

Extraction of radio link parameters for GSM signals in the 850 MHz band using SDR

Extracción de parámetros de radioenlace para señales GSM en la banda de 850 MHz usando SDR

PhD. Edward Paul Guillen Pinto, MSc. Juan Carlos Martínez Quintero, Daniel Ricardo Cortés Garzón.

Universidad Militar Nueva Granada

Programa de Ingeniería en Telecomunicaciones
Sede Bogotá, Carrera 11 # 101-80, Bogotá, Colombia
Tel: 57-1-650 0000

E-mail: {edward.guillen, juan.martinezq, u1401181}@unimilitar.edu.co

Abstract: Nowadays, GSM technology is still in force with approximately 1,660 million subscriptions worldwide according to the Ericsson company, so the study of this technology maintains interest in research and academic topics. In this article, SDR technology was implemented for the development of a system for extracting parameters from the GSM signal of a commercial cell. As part of the methodology, GSM channels in use were scanned and an analysis of RF parameters such as the frequency spectrum, GMSK modulation constellation diagram and power versus time measurement was performed. Information was also obtained from the BCCH, CCCH and SDCCH control channels that allow the validation of signaling and access information of a GSM cell in the 850 MHz band, using a Hack RF One.

Keywords: *GSM —Global System for Mobile Communication, SDR — Software Defined Radio, GMSK —Gaussian Minimum Shift Keying*

Resumen: Actualmente, la tecnología GSM sigue vigente con aproximadamente 1.660 millones de suscripciones a nivel mundial según la compañía Ericsson, por lo cual el estudio de esta tecnología mantiene interés en temas de investigación y academia. En este artículo se implementó la tecnología SDR para el desarrollo de un sistema de extracción de parámetros de la señal de GSM de una celda comercial. Como parte de la metodología se escanearon canales GSM en uso y se realizó un análisis de parámetros de RF como el espectro de frecuencia, diagrama de constelación de la modulación GMSK y medición de potencia contra tiempo. Se obtuvo también información de los canales de control BCCH, CCCH Y SDCCH que permiten validar información de señalización y acceso de una celda GSM en la banda 850 MHz, utilizando un Hack RF One.

Palabras clave: *GSM —Global System for Mobile Communication, SDR — Software Defined Radio, GMSK —Gaussian Minimum Shift Keying*

1. INTRODUCCIÓN

GSM es una tecnología de comunicaciones móviles, cuyo beneficio principal es facilitar los servicios de voz y datos permitiendo que los usuarios tengan una comunicación con movilidad (VIU, 2019). Esta tecnología se caracteriza por operar en las bandas de frecuencia de 850MHz y 1900MHz para la provisión del servicio. En términos de uso el informe “Ericsson Mobility Report 2020”, muestra que, para finales del año 2019, a nivel global, la cantidad de suscriptores móviles a GSM fue de 1.660 millones y para el año 2025 se espera una cifra de 840 millones. Estas cifras, evidencian que la tecnología aún es vigente y que su retirada se presenta con lentitud

(Jedling, 2020). En muchos países se sigue utilizando aun en las ciudades capitales y aún más en lugares apartados, como zonas rurales o pueblos lejanos donde las nuevas tecnologías no han penetrado principalmente por el factor económico.

El mantenimiento de la infraestructura de GSM implica el uso de instrumentación de diferente tipo con el fin de asegurar el correcto funcionamiento de las estaciones base. Los equipos de medición de RF tienen funciones para realizar mediciones dentro y fuera de cada canal de GSM, sin embargo, su costo es elevado. En los últimos años, con el desarrollo de la tecnología de radio definida por software (SDR) ha sido posible

suplir algunas de las funciones realizadas por instrumentos convencionales, incorporado por software características de operación como las de los instrumentos especializados, a un costo inferior. Esto último limitado por la exactitud de los componentes usados en la construcción de las plataformas SDR. De este modo SDR permite el estudio y supervisión de parámetros de GSM a un costo bajo.

En este artículo se evidencia el uso de SDR como alternativa para supervisar el funcionamiento de la tecnología GSM. El artículo se divide en tres secciones.

La primera sección describe el escenario en el que se realizaron las mediciones y los requerimientos de hardware y software necesarios para su implementación. La segunda sección, muestra el análisis de las ráfagas de tráfico GSM y los parámetros de caracterización de celdas GSM. La información se extrae de los canales BCCH —*Broadcast Control Channel* y CCCH —*Common Control Channel*. La tercera sección consiste en el análisis de algunos de los parámetros de radioenlace como: PVT —*Power versus Time*, disponibilidad de canales, diagramas de constelación, ocupación del canal, y análisis espectral de la señal. Las mediciones anteriores se obtuvieron a partir del uso de software como Gnu Radio, Matlab, Wireshark y gqrx. Todas las pruebas fueron realizadas en la banda 850 MHz, usando celdas GSM comerciales instaladas en el municipio de Mosquera, Cundinamarca (Colombia).

A continuación, se presentan investigaciones relacionadas a la extracción de parámetros de las señales GSM, no necesariamente en la banda de 850 MHz, sin embargo, estos contextualizan y contribuyen de manera oportuna al desarrollo de la investigación en este artículo.

2. ESTADO DEL ARTE

La tecnología SDR, permite a académicos e investigadores el acceso práctico a tecnologías inalámbricas de RF. El uso de esta tecnología facilita no solo la extracción de parámetros de RF de la señal, sino también la detección y explotación de vulnerabilidades en tecnologías como GSM. Diferentes investigaciones se han realizado entorno a las plataformas de SDR y la integración con Gnu Radio para abordar la extracción de parámetros de radioenlace en señales GSM, muchas de estas surgen gracias a la compatibilidad entre herramientas de desarrollo libres y abiertas con plataformas SDR de bajo costo. Un claro ejemplo se evidencia en el artículo “implementación de un modelo de medición de señales GSM mediante SDR”, donde los autores

realizan la implementación de un modelo de medición de señales GSM mediante HackRf One, Gnu Radio y Wireshark. Este modelo consiste en analizar las principales características de una señal GSM con plataformas SDR, con el fin de capturar la señal GSM, decodificarla y realizar un escaneo para determinar qué canales están disponibles y cuáles presentan mayor tráfico (Sánchez y Vargas, 2018).

También en la investigación “Implementación de un receptor simple GSM mediante plataforma Software Defined Radio”, presenta un conjunto de plataformas SDR para capturar y decodificar paquetes de las tramas de señales GSM, relacionando los protocolos que intervienen en el estándar y la seguridad del enlace. Específicamente abarcan la decodificación de los canales lógicos de control para su análisis (Morcillo, 2014).

Otras investigaciones aprovechan la utilización de la tecnología de SDR para analizar el funcionamiento de GSM a través de mediciones de radio frecuencia, esto con el objetivo general de aportar en la construcción del conocimiento colectivo en esta área y dar soluciones alternativas de trabajo obteniendo datos reales sin tener que recurrir a instrumentos más costosos y sofisticados. En la investigación “Performance Analysis of Various Modulation Techniques using Gnu Radio”, se evalúa diferentes técnicas de modulación digitales a través de la programación en bloques con Gnu radio y la integración de una USRP, donde se resalta analíticamente parámetros como la representación de señales en el dominio del tiempo y diagramas de constelación como parámetro fundamental para verificar la calidad de la modulación GMSK (Rebica *et al.*, 2016).

También existen estudios que evidencian la vulnerabilidad de la información que viaja a través de la red GSM de un usuario a otro, como por ejemplo el caso que expone el autor Alonso (2014) en su investigación, donde referencia el trabajo realizado por Karsten Nohl, en su conferencia “Wideband GSM Sniffing” donde demostró que fue posible descifrar las ráfagas de tramas de los canales que contienen la información de los datos de usuario, vulnerando el algoritmo A5 propio de GSM con Rainbow Tables, herramientas destinadas a descifrar contraseñas. El entorno de prueba fue la captura de mensajes cortos de SMS —*Short Message Service*, y llamadas utilizando teléfonos móviles modificados con OsmocomBB, un firmware gratuito destinado a la codificación y la comunicación de voz y datos por radio.

En relación con lo anterior, la investigación titulada “Investigating GSM Control Channels

with RTL-SDR and Gnu Radio,” se comprueba la vulnerabilidad existente en la seguridad y privacidad de los suscriptores a GSM a través del análisis de tramas GSM (Vohra *et al.*, 2016).

En coherencia con lo anterior en la investigación “Analizando Comunicaciones GSM con Radios Definidas por Software (SDR)”, se desarrolló un análisis de las herramientas SDR para entender de manera práctica los diferentes procesos de comunicación de los protocolos en GSM, el enfoque principal de la investigación son las capturas y análisis de tramas transmitidas por una BTS —*Base Transceiver Station*, mediante un receptor SDR para obtener métricas de rendimiento para el funcionamiento de la red. Con este análisis los autores esperan desarrollar diferentes aplicaciones para que sean utilizadas por organismos de control en la detección de problemas y vulnerabilidades en la red (Riva *et al.*, 2017).

Las investigaciones anteriores son un punto de referencia para el presente artículo, en el cual se abordan los requerimientos de hardware y software necesarios para extraer parámetros de radio haciendo uso de una plataforma SDR de bajo costo, específicamente el Hack RF One. Los parámetros obtenidos más adelante son producto del análisis basado en el funcionamiento de la tecnología GSM, así como también de la integración de otras herramientas de software como Gnu Radio y Matlab.

3. METODOLOGÍA

Para el desarrollo del proyecto se implementa una metodología descriptiva en la cual se determinan el diseño del sistema y las variables que se requieren medir. De modo general, la extracción de parámetros además de depender de la implementación física también comprende dos secciones, la primera centrada sobre el análisis de canales lógicos GSM, los cuales pueden ser estudiados mediante wireshark y la compatibilidad que tiene con Gnu Radio para capturar tramas GSM y la segunda con la obtención de las mediciones de radiofrecuencia. En la Fig. 1, se presenta el esquema general de la metodología.

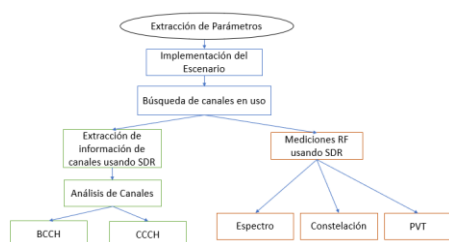


Fig. 1. Metodología general para extracción de parámetros GSM.

A continuación, se describen los requerimientos de hardware y software.

3.1 Requisitos de hardware

Se utilizó una plataforma SDR Hack RF One la cual permite la transmisión y recepción de señales de radio en modo half-duplex. Esta plataforma de hardware libre se diseñó para ser utilizada vía USB o programada para que tenga un funcionamiento autónomo. Tiene un rango de frecuencia programable de 1 MHz a 6GHz (Scottgadgets, 2016). En la Fig. 2, se muestra una imagen del dispositivo.

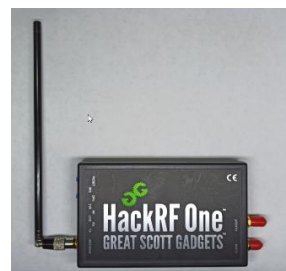


Fig. 2. Plataforma SDR Hack RF One

Además de las características anteriores cuenta con una frecuencia de muestreo máxima de 20 Msps con 8 bits por muestra, es compatible con Gnu Radio y otros programas de SDR para Windows y Linux. Como hardware adicional se usó un computador portátil y los accesorios que vienen incluidos con el HackRF, entre ellos la antena ANT500.

3.2 Requisitos de Software

Se usó la herramienta gr-gsm la cual es un repositorio que cuenta con varias librerías complementarias para Gnu Radio. La librería utilizada en este caso es grgsm-livemon, la cual es estable si se utiliza en una distribución de Linux. Para este caso específico se utilizó Debian 9.6t.

Para sincronizar y configurar el Hack RF One se deben utilizar las librerías del repositorio Kalibrate-Hackrf, este permite la compatibilidad entre el periférico y el sistema operativo, además de escanear los canales GSM en uso.

También es fundamental contar con Gnu Radio el cual haciendo uso de la librería grgsm_livemon permite la conexión con Wireshark para la extracción de tramas GSM. Otro software imprescindible es Matlab, este es necesario para dar sentido a la medición de PVT a través del análisis de las señales almacenadas con grgsm_livemon.

A través de la herramienta Wireshark se debe monitorear la interfaz loopback, la cual está definida en el socket que conecta al Hack RF One, en esta interfaz es donde se evidencia el flujo de tráfico recibido. Posteriormente, mediante el protocolo GSMTAP, es posible filtrar las tramas GSM y observar información del canal de control de una celda GSM. En este caso la información detallada del canal CCCH se encuentra al desplegar cualquiera de las tramas señaladas, ver Fig. 14.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	GSMTAP	100	GSMTAP (R) Paging Request Type 1
2	0.04235779	127.0.0.1	127.0.0.1	GSMTAP	100	GSMTAP (R) Paging Request Type 1
3	0.04670495	127.0.0.1	127.0.0.1	GSMTAP	100	GSMTAP (R) Paging Request Type 1
4	0.708513416	127.0.0.1	127.0.0.1	GSMTAP	100	GSMTAP (R) Paging Request Type 1
5	0.785252296	127.0.0.1	127.0.0.1	GSMTAP	100	GSMTAP (R) Paging Request Type 1
6	0.789807911	127.0.0.1	127.0.0.1	GSMTAP	100	GSMTAP (R) Paging Request Type 1
7	0.135474689	127.0.0.1	127.0.0.1	GSMTAP	100	GSMTAP (R) Paging Request Type 1
8	0.314345814	127.0.0.1	127.0.0.1	GSMTAP	100	GSMTAP (R) Paging Request Type 1
9	0.351179992	127.0.0.1	127.0.0.1	GSMTAP	100	GSMTAP (R) Immediate Assignment
10	0.397296434	127.0.0.1	127.0.0.1	GSMTAP	100	GSMTAP (R) Immediate Assignment
11	0.435218992	127.0.0.1	127.0.0.1	GSMTAP	100	GSMTAP (R) System Information Type 2/Quarter
12	0.254466096	127.0.0.1	127.0.0.1	GSMTAP	100	GSMTAP (R) Paging Request Type 1
13	0.587775275	127.0.0.1	127.0.0.1	GSMTAP	100	GSMTAP (R) Immediate Assignment
14	0.689876242	127.0.0.1	127.0.0.1	GSMTAP	100	GSMTAP (R) Immediate Assignment
15	0.679636966	127.0.0.1	127.0.0.1	GSMTAP	100	GSMTAP (R) Immediate Assignment
16	0.741989528	127.0.0.1	127.0.0.1	GSMTAP	100	GSMTAP (R) Paging Request Type 1

Fig. 14. Tramas GSM en wireshark.

A partir de la rama de canales comunes, se puede obtener información general de la celda GSM mediante los detalles del parámetro (BCCH) como: el nivel de la señal que entre más cercano esté a cero significa que la recepción de la señal es mejor, la relación señal a ruido, el tipo de canal BCCH, correspondiente a un canal broadcast (1) que hace referencia a 1 de los 8 slots que usa GSM para la comunicación y el número de la antena en la zona, ver Fig. 15.

Parameter	Value
Version	2
Header Length	16 bytes
Payload Type	GSMTAP (R) Paging Request Type 1
Time Slot	0
Signal Level (dBm)	-26
Signal/Noise Ratio (dB)	0
GSM Frame Number	1591638
Channel Type	CCCH (2)
Antenna Number	199
Sub-Slot	7

Fig. 15. Parámetros generales de la celda GSM.

También se puede verificar a cuál ARFCN o canal de radio está enganchado el receptor, se puede evidenciar que el ARFCN es 240, el mismo que se sintonizó con el receptor para la visualización del espectro. Esta información se obtiene de la descripción del canal, ver Fig. 16.

Parameter	Value
Element ID	0x64
Subchannel	2
Training Sequence	3
Hopping Channel	No
Single channel ARFCN	240

Fig. 16. ARFCN utilizado en canal CCCH.

También es posible identificar parámetros como el LAI —Identificador de Área local, El cual se compone de otros tres códigos, el MCC —Código móvil de país, MNC —Código de red móvil y LAC —Código de área local. Estos permiten conocer el país en donde se hace la recepción, en este caso Colombia, el operador de quien es la

infraestructura y un código de área local que el operador utiliza por zona. Cada uno descrito respecto al orden según la Fig. 17.

Parameter	Value
Location Area Identification (LAI)	732/123/1861
Mobile Country Code (MCC)	Colombia (732)
Mobile Network Code (MNC)	Telefonica Moviles Colombia S.A. (123)
Location Area Code (LAC)	8x8745 (1861)

Fig. 17. Identificación de área local.

7. EXTRACCIÓN DE PARÁMETROS DE RF GSM CON HACK RF ONE

Con el Hack RF One también es posible obtener algunos parámetros de radio que ponen a prueba la calidad de la modulación GMSK, estos parámetros se obtienen a través del análisis y transformación de los datos transmitidos por una BTS.

Para empezar, es necesario almacenar la señal recibida en un bloque “file sink” de Gnu radio, el cual se puede añadir a la configuración de bloques conectado directamente al bloque de recepción. Con la siguiente configuración de bloques se hace un tratamiento a la señal recibida por el Hack Rf One, el contenido almacenado son datos binarios los cuales pasan por un proceso de remuestreo de la señal. La duración de las señales almacenadas es de aproximadamente 15 segundos. En la Fig. 18, se muestra el procesamiento de la señal.

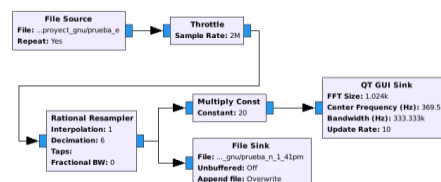


Fig. 18. Remuestreo en GNU Radio.

El proceso de decimación (remuestreo) se utiliza para limitar la banda a 200KHz, ver Fig. 19.

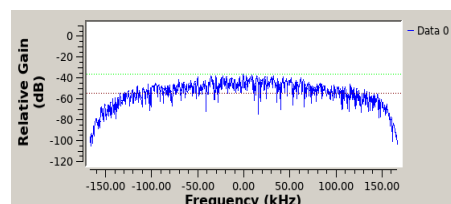


Fig. 19. Remuestreo de la señal.

7.1 Diagrama de constelación con GNU Radio

Sobre el rango de frecuencia específico, se puede observar el diagrama de constelación correspondiente a una modulación GMSK cuya forma de onda es una envolvente de potencia constante de forma circular, el comportamiento es constante debido a que existe una diferencia de frecuencia entre el estado de cero lógico y uno

lógico, de este modo se suavizan las transiciones de fase entre estados que sufren los flujos de bits, para un aumento en la fase de la portadora, representa un estado lógico y para una disminución de fase representa otro estado lógico diferente (NI, 2014), ver Fig. 20.

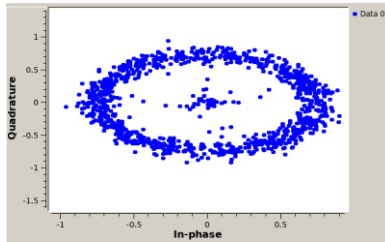


Fig. 20. Diagrama de constelación GMSK.

7.2 Potencia versus tiempo (PVT) con Matlab

La señal muestreada de la Fig. 18, se almacenó y se exportó en un archivo binario, la intención de esta acción es separar las componentes I/Q de la señal. De este modo se pueden representar por separado, también es útil para realizar el cálculo de potencia vs tiempo. Una trama GSM opera con un esquema TDMA — *Time Division Multiple Access*, con capacidad de ocho slots o ranuras de tiempo por cada canal de radio frecuencia. La ráfaga GSM alberga un total de 148 bits, estos se distribuyen en datos de usuario, señalización y datos de sincronización. En la Fig. 21, se muestra la distribución de bits de cada time slot (NI, 2014).

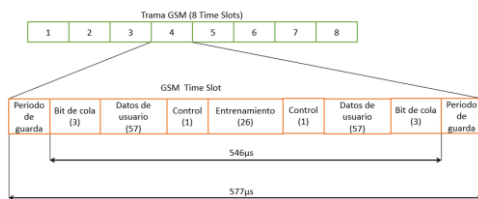


Fig. 21. Distribución de bits en trama GSM.

Una forma de visualizar los time slots es a través del parámetro PVT. El cual básicamente se refiere a la medición de la potencia de la transmisión durante la parte útil de las ráfagas GSM, también permite ver un aumento o caída de potencia de la parte útil de la ráfaga GSM, evidenciando la forma rectangular del slot de tiempo (NI, 2014).

La obtención de la PVT se obtuvo mediante Matlab con la separación de las componentes I/Q de la señal. De este modo fue posible calcular la potencia relativa, el procedimiento se llevó a cabo con la ecuación (1), la cual es aplicada a cada uno de los elementos de los vectores I/Q. Posteriormente con la ecuación (2) se calculó la potencia en dBm.

$$P(dB) = 10 \log(I^2 + Q^2) \quad (1)$$

$$P(dBm) = P(dB) + 30 \quad (2)$$

En la Fig. 22 se evidencia un slot de tiempo sintonizado por el receptor a una frecuencia de 891.6 MHz, es decir, sobre el ARFCN 240 de downlink. Los ARFCN elegidos se reparten entre 8 usuarios, cada uno tiene su propio intervalo de tiempo, por lo tanto, el slot de la Fig. 22 es producto de graficar la potencia en dBm versus el tiempo total de la señal almacenada previamente. En este caso está restringido a un intervalo de tiempo específico para capturar un slot activo, el cual refleja la ocupación por parte de un usuario cuya MS está enlazada a la BTS en cuestión.

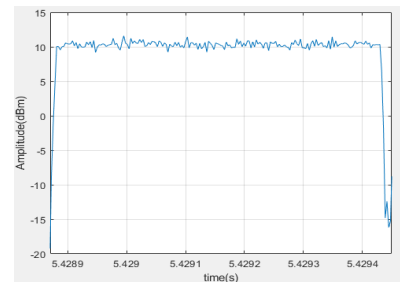


Fig. 22. Slot de tiempo en uso.

También se puede evidenciar una medición de PVT para dos o más ranuras de tiempo ocupadas consecutivas, estas indican la ocupación de un usuario por ranura de tiempo activa, algunas ranuras de tiempo presentan una amplitud mayor comparadas con sus adyacentes, del mismo modo existen ranuras las cuales su potencia es menor. Este comportamiento se presenta debido al control de potencia sobre la MS, a medida que este se mueve en el radio de cobertura de una celda, la BTS debe variar su potencia de transmisión. Cuando la MS está cerca de la BTS, los niveles de potencia disminuyen para reducir la interferencia con los otros usuarios. Cuando la MS está más lejos de la BTS, el nivel de potencia aumenta para compensar las pérdidas por trayectoria (MI, 2003). Un ejemplo claro de este comportamiento se evidencia en la Fig. 23.

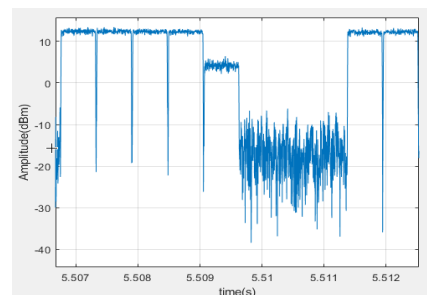


Fig. 23. Slots de tiempo activos consecutivos.

8. CONCLUSIONES

La tecnología de SDR es una alternativa para el análisis, desarrollo y prueba de tecnologías

inalámbricas de RF. En este artículo se demuestra el potencial de la tecnología SDR para realizar funciones de equipos de instrumentación o sistemas de difícil adquisición, aunque en ocasiones la precisión y calidad no llegue a la altura de las herramientas profesionales debido a los componentes con los que se construyen este tipo de plataformas. De cualquier forma, este tipo de soluciones de bajo costo pueden ser aceptables en el ámbito de investigación y académico.

Mediante la implementación de modelos de medición de señales GSM y el uso de SDR se pueden entender y aplicar conocimientos técnicos y teóricos sobre esta tecnología. Con un conocimiento básico sobre GSM y manejo de plataformas SDR se puede caracterizar y validar el funcionamiento de esta tecnología. También sirven como introducción para considerar otras posibilidades de estudio, como analizar otras tecnologías de comunicación inalámbrica. Partiendo de las especificaciones de hardware y software es posible explorar y adentrarse a explicar otras tecnologías de radio.

La compatibilidad entre herramientas de SDR y software libre permitió en este caso utilizar un Hack RF One como un receptor de bajo costo, el cual se pudo integrar con GNU Radio y herramientas como Wireshark y Matlab, de este modo se pudo analizar varias propiedades y características de la tecnología GSM.

Los parámetros de radio obtenidos en esta investigación demuestran de forma práctica la utilización de SDR específicamente para GSM, por ejemplo, la obtención del diagrama de constelación y la PVT permiten observar el comportamiento práctico de esta tecnología, sin embargo, a futuro se planea obtener más parámetros importantes como error de fase y frecuencia para obtener datos más precisos sobre la calidad de la modulación GMSK, de este modo se podrá comparar la precisión de las implementaciones usadas contra instrumentos de medición de gama alta y la normatividad que rige a GSM.

9. RECONOCIMIENTO

Esta investigación fue desarrollada al interior del grupo de investigación GISSIC como producto derivado del proyecto de investigación INV ING 2998 financiado por la vicerrectoría de investigaciones de la Universidad Militar Nueva Granada.

REFERENCIAS

Morcillo, I. (2014) *Implementación de un receptor simple GSM mediante plataforma Software Defined Radio*, Trabajo de grado,

Universidad Carlos III de Madrid, Madrid, España.

Rebica, L., Rani, S., y Kakkar, S. (2016). "Performance analysis of various modulation techniques using GNU radio". *International journal of computer applications*, 975, 8887.

Riva, G., Kunst, J., Zerbini, C., Airasca, E. y González, E. (2017) "Analizando Comunicaciones GSM con Radios Definidas por Software (SDR)". Universidad Tecnológica Nacional, Buenos Aires, Argentina.

Sánchez, E. Vargas, J., C. and Chamorro, M. (2018) "Implementación de un modelo de medición de señales GSM mediante SDR". *Universitaria Agustiniana*, Bogotá, Colombia.

Vohra, D., Dubey, A. y Vachhhani, K. (2016) "Investigating GSM Control Channels with RTL-SDR and GNU Radio" *IEEE Int. Conf. Wirel. Commun. Signal Process. Networking*.

SITIOS WEB

Alonso, C. (2014). *Un informático en el lado del mal: Hacking de comunicaciones móviles GSM con RTL-SDR*. <http://www.elladodelmal.com/2014/01/aumentala-vulnerabilidad-de-la-red-gsm.html>. (05 mayo 2020)

Jejdling, F. (2020). *The Mobile Economy 2020*. <https://www.ericsson.com/49e7b3/assets/local/mobility-report/documents/2020/emr-june2020-spanish.pdf> (06 de agosto 2020)

Maxime Integrated Inc, MI (2003), *Introduction to GSM and GSM Mobile RF Transceiver Derivation*. <https://pdfserv.maximintegrated.com/en/an/AN2157.pdf> (26 de Julio 2020)

National Instruments, NI. (2014). *Introduction to GSM Device Testing*. from http://download.ni.com/evaluation/rf/Introduction_to_GSM_Device_Testing.pdf (18 de Junio 2020)

Scottgadgets. (2016). *HackRF One*. <https://greatscottgadgets.com/hackrf/one/>. (26 de mayo 2020)

VIU. (2019). *Evolución de la red de comunicación móvil, del 1G al 5G | VIU.* <https://www.universidadviu.com/evolucion-la-red-comunicacion-movil-del-1g-al-5g/>. (23 de marzo 2020)