Sistema de transmisión encriptada con HackRF

Encrypted Transmission System with HackRF

Juan José Mejía Gallo
Universidad de San Buenaventura
juanmejia@tau.usbmed.edu.co

Carlos Andrés Gómez Gutiérrez
Universidad de San Buenaventura
carlos.gomez211@tau.usbmed.edu.co

Evelyn Rendón Kalil
Universidad de San Buenaventura
evelyn.rendon@tau.usbmed.edu.co

Tipo de Artículo: Investigación científica y tecnológica

DOI: 10.21500/20275846.8025

Recibido: 2025-03-28

Revisado: 2025-07-08

Aceptado: 2025-09-05

Referenciar así: J.J. Mejia Gallo et al , "Sistema de transmisión encriptada con HackRF,"Ingenierías USBMed, vol. 16, n.º2, pp 14 - 19., 2025.

Resumen. Este proyecto presenta un sistema de transmisión encriptada de audio mediante HackRF y GNU Radio. El sistema captura una señal de audio de un micrófono, la limpia y la encripta. La señal encriptada se modula y se transmite a través de un HackRF. La señal se recibe con otro HackRF y se desencripta para recuperar la señal de audio original.

Palabras Clave. HackRF, GNU radio, encriptación, transmisión.

Abstract. This project presents an encrypted audio transmission system using the Software Defined Radio called HackRF and the software GNU Radio. The system captures an audio signal from a microphone, cleans it, and encrypts it using a robust encryption algorithm. The encrypted signal is modulated and transmitted using a HackRF device. The signal is received with another HackRF, demodulated, and decrypted to recover the original audio signal.

Keywords. HackRF, GNU radio, encryption, transmission, software defined radio.

Objetivos. Desarrollar y validar un sistema seguro y eficiente de transmisión de audio encriptado, el cual, mediante la tecnología de HackRF y GNU Radio, permita garantizar la privacidad y la confidencialidad en comunicaciones críticas.

Objetivos específicos.

• Investigar y seleccionar técnicas de encriptación apropiadas: evaluar diferentes algoritmos de encriptación para encontrar el más adecuado en términos de seguridad, eficiencia y compatibilidad con transmisiones de audio en tiempo real.

• Diseñar un sistema de transmisión de audio encriptado: crear un diseño detallado que integre la captura de audio, su encriptación, modulación, transmisión, recepción, desencriptación y reproducción, y cuyo énfasis sea garantizar la integridad y confidencialidad del contenido.

• Implementar el sistema en GNU Radio y HackRF: utilizar GNU Radio para desarrollar el flujo de procesamiento de señales, y configurar los dispositivos HackRF para la transmisión y recepción del audio encriptado.

• Realizar pruebas de seguridad y funcionalidad: verificar la robustez del sistema frente a potenciales vectores de ataque, y asegurar la calidad y claridad del audio transmitido al aplicar los ajustes necesarios para cumplir con los requisitos de seguridad.

I. Introducción

En un mundo cada vez más digital, la seguridad de la información se vuelve un tema crucial. La transmisión de audio segura es una necesidad en diversas aplicaciones, como pueden ser comunicaciones militares, teleconferencias confidenciales y radiodifusión digital. Los sistemas tradicionales de transmisión de audio pueden ser interceptados y manipulados fácilmente, lo que hace que la información sea vulnerable. La encriptación de la señal de audio antes de la transmisión puede proteger la información confidencial y garantizar la privacidad de las comunicaciones.

Este proyecto presenta un sistema de transmisión encriptada de audio que utiliza HackRF y GNU Radio para garantizar la seguridad y privacidad de las comunicaciones. HackRF es un dispositivo de radio definido por *software* (SDR) que permite la transmisión y recepción de señales de radio de banda ancha. GNU Radio es una plataforma de *software* libre para el procesamiento de señales de radio. El sistema captura, limpia, encripta, modula y transmite la señal de audio utilizando un HackRF. Esta es recibida por otro HackRF, en el que se desencripta y se recupera la señal de audio original.

El sistema ofrece una solución robusta, segura y flexible para la transmisión de audio, por lo que es ideal para aplicaciones donde la privacidad y la confidencialidad son fundamentales. Sus beneficios incluyen seguridad, privacidad, flexibilidad y bajo costo. Por ello, se puede aplicar en comunicaciones militares y gubernamentales, transmisión de información confidencial, entrevistas y reuniones privadas, telemedicina y educación a distancia.

II. Marco teórico

A. Radiofrecuencia

Las ondas de radio son una forma de radiación electromagnética que se propaga a través del espacio en forma de ondas sinusoidales. La frecuencia (f) de una onda de radio está relacionada con su longitud de onda (λ) por la velocidad de la luz:

$$(c): c = f \cdot \lambda$$

B. Antenas

Las antenas son dispositivos que emiten o reciben ondas electromagnéticas. La potencia radiada (Pr) por una antena isotrópica (que irradia energía uniformemente en todas las direcciones) se relaciona con la potencia transmitida (Pt) y la ganancia de la antena (G) por la ecuación de Friis:

$$P_r = P_t \cdot G \cdot \frac{\lambda^2}{(4\pi r)^2}$$

Donde r es la distancia entre las antenas.

C. Ganancia y potencia

La ganancia de una antena (G) se define como la relación entre la intensidad radiada en una dirección específica y la intensidad radiada por una antena isotrópica. La potencia (P) transmitida se relaciona con la intensidad del campo eléctrico (E) por la fórmula:

$$P = \frac{1}{2} \cdot \frac{E^2}{y}$$

Donde η es la impedancia del medio.

D. Desvanecimiento de señal

El desvanecimiento de señal es la atenuación que sufre esta debido a efectos como la reflexión, la difracción y la dispersión durante la propagación. Se puede modelar utilizando distribuciones estadísticas, como la distribución Rayleigh para canales inalámbricos.

E. Modulación y desmodulación

La modulación es el proceso de combinar la información de la señal con una portadora de alta frecuencia para transmitirla. La demodulación es el proceso inverso de extraer la información de la señal modulada.

F. Ruido y relación señal-ruido (SNR)

El ruido en un sistema de comunicación introduce aleatoriedad y puede degradar la calidad de la señal.

La SNR es la relación entre la potencia de la señal y la potencia del ruido, y es importante para determinar la calidad de la comunicación.

G. Multiplexación

La multiplexación es la técnica que permite combinar múltiples señales en un único medio de transmisión. Esto se logra asignando rangos de frecuencia o intervalos de tiempo específicos a cada señal para evitar interferencias entre ellas.

H. Propagación de ondas de radio

La propagación de ondas de radio se refiere al comportamiento de las ondas electromagnéticas mientras se propagan a través del espacio. Factores como la distancia, la frecuencia de la onda y las condiciones atmosféricas pueden afectar la propagación de las ondas de radio.

I. *Scrambler*

Un *scrambler* (o mezclador) en GNU Radio no es una herramienta de encriptación en el sentido tradicional de cifrado, como podrían ser los algoritmos AES o RSA, que utilizan claves secretas para cifrar y descifrar datos de manera segura. En cambio, un *scrambler* se utiliza para dispersar o "mezclar" la secuencia de bits de una señal de manera pseudoaleatoria con el fin de evitar largas secuencias de bits idénticos y mejorar la eficiencia de la transmisión. Aunque puede añadir una capa de ofuscación, por sí solo no debe considerarse una forma segura de encriptación.

El *scrambler* no es una herramienta única de GNU Radio, sino que se encuentra en muchas otras aplicaciones y tiene bastantes usos. Ahora bien, en el caso de GNU Radio, este funciona a través del uso de registros de desplazamiento con retroalimentación lineal (LFSR, por sus siglas en inglés). Los LFSR son populares debido a su simplicidad y eficiencia en la generación de secuencias pseudoaleatorias que son necesarias para el proceso de *scrambling*.

La operación de un LFSR puede describirse mediante una ecuación de retroalimentación lineal. Aunque el diseño específico puede variar, una forma general de la ecuación para un LFSR de n bits es:

$$S(t) = \big(a1 \cdot S(t-1) + a2 \cdot S(t-2) + \cdots + an \cdot S(t-n)\big) mod$$

Donde:

• $S(t)$ es el bit de salida en el tiempo t.

• $a1$, $a2$, …, an son los coeficientes que determinan qué bits del registro se utilizan para la retroalimentación. Estos coeficientes son fijos y definen el polinomio de retroalimentación del LFSR. Por ejemplo, para un LFSR con un polinomio de retroalimentación de $xn + xn - 1 + 1$, los coeficientes $an \times y\ an - 1$ serían 1, y todos los demás coeficientes serían 0, excepto el término constante.

• mod2 indica que la operación se realiza en aritmética de módulo 2 (es decir, aritmética XOR).

III. Método

Este proyecto se enfoca en el desarrollo de un sistema de encriptación para la transmisión de audio en tiempo real. La estructura del proyecto se divide en cinco etapas principales:

A. Preparación y planificación

• Definición del alcance del proyecto: determina los requisitos específicos, objetivos y límites del proyecto.

• Estudio de tecnologías y herramientas: conocer HackRF, GNU Radio y las tecnologías de encriptación disponibles.

• Equipos y *software*: implican tener el hardware y *software* necesario para el experimento (HackRF, computadora, cables, antena, GNU Radio, herramientas de encriptación, etc.).

B. Diseño del sistema

• Selección del método de encriptación: elección del método de encriptación adecuado para transmisión de audio en tiempo real.

• Definición de la arquitectura: diseño del flujo de señal completo, desde la captura hasta la recepción del audio, en el que se incluyan los puntos para la encriptación y desencriptación.

• Diseño de los flujos en GNU Radio: creación de los flujos de procesamiento de señales usando GNU Radio Companion (GRC) para capturar, encriptar, modular, transmitir, recibir, desencriptar y reproducir el audio.

C. Implementación

• Configuración del entorno de desarrollo: instalación de la herramienta GNU Radio y cualquier otra herramienta necesaria. Los HackRF deben estar correctamente configurados y deben instalarse los drivers necesarios para que sean reconocidos por el sistema.

• Desarrollo de los flujos en GNU Radio: mediante GNU Radio Companion, implementar los diseños de flujos creados en la fase de diseño. Esto incluye bloques para la captura, encriptación, modulación, transmisión, recepción, desencriptación y reproducción del audio.

• Integración del sistema de encriptación: ejecución del algoritmo de encriptación seleccionado dentro del flujo de GNU Radio, de modo que el audio se encripte antes de la transmisión y se desencripte después de la recepción.

D. Pruebas

• Pruebas de funcionalidad: cada componente del sistema (captura, encriptación, transmisión, recepción, desencriptación) debe funcionar correctamente de forma aislada.

• Pruebas de sistema: realización de pruebas del sistema completo para asegurar que el proceso de encriptación y transmisión de audio funcione de manera fluida y segura.

• Pruebas de seguridad: evaluación de la robustez del sistema de encriptación contra ataques potenciales, con énfasis en la preservación de la confidencialidad e integridad de las comunicaciones.

E. Ajustes y optimización

• Análisis de resultados de pruebas: identificación de cualquier problema o área de mejora basándose en las pruebas.

• Optimización: ejecución de ajustes en la configuración, el código o el diseño del sistema para mejorar el rendimiento, la seguridad y la eficiencia.

• Documentación: documentación del diseño del sistema, la configuración, los procedimientos de operación y cualquier detalle relevante para usuarios y administradores de este.

• El sistema de transmisión encriptada de audio se compone de dos partes principales: el transmisor y el receptor.

Por un lado, el transmisor:

- Captura la señal de audio de un micrófono.
- Limpia la señal de audio para eliminar el ruido no deseado.
- Encripta la señal de audio utilizando un algoritmo de criptografía.
- Modula la señal encriptada a través de una técnica de modulación digital.
- Transmite la señal modulada mediante un HackRF.

Por otro lado, el receptor:

- Recibe la señal modulada utilizando un HackRF.
- Demodula la señal para recuperar la señal encriptada.
- Desencripta la señal empleando el mismo algoritmo de criptografía utilizado en el transmisor.
- Reproduce la señal de audio original.

IV. Resultados

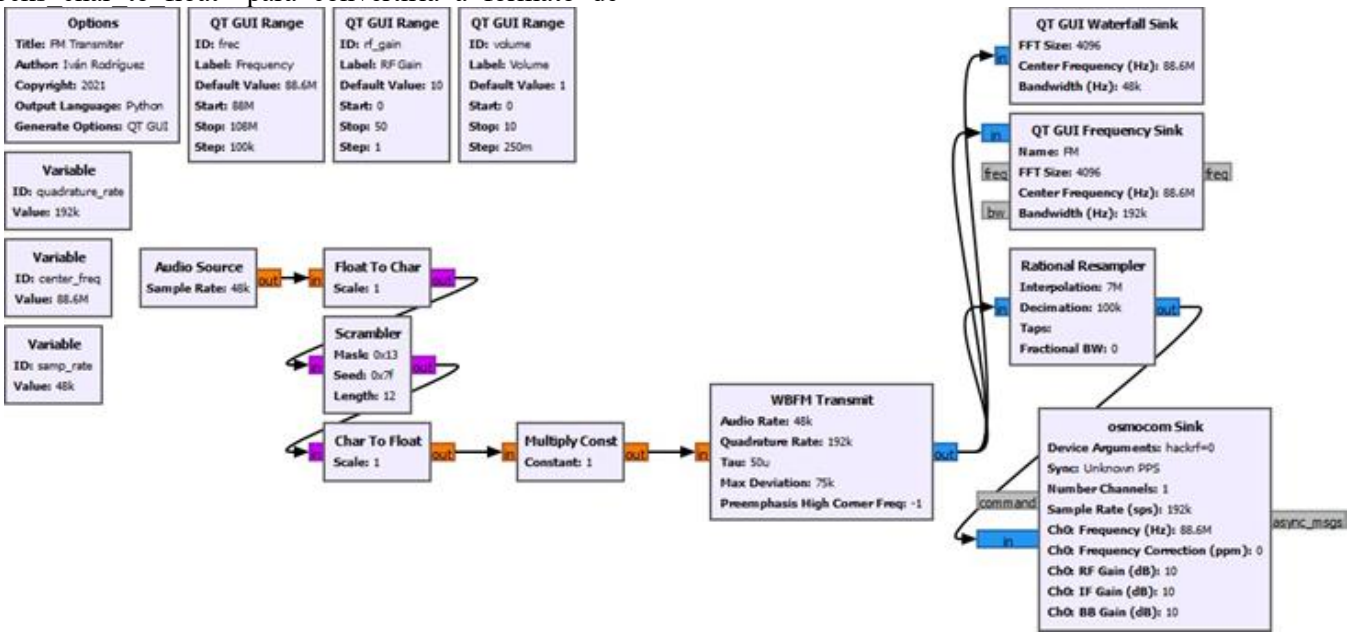
El transmisor diseñado utilizando GNU Radio y HackRF Pro descompone el proceso de transmisión en varias etapas clave que garantizan la calidad y seguridad de la señal de audio encriptada. En primer lugar, el código utiliza un bloque de "audio_source" para capturar la señal de audio del micrófono a una tasa de muestreo específica, definida por el parámetro "samp_rate". Luego, la señal de audio se procesa mediante un bloque "blocks_char_to_float" para convertirla a formato de punto flotante y se aplica una multiplicación constante para ajustar el volumen del audio, lo que proporciona flexibilidad en el nivel de salida.

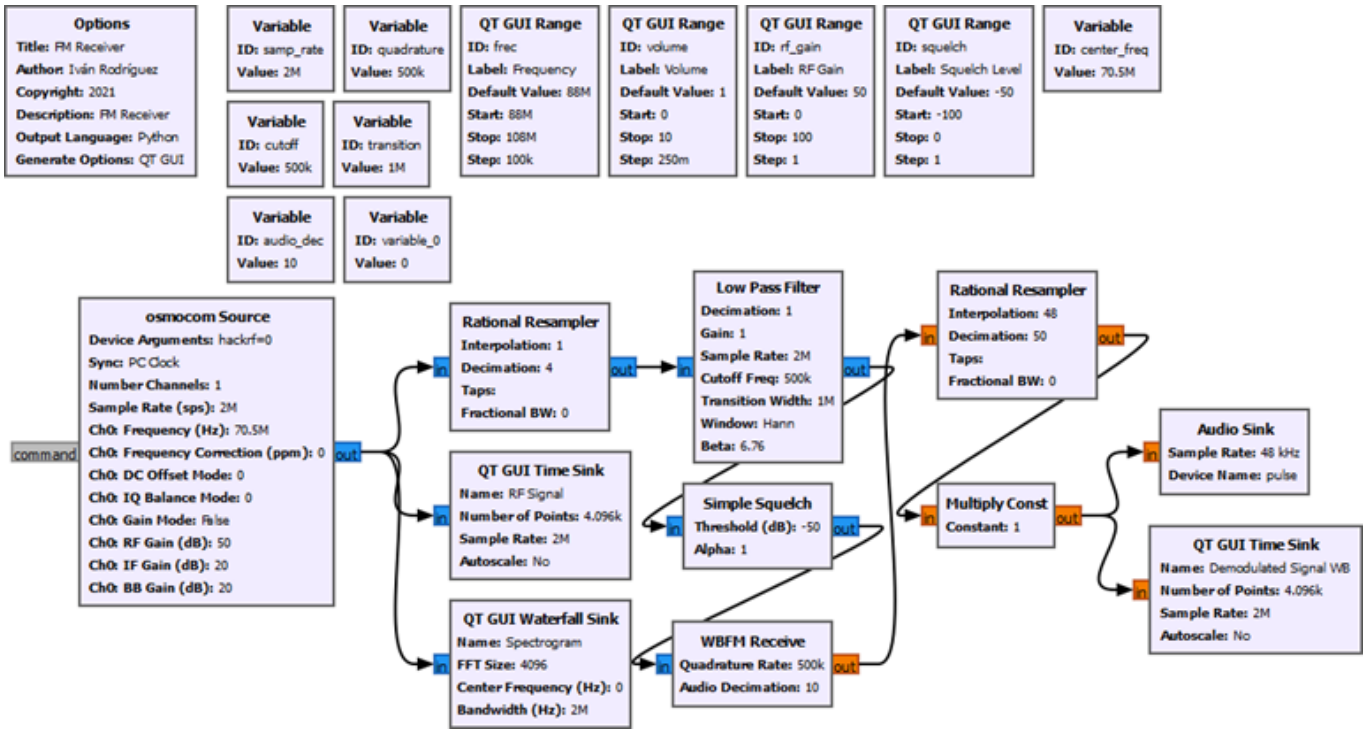
Posteriormente, la señal de audio se somete a un bloque de "digital_scrambler_bb" que aplica un algoritmo de mezcla pseudoaleatorio para encriptar la señal y agregar una capa adicional de seguridad. Este proceso garantiza que la señal transmitida no sea comprensible sin la clave de desencriptación adecuada.

A continuación, la señal encriptada se modula utilizando un bloque "analog_wfm_tx", que implementa la modulación de frecuencia (FM) para adaptar la señal al formato adecuado para su transmisión a través del HackRF. La frecuencia central de la modulación se establece mediante el parámetro "center_freq".

Finalmente, el transmisor utiliza un bloque "osmosdr_sink" para enviar la señal modulada al HackRF para su transmisión. Se especifican varios parámetros, como la ganancia de RF (rf_gain), la frecuencia central de transmisión ("center_freq"), y la tasa de muestreo del HackRF ("quadrature_rate"), para optimizar la transmisión y garantizar una recepción adecuada en el receptor.

El diseño modular del transmisor permite una configuración flexible y adaptable a diferentes condiciones de señal y requisitos de seguridad. La implementación exitosa de este transmisor contribuye significativamente a la capacidad del sistema para capturar, encriptar y transmitir señales de audio de manera segura y eficiente.





El receptor de FM en GNU Radio define una serie de bloques que componen el flujo de señal. Entre estos bloques se incluyen las configuraciones para el decodificador de audio, la frecuencia central de la señal, el filtro de paso bajo y la fuente de la señal de radio. Estos bloques están interconectados de acuerdo con el flujo de la señal, con conexiones que van desde la fuente de la señal de radio hasta la salida de audio. Además, se incluyen bloques para el control de parámetros como el volumen, la ganancia de RF y la frecuencia, así como interfaces gráficas para visualizar la señal de radio y el espectrograma en tiempo real. La configuración general del receptor permite ajustar parámetros clave como la frecuencia, el volumen y el umbral de silenciamiento, lo que facilita la recepción y demodulación de señales FM.

Con dos HackRF y dos computadoras, una ejecutando el código del transmisor y la otra el del receptor, se puede lograr una comunicación de radio bidireccional. El transmisor tomará la señal de audio de entrada, la modulará y la transmitirá a través del HackRF. La señal transmitida será captada por el receptor, que la recibirá mediante su HackRF. El receptor demodulará la señal y la presentará como salida de audio en la segunda computadora. De esta manera, se establecerá una conexión de comunicación de audio en tiempo real entre las dos computadoras a través de la radio. Las frecuencias y configuraciones de los HackRF deberán estar sincronizadas entre el transmisor y el receptor para garantizar una comunicación efectiva.

V. Discusión y conclusiones

• El uso de herramientas como HackRF y GNU Radio otorga al proyecto flexibilidad y potencia para el desarrollo de sistemas de comunicación personalizados y seguros, a la vez que permite abrir caminos para innovaciones futuras en el ámbito de las telecomunicaciones.

• La implementación de la encriptación y desencriptación en tiempo real introduce desafíos en términos de latencia, lo cual es crítico para aplicaciones que dependen de esta comunicación, lo que señala un área para mejoras futuras.

• Aunque el sistema funciona bien, todavía hay espacio para hacerlo más rápido, más fácil de usar y aún más seguro.

• La capacidad de enviar y recibir señales de radio mediante el uso de HackRF y *software* personalizado proporciona flexibilidad en la configuración de comunicaciones, lo que permite adaptarse a diversas necesidades y entornos.

• La comunicación por radio permite que dicha configuración funcione independientemente de la infraestructura de red convencional, lo que resulta útil en áreas donde la conectividad de red es limitada o inexistente.

• Aunque ofrece flexibilidad, la comunicación por radio tiene limitaciones en términos de alcance y potencia. Esto puede afectar la calidad y confiabilidad de la transmisión, sobre todo en entornos con interferencias.

Referencias

GNU Radio, “Tutorials,” GNU Radio Wiki. [En línea]. Disponible en: https://wiki.gnuradio.org/index.php/Tutorials

Great Scott Gadgets, “Software Defined Radio with HackRF, Lesson 1,”. [En línea]. Disponible en: https://greatscottgadgets.com/sdr/1/

W. H. Tranter, K. S. Shanmugan, T. Rappaport y K. Kosbar, Principles of Communication Systems Simulation with Wireless Applications, Upper Saddle River, NJ, USA: Prentice Hall, 2003.

J. Proakis y M. Salehi, Communication Systems Engineering, New Jersey, USA: Prentice Hall, 1994.

T. S. Rappaport, Wireless Communications: Principles and Practice, Upper Saddle River, NJ, USA: Prentice Hall, 1996.

J. G. Proakis y M. Salehi, Comunicaciones digitales, 5ª ed., México: Pearson Educación, 2008.

S. S. Haykin, Sistemas de comunicación, 5ª ed., México: McGraw-Hill, 2009.

A. Srinivasan y P. Arul Selvan. “A Review of Analog Audio Scrambling Methods for Residual Intelligibility,” ISDE, vol. 3, no. 7, 2012. [En línea]. Disponible en: https://core.ac.uk/outputs/234643036/?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1