

TRABAJO FIN DE GRADO
INGENIERÍA DE TECNOLOGÍAS DE TELECOMUNICACIÓN

Sincronización en redes 5G: dispositivo final

Captura y decodificación de señales de sincronización en
equipos reales

Autor

Ángel Gómez Hurtado

Directores

Jorge Navarro Ortiz

Lorena Chinchilla Romero



ESCUELA TÉCNICA SUPERIOR DE INGENIERÍAS INFORMÁTICA Y DE
TELECOMUNICACIÓN

Granada, 13 de julio de 2023

Sincronización en redes 5G: dispositivo final

Captura y decodificación de señales de sincronización en
equipos reales.

Autor

Ángel Gómez Hurtado

Directores

Jorge Navarro Ortiz

Lorena Chinchilla Romero



DEPARTAMENTO DE TEORÍA DE LA SEÑAL, TELEMÁTICA
Y COMUNICACIONES

—
Granada, 13 de julio de 2023

Sincronización en redes 5G: dispositivo final

Ángel Gómez Hurtado

Palabras clave: 5G, sincronización, SIBs

Resumen

Con la llegada de Fifth Generation (5G) en los últimos años han emergido diversos casos de uso con demandas de requisitos de red específicos. La industria 4.0 es uno de los casos que ha experimentado un crecimiento significativo en diversas áreas en las últimas décadas. Desde mejorar la capacidad de movilidad hasta lograr una sincronización precisa entre dispositivos, se han planteado diferentes necesidades. Este proyecto se enfoca precisamente en la sincronización precisa de múltiples dispositivos inalámbricos.

En este documento, se presentan las señales 5G poniendo una atención especial a las señales de sincronización. Se describe con gran precisión sus características físicas de transmisión, su estructura y la información que transportan. Posteriormente, se realiza un análisis de señales 5G, utilizando tanto señales sintéticas generadas mediante una aplicación de la *toolbox* de MATLAB, como señales reales transmitidas por la estación base de Amari-soft. Además, se examinarán los mensajes necesarios para la sincronización de los dispositivos, destacando el mensaje denominado System Information Block (SIB)9. Sin embargo, para decodificar este mensaje, es necesario realizar la decodificación de otros mensajes previos, como el Master Information Block (MIB) o el SIB1, los cuales se han abordado en detalle en este documento.

Synchronization in 5G Networks: End Device

Ángel Gómez Hurtado

Keywords: 5G, synchronization, SIBs

Abstract

With the arrival of 5G in recent years, various use cases with specific network requirements have emerged. Industry 4.0 is one of the cases that has experienced significant growth in different areas over the past decades. From improving mobility capabilities to achieving precise synchronization between devices, different needs have been raised. This project specifically focuses on the precise synchronization of multiple wireless devices. In this document, 5G signals are presented with special attention to synchronization signals. Their transmission physical characteristics, structure, and the information they carry are described with great precision. Subsequently, an analysis of 5G signals is performed using both synthetic signals generated through a MATLAB toolbox application and real signals transmitted by the Amarisoft base station. Furthermore, the necessary messages for device synchronization will be examined, highlighting the message called SIB9. However, to decode this message, it is necessary to perform the decoding of previous messages such as MIB or SIB1, which have been addressed in detail in this document.

Yo, **Ángel Gómez Hurtado**, alumno de la titulación Grado en Ingeniería de Tecnologías de Telecomunicación de la **Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación de la Universidad de Granada**, con DNI 77770549M, autorizo la ubicación de la siguiente copia de mi Trabajo Fin de Grado en la biblioteca del centro para que pueda ser consultada por las personas que lo deseen.

Fdo: Ángel Gómez Hurtado

Granada, a 13 de julio de 2023.

D. **Jorge Navarro Ortiz**, Profesor del Área de Ingeniería Telemática del Departamento de Teoría de la Señal, Telemática y Comunicaciones de la Universidad de Granada.

D. **Lorena Chinchilla Romero**, estudiante de doctorado del Área de Ingeniería Telemática del Departamento de Teoría de la Señal, Telemática y Comunicaciones de la Universidad de Granada.

Informan:

Que el presente trabajo, titulado *Sincronización en redes 5G: dispositivo final*, ha sido realizado bajo su supervisión por **Ángel Gómez Hurtado**, y autoriza la defensa de dicho trabajo ante el tribunal que corresponda.

Y para que conste, expide y firma el presente informe en Granada, a 13 de julio de 2023.

Los directores:

Jorge Navarro Ortiz

Lorena Chinchilla Romero

Agradecimientos

Hace 4 años empezó esta etapa que acaba ahora. Una etapa en la que he crecido como persona y en la que he adquirido conocimiento y más preguntas que espero responder. He tenido la suerte de no recorrerla solo, sino rodeado de buena gente. Gente que siempre quiso lo mejor para mí. Es por ello que me gustaría agradecer a:

Mi tutor Jorge Navarro, por todas las horas dedicadas, no solo en las reuniones, sino también esas horas extras que le ha dedicado para que pudiera seguir avanzando en mi proyecto. También por las correcciones y los consejos a la hora de redactar, los cuales ha hecho que haya mejorado mi forma de escribir.

Mi familia, por haber confiado en mí y en mi trabajo, dejándome trabajar como mejor sé. Cuidando de mí y haciendo que el camino haya sido lo más liviano posible.

Mis amigos, quienes han hecho que me lo haya pasado bien y que haya podido despejar la cabeza cuando más saturado estaba. El descanso también es parte del trabajo.

Por último, me gustaría hacer una mención especial a mi co-tutora, Lorena Chinchilla. Sin ella, este proyecto no hubiese salido como ha salido. Gracias de verdad por el tiempo dedicado, por los consejos y por la ayuda dada. No solo me has demostrado ser una gran profesional, sino también una gran persona. Un placer haberte conocido.

Índice general

Siglas	6
1. Introducción	7
1.1. Motivación	8
1.2. Objetivos	9
1.3. Estructura del documento	9
2. Estado del arte	13
3. Planificación y estimación de costes	15
3.1. Planificación de tareas	15
3.2. Planificación de recursos	18
3.2.1. Recursos hardware.	18
3.2.2. Recursos software.	18
3.2.3. Recursos humanos.	18
3.3. Presupuesto	19
4. Fundamento Teórico	21
4.1. Canal y señal	21
4.2. Estructura de una trama en 5G	25
4.3. Canales implicados en la obtención del mensaje SIB9.	28
4.3.1. PBCH	28
4.3.2. PDCCH	30
4.3.3. PDSCH	31
4.4. Mensajes implicados en la obtención del SIB9.	31
4.4.1. MIB	31
4.4.2. Mensajes SIBs	33
4.5. Sincronización en 5G	45
4.5.1. SS/PBCH BLOCKS AND BURSTS	45
PSS	46
SSS	46

5. Herramientas usadas.	47
5.1. USRP-2901	47
5.2. srsRAN	48
5.3. Amarisoft	49
5.4. Toolbox 5G MATLAB	49
6. Análisis de una señal 5G sintética usando la toolbox 5G de MATLAB y análisis de señales 5G reales	51
6.1. Transmisión y recepción de una señal sintética	51
6.2. Análisis bits de los mensajes MIB y SIB1 procedentes de una transmisión con el software srsRAN	59
6.3. Análisis mensajes MIB y SIBs procedentes de una señal transmitida mediante la estación base de Amarisoft	66
7. Conclusiones	83
7.1. Conclusiones	83
7.2. Trabajo futuro	85
Bibliografía	89
A. Función pcapSIB1	91

Índice de figuras

3.1. Diagrama de Gantt.	17
4.1. Mapa canales y señales para Up-link (UL)	22
4.2. Mapa canales y señales para Down-link (DL)	23
4.3. Canales y señales contenidos en el canal PBCH.	24
4.4. Canales y señales contenidos en el canal PDSCH	25
4.5. Estructura trama en 5G según el valor de μ	26
4.6. Posicionamiento de los SSBlock en los símbolos OFDM.	28
4.7. Opciones mapeado de la señal DMRS dentro del canal PBCH para pccmod 4.	29
4.8. Compensación Bloques de Recursos.	35
4.9. Compensación Bloques de Recursos en espectrograma.	35
4.10. Duración del canal tanto en símbolos como en frecuencia.	36
4.11. Estructura general Synchronization Signal (SS)/Physical Broad- cast Channel (PBCH) BLOCKS	45
4.12. Ejemplo Physical Layer Cell Identity (PCI) mod3.	46
5.1. USRP-2901	47
5.2. Componentes e interfaces gNB del srsRAN proyect.	49
5.3. Estación base Amarisoft.	50
6.1. Espectrograma señal sintética.	52
6.2. Espectrograma señal sintética parte bloque SS/PBCH.	53
6.3. Espectrograma señal sintética parte canales PDSCH y PDCCH.	53
6.4. PSS señal sintética.	54
6.5. SSS señal sintética.	55
6.6. SNR de cada SSB.	55
6.7. Constelación PBCH.	56
6.8. Contenido MIB señal sintética.	56
6.9. Cuadrícula de recursos recibida.	57
6.10. Constelación PDCCH.	57
6.11. Slot que contiene el PDSCH a decodificar.	58
6.12. Constelación PDSCH.	58

6.13. Datos mostrados por pantalla por el programa.	59
6.14. Espectrograma trozo señal transmitida mediante srsRAN. . .	61
6.15. Detección PSS señal transmitida mediante srsRAN.	61
6.16. Detección SSS señal transmitida mediante srsRAN.	62
6.17. Datos MIB de la señal transmitida mediante srsRAN.	62
6.18. Ranura que contiene a los canales PDCCH y PDSCH de la señal transmitida mediante srsRAN.	63
6.19. Constelación canal PDSCH de la señal transmitida mediante srsRAN.	63
6.20. Contenido general SIB1 de transmisión con srsRAN.	64
6.21. Contenido campo <i>cellSelectionInfo</i> SIB1.	64
6.22. Contenido campo <i>cellAccessRelatedInfo</i> SIB1 original. . . .	65
6.23. Contenido campo <i>cellAccessRelatedInfo</i> SIB1 decodificado. .	66
6.24. Contenido campo <i>connEstFailureControl</i> SIB1.	66
6.25. Contenido campo <i>servicingCellConfigCommonDowlink</i> SIB1.	67
6.26. Contenido campo <i>servicingCellConfigCommonUplink</i> SIB1. .	67
6.27. Contenido campo <i>servicingCellConfigCommon</i> Parte3 SIB1. .	68
6.28. Contenido campo <i>ueTimerConstants</i> SIB1.	68
6.29. Espectrograma trozo señal Amarisoft.	69
6.30. Detección PSS señal Amarisoft.	70
6.31. Detección SSS señal Amarisoft.	70
6.32. MIB decodificado de la señal de Amarisoft.	71
6.33. Haces detectados de la señal de Amarisoft.	71
6.34. Constelación PDCCH de la señal de Amarisoft.	72
6.35. Cuadrícula de recursos recibida de la señal de Amarisoft. . .	72
6.36. Constelación PDSCH de la señal de Amarisoft.	73
6.37. Datos mostrados por pantalla de la señal Amarisoft.	73
6.38. Comparación campo <i>cellSelectionInfo</i> SIB1 señal Amari- soft.	74
6.39. Campo <i>cellAccessRelatedInfo</i> SIB1 de la señal de Amarisoft original.	74
6.40. Campo <i>cellAccessRelatedInfo</i> SIB1 de la señal de Amarisoft decodificada.	75
6.41. Comparación campo <i>connEstFailureControl</i> SIB1 de la señal de Amarisoft.	75
6.42. Comparación campo <i>ue – TimersAndConstants</i> SIB1 de la señal de Amarisoft.	76
6.43. Comparación campo <i>servicingCellConfigCommon_DL</i> SIB1 de la señal de Amarisoft.	76
6.44. Comparación campo <i>servicingCellConfigCommon_UL</i> SIB1 de la señal de Amarisoft.	77
6.45. Resto comparación campo <i>servicingCellConfigCommon</i> SIB1 de la señal de Amarisoft.	78

6.46. Constelación canal PDSCH de la señal de Amarisoft no demodulado.	79
6.47. Espectrograma de la señal capturada de ancho de banda de 15 MHz transmitida con la estación base de Amarisoft.	79
6.48. Constelación del canal PDSCH de la señal capturada de ancho de banda de 15 MHz transmitida con la estación base de Amarisoft.	80
6.49. Constelación del canal PDSCH de la señal capturada de ancho de banda de 20 MHz transmitida con la estación base de Amarisoft.	80
6.50. Campo <i>si - SchedulingInfo</i> del SIB1 de la señal de Amarisoft.	81
6.51. Contenido del mensaje SIB9 de la señal de Amarisoft.	81

Índice de tablas

3.1. Tabla resumen de las horas dedicadas al TFG.	16
3.2. Características del portatil.	18
3.3. Recursos humanos necesarios para la elaboración del Trabajo de Fin de Grado (TFG).	18
3.4. Tabla estimación precio supuesto por mi uso.	19
3.5. Presupuesto final.	20
4.1. Valor μ en función de la separación entre subportadoras . . .	25
4.2. Duración del símbolo Orthogonal Frequency-Division Multiplexing (OFDM) en función de la separación entre subportadoras	26
4.3. Resumen estructura trama según μ	27
4.4. Características de los casos según separación entre subportadoras	27
4.5. Estructura del MIB	32
4.6. Tabla configuración Control Resource Set (CORESET) para separación entre subportadoras 15 KHz en SS/PBCH y del Physical Down-Link Control Channel (PDCCH).	34
4.7. Tabla configuración CORESET para separación entre subportadoras 30 KHz en SS/PBCH y del PDCCH.	36
4.8. Tabla valor <i>searchSpaceZero</i> para FR1 y patrón de multiplexación 1.	37
4.9. Contenido SIB1.	38
4.10. Parámetro si-SchedulingInfo.	39
4.11. Parámetro servingCellConfigCommon Parte 1.	40
4.12. Parámetro servingCellConfigCommon Parte 2.	41
4.13. Parámetro servingCellConfigCommon Parte 3.	42
4.14. Parametros uac-BarringInfo.	43
5.1. Características transmisión USRP-2901	48
5.2. Características recepción USRP-2901	48
6.1. Datos de generación de la señal de srsRAN.	60
6.2. Datos de generación de la señal de Amarisoft.	68

Siglas

1G First Generation.

3GPP Third Generation Partnership Project.

4G Fourth Generation.

5G Fifth Generation.

BCCH Broadcast Control Channel.

BCH Broadcast Channel.

BS Base Station.

BTS Base Transceiver Station.

C Cell.

CCCH Common Control Channel.

CORESET COntrol REsource SET.

CRC Cyclic Redundancy Check.

CS Configured Scheduling.

CSIRS Channel State Information Reference Signal.

CU Centralized Unit.

DCCH Dedicated Control Channel.

DCI Down-link Control Information.

DL Down-link.

DMRS Demodulation Reference Signal.

DTCH Dedicated Traffic Channel.

DU Distributed Unit.

eMBB enhanced Mobile Broadband.

FR1 Frequency Range 1.

FR2 Frequency Range 2.

GPS Global Positioning System.

IaaS Infrastructure as a Service.

IoT Internet of Things.

MAC Medium Access Control.

MCS Modulation Coding Scheme.

MIB Master Information Block.

mMTC massive Machine Type Communication.

NI National Instruments.

NR New Radio.

OFDM Orthogonal Frequency-Division Multiplexing.

P Paging.

PaaS Platform as a Service.

PBCH Physical Broadcast Channel.

PCCH Paging Control Channel.

PCH Paging Channel.

PCI Physical Layer Cell Identity.

PDCCH Physical Down-Link Control Channel.

PDSCH Physical Down-Link Shared Channel.

PLMN Public Land Mobile Network.

PRACH Physical Random Access Channel.

PSS Primary Synchronisation Signal.

PTRS Phase Tracking Reference Signal.

PUCCH Physical Up-link Control Channel.

PUSCH Physical Up-link Shared Channel.

QAM Quadrature Amplitude Modulation.

QCL Quasi Co-Location.

QPSK Quadrature Phase-Shift Keying.

RA Random Access.

RACH Random Access Channel.

RLC Radio Link Control.

RNTI Radio Network Temporary Identifier.

RRC Radio Resource Control.

SaaS Software as a Service.

SCH Shared Channel.

SDR Software Defined Radio.

SFN System Frame Number.

SI System Information.

SIB System Information Block.

SNR Signal-to-Noise Ratio.

SRB Signalling Radio Bearer.

SRS Sounding Reference Signal.

SS Synchronization Signal.

SSS Secondary Synchronization Signal.

TC Temporary Cell.

TFG Trabajo de Fin de Grado.

TRS Tracking Reference Signal.

UAC Unified Access Control.

UCI Up-link Control Information.

UE User Equipment.

UL Up-link.

URLLC Ultra Reliable Low Latency Communication.

USRP Universal Software Radio Peripheral.

UTC Coordinated Universal Time.

Capítulo 1

Introducción

Desde el comienzo de la primera generación de redes móviles (conocida como First Generation (1G)) hasta la generación actual (Fifth Generation (5G)) las necesidades de los usuarios han cambiado de forma drástica, así como el número de dispositivos usados, que se han incrementado de forma exponencial. Estas necesidades de los usuarios y las aplicaciones de los dispositivos actuales pasan por un abanico muy amplio, que implica desde la navegación automática hasta la cirugía a distancia, entre otros. La tecnología 5G surge como respuesta a dichas necesidades, permitiendo que la realización de estas sea posible. Para ello, 5G muestra un abanico de capacidades amplio tal que permita satisfacer las necesidades de los usuarios, entre las cuales podemos destacar un aumento del espectro usado para poder transmitir a nuevas frecuencias anteriormente no usadas, un ensanchamiento en el ancho de banda usado para poder aumentar la capacidad de envío masivo de datos, una mayor robustez para las conexiones críticas, capacidad para optimizar la energía, capacidad de movilidad por parte del usuario para casos automovilísticos, y latencias mínimas para poder hacer que una red entera trabaje de forma coordinada. Esta última característica es clave y crucial para muchas aplicaciones y servicios que emergen en 5G, y es lo que motiva la realización de este proyecto [1].

5G habilita además la aparición de nuevos servicios y paradigmas de modelos de negocio, tales como las Infrastructure as a Service (IaaS), las Software as a Service (SaaS) o las Platform as a Service (PaaS), en las que se proporciona a los usuarios de una infraestructura virtualizada, quitando la necesidad de tener todo el hardware de red específico, y un entorno de desarrollo y despliegue de aplicaciones virtualizado, respectivamente. Asimismo, el diseño de la arquitectura de los sistemas 5G basada en servicios permite una gran flexibilidad para optimizar el uso de la red y sus recursos, de forma que una gran variedad de casos de usos demandantes de distintos tipos de servicios pueden ser ofrecidos. Los distintos tipos de servicios soportados por 5G son clasificados en tres categorías, denominadas enhanced Mobile Broadband

(eMBB), massive Machine Type Communication (mMTC) y Ultra Reliable Low Latency Communication (URLLC). Los sistemas 5G no solo prometen una mejora en el ancho de banda ofrecido por usuario (eMBB), sino que también prometen la capacidad de soportar comunicaciones extremadamente fiables y con muy baja latencia (URLLC), y la capacidad de tener muchos dispositivos conectados simultáneamente (mMTC) para aplicaciones de ciudades o industrias inteligentes (paradigma conocido como Internet of Things (IoT)).

Tal y como se ha mencionado anteriormente, el rendimiento superior que ofrece 5G en comparación con otras tecnologías ha dado lugar a la aparición de innovaciones como la agricultura inteligente o la industria 4.0, entre otras. Una de las capacidades de 5G que ha hecho posible todo esto es la sincronización entre terminales y la red de acceso radio. Una mayor sincronización garantiza una red más fiable y eficiente, lo cual conlleva una mejora en la capacidad de la red mediante el aprovechamiento óptimo del espectro y el tiempo en las transmisiones. Esto se traduce en una mayor tasa de datos, menos colisiones y una mayor cantidad de dispositivos conectados a la red. Además, la sincronización es esencial para aplicaciones sensibles a la latencia, como la asistencia sanitaria a distancia o la automoción inteligente, ya que permite un rendimiento óptimo en situaciones en las que el tiempo es un factor crítico. Asimismo, 5G ofrece una mayor movilidad a los usuarios tanto a nivel intra-celda como a nivel intra-red, lo que hace que la sincronización entre celdas y redes sea necesaria para facilitar estos procesos.

Esta sincronización no es fácil de lograr, ya que los dispositivos (a los que nos referiremos también como User Equipment (UE) a lo largo del documento) requieren mecanismos para detectar las señales de la estación base (a la que nos referiremos como Base Station (BS) a lo largo de este documento) y sincronizarse rápidamente en tiempo, frecuencia y fase con ella. Para ello, se utilizan secuencias al inicio de cada señal que permiten a cada dispositivo detectarlas y sincronizarse adecuadamente. Además de la información básica de sincronización, la BS también manda la hora en Coordinated Universal Time (UTC) dentro de algunos mensajes de señalización, la cual es útil para algunos servicios, que se estudiarán en el proyecto [2].

1.1. Motivación

En el siglo XXI se ha producido un gran incremento de entidades conectadas entre sí, desde el ámbito de la seguridad hasta en el ámbito automovilístico, pasando por muchos otros. Esto ha hecho que se den muchos escenarios en los que las prestaciones, tales como la tasa de datos, la movilidad, la latencia, la fiabilidad o la cobertura, entre otras, necesarias sean variadas. Por ejemplo, el control de tráfico y conducción automático necesita

una gran capacidad de movilidad, baja latencia, gran fiabilidad y cobertura, pero no es crítico el envío de datos de manera masiva, sin embargo, para la cirugía remota, la capacidad de movilidad no es necesaria, pero es crítico el envío de datos masivos, la latencia y la fiabilidad.

La Industria 4.0 necesita que todos los dispositivos que pertenecen a una misma red tengan una sincronización máxima en cuanto a la hora de sus relojes internos para poder optimizar todas estas prestaciones, y es aquí donde entra el proceso de sincronización que se estudiará en este Trabajo de Fin de Grado (TFG). El bloque de la señal que permite esta sincronización se llama System Information Block (SIB)9, el cual transporta la hora UTC de la estación base, y será el objeto final de estudio de este documento.

Los resultados de este TFG serán utilizados en un proyecto de investigación denominado 6G-CHRONOS[3]. Un proyecto del grupo de investigación WiMuNet, del Departamento de Teoría de la Señal, Comunicaciones y Telemática de la UGR. Es un proyecto que ha sido subvencionado a nivel nacional por el ministerio de Asuntos Económicos y Transformación Digital de España, cuyo objetivo es conseguir que la red 5G proporcione una comunicación determinista, confiable, de gran ancho de banda y de baja latencia. Además, tiene como objetivo conseguir una integración fluida entre TSN y 5G.

1.2. Objetivos

El objetivo de este trabajo es estudiar y analizar las señales 5G para así poder hallar la manera de recibir y decodificar el mensaje SIB9 de una señal real 5G. Esto no será directo, pues, como se verá en el capítulo de teoría 4, necesitaremos decodificar otros mensajes anteriores a este, tales como el mensaje Master Information Block (MIB) y el mensaje SIB1 (descritos en las secciones 4.4.1 y 4.4.2, respectivamente). Por lo tanto, tendremos subobjetivos tales como:

- Saber detectar señales 5G y poder sincronizarnos a la BS mediante la detección y demodulación del Synchronization Signal (SS)/Physical Broadcast Channel (PBCH)Burst.
- La posterior detección y demodulación de los canales Physical Down-Link Control Channel (PDCCH) y Physical Down-Link Shared Channel (PDSCH) (descritos en las secciones 4.3.2 y 4.3.3, respectivamente) para la detección de los mensajes SIBs.

1.3. Estructura del documento

En esta sección se explican brevemente en que van a consistir cada una de las partes del proyecto.

1. **Capítulo 1: Introducción.** En este primer capítulo, se pretende poner en contexto sobre el proyecto al lector.
 - a) Motivación. Se expone el porqué del estudio que se va a realizar en esta memoria.
 - b) Objetivos. Se presenta el problema que se pretende abordar y solucionar durante el proyecto.
 - c) Estructura del documento. Se muestra la organización del mismo.
2. **Capítulo 2: Estado del arte.** En este capítulo se presentan proyectos que tienen relación con este TFG.
3. **Capítulo 3: Planificación y estimación de costes.** En este tercer capítulo se detalla como ha sido la planificación llevada a cabo para la realización de la memoria, así como la estimación de los costes producidos.
 - a) Planificación de tareas. Se describe una planificación inicial de las tareas.
 - b) Planificación de recursos. Se listan los recursos hardware, software y humanos que han sido requeridos para la realización del mismo, así como los costes asociados a cada uno de ellos.
 - c) Presupuesto. Se hace un resumen de los costes totales asociados al proyecto.
4. **Capítulo 4: Marco teórico.** En este capítulo se desglosa la parte teórica que es necesaria conocer para entender las señales 5G usadas en este proyecto.
 - a) Canal y señal. Se habla sobre cómo está estructurado el canal para la transmisión de señales 5G y de cómo puede ser transmitida la señal según las especificaciones Third Generation Partnership Project (3GPP).
 - b) Estructura de una trama en 5G. Se presentan las posibles configuraciones que tienen las tramas en 5G.
 - c) Canales implicados en la obtención del SIB9. Se explican los canales implicados en la obtención del mensaje SIB9.
 - d) Bloques de información implicados en la obtención del SIB9. Se explican los mensajes que son necesarios para poder obtener el mensaje SIB9.
 - e) Sincronización en 5G. Se exponen con un poco más de detalle qué bloques dentro de la señal de 5G se utilizan para realizar la sincronización con la estación base en 5G.

-
5. **Capítulo 5: Herramientas usadas.** En este capítulo se describen las herramientas tanto hardware como software usadas para la realización de las tareas descritas en el capítulo 6.
 6. **Capítulo 6: Análisis de una señal 5G sintética usando la toolbox 5G de MATLAB y análisis de señales 5G reales.** En este capítulo se explican el proceso seguido y los resultados de cada una de las pruebas que se han realizado para el análisis de las señales 5G.
 7. **Capítulo 7: Conclusiones.** En este último capítulo se exponen las conclusiones que se pueden sacar de los resultados obtenidos.

Capítulo 2

Estado del arte

En este capítulo, se examinará el estado del arte sobre la sincronización en la tecnología 5G, un elemento crucial para el funcionamiento eficiente de las redes de próxima generación. Se realizará un análisis de algunas de las investigaciones más recientes y de los avances tecnológicos en el campo de la sincronización en 5G. Se explorarán los enfoques y técnicas utilizados para lograr una sincronización confiable, así como las soluciones innovadoras que han surgido para superar los desafíos existentes.

Mediante la comprensión de este estado del arte en sincronización en 5G, se sentará una base sólida para el desarrollo de nuestro proyecto, permitiéndonos aprovechar los conocimientos y avances más recientes en el campo para abordar los desafíos específicos y lograr una sincronización óptima en nuestro entorno de trabajo. Son varios los proyectos encontrados en la literatura existente los que abordan de alguna forma el procedimiento de sincronización en 5G New Radio (NR) [4, 5, 6, 7, 8, 9], los cuales describiremos a continuación.

El primer proyecto del que se va a hablar es el proyecto de la referencia [4]. En este proyecto se describen los bloques que tiene el SSBlock y de cómo se realiza la sincronización de la trama y la búsqueda del número de la celda en la que se encuentra el dispositivo. También realiza un estudio sobre cómo influye la relación señal a ruido de la señal (término conocido en inglés como Signal-to-Noise Ratio (SNR)) a la recepción de cada bloque dentro del SSBlock.

Los autores en [5] describen de forma detallada el procedimiento de sincronización en 5G NR. Primero presentan minuciosamente los detalles de la capa física de 5G NR, describiendo los canales y las señales involucradas en el procedimiento de sincronización. Después pasan a describir el procedimiento de sincronización propiamente dicho, y por último, proporcionan unos resultados para describir los principales retos y problemas en este ámbito. En [6], los autores describen la estructura del bloque y las señales de sincronización de 5G. Además proponen un algoritmo de correlación y autocorrelación utili-

zando FPGA para detección precisa y la eliminación de desfases de tiempo y frecuencia para la búsqueda de celdas. Por último, los autores evalúan cómo influye el valor de la SNR para la correcta sincronización en tiempo y frecuencia.

El trabajo realizado en [7] pretende resaltar la importancia de la sincronización en la tecnología 5G. En este artículo de investigación, los autores proporcionan una descripción general sobre la evolución de las redes inalámbricas a través de las distintas generaciones 2G, 3G, 4G y 5G. Además, comparan los requisitos de sincronización y su importancia a lo largo de estas generaciones de redes móviles.

Los autores en [8] presentan una evaluación detallada de la precisión alcanzable del servicio de sincronización de tiempo de la Release 16 teniendo en cuenta las deficiencias de los UEs, los componentes multitrayecto en la transmisión de la señal y los parámetros de despliegue.

El último proyecto es el proyecto [9]. Este proyecto analiza una transmisión y recepción de una señal 5G para la sincronización temporal, en frecuencia y en fase del dispositivo receptor con el emisor en tiempo real. Hace pruebas con diferentes configuraciones físicas y de software tanto en el transmisor como en el receptor.

De los dos primeros proyectos presentados en esta sección podemos sacar información sobre cómo se ha de obtener el SSBlock, que es el primero de los bloques que se demodularán y decodificarán en este documento. El trabajo en [7] nos ayuda a ver la necesidad de la sincronización en la tecnología actual proporcionando una visión general de los requisitos de sincronización a lo largo de la evolución de redes móviles. Sin embargo, este trabajo no cubre ningún aspecto práctico en cuanto a obtención y decodificación de las señales y los mensajes que transportan la información de tiempo necesario para la sincronización de distintos dispositivos. Tan solo el trabajo realizado en [9] nos proporciona una base de cómo demodular y decodificar señales en 5G. Aún así, en este proyecto solo se demodula el SSBlock, y no se continúa demodulando más canales de las señales 5G. Por lo tanto, en este TFG pretendemos seguir con el estudio de la señal 5G y así, con la demodulación y decodificación de los siguientes canales que contienen las señales 5G, obtener el mensaje SIB9.

Capítulo 3

Planificación y estimación de costes

En este capítulo se van a mostrar tanto la planificación temporal como la estimación de costes de este proyecto.

La planificación temporal será una primera idea de como va a estar planificado el proyecto. Qué tareas se van a realizar y cuanto tiempo va a durar cada una de manera aproximada.

En la sección de estimación de costes se dará un presupuesto de los costes que han supuesto todos los recursos usados durante la realización de este proyecto.

3.1. Planificación de tareas

En esta sección se van a explicar las tareas que se van a realizar durante la realización de este TFG. Todas estas tareas están enumeradas a continuación.

1. Estudio sobre 5G.

Para poder trabajar con señales 5G primero hay que conocer el escenario de 5G y eso es lo que se hará en esta tarea. Habrá que buscar artículos y proyectos que hablen de 5G para poder familiarizarme con esta tecnología.

2. Estudio señal 5G.

Como se va a trabajar con señales 5G, primero se tiene que saber cómo se transmiten, su estructura y qué transmiten. Esta tarea consistirá en el estudio de estos aspectos.

3. Familiarización con *toolbox* 5G de MATLAB.

Tanto para la recepción de la señal como el análisis de las señales se usará MATLAB. Esta es una herramienta que se ha usado a lo largo

de la carrera, pero, para este proyecto, se va a utilizar una *toolbox* específico de 5G. Esta *toolbox* contiene funciones y scripts que han de ser conocidos para, en caso de que sea necesario, tener la capacidad de modificarlos.

4. Familiarización con SDR y transmisión de señales con SDR.
Se van a trabajar con señales inalámbricas, por lo tanto, he de ser capaz de recibir y transmitir señales con MATLAB.
5. Familiarización con srsRAN y Amarisoft.
Los software que se van a usar que permiten generar y recibir señales en 5G son srsRAN y la estación de Amarisoft. Por lo tanto, voy a tener que familiarizarme con estos recursos.
6. Capturas y demodulación de señales.
Una vez que entiendo las señales de 5G y que soy capaz de transmitir y recibirlas, procederé a capturarlas y estudiarlas. En esta tarea se usarán todos los conocimientos adquiridos hasta este momento.
7. Escritura de memoria.
En esta última tarea escribiré la memoria de mi TFG. También se realizará la presentación para su defensa, así como la preparación de la propia defensa.

En la tabla 3.1 podemos ver la planificación en horas para este proyecto.

Tabla 3.1: Tabla resumen de las horas dedicadas al TFG.

ID	Descripción de la tarea	Tiempo (h)
1	Estudio sobre 5G	16
2	Estudio señal 5G.	60
3	Familiarización con la <i>toolbox</i> de MATLAB.	30
4	Familiarización con SDR y transmisión de señales con SDR.	20
5	Familiarización con srsRAN y Amarisoft.	45
6	Capturas y demodulación de señales.	85
7	Escritura de memoria.	130
Tiempo Total		386

Y en la figura 3.1 se muestra el diagrama de Gantt que se pretende seguir para la realización del proyecto.

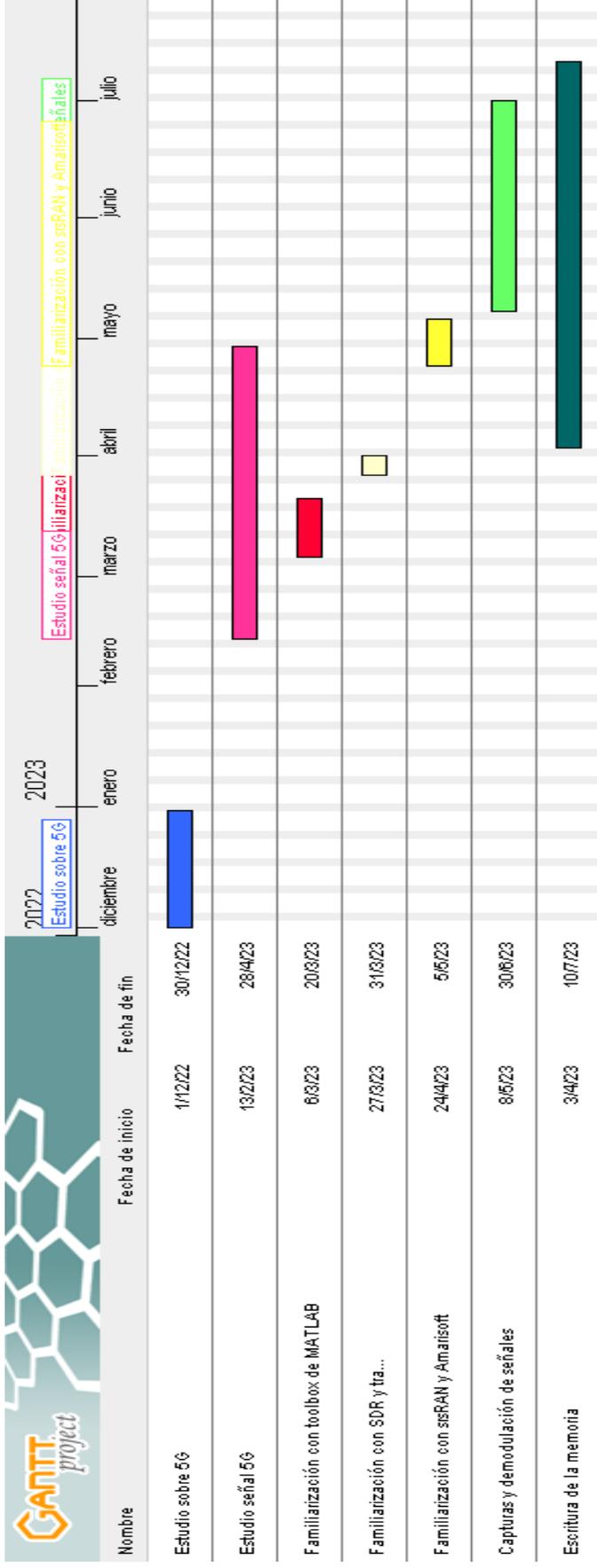


Figura 3.1: Diagrama de Gantt.

3.2. Planificación de recursos

Se analizarán y desglosarán los tres tipos de recursos usados, el hardware, el software y el humano.

3.2.1. Recursos hardware.

Como recursos hardware tenemos el portátil usado para escribir la memoria y para poder realizar todo el proyecto y los dispositivos usados para la transmisión y recepción de las señales, tales como los Software Defined Radio (SDR), las antenas, el reloj basado en GPS (GPSDO, *GPS disciplined oscillator*) y la estación base de Amarisoft.

Las características del portátil se pueden ver en la tabla 3.2.1.

Tabla 3.2: Características del portátil.

Procesador 11th Gen Intel(R) Core(TM) i5-1135G7
Memoria RAM de 8 GB
Tarjeta gráfica Gráficos Intel UHD
Capacidad de 512 GB

3.2.2. Recursos software.

Los recursos software usados son el MATLAB 2022b, con la *toolbox* de 5G, el Overleaf, para la escritura de la memoria, y Wireshark, para el análisis de trazas 5G obtenidas a partir de los bits decodificados de las señales 5G. Además, se ha usado el software srsRAN.

3.2.3. Recursos humanos.

Los recursos humanos son las personas que han ayudado a la realización de este proyecto, que son Jorge Navarro, Lorena Chinchilla y un servidor, Ángel Gómez. Estos recursos están descritos en la tabla 3.3.

Tabla 3.3: Recursos humanos necesarios para la elaboración del TFG.

Persona	Horas	Coste/Hora
Ángel	386	25
Lorena	30	50
Jorge	30	50

3.3. Presupuesto

En esta sección se mostrará el coste total de los tres recursos mencionados.

El portátil usado es un DESKTOP-FQM06PO-HP que costó 850 euros y con una vida útil de 4 años. El SDR usado cuesta 1400 euros y las antenas 75 euros cada una. La estación base de Amarisoft costó 15000 euros en total, con un tiempo de amortización de 3 años.

La licencia de MATLAB ha costado 2000 euros con un año de uso. El resto de recursos software son gratuitos.

El reloj basado en GPS(GPSDO, GPS *disciplined oscillator*) ha costado 228,58 euros y tiene una vida útil de 3 años. Se le ha dado uso durante una semana.

La tabla 3.4 muestra, entre otras cosas, el precio total de cada componente, así como el precio que ha supuesto mi uso.

Tabla 3.4: Tabla estimación precio supuesto por mi uso.

Herramienta	Precio unidad (€)	Vida Útil (años)	Tiempo usado (meses)	Precio total (€)
Portátil	850	4	9	159,38
MATLAB	2000	1	9	1500
Amarisoft	15000	3	0.75	312,5
SDR	1400	4	3	87,5
Antenas	75	4	3	4,69
Reloj basado en GPS	228,58	3	0.25	1,04

Y a continuación se muestra la tabla de costes totales.

Por lo tanto, como se puede ver en la tabla 3.5, el presupuesto final es de 14807,30 euros,

Tabla 3.5: Presupuesto final.

Herramienta	Precio total (€)	Unidades	Subtotal final (€)
Portátil	159,38	1	159,38
MATLAB	1500	1	1500
Amarisoft	312,5	1	312,5
SDR	87,5	2	175
Antenas	4,69	2	9,38
Reloj basado en GPS	4,69	1	1,04
Ángel Gómez	25	386	9650
Jorge Navarro	50	30	1500
Lorena Chinchilla	50	30	1500
TOTAL (€)			14807,30

Capítulo 4

Fundamento Teórico

En este capítulo se describen los canales y las señales que se usan en las transmisiones en 5G NR. También se detallan las posibles estructuras de una trama en 5G NR, y por último se explica en profundidad cómo obtiene el UE la hora UTC de la BS y como se realiza la sincronización del UE con la BS [5]. En la parte de la obtención de la hora UTC se exponen los mensajes SIBs, poniendo especial atención al mensaje SIB9, ya que es el que contiene la información de la hora UTC, la cual es la información que se pretende obtener en este proyecto, siendo crucial para la sincronización.

4.1. Canal y señal

Para poder empezar a hablar de los canales y de las señales que se utilizan en 5G, debemos empezar diferenciando los dos tipos de enlaces que existen. El enlace ascendente, o Up-link (UL), que es usado por el UE para contactar con la BS, y el enlace descendente o Down-link (DL), que es el que utiliza la BS para contactar con los UE[10].

Para poder tener una primera visión genérica de todos los canales y señales del UL, nos fijamos en la figura 4.1 [11]. En ella podemos ver los diferentes canales que existen.

Entre la capa Radio Link Control (RLC) y la capa Medium Access Control (MAC) está el canal lógico, por el que se transmiten los canales Common Control Channel (CCCH), Dedicated Control Channel (DCCH), y Dedicated Traffic Channel (DTCH). Los canales CCCH y DCCH son usados para transmitir los mensajes de señalización Radio Resource Control (RRC) y el canal DTCH es usado para transmitir datos de aplicación.

Entre la capa MAC y la capa física se encuentran los canales de transporte Random Access Channel (RACH) y UL-Shared Channel (SCH). El canal RACH es usado para identificar el preámbulo de acceso aleatorio que se utiliza para que dos UE no colisionen cuando intentan acceder al medio de manera simultánea y el UL-SCH es usado para la transmisión de datos del

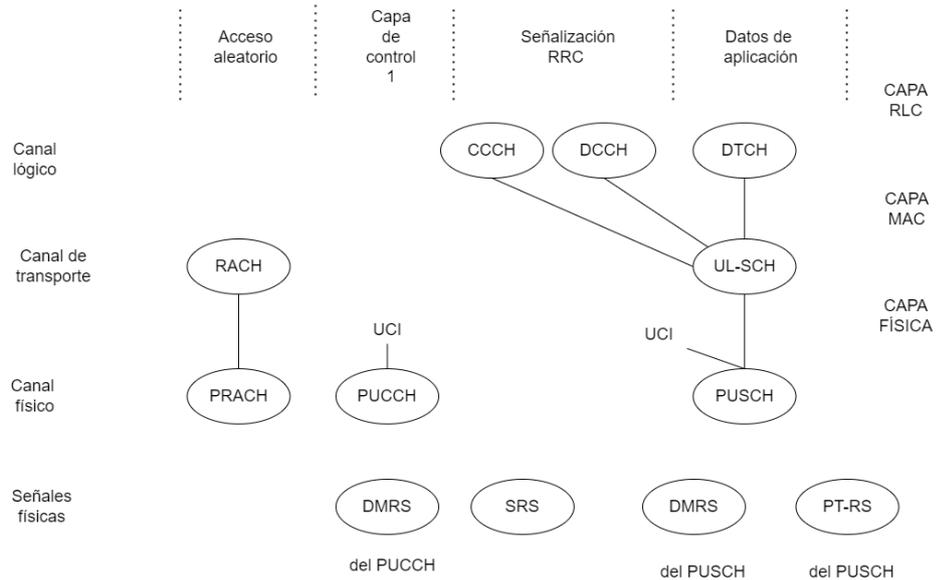


Figura 4.1: Mapa canales y señales para UL

enlace ascendente.

Dentro de los canales físicos nos encontramos los canales Physical Random Access Channel (PRACH), Physical Up-link Control Channel (PUCCH) y Physical Up-link Shared Channel (PUSCH). El canal PRACH se utiliza para el acceso al canal, el canal PUCCH no tiene asociado ningún canal lógico ni ningún canal de transporte y se encarga de transportar el Up-link Control Information (UCI), que, entre otras cosas, da información a cerca del estado del canal. Y por último el canal PUSCH, que se utiliza para transportar los datos del UL-SCH.

Por último queda mencionar las señales físicas, que son las señales Demodulation Reference Signal (DMRS) de los canales PUCCH y PUSCH, la señal Sounding Reference Signal (SRS) y la señal Phase Tracking Reference Signal (PTRS) del canal PUSCH. Las señales DMRS son secuencias conocidas y sirven para saber el impacto que tiene el canal sobre la señal. Al igual que la señal SRS, que también nos sirve para estimar el canal. Por último, la señal PTRS, que nos sirve para compensar el error de fase que se genera en el oscilador local del transmisor.

No se profundizará más en cada uno de estos canales y estas señales porque el UL no es objetivo de estudio en este proyecto.

Ahora se va a hablar del DL. Para ello nos fijamos en la figura 4.2. En ella podemos ver el mapa de los canales y señales que se utilizan para la señalización DL[10].

Entre la capa RLC y la capa MAC se transmiten los canales lógicos, que

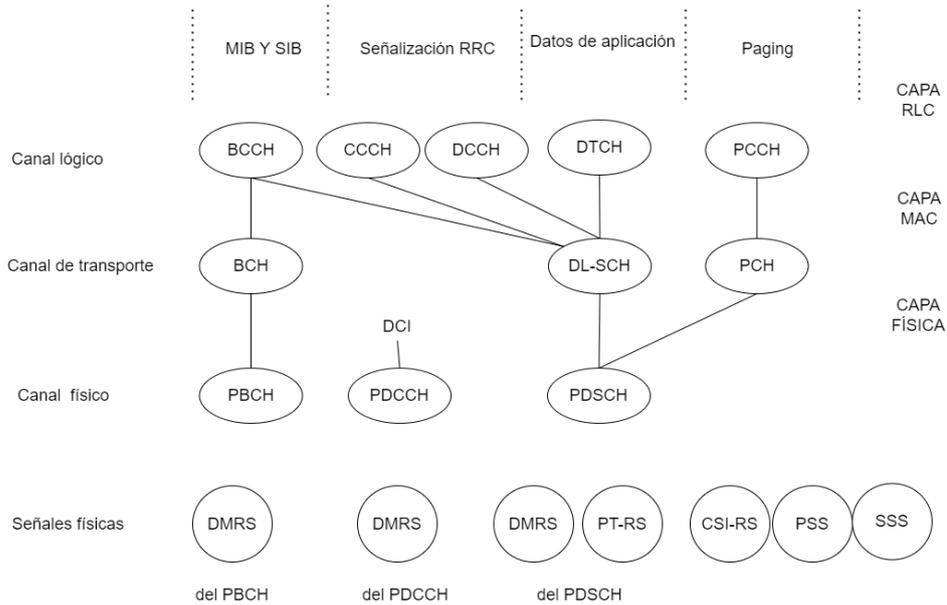


Figura 4.2: Mapa canales y señales para DL

son, el Broadcast Control Channel (BCCH), el CCCH, el DCCH, el DTCH y el Paging Control Channel (PCCH). En el canal BCCH se envía el mensaje MIB y los mensajes SIBs. El mensaje MIB se transmite en el canal Broadcast Channel (BCH) y los mensajes SIBs en el canal PDSCH. De estos dos mensajes se hablará con mayor detenimiento en la sección 4.4.1 y en la sección 4.4.2 respectivamente. Los canales CCCH y DCCH aparecen también en el enlace descendente y sirven para mandar los mensajes de señalización RRC, que se utilizan entre otras cosas para la asignación de recursos radio. En el canal DTCH se transfieren datos de aplicación, así como información de usuario. Esta información está contenida dentro del canal PDSCH. El canal PCCH es usado para la transmisión de mensajes de radio búsqueda, los cuales sirven para informar al UE sobre cambios en el sistema (por ejemplo, del estado del canal).

En los canales de transporte, nos encontramos con los canales BCH, DL-SCH y Paging Channel (PCH). En el canal BCH se transmite la información del mensaje MIB como se mencionó anteriormente y este, a su vez, se transmite en el canal PBCH y tiene un formato específico. El canal PCH se utiliza para transmitir la información del canal lógico PCCH y se puede configurar para que solo esté activo cuando sea necesario y así ahorrar energía. El canal DL-SCH se usa para transmitir los mensajes SIBs y para la transmisión de datos del enlace descendente.

Existen tres tipos de canales físicos en el enlace descendente, los canales

PBCH, PDCCH y PDSCH. En el canal PBCH se transmite la información necesaria para la sincronización del UE con la BS. Usa un formato fijo de datos tal y como se explicará con más detalle en la sección 4.3.1. El canal PDCCH no tiene asociado ningún canal lógico ni de transporte. Se usa para transmitir el mensaje Down-link Control Information (DCI), el cual es usado por el UE para la asignación de recursos del enlace ascendente y descendente, los recursos radio de los canales PUSCH y PDSCH respectivamente. Por último, en los canales físicos, el canal PDSCH. En este canal se transmite la mayor parte de la información del enlace, tal y como se puede observar en la figura 4.2. Transporta los datos de usuario y los mensajes SIBs. Tanto el canal PDCCH como el canal PDSCH se muestran en las figuras 4.3 y 4.4, junto con todos los canales y señales que contienen de forma gráfica.

Por último, tenemos que hablar de las señales físicas. Encontramos las

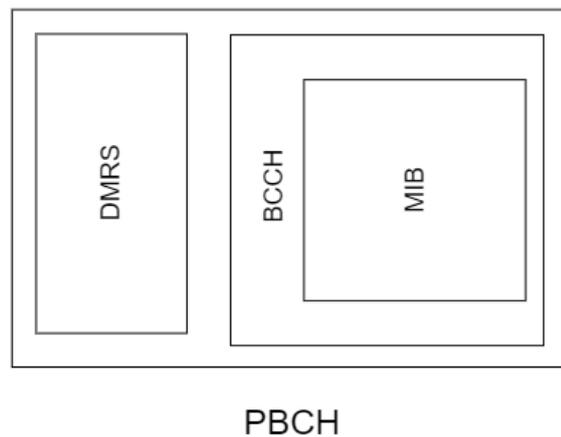


Figura 4.3: Canales y señales contenidos en el canal PBCH.

señales DMRS y PTRS, que se usan para lo mismo que en el UL, la señal Channel State Information Reference Signal (CSI-RS) se usa para conocer mejor como es el canal y que impacto tiene sobre las señales transmitidas y así poder adaptar variables como el throughput o la modulación usada. Las señales Primary Synchronisation Signal (PSS) y Secondary Synchronization Signal (SSS) son usadas para la sincronización del UE con la BS. Son señales que el receptor conoce previamente para poder detectarlas, tal y como se detallará en la sección 4.5.1.

Con respecto a las señales y canales del enlace descendente, se profundizará más en las que sean estudio de este proyecto en las secciones 4.5, 4.3 y 4.4.

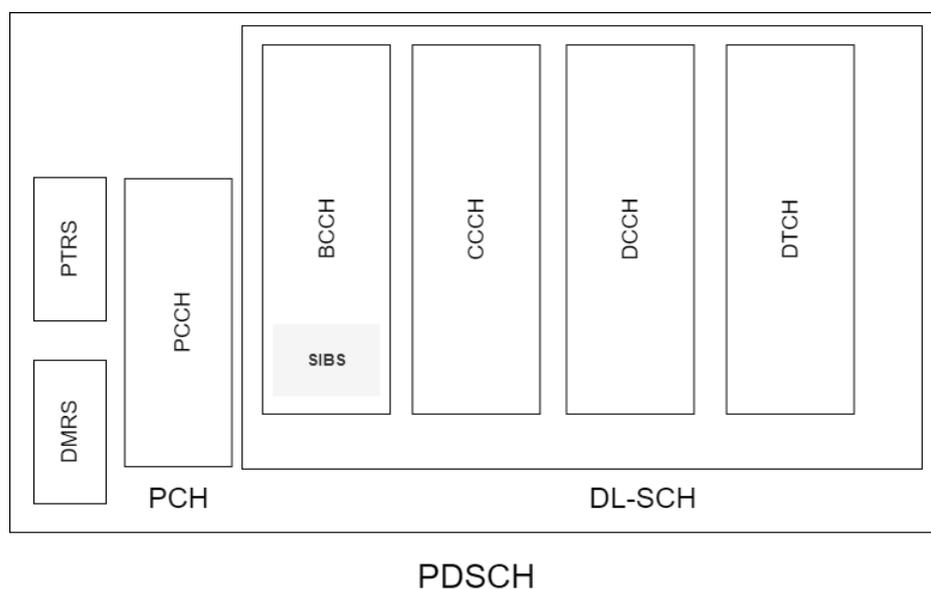


Figura 4.4: Canales y señales contenidos en el canal PDSCH

4.2. Estructura de una trama en 5G

En esta sección se va a hablar sobre la estructura que tiene una trama en 5G según está estipulado en las especificaciones del 3GPP [10].

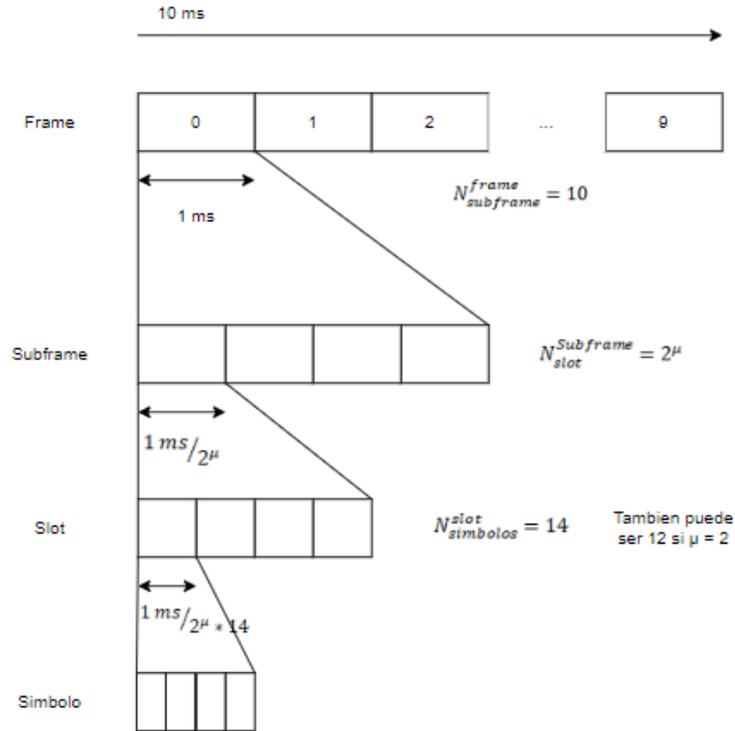
La estructura de la trama depende de la numerología μ , que determina la separación entre subportadoras, el número de subtramas, y el número de slots de una trama. La separación entre subportadoras según el valor de μ se puede ver en la figura 4.1.

Tabla 4.1: Valor μ en función de la separación entre subportadoras

μ	Separación Subportadoras
0	15kHz
1	30kHz
2	60kHz
3	120kHz
4	240kHz

Y la configuración que tiene cada trama de 5G en función del parámetro μ es la mostrada en la figura 4.5.

La duración de cada símbolo Orthogonal Frequency-Division Multiplexing (OFDM) depende de la separación entre subportadoras, y se puede ver en

Figura 4.5: Estructura trama en 5G según el valor de μ

la tabla 4.2.

Tabla 4.2: Duración del símbolo OFDM en función de la separación entre subportadoras

Separación Subportadoras (kHz)	15	30	60	120	240
Duración símbolo OFDM (us)	66,67	33,33	16,67	8,33	4,17
Duración prefijo cíclico (us)	4,69	2,34	1,17	0,57	0,29
Duración total (us)	71,35	35,68	17,84	8,92	4,46

A modo de resumen, en la tabla 4.3 se muestran el número de símbolos, el número de slot por trama y el número de slot por subtrama según la separación entre subportadoras.

Se ha hablado de los diferentes valores que puede tomar la separación entre subportadoras en 5G, algo novedoso con respecto a Fourth Generation (4G). Ahora vamos a profundizar un poco más sobre esto, ya que, para cada configuración, la señal tendrá diferentes posibles valores de sus parámetros. El primer valor que varía es el número de haces que se pueden transmitir.

Tabla 4.3: Resumen estructura trama según μ

μ	0	1	2	3	4
Nº símbolos por slot	14	14	14	14	14
Nº slot por trama	10	20	40	80	160
Nº slot por subtrama	1	2	4	8	16

Este valor puede ser 4, 8 o 64 y depende de la frecuencia a la que se transmite la señal y de la separación entre subportadoras. En la tabla 4.4 podemos ver cada uno de esos valores. Además, también varía la posición del símbolo inicial y la posición del símbolo de inicio de cada uno de los bloques a transmitir.

A cada separación entre subportadoras se le asigna una letra para poder diferenciarlas entre ellas, denominándose así desde el caso A hasta el caso G.

Tabla 4.4: Características de los casos según separación entre subportadoras

Separación entre subportadoras	Símbolo OFDM inicio	$f_c < 3 \text{ GHz}$	$3 \text{ GHz} < f_c < 7,125 \text{ GHz}$	$7,125 \text{ GHz} < f_c$
Caso A 15 KHz	$\{2,8\} + 14n$	$n = 0,1$ $L_{\max} = 4$	$n = 0,1,2,3$ $L_{\max} = 8$	
Caso B 30 KHz	$\{4,6,16,20\} + 28n$	$n = 0$ $L_{\max} = 4$	$n = 0,1$ $L_{\max} = 8$	
Caso C 30 KHz	$\{2,8\} + 14n$	$n = 0,1$ $L_{\max} = 4$	$n = 0,1,2,3$ $L_{\max} = 8$	
Caso D 120 KHz	$\{4,8,16,20\} + 28n$			$n = 0,1,2,3,5,6,7,8,10,11,12,13,15,16,17,18$ $L_{\max} = 64$
Caso E 240 KHz	$\{8,12,16,20,32,36,40,44\} + 56n$			$n = 0,1,2,3,5,6,7,8$ $L_{\max} = 64$
Caso F 480 KHz	$\{2,9\} + 14n$			$n = 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31$ $L_{\max} = 64$
Caso G 960 KHz	$\{2,9\} + 14n$			$n = 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31$ $L_{\max} = 64$

Sobre el caso C, este ha ido cambiando a lo largo de las especificaciones. Para esta tabla, se ha tenido en cuenta la especificación de 3GPP [12] por lo

que puede ser distinta a otras que no hayan usado esta misma especificación. Como se puede observar en la tabla 4.4, existen rangos de frecuencia con señales con características diferentes. El Frequency Range 1 (FR1) es aquel rango de frecuencias entre 450 MHz y 7125 MHz y el Frequency Range 2 (FR2) es aquel entre 24250 MHz y 71000 MHz[13]. Por lo tanto, para FR1 se pueden usar los casos A, B y C y para el FR2 los casos D, E, F y G. Se va a profundizar sobre el caso A para una $fc < 3$ GHz sobre la transmisión de los bloques SS para intentar esclarecer un poco más la tabla 4.4. Como los valores de n son 0 y 1, los símbolos que inician los bloques de transmisión son 2,8,16,22. Esto se pretende aclarar en la figura 4.6.

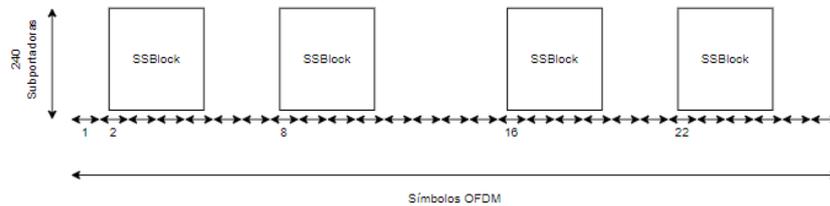


Figura 4.6: Posicionamiento de los SSBlock en los símbolos OFDM.

Los bloques duran 4 símbolos OFDM, tal y como se explicará en la sección 4.5.1.

4.3. Canales implicados en la obtención del mensaje SIB9.

En esta sección se tratan los diferentes canales físicos implicados en la obtención del mensaje SIB9. Para la obtención del mensaje SIB9 previamente hay que obtener tanto el mensaje MIB como el mensaje SIB1. Por lo tanto, también se explicarán los canales implicados en estos dos bloques. El canal PBCH contiene al mensaje MIB y el canal PDSCH contiene a los mensajes SIBs. Para la decodificación del canal PDSCH hace falta la decodificación del canal PDCCH por lo que se hablará de este último también[10].

4.3.1. PBCH

El canal PBCH [10] usa una modulación Quadrature Phase-Shift Keying (QPSK) [12] y se encuentra en los símbolos 2, 3 y 4 del SSBlock. En los símbolos 2 y 4 en todas las subportadoras y en el símbolo 3 en las subportadoras que no están ocupadas por la señal SSS. Todo esto se puede ver en la figura 4.11 de la sección 4.5.

En el canal PBCH se transmite, aparte de información esencial para la sincronización de la que se hablará posteriormente, una señal DMRS. Esta es

una señal pseudoaleatoria que está mapeada dentro del canal PBCH según el valor del Physical Layer Cell Identity (PCI) de la celda transmisora. En la figura 4.7 se muestra un ejemplo de los posibles mapeados del DMRS dentro del canal PBCH si el PCI fuera mod4. Al ser mod4, existen 4 posibles mapeados. Cada uno de estos bloques simula un bloque de recursos, que contiene 12 subportadoras. El valor del PCI lo sabemos tras detectar

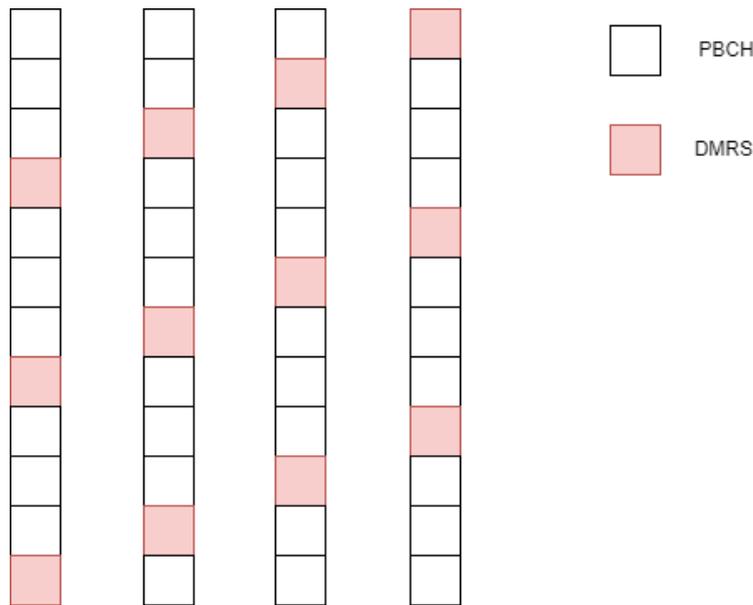


Figura 4.7: Opciones mapeado de la señal DMRS dentro del canal PBCH para $pci \bmod 4$.

la señal PSS y la señal SSS, de las que hablamos en la sección 4.5.1. Esta secuencia de la señal DMRS es la mencionada en la subsección de la señal SSS, 4.5.1, por lo que es necesaria para realizar la estimación del canal.

El tamaño de carga útil del canal PBCH es de 56 bits, de los cuales, 24 son para el mensaje Cyclic Redundancy Check (CRC), para la corrección de posibles errores, 23 pertenecientes al mensaje MIB, 1 del canal BCCH y 8 para otra información. De estos 8 bits que contiene el canal PBCH, 4 de ellos son para el System Frame Number (SFN). Si estamos en FR1, 1 para la compensación de subportadora del SSB y 2 reservados y si estamos en FR2, esos tres bits se utilizan para el índice SSB, que sirve para saber a qué haz pertenece ese SSB. El último bit que queda en ambos casos se utiliza para saber si esa transmisión se ha realizado en la primera media parte de los 10 ms de transmisión o en la segunda media parte de la misma. Esto sirve para conseguir la sincronización de trama.

De los 23 bits del mensaje MIB se hablarán en la sección 4.4.1.

4.3.2. PDCCH

En esta sección se hablará de manera breve del canal PDCCH[10], ya que transporta la información DCI [14], el cual es necesario para la decodificación del mensaje SIB1.

El canal PDCCH se encuentra dentro del COntrol REsource SET (CORE-SET), el cual es un recurso físico diseñado para transmitir a este canal, y tiene su señal DMRS asociada. Usa una modulación QPSK.

Los mensajes DCI contiene, entre otra información, la necesaria para la decodificación del canal PDSCH, que es donde se encuentran los mensajes SIBs, tal y como se verá en la sección 4.3.3. Hay varios tipos de mensajes DCI según qué tipo de información se quiere transmitir, en total son 14, pero en esta sección solo nos vamos a centrar en los denominados 1.0 y 1.1 que son los que nos aportan la información sobre el canal PDSCH. Para poder saber qué tipo de mensaje se está mandando de esos 14, se mira el valor del Radio Network Temporary Identifier (RNTI). Existen algunos valores de RNTI conocidos por todos los UE, pero la mayoría de ellos son asignados específicamente a un UE.

Dentro del mensaje DCI con formato 1.0 se transmiten varios campos. Estos campos son: System Information (SI)-RNTI, Paging (P)-RNTI, Random Access (RA)-RNTI, Temporary Cell (TC)-RNTI, Cell (C)-RNTI, Modulation Coding Scheme (MCS)-C-RNTI y Configured Scheduling (CS)-RNTI.

- *SI – RNTI*. Es un mensaje de multi-difusión que contiene información de sistema. Su valor de RNTI es de 65535.
- *P – RNTI*. Es usado para transportar información sobre la paginación de manera multi-difusión. Su valor del RNTI es de 65534.
- *RA – RNTI*. Es usado durante el proceso de acceso aleatorio al canal.
- *TC – RNTI*. Es usado también durante el proceso de acceso aleatorio al medio.
- *C – RNTI*. Sirve para que la BS pueda diferenciar a los diferentes UE en las transmisiones UL.
- *MCS – C – RNTI*. Sirve para indicar la tabla MCS alternativa que tiene que usar un UE. No es multi-difusión.
- *CS – RNTI*. Es una identificación utilizada para la programación semipersistente en el enlace descendente.

Y dentro del mensaje DCI con formato 1.1 se encuentra información sobre los bloques de recursos y los símbolos que ocupa el canal PDSCH, así como en que símbolo empieza entre otra información que ayuda a la detección y decodificación del canal PDSCH.

Una vez conocida esta información, el UE ya está capacitado para detectar y decodificar el canal PDSCH.

4.3.3. PDSCH

[10] Como se vio en la figura 4.2, este canal físico contiene a los canales de transporte DL-SCH y PCH. Este canal es usado para transmitir datos de aplicación al usuario, mensajes de señalización de portadora radio o Signalling Radio Bearer (SRB) y los mensajes SIBs que se transmitan [15]. No siempre se transmiten todos los mensajes SIBs. Además de esto, también puede transportar información de la capa MAC.

Puede ser transmitida usando modulación QPSK, 16 Quadrature Amplitude Modulation (QAM) o 256QAM. Tiene asociada una señal DMRS y puede además tener asociada una señal PTRS o una señal Tracking Reference Signal (TRS). El concepto de Quasi Co-Location (QCL) puede también ser usado con el SSB (véase la sección 4.5.1) para facilitar la recepción de la propia señal. QCL se refiere a los puertos de una antena cuyas señales experimenta un canal de radio con propiedades comunes.

A continuación se exponen los campos más relevantes para nosotros que tiene el mensaje sobre el canal PDSCH.

- *dataScramblingIdentityPDSCH*. Secuencia de 10 bits que se utiliza para iniciar la secuencia psuedoaleatoria que codifica la carga útil del PDSCH.
- *pdsch – TimeDomainAllocationList*. Define una tabla de búsqueda con filas las cuales pueden ser elegidas cuando se hace la asignación de recursos en el dominio del tiempo. Cada fila especifica un desplazamiento de ranura (k_0), un tipo de mapeo (A o B) y el símbolo inicial, así como su duración.
- *rbg – Size*. Define el tamaño del grupo de bloques de recursos.
- *mcs – Table*. Especifica la modulación y la tabla del esquema de codificación que usa el PDSCH.

4.4. Mensajes implicados en la obtención del SIB9.

En esta sección se describirán los bloques de información útiles para la sincronización de los dispositivos con una estación base. Se hablará del mensaje MIB y de los mensajes SIB 1 y 9 [16].

4.4.1. MIB

El mensaje MIB [15] se encuentra dentro del canal lógico BCCH, que se transmite dentro del canal de transporte BCH y este a su vez se transmite

dentro del canal físico PBCH(figura 4.2). Dentro del canal PBCH, como se dijo anteriormente, el mensaje MIB es una secuencia de 23 bits. En esta sección se pretende desglosar la información que nos aporta este bloque. En la tabla 4.5 se observan para que están destinados cada uno de los 23 bits que componen el mensaje MIB.

Tabla 4.5: Estructura del MIB

MIB	Nº de bits
<i>systemFrameNumber</i>	6
<i>subCarrierSpacingCommon</i>	1
<i>ssb – SubcarrierOffset</i>	4
<i>dmrs – TypeA – position</i>	1
<i>pdccch – ConfigSIB1</i>	8
<i>cellBarred</i>	1
<i>intraFreqReselection</i>	1
<i>spare</i>	1

- *systemFrameNumber*. El *systemFrameNumber* son los 6 bits más significativos del SFN, que junto con los 4 del canal PBCH, forma una cadena de 10 bits que nos indica el número de la trama, cuando este llega a 1023 se reinicia a 0.
- *subCarrierSpacingCommon*. Indica la separación entre subportadoras usada para el SIB1. Si estamos en FR1, puede ser 15 KHz o 30 KHz (bit a 0 o 1 respectivamente) y si estamos en FR2, puede ser 60 KHz o 120 KHz (bit a 0 o 1 respectivamente).
- *ssb – SubcarrierOffset*. Da el valor de la k_{ssb} , que indica el desplazamiento en el dominio de la frecuencia en número de subportadoras entre el SSB y la cuadrilla de bloque de recursos general.
- *dmrs – TypeA – position*. Indica cuál es la posición del primer símbolo de la señal DMRS del canal PDSCH. Puede tomar los valores 2 o 3 (bit a 0 o 1 respectivamente).
- *pdccch – ConfigSIB1*. Da una importante información sobre la configuración del CORESET0, del *searchspace0* y del canal PDCCH necesaria para la posterior obtención del mensaje SIB1. Contiene dos campos, el *controlResourceSetZero* y el *searchSpaceZero*, de 4 bits cada uno.
- *cellBarred*. Indica si los UE en la celda pueden acceder a ella o no. Toma valores barred o notBarred (bit a 0 o 1 respectivamente).

- *intraFreqReselection*. Indica si el UE tiene permitido conectarse a otra celda que trabaje a la misma frecuencia si ha sido rechazado de la celda de mayor rango. Toma valores `allowed` o `notAllowed` (bit a 0 o 1 respectivamente).
- *spare*. Un bit libre, sin uso determinado dentro del mensaje MIB.

[14] [12]

4.4.2. Mensajes SIBs

Por último, se hablará sobre los mensajes SIBs. En concreto, se hablará sobre el mensaje SIB1, que contiene información, entre otras cosas, para saber dónde y si están los otros mensajes SIBs, y del mensaje SIB9, que contiene la información de la hora en formato UTC de la BS [15].

El SIB1 es transmitido usando el canal lógico BCCH, el canal de transporte DL-SCH y el canal físico PDSCH con un periodo de 160ms. Contiene información que permite al UE saber si puede conectarse o no a la celda. Además, contiene la información sobre los demás mensajes SIBs e información sobre la configuración de los recursos radio. Usa el formato DCI 1.0 y con un conjunto de espacio de búsqueda que se explicarán a continuación. Para ello tenemos que recordar dos campos del mensaje MIB vistos en la tabla 4.5. En concreto, el *subCarrierSpacingCommon*, que nos indica la separación entre subportadoras que utiliza el mensaje SIB1 y el *pdccch-configSIB1*, que contiene 8 bits, 4 para el *controlResourceSetZero* y los otros 4 para el *searchSpaceZero*. Estos valores se usan como punteros para tablas dentro de la configuración del CORESET. Para el valor del *controlResourceSetZero* 3GPP tiene especificadas muchas tablas, cada una específica para una separación entre subportadoras del SS/PBCH Block y del canal PDCCCH. Están en la especificación [17]. Aquí se expondrán dos de ellas en la tabla 4.6 y 4.7. La tabla 4.6 corresponde a 15 KHz de separación entre subportadoras para ambos bloques. El índice es el valor que toma el parámetro *controlResourceSetZero*, el n^o de bloques de recursos son el ancho de banda que ocupa el CORESET, y el n^o de símbolos son los símbolos que ocupa (dominio temporal). Por último, el valor de la compensación de bloques de recursos da la compensación entre el bloque SS/PBCH y el CORESET. Para esclarecer esto último está la figura 4.8. Los valores RB son los valores que puede tomar la compensación de bloques de recursos para los casos de índice 0 a 5.

En las figuras 4.9 4.10 y se muestra un ejemplo de una señal que cumple con las especificaciones de la tabla 4.6. En este ejemplo, el valor que toma el parámetro *controlResourceSetZero* es 0. Por lo tanto, tiene 24 bloques de recursos, ocupa 2 símbolos y la compensación es de 0. En la figura 4.9 podemos ver cómo la compensación es 0. Y en la figura 4.10 podemos ver

Tabla 4.6: Tabla configuración CORESET para separación entre subportadoras 15 KHz en SS/PBCH y del PDCCH.

Indice	Nº Bloques de recursos	Nº de símbolos	Compensación de Bloques de recursos.
0	24 (4.32 MHz)	2	0
1			2
2			4
3		3	0
4			2
5			4
6	48 (8.64 MHz)	1	12
7			16
8		2	12
9			16
10		3	12
11			16
12	96 (17.28 MHz)	1	38
13		2	
14		3	
15	Reservado		

cómo ocupa dos símbolos y como ocupa 24 bloques de recursos, que son 288 subportadoras. Ahora se muestra la tabla del valor *controlResourceSetZero* cuando la separación entre subportadoras del bloque SS/PBCH y del canal PDCCH es de 30 KHz. La cual es la configuración que se usará en las señales con las que se trabajarán en este proyecto. La tabla de la que se está hablando es la tabla 4.7

Para el valor del *searchSpaceZero* 3GPP propone diferentes tablas en función del rango de frecuencia de la señal, FR1 o FR2, y del patrón de multiplexación. En la tabla 4.8 vemos la tabla que se usa para los casos FR1 y patrón de multiplexación 1. El índice es el valor que toma la variable *searchSpaceZero*. El valor de la *O* indica el retardo en número de slot relativo al inicio de la trama, el número de espacios de búsqueda establecido por ranura y el valor de la *M* esta relacionados, y ayudan a calcular el número de ranuras de un bloque SS/PBCH concreto. Por último, el índice del primer símbolo, como su nombre indica, marca el primer símbolo, dentro del slot, que contiene información útil.

Ahora se muestra, en la tabla 4.9, todo el contenido que tiene el mensaje SIB1.

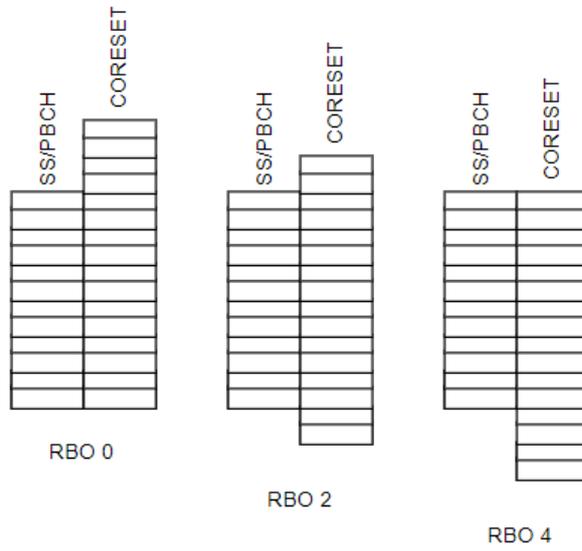


Figura 4.8: Compensación Bloques de Recursos.

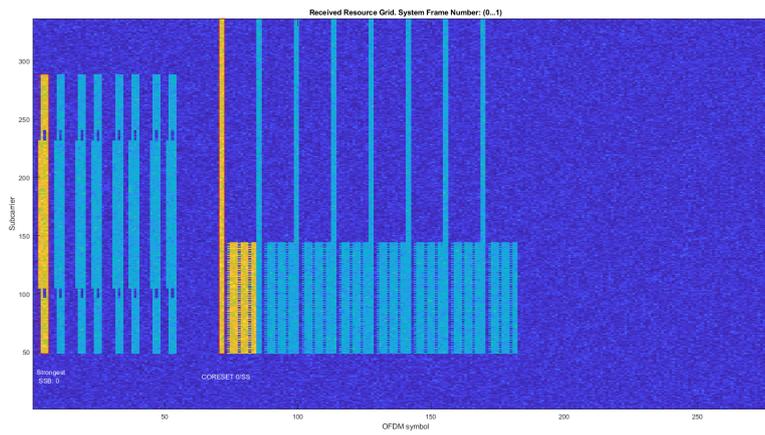


Figura 4.9: Compensación Bloques de Recursos en espectrograma.

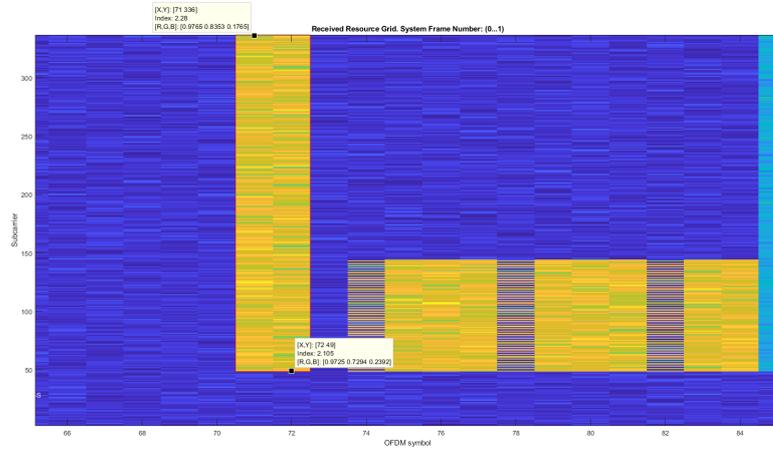


Figura 4.10: Duración del canal tanto en símbolos como en frecuencia.

Tabla 4.7: Tabla configuración CORESET para separación entre subportadoras 30 KHz en SS/PBCH y del PDCCH.

Indice	Nº Bloques de recursos	Nº de símbolos	Compensación de Bloques de recursos
0	24 (4.32 MHz)	2	0
1			1
2			2
3			3
4		3	4
5			0
6			1
7			2
8			3
9	4		
10	48 (8.64 MHz)	1	12
11			14
12			16
13		2	12
14			14
15			16

Tabla 4.8: Tabla valor *searchSpaceZero* para FR1 y patrón de multiplexación 1.

Indice	O	Nº de espacio de búsqueda establecido por ranura	M	Indice Primer Símbolo	
0	0	1	1	0	
1		2	1/2	0 si 'i' es par 1 si 'i' es impar	
2	2	1	1	0	
3		2	1/2	0 si 'i' es par 1 si 'i' es impar	
4	5	1	1	0	
5		2	1/2	0 si 'i' es par 1 si 'i' es impar	
6	7	1	1	0	
7		2	1/2	0 si 'i' es par 1 si 'i' es impar	
8	0	1	2	0	
9	5			0	
10	0		1	1	1
11					2
12	2				1
13					2
14	5			1	
15				2	

Tabla 4.9: Contenido SIB1.

cellSelectionInfo	q-RxLevMin	-70 a -22 dBm (valor real = valor señalado * 2)	
	q-RxLevMinOffset	1 a 8 dB (valor real = valor señalado * 2)	
	q-RxLevMinSUL	-70 -22 dBm (valor real = valor señalado * 2)	
	q-QualMin	-43 a -12 dBm	
cellAccessRelatedInfo	q-QualMinOffset	1 a 8	
	1 to 12 instances of PLMN-Identity Info	1 to 12 instances of PLMN-Identity	
		trackingAreaCode	mcc (secuencia de 3 dígitos) mnc (secuencia de 2 o 3 dígitos)
		ranac	24 bits De 0 a 255
	cellIdentity	36 bits	
	cellReservedForOperatorUse	Reserved, notReserved	
connEstFailureControl	cellReservedForOtherUse	true	
	connEstFailCount	1,2,3,4	
	connEstFailOffsetValidity	30, 60, 120, 240, 300, 420, 600, 900 seconds	
si-SchedulingInfo	connEstFailOffset	0 a 15	
	mirar tabla 4.10.		
servingCellConfigCommon	mirar tabla 4.11 4.12 4.13		
ims-EmergencySupport	true		
	true		
eCallOverIMS-Support	100,200,300,400,600, 1000, 1500, 2000ms		
	100,200,300,400,600, 1000, 1500,2000ms		
	0, 50, 100 , 200,500, 1000, 2000 ms		
	1, 2, 3, 4, 6, 8, 10, 20		
	1000, 3000, 5000, 10 000, 15 000, 20 000, 30 000 ms		
	1, 2, 3, 4, 5, 6, 8, 10		
ue-TimerAndConstants	100,200,300,400,600, 1000, 1500,2000ms		
	mirar tabla 4.14		
uac-BarringInfo	true		
useFullResumeID	true		

Tabla 4.10: Parámetro si-SchedulingInfo.

schedulingInfoList	1 to 32 instances of SchedulingInfo	si-BroadcastStatus	broadcasting, notBroadcasting	
		si-Periodicity	8, 16, 32, 64, 128, 256, 512 radio frames	
si-WindowLength	5, 10, 20, 40, 80, 160, 320, 640, 1280 slots	sib-MappingInfo	1 to 32 type instances of SIB-TypeInfo	
			type	SIB 2, 3, 4, 5, 6, 7, 8, 9
			valueTag	0 a 31
			areaScope	true
si-RequestConfig	rach-OccasionsSI	rach-ConfigSI	prach-Configuration Index	
			msg1-FDM	0 a 255
			msg1-FrequencyStart	1, 2, 4, 8
			zeroCorrelationZoneConfig	0 a 274
			preambleReceivedTargetPower	0 a 15
				-202 a -60
			preambleTransMax	3, 4, 5, 6, 7, 8, 10, 20,
			powerRampingStep	50, 100, 200
				0, 2, 4, 6 dB
			ra-ResponseWindow	1, 2, 4, 8, 10, 20, 40, 80 slots
si-RequestPeriod	si-RequestPeriod	ssb-perRACH-Occasion	oneEighth, oneFourth, oneHalf, one, two, four, eight, sixteen	
			1, 2, 4, 6, 8, 10, 12, 16	
si-RequestResources	si-RequestResources	I to 32 instances of SI-RequestResources	ra-PreambleStartIndex	
			ra-Association PeriodIndex	0 a 63
			ra-ssb-OccasionMaskIndex	0 a 15
si-RequestConfigSUL	mismos parámetros que la estructura usada para el si-RequestConfig	ssb-perRACH-Occasion	oneEighth, oneFourth, oneHalf, one, two, four, eight, sixteen	
			1, 2, 4, 6, 8, 10, 12, 16	
systemInformationAreaID	24 bits.			

Tabla 4.11: Parámetro servingCellConfigCommon Parte 1.

downlinkConfigCommon	frequencyInfoDL	frequencyBandList	freqBandIndicatorNR	Secuencia de 1 a 8 valores 1 a 1024		
			nr-NS-PmaxList	additionalPmax	Secuencia de 1 a 8 valores -30 a 33 dBm	
	frequencyInfoDL	offsetToPointA	offsetToCarrier	additionalSpectrumEmission	0 a 7	
				subcarrierSpacing	0 a 2199	
				carrierBandwidth	Secuencia de 1 a 5 valores 0 a 2199	
				txDirectCurrentLocation	15, 30, 60, 120 kHz 1 a 275	
				locationAndBandwidth	0 a 4095 0 a 37949	
	initialDownlinkBWP	genericParameters	subcarrierSpacing	15, 30, 60, 120 kHz		
			carrierBandwidth	1 a 275		
			locationAndBandwidth	0 a 4095		
			subcarrierSpacing	15, 30, 60, 120 kHz		
	bcch-Config	modificationPeriodCoeff	cyclicPrefix	extended		
			pdccch-ConfigCommon	SetupRelease { PDCCCH-ConfigCommon }		
			pdccch-ConfigCommon	SetupRelease { PDCCCH-ConfigCommon }		
	pcch-Config	nAndPagingFrameOffset	modificationPeriodCoeff	2, 4, 8, 16		
			defaultPagingCycle	32, 64, 128, 256 radio frames		
			ns	Elegir halfT 0 a 3 four, two, one firstPDCCCH-MonitoringOccasionOIPO		
	pcch-Config	nAndPagingFrameOffset	oneT	halfT	oneEightT	oneSixteenthT
			0, 1	0 a 3	0 a 7	0 a 15
			ns	four, two, one firstPDCCCH-MonitoringOccasionOIPO		

Tabla 4.12: Parámetro servingCellConfigCommon Parte 2.

uplinkConfigCommon	frequencyInfoUL	frequencyBandList	freqBandIndicatorNR	Secuencia de 1 a 8 ejemplos
			nr-NS-PmaxList	Secuencia de 1 a 8 ejemplos
				additionalPmax
	frequencyInfoUL	absoluteFrequencyPointA	additionalSpectrumEmission	0 a 7
			Secuencia de 1 a 15 ejemplos	
			offsetToCarrier	0 a 2199
			subcarrierSpacing	15,30,60, 120,240
			carrierBandwidth	1 to 275
			p-Max	-30 to 33 dBm
			frequencyShift7p5kHz	true
initialUplinkBWP	genericParameters	BWP	locationAndBandwidth	0 a 37949
			subcarrierSpacing	15,30,60, 120,240
			cyclic Prefix	extended
			SetupRelease { RACH-ConfigCommon }	
timeAlignmentTimerCommon	supplementaryUplink	mismos parámetros que el parámetro uplinkConfigCommon	SetupRelease { PUSCH-ConfigCommon }	
			SetupRelease { PUCCH-ConfigCommon }	
			500, 150, 1280, 1920, 2560, 5120, 10240 ms, infinity	

Tabla 4.13: Parámetro servingCellConfigCommon Parte 3.

n-TimingAdvanceOffset	0, 25600, 39936	
ssb-PositionsInBurst	inOneGroup	8 bits
	groupPresence	8 bits
ssb-PeriodicityServingCell	5, 10, 20, 40, 80, 160 ms	
tdd-UL-DL-ConfigurationCommon	Tabla configuración UL-DL	
ss-PBCH-BlockPower	-60 a 50dBm	

Tabla 4.14: Parametros uac-BarringInfo.

uac-BarringInfo	uac-BarringForCommon	Secuencia de 1 a 63 ejemplos	
		accessCategory	1 a 63
		uac-barringInfoSetIndex	1 a 8
		Secuencia de 1 a 12 ejemplos	
		plmn-IdentityIndex	1 a 12
	uac-BarringPLMN-List	Elegir	
		uac-ImplicitACBarringList	uac-ExplicitACBarringList
		uac-ACBarringListType	Secuencia de 1 a 63
		1 a 8	accessCategory 1 a 63
			uac-barringInfoSet Index 1 a 8
	Secuencia de 1 a 8 ejemplos		
uac-BarringInfoSetList	uac-BarringFactor	[0-0.95] de 0.05 en 0.05	
	uac-BarringTime	4, 8, 16, 32, 64, 128, 256, 512 s	
	uac-BarringForAccessIdentity	7 bits	
	Elegir		
uac-AccessCategory1-SelectionAssistanceInfo	plmnCommon	individualPLMNList	
	a, b, c	Secuencia de 2 a 12 ejemplos	
		a, b, c	

De todas estas tablas que conforman los parámetros del mensaje SIB1 se va a hablar solo de los parámetros más importantes para la decodificación del mensaje SIB9 y la sincronización del UE con la BS.

En la tabla 4.9, el parámetro *cellAccesRelatedInfo* permite enumerar las diferentes Public Land Mobile Network (PLMN).

En la tabla 4.10, el parámetro *schedulingInfoList* nos da información sobre los diferentes mensajes SIBs. El parámetro *si – BroadcastStatus* indica si el mensaje SIB del que se está informando se manda en periódicamente o tiene que ser solicitado para ser mandado. El parámetro *si – Periodicity* indica la periodicidad de este mensaje SIB en tramas radio y el parámetro *si – MappingInfo* nos da la información sobre qué mensaje SIB es del que se está refiriendo en los anteriores datos y si ha cambiado con respecto a la anterior transmisión del mismo, valor *valueTag*, este valor incrementa en 1 si ha cambiado y el UE debe actualizarlo. El valor *si – WindowLenght* da la duración de la ventana de tiempo durante la cual se transmiten los mensajes SIBs.

La tabla 4.11 trata los parámetros del mensaje SIB1 que tratan sobre la parte de DL, la tabla 4.12 trata los parámetros sobre la transmisión UL y la tabla 4.13 trata más opciones sobre la transmisión de las señales. En concreto hay unos parámetros (*ssb – PositionsInBurst* y *ss – PDCI – BlockPower*) que dan información sobre el SS/PBCH Block

La tabla 4.14 da información aplicable a la restricción de celdas basadas en el Unified Access Control (UAC).

El mensaje SIB9 da información sobre la hora UTC, la hora Global Positioning System (GPS) y la hora local. Sus campos son los siguientes:

- *timeInfoUTC*. Especifica, en saltos de 10 ms, la hora UTC de la trama en la que se envía el propio SIB9.
- *dayLightSavingTime*. Es necesario debido al cambio de hora que se produce en los cambios de estación de algunos países, ya que la hora UTC no tiene estos cambios. Indica propiamente si se han de tener en cuenta esos cambios o no a la hora de decodificar la hora del sistema.
- *leapSeconds*. Permite calcular la hora GPS a partir de la hora UTC, ya que, la hora GPS es la suma del UTC y el *leapSeconds*.
- *localTimeOffset*. Permite calcular la hora local. Da la diferencia, en saltos de 15 minutos, entre la hora UTC y la hora local, esto es necesario debido a que no es la misma hora en todos los países a la vez.
- *referenceTimeInfo – r16*. Este campo fue añadido en la Release 16 del [18]. Este valor añade una granularidad de 10ns a la hora UTC, por lo que permite mayor precisión.

El SIB9 se transmite en el canal lógico BCCH y dentro del canal físico PDSCH y bajo demanda del UE, como todos los mensajes SIBs que no sean el 1.

4.5. Sincronización en 5G

En esta última sección se van a describir los bloques y señales que se utilizan para la sincronización temporal, en frecuencia y en fase de la transmisión de la BS con el UE.

4.5.1. SS/PBCH BLOCKS AND BURSTS

El SS Burst está compuesto por tantos SS Blocks como haces se generen en el transmisor. Cada uno de estos SS Blocks contiene la información necesaria para poder establecer la sincronización del terminal con la estación base. En ellos se encuentran las señales PSS y SSS, y el canal PBCH, del que ya se habló en la sección 4.3.1 [14] [10] [19].

Estos bloques se transmiten en 4 símbolos en el dominio del tiempo y en 20 bloques de recursos en el dominio de la frecuencia, teniendo en cuenta que cada bloque ocupa 12 subportadoras, en total ocupan 240 subportadoras.

En la figura 4.11 podemos ver como es la estructura general del SS/PBCH Bloqs.

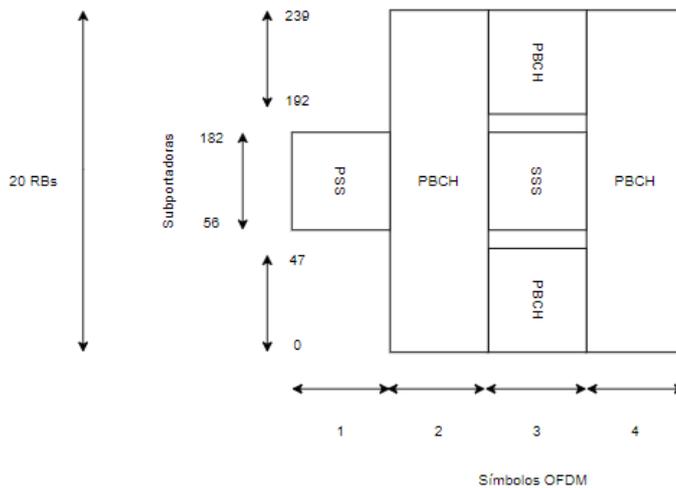


Figura 4.11: Estructura general SS/PBCH BLOCKS

La periodicidad de este bloque puede variar según las especificaciones de 3GPP.

PSS

En este subapartado voy a hablar sobre qué información nos proporciona la señal PSS, donde encontrarlo en el SSB y que estructura tiene.

La señal PSS es el primer bloque que recibe el terminal y ocupa el primer símbolo del SS/PBCH Block y las 127 portadoras centrales del mismo, tal y como se puede ver en la figura 4.11. Es una secuencia de símbolos predeterminada, lo cual hace que al receptor le resulte sencillo detectar la presencia de dicha secuencia. Sirve para corregir el error en frecuencia, para saber el instante de tiempo en el que se transmitió el SSB y, junto con otra información que nos proporciona la señal SSS, saber el sector de la Base Transceiver Station (BTS) en el que nos encontramos que nos da servicio. El número de secuencias predeterminadas depende del modo del PCI. En la figura 4.12 vemos un ejemplo de como sería el modo 3.

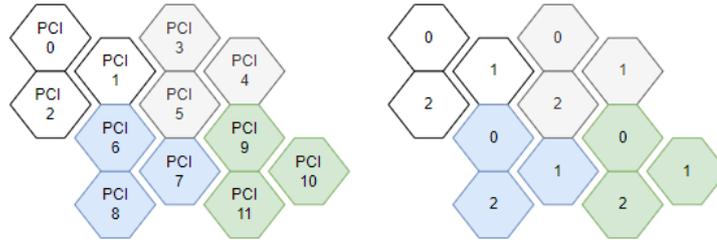


Figura 4.12: Ejemplo PCI mod3.

SSS

La señal SSS es el segundo bloque necesario para realizar la sincronización del UE con la BTS que le da cobertura. Dentro del SS Block está ubicado en el tercer símbolo y ocupa las 127 subportadoras centrales del mismo. Esto se puede ver en la figura 4.11. Es una secuencia predeterminada de 127 símbolos que nos ayuda a saber con exactitud qué BTS y a qué sector de esa BTS está conectado el terminal. Este proceso se explicará en el capítulo 6.1. También se utiliza para, junto con la señal DMRS del canal PBCH, estimar el impacto que tiene el canal en la señal.

Capítulo 5

Herramientas usadas.

En este capítulo se presentan las herramientas, tanto hardware como software, usadas para la realización de este proyecto.

5.1. USRP-2901

El Universal Software Radio Peripheral (USRP)-2901 es un SDR que permite "diseñar, crear prototipos e implementar rápidamente sistemas inalámbricos con procesamiento de señales personalizado", según afirma su fabricante National Instruments (NI) en su página web [20]. Podemos verlo en la imagen 5.1.



Figura 5.1: USRP-2901

Este dispositivo nos permite transmitir y recibir señales simultáneamente, ya que consta de dos canales de salida y de dos canales de entrada. Permite además conectarse a los ordenadores a través de USB 2.0 y USB 3.0. Las características técnicas más significativas se muestran en las tablas 5.1 y 5.2. La tabla 5.1 muestra las características para la transmisión de las señales

Tabla 5.1: Características transmisión USRP-2901

Rango de frecuencias	70 MHz a 6 GHz
Saltos de frecuencias	<1 KHz
Máxima potencia de salida	20 dBm
Rango de ganancia	89.75 dB
Saltos de ganancia	0.25 dB
Ancho de banda máximo	56 MHz

Tabla 5.2: Características recepción USRP-2901

Rango de frecuencias	70 MHz a 6 GHz
Saltos de frecuencias	<1 kHz
Máxima potencia de entrada	-15 dBm
Rango de ganancia	76 dB
Saltos de ganancia	1 dB
Figura del ruido	5 dB a 7 dB
Ancho de banda máximo	56 MHz

y la tabla 5.2 muestra las características para la recepción de señales. Estas tablas salen de las especificaciones del fabricante [21].

Para poder transmitir y recibir se han usado antenas VERT2450 [22], que trabajan a frecuencias en los rangos 2.4-2.5 y 4.9-5.9 GHz, bandas en las que trabaja 5G, entre otras.

5.2. srsRAN

srsRAN [23] es un software que permite el estudio de sistemas radio. Tiene dos proyectos, uno para 4G (srsRAN-4G) y otro para 5G (srsRAN-Project). El proyecto de 4G implementa tanto los UE como las BS y el core. Por otro lado, el proyecto de 5G implementa la BS de una red 5G, pudiendo utilizar el UE del proyecto srsRAN-4G, que soporta 5G SA. Cumple tanto las especificaciones de 3GPP [24] como las de O-RAN [25].

Para este proyecto se usará el gNB, que es como se le denomina a la BS en 5G, del proyecto del srsRAN de 5G, y el proyecto sobre 4G se usará para el srsUE. Además, la red troncal utilizada será Open5GS.

La arquitectura del gNB que implementa el srsRAN-Project es la mostrada en la figura 5.2.

Los bloques en azul son los que este proyecto implementa mediante software. En concreto, simula las entidades Centralized Unit (CU) y Distributed Unit (DU) así como la capa física.

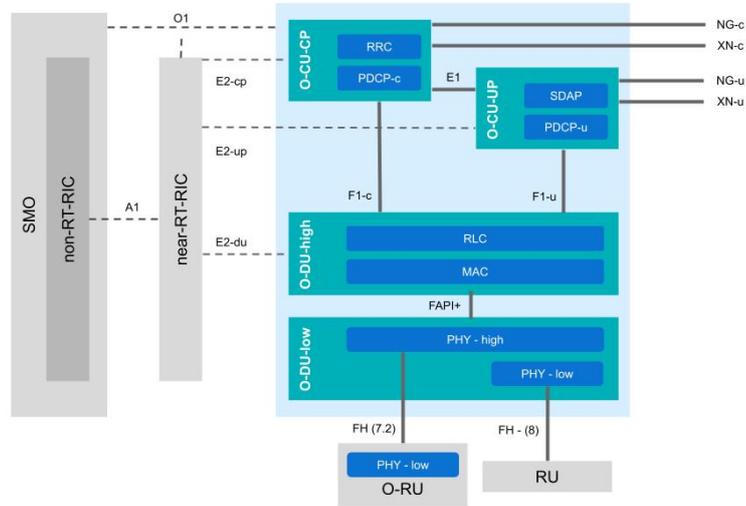


Figura 5.2: Componentes e interfaces gNB del srsRAN project.

5.3. Amarisoft

Amarisoft [26] es un software que permite implementar tanto una estación base 4G y 5G así como la red troncal. En este proyecto se configurará para implementar una estación base 5G y su red troncal. Tiene un fichero de configuración para el gNB que permite cambiar parámetros tales como la frecuencia, el ancho de banda y el número de antenas en la transmisión, entre otros. Permite también añadir los mensajes SIBs 2, 3, 4 y 9 a la transmisión. La estación base de Amarisoft Callbox Classic[27], se puede ver en la figura 5.3.

5.4. Toolbox 5G MATLAB

El toolbox de 5G de MATLAB tiene funciones conformes al estándar de 3GPP. Permite la configuración, simulación, medición y análisis de señales 5G. Aporta ejemplos de configuración de señales, además de la capacidad de generarlas con los parámetros que quiera el usuario si estos parámetros están conformes con las especificaciones de 3GPP. Permite también la transmisión de las señales generadas a través de diferentes dispositivos, como por ejemplo SDRs. Para más información puede visitar la página web de la referencia [28].

Tiene además un *script* llamado

“NRCellSearchMIBAndSIB1RecoveryExample” que permite demodular y decodificar una señal 5G. Esta función es la que se va a usar para la realización



Figura 5.3: Estación base Amarisoft.

de este proyecto. La función está descrita en la referencia [29].

Capítulo 6

Análisis de una señal 5G sintética usando la toolbox 5G de MATLAB y análisis de señales 5G reales

En el presente capítulo se describe el proceso de sincronización entre un UE y una BS. Se llevan a cabo diversas pruebas. Se inicia con el análisis de una señal sintética transmitida mediante un SDR y recibida por otro. El propósito es comprender y demostrar cómo se realiza la sincronización temporal, en frecuencia y en fase del UE con la BS así como la obtención de los mensajes MIB y SIB1 usando una señal sintética. Primero, se examinan los bloques SS/PBCH y, tras esto, los canales PDCCH y PDSCH en la sección 6.1.

Posteriormente, se analizan los bits del MIB y del SIB1 obtenidos mediante el uso de srsRAN (sección 5.2), con la intención de realizar un análisis real del mensaje SIB1 basado en los bits decodificados. Para ello, se utilizarán MATLAB (sección 5.4) y Wireshark, como se explica más adelante.

Por último, se analizan señales reales transmitidas mediante la estación base de Amarisoft (sección 5.3). El objetivo es poder demodular y decodificar una señal real transmitida y recibida mediante USRP (sección 5.1) y obtener los mensajes MIB y SIBs. En esta última parte se pretende analizar el mensaje SIB9.

6.1. Transmisión y recepción de una señal sintética

En esta sección se presenta el procedimiento para la transmisión y recepción de una señal generada sintéticamente utilizando USRPs (sección 5.1)

seguido del análisis de dicha señal.

La transmisión y recepción de la señal no se ha podido realizar desde un mismo portátil porque no tenía capacidad computacional, así que se ha tenido que emplear un ordenador conectado a un USRP para transmitir y otro para recibir. La señal se ha generado y transmitido usando una aplicación dentro de la *toolbox* de 5G de MATLAB (sección 5.4).

A partir de esta señal, se van a extraer los bloques SS/PBCH y se demodulará el canal PDSCH con el objetivo de obtener los bits del mensaje SIB1. Primero se muestra el espectrograma de la señal recibida en la figura 6.1.

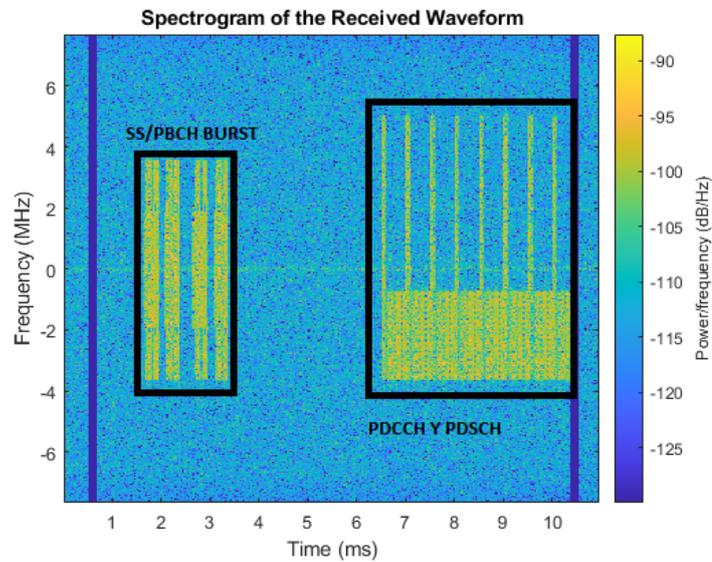


Figura 6.1: Espectrograma señal sintética.

Como se puede observar, existen 8 SSBlocks, por lo que se están simulando 8 haces. En la parte izquierda de la imagen podemos distinguir 4 bloques, que cada uno de ellos tiene 2 SSBlocks, mientras que, en la parte derecha de la imagen, podemos distinguir 8 bloques, los cuales pertenecen cada uno a una pareja de PDCCH y PDSCH tal y como se explicará posteriormente. En las figuras 6.2 y 6.3 podemos observar con más claridad todo esto que se acaba de explicar. En la figura 6.2 podemos ver dos bloques, que corresponden con los 4 últimos SSBlocks y en la figura 6.3 podemos ver la parte del espectrograma en la que están los canales PDCCH y PDSCH.

En lo que se refiere al bloque SS, se busca detectar y demodular las señales PSS y SSS. Como se mencionó en la sección 4.5.1, la señal PSS consiste en una secuencia predefinida de un banco de secuencias, donde el número de secuencias depende del modPCI. La detección se realiza mediante la correlación entre la señal recibida y las señales predefinidas. En general, el modo

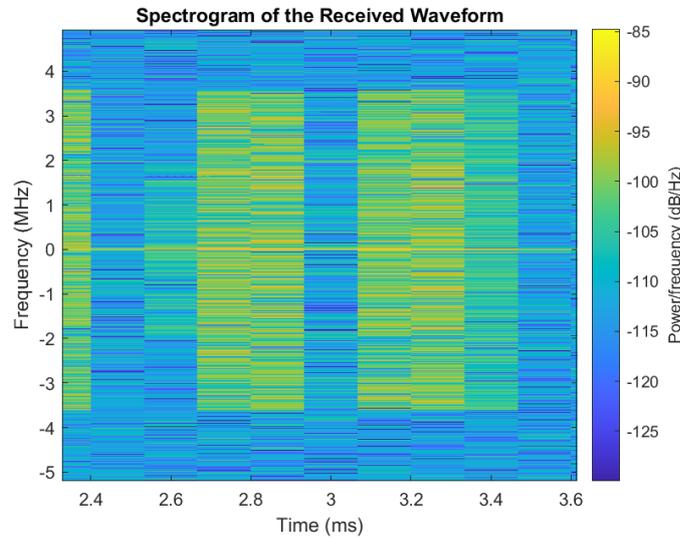


Figura 6.2: Espectrograma señal sintética parte bloque SS/PBCH.

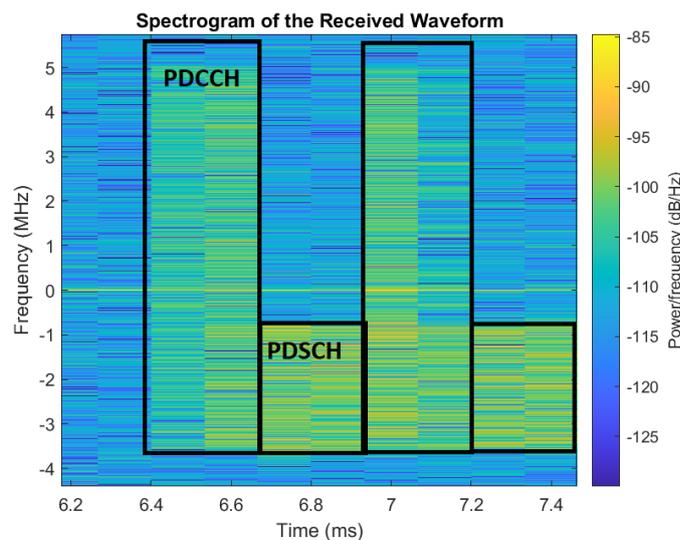


Figura 6.3: Espectrograma señal sintética parte canales PDSCH y PDCCH.

óptimo suele ser el 3, lo que implica tres posibles valores para la señal PSS. El número resultante de esta comparación entre las secuencias predefinidas y la secuencia recibida de la señal PSS se denomina N_{ID}^2 , que indica a qué sector de una BS pertenece. Junto con el valor N_{ID}^1 de la señal SSS, el UE puede determinar en qué celda se encuentra en un mapa de celdas. Un ejemplo de un mapa de celdas se muestra en la figura izquierda de la figura 4.12. Al detectar la señal PSS, también se obtiene el error de frecuencia de la señal, que representa el desplazamiento de la posición central, en frecuencia,

de la secuencia de la señal PSS con respecto a la frecuencia central de transmisión de la señal, así como el desplazamiento temporal del primer símbolo OFDM encontrado con respecto a una cuadrícula de referencia.

La secuencia de la señal SSS también es una secuencia predefinida de un banco de 336 posibles señales. Nuevamente, se detecta mediante correlación y el valor obtenido en esta comparación se denomina N_{ID}^1 . Una vez conocidos los valores N_{ID}^1 y N_{ID}^2 , se puede aplicar la fórmula 6.1.

$$N_{ID}^{cell} = 3 * N_{ID}^1 + N_{ID}^2 \quad (6.1)$$

Este valor es necesario para demodulaciones posteriores, tal y como se explicará cuando sea necesario.

En total, existen 1008 valores posibles para N_{ID}^{cell} , lo que implica que el mapa está dividido en 1008 celdas. Estas dos señales se muestran en las figuras 6.4 y 6.5.

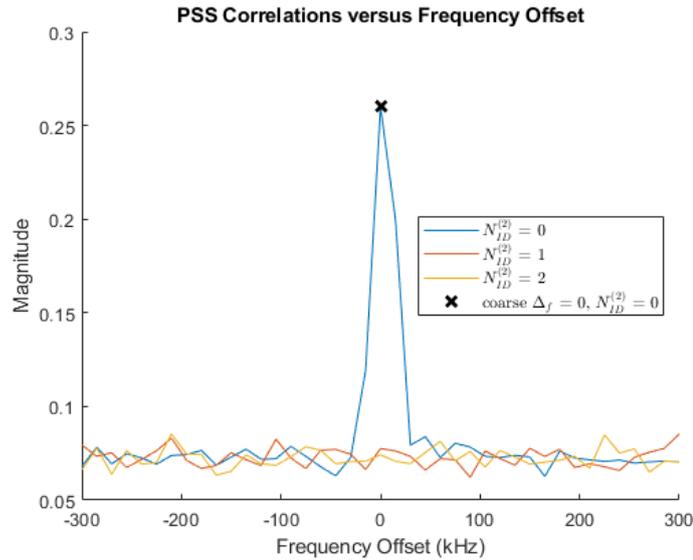


Figura 6.4: PSS señal sintética.

Como podemos ver, el valor del N_{ID}^2 es 0 y del N_{ID}^1 es de 34, lo que, según la ecuación 6.1, hace que el valor del N_{ID}^{cell} sea de 102.

También se detecta cuál de todos los haces transmitidos se recibe con mayor intensidad. Esto se hace comparando las SNR de cada haz. En nuestro caso, el haz con mayor SNR es el de índice 2, tal y como se ve en la figura 6.6.

El valor de N_{ID}^2 es utilizado para mapear la señal DMRS del canal PBCH, que es el siguiente bloque a decodificar del bloque SS/PBCH. Tanto esta señal como la de la señal SSS se utilizan, como se mencionó en la sección teórica 4.5.1, para evaluar el impacto del canal en la señal. Una vez conocido

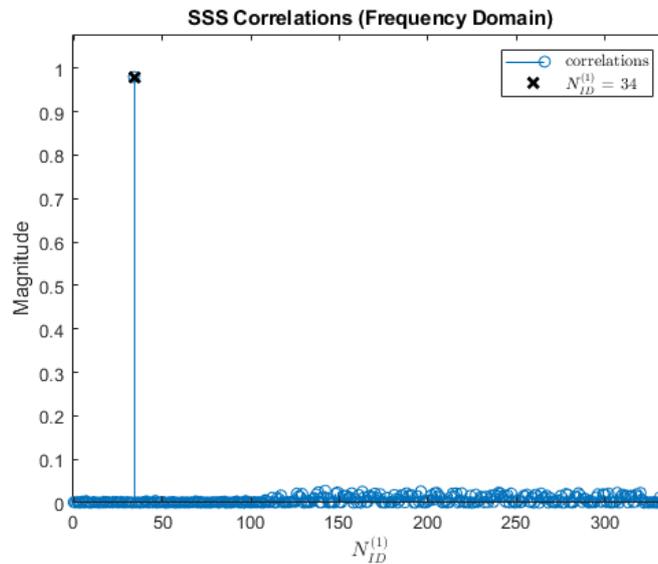


Figura 6.5: SSS señal sintética.

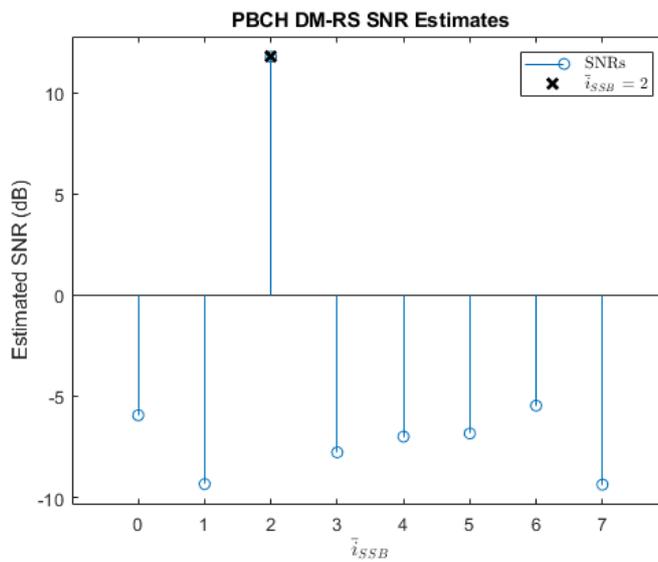


Figura 6.6: SNR de cada SSB.

el impacto del canal en la señal, se procede a decodificar la información del canal PBCH y, con ella, la información del mensaje MIB. En la figura 6.7 podemos ver la constelación del canal PBCH una vez demodulado.

El contenido del mensaje MIB obtenido se muestra en la figura 6.8. Podemos ver cada bloque de la tabla 4.5 en esta figura.

Una vez que se ha decodificado este bloque, ya se tiene la información ne-

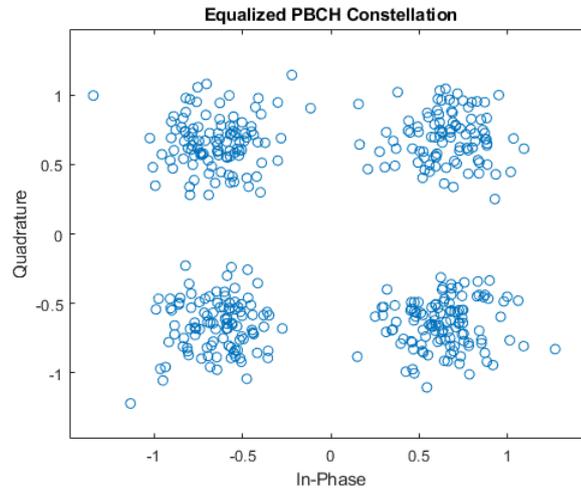


Figura 6.7: Constelación PBCH.

```

BCH/MIB Content:
                NFrame: 0
SubcarrierSpacingCommon: 30
                k_SSB: 0
DMRSTypeAPosition: 3
PDCCHConfigSIB1: [1x1 struct]
                CellBarred: 0
IntraFreqReselection: 0

```

Figura 6.8: Contenido MIB señal sintética.

cesaria para decodificar los canales PDCCH y PDSCH. A partir del canal PDCCH se extrae la información necesaria para decodificar el canal PDSCH, tal y como se dijo en la sección 4.3.2. Este último canal físico proporciona el canal de transporte DL-SCH, el cual contiene el mensaje SIB1.

Tanto la cuadrícula de recursos recibida como la constelación del canal PDCCH se pueden ver las figuras 6.9 y 6.10 respectivamente.

En las figuras 6.11 y 6.12 se nos muestran tanto el slot que contiene al canal PDSCH como la constelación del mismo.

Una vez demodulado el canal PDSCH y decodificado el canal DL-SCH, el programa nos da como variable los bits del mensaje SIB1. En este caso, los bits que nos da no contienen información útil, por lo que no se mostrarán en el documento.

Mientras se iba ejecutando el programa, este mostraba por pantalla infor-

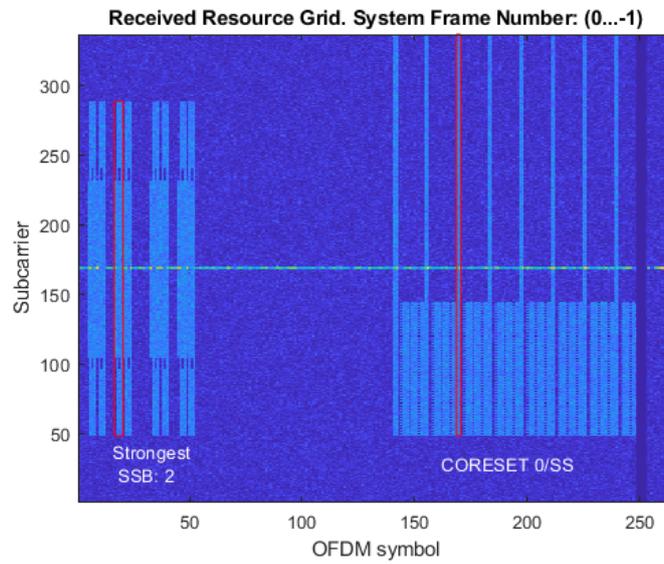


Figura 6.9: Cuadrícula de recursos recibida.

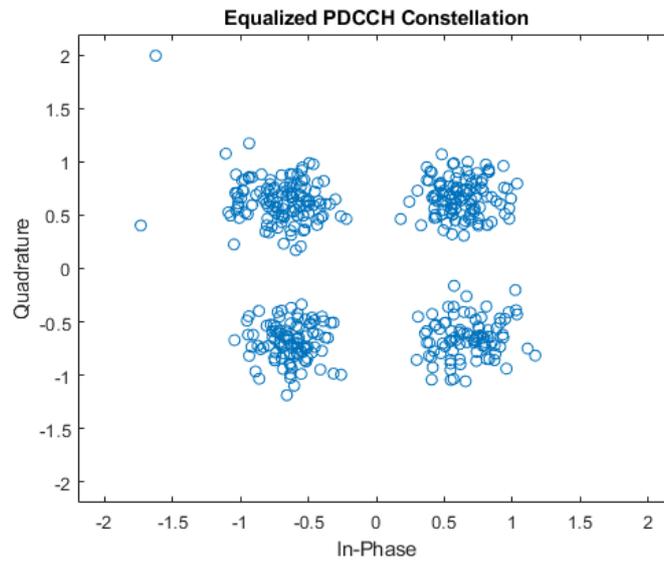


Figura 6.10: Constelación PDCCH.

mación sobre lo que iba ejecutando. Esto se muestra en la figura 6.13.

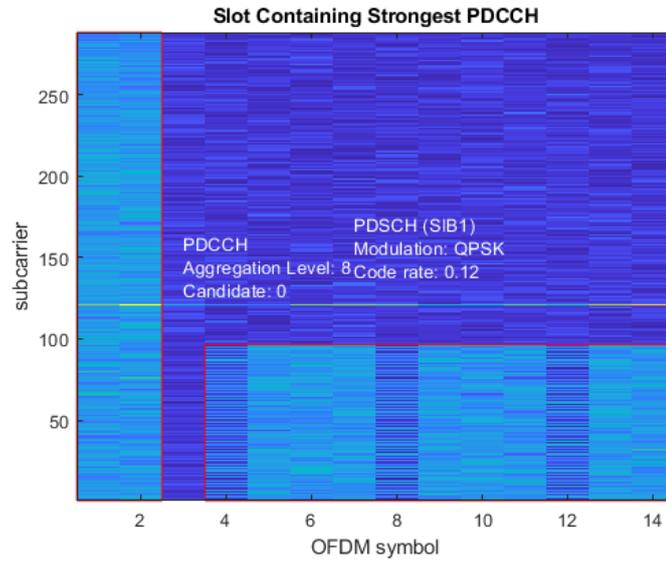


Figura 6.11: Slot que contiene el PDSCH a decodificar.

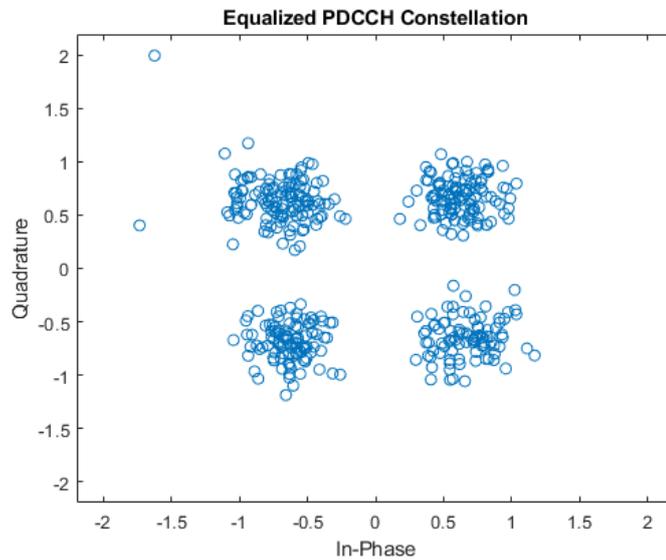


Figura 6.12: Constelación PDSCH.

```
>> NRCellSearchMIBAndSIB1RecoveryPropio
-- Frequency correction and timing estimation --
Frequency offset: 3288 Hz
Time offset to synchronization block: 31943 samples (2.0796 ms)
Cell identity: 102
-- PBCH demodulation and BCH decoding --
PBCH RMS EVM: 26.757%
BCH CRC: 0
SSB index: 2
BCH/MIB Content:
      NFrame: 0
SubcarrierSpacingCommon: 30
      k_SSB: 0
      DMRSTypeAPosition: 3
      PDCCHConfigSIB1: [1x1 struct]
      CellBarred: 0
      IntraFreqReselection: 0

-- Downlink control information message search in PDCCH --
Decoded PDCCH candidate #1 at aggregation level 8
PDCCH RMS EVM: 28.047%
PDCCH CRC: 0
-- PDSCH demodulation and DL-SCH decoding --
PDSCH RMS EVM: 25.614%
PDSCH CRC: 0
SIB1 decoding succeeded.
```

Figura 6.13: Datos mostrados por pantalla por el programa.

6.2. Análisis bits de los mensajes MIB y SIB1 procedentes de una transmisión con el software srsRAN

En esta actividad se busca demodular y decodificar los bits reales de los mensajes MIB y SIB1 usando el software srsRAN (sección 5.2). Este software implementa una estación base 5G NR, la cual se ha usado, junto con un USRP, para transmitir una señal 5G. Haciendo uso de otro USRP y de MATLAB se ha recibido esta señal 5G para su posterior análisis. Se va a hacer el mismo análisis de la señal recibida que se hizo en la actividad anterior. Además, este software permite, mediante registros, ver la información que está generando la estación base y recibiendo el dispositivo. Esto será útil para comprobar si la información que decodificamos de la señal es correcta. Hay que mencionar que este software solo permite el envío del mensaje SIB1 y no permite el envío de otros mensajes SIBs.

Antes de empezar con el análisis de la señal cabe destacar el uso de un reloj basado en GPS (GPSDO, GPS *disciplined oscillator*) [30]. Este reloj ha sido adquirido días antes de la finalización del TFG. Antes de obtener este reloj, la recepción de señales transmitidas entre la estación base del software srsRAN y un USRP no era posible debido a, según se leyó tras una búsqueda exhaustiva en los foros técnicos de srsRAN, un problema en la precisión del

6.2. Análisis bits de los mensajes MIB y SIB1 procedentes de una transmisión con el software srsRAN

reloj. Este reloj, basado en GPS, tiene una salida que se puede ajustar para generar una señal senoidal de 10 MHz y que se puede conectar a la entrada REF IN de los SDR usados. Por lo tanto, se ha podido conectar este reloj a la estación transmisora y al receptor y se ha solucionado el problema de precisión de reloj existente. Mencionado esto, se procede a analizar la señal transmitida.

Primero de todo, se muestran en la tabla 6.1 las características más relevantes de la señal recibida.

Tabla 6.1: Datos de generación de la señal de srsRAN.

<i>banda de trabajo</i>	n78
<i>frecuencia de transmisión</i>	3489,42 MHz
<i>ancho de banda</i>	20 MHz
<i>n_{id_cell}</i>	1
<i>espacio entre subportadoras</i>	30 kHz
<i>cell_barred</i>	true
<i>intraFreqReselection</i>	true
<i>dmrs – TypeA – Position</i>	pos2

Como se puede ver en esta tabla, la señal se transmite a con una frecuencia central de 3489,42 MHz y con un ancho de banda de 20 MHz. Esto implica que la frecuencia de muestreo es de 30.72 MHz. También se puede observar que el N_{ID}^{cell} es el 1. El resto de valores se comentarán cuando se decodifique el mensaje MIB de la señal.

Para el análisis de esta señal se ha recibido medio segundo y luego se ha segmentado para obtener un trozo de la propia señal en el que estuviesen el bloque SS/PBCH y los canales PDCCH y PDSCH.

Este trozo de señal es el que se ha usado en MATLAB para demodularlo y decodificarlo. A continuación, se van a mostrar las gráficas más significativas que nos proporciona el *script* de MATLAB mientras hace la demodulación y decodificación de la señal tal y como se vio en la sección 6.1. Este *script* ha tenido que ser modificado para poder detectar todo el ancho de banda que ocupa la señal. Ya que es superior al que usaba la señal sintética del apartado anterior.

En la figura 6.14 se muestra el espectrograma de este trozo mencionado. Se puede observar cómo solo se transmite un haz.

Lo primero que hace el *script* de MATLAB es detectar las señales PSS y el SSS del bloque SS. Las figuras que muestran las correlaciones entre las secuencias de estas señales y las señales predeterminadas son las 6.15 y 6.16.

Como se puede observar, el valor del N_{ID}^1 es 0 y el del N_{ID}^2 es 1. Si calculamos el valor del N_{ID}^{cell} con la ecuación 6.1 obtenemos el valor 1, que se

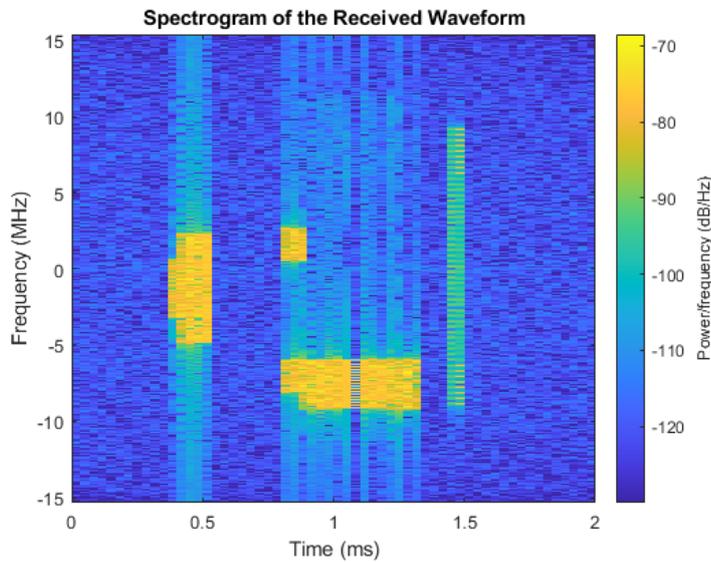


Figura 6.14: Espectrograma trozo señal transmitida mediante srsRAN.

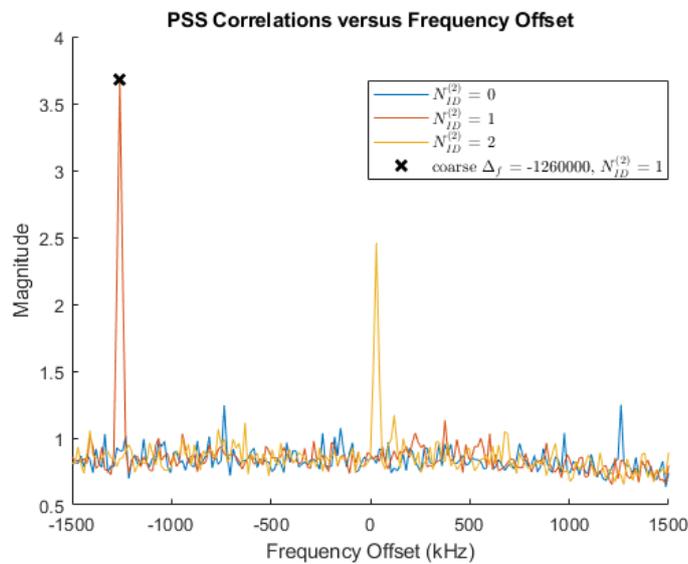


Figura 6.15: Detección PSS señal transmitida mediante srsRAN.

corresponde con lo descrito en la tabla 6.1.

Tras esto, se pasa a demodular el canal PBCH y a decodificar el MIB. Tras la decodificación del MIB, nos muestra la información que contiene. Esta información se muestra en la figura 6.17.

Ahora podemos comparar la información decodificada con la que nos daba la tabla 6.1. Podemos observar que el espaciado entre subportadoras es de

6.2. Análisis bits de los mensajes MIB y SIB1 procedentes de una transmisión con el software srsRAN

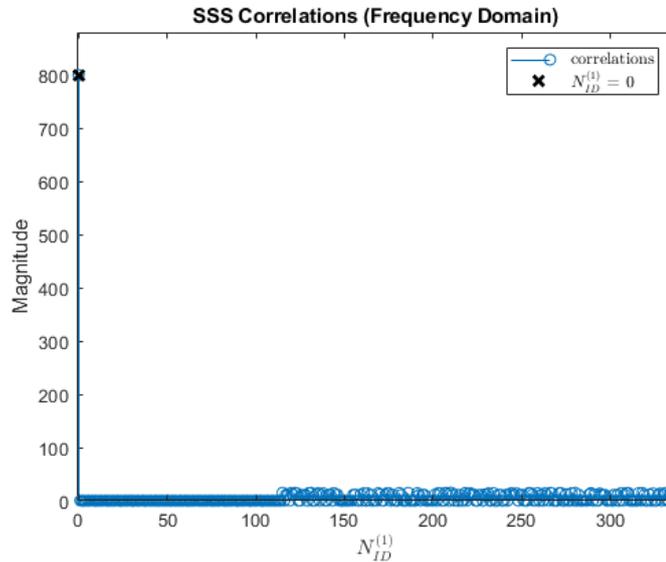


Figura 6.16: Detección SSS señal transmitida mediante srsRAN.

```
BCH/MIB Content:
                    NFrame: 896
SubcarrierSpacingCommon: 30
                    k_SSB: 0
DMRSTypeAPosition: 2
PDCCHConfigSIB1: [1x1 struct]
                    CellBarred: 1
                    IntraFreqReselection: 1
```

Figura 6.17: Datos MIB de la señal transmitida mediante srsRAN.

30 kHz, y que los valores de *cellBarred* y *IntraFreqReselection* coinciden. En concreto, son *notBarred* y *notAllowed* según lo visto en la sección de teoría 4.4.1.

Tras la decodificación del MIB, el siguiente paso es la detección y demodulación de los canales PDCCH y PDSCH. A continuación, en la figura 6.18, se muestra la ranura que contiene a estos dos canales.

Y en la figura 6.19 se muestra la constelación del canal PDSCH, el cual usa modulación QPSK. Como podemos observar, la constelación no es perfecta, existen puntos que no están en las nubes principales que corresponden a los 4 símbolos de la modulación y, por lo tanto, no se demodulan correctamente. Sin embargo, al decodificar la señal demodulada, gracias a la codificación de canal, se decodifica correctamente la información que transporta.

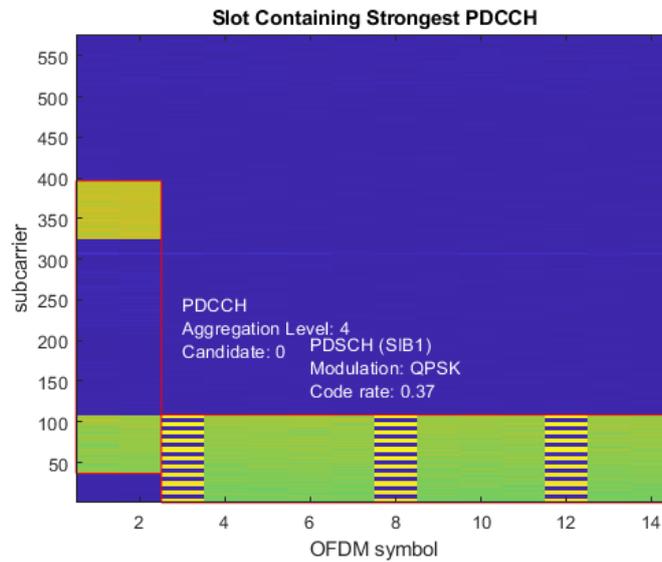


Figura 6.18: Ranura que contiene a los canales PDCCH y PDSCH de la señal transmitida mediante srsRAN.

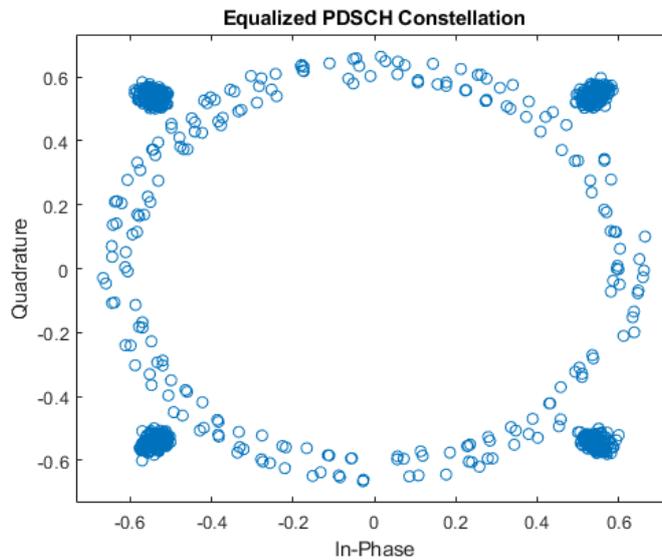


Figura 6.19: Constelación canal PDSCH de la señal transmitida mediante srsRAN.

Tras la decodificación del canal PDSCH ya se puede demodular el canal DL-SCH y obtener los bits del mensaje SIB1. Los bits del mensaje SIB1 se han procesado mediante una función de MATLAB denominada "pcapSIB1". Esta función recibe como argumento de entrada

6.2. Análisis bits de los mensajes MIB y SIB1 procedentes de una transmisión con el software srsRAN

los bits del mensaje SIB1 y genera un archivo en formato .pcapng, el cual es compatible con Wireshark y permite visualizar de forma estructurada y comprensible la información transmitida por el mensaje SIB1. En el apéndice A se puede ver esta función. La llamada a la función que se realiza sería el siguiente comando: `pcapSIB1(bitsSIB1)`

El objetivo de poder visualizar esta información es compararla con la información que se transmitió. La información que se envió se puede ver en los registros del software tal y como se explicó anteriormente. A continuación, se va a comparar la información obtenida de estos registros con la que nos proporciona el archivo compatible con Wireshark generado, el cual contiene la información del SIB1 decodificado anteriormente. Primero se van a mostrar los campos del mensaje SIB1 decodificado, que tienen que coincidir con los vistos en la tabla 4.9.

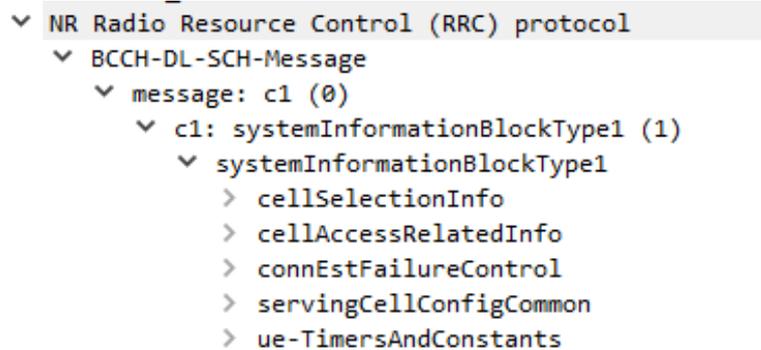


Figura 6.20: Contenido general SIB1 de transmisión con srsRAN.

En la figura 6.20 podemos ver todos estos campos a excepción del campo *si – SchedulingInfo*, porque en la transmisión con srsRAN no se transmiten más mensajes SIBs que el mensaje SIB1 y el campo *uacBarringInfo*, ya que esta transmisión no contempla la restricción de celdas basadas en el control de acceso unificado, que es la información que transporta este campo. Y a continuación se muestra la comparación de cada uno de los campos. Primero vamos a comparar el campo *cellSelectionInfo* en la figura 6.21.

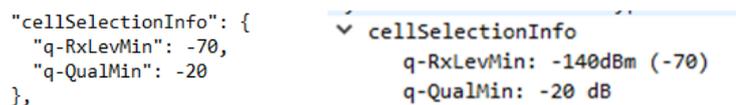


Figura 6.21: Contenido campo *cellSelectionInfo* SIB1.

A la izquierda de la imagen podemos ver los datos originales y a la derecha los datos extraídos de Wireshark.

El siguiente campo a comprobar es el *cellAccessRelatedInfo*, el cual podemos ver en la figura 6.22 y 6.23.

```

"cellAccessRelatedInfo": {
  "plmn-IdentityList": [
    {
      "plmn-IdentityList": [
        {
          "mcc": [
            9,
            0,
            1
          ],
          "mnc": [
            7,
            0
          ]
        }
      ],
      "trackingAreaCode": "00000000000000000000111",
      "cellIdentity": "000000000000000001100110110000001",
      "cellReservedForOperatorUse": "notReserved"
    }
  ]
},

```

Figura 6.22: Contenido campo *cellAccessRelatedInfo* SIB1 original.

En la imagen 6.22 se puede observar los datos originales y en la imagen 6.23 los datos de Wireshark. Los campos *trackingAreaCode* y *cellIdentity* de los datos originales están expresados en binario y los de Wireshark están expresados en hexadecimal.

El siguiente campo es el de *connEstFailureControl*, presentado en la figura 6.24. De nuevo, a la izquierda los datos originales y a la derecha los extraídos de los bits del SIB1. A continuación se va a mostrar el campo *-servingCellConfigCommon*, que, como se vio en la parte de teoría, tiene varias tablas.

Se pueden observar los parámetros de este campo que se vieron en la sección de teoría 4.4.2.

Y por último se muestra el campo del *ueTimerAndConstants* en la figura 6.28.

Como se puede observar en todas estas figuras, la información recibida y decodificada se corresponde con la información que se mandó originalmente en la BS simulada. Por lo que se puede afirmar que se ha realizado una correcta decodificación de los bits del SIB1. Esto nos será útil cuando podamos recibir señales 5G que contengan el SIB9.


```

    servingCellConfigCommon
    ▼ downlinkConfigCommon
      ▼ frequencyInfoDL
        ▼ frequencyBandList: 1 item
          ▼ Item 0
            ▼ NR-MultiBandInfo
              freqBandIndicatorNR: 3
            offsetToPointA: 13 PRBs
            ▼ scs-SpecificCarrierList: 1 item
              ▼ Item 0
                ▼ SCS-SpecificCarrier
                  offsetToCarrier: 0
                  subcarrierSpacing: kHz15 (0)
                  carrierBandwidth: 52
            ▼ initialDownlinkBWP
              ▼ genericParameters
                locationAndBandwidth: 14025
                subcarrierSpacing: kHz15 (0)
              > pdccch-ConfigCommon: setup (1)
              > pdsch-ConfigCommon: setup (1)
            ▼ bcch-Config
              modificationPeriodCoeff: n4 (1)
            > pcch-Config

    "servingCellConfigCommon": {
      "downlinkConfigCommon": {
        "frequencyInfoDL": {
          "frequencyBandList": [
            {
              "freqBandIndicatorNR": 3
            }
          ],
          "offsetToPointA": 13,
          "scs-SpecificCarrierList": [
            {
              "offsetToCarrier": 0,
              "subcarrierSpacing": "kHz15",
              "carrierBandwidth": 52
            }
          ]
        },
        "initialDownlinkBWP": {
          "genericParameters": {
            "locationAndBandwidth": 14025,
            "subcarrierSpacing": "kHz15"
          }
        },
        "bcch-Config": {
          "modificationPeriodCoeff": "n4"
        }
      }
    }
  
```

Figura 6.25: Contenido campo *servingCellConfigCommon*downlink SIB1.

```

    "uplinkConfigCommon": {
      "frequencyInfoUL": {
        "frequencyBandList": [
          {
            "freqBandIndicatorNR": 3
          }
        ],
        "absoluteFrequencyPointA": 348564,
        "scs-SpecificCarrierList": [
          {
            "offsetToCarrier": 0,
            "subcarrierSpacing": "kHz15",
            "carrierBandwidth": 52
          }
        ],
        "p-Max": 10
      },
      "initialUplinkBWP": {
        "genericParameters": {
          "locationAndBandwidth": 14025,
          "subcarrierSpacing": "kHz15"
        },
        "timeAlignmentTimerCommon": "infinity"
      },
      "n-TimingAdvanceOffset": "n0",
    }

    ▼ uplinkConfigCommon
      ▼ frequencyInfoUL
        ▼ frequencyBandList: 1 item
          ▼ Item 0
            ▼ NR-MultiBandInfo
              freqBandIndicatorNR: 3
              absoluteFrequencyPointA: 348564
            ▼ scs-SpecificCarrierList: 1 item
              ▼ Item 0
                ▼ SCS-SpecificCarrier
                  offsetToCarrier: 0
                  subcarrierSpacing: kHz15 (0)
                  carrierBandwidth: 52
            p-Max: 10 dBm
            ▼ initialUplinkBWP
              ▼ genericParameters
                locationAndBandwidth: 14025
                subcarrierSpacing: kHz15 (0)
              > rach-ConfigCommon: setup (1)
              > pusch-ConfigCommon: setup (1)
              > pucch-ConfigCommon: setup (1)
              timeAlignmentTimerCommon: infinity (7)
            n-TimingAdvanceOffset: n0 (0)
  
```

Figura 6.26: Contenido campo *servingCellConfigCommon*uplink SIB1.

de un SDR para su posterior análisis en MATLAB. El objetivo es aplicar los conocimientos adquiridos en la sección de la señal sintética 6.1 para poder decodificar esta señal y obtener el mensaje SIB1 y los adquiridos en la sección 6.2 para interpretarlo. La función de MATLAB usada en la sección 6.1 ha tenido que ser modificada para poder realizar la detección, demodulación y decodificación de todos los bloques, canales y señales de la señal 5G de Amarisoft. Se ha modificado el ancho de banda en el que buscaba a la señal

6.3. Análisis mensajes MIB y SIBs procedentes de una señal transmitida mediante la estación base de Amarisoft

68

```

"ssb-PositionsInBurst": {
  "inOneGroup": "10000000"
},
"ssb-PeriodicityServingCell": "ms10",
"ss-PBCH-BlockPower": 0

▼ ssb-PositionsInBurst
  inOneGroup: 80 [bit length 8, 1000 0000 decimal value 128]
  ssb-PeriodicityServingCell: ms10 (1)
  ss-PBCH-BlockPower: 0 dBm

```

Figura 6.27: Contenido campo *servingCellConfigCommon* Parte3 SIB1.

```

"ue-TimersAndConstants": {
  "t300": "ms1000",
  "t301": "ms1000",
  "t310": "ms1000",
  "n310": "n1",
  "t311": "ms30000",
  "n311": "n1",
  "t319": "ms1000"
}

▼ ue-TimersAndConstants
  t300: ms1000 (5)
  t301: ms1000 (5)
  t310: ms1000 (5)
  n310: n1 (0)
  t311: ms30000 (6)
  n311: n1 (0)
  t319: ms1000 (5)

```

Figura 6.28: Contenido campo *ueTimerConstants* SIB1.

para poder adaptarlo al ancho de banda de nuestra señal.

A continuación se empezará con el análisis de la señal. Para ello, primero se van a ver las características de la señal que nos interesan en la tabla 6.2.

Tabla 6.2: Datos de generación de la señal de Amarisoft.

<i>banda de trabajo</i>	n78
<i>frecuencia de transmisión</i>	3489,42 MHz
<i>ancho de banda</i>	10 MHz
<i>ssb_pos_bitmap</i>	10000000
<i>n_id_cell</i>	500
<i>espacio entre subportadoras</i>	30 KHz
<i>cell_barred</i>	false
<i>intraFreqReselection</i>	true
<i>dmrs – TypeA – Position</i>	pos2

La señal se está transmitiendo a una frecuencia de 3489,42 MHz y con un ancho de banda de 10 MHz. Esto implica que la recepción de la señal se tiene que hacer con una frecuencia de muestreo de 15,36 MHz. El dato del *ssb_pos_bitmap* nos indica cuantos haces se están mandando. En este caso

solo 1 de los posibles 8 que puede haber como máximo según las especificaciones 3GPP (tabla 4.4). También se nos indica que el valor del N_{ID}^{cell} es de 500.

Después de esto, hay ciertos valores de la configuración que pertenecen al mensaje MIB, por lo que, cuando pasemos a la decodificación del mensaje MIB de la señal recibida, los compararemos.

Tras realizar la recepción de la señal, de una duración de medio segundo, se ha segmentado para solo quedarnos con un trozo que contenga todos los bloques necesarios para la sincronización. Esto podemos verlo en la figura 6.29.

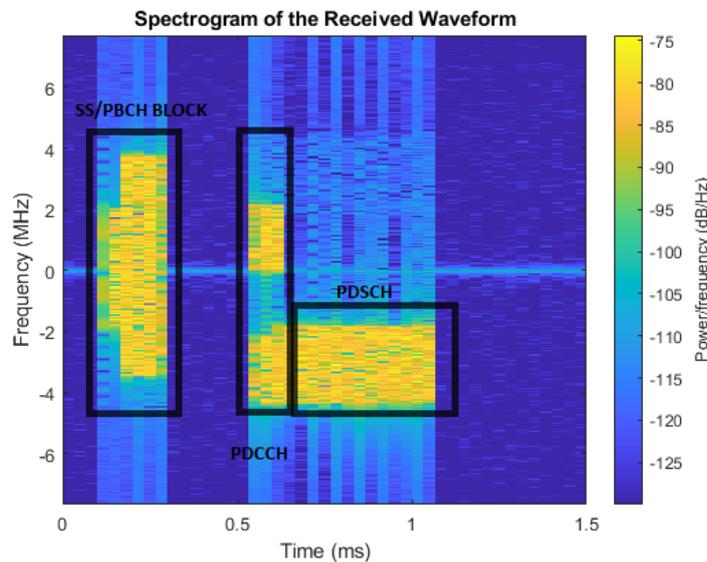


Figura 6.29: Espectrograma trozo señal Amarisoft.

Aquí podemos ver además cómo solo hay un haz en la transmisión de esta señal 5G. Ahora, esta señal la vamos a pasar por el script de MATLAB que se usó en el apartado de la señal sintética (sección 6.1) para poder sacar la información que transporta. Lo primero que hace es detectar las secuencias del PSS y del SSS para poder sacar el N_{ID}^{cell} . La correlación que aplica para poder obtener los valores del N_{ID}^1 y del N_{ID}^2 se puede ver en las figuras 6.30 y 6.31.

Como se puede observar, el valor del N_{ID}^1 es 166 y el del N_{ID}^2 es 2. Si calculamos el valor del N_{ID}^{cell} con la ecuación 6.1 obtenemos el valor 500, que se corresponde con lo descrito en la tabla 6.2. Lo siguiente que hace el script es demodular el canal PBCH, decodificar el canal BCH y, tras esta decodificación, obtener el mensaje MIB.

Los datos del mensaje MIB se muestran en la figura 6.32. Como podemos observar, el valor del espaciado entre subportadoras es de 30 kHz, el valor

70 **6.3. Análisis mensajes MIB y SIBs procedentes de una señal transmitida mediante la estación base de Amarisoft**

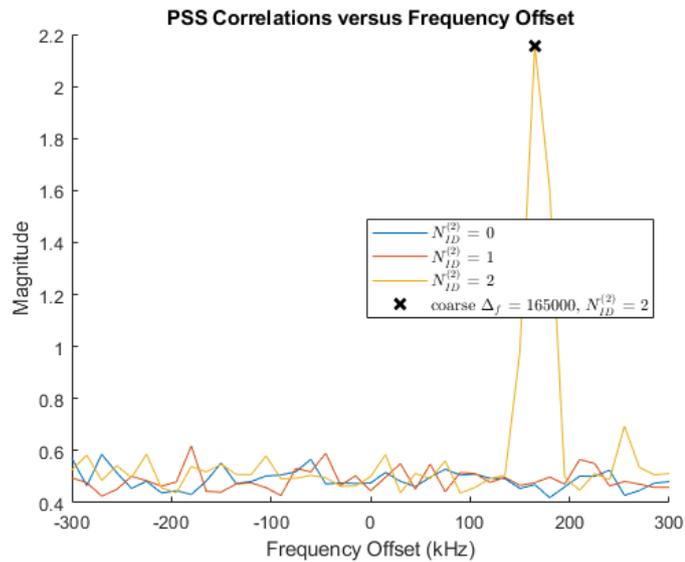


Figura 6.30: Detección PSS señal Amarisoft.

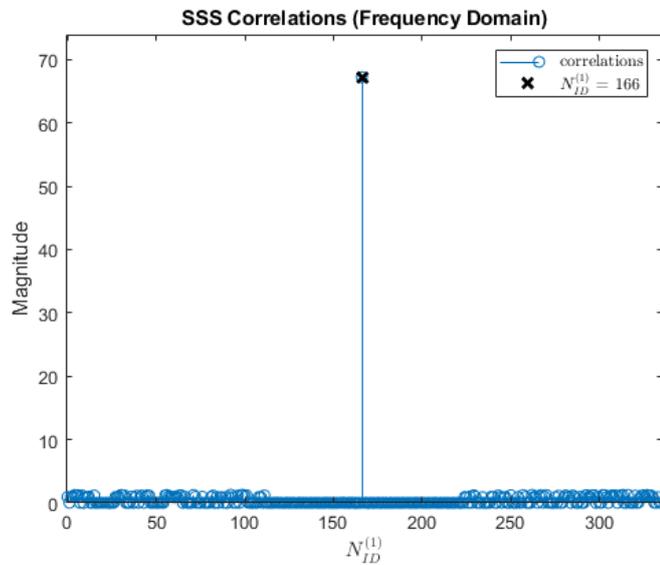


Figura 6.31: Detección SSS señal Amarisoft.

del *dmrs - TypePosition* es *pos2*, el valor del *cellBarred* es *notBarred* y el *intraFreqReselection* es *allow*, lo cual cuadra con lo que hay en la tabla 6.2.

Además, MATLAB detecta el haz que llega con más fuerza y como solo hay uno, obtenemos la figura 6.33.

Una vez decodificado el mensaje MIB, el *script* pasa a demodular el canal

```
BCH/MIB Content:
                NFrame: 786
SubcarrierSpacingCommon: 30
                k_SSB: 12
DMRSTypeAPosition: 2
PDCCHConfigSIB1: [1x1 struct]
                CellBarred: 1
IntraFreqReselection: 0
```

Figura 6.32: MIB decodificado de la señal de Amarisoft.

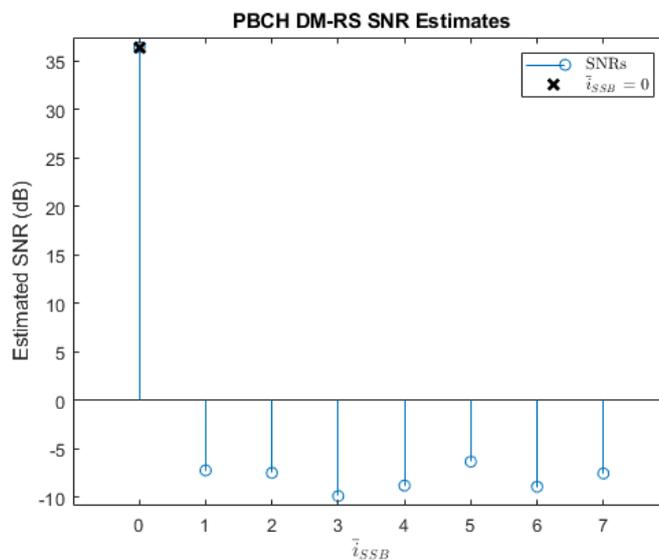


Figura 6.33: Haces detectados de la señal de Amarisoft.

PDCCH y a decodificar el mensaje DCI tal y como se hizo en la sección de la señal sintética 6.1.

Tanto la constelación del canal PDCCH como la cuadrícula de recursos recibida se muestran en las figuras 6.34 y 6.35 respectivamente.

Y una vez decodificado el mensaje DCI del canal PDCCH podemos demodular el canal PDSCH. En este caso usa una modulación QPSK y su constelación se muestra en la figura 6.36.

Como podemos observar, la constelación no es perfecta, existen puntos que no están en las nubes principales que corresponden a los 4 símbolos de la modulación y, por lo tanto, no se demodulan correctamente. Sin embargo, al decodificar la señal demodulada, gracias a la codificación de canal, se decodifica correctamente la información que transporta.

Tras esto, el script nos devuelve los bits del mensaje SIB1. Los cuales usaremos posteriormente. Antes de esto se muestra en la figura 6.37 lo que el programa nos ha ido mostrando por pantalla mientras ejecutaba el script.

6.3. Análisis mensajes MIB y SIBs procedentes de una señal transmitida mediante la estación base de Amarisoft

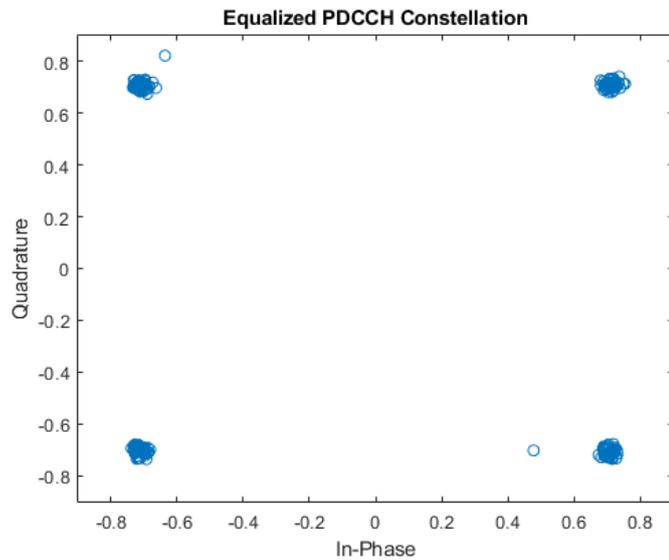


Figura 6.34: Constelación PDCCH de la señal de Amarisoft.

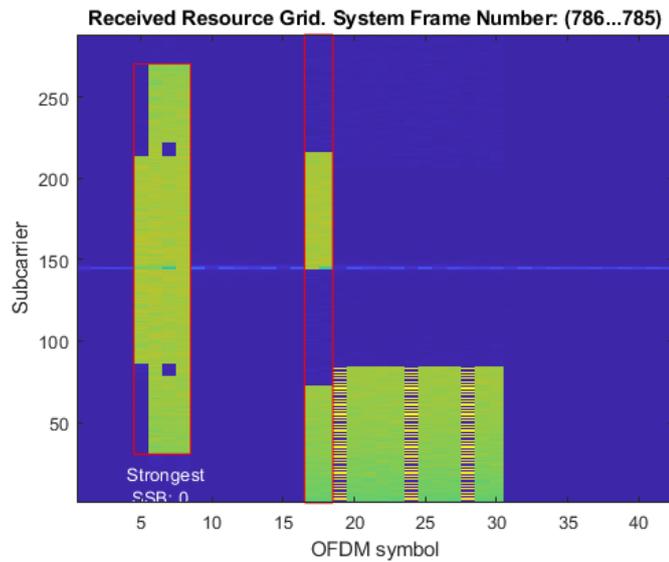


Figura 6.35: Cuadrícula de recursos recibida de la señal de Amarisoft.

Ahora se va a usar la función `pcapSIB1` usada en la sección 6.2 para poder obtener un fichero compatible con Wireshark que contenga la información del mensaje SIB1. Con esta información se va a realizar una comparación entre los datos decodificados y los datos que nos proporcionan los registros de Amarisoft. Tal y como se hizo en la sección 6.2. Se empezará por el campo `cellSelectionInfo` en la figura 6.38. A continua-

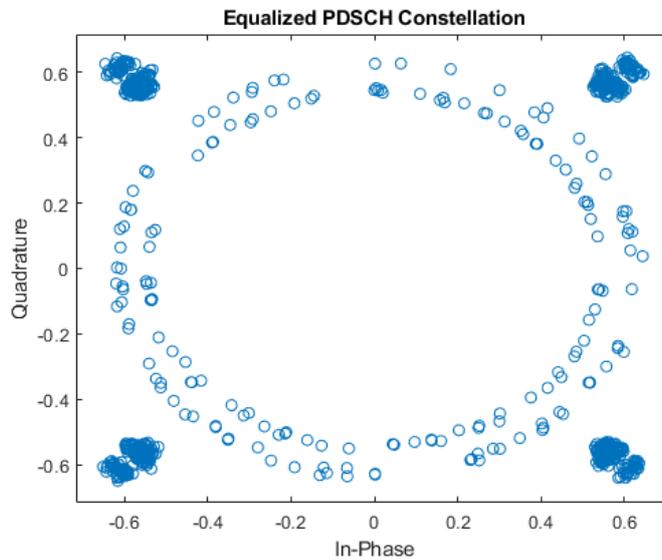


Figura 6.36: Constelación PDSCH de la señal de Amarisoft.

```
>> NRCellSearchMIBAndSIB1RecoveryPropio
-- Frequency correction and timing estimation --
Frequency offset: 168120 Hz
Time offset to synchronization block: 2010 samples (0.1309 ms)
Cell identity: 500
-- PBCH demodulation and BCH decoding --
PBCH RMS EVM: 2.727%
BCH CRC: 0
SSB index: 0
BCH/MIB Content:
      NFrame: 786
SubcarrierSpacingCommon: 30
      k_SSB: 12
DMRSTypeAPosition: 2
  PDCCHConfigSIB1: [1x1 struct]
    CellBarred: 1
  IntraFreqReselection: 0

-- Downlink control information message search in PDCCH --
Decoded PDCCH candidate #1 at aggregation level 4
PDCCH RMS EVM: 2.690%
PDCCH CRC: 0
-- PDSCH demodulation and DL-SCH decoding --
PDSCH RMS EVM: 22.667%
PDSCH CRC: 0
SIB1 decoding succeeded.
```

Figura 6.37: Datos mostrados por pantalla de la señal Amarisoft.

ción, se verán los campos *cellAccessRelatedInfo*, *connEstFailureControl* y *ue – TimersAndConstants* en las figuras 6.39, 6.40, 6.41 y 6.42 respecti-

6.3. Análisis mensajes MIB y SIBs procedentes de una señal transmitida mediante la estación base de Amarisoft

vamente. Y, por último, se verá la comparación del campo *servicingellConfigCommon* en las figuras 6.43 6.44 y 6.45.

```
cellSelectionInfo {
  q-RxLevMin -70,
  q-QualMin -20
},
cellSelectionInfo
  q-RxLevMin: -140dBm (-70)
  q-QualMin: -20 dB
```

Figura 6.38: Comparación campo *cellSelectionInfo* SIB1 señal Amarisoft.

```
cellAccessRelatedInfo {
  plmn-IdentityInfoList {
    {
      plmn-IdentityList {
        {
          mcc {
            9,
            0,
            1
          },
          mnc {
            7,
            0
          }
        }
      },
      trackingAreaCode '000064'H,
      cellIdentity '0012345010'H,
      cellReservedForOperatorUse notReserved
    }
  },
}
```

Figura 6.39: Campo *cellAccessRelatedInfo* SIB1 de la señal de Amarisoft original.

Como se puede observar tras todas estas figuras, la recepción de la señal transmitida desde la estación base de Amarisoft y recibida por un SDR se ha realizado correctamente.

Como se puede comprobar, en la transmisión realizada no se transmiten más SIBs. Esto se puede saber porque no está el campo *si – SchedulingInfo*, el cual es el que transmite esta información.

En este punto nos parece importante resaltar que se han tenido problemas con las capturas. Tras una búsqueda exhaustiva en los foros técnicos de srs-RAN, tal y como se mencionó en la sección 6.2, es probable que se deba a la

```

    cellAccessRelatedInfo
    └─ plmn-IdentityList: 1 item
        └─ Item 0
            └─ PLMN-IdentityInfo
                └─ plmn-IdentityList: 1 item
                    └─ Item 0
                        └─ PLMN-Identity
                            └─ mcc: 3 items
                                └─ Item 0
                                    MCC-MNC-Digit: 9
                                └─ Item 1
                                    MCC-MNC-Digit: 0
                                └─ Item 2
                                    MCC-MNC-Digit: 1
                            └─ mnc: 2 items
                                └─ Item 0
                                    MCC-MNC-Digit: 7
                                └─ Item 1
                                    MCC-MNC-Digit: 0
                            trackingAreaCode: 000064 [bit length 24, 000]
                            cellIdentity: 0012345010 [bit length 36, 4 L]
                            cellReservedForOperatorUse: notReserved (1)
    
```

Figura 6.40: Campo *cellAccessRelatedInfo* SIB1 de la señal de Amarisoft decodificada.

```

connEstFailureControl {
    connEstFailCount n1,
    connEstFailOffsetValidity s30,
    connEstFailOffset 1
},
    connEstFailureControl
    connEstFailCount: n1 (0)
    connEstFailOffsetValidity: s30 (0)
    connEstFailOffset: 1 dB
    
```

Figura 6.41: Comparación campo *connEstFailureControl* SIB1 de la señal de Amarisoft.

precisión del reloj, ya que la mayoría de usuarios utiliza un reloj basado en GPS (GPSDO, GPS *disciplined oscillator*). Por eso, la mayoría de señales capturadas no se decodifican correctamente, al encontrarse errores en la demodulación inicial. El tutor ha adquirido un reloj GPSDO, tal y como se comentó anteriormente, días antes de la entrega de este TFG. Esto ha hecho que se hayan podido realizar pruebas con srsRAN pero que no haya habido tiempo para probar con la estación base de Amarisoft. Por esto mismo, de las señales recibidas solo alguna ha sido demodulada completamente, y en esa no se mandaba más que el SIB1 porque es algo que se configura en Amarisoft. En otras pruebas sí se han incluido el resto de SIBs (SIB2, 3, 4 y 9)

6.3. Análisis mensajes MIB y SIBs procedentes de una señal transmitida mediante la estación base de Amarisoft

76

```

ue-TimersAndConstants {
  t300 ms1000,
  t301 ms1000,
  t310 ms1000,
  n310 n1,
  t311 ms30000,
  n311 n1,
  t319 ms1000
}
}
}

```

```

▼ ue-TimersAndConstants
  t300: ms1000 (5)
  t301: ms1000 (5)
  t310: ms1000 (5)
  n310: n1 (0)
  t311: ms30000 (6)
  n311: n1 (0)
  t319: ms1000 (5)

```

Figura 6.42: Comparación campo *ue – TimersAndConstants* SIB1 de la señal de Amarisoft.

```

servingCellConfigCommon {
  downlinkConfigCommon {
    frequencyInfoDL {
      frequencyBandList {
        {
          freqBandIndicatorNR 78
        }
      },
      offsetToPointA 4,
      scs-SpecificCarrierList {
        {
          offsetToCarrier 0,
          subcarrierSpacing kHz30,
          carrierBandwidth 24
        }
      }
    },
    initialDownlinkBWP {
      genericParameters {
        locationAndBandwidth 6325,
        subcarrierSpacing kHz30
      },
      bcch-Config {
        modificationPeriodCoeff n4
      },
      pcch-Config {
        defaultPagingCycle rf128,
        nAndPagingFrameOffset oneT: NULL,
        ns one
      }
    }
  },
}

```

```

▼ servingCellConfigCommon
  ▼ downlinkConfigCommon
    ▼ frequencyInfoDL
      ▼ frequencyBandList: 1 item
        ▼ Item 0
          ▼ NR-MultiBandInfo
            freqBandIndicatorNR: 78
            offsetToPointA: 4 PRBs
          ▼ scs-SpecificCarrierList: 1 item
            ▼ Item 0
              ▼ SCS-SpecificCarrier
                offsetToCarrier: 0
                subcarrierSpacing: kHz30 (1)
                carrierBandwidth: 24
    ▼ initialDownlinkBWP
      ▼ genericParameters
        locationAndBandwidth: 6325
        subcarrierSpacing: kHz30 (1)
      > pdcc-ConfigCommon: setup (1)
      > pdsch-ConfigCommon: setup (1)
    ▼ bcch-Config
      modificationPeriodCoeff: n4 (1)
    ▼ pcch-Config
      defaultPagingCycle: rf128 (2)
    ▼ nAndPagingFrameOffset: oneT (0)
      oneT: NULL
      ns: one (2)

```

Figura 6.43: Comparación campo *servingcellConfigCommon_DL* SIB1 de la señal de Amarisoft.

que puede mandar Amarisoft por lo que tenemos los registros con sus campos y valores, pero no tenemos una señal que se decodifique correctamente. En la figura 6.46 se muestra la constelación del canal PDSCH obtenida tras el intento de obtención del SIB1 a través de una señal de ancho de banda de

```

uplinkConfigCommon {
  frequencyInfoUL {
    scs-SpecificCarrierList {
      {
        offsetToCarrier 0,
        subcarrierSpacing kHz30,
        carrierBandwidth 24
      }
    },
    p-Max 10
  },
  initialUplinkBWP {
    genericParameters {
      locationAndBandwidth 6325,
      subcarrierSpacing kHz30
    },
    timeAlignmentTimerCommon infinity
  },
}

```

```

▼ uplinkConfigCommon
  ▼ frequencyInfoUL
    ▼ scs-SpecificCarrierList: 1 item
      ▼ Item 0
        ▼ SCS-SpecificCarrier
          offsetToCarrier: 0
          subcarrierSpacing: kHz30 (1)
          carrierBandwidth: 24
        p-Max: 10 dBm
      ▼ initialUplinkBWP
        ▼ genericParameters
          locationAndBandwidth: 6325
          subcarrierSpacing: kHz30 (1)
        > rach-ConfigCommon: setup (1)
        > pusch-ConfigCommon: setup (1)
        > pucch-ConfigCommon: setup (1)
        timeAlignmentTimerCommon: infinity (7)

```

Figura 6.44: Comparación campo *servingcellConfigCommon_UL* SIB1 de la señal de Amarisoft.

10 MHz. Se puede observar una constelación que no ha sido bien recibida. También se ha probado con señales de distinto ancho de banda, pero se ha tenido el mismo problema de precisión de los relojes. Se han probado señales de ancho de banda de 15 y 20 MHz. Sobre la señal de 15 MHz, podemos ver su espectrograma en la figura 6.47 y la constelación del canal PDSCH en la figura 6.48.

Y a continuación se muestra la constelación del canal PDSCH para la señal de ancho de banda de 20 MHz en la figura 6.49.

Se pueden observar en ambas constelaciones como están rotadas y no se demodulan correctamente.

Como se ha dicho, los registros de Amarisoft nos permiten ver los campos del SIB1 cuando se están transmitiendo el resto de SIBs. Además, también permite ver los campos de estos SIBs. En las figuras 6.50 y 6.51 podemos ver el campo *si – SchedulingInfo* y el contenido del SIB9 respectivamente.

Como se puede observar en la figura 6.50, se transmiten los SIBs 2, 3, 4 y 9. Los SIBs 2 y 3 con una periodicidad de 16 tramas y los SIBs 4 y 9 con una periodicidad de 32 tramas.

Por último, en la figura 6.51 podemos ver el contenido del SIB9. Si nos fijamos, podemos encontrar todos los campos vistos en la sección 4.4.2 menos el campo *referenceTimeInfo-r16* porque nuestra estación base de Amarisoft usa un Release anterior al 16. Podemos ver el tiempo en UTC en el campo *timeInfoUTC*. El campo *dayLightSavingTime* nos indica que hay 1 hora más con respecto el DST por un cambio horario y el campo *leapSeconds* nos permite conocer la hora GPS. Por último, el *localTimeOffset* nos indica

6.3. Análisis mensajes MIB y SIBs procedentes de una señal transmitida mediante la estación base de Amarisoft

78

```
ssb-PositionsInBurst {
  inOneGroup '80'H
},
ssb-PeriodicityServingCell ms20,
tdd-UL-DL-ConfigurationCommon {
  referenceSubcarrierSpacing kHz30,
  pattern1 {
    dl-UL-TransmissionPeriodicity ms5,
    nrofDownlinkSlots 7,
    nrofDownlinkSymbols 6,
    nrofUplinkSlots 2,
    nrofUplinkSymbols 4
  }
},
ss-PBCH-BlockPower -32
},
```

- ▼ ssb-PositionsInBurst
 - inOneGroup: 80 [bit length 8, 1000 0000 decimal value 128]
- ssb-PeriodicityServingCell: ms20 (2)
- ▼ tdd-UL-DL-ConfigurationCommon
 - referenceSubcarrierSpacing: kHz30 (1)
 - ▼ pattern1
 - dl-UL-TransmissionPeriodicity: ms5 (6)
 - nrofDownlinkSlots: 7
 - nrofDownlinkSymbols: 6
 - nrofUplinkSlots: 2
 - nrofUplinkSymbols: 4
- ss-PBCH-BlockPower: -32 dBm

Figura 6.45: Resto comparación campo *servingcellConfigCommon* SIB1 de la señal de Amarisoft.

que existe una diferencia entre la hora local y la hora UTC de 2 horas.

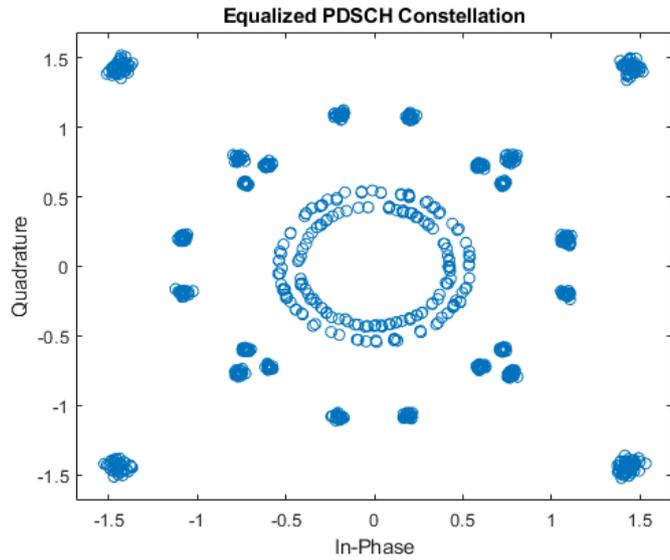


Figura 6.46: Constelación canal PDSCH de la señal de Amarisoft no demodulado.

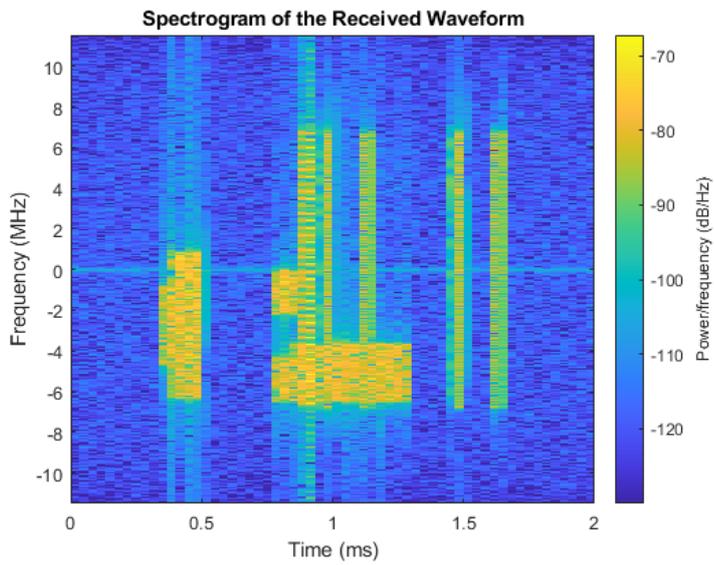


Figura 6.47: Espectrograma de la señal capturada de ancho de banda de 15 MHz transmitida con la estación base de Amarisoft.

80 **6.3. Análisis mensajes MIB y SIBs procedentes de una señal transmitida mediante la estación base de Amarisoft**

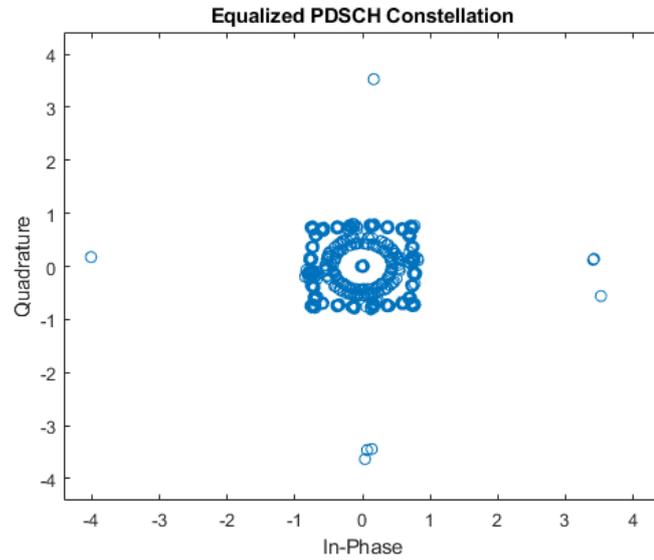


Figura 6.48: Constelación del canal PDSCH de la señal capturada de ancho de banda de 15 MHz transmitida con la estación base de Amarisoft.

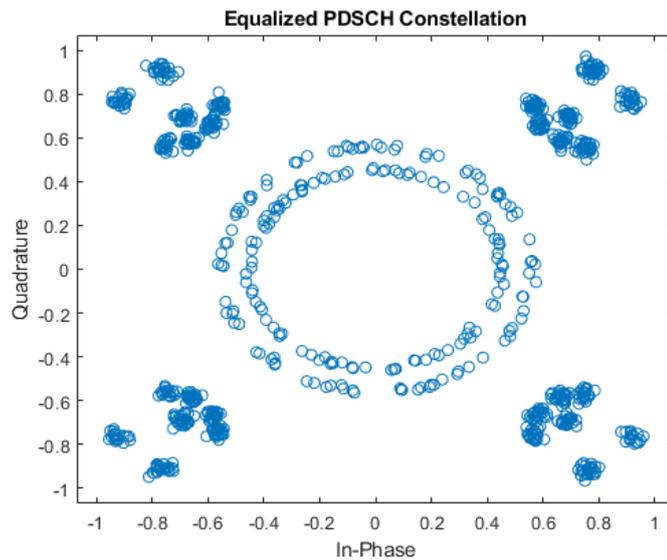


Figura 6.49: Constelación del canal PDSCH de la señal capturada de ancho de banda de 20 MHz transmitida con la estación base de Amarisoft.

```
si-SchedulingInfo {
  schedulingInfoList {
    {
      si-BroadcastStatus broadcasting,
      si-Periodicity rf16,
      sib-MappingInfo {
        {
          type sibType2,
          valueTag 0
        }
      }
    },
    {
      si-BroadcastStatus broadcasting,
      si-Periodicity rf16,
      sib-MappingInfo {
        {
          type sibType3,
          valueTag 0
        }
      }
    }
  },
}
```

Figura 6.50: Campo *si – SchedulingInfo* del SIB1 de la señal de Amarisoft.

```
From: ENB
Info: 150.214.190.85:9001, v2023-06-10
Time: 12:55:03.812
Index: 383
Message: SIB

Data:
{
  message c1: systemInformation: {
    criticalExtensions systemInformation: {
      sib-TypeAndInfo {
        sib9: {
          timeInfo {
            timeInfoUTC 389702490384,
            daylightSavingTime '01'B,
            leapSeconds 18,
            localTimeOffset 8
          }
        }
      }
    }
  }
}
```

Figura 6.51: Contenido del mensaje SIB9 de la señal de Amarisoft.

**6.3. Análisis mensajes MIB y SIBs procedentes de una señal
82 transmitida mediante la estación base de Amarisoft**

Capítulo 7

Conclusiones

En este capítulo se presentan las conclusiones obtenidas a partir del estudio realizado sobre la sincronización con señales 5G. Estas conclusiones resumen los principales hallazgos, resultados y contribuciones del trabajo. Además, se brinda una reflexión crítica sobre las limitaciones del estudio y se ofrecen recomendaciones para trabajos futuros en esta área.

7.1. Conclusiones

Debido a que ciertos servicios (e.g. uso de TSN para Industria 4.0) tienen mayores requisitos de sincronización, se ha estudiado cómo se decodifican las señales 5G para obtener una sincronización precisa y fiable con una estación base. La sincronización del reloj entre los diferentes dispositivos y la estación base se realiza mediante el mensaje SIB9. El mensaje SIB9 transmite la información sobre el reloj de la estación base, de forma que el UE puede sincronizarse a dicho reloj si recibe y decodifica este mensaje. El objetivo de este trabajo ha sido obtener esta información y, aunque hubo algunas dificultades debido a la precisión del reloj, se logró en gran medida.

El estudio de la sincronización ha sido precedido por el estudio de los canales y señales de 5G, así como su estructura y sus características de transmisión. También ha sido imprescindible el manejo del software y hardware necesario para poder trabajar con estas señales. Ha sido preciso familiarizarse con el software srsRAN, la estación base de Amarisoft y también realizar un estudio exhaustivo de la *toolbox* 5G de MATLAB, empleados para la elaboración de este proyecto.

Durante el proceso de realización de este trabajo, se han tenido que dar pasos independientes entre sí que han sido usados posteriormente para poder realizar un análisis de una señal 5G profundizando en los parámetros que transportan la información necesaria para el procedimiento de sincronización.

En primer lugar, se estudió cómo se realiza la demodulación y decodifica-

ción del bloque SS/PBCH y de los canales PDCCH y PDSCH de una señal sintética transmitida y recibida mediante el uso de SDRs. Esto se hizo para poder obtener el mensaje SIB1 del canal PDSCH. El mensaje SIB1 es importante porque transporta, entre otros datos, información sobre los demás SIBs y, por tanto, es necesario para poder decodificar el SIB9. El problema que tuvo este mensaje SIB1 es que no transportaba información útil (es decir, la información transportada en este mensaje era una secuencia aleatoria de bits) porque la señal sintética que se genera con la *toolbox* de MATLAB solo transmite el bloque SS/PBCH y los canales PDCCH y PDSCH (este último canal solo transporta el mensaje SIB1, no transporta más información que sí se transporta en las señales reales).

Posteriormente, se analizaron los bits que correspondían a un mensaje SIB1 real obtenidos de la decodificación de una señal transmitida mediante el software srsRAN. Con este software generamos y transmitimos una señal 5G real. Se ha comprobado que el análisis de esos bits se hizo correctamente comparándolos con la información del mensaje SIB1 que se estaba enviando, la cual se podía saber a través de los registros de este software. Como se comentó en el análisis de esta actividad, el software srsRAN no permite el envío de otros mensajes SIBs. Estas actividades anteriores han permitido tener los conocimientos y el manejo de las herramientas necesarios para poder trabajar con señales reales transmitidas inalámbricamente que envían el mensaje SIB9.

La última actividad realizada ha sido la recepción, demodulación y decodificación de los bits del mensaje SIB1 de una señal real transmitida a través de la estación base de Amarisoft. Esta estación base sí permite el envío de otros mensajes SIBs, tales como el SIB2, 3, 4 y 9. Esta demodulación y decodificación de la señal no ha sido sencilla. De hecho, no se ha podido realizar como nos hubiese gustado. Si bien es cierto que se consiguió demodular y decodificar bien una señal hasta el punto de obtener el mensaje SIB1, esta no contenía el mensaje SIB9, algo que se configura en Amarisoft. Debido a un problema de precisión de reloj del dispositivo, tal y como se ha indicado en la sección 6.3, la demodulación de las señales transmitidas por la estación base de Amarisoft no ha podido llevarse a cabo en todas las pruebas que se han realizado. Aun así, se consiguió obtener el mensaje SIB1 de una de ellas de manera correcta, denotando que, en cuanto se solucione el problema de precisión de reloj, será posible conseguirlo en más escenarios. Aunque esta señal no transmitía el mensaje SIB9, Amarisoft permite, mediante una interfaz gráfica, ver los mensajes enviados en tiempo real, por lo que sí se ha podido hacer un análisis del mensaje SIB9. Se ha podido comprobar que este mensaje almacena y transporta la información de la hora UTC de la estación base transmisora.

7.2. Trabajo futuro

Enlazando con la última parte de la sección de conclusiones, los retos que plantea esta investigación están claros:

- Decodificación de la señal 5G de Amarisoft con diferentes configuraciones una vez que el reloj GPSDO esté conectado a la estación.
- Decodificación del mensaje SIB9 a partir de señales capturadas con la estación base de Amarisoft.
- Implementación en tiempo real de la decodificación del MIB, SIB1 y SIB9 para poder implementarlo en el banco de pruebas del proyecto 6G-CHRONOS.

Bibliografía

- [1] A. T. y. T. N. Harry Holma, *5G TECHNOLOGY 3GPP NEW RADIO*. WILEY and Sons ltd., 2020.
- [2] C. Johnson, *5G New Radio in Bullets*, 2019.
- [3] WiMuNet. Wimunet. [Online]. Available: <https://wimunet.ugr.es/>
- [4] D. P. Yakov Kryukov and E. Rogozhnikov, “Cell search and synchronization in 5g nr,” *ITM Web Conf*, no. 04007, 2019.
- [5] A. Omri, M. Shaqfeh, A. Ali, and H. Alnuweiri, “Synchronization procedure in 5g nr systems,” *IEEE Access*, vol. 7, pp. 41 286–41 295, 2019.
- [6] J. Boiko, I. Pyatin, and O. Eromenko, “Analysis of signal synchronization conditions in 5g mobile information technologies,” in *2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 2022, pp. 01–06.
- [7] J.-C. Lin, “Synchronization requirements for 5g: An overview of standards and specifications for cellular networks,” *IEEE Vehicular Technology Magazine*, vol. 13, no. 3, pp. 91–99, 2018.
- [8] M. U. Hadi, T. Jacobsen, R. Abreu, and T. Kolding, “5g time synchronization: Performance analysis and enhancements for multipath scenarios,” in *2021 IEEE Latin-American Conference on Communications (LATINCOM)*, 2021, pp. 1–5.
- [9] R. Verdecia-Peña and J. I. Alonso, “Design and synchronization procedures of a d&f co-operative 5g network based on sdr hardware interface: performance analysis,” *Sensors*, vol. 22, no. 3, p. 913, 2022.
- [10] 3GPP, “NR Physical channels and modulation (Release17),” 3GPP, Tech. Rep., 12 2022.
- [11] electronicsnotes. 5g data channels: Physical; transport; logical. [Online]. Available: <https://www.electronics-notes.com/>

- com/articles/connectivity/5g-mobile-wireless-cellular/
data-channels-physical-transport-logical.php
- [12] 3GPP, “NR Physical layer procedures for control (Release17),” 3GPP, Tech. Rep., 03 2023.
- [13] —, “NR User Equipment (UE) radio transmission and reception; Part 1: Range 1 Standalone (Release17),” 3GPP, Tech. Rep., 03 2023.
- [14] —, “NR Multiplexing and channel coding (Release17),” 3GPP, Tech. Rep., 03 2023.
- [15] —, “NR Radio Resource Control (RRC) protocol specification (Release17),” 3GPP, Tech. Rep., 03 2023.
- [16] S. Hong, D. Kim, J. Moon, K. Lee, and I. Joe, “5g nr based initial access procedure simulation environment implementation including system information using ns-3 simulator,” in *2023 25th International Conference on Advanced Communication Technology (ICACT)*, 2023, pp. 171–173.
- [17] 3GPP, “NR Physical layer procedures for control (Release17),” 3GPP, Tech. Rep., 06 2023.
- [18] —, “NR Radio Resource Control (RRC) protocol specification (Release16),” 3GPP, Tech. Rep., 03 2023.
- [19] M. Korde, “Synchronization aspects in 5g,” in *2020 International Conference on Communication and Signal Processing (ICCSP)*, 2020, pp. 0474–0478.
- [20] N. Instruments. Dispositivo de radio definido por software usrp. [Online]. Available: <https://www.ni.com/es-es/shop/hardware/products/usrp-software-defined-radio-device.html?modelId=125046>
- [21] —. Usrc-2901 specifications. [Online]. Available: <https://www.ni.com/docs/en-US/bundle/usrp-2901-specs/page/specs.html#note-d730e476>
- [22] —. Vert2450 antenna certificaciones de productos. [Online]. Available: <https://www.ni.com/es-es/support/documentation/product-certifications/model.vert2450-antenna.html>
- [23] srs RAN Project. Open source ran. [Online]. Available: <https://www.srslte.com/>
- [24] 3GPP. 3gpp specifications. [Online]. Available: <https://www.3gpp.org/specifications-technologies>

-
- [25] O.-R. alliance. O-ran specifications lead the telecom industry towards open and intelligent radio access networks. [Online]. Available: <https://www.o-ran.org/specifications>
- [26] amarisoft. amarisoft. [Online]. Available: <https://www.amarisoft.com/>
- [27] ——. amarisoft. [Online]. Available: https://www.amarisoft.com/app/uploads/2022/03/userguide_callbox_classic.pdf
- [28] MATLAB. 5g toolbox. [Online]. Available: <https://es.mathworks.com/products/5g.html#wavegen>
- [29] Matlab. Nr cell search and mib and sib1 recovery. [Online]. Available: <https://es.mathworks.com/help/5g/ug/nr-cell-search-and-mib-and-sib1-recovery.html>
- [30] L. B. ELECTRONICS. Precision gps reference clock. [Online]. Available: http://www.leobodnar.com/shop/index.php?main_page=product_info&cPath=107&products_id=234

Apéndice A

Función pcapSIB1

La función pcapSIB1 se puede ver a continuación.

```
1 function pcapSIB1(sib1bits)
2
3     % write transport block to a PCAPNG file
4     filename = 'SIB1_Amarisoft_23_06';
5     if (exist([filename '.pcapng'],'file'))
6         delete([filename '.pcapng']);
7     end
8     w = pcapngWriter('FileName',filename);
9
10    interface = '5GNR';           % Interface name
11    linkType = 252;               % EXPORTED_PDU
12    interfaceID = writeInterfaceDescriptionBlock(w,linkType,interface)
13        ;
14
15    name = 'nr-rrc.bcch.dl.sch';
16    tagProtoName = ['00'; '0C'];           % Tag: PDU content
17    protocol name (12)
18    protoLength = ['00'; dec2hex(length(name),2)]; % Length
19    protoName = dec2hex(double(name).'); % Protocol Name
20    tagEndOfOptions = ['00'; '00'];           % Tag: End-of-
21    options (0)
22    optionlength = ['00'; '00'];           % Length (0)
23
24    sib1Octets = dec2hex(bin2dec(char(reshape(sib1bits,8,[]).' + '0'))
25        );
26
27    packet = [tagProtoName; protoLength; protoName; tagEndOfOptions;
28        optionlength; sib1Octets];
29
30    t = datetime('now','TimeZone','local');
31    timestamp = posixtime(t) * 1e6;
32
33    write(w,packet,timestamp,interfaceID);
34    clear w;
35
36    % decode with tshark
37    %system('tshark -r BCCH_DLSCH_Message.pcapng -V');
38
39 end
```