GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

DETECCIÓN Y DECODIFICACIÓN DE SEÑALES "ENHANCED WI-FI"

Autor: Miguel Ángel Fernández Villar

Director: Javier Matanza Domingo

Madrid

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título

Detección y decodificación de señales “Enhanced Wi-Fi”

en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el

curso académico 2023/24 es de mi autoría, original e inédito y

no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido

tomada de otros documentos está debidamente referenciada.

Fdo.: Miguel Ángel Fernández Villar Fecha: 1/ 07/ 2024

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

Firmado por ***223*1-****-***6-ab5e-********565* el día 02/07/2024 con un certificado emitido por net+DC=windows+CN=MS-Organization-Access+OU=82dbaca4-3e81-46ca-9c73-0950c1eaca97

Fdo.: Javier Matanza Domingo Fecha: ……/ 07/ 2024

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

DETECCIÓN Y DECODIFICACIÓN DE SEÑALES "ENHANCED WI-FI"

Autor: Miguel Ángel Fernández Villar

Director: Javier Matanza Domingo

Madrid

Agradecimientos

A mi madre, a mi padre y a mi hermano por siempre haber estado a mi lado.

A mis amigos Cano, Charly y el francés por haberse convertido en familia.

A mis amigos de siempre.

A mis compañeros de universidad y profesores.

Gracias a todos.

DETECCIÓN Y DECODIFICACIÓN DE SEÑALES "ENHANCED WI-FI"

Autor: Fernandez Villar, Miguel Angel.
Director: Matanza Domingo, Javier.
Entidad Colaboradora: ICAI – Universidad Pontificia Comillas

RESUMEN DEL PROYECTO

Este proyecto se centra en la detección y decodificación de señales "Enhanced Wi-Fi", específicamente señales OFDM de 5 MHz utilizadas en la comunicación de drones DJI. Se desarrollará un algoritmo capaz de identificar y procesar estas señales, superando las limitaciones de las tarjetas de red inalámbricas convencionales. Los resultados finales mostrarán una detección precisa y la extracción fiable de direcciones MAC, validando la eficacia del algoritmo en condiciones reales.

Palabras clave: OFDM, señales Wi-Fi, drones DJI, Preámbulos PLCP, direcciones MAC.

1. Introducción

DJI, una empresa china líder en drones utiliza un sistema de transmisión Wi-Fi que controla eficientemente sus UAVs mediante una red Wi-Fi privada. A pesar de su eficacia, este sistema tiene un alcance limitado, haciéndolo más adecuado para usuarios principiantes. La técnica OFDM, usada en algunos drones DJI, permite adaptarse a diferentes anchos de banda. Sin embargo, las tarjetas de red convencionales no pueden detectar señales OFDM de 5 MHz debido a su diseño para anchos de banda mínimos de 20 MHz, presentando un desafío para la identificación de señales más estrechas, que son más susceptibles a interferencias. [1]

Las señales de banda estrecha tienen menor energía y son difíciles de diferenciar del ruido, requiriendo tecnología y métodos avanzados de procesamiento para su identificación. La motivación del proyecto radica en la creciente popularidad de los drones y la necesidad de una detección eficiente y segura de este tipo de señales, especialmente en áreas sensibles. Estas señales de banda estrecha presentan desafíos adicionales como mayor susceptibilidad a interferencias y menor energía total, lo que complica su detección y procesamiento. Debido a estas dificultades, se requiere el desarrollo de algoritmos especializados y métodos avanzados de procesamiento de señales digitales que puedan filtrar eficientemente el ruido, manejar interferencias cercanas y mejorar la relación señal-ruido.

El objetivo principal del proyecto es desarrollar un algoritmo que pueda superar estas limitaciones técnicas, permitiendo la detección precisa de las señales OFDM de 5 MHz y la extracción fiable de información crucial, como las direcciones MAC de los dispositivos transmisores y receptores, lo cual es esencial para el seguimiento y la autenticación de dispositivos en redes complejas.

2. Descripción del modelo

El modelo desarrollado para este proyecto se centra en la detección y decodificación de señales OFDM de 5 MHz, con el objetivo de extraer las direcciones MAC de los dispositivos involucrados. El desarrollo del software sigue una metodología sistemática basada en la creación y análisis de señales ideales y reales.

Inicialmente, se generaron señales ideales utilizando MATLAB para comprender las características y comportamientos de las señales OFDM según el estándar 802.11. Estas señales ideales sirvieron como referencia para comparar y validar el procesamiento de señales reales. Se generaron los preámbulos L-STF, L-LTF y L-SIG utilizando funciones específicas de MATLAB como wlanNonHTConfig, wlanLSTF, wlanLLTF y wlanLSIG. Estas funciones configuran los parámetros del paquete WLAN y generan las señales de entrenamiento necesarias para la sincronización y estimación de frecuencia en la recepción de señales Wi-Fi.[2]

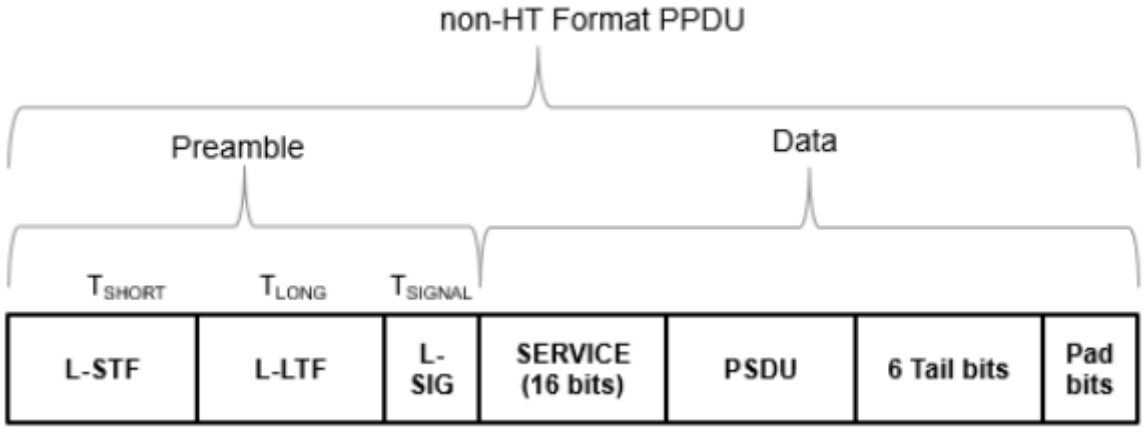

Figure 1: Non-HT PPDU Structure[2]

La señal real fue capturada de la comunicación de un dron DJI con su control remoto y convertida en un archivo MATLAB .mat para su análisis. Se comenzó con la representación temporal de la señal, seguida por su transformación al dominio de la frecuencia utilizando la Transformada de Fourier (FFT) para analizar su espectro.

Uno de los principales desafíos fue corregir el desplazamiento de frecuencia del portador (CFO), causado por diferencias entre las frecuencias del oscilador del transmisor y del receptor. Se desarrolló una función personalizada en MATLAB, correccionCFO, para centrar el espectro de la señal y ajustar la frecuencia, asegurando que las subportadoras estén correctamente alineadas.[3]

Para detectar la presencia de una trama válida, se utilizó una correlación entre la señal recibida y un preámbulo STF ideal. La función personalizada correlacionSTF realiza esta correlación, evaluando la fuerza del patrón de correlación para determinar si la señal contiene una trama válida basada en un umbral predefinido.

Para el preámbulo L-LTF, se implementó un proceso de ecualización para ajustar la señal recibida y asemejarla lo más posible a la señal ideal. Esto se realizó mediante la creación de la función correlacionLTFeq, que hace una correlación de la señal recibida ecualizada con el LTF ideal, mejorando la calidad y precisión de la señal.

Se utilizó la función wlanLSIGRecover para extraer los bits de datos del campo L-SIG, que contienen información crucial sobre la longitud del PSDU y otros parámetros. Esto permitió ajustar correctamente la longitud del PSDU para la posterior recuperación de datos.

La señal de datos fue demodulada utilizando wlanNonHTOFDMDemodulate, que convierte la señal temporal en símbolos OFDM. Estos símbolos fueron procesados por wlanNonHTDataBitRecover para recuperar los bits de datos originales del PSDU.

Finalmente, se desarrolló una función personalizada, extract_mac_from_psdu, para extraer las direcciones MAC de los bits del PSDU. Esta función convierte los bits a bytes y luego extrae las direcciones MAC en formato hexadecimal, proporcionando las direcciones del receptor, transmisor y una tercera dirección.

3. Análisis de resultados

El desarrollo e implementación del software para la detección y decodificación de señales "Enhanced Wi-Fi" ha producido resultados significativos que demuestran la eficacia y precisión del algoritmo especializado diseñado para procesar señales OFDM de 5 MHz utilizadas por drones DJI.

Uno de los primeros logros notables fue la capacidad del algoritmo para detectar señales OFDM de 5 MHz con alta precisión. Utilizando una combinación de correlación con preámbulos ideales y técnicas avanzadas de procesamiento de señales, el algoritmo logró identificar la presencia de señales válidas en entornos con ruido y CFO. La correlación con preámbulos STF y LTF mostró resultados de detección superiores al 80%, indicando una robusta capacidad del sistema para diferenciar señales de interés de posibles interferencias.

La corrección del CFO fue un componente esencial del modelo desarrollado. La función correccionCFO demostró ser efectiva en recentrar el espectro de la señal, permitiendo una alineación precisa de las subportadoras OFDM. Esto no solo mejoró la detección de señales, sino que también facilitó la posterior demodulación y recuperación de datos, asegurando la integridad y precisión de los bits de datos extraídos.

La implementación del software mostró un éxito significativo en la extracción de datos del PSDU y la recuperación de direcciones MAC. La función wlanLSIGRecover permitió determinar la longitud exacta de los datos, resolviendo problemas iniciales con la función wlanNonHTDataBitRecover que esperaba una longitud de datos predefinida. La capacidad de extraer direcciones MAC de la señal real validó la efectividad del algoritmo en condiciones prácticas, confirmando su utilidad para aplicaciones de seguimiento y autenticación en redes complejas.

El proceso de ecualización aplicado al preámbulo L-LTF mejoró significativamente la calidad de la señal recibida, alineándola con la señal ideal y reduciendo errores en la demodulación y decodificación de datos. La utilización de técnicas de filtrado adaptativo y estimación de canal fue fundamental para mejorar la relación señal-ruido (SNR), asegurando una comunicación más robusta y precisa en entornos con interferencias.

4. Conclusión

El proyecto ha demostrado ser una solución efectiva para superar las limitaciones actuales de las tarjetas de red inalámbricas convencionales en la detección de señales OFDM de 5 MHz. Mediante el desarrollo de un algoritmo especializado y su implementación utilizando MATLAB, se ha logrado identificar y procesar estas señales con alta precisión, así como extraer información crítica como las direcciones MAC.

Los resultados obtenidos validan la viabilidad técnica del modelo desarrollado y destacan su potencial para aplicaciones prácticas en diversos campos, incluyendo la seguridad y el control de drones, la vigilancia, y el seguimiento de dispositivos en redes complejas. La capacidad de detectar y decodificar señales de banda estrecha mejora la monitorización y el control de drones en áreas sensibles, contribuyendo a la protección de la privacidad y seguridad de individuos e instituciones.

Además, la futura adaptación del código para recibir señales de antenas reales y su posible integración en hardware, como tarjetas de red inalámbricas convencionales, representa un paso importante hacia la mejora de la tecnología actual. La optimización del algoritmo para su ejecución en dispositivos con recursos limitados, como módulos de comunicación integrados en drones, abre nuevas posibilidades para la expansión de las capacidades de los sistemas de comunicación inalámbrica.

En términos de impacto, este proyecto contribuye significativamente a la seguridad y eficiencia de la comunicación en drones, proporcionando una base sólida para futuros desarrollos y aplicaciones. La implementación de este algoritmo en hardware puede revolucionar la forma en que se gestionan y controlan las comunicaciones de drones, mejorando la calidad y fiabilidad de las operaciones en diversas industrias.

5. Bibliografía

[1] Business Insider: Cómo DJI se ha convertido en el mayor fabricante de drones del mundo. URL: https://www.businessinsider.es/como-dji-ha-convertido-mayor-fabricante-drones-mundo-1197696

[2] MathWorks. (n.d.). Non-HT PPDU Structure. URL: https://es.mathworks.com/help/wlan/gs/non-ht-ppdu-structure.html

[3] Wang, Z.; Wei, S.; Zou, L.; Liao, F.; Lang, W.; Li, Y. Deep-Learning-Based Carrier Frequency Offset Estimation and Its Cross-Evaluation in Multiple-Channel Models. Information 2023, 14, 98. https://doi.org/10.3390/info14020098

DETECTION AND DECODING OF “ENHANCED WI-FI” SIGNALS

Author: Fernandez Villar, Miguel Angel.
Supervisor: Matanza Domingo, Javier.
Collaborating Entity: ICAI – Universidad Pontificia Comillas)

ABSTRACT

This project focuses on the detection and decoding of "Enhanced Wi-Fi" signals, specifically 5 MHz OFDM signals used in the communication of DJI drones. An algorithm will be developed capable of identifying and processing these signals, overcoming the limitations of conventional wireless network cards. The final results will show precise detection and reliable extraction of MAC addresses, validating the algorithm's effectiveness in real-world conditions.

Keywords: OFDM, Wi-Fi signals, DJI drones, PLCP Preambles, MAC addresses.

1. Introduction

DJI, a leading Chinese drone company, uses a Wi-Fi transmission system that efficiently controls its UAVs through a private Wi-Fi network with dual frequency bands. Despite its effectiveness, this system has limited range, making it more suitable for beginner users. The OFDM technique, used in some DJI drones, allows adaptation to different bandwidths. However, conventional network cards cannot detect 5 MHz OFDM signals due to their design for minimum bandwidths of 20 MHz, presenting a challenge for identifying narrower signals, which are more susceptible to interference. [1]

Narrowband signals have lower energy and are difficult to differentiate from noise, requiring advanced technology and processing methods for identification. The project's motivation lies in the growing popularity of drones and the need for efficient and secure detection of these signals, especially in sensitive areas. These narrowband signals present additional challenges, such as higher susceptibility to interference and lower total energy, complicating their detection and processing. Due to these difficulties, the development of specialized algorithms and advanced digital signal processing methods is required to efficiently filter noise, manage nearby interference, and improve the signal-to-noise ratio.

The main goal of the project is to develop an algorithm that can overcome these technical limitations, allowing precise detection of 5 MHz OFDM signals and reliable extraction of crucial information, such as the MAC addresses of transmitting and receiving devices, which is essential for tracking and authenticating devices in complex networks.

2. Model Description

The model developed for this project focuses on the detection and decoding of 5 MHz OFDM signals, with the aim of extracting the MAC addresses of the involved devices. The software development follows a systematic methodology based on the creation and analysis of both ideal and real signals.

Initially, ideal signals were generated using MATLAB to understand the characteristics and behaviors of OFDM signals according to the 802.11 standard. These ideal signals served as a reference to compare and validate the processing of real signals. The L-STF, L-LTF, and L-SIG preambles were generated using specific MATLAB functions such as wlanNonHTConfig, wlanLSTF, wlanLLTF, and wlanLSIG. These functions configure the parameters of the WLAN packet and generate the necessary training signals for synchronization and frequency estimation in the reception of Wi-Fi signals.[2]

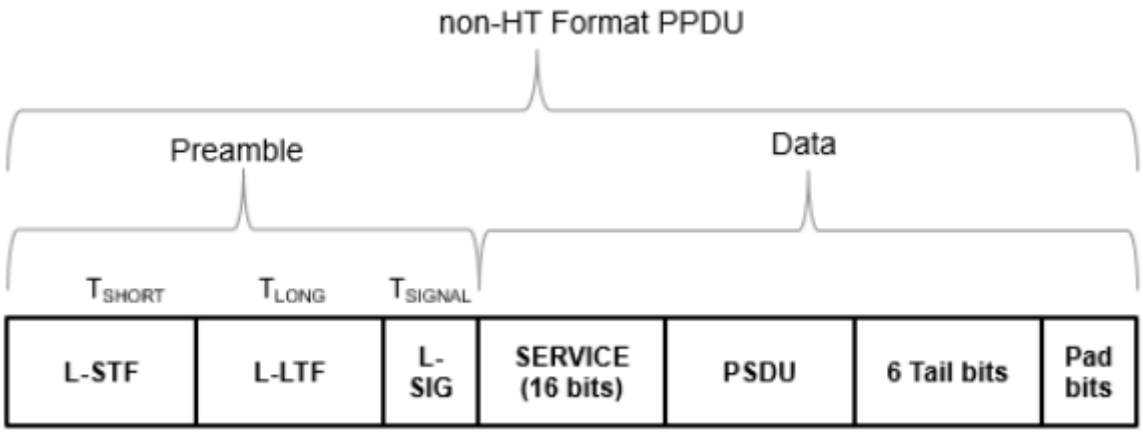

Figure 2: Non-HT PPDU Structure[2]

The real signal was captured from the communication between a DJI drone and its remote control, and it was converted into a MATLAB .mat file for analysis. The process began with the time-domain representation of the signal, followed by its transformation to the frequency domain using the Fast Fourier Transform (FFT) to analyze its spectrum.

One of the main challenges was correcting the carrier frequency offset (CFO), caused by differences between the transmitter and receiver oscillator frequencies. A custom MATLAB function, correccionCFO, was developed to center the signal spectrum and adjust the frequency, ensuring that the subcarriers are correctly aligned. [3]

To detect the presence of a valid frame, a correlation between the received signal and an ideal STF preamble was used. The custom function correlacionSTF performs this correlation, evaluating the strength of the correlation pattern to determine if the signal contains a valid frame based on a predefined threshold.

For the L-LTF preamble, an equalization process was implemented to adjust the received signal and make it resemble the ideal signal as closely as possible. This was done by creating the function correlacionLTFeq, which correlates the equalized received signal with the ideal LTF, improving the quality and accuracy of the signal.

The wlanLSIGRecover function was used to extract the data bits from the L-SIG field, which contain crucial information about the PSDU length and other parameters. This allowed for the correct adjustment of the PSDU length for subsequent data recovery.

The data signal was demodulated using wlanNonHTOFDMDemodulate, which converts the time-domain signal into OFDM symbols. These symbols were processed by wlanNonHTDataBitRecover to recover the original data bits from the PSDU.

Finally, a custom function, extract_mac_from_psdu, was developed to extract the MAC addresses from the PSDU bits. This function converts the bits to bytes and then extracts the MAC addresses in hexadecimal format, providing the receiver, transmitter, and a third address.

3. Results Analysis

The development and implementation of software for detecting and decoding "Enhanced Wi-Fi" signals have yielded significant results, demonstrating the effectiveness and precision of the specialized algorithm designed to process 5 MHz OFDM signals used by DJI drones.

One of the first notable achievements was the algorithm's ability to detect 5 MHz OFDM signals with high accuracy. Using a combination of correlation with ideal preambles and advanced signal processing techniques, the algorithm successfully identified the presence of valid signals in noisy environments with CFO. The correlation with STF and LTF preambles showed detection results exceeding 80%, indicating the system's robust capability to differentiate signals of interest from potential interferences.

CFO correction was an essential component of the developed model. The correccionCFO function proved effective in re-centering the signal spectrum, allowing precise alignment of OFDM subcarriers. This not only improved signal detection but also facilitated subsequent data demodulation and recovery, ensuring the integrity and accuracy of the extracted data bits.

The software implementation showed significant success in extracting PSDU data and recovering MAC addresses. The wlanLSIGRecover function allowed determining the exact data length, resolving initial issues with the wlanNonHTDataBitRecover function that expected a predefined data length. The ability to extract MAC addresses from the real signal validated the algorithm's effectiveness in practical conditions, confirming its utility for tracking and authentication applications in complex networks.

The equalization process applied to the L-LTF preamble significantly improved the quality of the received signal, aligning it with the ideal signal and reducing errors in data demodulation and decoding. The use of adaptive filtering techniques and channel estimation was fundamental in improving the signal-to-noise ratio (SNR), ensuring more robust and precise communication in interference-prone environments.

4. Conclusion

The project has proven to be an effective solution for overcoming the current limitations of conventional wireless network cards in detecting 5 MHz OFDM signals. By developing a specialized algorithm and implementing it using MATLAB, it has been possible to identify and process these signals with high precision and extract critical information such as MAC addresses.

The results obtained validate the technical feasibility of the developed model and highlight its potential for practical applications in various fields, including drone security

and control, surveillance, and device tracking in complex networks. The ability to detect and decode narrowband signals enhances the monitoring and control of drones in sensitive areas, contributing to the protection of the privacy and security of individuals and institutions.

Furthermore, the future adaptation of the code to receive signals from real antennas and its potential integration into hardware, such as conventional wireless network cards, represents a significant step towards improving current technology. Optimizing the algorithm for execution in resource-limited devices, such as communication modules integrated into drones, opens new possibilities for expanding the capabilities of wireless communication systems.

In terms of impact, this project significantly contributes to the security and efficiency of drone communication, providing a solid foundation for future developments and applications. Implementing this algorithm in hardware could revolutionize the management and control of drone communications, improving the quality and reliability of operations across various industries.

5. Bibliography

[1] Business Insider: Cómo DJI se ha convertido en el mayor fabricante de drones del mundo. URL: https://www.businessinsider.es/como-dji-ha-convertido-mayor-fabricante-drones-mundo-1197696

[2] MathWorks. (n.d.). Non-HT PPDU Structure. URL: https://es.mathworks.com/help/wlan/gs/non-ht-ppdu-structure.html

[3] Wang, Z.; Wei, S.; Zou, L.; Liao, F.; Lang, W.; Li, Y. Deep-Learning-Based Carrier Frequency Offset Estimation and Its Cross-Evaluation in Multiple-Channel Models. Information 2023, 14, 98. https://doi.org/10.3390/info14020098

Índice de la memoria

Índice de figuras

Índice de tablas

Capítulo 1. INTRODUCCIÓN

DJI es una empresa china fundada en 2006 con sede en Shenzhen, Guangdong, que se ha consolidado como líder mundial en el mercado de drones y tecnologías relacionadas, controlando más del 70% del mercado global de drones [1]. DJI ofrece una amplia gama de productos utilizados en el mercado de los Vehículos Aéreos No Tripulados (UAVs). Una de las tecnologías destacadas de DJI es el sistema de transmisión Wi-Fi utilizado por algunos de sus drones, que representa una solución económica y efectiva para controlar los UAVs. Este sistema se basa en la creación de una red Wi-Fi privada, y se caracteriza por su capacidad para utilizar bandas de frecuencia dual, que pueden cambiar automáticamente para optimizar el control del dron [2]. A pesar de su conveniencia y facilidad de uso, este sistema tiende a tener un alcance más limitado en comparación con otros métodos, lo que lo hace más adecuado para drones de consumo y usuarios principiantes [3].

OFDM (Orthogonal Frequency-Division Multiplexing) es la técnica de modulación utilizada por algunos drones DJI, capaz de adaptarse a diferentes anchos de banda. En el contexto de DJI, se utiliza para la comunicación entre los drones y sus mandos de control remoto, donde el ancho de banda específico depende de la aplicación y las normas relevantes. En particular, el uso de un ancho de banda de 5 MHz, aunque menos común que los anchos de banda de 20 MHz o 40 MHz típicamente utilizados en Wi-Fi, es más eficiente para sistemas que requieren un uso más eficiente del espectro o que operan en entornos con un espectro de radiofrecuencia más limitado [4]. Esto es especialmente relevante en aplicaciones donde se necesita reducir la interferencia o cuando el espectro disponible es limitado, ya que se necesita un control total del dron. Sin embargo, las tarjetas de red inalámbricas están diseñadas para la detección de señales de un ancho de banda mínimo de 20 MHz, lo que impide que identifiquen preámbulos de señales Wi-Fi de menor ancho de banda.

El uso de un ancho de banda de 5 MHz presenta ciertos desafíos. La principal diferencia es que las tarjetas de red inalámbricas están optimizadas para detectar señales de un ancho de banda mínimo de 20 MHz,[7] por lo que no pueden identificar preámbulos de señales más estrechas. Las señales de ancho de banda estrecho son más susceptibles a la interferencia de señales de frecuencias cercanas, lo que puede dificultar su identificación en entornos con muchas señales competidoras. Los dispositivos como las tarjetas de red inalámbricas están diseñados con filtros y algoritmos de procesamiento de señales para trabajar eficientemente con señales de anchos de banda más amplios, como los utilizados en redes Wi-Fi convencionales. Por lo tanto, no están adecuadamente equipados para identificar señales más estrechas, que requieren una mayor precisión y sensibilidad en el procesamiento de señales. Esto puede incluir la necesidad de filtros más precisos y algoritmos especializados que puedan discernir señales más sutiles del ruido de fondo y de las señales cercanas en el espectro. [8]

Las señales de banda estrecha pueden ser más difíciles de diferenciar del ruido o de otras señales debido a su menor "presencia" en el espectro. Además, las señales de banda estrecha suelen tener una menor energía total, lo que puede hacer que su detección sea más desafiante, especialmente en presencia de ruido o atenuación de la señal. Por estas razones, se necesita una tecnología más especializada y métodos de procesamiento de señales avanzados para identificar y trabajar con señales de ancho de banda pequeño de manera efectiva.

La motivación detrás de este proyecto radica en la creciente popularidad y el uso de drones, tanto en ámbitos personales, como la fotografía o videografía, como en ámbitos profesionales y militares. La manejabilidad perfecta de los drones es fundamental, ya que la mayoría son dirigidos a distancia, eliminando la necesidad de que el operador esté a bordo. Una comunicación perfecta entre el mando y el dron es crucial para su operación eficiente. Sin embargo, los drones no pueden volar sobre cualquier zona debido a preocupaciones de privacidad y seguridad, especialmente en áreas privadas o militarizadas. Es vital que la detección de drones y las señales que emiten puedan realizarse de manera rápida y eficaz. No todos los drones utilizan modulaciones fáciles de detectar, como el caso de OFDM de 5 MHz. Debido a que estas señales tienen preámbulos de un ancho de banda tan pequeño,

muchos sistemas no son capaces de detectarlas a tiempo. Por lo tanto, es necesario desarrollar un algoritmo capaz de detectar estas señales y decodificarlas.

El objetivo del proyecto es desarrollar un algoritmo capaz de identificar señales OFDM de 5 MHz utilizadas en la comunicación de los drones DJI. Este algoritmo representaría un avance significativo en la tecnología de detección de señales, abordando el desafío actual de las tarjetas de red inalámbricas convencionales que no pueden detectar señales con anchos de banda inferiores a 20 MHz. Al identificar eficientemente estas señales de menor ancho de banda, el algoritmo podría ampliar sus capacidades para extraer información adicional, como las direcciones MAC de los dispositivos transmisores y receptores. Esto sería especialmente valioso para aplicaciones que requieren el seguimiento y autenticación de dispositivos en redes complejas.

Capítulo 2. DESCRIPCIÓN DE LAS TECNOLOGÍAS

Tras establecer el contexto y la motivación del proyecto en el capítulo 1, donde se aborda la creciente necesidad de mejorar la detección de señales de 5 MHz utilizadas por los drones DJI, el capítulo 2 se centrará en las tecnologías que posibilitan la realización de este software. La implementación del algoritmo de detección y decodificación requiere herramientas robustas y flexibles que permitan el desarrollo y la validación de soluciones complejas. En este sentido, MATLAB se destaca como una plataforma ideal para el proyecto. MATLAB, con su potente capacidad de manipulación y análisis de datos, junto con un conjunto de funciones matemáticas y herramientas de visualización avanzadas, proporciona un entorno propicio para la creación y prueba de algoritmos. En las siguientes secciones, se explorará en detalle cómo MATLAB y sus toolboxes especializados son utilizados para implementar y optimizar el algoritmo, facilitando así la detección precisa y eficiente de señales OFDM de 5 MHz.

2.1 MATLAB

MATLAB, acrónimo de "Matrix Laboratory", es una plataforma de programación y un entorno de computación numérica desarrollado por MathWorks. Desde su creación, MATLAB se ha consolidado como una herramienta esencial en el ámbito académico e industrial, especialmente en disciplinas que requieren la manipulación y análisis de grandes volúmenes de datos y la implementación de algoritmos complejos. Su principal fortaleza radica en su capacidad para trabajar con matrices y vectores, lo que facilita la realización de cálculos matemáticos y la visualización de datos de manera eficiente. [9]

MATLAB proporciona un entorno interactivo que combina un lenguaje de alto nivel, un conjunto extenso de funciones matemáticas y herramientas de visualización avanzadas. Esto permite a los usuarios desarrollar algoritmos, analizar datos y crear aplicaciones con rapidez y precisión. Además, MATLAB es compatible con otros lenguajes de programación como C, C++, Java y Python, lo que amplía sus posibilidades de integración y colaboración con diversas plataformas y sistemas.[9]

2.1.1 IMPLEMENTACIÓN DE MATLAB

En el contexto del proyecto destinado a desarrollar un algoritmo para identificar señales OFDM de 5 MHz utilizadas en la comunicación de drones DJI, MATLAB se presenta como una solución óptima. Las señales OFDM son empleadas ampliamente en sistemas de comunicación inalámbrica debido a su eficiencia espectral y robustez frente a interferencias y desvanecimientos. Sin embargo, la detección y análisis de estas señales, especialmente aquellas con anchos de banda menores a 20 MHz, representa un desafío significativo para las tarjetas de red inalámbricas convencionales.

2.1.2 TOOLBOXES EN MATLAB

Para llevar a cabo este proyecto de manera efectiva, se utilizarán varios toolboxes especializados de MATLAB. Los toolboxes son colecciones de funciones y aplicaciones diseñadas para abordar tareas específicas, ampliando así las capacidades básicas de MATLAB y facilitando el desarrollo de soluciones complejas. En particular, estos toolboxes permiten acceder a algoritmos y funciones que han sido probados y optimizados para tareas específicas, reduciendo significativamente el tiempo de desarrollo y mejorando la precisión de los resultados.

Los Toolbox utilizados son los siguientes:

El **Communications Toolbox** es una herramienta fundamental en este proyecto. Este toolbox proporciona una amplia gama de algoritmos y aplicaciones para el diseño, simulación y análisis de sistemas de comunicación. Entre las funciones disponibles, se incluyen aquellas para la modulación y demodulación digital, corrección de errores y generación de señales. Estas herramientas permiten simular y analizar sistemas de comunicación complejos, lo cual es crucial para el procesamiento y análisis de señales OFDM. Por ejemplo, las funciones de modulación y demodulación digital permiten trabajar con una variedad de esquemas de modulación utilizados en las comunicaciones modernas, incluyendo QPSK, QAM y otros, facilitando la adaptación del algoritmo a las características específicas de las señales OFDM de 5 MHz utilizadas por los drones DJI [10]

El **Signal Processing Toolbox** también será esencial para el proyecto. Este toolbox ofrece una extensa colección de funciones para el análisis y diseño de señales. Incluye herramientas para el filtrado digital, transformadas, análisis espectral y mucho más. Estas herramientas son vitales para la descomposición detallada de las señales OFDM capturadas, permitiendo una comprensión profunda de sus componentes frecuenciales y temporales. Por ejemplo, las herramientas de filtrado permiten eliminar el ruido de las señales capturadas, mejorando la calidad de los datos procesados. Las transformadas, como la Transformada de Fourier, facilitan el análisis espectral, identificando las frecuencias presentes en las señales OFDM y permitiendo así la detección y caracterización precisa de las mismas [11]

El **WLAN Toolbox** es otro componente clave en el proyecto. Este toolbox está diseñado específicamente para el diseño y verificación de sistemas de comunicación inalámbrica. Proporciona funciones y ejemplos para la generación de formas de onda WLAN, lo cual es especialmente útil dado que las señales OFDM de los drones DJI son similares a las utilizadas en las redes WLAN. Este toolbox permite simular y analizar estas señales de manera efectiva, facilitando el desarrollo de algoritmos que puedan identificar y demodular las señales de 5 MHz. Por ejemplo, las funciones de generación de formas de onda permiten crear señales de prueba que replican las características de las señales reales, mientras que las herramientas de análisis permiten examinar estas señales para extraer información crucial, como las direcciones MAC de los dispositivos [12].

El uso de estos toolboxes no solo acelera el proceso de desarrollo, sino que también garantiza que los algoritmos implementados se basen en métodos y técnicas de última generación, respaldados por la comunidad científica y técnica. Esto es fundamental en un proyecto que busca abordar el desafío de identificar señales OFDM de menor ancho de banda, algo que las tarjetas de red inalámbricas convencionales no pueden hacer de manera eficiente. Al aprovechar las capacidades avanzadas de estos toolboxes, el proyecto puede lograr una detección precisa y confiable de señales, así como la extracción de información crucial como las direcciones MAC de los dispositivos transmisores y receptores, contribuyendo significativamente al seguimiento y autenticación de dispositivos en redes complejas.

Capítulo 3. ESTADO DE LA CUESTIÓN

En la actualidad, el desarrollo de algoritmos capaces de identificar señales OFDM de 5 MHz utilizadas en la comunicación de drones DJI representa un avance tecnológico significativo. Este desarrollo aborda la limitación de las tarjetas de red inalámbricas convencionales que no pueden detectar señales con anchos de banda inferiores a 20 MHz, lo cual es un desafío crítico en la detección y autenticación de dispositivos en redes complejas.

Las señales de banda estrecha son particularmente desafiantes de identificar debido a varios factores inherentes a su naturaleza. Primero, la menor anchura de banda implica que la energía de la señal se distribuye sobre un espectro más reducido, lo que puede dificultar la diferenciación de la señal frente al ruido de fondo. Segundo, la proximidad de las frecuencias de las señales competidoras puede causar interferencias significativas, complicando aún más el proceso de detección. Esto es especialmente problemático en entornos urbanos densos o en escenarios donde múltiples dispositivos de comunicación operan simultáneamente en bandas de frecuencia adyacentes.

Para abordar estos desafíos, es necesario desarrollar algoritmos especializados que puedan detectar y procesar señales de banda estrecha con alta precisión. Estos algoritmos deben ser capaces de filtrar eficazmente el ruido y las interferencias, además de ser lo suficientemente sensibles para captar señales de baja energía. Esto puede incluir el uso de técnicas avanzadas de procesamiento de señales digitales (DSP), como la utilización de filtros adaptativos y algoritmos de estimación de canal que mejoren la relación señal-ruido (SNR) .

La modulación OFDM es una técnica ampliamente estudiada debido a su eficiencia en la transmisión de datos en sistemas de comunicación inalámbrica. OFDM permite la transmisión de datos mediante múltiples subportadoras ortogonales, lo que aumenta la eficiencia espectral y proporciona robustez frente a la interferencia y el desvanecimiento. Sin embargo, un problema bien conocido de OFDM es su sensibilidad a los desplazamientos

de frecuencia de la señal (CFO), que pueden ser causados por la diferencia entre las frecuencias del oscilador local del transmisor y el receptor .

La estimación y corrección del CFO es crucial para mantener la ortogonalidad de las subportadoras y minimizar la interferencia entre portadoras (ICI) El CFO puede provocar una rotación de fase no deseada en las subportadoras, resultando en una degradación significativa del rendimiento del sistema. Por lo tanto, la detección precisa y la corrección de estos desplazamientos son esenciales para asegurar una comunicación fiable y eficiente.[6]

Existen varias técnicas de estimación de CFO, como las basadas en secuencias de entrenamiento y en símbolos piloto. Las secuencias de entrenamiento suelen consistir en patrones conocidos que se transmiten al inicio de una trama de datos, permitiendo al receptor estimar y corregir el CFO antes de la recepción de los datos útiles. Los símbolos piloto, por otro lado, se insertan de manera periódica en la trama de datos y se utilizan para realizar ajustes continuos del CFO durante la transmisión.[6]

Una de las técnicas de estimación más efectivas es el método MMSE (Error Cuadrático Medio Mínimo). Este método se ha demostrado eficaz para la estimación del CFO utilizando símbolos piloto, minimizando el error cuadrático medio mediante la comparación de las fases de todas las subportadoras en cada símbolo OFDM. Al reducir el error cuadrático medio, el método MMSE mejora la precisión de la detección de señales y la calidad de la comunicación, especialmente en presencia de ruido y atenuación. Esto lo convierte en una herramienta valiosa para el procesamiento de señales en sistemas OFDM .

La investigación en este campo continúa evolucionando, con estudios recientes explorando nuevas formas de optimizar la estimación y corrección del CFO, así como técnicas avanzadas de DSP para mejorar la detección de señales de banda estrecha. Estos avances son esenciales para el desarrollo de soluciones que puedan superar las limitaciones actuales de

las tarjetas de red inalámbricas y mejorar la capacidad de detectar y procesar señales OFDM de 5 MHz .

Varios trabajos de investigación han abordado la detección y procesamiento de señales OFDM en diferentes contextos, explorando técnicas avanzadas para mejorar la precisión y eficiencia de estos sistemas. Recientemente, se han propuesto enfoques basados en DeepLearning para la detección de señales OFDM. Por ejemplo, un estudio desarrollado por investigadores en 2021 propuso un esquema de detección de señales basado en DeepLearning para sistemas OFDM. Este enfoque, denominado DDLSD (Data-driven Deep Learning for Signal Detection), utiliza redes neuronales para reemplazar el proceso de estimación de canal, ecualización y detección de señales. Los resultados mostraron que el método DDLSD tiene una robustez significativamente mayor y una tasa de error de bit (BER) más baja en comparación con los métodos tradicionales, especialmente en condiciones de ruido y atenuación [15].

Además, la investigación de Yimeng Huang. sobre algoritmos de detección de paquetes OFDM en sistemas de comunicación con sensores inalámbricos para el hogar destacó la importancia de la precisión en la detección y el consumo de energía. Compararon y discutieron el rendimiento de varios algoritmos de detección de paquetes, mostrando que el algoritmo de autocorrelación tenía el mejor rendimiento general. También señalaron los desafíos abiertos y las direcciones futuras de investigación en este campo, subrayando la necesidad de mejoras continuas en los algoritmos de detección de señales para entornos de IoT [14].

Finalmente, los avances en la detección de señales OFDM utilizando técnicas de DeepLearning han mostrado promesas significativas. Por ejemplo, se ha investigado el uso de redes neuronales convolucionales (CNN) y redes neuronales de memoria a largo plazo (LSTM) para mejorar la detección de señales en sistemas OFDM, demostrando una mejora notable en la precisión de detección y la resistencia al ruido y a las interferencias [15].

Estos trabajos ilustran la diversidad de enfoques y tecnologías que se están explorando para mejorar la detección de señales OFDM, proporcionando una base sólida para el desarrollo de algoritmos más eficientes y precisos en el futuro.

Capítulo 4. DEFINICIÓN DEL TRABAJO

4.1 JUSTIFICACIÓN

La importancia de este proyecto está en la identificación y resolución de un problema técnico específico que afecta directamente a la operatividad y seguridad de los sistemas de comunicación en drones. En el mundo actual, los drones se utilizan ampliamente en una variedad de aplicaciones que van desde el entretenimiento personal hasta la vigilancia militar, pasando por la agricultura, la fotografía y la entrega de paquetes. Esta auge en su uso ha llevado a una necesidad urgente de mejorar y optimizar los sistemas, especialmente en lo que respecta a la detección y decodificación de señales de radiofrecuencia.

Este proyecto puede contribuir a la mejora del desarrollo de nuevas tecnologías en nuestra sociedad. La capacidad de los drones para realizar tareas complejas de manera autónoma y eficiente ha revolucionado industrias enteras. Por ejemplo, en la agricultura, los drones permiten la monitorización precisa de cultivos, la gestión del riego y la aplicación de pesticidas con una eficiencia sin precedentes. En la industria de la cinematografía, los drones han abierto el acceso a tomas aéreas espectaculares que antes solo eran posibles con costosos helicópteros. En la vigilancia y seguridad, los drones proporcionan una herramienta invaluable para la monitorización de grandes áreas con un coste relativamente bajo.

En este contexto, las soluciones e-health también juegan un papel crucial. Los drones pueden ser equipados con sensores y dispositivos médicos para entregar suministros urgentes en áreas de difícil acceso o para realizar tareas de monitorización remota de la salud. Estas aplicaciones demuestran cómo la tecnología puede ser una fuerza para el bien, mejorando la calidad de vida y resolviendo problemas complejos de manera innovadora.

Desde un punto de vista técnico, la justificación de este proyecto se centra en la necesidad de superar las limitaciones actuales de las tarjetas de red inalámbricas convencionales, que están diseñadas para detectar señales con anchos de banda mínimos de 20 MHz. Esta

especificación limita su capacidad para identificar señales OFDM de 5 MHz utilizadas en la comunicación de drones DJI, creando un vacío tecnológico que este proyecto busca llenar. Al desarrollar un algoritmo capaz de detectar y procesar estas señales de banda estrecha, se mejora significativamente la capacidad de los sistemas de comunicación para operar de manera efectiva en entornos desafiantes.

La justificación del proyecto no solo se basa en la superación de una limitación técnica, sino también en la oportunidad de mercado que presenta. En el caso específico de los drones DJI y la modulación OFDM de 5 MHz, el mercado presenta una oportunidad. La creciente demanda de drones y la necesidad de sistemas de comunicación más robustos y eficientes hacen de este proyecto una inversión prometedora. Además, la capacidad de extraer direcciones MAC de los dispositivos transmisores y receptores añade un nivel adicional de funcionalidad que puede ser extremadamente valioso para aplicaciones que requieren el seguimiento y autenticación de dispositivos en redes complejas, como las redes IoT (Internet de las Cosas).

Haciendo un análisis de lo comentado en el capítulo 3, se puede observar que, aunque ha habido avances significativos en la detección y procesamiento de señales OFDM, persisten desafíos importantes. La modulación OFDM es una técnica bien establecida en la transmisión de datos, pero su aplicación en señales de banda estrecha, como las de 5 MHz utilizadas por los drones DJI, plantea problemas únicos. Los estudios han demostrado que la menor anchura de banda de estas señales las hace más susceptibles a la interferencia y al ruido, complicando su detección precisa.

Investigaciones como las de Yimeng Huang, comentadas en el capítulo 3 [14], han explorado técnicas avanzadas para la estimación y corrección del desplazamiento de frecuencia del portador (CFO) y la reducción del error cuadrático medio (MMSE). Estos trabajos han proporcionado un marco valioso para el desarrollo de algoritmos de detección, mostrando que la utilización de secuencias de entrenamiento y símbolos piloto puede mejorar significativamente la precisión de la detección en sistemas OFDM.

Sin embargo, a pesar de estos avances, la detección de señales OFDM de 5 MHz sigue siendo un área con desafíos abiertos. Las investigaciones recientes han comenzado a explorar el uso de técnicas de DeepLearning para mejorar la detección de señales. Por ejemplo, el esquema DDLSD utiliza redes neuronales para reemplazar los procesos tradicionales de estimación de canal, ecualización y detección de señales, mostrando una mejora notable en la precisión de detección y la resiliencia al ruido. [13]

Este proyecto se posiciona en la vanguardia de la innovación tecnológica al abordar directamente estos desafíos mediante el desarrollo de un algoritmo especializado que no solo detecta señales OFDM de 5 MHz, sino que también es capaz de extraer información crítica de las señales, como las direcciones MAC. Esto no solo mejora la capacidad de los sistemas de comunicación actuales, sino que también abre nuevas posibilidades para aplicaciones avanzadas en redes IoT y en la monitorización y control de drones.

Además, la implementación de este algoritmo ha utilizado herramientas avanzadas de procesamiento de señales digitales (DSP) representa un enfoque novedoso. MATLAB, con su Communications Toolbox y Signal Processing Toolbox, proporciona un entorno robusto para la implementación y prueba de estos algoritmos, permitiendo una experimentación y optimización rápidas.

El impacto de este proyecto se extiende más allá del ámbito técnico, influyendo en varios aspectos de la sociedad y el mercado. En términos de seguridad, la capacidad de detectar y decodificar señales de banda estrecha mejora la monitorización y control de drones en áreas sensibles, ayudando a proteger la privacidad y seguridad de los individuos y las instituciones. Esto es especialmente relevante en zonas urbanas densas y en instalaciones críticas donde la presencia de drones no autorizados puede representar una amenaza significativa.

En el mercado, la solución propuesta tiene el potencial de convertirse en un estándar para la comunicación de drones, estableciendo nuevos benchmarks en términos de eficiencia y seguridad. La capacidad de detectar señales de 5 MHz y extraer direcciones MAC también puede ser un diferenciador clave en la industria de los drones, proporcionando a los fabricantes una ventaja competitiva significativa.

Aunque el desarrollo de un algoritmo de detección de señales OFDM de 5 MHz es un paso crucial, hay varios desafíos y oportunidades futuras que deben considerarse. La evolución de las técnicas de procesamiento de señales y DeepLearning continuará presentando nuevas posibilidades para mejorar la precisión y eficiencia de los algoritmos de detección. La integración de tecnologías emergentes, como el 5G y las redes de sensores avanzados, también ofrecerá nuevas oportunidades para expandir las capacidades del sistema.

Además, la implementación en hardware de estas soluciones presenta sus propios desafíos. La optimización del algoritmo para su ejecución en dispositivos con recursos limitados, como wearables y módulos de comunicación integrados en drones, requerirá un enfoque cuidadoso para equilibrar el rendimiento y el consumo de energía.

4.2 OBJETIVOS

Este proyecto tiene como objetivo principal el desarrollo de un algoritmo capaz de identificar señales OFDM de 5 MHz utilizadas en la comunicación entre drones DJI y sus mandos. Como ya se ha comentado anteriormente, esta tarea representa un avance significativo en la tecnología de detección de señales debido a la limitación actual de las tarjetas de red inalámbricas, las cuales están diseñadas para detectar señales con un ancho de banda mínimo de 20 MHz. Esta especificación implica una incapacidad para detectar señales cuyos preámbulos son de un ancho de banda inferior, como es el caso de las señales de 5 MHz empleadas por algunos modelos de drones DJI bajo el estándar “Enhanced Wi-Fi”.

La incapacidad de las tarjetas de red convencionales para detectar estas señales de banda estrecha se debe a que están optimizadas para los estándares de comunicación Wi-Fi predominantes, que operan en anchos de banda más amplios. Esta limitación presenta un desafío crítico en la detección y autenticación de dispositivos en redes complejas, especialmente en entornos donde la comunicación con drones es fundamental para su operación eficiente y segura. Por lo tanto, el desarrollo de un algoritmo que pueda identificar

estas señales de menor ancho de banda y extraer información adicional, como las direcciones MAC de los dispositivos transmisores y receptores, es una necesidad imperante.

La importancia de este proyecto se extiende más allá de la mera detección de señales. Al lograr identificar eficientemente estas señales de banda estrecha, se abre la posibilidad de mejorar la seguridad y la eficiencia de la comunicación en drones, lo cual es esencial para aplicaciones en áreas donde la privacidad y la seguridad son preocupaciones primordiales.

4.3 METODOLOGÍA

El enfoque metodológico para este proyecto se va a dividir en varias etapas, cada una de las cuales permite la incorporación de nuevas ideas y planteamientos a medida que avanza el proyecto. Esta metodología estructurada garantiza que el desarrollo del algoritmo sea riguroso y sistemático, abordando todos los aspectos críticos necesarios para su implementación y optimización.

4.3.1 ANÁLISIS DE REQUISITOS

Esta primera etapa implica identificar y comprender las necesidades específicas que debe cubrir la solución. Esto incluye una recolección exhaustiva de datos a través de la investigación de los estándares utilizados en la comunicación de drones DJI, analizando y entendiendo los formatos y modelos que deben implementarse. Esta etapa es crucial para establecer una base sólida sobre la cual construir el algoritmo, asegurando que todos los requisitos técnicos y de mercado sean abordados adecuadamente.

4.3.2 DISEÑO DE SEÑAL IDEAL

La segunda etapa se enfoca en la creación y diseño de una señal ideal que cumpla con todos los estándares aplicados de forma óptima. La intención es experimentar primero con esta señal ideal para obtener una idea clara de los resultados esperados posteriormente. Esta fase permite realizar pruebas y ajustes iniciales en un entorno controlado, proporcionando una base de comparación para las siguientes etapas del proyecto.

4.3.3 DISEÑO DE SEÑAL REAL EN LOCAL

En la tercera etapa se procederá a experimentar con una señal real capturada de un dron DJI. Esta fase es crucial para validar los resultados obtenidos con la señal ideal en un entorno realista, asegurando que el algoritmo sea capaz de detectar y procesar señales de banda estrecha de manera efectiva en condiciones reales de operación. El objetivo es recrear los resultados obtenidos anteriormente, pero esta vez utilizando señales reales generadas por drones, lo que proporciona una validación práctica del algoritmo.

4.3.4 EVALUACIÓN FINAL

La cuarta y última etapa consiste en la evaluación de los desarrollos realizados y la implementación de mejoras según sea necesario. Se buscará feedback para afinar y optimizar el producto final, asegurando que cumpla con todos los requisitos técnicos y de mercado. Esta etapa garantiza que el algoritmo no solo sea técnicamente sólido, sino también práctico y útil para las aplicaciones previstas.

Capítulo 5. ANÁLISIS TEÓRICO

Una vez expuestos los motivos y la metodología del proyecto, es fundamental proceder con un desarrollo detallado. En esta sección, se presentará el marco teórico que sustenta el proyecto, describiendo los conceptos, ya que el marco teórico es esencial para comprender el contexto y la relevancia del proyecto. Este apartado se centrará en los conceptos fundamentales y las teorías previas que han guiado el desarrollo del proyecto.

5.1 SEÑALES OFDM

La tecnología OFDM (Orthogonal Frequency Division Multiplexing) es una técnica utilizada para la transmisión de datos en las redes Wi-Fi definidas por el estándar IEEE 802.11. Comprender una señal OFDM, el proceso de codificación de un PPDU (Physical Protocol Data Unit), y la estructura del PLCP (Physical Layer Convergence Protocol) es esencial para aprovechar al máximo las capacidades de estas redes. A continuación, se van a explicar una visión general de que son este tipo de señales, que procesos y protocolos están integrados, incluyendo la naturaleza de una señal OFDM, los pasos involucrados en la codificación de un PPDU, y los formatos de campo del PLCP en diferentes versiones del estándar IEEE 802.11.[20]. Posteriormente, en el apartado ***5.2,*** se entrará en el detalle, hablando de cuales se han utilizado específicamente para este proyecto y los motivos,

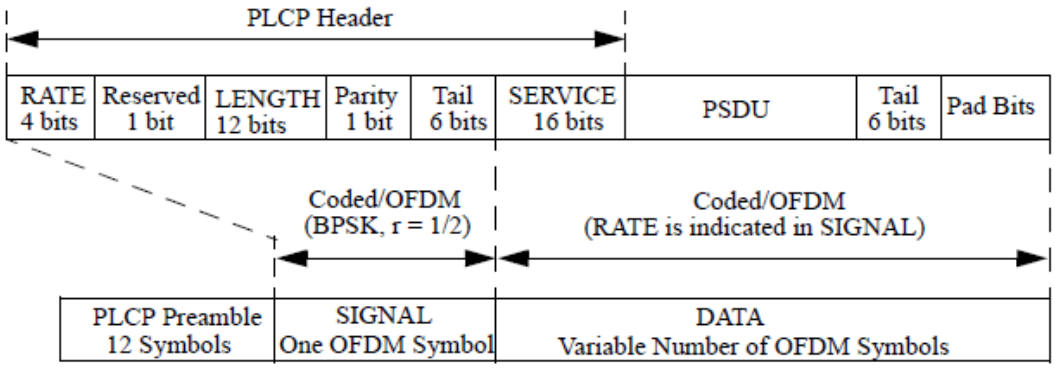

Figura 5-1: Formato de PPDU [20]

5.1.1 ¿QUÉ ES UNA SEÑAL OFDM?

OFDM, o Orthogonal Frequency Division Multiplexing, es una técnica de modulación que divide un canal de comunicaciones en múltiples subcanales de frecuencia estrecha y ortogonales entre sí. Esta ortogonalidad asegura que las señales transmitidas en diferentes subportadoras no interfieran entre sí, permitiendo así un uso más eficiente del espectro. Cada subportadora en OFDM se modula de manera independiente, y todas se transmiten simultáneamente, lo que maximiza la capacidad de transmisión de datos y minimiza los efectos negativos de la interferencia y el desvanecimiento selectivo en frecuencia.

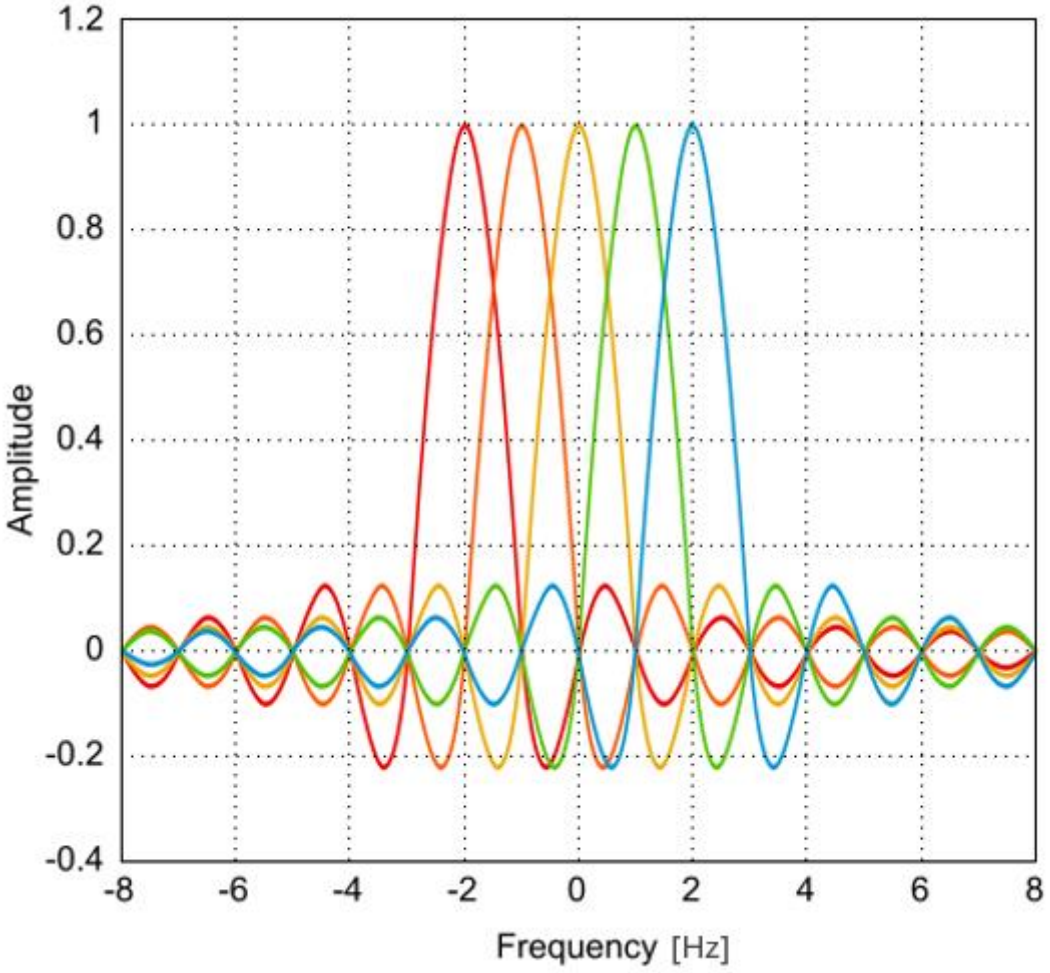

Figura 5-2: Espectro en frecuencia de una señal OFDM [22]

En un sistema OFDM, el ancho de banda total del canal se divide en N subportadoras equiespaciadas. La señal transmitida se obtiene mediante la combinación de todas estas subportadoras. En el receptor, la señal se descompone nuevamente en sus subportadoras componentes, y cada una de estas subportadoras se demodula de manera independiente. Esto hace que OFDM sea particularmente robusto frente a los efectos s de distorsión del canal. [15]

5.1.2 ¿QUÉ ES EL PPDU?

El PPDU, o Physical Protocol Data Unit, es el paquete de datos que se transmite a través del medio físico en un sistema de comunicaciones IEEE 802.11. Aquí están los bits los cuales nos dicen cuál es la dirección MAC origen y destino y de la cual sacaremos la información más adelante. El proceso de codificación de un PPDU en un sistema OFDM incluye varios pasos clave: [21]

1. **Generación de Datos**: Los datos de usuario (o datos de carga útil) que se desean transmitir se recogen y se preparan para la transmisión.
2. **Codificación de Canal**: Los datos se codifican usando un esquema de codificación de canal, como la codificación convolucional, para añadir redundancia y permitir la corrección de errores.
3. **Interleaving**: Los datos codificados se intercalan para distribuir los bits de manera que se reduzcan los errores en ráfaga.
4. **Mapeo de Símbolos**: Los bits intercalados se mapean en símbolos de modulación, utilizando técnicas como BPSK, QPSK, 16-QAM, 64-QAM, etc.
5. **Asignación de Subportadoras**: Los símbolos de modulación se asignan a las subportadoras OFDM.
6. **Transformada IFFT**: Los símbolos de las subportadoras se transforman del dominio de la frecuencia al dominio del tiempo mediante la Transformada Inversa de Fourier (IFFT).
7. **Añadido de Ciclo Prefijo**: Se añade un intervalo de guarda (ciclo prefijo) al inicio de cada símbolo OFDM para mitigar la interferencia intersímbolos.
8. **Conversión Digital-Analógica**: La señal digital se convierte a una señal analógica para su transmisión a través del medio físico. [21]

Existen diferentes formatos dependiendo de la versión del estándar IEEE, de los cuales se hablará en el apartado **5.1.5**.

5.1.3 EL PROTOCOLO FÍSICO (PHY)

La capa física (PHY) del estándar IEEE 802.11 define las características físicas de la red inalámbrica, incluyendo cómo se modulan las señales, cómo se transmiten y reciben, y cómo se manejan las diferentes frecuencias de radio y canales. Esta capa es fundamental para asegurar la transmisión eficiente y fiable de datos a través del aire, y se divide en varias subcapas y funciones clave: [21]

1. **Modulación y Demodulación**: La capa PHY especifica los esquemas de modulación utilizados para convertir los datos digitales en señales analógicas adecuadas para la transmisión a través del medio inalámbrico, como es en este caso OFDM. La demodulación es el proceso inverso, donde las señales analógicas recibidas se convierten nuevamente en datos digitales.
2. **Codificación y Decodificación**: Para mejorar la robustez y fiabilidad de la transmisión, la capa PHY también define los métodos de codificación de canal, como la codificación convolucional y los códigos LDPC (Low-Density Parity-Check). Estos métodos añaden redundancia a los datos transmitidos, permitiendo la detección y corrección de errores en el receptor.
3. **Manejo del Espectro de Frecuencia**: La capa PHY especifica cómo se utilizan las diferentes bandas de frecuencia y canales disponibles para la comunicación inalámbrica. Esto incluye la asignación de frecuencias, la gestión de interferencias, y la coordinación del uso del espectro entre múltiples dispositivos.
4. **Control de Potencia de Transmisión**: La capa PHY también define cómo se controla la potencia de transmisión de las señales para optimizar la cobertura y reducir la interferencia con otros dispositivos.
5. **Formación de Tramas**: La capa PHY estructura los datos en tramas específicas para su transmisión. Esto incluye la preparación de la PDU física, también conocida como PPDU, que como se comentó en el apartado ***5.1.2***, encapsula los datos de usuario junto con la información necesaria para la sincronización y la gestión de la transmisión. [21]

5.1.4 ¿QUÉ ES EL PLCP?

El PLCP, o Physical Layer Convergence Protocol, es una subcapa del protocolo físico (PHY). El PLCP es responsable de preparar los datos para su transmisión a través del medio físico y de procesar los datos recibidos. Actúa como un puente entre las capas superiores del protocolo y la subcapa PMD (Physical Medium Dependent), que se ocupa de la transmisión y recepción real de las señales.

El PLCP encapsula los datos en la estructura PPDU y añade información adicional necesaria para la sincronización y la gestión de la comunicación. Esto incluye preámbulos para la sincronización de la señal, encabezados que especifican el formato y la tasa de datos, y otros campos necesarios para una transmisión eficiente y confiable. Esto se puede apreciar en la figura 5.3 y de lo cual se entrará más es detalle en el apartado 5.2.2.

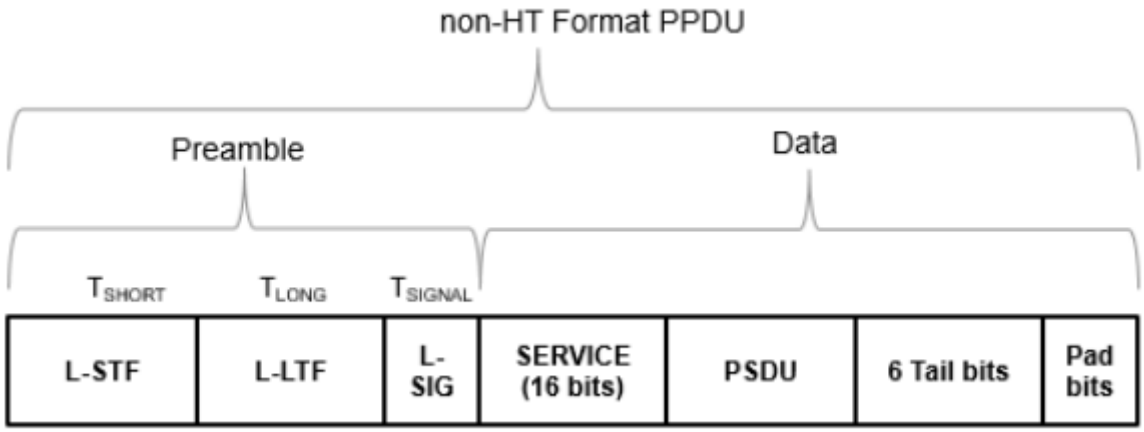

Figura 5-3: Non-HT PPDU Structure [26]

Aquí cabe destacar el preámbulo PLCP es una parte crucial de la trama de datos transmitida en las redes inalámbricas y crucial para el desarrollo de este proyecto. Su función principal

es facilitar la sincronización y la estimación de parámetros necesarios para la correcta recepción y decodificación de la señal por parte del receptor. El preámbulo PLCP incluye una secuencia de bits que permite al receptor sincronizarse con la señal entrante, ajustar sus parámetros de recepción y preparar la decodificación de los datos subsiguientes. Gracias a estas características, este preámbulo será el utilizado para la detección de la señal en este proyecto.[23] (Se entrar más en detalle en el apartado **5.2**)

5.1.5 FORMATOS DE PPDU NON-HT, VHT Y HT-MIXED

En las redes Wi-Fi basadas en el estándar IEEE 802.11, los PPDU pueden tener diferentes formatos dependiendo de la versión del estándar y la tecnología de modulación utilizada. En las versiones IEEE 802.11a y 802.11g, el formato del PPDU OFDM incluye los siguientes campos: [26]

- **Preámbulo**: Incluye 12 símbolos OFDM de entrenamiento.

- **SIGNAL**: Un símbolo OFDM que contiene información sobre la tasa y la longitud del paquete.

- **Datos**: Los símbolos OFDM que contienen los datos de usuario, codificados y modulados.

Algunos de los formatos comunes de PPDU incluyen:

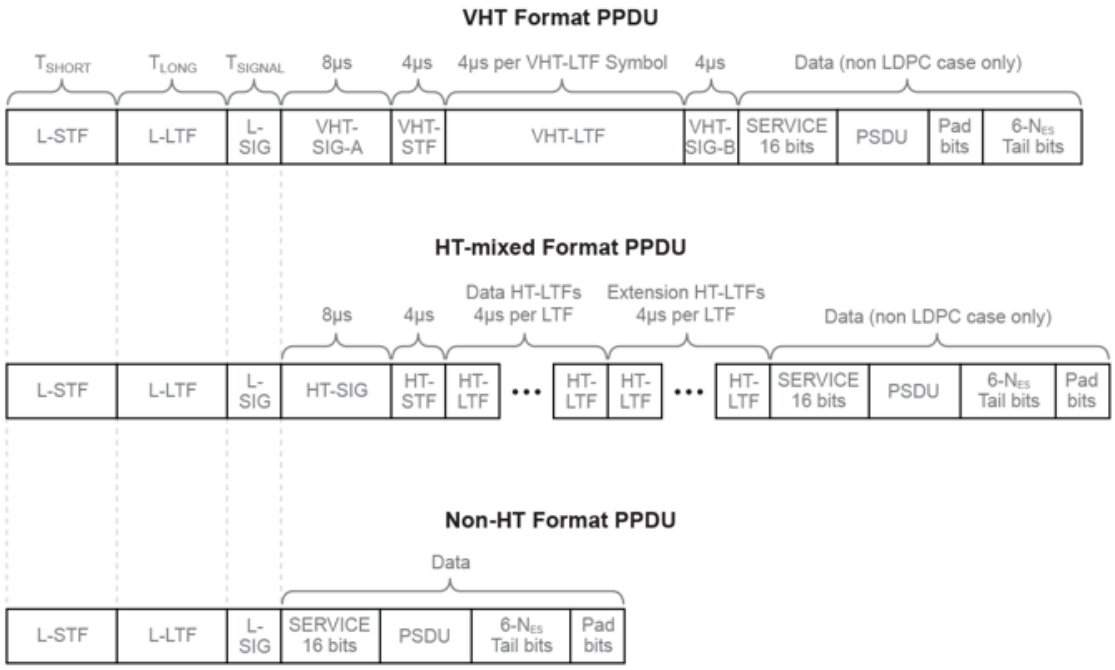

Figura 5-4: estructura de formatos de PPDU [26]

1. **VH-Mixed (Very High Throughput Mixed):** El formato VH-Mixed de la PPDU es una de las configuraciones avanzadas definidas en los estándares de comunicación inalámbrica, específicamente en el IEEE 802.11ac. Este formato está diseñado para optimizar la transmisión de datos en redes Wi-Fi de alta eficiencia, adaptándose tanto a las necesidades de dispositivos antiguos como a los más modernos. Su objetivo es asegurar compatibilidad y mejora en el rendimiento de la red inalámbrica.[26]

2. **VHT (Very High Throughput)**: Introducido con IEEE 802.11ac, el formato VHT se diseñó para soportar tasas de datos extremadamente altas mediante el uso de anchos de banda más amplios (hasta 160 MHz), MU-MIMO y 256-QAM. Un PPDU VHT, el cual se puede ver en la figura 5.4, incluye los siguientes campos adicionales y modificados:
    - VHT-SIG A: Contiene información sobre el ancho de banda, el número de antenas espaciales y otros parámetros.

- VHT-STF y VHT-LTF: Campos de entrenamiento para la estimación del canal en configuraciones MIMO avanzadas.
- VHT-SIG B: Proporciona detalles adicionales sobre la longitud del paquete y otros parámetros específicos de VHT.[26]

3. **El formato Non-HT (Non-High Throughput)** en PPDU se refiere al formato utilizado que preceden a las mejoras de alta velocidad introducidas con 802.11n y posteriores (como 802.11ac y 802.11ax). Estos formatos más antiguos son a menudo referidos simplemente como 802.11a/b/g.[21] El formato Non-HT es el estándar básico de modulación y codificación que no utiliza las técnicas de alta velocidad de las generaciones posteriores. [26]

   Como se puede apreciar en la figura 5.1, el PPDU Non-HT se compone de las siguientes partes:

   - **Preámbulo**: Esta es la primera parte de la PPDU y se utiliza para la sincronización y el establecimiento de la señal. Incluye partes como el Synchronization Short Training Field (STF) y el Long Training Field (LTF), que ayudan al receptor a bloquear la frecuencia y la fase de la señal entrante.
   - **Encabezado PLCP** (PHY Header): Contiene información meta sobre la transmisión, como la tasa de datos, la longitud del PSDU y la paridad. El encabezado PLCP permite al receptor entender cómo procesar los datos que siguen. Para los formatos non-HT, este encabezado es más simple en comparación con los encabezados HT o VHT que se encuentran en los estándares más nuevos.
   - **PSDU**: La carga útil real que contiene la información a ser transmitida. Este es el dato que fue pasado de la capa MAC a la capa PHY para la transmisión.

- **Tail Bits**: Bits de relleno para asegurar que el bloque de codificación tiene el tamaño correcto para el proceso de codificación convolucional.
- **Pad Bits**: Se añaden al final para garantizar que la longitud de la transmisión sea un múltiplo del número de subportadoras utilizados en la OFDM. [27]

A lo largo del proyecto, se ha utilizado el formato non-HT. El motivo será explicado en el apartado 5.2.

5.1.6 TIPOS DE FRAMES Y FORMATOS PARA EL ESTÁNDAR 802.11

En la comunicación inalámbrica, los marcos 802.11 se clasifican en tres categorías principales: marcos de gestión, marcos de control y marcos de datos. Cada tipo de marco tiene un formato específico y cumple funciones distintas dentro de la red. Los marcos 802.11 están compuestos por tres partes principales: encabezado, cuerpo y trailer. [28]

El encabezado contiene información sobre el destino del marco, la tasa de datos, el conjunto de cifrado utilizado para cifrar los marcos de datos y más. Los campos de dirección en el encabezado son críticos, ya que determinan la fuente, el destino, el transmisor y el receptor de la trama.

El cuerpo de la trama contiene la información de las capas 3 a 7, que está encapsulada y protegida. El tamaño del cuerpo varía dependiendo del tipo de transmisión; por ejemplo, los marcos de tráfico de voz son más pequeños que los marcos utilizados para la descarga de archivos.

La última parte de la trama incluye la secuencia de verificación de tramas (FCS), que es un control de redundancia cíclica de 32 bits usado para validar que el contenido de la trama no ha sido alterado o corrompido durante la transmisión. [28]

5.1.6.1 Campos de Dirección

Un aspecto crítico para este proyecto del formato de trama 802.11 es la estructura de los campos de dirección. Como se aprecia en la figura 5.5, los marcos pueden tener hasta cuatro campos de dirección, dependiendo de la dirección del marco (To DS y From DS), cada uno de ellos lleva una información diferente:

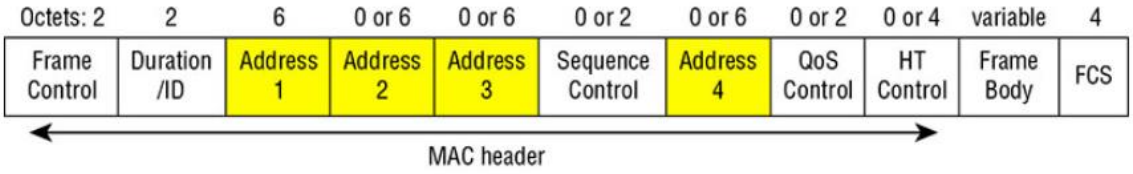

Figura 5-5: Formato de frame detallado por bytes [28]

- **Address 1** (Dirección 1): Siempre contiene la dirección MAC del receptor del marco. En los marcos de datos, este es el destinatario final.

- **Address 2 (**Dirección 2): Contiene la dirección MAC del transmisor del marco.

- **Address 3** (Dirección 3): Utilizado en escenarios de infraestructura, contiene la dirección MAC de la estación final o el AP, dependiendo de la dirección del marco.

- **Address 4** (Dirección 4): Este campo se usa solo en configuraciones de distribución (DS) y no siempre está presente. Es relevante en configuraciones de redes en malla o WDS.

Estos campos de dirección son fundamentales para el correcto enrutamiento y entrega de tramas, permitiendo que las estaciones y los puntos de acceso identifiquen correctamente el origen y destino de cada trama. [28]

En el contexto de este proyecto, se centrará en la extracción de direcciones MAC de los campos Address 1, Address 2 y Address 3 de las tramas capturadas. Este análisis es crucial para la identificación y autenticación de dispositivos en la red. La capacidad de detectar y extraer direcciones MAC con precisión permitirá la implementación de medidas de seguridad avanzadas y mejorará la gestión de la red.

Como se comentó en capítulos anteriores, al capturar y analizar estas tramas, se pueden identificar patrones de comunicación, detectar dispositivos no autorizados y optimizar el rendimiento de la red mediante la identificación de cuellos de botella y la mitigación de interferencias. La información extraída de los campos de dirección puede ser utilizada para mapear la topología de la red, identificar puntos de acceso saturados y mejorar la planificación de la capacidad.

5.2 APLICACIÓN DE LA TEORÍA EN EL PROYECTO

Una vez entendida una parte teórica inicial involucrada en este proyecto, ahora se concretará y hablará más en específico a las partes involucradas en el proyecto en cuestión, el que se ha utilizado, y el motivo.

5.2.1 FORMATO NON-HT

Para empezar, se eligió utilizar el formato Non-HT como formato de las señales a detectar, ya que la demodulación y la decodificación de estas señales son menos complejas en comparación con los formatos HT y VHT, que incluyen técnicas como el MIMO, la modulación de orden superior y el canal de ancho de banda más amplio. También uno de los

motivos por el cual se eligió este tipo de señales es por el preámbulo PLCP. Como se puede apreciar en la figura 5.6, los tres formatos tienen en común una parte inicial, que coincide con este preámbulo. Como el objetivo de este proyecto se centra en la detección de señales, al tener los tres el mismo preámbulo, con conseguir detectar el preámbulo, sería suficiente para poder detectar una señal con cualquiera de estos formatos. [29]

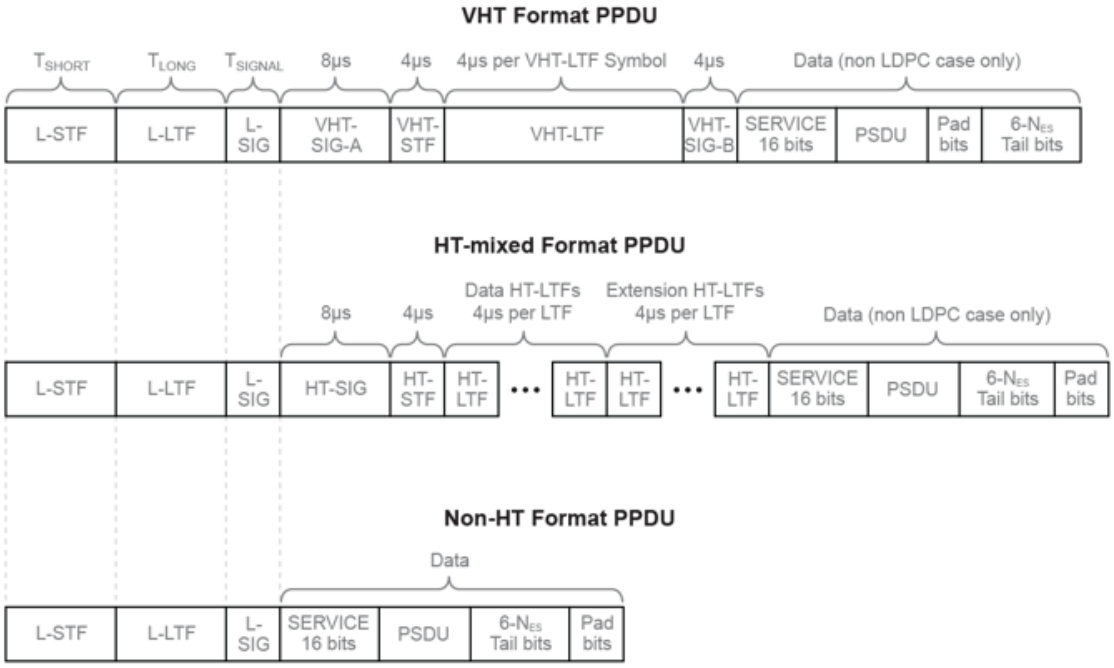

Figura 5-6: Estructura de formatos de PPDU [26]

5.2.2 PREÁMBULO PLCP

Como ya se comentó en apartados anteriores, el preámbulo PLCP, o preámbulo de legado, desempeña un papel crucial en la preparación del receptor para la correcta recepción y decodificación de este tipo de señales. Especialmente en las tramas Non-HT, que son compatibles con las versiones más antiguas del estándar. El preámbulo PLCP está diseñado para asegurar una detección y sincronización eficiente de las señales OFDM. Como se puede apreciar en la figura 5.7, el preámbulo PLCP en las tramas Non-HT generalmente consta de

tres componentes principales: los Campos de Entrenamiento Corto (Short Training Fields, STF), los Campos de Entrenamiento Largo (Long Training Fields, LTF) y el Campo de Señal (SIGNAL). Cada uno de estos componentes cumple una función específica para garantizar que el receptor esté adecuadamente preparado para recibir y procesar la señal OFDM. [26]

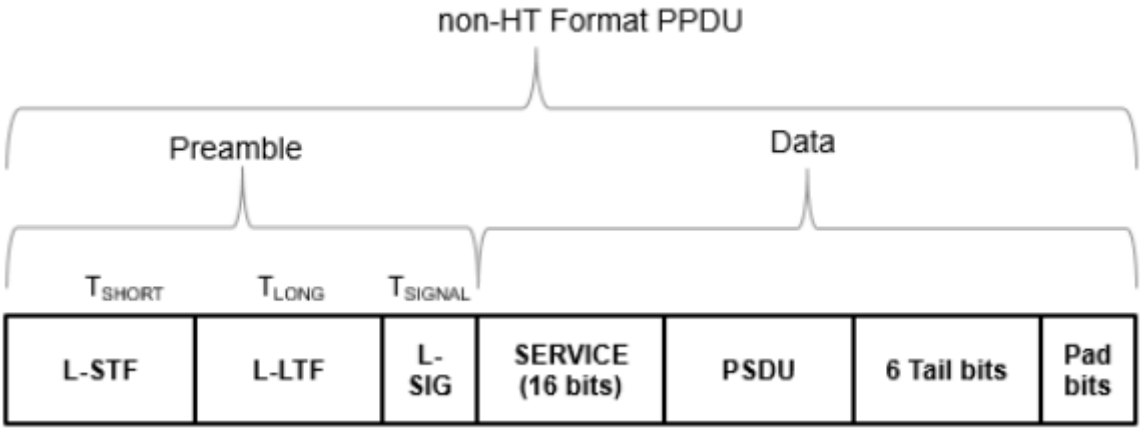

Figura 5-7: Non-HT PPDU Structure [26]

5.2.2.1 Campos de Entrenamiento Corto (STF)

Los Campos de Entrenamiento Corto (STF) consisten en 12 símbolos OFDM cortos, los cuales se pueden apreciar al mirar el espectro del preámbulo STF en la figura 5.8. Estos símbolos permiten que el receptor detecte la presencia de una señal y realice ajustes iniciales en la frecuencia del oscilador local, ayudando a corregir cualquier desajuste de frecuencia entre el transmisor y el receptor. Los receptores utilizan esta secuencia para la detección del inicio del paquete, la corrección gruesa de frecuencia (CFO, de lo cual se hablará de ello más adelante) y el ajuste del Control Automático de Ganancia (AGC). La duración del STF varía según el ancho de banda del canal, ya que la secuencia tiene propiedades de correlación adecuadas. Como las señales con las que vamos a trabajar son señales de 5MHz, correspondería una duración de 32 μs, como podemos apreciar en la tabla 5.1[27]

Channel Bandwidth (MHz)	**Subcarrier Frequency Spacing, Δ_F (kHz)**	**Fast Fourier Transform (FFT) Period (T_{FFT} = 1 / Δ_F)**	**L-STF Duration (T_{SHORT} = 10 × T_{FFT} / 4)**
20, 40, 80, 160, and 320	312.5	3.2 µs	8 µs
10	156.25	6.4 µs	16 µs
5	78.125	12.8 µs	32 µs

Tabla 5-1: duración del L-STF dependiendo de la frecuencia [26]

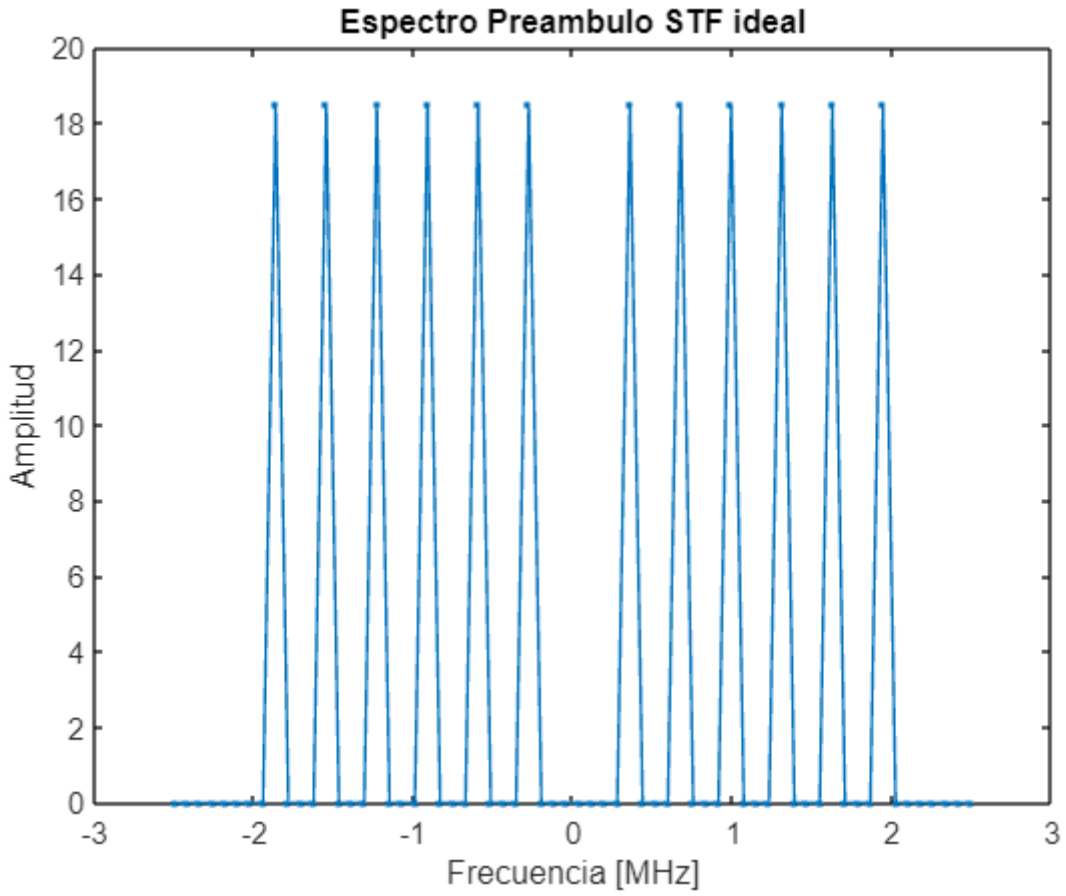

Figura 5-8: Espectro de preámbulo STF [Propio]

5.2.2.2 Campos de Entrenamiento Largo (LTF)

Los Campos de Entrenamiento Largo (LTF) consisten en dos símbolos OFDM largos que se utilizan para la estimación del canal y los cuales se pueden apreciar al mirar el espectro del preámbulo LTF en la figura 5.9. Estos símbolos permiten que el receptor mida las características del canal de comunicación, como la atenuación y la dispersión del multipath, ajustando sus parámetros para optimizar la recepción de la señal. De igual manera que el preámbulo STF, La duración del preámbulo LTF varía según el ancho de banda del canal. Al mirar la tabla 5.2 podemos ver que para 5MHz, la duración es de 32 μs. [26]

Channel Bandwidth (MHz)	Subcarrier Frequency Spacing Δ_F (kHz)	Fast Fourier Transform (FFT) Period ($T_{FFT} = 1 / \Delta_F$)	Cyclic Prefix or Training Symbol Guard Interval (GI2) Duration ($T_{GI2} = T_{FFT} / 2$)	L-LTF Duration ($T_{LONG} = T_{GI2} + 2 \times T_{FFT}$)
20, 40, 80, 160, and 320	312.5	3.2 µs	1.6 µs	8 µs
10	156.25	6.4 µs	3.2 µs	16 µs
5	78.125	12.8 µs	6.4 µs	32 µs

Tabla 5-2: duración del L-LTF dependiendo de la frecuencia [26]

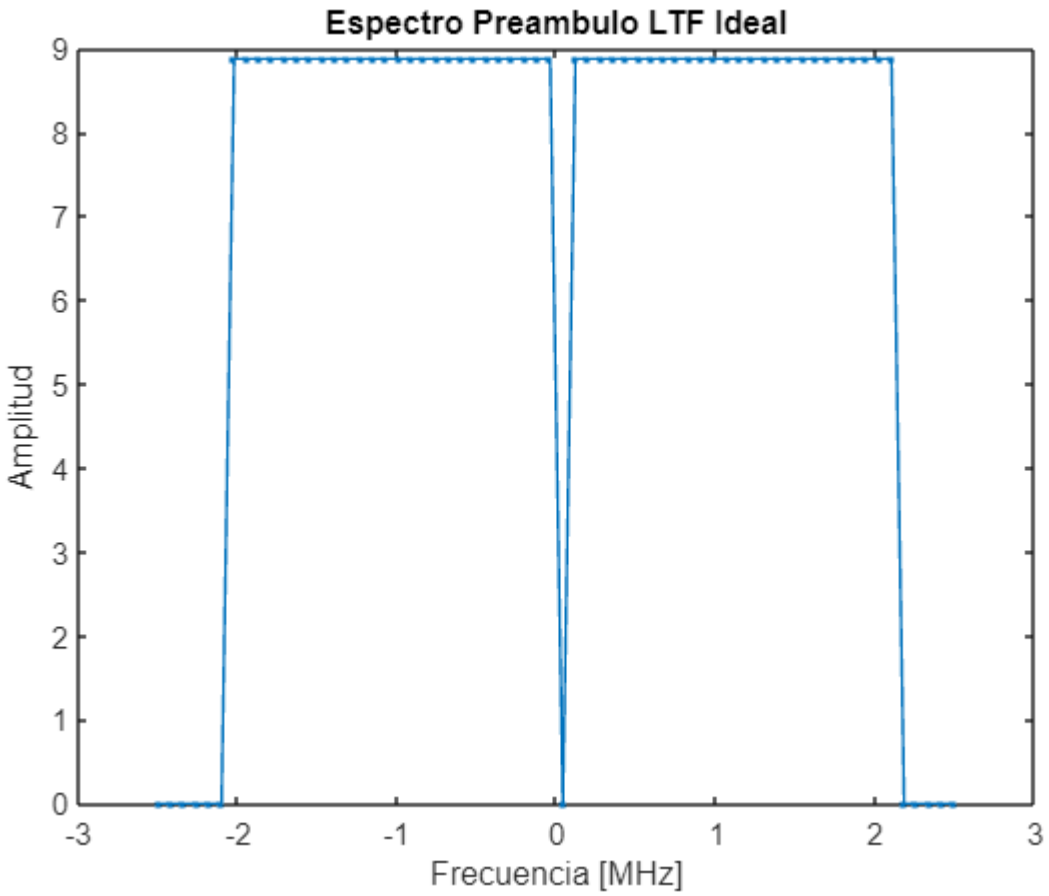

Figura 5-9: Espectro de preámbulo LTF [Propio]

5.2.2.3 Campo de Señal (SIGNAL o L-SIG)

El Campo de Señal (SIGNAL o L-SIG) es el último tramo de los preámbulos de legado PLCP, y contiene información crucial sobre la tasa de transmisión y la longitud del paquete de datos que se va a transmitir. Este campo permite que el receptor entienda cómo procesar los datos que siguen al preámbulo. En la figura 5.10 podemos ver la distribución de bits que contiene el paquete de información de L-SIG: [26]

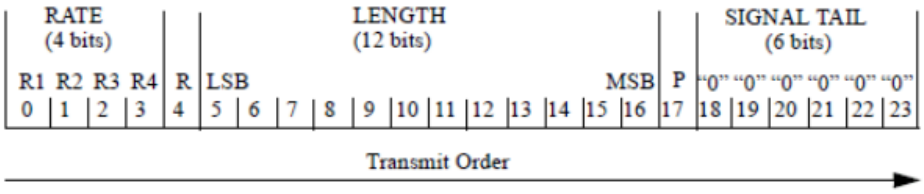

Figura 5-10: Distribución de bits del paquete de información de L-SIG [26]

- Los bits del 0 al 3 son la parte de Rate, que indica la tasa de transmisión de los datos, y para 5MHz, puede tener la tasa que indica la tabla 5.3.

Rate (Bits 0–3)	Modulation	Coding Rate (*R*)	Data Rate (Mb/s)
1101	BPSK	1/2	1.5
1111	BPSK	3/4	2.25
0101	QPSK	1/2	3
0111	QPSK	3/4	4.5
1001	16-QAM	1/2	6
1011	16-QAM	3/4	9
0001	64-QAM	2/3	12
0011	64-QAM	3/4	13.5

Tabla 5-3: tabla de velocidad de datos, tipo de modulación y ratio de codificación de la señal dependiendo de los bits de Rate [26]

- Los bits del 5 al 16 corresponden al Length, que especifica la longitud del campo de datos. Esta parte será útil para conseguir posteriormente los datos de las señales demoduladas y poder conseguir las direcciones MAC
- El bit 17 es un bit de paridad para la detección de errores;
- Por último, el Tail, bits del 18 al 23 de cola a 0 para restaurar el estado del codificador convolucional. Esta información es vital para la correcta decodificación de los datos subsiguientes.[26]

5.2.3 CAMPO DE DATOS DE NON-HT

El campo de datos en el formato Non-HT está diseñado para transmitir los datos de usuario a través de la capa física (PHY) del protocolo IEEE 802.11 y es una parte crítica de la trama utilizada para la transmisión de tramas MAC. Esta es una de las partes más importantes de la señal y del proyecto ya que el objetivo conlleva extraer esta parte de la señal recibida para

poder extraer las direcciones MAC incluidas en este campo. Este campo está estructurado para garantizar una transmisión eficiente y precisa de los datos, y está compuesto por los subcampos que se pueden ver en la figura 5.11. [25]

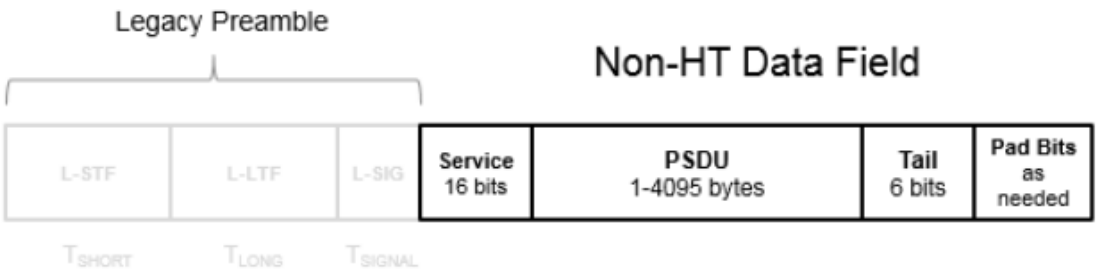

Figura 5-11:estructura campo de datos de formato non-HT [26]

- El **campo de servicio** contiene 16 bits de valor cero que se utilizan para inicializar el codificador de datos. La inicialización del codificador es esencial para asegurar que el proceso de codificación de los datos sea correcto y que los datos puedan ser recuperados de manera fiable en el receptor. Estos 16 ceros aseguran que el codificador comience en un estado conocido, minimizando la posibilidad de errores durante la transmisión y la recepción de datos.

- El PSDU es el campo de longitud variable que contiene la unidad de datos de servicio del PLCP (PSDU). Este es el campo donde esencialmente esta la carga útil de la trama y contiene los datos que se están transmitiendo desde la capa MAC y los cuales se necesitaran extraer. La longitud del PSDU puede variar según la cantidad de datos que necesiten ser transmitidos.

- Los bits de cola son necesarios para terminar el proceso de codificación convolucional utilizado en la transmisión de datos. El campo de cola utiliza seis bits de valor cero para asegurar que el codificador convolucional vuelva a un estado

conocido al final de la transmisión. Esto facilita la correcta decodificación de los datos en el receptor, permitiendo la recuperación precisa de los datos originales.

- Por último, los bits de relleno son un campo de longitud variable que se utiliza para asegurar que el campo de datos Non-HT contenga un número entero de símbolos OFDM. Dado que la modulación OFDM requiere que la cantidad de datos sea un múltiplo entero del tamaño de los símbolos, los bits de relleno se añaden para completar cualquier espacio adicional necesario. Estos bits no contienen información útil y se eliminan en el receptor después de que se hayan recibido los datos. [26]

Capítulo 6. DESARROLLO DEL SOFTWARE

En el capítulo 5 se describió la parte teórica que envuelve este proyecto, lo cual era estrictamente necesario, ya que entender la naturaleza de este tipo de señales para ahora poder empezar con el proyecto en sí es crucial. En este capítulo 6 entraremos en detalle en el desarrollo del software el cual tiene como objetivo final poder detectar señales del estándar "Enhance-wifi" para su posterior decodificación y por último poder extraer las direcciones MAC correspondientes al Propio dron y al mando enlazado a este.

La estructura que seguirá este capítulo será una descripción de como paso por paso se va a conseguir culminar con el objetivo del proyecto, siguiendo con la metodología explicada en el capítulo 4. Se empezará con una primera visión de señales creadas en ámbito local, las cuales se consideran ideales, para poder ver representada la teoría explicada en el capítulo 5 de manera visual. También se hace esto primero para posteriormente poder comparar con una señal real recogida de la comunicación real de un dron con su señal. Por último, una vez trabajado con las señales ideales y con la señal real, se procederá a realizar el algoritmo el cual será capaz de detectar y decodificar la señal real, para después poder extraer las direcciones MAC requeridas.

6.1 SEÑAL IDEAL

El primer objetivo de este proyecto es la detección de la señal, y como se explicó en el capítulo anterior, se utilizará el preámbulo PLCP de legado para esta tarea. El primer paso será la creación de un preámbulo ideal, que servirá como referencia para comprender las distintas partes y características de este. Este preámbulo ideal permitirá una comprensión detallada de los componentes y funciones del preámbulo PLCP, facilitando la identificación de sus elementos en señales reales.

6.1.1 L-STF

Para comenzar, empezaremos con la parte de L-STF del preámbulo, donde se han utilizado las funciones de MATLAB `wlanNonHTConfig` y `wlanLSTF` para su creación.

La función `wlanNonHTConfig` en MATLAB se utiliza para crear una configuración de objeto que especifica los parámetros de un paquete WLAN no-HT, que es fundamental para los estándares 802.11a/g/n. Este objeto configurado sirve como entrada para otras funciones de generación y análisis de señales WLAN. Los parámetros de entrada incluyen la configuración de los índices de modulación y codificación, el tamaño de la FFT, y otros atributos del paquete WLAN. En esta parte, para codificarla acorde a las especificaciones del proyecto, se pondrá que el tamaño del ancho de banda del canal sea de 5MHz. La salida de esta función es un objeto de configuración que encapsula todos estos parámetros y está listo para ser usado en la siguiente función. [28]

La función `wlanLSTF` genera la señal del campo de entrenamiento corto (L-STF) utilizando el objeto de configuración creado por `wlanNonHTConfig`. El L-STF es crucial para la sincronización de tiempo y la estimación de frecuencia en la recepción de señales Wi-Fi. Esta función toma como entrada el objeto de configuración de `wlanNonHTConfig` y produce una señal de entrenamiento corta que puede ser transmitida o utilizada en simulaciones de canal. La salida es una secuencia de muestras complejas que representan la señal L-STF, la cual puede ser procesada y analizada para comprender mejor su comportamiento en diferentes escenarios de comunicación. [29]

Al emplear estas funciones, se asegura que el preámbulo generado cumple con los estándares 802.11 y se puede utilizar para la detección precisa de señales en la comunicación de drones. Esta metodología permite un análisis detallado y una implementación robusta, sentando las bases para el desarrollo de algoritmos avanzados de detección de señales de banda estrecha.

Una vez obtenida la señal de preámbulo L-STF ideal, se obtuvo su espectro a través de la funciones `fft` y la `fftshift`. La función `fft` convierte una señal del dominio del tiempo al dominio de la frecuencia, permitiendo el análisis espectral. Mientras que `fftshift`

reorganiza los coeficientes de la transformada de Fourier para centrar la frecuencia cero, facilitando la visualización y análisis de la señal en el dominio de la frecuencia. El resultado se puede apreciar en la figura 6.1. [20]

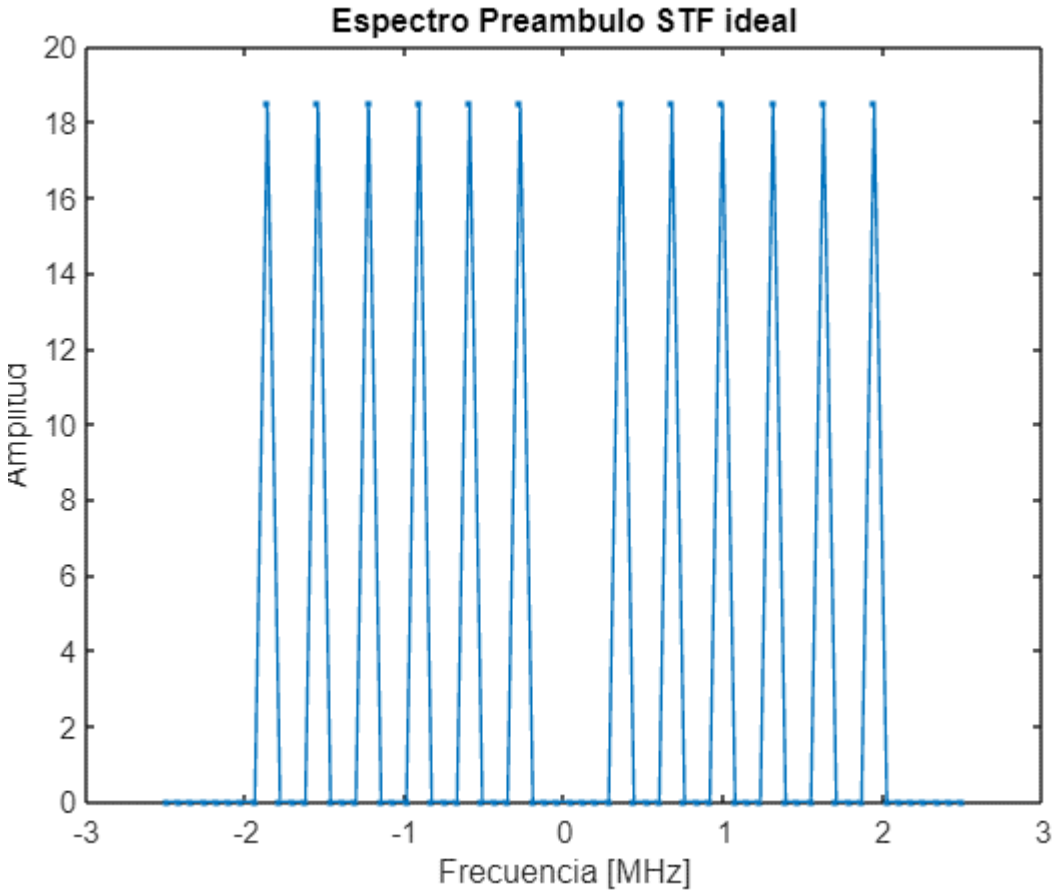

Figura 6-1: Espectro del preámbulo STF [Propio]

En el espectro, se observan picos periódicos que representan las subportadoras OFDM comentadas en el capítulo 5. Estas subportadoras están espaciadas uniformemente y son esenciales para la eficiencia espectral y la robustez contra interferencias. La utilización de las funciones `wlanNonHTConfig` y `wlanLSTF` en MATLAB ha permitido generar esta señal ideal, cuyo espectro refleja la estructura específica del STF según el estándar 802.11. Los picos en el espectro confirman la presencia de las subportadoras utilizadas para la

modulación OFDM, que son fundamentales para la comunicación eficaz y precisa en redes Wi-Fi.

También, en la figura 6.2 podemos ver un scatterplot de las portadoras del preámbulo, el cual es una representación gráfica de datos donde cada punto en el gráfico representa un par de valores de las variables en estudio. En el contexto, el scatterplot se utiliza para visualizar la constelación de la señal modulada, mostrando cómo los símbolos de datos se distribuyen en el plano complejo.

El scatterplot es útil porque permite evaluar la calidad de la señal modulada y la eficacia del algoritmo de detección. Al crear un scatterplot de la señal STF ideal, se podrá observar cómo los símbolos OFDM se distribuyen y si se alinean correctamente con los puntos esperados de la constelación. Esto es esencial para verificar que la señal generada cumple con los estándares de modulación y para identificar posibles errores o interferencias que puedan afectar la precisión de la detección de señales.

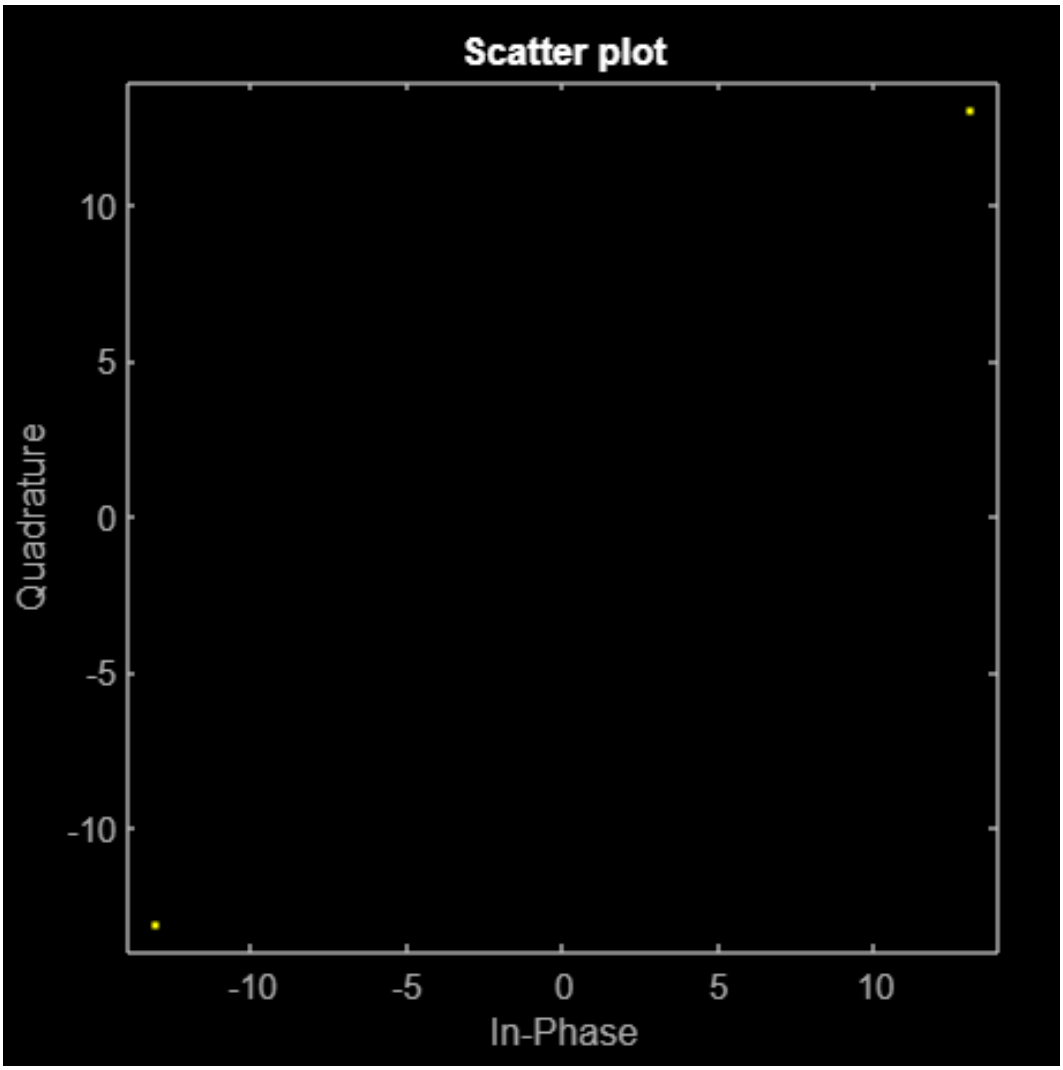

Figura 6-2: Scatterplot del las portadoras del STF [Propio]

Como se aprecia en la figura 6.2, la presencia de solo dos puntos sugiere una modulación BPSK, donde cada punto representa una de las dos posibles fases de la señal modulada. Este scatterplot indica una señal de alta calidad, ya que los puntos están claramente separados y bien definidos. En el contexto del estándar 802.11, este análisis visual permite verificar que la señal generada se ajusta correctamente a la modulación esperada, asegurando que el algoritmo de detección puede identificar y procesar las señales de manera precisa y eficiente.

Por último, se realizó un plot del ángulo de las portadoras lo cual es importante para el análisis de la fase de las subportadoras. Este tipo de análisis es crucial para detectar y corregir problemas relacionados con la fase de la señal, que pueden afectar la calidad y la precisión de la comunicación.

Este grafico se consigo con la señal transformada a frecuencia, cada valor complejo obtenido representa una subportadora de la señal. Utilizando la función `angle` en MATLAB, se calcula el ángulo de cada valor complejo, que corresponde a la fase de cada subportadora. Este ángulo, expresado en radianes, proporciona información sobre la fase de las subportadoras en la señal OFDM.

Este análisis será útil más a delante para ya que permite identificar cualquier desviación de fase que pueda ocurrir debido a problemas en el transmisor, el canal de comunicación o el receptor. Las variaciones no deseadas en la fase pueden provocar errores en la demodulación y en la detección de los datos transmitidos.

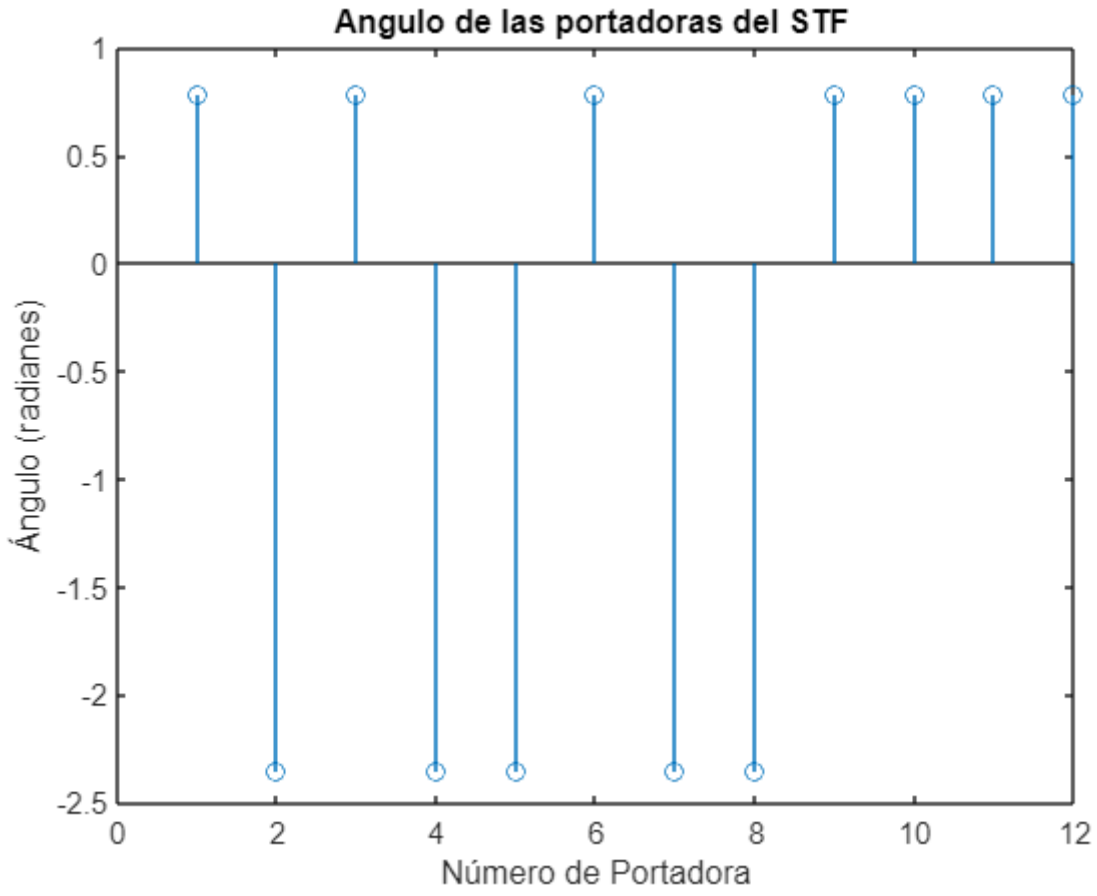

Figura 6-3: Ángulo de las portadoras del STF [Propio]

En la figura 6.3 se aprecia como cada punto representa el ángulo de una subportadora específica. Los ángulos están medidos en radianes y son cruciales para evaluar la calidad de la modulación y la sincronización de la señal. Se puede observar cómo no existe distorsión entre los ángulos y tienen las mismas amplitudes.

6.1.2 PREÁMBULO L-LTF

De igual manera que para el preámbulo L-STF, en este apartado se han utilizado las funciones de MATLAB `wlanNonHTConfig` y `wlanLLTF` para su creación de un preámbulo L-LTF ideal.

La función `wlanLLTF` de igual manera que la función `wlanLSTF`, toma como entrada un objeto de configuración creado por `wlanNonHTConfig`, que define los parámetros del paquete WLAN. La salida de `wlanLLTF` es una secuencia de muestras complejas que representan el LTF, el cual puede ser utilizado para la sincronización de tiempo y la estimación del canal en sistemas WLAN. [34]

A continuación, se va a ver alguno de los datos relevantes.

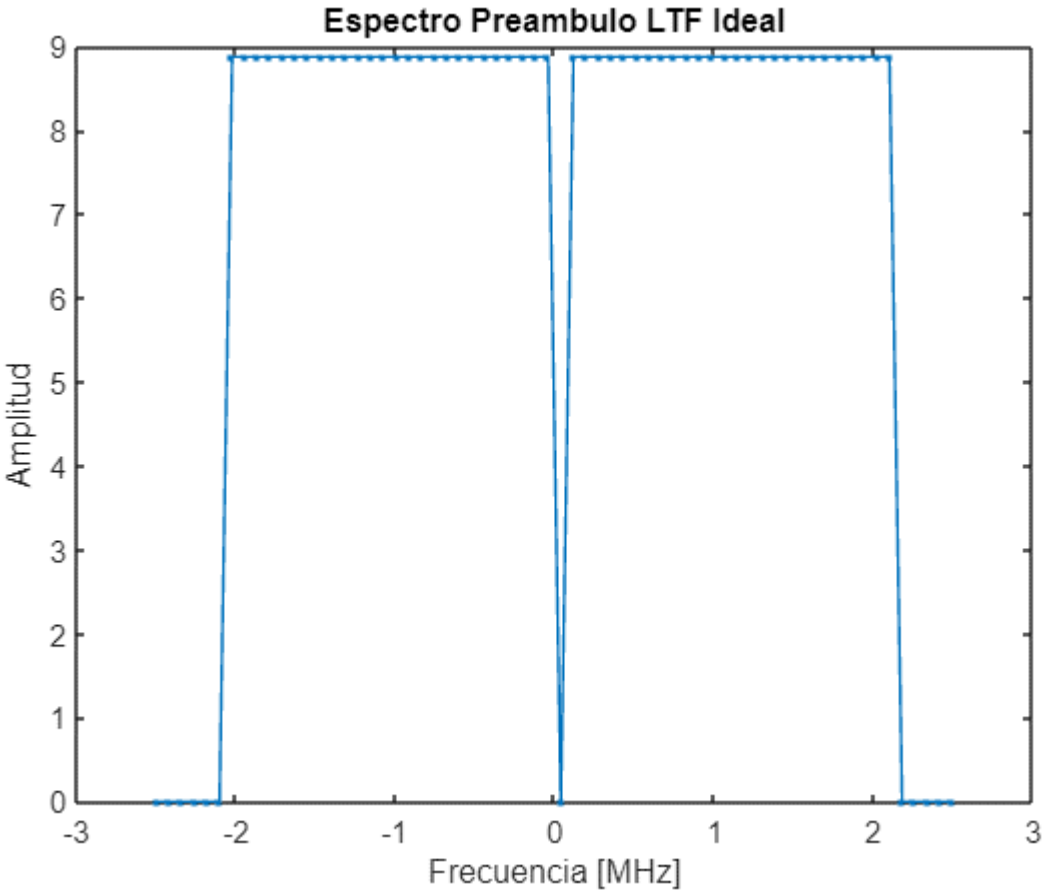

Figura 6-4: Espectro preámbulo LTF ideal [Propio]

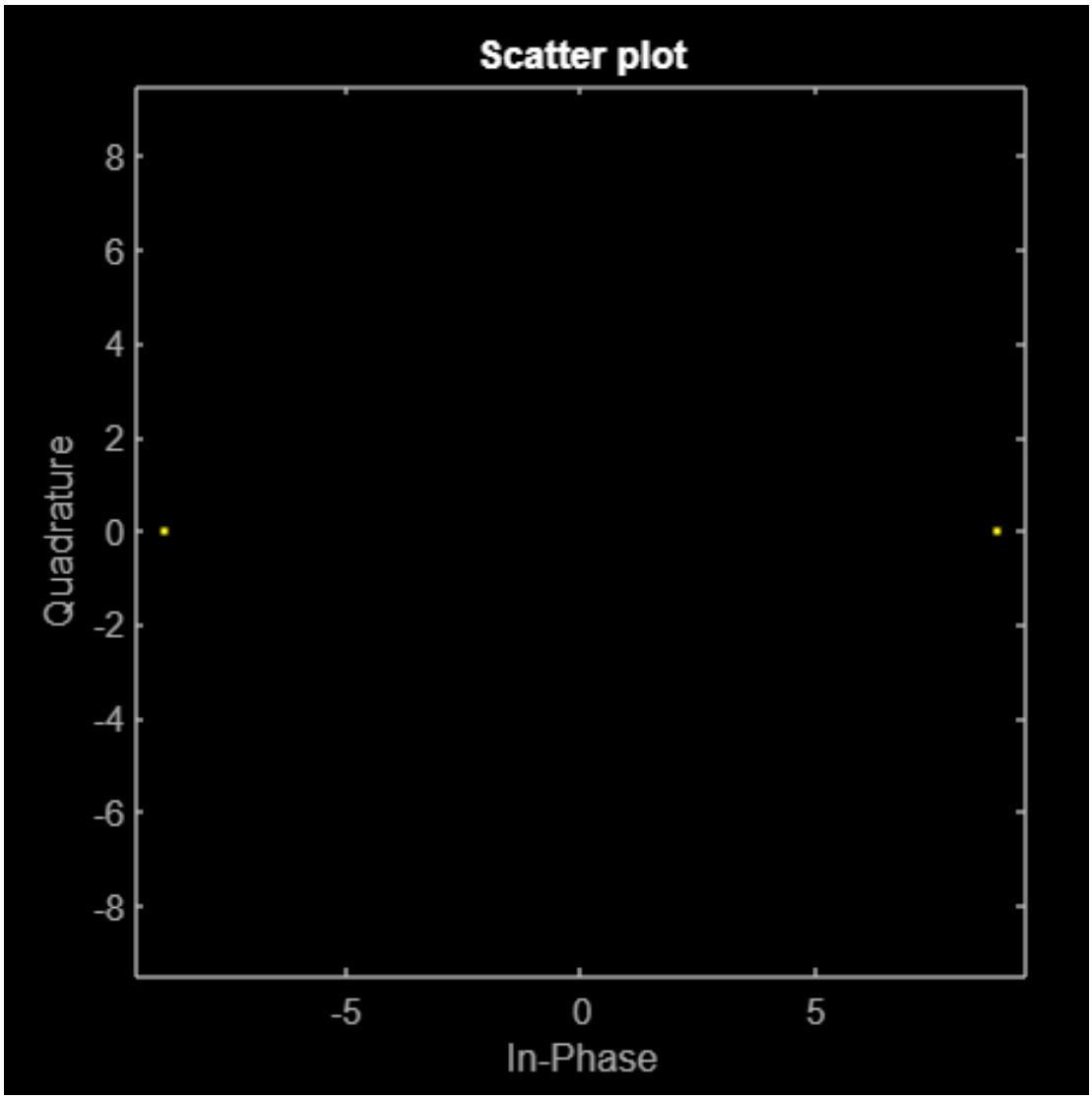

Figura 6-5: Scatterplot de las portadoras del LTF [Propio]

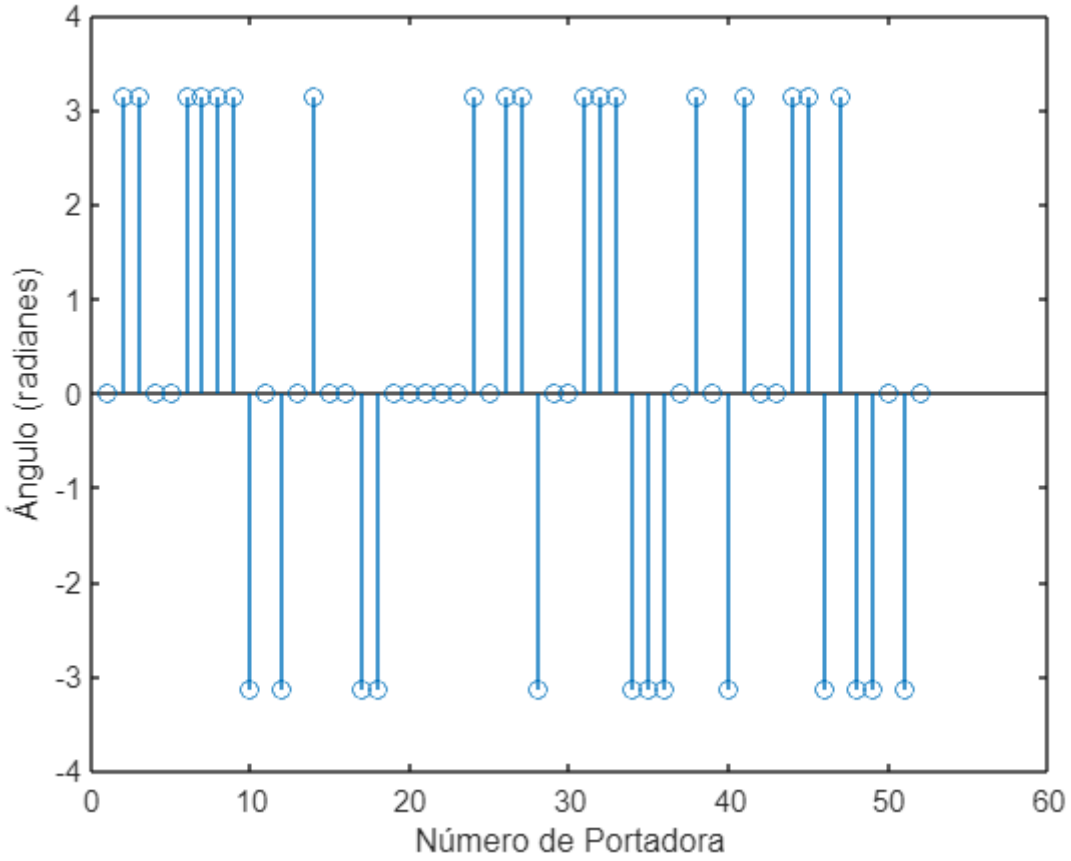

Figura 6-6: Ángulo de las portadoras del STF [Propio]

De igual manera que en el STF, en la figura 6.4 se puede ver como el espectro mostrado es característico de las señales OFDM, con una distribución uniforme de energía a través de las subportadoras activas. La forma plana y ancha del espectro indica que todas las subportadoras dentro del ancho de banda están siendo utilizadas eficientemente. La visualización del espectro del LTF ideal permite verificar que la señal generada cumple con los estándares esperados, lo cual es fundamental para asegurar que el sistema de comunicación inalámbrica funcione correctamente. También en la figura 6.5 se observan dos puntos claramente definidos, lo que sugiere una modulación BPSK. Cada punto representa una de las dos posibles fases de la señal modulada. Esta distribución indica que la señal es de alta calidad, con una modulación precisa y consistente. Y por último en la figura 6.6 le

aprecia una distribución consistente de los ángulos que indica que la señal está bien modulada y que las subportadoras mantienen su fase correcta, lo cual es esencial para la sincronización y la demodulación adecuadas en el receptor.

Por el momento simplemente se están enseñando estas funciones, tanto del L-STF como del L-LTF, porque serán de gran utilidad en el apartado 6.3 cuando las comparemos con los mismos gráficos, pero de la señal real y también se hablará de la ecualización de la señal real con los datos creados de la señal real, para poder corregir las distorsiones introducidas por el canal de transmisión. Ya que la señal real, al pasar por un sistema de comunicación inalámbrica, la señal transmitida sufre varios tipos de interferencias y atenuaciones que distorsionan su forma original. La ecualización ayuda a mitigar estos efectos al ajustar la señal recibida para que coincida lo más posible con la señal idealmente transmitida. Pero como ya se ha dicho, de esto se hablará en el apartado 6.2.

6.1.3 PREÁMBULO L-SIG

En este apartado centrado para el preámbulo L-SIG se va a plantear de la misma forma que los dos predecesores de L-STF y L-LTF por el motivo explicado en el apartado anterior, ahora, en esta parte se mostraran en las figuras 6.7, 6.8 y 6.9 tanto el espectro de la frecuencia de esta parte del preámbulo, como un scatterplot de las portadoras, y también el ángulo de las portadoras respectivamente. Esto se hace para poder entender bien su comportamiento y codificación, pero más importante, para poder ser referenciado en los siguientes apartados para poder ser comparados.

Empezamos con la función que se empleó en MATLAB para la creación de un preámbulo L-SIG ideal, el cual fue `wlanLSIG`, de igual manera que las funciones vistas anteriormente, esta función recibe una configuración creada por la función wlanNonHTConfig, y con esta información, crea una secuencia de muestras complejas que representan el L-SIG.

Con esta señal se han sacado las siguientes figuras:

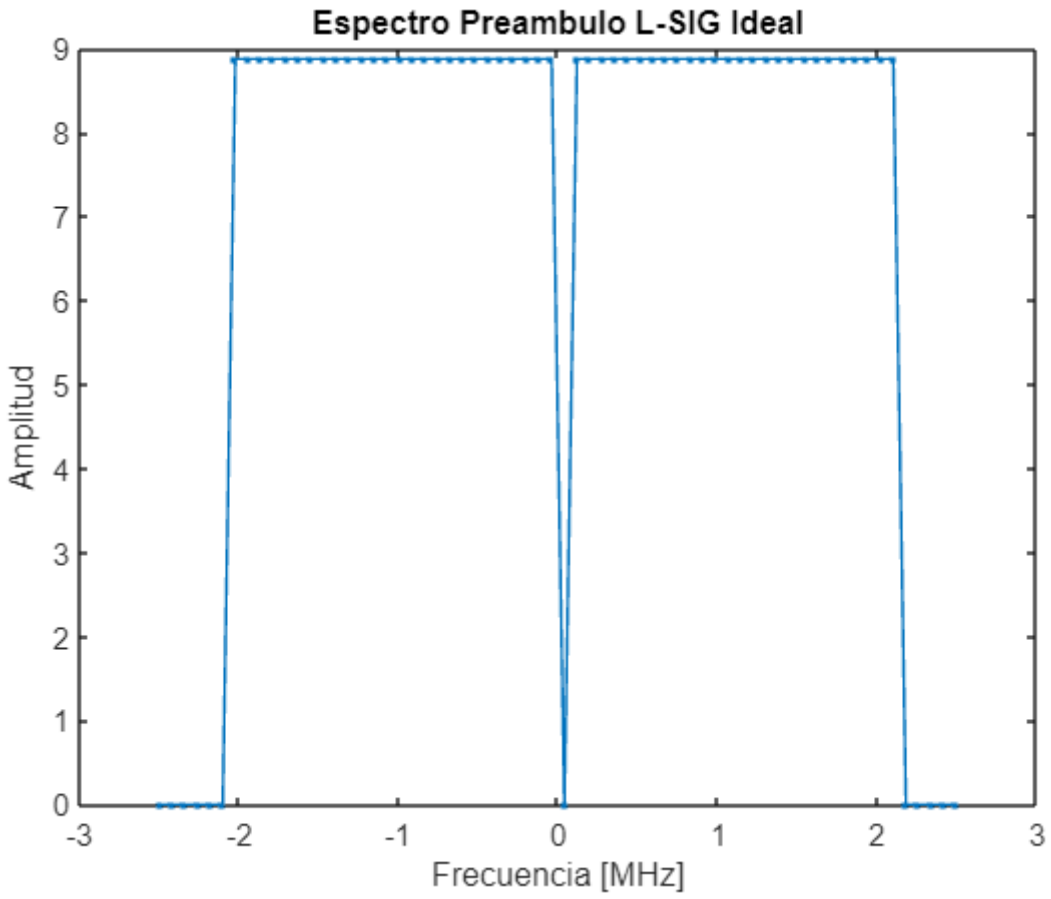

Figura 6-7: Espectro de frecuencia del preámbulo L-SIG [Propio]

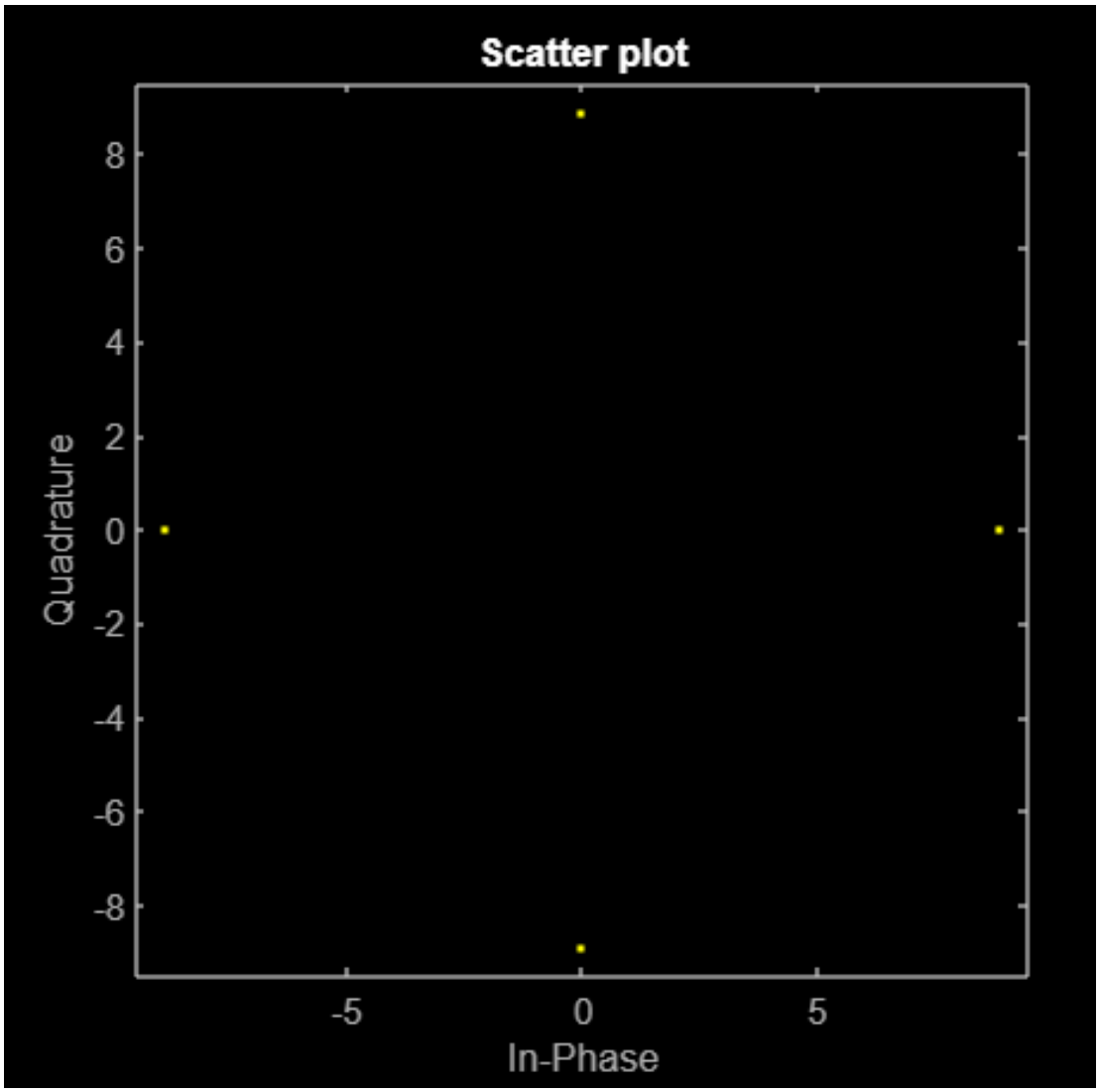

Figura 6-8: Scatterplot de las portadoras del L-SIG [Propio]

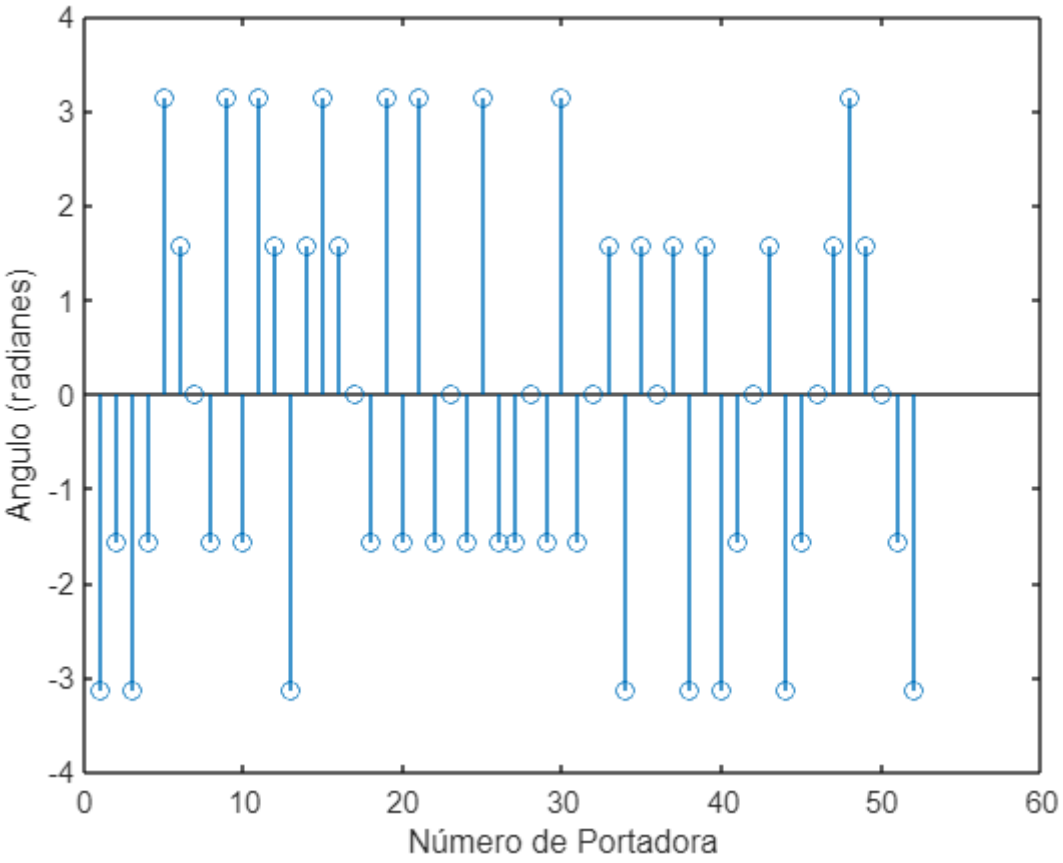

Figura 6-9: Ángulo de las portadoras de L-SIG [Propio]

Observando esta última figura, la 6.9 se puede apreciar como esta parte del preámbulo es mucho más compleja que las anteriores. Esto se debe a que la información que esta parte de la señal contiene es mucho más extensa que las anteriores, ya que esta parte del preámbulo debe contener en su interior, como ya se vio en el capítulo 5, el ratio de modulación y codificación y la longitud del aparte de datos. Al tener la necesita de transmitir más información en el mismo ancho de banda, se puede comprobar que, en este caso, el L-SIG es codificado con QPSK, figura 6.8. QPSK utiliza cuatro fases diferentes para representar los datos, lo que duplica la tasa de datos en comparación con BPSK. La parte SIG del preámbulo contiene información crucial sobre la configuración de la trama, como la tasa de datos y la longitud de la trama. La mayor eficiencia espectral de QPSK permite transmitir

esta información adicional sin aumentar el ancho de banda necesario. Al contrario que LTF y STF, los cuales tienen una codificación BPSK, la cual, es una técnica de modulación que usa dos fases para representar los datos, lo que la hace menos susceptible al ruido y a las interferencias. [29]

6.1.4 FUNCIÓN WLANLSIGRECOVER

Como ya se comentó en capítulos anteriores, la parte del preámbulo de legado L-SIG es una parte crucial de las señales OFDM, ya que estas contienen información importante respecto al ratio de modulación y codificación y la longitud del aparte de datos codificado en su interior. Esta información es muy útil para la posterior extracción de bits de la parte de datos de las señales.

Una manera que brinda MATLAB a sus usuarios para conseguir obtener los datos codificados dentro de la parte del L-SIG, es la función `wlanLSIGRecover`. Esta función se utiliza para recuperar y decodificar la información contenida en el campo L-SIG. Para utilizar `wlanLSIGRecover`, se necesita proporcionar la señal recibida en el dominio del tiempo y una configuración de canal que describa las condiciones del canal de transmisión. La función procesa esta señal y devuelve los bits decodificados del campo L-SIG, así como la métrica de la decodificación. [30]

Cuando a esta función se le dio la parte de la señal L-SIG creada en el apartado 6.1.3, esta devolvió los bits que están dentro de la trama. Los primeros 4 bits que dio se aprecian en la figura 6.10.

```
ans = 1×4 int8 row vector
     1     1     0     1
```

Figura 6-10: Bits 0-4 de la trama de L-SIG [Propio]

Rate (bits 0–3)	Modulation	Coding rate (*R*)	Data Rate (Mb/s)
			5 MHz channel bandwidth
1101	BPSK	1/2	1.5
1111	BPSK	3/4	2.25
0101	QPSK	1/2	3
0111	QPSK	3/4	4.5
1001	16-QAM	1/2	6
1011	16-QAM	3/4	9
0001	64-QAM	2/3	12
0011	64-QAM	3/4	13.5

Tabla 6-1: Tabla de velocidad de datos, tipo de modulación y ratio de codificación de la señal dependiendo de los bits de Rate [30]

Como se aprecia en la figura 6.10 y en la tabla 6.1, al tener los bits de Rate de la parte de L-SIG a 1101, esto corresponde a una modulación de la señal de BPSK, un Coding rate de 1/2 y un data rate de 1.5.

6.1.5 PRUEBA DE EXTRACCIÓN DE DATOS DE SEÑAL IDEAL

Para concluir con la parte de las señales ideales, falta por hablar de la parte de datos en sí, la parte de la cual gira entorno este proyecto. Esta parte de la señal es crucial ya que, en ella, que ya se entró en detalle de los componentes en el capítulo 5, tiene dentro la parte de PSDU, la cual contiene en su interior los bits correspondientes a las direcciones MAC del dron y de su mando asociado.

Para extraer estos datos se ha utilizado la función propia de MATLAB `wlanNonHTDataBitRecover` para recuperar los bits de la trama después de que se ha realizado la demodulación de la señal. Las entradas requeridas por la función son:

1. **rxDataSymbols**: Esta entrada es una matriz de símbolos demodulados recibidos, que representan la señal modulada en el dominio de la frecuencia. Cada columna de la matriz corresponde a un OFDM symbol.

2. **Rate**: Una cadena de caracteres que especifica la tasa de datos de transmisión utilizada para la modulación.

3. **noiseVarEst**: Una estimación de la varianza del ruido del canal. Este valor es crucial para ajustar la recuperación de datos a las condiciones reales del canal.

4. **cfg**: Un objeto de configuración creado mediante la función `wlanNonHTConfig`, hablada de ella anteriormente.

Las salidas de la función son las siguientes:

1. **rxPSDU**: La salida principal, una matriz de bits que representa la PSDU recuperada. Esta matriz contiene los datos originales que fueron transmitidos antes de ser modulados y enviados a través del canal. Este proyecto se centrará en esta salida.

2. **eqDataSymbols**: (Opcional) Los símbolos de datos ecualizados. Esta salida proporciona los símbolos después de que se ha aplicado la ecualización para compensar las distorsiones del canal.

3. **csi**: (Opcional) La información del estado del canal. Esta salida proporciona una estimación de la calidad del canal, que puede ser útil para análisis adicionales y optimizaciones.

La función `wlanNonHTDataBitRecover` toma los símbolos de datos demodulados y aplica técnicas de decodificación y corrección de errores para recuperar los bits de datos originales. Este procedimiento es fundamental para asegurar que los datos transmitidos se reciban de manera precisa y eficiente, permitiendo una comunicación inalámbrica robusta y confiable. La función es parte de la suite de herramientas WLAN de MATLAB, que facilita el desarrollo y análisis de sistemas de comunicación inalámbrica siguiendo los estándares IEEE 802.11. [31]

Una vez entendida la función, se procedió a su uso para su entendimiento. La manera empleada fue creando una señal OFDM de 5MHz con formato non-HT de manera ideal utilizando la función `wlanWaveformGenerator`, la cual se le dio la configuración de la figura 6.11 que corresponde con la explicada, con una longitud de PSDU de 1000 bytes. Además, a esta función, se le dio la trama de bits 11100010, escogida aleatoriamente. La función dio como resultado una señal OFDM en tiempo, con el formato de la figura 6.11 y con un PSDU del byte 11100010 repetido durante toda la trama.

```
cfg_nonHT_CBW5 =
  wlanNonHTConfig with properties:

         Modulation: 'OFDM'
    ChannelBandwidth: 'CBW5'
                 MCS: 0
          PSDULength: 1000
```

Figura 6-11: configuración de señal OFDM [Propio]

Una vez teniendo la señal, se recortó para tener únicamente la parte de la señal correspondiente a los datos, esto se consiguió quitándole 32 μs del preámbulo STF, 32 μs del preámbulo LTF y 16 μs del preámbulo SIG. Una vez teniendo la señal de datos, el siguiente paso será su demodulación, ya que, si no, será imposible obtener los datos. Para ello se utilizó la función `wlanNonHTOFDMDemodulate` la cual se utiliza para demodular señales OFDM no-HT. Esta toma como entrada una señal recibida en el dominio del tiempo y la convierte al dominio de la frecuencia, separando las subportadoras OFDM. La salida es una matriz de símbolos OFDM demodulados.[32]

Ahora, una vez obtenido los símbolos de la parte de datos de la señal ideal, estos fueron introducidos en la función `wlanNonHTDataBitRecover`, lo cual devolvió una PSDU vista en la figura 6.12.

```
ans = 1×8000 int8 row vector
     1   1   1   0   0   0   1   0   1   1   1   0   0   0   1   0
```

Figura 6-12: PSDU obtenido de la función wlanNonHTDataBitRecover [Propio]

Como se puede apreciar en la figura 6.12, el PSDU obtenido es una repetición del byte que se creó al inicio, lo cual es buena señal, ya que se recuperó de manera correcta. El problema que se tiene ahora es que se tiene los bits recuperados de la señal. Pero falta obtener las direcciones MAC. Por lo tanto, se creó una función propia llamada `extract_mac_from_psdu`, la cual pasando una ristra de bits de PSDU, devuelve las direcciones MAC. El PSDU sigue el formato de señales wifi del estándar 802.11, explicado en el capítulo 5. La función es la siguiente:

```
function mac_address = extract_mac_from_psdu(bits)

    % bits a bytes
    bytes = reshape(bits, 8, []).';
    bytes = bin2dec(num2str(bytes));

    % El campo Frame Control ocupa los primeros 2 bytes (16 bits)
    frame_control = bytes(1:2);

    % El campo Duration/ID ocupa los siguientes 2 bytes (16 bits)
    duration_id = bytes(3:4);

    % La primera dirección MAC (Receiver Address) ocupa los siguientes 6 bytes
    receiver_address = bytes(5:10);

    % La segunda dirección MAC (Transmitter Address) ocupa los siguientes 6 bytes
    transmitter_address = bytes(11:16);

    % La tercera dirección MAC (Address 3) ocupa los siguientes 6 bytes
    address_3 = bytes(17:22);

    % Convierte las direcciones MAC a formato hexadecimal
    receiver_mac = sprintf('%02X:', receiver_address);
```

```
    receiver_mac = receiver_mac(1:end-1);

    transmitter_mac = sprintf('%02X:', transmitter_address);
    transmitter_mac = transmitter_mac(1:end-1);

    address_3_mac = sprintf('%02X:', address_3);
    address_3_mac = address_3_mac(1:end-1);

    % Guarda las MAC addresses en una estructura
    mac_address.frame_control = frame_control;
    mac_address.duration_id = duration_id;
    mac_address.receiver = receiver_mac;
    mac_address.transmitter = transmitter_mac;
    mac_address.address3 = address_3_mac;
end
```

El resultado obtenido de extraer las direcciones MAC del PSDU es el resultado visto en la figura 6.13.

```
mac_address = struct with fields:
    frame_control: [2x1 double]
      duration_id: [2x1 double]
         receiver: 'E2:E2:E2:E2:E2:E2'
      transmitter: 'E2:E2:E2:E2:E2:E2'
         address3: 'E2:E2:E2:E2:E2:E2'
```

Figura 6-13: direcciones MAC extraídas [Propio]

Como se aprecia en la figura 6.13, se ha conseguido extraer con éxito las direcciones MAC de una señal ideal. Esto es una buena notica ya que ahora se tendrá que replicar lo mismo para señales reales y al haber conseguido extraer con éxito las MAC, todo indica que se podrá hacer lo mismo con señales reales.

6.2 SEÑAL REAL

En el apartado anterior se ha visto las partes importantes de una señal creada de forma ideal en MATLAB, entrando en detalle en el preámbulo PLCP con sus espectros y viendo los ángulos de las portadoras. Esto es de gran utilidad ya que servirá para, una vez visto para la señal real, pueda ser comparado con dichas partes de la señal ideal. En este apartado se entrará en detalle y se realizaran pasos similares a los realizados con la señal real para conseguir al final extraer las direcciones MAC de la señal.

La denominada señal real es una señal extraída de la comunicación de un dron DJI con su mando radiocontrol. Esta ha sido transformada a un fichero de MATLAB .mat, en el cual contiene la señal en tiempo y su frecuencia de muestreo. Abriendo el fichero mat y haciendo un plot de la señal en tiempo obtenemos la señal de la figura 6.14.

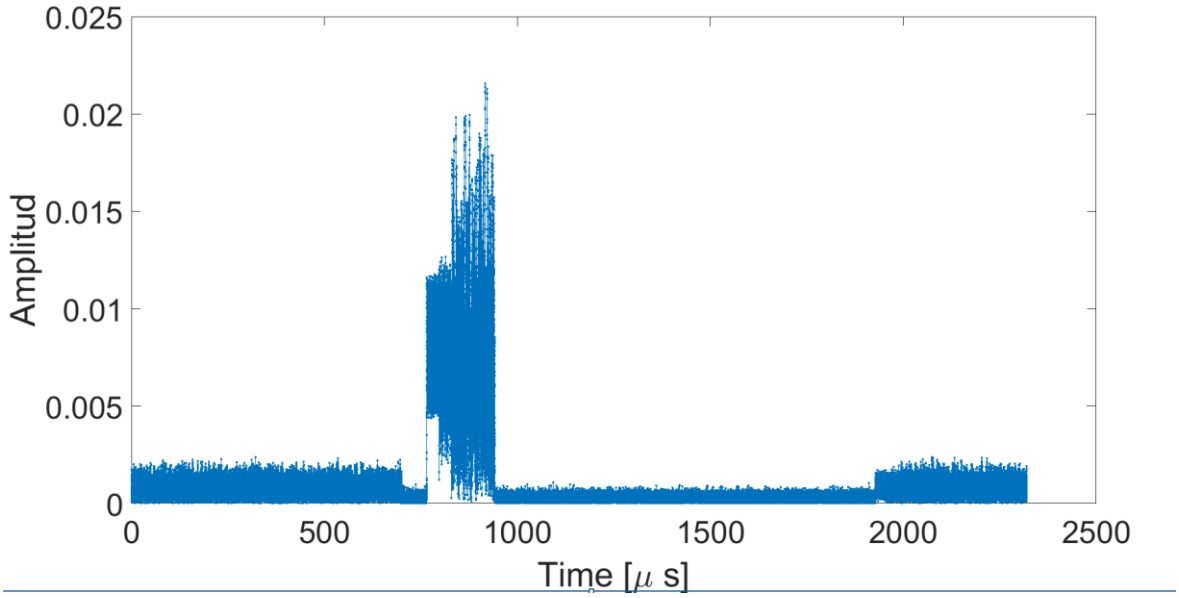

Figura 6-14: Representación en tiempo de la señal real [Propio]

En la figura 6.14 se puede apreciar como entre los puntos 700 al 1000 aproximadamente tenemos la codiciada señal, la señal en la que se envuelve este proyecto. El resto será considerado como ruido.

6.2.1 ENTENDIMIENTO Y TRABAJO PREVIO CON LA SEÑAL

Para tener un mejor entendimiento de la señal, se convierte la señal en tiempo al espectro de la frecuencia gracias a Transformada de Fourier, en cual se puede ver en la figura 6.15 .

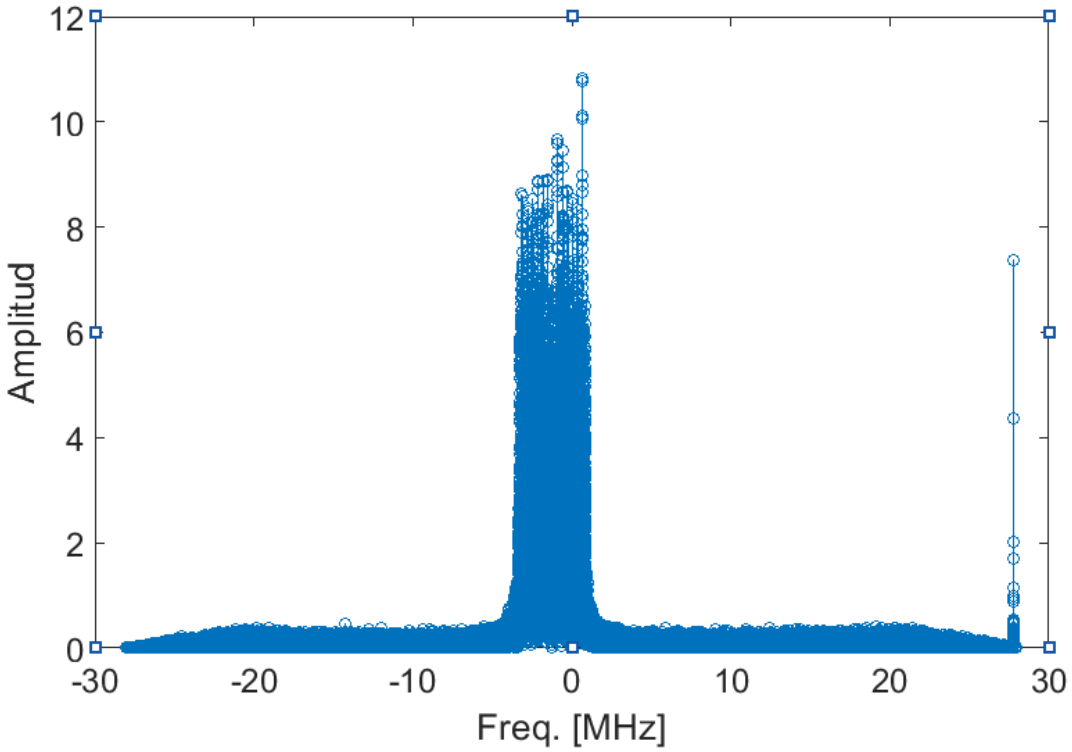

Figura 6-15: Espectro de la señal

En la figura 6.15 se puede apreciar uno de los primeros problemas que tiene la señal real frente a la ideal. El espectro de la señal no está centrado en 0 MHz, esto se puede deber a varios factores, siendo en este caso el desplazamiento de frecuencia del portador (Carrier Frequency Offset, CFO). El CFO ocurre cuando hay una diferencia entre las frecuencias del oscilador local del transmisor y del receptor. Esta diferencia puede ser causada por inexactitudes en los osciladores, movimientos relativos entre el transmisor y el receptor (efecto Doppler), o condiciones ambientales que afectan los componentes electrónicos. [33]

El CFO introduce un desplazamiento en el espectro de la señal recibida como el que se aprecia en la figura 6.15, lo que significa que las subportadoras de la señal OFDM no estarán perfectamente alineadas con las frecuencias esperadas. Esto puede causar que a la hora de detectar la señal o a la hora de extraer la PSDU, no sea posible o se extraiga de manera errónea, dando lugar a equivocaciones.

Para mitigar los efectos del CFO, se ha creado una función de MATLAB, la cual es la siguiente:

```
function senal_corregida = correccionCFO(senal,Fs_orig, boolean)

    PLOT = boolean;


    % IEEE 802.11 WI-FI Frame Format
    % 802.11 constants
    deltaF = 312.5e3;
    NFFT = 64;
    Fs_802_11 = deltaF*NFFT;
    Fs_802_11 = Fs_802_11/4;

    Ts_orig = 1/Fs_orig;
    t = 0:Ts_orig:(length(senal)-1)*Ts_orig;

    Y = fft(senal);
    f = linspace(-.5,.5,length(senal))*Fs_orig;


    if PLOT
    figure
    plot(f*1e-6,fftshift(abs(Y)),'o-')
    xlabel('Freq. [MHz]')
    title('espectro de la señal antes de la correccion CFO')
    end
```

```
    x = fftshift(abs(Y));

    THRESHOLD = max(x)*0.2

    ind = find(x >= THRESHOLD);
    ancho = f(ind);
    filter = find(ancho > -10e6 & ancho < 10e6);
    x = ancho(filter);

    x = abs(x);
    cfo = (x(1)-x(end))/2

    if cfo > 1e6
        cfo = round(cfo,-5)
    else
        cfo = 0
    end

    y = senal.*exp(1i*2*pi*cfo*t.');

    if PLOT
    figure
    Y = fft(y);
    f = linspace(-.5,.5,length(y))*Fs_orig;
    plot(f*1e-6,fftshift(abs(Y)),'o-')
    xlabel('Freq. [MHz]')
    title('espectro de la señal despues de la correccion CFO')
    end

    [P,Q] = rat(Fs_802_11/Fs_orig);

    senal_corregida = resample(double(y),P,Q);
end
```

Como se puede apreciar en la función `correccionCFO`, el primer objetivo es encontrar el centro del espectro de la señal, para saber cuánto se ha desplazado. Para conseguir esto, primero se cogen todos los valores del espectro que tengan una amplitud mayor que el 20% del máximo valor que contenga el espectro. También se le aplica un filtro paso bajo a 10MHz ya que como se aprecia en la figura 6.15, a la derecha del todo tenemos un pico de frecuencia lo cual se considera como ruido. Con esto se consigue tener el primer valor útil y el ultimo valor útil de la señal. Con estos dos valores, obtenemos el centro de la frecuencia, lo cual, en la función, está considerado como CFO y es lo que se ha desviado la frecuencia del 0.

Una vez teniendo estos valores, aplicando la formula del desplazamiento de frecuencia conseguimos recentrar la señal.

$$y(t) = x(t) * e^{j2\pi\Delta f t}$$

donde:

- y(t) es la señal corregida
- x(t) es la señal original
- Δf es el desplazamiento de frecuencia del portador (CFO)
- t es el tiempo
- j es la unidad imaginaria

Por último, al final de la función, se aprecia que se realiza un remuestreo a la señal, el objetivo de esto es para que coincida con la frecuencia de muestreo del estándar IEEE 802.11, proporcionando una señal lista para su posterior procesamiento.

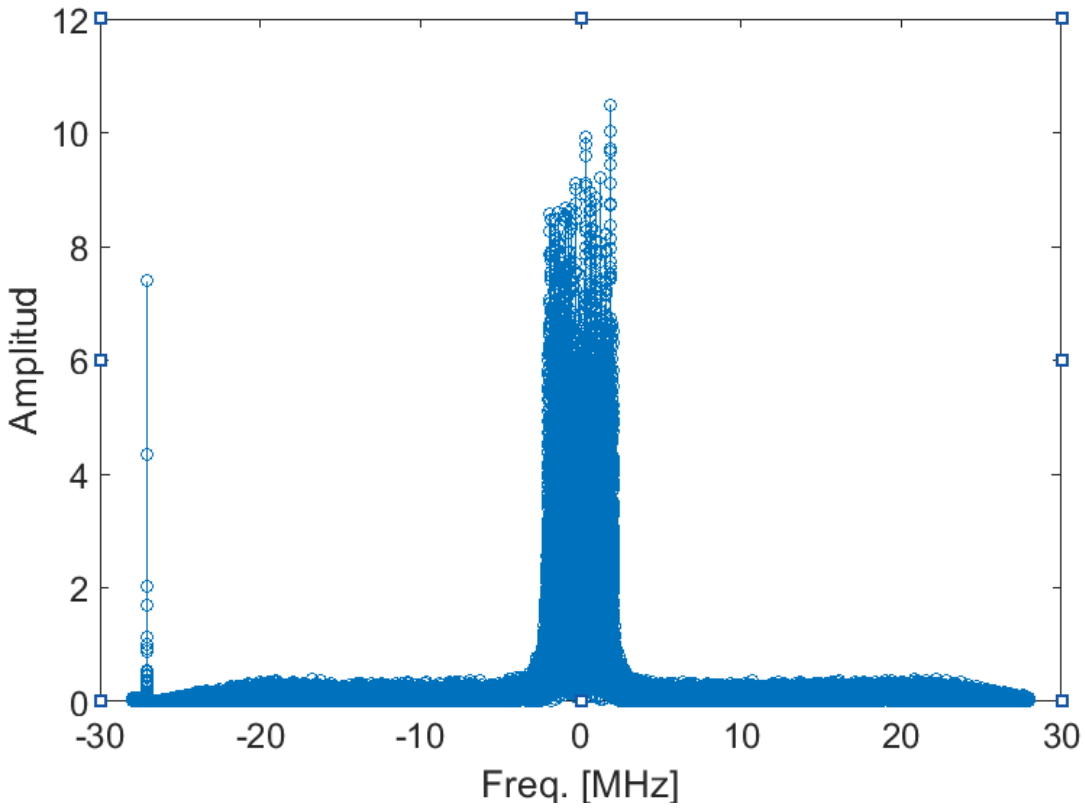

Figura 6-16: Espectro de la señal después de la corrección de CFO [Propio]

Como se aprecia en la figura 6.16, al pasar la señal por la función correccionCFO, se consigue centrar la señal en frecuencia y ya se puede seguir con el trabajo.

Una vez corregida la señal, se decidió plasmar el espectrograma de la señal, para seguir entendiendo el comportamiento y poder seguir con el proyecto. El motivo de esto es que el espectrograma de una señal muestra cómo la energía de una señal se distribuye en función del tiempo y la frecuencia. Esta herramienta es fundamental en el análisis de la señal porque proporciona una visión detallada de cómo las características frecuenciales de la señal cambian con el tiempo, lo que no es posible observar con una simple representación en el dominio del tiempo o de la frecuencia por separado.

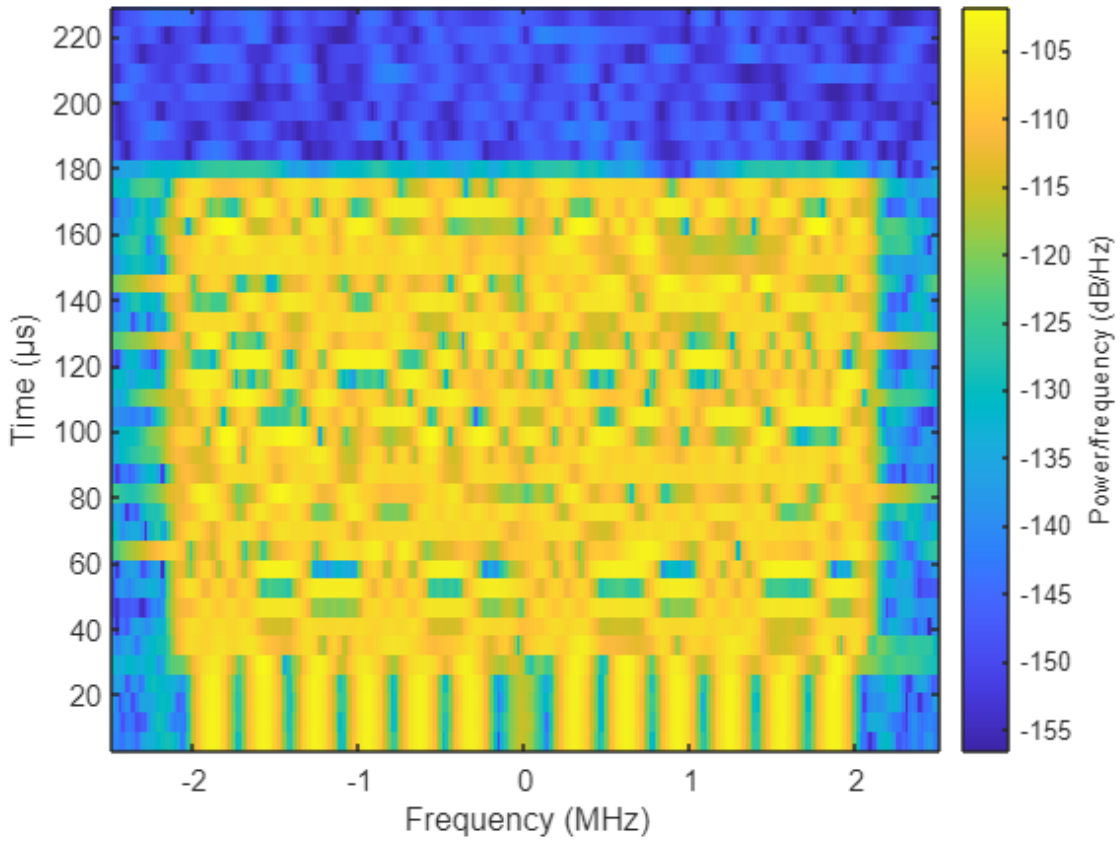

Figura 6-17: Espectrograma de la señal [Propio]

Como se aprecia en la figura 6.17, se puede ver el espectrograma de la señal, a grandes rasgos, no dice nada importante, pero la parte más interesante de este espectrograma es entre los μs 0 al 40 aproximadamente. Esa parte de la señal corresponde al preámbulo PLCP de la señal, ya que se pueden apreciar los 12 símbolos OFDM de entrenamiento. Como estos símbolos se pueden apreciar de manera tan clara, se decidió que la manera mediante la cual se detectaría la señal seria con una correlación de la señal con un preámbulo ideal, como el creado en el apartado 6.1.

6.2.2 PREÁMBULOS SEÑAL REAL

Una vez vista y corregida el CFO de la señal, para entrar más es detalle en el preámbulo de la señal, se recortó la señal a dedo para quedarnos únicamente con la parte que interesa quitando todo lo extra innecesario. Esto se ha conseguido mirando la señal en tiempo y viendo donde comienza la señal, cotar todo lo demás. Se entiende que esto se hace únicamente porque es posible ver la señal, y únicamente se hace para un mejor entendimiento de la señal. Esta no será la manera que en apartados siguiente se hará para aislar la parte que interesa para el proyecto, pero para este apartado, con este método es suficiente. En la figura 6.17 se aprecia la señal limpia

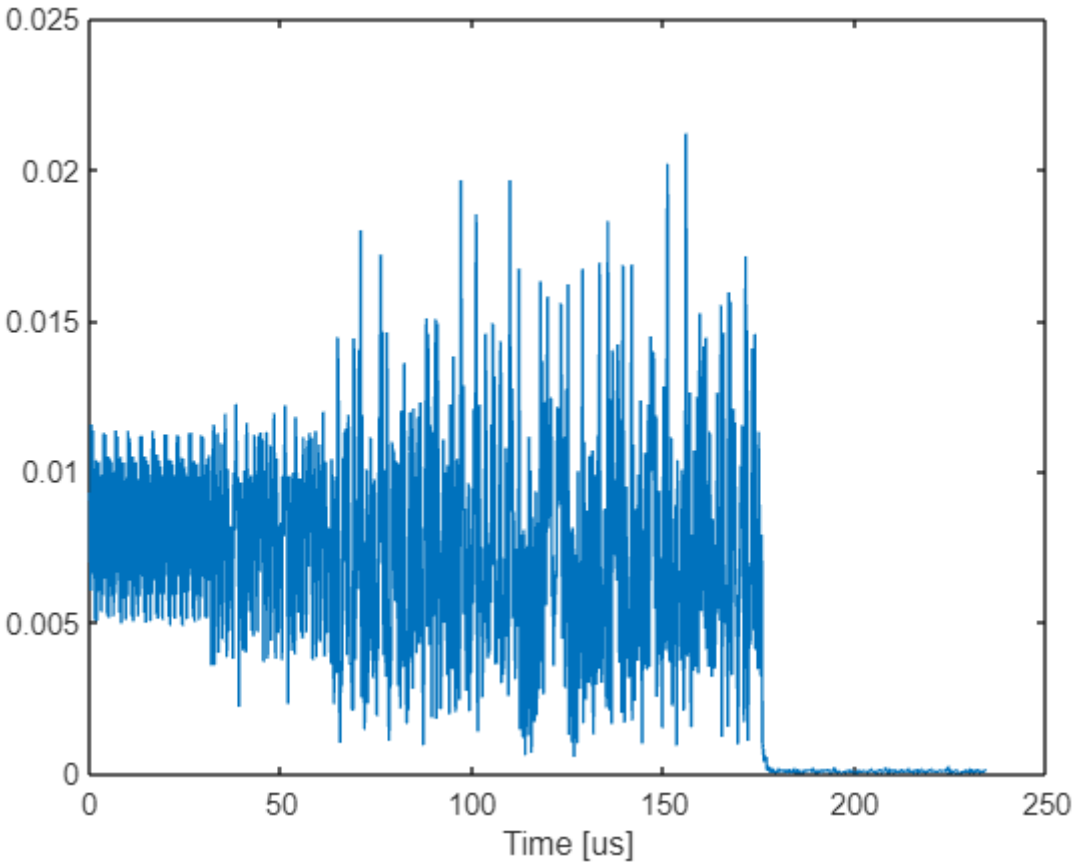

Figura 6-18: Señal real limpia [Propio]

En la figura 6.18 cabe destacar como al inicio entre el μs 0 y el 80 aproximadamente se aprecia el preámbulo PLCP con el cual se trabajará ahora.

Sabiendo que los preámbulos STF y LTF duran ambos 32 μs y el preámbulo SIG dura 16 μs, de la misma manera que para la señal ideal, se han extraído su espectro, el ángulo de las portadoras y un scatterplot de ellas para poder ser comparadas con sus respectivos ideales.

6.2.2.1 Preámbulo L-STF

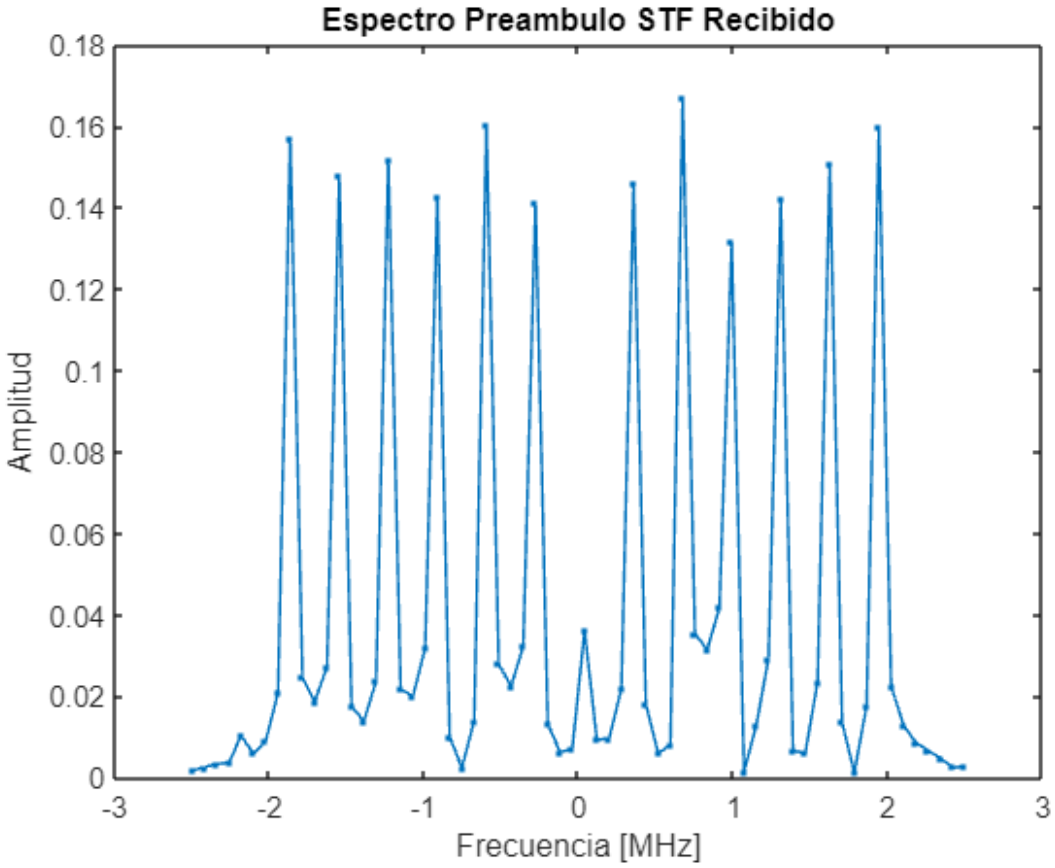

Figura 6-19: Espectro Preámbulo STF real [Propio]

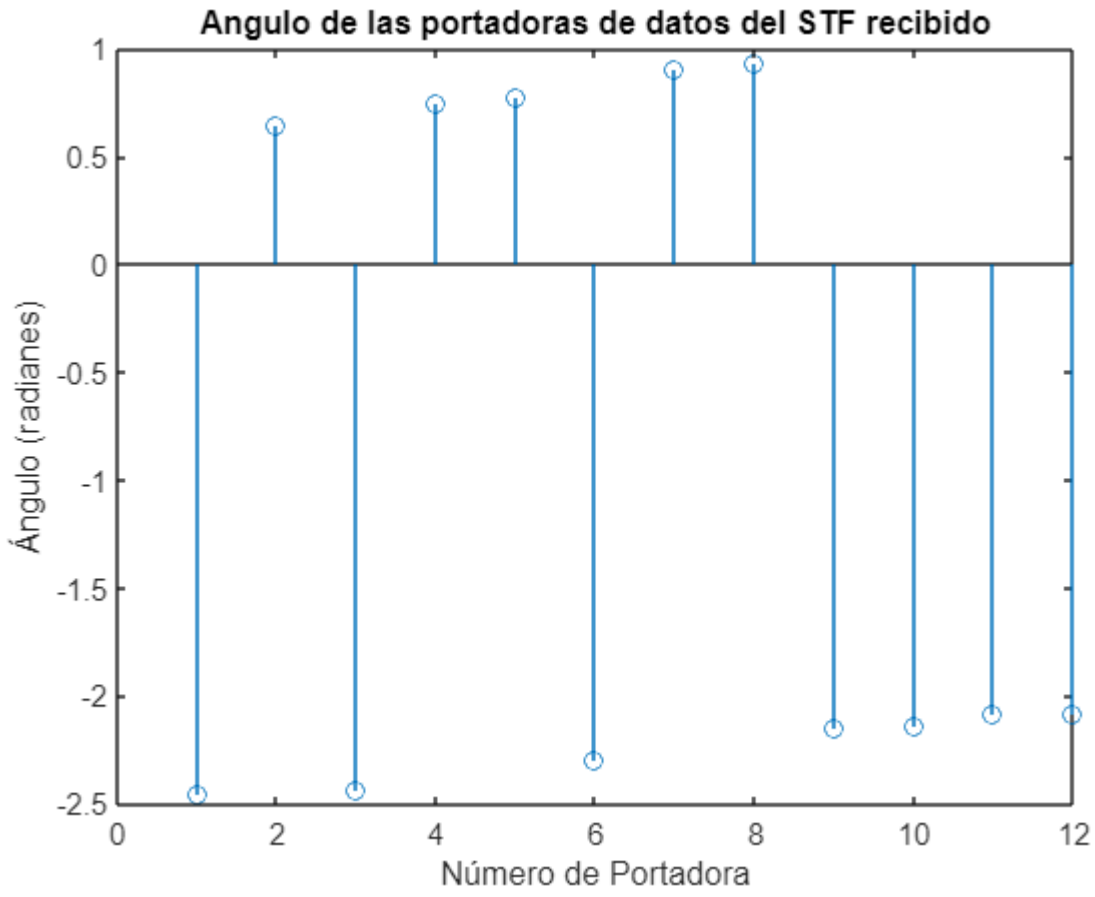

Figura 6-20: Ángulo de las portadoras de datos del STF real [Propio]

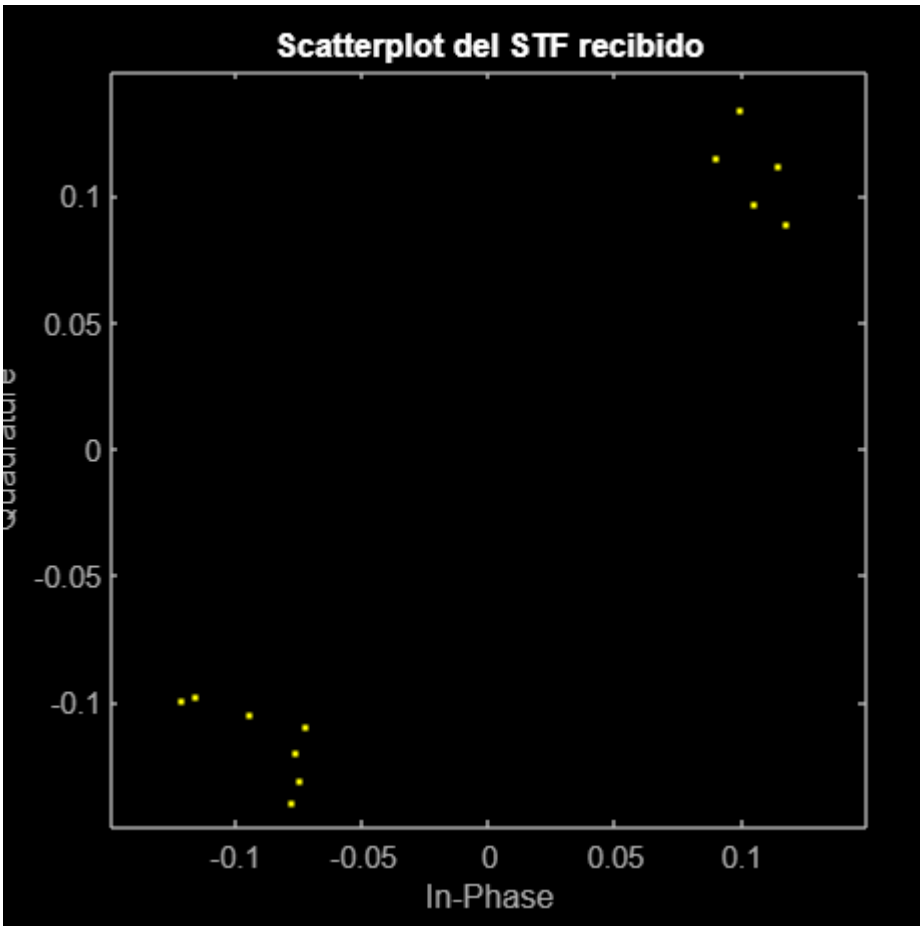

Figura 6-21: Scatterplot del STF real [Propio]

Como se puede ver en las figuras 6.19-20-21 al compararlas con las figuras 6.1-2-3 del mismo preámbulo, pero de señales ideales, se aprecia una gran similitud, esto es una señal positiva, ya que indica que, aun habiendo ruido y desplazamiento en fase, la señal no ha sufrido variaciones excesivas que puedan alterar los resultados finales o que consigan imposibilitar la detección y decodificación de la señal para extraer los datos requeridos. Gracias a su parecido, este preámbulo será utilizado para la detección de las señales. (explicado en detalle cómo se hará en el apartado 6.3)

6.2.2.2 Preámbulo LTF

De igual manera que para el L-STF, ahora se van a mostrar el espectro, el ángulo de las portadoras y un scatterplot del preámbulo L-LTF de la señal real.

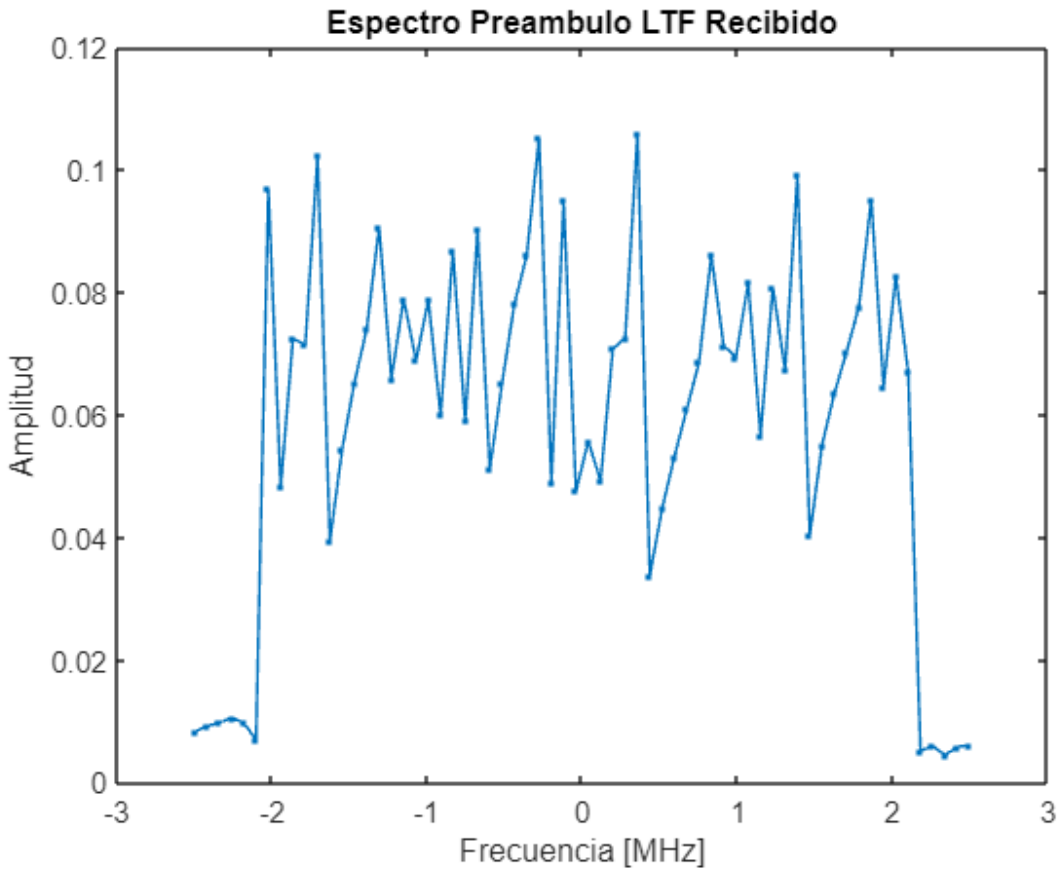

Figura 6-22: Espectro Preámbulo LTF real [Propio]

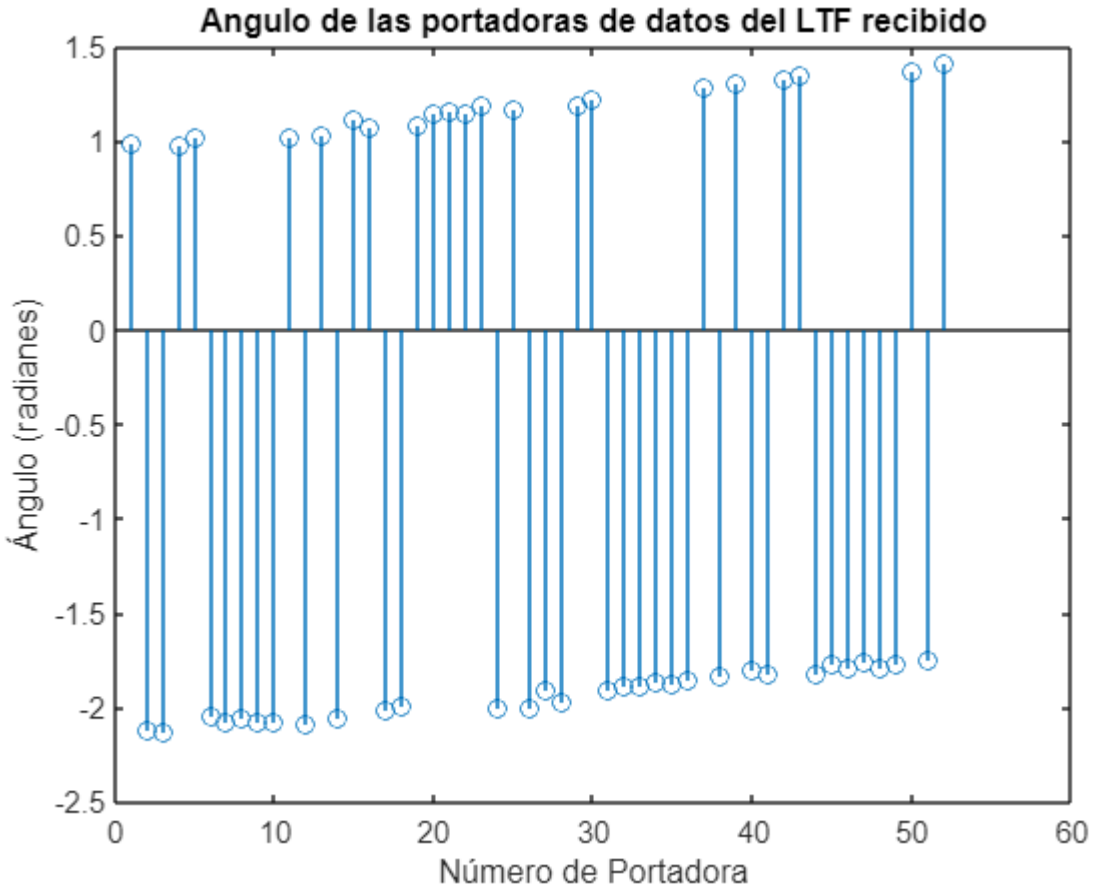

Figura 6-23: Ángulo de las portadoras de datos del LTF [Propio]

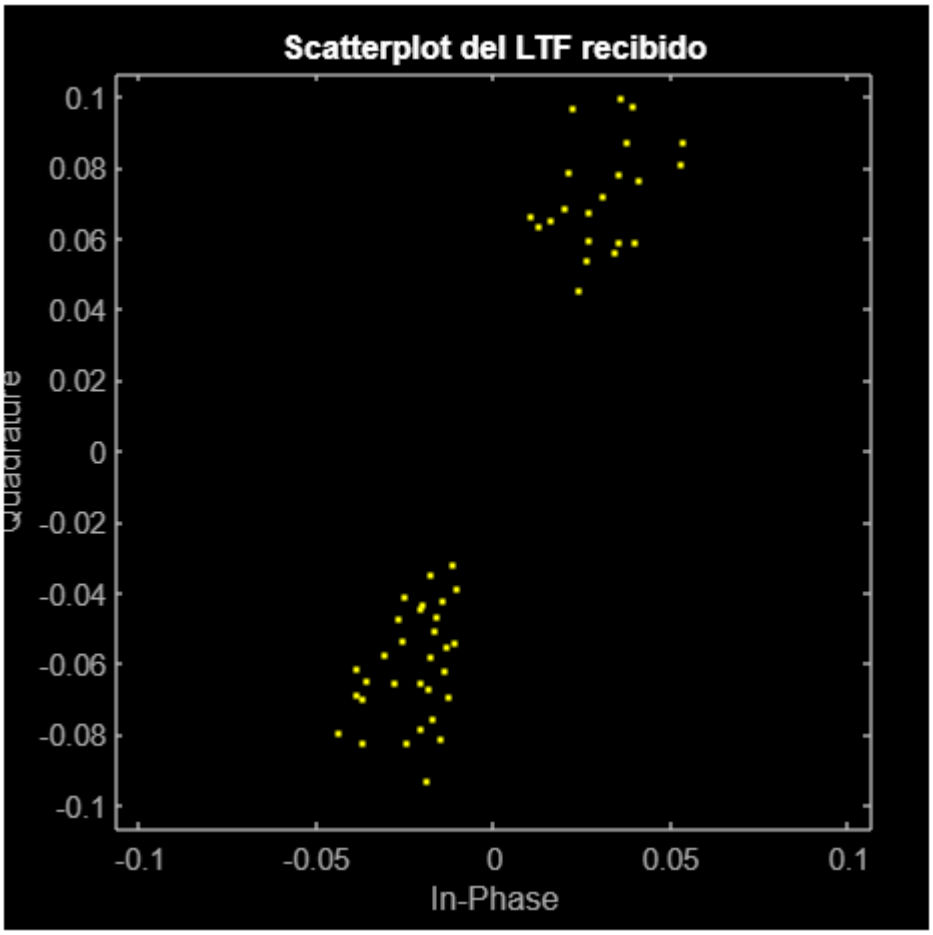

Figura 6-24: Scatterplot del LTF real [Propio]

De igual manera que en el preámbulo STF, como se puede ver en las figuras 6.22-23-24 al compararlas con las figuras 6.4-5-6 del mismo preámbulo, pero de señales ideales, se aprecia una cierta similitud, pero en este caso, al ser el preámbulo LTF más complejo que su predecesor, las distorsiones y diferencias entre ambas señales es más notable. Para mitigar este problema, se ha optado por realizar un paso extra, en este caso se realizará una ecualización del preámbulo L-LTF real con los datos obtenidos del preámbulo L-LTF ideal.

Lo que se consigue con la ecualización es ajustar la señal recibida para que se asemeje lo más posible a la señal ideal, eliminando o reduciendo las distorsiones causadas por el canal. Este proceso mejora significativamente la calidad de la señal y asegura que los datos transmitidos puedan ser correctamente demodulados y decodificados.

El proceso de ecualización comienza identificando las distorsiones en la señal recibida, como atenuación, interferencia y desvanecimiento. Estas distorsiones se comparan con la señal ideal para determinar su impacto. Luego, el ecualizador aplica filtros para corregir la amplitud y la fase de la señal, alineándola con la señal ideal, lo que permite una demodulación y decodificación más precisa y reduce la tasa de error de bits (BER). [34]

Los resultados obtenidos al ecualizar la señal son los siguientes:

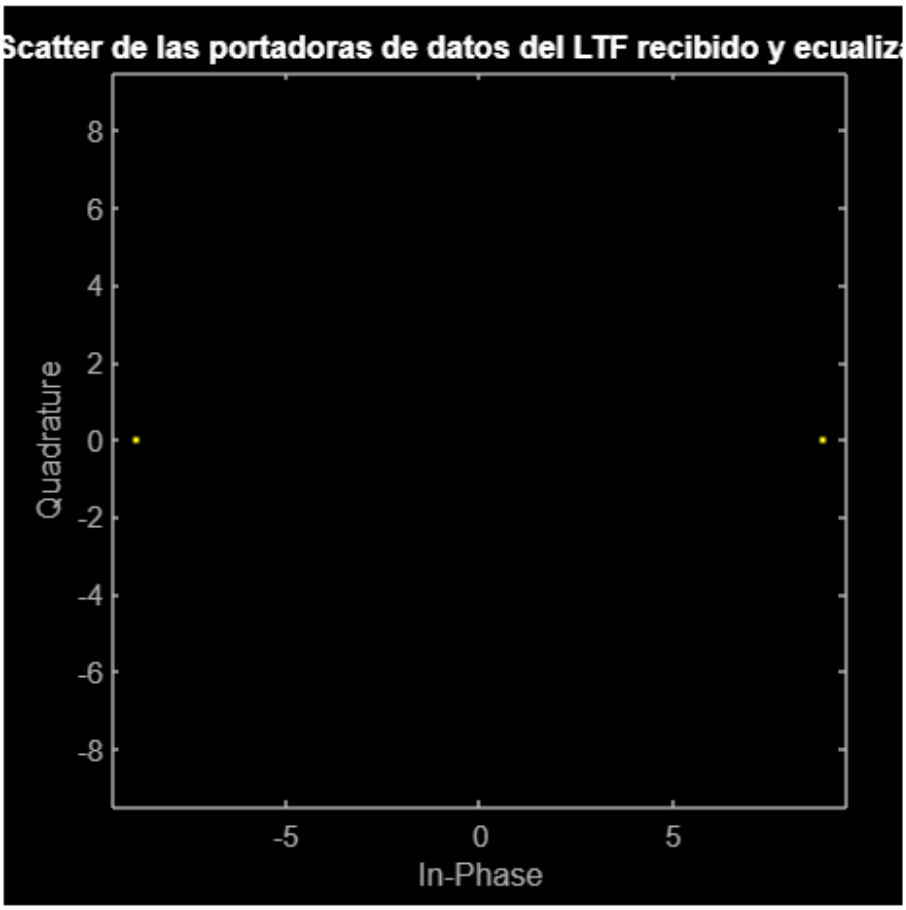

Figura 6-25: Scatterplot de las portadoras de datos del LTF recibido y ecualizado [Propio]

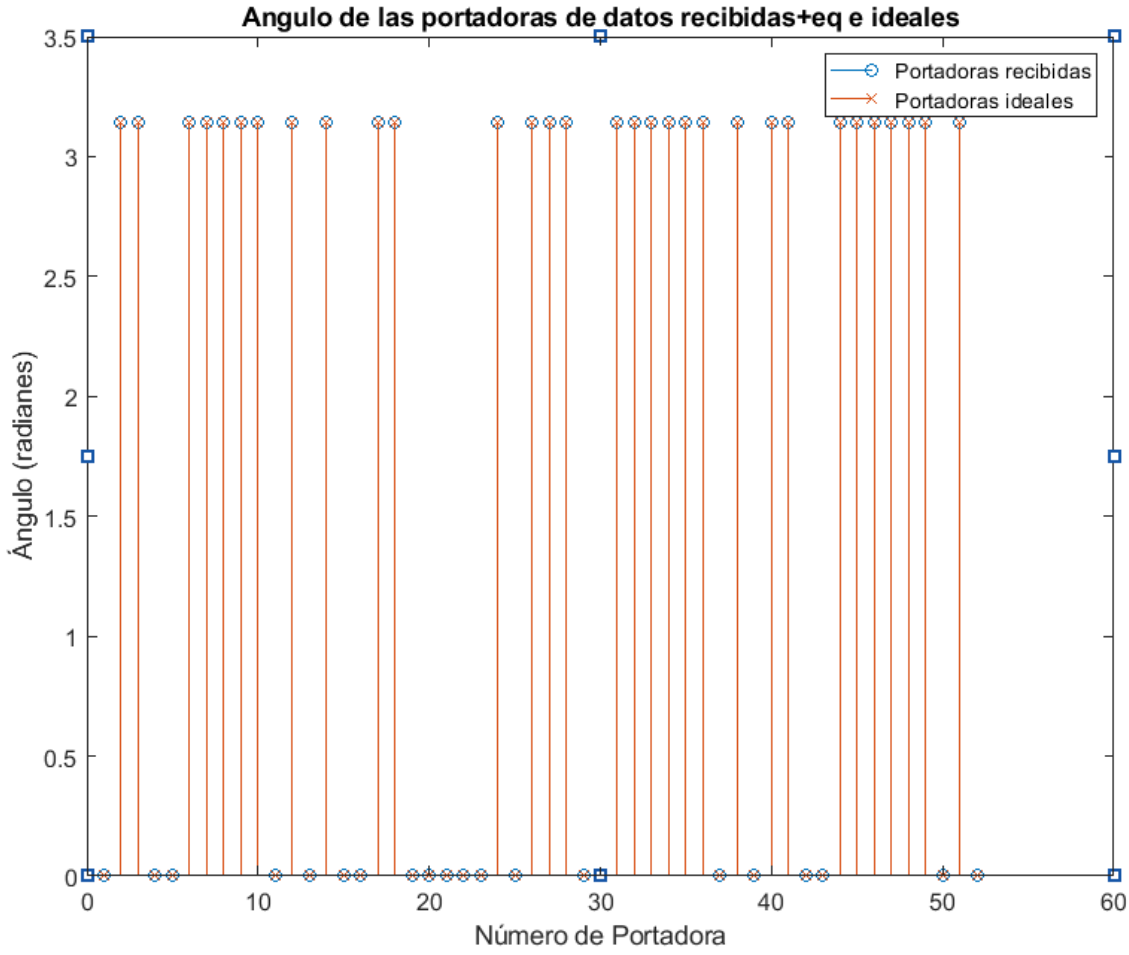

Figura 6-26: Comparación del Angulo de las portadoras de datos recibidas y ecualizadas con las ideales [Propio]

Como se puede apreciar en las figuras 6.25 y 6.26, una vez realizado la ecualización de la señal la codificación de la señal se afina de la misma manera de lo que esta la señal ideal y al mirar el ángulo de las portadoras se puede apreciar cómo se alinean todas las portadoras

teniendo el mismo ángulo. Este método es muy útil porque como se ve, se alinea más estrechamente con la señal ideal, lo que facilita una demodulación y decodificación precisas de los datos. Este proceso de ecualización será empleado más adelante para alcanzar el objetivo del proyecto.

6.2.2.3 Preámbulo L-SIG

Por último, se va a comentar un dato importante que, gracias al preámbulo SIG, se ha podido averiguar. Como se comentó en capítulos anteriores, L-SIG trae en si una serie de información en relación con la señal como es la modulación que sigue la señal o el ratio de transmisión de datos, pero ahora nos vamos a centrar en la longitud de la parte de la señal correspondiente a los datos. Esta información viene dada dentro del preámbulo L-SIG. Esta Información es de gran utilidad, ya que, gracias a ella, se puede saber que cantidad de datos esperar en la parte de PSDU de la señal.

Para extraer esta información, se ha utilizado la función de MATLAB wlanLSIGRecover de la cual ya se ha comentado anteriormente. Gracias a esta función podemos recuperar los bits que vienen dentro codificados en el preámbulo L-SIG, los cuales son los siguientes:

```
ans = 1×4 int8 row vector
     1     1     0     1
```

Figura 6-27: Bits 0-3 del L-SIG [Propio]

Como se aprecia en la figura 6.27, los 4 primeros bits, que corresponden a la parte de ratio de la señal, coinciden con los mismos 4 primeros bits de las señales ideales, esto cabe a entender que se está siguiendo un proceso correcto. Estos bits 1101 corresponden con la codificación BPSK vista en la tabla 5.3.

```
data_length = 1×12 int8 row vector
     0     1     1     1     0     0     0     0     0     0     0     0
```

Figura 6-28: Bits 5-16 del L-SIG [Propio]

En la figura 6.28 se pueden apreciar los bits correspondientes a la parte de longitud de datos, lo que se traduce a 1792 bits o 224 bytes de longitud de información dentro del PSDU. Este dato será de gran ayuda para extraer las direcciones MAC de dicho segmento.

6.3 DETECCIÓN Y EXTRACCIÓN DE DATOS

Después de haber comprendido en profundidad las señales ideales, incluyendo los preámbulos y las secciones de datos, y tras analizar detalladamente los problemas y técnicas empleadas para interpretar la señal real, se está ahora en la posición adecuada para abordar el proceso completo de detección de la señal real. En esta fase crucial, se expondrá cómo se ha logrado no solo detectar con precisión la señal real, sino también extraer exitosamente las direcciones MAC contenidas dentro del PSDU. Este logro no solo representa un avance técnico significativo, sino que también destaca el dominio de las complejidades inherentes a las comunicaciones inalámbricas. A continuación, se procederá a detallar meticulosamente este proceso.

El software comienza con la lectura de la señal de entrada la cual es la señal real. Esta señal, como ya se vio en apartados anteriores, al estar distorsionada debido a varios factores del canal de transmisión, como el desplazamiento de frecuencia del portador (CFO), interferencias y desvanecimiento, se tiene que abordar estos problemas primero. Para abordar estos problemas, se utiliza un conjunto de funciones que realizan la corrección de la señal, la detección de la trama, y la extracción de datos. La función principal de creación propia y a la cual se envuelve este proyecto es `detector_OFDM_CB5`, la cual se encarga de procesar la señal y devolver la dirección MAC extraída del PSDU.

Descripción de las Funciones

1. **Función principal** detector_OFDM_CB5:

Esta función es el núcleo del proyecto y su objetivo principal es detectar una señal OFDM, corregir cualquier desplazamiento de frecuencia, y extraer las direcciones MAC de la trama de datos. Recibe como entrada la señal a procesar (senal), la frecuencia de muestreo original (Fs_orig), y un parámetro booleano para habilitar la visualización de gráficos.

El proceso comienza ajustando la señal de entrada a la frecuencia de muestreo estándar IEEE 802.11 mediante la corrección del CFO con la función `correccionCFO` vista en apartados anteriores. Una vez corregida, la señal se somete a un proceso de correlación con un preámbulo ideal para detectar la presencia de una trama válida. Si se detecta una señal válida, se extrae y procesa el campo L-SIG para obtener la longitud del PSDU y continuar con la recuperación de los datos.

```
function mac_address = detector_OFDM_CB5(senal,Fs_orig,boolean)

    % IEEE 802.11 WI-FI Frame Format
    % 802.11 constants
    deltaF = 312.5e3;
    NFFT = 64;
    Fs_802_11 = deltaF*NFFT;
    Fs_802_11 = Fs_802_11/4;

    LTF_length_sec = 32e-6;
    STF_length_samp = LTF_length_sec*Fs_802_11;

    LTF_length_sec = 32e-6;
    LTF_length_samp = LTF_length_sec*Fs_802_11;

    SIG_length_sec = 16e-6;
    SIG_length_samp = SIG_length_sec*Fs_802_11;

    ini_L_SIG = STF_length_samp + LTF_length_samp;
    end_L_SIG = ini_L_SIG + SIG_length_samp-1;


    chanEst = ones(52,1);
    bandwidth = 'CBW5';

    snr = 30;
```

```
    noiseVarEst = 10^(-snr/10);
    field = 'NonHT-Data';

    % deteccion

    senal_corregida = correccionCFO(senal,Fs_orig, boolean);

    [output,detected]  = correlacionSTF(senal_corregida,boolean);

    correlacion_LTF_eq = correlacionLTFeq(output(STF_length_samp:ini_L_SIG));


    if detected && isequal(correlacion_LTF_eq,1)

        L_SIG = output(ini_L_SIG:end_L_SIG);


        [rxLSIGData,~] = wlanLSIGRecover(L_SIG,chanEst,0.01,bandwidth);

        rxLSIGData(1:4)'
        data_length = rxLSIGData(6:17)'


        % binario a decimal
        cadena_binaria = num2str(data_length);
        cadena_binaria(cadena_binaria==' ') = '';
        PSDULength_bits = bin2dec(cadena_binaria)
        PSDULength = PSDULength_bits/8

        % Verifica si el número de bits es múltiplo de 8 y establecemos el lenght
del PSDU
        if mod(PSDULength_bits, 8) ~= 0
            warning('El número de bits no es un múltiplo de 8.');
            PSDULength = 1000

        else
            PSDULength = PSDULength_bits/8;
        end


        X_DATA = output(end_L_SIG+1:end);

        if boolean
            figure
            plot(abs(X_DATA))
        end

        cfg_nonHT_CBW5 = wlanNonHTConfig
('ChannelBandwidth',bandwidth,'PSDULength',PSDULength);


        sym = wlanNonHTOFDMDemodulate(X_DATA,field,bandwidth);
        info = wlanNonHTOFDMInfo(field,bandwidth);
```

```
        sym = sym(info.DataIndices,:,:);

        psdu = wlanNonHTDataBitRecover(sym,noiseVarEst,cfg_nonHT_CBW5)'



        mac_address = extract_mac_from_psdu(psdu);


    else
        mac_address = 'no detectada';
    end


end
```

2. **Función** `correlacionSTF`:

Esta función de creación propia realiza la correlación de la señal recibida con un preámbulo ideal STF. La correlación es una técnica utilizada para detectar patrones específicos en la señal, en este caso, el preámbulo STF. La función evalúa la fuerza de la correlación y determina si la señal recibida contiene una trama válida basada en un umbral predefinido.

```
function [output,detected]  = correlacionSTF(senal,boolean)


    THRESHOLD = 0.8;


    % 802.11 constants
    deltaF = 312.5e3;
    NFFT = 64;
    Fs_802_11 = deltaF*NFFT;

    % 802.11 constants - redefino para quarter-channel
    Fs_802_11 = Fs_802_11/4;

    LTF_length_sec = 32e-6;
    STF_length_samp = LTF_length_sec*Fs_802_11;

    % Creo un preambulo ideal
    cfg_nonHT_CBW5 = wlanNonHTConfig ('ChannelBandwidth','CBW5');
    ideal_preamble_STF = wlanLSTF(cfg_nonHT_CBW5);

    % Correlo con la senyal recibida
```

```
    corr_res = nan(length(senal)-STF_length_samp-1,1); % Pre-allocation
    for iter = 1:length(senal)-STF_length_samp-1
        corr_res(iter) = corr(senal(iter:iter+STF_length_samp-1),
ideal_preamble_STF);
    end


    [max_corr, index] = max(corr_res);


    disp("la correlacion maxima con el preambulo L-STF es de : " + abs(max_corr))

    if boolean
        figure
        plot(-16/2: length(corr_res)-16/2-1, abs(corr_res),'.-')
        hold on
        yyaxis right
        plot(abs(senal),'.-')
        xlabel('Samples')
        legend('correlation output','received signal')
    end

    if abs(max_corr) > THRESHOLD
        disp("señal detectada")
        output = senal(index+1:end);
        detected = true;
    else
        disp("señal NO detectada")
        output = senal;
        detected = false;
    end

end
```

Si la correlación es alta, se asume que la señal contiene una trama válida y se extrae la porción relevante de la señal para su posterior procesamiento. La función también puede visualizar la salida de la correlación y la señal recibida para facilitar la evaluación manual.

3. **Función** `correlacionLTFeq`:

Esta función de creación propia verifica la correlación del LTF después de la ecualización hablada en apartados anteriores. La función calcula la transformada de Fourier del LTF recibido y lo compara con un LTF ideal. La correlación resultante indica la calidad de la señal y la precisión de la estimación del canal.

```
function correlacion = correlacionLTFeq(x_LTF)

NFFT = 64;
cfg_nonHT_CBW5 = wlanNonHTConfig ('ChannelBandwidth','CBW5');
ideal_preamble_LTF = wlanLLTF(cfg_nonHT_CBW5);
Y_ideal_LTF = fftshift(fft(ideal_preamble_LTF(1:NFFT)));
ind_LTF = find(abs(Y_ideal_LTF)> 1);
Y_ideal_LTF_carriers = Y_ideal_LTF(ind_LTF);


X_LTF = fftshift(fft(x_LTF(1:NFFT)));
X_LTF_carriers = X_LTF(ind_LTF);

H_hat = X_LTF_carriers./Y_ideal_LTF_carriers;

X_LTF_carriers_eq = X_LTF_carriers./H_hat;

correlacion = round(abs(corr(X_LTF_carriers_eq,Y_ideal_LTF_carriers)));

end
```

4. **Functions** `extract_mac_from_psdu`:

Esta función de creación propia extrae las direcciones MAC del PSDU, que es la unidad de datos contenida en la trama Wi-Fi. La función toma los bits del PSDU, los convierte en bytes, y luego extrae las direcciones MAC (receptor, transmisor y una tercera dirección) en formato hexadecimal. Estas direcciones son cruciales para la identificación y autenticación de dispositivos en la red.

6.3.1 ORQUESTACIÓN DE DETECTOR_OFDM_CB5

La función `detector_OFDM_CB5` es la pieza central del software desarrollado para la detección de señales OFDM y la extracción de direcciones MAC. Esta función combina varias técnicas de procesamiento de señales para identificar y corregir distorsiones en la señal recibida, detectar tramas válidas y extraer información crítica de las mismas. A continuación, se presenta una explicación detallada de cada paso involucrado en esta función.

6.3.1.1 Entradas y Parámetros

- **senal**: La señal recibida que contiene la trama OFDM que se desea procesar.
- **Fs_orig**: La frecuencia de muestreo original de la señal recibida.
- **boolean**: Un parámetro booleano que, si es verdadero, activa la visualización de gráficos que ayudan a diagnosticar y evaluar el procesamiento de la señal.

Paso 1: Inicialización y Configuración de Parámetros

La función comienza definiendo constantes y parámetros esenciales conforme al estándar IEEE 802.11. Estas constantes incluyen:

- **deltaF** que representa la separación en frecuencia entre subportadoras.
- **NFFT** que es el número de puntos de la FFT (Fast Fourier Transform).
- **Fs_802_11** que es la frecuencia de muestreo estándar para un canal Wi-Fi, ajustada para un cuarto de canal (CBW5).

Paso 2: Corrección del Desplazamiento de Frecuencia del Portador (CFO)

Como ya se ha explicado en apartados anteriores, la señal recibida es susceptible a desviaciones de frecuencia que pueden distorsionar la señal. Para corregir estas desviaciones, se utiliza la función `correccionCFO`, que ajusta la señal en función del CFO estimado, asegurando que las subportadoras estén correctamente alineadas en el dominio de la frecuencia.

Paso 3: Detección del preámbulo mediante Correlación

Una vez corregida la señal, se procede a detectar la presencia de una trama válida mediante correlación con un preámbulo ideal. La función `correlacionSTF` se encarga de correlacionar la señal corregida con un preámbulo STF ideal. Si la correlación supera un umbral predefinido, se considera que la señal contiene una trama válida y se extrae la porción relevante de la señal.

Paso 4: Verificación de la Correlación del LTF

Para asegurar la validez de la trama detectada, se verifica la correlación del LTF con la función `correlacionLTFeq`. Esta función compara el LTF recibido con un LTF ideal ecualizado, asegurando que las condiciones del canal han sido correctamente estimadas y corregidas.

Paso 5: Recuperación del Campo L-SIG

Si las correlaciones del STF y LTF son satisfactorias, se procede a recuperar el campo L-SIG de la señal. El campo L-SIG contiene información sobre la longitud del PSDU y otros parámetros críticos. Utilizando la función `wlanLSIGRecover`, se extraen los bits de datos del L-SIG, que luego se convierten de binario a decimal para determinar la longitud del PSDU en bytes.

Paso 6: Demodulación y Recuperación de Datos

Con la longitud del PSDU conocida, se configura un objeto wlanNonHTConfig para un canal de 5 MHz (CBW5). La señal de datos restante se demodula utilizando la función wlanNonHTOFDMDemodulate, que convierte la señal de tiempo en símbolos OFDM. Estos símbolos se procesan con wlanNonHTDataBitRecover para recuperar los bits de datos originales del PSDU.

Paso 7: Extracción de Direcciones MAC

Finalmente, la función propia `extract_mac_from_psdu` toma los bits del PSDU recuperados y extrae las direcciones MAC. Esta función convierte los bits a bytes y luego a direcciones MAC en formato hexadecimal, proporcionando datos importantes como el frame control o la duración de id, pero más importante, la función devuelve las direcciones MAC del receptor, transmisor y una tercera dirección.

Salida

mac_address: Una estructura que contiene las direcciones MAC extraídas del PSDU. Si no se detecta una señal válida, la función retorna *'no detectada'*.

6.3.2 RESULTADOS OBTENIDOS

Al utilizar el software, se obtienen resultados precisos y fiables. La corrección del CFO mejora significativamente la calidad de la señal, permitiendo una detección más precisa. La correlación con los preámbulos STF y LTF asegura que solo se procesen señales válidas, minimizando la probabilidad de errores.

Al aplicar el software a la señal real que se tenía desde el principio se consiguen los siguientes resultados:

```
THRESHOLD = single
    2.1645
cfo = 1.2387e+06
cfo = 1200000
la correlacion maxima con el preambulo L-STF es de : 0.8219
Correlacion STF satisfactoria
Señal Detectada
bits_rate = 1×4 int8 row vector
     1   1   0   1

data_length = 1×12 int8 row vector
     0   1   1   1   0   0   0   0   0   0   0   0
```

Figura 6-29: Resultados obtenidos al aplicar el software a la señal real (Parte 1)

Como se puede apreciar en la figura 6.29, estos han sido los resultados y variables requeridas para la detección y extracción de datos de la señal. El THRESHOLD utilizado es de 2.1265, lo que indica que para hallar el ancho de la señal en frecuencia y obtener asi el CFO se cogieron todos los valores con energía superior a ese valor, dando un desplazamiento CFO de 1200000. Una vez corregida la señal, se le aplica una correlación con el preámbulo STF ideal, lo que da como resultado una correlación del 82,18%, un valor bastante razonable para pasar a la siguiente prueba que sería la ecualización del preámbulo LTF de la señal real y su posterior correlación con un preámbulo LTF ideal. Como se aprecia en la figura, estas dos pruebas fueron satisfactorias, por lo tanto, la señal fue detectada exitosamente.

El siguiente paso será comprobar si se extrajeron con éxito las direcciones MAC de la señal:

```
bits_rate = 1×4 int8 row vector
     1   1   0   1

data_length = 1×12 int8 row vector
     0   1   1   1   0   0   0   0   0   0   0   0

PSDULength_bits = 1792
PSDULength = 224
psdu = 1×1792 int8 row vector
     0   1   0   1   0   1   1   1   1   1   0   0   1   0   1   0   1   1   ...
```

Figura 6-30: Resultados obtenidos al aplicar el software a la señal real (Parte 2)

Los pasos siguientes seguidos por el software se aprecian gracias a los resultados y valores vistos en la figura 6.30. Al pasar la señal por la función de `wlanLSIGRecover`, se extrajeron dos datos importantes. Primero se extrajo los bits de rate de la parte del preámbulo L-SIG, los cuales nos confirman que la codificación en una BPSK, pero los más importantes fueron los bits correspondientes a Data Length, ya que, gracias a este valor, se pudo saber cuál era el número de bits utilizados para la transmisión de datos, que como se aprecia fueron 1792 bits o 224 bytes de información. Gracias a saber este número, ser puedo solucionar uno de los problemas que daba este software, en específico la función wlanNonHTDataBitRecover. Esta función, por predeterminado, siempre busca un Data Length de 1000 bytes, esto fue un problema ya que al pasar la señal con bastantes menos bytes de los que estaba buscando, no era capaz de extraer lo bits del PSDU y daba el error visto en la figura 6.31. Como se aprecia, la función espera más símbolos OFDM, pero no los está recibiendo ya que los datos enviados son menores de los que espera la función.

```
Error using wlanNonHTDataBitRecover
Expected 335 OFDM symbols in the received signal. Received 92 OFDM symbols.

Error in detector_OFDM_CB5 (line 85)
        psdu = wlanNonHTDataBitRecover(sym,noiseVarEst,cfg_nonHT_CBW5)'
```

Figura 6-31: Error de falta de símbolos OFDM

Pero gracias a la función wlanLSIGRecover y gracias a saber que el PSDU tiene un Data Length de 1792 bits o 224 bytes. Se pudo corregir este error y como se aprecia en la figura 6.30, se pudo extraer el PSDU de manera exitosa. Por último, el PSDU se fue aplicado la función de extracción de direcciones MAC, y dio como resultado las direcciones MAC vistas en la figura 6.32.

```
mac_address = struct with fields:
    frame_control: [2×1 double]
      duration_id: [2×1 double]
         receiver: 'D9:0A:0B:DE:1C:68'
      transmitter: '51:05:CA:29:43:5B'
         address3: '8E:EC:E9:54:0B:FC'
```

Figura 6-32: Resultados obtenidos al aplicar el software a la señal real (Parte 3)

Capítulo 7. CONCLUSIONES Y TRABAJOS FUTUROS

El proyecto de detección y decodificación de señales "Enhanced Wi-Fi" ha resultado en un avance significativo en el campo de las comunicaciones inalámbricas, específicamente en la capacidad de identificar y procesar señales OFDM de 5 MHz utilizadas en la comunicación de drones DJI. El desarrollo de este proyecto ha abordado varios desafíos técnicos inherentes a la detección de señales de banda estrecha, las cuales son típicamente difíciles de captar y procesar con precisión debido a sus características específicas y la susceptibilidad a interferencias y ruido.

Desde el inicio, la necesidad de un algoritmo capaz de detectar y decodificar señales de 5 MHz se destacó como una prioridad debido a la limitación de las tarjetas de red inalámbricas convencionales que no pueden procesar señales con anchos de banda inferiores a 20 MHz. Este proyecto ha abordado esta brecha tecnológica mediante el diseño y la implementación de un algoritmo especializado que no solo detecta estas señales, sino que también extrae información crítica, como las direcciones MAC de los dispositivos transmisores y receptores, lo cual es esencial para aplicaciones de seguimiento y autenticación en redes complejas.

El proceso de desarrollo comenzó con la creación de una señal ideal utilizando MATLAB, que sirvió como referencia para entender y optimizar los diferentes componentes de las señales OFDM, incluyendo los preámbulos PLCP. Este enfoque permitió una comprensión profunda de las estructuras de las señales y facilitó la identificación de las características clave necesarias para la detección precisa de señales en el entorno real.

En el desarrollo del software, se utilizaron diversas funciones y toolboxes de MATLAB, los cuales proporcionaron las herramientas necesarias para la modulación, demodulación y análisis de las señales. La capacidad de generar y procesar señales de prueba que replican las características de las señales reales fue crucial para la validación del algoritmo. El uso de

técnicas avanzadas de procesamiento de señales digitales permitió mejorar la precisión y fiabilidad del algoritmo, abordando eficazmente los desafíos de interferencia y ruido.

La aplicación del software a señales reales capturadas de drones DJI demostró la eficacia del algoritmo desarrollado. Los resultados mostraron que el algoritmo no solo podía detectar señales OFDM de 5 MHz con alta precisión, sino que también era capaz de extraer las direcciones MAC de manera confiable. Este logro es significativo, ya que valida la capacidad del algoritmo para operar en condiciones reales y su potencial aplicación en escenarios prácticos.

Uno de los resultados más destacados fue la capacidad del algoritmo para corregir desplazamientos de frecuencia del portador (CFO) y eliminar el ruido de las señales capturadas, lo cual es esencial para mantener la integridad de los datos transmitidos y recibidos. La implementación de filtros adaptativos y técnicas de estimación de canal mejoraron la SNR, permitiendo una detección más precisa y una mejor calidad de comunicación.

El proyecto ha demostrado que, mediante el uso de algoritmos especializados y herramientas avanzadas de procesamiento de señales, cabe la posibilidad de superar las limitaciones actuales de las tarjetas de red inalámbricas convencionales, aplicando estos algoritmos. La capacidad de detectar señales de 5 MHz y extraer direcciones MAC añade un nivel de funcionalidad que puede ser extremadamente valioso para aplicaciones que requieren seguimiento y autenticación de dispositivos en redes complejas, como en las redes IoT.

Además, la implementación de este algoritmo en hardware presenta un potencial significativo para aplicaciones futuras. La optimización del algoritmo para su ejecución en dispositivos con recursos limitados abre nuevas posibilidades para la expansión de las capacidades de los sistemas de comunicación inalámbrica.

En términos de impacto, este proyecto contribuye a la seguridad y eficiencia de la comunicación en drones, lo cual es crucial en aplicaciones donde la privacidad y la seguridad son preocupaciones primordiales. La capacidad de detectar y decodificar señales de banda

estrecha mejora la monitorización y control de drones en áreas sensibles, protegiendo la privacidad y seguridad de individuos e instituciones.

Para cerrar este proyecto de detección y decodificación de señales "Enhanced Wi-Fi", se destaca que este ha mostrado ser una solución efectiva para superar las limitaciones actuales de las tarjetas de red inalámbricas convencionales en la detección de señales OFDM de 5 MHz. A través del desarrollo de un algoritmo especializado y su implementación utilizando MATLAB, se ha logrado identificar y procesar estas señales con alta precisión, así como extraer información crítica como las direcciones MAC. Además, la futura adaptación del código para recibir señales de antenas reales y su posible integración en tarjetas de red inalámbricas convencionales representan pasos importantes hacia la mejora de la tecnología actual.

Capítulo 8. BIBLIOGRAFÍA

[1] Business Insider: Cómo DJI se ha convertido en el mayor fabricante de drones del mundo URL: https://www.businessinsider.es/como-dji-ha-convertido-mayor-fabricante-drones-mundo-1197696

[2] Merca 2.0: La empresa china "DJI" sigue liderando en el mercado de drones URL: https://www.merca20.com/la-empresa-china-dji-sigue-liderando-en-el-mercado-de-drones/

[3] CNBC: World's largest drone maker is unfazed. URL: https://www.cnbc.com/2023/02/08/worlds-largest-drone-maker-dji-is-unfazed-by-challenges-like-us-blacklist.html#:~:text=DJI%20currently%20dominates%20more%20than,to%20%2455.8%20billion%20by%202030.

[4] 5G Technology World: The basics of 5G's modulation, OFDM. URL: https://www.5gtechnologyworld.com/the-basics-of-5gs-modulation-ofdm/#

[5] Andreas F. Molisch, "Orthogonal Frequency Division Multiplexing (OFDM)," in Wireless Communications , IEEE, 2011, pp.417-443, doi: 10.1002/9781119992806.ch19.

[6] Wang, Z.; Wei, S.; Zou, L.; Liao, F.; Lang, W.; Li, Y. Deep-Learning-Based Carrier Frequency Offset Estimation and Its Cross-Evaluation in Multiple-Channel Models. Information 2023, 14, 98. https://doi.org/10.3390/info14020098

[7] Computer Mesh: "WiFi Channel Width - 20 MHz vs 40 MHz vs 80 MHz Explained" URL: https://computermesh.com/wifi-channel-width-20-mhz-vs-40-mhz-vs-80-mhz/

[8] "IEEE 802.11be – Wi-Fi 7: New Challenges and Opportunities". arXiv preprint arXiv:2007.13401. URL: https://ar5iv.labs.arxiv.org/html/2007.13401

[9] MathWorks. "MATLAB Overview". MathWorks, URL: https://es.mathworks.com/products/MATLAB.html

[10] MathWorks. "Communications Toolbox". MathWorks, URL: https://es.mathworks.com/products/communications.html

[11] MathWorks. "Signal Processing Toolbox". MathWorks URL: https://es.mathworks.com/products/signal.html

[12] MathWorks. "WLAN Toolbox". MathWorks
URL: https://es.mathworks.com/products/wlan.html

[13] Wang, J., & Huang, Z. (2021). A Signal Detection Scheme Based on Deep Learning in OFDM Systems. *arXiv preprint arXiv:2107.13423*.
URL: https://arxiv.org/abs/2107.13423.

[14] Huang, Y.; Yuan, L.; Gong, W. "Research on IEEE 802.11 OFDM Packet Detection Algorithms for Household Wireless Sensor Communication," *Applied Sciences*, 2022, 12(14), 7232. https://doi.org/10.3390/app12147232.

[15] "Power of Deep Learning for Channel Estimation and Signal Detection in OFDM Systems," *arXiv*, https://arxiv.org/abs/1708.08514.

[16] IEEE Communications Magazine, "Distributed Wireless Communication System", Marzo 2003.

[17] IEEE Communications Magazine, "Transparent IP Radio Access For Next Generation Mobile Networks", Agosto 2003.

[18] IEEE Communications Magazine, "Switching Architectures", Octubre 2003.

[19] Hewlett Packard, "Wi-FiTM and BluetoothTM - Interference Issues", Enero 2003.

[20] MathWorks. "fft." *MathWorks Documentation*,
https://es.mathworks.com/help/MATLAB/ref/fft.html?searchHighlight=fft&s_tid=srchtitle_support_results_1_fft.

[21] MathWorks. (n.d.). What Is OFDM?.
URL: https://es.mathworks.com/videos/what-is-ofdm-1623999558386.html

[22] IEEE Std. 802.11-1999b, IEEE Standards for Local and Metropolitan Area Networks: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. http://www.ieee.org

[23]

[24] IEC3588, "DIAMETER BASE PROTOCOL", Septiembre 2003. Obtenido de http://www.iee.org

[25] MathWorks. (n.d.). Non-HT PPDU Structure.
URL: https://es.mathworks.com/help/wlan/gs/non-ht-ppdu-structure.html

[26] MathWorks. (n.d.). wlanLSIG (WLAN Toolbox). URL:
https://es.mathworks.com/help/wlan/ref/wlanlsig.html

[27] "802.11 Frame Types and Formats." *How I Wi-Fi*, 13 Jul. 2020, URL:
https://howiwifi.com/2020/07/13/802-11-frame-types-and-formats/.

[28] MathWorks. "wlanNonHTConfig." *MathWorks Documentation*, https://es.mathworks.com/help/wlan/ref/wlannonhtconfig.html?s_tid=doc_ta.

[29] MathWorks. "wlanLSIGRecover." *MathWorks Documentation*, https://es.mathworks.com/help/wlan/ref/wlanlsigrecover.html?s_tid=doc_ta

[30] MathWorks. "wlanNonHTDataBitRecover." *MathWorks Documentation*, https://es.mathworks.com/help/wlan/ref/wlannonhtdatabitrecover.html?s_tid=doc_ta

[31] MathWorks. "wlanNonHTOFDMDemodulate." *MathWorks Documentation*, https://es.mathworks.com/help/wlan/ref/wlannonhtofdmdemodulate.html?s_tid=doc_ta.

[32] "How does carrier frequency offset effect the constellation diagram in OFDM?" *Signal Processing Stack Exchange*, dsp.stackexchange.com

[33] Atef, Mohamed, y Horst Zimmermann. "Equalization Techniques." En *Optical Communication over Plastic Optical Fibers*, Springer Series in Optical Sciences, vol. 172, Springer, Berlin, Heidelberg, 2013, pp. 23-40.

[34] MathWorks. "wlanLLTF." *MathWorks Documentation*, https://es.mathworks.com/help/wlan/ref/wlanlltf.html?s_tid=doc_ta

ANEXO I: ALINEACIÓN DEL PROYECTO CON LOS ODS

Este trabajo esta alineado con los siguientes Objetivos de Desarrollo Sostenible:

Figura Anexo I-0-1: Objetivos de Desarrollo Sostenible de la Agenda 2030

Objetivo 4 - EDUCACIÓN DE CALIDAD

El proyecto puede contribuir a la Educación de Alta Calidad ya que se fomenta en tecnologías de la información y la comunicación (TIC), proporcionando herramientas innovadoras para el aprendizaje de conceptos avanzados en telecomunicaciones y redes inalámbricas. Esto puede ser especialmente relevante en contextos donde el acceso a este tipo de educación es limitado.

Objetivo 9 - INDUSTRIA, INNOVACIÓN E INFRAESTRUCTURA

El desarrollo del algoritmo para identificar, codificar y decodificar señales OFDM de 5 MHz puede ser una innovación significativa en el campo de las telecomunicaciones, contribuyendo a la infraestructura tecnológica y fomentando la investigación y desarrollo en el sector.

Objetivo 11 - CIUDADES Y COMUNIDADES SOSTENIBLES

La implementación del algoritmo puede mejorar la eficiencia y seguridad en el uso de drones para diversas aplicaciones en entornos urbanos, lo que puede contribuir a la gestión sostenible de las ciudades y comunidades. También puede contribuir a la seguridad urbana ya que se puede detectar la presencia de drones en lugares no deseados y asi prevenir situaciones abruptas.