EMULACIÓN DE UN SISTEMA DETECTOR DE RECEPTORES IMSI EN FPGA CON MATLAB Y SYSTEM GENERATOR FOR DSP

EMULATION OF AN IMSI RECEIVER DETECTOR SYSTEM IN FPGA WITH MATLAB AND SYSTEM GENERATOR FOR DSP

Jesús Osvaldo Sandoval Solís
Instituto Politécnico Nacional, México
jsandoval@citedi.mx

Miguel Ángel Estudillo Valdez
Instituto Politécnico Nacional, México
mestudillo@citedi.mx

José Cruz Núñez Pérez
Instituto Politécnico Nacional, México
nunez@citedi.mx

Recepción: 21/noviembre/2024 **Aceptación:** 5/febrero/2025

Resumen

Este artículo presenta la simulación, diseño e implementación de una solución capaz de detectar receptores IMSI. Para ello se analizaron distintas tecnologías para replicar una estación base y desarrollar un detector que recolecta información de las estaciones base para evaluarlas. La primera aportación consiste en un detector de receptores IMSI, basado en un transceptor codificado en lenguaje VHDL usando tarjetas FPGA y simulado en Active-HDL. La segunda aportación consistió en un programa que emula una tarjeta de FPGA para establecer comunicación entre el receptor IMSI y el detector para evaluar la estación base y definir su autenticidad. También se implementó un generador de inferencia para canales TDMA para evitar que los equipos se conecten a la estación. Los resultados obtenidos en la aplicación del detector de receptores IMSI demuestra que es posible recibir información de las estaciones base para determinar su autenticidad mediante el MNC, MCC, LAC y Cell-ID.

Palabras Clave: Detector IMSI, FPGA, Receptor, System Generator for DSP, VHDL.

Abstract

Simulating, designing, and implementing a solution capable of detecting IMSI catchers is presented in this article. The goal was to develop a detector that collects information from base stations in order to replicate a base station for evaluation. A variety of technologies were analyzed in order to achieve this. A VHDL-coded, FPGA-based, Active-HDL-simulated IMSI catcher detector is the first contribution. In the second contribution, we simulated an FPGA card in order to establish communication between the IMSI catcher and the detector in order to evaluate the authenticity of the base station. To prevent devices from connecting to the station, an inference generator was also implemented for TDMA channels. Using the IMSI catcher detector, it was demonstrated that it is possible to receive information from base stations to determine their authenticity through the MNC, MCC, LAC, and Cell-ID.

Keywords: *IMSI Catcher, FPGA, Receiver, System Generator for DSP, VHDL.*

1. Introducción

En la actualidad, la mayoría de las personas cuentan con un dispositivo móvil ya sea un teléfono celular, tableta o reloj inteligente. Los cuales permiten mantener una comunicación mientras el usuario se desplaza de un lugar a otro. Estos dispositivos han adquirido una relevancia importante en la vida diaria, permitiendo a los usuarios realizar tareas como navegar por internet, enviar mensajes de texto y acceder a su posición vía GPS. Uno de los principales estándares de telecomunicaciones es la red 2G o GSM, cuyas características principales son la calidad de servicio, cantidad de terminales, bajo costo, *roaming*, eficacia espectral, entre otras [Márquez, 2018]. Sin embargo, estas tecnologías también permitieron que aparecieran los piratas telefónicos (en inglés *phreakers*) con la intención de interferir y robar datos de los usuarios [Santaella, 2019]. Algunos de estos ataques se llevan a cabo mediante la implementación de receptores IMSI (en inglés *International Mobile Subscriber Identity*), en 1996 la compañía alemana *Rohde & Schwarz* presento el primer receptor IMSI llamado IMSI GA 900 en Múnich [Márquez, 2018]. Estos equipos operan aprovechándose de su configuración similar a una estación lo que permite

que los teléfonos celulares cercanos se conecten a este receptor y capturando información del teléfono como datos de la tarjeta SIM, numero IMSI, TMSI y de ser posible mensajes de texto SMS y llamadas. Al dispositivo receptor IMSI también se le conoce como *Stingray*, que es capaz de ejecutarse pasivamente recolectando número IMSI [Gonzalez, 2015]. En la literatura se aportan varias soluciones basadas en aplicaciones de teléfono móvil. En [Mjolsnes, 2017] se describe el *Catcher-Catcher*, que es una herramienta que permite al teléfono móvil detectar irregularidades sobre las actividades de las estaciones base. También el *Snoot-Snitch* que consiste en una aplicación que recolecta y analiza datos obtenidos de manera inalámbrica para compararlos con datos recopilados por otros usuarios, y así determinar si una estación base es falsa o autentica. Y en [Van, 2016] se describe el AIMSICD, que detecta estaciones base falsas en las redes GSM/UMTS. Existen otros métodos para detectar receptores IMSI, como los basados en red, cuya infraestructura es completamente interna de la arquitectura de las compañías de telefonía móvil para otorgar seguridad a los usuarios. Sin embargo, la desventaja es que la configuración es robusta y costosa, donde una mala configuración dejaría sin servicio a los usuarios del área en el que se implementa el detector.

2. Métodos

El Equipo de Identidad Internacional de la Estación Móvil (en inglés IMEI) representa una serie de números que únicamente identifican a la estación móvil o teléfono, y provee datos de fabricación del dispositivo móvil. Este se registra por el operador de red, quien es alojado en los registros de equipos (en inglés IER) [Kukushkin, 2018]. Por otro lado, el IMSI se encuentra localizado en la tarjeta SIM, y tiene un máximo de 15 dígitos en decimal que consisten en 3 partes: el código móvil del país (MCC), que consta de 3 dígitos; el código móvil de red (MNC), que consta de 2-3 dígitos; y el número de identificación del suscriptor (MSIN). El orden de un número IMSI empieza con los dígitos MCC, seguido del MNC y finalmente el MSIN. En la tecnología GSM se combinan la técnica de canalización de acceso múltiple por división de frecuencia (en inglés FDMA) y acceso múltiple por división de tiempo (en inglés TDMA). Estos canales se dividen por $25\,MHz$, uno para

transmitir y otro para recibir información. Donde cada banda cuenta con 124 canales dúplex con $200\ kHz$ de separación por canal para transmitir. El sistema entrega una tasa de transferencia de $279\ kbps$, donde se transfiere mediante una modulación mínima por desplazamiento gaussiano (en inglés GMSK), y cada frecuencia es asignada por el Número de Canal de Radio Frecuencia Absoluto (del inglés ARFCN) por lo que a un usuario nunca se le asignaran todos los espacios de tiempo. Los sistemas TDMA también tienen capacidades de transmitir y recibir en diferentes tiempos mientras que las estaciones móviles transmiten y reciben simultáneamente [Kukushkin, 2018], [Hasse, 2013]. Los canales TDMA entre la estación móvil y la estación base se encuentran desfasadas por $1{,}154\ \mu s$ lo que corresponde a dos espacios de tiempo de $577\ \mu s$. La sincronización de transmisión de una estación base esta acoplada en frecuencia y tiempo con la antena de recepción de la estación móvil, y funciona de la misma manera para la recepción de la estación base y la transmisión de la estación móvil. La casilla de tiempo contiene una trama de información de $156\ bits$ que deben ser transmitidos en $577\ \mu s$ [Hasse, 2013]. Hay cinco diferentes tipos de tramas en la tecnología GMS: normal, sincronización, accesos, corrección de frecuencia y control. La trama normal se utiliza para acarrear información sobre el canal de tráfico y de control. La trama de corrección de frecuencia es utilizada como un filtro en formato idéntico a la trama normal, pero sin acarrear información. La trama de acceso contiene una secuencia de datos de prueba y un patrón de bits predefinidos de la información encriptada.

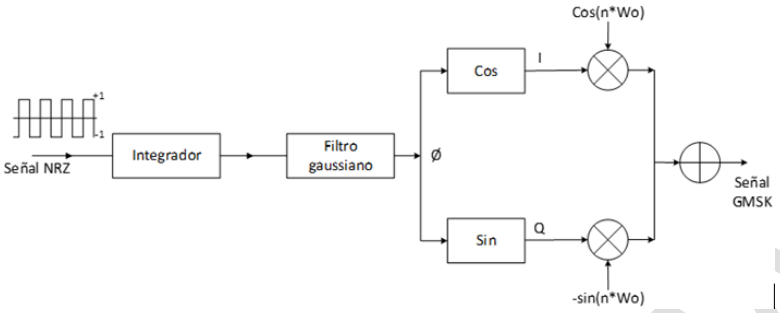
Modulación y demodulación GMSK

La modulación GMSK es utilizada en redes celulares GSM, debido a que cuenta con varias ventajas: eficacia espectral, fases constantes, y es utilizada en amplificadores de potencia no lineales.

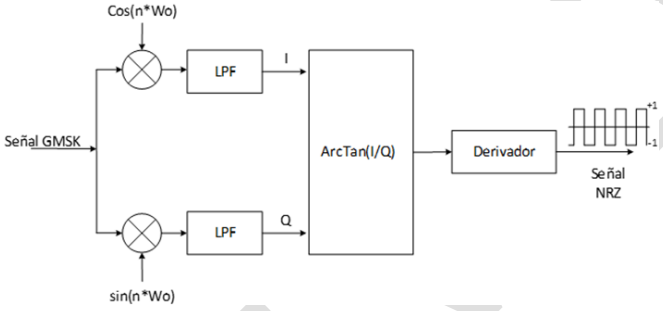
En la Figura 1 se presentan los diagramas a bloques de un modulador GMSK y un demodulador GMSK.

El proceso de esta técnica empieza con un filtro pasa bajos gaussianos, donde el espectro MSK es manipulado por un pulso cuadrado de información por una campana de Gauss. Este proceso está representado mediante la Ecuación 1.

$$h(t) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{t^2}{2\sigma^2}}, \qquad \text{donde } \sigma^2 = \frac{ln(2)}{(2\pi B)^2} \tag{1}$$



a) Modulador GMSK.



Fuente: elaboración propia

Figura 1 Diagrama de bloques.

Donde el parámetro B representa el ancho de banda de $3\ dB$ del filtro pasa bajos, el cual está determinado de un parámetro llamado BT_b, donde T_b es el periodo del bit y t la variable tiempo. Si la entrada del filtro es aislada a un pulso rectangular entonces $(p(t), 0 \leq t \leq T_b)$, la respuesta del filtro se asemeja a la Ecuación 2.

$$g(t) = \frac{1}{2T_b}\left[Q\left(\left(\frac{2\pi BT_b}{\sqrt{\ln(2)}}\right)\left(\frac{t}{T_b} - 1\right)\right) - Q\left(\left(\frac{2\pi BT_b}{\sqrt{\ln(2)}}\right)\left(\frac{t}{T_b}\right)\right)\right] \tag{2}$$

Donde $Q(x)$ se ve expresado en la Ecuación 3, como la función *Marcum*.

$$Q(x) = \int_0^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{y^2}{2}} dy, \quad -\infty \leq t \leq \infty \tag{3}$$

Pero el diseño más comprensible, requiere una implementación de Fase y Cuadratura como se muestra en la Figura 1 a), como se expresa en la Ecuación 4. Donde t representa la variable tiempo y f_c la frecuencia de corte del transmisor.

$$s(t) = \mathrm{I(t)}\cos(2\pi f_c \mathrm{t}) - \mathrm{Q(t)}\sin(2\pi f_c \mathrm{t}) \tag{4}$$

Modelado de canalización

La densidad de potencia espectral depende de la distribución del ángulo incidente, y esta se relaciona en la ganancia de la antena $G(\alpha)$, la cual está dada por la Ecuación 5.

$$S(f) = \frac{A[p(\alpha)G(\alpha) + p(-\alpha)G(-\alpha)]}{f_m\sqrt{1 - \left(\frac{f - f_c}{f_m}\right)^2}} \quad (5)$$

Donde $p(\alpha)$ es la variación de la potencia de entrada con el ángulo, A es la potencia de ganancia recibida con respecto a la antena isotrópica, $AG(\alpha)p(\alpha)$ es la potencia total recibida y la frecuencia fm es el desplazamiento máximo de *Doppler*. El espectro de banda base para la señal debe ser de $2\,fm$ [Sadkhan, 2011]. El espectro es centrado sobre la frecuencia central $f = fc$ la frecuencia portadora es cero para las siguientes condiciones $f < fc - fm$ y$f > fc + fm.$ En los límites de $\alpha = 0$ y $\alpha = \pi,\ f = fc + fm$, y los componentes de la frecuencia tienen una densidad de potencia espectral infinita [Sadkhan, 2011].

Receptores IMSI

En 1996 la compañía *Rodhe & Schwarz* presentó el primer receptor IMSI en Munich [Mjolsnes, 2017], cuya idea principal fue identificar suscriptores que forzaban a las estaciones móviles a transmitir la información IMSI. Los teléfonos móviles víctimas se contactan por el simple hecho de contar con mayor cobertura o tener una potencia de señal más alta por parte de la estación base falsa. A este tipo de ataque se le conoce como ataque de intermediario (en inglés MitM). Los equipos receptores de IMSI proveen las herramientas para la demodulación de voz y datos digitales, obteniendo el IMSI e IMEI de los usuarios [Iosif, 2011], [Adrian, 2016]. Para lograr la comunicación, el teléfono móvil, primero se recibe una solicitud de conexión del teléfono móvil, enviando las configuraciones de seguridad. Después el receptor de IMSI solicita la identidad a la estación móvil. Posteriormente el teléfono móvil envía la información IMSI a la estación base, y en ese instante el receptor de IMSI obtendrá con éxito la información IMSI. Finalmente, el teléfono móvil recibe un

numero aleatorio RAND del receptor IMSI, y envía la firma de respuesta (en inglés SRES), y así recibe el número TMSI. Existen tres tipos de ataques a los teléfonos móviles utilizados por los receptores IMSI: 1) ataques pasivos, capturan los números IMSI de los teléfonos móviles cercanos en el área, 2) ataques activos, arman una red completa de una torre de telefonía móvil o estación base, para representar una estación base autentica y obligar a los teléfonos a migrar a la tecnología de menor seguridad que sería la 2G; 3) ataque de entrega, aplicado a los registros y cambios de estación base vecina, conservando la conexión entre el teléfono móvil y el receptor IMSI.

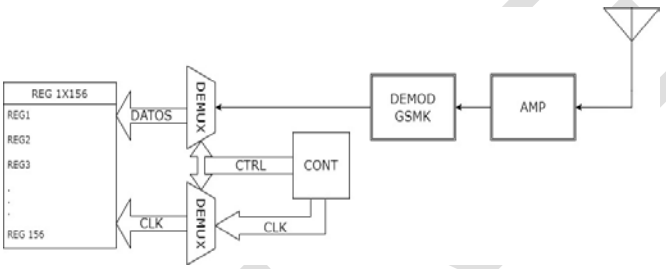
Detectores de receptores IMSI

Existen varios métodos para detectar receptores IMSI. El proyecto FBS-Radar detecta solo receptores IMSI que envían spam o SMS no deseados. La universidad de Washington desarrollo un sistema llamado SeaGlass para reportar receptores IMSI [Ziayi, 2021], [Khan, 2018]. Pero existen otras herramientas basadas en dispositivos móviles como las aplicaciones *Snoot-Snitch*, *Catcher-Catcher* y AIMSICD, donde su principal ventaja es que el dispositivo móvil no tiene que conectarse a la red del receptor IMSI entregando sus datos, solamente verifica la señalización de las estaciones base de la zona. La principal desventaja en los detectores de receptores IMSI basado en aplicaciones móviles, es que el teléfono no conoce realmente el estatus de las redes, algunas aplicaciones otorgan información falsa a los usuarios. El uso de estas aplicaciones también requiere de un alto procesamiento que genera un consumo rápido de la batería del dispositivo, y para que las aplicaciones realicen un estudio más preciso de las estaciones base, se requiere configurar el celular en modo super usuario, causando así la perdida de la garantía de este.

3. Resultados

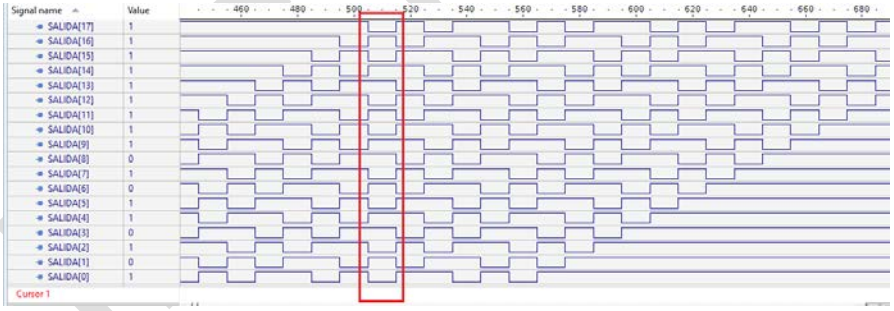
La Figura 2 muestra un diagrama con todos los bloques necesarios para el sistema receptor del detector de receptores IMSI. En el diseño del sistema de memoria y recepción de señal de la estación base, se consideró que cada trama

contara con $156\ bits$ que serán guardados en una memoria basada en registros de corrimiento de $156\ bits\ x\ 156\ espacios$. Esta memoria fue controlada por dos multiplexores encargados de manipular el registro donde se guarda la información recibida en la simulación que a su vez es controlado por un contador anidado y limitado hasta el número 156. Lo que representa la cantidad de espacios en el registro y el cambio del registro. Como se aprecia en la Figura 3a, donde el dato se recorre para guardar la información en cada registro de memoria. En la Figura 3b se ilustra que cada salida genera los datos de entrada. Lo que representa la cantidad de espacios en el registro y el cambio del registro.

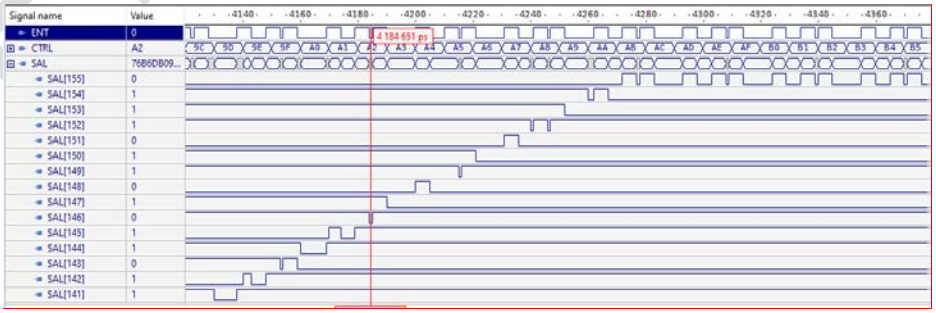


Fuente: elaboración propia

Figura 2 Diseño del sistema de memoria y receptor.



a) Guardado de datos en el tiempo.

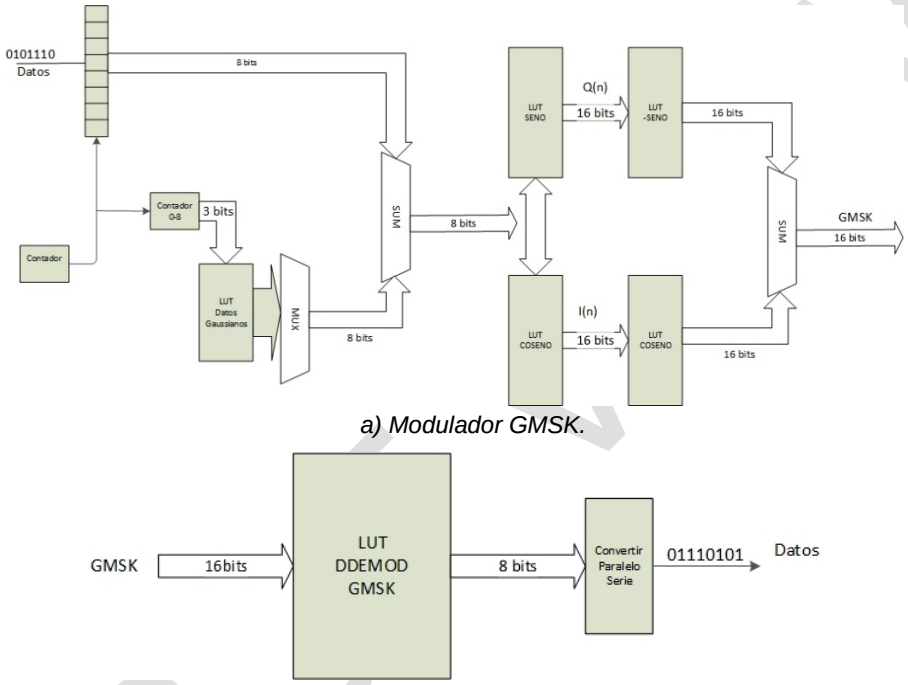


b) Datos para el valor [CTRL].

Fuente: elaboración propia

Figura 3 Simulación del manejo de registros de corrimiento y activación en ActiveHDL.

Los sistemas de comunicación GSM requieren de modulación y demodulación GMSK para que los datos puedan ser procesados y guardados en los registros. Se implementó un sistema de modulación GMSK con precisión de $16\ bits$ para el transmisor en bloques digitales como lo muestra la Figura 4a. En el demodulador GMSK, se utilizó una tabla de búsqueda (LUT) con una precisión de $16\ bits$, como lo muestra la Figura 4b.



a) Modulador GMSK.

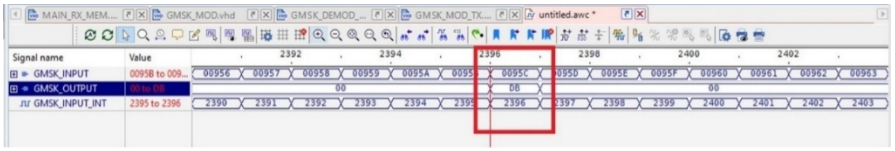
b) Demodulador GMSK.

Fuente: elaboración propia

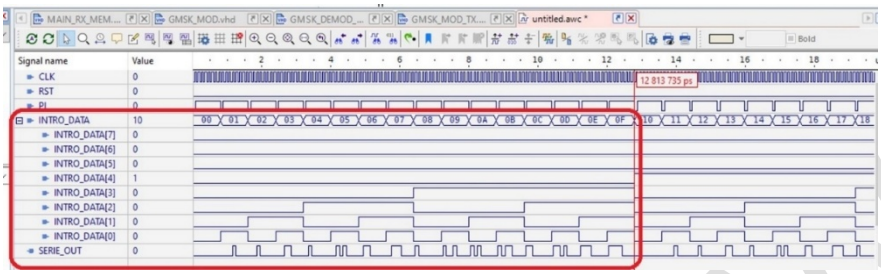
Figura 4 Diagrama a bloques de modulación y demodulación GMSK.

En la Figura 5a se muestra una simulación del demodulador GMSK mientras que la Figura 5b muestra los datos de la señalización transformada en paralelo.

Después de programar y simular el receptor con la memoria, se desarrolló el transmisor. El transmisor entabla comunicación con la estación base, introduciendo datos a enviar. La Figura 6 muestra el esquema de funcionamiento del transmisor, el cual contiene un multiplexor, un contador y una memoria interna configurable, todos conformados por $156\ bits$: $3\ bits$ de cola inicial, $39\ bits$ de datos codificados, $64\ bits$ de sincronización, $39\ bits$ de datos codificados, $3\ bits$ de cola final y $8\ bits$ de guardia.



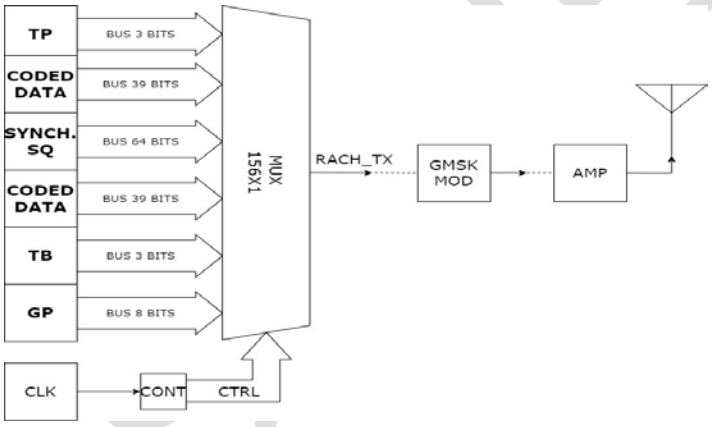
a) Simulación del demodulador GMSK.



b) Conversión de la señal paralela a serie.

Fuente: elaboración propia

Figura 5 Simulación del proceso de demodulación GMSK en Active-HDL y VHDL.

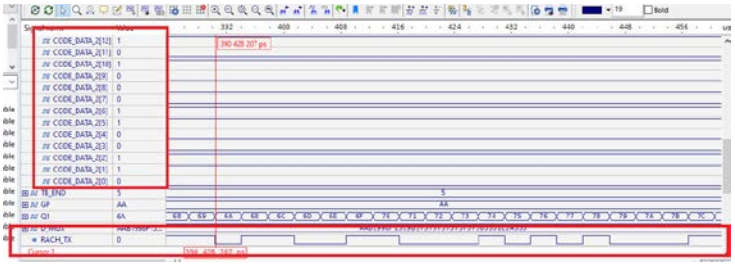


Fuente: elaboración propia

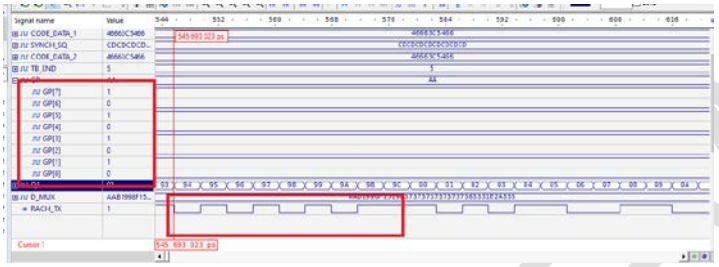
Figura 6 Diagrama del sistema transmisor del detector de receptores IMSI.

En la Figura 7a se aprecia la simulación del sistema de transmisión de datos codificados en serie, la Figura 7b muestra los últimos bits de guardia con la siguiente secuencia [0,1,0,1,0,1,0,1], representando el final del mensaje enviado para pasar a reiniciar los datos, arrancando con los bits de cola mostrado en la Figura 7c.

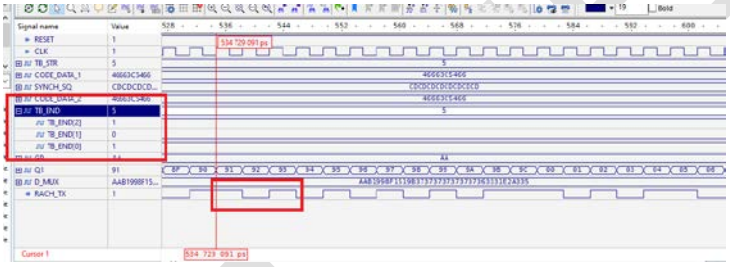
En la emulación de un Detector de Receptores IMSI se utilizó Matlab, Simulink y la herramienta de *Xilinx System Generator for DSP*, para desarrollar un programa base de un software de pruebas de estaciones base o detectores de receptores IMSI. Se sintetizaron y crearon bloques de control para los canales TDMA con la finalidad de observar una comunicación entre una terminal móvil (celular) y la estación base. El programa detector de receptor IMSI se compone de tres programas.



a) Condicionados.



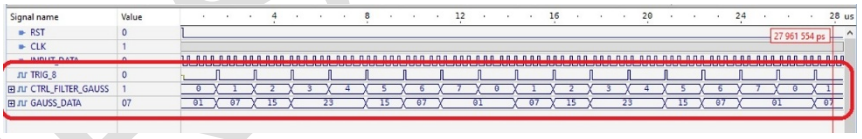
b) Tiempo de espera.



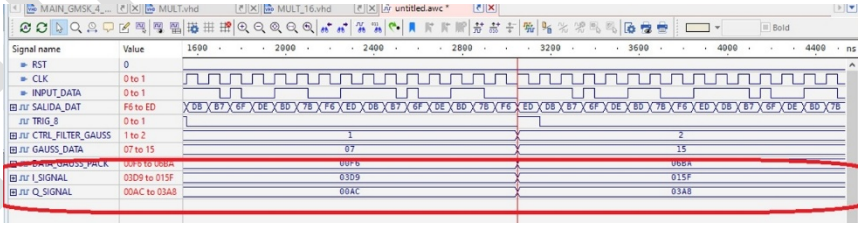
c) Segundo paquete de datos de cola.

Fuente: elaboración propia

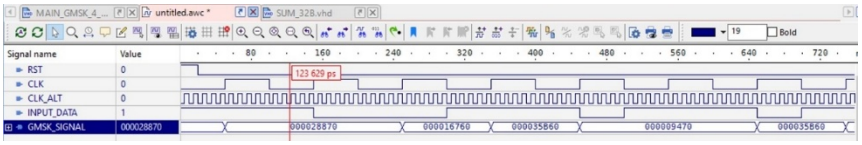
Figura 7 Envío de datos.



a) Simulación de un filtro Gaussiano en Active-HDL.



b) Generación de señales I-Q.



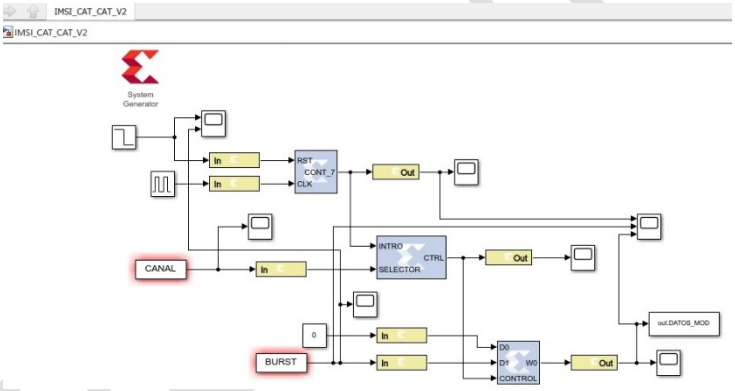
c) Generación de la señal GMSK.

Fuente: elaboración propia

Figura 8 Generación de la señalización GMSK en VHDL y Active-HDL.

El **primer programa** es un simulador de interferencia para los canales TDMA a una frecuencia específica. Este se divide en dos opciones: apoderarse de un canal TDMA específico y enviar información a la estación base en todos los canales TDMA. De este modo si se conoce la presencia de un receptor IMSI, se cubrirán todos los canales TDMA con el fin de que otros equipos no logren sufrir robo de información.

El **segundo programa** es un simulador de detector de receptores IMSI. El usuario introduce un supuesto IMSI señuelo para que el receptor IMSI lo capture, pero a su vez el receptor IMSI entrega información para que el detector reciba los datos MCC, MNC, LAC y Cell-ID. Estos son parámetros básicos para determinar la autenticidad de una estación base. La Figura 9 se muestra la emulación de varios códigos VHDL, un contador de $0-7$, un selector de canal $1x156$ y un control de envió de datos.



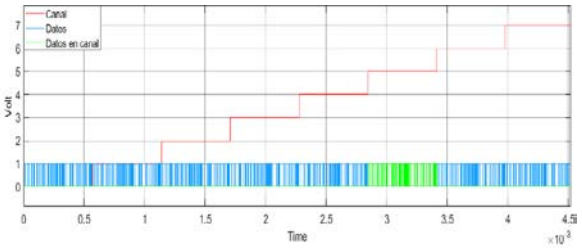
Fuente: elaboración propia

Figura 9 Co-simulación de un sistema de canalización TDMA en Simulink y SysGen.

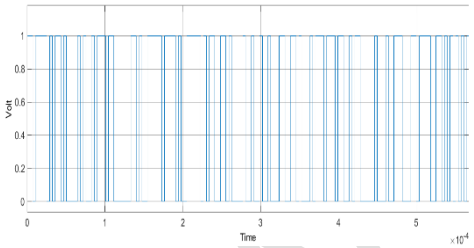
Resultados de un generador de Interferencia para canales TDMA

El primer programa consistió en la ejecución de un sistema que crea interferencia a una trama TDMA con fines de sabotaje en los sistemas de comunicaciones móviles en la tecnología 2G. La Figura 10a muestra una señal escalonada en color rojo, que representa el valor numérico del canal TDMA, en color azul se presenta la señal del generador de interferencia, pero repetidamente, con la finalidad de tener listos los datos a enviar cada vez que se cambie de canal. Y finalmente una señal de color verde, que representa la información que se enviará a la estación base, demostrando que el canal de envío de datos fue el canal 5. En la Figura 10b se

muestra una simulación de datos de envió correspondiente a la trama de información con un tiempo de $577\ \mu s$.



a) Datos activados en el canal 5.



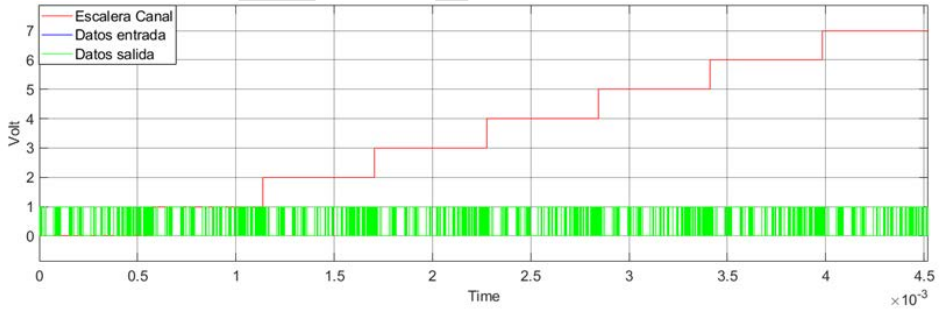
b) Datos enviados en un tiempo de $577\ \mu s$.

Fuente: elaboración propia

Figura 10 Simulación del manejo TDMA en SysGen.

Resultados de un Generador de Interferencia para una trama TDMA

Se simuló un ataque de interferencia total a todos los canales TDMA de una estación base de telecomunicaciones móviles. Se enviaron datos aleatorios a cada uno de los 8 canales TDMA, emulando ser 8 dispositivos al mismo tiempo. En la Figura 11 la línea roja representa el canal en que se transmitirá la información, la azul representa la entrada de datos y la verde muestra la señal de datos de salida.



Fuente: elaboración propia

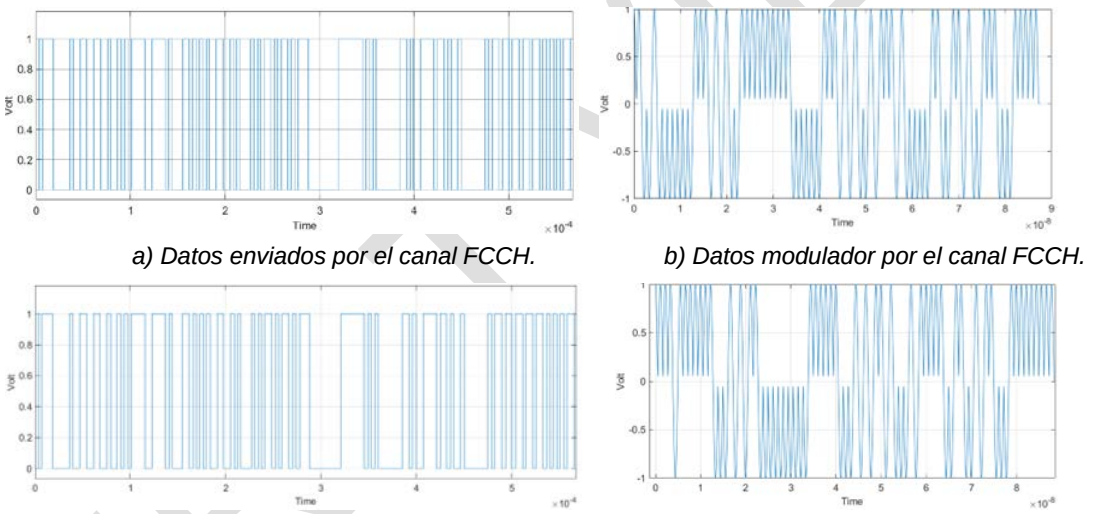
Figura 11 Transmisión de datos en cada uno de los canales TDMA.

Ejecución de un Detector de Receptores IMSI

El **tercer programa** implementado en el emulador representa un detector de receptores IMSI. El programa genera el número IMSI señuelo con el dato introducido. Una vez que se configura el número IMSI, se crea una señal en tren de pulso que representa una trama de comunicación que será transmitida en la simulación a fin de entablar una conexión en el canal de control de frecuencia

(FCCH), como se aprecia en la Figura 12a. La Figura 12b se muestra el siguiente paso por parte del detector de receptores IMSI, el cual consiste en modular la información para ser transmitida y recibida por la estación base falsa o el receptor de IMSI. Después que la estación base recibe la señal, entonces se procede a enviar información al detector de receptores IMSI con una trama de información entablando comunicación por el canal FCCH como se muestra en la Figura 12c. La Figura 12d muestra la señal de modulación por parte de la estación base.

Debido a que los sistemas comparten información, el software logra capturar los datos importantes de la estación base o receptor IMSI, para ser codificados y mostrar los datos MCC, MNC, LAC y el Cell-ID de la estación base, como se muestra en la Figura 13. Con lo anterior se logra la detección del receptor IMSI.



a) Datos enviados por el canal FCCH. *b) Datos modulador por el canal FCCH.*

c) Datos transmitidos por el canal FCCH. *d) Datos modulador por el receptor IMSI.*

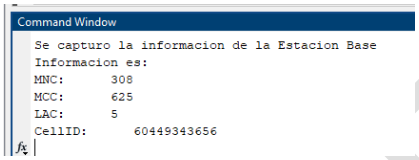
Fuente: elaboración propia

Figura 12 Simulación de datos entre el receptor de IMSI y el detector de receptores.

4. Discusión

Como se pudo apreciar con los diferentes equipos y maneras de detectar receptores IMSI. Donde la mayoría de los trabajos encontrados en la literatura se trabaja a nivel software o aplicación para detectar esta clase de equipos. El trabajo propuesto implementó un sistema basado en tarjetas FPGA reconfigurable y escalable para detectar receptores IMSI evaluando parámetros clave que la mayoría de los atacantes suelen omitir, como lo son el no configurar una estación base para

que aparente ser autentica. Este trabajo dará buenos resultados en la aplicación de otras tecnologías más recientes en redes de telefonía móvil. Añadiendo que se pueden investigar otro tipo de técnicas con menor capacidad y que se pueden ofrecer a las empresas de telecomunicaciones móviles para la operación de sus redes. Este sistema permite investigaciones en el análisis forense en la transmisión de datos de manera inalámbrica para proteger las redes de telefonía móvil ante ataques DoS, robo de información, entre otros delitos.



Fuente: elaboración propia

Figura 13 Información capturada del receptor IMSI.

5. Conclusiones

Se realizó la emulación de un detector de receptores IMSI, empleando una interfaz Matlab-Simulink y *System Generator for DSP de Xilinx*. El sistema brinda varias funcionalidades, desde un selector de canal TDMA en código VHDL hasta la comunicación entre un detector de receptores IMSI y una estación base falsa para recibir la información, codificarla y mostrarla al usuario. Esto con fines de crear una solución de monitoreo y auditoria para las redes de telefonía móvil, en especial las redes 2G debido a que los atacantes suelen conectar los equipos de los usuarios a la tecnología con seguridad más vulnerable, como son las redes GSM. También se desarrolló el código base para un sistema detector de receptores IMSI completamente en hardware que le da la capacidad de guardar información capturada en un registro de memoria para ser interpretada por el usuario, llevando a cabo un proyecto orientado al análisis forense de señales digitales que son transmitidas por estaciones base.

6. Bibliografía y Referencias

[1] Adrian, D. Geord, P. Edgar, R. W. The Messenger Shoots Back: Network Operator based IMSI Catcher Detection, 19th International Symposium,

Research in Attacks, Intrussions and Defenses, Springer, Paris, Francia, vol. 9854, pp. 279-302, 2016.

[2] González Garrido, A., Prototipo de estación base GSM usando OpentBTS, Tesis de examen de grado en Ingeniería de Telecomunicaciones, Universidad de Granada, 2015.

[3] Hasse, J., Gloe, T., Beck, M., et al. Forensic Identification of GSM Mobile Phones, Proceedings of the first ACM workshop on Information hiding and multimedia security, AMC Digital Library, NY, USA, pp. 131-140, 2013.

[4] Losif, A. Intercepting Mobile Phone Calls and Short Messagers Using a GSM Tester, 18th Conference, Computer Networks, Springer, Ustron, Polonia, vol.160, pp. 281-288, 2011.

[5] Khan, M. Niemi, V. Ginzboorg P. IMSI-Based routing and Identity Provacy in 5G, Proceeding of the 22nd Conference of Open Innovations Associations FRUCT, Finlandia, pp. 338-343, 2018.

[6] Kukushkin, A. Introduction to Mobile Networks Engineering GSM 3G-WCDMA, LTE and the Road to 5G, 1st Ed. Wiley, Australia, 2018.

[7] Márquez, R. Historia de una provocación tecno-cultural. Memes, subculturas irónicas e identidades digitales, Tesis de Maestría, Universidad Autónoma de Madrid, Departamento de Historia Contemporánea, 2018.

[8] Mjolsnes, S. F., Ruxandra, F. O., Easy 4G/LTE IMSI Catcher for Non-Programmers, International, Conference on Mathematical Methods, Models, and Architecture for Computer Network Security, ICMMACNT, Warsaw, Polonia, vol. 10446, pp. 235-246, 2017.

[9] Sadkhan, S., Abbas, N., Hutahit, M., Wireless Communication System Base on GMSK Modulation Scheme, Atti Della Fondozione Giorgio Ronchi, vol. 66, num. 2, 2011.

[10] Santaella, J. A., Comunicado de prensa 179/79, INEGI, SCT, IFT, Cd. de México, 2019.

[11] Van, R. K., The Effectiveness of a Homemade IMSI Catcher Build with YateBTS and BladeRF, Universidad de Amsterdam, Amsterdam, 2016.