Analizando Comunicaciones GSM con Radios Definidas por Software (SDR)

Guillermo Riva*†, James Kunst*, Carlos Zerbini*†, Emanuel Airasca*, Eduardo Gonzalez*
*Grupo de Investigacion y Transferencia en Electronica Avanzada (GInTEA)
†Laboratorio de Comunicaciones (LdC)
Universidad Tecnologica Nacional, Facultad Regional Cordoba (UTN-FRC)
Email: griva@frc.utn.edu.ar

***Resumen*—El uso de redes de telefonía móvil GSM es habitual para la mayoría de las personas en la actualidad. Desde el momento en que se activa un teléfono móvil se establece un intercambio de comunicación de datos permanente con la celda de servicio más próxima, principalmente debido al manejo de la movilidad en la comunicación. Sin embargo, procedimientos simples para capturar tramas con el fin de analizar y comprender detalles subyacentes del funcionamiento de la red son poco conocidos. Estos pueden ser utilizados por los prestadores de servicios u organismos de control para detectar problemas en la red. El desarrollo de la tecnología de radio definida por software posibilita analizar las comunicaciones inalámbricas de una manera flexible y simple. En este trabajo se describe un procedimiento para demodular comunicaciones GSM y se presentan dos implementaciones que permiten tanto comprender el funcionamiento de estas redes como hacer uso de su información para desarrollar aplicaciones innovadoras.**

I. Introducción

Las características de funcionamiento del sistema de comunicación GSM es dado de manera conceptual en las cátedras de sistemas de comunicaciones en las carreras de ingeniería. Sin embargo, la posibilidad de observar el tráfico de estas redes y verificar los conceptos teóricos de su funcionamiento permite transferir el conocimiento de una manera mas clara y completa, y es un disparador para el desarrollo de aplicaciones innovadoras.

En los últimos años ha surgido una nueva tecnología, denominada radio definida por software (software-defined radio, SDR), que permite simplificar y hacer mas versátil y flexible el uso de redes de comunicaciones inalámbricas. La misma se basa en radios con capacidad de procesamiento de las señales por software (modulación, demodulación, filtrado, etc), en lugar de implementarlo por hardware como lo hacen las radio tradicionales. Este tipo de estrategia posibilita configurar el modo de funcionamiento de una radio de manera rápida por software y llegar en un futuro a la implementación de radios cognitivas, y redes inteligentes [1], [2].

En este trabajo se presentan las primeras experiencias en la demodulación y análisis de comunicaciones GSM mediante el uso de receptores basados en tecnología SDR. Esto posibilita comprender de manera práctica todas los mecanismos utilizados en este tipo de redes para hacer frente a la movilidad de los usuarios y garantizar un servicio de comunicación adecuado. Inicialmente, se presenta una implementación que posibilita calibrar el oscilador a cristal del receptor SDR en función de un patrón de frecuencia mucho mas preciso proporcionado por las celdas de servicio de la red GSM. Finalmente, se presenta una implementación que permite analizar los paquetes transmitidos por las celdas de GSM y utilizar la información contenida en los mismos para desarrollar nuevas aplicaciones.

Este trabajo está estructurado de la siguiente forma. En la sección II se introduce al sistema de telefonía móvil GSM y a su demodulación. Las herramientas de hardware y software utilizadas para la demodulación de señales de GSM son descritas en la sección III. En la sección IV se describen las implementaciones realizadas. Finalmente, en la sección V se dan las conclusiones del trabajo y se citan trabajos futuros.

II. Sistema GSM y modulación GSMK

GSM (Global System for Mobile Communications) es el sistema digital de telefonía móvil de mayor uso a nivel mundial. El sistema puede operar en cuatro bandas de frecuencia, 850, 900, 1800 y 1900 MHz, y es estandarizado por el ETSI (European Telecommunications Standards Institute). Sin embargo cada país regula las bandas de operación permitidas. Particularmente, en Argentina se utilizan las bandas de frecuencia de 850 MHz y 1900 MHz. Si bien el sistema fue concebido como un sistema de comunicación para voz, el mismo ha ido evolucionando para poder brindar soporte de comunicaciones de datos a los usuarios de la red.

Dentro de la arquitectura GSM, las estaciones transceptoras base (Base Transceiver Station, BTS) son las encargadas de comunicarse con la estaciones móviles (Mobile Station, MS) a través de la modulación por desplazamiento mínimo Gaussiano (Gaussian Minimum Shift Keying, GMSK). Este tipo de modulación no contiene discontinuidades abruptas de fase como es el caso de otros tipos de modulación digital, lo que requiere un menor uso del ancho de banda, por lo que es muy utilizado en comunicaciones inalámbricas para servicios de telefonía móvil con múltiples usuarios.

Para realizar la transmisión y la recepción con una gran cantidad de usuarios, el sistema GSM utiliza la duplexacion por división de frecuencia (Frequency-Division Duplexing, FDD), es decir, el transmisor y el receptor operan a diferentes frecuencias, desplazadas por lo general en 45 MHz. Para poder dar soporte a un gran número de clientes, el sistema utiliza un esquema de multiplexación en el dominio de la frecuencia (Frequency Domain Multiple Access, FDMA) combinado con

multiplexación en el dominio del tiempo (Time Division Multiple Access, TDMA) a través de la asignación de slots de tiempo para cada usuario. Este ultimo esquema de acceso requiere de tareas de sincronismo las cuales son descriptas en este trabajo.

El sistema GSM-850, que es el analizado en este trabajo utiliza la banda de 824.0–849.0 MHz para las transmisiones desde la MS hacia el BTS (MS→BTS, canal de "uplink"), y la banda de 869.0–894.0 MHz para las transmisiones desde el BTS hacia el MS (BTS→MS, canal de "downlink"). Estas bandas de frecuencias superiores e inferiores se dividen en canales de 200 KHz de ancho de banda, donde cada canal se denomina *número de canal de radio frecuencia absoluto ("Absolute Radio Frequency Channel Number", ARFCN)*. El ARFCN denota un par de canales "uplink" y "downlink" separados por 45 MHz, y cada canal es compartido por hasta 8 usuarios usando TDMA.

En el sistema GSM se utilizan diferentes tipos de canales lógicos de comunicación, divididos entre canales de tráfico (TCH) y canales de control (CCCH).

II-A. De-modulación de GMSK

Para la demodulación de señales GMSK se hace uso de un montaje similar a los que se usan en las modulaciones digitales QAM y QPSK, aunque presenta ciertas dificultades ya que en el caso del modulador que usa el VCO, el índice de modulación oscila con la temperatura.

Un demodulador GMSK típico consiste de dos demoduladores de producto a los cuales se aplica la misma portadora ya recuperada, pero en uno de ellos se recibe la portadora desfasada en $\pi/2$ radianes (90°) (Figura 1). Las señales a la salida son filtradas adecuadamente y son aplicadas a un generador de fase que reconstruye las posibles transiciones de fase. Finalmente, un bloque derivador reconstruye los bits en forma bipolar o NRZ.

III. Receptor RTL-SDR y GNU Radio Companion

Existe en el mercado un dispositivo denominado *Dongle RTL-SDR* [3], comercializado como receptor de televisión digital terrestre (Digital Video Broadcasting - Terrestrial, DVB-T). El mismo está basado en el sintonizador R820T de Rafael Microelectronic y en el chip RTL2832 de Realtek (Figura 2). El primero es responsable de sintonizar la frecuencia deseada, mientras que el segundo es responsable de demodular las señales recibidas y enviarlas a una interfaz USB. En la Figura 3 se muestra un diagrama en bloques interno del receptor. Sin embargo, si se reemplaza el controlador que trae originalmente por uno que nos permita controlar sus parámetros (frecuencia, ancho de de banda, etc) y brinde acceso a los datos I/Q resultantes de la demodulación, podemos tener un control completo sobre el dispositivo. Dichos controladores fueron diseñados con herramientas de código abierto por parte de diferentes investigaciones realizadas por radio aficionados en un entorno denominado GNU Radio Companion [5], el cual es una herramienta de desarrollo libre y abierta que provee

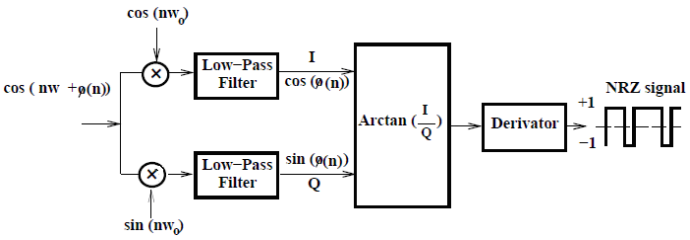

Figura 1. Demodulador GMSK.

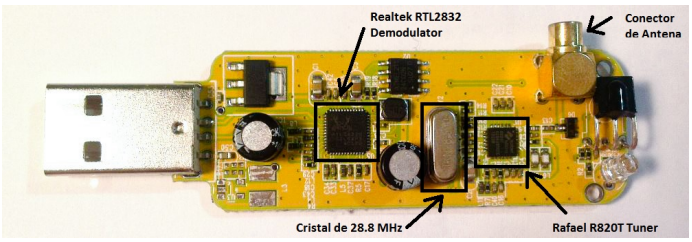

Figura 2. Receptor SDR utilizado.

bloques de procesamiento de señal para implementar sistemas de radio definida por software. Puede utilizarse con hardware de RF de bajo costo para la creación de radios basadas en SDR, o sin hardware en un ambiente de simulación. Es utilizada extensivamente por ambientes académicos, aficionados y comerciales para dar soporte a la investigación en comunicaciones inalámbricas y en sistemas de radio en el mundo real [4].

IV. Implementación

Utilizando herramientas libres de procesamiento de señales de sistemas de radio frecuencia como *GNU Radio Companion* [5] en conjunto con herramientas de análisis de protocolos de comunicaciones como *Wireshark* [6], se puede lograr interceptar las señales provenientes de las estaciones BTS para su demodulación y análisis con fines prácticos y de investigación. A continuación presentamos las primeras experiencias con dichas herramientas, las cuales nos permiten entender de manera practica los procesos de comunicación del protocolo GSM.

IV-A. Implementación N°1: Calibración del cristal del oscilador del RTL-SDR mediante BTS de GSM

El receptor SDR utilizado esta compuesto por un cristal oscilador de 28.8 MHz, que otorga la frecuencia de referencia utilizada por el sintonizador. El cristal es conocido por tener baja calidad, por lo que puede presentar una considerable deriva de frecuencia con el tiempo o con la temperatura ambiente. La deriva es medida en partes por millón (PPM) y puede ser tan alta como ± 50 ppm en este tipo de dispositivos. El resultado de dicha deriva dificulta el correcto funcionamiento del sintonizador, debido a que existirá un error de frecuencia con respecto a la frecuencia sintonizada. Dicho error es proporcional a la frecuencia central y es aun mayor a medida que se aumenta la frecuencia de trabajo.

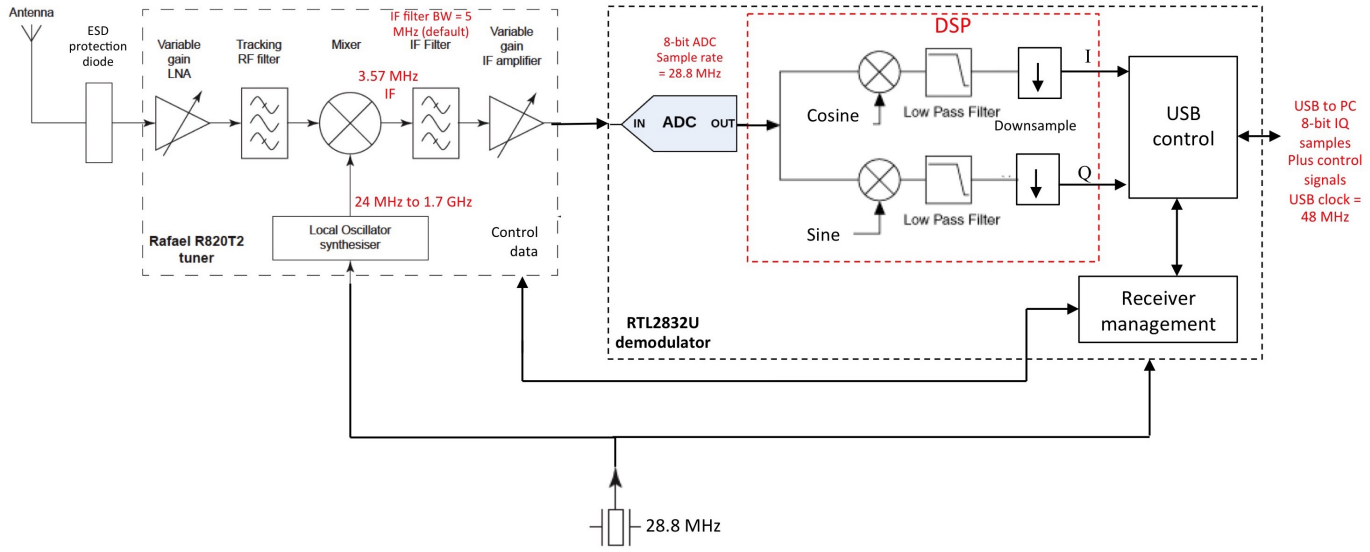

Figura 3. Diagrama en bloques del receptor RTL-SDR.

Este tipo de deriva del oscilador existe en otros dispositivos tal como en los celulares y debe ser corregido para que la comunicación con la estación base (BTS) y es la estación móvil (MS) sea precisa y pueda concretarse de manera correcta. Para poder realizar dicha corrección las estaciones base GSM tienen el requisito de tener una exactitud de reloj de 0.05 ppm, por lo que son una excelente fuente de señales con buena exactitud y es esta misma fuente de señal la que es utilizada por un celular basado en GSM para calibrar su reloj interno [7], [8].

Error de frecuencia a 900 MHz

- Dispositivo SDR-RTL ± 50 ppm: $900MHz \pm 45KHz$
- Torre BTS $\pm 0,05$ ppm: $900MHz \pm 45Hz$

En esta primera experiencia explicaremos brevemente la señal de corrección de frecuencia que es utilizada por la BTS y la utilizaremos para calibrar nuestro dispositivo.

IV-A1. Canal de corrección de frecuencia (FCCH): Para nuestro propósito utilizaremos la ráfaga de corrección de frecuencia (Frequency correction burst, FB) (Figura 4), que se transmite dentro del un canal denominado canal de corrección de frecuencia o Frequency correction channel (FCCH), es enviado desde la BTS a la MS y se encuentra dentro del canal lógico de control que esta compuesto por lo que se denomina canal multi-trama, esta conformado por 51 tramas TDMA (0-50) y es 235,4 ms de largo. Dicha ráfaga FB posee una frecuencia pura a 1/4 de la tasa de bits de GSM o $(1625000Hz/6)/4 = 67708{,}3Hz$, se repite cada 51 tramas y se produce en el segmento de tiempo TS0 en las tramas 0, 10, 20, 30 y 40 del denominado canal de control multi-trama [9] (Figura 5).

Si logramos sintonizar la frecuencia de transmisión de una estación base cercana a nuestra posición estas ráfagas de co-

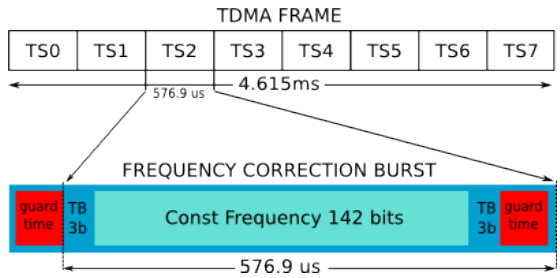

Figura 4. Trama TDMA y ráfaga de corrección de frecuencia FB.

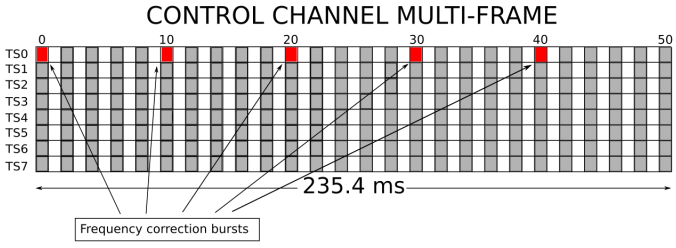

Figura 5. Frequency correction bursts: El intervalo entre ráfagas FB dentro de la multi-trama es de 46.15 ms, y el intervalo entre la última ráfaga en una trama y la primera ráfaga siguiente es de 50.765 ms.

rrección deben estar en portadoras a 67.7083 kHz con respecto a la frecuencia central del canal. Si la frecuencia es diferente que ese valor entonces podemos calcular su desplazamiento con respecto a su verdadera frecuencia y encontrar el valor en ppm para realizar corrección que se necesita para calibrar nuestra radio definida por software.

IV-A2. Diagrama en bloques GNU Radio Companion: Para la sintonización de la estación base se hará uso de los diagramas en bloques provisto por el software GNU Radio el

cual nos da un entorno gráfico sencillo.

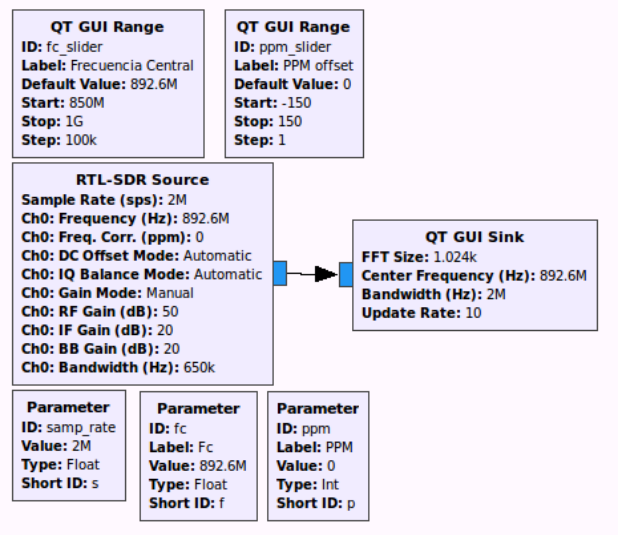

Figura 6. Diagrama en bloques en GNU Radio.

El software nos provee un bloque diseñado específicamente para controlar el dispositivo SDR el cual nos permite ingresar los parámetros de frecuencia de sintonía, ganancia, deriva de frecuencia del oscilador en ppm, entre otros (Figura 6). Es este último parámetro de ppm el que utilizaremos para la calibración de nuestro receptor SDR, modificación que es aplicada al demodulador RTL2832.

IV-A3. Pasos para la calibración:

- Encontrar estación base (BTS):
  El primer paso para poder interceptar las ráfagas de corrección es el de sintonizar una estación base. Si tenemos en cuenta que el FCCH solo es transmitido en el canal de bajada o ”downlink”, luego de buscar las BTS cercanas encontramos una en la frecuencia 892,6 MHZ que pertenece al canal 245 según el ARFCN [10] (Figura 7).
- Encontrar las ráfagas FB:
  Como especificamos anteriormente las ráfagas denominadas de corrección de frecuencia se deberían encontrar a 67708.3Hz de la frecuencia central del canal si capturamos y mantenemos el mayor valor podemos observa claramente una portadora de mayor amplitud perteneciente al FB (Figura 8).
- Lectura de frecuencia de FB:
  Si aplicamos zoom al espectrograma podemos leer su frecuencia lo que nos da un valor medido de 892,624 MHz (Figura 9).
- Calculo de corrección:
  Teniendo en cuenta que nuestra frecuencia central debería ser de 892,6 MHz y nuestra ráfaga FB medida esta a 892,624 MHz cuando su frecuencia según lo dicho anteriormente tendría que ser de:

$$892,6 + 67708,3 = 892,6677083MHz \qquad (1)$$

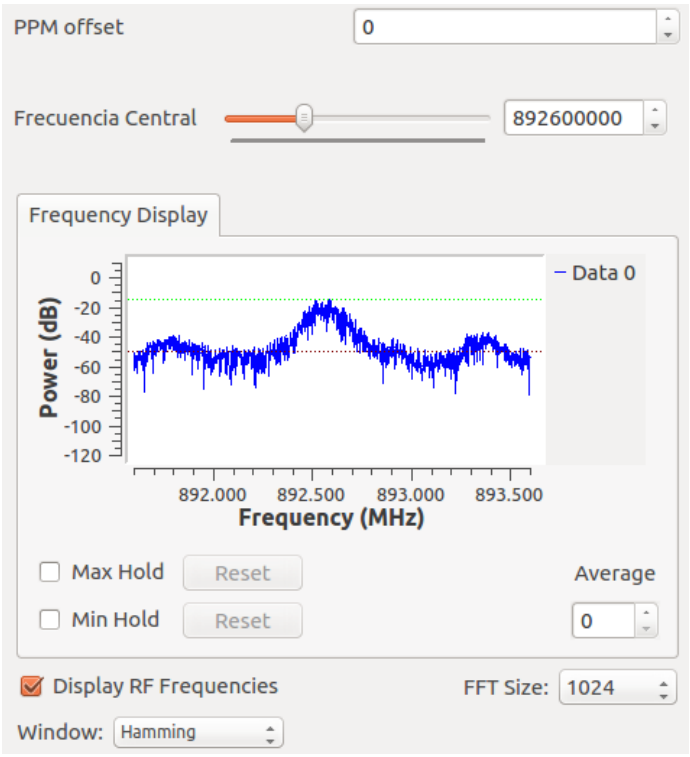

Figura 7. Interfaz de salida con BTS sintonizada en el espectrograma a 892,6 MHz sin calibración.

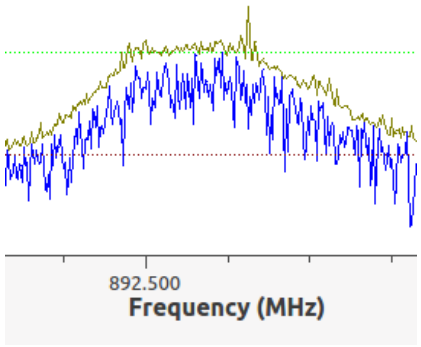

Figura 8. Ráfaga de corrección de frecuencia (FB) detectada

podemos darnos cuenta que existe un desplazamiento de frecuencia con respecto a la frecuencia original. Ahora para encontrar el valor ppm necesario para la calibración utilizamos la ecuación (2).

$$\frac{FB_{medida} - FB_{correcta}}{FB_{medida}} \cdot 1 \cdot 10^6 = ppm \qquad (2)$$

El valor obtenido de la ecuación (2) es el error de frecuencia que existe en términos de partes por millón, es decir que para corregir nuestro dispositivo el valor a ingresar el los parámetros es de signo opuesto.
Aplicando la ecuación a nuestras medidas tenemos:

$$\frac{892,624 - 892,6677083}{892,624} \cdot 1 \cdot 10^6 \approx -49ppm \qquad (3)$$

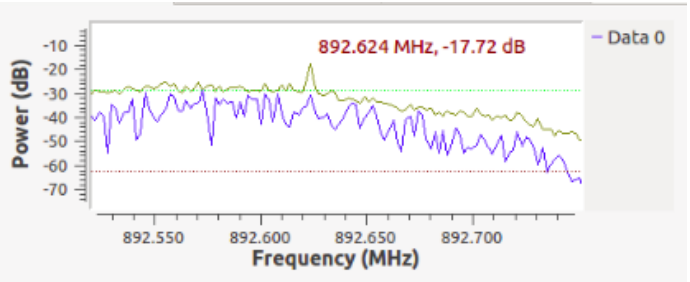

Figura 9. Frecuencia del FB a 67,708 KHz de la frecuencia central

Nuestro valor de corrección según la ecuación (3) tendría que ser de 49 ppm. Este valor debe ser ingresado en el parámetro ppm de nuestro bloque de control del dispositivo SDR y nuestra calibración estará concluida.

IV-A4. Comprobación de la Calibración: Para corroborar que la técnica de calibración es correcta vamos a utilizar un transmisor de marca Signal Hound modelo USB-TG44A [11] que pose las siguientes características:

- Rango de frecuencia : 1 Hz a 4.4 GHz
- Deriva del oscilador interno : ± 1 ppm
- Error a la frecuencia de trabajo: $900MHz \pm 900Hz$

La salida entregada por GNU Radio tiene una precisión de 3 decimales por lo que el error no afectara la comprobación.

- Generamos una portadora a 900 MHz (Figura 7).

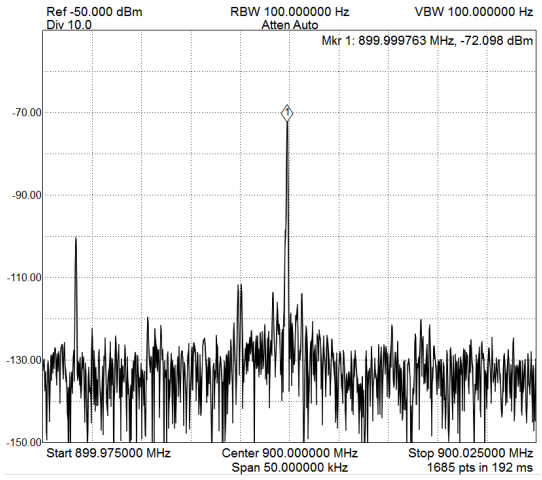

Figura 10. Señal Generada.

- Sintonización de portadora sin calibrar (Figura 11).
- Sintonización de portadora calibrada con 49 ppm (Figura 12).

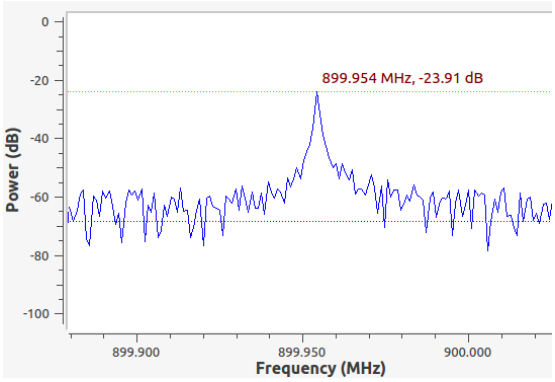

Figura 11. Portadora sin calibrar.

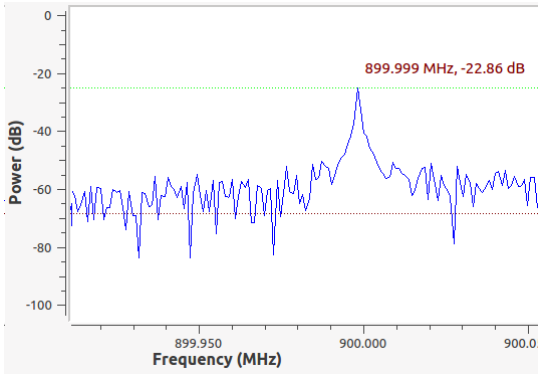

Figura 12. Portadora calibrada.

IV-B. Implementación N°2: Análisis de paquetes de GSM

En esta implementación se realizaron capturas de tramas transmitidas por las BTS mediante el receptor SDR. Se realizó la demodulación GMSK de las comunicaciones GSM mediante la modificación de la aplicación *GR-GSM* o *airprobe* [12], desarrollada en Python y GNU Radio. Esta aplicación demodula y decodifica comunicaciones GSM y envía las tramas GSM layer2 resultantes vía GSMTAP [13] . GSMTAP [14] es un pseudo encabezado (encabezado adicional que no es parte del protocolo) que es usado para transportar tramas de la interfaz aire de GSM (Interfaz Um) dentro de paquetes UDP/IP, los cuales pueden ser visualizados en una PC utilizando analizadores de protocolos de redes, como por ejemplo Wireshark.

Entre los tipos de mensajes recibidos de las BTS con el receptor RTL-SDR se encuentran los siguientes: *immediate assignment, paging request, paging response, system information type x, identity request, ciphering mode command, channel release, authentication request, CM service request, y location updating request*. La descripción de cada uno de ellos está bien especificada en las normas ETSI de GSM [15], [16]. A continuación se describe la información mas relevante aportada por cada uno de estos mensajes y de potenciales aplicaciones.

El mensaje *system information type 6* brinda información de la identidad de la celda (cell identity) transmisora y de

su localización geográfica a través del *LAI (location area identification)* (Figura 13). El LAI está conformado por los siguientes subcampos: *mobile country code (MCC)*, *mobile network code (MNC)*, y *location area code (LAC)*. Con estos códigos y haciendo uso de herramientas Web tales como http://opencellid.org/ o http://www.cell2gps.com/ se puede localizar geográficamente a la BTS.

Por otro lado, el mensaje *system information type 5ter* brinda información de las BTSs o celdas vecinas de la BTS que está transmitiendo (neighbour cell description), a través de la lista de sus ARFCNs, en el caso del sistema PCS1900. El mensaje *system information type 5bis* brinda el mismo tipo de información pero para el sistema GSM850. Cabe aclarar que una misma BTS puede operar en ambos sistemas.

Uno de los mensajes más interesantes para aplicaciones prácticas es el *location updating request*. Con el mismo se transmite información de la identidad del MS, mas específicamente el *International Mobile Subscriber Identity, IMSI*, el cual es un código de usuario. Sin embargo, esta última información trata de ser resguardada por cuestiones de seguridad. Solamente cuando una MS que es visitante de una BTS se registra por primera vez hay un intercambio de su IMSI, pero luego de un breve tiempo esta información es codificada en un *Temporary Mobile Subscriber Identity, TMSI*.

Información extra que puede ser obtenida de las tramas recibidas son: el valor de timing advance de cada MS, el nivel de potencia de transmisión de cada MS, el nivel de señal recibida en dBm, el rango del nivel de señal para la conmutación de celdas, entre otros.

Procesando un conjunto de la información transmitida por las BTS se puede analizar su funcionamiento y comprender su dinámica. Por ejemplo, se pueden generar gráficos de como está conformada la red, como se interconectan las BTS adyacentes, en que frecuencias operan, a cuantos clientes dan servicio, como se mueven las MS, generar mapas con los niveles de señal, etc.

V. Conclusiones

La utilización de la nueva tecnología de SDR posibilita analizar de manera simple los mecanismos utilizados por los sistemas de comunicaciones inalámbricos actuales para el manejo de la movilidad, acceso al medio, seguridad, etc.

En este trabajo se describieron dos implementaciones realizadas que haciendo uso de la demodulación de comunicaciones GSM permiten inicialmente calibrar nuestro receptor SDR y posteriormente obtener información del funcionamiento de la red, a través del análisis de la información transportada por las tramas de las BTS y utilizarla para desarrollar aplicaciones innovadoras. Estas aplicaciones pueden ser utilizadas por los prestadores de servicio u organismos de control para detectar problemas en la red.

Como trabajo futuro se plantea el desarrollo de una celda BTS de GSM mediante tecnología SDR de arquitectura abierta, considerando una placa SDR con capacidad tanto de recepción como de transmisión.

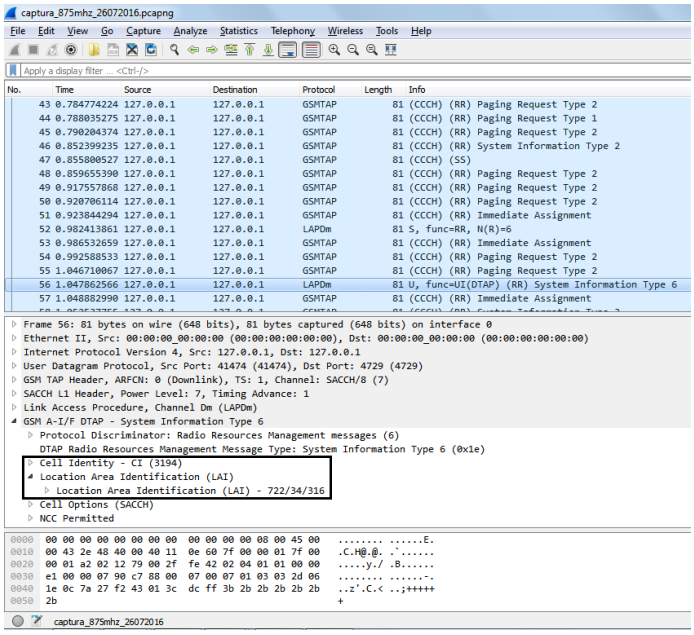

Figura 13. Analizando trama *system information type 6* con Wireshark.

Referencias

[1] J. Mitola, *Cognitive Radio: Making Software Radios more Personal*, IEEE Personal Communication, 6, 13-18, 1999.

[2] F. Joundral, *Software-Defined Radio—Basics and Evolution to Cognitive Radio*, EURASIP Journal on Wireless Communications and Networking 2005:3, 275–283, 2005.

[3] *RTL-SDR*, http://www.rtl-sdr.com/about-rtl-sdr

[4] P. Koszut, *Intercepting GSM Communication using Open-Source and Open-Hardware Technologies*, Institute of Telecommunications, Warsaw University of Technology, 2008.

[5] *GNU Radio Companion*, http://gnuradio.org/

[6] *Wireshark Network Protocol Analyzer*, https://www.wireshark.org

[7] W. Chen, *Frequency Correction Channel Burst Detector in a GSM/EDGE Communication System*, Publication number US 20070274477 A1, 2007, http://www.google.com/patents/US20070274477

[8] *Calibration of the SDR frequency using GSM signals*, https://inst.eecs.berkeley.edu/~ee123/sp14/lab/lab2/lab2-Time_Frequency_Part_II_GSM.html

[9] ETSI Recommendation GSM 05.01, *Digital cellular telecommunications system (Phase 2+), Physical layer on the radio path*, 1996.

[10] *GSM ARFCN frequency determination*, http://niviuk.free.fr/gsm_arfcn.php

[11] *Signal Hunt, TG44A User Manual*

[12] P. Krysik, *GR-GSM, GNU Radio Blocks and Tools for Receiving GSM Transmissions*, https://github.com/ptrkrysik

[13] *RTL-SDR Tutorial Analyzing GSM with Airprobe, GR-GSM and Wireshark*, http://www.rtl-sdr.com/rtl-sdr-tutorial-analyzing-gsm-with-airprobe-and-wireshark

[14] *Pseudo encabezado GSMTAP*, http://bb.osmocom.org/trac/wiki/GSMTAP

[15] ETSI Recommendation GSM 04.22, *Digital cellular telecommunications system (Phase 2+); Radio Link Protocol (RLP) for data and telematic services on the Mobile Station - Base Station System (MS - BSS) interface and the Base Station System - Mobile-services Switching Centre (BSS - MSC) interface*, 1995.

[16] ETSI Recommendation GSM 04.08, *Mobile Radio Interface - Layer 3 Specification*, 1992.