P.I
(043) 621.39
M 589
2021

TESIS DE GRADO DE INGENIERÍA EN TELECOMUNICACIONES

DEMODULACIÓN Y SÍNTESIS DE SEÑALES OFDM, IEEE 802.11

Daniel Milanés Chau
Estudiante

Dr. Juan Pablo Pascual
Director

Mgter. Gustavo Fabián Rinalde
Co-director

Miembros del Jurado
Mgter. Roberto Costantini (INVAP-IB)
Ing. Javier Smidt (UNLP)

15 de Diciembre de 2021

Departamento de Ingeniería en Telecomunicaciones – Centro Atómico de Bariloche

Instituto Balseiro
Universidad Nacional de Cuyo
Comisión Nacional de Energía Atómica
Argentina

(Biblioteca Leo Falicov CAB-IB)

Inventario 24604
25/08/2022

A mis padres y a mi hermana

Índice de símbolos

Ack:	*Acknowledgment* - Confirmación
AP:	*Access Point* - Punto de acceso
ATIM:	*Announcement Traffic Indication Message* - Mensaje de indicación de tráfico de anuncio
BPSC:	*Bits Per SubCarrier* - Bits por subportadora
BSSID:	*Basic Service Set Identifier* - Identificador de conjunto de servicios básicos
BW:	*Bandwidth* - Ancho de banda
CBPS:	*Code Bits Per Symbol* - Bits de código por símbolo
CF:	*Contention Free* - Libre de contención
CTS:	*Clear To Send* - Libre para el envío
Data:	*Destination Address* - Dirección de destino
DBPS:	*Data Bits Per Symbol* - Bits de datos por símbolo
DFS:	*Dinamic Frequency Selection* - Selección dinámica de frecuencia
DLL:	*Data Link Layer* - Capa de enlace de datos
DMG:	*Directional Multi-Gigabit* - Multi-Gigabit Direccional
FCS:	*Frame Check Sequence* - Secuencia de chequeo de trama
GI:	*Guard Interval* - Intervalo de guarda
HT:	*High Throughput* - Alta capacidad de transmisión
HTC:	*HT Control* - Control HT
IDFT:	*Inverse Discrete Fourier Transform* - Antitransformada discreta de Fourier
IFFT:	*Inverse Fast Fourier Transform* - Antitransformada rápida de Fourier
ITU:	*International Telecommunication Union* - Unión Internacional de Telecomunicaciones
LLC:	*Logical Link Control* - Control de enlace lógico
LSB:	*Least Significant Bit* - Bit menos significativo
MAC:	*Media Access Control* - Control de acceso al medio
MSB:	*Most Significant Bit* - Bit más significativo
MSDU:	*MAC Service Data Unit* - Unidad de datos de servicio de la capa MAC
NDP:	*Null Data Packet* - Paquete de datos nulo
OFDM:	*Orthogonal Frequency Division Multiplexing* - Multiplexación por División

	de Frecuencias Ortogonales
PAPR:	*Peak-to-Average Power Ratio* - Relación entre potencias máxima y media
PHY:	*Physical Layer* - Capa Física
PRF:	*Pulse Repetition Frequency* - Frecuencia de repetición de pulsos
PS:	*Power Save* - Estado de bajo consumo
PSDU:	*PHY Service Data Unit* - Unidad de datos de servicio de la capa física
QoS:	*Quality of Service* - Calidad de Servicio
RA:	*Receiver Address* - Dirección del Receptor
RF:	*Radio Frequency* - Frecuencia de Radio
RLAN:	*Radio Local Area Network* - Red Local de Radio
SA:	*Source Address* - Dirección de Origen
SDR:	*Software Defined Radio* - Radio definido por software
SNR:	*Signal to Noise Ratio* - Relación entre señal y ruido
SPR:	*Service Period Request* - Petición de período de servicio
SSW:	*Sector Sweep* - Barrido de Sector
TA:	*Transmitter Address* - Dirección del Transmisor
USRP:	*Universal Software Radio Peripheral* - Periférico Universal de Radio Programable
VHT:	*Very High Throughput* - Muy alta capacidad de transmisión
WLAN:	*Wireless Local Area Network* - Red Local Inalámbrica

Índice de contenidos

Índice de símbolos v

Índice de contenidos vii

Índice de figuras xi

Índice de tablas xv

Resumen xvii

Abstract xix

1. Introducción 1

1.1. Motivación del proyecto 1

1.2. Objetivos del Proyecto Integrador 2

1.3. Organización de la tesis 3

2. Descripción de la trama IEEE 802.11a 5

2.1. Descripción de la modulación OFDM 5

2.2. Estructura de la trama de datos 7

2.2.1. Preámbulo 8

2.2.2. Símbolo SIGNAL 9

2.2.3. Campo DATA 10

2.3. Conclusiones 11

3. Síntesis y demodulación de la señal IEEE 802.11a 13

3.1. Preámbulo 13

3.1.1. Símbolos cortos 15

3.1.2. Símbolos largos 15

3.2. Síntesis de los símbolos OFDM 16

3.2.1. Scrambler 17

3.2.2. Codificador 17

3.2.3. Entrelazador 18

3.2.4. Modulación e inserción de tonos piloto y prefijo cíclico 19
3.3. Síntesis del símbolo SIGNAL 21
3.4. Síntesis de los símbolos del campo DATA 23
3.5. Estudio de desempeño de las etapas de síntesis 25
3.5.1. Ganancia de código 25
3.5.2. Canal con desvanecimiento 28
3.6. Demodulación de la señal OFDM IEEE 802.11a 30
3.7. Conclusiones 31

4. Demodulación de mediciones reales 33
4.1. Descripción de los datos 33
4.2. Detección y corrección de errores 36
4.2.1. Detección 36
4.2.2. Sincronismo de frecuencia 37
4.2.3. Ecualización del canal 42
4.3. Demodulación de los símbolos del paquete 45
4.3.1. Demodulación del símbolo SIGNAL 45
4.3.2. Demodulación de los símbolos de DATA 47
4.4. Conclusiones 48

5. Extracción de información de capas superiores 49
5.1. Estructura del formato de la capa MAC 49
5.1.1. Frame Control 50
5.2. Frame Control Sequence 51
5.3. Interpretación de los bits de la trama obtenida 52
5.3.1. Frame Control de la trama obtenida 52
5.3.2. FCS de la trama obtenida 53
5.4. Conclusiones 53

6. Análisis completo de un segundo paquete 55
6.1. Procesamiento del paquete en capa física 55
6.2. Procesamiento del paquete en la capa MAC 60
6.2.1. Lectura de Direcciones 61
6.2.2. Cálculo de la FCS 62
6.3. Conclusiones 62

7. Conclusiones 63

A. Tipos y Subtipos de tramas MAC 67

B. Proyecto y diseño 71

Bibliografía **73**

Agradecimientos **75**

Índice de figuras

2.1. Espectros de un subcanal OFDM y de una señal con múltiples subportadoras ortogonales que se superponen. Los espectros tienen la forma de la función seno cardinal (*sinc*). 6
2.2. Estructura general del paquete OFDM. 8
2.3. Estructura de los bits que componen al símbolo SIGNAL. 9
2.4. Estructura general del campo DATA. 10

3.1. Mapeo de la secuencia de 53 subportadoras para obtener las muestras temporales empleando la IFFT. 14
3.2. Muestras de la señal temporal correspondiente a la envolvente compleja de la secuencia de símbolos cortos del Preámbulo en banda base. 15
3.3. Muestras de la señal temporal correspondiente a la envolvente compleja de la secuencia de símbolos largos del Preámbulo en banda base. 16
3.4. Esquema de la síntesis del símbolo SIGNAL y de los del campo DATA. 16
3.5. Esquema del scrambler del estándar. 17
3.6. Esquema del codificador convolucional que emplea el estándar. 18
3.7. Esquemas de perforado propuestos en el estándar. 18
3.8. Equivalencias entre bits a la salida del entrelazador y las muestras espectrales para las distintas modulaciones empleadas. 19
3.9. Bits de fuente del símbolo SIGNAL del ejemplo. 21
3.10. Bits codificados para el símbolo SIGNAL del ejemplo. El orden de los bits al pasar a la siguiente etapa es de arriba a abajo y de izquierda a derecha. 22
3.11. Permutaciones de las posiciones en los bits codificados para $N_{BPSC} = 1$ y $N_{CBPS} = 48$, valores correspondientes a la síntesis del símbolo SIGNAL. 22
3.12. Espectro de 64 muestras del símbolo SIGNAL del ejemplo. 23
3.13. Muestras de la señal temporal correspondiente a la envolvente compleja del símbolo SIGNAL en banda base. 23
3.14. Muestras de la señal temporal correspondiente a la envolvente compleja del paquete IEEE 802.11a del ejemplo en banda base. 24

3.15. Comparación de los valores de BER en función de la E_b/N_0 al usar distintos códigos convolucionales sobre un sistema de modulación BPSK. 26
3.16. Comparación de los valores de BER en función de la E_b/N_0 entre la curva teórica del sistema de codificación que emplea el estándar en cuestión y la obtenida mediante simulaciones. 27
3.17. Comparación de las curvas de BER para los canales simulados empleando el modelo de Clarke con modulación BPSK y detección coherente. . 28
3.18. Esquema de la demodulación del símbolo SIGNAL y de los del campo DATA. 30

4.1. Esquema experimental y dispositivos empleados en la adquisición de datos. 34
4.2. Configuración del router para la comunicación. 35
4.3. Muestras adquiridas con el USRP correspondientes a las componentes I y Q de la señal en banda base y corrección del nivel de continua en las mismas. 35
4.4. Detalle de la forma de onda de la componente I de la señal en banda base de uno de los paquetes adquiridos. Se resalta la secuencia de símbolos cortos del paquete. 36
4.5. Módulo de la correlación de las muestras adquiridas con la secuencia de símbolos cortos. 37
4.6. Comparación entre las secuencias de símbolos cortos sintéticos con $\Delta f = 0$ (arriba) y con $\Delta f = 20$ kHz (abajo). 38
4.7. Comparación entre los espectros de símbolos cortos con $\Delta f = 0$ (arriba), donde las partes real e imaginaria coinciden, y con $\Delta f = 20$ kHz usando los símbolos $3 \sim 6$ (abajo). 38
4.8. Constelación del espectro de símbolos cortos para $\Delta f = 20$ kHz. En azul, las subportadoras que valen $1 + j$ al eliminar el valor de normalización $\sqrt{13/6}$ en la secuencia $S_{-26,26}$ y en rojo, las subportadoras que valen $-(1 + j)$. 39
4.9. Comparación entre los espectros de símbolos cortos ideales (arriba) y los correspondientes al paquete adquirido (abajo). $T_{SHORT} = 8$ μs para canales de 20 MHz. 40
4.10. Constelación del espectro de símbolos cortos del paquete adquirido. En azul, las subportadoras que corresponden a $1 + j$ según $S_{-26,26}$, en rojo, las que corresponden a $-(1 + j)$. 40
4.11. Valores máximos de la correlación cruzada de las muestras de la secuencia de símbolos cortos del paquete adquirido con la señal de referencia sintetizada en función del Δf. 41

4.12. Constelación del espectro de símbolos cortos del paquete adquirido luego de corregir el sincronismo en frecuencia. En azul, las subportadoras que corresponden a $1 + j$, en rojo, las subportadoras que corresponden a $-(1 + j)$. 42
4.13. Espectro obtenido para un símbolo largo del paquete. 43
4.14. $H(f)$ obtenida empleando un símbolo largo como señal de referencia. En la gráfica de arriba se observa su módulo y en la de abajo su fase, en función de la frecuencia. 44
4.15. Comparación entre las $H(f)$ estimadas con un símbolo largo y con los cortos. En la gráfica de arriba el módulo y en la de abajo la fase, en función de la frecuencia. 44
4.16. Comparación de las constelaciones con y sin corrección del símbolo SIGNAL. 45
4.17. Bits de fuente del símbolos SIGNAL del paquete adquirido. 46
4.18. Constelaciones 16-QAM de los símbolos del campo DATA luego de las correcciones, el cálculo del espectro y la eliminación de las subportadoras piloto y símbolos nulos. 47

5.1. Formato de los campos de la capa MAC. 50
5.2. Estructura del Frame Control según los campos Tipo y Subtipo. 50
5.3. Frame Control correspondiente al paquete demodulado. 52
5.4. Estructura de la trama de Control Ack. 52

6.1. Detalle de la forma de onda de la componente I de la señal en banda base del paquete. 56
6.2. $H(f)$ obtenida empleando un símbolo largo como señal de referencia. En la gráfica de arriba se observa su módulo y en la de abajo su fase, en función de la frecuencia. 56
6.3. Constelación del símbolo SIGNAL. 57
6.4. Bits de fuente del símbolo SIGNAL. 57
6.5. Constelaciones 64QAM de los símbolos del campo DATA luego de las correcciones, el cálculo del espectro y la eliminación de las subportadoras piloto y símbolos nulos. 59
6.6. Estructura de la trama MAC para el Tipo Data. 60

Índice de tablas

2.1. Parámetros de señal en función de BW. 7
2.2. Tasas de transmisión en [Mbps] correspondientes a cada combinación de bits del campo RATE en función del ancho de canal. 9
2.3. Parámetros de modulación de los símbolos correspondientes al campo DATA en función de los bits del campo RATE del símbolo SIGNAL. . . 10

3.1. Constante de normalización de energía correspondientes a cada modulación 20

6.1. Campos de Direcciones para las tramas de Tipo Data según su Frame Control. 60
6.2. Bits en los distintos campos de la estructura de la trama. 61

A.1. Descripción de las funciones de las tramas según su Tipo y Subtipo. . . 68
A.2. Descripción de las funciones de las tramas de Control con extensión. . . 69

Resumen

Los dispositivos WLAN/RLAN que emplean el estándar IEEE 802.11 no siempre cumplen con las regulaciones establecidas diseñadas para que su comunicación no afecte la actividad de los radares meteorológicos con los que comparten el espectro radioeléctrico. Como medida de control del uso del espectro se planteó identificar a los dispositivos interferentes a partir de determinar su dirección MAC.

Para adquirir la información de la subcapa MAC es necesario comprender las características del estándar. Este trabajo se enfoca en la cláusula IEEE 802.11a en particular, debido a que todos los canales que esta emplea se encuentran en la zona de los 5 GHz, correspondientes al rango de frecuencias de banda C que emplean los radares meteorológicos de la República Argentina.

En primer lugar, se estudió la estructura de los paquetes de dicha cláusula para entender cómo operan los mecanismos de síntesis y demodulación de sus paquetes en capa física bajo la modulación multiportadora por división de frecuencias ortogonales (OFDM). Luego, se procesaron registros de datos reales correspondientes a la comunicación entre dispositivos inalámbricos que empleaban dicho estándar. La señal correspondiente a los paquetes medidos se encontraba distorsionada, en especial como consecuencia de los efectos no deseados del canal y errores de sincronismo. Por lo tanto, se desarrolló un método para corregirlos previo a realizar la demodulación, de modo de extraer los bits provenientes de capas superiores sin errores.

Por último, se estudió la estructura de la trama de datos a nivel de capa MAC. Esto permitió implementar rutinas para desempaquetar la información contenida en dicha trama, identificar el tipo de paquete que se transmite, realizar el control de errores y extraer los valores de las direcciones MAC de los dispositivos involucrados en la comunicación, lo que conformaba el objetivo final de este proyecto.

Palabras clave: OFDM, IEEE 802.11A, SÍNTESIS, DEMODULACIÓN, DIRECCIÓN MAC

Abstract

WLAN/RLAN devices that use the IEEE 802.11 standard do not always comply with the established regulations designed so that their communication does not affect the activity of weather radars with which they share the radio spectrum. As a measure to control the use of the spectrum, we propose to identify the interfering devices by determining their MAC address.

To acquire the information of the MAC sublayer, it is necessary to understand the characteristics of the standard. This work focuses on the IEEE 802.11a clause in particular, since all the channels it uses are in the region of the 5 GHz, corresponding to the C-band frequency range used by weather radars of the Argentine Republic.

In the first place, the structure of the packets of said clause was studied to understand how the synthesis and demodulation mechanisms of its packets operate in the physical layer under Orthogonal Frequency Division Multicarrier Modulation (OFDM). Then, real data records corresponding to the communication between wireless devices that used the standard were processed. The signal corresponding to the measured packets was distorted, especially as a consequence of undesired channel effects and synchronization errors. Therefore, a method was developed to correct them prior to demodulation, in order to extract the bits from the higher layers without errors.

Finally, the structure of the data frame at the MAC layer was studied. This allowed the implementation of routines to unpack the information contained in said frame, identify the type of packet transmitted, perform the error control and extract the MAC addresses of the devices involved in the communication, which constituted the final objective of this project.

Keywords: OFDM, IEEE 802.11A, SYNTHESIS, DEMODULATION, MAC ADDRESS

Capítulo 1

Introducción

1.1. Motivación del proyecto

En el año 2003 la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés) tomó la decisión de asignar las bandas de 5,150 a 5,350 y de 5,470 a 5,725 GHz a sistemas de acceso inalámbricos, incluyendo las redes WLAN/RLAN (Wireless/Radio Local Area Networks), siempre que no causen interferencia a los servicios existentes, como los radares meteorológicos de banda C (entre los 4 y 8 GHz) [1]. Se esperaba que los dos grupos de usuarios coexistieran en el mismo entorno, requiriendo que las redes WLAN/RLAN utilizaran un sistema de selección dinámica de frecuencia (DFS, por sus siglas en inglés). Este protocolo define un mecanismo por el cual, antes de usar un canal la red WLAN/RLAN debe chequear la presencia de señales de radar por un período de tiempo y evitar usar aquellas frecuencias que el radar esté utilizando.

Sin embargo, cerca de cumplirse dos décadas de haber tomado esta decisión, la interferencia debida a redes WLAN/RLAN en radares meteorológicos de banda C es un problema a nivel mundial y se encuentra entre los factores limitantes de su desempeño [2]. Uno de los motivos de esta situación consiste en que se encuentran en el mercado versiones obsoletas del sistema DFS, las cuales presentan fallas como las que se mencionan a continuación [3]:

- Posibilidad de deshabilitar la función DFS por parte del usuario.
- Ancho mínimo del pulso: si el ancho del pulso está por debajo de los mínimos detectables el dispositivo no detectará el radar y seguirá utilizando el canal.
- Frecuencia de repetición de pulso (PRF, por sus siglas en inglés) fija: recién a partir de 2013 se obliga a los dispositivos a detectar PRF fijas, alternadas o entrelazadas.
- Intervalo de tiempo disponible en el que el sistema DFS libera el canal: para algunas estrategias de operación de los radares puede resultar insuficiente.

Los radares meteorológicos nacionales, que fueron fabricados e instalados a lo largo del país por la empresa INVAP desde el lanzamiento del Sistema Nacional de Radares Meteorológicos (SINARAME) en el año 2011, operan en banda C [4]. Por lo tanto, la interferencia debida a las redes WLAN/RLAN que transmiten en esta banda se convirtió en una de las principales causas de degradación de su desempeño en los sitios densamente poblados, como por ejemplo en Córdoba o Ezeiza. En el ámbito nacional existen trabajos recientes que abordan el problema de la detección y la mitigación de la interferencia WLAN/RLAN en radares meteorológicos con soluciones desde el punto de vista del procesamiento estadístico de señales [5], [6], [7]. En [5] proponen técnicas de filtrado basadas en la transformada de wavelet. Por su parte en [6] y [7] se propone un esquema de detección del preámbulo de la señal WiFi a la salida del filtro adaptado del radar. El mismo se basa en un test de hipótesis sobre el criterio de la señal de Neyman-Pearson [8] y explota la estructura determinística que posee el preámbulo [9].

Si bien el Estado Nacional posee la prerrogativa para fiscalizar el cumplimiento de la no interferencia a los radares meteorológicos, en la actualidad la misma no se ejerce. Además, de hacerlo, el ente fiscalizador debe conocer la ubicación precisa de las fuentes WLAN/RLAN que operan en banda C. El ángulo acimutal desde donde arriba la interferencia se obtiene fácilmente a partir del radar. Sin embargo, determinar la distancia al transmisor WLAN/RLAN es una tarea compleja, debido a que los radares que se encuentran en operación no fueron diseñados para recibir este tipo de señales. Una posible solución a esta problemática, alternativa a la mitigación mediante procesamiento de señales, consiste en contar con un dispositivo que reciba las señales WLAN/RLAN en simultáneo con el radar, cuya función sea la de demodular dichas señales, de modo tal de determinar quién es el usuario que está interfieriendo, a partir de la información que se pueda extraer de los paquetes recibidos, como su dirección MAC.

1.2. Objetivos del Proyecto Integrador

Actualmente, varios tipos de dispositivos WLAN utilizan canales de transmisión entre los 5,470 GHz y los 5,725 GHz. Las especificaciones de capa física para estos sistemas están contenidas en las cláusulas IEEE 802.11a, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax. Sin embargo, la cláusula IEEE 802.11a, es la única que opera exclusivamente en la banda de 5 GHz y lo hace empleando multiplexación por división de frecuencias ortogonales (OFDM, por sus siglas en inglés) [9].

En este contexto, el presente Proyecto Integrador tiene como objetivo general el desarrollo de un demodulador de señales OFDM IEEE 802.11a, sobre un entorno de programación de alto nivel de abstracción (MATLAB o Python) a partir de mediciones tomadas por un dispositivo de radio (SDR, por sus siglas en inglés), específicamente un Periférico Universal de Radio Programable (USRP, por sus siglas en inglés) de la

empresa National Instrument, disponible en el lugar de trabajo.

El trabajo se concentra en las capas física (PHY) y de enlace de datos (DLL, por sus siglas en inglés) de los sistemas de comunicación que utilizan este estándar [9]. Si bien esta última capa, está compuesta por las subcapas de control de acceso al medio (MAC, por sus siglas en inglés) y de control de enlace lógico (LLC, por sus siglas en inglés), para alcanzar los objetivos de este trabajo, solo es necesario considerar la más baja, es decir, la subcapa MAC.

Los objetivos específicos del proyecto consisten en:

- Estudiar en detalle la composición y formato de los paquetes OFDM de las distintas tecnologías IEEE 802.11.x.
- Realizar la sincronización de símbolo, de modo de determinar el comienzo del símbolo OFDM correspondiente a la configuración y de los símbolos OFDM a continuación.
- Demodular y extraer la información del símbolo OFDM de configuración.
- Desempaquetar los símbolos OFDM del paquete IEEE 802.11a correspondientes a la trama de datos.
- Demodular la trama de datos y extraer la información de los mismo hasta el punto que la seguridad lo permita.

Asimismo, a partir del estudio de la estructura de los paquetes del paquete IEEE 802.11a, se contempla el desarrollo de una rutina de generación de datos sínteticos OFDM IEEE 802.11a que será utilizada para la validación de las implementaciones con experimentos controlados. Para todas las implementaciones y simulaciones realizadas para este proyecto se empleó el software MATLAB.

1.3. Organización de la tesis

Las partes que componen este trabajo son las siguientes:

- Este primer capítulo de carácter introductorio, que además de su motivación contiene los objetivos del proyecto y un resumen de contenidos.
- El capítulo 2 en el que se detalla las partes que componen una trama IEEE 802.11a, estándar que emplea OFDM.
- El capítulo 3 en el que se describen los procesos de síntesis de un paquete OFDM a partir de una trama dada, y de demodulación de la señal correspondiente a un paquete para recuperar los bits transmitidos.

- El capítulo 4 en el que se describe el proceso de demodulación de un paquete IEEE 802.11a real, adquirido con un dispositivo de radio definida por software (SDR, por sus siglas en inglés), incluyendo una etapa previa en la que se realiza la ecualización del canal y la compensación de los errores de sincronismo.

- El capítulo 5 en el que se estudia de manera general la subcapa MAC y se interpreta el significado de los bits demodulados en el capítulo 4.

- El capítulo 6 en el que se muestra el proceso de demodulación en capa física y la lectura de la trama MAC obtenida para un segundo paquete adquirido, siguiendo la misma línea de los capítulos 4 y 5.

- El capítulo 7 y último en el que, a modo de conclusión, se marca el cierre del proyecto una vez cumplidos sus objetivos.

- Un apéndice con tablas con parámetros específicos relativos a la trama MAC del estándar IEEE 802.11a que contiene los valores de dos campos de dicha trama, que determinan el tipo de paquete que se transmite.

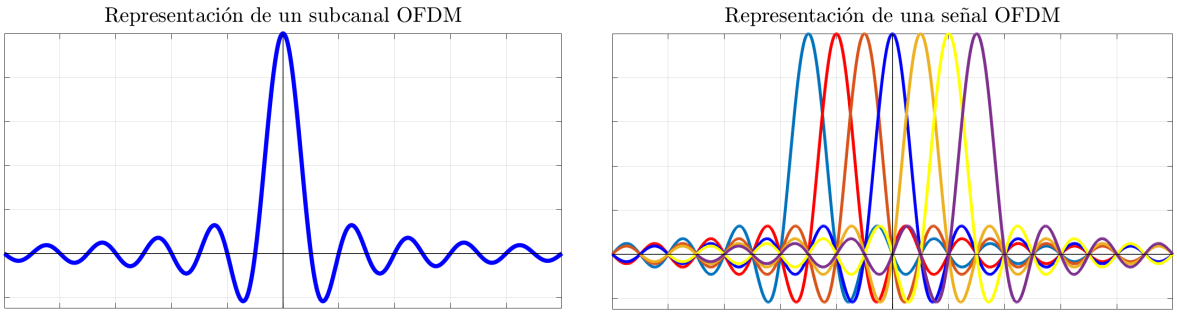
Capítulo 2

Descripción de la trama IEEE 802.11a

Como se ha mencionado, es de interés analizar las señales OFDM que podrían interferir con los radares en la banda de los 5 GHz. En este estudio se deben tener en cuenta las distintas partes que componen a estas señales para poder realizar su detección, sincronismo, demodulación y posteriormente la extracción de información. Es por esto que en el presente capítulo se detallan las características de este tipo de modulación y se describen las distintas partes que componen un paquete de datos según el estándar IEEE 802.11a. Se mencionan los diferentes valores para los parámetros de anchos de banda de canal, tasas de transmisión de bits, duración temporal de los paquetes y esquemas de codificación posibles que emplean estas señales y que deben ser tenidos en cuenta al momento de su síntesis.

2.1. Descripción de la modulación OFDM

La Multiplexación por División de Frecuencias Ortogonales (OFDM por sus siglas en inglés) es un tipo de modulación que consiste en enviar múltiples portadoras de forma simultánea, a las que habitualmente se denominan subportadoras. La información modula cada subportadora con algún esquema del tipo QAM o PSK en el dominio del espectro. Si bien las señales generadas a partir de cada subportadora se superponen tanto en el dominio del tiempo como del espectro como se observa en la figura 2.1, esta superposición de los espectros no implica que la señal correspondiente a una sola de las subportadoras afecte a las demás en el momento de demodular, siempre y cuando estos espectros sean ortogonales entre sí, propiedad que mantienen las señales luego de transitar por un canal modelado como un sistema lineal e invariante en el tiempo (LTI, por sus siglas en inglés).



(a) OFDM: 1 subportadora. **(b)** OFDM: 7 subportadoras.

Figura 2.1: Espectros de un subcanal OFDM y de una señal con múltiples subportadoras ortogonales que se superponen. Los espectros tienen la forma de la función seno cardinal (*sinc*).

En la generación de la señal, luego de que cada subportadora es modulada se aplica la antitransformada discreta de Fourier (IDFT, por su sigla en inglés) para llevar la señal al dominio temporal, lo que produce la envolvente compleja de la señal que se va a transmitir.

En el receptor, una vez que la señal es llevada a banda base y muestreada, se debe realizar el proceso inverso, es decir llevar la señal al dominio de las frecuencias, para lo cual se aplica la transformada discreta de Fourier (DFT, por sus siglas en inglés) para obtener el espectro.

Entre las ventajas que caracterizan a este esquema de modulación, se destacan que [10], [11]:

- Hace un uso eficiente del espectro superponiendo varias señales no interfirientes.
- Al dividir el canal en subcanales más estrechos que el ancho de banda total que ocupa un símbolo OFDM, se gana resistencia a los efectos de selectividad en frecuencia del canal.
- Usando un prefijo cíclico para los símblos, OFDM reduce la Interferencia Entre Símbolos (ISI, por sus siglas en inglés) y la Interferencia Entre Tramas (IFI, por sus siglas en inglés).
- Aplicando codificación y entrelazado, es posible recuperar los símbolos perdidos por la selectividad que pueda tener el canal.
- La ecualización de los canales es mucho más simple que para los sistemas de portadora única.
- A diferencia de Modulación por División de Frecuencias (FDM, por sus siglas en inglés) convencional, no hay receptores por cada subcanal que requieran filtros.

Por otra parte, entre las desventajas de OFDM se encuentra que [10], [11]:

- Requiere amplificadores con alta relación entre potencias máxima y media (PAPR, por sus siglas en inglés).

- Es más sensible a errores de sincronismo de portadora que sistemas de portadora única, debido a que esto introduce Interferencia entre Portadoras (ICI, por sus siglas en inglés).

- Hay una pérdida de eficiencia al incorporar un prefijo cíclico, cuya duración representa una parte significativa de la señal.

El estándar IEEE 802.11a establece los mecanismos de modulación y demodulación donde se utiliza OFDM para la modulación de los paquetes a nivel de capa física.

2.2. Estructura de la trama de datos

El ancho de banda espectral (BW) que ocupa un canal de OFDM de la 802.11a puede ser de 20, 10 o 5 MHz. Estos canales están representados por $N_{SD} = 48$ subportadoras moduladas que transmiten datos, a las cuales se añaden $N_{SP} = 4$ subportadoras piloto en determinadas posiciones cuya modulación está fijada previamente por el estándar, y luego se completa el espectro con símbolos de valor 0 para tener $N_{FFT} = 64$ para aplicar el algoritmo de la transformada rápida de Fourier (FFT, por sus siglas en inglés).

En la tabla 2.1 se muestran los parámetros que permiten caracterizar a un paquete de capa física de este estándar para cada ancho de canal que puede emplear.

En la figura 2.2 se presenta un esquema de la estructura de los paquetes OFDM correspondientes al estándar IEEE 802.11a. Dicha estructura permite comprender mejor qué representa cada uno de los parámetros.

Parámetro \ BW	20 MHz	10 MHz	5 MHz
Espaciamiento entre subportadoras [MHz]: Δ_F	0,3125	0,15625	0,078125
Período de FFT [μs]: $T_{FFT} = 1/\Delta_F$	3,2	6,4	12,8
Prefijo cíclico [μs]: $T_{GI} = T_{FFT}/4$	0,8	1,6	3,2
Símbolo OFDM [μs]: $T_{SYM} = T_{GI} + T_{FFT}$	4	8	16
Símbolos cortos (10) [μs]: $T_{SHORT} = 10 \cdot T_{FFT}/4$	8	16	32
Prefijo cíclico de los símbolos largos [μs]: T_{GI2}	1,6	3,2	6,4
Símbolos largos [μs]: $T_{LONG} = T_{GI2} + 2 \cdot T_{FFT}$	8	16	32
Preámbulo completo [μs]: $T_{PREAMBLE}$	16	32	64

Tabla 2.1: Parámetros de señal en función de BW.

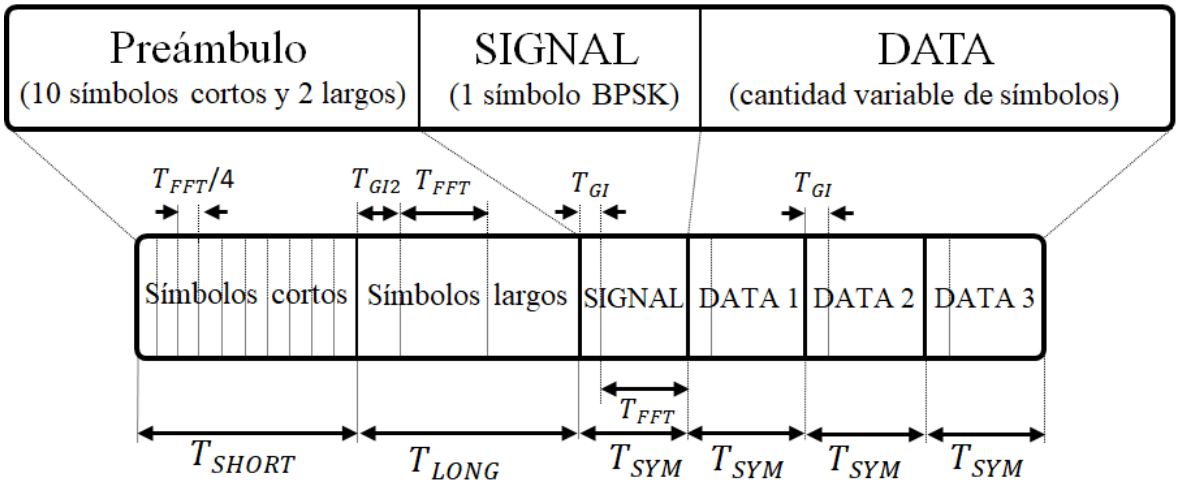


Figura 2.2: Estructura general del paquete OFDM.

Al inicio de todo paquete OFDM encontramos al Preámbulo, el cual consiste en una estructura formada por una secuencia de 10 símbolos cortos y otros 2 símbolos largos, los cuales son siempre iguales para todas las tramas que tengan igual BW.

A continuación, se encuentra el símbolo SIGNAL, el cual contiene información sobre la configuración de la transmisión, Específicamente indica qué tipos de modulación y codificación se emplean en los símbolos correspondientes al siguiente campo (lo que determina una tasa para cada ancho de canal posible) y, además indica cuántos bits de información provenientes de las capas superiores se transmiten en el paquete, lo cual también define su longitud.

El campo siguiente se llama DATA, y está conformado por una cantidad variable de símbolos, cuyas características quedan registradas en la información del símbolo SIGNAL. Tanto para la sección de símbolos largos del Preámbulo como para los símbolos SIGNAL y cada uno de los DATA, se coloca un prefijo cíclico que repite la última parte de la señal al inicio de cada uno.

2.2.1. Preámbulo

Como se mencionó, el Preámbulo está compuesto por una secuencia de 10 símbolos cortos de duración equivalente a 2 símbolos OFDM y una secuencia de 2 símbolos largos que incluyen un prefijo cíclico, también con una duración equivalente a 2 símbolos OFDM, resultando la duración total del Preámbulo igual a $T_{PREAMBLE} = 4 \cdot T_{SYM}$ donde T_{SYM} es la duración de un símbolo OFDM para el ancho de canal empleado.

Esta parte del paquete es importante para su detección y para el sincronismo en tiempo y frecuencia, así como para la ecualización del canal. Los detalles más específicos de su composición se abordan en 3.1, donde también se muestra el proceso de síntesis del mismo. Su estructura es siempre la misma para cualquier paquete, donde solo cambia la duración temporal según el BW siguiendo la tabla 2.1.

2.2.2. Símbolo SIGNAL

Como se indicó en la figura 2.2, a continuación del Preámbulo y antes de los símbolos del campo DATA, se encuentra un símbolo de configuración llamado SIGNAL que contiene información sobre la tasa de transmisión y la cantidad de bits a transmitir. Los campos que lo componen se muestran en la figura 2.3, y es a partir de esta secuencia de 24 bits que se generan las muestras de la señal en tiempo.

RATE (4 bits)				R	LENGTH (12 bits)												P	SIGNAL TAIL (6 bits)					
R1	R2	R3	R4	"0"	menos significativo											más significativo	P	"0"	"0"	"0"	"0"	"0"	"0"
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23

Figura 2.3: Estructura de los bits que componen al símbolo SIGNAL.

De izquierda a derecha, el primer campo, denominado RATE, está formado por 4 bits cuya combinación establece una tasa de transmisión para cada ancho de canal posible como se indica en la tabla 2.2.

R1-R4	Tasa (20 MHz)	Tasa (10 MHz)	Tasa (5 MHz)
'1101'	6	3	1,5
'1111'	9	4,5	2,25
'0101'	12	6	3
'0111'	18	9	4,5
'1001'	24	12	6
'1011'	36	18	9
'0001'	48	24	12
'0011'	54	27	13,5

Tabla 2.2: Tasas de transmisión en [Mbps] correspondientes a cada combinación de bits del campo RATE en función del ancho de canal.

El campo siguiente no es más que un bit reservado (R) que por indicaciones de la norma, se le asigna el valor fijo '0'. Esto también ocurre con los últimos 6 bits que conforman el campo TAIL, cuya función se explica en 3.2.2.

El campo LENGTH indica el número de octetos que se desean transmitir provenientes de las capas superiores representado como un número binario con los bits ordenados del menos al más significativo. Al tener 12 bits, el máximo de octetos posibles a transmitir por paquete es 4095.

Luego de este campo aparece un bit de paridad (P) al que se le asigna un valor de manera tal que la cantidad de bits en '1' de toda la estructura sea par.

2.2.3. Campo DATA

A continuación del símbolo SIGNAL, aparecen los correspondientes al campo DATA, en el cual se transmiten bits provenientes de capas superiores cuya cantidad se especifica en el campo LENGHT y que constituyen la unidad de datos de servicio de la capa física (PSDU, por sus siglas en inglés). A estos, se le anteponen $N_{SERVICE} = 16$ bits conocidos como el campo SERVICE y se le añaden otros $N_{TAIL} = 6$ bits al final que constituyen el campo TAIL, todos en '0'. La utilidad de estos campos de bits agregados se explica con el uso del scrambler y el codificador, los cuales se detallan en el capítulo 3. Para un dado ancho de canal, la tasa de transmisión determina un esquema de modulación para cada subportadora (lo que fija el número de bits de canal asignado a cada subportadora N_{BPSC}) y, además, determina una tasa de codificación R (lo que fija el número de bits de fuente N_{DBPS} y de canal N_{CBPS} por cada símbolo OFDM). En la tabla 2.3 se detalla esta dependencia según lo establecido en la norma.

RATE	Modulación	R	N_{BPSC}	N_{CBPS}	N_{DBPS}
1101	BPSK	1/2	1	48	24
1111	BPSK	3/4	1	48	36
0101	QPSK	1/2	2	96	48
0111	QPSK	3/4	2	96	72
1001	16-QAM	1/2	4	192	96
1011	16-QAM	3/4	4	192	144
0001	64-QAM	2/3	6	288	192
0011	64-QAM	3/4	6	288	216

Tabla 2.3: Parámetros de modulación de los símbolos correspondientes al campo DATA en función de los bits del campo RATE del símbolo SIGNAL.

Para generar la señal a transmitir, es necesario que el número total de bits del campo DATA (N_{DATA}) sea múltiplo entero de N_{DBPS}. Generalmente esto no ocurre, y en tal caso, se deben añadir bits de relleno hasta que esto se cumpla. A estos, denominados PAD bits, se les asigna el valor '0'. Los bits de DATA son procesados por todo el esquema de síntesis, el cual se detalla en la sección 3.2, para obtener las muestras complejas de la señal en banda base de los $N_{sym} = N_{DATA}/N_{DBPS}$ símbolos como se muestra en la figura 2.4. Una vez sintetizado todo el paquete, solo quedaría modularlo en fase y cuadratura con alguna frecuencia portadora alrededor de los 5 GHz.

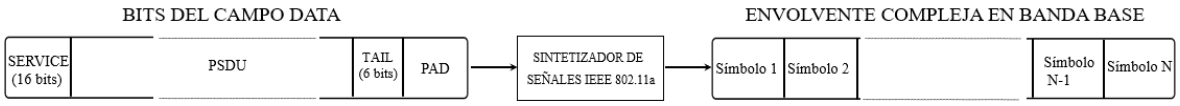


Figura 2.4: Estructura general del campo DATA.

2.3. Conclusiones

Se ha analizado la estructura general de los paquetes de señal de la norma IEEE 802.11a, la cual está formada por: un Preámbulo fijo, un símbolo de configuración llamado SIGNAL y varios símbolos del campo DATA. El uso de la modulación OFDM con la inserción del prefijo cíclico le dan una ventaja relativa a este frente a otros sistemas que emplean portadora única.

En el símbolo SIGNAL, se encuentra información esencial sobre la trama de datos, por lo que, en la recepción de la misma, para poder demodular los símbolos de DATA (que contienen la información de interés), primero hay que procesar al SIGNAL para saber con certeza cuántos símbolos esperar, y qué modulación y qué tasa de codificación se les aplicó.

Una vez comprendidas las estructuras, hay que analizar cómo operan sobre los bits de fuente, provenientes de capas superiores, los distintos componentes de la síntesis que se emplean para armar los paquetes.

Capítulo 3

Síntesis y demodulación de la señal IEEE 802.11a

Una vez comprendida la estructura general de un paquete OFDM de la IEEE 802.11a, es necesario adentrarse en detalles más específicos que se deben comprender para implementar los bloques de síntesis de cada una de las partes de la señal y los que realizan la demodulación de la misma, que realizan las funciones inversas a los primeros. En el presente capítulo se describen dichos componentes, detallando paso a paso el procedimiento de síntesis y demodulación general de un paquete de señal de este estándar. Además, dichas rutinas se validaron siguiendo un ejemplo que se encuentra detallado en [9, Anexo I] en el que se construye un paquete a partir de los bits provenientes de capas superiores.

También se analizó la importancia que tienen algunos de los bloques de síntesis en el sistema de comunicaciones mediante las simulaciones de transmisión de bits sobre un canal ruidoso.

3.1. Preámbulo

Como se mencionó en el capítulo 2, el Preámbulo es la parte del paquete que se encuentra en su comienzo, y es siempre igual independientemente del tipo de modulación o tasa de transmisión para un BW fijo. La secuencia de 10 símbolos cortos se generan a partir de la secuencia

$$\begin{aligned} S_{-26,26} = \sqrt{13/6} \cdot \{&0,0,1+j,0,0,0,-1-j,0,0,0,1+j,0,0,0, \\ &-1-j,0,0,0,-1-j,0,0,0,1+j,0,0,0,0,0,0,0,-1-j,0,0,0, \\ &-1-j,0,0,0,1+j,0,0,0,1+j,0,0,0,1+j,0,0,0,1+j,0,0\} \end{aligned} \tag{3.1}$$

donde el coeficiente $\sqrt{13/6}$ es introducido en el estándar para normalizar la energía de los símbolos OFDM. Cabe destacar que en dicha secuencia son no nulos solamente los

valores de índices múltiplos de 4 excepto el valor central (de índice 0). Por su parte, para sintetizar los 2 símbolos largos se parte de

$$\begin{aligned} L_{-26,26} = \{&1,1,-1,-1,1,1,-1,1,-1,1,1,1,1,1,1,-1,\\ &-1,1,1,-1,1,-1,1,1,1,1,0,1,-1,-1,1,1,-1,1,-1,\\ &1,-1,-1,-1,-1,-1,1,1,-1,-1,1,-1,1,-1,1,1,1,1\}. \end{aligned} \tag{3.2}$$

Las secuencias $S_{-26,26}$ y $L_{-26,26}$ representan las $N_{ST} = 52$ subportadoras de los símbolos OFDM que, para los campos de SIGNAL y DATA, $N_{SD} = 48$ se usan para transmitir información y $N_{SP} = 4$ son tonos piloto, separadas por un valor nulo en el centro que corresponde a la componente continua. Aplicando la IDFT, se obtienen las muestras en el dominio temporal.

Con el objetivo de realizar las operaciones de forma eficiente desde el punto de vista del costo computacional, se utiliza el algoritmo de la IFFT para evaluar la IDFT. Por este motivo, se extiende la secuencia en el dominio del espectro insertando valores nulos para obtener un número de muestras que sea potencia de 2. En este caso se trabajó con 64, siendo que es la potencia de 2 inmediata superior. Luego, como lo establece la norma, se realiza el mapeo indicado en la figura 3.1, que en términos de frecuencia normalizada del espectro de una secuencia discreta, consiste en mapear las componentes de frecuencia del intervalo $[-0{,}5; 0{,}5]$ al intervalo $[0; 1]$, previo a aplicar la IFFT.

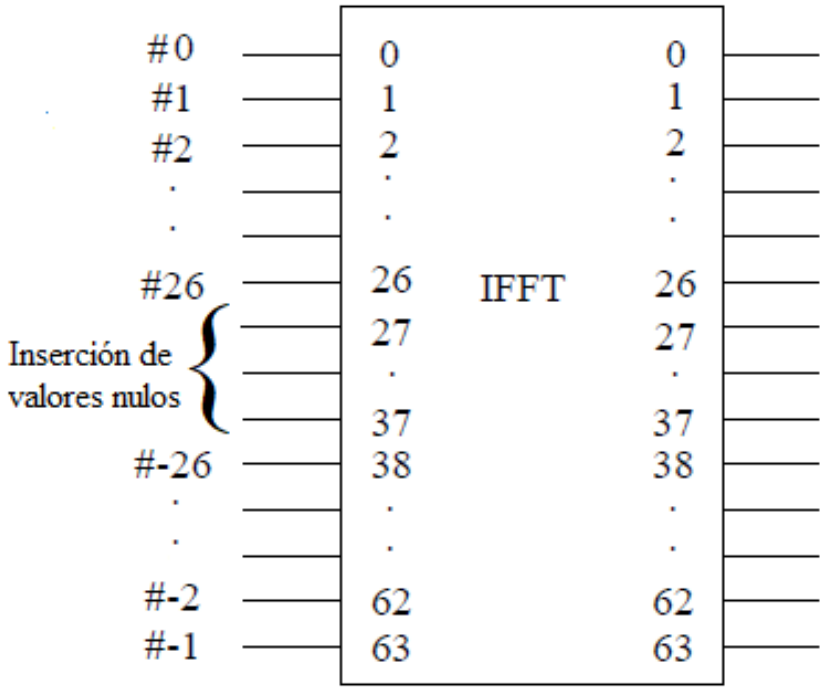


Figura 3.1: Mapeo de la secuencia de 53 subportadoras para obtener las muestras temporales empleando la IFFT.

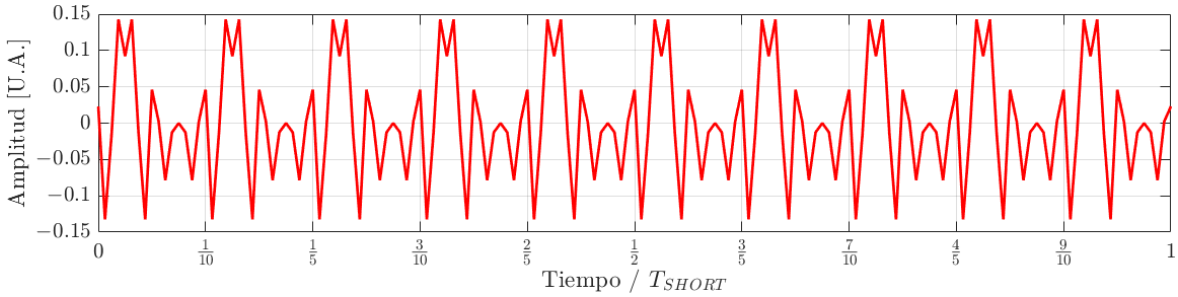
3.1.1. Símbolos cortos

Las muestras resultantes para los símbolos cortos quedan con una periodicidad de $T_{FFT}/4$, lo que representa 16 muestras temporales que constituyen como tal un símbolo corto. Entonces se extraen las primeras 16 muestras obtenidas por la IFFT y se replican 10 veces, lo que da como resultado toda la secuencia de símbolos cortos. Esta sencilla implementación se realizó con éxito y se obtuvieron los valores que brinda [9, Anexo I] en sus tablas I-3 e I-4. En el ejemplo de la norma se añade la primera muestra al final de la secuencia para un total de 161 muestras y se multiplica por la función de ventana

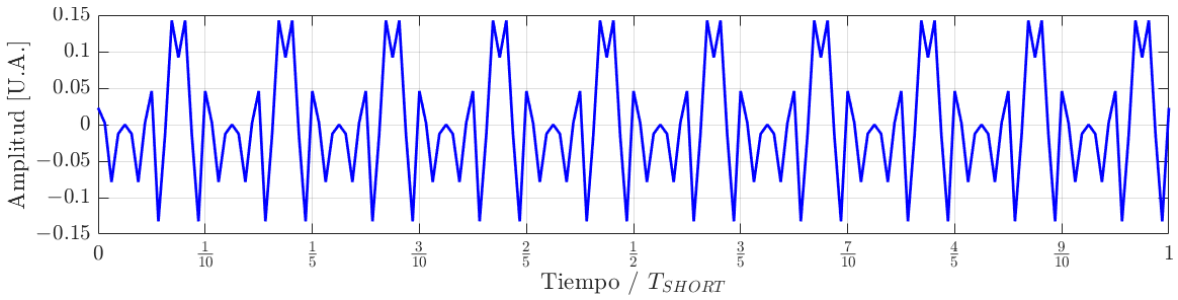
$$W(k) = \begin{cases} 0{,}5 & k \in \{0, 160\} \\ 1 & 1 \leq k \leq 159 \end{cases}$$

aunque el uso de una función de ventana no es obligatorio para el estándar.

En la figura 3.2, se presenta la secuencia de símbolos cortos del Preámbulo en el dominio temporal que se obtuvo de la rutina de generación realizada.



(a) Parte real.



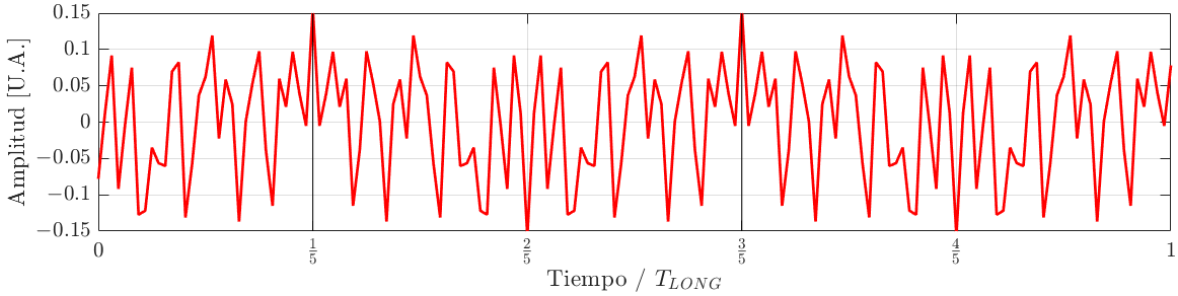
(b) Parte imaginaria.

Figura 3.2: Muestras de la señal temporal correspondiente a la envolvente compleja de la secuencia de símbolos cortos del Preámbulo en banda base.

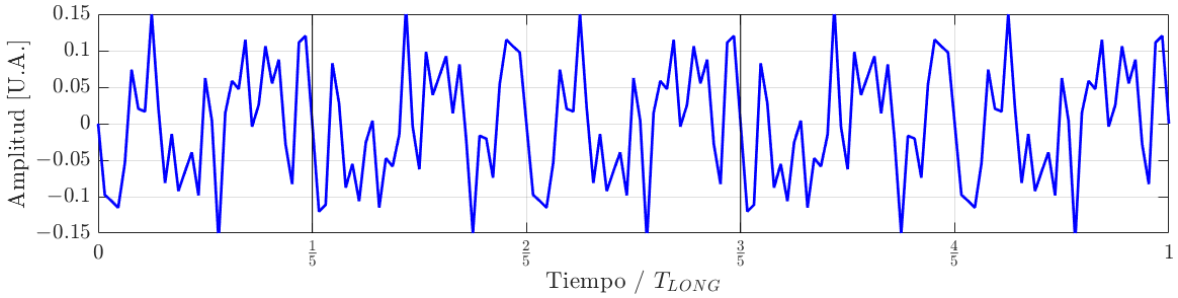
3.1.2. Símbolos largos

Al aplicar a $L_{-26,26}$ el procesamiento descrito la figura 3.1, se obtienen 64 muestras que corresponden a un símbolo largo, lo que representa una duración de T_{FFT}. Para completar la secuencia, se replica una vez las muestras de un símbolo largo y, además, se le agregan al inicio las 32 últimas, que corresponden al prefijo cíclico de duración

T_{GI2}. El resultado se presenta en la figura 3.3, en la que se delimitan el prefijo cíclico y los dos símbolos.



(a) Parte real.



(b) Parte imaginaria.

Figura 3.3: Muestras de la señal temporal correspondiente a la envolvente compleja de la secuencia de símbolos largos del Preámbulo en banda base.

Como se puede consultar en la tabla 2.1, tanto la duración de la secuencia de símbolos cortos como la de los símbolos largos, es de $T_{LONG} = T_{SHORT} = 2 \cdot T_{sym}$, independientemente del BW que se emplee, por lo que el Preámbulo tiene una duración de $T_{PREAMBLE} = 4 \cdot T_{sym}$.

3.2. Síntesis de los símbolos OFDM

Tanto el símbolo SIGNAL como los símbolos del campo DATA se generan por el procesamiento de sus bits de entrada con el esquema de bloques que se muestra en la figura 3.4, exceptuando que para el SIGNAL no se usa el scrambler. Para el caso de DATA, cuando se transmite más de un símbolo OFDM, se indica con las llaves de la figura que los bits a la salida del codificador se separan en N_{sym} bloques de N_{DBPS} bits, se procesa cada bloque en paralelo, y las muestras finales de cada uno, luego de la inserción de sus prefijos cíclicos, se vuelven a agrupar.

Figura 3.4: Esquema de la síntesis del símbolo SIGNAL y de los del campo DATA.

Como resultado, se obtiene la envolvente compleja de la señal en banda base que representa al paquete OFDM, que debe ser modulado en fase y cuadratura y transmitido con alguna frecuencia portadora en la banda de 5 GHz.

Para generar los símbolos en DATA, se utilizan los parámetros de configuración que fija el campo RATE del símbolo SIGNAL, mientras que este último ya tiene fijados por norma sus parámetros de codificación, entrelazado y modulación.

3.2.1. Scrambler

El scrambler es la primera etapa de síntesis de los símbolos de DATA. Este bloque consiste en una máquina de estados con una memoria de 7 bits que, dada una semilla, es capaz de generar una secuencia pseudoaleatoria periódica cuyo período es de 127 bits, repetida hasta tener N_{DATA} bits, la cual se opera bit a bit con el campo DATA empleando una compuerta *xor*. Esta semilla, compuesta por 7 bits, dependerá en cada paquete de parámetros fijados por capas superiores. En la figura 3.5 se observa un esquema de este componente, cuyo polinomio generador es $S(x) = x^7 + x^4 + 1$.

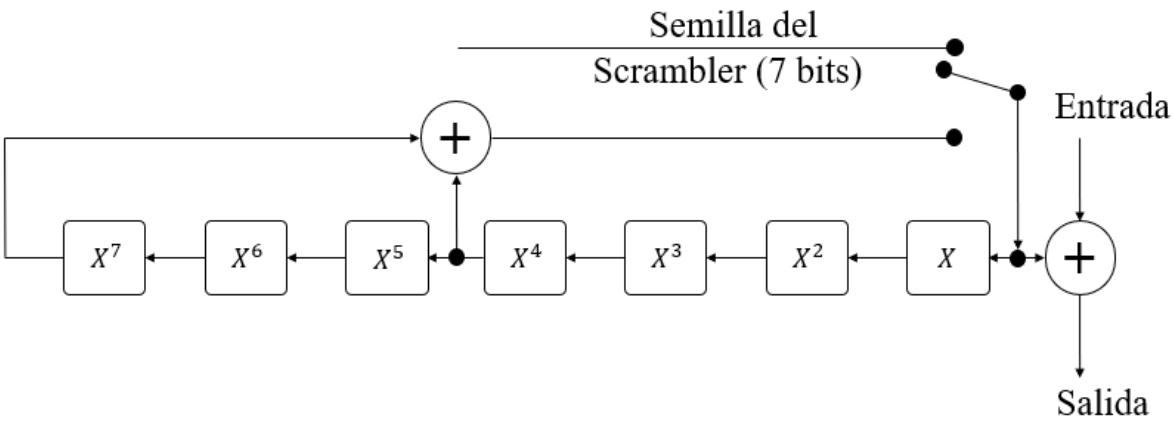


Figura 3.5: Esquema del scrambler del estándar.

Los bits a la salida que quedan en la posición que ocupaban los bits del campo TAIL en DATA, son puestos a '0' nuevamente luego del procesamiento con el scrambler, con la finalidad de que el codificador, detallado en 3.2.2, que recibe los bits a la salida de este, quede en el estado inicial ('000000') después de codificar los bits. En el caso del ejemplo de paquete de [9, Anexo I], la semilla empleada es '1011101'.

3.2.2. Codificador

El codificador que emplea la norma [9, Cláusula 17] y que se muestra en la figura 3.6 es de tipo convolucional. Este devuelve, por cada bit de entrada, 2 bits de salida, con lo que su tasa de codificación es de R = 1/2, y tiene 64 posibles estados (K = 7).

En conjunto con el codificador, es posible usar un esquema de perforado de bits como los mostrados en la figura 3.7 para cambiar la tasa de codificación a los valores 2/3 o 3/4 en función de la tasa de transmisión y del tipo de modulación que se utilicen según lo que se muestra en la tabla 2.3.

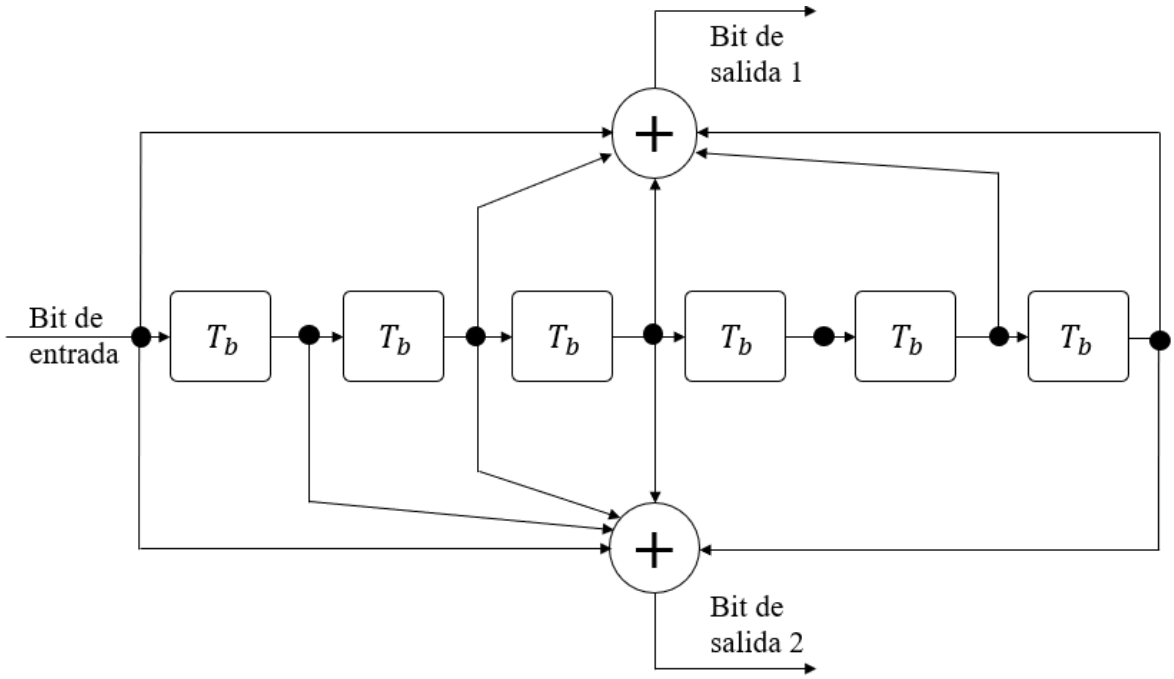


Figura 3.6: Esquema del codificador convolucional que emplea el estándar.

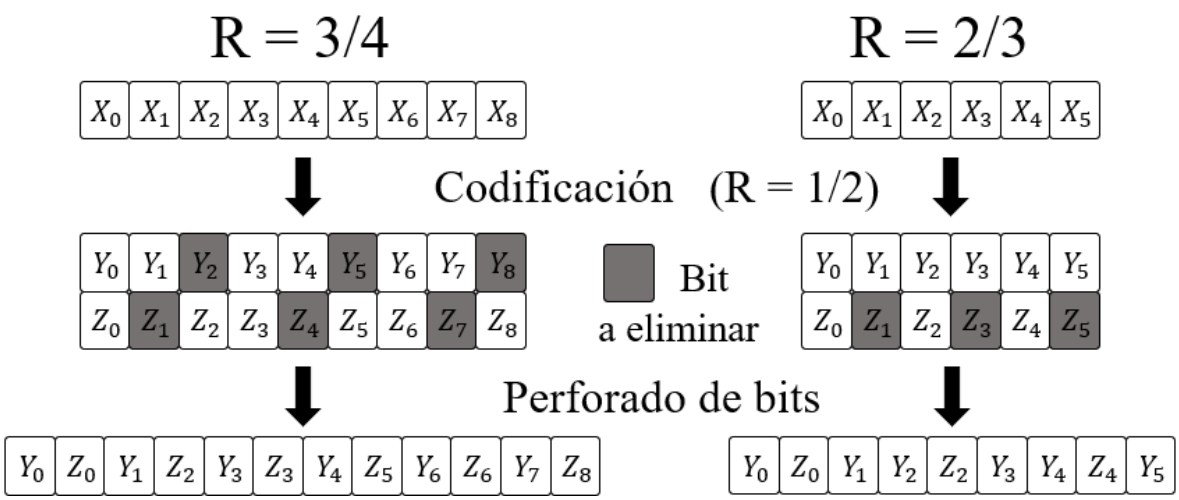


Figura 3.7: Esquemas de perforado propuestos en el estándar.

3.2.3. Entrelazador

Luego de la codificación, se emplea un esquema de entrelazado de bits, que en conjunto con el codificador, tiene el objetivo de mejorar el desempeño general en cuanto a BER (tasa de error de bit, por sus siglas en inglés) como se analiza en la sección 3.5.

El entrelazador del estándar está definido por un par de permutaciones consecutivas, recibe N_{CBPS} bits (un símbolo a la vez) y los devuelve en distintas posiciones. Si el orden de los bits de entrada se denota con un índice $k = 0, 1, ..., N_{CBPS} - 1$ el bit en la k-ésima posición, luego de la primera permutación, estará en la i-ésima posición, donde

$$i = (N_{CBPS}/16) \cdot (k \text{ mód } 16) + \lfloor k/16 \rfloor \qquad k = 0, 1, ..., N_{CBPS} - 1.$$

Para la segunda permutación, se introduce el parámetro $s = \text{máx}\{N_{BPSC}/2, 1\}$ y el bit de la posición i-ésima pasa a estar en la j-ésima donde

$$j = s\lfloor i/s \rfloor + (i + N_{CBPS} - \lfloor 16 \cdot i/N_{CBPS} \rfloor) \text{ mód } s \qquad i = 0, 1, ..., N_{CBPS} - 1.$$

3.2.4. Modulación e inserción de tonos piloto y prefijo cíclico

Para construir la señal en tiempo, como se ha mencionado, se deben tener 64 muestras espectrales que, mediante el algoritmo de la IFFT pasan del dominio de las frecuencias al temporal. Cada símbolo, luego del entrelazado, se divide en $N_{SD} = 48$ bloques de N_{BPSC} bits (obsérvese en la tabla 2.3 que $N_{CBPS} = N_{SD} \cdot N_{BPSC}$) que representan a las subportadoras que transportan información, las que se modulan mapeando esos bloques de bits a números complejos como se indica en la figura 3.8.

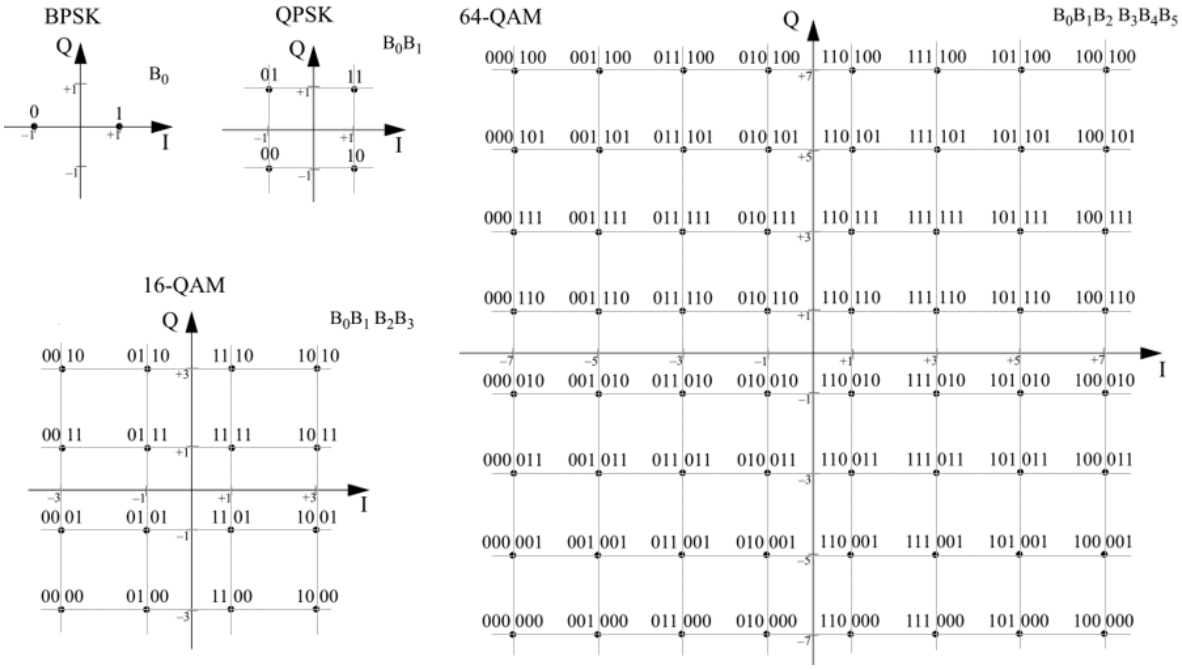


Figura 3.8: Equivalencias entre bits a la salida del entrelazador y las muestras espectrales para las distintas modulaciones empleadas.

Estos números complejos que representan el espectro deben ser normalizados para que todos los símbolos tengan en promedio la misma energía, independientemente del

tipo de modulación empleada. Es para esto, que el estándar define la constante de normalización K_{mod} que multiplica a los números complejos resultantes de la modulación y cuyos valores posibles se muestran en la tabla 3.1.

Modulación	K_{mod}
BPSK	1
QPSK	$1/\sqrt{2}$
16-QAM	$1/\sqrt{10}$
64-QAM	$1/\sqrt{42}$

Tabla 3.1: Constante de normalización de energía correspondientes a cada modulación

Una vez normalizados, se obtienen las $N_{SD} = 48$ muestras espectrales que contienen la información a transmitir. A esta secuencia de números complejos se la enumera con un índice $k = 0, 1, ..., N_{SD} - 1$ para luego mapear las subportadoras a los índices

$$M(k) = \begin{cases} k - 26 & 0 \leq k \leq 4 \\ k - 25 & 5 \leq k \leq 17 \\ k - 24 & 18 \leq k \leq 23 \\ k - 23 & 24 \leq k \leq 29 \\ k - 22 & 30 \leq k \leq 42 \\ k - 21 & 43 \leq k \leq 47 \end{cases}$$

con el fin de insertar los tonos piloto. Como resultado, los índices de la secuencia pasan a ser desde -26 hasta 26 (como en las ya mencionadas $S_{-26,26}$ y $L_{-26,26}$ del Preámbulo). En las posiciones -21, -7, 7 y 21 se insertan las subportadoras piloto y en la posición 0 se introduce una muestra de energía nula. Las portadoras piloto poseen modulación BPSK y sus valores, en dependencia del número de símbolo en el paquete n, iniciando por SIGNAL que este ocupe en el paquete, serán $p_{0,126}[n] \cdot \{1, 1, 1, -1\}$, donde

$$\begin{aligned} p_{0,126} = \{&1,1,1,1,-1,-1,-1,1,-1,-1,-1,-1,1,1,-1,1,-1,-1,1,1,-1,1,1,-1,\\ &1,1,1,1,1,1,-1,1,1,1,-1,1,1,-1,-1,1,1,1,-1,1,-1,-1,-1,1,-1,1,-1,-1,1,\\ &-1,-1,1,1,1,1,1,-1,-1,1,1,-1,-1,1,-1,1,-1,1,1,-1,-1,-1,1,1,-1,-1,-1,\\ &-1,1,-1,-1,1,-1,1,1,1,1,-1,1,-1,1,-1,1,-1,-1,-1,-1,-1,1,-1,1,1,\\ &-1,1,-1,1,1,1,-1,-1,1,-1,-1,-1,1,1,1,-1,-1,-1,-1,-1,-1,-1\} \end{aligned}$$

es una secuencia de 127 elementos que toman valores 1 o -1 y que se genera usando el scrambler descrito en la sección 3.2.1, en donde la semilla que la genera es '1111111' y los bits en '0' son cambiados por el valor $+1$ y los bits en '1' por el valor -1.

Con esto, quedan definidas las 53 subportadoras del espectro y para obtener la señal en tiempo, se opera usando el bloque de la figura 3.1. Una vez hecho esto, basta con repetir al inicio las últimas 16 muestras resultantes de la IFFT, que constituyen el segmento correspondiente al prefijo cíclico, y así quedaría conformada la señal correspondiente al símbolo OFDM en banda base.

3.3. Síntesis del símbolo SIGNAL

El campo SIGNAL consiste de un único símbolo OFDM que su síntesis involucra la mayor parte de las etapas involucradas en los símbolos OFDM generales: la codificación, el entrelazamiento de bits, la modulación de cada subportadora, la inserción de los tonos piloto, la aplicación de la IDFT y la inserción del prefijo cíclico.

En esta sección se analiza la síntesis de este símbolo a partir de las rutinas implementadas, siguiendo el mencionado ejemplo de la norma, para el cual tenemos que RATE = '1011' y el campo LENTGH = '001001100000' (que representa al número decimal 100), con lo que el bit de paridad es '0' como bien se muestra en la figura 3.9.

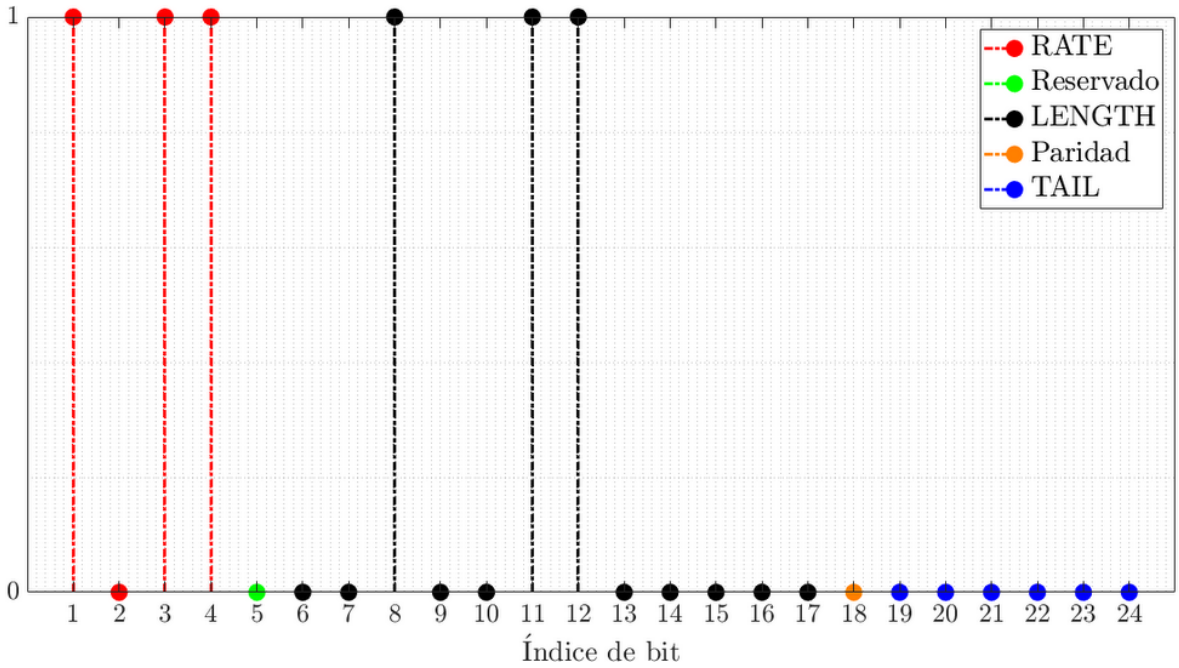


Figura 3.9: Bits de fuente del símbolo SIGNAL del ejemplo.

El campo SIGNAL no emplea ningún esquema de perforado de bits, con lo que la tasa de codificación es de R = 1/2, resultando en $N_{CBPS} = 48$ los bits a la salida del codificador, que para el caso del ejemplo se presentan en la figura 3.10.

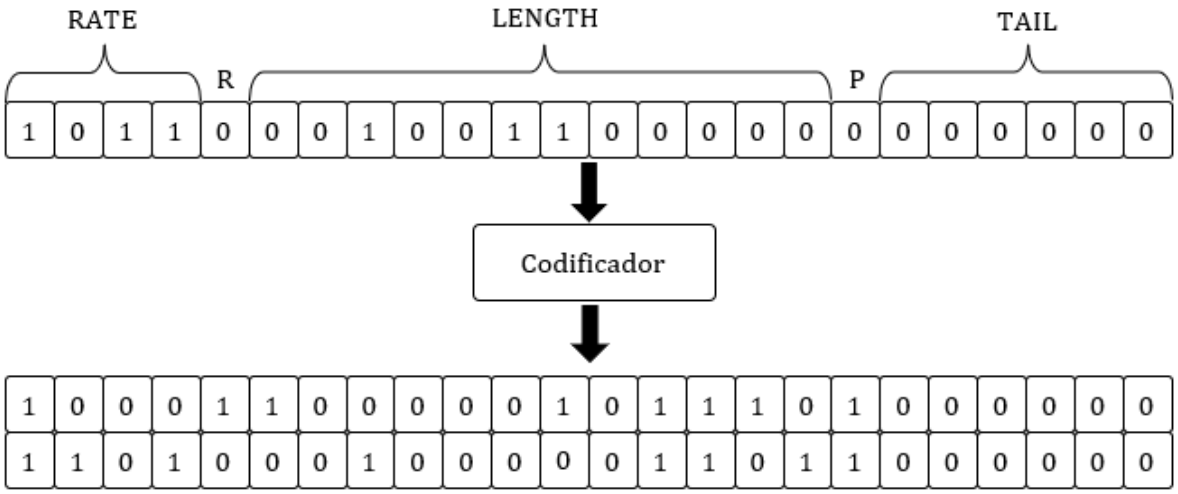


Figura 3.10: Bits codificados para el símbolo SIGNAL del ejemplo. El orden de los bits al pasar a la siguiente etapa es de arriba a abajo y de izquierda a derecha.

El símbolo SIGNAL emplea modulación BPSK, es decir, que $N_{BPSC} = 1$ y $N_{CBPS} = 48$, por lo que las permutaciones resultantes de aplicar las ecuaciones vistas en la sección 3.2.3, quedan como se indican en la figura 3.11, en la que los bits consecutivos pasan a tener distancia 3 entre ellos.

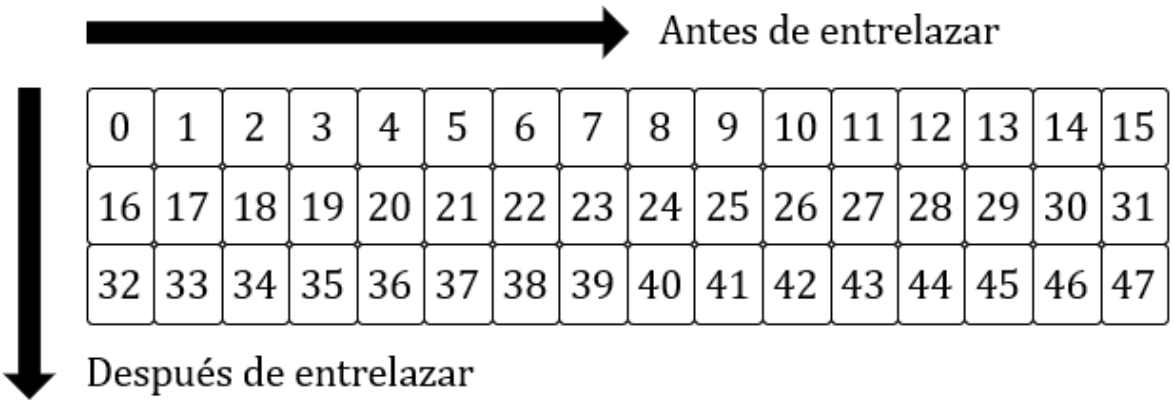


Figura 3.11: Permutaciones de las posiciones en los bits codificados para $N_{BPSC} = 1$ y $N_{CBPS} = 48$, valores correspondientes a la síntesis del símbolo SIGNAL.

Como el primer valor de $p_{0,126}$ es 1, los valores de las subportadoras piloto de este símbolo siempre son $\{1, 1, 1, -1\}$. En la figura 3.12 se observan las 64 muestras que componen el espectro previo a la aplicación de la IFFT con las frecuencias normalizadas en el intervalo $[-0{,}5; 0{,}5]$ donde se señalan los símbolos insertados, y en la figura 3.13 se visualiza la envolvente compleja del símbolo SIGNAL en banda base, y se distingue la parte correspondiente al prefijo cíclico.

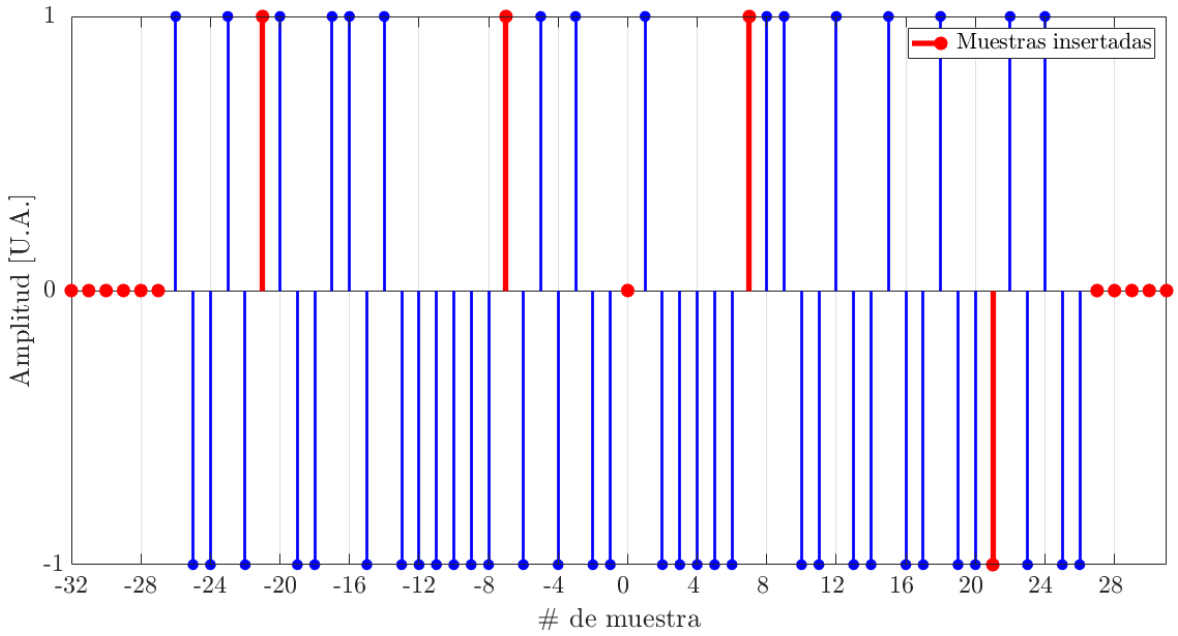
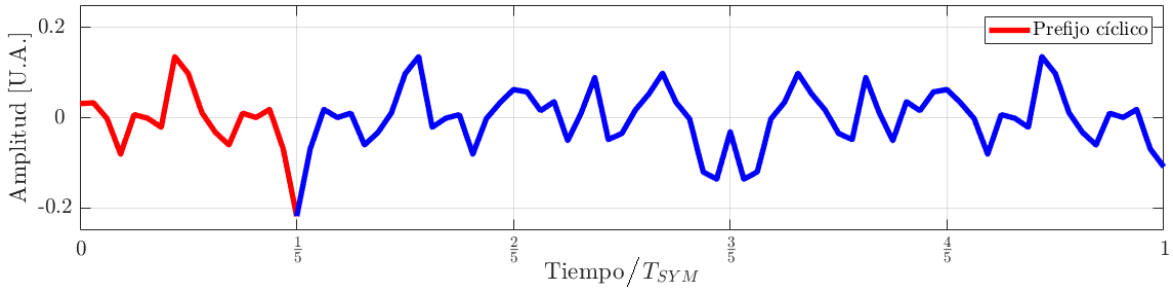
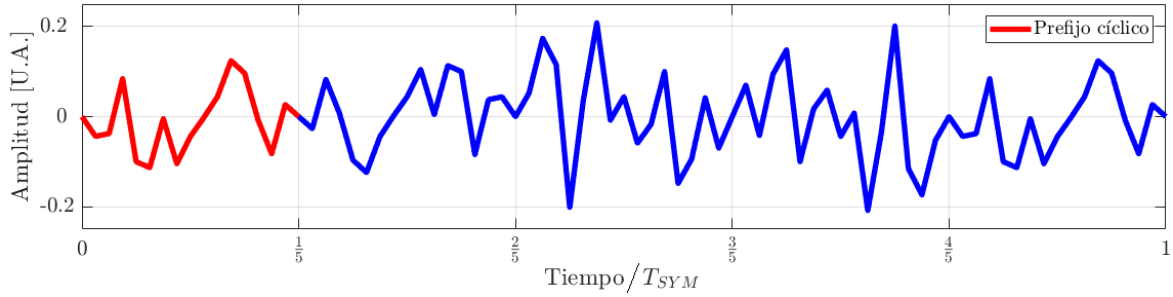


Figura 3.12: Espectro de 64 muestras del símbolo SIGNAL del ejemplo.



(a) Parte real.



(b) Parte imaginaria.

Figura 3.13: Muestras de la señal temporal correspondiente a la envolvente compleja del símbolo SIGNAL en banda base.

3.4. Síntesis de los símbolos del campo DATA

Para la síntesis de los símbolos del campo DATA se emplean por norma los mismos bloques requeridos para el símbolo SIGNAL más el scrambler detallado en la sección 3.2.1. En el ejemplo de la norma, se tienen 100 octetos de PSDU, a lo que se añaden

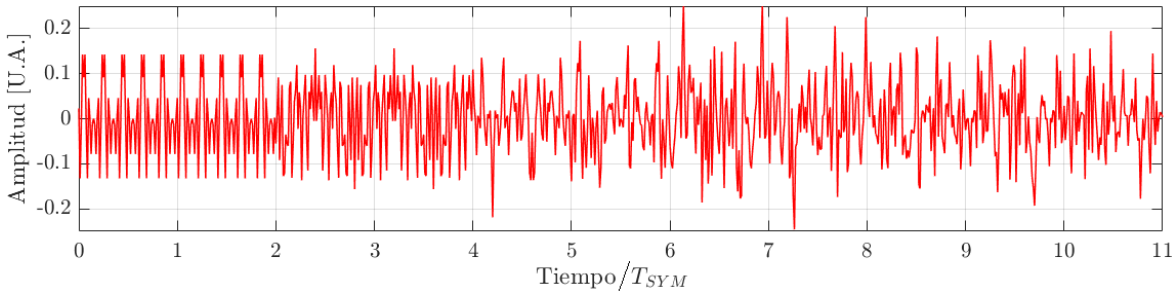
los 16 bits de SERVICE y los otros 6 de TAIL. Como RATE = '1011', según la tabla 2.3, el número de bits de DATA en cada símbolo es de $N_{DBPS} = 144$ por lo que se debe completar con bits de relleno (PAD) al final hasta obtener $N_{DATA} = 864$ ($N_{sym} = 6$).

Luego del scrambler, todo el conjunto de bits es codificado, para lo que se emplea el bloque descrito en la sección 3.2.2, y para el caso del ejemplo analizado en cuestión, se emplea el esquema de perforado de tasa R= 3/4 que se muestra en la figura 3.7, tal y como lo indica la tabla 2.3. Como resultado se obtienen 1152 bits, que se dividen en $N_{sym} = 6$ bloques de $N_{CBPS} = 192$ bits cada uno.

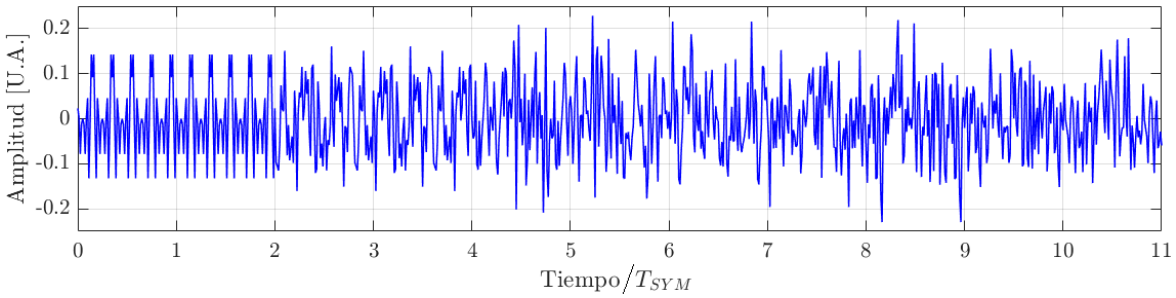
A continuación, se emplea el entrelazador, detallado en la sección 3.2.3, para procesar cada uno de los bloques obtenidos luego de la codificación de manera paralela. Los bloques reordenados resultantes pasan a ser modulados con un esquema 16-QAM, que sigue el gráfico correspondiente a dicha modulación que aparece en la figura 3.8 teniendo en cuenta que $N_{BPSC} = 4$ y, finalmente, cada símbolo es escalado por el factor $K_{mod} = 1/\sqrt{10}$ de acuerdo con lo que se indica en la tabla 3.1.

Los siguientes procedimientos sobre cada símbolo son los mismos que para el símbolo SIGNAL, donde hay que tener en cuenta los valores desde la segunda hasta la séptima posición de la secuencia $p_{0,126}$ para decidir la polaridad de las subportadoras.

Por último, los símbolos son concatenados uno tras otro a continuación del Preámbulo y del campo SIGNAL, con lo que se obtiene la señal completa que representa el paquete en banda base. Dichas muestras sintetizadas a partir del ejemplo abordado en [9, Anexo I], se presentan en la figura 3.14.



(a) Parte real.



(b) Parte imaginaria.

Figura 3.14: Muestras de la señal temporal correspondiente a la envolvente compleja del paquete IEEE 802.11a del ejemplo en banda base.

3.5. Estudio de desempeño de las etapas de síntesis

Al ser transmitidas por un canal ruidoso, las señales se distorsionan, por lo que se producen errores en la demodulación y recuperación de los bits transmitidos. Por esta razón, se suele aplicar algún tipo de codificación a la trama de bits. Además, en los canales inalámbricos, que es en donde se emplea el estándar IEEE 802.11, cabe la posibilidad de operar en desvanecimiento profundo, lo que puede producir errores en ráfagas en conjuntos de bits consecutivos. Es por esto que la codificación suele acompañarse de un reordenamiento estratégico de los bits conocido como entrelazado. Esto permite que, al ser reordenados, los bits con error queden separados para la etapa de decodificación, y si quedan lo suficientemente alejados con respecto a la capacidad de corrección del código, se tenga la posibilidad de corregir estos errores.

En la sección 3.2 se describen los bloques que realizan las operaciones de codificación y entrelazado para los paquetes OFDM del estándar. Posteriormente, se estudia la mejora que estos bloques introducen a la tasa de errores de bits (BER) del sistema buscando la ganancia de código que estos componentes aportan mediante simulaciones de transmisiones de bits, aplicando el esquema de codificación y entrelazado en diferentes condiciones y midiendo la tasa de errores al comparar los bits recibidos con los transmitidos.

3.5.1. Ganancia de código

En las comunicaciones digitales se define como ganancia de código para una determinada BER al valor de la relación E_b/N_0 (energía de bit sobre nivel de densidad espectral de potencia de ruido del canal) cuando dicho código se aplica a un sistema, dividido por la misma relación para el mismo valor de BER cuando este no se aplica. Normalmente tanto el cociente E_b/N_0 como la ganancia de código se expresan en decibeles [dB]. La señal recibida en este caso es de la formada $y[m] = x[m] + w[m]$, donde $x[m]$ son los símbolos transmitidos y $w[m]$ las variaciones por ruido introducidas por el modelo de canal.

Es posible hacer estimaciones de la ganancia de manera teórica para los distintos códigos aplicando suposiciones, como la de tener un canal con AWGN (ruido aditivo blanco gaussiano, por sus siglas en inglés) de distribución gaussiana de media nula y densidad espectral de potencia $N_0/2$, que permiten obtener cotas de la BER asociadas a los diferentes esquemas de codificación en función de la E_b/N_0. En la figura 3.15, tomada de [12], se presentan algunos ejemplos de estas cotas de la BER obtenidas a partir de cálculo teórico. En la misma se destacan las curvas correspondientes al sistema BPSK sin codificación y al que emplea tasa R = 1/2 y K = 7 (decisión dura), que se corresponde con el codificador de la sección 3.2.2. La ganancia que aporta este bloque

al sistema en el punto de BER = 10^{-6}, tasa más baja que se muestra en la gráfica, es G $\approx$ 3,5 dB.

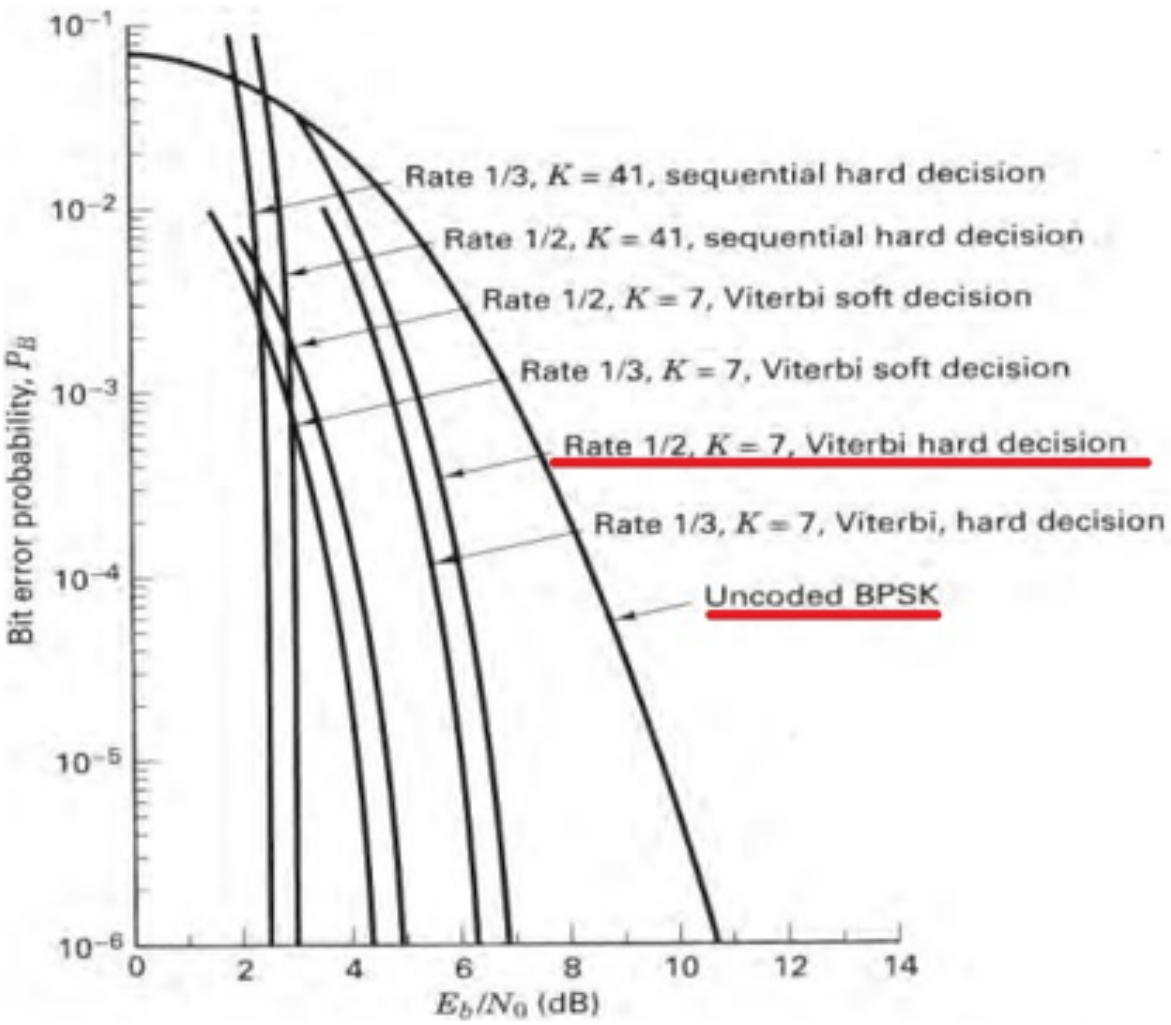


Figura 3.15: Comparación de los valores de BER en función de la E_b/N_0 al usar distintos códigos convolucionales sobre un sistema de modulación BPSK.

Se buscó llegar a este valor teórico mediante la comparación de las curvas marcadas con unas obtenidas mediante la simulación de una transmisión de un gran número de secuencias de bits sobre un canal con AWGN generado aleatoriamente variando su nivel de densidad espectral de potencia, $N_0/2$, manteniendo fija la amplitud de los símbolos modulados con BPSK para simular los distintos valores de E_b/N_0 que se ven en la gráfica de la figura 3.15. Las secuencias generadas para las simulaciones de transmisión fueron las distintas combinaciones de 24 bits con las que es posible generar un símbolo SIGNAL tal como se describió en la sección 2.2.2. Estos símbolos eran transmitidos aplicando previamente la codificación de la sección 3.2.2 para R = 1/2, y empleando modulación BPSK. En la recepción teníamos una muestra de señal más ruido, que, según su signo, se consideraba que representaba un bit en '1' o en '0' (bit de canal), y sobre los que se aplicó el algoritmo de Viterbi para obtener los bits de

fuente. Como estimador de la BER se calculó el cociente entre las cantidades de bits errados y transmitidos en cada caso.

La expresión teórica de la BER para el caso de modulación BPSK (sin codificación) está dada por [13],

$$\mathrm{BER} = Q(\sqrt{2E_b/N_0}) = 0{,}5\,\mathrm{erfc}\,(\sqrt{E_b/N_0}). \tag{3.3}$$

En la figura 3.16 se presenta la curva BER en función de la relación E_b/N_0 obtenida a partir de la simulación del sistema BPSK con codificación, junto con la curva de la BER que se obtiene para el caso sin codificación, que, obtenida de manera simulada, coincide con su expresión teórica, dada por la ecuación 3.3. En dicha figura se incluye, además, una cota teórica que aparece en [12] para la probabilidad de error de bit cuando se emplea el codificador convolucional del estándar. Se observa que los valores de BER obtenidos mediante las simulaciones se mantienen por debajo de dicha cota y se le acercan cada vez más a medida que se aumenta la relación E_b/N_0, cuyo valor para estas curvas difiere uno del otro en aproximadamente 0,5 dB para el punto de menor BER que se muestra.

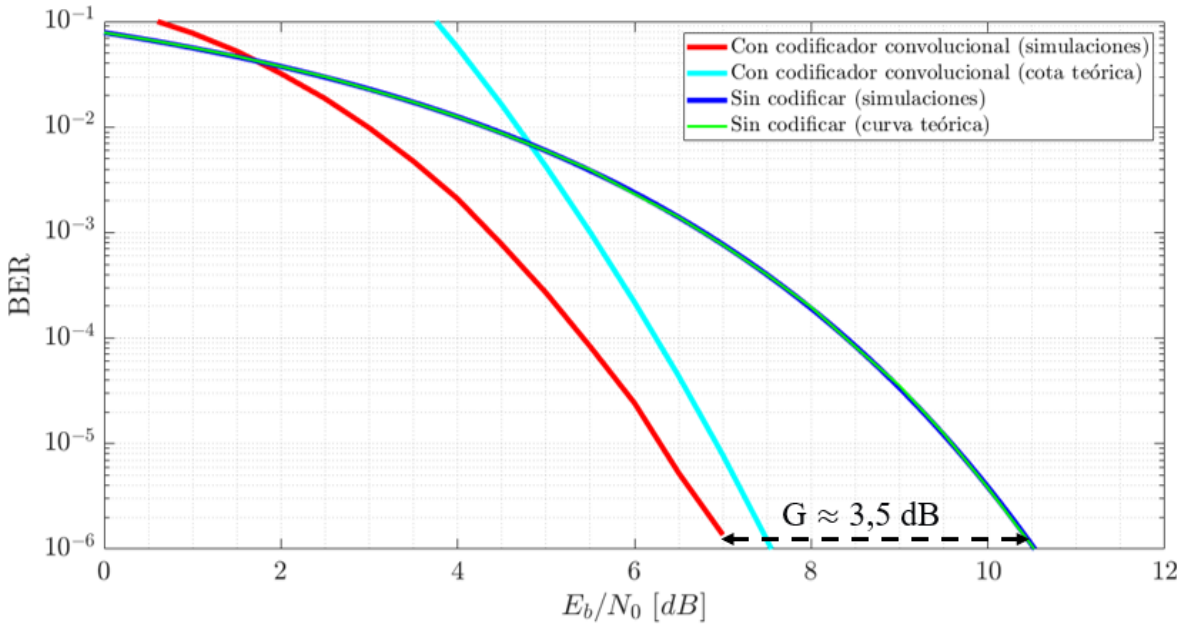


Figura 3.16: Comparación de los valores de BER en función de la E_b/N_0 entre la curva teórica del sistema de codificación que emplea el estándar en cuestión y la obtenida mediante simulaciones.

Estas simulaciones también arrojaron una ganancia de código de G $\approx$ 3,5 dB para un valor de BER $\approx 10^{-6}$, similar a lo que se muestra en la figura 3.15.

3.5.2. Canal con desvanecimiento

Una forma de verificar el efecto que posee el entrelazador sobre el desempeño del sistema es mediante la simulación de transmisiones de tramas de bits en un canal que sigue el modelo de Clarke. Al igual que en la sección 3.5.1, no se empleó todo el esquema de síntesis de OFDM del estándar, sino solamente modulación BPSK en tiempo. Para la transmisión se continuó con el uso de los campos codificados de SIGNAL como señales a transmitir, y se mantiene la codificación de tasa R = 1/2.

Se introduce un desvanecimiento de Rayleigh en el canal que, en conjunto con el ruido, termina afectando a la señal a la salida del mismo, obteniéndose en el receptor $y[m] = h[m] \cdot x[m] + w[m]$, donde $h[m]$ son los valores complejos de respuesta al impulso del canal y la distribución que siguen es $h[m] \sim \mathcal{CN}(0,1)$, mientras que $w[m] \sim \mathcal{CN}(0, N_0/2)$. Esto hace que, sin aplicar codificación, un sistema BPSK con detección coherente tenga una BER [13]

$$\mathrm{BER} = \frac{1}{2}\left(1 - \sqrt{\frac{\frac{E_b}{N_0}}{1 + \frac{E_b}{N_0}}}\right). \tag{3.4}$$

Primero se simuló la transmisión del sistema sin codificar y se comprobó que los valores obtenidos según las simulaciones se ajustaban a la curva teórica de la BER, como se muestra en la figura 3.17, en las que ambas se localizan en la parte superior de la misma.

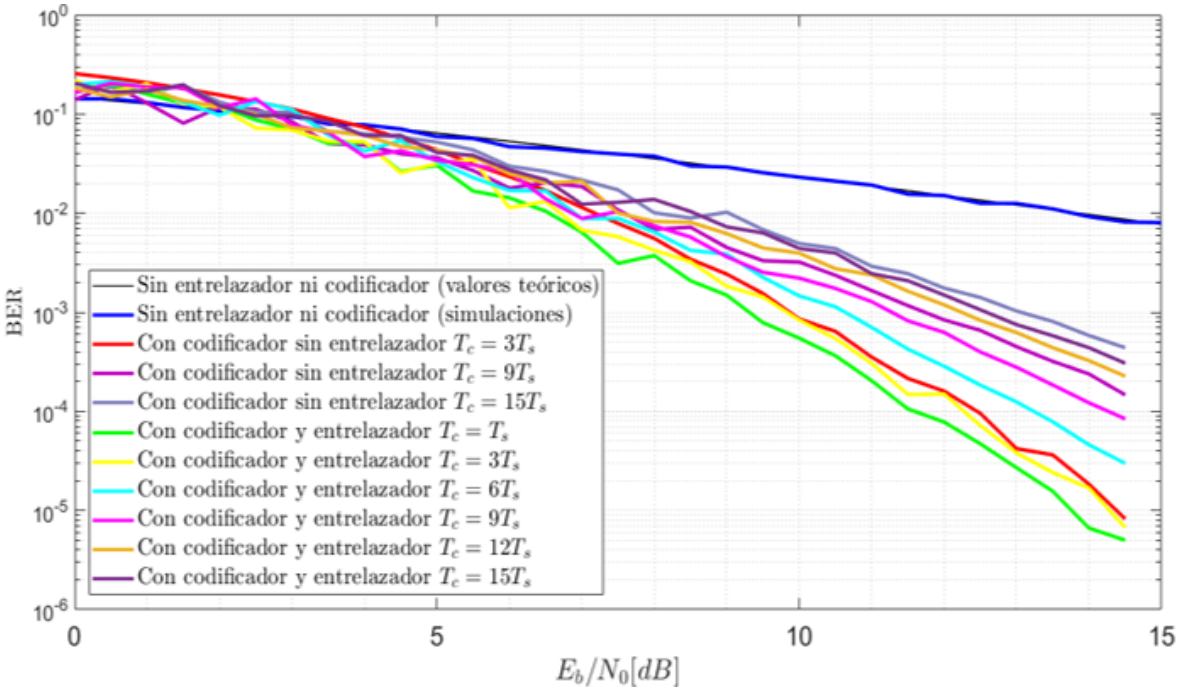


Figura 3.17: Comparación de las curvas de BER para los canales simulados empleando el modelo de Clarke con modulación BPSK y detección coherente.

Solo en esos dos casos no se emplean ni el codificador ni el entrelazador. A continuación, se empleó el modelo de canal de Clarke. El objetivo era tener desvanecimiento del canal que afecte a la señal recibida, lo que llevaría a correlacionar el ruido al momento de la detección, cuando se conoce el canal. Operando sobre la señal recibida $y[m]$, definida por la ecuación

$$y[m] = h[m] \cdot x[m] + w[m], \tag{3.5}$$

conociendo la respuesta de canal $h[m]$ es posible compensar su efecto sobre la señal recibida tomando la parte real del producto de $y[m]$ por $h^*[m]/|h[m]|^2$, es decir,

$$\tilde{x}[m] = \Re\left\{y[m] \cdot \frac{h^*[m]}{|h[m]|^2}\right\} = x[m] + \Re\left\{w[m] \cdot \frac{h^*[m]}{|h[m]|^2}\right\} \tag{3.6}$$

donde $\tilde{x}[m]$ es una aproximación del símbolo BPSK transmitido, $x[m]$, afectada por ruido. El valor de $\tilde{x}[m]$ se compara con 0 para decidir cuál es el valor del bit de canal.

Al valor del símbolo $x[m]$ queda sumado un término que depende de la respuesta del canal, que por ser de Clarke tiene una función de autocorrelación [13] $R_h[n] = \pi J_0(n\pi D_s/W)$, donde W es el ancho de banda de coherencia y D_s es el ensanchamiento Doppler, el cual es inversamente proporcional al tiempo de coherencia T_c. Este último da una medida de la separación temporal que deben tener dos muestras del canal para que la correlación entre ellas se anule.

Lo que se buscaba era observar cómo un cambio en el parámetro T_c afecta a la BER. Para generar la respuesta al impulso del canal de Clarke, se siguió el algoritmo sugerido por [14] y se probaron varios valores de T_c y se simuló transmisión de bits sin aplicar entrelazado (solo codificación) y luego con ambos. Los resultados mostrados en la figura 3.17 para el primer caso, en los que se usaron valores de T_c equivalentes a 3, 9 y 15 veces el tiempo de un símbolo BPSK (T_s) indican que las curvas de BER obtenidas se desplazan hacia valores mayores para una misma relación E_b/N_0. Este resultado tiene sentido ya que, a mayor valor de T_c, mayor correlación hay entre las muestras cercanas correspondientes al término de ruido que queda en la detección, por lo que hay más chances de tener una ráfaga de errores.

Al usar el entrelazador, hay que notar que para el caso en que se usa BPSK este reordena los bits como se indica en la figura 3.11, con lo que la distancia entre los bits consecutivos aumenta a 3, por lo que en este caso se simularon canales con múltiplos de $3T_s$ (y también $T_c = T_s$). Si se comparan las curvas que tienen igual T_c entre las que usan el entrelazador y las que no, se observa una ligera disminución de la BER en el segundo conjunto de curvas para cada uno de los valores de T_c simulados. Sin embargo, dicha mejora no es lo suficientemente significativa de acuerdo a lo esperado. Una de las posibles causas consiste en que la dispersión de las curvas es elevada como

consecuencia de que se empleó un número de corridas relativamente bajo para los valores de probabilidad de error evaluadas en las simulaciones. El motivo es que no se disponía de la capacidad de cómputo que permitiera, no solo aumentar la cantidad de simulaciones para cada valor de E_b/N_0 sino también simular valores mayores de este cociente en un tiempo razonable. Sin perjucio de lo cual, se aprecia la mejora del sistema codificador-entrelazador a medida que T_c se hace cada vez menor.

3.6. Demodulación de la señal OFDM IEEE 802.11a

Con el objetivo de recuperar los bits de fuente a partir de la señal recibida en el dominio del tiempo, es necesario implementar las etapas involucradas en la demodulación, las cuales realizan las operaciones inversas a las analizadas en el proceso de síntesis.

En este caso se supone el paquete ya en banda base sin ruido, distorsiones del canal ni errores de sincronismo y muestreado con una frecuencia igual al ancho del canal OFDM de la señal (20, 10 o 5 MHz), y por tanto, se pueden remover tanto el Preámbulo como los prefijos cíclicos, los cuales no transmiten información como tal.

El esquema completo del demodulador de los símbolos del paquete se muestra en la figura 3.18, el cual recibe como entrada la señal recibida por el receptor llevada a banda base, y devuelve los bits de fuente correspondientes.

Figura 3.18: Esquema de la demodulación del símbolo SIGNAL y de los del campo DATA.

Los pasos para obtener los bits de información de los símbolos, tanto del campo SIGNAL como los de DATA son:

1. Se eliminan las muestras temporales del prefijo cíclico.

2. Se aplica la FFT para obtener el espectro.

3. Se eliminan las subportadoras piloto y las de valor nulo.

4. Se mapean los números complejos de cada subportadora a los bits correspondientes según la modulación empleada, antes corrigiendo con la K_{mod} correspondiente.

5. Se decodifican los bits obtenidos en la demodulación.

6. Se desentrelazan los bits obtenidos de la decodificación.

Cabe destacar que el símbolo SIGNAL debe procesarse primero, debido a que el receptor no sabe a priori las características de la modulación ni la longitud del campo DATA.

Por otro lado, como se describió en la sección 3.4, en el caso de la demodulación de los símbolos del campo DATA, se debe emplear el descrambler como última etapa del procesamiento para la obtención de los bits de fuente.

El bloque desentrelazador no hace otra cosa que aplicar las permutaciones inversas a las de la sección 3.2.3 sobre los bits decodificados para devolverlos al orden que tenían justo después de la etapa de codificación.

$$i = s \cdot \lfloor j/s \rfloor + (j + \lfloor 16 \cdot j/N_{CBPS} \rfloor) \text{ mód } s \quad j = 0, 1, ..., N_{CBPS} - 1$$
$$k = 16 \cdot i - (N_{CBPS} - 1) \cdot \lfloor 16 \cdot i/N_{CBPS} \rfloor \quad i = 0, 1, ..., N_{CBPS} - 1$$

donde j, i y k son los índices antes de la primera permutación, luego de esta y posterior a la segunda respectivamente.

Como bien se ha mencionado, SIGNAL se modula con un esquema BPSK y se codifica con tasa R = 1/2, sin esquema de perforado de bits. Para decodificarlo, se emplea el algoritmo de Viterbi aplicado a los 64 estados que tiene el codificador visto en la sección 3.2.2. Para el caso de los símbolos en DATA, estos se decodifican todos en conjunto y teniendo en cuenta el correspondiente esquema de perforado de bits vistos en la sección 3.2.2, en caso de que el paquete hubiese empleado alguno.

Como descrambler, se usa exactamente el mismo bloque de la sección 3.2.1, ya que al operar bit a bit con una compuerta *xor* sobre secuencias de bits cualesquiera x y s se tiene que $x = x \oplus s \oplus s$ donde x sería la entrada (los bits de fuente de DATA) y s sería la secuencia generada por el scrambler. Es posible obtener la secuencia en el receptor, ya que los primeros 7 bits del campo SERVICE del DATA son '0', y probando con las 127 semillas posibles, se encuentra cuál es la que produce el estado inicial, que corresponde a los 7 primeros bits que llegan a la entrada de esta etapa y usarla para generar la secuencia y procesar todo el conjunto de bits de DATA.

Al aplicar todos los pasos descritos en esta sección sobre la envolvente compleja en banda base que aparece en la figura 3.14, fue posible recuperar con éxito los bits de fuente usados para generar el paquete IEEE 802.11a tratado por [9, Anexo I].

3.7. Conclusiones

Se ha estudiado el proceso de síntesis de un paquete OFDM del estándar IEEE 802.11a examinando las operaciones que realizan sobre los bits a transmitir cada uno de los bloques que intervienen en dicho proceso. Estos fueron probados con un ejemplo concreto que aparece en la norma en el apéndice I, en donde se genera todo el paquete

(Preámbulo, SIGNAL y DATA) paso a paso y se muestran los valores de los bits y las muestras en cada una de las etapas de síntesis, los cuales fueron obtenidos en cada etapa de manera exitosa. Dados los bits de la PSDU, con el esquema de síntesis implementado es posible generar los paquetes OFDM con cualquiera de las configuraciones de transmisión que admite esta cláusula de la norma.

Siguiendo esta misma línea, se implementó el esquema correspondiente de demodulación completo y se obtuvieron con éxito los bits de fuente del paquete del ejemplo sintetizado, con lo que se tienen las implementaciones necesarias para trabajar en capa física suponiendo un canal ideal.

Asimismo, se simularon varias transmisiones de tramas de bits en las que se obtuvo la ganancia de código que aporta el esquema de codificación con entrelazado de bits a un esquema de comunicaciones digitales simple como lo es el de modulación con BPSK, coincidiendo con el valor encontrado en la bibliografía. Además, se comprobó que el aumento de distancia entre bits consecutivos que surge con el entrelazador es capaz de hacer disminuir la BER del sistema, lo cual da a entender que estos bloques tienen una importancia significativa en la comunicación de los dispositivos que usan el estándar IEEE 802.11a.

Aún resta analizar los efectos no deseados que introduce el canal, y que es necesario que se corrijan en la capa física, previo a la aplicación del esquema de demodulación implementado, como lo son por ejemplo errores de sincronismo en el instante de muestreo o de frecuencia en el oscilador local del receptor.

Capítulo 4

Demodulación de mediciones reales

Una vez implementados los esquemas completos de síntesis y demodulación, se procede a buscar que estos alcancen el objetivo de demodular una señal real de IEEE 802.11a y obtener sus bits de fuente.

Se cuenta con las muestras en banda base de paquetes de wifi adquiridos en el grupo de trabajo con un Dispositivo de Radio Definido por Software USRP, de la empresa National Instruments. Las mediciones corresponden a señales IEEE 802.11a con un ancho de canal de 20 MHz adquiridas con una tasa de muestreo de $f_s = 40$ MHz. Estos han pasado por un canal inalámbrico real, lo que termina afectando a las muestras de la señal adquiridas, y que, por tanto, se deben corregir estos efectos previamente a la demodulación en cada uno de los paquetes.

Para realizar las correcciones pertinentes, se parte del Preámbulo, el cual es una estructura siempre presente e invariante que aparece al inicio en todos los paquetes. Mediante la comparación de la forma del Preámbulo original y el adquirido en el receptor se pueden estudiar los efectos del canal sobre la señal y plantear un modelo de este que permita encontrar las correcciones que se deben realizar sobre las muestras para que este se asemeje lo máximo posible al estándar y aplicar estas mismas correcciones a las otras partes del paquete para demodular correctamente todos los símbolos.

4.1. Descripción de los datos

El esquema experimental se detalla en la figura 4.1, la cual muestra los componentes empleados en el proceso de adquisición de la señal, los cuales son:

- El Dispositivo de Radio Definido por Software USRP 2953, de la empresa National Instruments, que se muestra en la figura 4.1c a la que se conectó una antena VERT como la que se observa en la figura 4.1d.

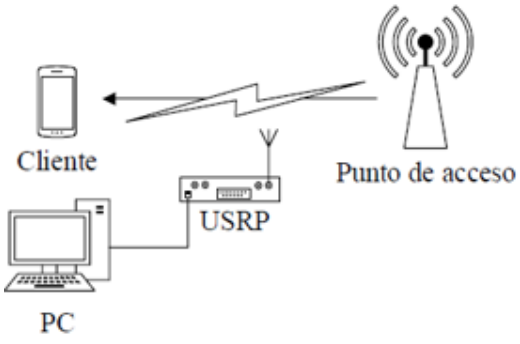
- Una computadora conectada al USRP que permite la configuración del dispositivo y realizar el almacenamiento de las muestras adquiridas.

- Un teléfono celular como cliente que recibe las señales wifi correspondientes a la comunicación con un punto de acceso.

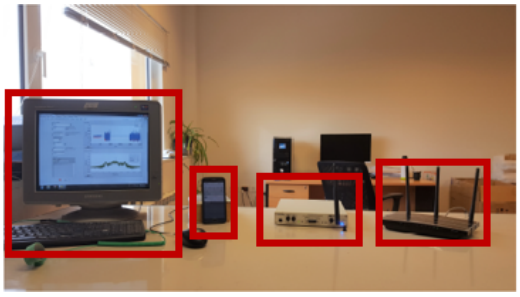
- Un router TP Link N750 como el que se observa en la figura 4.1e usado como punto de acceso, y que se configuró con los parámetros que muestra la figura 4.2 (frecuencia portadora de $f_c = 5745$ MHz y ancho de canal de BW = 20 MHz).

Para configurar el URSP, se empleó una rutina desarrollada con el software *LabView* y se fijó un número de muestras a tomar de $N_{samp} = 20000$ con una frecuencia de muestreo de $f_s = 40$ MHz (duración de 0,5 ms). Las muestras correspondientes a las componentes I y Q en banda base fueron almacenadas en la computadora.

Al analizarlas, se encontró que existía una componente continua que, como ya se ha visto en la sección 3.2.4, no se corresponde con el valor de energía 0 que se fija en el centro del espectro de los símbolos OFDM en banda base para el estándar IEEE 802.11a. Para comprobarlo, el equipo que realizó las mediciones colocó una carga de 50 Ω en el puerto donde estaba previamente conectada la antena. Las curvas del nivel de continua para las componentes I y Q de la señal, denotadas como I_{DC} y Q_{DC} en la figura 4.3, se corresponden con el nivel de continua detectado en las muestras adquiridas. Esto demuestra que es un efecto agregado por el dispositivo de recepción, el cual se corrige al restar en cada componente su nivel de continua, lo que se muestra en la figura 4.3.



(a) Diagrama del esquema experimental.



(b) Mesa de medición.

(c) SDR USRP 2953.

(d) Antena VERT 2450.

(e) Router TP-Link N750.

Figura 4.1: Esquema experimental y dispositivos empleados en la adquisición de datos.

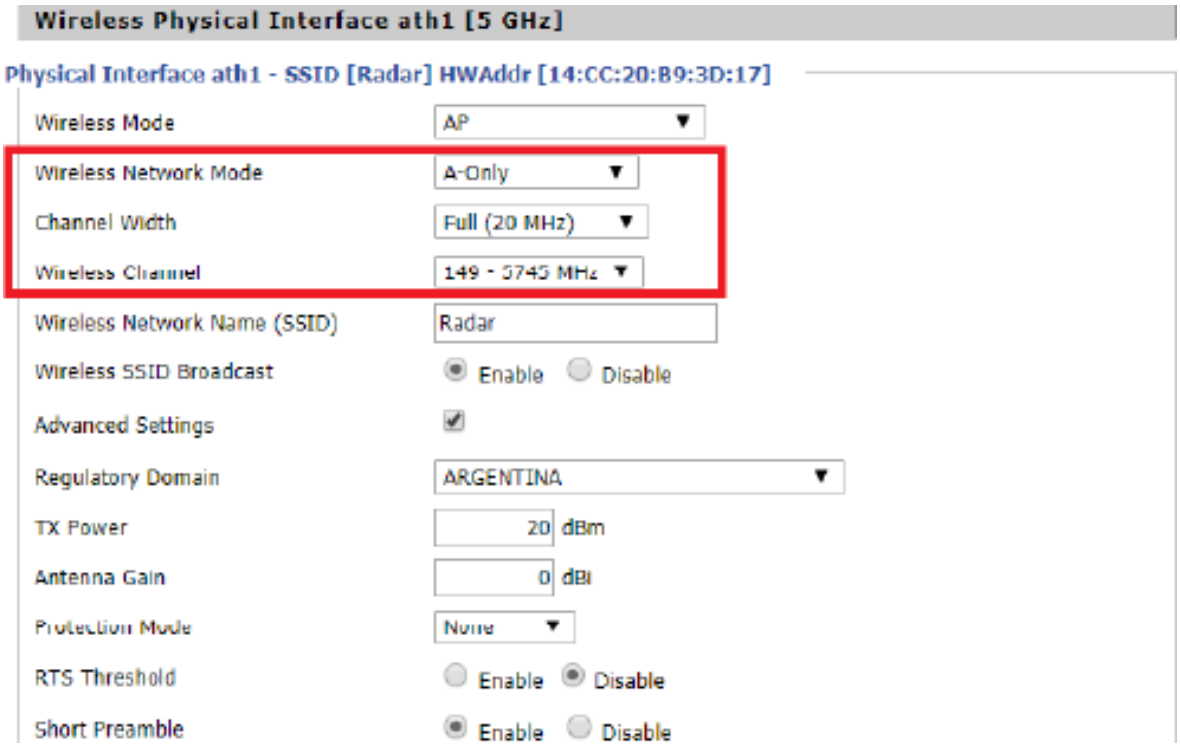


Figura 4.2: Configuración del router para la comunicación.

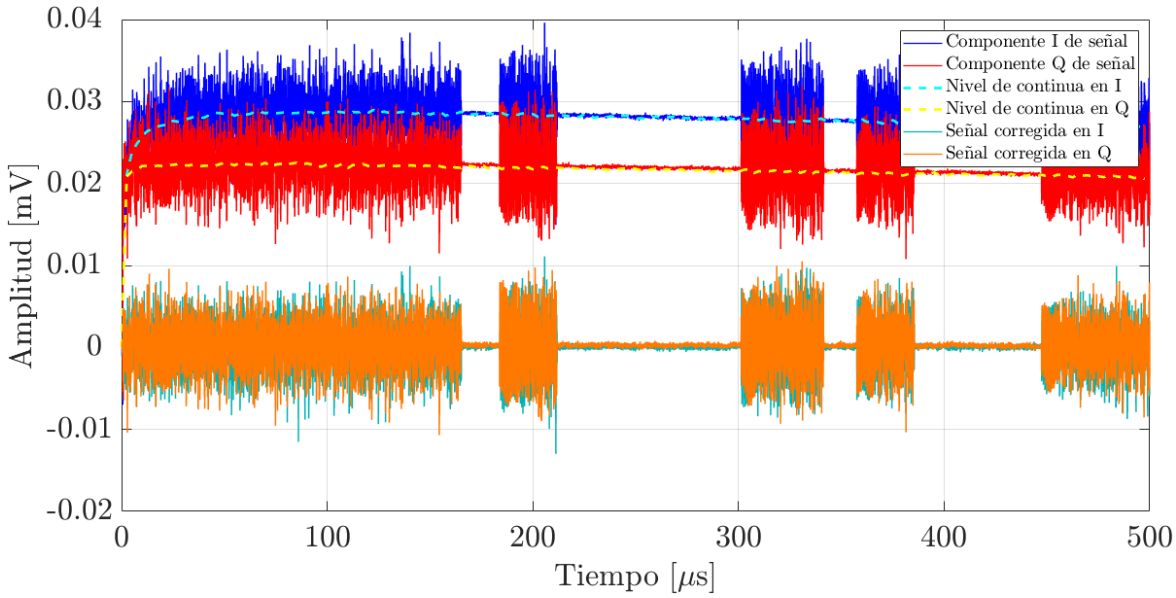


Figura 4.3: Muestras adquiridas con el USRP correspondientes a las componentes I y Q de la señal en banda base y corrección del nivel de continua en las mismas.

Al hacer zoom en la región centrada en los 200 μs se reconoce un paquete de señal, que se muestra en la figura 4.4. Si se observa detenidamente, es posible apreciar que su primera parte presenta una estructura repetitiva que se asemejan a los 10 símbolos cortos del Preámbulo pero distorsionados por los efectos del canal y los posibles errores de sincronismo. Otros paquetes que se pueden distinguir por sus símbolos cortos se encuentran alrededor de los 300, 360 y 450 μs en la gráfica de la figura 4.3. Cabe

aclarar que en los capítulos 4 y 5 se verán en detalle los resultados obtenidos con este paquete en particular ilustrando el procedimiento que, en el caso general, se aplicaría también a otros paquetes, y que en el capítulo 6 se hace lo mismo para el paquete que le sigue, que tiene características distintas.

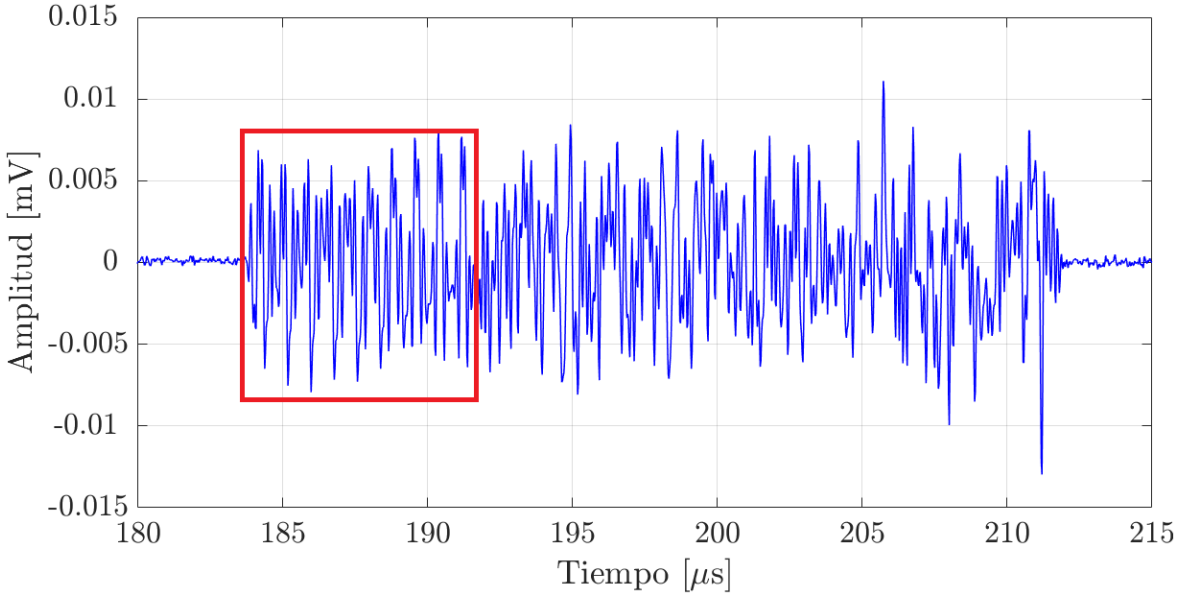


Figura 4.4: Detalle de la forma de onda de la componente I de la señal en banda base de uno de los paquetes adquiridos. Se resalta la secuencia de símbolos cortos del paquete.

4.2. Detección y corrección de errores

Al transitar por un canal inalámbrico, cualquier señal $x(t)$ sufre un deterioro producto de diversos factores. Una manera sencilla de representar a la señal recibida en forma matemática es

$$y(t) = (x(t) \star h(t))e^{-j2\pi\Delta ft} + n(t) \tag{4.1}$$

donde $h(t)$ es la respuesta impulsiva del canal, Δf es el error de sincronismo de frecuencia de portadora en el receptor y $n(t)$ es el ruido del canal, el cual se supondrá del tipo AWGN en el rango de frecuencias de interés alrededor de la portadora.

4.2.1. Detección

Para conocer la primera muestra del Preámbulo y, por tanto, del paquete OFDM, se pretende usar al primero como señal de referencia, computando la correlación de la secuencia de símbolos cortos sintética ideal, con todo el registro de datos. De esta manera, se espera obtener valores máximos locales en el módulo de la correlación en los instantes de inicio de cada paquete adquirido. En la figura 4.5 se muestra el módulo

de la correlación, donde se observan "picos" correspondientes a máximos locales de dicha función. La comparación de la correlación con la señal en el dominio del tiempo que se presentó en la figura 4.3, permite corroborar que esos máximos se dan en las regiones que se identificaron paquetes, siendo el de mayor magnitud el que corresponde al paquete analizado en detalle en la figura 4.4. Cabe remarcar que, si bien el análisis anterior permite identificar la ubicación de los paquetes, eso no quita que pueda existir algún error en la muestra exacta de inicio de cada uno de ellos.

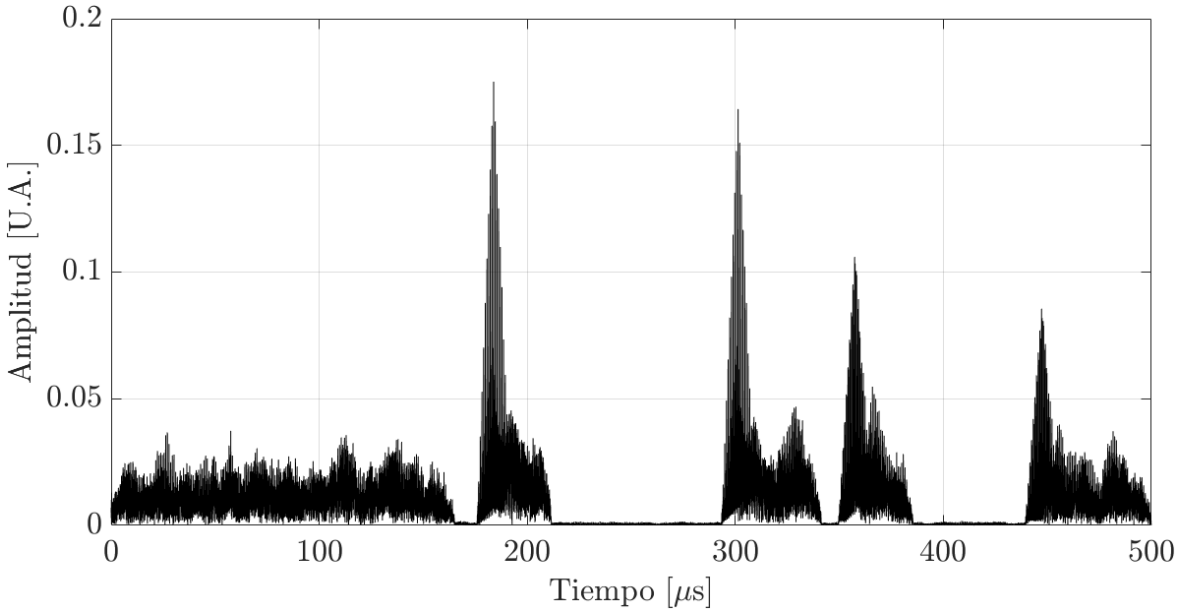


Figura 4.5: Módulo de la correlación de las muestras adquiridas con la secuencia de símbolos cortos.

4.2.2. Sincronismo de frecuencia

El Preámbulo del estándar no solo sirve de señal de referencia para la detección, sino también para corregir ciertos errores que produce la transmisión. Uno de los más significativos es el de sincronismo en la frecuencia de portadora, siendo necesario estudiar qué efecto tiene este tipo de error sobre la señal de referencia. Es importante aclarar que en esta etapa del procesamiento solo se emplea la secuencia de símbolos cortos como señal de referencia. Además, se supone que el valor de Δf permanece invariante para todos los símbolos de un mismo paquete.

Se procedió a generar la señal de referencia y se multiplicó a la señal en tiempo por una exponencial como se indica en la ecuación 4.1, fijando el valor $\Delta f = 20$ kHz. En la figura 4.6 se aprecian las diferencias que se producen debido al Δf, siendo más notorias en los últimos símbolos, ya que para distintos instantes de tiempo, el valor de la fase que introduce se va incrementando, por lo que ahora los símbolos cortos dejan de ser iguales. Recordando que 4 símbolos cortos de la secuencia tienen la duración de un símbolo OFDM sin prefijo cíclico, hay que remarcar en que esas diferencias en los

símbolos cortos se traducen en cambios en las subportadoras del espectro en función de qué conjunto de 4 símbolos se usen para calcularlo (los símbolos $1 \sim 4$ son muy distintos a los $7 \sim 10$).

En la figura 4.7 se muestra una comparación entre el espectro ideal de los símbolos cortos, donde sus partes real e imaginaria son iguales, y el obtenido del ejemplo con $\Delta f = 20$ kHz seleccionando los símbolos $3 \sim 6$, en la que se observa cómo las subportadoras cambian su fase.

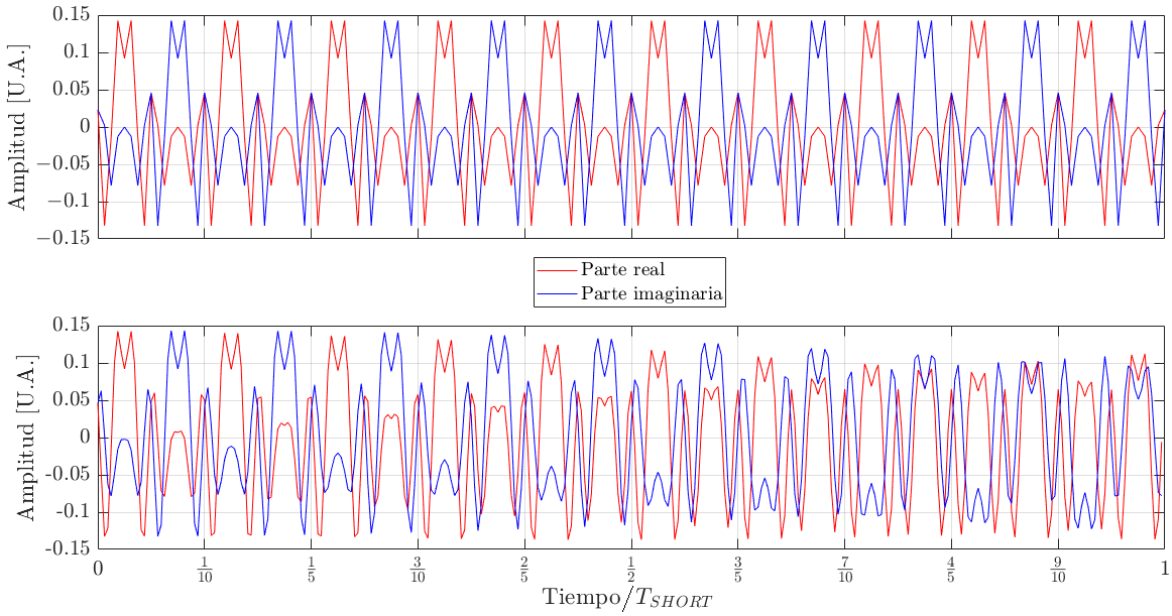


Figura 4.6: Comparación entre las secuencias de símbolos cortos sintéticos con $\Delta f = 0$ (arriba) y con $\Delta f = 20$ kHz (abajo).

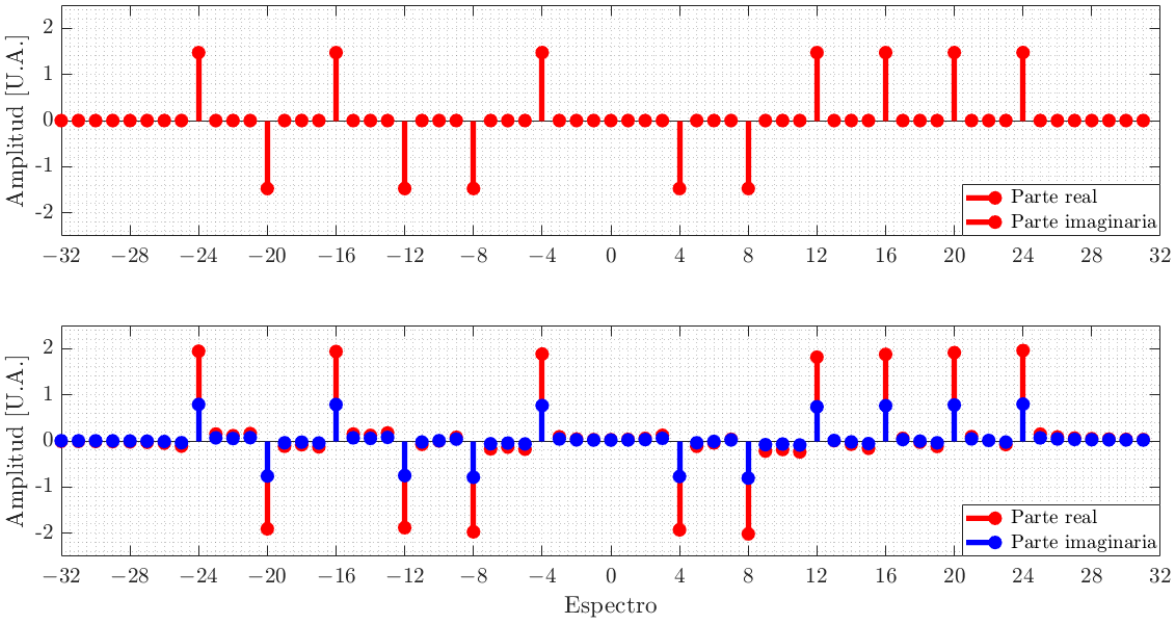
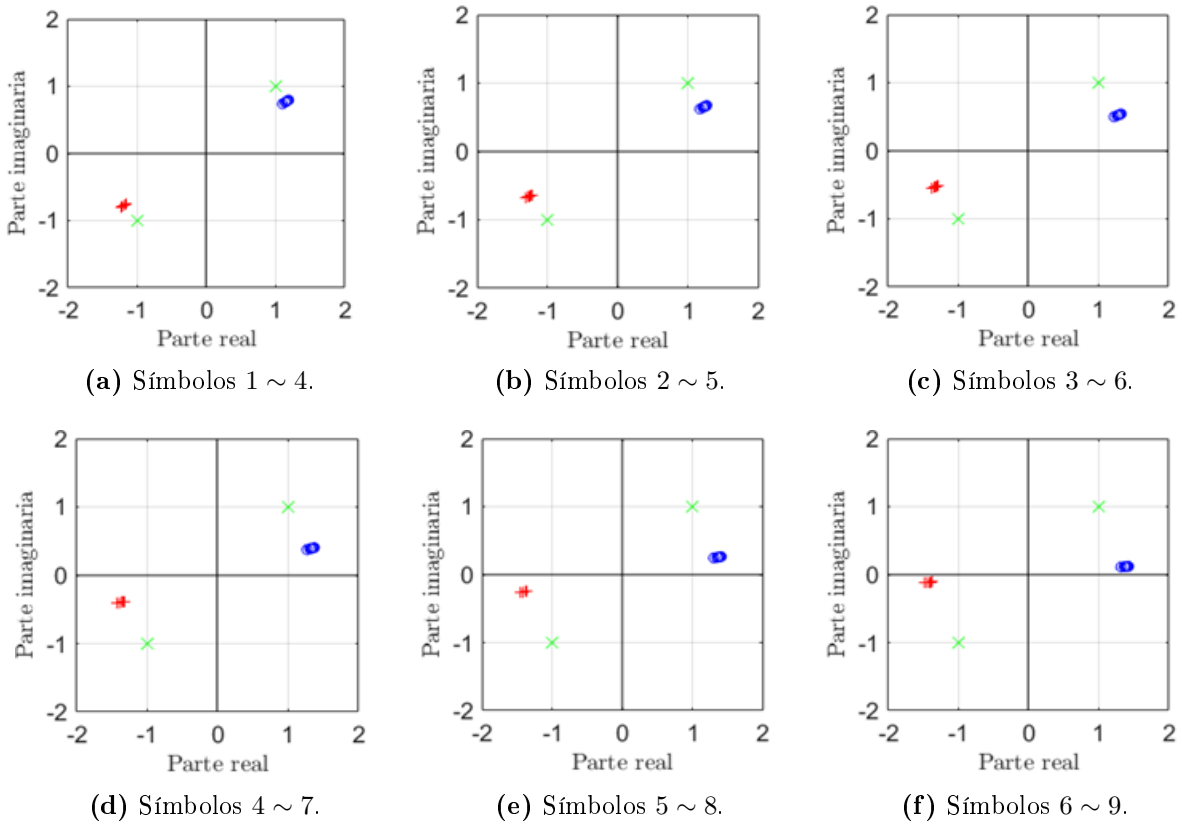


Figura 4.7: Comparación entre los espectros de símbolos cortos con $\Delta f = 0$ (arriba), donde las partes real e imaginaria coinciden, y con $\Delta f = 20$ kHz usando los símbolos $3 \sim 6$ (abajo).

Una manera de apreciar mejor el cambio de fase de las subportadoras consiste en observar el espectro modificando los símbolos cortos con los que se evalúa, seleccionando de los que menos cambian con respecto a los ideales a los que más se diferencian.

En la figura 4.8 se presentan en el plano complejo las coordenadas de las subportadoras obtenidas para los distintos conjuntos de símbolos cortos cuando existe un error de frecuencia de $\Delta f = 20$ kHz, junto con los valores ideales de las coordenadas dados por la secuencia $S_{-26,26}$ (estas últimas divididas por el factor de normalización $\sqrt{13/6}$).



(a) Símbolos $1 \sim 4$. **(b)** Símbolos $2 \sim 5$. **(c)** Símbolos $3 \sim 6$.

(d) Símbolos $4 \sim 7$. **(e)** Símbolos $5 \sim 8$. **(f)** Símbolos $6 \sim 9$.

Figura 4.8: Constelación del espectro de símbolos cortos para $\Delta f = 20$ kHz. En azul, las subportadoras que valen $1+j$ al eliminar el valor de normalización $\sqrt{13/6}$ en la secuencia $S_{-26,26}$ y en rojo, las subportadoras que valen $-(1+j)$.

Como se aprecia en la imagen anterior, a medida que se mueve la ventana de símbolos cortos de la secuencia usados en el cálculo del espectro, la rotación de la constelación crece, alejándose de los puntos marcados que representan el caso ideal sin error en frecuencia. Entonces, es posible comprobar que este problema está presente en el paquete en análisis si se grafica su constelación de manera similar, calculando el espectro con distintos conjuntos de símbolos cortos consecutivos y observando si se produce esta rotación en los valores de las subportadoras.

La secuencia de símbolos cortos del paquete adquirido se muestra junto a la ideal en la figura 4.9, donde se ven ciertas similitudes en la forma de las partes real e imaginaria de algunos de los símbolos mientras que hay otros que lucen muy distorsionados.

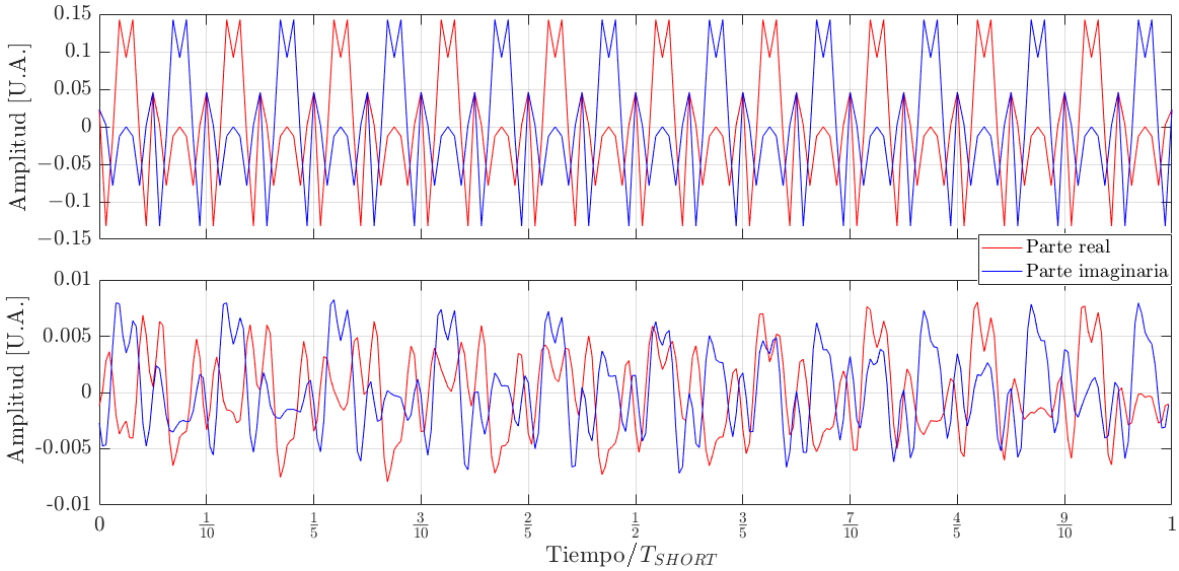
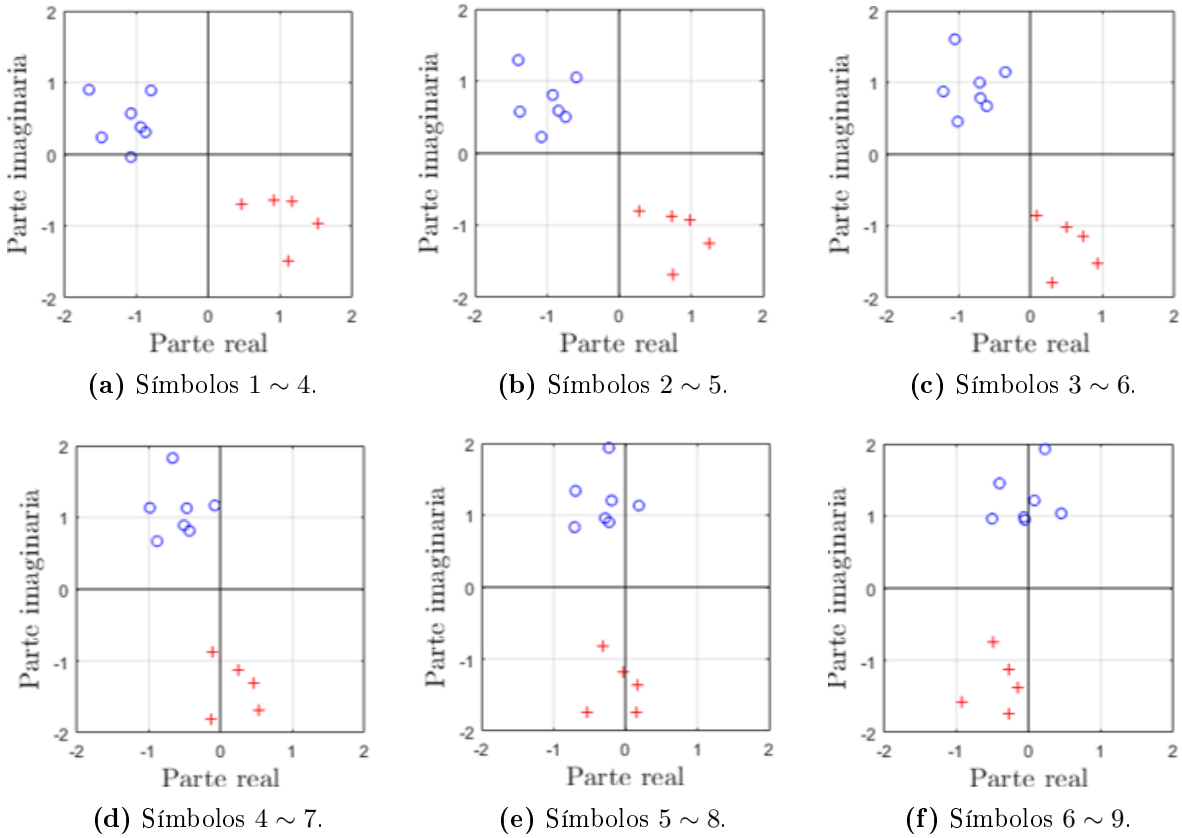


Figura 4.9: Comparación entre los espectros de símbolos cortos ideales (arriba) y los correspondientes al paquete adquirido (abajo). $T_{SHORT} = 8$ μs para canales de 20 MHz.

Siguiendo el procedimiento anterior, se calculó el espectro de los símbolos cortos del paquete adquirido, variando el conjunto de 4 símbolos consecutivos con los cuales se opera, obteniendo las constelaciones mostradas en la figura 4.10.



(a) Símbolos $1 \sim 4$. **(b)** Símbolos $2 \sim 5$. **(c)** Símbolos $3 \sim 6$.

(d) Símbolos $4 \sim 7$. **(e)** Símbolos $5 \sim 8$. **(f)** Símbolos $6 \sim 9$.

Figura 4.10: Constelación del espectro de símbolos cortos del paquete adquirido. En azul, las subportadoras que corresponden a $1+j$ según $S_{-26,26}$, en rojo, las que corresponden a $-(1+j)$.

Como puede verse, de manera similar a la figura 4.8, este efecto de rotación de los puntos en el plano complejo está presente en el paquete analizado, lo que indica que existe un error de sincronismo de frecuencia significativo.

Una manera de buscar el valor de Δf es generar señales de referencia que consistan en secuencias sintéticas de símbolos cortos con distintos errores de frecuencia y correlacionarlas con el registro de datos. Luego, se comparan los máximos de las distintas correlaciones en la ubicación del paquete correspondiente, se selecciona el mayor de dichos máximos y se establece que el error de frecuencia es el que corresponde a la señal de referencia que dio lugar a esa correlación. Los valores de Δf usados para generar estas secuencias, están en el rango $[-100 \sim 100]$ kHz con un espaciado de 1 kHz. Esto produjo un máximo de correlación en 46 kHz. En pos de contar con un valor más preciso del error de frecuencia, se repitió el proceso reduciendo el intervalo al rango $[45 \sim 47]$ kHz, con un espaciado de 10 Hz, lo que arrojó un estimado del error de frecuencia de $\Delta f = 46{,}43$ kHz. En la figura 4.11 se presentan los valores de los máximos de la correlación para cada valor de Δf y se destaca el máximo correspondiente a 46,43 kHz.

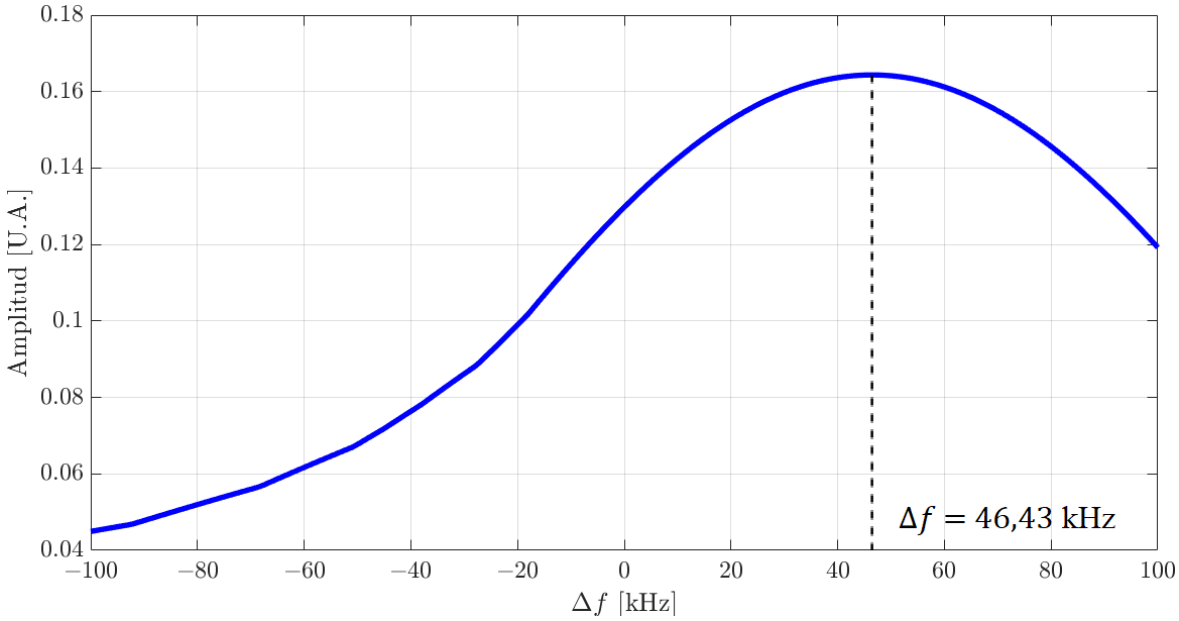
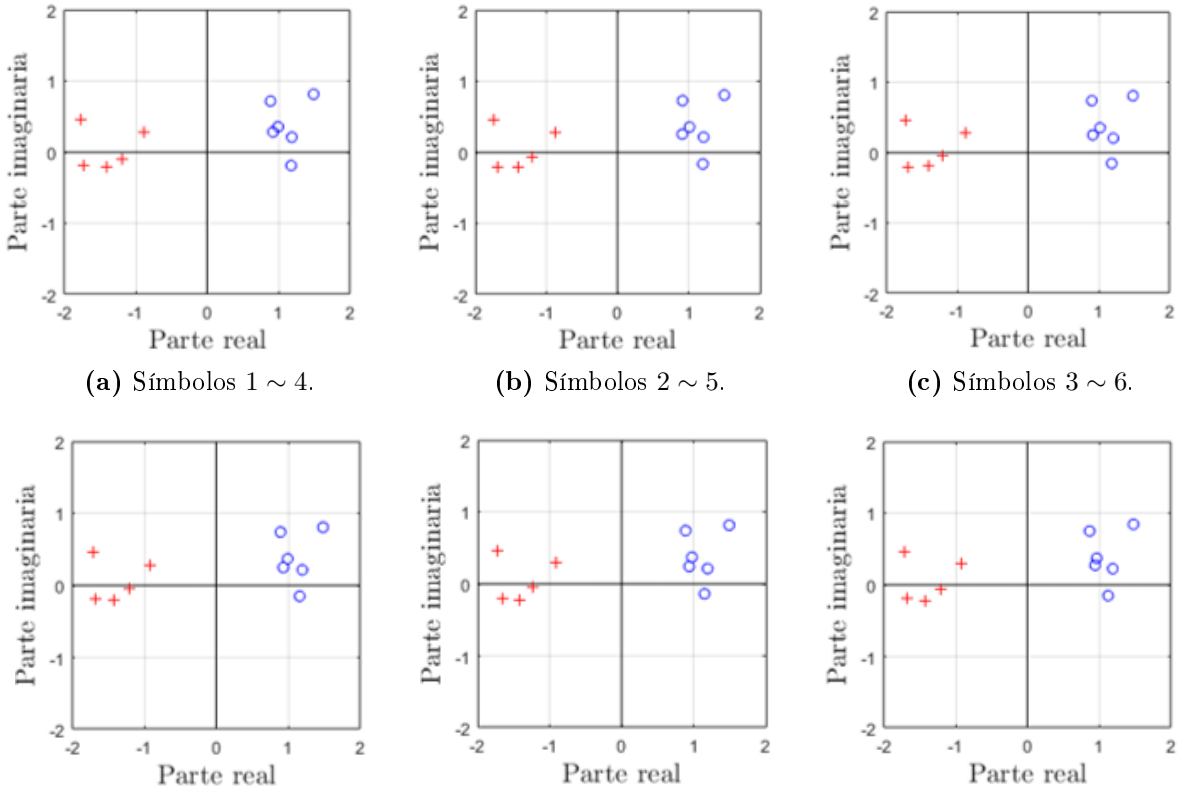


Figura 4.11: Valores máximos de la correlación cruzada de las muestras de la secuencia de símbolos cortos del paquete adquirido con la señal de referencia sintetizada en función del Δf.

Una vez encontrado el valor, para corregirlo basta con multiplicar toda la secuencia de muestras adquiridas por $e^{2\pi j \Delta f t[n]}$, donde $t[n] = n/f_s$ con $n = 0, 1, ..., N_{samp} - 1$ el índice de las muestras. En la figura 4.12 se muestran las coordenadas presentadas en la figura 4.10, luego de estimar el error de frecuencia y aplicar la corrección. Como resultado se compensa el efecto de rotación debido al error de frecuencia de las constelaciones calculadas. Cabe destacar que la constelación aun se encuentra rotada respecto de lo esperado, sin embargo, dicha rotación es uniforme para todos los grupos

de símbolos. El error de fase constante se compensa fácilmente midiendo la fase de la correlación.



(a) Símbolos $1 \sim 4$. **(b)** Símbolos $2 \sim 5$. **(c)** Símbolos $3 \sim 6$.

(d) Símbolos $4 \sim 7$. **(e)** Símbolos $5 \sim 8$. **(f)** Símbolos $6 \sim 9$.

Figura 4.12: Constelación del espectro de símbolos cortos del paquete adquirido luego de corregir el sincronismo en frecuencia. En azul, las subportadoras que corresponden a $1 + j$, en rojo, las subportadoras que corresponden a $-(1 + j)$.

4.2.3. Ecualización del canal

Aun cuando el error de sincronismo de frecuencia se ha corregido, en la figura 4.12 se observa que los puntos de la constelación presentan una dispersión significativa. Teniendo en cuenta que la Relación Señal a Ruido (SNR, por sus siglas en inglés) es alta, la misma se debe a efectos de distorsión de canal. Es necesario corregir este efecto, debido a que, como se verá más adelante, para esquemas de modulación de subportadoras tales como QPSK o 16-QAM, conlleva a que las coordenadas crucen las fronteras de decisión, lo que implica errores en la detección.

Para ecualizar el canal, se supone que su respuesta impulsiva, $h(t)$, y por tanto su respuesta en frecuencia $\mathcal{F}\{h(t)\} = H(f)$, son invariantes durante el tiempo que dura la transmisión de un paquete completo. Bajo esta hipótesis, basta encontrar una estimación de $H(f)$ para cada frecuencia de subportadoras de este canal y usarlos para corregir el espectro obtenido para cada símbolo dividiendo por la respuesta del canal. Un camino para encontrar $H(f)$ es empleando una señal de referencia, pero en este

caso no conviene usar los símbolos cortos, pues la mayoría de las subportadoras valen 0, mientras que sí conviene usar los largos, donde las 52 subportadoras toman los valores ± 1.

Si al pasar por el canal, la señal a la salida del mismo está dada por $y(t) = x(t) \star h(t)$, en donde se ha suprimido el término de ruido al suponer que se tiene una alta SNR, la manera de calcular la respuesta del canal es aplicar las propiedades de la transformada de Fourier para obtener la expresión $H(f_k) = Y(f_k)/X(f_k)$, siendo $X(f) = \mathcal{F}\{x(t)\}$ y $Y(f) = \mathcal{F}\{y(t)\}$ y f_k son las frecuencias que corresponden a las $N_{ST} = 52$ subportadoras de interés, es decir, las que no tienen valor nulo fijado por el estándar. El espectro de los símbolos largos queda establecido por el estándar como se ha visto en la sección 3.1 y el espectro de uno de los dos símbolos largos del paquete luego de la corrección del Δf se muestra en la figura 4.13. A diferencia del caso ideal, en este caso la parte imaginaria del espectro del símbolo no es nula, por el contrario, presenta valores significativos en comparación con la parte real en la mayoría de las subportadoras, lo que indica que se debe tener en cuenta la distorsión producida por el canal.

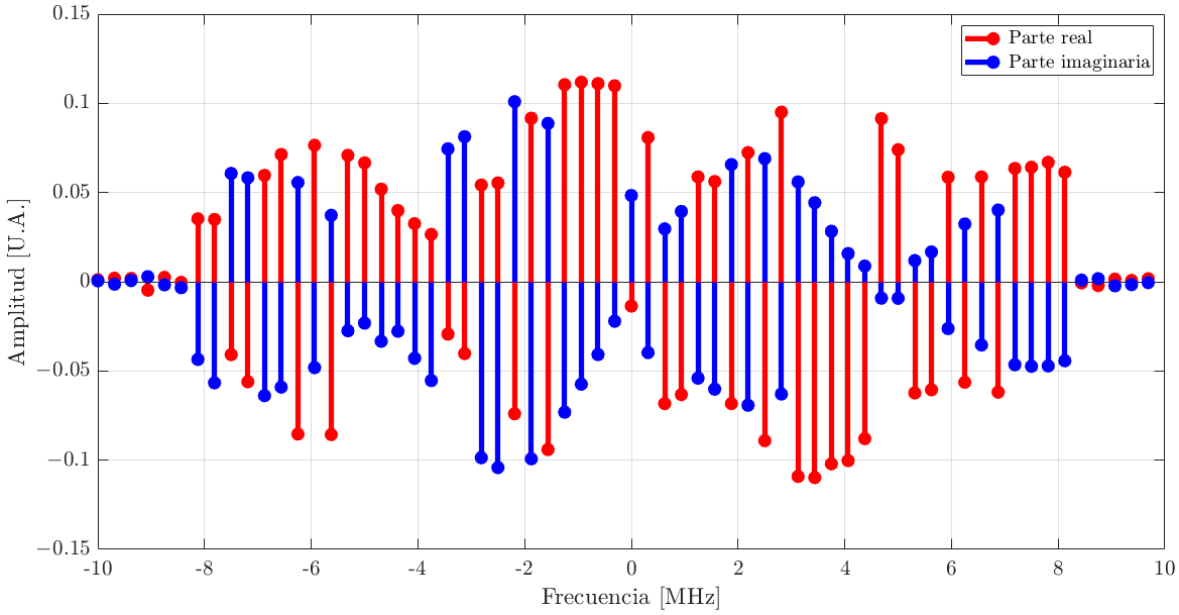


Figura 4.13: Espectro obtenido para un símbolo largo del paquete.

El segundo símbolo largo tenía un espectro muy parecido al primero, con mínimas diferencias que pueden deberse al ruido.

El cociente $H(f_k)$ obtenido para todas las f_k, se muestra en la figura 4.14, donde se observan su módulo y fase.

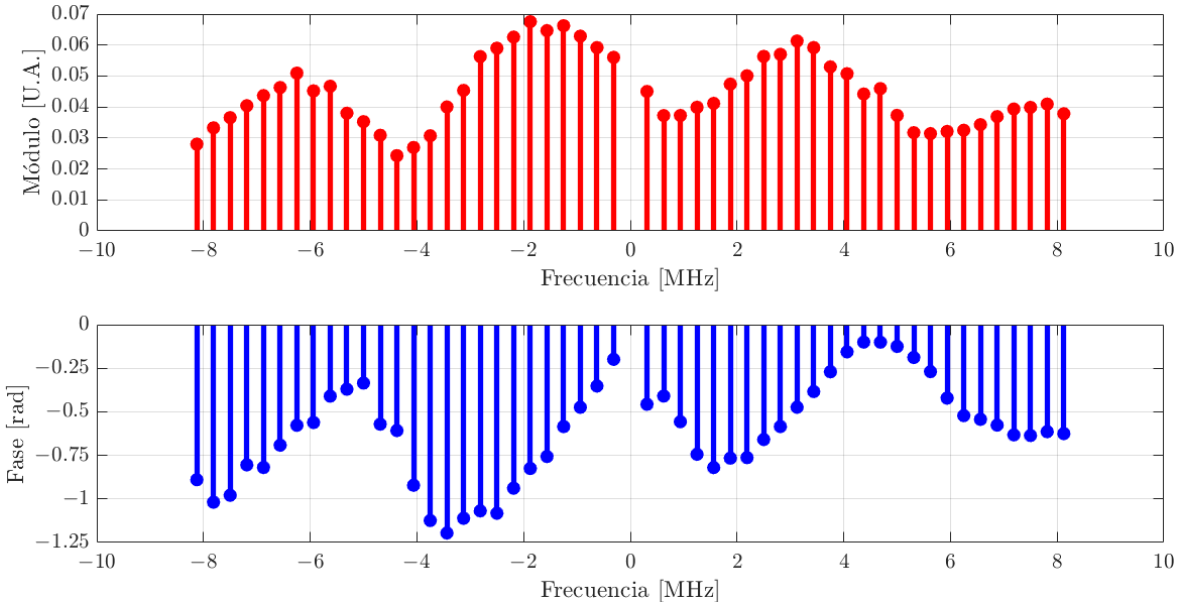


Figura 4.14: $H(f)$ obtenida empleando un símbolo largo como señal de referencia. En la gráfica de arriba se observa su módulo y en la de abajo su fase, en función de la frecuencia.

Si bien con los símbolos cortos no se puede obtener el valor de $H(f_k)$ para todas las f_k de interés, es posible hacer una comparación con el resultado anterior para las subportadoras no nulas del espectro de la secuencia de símbolos cortos, lo que permite tener una idea de cuán válida es la hipótesis de invarianza establecida para la $H(f)$. En la figura 4.15 se comparan las $H(f)$ que se obtuvieron de tomar una u otra parte del Preámbulo como señal de referencia.

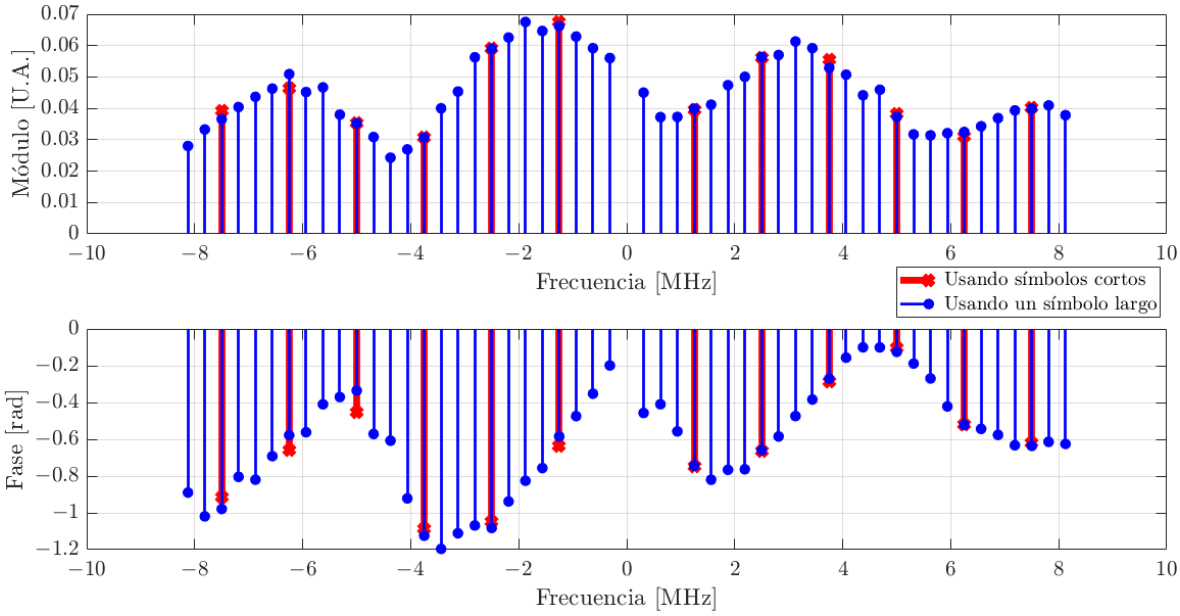


Figura 4.15: Comparación entre las $H(f)$ estimadas con un símbolo largo y con los cortos. En la gráfica de arriba el módulo y en la de abajo la fase, en función de la frecuencia.

4.3. Demodulación de los símbolos del paquete

4.3.1. Demodulación del símbolo SIGNAL

Para probar las correcciones realizadas, estas serán aplicadas al símbolo SIGNAL del paquete, el cual aparece a continuación del Preámbulo y usa modulación BPSK.

El procedimiento fue el mismo que antes: se compensó el error de sincronismo con el valor de $\Delta f = 46{,}43$ kHz encontrado y se calcularon las muestras correspondientes a las subportadoras dividiendo espectro del símbolo SIGNAL obtenido por los valores correspondientes de $H(f_k)$ mostrados en la figura 4.14. En la figura 4.16 se observa una comparación en la constelación del símbolo antes y después de la corrección con la respuesta del canal. Para el caso con corrección, se ha normalizado para que la energía de las N_{SD} subportadoras que contienen la información sea la misma que en el caso ideal (donde se esperan valores de ± 1). Como se aprecia, la dispersión de la constelación se ha reducido considerablemente y se distinguen perfectamente una constelación propia de la modulación BPSK, que es la que emplea este símbolo. Entre las muestras descartadas se encuentran las subportadoras piloto, en las cuales se comprobó que tenían el signo esperado para un símbolo SIGNAL ($[1, 1, 1, -1]$) según la secuencia $p_{0,126}$ tratada en la sección 3.2.4.

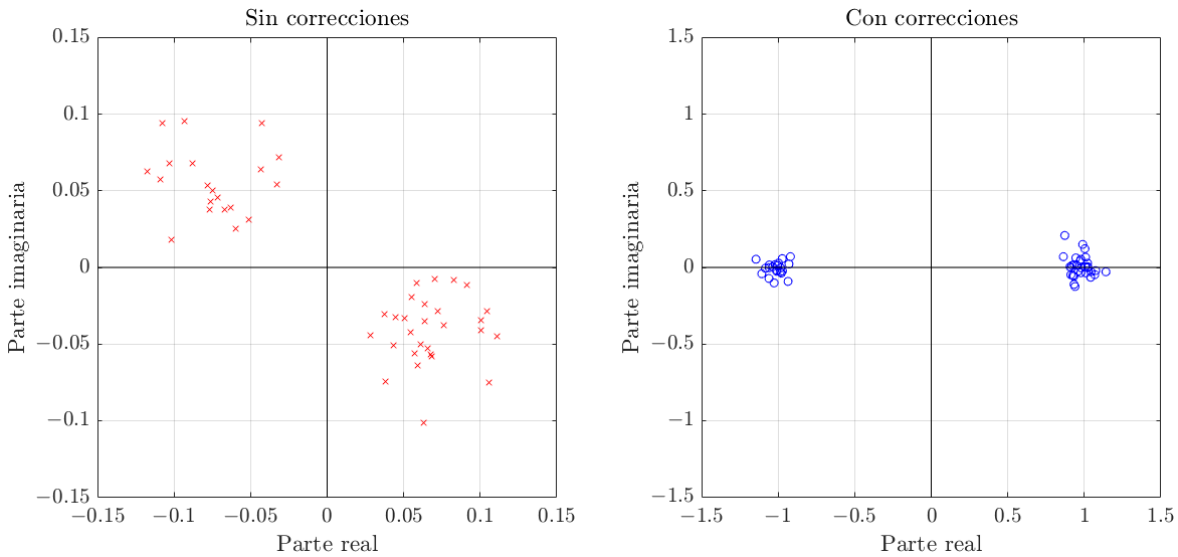


Figura 4.16: Comparación de las constelaciones con y sin corrección del símbolo SIGNAL.

Los valores complejos de la constelación fueron sustituidos por bits teniendo en cuenta el signo de su parte real como se observa en la figura 3.8, quedando un total de $N_{CBPS} = 48$. Estos deben ser desentrelazados y decodificados como se indica en la sección 3.6, en donde $N_{BPSC} = 1$ por tratarse de modulación BPSK, con lo que la tasa de codificación toma valor R= 1/2 y el resultado final son los 24 bits de fuente que generaron al símbolo SIGNAL y que se muestran en la figura 4.17. En dicha

imagen, se distinguen los distintos campos, de los cuales los que aportan información útil para la demodulación de los símbolos de DATA son: RATE = '1001' y LENGTH = '011100000000' (14 octetos). El bit de Paridad en este caso tiene el valor 1, siendo este el valor correcto en función de los demás bits, y tanto el bit Reservado como los del campo TAIL valen '0'.

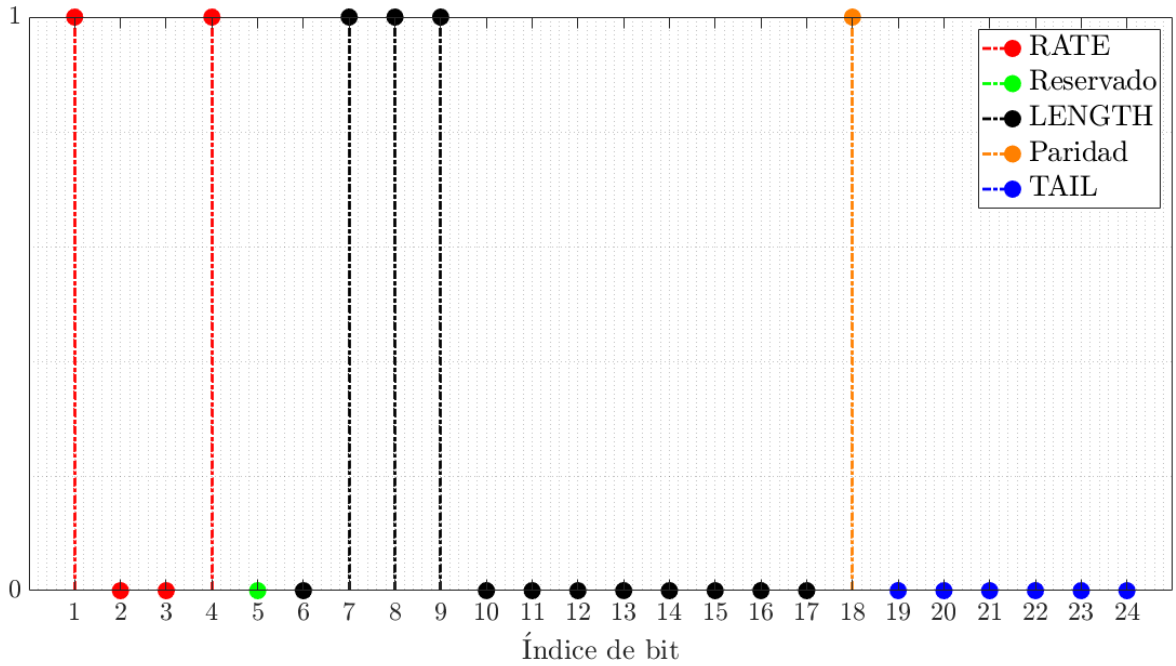


Figura 4.17: Bits de fuente del símbolos SIGNAL del paquete adquirido.

Según la tabla 2.3, para el campo RATE obtenido, la modulación usada en el campo DATA es 16-QAM, por lo que $N_{BPSC} = 4$ y $N_{DBPS} = 96$, y se aplica una tasa de codificación de $R = 1/2$ (sin esquema de perforado de bits), por lo que $N_{CBPS} = 192$. Con esta información, y sabiendo que se envían 14 octetos o $N_{PSDU} = 112$ bits, con lo que la cantidad de bits en DATA es el menor múltiplo de N_{DBPS} tal que se cumpla que $N_{DATA} \geq N_{SERVICE} + N_{PSDU} + N_{TAIL} = 134$, por tanto queda que $N_{DATA} = 192$ donde a los demás campos se sumaron $N_{PAD} = 58$ bits de relleno y el número de símbolos de DATA es $N_{sym} = N_{DATA}/N_{DBPS} = 2$. Al ser el ancho de canal de 20 MHz, la duración de cada símbolo OFDM es de 4 μs como lo indica la tabla 2.1, por lo que, sumando la duración del Preámbulo (16 μs), la del símbolo SIGNAL (4 μs) y la de los símbolos del campo DATA (8 μs), se tiene que la duración total del paquete es de 28 μs. Este resultado es consistente con la duración que tiene el paquete en el registro de datos, tal como se aprecia en la figura 4.4, donde se encuentra representado. Por lo tanto, esto hace pensar que no hubo ningún error en la detección y decodificación de los bits del campo SIGNAL de este paquete.

4.3.2. Demodulación de los símbolos de DATA

Para obtener los bits de fuente del campo DATA, habría que aplicar las mismas correcciones a las muestras y demodular esta vez con 16-QAM, $N_{BPSC} = 4$, $N_{DBPS} = 96$, $N_{CBPS} = 192$ y R= 1/2. Similar al caso de SIGNAL, se comprobó que las subportadoras piloto insertadas tuviesen todas la polaridad que establece la norma, donde en este caso, ambos símbolos tenían $\{1; 1; 1; -1\}$. Las constelaciones resultantes se muestran en la figura 4.18, donde se distingue la forma de un sistema 16-QAM, el cual fue normalizado para que el valor medio de la energía de las subportadoras piloto sea 4 como lo establece la norma, y luego, dividido por la constante $k_{mod} = 1/\sqrt{10}$ que le corresponde según la tabla 3.1.

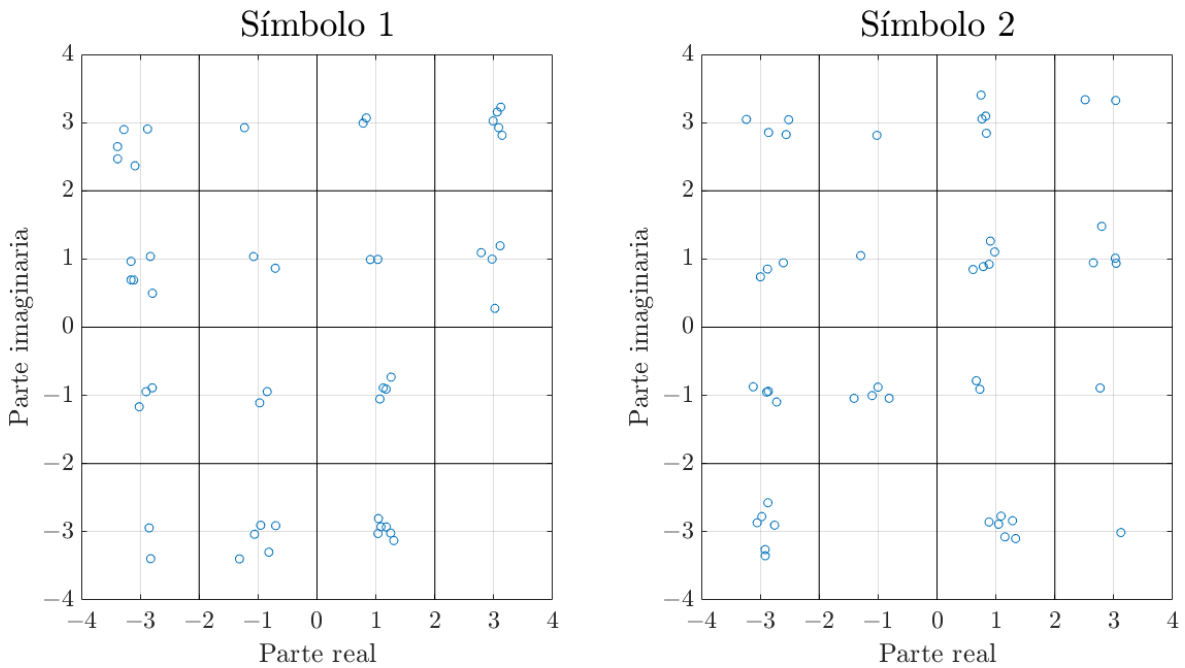


Figura 4.18: Constelaciones 16-QAM de los símbolos del campo DATA luego de las correcciones, el cálculo del espectro y la eliminación de las subportadoras piloto y símbolos nulos.

Luego de sustituir los puntos de la constelación por los bits correspondientes siguiendo las fronteras de decisión, se aplicó el desentrelazado y la decodificación. Además, se recodificó toda la trama de bits para ver si hubo algún error producido por el canal que el código pudo corregir, en donde se obtuvo que no se produjeron errores.

El último paso que es característico de la demodulación del campo DATA es el uso del descrambler, en donde primero se buscó la semilla como se indica en la sección 3.6, cuya secuencia de bits obtenida fue de '0001001', y luego se procesaron los bits con lo que se llegó a los 192 bits de fuente que componían a los dos símbolos. Los primeros 16 fueron descartados (campo SERVICE) y a partir de ahí se contaron los 112 bits de la PSDU, que son los que contienen la información proveniente de capas superiores, y que serán analizados en detalle en el capítulo 5.

4.4. Conclusiones

Se ha logrado demodular un paquete IEEE 802.11a correspondiente a la comunicación inalámbrica de un celular con un router. Tomando como base un modelo de canal inalámbrico simple y, bajo la hipótesis de que el mismo es invariante en el tiempo durante el tiempo de transmisión de un paquete y teniendo en cuenta que la SNR es alta, se desarrolló un algoritmo que fue capaz de corregir los errores introducidos por el canal y además el error de sincronismo en el receptor. Para lograrlo, se emplearon como señales de referencia las secuencias de símbolos del Preámbulo, tanto la de símbolos cortos como la de los largos, presentes en todos los paquetes del estándar. Esto permitió la demodulación inequívoca, primero del símbolo SIGNAL, y con la información extraída de este, la del conjunto de símbolos de DATA.

Como parte del proceso, se comprobó que se estuviese cumpliendo con lo establecido por la norma en todas las etapas, lo que da una validación positiva al procedimiento seguido:

- El signo de las subportadoras piloto fue el esperado según la secuencia $p_{0,126}$ en cada símbolo.
- La información contenida en el símbolo SIGNAL resultó coherente con las características del campo DATA.
- El bit de Paridad de SIGNAL tenía el valor correcto.
- Los bits con valor fijo '0' tanto en SIGNAL como en DATA tenían justamente ese valor.

Es posible en esta instancia, proceder a extraer información proveniente de las capas superiores, para lo que se debe chequear en el estándar [9, Cláusula 9] cuáles son los campos que componen a la PSDU desde el punto de vista de las capas superiores.

Capítulo 5

Extracción de información de capas superiores

Hasta este punto, se ha logrado la demodulación completa de un paquete del estándar IEEE 802.11a. El trabajo por delante es analizar qué significan dichos bits en términos de capas superiores. En [9, Cláusula 9] se explica la estructura de la capa de control de acceso al medio (MAC, por sus siglas en inglés) que le da un significado a esos bits, interpretando a la PSDU como la unidad de datos de servicio de la capa MAC (MSDU, por sus siglas en inglés).

En el presente capítulo, se estudian los campos que componen la trama en capa MAC y se extrae la información correspondiente a los campos de la trama demodulada a partir del paquete analizado en el capítulo 4. El objetivo es analizar qué función cumple el mismo y si es posible obtener a partir de este las direcciones de capa MAC de los dispositivos empleados.

5.1. Estructura del formato de la capa MAC

Si bien no existe un formato único para la MSDU que englobe a todos los paquetes, ya que para algunos aparecen campos de información adicionales según su función en la comunicación, haciendo que su longitud sea variable, sí existen algunos campos básicos de la MSDU que van a estar presentes en todas las tramas MAC del estándar. La estructura más general de la trama MAC está dada por:

- Un encabezado MAC que contiene:
    - El Frame Control.
    - La duración.
    - Al menos una dirección MAC (y hasta 4) según el tipo de trama.
    - Otros campos de bits opcionales según el tipo de trama.

- El cuerpo (opcional), de longitud variable, según el tipo y subtipo de trama.
- Una Secuencia de Verificación de Trama (FCS, por sus siglas en inglés) que contiene un CRC de 32 bits de longitud basado en la recomendación ITU-T V.42 [15].

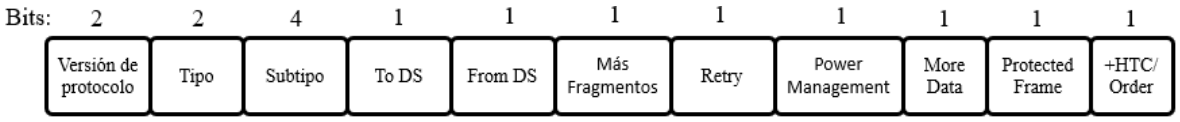
Solo los campos que corresponden al Código de Redundacia Cíclica (CRC, por sus siglas en inglés) se transmiten comenzando por el bit más significativo, en caso contrario, al inicio estará el bit menos significativo.

En la figura 5.1 se observan las diferentes partes del formato de una trama MAC genérica, en donde se indica la longitud en octetos para cada uno. Los campos Frame Control, Duración/ID, Dirección 1 y Frame Check Sequence constituyen el formato mínimo que puede tener una trama, y según el valor que toman los parámetros Tipo y Subtipo aparecen en el Frame Control como se explica en la sección 5.1.1, pueden aparecer o no los restantes campos.

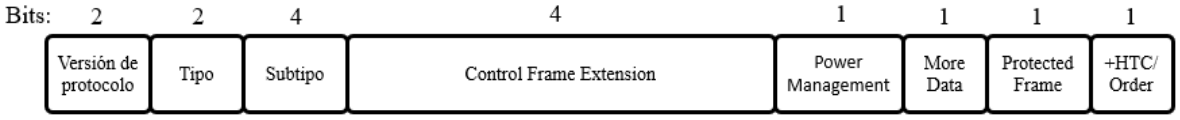
Figura 5.1: Formato de los campos de la capa MAC.

5.1.1. Frame Control

En la figura 5.2 se aprecian las distintas estructuras posibles para el campo Frame Control, el cual consta de dos octetos, por lo que los bits van desde un B0 hasta un B15. En dependencia de los subcampos Tipo y Subtipo, los cuales aparecen en ambas formas, se va a emplear una u otra estructura.



(a) Cuando Tipo es distinto de 1 o Subtipo es distinto de 6, expresados como números decimales.



(b) Cuando Tipo es igual a 1 y Subtipo es igual a 6, expresados como números decimales.

Figura 5.2: Estructura del Frame Control según los campos Tipo y Subtipo.

De acuerdo con el estándar, los dos bits correspondientes a la Versión de Protocolo (B0 y B1) se fijan en '0', por lo que este campo no aporta información. En cuanto al Tipo (B2 y B3), existen cuatro posibles combinaciones:

- Trama de control (Control): '10'.
- Trama de datos (Data): '01'.
- Trama de administración (Management): '00'.
- Extensión (Extension): '11'.

Estos bits, en combinación con los del Subtipo (B4, B5, B6 y B7), determinan qué función tiene esta trama en la comunicación y también cuáles de los campos opcionales aparecen en una determinada trama MAC, cosa que no es necesario analizar en profundidad para continuar con el desarrollo del proyecto, así que se abordan un poco más en detalle en el apéndice A.

Los subcampos restantes del Frame Control son descritos en detalle en la [9, Cláusula 9], lo cual no ha sido incluido en el presente capítulo debido a que excede los objetivos de este Proyecto Integrador. La información brindada hasta este punto es suficiente para realizar el análisis de la trama demodulada que se quiere lograr en este trabajo.

5.2. Frame Control Sequence

La FCS está compuesta por 4 octetos (32 bits) que no es otra cosa que un CRC. Este se calcula operando sobre todos los campos del encabezado MAC y del Frame Body (en caso de que este exista), cuya unión se denomina *Calculation Fields* y usa el polinomio generador

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1.$$

El FCS es el complemento a 1 de la suma módulo 2 de los siguientes polinomios:

- El resto de $x^k \cdot (x^{31} + x^{30} + ... + x + 1)/G(x)$ (dividido en módulo 2), donde k es el número de bits totales en *Calculation Fields*.
- El resto de multiplicar los bits de la trama (vistos como polinomio) con x^{32} y luego dividir por $G(x)$.

Para obtener el complemento a 1 a partir de un número binario, solo hay que negar el valor de cada bit. Hay que recordar que el FCS se transmite con el MSB en la posición inicial a diferencia de los otros campos de la estructura de la trama.

5.3. Interpretación de los bits de la trama obtenida

Como se deduce de la figura 5.1, la trama MAC que tiene la menor duración posible es de 14 octetos, lo que coincide con la longitud de la trama de bits obtenida en la demodulación, por lo que solo posee los campos Frame Control, la Duración/ID, la Dirección 1 y la FCS.

Los bits de la Duración/ID en este caso son todos '0'. La Dirección 1 de la trama fue convertida de bits a números hexadecimales resultando ser

$$14 : CC : 20 : B9 : 3D : 17$$

que es justamente la dirección de identificador de conjunto de servicios básicos (BSSID, por sus siglas en inglés) del router y que se encuentra en la figura 4.2, donde se muestra la configuración que este empleó durante la comunicación entre los dispositivos.

5.3.1. Frame Control de la trama obtenida

El Frame Control de la trama en cuestión se expone en la figura 5.3, donde se ve que la Versión de Protocolo es '00' y el Tipo del paquete es '10' (Tipo Control). Los bits del Subtipo son '1011', por lo que corresponde con una estructura como la de la figura 5.2a. Al consultar la tabla A.1 que se encuentra en el apéndice A, podemos encontrar que esta combinación de Tipo-Subtipo corresponde a una trama de control Ack. El resto de los campos del Frame Control son '0' para este caso, coincidiendo esto con lo que se muestra en la figura 5.3.

Versión de protocolo: 00	Tipo: 10	Subtipo: 1011	To DS: 0	From DS: 0	Más Fragmentos: 0	Retry: 0	Power Management: 0	More Data: 0	Protected Frame: 0	+HTC/ Order: 0

Figura 5.3: Frame Control correspondiente al paquete demodulado.

En este tipo de tramas, cuya estructura se muestra en la figura 5.4, la única dirección MAC que aparece en el encabezado (RA) es la misma que aparece en el campo Dirección 2 de la trama inmediata anterior de Tipo Data o Management o de algunos subtipos específicos de tramas de Control. Entre estos, hay tramas de Tipo Data que pueden tener al BSSID en dicho campo según la tabla 6.1, como ocurre con la trama analizada en este capítulo.

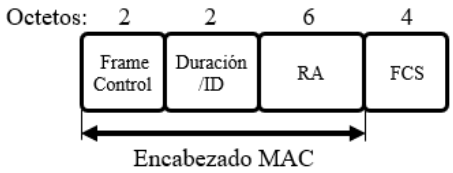


Figura 5.4: Estructura de la trama de Control Ack.

5.3.2. FCS de la trama obtenida

Los 4 octetos del FCS correspondientes a la trama analizada se listan a continuación:

$$\text{FCS} = \{01010011 \qquad 10100101 \qquad 00101010 \qquad 01000001\}$$

Conociendo la trama obtenida, podemos calcular el FCS de la misma según el algoritmo descrito en la sección 5.2 y compararlo con el anterior, para verificar que los bits son iguales y que no hubo errores en la transmisión.

Al calcular los dos polinomios de dicho algoritmo que se denotan P_1 y P_2, se obtiene como resultado:

$$\begin{aligned} P_1 = {} & x^{31} + x^{28} + x^{24} + x^{23} + x^{22} + x^{21} + x^{19} + \\ & + x^{16} + x^{15} + x^{13} + x^{11} + x^{10} + x^{9} + x^{5} + x^{4} + x^{3} \end{aligned}$$

$$\begin{aligned} P_2 = {} & x^{29} + x^{28} + x^{27} + x^{26} + x^{24} + x^{23} + x^{21} + x^{20} + x^{17} + \\ & + x^{16} + x^{14} + x^{13} + x^{12} + x^{11} + x^{9} + x^{8} + x^{7} + x^{2} + x \end{aligned}$$

y al aplicar la suma con módulo 2 a los dos polinomios anteriores, se obtiene como resultado

$$P = x^{30} + x^{28} + x^{25} + x^{24} + x^{23} + x^{21} + x^{18} + x^{16} + x^{13} + x^{11} + x^{9} + x^{6} + 1.$$

Este polinomio (contando con el término implícito $0 \cdot x^{31}$) es igual al FCS si interpretamos cada término del mismo como un bit, por lo que la trama MAC obtenida cumple con todos los requisitos que la norma establece para su tipo.

5.4. Conclusiones

Se realizó un estudio general de la estructura de la trama MAC del estándar IEEE 802.11a, que no es más que el conjunto de bits a transmitir que pasan a capa física como PSDU. Esto permitió conocer sus principales partes según la función que cumple en la comunicación.

Se retomó la PSDU demodulada y decodificada en el capítulo 4 para extraer la información de la capa MAC y verificar que la trama no tuviese errores. Se encontró que esta trama cumple la función de Ack, cuyo Tipo es de Control. Se pudo extraer la dirección MAC del BSSID a partir de estos bits. Se calculó el campo FCS a partir del encabezado MAC de la trama y se verificó que el resultado coincide con los últimos 32 bits extraídos, como lo establece la norma.

Estas implementaciones para los bits en la capa MAC, en conjunto con las anteriores de la capa física, pueden ser aplicadas a otros paquetes OFDM para obtener todo

(Biblioteca Leo Falicov CAB-IB)

tipo de información sobre la comunicación de los dispositivos en cuestión. En caso de encontrarse con otros tipos de tramas, habría que consultar en la norma de IEEE 802.11a para analizarlos, ya que la clasificación de estas es muy amplia, y si bien todas tienen una estructura general, hay campos opcionales que aportan información útil y que aparecen según el Tipo y Subtipo en cada caso.

Capítulo 6

Análisis completo de un segundo paquete

Una vez sistematizado el procesamiento para demodular las señales recibidas, decodificar los bits en capa física y analizar la información a nivel de subcapa MAC, se procedió a analizar un segundo paquete con el objetivo de extraer información adicional sobre los dispositivos que intervienen en la comunicación.

El procedimiento fue análogo al del paquete previo, que incluyen los pasos generales descriptos en los capítulos 4 y 5:

- Realizar la detección y determinar la muestra inicial del paquete.
- Corregir el error de sincronismo en frecuencia usando la secuencia de símbolos cortos del Preámbulo.
- Corregir el error por distorsión del canal empleando la secuencia de símbolos largos del canal.
- Demodular y decodificar el símbolo SIGNAL y obtener sus bits de fuente para conocer las características de la modulación, codificación y longitud del campo DATA.
- Demodular y decodificar los símbolos del campo DATA para obtener sus bits de fuente (PSDU).
- Interpretar la PSDU como MSDU para encontrar qué función tiene la trama demodulada en la comunicación.

6.1. Procesamiento del paquete en capa física

El paquete escogido fue el encontrado a continuación del analizado en el capítulo 4, cuyo inicio se encuentra alrededor de los 300 μs como bien se observa en la figura

4.3. Dicho paquete se visualiza de manera más detallada en la figura 6.1, en donde se remarca su secuencia de símbolos cortos.

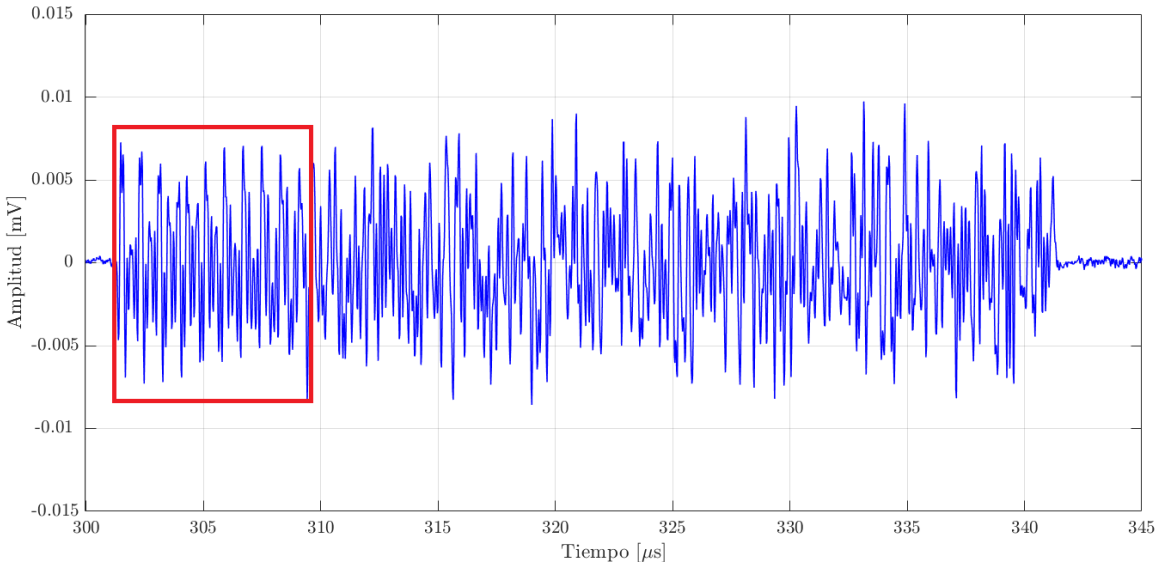


Figura 6.1: Detalle de la forma de onda de la componente I de la señal en banda base del paquete.

La detección se realiza a partir de la correlación de los símbolos cortos del Preámbulo con el registro de datos, con lo que se pudo encontrar la muestra inicial del paquete, localizando el máximo local alrededor de los 300 μs de la gráfica de la figura 4.5.

El error de frecuencia coincide con el del paquete anterior ($\Delta f = 46{,}43$ kHz), que se presentó en la figura 4.11. Luego de corregir este error, se buscó la respuesta en frecuencia del canal usando los símbolos largos, y el espectro obtenido se muestra en la figura 6.2.

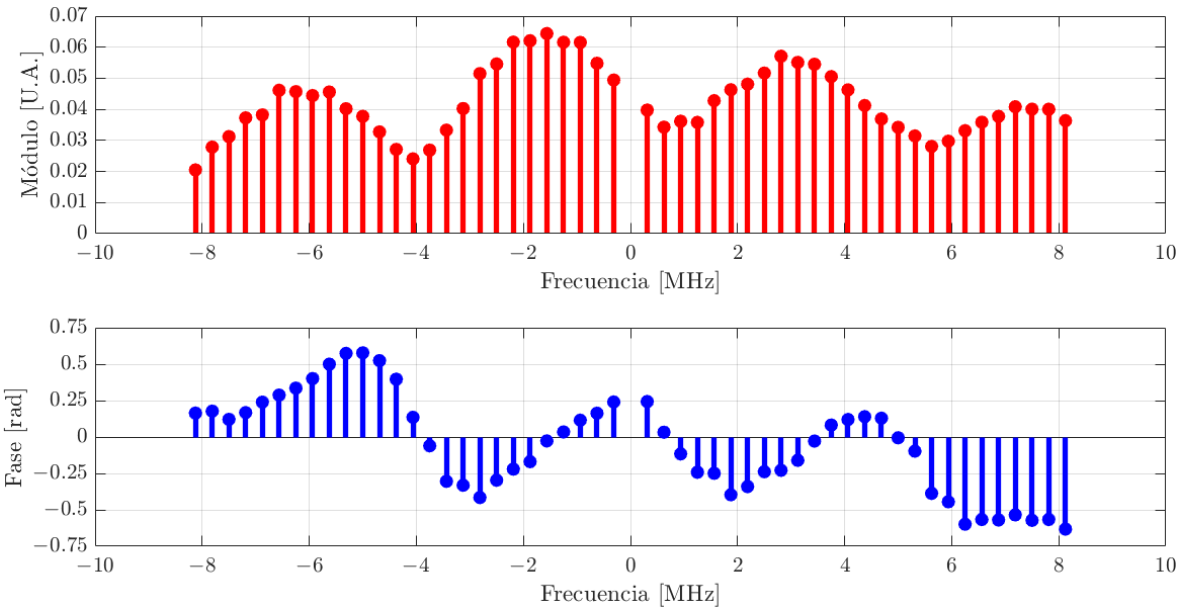


Figura 6.2: $H(f)$ obtenida empleando un símbolo largo como señal de referencia. En la gráfica de arriba se observa su módulo y en la de abajo su fase, en función de la frecuencia.

Una vez hecho esto, se procedió a demodular y decodificar el símbolo SIGNAL aplicando previamente las correcciones de error de frecuencia y distorsión del canal y se llegó a la constelación que aparece en la figura 6.3, donde se aprecia la mejora que producen las correcciones del canal sobre la constelación BPSK de este símbolo.

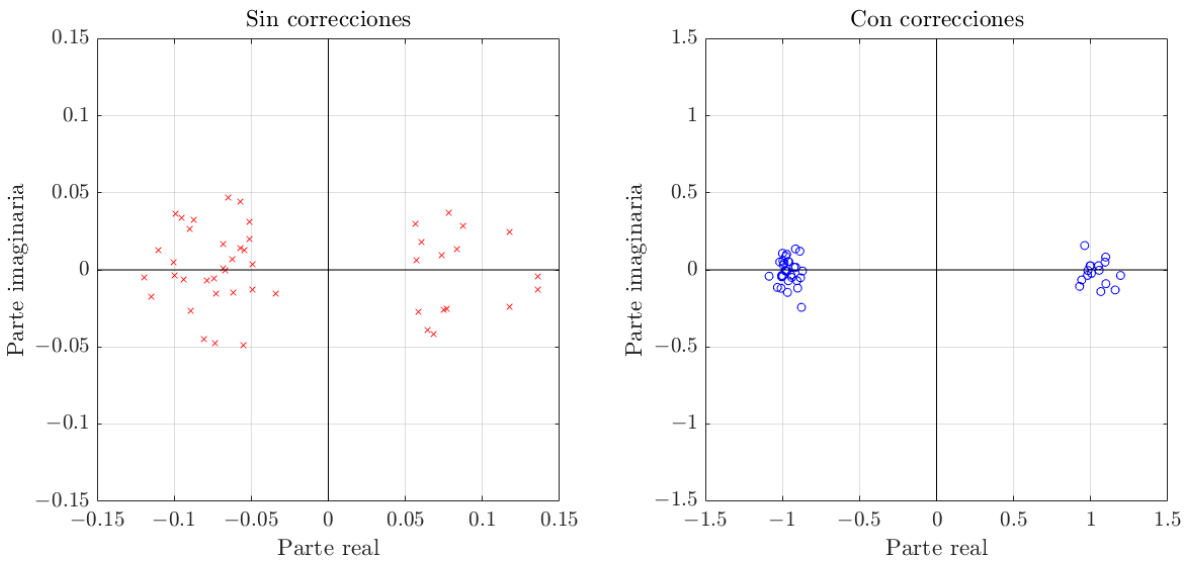


Figura 6.3: Constelación del símbolo SIGNAL.

Al procesar la constelación con correcciones, se llega a los bits de fuente del símbolo SIGNAL mostrados en la figura 6.4

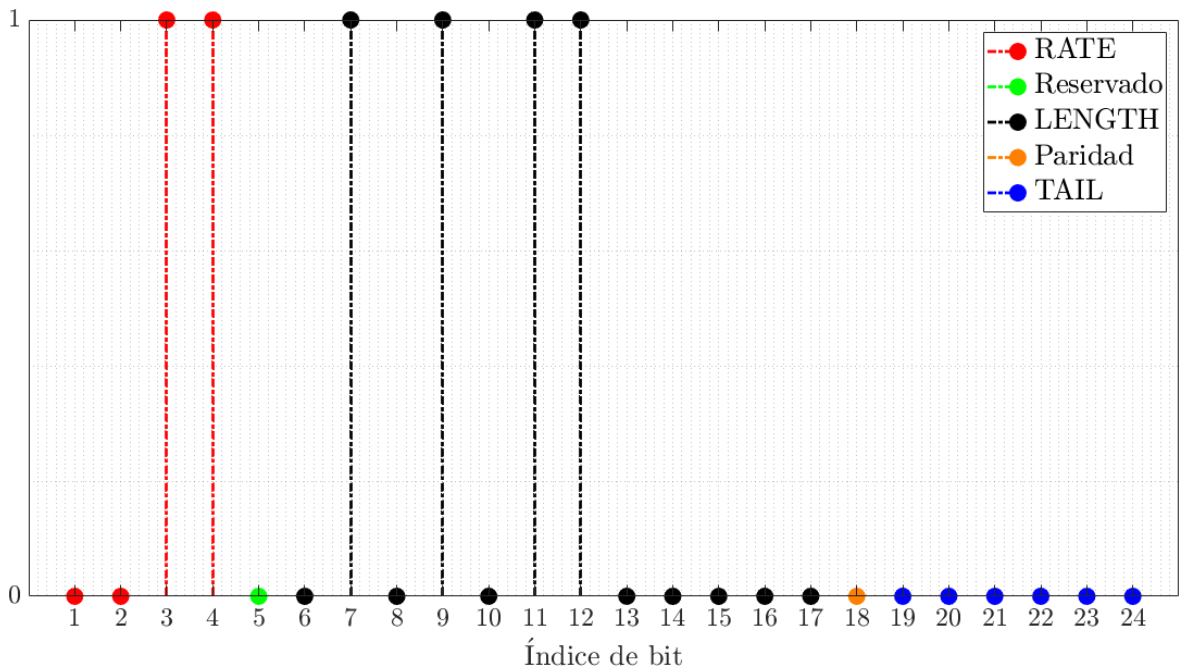


Figura 6.4: Bits de fuente del símbolo SIGNAL.

Al recurrir a las tablas 2.2 y 2.3 se encuentra que, para el ancho de canal de 20 MHz, la tasa de transmisión usada en este paquete es de 54 Mbps, la codificación

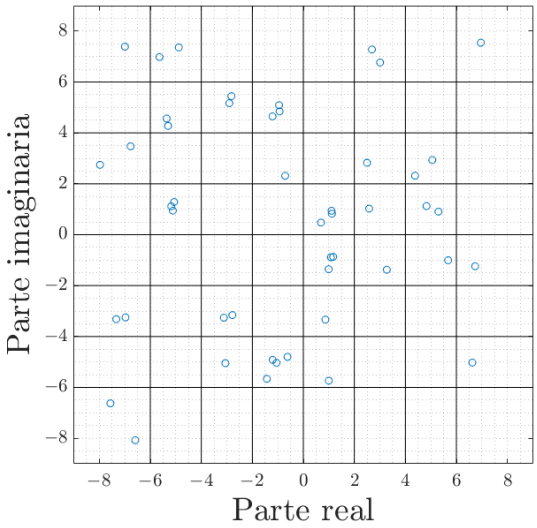
emplea una tasa R = 3/4 y cada símbolo contendrá $N_{DBPS} = 216$ bits de datos, con lo que los bits de código por símbolo son $N_{CBPS} = 288$. El valor del campo LENGTH expresado como un número decimal es 106, con lo que se van a transmitir 848 bits de datos provenientes de capas superiores (PSDU), a los que hay que añadir los 16 bits de SERVICE y los 6 bits de TAIL (llegando a 870). Luego se deben agregar los bits del campo PAD, con lo que la cantidad de bits de DATA llega al múltiplo más cercano de 216, que es $1080 = 5 \cdot 216$, por lo que la cantidad de símbolos del paquete resulta $N_{sym} = 5$, lo que arroja una duración del paquete de 40 μs como se muestra en la figura 6.1, en la cual se puede ver la componente I correspondiente a dicho paquete. Esta información permitió la demodulación y decodificación de los símbolos de DATA.

Las constelaciones de los símbolos se muestran en la figura 6.5, en la que se marcan las líneas correspondientes a las fronteras de decisión para el esquema de modulación de 64-QAM. Se observa que para algunos de los símbolos aparecen puntos de la constelación sobre las fronteras, lo que permite inferir que existirán errores en los bits de canal luego de la detección, como consecuencia del desplazamiento de las coordenadas fuera de la región determinada por las fronteras de decisión que les correspondía originalmente cuando fueron modulados.

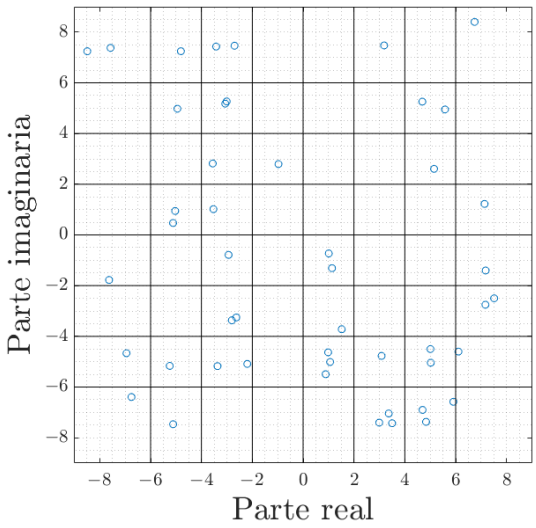
Previo a la demodulación, se comprobó que tanto para estos símbolos como para el SIGNAL, las subportadoras piloto que se introducen tuviesen el signo correcto según lo que establece la norma. A continuación, se realizó el mapeo de las coordenadas a bits de canal usando las fronteras de decisión indicadas en la figura 6.5, y seguidamente se aplicaron las operaciones de desentrelazado y decodificación.

Los bits desentrelazados y decodificados se codificaron nuevamente siguiendo el mismo esquema de codificación con R = 3/4 y al comparar el registro de bits obtenidos con los que se tenían a la salida del desentrelazador, 19 de estos eran distintos, los cuales fueron corregidos por el decodificador de Viterbi.

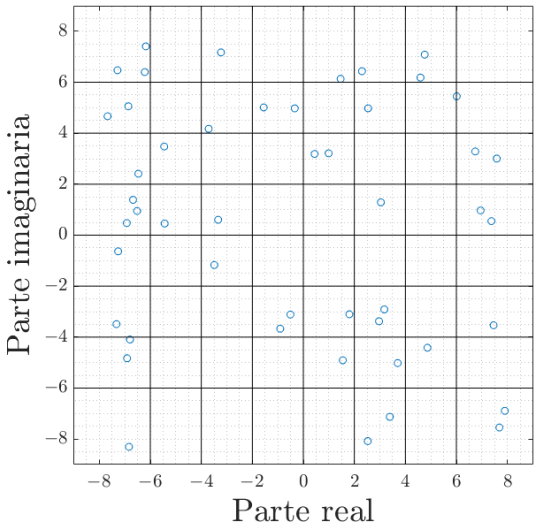
Una vez decodificados, los bits fueron procesados con el descrambler aplicando la misma secuencia generada para el paquete analizado en el capítulo 4, y de los bits obtenidos, los primeros 16 (SERVICE) fueron descartados y se tomaron los siguientes 848, que constituyen la PSDU y se interpretaron como bits de trama MAC (MSDU) aplicando lo que ya se vio en el capítulo 5.



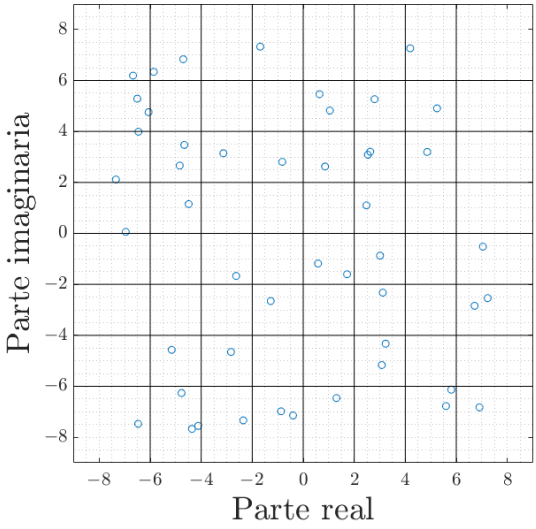
(a) Símbolo 1.



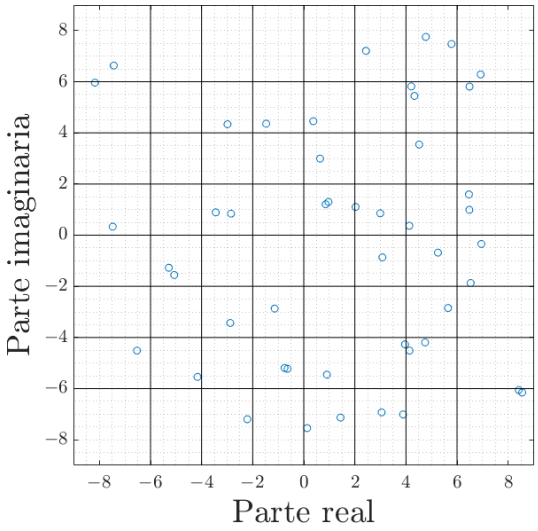
(b) Símbolo 2.



(c) Símbolo 3.



(d) Símbolo 4.



(e) Símbolo 5.

Figura 6.5: Constelaciones 64QAM de los símbolos del campo DATA luego de las correcciones, el cálculo del espectro y la eliminación de las subportadoras piloto y símbolos nulos.

6.2. Procesamiento del paquete en la capa MAC

Para analizar este MSDU, visiblemente más largo que el anterior, fue necesario volver a consultar en el estándar para encontrar cuáles de los campos de la trama MAC que aparecen en la figura 5.1 utiliza esta trama en particular.

El primer paso consiste en extraer la información del Frame Control para determinar su estructura, dentro de las posibilidades que se muestran en la figura 5.2 y así conocer qué tipo de paquete es y qué función realiza. Se verificó que la versión tuviese el valor esperado ('00'). El Tipo encontrado fue '01', lo que corresponde a una trama de datos (Data) y el Subtipo fue '0001', que indica que se trata de QoS DATA, como se indica en la tabla A.1. De los restantes campos del Frame Control, los que tienen valor '1' son To DS y Protected y los restantes poseen valor '0'. El valor '1' del campo Protected indica que el Frame Body está encriptado, por lo que en principio no podemos acceder a la información que este contiene.

La norma establece que, para las tramas de Tipo Data, la estructura está dada por el esquema de la figura 6.6, donde se observa que estas contienen al menos 3 de las 4 direcciones que pueden estar presentes según la estructura general de la trama MAC vista en la figura 5.1.

Figura 6.6: Estructura de la trama MAC para el Tipo Data.

Para saber si la Dirección 4 se encuentra o no, hay que consultar la tabla 6.1 cuya información fue extraída del estándar, en donde se establece que las direcciones que aparecen dependen de los campos To DS y From DS.

To DS	From DS	Dirección 1	Dirección 2	Dirección 3	Dirección 4
0	0	RA = DA	TA = SA	BSSID	N/A
0	1	RA = DA	TA = BSSID	SA	N/A
1	0	RA = BSSID	TA = SA	DA	N/A
1	1	RA	TA = SA	DA	SA

Tabla 6.1: Campos de Direcciones para las tramas de Tipo Data según su Frame Control.

Para los valores de estos campos de la trama en cuestión (To DS = 1 y From DS = 0), se observa que no se utiliza la Dirección 4. El campo Secuencia de Control, compuesto por 2 octetos, está dividido en dos partes:

- Los primeros 4 bits constituyen el Número de Fragmento y para la trama en cuestión valen todos '0', con lo que se indica que es el primer fragmento de la misma, y también el único, pues como establece el estándar, al ser '0' el campo Más Fragmentos del Frame Control, se indica que no hay más fragmentos de datos a enviar en el próximo paquete.

- Los 12 bits restantes constituyen el Número de Secuencia, los cuales valen para la trama demodulada '010001101111', lo que indica que esta es la trama número 3938 de la comunicación.

Al tener como Subtipo QoS DATA, el campo QoS Control aparece en el encabezado de esta trama, siendo en este caso en particular '0' todos sus bits. El bit +HTC/Order del Frame Control está en '0' por lo que no se utiliza el campo HT Control de la trama, con lo que ya quedan determinados todos los campos (los últimos 32 bits son la FCS y antes de esta, hay 76 octetos o 608 bits de Frame Body).

La tabla 6.2 resume los valores de los bits en los campos presentes analizados de esta trama MAC.

Frame Control	00010001 10000010
Duración / ID	00110100 00000000
Dirección 1	00101000 00110011 00000100 10011101 10111100 11101000
Dirección 2	00110111 11111000 01001110 11101010 00001010 11011101
Dirección 3	00101000 00110011 00000100 10011101 10111100 01101000
Secuencia de Control	00000100 01101111
QoS Control	00000000 00000000
FCS	01110101 01011011 11011011 11001111

Tabla 6.2: Bits en los distintos campos de la estructura de la trama.

6.2.1. Lectura de Direcciones

Una vez acotados los bits correspondientes a cada campo, fueron convertidas las direcciones MAC de bits a números hexadecimales. En la Dirección 1 el valor encontrado fue

$$14 : CC : 20 : B9 : 3D : 17,$$

lo que se corresponde con el valor del BSSID y que es el mismo que se encontró en el capítulo 5. La Direción 2, correspondiente al transmisor, es

$$EC : 1F : 72 : 57 : 50 : BB,$$

que en este caso sería el teléfono celular, la cual lamentablemente, no se pudo verificar debido a que no fue registrada y el dispositivo se dañó y se encuentra fuera de servicio desde entonces. La Dirección 3 obtenida fue

$$14 : CC : 20 : B9 : 3D : 16,$$

muy similar a la Dirección 1, y que corresponde a la dirección de destino. La Dirección 3 es la correspondiente al puerto inalámbrico del router, mientras que la Dirección 1 sería el identificador propio de la red en la capa de enlace de datos.

6.2.2. Cálculo de la FCS

Para comprobar que no hubo errores en los bits de la trama, se procedió a calcular la FCS de la misma siguiendo el algoritmo descrito en la sección 5.2 que opera sobre su *Calculation Fields*, para compararlo con los 4 octetos que se muestran en la última fila de la tabla 6.2. Al seguir estas operaciones, se obtuvo que la FCS calculada era igual a la esperada, por lo que se afirma que no se produjeron errores en la comunicación y, por tanto, los valores de los bits en cada campo de la trama son correctos.

6.3. Conclusiones

Aplicando los procedimientos vistos en los capítulos 4 y 5, se analizó completamente un segundo paquete OFDM extraído del registro de mediciones.

Dentro del paquete se hallaron las direcciones MAC de los dispositivos y se extrajo la información de los otros campos de la trama, exceptuando el Frame Body, donde hay una restricción de acceso aplicada por el estándar como medida de seguridad proveniente de capas superiores, que indica que este campo está encriptado.

Con este resultado se cumple con el objetivo último del proyecto, que consiste en obtener las direcciones MAC de los dispositivos involucrados en una comunicación inalámbrica.

Asimismo, al haber sistematizado el proceso, las implementaciones realizadas permiten repetir el análisis para los paquetes restantes que contienen el registro de datos disponible o bien para nuevas mediciones que se realicen en el futuro. Con este procedimiento se encontrarán las direcciones MAC de los dispositivos y se determinará la función que cumplen, verificando a partir de la FCS que no hayan existido errores en la demodulación de la trama.

Capítulo 7

Conclusiones

En este proyecto integrador se ha estudiado el mecanismo de síntesis y demodulación de señales IEEE 802.11a con la motivación de identificar a los usuarios de dispositivos que no cumplen con las regulaciones establecidas e interfieren a los radares meteorológicos de banda C como los que existen en la República Argentina. La identificación de estos es posible a través de la lectura de su dirección MAC, la cual pasa en formato binario a las etapas de síntesis de capa física y es transmitida en cada paquete modulado en OFDM.

Para entender estos mecanismos, se ha remitido al documento normativo de la IEEE [9], que contiene las especificaciones de la capa física y la capa MAC del estándar IEEE 802.11a. Una vez entendida la composición de los paquetes que constituyen las señales, se implementaron los bloques necesarios para sintetizar las señales IEEE 802.11a en banda base a partir de los bits provenientes de la configuración y las capas superiores. Luego, se realizaron las implementaciones de las etapas correspondientes al proceso de demodulación. En ambos casos se contempló que puedan operar con cualquiera de las tasas de transmisión que establece la norma, las que quedan determinadas por el ancho de canal y fijan la modulación de cada subportadora y la tasa de codificación.

Con el propósito de validar las implementaciones de las etapas de codificación y entrelazado, y llevar a cabo pruebas de concepto de sus funcionalidades, se realizó un estudio de desempeño mediante simulaciones numéricas. Estas consistieron en estimar la tasa de error de bit en función de la relación energía de bit a nivel de densidad espectral de potencia del ruido para un esquema de modulación BPSK, considerando dos tipos de canales: AWGN y canal con desvanecimiento siguiendo el modelo de Clark. Los resultados permitieron verificar cómo estas etapas en conjunto permiten la corrección de errores reduciendo la BER para un mismo valor de E_b/N_0.

Una vez comprendido todo el proceso de demodulación, de haber implementado los bloques necesarios que permiten realizarla y de haber verificado uno a uno su correcto funcionamiento, se procedió a demodular paquetes de un registro de datos adquiri-

dos con un dispositivo de software definido por radio USRP de la empresa National Instruments. Se contaba con las muestras complejas correspondientes a la envolvente compleja a la salida del demodulador en cuadratura con el que se realizaron mediciones sobre una comunicación inalámbrica establecida entre un router y un teléfono celular.

En primer lugar, se llevó a cabo la detección de los paquetes. Para ello se evaluó la correlación de todo el registro de muestra complejas con la señal temporal correspondiente a la secuencia de símbolos cortos del Preámbulo, aprovechando la estructura determinística de esa señal, establecida por la norma y que se encuentra presente en cada paquete transmitido. Siguiendo el procedimiento mencionado, se identificaron varios paquetes a partir de los máximos locales del resultado. El paso siguiente consistió en la demodulación completa de uno de los paquetes detectados para extraer la información que contenía.

En los sistemas de modulación multiportadora que emplean OFDM existe una serie de imperfecciones que es necesario compensar [16] para evitar que incrementen la tasa de error de bit al momento de la detección. Las que se consideraron más dañinas fueron el error de sincronismo de portadora y la distorsión producida por el canal.

Para lidiar con el primero de estos problemas, se realizó una estimación del error de frecuencia mediante un procedimiento que consistía en calcular las correlaciones de secuencias de símbolos cortos del Preámbulo sintetizadas con la incorporación de un error de frecuencia en un determinado rango, y luego buscar qué valor correspondía al máximo de correlación obtenido. Con dicho valor, se pudo corregir el efecto del error de sincronismo de portadora para continuar con la demodulación del paquete.

El otro de los efectos considerados, la distorsión producida por el canal, ocurre como consecuencia de las múltiples trayectorias de los rebotes de la señal. El método de ecualización elegido consistió en hallar una estimación de la transferencia del canal y aplicar un filtro inverso. Para encontrar la respuesta en frecuencia del canal se utilizó la secuencia de símbolos largos del Preámbulo, debido a que también es una señal determinística conocida, con la característica que excita todas las subportadoras utilizadas por el sistema OFDM. Se tuvo en cuenta que la relación señal a ruido del registro de datos es elevada y, además, se supuso que el canal permanece invariante durante el intervalo de tiempo que dura la trasmisión de cada paquete, debido que se utilizó la misma transferencia para la demodulación de cada símbolo OFDM que compone la trama.

Una vez concluido todo el proceso de compensación de efectos degradantes, se verificó su funcionamiento. Debido a que el error de frecuencia es pequeño, el efecto sobre la constelación de la secuencia de símbolos cortos del Preámbulo se manifiesta como una rotación de la misma, que cambia con el tiempo, es decir con el conjunto de 4 símbolos cortos que se toman para determinarla. Se mostró que cuando se compensa dicho error empleando el valor que devuelve el algoritmo implementado, la constelación

permanece fija independientemente del conjunto de símbolo utilizado para evaluarla.

Por otro lado, para validar el método de ecualización se utilizó la constelación obtenida al demodular el símbolo SIGNAL que contiene la información de configuración de la transmisión. Se observó cualitativamente cómo al ecualizar se reduce la dispersión de las coordenadas correspondientes a la constelación BPSK que utiliza este símbolo.

Con los efectos degradantes compensados y una vez determinado el instante de inicio del primer símbolo OFDM del paquete, se procedió a demodularlos. Se comenzó por el primero de los símbolos, denominado SIGNAL en la norma, debido a que contiene información de configuración, como son la longitud del campo de datos, el tipo de modulación y la tasa de codificación empleada. Esto se realizó mediante las rutinas implementadas que llevan a cabo cada una de las etapas de la demodulación de señales IEEE 802.11a y sabiendo las características preestablecidas por el estándar para este símbolo. A partir de la información extraída del símbolo SIGNAL se demodularon los símbolos OFDM del campo de datos. Esto permitió obtener el conjunto de bits de fuente que contiene la información útil transportada sobre la capa física, lo que se conoce como PSDU.

El último paso consistió en analizar la PSDU desde el punto de vista de la subcapa MAC, con el propósito de interpretar la información que contiene. Para ello fue necesario estudiar la estructura general de la trama MAC, que está conformada por los bits de fuente del paquete IEEE 802.11a. Se verificó que el paquete fue transmitido sin errores, que cumplía con todas las especificaciones de la norma y se identificó como un paquete del tipo Ack, que contenía la dirección MAC del router utilizado en uno de los campos de su estructura.

Con el proceso sistematizado se realizó el mismo procedimiento para un segundo paquete, lo que permitió validar su correcto funcionamiento, a la vez que fue posible extraer información adicional relativa a la comunicación entre los dispositivos.

Como conclusiones finales, cabe destacar la implementación en MATLAB del conjunto de rutinas que permitió desde demodular las señales OFDM, pasando por la detección de las subportadoras, desentrelazador, decodificador y descrambler, hasta la interpretación de la trama de bits de fuente a nivel de subcapa MAC. Asimismo, se mostró que se puede extraer la dirección MAC de los usuarios que intervienen en este tipo de comunicación y que potencialmente se podrían identificar a los dispositivos que interfieren la operación de los radares meteorológicos con los que comparten la banda de trabajo.

Apéndice A

Tipos y Subtipos de tramas MAC

Dado a que la cantidad de combinaciones Tipo-Subtipo de las tramas MAC es muy grande debido a la cantidad considerable de funciones distintas que emplea el estándar para lograr una comunicación eficaz, estas no se mencionaron en la sección 5.1.1. Es por esto que se resumieron en la tabla A.1 las funciones que realiza un paquete según los valores de los campos Tipo y Subtipo del Frame Control.

Tipo ‘B2 B3’	Descripción del Tipo	Subtipo ‘B4 B5 B6 B7’	Descripción del Subtipo
‘00’	Management	‘0000’	Solicitud de asociación
‘00’	Management	‘1000’	Respuesta de asociación
‘00’	Management	‘0100’	Solicitud de reasociación
‘00’	Management	‘1100’	Respuesta de reasociación
‘00’	Management	‘0010’	Solicitud de prueba
‘00’	Management	‘1010’	Respuesta de prueba
‘00’	Management	‘0110’	Aviso de tiempo
‘00’	Management	‘1110’	Reservado
‘00’	Management	‘0001’	Baliza
‘00’	Management	‘1001’	ATIM
‘00’	Management	‘0101’	Desasociación
‘00’	Management	‘1101’	Autenticación
‘00’	Management	‘0011’	Desautenticación
‘00’	Management	‘1011’	Acción
‘00’	Management	‘0111’	Acción sin Ack
‘00’	Management	‘1111’	Reservado
‘10’	Control	‘0000 $\sim$ 1100’	Reservado
‘10’	Control	‘0010’	Beamforming Report Poll

Continúa en la página siguiente

Tipo ‘B2 B3’	Descripción del Tipo	Subtipo ‘B4 B5 B6 B7’	Descripción del Subtipo
‘10’	Control	‘1010’	Anuncio VHT NDP
‘10’	Control	‘0110’	Extensión del Frame Control
‘10’	Control	‘1110’	Envoltura de Control
‘10’	Control	‘0001’	BlockAckReq
‘10’	Control	‘1001’	BlockAck
‘10’	Control	‘0101’	PS-Poll
‘10’	Control	‘1101’	RTS
‘10’	Control	‘0011’	CTS
‘10’	Control	‘1011’	Ack
‘10’	Control	‘0111’	CF-End
‘10’	Control	‘1111’	CF-End + CF-Ack
‘01’	Data	‘0000’	Data
‘01’	Data	‘1000’	Data + CF-Ack
‘01’	Data	‘0100’	Data + CF-Poll
‘01’	Data	‘1100’	Data + CF-Ack + CF-Poll
‘01’	Data	‘0010’	Null (sin datos)
‘01’	Data	‘1010’	Null + CF-Ack
‘01’	Data	‘0110’	Null + CF-Poll
‘01’	Data	‘1110’	Null + CF-Ack + CF-Poll
‘01’	Data	‘0001’	QoS Data
‘01’	Data	‘1001’	QoS Data + CF-Ack
‘01’	Data	‘0101’	QoS Data + CF-Poll
‘01’	Data	‘1101’	QoS Data + CF-Ack + CF-Poll
‘01’	Data	‘0011’	QoS Null
‘01’	Data	‘1011’	Reservado
‘01’	Data	‘0111’	QoS Null + CF-Poll
‘01’	Data	‘1111’	QoS Null + CF-Ack + CF-Poll
‘11’	Extension	‘0000’	Baliza DMG
‘11’	Extension	‘1000’∼‘1111’	Reservado

Tabla A.1: Descripción de las funciones de las tramas según su Tipo y Subtipo.

Las tramas que tienen Tipo = ‘10’ y Subtipo = ‘0110’ cuentan con un campo dentro del Frame Control llamado Control Frame Extension de 4 bits y su estructura es la de la figura 5.2b. Las funciones de estas tramas particulares se resumen en la tabla A.2.

Control Frame Extension ‘B8 B9 B10 B11’	Descripción
‘0000’∼‘1000’	Reservado
‘0100’	Poll
‘1100’	SPR
‘0010’	Grant
‘1010’	DMG CTS
‘0110’	DMG DTS
‘1110’	Grant Ack
‘0001’	SSW
‘1001’	SSW-Feedback
‘0101’	SSW Ack
‘1101’∼‘1111’	Reservado

Tabla A.2: Descripción de las funciones de las tramas de Control con extensión.

Una vez que se conoce la función de una trama, se puede saber qué campos de la estructura general mostrada en la figura 5.1 están presentes en esta, para así poder extraer su información.

Apéndice B

Proyecto y diseño

Las actividades de proyecto y diseño son inherentes a este tipo de trabajos. Sin embargo, en el presente Proyecto Integrador cabe destacar una instancia en particular que involucró específicamente proyecto y diseño: desarrollo de un algoritmo de demodulación de señales correspondientes a la trama IEEE 802.11a con modulación OFDM.

Esta instancia involucró: la revisión de los conceptos teóricos de las distintas etapas que componen el demodulador de señales OFDM (FFT, detección de subportadoras, desentrelazador, decodificador, descrambler); el diseño de las distintas etapas que componen el demodulador; la implementación en lenguaje de programación de alto nivel de abstracción de los algoritmos que cumplen con las funciones requeridas en cada etapa; y finalmente la validación de su funcionamiento.

Por otro lado, fue necesario revisar el diseño original del demodulador teniendo en cuenta las imperfecciones del canal y del receptor, tales como la distorsión y los errores de sincronismo. Lo que llevó a incorporar soluciones a estas problemáticas, implementarlas y validar nuevamente el funcionamiento. Cabe remarcar que en todo el proceso los diseños propuestos fueron contrastados contra simulaciones numéricas y luego empleando mediciones reales.

Las actividades en relación a este tema se encuentran descriptas en diferentes pasajes de los Capítulos 3, 4 y 5, respectivamente.

Por último, se deja constancia que las actividades de proyecto y diseño desarrolladas por Daniel Milanés Chau superaron las 200 horas requeridas para el Proyecto Integrador.

Juan Pablo Pascual	Fabián Rinalde

Bibliografía

[1] ITU-R Res. 229 [COM5/16]. Use of the bands 5150-5250 MHz, 5250-5350 MHz and 5470-5725 MHz by the mobile service for the implementation of wireless access systems including radio local area networks. En: The World Radiocommun. Conf. (WRC-03). Ginebra, 2003. 1

[2] Rojas, L., Moisseev, D., Chandrasekar, V., Selzler, J., Keränen, R. Dual-polarization spectral filter for radio frequency interference suppression. En: 7th Eur. Conf. Radar Meteorol. Hydrol. (ERAD). Toulouse, France, 2012. 1

[3] Saltikoff, E., Cho, J., Tristant, P., Huuskonen, A., Allmon, L., Cook, R., *et al.* The threat to weather radars by wireless technology. *Bulletin of the American Meteorological Society*, **97** (7), 1159–1167, ago. 2016. 1

[4] Rodríguez, A., Lacunza, C., Serra, J., Saulo, C., Ciappesoni, H., Caranti, G., *et al.* SiNaRaMe: Integración de una red de radares hidro-meteorológicos en latinoamérica. *Rev. Fac. Ciencias Exac., Fís. y Nat.*, **4** (1), 41–48, mar. 2017. 2

[5] Petracca, G., Lugo, J. Mitigation of WLAN/RLAN interference in meteorological radar using wavelet filtering. En: XIV Reunión Trab. Proc. Inf. y Control (RPIC'17), págs. 1–6. Mar del Plata, Argentina, 2017. 2

[6] Leal, O. B., Rinalde, F., Cogo, J., Pascual, J. WLAN signal detection in weather radar data. En: Actas de la XIX Reunión de Trabajo Procesamiento de la Información y Control (RPIC'21). San Juan, Argentina, 2021. 2

[7] Cogo, J., Collado Rosell, A., j. Areta, Pascual, J. Weather radar receiver identification for improving wi-fi interference detection. En: Actas de la XIX Reunión de Trabajo Procesamiento de la Información y Control (RPIC'21). San Juan, Argentina, 2021. 2

[8] Richards, M. A. Fundamentals of Radar Signal Processing. New York: McGraw-Hill, 2005. 2

[9] IEEE Computer Society LAN MAN Standards Committee, *et al.* Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *IEEE Std 802.11*, 2016. 2, 3, 13, 15, 17, 24, 31, 48, 49, 51, 63

[10] Intini, A. L. Orthogonal frequency division multiplexing for wireless networks multiplexing for wireless networks. *University of California–Santa Barbara*, págs. 15–34, 2000. 6

[11] Chadha, A., Satam, N., Ballal, B. Orthogonal frequency division multiplexing and its applications, Sep 2013. URL https://arxiv.org/abs/1309.7334v1. 6

[12] Omura, J., Levitt, B. Coded error probability evaluation for antijam communication systems. *IEEE Transactions on Communications*, **30** (5), 896–903, 1982. 25, 27

[13] Tse, D., Viswanath, P. Fundamentals of wireless communication. Cambridge university press, 2005. 27, 28, 29

[14] Zrnić, D. S. Simulation of weatherlike doppler spectra and signals. *Journal of Applied Meteorology*, **14** (4), 619–620, 1975. 29

[15] ITU-T V.42: Error-correcting procedures for dces using asynchronous-to-synchronous conversion, 1993. URL https://www.itu.int/rec/T-REC-V.42/en. 50

[16] Liu, H., Li, G. OFDM-based broadband wireless networks: design and optimization. John Wiley & Sons, 2005. 64

Agradecimientos

Me cuesta creer que se haya llegado hasta este punto cuando hace unos años parecía tremenda utopía. La culminación de mis estudios de grado es debida al trabajo de todos los docentes que a lo largo de mi vida contribuyeron a mi formación y a los maravillosos compañeros que tuve y que se han vuelto valiosas amistades, tanto los caballitos de la CUJAE como los de *Teleski & Co*. También quiero agradecer a Alma Flor Ada e Isabel Campoy, quienes hicieron posible que pudiera estudiar fuera de mi país, lo que transformó mi vida positivamente tanto en lo profesional como en lo personal. Entre los docentes por cuyas aulas pasé, se encuentra el Dr. Juan Pablo Pascual, quien realizó la dirección de este proyecto y me tuvo bastante paciencia durante el desarrollo del mismo, por lo que le agradezco profundamente. Y agradezco de todo corazón a mis padres y a mi hermana por apoyarme en todo momento y hacerme crecer como ser humano.