



Implementación de una estación base GSM (2G) y recepción de señales LTE (4G), aplicando radio definido por software

Autores: G.Chica¹, A.Díaz², M.Espinosa³, D.Angulo⁴

¹ Ing. Telecomunicaciones, U. Santo Tomás, gustavochica@usantotomas.edu.co

² Ing. Telecomunicaciones, U. Santo Tomás, angel.diaz@usantotomas.edu.co

³ Ing. Telecomunicaciones, U. Santo Tomás, monica.espinosa@usantotomas.edu.co

⁴ Ing. Telecomunicaciones, U. Santo Tomás, davidangulo@usantotomas.edu.co

Abstract- *The research work was aimed at the implementation of a cellular mobile telephone (for its acronym in Spanish TMC) base station, GSM 2G and developing a reception system 4G LTE signals. Applying software defined radio and free software tools. Relative to the base station, it generates and manages wireless resource issued by the same, in order to, provisioning services of short text messaging and voice call. While the reception system 4G LTE signals, was developed in the gnuradio software.*

Key Words — TMC, GSM 2G, LTE 4G, software defined radio, free software, GNURadio.

Resumen— El trabajo de investigación tuvo como finalidad, la implementación de una estación base de telefonía móvil celular (TMC), GSM 2G y el desarrollo de un sistema de recepción de señales LTE 4G. Aplicando radio definido por software y herramientas de software libre. Con relación a la estación base, se genera y gestiona el recurso inalámbrico emitido por la misma, con el fin de, aprovisionar servicios de mensajería de texto corta y llamada de voz. Mientras que, el sistema de recepción de señales LTE 4G fue desarrollado en el software GNURadio.

Palabras claves — TMC, GSM 2G, LTE 4G, radio definido por software, software libre, GNURadio.

I. INTRODUCCIÓN

En un mercado donde los servicios de telecomunicaciones han presentado en las últimas décadas gran demanda por parte de sus usuarios, es vital realizar constantes innovaciones en temáticas de infraestructura, e igualmente desarrollar nuevas plataformas que soporten el auge tecnológico.

Los sistemas SDR (Radio Definido por Software) permiten la implementación y el desarrollo de la infraestructura de servicios móviles, que orientados hacia la academia generan fortalezas en las competencias trabajadas sobre el contexto tecnológico. Puesto que, facilita el diseño de la infraestructura de un operador de telecomunicaciones con fines didácticos. Por lo tanto, el estudiante que utiliza los sistemas SDR, obtiene apropiaciones tecnológicas de las distintas generaciones de los sistemas de telefonía móvil, para posteriormente desarrollar innovación en este campo.

Acorde con la formación de un estudiante de ingeniería de telecomunicaciones, enfocada en el sector de las tecnologías de la información y de las comunicaciones (TIC), el pleno desarrollo de prácticas de laboratorio le permite interactuar con las herramientas que hacen parte de la implementación de una estación base GSM (Global System for Mobile Telecommunications), y el desarrollo del sistema de recepción de señales LTE (Long Term Evolution).

Para desarrollar las prácticas de laboratorio se utilizaron herramientas de software libre basadas en sistemas operativos de distribución Linux, por su parte, GNURadio realiza el procesamiento de la señal LTE detectada, inmersa en procesos de demultiplexación y decodificación. Por último, el dispositivo USRP (Universal Software Radio Peripheral) N210, es indispensable para la recepción y transmisión de señales en diferentes bandas de frecuencia.

La implementación de la estación base, permite exitosamente la funcionalidad de los servicios de mensajería de texto corta y llamadas de voz, sobre banda de frecuencia de 900 MHz. En relación con el sistema de recepción de señales LTE, se desarrolla sobre una serie de bloques para el procesamiento de la señal, con el fin de entregar el canal de difusión BCH (Broadcast Channel) en conjunto con el MIB (Master Information Control).

II. SISTEMAS DE RADIO DEFINIDO POR SOFTWARE

Radio definido por software permite a un sistema de radiocomunicaciones convencional, tener un funcionamiento basado en software, debido a la utilización de diferentes circuitos electrónicos que permiten ser reconfigurables. En particular consiste en un sistema periférico universal de radio que permite que un computador estándar funcione como un alto rendimiento y con operación de banda ancha de amplia capacidad. [1].

Específicamente el dispositivo USRP N210, disponible en las instalaciones de la Universidad Santo Tomás, tiene características sobresalientes respecto a otros dispositivos que trabajan sobre los sistemas SDR. Las características principales enfocadas hacia la recepción y transmisión de señales en sistemas de telefonía móvil, se observan en la Tabla 1 [2].

Equipo	Características
	Maneja un rango de frecuencias DC hasta de



B. Implementación OpenBTS Software

OpenBTS es un software con funcionalidad en telefonía móvil celular de segunda generación, estructurado bajo el contexto de la convergencia de servicios. Soporta además la prestación del servicio de llamadas de voz y el envío de mensajería de texto, con la aplicación de sistemas de radio definido por software.

Para la implementación del software OpenBTS, es necesario la instalación de una serie de herramientas gestionadas desde su propia interfaz de línea CLI (Command Line Interface), estas herramientas se observan en la Tabla 2. Además, todas las herramientas son instaladas en conjunto con OpenBTS en sistema operativo de distribución Linux [6].

Herramienta de Gestión	Software Instalado	Descripción de la herramienta
OpenBTS	Sipauthserver	Es un servidor funcional para la gestión de los usuarios. Permite verificar y modificar los permisos de cada usuario conectado a la red, al igual que eliminar o agregar nuevos terminales.
	Smqueue	Ejecuta y verifica los permisos necesarios para el envío de mensajería de texto corta entre usuarios inscritos previamente en la estación base.
	Asterisk	Modifica la conexión de los usuarios, mediante la interfaz de aire Um, para ser visualizados por la red como clientes SIP (Session Initiation Protocol) y de esta manera, realizar llamadas de voz entre terminales o entre terminal y estación base.

Tabla 2. Herramientas utilizadas para la puesta en marcha de la estación base GSM (2G).

Una vez culmine el proceso de instalación del software OpenBTS, se realiza las configuraciones necesarias para generar una portadora en banda de frecuencia de 900 MHz y corrimiento de señal de 59.5 MHz, con el fin de, disminuir los niveles de interferencia. Se observa en la Figura 2, la portadora emitida por la estación base, graficada en analizador de espectro ROHDE & SCHWARZ.



Figura 2. Portadora estación base.

Posterior a la configuración de la banda de frecuencia y la canalización de la portadora, es posible buscar la red en los terminales. El método utilizado para acceder a la red difiere según el sistema operativo del terminal, a continuación se realiza la demostración del proceso de búsqueda para terminales iOS y Android.

Terminal iOS.

En la Figura 3, se observa la metodología utilizada para la selección de red. Los pasos para encontrar la red **Test PLMN 1-1** en un terminal con sistema operativo iOS son:

- Ingresar a ajustes.
- Seleccionar la barra de operadores.
- Deshabilitar la opción de operador automático (inmediatamente el terminal buscará las redes disponibles).
- Seleccionar la red **Test PLMN 1-1**.

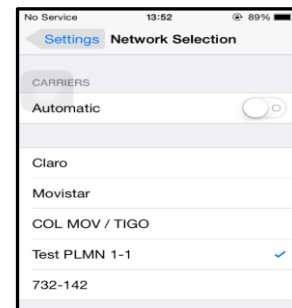


Figura 3. Búsqueda de la red en terminal iOS.

Terminal Android.

En la Figura 4, se observa la metodología utilizada para la selección de red. Los pasos para encontrar la red **Test PLMN 1-1** en un terminal con sistema operativo Android son:

- Ingresar a ajustes o configuraciones.
- Seleccionar la barra mas.
- Seleccionar la barra de redes móviles.



- Seleccionar la barra de operador de red. (Automáticamente el terminal realiza la búsqueda de las redes disponibles, en caso contrario seleccionar la barra buscar redes).
- Seleccionar la red **Test PLMN 0001-01**.



Figura 4. Búsqueda de la red en terminal Android.

Finalizado el proceso de suscripción de los terminales en la red, con el comando (**tmsis**) en el CLI de OpenBTS, pueden ser vistos por el administrador de la estación base. Se observa a continuación en la Figura 5, IMEI e IMSI que caracterizan a cada dispositivo.

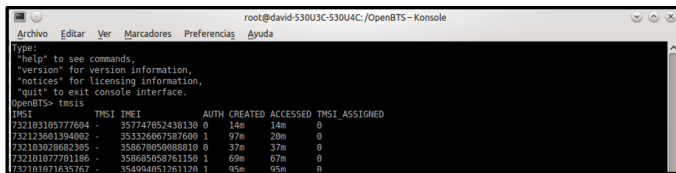


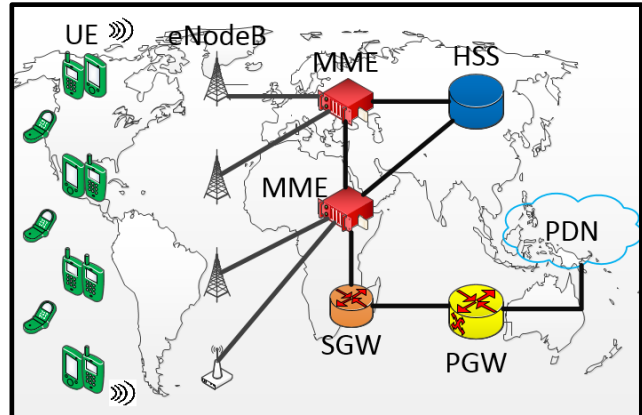
Figura 5. Información dispositivos conectados a la red.

IV. RECEPCIÓN DE SEÑALES LTE (4G)

Aproximadamente en el año 2008 se genera el release ocho (R8) por parte del 3GPP, con el cual se estandariza el mercado de la tecnología LTE. En relación con el espectro radioeléctrico, el nuevo estándar revolucionó la industria de telefonía móvil, ya que, la tecnología de acceso al medio de LTE permite un uso más adecuado de este recurso limitado, utiliza portadoras con mucho más ancho de banda que además tienen la ventaja de ser variables y de hasta de 20 MHz, incorpora también términos relevantes para el avance de las redes de siguiente generación (NGN), como all-IP y la convergencia de servicios [7].

A. Arquitectura de red LTE

En la arquitectura general del estándar LTE, se realizó una reducción en los nodos de la red a comparación de 2G/3G. En la Figura 6, se observa la arquitectura de cuarta generación (4G).



Fuente: Propia.

Figura 6. Arquitectura red LTE.

La red se encuentra fragmentada en dos subsistemas de trabajo, el primero llamado Eutran (Evolved Universal Terrestrial Radio Access Network), que es la subdivisión de la red encargada del acceso y la segunda que hace énfasis en el núcleo de la misma, llamada EPC (Evolved Packet Core).

Entorno red de acceso, Eutran [8].

- **User Equipment (UE):** nombre adoptado para el dispositivo móvil en una red LTE.
- **Evolution Node B (eNB):** son las estaciones base que se encargan del manejo de los protocolos para la interfaz de aire (Uu), además unen las funciones de las estaciones base y controladoras diseñadas en la tercera generación (3G), Node B y RNC (Radio Network Controller) respectivamente. Las funciones principales son la asignación de recursos, control de potencia, handoff, señalización, entre otras.

Entorno núcleo de la red, EPC [8].

- **Mobility Management Entity (MME):** es el nodo evolucionado para un SGSN de segunda generación, aunque se agregaron funciones de listado para el seguimiento de la gestión en los abonados y la selección de la puerta de enlace en la conexión con otras redes.
- **Serving Gateway (Serving GW):** es un nodo de gran importancia, ya que, se encarga de enrutar todos los paquetes entre el Eutran y el EPC. Además, al poseer conectividad directa por medio de la interfaz S1-U con los nodos de ENodeB una de sus funciones adicionales es el anclaje del handoff, también cuando este procedimiento ocurre con otra infraestructura distinta a un ENodeB.

Los nodos anteriores poseen la flexibilidad de instalarse de manera conjunta o por separado según la demanda a soportar. En caso de escoger la segunda opción el MME se comunica con la Eutran por medio de la interfaz S1-MME.

- **Packet Data Network Gateway (PDN GW):** es un nodo de mucha importancia para la protección de información interna de la red del operador, ya que, aunque su función principal es la interconexión con redes externas PDN (Packet Data Network),

también, posee sistemas como firewall de alta seguridad para la protección de la red.

- **Home Subscriber Server (HSS):** básicamente es la única base de datos en la nueva arquitectura de red, allí se unieron todas las funciones de las bases de datos (HLR, VLR, EiR, AuC), tales como identificación del usuario, estado del dispositivo móvil, información del usuario, entre otras.

B. Sistema de recepción LTE en GNURadio

GNURadio es una herramienta de código abierto que ha generado un nuevo concepto en el área de sistemas de radio definido por software, con la capacidad de variación hardware-software, es decir, el hardware de GNURadio puede variar sus funciones acorde al paso de tiempo y a la aplicación que se esté utilizando [9].

Para desarrollar aplicaciones en GNURadio se utilizan dos lenguajes de programación, C++ y Python, la diferencia radica en el procesamiento que sea necesario para el funcionamiento de la aplicación, mientras que Python es utilizado generalmente para aplicaciones de bajo procesamiento que necesiten igualmente de bajos recursos, C++ se utiliza cuando el procesamiento de señal es bastante alto, como en tecnologías de tiempo real [9].

El diseño del sistema de recepción de señales LTE realizado en GNURadio, contiene una serie de bloques de procesamiento que a vez trabajan con un código de programación en lenguaje C y un código de cabecera para configurar el número de entradas y salidas del bloque, y los parámetros de funcionamiento. En la Figura 7, se observa los códigos de programación y de cabecera que hacen parte del funcionamiento del bloque *Channel Estimator Generic* [10].

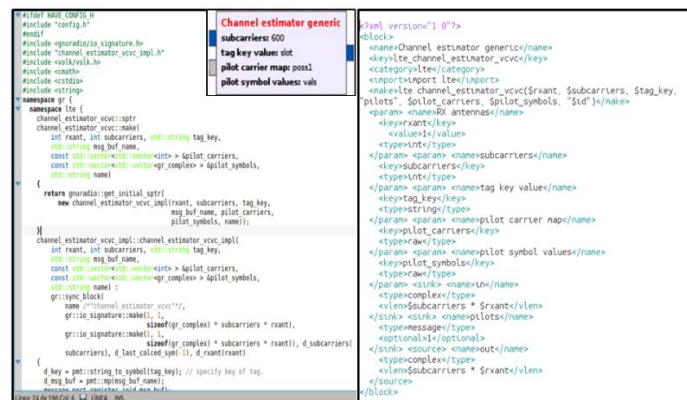
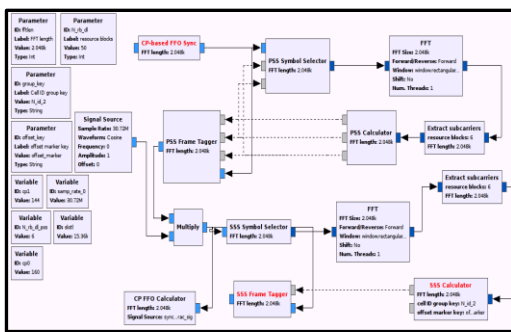


Figura 7. Programación bloques en GNURadio.

El sistema de recepción de señales LTE, cuenta en total con 28 bloques de procesamiento para las etapas de sincronización, recepción OFDM (Orthogonal Frequency Division Multiplexing), demultiplexación y decodificación PBCH (Physical Broadcast Channel) y decodificación BCH (Broadcast Channel).



En la Figura 8, se observan los bloques utilizados para la sincronización de la señal receptionada, determinando los símbolos primarios y secundarios de la señal. También se extrae el cifrado que proporciona identificación de la celda transmisora.

Figura 8. Diagrama de bloques de sincronización en GNURadio.

De acuerdo a la capacidad de procesamiento del ordenador, se realiza la configuración de la cantidad de resource blocks a trabajar y de acuerdo a este parámetro, se determinan la cantidad de bloques para la estimación del canal. En la Figura 9, se observan los bloques utilizados para la recepción de la señal OFDM y la configuración de 50 resource blocks, conformados cada uno por 12 subportadoras y 7 símbolos, es decir, 84 resource elements.

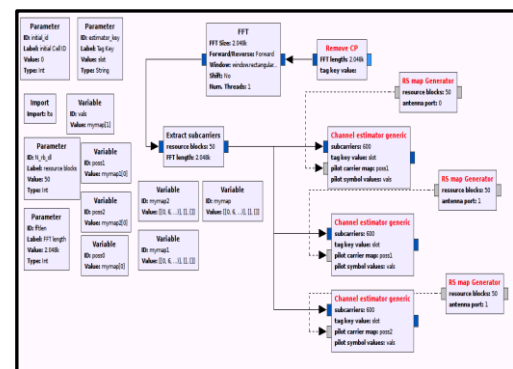


Figura 9. Diagrama de bloques de recepción OFDM en GNURadio.

Referente a la etapa de demultiplexación y decodificación del canal de difusión PBCH, se utiliza un bloque en modulación QPSK (Quadrature Phase Shift Keying), trabajada en el estándar LTE. Esta etapa, entrega a su homónima posterior, el canal BCH y la trama MIB (Master Information Control). En la Figura 10, se observan los bloques utilizados en la etapa descrita anteriormente.

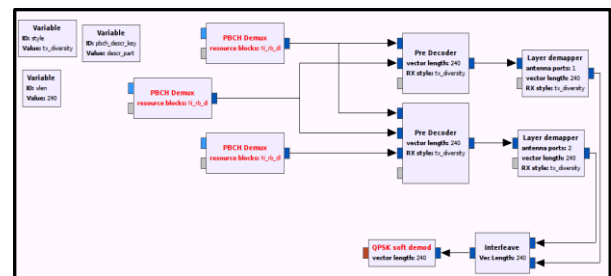


Figura 10. Diagrama de bloques demultiplexación y decodificación PBCH.

En la Figura 11, se observan los bloques utilizados para el desarrollo de la etapa de decodificación del canal BCH y la entrega de la trama MIB.

Figura 11. Diagrama de bloques decodificación BCH y trama MIB en GNURadio.

V. APLICACIÓN Y RESULTADOS

Para verificar el funcionamiento de los sistemas desarrollados, se han realizado diversas pruebas con base en los servicios suministrados por una estación base GSM (2G) y la correcta detección de señales LTE (4G). El software Wireshark, permite capturar el tráfico generado en la interfaz Gigabit Ethernet del ordenador conectado al USRP N210, para ser analizado posteriormente.

A. Servicio de Mensajería de texto

Para verificar el servicio de mensajería de texto en los terminales, se envía un mensaje de texto al número 411, la estación base retorna un mensaje de acuso que permite hacer veraz la comunicación, esta prueba se puede observar en la Figura 12.

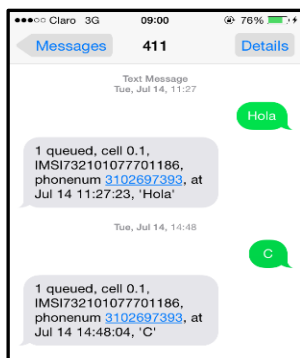


Figura 12. Verificación servicio de mensajería de texto.

B. Servicio de llamadas de voz

Para realizar una llamada de voz de un terminal hacia la estación base, es necesario ingresar al panel numérico y digitar el número 2602. Es generado un canal de tráfico por el terminal y la estación base retorna los mismos sonidos enviados. También se puede llamar al número 2600 y la estación base esta vez retorna un sonido continuo como prueba del servicio de llamadas de voz activo.

En la Figura 13, se observa que existe un canal de tráfico TCH (Traffic Channel) en uso, que es canalizado al momento de realizar un llamado de voz al número 2602, igualmente se observan parámetros de transmisión y finalmente el IMSI del terminal que efectuó la llamada.

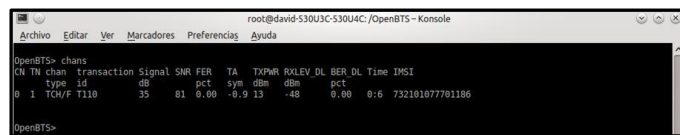
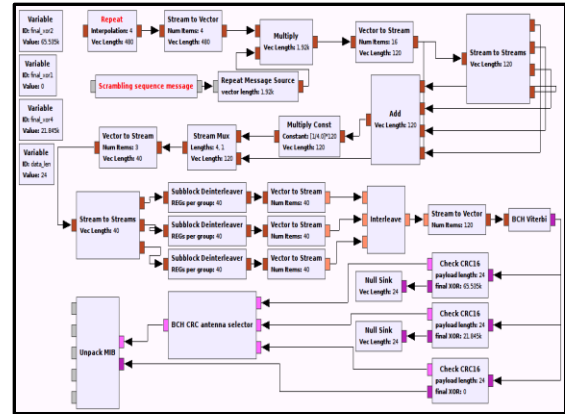


Figura 13. Verificación servicio de llamadas de voz.

Una vez mínimo dos terminales se encuentren registrados en la base de datos de OpenBTS y estén conectados a la red, pueden realizar llamadas de voz entre sí. Digitando el número con el cual fue

registrado en la base de datos en el panel numérico, es posible efectuar la comunicación entre ellos.



En la Figura 14, se observan dos canales de tráfico ocupados en la estación base, de esta manera se comprueba que la llamada ha sido satisfactoria.

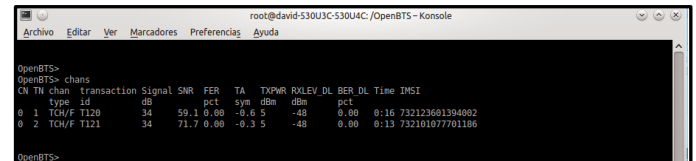


Figura 14. Llamadas de voz entre dos terminales.

C. Capturas de tráfico en el software Wireshark para la estación base

A continuación se observan los protocolos capturados en cada uno de los procesos de señalización y tráfico. En la Figura 15, es posible visualizar el proceso de señalización que se establece con el uso del protocolo SIP. Además, del terminal fuente que corresponde al IMSI 732101077701186, utilizando el canal de tráfico.

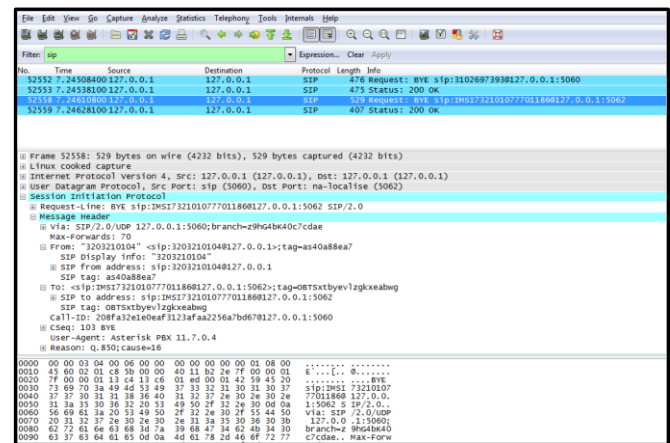


Figura 15. Captura del protocolo SIP.

A continuación, se observa la verificación del canal seleccionado para la transmisión de datos en la estación base, el cual fue el canal 121 con frecuencia central de 959.2 MHz en enlace descendente y 914.2 MHz para enlace ascendente. La Figura 16, permite observar



igualmente la utilización del protocolo gsmmap en la estación base. El protocolo gsmmap encapsula tramas GSM procedentes de la interfaz de aire (um).

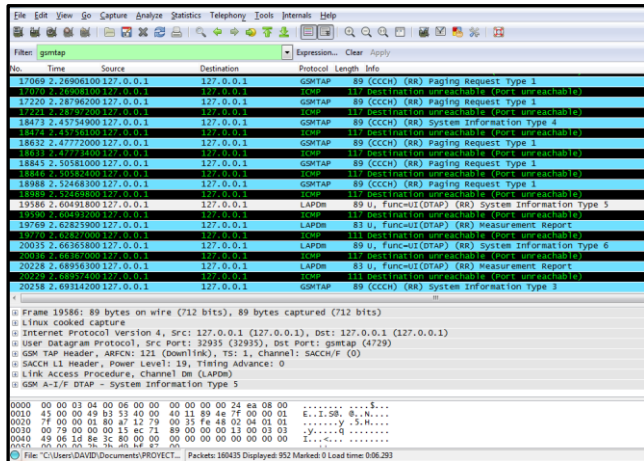


Figura 16. Captura del protocolo gsmmap.

D. Capturas de tráfico en el software Wireshark para la recepción de señales LTE

En la Figura 17, se observa la captura del tráfico generado una vez se ejecute el programa en GNURadio, además de la dirección IP fuente, correspondiente al dispositivo USRP. El tráfico se encapsula en el protocolo UDP (User Datagram Protocol).

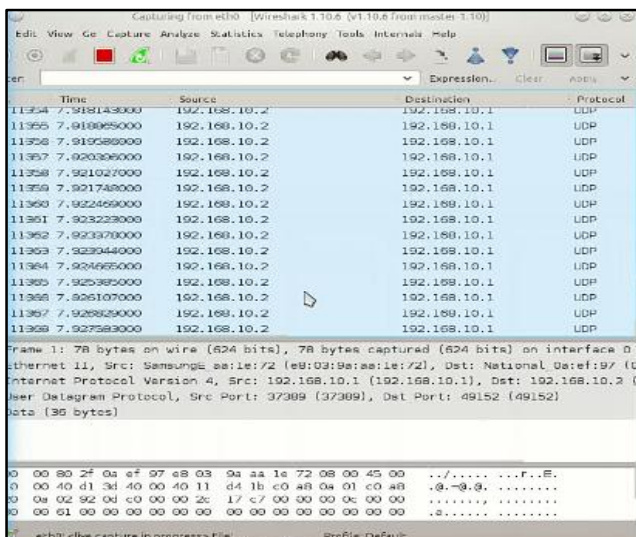


Figura 17. Captura de trama UDP.

E. Estadísticas de captura

En la Tabla 3, se realiza una comparación del número de paquetes capturados por cada protocolo al momento de realizar una llamada de voz utilizando la estación base. La captura es de 200 Mbytes y tuvo duración aproximada de 5 minutos.

RTCP	4
SIP	11
RTP	1774
ICMP	630
LAPDm	49
ICMP	595
UDP	165417
TCP	22
Otros	369
Total paquetes capturados	169466

Tabla 3. Estadísticas de captura llamada de voz.

Con relación a la captura de señales LTE, se observa que, todos los paquetes capturados corresponden al protocolo UDP.

VI. CONCLUSIONES.

La práctica de laboratorio comprendida en la implementación de una estación base de segunda generación, fue determinante para evidenciar los factores tecnológicos necesarios para el adecuado servicio de la estación base. Por lo tanto, se determinó que las herramientas elementales para la puesta en marcha de la misma son: un servidor funcional en el manejo y control de las bases de datos, otro para el servicio de mensajería de texto corta, otro para la canalización del tráfico de voz y una última herramienta para generar y realizar configuraciones de la portadora en el canal descendente.

Una vez los terminales buscan la portadora en las configuraciones de red, para realizar el proceso de enganche con la estación base, se observó que, la red no entrega los permisos suficientes a los usuarios para activar servicios de telecomunicaciones. Solo se activa el servicio cuando el terminal es registrado en el servidor de bases de datos sipauthserve.

El servicio de llamadas de voz demostró gran calidad de servicio al momento de realizar el cambio de la banda de frecuencia de 850MHz a 900MHz. La comunicación entre dos terminales fue clara y no se observaron interferencias notorias.

En la recepción de señales LTE de cuarta generación, la práctica de laboratorio se trabajó mediante la jerarquización de bloques, y se observó que fue funcional para completar cada una de las etapas de sustracción de cabeceras y demás códigos que hacen parte de la señal pura transmitida por un eNodeB. Además de visualizar los componentes que son incorporados en una señal 4G de forma práctica.

Los futuros procesos de investigación, desarrollados por los integrantes del semillero telesoft, tendrán como apoyo el trabajo realizado anteriormente en proyectos que conciernen las temáticas de los sistemas de comunicaciones móviles y de radio definido por

Captura protocolos en llamadas de voz

GSM TAP	595
---------	-----

	Universidad Santo Tomás. División de Ingenierías Implementación de una estación base GSM (2G) y recepción de señales LTE (4G), aplicando radio definido por software Semillero Telesoft	
---	--	---

software. Como auxiliar de investigación fue fundamental para mi formación la participación dentro del semillero, ya que me permite fortalecer mis conocimientos en el área investigativa.

VII. AUTORES.

Universidad Santo Tomás, Facultad de Ingeniería de Telecomunicaciones. Gustavo Alonso Chica, Ángel Felipe Díaz, Mónica Espinosa Buitrago, David Norberto Angulo.

VIII. REFERENCIAS BIBLIOGRÁFICAS.

- [1] H. A. Angulo Orquera and D. M. Paredes Calderón, “Diseño y desarrollo de un radio definido por software, para el ejército ecuatoriano, mediante la utilización de una tarjeta USRP y la herramienta simulink de matlab,” 2011.
- [2] J. de J. R. Uribe, T. M. Bojacá, and C. H. C. Sánchez, “Caracterización de la plataforma de radio definido por software USRP N210-WBX,” *Gerencia Tecnológica Informática*, vol. 12, no. 34, pp. 91–102, 2013.
- [3] A. Pachón, “Evolución de los sistemas móviles celulares GSM,” *Sistemas & Telemática*, vol. 2, no. 4, 2006.
- [4] C. Bettstetter, H.-J. Vogel, and J. Eberspacher, “GSM phase 2+ general packet radio service GPRS: Architecture, protocols, and air interface,” *Communications Surveys & Tutorials, IEEE*, vol. 2, no. 3, pp. 2–14, 1999.
- [5] C. P. Hugo, *Redes móviles celulares*, Editorial@usantotomas.edu.co. Bogota, D. C., Colombia: Universidad Santo Tomás, 2009.
- [6] M. Iedema, *Getting Started with OpenBTS*. O’Reilly Media, Inc., 2014.
- [7] E. A. C. Pedraza and R. F. Escobar, “SISTEMAS MULTIMEDIA BASADOS EN PROTOCOLO IP IMS APLICADOS A SERVICIOS LTE DE 4G,” *REDES DE INGENIERÍA*, vol. 3, no. 2, pp. 100–108, 2013.
- [8] C. P. Hugo, *Comunicaciones Móviles de última generación*, María Paula Godoy Casasbuenas. Bogota, D. C., Colombia: Universidad Santo Tomás, 2012.
- [9] R. Anand, G. Xavier, V. Hariharan, N. Prasannan, R. Peter, and K. Soman, “GNU Radio Based Control System,” in *Advances in Computing and Communications (ICACC), 2012 International Conference on*, 2012, pp. 259–262.
- [10] J. Demel, S. Koslowski, and F. K. Jondral, “A LTE Receiver Framework Implementation in GNU Radio.”