protocol specification*, 3GPP TS 36.311
[49] *Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures*, 3GPP TS 36.213
[50] Duplexers for OAI, EURECOM Mailing lists, *https://lists.eurecom.fr/sympa/arc/openair5g-user/2016-06/msg00111.html*
[51] Checko, Aleksandra et al. "Cloud RAN For Mobile Networks—A Technology Overview". IEEE Communications Surveys & Tutorials 17.1 (2015): 405-426. Web. 12 June 2016.
[52] A. Dawson, M. K. Marina, and F. J. Garcia. On the Benefits of RAN Virtualization in C-RAN Based Mobile Networks. In Proc. European Workshop on Software-Defined Networks (EWSDN), 2014.
[53] How to Connect OAI eNB with COTS UE via the OAI RRH GW, Gitlab Eurecom, Web. June 2016