Measurement of 4G LTE Cells with SDR Technology

D. Gutierrez, F. Gimenez, C. Zerbini, and G. Riva

***Abstract*—Today, measurements on wireless mobile systems require specific, high-cost instruments. This hinders both its access from academia for education and research, and its widespread use by service providers for optimization of their networks. To address these problems, we present and demonstrate choices for measurement of 4G LTE access networks through open-source Software Defined Radio (SDR) tools. As first contribution, we survey and sort the most relevant measurements present in commercial equipment for measurement of LTE cells. In second place, we survey and compare available SDR libraries for this application, describing their technical details and trade-offs. As third and main contribution, we combine these tools for selected measurements, demonstrating its application in field measurement cases. The applications of our work go from teaching, research and development, to health monitoring of in-service networks.**

***Index Terms*—LTE, SDR, Open Source, eNodeB.**

I. Introducción

En la actualidad, la medición y diagnóstico de redes móviles de cuarta generación (Long Term Evolution, LTE) [1] se realiza mediante instrumental de gran complejidad y muy elevado costo, sólo afrontable por grandes prestadores de servicio. Esta situación acota fuertemente el acceso a tales mediciones para su uso en el ambiente académico con fines de enseñanza y de investigación/desarrollo. Asimismo, limita las posibilidades de monitoreo de parámetros específicos en múltiples locaciones a fin de controlar y optimizar la salud de estas redes.

La tecnología SDR permite implementar múltiples sistemas de comunicaciones sobre un mismo hardware, entre ellos las redes de telefonía móvil de cuarta generación. En particular, poseen potencial para implementar mediciones que actualmente se presentan sólo en instrumentos específicos de muy alto costo. Si bien existe una gran variedad de proyectos que permiten extraer información de las redes LTE, no existe trabajo que procese esta información para realizar mediciones. Sobre esta base, el presente trabajo pretende demostrar cómo las herramientas SDR se pueden aplicar en casos concretos de medición.

El artículo se estructura en las siguientes secciones. En la Sec. II, se repasan los sistemas SDR y las redes 4G LTE. En la Sec. III, se investigan los trabajos previos en SDR y se clasifican las mediciones de interés. Sobre esta base, en la Sec. IV se detalla la implementación de las plataformas necesarias. En la Sec. V se presentan los resultados obtenidos. Finalmente, en la Sec. VI se plantean conclusiones y trabajo futuro.

D. Gutiérrez, F. Giménez, C. Zerbini and G. Riva are with the Group for Research and Transfer in Advanced Electronics (GInTEA), Universidad Tecnológica Nacional, Facultad Regional Córdoba (see http://www.investigacion.frc.utn.edu.ar/gintea/).

II. Radio Definida por Software y Sistemas LTE

A. Radio Definida por Software

El flujo de procesamiento en un sistema SDR consta de dos secciones principales: el *dominio analógico*, y el *dominio digital* (ver Fig. 1). El primero de ellos involucra elementos tales como amplificadores de potencia (TX) o de bajo ruido (LNAs, RX), mezcladores, osciladores, filtros pasa-bajos y pasa-banda, amplificadores de ganancia variable (VGAs), y DACs para corrección de errores de tensión continua, integrados en un chip de RF programable (RFIC). La salida de este dominio consta de la señal modulada analógica en una frecuencia intermedia (IF) determinada, comunmente 0 Hz o una frecuencia muy baja. A continuación se encuentra el bloque de conversión AD y DA, cuya tasa de muestras depende del ancho de banda de modulación. El dominio digital, en tanto, es donde reside la inteligencia de un sistema SDR para realizar procesamiento de banda base, adaptándose a distintos sistemas y modulaciones; es donde se extrae la información útil de la señal modulada. Consta de una sección de procesamiento digital por hardware, comúnmente un FPGA, un DSP o un chip de propósito específico (ASIC), que realiza tareas de extracción de canales de interés y conversión de tasas de muestreo para su inter-conexión con una etapa de software. En esta última se realizan tareas de capa física tales como modulación/demodulación, codificación de canal, ecualización, y codificación; y tareas de capas superiores como gestión de acceso al medio y procesamiento de tramas.

B. Sistemas Móviles 4G LTE

El sistema de telefonía móvil de cuarta generación *Long-Term Evolution (LTE)* logra alta tasa de transferencia de datos y eficiencia espectral a través del uso de múltiples subportadoras ortogonales entre sí (Orthogonal Frequency Divison Multiplex, OFDM y su variante de acceso al medio, OFDMA), las cuales son moduladas por flujos de datos a tasas relativamente bajas. Adicionalmente, considera el uso de múltiples transmisores y receptores (Multiple Input Multiple Output, MIMO). De este modo, se logran tasas de datos teóricas de 100 Mbps en downlink con ancho espectral de 20 MHz. La Fig. 2 ilustra el procesamiento digital necesario para generar una señal OFDM, que para el caso más exigente (20MHz o 1200 sub-portadoras) involucra realizar una transformación de Fourier inversa (IFFT) desde 2048 bins a tasa 15 kHz hacia 2048 muestras temporales a tasa 30.72 MHz. Estas son

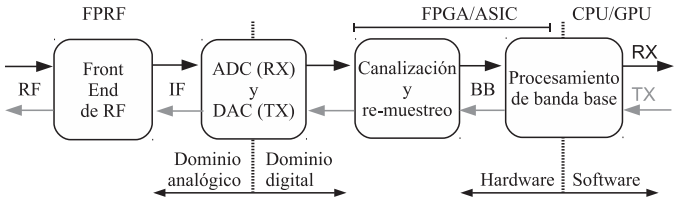

Fig. 1. Esquema general de un sistema SDR.

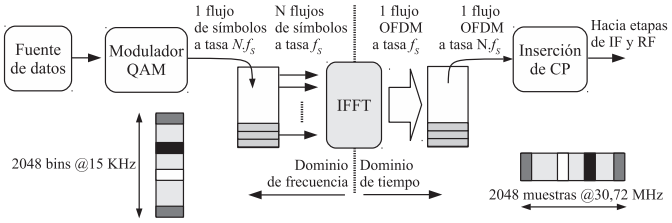

Fig. 2. Procesamiento OFDM en un transmisor de DL.

finalmente trasladadas en frecuencia a su portadora final en las etapas analógicas.

La grilla tiempo-frecuencia para una trama Tipo 1 (FDD) LTE se muestra en la Fig. 3, junto con el significado de cada canal. Cada símbolo en el tiempo es resultante de la contribución de múltiples sub-portadoras ortogonales entre sí, distanciadas cada una a 15 kHz. La condición de ortogonalidad implica que, en el dominio de la frecuencia, la interferencia entre sub-portadoras adyacentes es mínima en los puntos de interés, aún con solapamiento entre sus contenidos espectrales. Según los requerimientos de cada canal físico, las sub-portadoras se modulan mediante distintos esquemas, tales como BPSK/QPSK (para robustez frente al ruido en canales de control) o 16QAM / 64QAM (para lograr alta tasa de transferencia en canales de datos con buenas condiciones de enlace).

La tasa de muestreo utilizada es 30.72 MHz. La mínima unidad es un *slot*, el cual se compone de 7 símbolos con prefijo cíclico (CP) normal, o 6 símbolos con CP extendido, y abarca 15360 muestras totalizando 0.5 ms. Dos slots componen un *sub-frame* con duración de 1 s. Finalmente, 10 sub-frames componen un *frame* LTE de 10 ms de duración.

El bloque constituido por 12 sub-portadoras en la frecuencia y 1 slot en el tiempo se denomina *Resource Element (RE)*, mientras que 12 subportadoras en 1 sub-frame constituyen un *Resource Block (RB)*, que es la mínima unidad de asignación a usuarios. Un frame Tipo 1, que es el más utilizado, combina sub-frames de tres tipos, indicados como A, B y C en la Fig. 3, cada uno de los cuales incluye distintos canales multiplexados. Estos canales transportan información de relevancia en distintas etapas de la comunicación [1].

III. Análisis de Problema

A. Trabajos Relacionados

Como primer aporte de nuestro trabajo, se compilan y comparan los principales trabajos existentes respecto a la información que ellos extraen de la red. Sus principales características se resumen en la Tabla I.

- *OpenLTE.* El principal objetivo de este proyecto es crear una estación base (eNB) básica [2]. Brinda asimismo scripts para simulación y configuración de tarjetas SIM. No incluye herramientas para medición de la red, si bien reporta todos los procedimientos que ejecuta. Actualmente se encuentra discontinuado.
- *gr-LTE.* Desarrollado como una librería de gnuradio [3], tiene el objetivo principal de sincronizarse con una señal LTE, en tiempo real o previamente generada, y decodificar el Master Information Block (MIB) contenido en el Physical Broadcast Channel (PBCH).
- *srsLTE.* Combina elementos de OpenLTE con la librería *libLTE* [4] [5]. Actualmente, la compañía Software Radio Systems (SRS) desarrolla dos productos principales, uno orientado a aplicación comercial y el otro al uso en investigación:
  - El software *Airscope*, que es un analizador de interfaz de aire LTE basado en SDR, con capacidades de decodificación en tiempo real. Decodifica el canal de downlink PDCCH (ver Fig. 3) y provee estadísticas de desempeño tanto a nivel de celda como a nivel de usuario. No obstante, requiere para su uso de licencia comercial, y no provee información de calidad de modulación.
  - La librería open-source *srsLTE* con sus aplicaciones *srsUE* y *srsENB*. srsLTE es una librería altamente modular, implementada en C, pensada como un conjunto de funciones DSP optimizadas. Algunas de sus características destacables son el soporte de LTE Release 15, con anchos de banda hasta 20 MHz, captura de la mayoría de los canales de DL y UL, y ecualizadores/decoders optimizados. En tanto, srsUE y srsENB son implementaciones de un UE (móvil) y de un eNB (celda) utilizando elementos de srsLTE.
- *Open Air Interface (OAI).* Este proyecto es el más completo, con una gran comunidad trabajando activamente [6]. Posee la capacidad de realizar mediciones e implementar una red LTE completa, aunque su instalación y configuración es excesivamente compleja para nuestros fines.
- *LTE Cell Scanner / LTE Cell Tracker.* Este es un proyecto exclusivamente diseñado para utilizarse con hardware SDR de bajo costo, tal como los dongles RTL-SDR, los cuales son sólo receptores y presentan algunas limitaciones, como ancho de banda menor a 3 MHz, variada estabilidad (100 PPM en las versiones más comunes, y hasta 1 PPM teórico en versiones optimizadas), y alcance en frecuencia hasta 1.7 GHz. Desarrollado por Evrytania LLC [7], este proyecto no se incluye en la Tabla I por no ser directamente comparable a los demás. Aun así, como se discute en la Sec. IV, es el único compatible al momento para utilizar dongles SDR. Como característica a destacar, este proyecto provee aplicaciones que decodifican el System Information Block 1 (SIB-1).

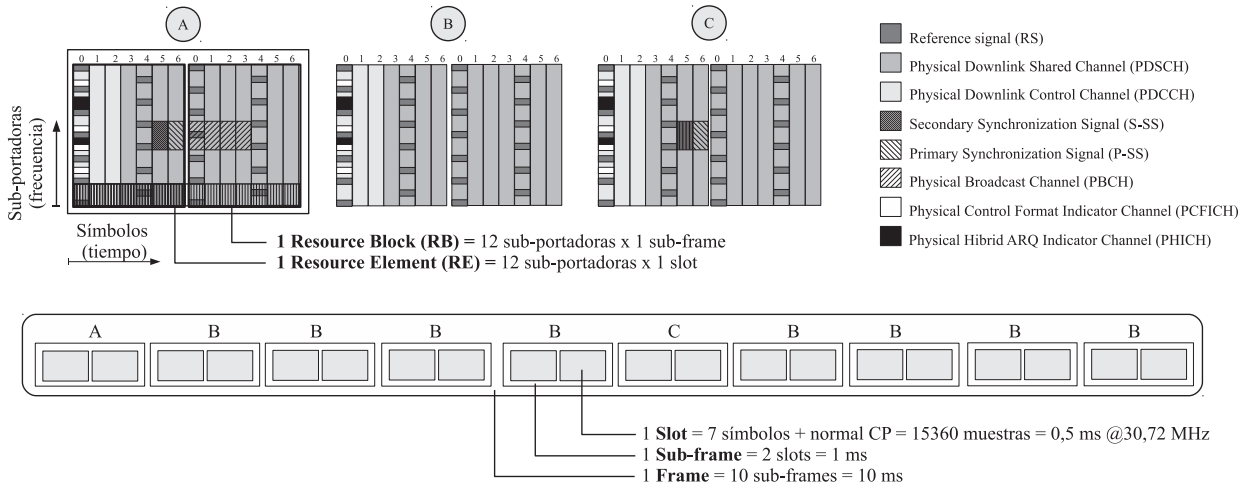

Fig. 3. Grilla tiempo-frecuencia en un frame LTE Tipo 1 (FDD).

B. Mediciones e Instrumentación para Señales LTE

A fin de abordar casos prácticos de medición mediante las herramientas mencionadas, el segundo aporte de este trabajo consiste en compilar e investigar las prestaciones de instrumentos comerciales típicos. Como casos de referencia, se investigaron las características de los equipos Anritsu BTS/Cell/Spectrum Master [8] y Rohde & Schwarz FSH Spectrum Analyzer [9], así como los analizadores vectoriales de las series Agilent PSA/MXA/EXA junto a su software 89601A VSA [10]. Nos concentramos en el caso de mediciones *de capa física en transmisión de Downlink, mediante instrumentos de campo*. Las mediciones de interés son:

1) Mediciones de calidad de radiofrecuencia (RF)
   a) Potencia y ancho de banda de canal
   b) Potencias en ON y OFF (sólo para frames TDD)
   c) Emisiones fuera de banda
      - Relación de fuga de canal adyacente
      - Máscara de emisión espectral
   d) Piso de ruido en recepción: interferencia en UL
2) Mediciones de calidad de modulación
   a) Magnitud de Error Vectorial (EVM) pico y RMS
      - Según canal o señal: PBCH (control), PDSCH (datos), PCFICH, PSS, SSS
      - Según modulación: QPSK, 16QAM, 64QAM
   b) Potencia de señales de soporte
      - Señales de sincronismo: PSS y SSS
      - Potencia en la señal de referencia (RS)
   c) Error o corrimiento de frecuencia
   d) Error de alineación de tiempo

C. Discusión

Analizando los trabajos relacionados se observa que, si bien todos ellos implementan procesamiento digital para sistemas LTE y ofrecen cierta información sobre la red, ninguno tiene en cuenta las mediciones más relevantes para su aplicación en campo.

En el caso de OpenLTE [2], si bien se trata de una implementación completa, no existe documentación que exponga cuidadosamente los resultados obtenidos en hardware. Esto, sumado a su obsolescencia, hace muy difícil una ponderación de sus resultados. Los autores de gr-LTE [3], por su parte, reportan detalladamente el procesamiento involucrado en un receptor de DL LTE y se enfocan luego en el análisis de su consumo computacional en una plataforma basada en GPP. OAI [6], en tanto, no considera las mediciones planteadas y se perfila más bien como una plataforma de experimentación con mediciones auxiliares. Evrytania LLC [7], en tanto, provee cierta información sobre celdas pero no documenta mediciones.

srsLTE resulta el trabajo más cercano al nuestro. En [4], se reportan abundantes resultados centrados en su aplicación como celda LTE. Sin embargo, su posible aplicación para medición es propietaria [5], lo cual dificulta mucho su uso en investigación.

De lo expuesto, las dos falencias que presenta en general el trabajo previo de libre acceso son limitada publicación de resultados, y falta de mediciones acorde a las necesidades reales para ajuste de equipos y detección de problemas en campo. Esto limita su adopción, tanto en el ambiente académico como frente a las necesidades de la industria.

Considerando estas necesidades, se plantea como tercer y principal aporte mejorar el impacto de estos trabajos en escenarios de medición de campo de redes LTE.

IV. DESARROLLO

Como se mencionó, LTE en su canal de DL, trabaja con un esquema de grilla tiempo-frecuencia con anchos de banda y modulaciones variables. Las mediciones, por su parte, pueden ser *pasivas*, donde se observa la red, o *activas*, donde el instrumento debe integrarse a la red e interactuar con el eNB. En este trabajo nos ocupamos únicamente de las mediciones pasivas. El procedimiento general para acceder a la información necesaria se ilustra en la Fig. 4 y se detalla a continuación:

TABLA I
PROYECTOS DE CÓDIGO ABIERTO PARA APLICACIONES LTE CON SDR

Características	OpenLTE	gr-LTE	srsLTE	Open Air Interface
Lanzamiento / Últ. Update	2012 / 2017	2013 / 2013	2015 / 2019	2016 / 2019
Lenguaje	C++	C++, Python	C/C++	C
Dificultad de instalación	media	media	baja	alta
Legibilidad de código	muy buena	buena	excelente	buena
Implementa UE/eNB/EPC	× / ✓/ ×	× / × / ×	✓/ ✓/ ✓	✓/ ✓/ ✓
Mediciones	×	✓	✓	✓
Licencia	AGPLv3	GPLv3	AGPLv3	OAI 5G y Apache V2.0
Soporte de Hardware	OsmoSDR	USRP, LimeSDR, BladeRF	USRP, LimeSDR, BladeRF	ExpressMIMO2, USRP

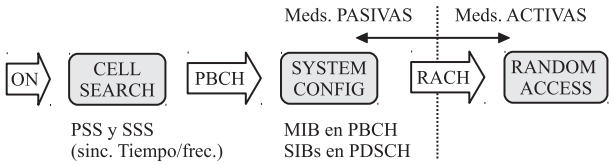

Fig. 4. Pasos necesarios para realizar mediciones en LTE.

1) El instrumento realiza el procedimiento de *cell search* para sincronizarse con la red y obtener las señales de sincronismo primario y secundario (PSS y SSS) con el ID físico de las celdas.
2) Posteriormente, se recupera el PBCH conteniendo el MIB con información esencial del sistema, como el ancho de banda utilizado, número de antenas y número de secuencia de frame.
3) Como tercera etapa, se recupera la información de scheduling del SIB-1, transportado en el PDSCH, a fin de conocer la periodicidad de los 31 tipos de SIBs necesarios para otras etapas del procesamiento.
4) Finalmente, el instrumento puede buscar el SIB Type 2 (SIB-2), que le permitirá realizar el procedimiento de *random access* mediante el Primary Random Access Channel (PRACH) para abordar mediciones activas.

Cabe mencionar que, para realizar estos pasos, se debe saber en qué zonas del espectro o Resource Blocks (RBs) se encuentran los SIBs. Para ello, el Physical Downlink Control Channel (PDCCH), ubicado al comienzo de cada subframe, informa a todos los UEs acerca de la posición de los SIBs en la grilla tiempo-frecuencia. En este contexto, se asigna a los UEs un identificador especial predefinido, el *System Information-Radio Network Temporary Identifier (SI-RNTI)*.

Asimismo, a fin de decodificar correctamente la señal, el instrumento se debe sincronizar en tiempo y en frecuencia según los siguientes procedimientos:

- Para sincronizar en tiempo, interesa recuperar el clock de muestreo, así como los comienzos de símbolo y de frame; mientras que en el caso de frecuencia interesa su desviación en el receptor respecto al transmisor. A fin de recuperar el clock de muestreo y el comienzo de símbolo, se auto-correlaciona el prefijo cíclico (CP) incluido en la señal como información redundante en el intervalo de un símbolo de duración. Las señales PSS y SSS, en tanto, se utilizan para recuperar el comienzo de frames.
- Para obtener la desviación de frecuencia, en tanto, se realizan dos pasos: primero, la señal PSS recibida se correlaciona contra las posibles secuencias de Zadoff-Chu [10], a fin de obtener la parte entera de la desviación (Integer Frequency Offset, IFO). En segundo lugar, se obtiene la parte fraccional de la desviación (Fractional Frequency Offset, FFO) observando la fase del máximo detectado al correlacionar el CP durante una ventana de un símbolo OFDM.

En este trabajo se utilizan dos plataformas hardware. Como plataforma principal, y por razones de simplicidad, se utiliza una computadora basada en un microprocesador de propósito general (GPP) Intel i7, combinada con la placa SDR *Ettus USRP B200*, con ancho de banda máximo 56 MHz, rango de frecuencia 50 MHz - 6 GHz, e interfaz USB 3.0. Posteriormente, a fin de explorar las limitaciones de una plataforma embebida de costo mínimo, se utiliza una PC embebida Raspberry Pi 3B+ en combinación con un Dongle RTL-SDR V3, receptor con ancho de banda máximo 2.56 MHz, rango de frecuencia 24 - 1766 MHz, e interfaz USB 2.0.

A. Aplicación de Gr-lte y Gnuradio

La librería gr-lte utiliza como framework las librerías del proyecto gnuradio. Esto le aporta gran facilidad para re-utilización de los bloques DSP en distintos casos de aplicación, a través del entorno gráfico *gnuradio-companion* y sus herramientas relacionadas. Por contraparte, esta dependencia requiere necesariamente la instalación previa de gnuradio y sus librerías asociadas, tales como C++ *Boost* [11] o *Vector Optimized Library of kernels (VOLK)* [12], las cuales pueden complicar su uso en ciertas plataformas hardware.

Gr-lte provee un diagrama de flujo citado en [3], que permite capturar señales en dos escenarios, que se diferencian fundamentalmente en la capacidad de cómputo requerida:

1) Medición *online* sobre tráfico en tiempo real.
2) Medición *offline* sobre datos capturados previamente mediante otras herramientas, como OpenLTE o *usrp_capture* de srsLTE.

B. Aplicación de SrsLTE

A fin de evaluar esta herramienta respecto a nuestros objetivos, se compilan las librerías srsLTE, srsUE y srsENB y

```
Found 3 cells
Found CELL 2125.0 MHz, EARFCN=2100, PHYID=59, 50 PRB, 4 ports, PSS power=-26.6 dBm
Found CELL 2125.2 MHz, EARFCN=2102, PHYID=2, 125 PRB, 1 ports, PSS power=-26.7 dBm
Found CELL 2137.5 MHz, EARFCN=2225, PHYID=177, 75 PRB, 2 ports, PSS power=-18.9 dBm
```

(a)

```
CFO:  +3.0179 kHz, SFO: -74.3200 Hz, RSSI: -115.5 dBm, RSSI/ref-symbol: -78.8 dBm, RSRP: -84.6 dBm, RSRQ:  -9.4 dB, SNR:   9
CFO:  +3.0179 kHz, SFO: -74.3200 Hz, RSSI: -115.5 dBm, RSSI/ref-symbol: -78.8 dBm, RSRP: -84.6 dBm, RSRQ:  -9.4 dB, SNR:   9
CFO:  +3.0179 kHz, SFO: -74.3200 Hz, RSSI: -115.5 dBm, RSSI/ref-symbol: -78.8 dBm, RSRP: -84.6 dBm, RSRQ:  -9.4 dB, SNR:   9
CFO:  +3.0179 kHz, SFO: -74.3200 Hz, RSSI: -115.5 dBm, RSSI/ref-symbol: -78.8 dBm, RSRP: -84.6 dBm, RSRQ:  -9.4 dB, SNR:   9
```

(b)

Fig. 5. srsLTE: (a) proceso de búsqueda de celdas, (b) monitoreo de una celda particular.

sus aplicaciones asociadas. En este proceso, se destacan los siguientes aspectos. Por un lado, estas librerías dependen del uso de instrucciones *Single Instruction Multiple Data (SIMD)* tales como Intel SSE4.1 y AVX, en particular para el Turbo Decoder utilizado a 100 Mbps. Si bien los autores mencionan que se puede deshabilitar esta optimización reduciendo el desempeño del decoder a 25 Mbps, en nuestro caso sólo se pudo compilar para plataformas ARM e Intel, sin poder hacerlo para plataformas basadas en procesadores AMD.

C. Migración a Plataforma Embebida

Con el fin de evaluar las limitaciones que impone una plataforma embebida de bajo costo, se considera como plataforma opcional una PC embebida Raspberry Pi 3B+ en combinación con un dongle RTL-SDR. Por su bajo costo, esta opción permitiría la realización de mediciones simultáneas en múltiples locaciones, brindando así una visión más amplia de la red de celdas 4G (E-UTRAN).

En primer término, se instala el OS Ubuntu 18.04.3 LTS x64, junto con las librerías gnuradio y su interfaz gráfica gnuradio-companion. Con estas dependencias, gr-lte puede ser instalado en esta plataforma sin inconvenientes. srsLTE también fue instalado con éxito; aunque requiere ciertas consideraciones sobre esta plataforma por dos motivos muy importantes: el primero es el requerimiento antes mencionado de uso de ciertas características específicas de los procesadores Intel; el segundo se refiere al elevado volumen de datos que el núcleo debe procesar.

Al considerar el uso de un dongle RTL-SDR, surge un inconveniente relevante. Éste reside en que tanto gr-lte como srsLTE asumen que el hardware SDR utiliza el reloj base del sistema LTE de 30.72 MHz y no realizan conversión de tasas de muestreo por software. En el caso de srsLTE, esto es debido a que se soportan todos los canales de LTE, con ancho máximo de 20 MHz. srsLTE soporta oficialmente las plataformas Ettus USRP (driver UHD), BladeRF y LimeSDR (mediante SoapySDR). SoapySDR es una librería neutral que, mediante la conexión de los denominados *device modules*, permite controlar los dongles RTL-SDR; sin embargo, debido a lo antes mencionado, srsLTE no es capaz de configurar correctamente el dispositivo. De este modo, no es posible aplicar gr-lte o srsLTE de modo directo utilizando un dongle RTL-SDR.

Aún así, los canales de control y sincronismo (PSS, SSS, y PBCH) ocupan sólo los 6 RBs centrados en la portadora, totalizando 72 sub-portadoras con ancho de banda 1.4 MHz. Considerando esto, un dongle es adecuado desde el punto de vista teórico para realizar estas mediciones. Las aplicaciones *LTE Cell Scanner* y *LTE Tracker* resultan idóneas para esta aplicación, dado que están diseñadas para capturar sólo estos canales.

Se instalaron ambas aplicaciones, junto con las librerías de C++ *Boost, ITPP y FTTW*, [11] [13] [14] para cálculo matemático y estadístico. Si bien existe una versión reciente de estas aplicaciones con soporte de OpenCL, particularmente resulta que no trabaja apropiadamente con el toolchain *gcc-arm-linux-gnueabihf*. Asimismo, durante el proceso de compilación se deben editar los caminos de búsqueda y los archivos de compilación para adaptarlos a la plataforma utilizada.

V. RESULTADOS

Mediante la combinación de las librerías mencionadas, y teniendo en cuenta las mediciones objetivo, se realizaron experiencias de medición de campo sobre celdas en servicio. Con fines de organización, se analizará la información obtenida según las etapas definidas en la Sec. IV y la Fig. 4.

A. Cell Search, Sincronización e Información General

Para realizar una medición de eNB por aire (Over The Air, OTA) sobre cierta celda, en primer término se debe buscar una localización que provea buena dominancia de su señal primaria de sincronismo (PSS), es decir, un eNB debe estar al menos 10 dB por encima de los demás. La PSS define la cobertura de la celda, con máximo cerca del eNB y mínimo en el punto de handoff. En la Fig. 5(a) se observa la información provista por la herramienta srsLTE durante el proceso de *cell search* en la banda 4 LTE [15]. En esta figura se observa la presencia de tres celdas circundantes, con sus respectivos canales *E-UTRA Absolute Radio Frequency Channel Number (EARFCN)*, PHYID, número de RBs utilizados, cantidad de antenas y potencia de PSS. El PHYID es un número único entre 0 y 503 asignado a celdas LTE, el cual resulta de la combinación jerárquica de un CELL_GROUP (0 a 167) dependiente de la PSS, y un CELL_NUMBER (0 a 2) dependiente de la SSS. Además de servir como identificador unívoco de la celda, este parámetro es fundamental como código de scrambling para separar los

```
Decoding PBCH for cell 132 (N_id_2=0)
MasterInformationBlock ::= {
     dl-Bandwidth: 3
     phich-Config: PHICH-Config ::= {
          phich-Duration: 0
          Phich-Resource: 2
     }
     SystemFrameNumber: 35
     Spare: 00 00
}
Decoded MIB. SFN: 292, offset: 1 frameCnt: 0, State: 1
```

Fig. 6. srsLTE: información sobre canal PBCH y MIB.

datos provenientes de distintos transmisores que llegan al instrumento. En la Fig. 5(a), podemos considerar que la celda de PHYID 177 es la que posee dominancia sobre las demás, si bien no llega a alejarse 10 dB de ellas.

A continuación, se realiza el proceso de sincronismo sobre la celda dominante y se monitorean sus parámetros de interés, como muestra la Fig. 5(b) para el caso de srsLTE.

B. Recuperación y Análisis del PBCH, MIB, y PCFICH

Luego de sincronizar el instrumento con la celda de mayor potencia, esta etapa va un paso más allá, analizando canales esenciales para recuperar información de control y obtener así información sobre la configuración de la celda. Para ello, en primer término se recupera el canal PBCH y se observa el contenido de los campos del MIB transportado en él. En la Fig. 6 se muestran adquisiciones en campo mediante la librería srsLTE, entre ellas el ancho de banda utilizado y el canal PHICH.

En la Fig. 7, en tanto, se observa la información brindada por gr-lte en cuanto al formato del PDCCH, indicado mediante el canal PCFICH. Este canal es puramente físico, y transporta información esencial para la posterior decodificación del canal PDCCH a través del parámetro *Control Format Indicator (CFI)*. El CFI especifica cuántos símbolos OFDM se utilizan como canales de control, a fin de que el receptor sepa dónde encontrar esta información. Define el intervalo de tiempo, medido en símbolos OFDM, asignado al PDCCH para un subframe particular. En el caso observado, los subframes 0 a 9 contienen valores CFI 1 a 3, que implica 1 hasta 3 slots asignados al PDCCH (ver Fig. 3). Finalmente, la Fig. 7 muestra información sobre el *valor de correlación*, que se refiere al valor obtenido durante el proceso de sincronización en base al CP.

Finalmente, se muestra otro caso de captura mediante srsLTE, combinando la etapa de búsqueda/sincronismo (Fig. 8(a)) y decodificación del MIB correspondiente (Fig. 8(b)).

C. Recuperación y Análisis de PDSCH y SIBs

El canal PDSCH transporta los datos de usuario, que no analizamos en este trabajo, así como información de control contenida en los mensajes SIB-1 a SIB-13. De éstos, es de particular interés el mensaje SIB-1, el cual aporta información relativa al estado de la celda, umbrales de potencia mínimos, tiempos asignados para transmisión de datos de usuario, y

```
pcfich_unpack_vfm_0  subframe = 0 CFI = 3 (correlation value = 8.212748)
pcfich_unpack_vfm_0  subframe = 1 CFI = 3 (correlation value = 15.962302)
**** CELLID= 297****
pcfich_unpack_vfm_0  subframe = 2 CFI = 2 (correlation value = 13.367598)
pcfich_unpack_vfm_0  subframe = 3 CFI = 2 (correlation value = 1.022552)
pcfich_unpack_vfm_0  subframe = 4 CFI = 2 (correlation value = 24.952812)
pcfich_unpack_vfm_0  subframe = 5 CFI = 1 (correlation value = 6.116179)
pcfich_unpack_vfm_0  subframe = 6 CFI = 2 (correlation value = 3.437153)
pcfich_unpack_vfm_0  subframe = 7 CFI = 2 (correlation value = 4.179561)
pcfich_unpack_vfm_0  subframe = 8 CFI = 2 (correlation value = 10.788361)
pcfich_unpack_vfm_0  subframe = 9 CFI = 3 (correlation value = 3.611236)
```

Fig. 7. gr-lte: información sobre formato del canal de control (PCFICH) para una celda específica.

```
Searching for cell...
*Found Cell_id: 177 FDD, CP: Normal,
DetectRatio=100% PSR=7.41, Power=1.5 dBm
 Found Cell_id:  0 FDD, CP: Normal, DetectRatio= 0%
PSR=0.00, Power=-inf dBm
 Found Cell_id:  2 FDD, CP: Normal, DetectRatio=100%
PSR=2.26, Power=-11.2 dBm
Decoding PBCH for cell 177 (N_id_2=0)
Setting sampling rate 15.36 MHz
 - Type:    FDD  7,9, FrameCnt: 0, State: 1
 - PCI:     177
 - Nof ports:  2
 - CP:     Normal
 - PRB:     75
 - PHICH Length: Normal
 - PHICH Resources: 1
 - SFN:     588
```

(a)

```
Decoded MIB. SFN: 588, offset: 2
    CFO: +2337,41 Hz
    RSRP: +41,2 dBm | +43,3 dBm
    SNR: +8,3 dB
    TM: 2
    Rb:  0,01 /  0,18 / 0,16 Mbps
         (net/maximum/processing)
     PDCCH-Miss: 58,53%
     PDSCH-BLER: 7,78%
    TB 0: mcs=3; tbs=176
    TB 1: mcs=0; tbs=0
```

(b)

Fig. 8. srsLTE: (a) mediciones sobre celdas disponibles, (b) mediciones referentes a la celda dominante.

```
Searching for cell...
*Found Cell_id: 177 CP: Normal , DetectedRadio=100% PSR=23.32,
    Power=-15.6 dBm
 Found Cell_id:   0 CP: Normal , DetectedRadio=100% PSR=0.00,
    Power=-inf dBm
 Found Cell_id:   0 CP: Normal , DetectedRadio=100% PSR=0.00,
    Power=-inf dBm
Decoding PBCH for cell 177 (N_id_2=0)
-- Asking for clock rate 15.360000 MHz...
-- Actually got clock rate 15.360000 MHz.
-- Performing timer loopback test... pass
Setting sampling rate 15.36 MHz
Decoded MIB.SFN: 0, offset: 1 FrameCnt: 0, State: 1
Decoded SIB1.                                  Close Subscriber Group
Payload: [48 5c 88 69 25 9a 07 6f d0 08 18 31 60 81 04 4c 23 c9 52];
          PLMN id    LAC/TAC  Cell id  Cell Selection Scheduling
```

Fig. 9. srsLTE: mediciones referentes al mensaje SIB-1.

posición en la grilla de los demás mensajes SIB-2 a SIB-13 (opcionales). El mensaje SIB-1 se transmite con periodicidad 80 ms en la sub-muestra 5, para frames múltiplos de 8, y se repite asimismo en frames múltiplos de 2. Como se muestra en la Fig. 9, srsLTE permite acceder a los campos del SIB-1, los cuales se decodifican posteriormente mediante aplicaciones incluidas en la librería *gr-lte-scanner*.

D. Diagramas de Constelación y Gráficas Adicionales

Finalmente, se analizan gráficas y valores de interés para controlar en tiempo real el rendimiento del sistema. En la Fig. 10 se resumen las mediciones de campo realizadas. En primer término, interesan los *diagramas de constelación* discriminados por canal, mostrados en la Fig. 10(a) para el PDSCH, y en la Fig. 10(b) para el PDCCH. A partir de estos diagramas, se puede calcular la *Magnitud del Error Vectorial (EVM)* diferenciada por canales. En referencia a la Fig. 11, el EVM es la relación entre la media cuadrática de los módulos $\{P_1, P_2, ...P_N\}$ y la distancia P_{REF} del símbolo teórico al centro de constelación. El EVM es la medida fundamental de calidad de modulación, ya que determina la tasa de error del sistema, y en definitiva la tasa de datos práctica en cada canal.

Otra gráfica de interés es la respuesta en frecuencia del canal, ilustrada en la Fig. 10(c). Esta gráfica se obtiene a partir de las *Reference Signals (RSs)* distribuidas en la grilla tiempo-frecuencia, y da idea de la ecualización necesaria para equiparar las potencias de los diferentes canales. Finalmente, la gráfica de la Fig. 10(d) muestra en tiempo real la tendencias estadísticas de correlación cruzada del canal PSS. Este parámetro es indicador de la probabilidad de caída de sesiones o llamadas a nivel de usuario en la red LTE.

E. Primeras Experiencias Sobre Plataforma Embebida

Como experiencia adicional, se realizaron ensayos exploratorios sobre la plataforma embebida detallada en la Sec. IV. En este caso, el alcance en frecuencia del dongle utilizado limita su aplicación a bandas por debajo de 1.7 GHz. Considerando esto, se ejecuta la aplicación LTE Cell Scanner para el rango de frecuencias [869-984 MHz], banda 5 según [15]. En la Fig. 12 se observa la detección de varias celdas en esta banda. Analizando la primera de ellas, observamos su Cell ID 168, en 869.6 MHz. La frecuencia de offset entre el receptor y la antena transmisora es 5.22 kHz. El nivel de potencia en el receptor es -16.3 dBm, con Prefijo Cíclico Normal (6 símbolos). Esta celda ocupa 255 Resource Blocks, mientras que el PHICH no es conocido en este caso. El último campo corresponde a la deriva del oscilador a cristal del dongle; este valor permite corregir la frecuencia por software a fin de obtener tiempos de detección de celdas más cortos. Esto es, la primera vez que el dongle realiza la búsqueda de las celdas, éste presenta un valor de corrimiento de frecuencia mayor a 100 ppm, demorando aproximadamente 6 segundos la busqueda por portadora. Luego, con 10 ppm de desplazamiento, el tiempo de busqueda se reduce a 1 segundo. Conociendo la frecuencia de la celda de interés y el factor de corrección del cristal correspondiente, LTE Cell Scanner permite especificar el valor de ppm como uno de los parámetros de configuración, siendo el valor mínimo de 10 ppm.

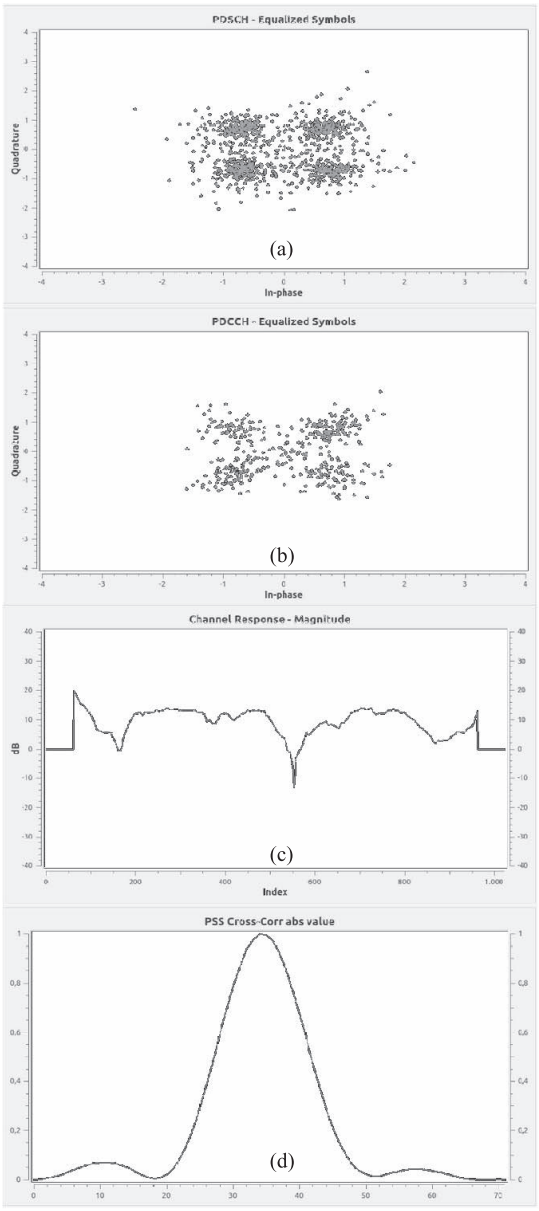

Fig. 10. srsLTE: (a, b) diagramas de constelación, (c) respuesta del canal inalámbrico, (d) sincronismo.

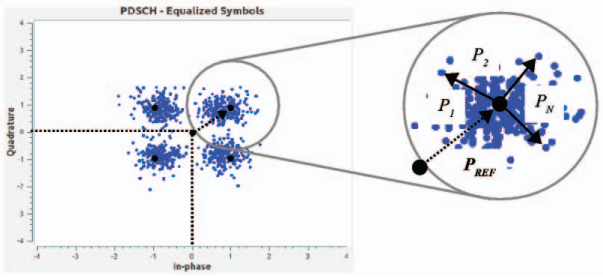

Fig. 11. srsLTE: cálculo de EVM sobre un canal en particular.

```
Detected the following cells:
A: #antenna ports C: CP type ; P: PHICH duration ; PR: PHICH resource type
CID A      fc    foff RXPWR C nRB P  PR CrystalCorrectionFactor
168255  869.6M  5.22k -16.3 N 255 U UNK 1.0000060004530020308
 89255  869.6M -31.5k -16.7 N 255 U UNK 0.9999637635235623101
408255  869.6M -51.8k -16.7 N 255 U UNK 0.9999404567029082091 5
 44255  869.6M -11.9k -16.9 E 255 U UNK 0.9999862851211266390 2
200255    870M -20.4k -16.5 N 255 U UNK 0.9999765301103246129
350255  869.6M -16.9k -17.3 N 255 U UNK 0.9999805765629168341 5
 31255  869.6M   -32k -17.3 E 255 U UNK 0.9999631615740297574 4
337255  869.7M -5.41k -16.1 E 255 U UNK 0.9999937788094401813 8
105255  869.7M -15.9k -16.5 N 255 U UNK 0.9999817508888992900 8
 52255    870M -4.02k   -16 N 255 U UNK 0.9999953800710812412 7
482255  869.7M -11.5k -16.6 N 255 U UNK 0.9999868122511501589 1
 28255  869.7M -19.4k -16.7 N 255 U UNK 0.9999776865217250287 9
 29255  869.7M -47.7k -16.7 E 255 U UNK 0.9999451657736350140 8
269255  869.7M -30.5k -16.8 E 255 U UNK 0.9999648918891477222 8
451255  869.7M -24.3k -16.9 E 255 U UNK 0.9999721153655510841 3
191255  869.7M    12k -16.9 E 255 U UNK 1.0000137507548252369
391255  869.7M -22.7k   -17 N 255 U UNK 0.9999738466759907629 1
226255  869.7M -34.3k   -17 E 255 U UNK 0.9999605714618151619 5
```

Fig. 12. Celdas LTE detectadas con LTE Cell Search en el rango de 869-894 MHz.

VI. Conclusión

En base a la experiencia obtenida, comprobamos que las mediciones sobre redes móviles, actualmente sólo realizables mediante instrumentos dedicados de elevado costo, pueden llevarse a cabo efectivamente combinando y adaptando herramientas SDR de código abierto. Estas técnicas permiten a la academia realizar investigación sobre redes móviles con recursos moderados, así como estudiar y optimizar la salud de estas redes.

Como trabajo futuro, se deben contrastar los resultados obtenidos con los arrojados por un instrumento comercial utilizado como patrón, a fin de calibrar la plataforma SDR. Asimismo, y con el fin de mejorar el compromiso costo vs. prestaciones, se deben explorar opciones para ampliar las prestaciones de la plataforma embebida.

Agradecimientos

El presente trabajo fue financiado mediante el PID UTN CCUTN-CO0004974, *Instrumentación Basada en Tecnología SDR para Medición en Sistemas de Comunicaciones*.

Referencias

[1] R. A. Comes, “LTE: Nuevas Tendencias en Comunicaciones Móviles, ” Fundación Vodafone España, 2010.
[2] “OpenLTE - An open source 3GPP LTE implementation, ” [Online:] http://openlte.sourceforge.net/
[3] J. Demel, S. Koslowski, and F. K. Jondral, “A LTE Receiver Framework Using GNU Radio, ” Journal of Signal Processing Systems, 78(3):313–320, 2015.
[4] I. Gomez-Miguelez, A. Garcia-Saavedra, P. D. Sutton, P. Serrano, C. Cano, and D. J. Leith, “srsLTE: an open-source platform for LTE evolution and experimentation, ” Proc. of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization (WiNTECH ’16). ACM, New York, NY, USA, 25-32, 2016.
[5] P. Sutton, “Examining 4G performance at MWC with AirScope, ” Mobile World Congress 2017.
[6] F. García Espigares, “Prototipo de una estación base 4G usando Open Air Interface”, 2017
[7] LTETools of Evrytania. Disponible: ⟨http://www.evrytania.com/lte-tools⟩. Accedido: Agosto 2019.
[8] *Anritsu BTS Master® MT8220T User Guide,* Anritsu Company, 2018.
[9] *R&S® FSH Handheld Spectrum Analyzer Operating Manual,* Rohde & Schwarz Test and Meaasurement Division, 2015.
[10] *LTE and the Evolution to 4G Wireless – Design and Measurement Challenges*, Agilent Technologies, 2008.
[11] (Agosto 2019) Boost C++ libraries. [Online]. Disponible: ⟨https://www.boost.org/⟩
[12] (Agosto 2019) Vector-Optimized Library of Kernels. [Online]. Disponible: ⟨http://libvolk.org/⟩
[13] (Agosto 2019) ITPP C++ libraries. [Online]. Disponible: ⟨http://itpp.sourceforge.net/4.3.1/⟩
[14] (Agosto 2019) FFTW C libraries. [Online]. Disponible: ⟨http://www.fftw.org/⟩
[15] (Agosto 2019) LTE Bands. [Online]. Disponible: ⟨http://niviuk.free.fr/lte_band.php⟩

Diego Gutiérrez es estudiante avanzado de Ingeniería en Electrónica en la Universidad Tecnológica Nacional (UTN) Facultad Regional Córdoba. Trabajó en los últimos años en proyectos I+D en GInTEA (UTN). Entre sus intereses de investigación se destacan: las redes de comunicaciones de datos, comunicaciones móviles, bases de datos, tecnología de radio definida por software (SDR), programación de sistemas embebidos y FPGAs.

Francisco Giménez obtuvo el título de Ingeniero en Electrónica en la Universidad Tecnológica Nacional (UTN) Facultad Regional Córdoba en el año 2019. Trabajó en los últimos años en proyectos de investigación en GInTEA (UTN). Entre sus intereses de investigación se destacan: las comunicaciones móviles, tecnología de radio definida por software (SDR) y programación de bajo nivel en sistemas embebidos y orientada a objetos.

Carlos Zerbini recibió el grado de Ingeniero en Electrónica de la Universidad Tecnológica Nacional en 2009, y de Doctor en Ciencias de la Ingeniería de la Universidad Nacional de Córdoba en 2015. Desde 2009 es Docente Investigador en la Universidad Tecnológica Nacional, Facultad Regional Córdoba. Entre sus intereses de investigación se encuentran la optimización de redes de datos, diseño en lógica reconfigurable (FPGAs), instrumental y técnicas de medición en electrónica, y sistemas de comunicaciones basados en radio definida por software (SDR).

Guillermo Riva obtuvo el título de Ingeniero en Electrónica en la Universidad Tecnologica Nacional Regional Cordoba, y el Doctorado en Ciencias de la Ingeniería en la Universidad Nacional de Córdoba en 2014. Desde 2014 es Profesor Asociado en UTN-FRC. Trabajó en los últimos años en proyectos en UTN, en UNC y en la industria. Entre sus intereses de investigación se destacan: comunicaciones inalámbricas, redes inalámbricas de sensores, enrutamiento de paquetes de datos basado en contenido y aprendizaje automático en sistemas embebidos.