Universidad Zaragoza

Escuela de Ingeniería y Arquitectura
Universidad Zaragoza

Proyecto Final de Carrera
Ingeniería de Telecomunicación
Curso 2011-2012

Modelado y simulación de un sistema de guerra electrónica (jamming) en una transmisión de datos inalámbrica crítica en seguridad

Marcos Félez Trasobares

Julio de 2012

Director: Oroitz Elgezabal Gómez
Codirector: Hannes Wagner
Ponente: Alfonso Ortega Giménez

Departamento de Sistemas de Seguridad e Ingeniería de Sistemas
German Aerospace Center (DLR)

Departamento de Ingeniería Electrónica y Comunicaciones
Escuela de Ingeniería y Arquitectura
Universidad de Zaragoza

Para mi familia y todos aquellos
que me apoyaron durante este largo camino

Modelado y simulación de un sistema de guerra electrónica (jamming) en una transmisión de datos inalámbrica crítica en seguridad

RESUMEN

Las infraestructuras de telecomunicaciones cableadas están siendo sustituidas por sus equivalentes inalámbricos debido a la versatilidad y flexibilidad de estos últimos, así como por su facilidad de despliegue. Los sistemas inalámbricos presentan, aun así, importantes desventajas que están retrasando su implantación en ciertos sectores donde la seguridad es crítica y donde es obligatorio garantizar cierto rendimiento del sistema bajo toda circunstancia de funcionamiento.

Hasta el momento la industria aeroespacial no ha introducido en sus sistemas los equivalentes inalámbricos, es ahora cuando se está implantando la tecnología inalámbrica para sistemas secundarios (como proporcionar internet al pasajero o un sistema interno de comunicaciones). El Instituto de Sistemas de Vuelo del Centro Aeroespacial Alemán (“German Aerospace Center”) va un paso más allá y está desarrollando el equivalente inalámbrico de los actuales Sistemas de Control de Vuelo cableados, presentes en toda la aviación actual.

Los sistemas de control de vuelo conforman una de las partes más sensibles del avión ya que es lo que permite al piloto controlar todos los elementos móviles del aparato. Por ello, las normativas que rigen el funcionamiento de estos sistemas críticos en seguridad son muy estrictas, ya que un fallo podría significar una catástrofe.

El uso de tecnologías inalámbricas implica que el sistema debe ser capaz de sobreponerse a las variaciones del canal, de adaptarse y reconfigurarse para poder funcionar en entornos hostiles (entornos con muchas interferencias, ruido etc.) y de combatir ataques electromagnéticos dirigidos hacia él, a fin de garantizar la fiabilidad del sistema en todo momento.

Con este objetivo se propone estudiar las diferentes posibilidades existentes entre las tecnologías inalámbricas para la creacion de un sistema de control de vuelo inalámbrico, asi como estudiar, clasificar y caracterizar los tipos de ataques que podrían ser perpetrados contra él. Posteriormente se diseñará la base de un sistema de control de vuelo inalámbrico y se construirá un entorno de simulación en Matlab/Simulink donde se procederá a comprobar el comportamiento del sistema diseñado y su funcionamiento en presencia de ataques electromagnéticos. Por último se diseñarán y se incluirán en el modelo de simulink medidas para combatir posibles ataques y también para mitigar la variabilidad del canal inalámbrico.

Página dejada en blanco
intencionadamente

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ACRÓNIMOS

AGC	Automatic Gain Control
AWGN	Additive White Gaussian Noise
BBJ	Broadband Jamming
BER	Bit Error Rate
BPS	Bits per Second
CAST	Commercial Aviation Safety Team
CDMA	Code Division Multiple Acces
CR	Cognitive Radio
CW	Continuous Rave
DF	Direction Finding
DLR	German Aerospace Center
DSSS	Direct Sequence Spread Spectrum
EA	Electronic Attack
EMCOM	Emission Control
EoB	Electronic Order of Battle
EP	Electronic Protect
ES	Electronic Support
FBW	Flight by Wire
FCS	Flight Control System
FDMA	Frequency Division Multiple Access
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
ICAO	International Civil Aviation Organization
ICI	Intercarrier Interference
IFFT	Inverse fast Fourier transform
ISI	Intersimbolic Interference
LPD	Low Probability of Detection
LPE	Low Probability of Exploitation

LPI	Low Probability of Interception
LS	Leas-square
MMSE	Minimum mean square error
MTJ	Multitone Jamming
NBJ	Narroband Jamming
OFDM	Orthogonal Frequency Division Multiplexing
PBJ	Partialband Jamming
POD	Probability of Detection
POE	Probability of Exploitation
POI	Probability of Interception
PSK	Phase Shift Keying
PTT	Push-to-talk
RF	Radio Frequency
RGPI	Range gate pull-in
RGPO	Range gate pull-off
RPI	Radar pulse interval
QAM	Quadrature Amplitude Modulation
SJ	Smart Jamming
SJR	Signal to Jamming Ratio
SNR	Signal to Noise Ratio
SPS	Symbols per Second
TDMA	Time Division Multiple Acces
TJ	Tone Jamming
VGPO	Velocity-gate pull-off

1. INTRODUCCIÓN

1.1 Contexto

Este proyecto se ha desarrollado en el departamento de Sistemas de Seguridad e Ingeniería de Sistemas (SSSE) del Instituto de Sistemas de Vuelo (IFT) del Centro Aeroespacial Alemán (DLR), concretamente en su sede en Braunschweig (Alemania). El proyecto se engloba dentro de una tesis doctoral que tiene como objetivo el diseño completo de un sistema de comunicaciones inalámbrico capaz de substituir a los actuales sistemas de control de vuelo cableados.

1.2 Estado del arte

Los sistemas de comunicaciones han estado tradicionalmente basados en cable, en este tipo de infraestructuras cada uno de los nodos participantes necesita estar conectado mediante cable con todos los nodos con los que se quiere comunicar (directamente o a través de otros nodos). Esta exigencia hace que el cableado necesario sea muy dependiente de la distancia entre los nodos y del número de estos. En entornos donde el acceso es difícil, el espacio para cableado es limitado o el peso máximo del dispositivo es bajo, los sistemas basados en cable presentan limitaciones que los sistemas inalámbricos solucionan.

En la actualidad se está tendiendo al uso de la tecnología inalámbrica como base para el desarrollo de tecnologías de comunicación. Entre las ventajas más significativas de los sistemas inalámbricos se puede destacar que no exigen un complicado despliegue, que dan una cobertura de zona global, que ofrecen libertad al receptor al no tener que estar conectado físicamente en todo momento, que

ahorran peso y espacio o que en caso de avería, ésta es más fácil de localizar y solucionar.

La aviación es un terreno donde las tecnologías inalámbricas no se habían abierto paso. Es ahora cuándo se están empezando a desarrollar sistemas inalámbricos destinados a este sector, principalmente sistemas destinados al usuario (pasajero) o a comunicaciones entre la tripulación.

El propósito de este proyecto es ir un paso más allá y confiar las comunicaciones críticas del avión (hasta ahora siempre realizadas por cable) a un sistema inalámbrico.

Entre estos sistemas críticos se encuentra el sistema de control de vuelo del avión. Este sistema es el que permite al piloto controlar las partes móviles del avión (turbinas, alerones, etc.), es decir, es el que controla el vuelo del avión. En la actualidad todos los sistemas de control de vuelo son cableados, lo que conlleva que una gran cantidad de cable, especialmente en los aviones grandes, desaparecería al cambiar a un sistema inalámbrico. Las ventajas de usar la tecnología inalámbrica se derivan no solo del hecho de evitar la fabricación e instalación del cable, también de que durante el diseño de la aeronave se prescinde del tiempo necesario para el cálculo de las rutas de cableado. El ahorro no se produce únicamente durante la fabricación. De igual manera, durante la vida útil del avión, tener un sistema inalámbrico trae consigo notables ventajas, como en las revisiones periódicas a las que se somete a un avión, especialmente durante el chequeo de mantenimiento exhaustivo (*heavy maintenance visit*), o en el ahorro en combustible derivado de no tener el peso de los cables.

Por otra parte, el hecho de que las comunicaciones sean críticas para la seguridad implica que los requerimientos por parte de las organizaciones de estandarización que validan los sistemas sean muy exigentes, ya que un fallo en el sistema podría suponer desembocar en un suceso catastrófico. Dichas exigencias presentan un reto a la hora de diseñar los sistemas inalámbricos.

1.3 Motivación

Dentro del ambicioso objetivo que es sustituir los actuales sistemas de control de vuelo basados en cable por sistemas inalámbricos, un paso significativo es crear un entorno de simulación en el que se puedan recrear las diferentes alternativas que se planteen para poder evaluarlas correctamente. A su vez, es conveniente elegir las opciones más apropiadas dentro del marco de las tecnologías inalámbricas y diseñar un sistema inicial desde el que trabajar. Es también una parte importante del

proyecto caracterizar los posibles ataques que nuestro sistema podría sufrir y que pondrían en peligro el funcionamiento y seguridad del avión.

Este proyecto proporcionará los primeros resultados acerca del comportamiento del sistema de control de vuelo inalámbrico en situación de funcionamiento normal y en entornos hostiles (ataques basado en jamming).

1.4 Objetivo y alcance del proyecto

Este proyecto fin de carrera tiene varias partes que confluyen en un objetivo final que consiste en la creación de un modelo en MATLAB/Simulink donde se pueda simular un sistema de control de vuelo inalámbrico, diferentes ataques electromagnéticos que se puedan perpetrar contra el sistema y las diferentes contramedidas para combatir dichos ataques.

Para lograr este objetivo se han seguido varias fases. La primera es la fase de documentación acerca de la guerra electrónica y sus formas (protección electrónica, soporte electrónico y ataque electrónico). La segunda es un estudio y documentación de las posibles alternativas existentes para la creación del sistema inalámbrico más apropiado (principalmente capa física). Dentro de esta parte se incluye también el diseño de un sistema de comunicaciones que pueda llegar a cumplir los requisitos y que sirva de punto de partida para sistemas posteriores. La tercera parte incluye la creación en MATLAB/Simulink de un modelo capaz de simular tanto el sistema diseñado, como diferentes ataques basados en jamming. La última fase es incluir en el modelo sistemas de protección contra ataques que simulen comportamientos basados en radios cognitivas con el objetivo de comprobar si son una vía de estudio válida para asegurar el cumplimiento de los requerimientos en todo momento. En la figura 1 se exponen las diferentes partes que componen el proyecto y como confluyen para dar el resultado final.

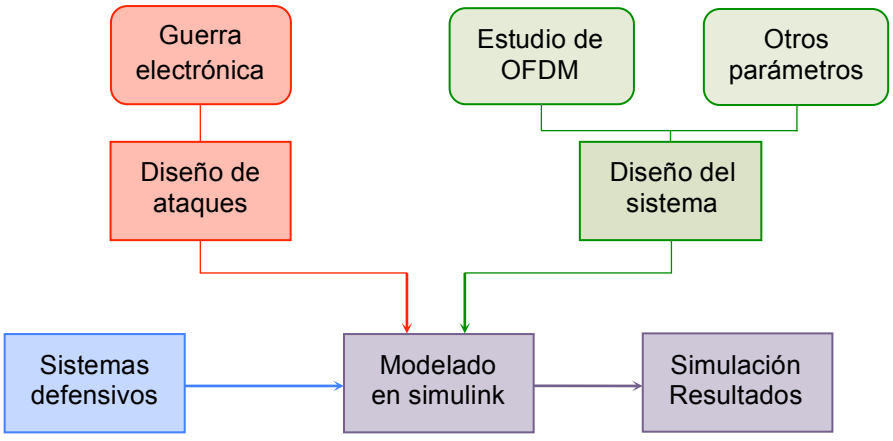


Figura 1: Partes en las que se divide el presente proyecto final de carrera

1.5 Organización

Esta memoria está organizada en 8 capítulos, de los cuales el primero es esta introducción, donde se presenta la motivación y objetivo del proyecto. Los capítulos 2 a 5 describen cada una de las partes de las que se compone el proyecto fin de carrera y los capítulos 6, 7 y 8 reflejan los resultados obtenidos, así como las conclusiones y posibles mejoras para futuras implementaciones.

- **Capítulo 2 Guerra electrónica:** esta sección contiene uno de los objetivos del proyecto, consistente en estudiar, documentar y clasificar las posibles amenazas en forma de ataque electromagnético premeditado que puede sufrir un sistema inalámbrico. Para ello en este capítulo se describe en que consiste el termino “Guerra electrónica”, qué engloba y cómo esta subdividido, dando especial énfasis a la parte de ataque electrónico. Igualmente, se describen los tipos de ataques que puede sufrir un sistema de comunicaciones inalámbrico.

- **Capítulo 3 Situación de partida y requerimientos:** este apartado incluye la relación de elementos dentro del sistema de control de vuelo inalámbrico que estaban diseñados al inicio de este proyecto, las hipótesis que se tomaron al inicio, así como los requisitos que deberá satisfacer el sistema una vez finalizado.

- **Capítulo 4 Diseño:** este capítulo define el proceso para alcanzar otro de los objetivos del proyecto: diseñar un sistema completo de comunicaciones para un sistema de control de vuelo inalámbrico. Aquí se exponen las tecnologías elegidas para las opciones de diseño y se incluyen también las medidas que se han diseñado para combatir posibles ataques intencionados, así como entornos no propicios para las comunicaciones inalámbricas.

- **Capítulo 5 Modelado:** En esta sección se describen las partes del modelo creado en simulink así como las operaciones llevadas a cabo para validarlo.

- **Capítulo 6 Resultados:** En este capítulo se explican las principales simulaciones que se han llevado a cabo y se analizan los correspondientes resultados.

- **Capítulo 7 Conclusiones y posibles mejoras:** Este apartado contiene las conclusiones extraídas de los resultados obtenidos y las posibles mejoras a tener en cuenta en futuras versiones del sistema para mejorar su rendimiento.

Para conconcluir se encuentran los anexos, donde se incluye información más detallada y/o adicional de alguno de los apartados incluidos en la memoria principal

y que no contienen una información imprescindible para entender el proyecto ni los resultados obtenidos. Esto anexos son fragmentos o resumenes de entregables que se han desarrollado durante la realización del proyecto y se encuentran escritos en inglés (a excepción del anexo F).

- **Anexo A Electronic support, electronic protect and radar jamming:** En este anexo se expanden los conceptos relacionados con la guerra electrónica.

- **Anexo B Flight control systems:** Este apartado proporciona una breve introducción a los sistemas de control de vuelo, se describen sus partes y sus funciones.

- **Anexo C Attack scenarios and defenses:** El anexo C proporciona una visión global acerca de los posibles ataques electromagnéticos que puede sufrir un sistema de control de vuelo inalámbrico. También se describen los dispositivos capaces de realizar ataques basados en jamming (jammers) y las suposiciones que se han tomado en este proyecto a la hora de generar el jamming.

- **Anexo D Frequency allocation:** Este anexo sugiere unos rangos de frecuencias en los que se podría encuadrar el sistema diseñado.

- **Anexo E Simulink models:** En este apartado se describen en detalle los modelos creados en simulink, es un complemento al capítulo 5 de la memoria.

- **Anexo F Evolución temporal:** El anexo F muestra la descripción del proyecto a lo largo del tiempo, los pasos que se fueron dando y el tiempo que se invirtió en cada uno de ellos.

1.6 Herramientas

La parte de programación realizada en este proyecto se ha llevado a cabo usando el programa MATLAB/Simulink the Mathworks, en concreto se han usado las librerías básicas de simulink y las toolboxes de *Communications system* y *DSP system*.

2. GUERRA ELECTRÓNICA

La guerra electrónica es toda una nueva sección dentro de la estrategia militar que va cobrando importancia conforme las comunicaciones se convierten una parte más crítica en la guerra. Oficialmente la OTAN define el término guerra electrónica como:

"Acciones militares para explotar el espectro electromagnético comprendiendo: la intención de interceptar e identificar emisiones electromagnéticas, el uso de energía electromagnética, incluyendo energía dirigida a reducir o prevenir el uso hostil del espectro electromagnético y acciones para asegurar su uso por parte de fuerzas aliadas" [1]

Actualmente la guerra electrónica comprende tres componentes diferenciados: soporte electrónico (*electronic support ES*), protección electrónica (*electronic protect EP*) y ataque electrónico (*electronic attack EA*).

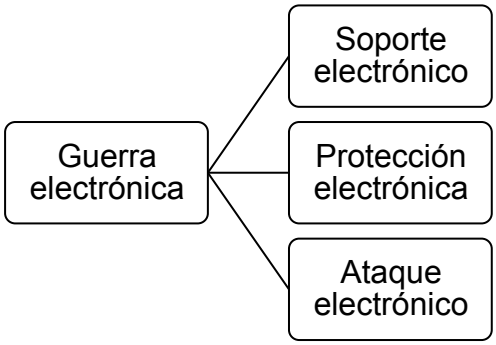


Figura 2: Componentes de la guerra electrónica

Aunque el estudio de la guerra de electrónica forma una parte importante de este proyecto, esta sección se centra únicamente en la sección de Ataque Electrónico. Los apartados de Soporte Electrónico y Protección Electrónica son descritos en el Anexo A.

2.1 Ataque electrónico

El ataque electrónico abarca todas las acciones cuyo objetivo es impedir que el enemigo haga un uso eficiente del espectro electromagnético. Dichas acciones se pueden clasificar en tres grupos en función del ataque que perpetran: energía dirigida, jamming de engaño y jamming de cobertura.

- **Energía dirigida (*directed energy*):** los ataques basados en energía dirigida consisten en la radiación de un pulso electromagnético tan grande que dañe los sistemas enemigos de manera permanente. Cabe destacar que esta técnica requiere ingentes cantidades de energía y que la mayoría de los dispositivos electrónicos se encuentran protegidos contra picos de entrada, protección que funcionaría igualmente contra este tipo de ataques.

- **Engaño (*deception*):** también llamado jamming de engaño (*deception jamming*) o jamming inteligente (*smart jamming* SJ), no tiene como objetivo destruir o dificultar las comunicaciones enemigas, sino engañar a los enemigos. El objetivo de esta técnica es minar la confianza del enemigo en sus propias transmisiones mediante engaños. El jamming de engaño tiene muchas formas, no existe un tipo de ataque general, sino que depende del sistema víctima. Es principalmente usado en ataques contra sistemas radar.

- **Jamming de cobertura (*cover jamming*):** el jamming de cobertura (en ocasiones llamado jamming de comunicaciones (*communication jamming*) consiste en aumentar el ruido en el receptor enemigo de manera que el ratio de señal-ruido (SNR) disminuya, dificulte o impida las comunicaciones. Estos objetivos se consiguen radiando energía directamente hacia el receptor objetivo.

El siguiente apartado de este capítulo explica los diferentes tipos de jamming que incluye cada uno de los grupos anteriormente mencionados.

2.2 Jamming

El jamming es un ataque que se realiza mediante la emisión de energía electromagnética al receptor víctima. La OTAN define el jamming como:

"La emisión, re-emisión o reflexión deliberada de energía electromagnética con el objetivo de perjudicar la efectividad de los dispositivos electrónicos, equipos o sistemas enemigos." [1]

Para el estudio del jamming podemos primero clasificarlo en dos grupos principales en función de las víctimas a las que va dirigido: jamming para comunicaciones y jamming para sistemas radar. Dado que el proyecto tiene como objetivo diseñar un sistema de comunicaciones esta sección se centra en el estudio del primer grupo mientras que el segundo grupo se desarrolla en el anexo A.

El jamming para comunicaciones es en ocasiones llamado jamming de cobertura, ya que la mayoría de sus variantes se engloban en ese grupo de ataques. Los ataques aquí presentados engloban aquellos que puede sufrir cualquier sistema de comunicaciones. La división realizada depende de cómo se distribuye la energía a lo largo del espectro y cómo lo hace en el espectro y en el tiempo. En la figura 3 puede observarse una aclaración de esta división con un ejemplo de jamming de banda ancha pulsado.

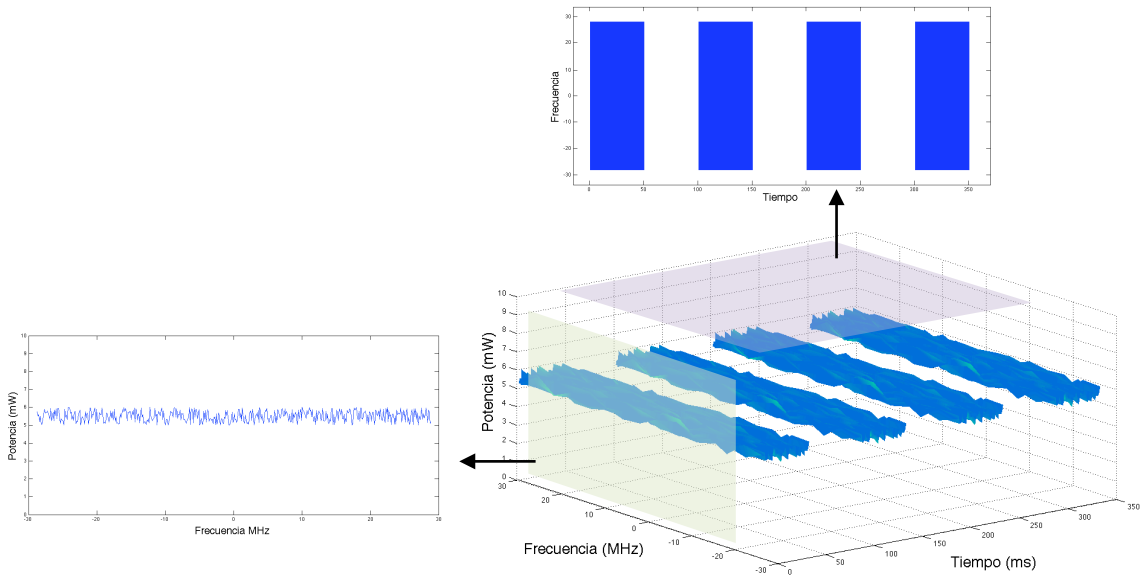


Figura 3: Esquema de la división en potencia-frecuencia y frecuencia-tiempo. La figura extraida en la izq. representa la distribución en potencia y espectro, mientras que la extraída de la parte superior representa el funcionamiento del jamming en la frecuencia y en el tiempo.

Hay que tener en cuenta que en muchas ocasiones el atacante desconoce parámetros del sistema victima, como por ejemplo la frecuencia central de emisión (puede conocer la banda de emisión), el periodo con el que transmite (es decir,

cuándo la comunicación víctima está activa y cuando no), etc. De averiguar estos datos se encargan los sistemas de soporte electrónico, pero por norma general y debido a las medidas de protección electrónica no se pueden averiguar con toda la precisión que el atacante desearía. Es por esto que el atacante tiene que hacer un uso inteligente de su energía disponible y distribuirla de la manera que él crea que puede causar el mayor daño.

2.2.1 Distribución de la energía en el espectro

Este primer grupo engloba las diferentes maneras que el atacante tiene de distribuir la energía de la que dispone en función de la sección del espectro electromagnético que quiere atacar.

- **Noise jamming**
  En el noise jamming, la portadora es modulada por una señal que es un ruido aleatorio (en general suele usarse ruido blanco gaussiano), dicha portadora se emite directamente hacia el receptor víctima. Dependiendo de cuán grande sea el espectro que cubre el jamming se distinguen tres categorías.

  El **jamming de banda ancha** (*full band jamming* o *broadband jamming* BBJ) ataca un gran ancho de banda. Generalmente se denomina jamming de banda ancha a aquel jamming que cubre toda la posible banda de transmisión de la señal atacada. La evolución del jamming de banda ancha es el **jamming de banda parcial** (*partial band jamming*), este jamming tiene las mismas propiedades que el jamming de banda ancha, la diferencia reside en que ahora la banda cubierta es mucho menor. Se denomina jamming de banda parcial a aquel jamming que sólo cubre una parte del espectro usado por la víctima. El tercer miembro dentro del grupo de los noise jamming es el **jamming de banda estrecha** (*narrow band jamming* NBJ), este tipo de ataques posee las mismas características que los dos anteriores pero el espectro atacado es muy estrecho en comparación con el espectro total usado por la víctima.

- **Tone jamming**
  Si disminuimos más el espectro atacado por el jammer de banda estrecha llegamos al tone jamming. Este tipo de ataques coloca uno (*single tone jamming* TJ) o varios tonos (*multitone jamming* MTJ) estratégicamente en el espectro como forma de ataque. En este tipo de ataques el trabajo realizado por el soporte electrónico es muy importante, dado que la efectividad del jamming depende altamente de la posición del/de los tonos.

2.2.2 Distribución de la energía en el espectro y en el tiempo

Además de distribuir la energía a lo largo del espectro es necesario determinar como se distribuyen los posibles ataques durante el tiempo. En este apartado se habla de tres tipos de ataques diferentes.

- **Jamming de barrido.**
  En este tipo de ataques el ancho de banda cubierto es variable con el tiempo. En el jamming de barrido (*swept jamming*) el jammer se va desplazando entre las bandas de interés.

- **Jamming pulsado**
  El jamming pulsado (*pulse jamming*) es el concepto de jamming intermitente. Independientemente de como sea el espectro del jamming un ataque pulsado es aquel que no está activo continuamente. Las estadísiticas muestran que para una cantidad fija de energía disponible un jamming pulsado es igual más dañino que el mismo ataque aplicado sin intermitencia [2].

- **Jamming de seguimiento**
  El jamming de seguimiento (*follower jamming*) es aquel que, en caso de que la víctima cambie la frecuencia su frecuencia central de transmisión, es capaz de detectar este salto y seguirlo, continuando así el ataque.

El jamming de seguimiento cierra el grupo de jammings de comunicación pertenecientes al grupo de jammings de cobertura. Los siguientes ataques aquí descritos corresponden al grupo de jamming inteligente o jamming de engaño.

- **Jamming inteligente**
  El jamming inteligente en comunicaciones puede tomar muchas formas y es altamente dependiente del tipo de sistema que se quiera atacar. Atacar los puntos débiles de la vícitama significa en muchos casos que si el ataque es exitoso elimina toda posibilidad de comunicación, a cambio, los conocimientos que el atacante debe poseer del sistema atacado han de ser muy precisos.

  Aunque el jamming inteligente también es denominado jamming de engaño, en realidad, éste es sólo un subgrupo del jamming inteligente, dentro del cual se pueden diferenciar dos conjuntos. El primero englobaría a los jammings de engaño. Estos ataques son principalmente usados contra sistemas de radar y consisten en enviar ordenes falsas y jugar con las señales pero sin bloquear las comunicaciones. El segundo subgrupo va un paso más allá, el llamado jamming brillante (*brilliant jamming*) consiste en copiar y sustituir una de las fuentes de información enemigas por una aliada, de manera que las fuerzas aliadas puedan introducir la información que ellos desean en el sistema enemigo si ser descubiertos. Esta técnica incluye modificar información

original (como coordenadas de posición) o crear nueva información. Con las técnicas de protección electrónica (como la encriptación) que existen en la actualidad alcanzar el éxito con una técnica de este estilo es altamente complicado.

Con el jamming inteligente finaliza la descripción de los diferentes ataques que puede sufrir un sistema de comunicaciones. En la figura 4 se puede observar un resumen de los diferentes tipos de cover jamming, así como una representación de la distribución en el espectro (caso de noise jamming y tone jamming) o de la distribución en frecuencia y en tiempo (jamming de barrido, jamming pulsado y jamming de seguimiento).

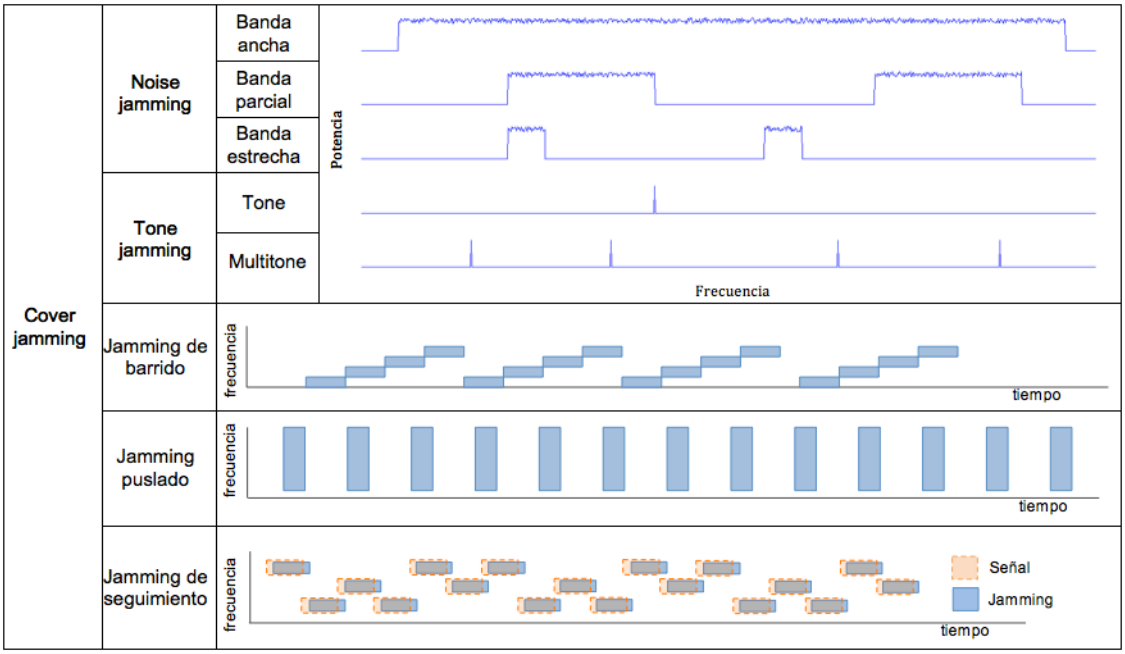


Figura 4: Relación de los diferentes tipos de cover jamming y su distribución en tiempo y frecuencia

3. SITUACIÓN DE PARTIDA Y REQUERIMIENTOS

El presente proyecto se engloba dentro de otro proyecto más ambicioso que consiste en el diseño completo de un sistema de control de vuelo inalámbrico capaz de sustituir a los actuales sistemas cableados, por tanto, al inicio de este proyecto final de carrera existían ciertas necesidades y restricciones que ya habían sido establecidas (tanto por el propio proyecto como por la normativa vigente que regula este tipo de sistemas). Al mismo tiempo también se establecieron puntos de partida y se aceptaron ciertas hipótesis. Todos estos puntos e hipótesis se recogen en este apartado de situación de partida y requerimientos.

3.1 Situación de partida

Los sistemas de control de vuelo tienen como objetivo, no sólo controlar las partes móviles del avión, sino además monitorizar el estado de dichas partes. En esta sección se presenta la posición de los nodos que conformarán la topología de la red inalámbrica. Una introducción a los sistemas de control de vuelo se puede encontrar en el anexo B.

La figura 5 representa la posición de los nodos que controlan las partes móviles en el sistema de control de vuelo inalámbrico. Son 43 nodos, de los cuales 24 controlan las partes de control de vuelo primario y 19 las partes de control de vuelo secundario. Cada nodo está conectado a un actuador que transmite 224 bits por mensaje y transmite 1 mensaje cada milisegundo [3].

La topología de la red estaba al inicio de este proyecto sin definir y para este proyecto se decidió usar una topología en estrella. La razón por la que se eligió una topología en estrella como punto de partida es que los sistemas de control de vuelo

cableados se basan en ella. En el caso que nos ocupa cada nodo se comunicará con el nodo central, el cual simboliza el ordenador de a bordo y está situado debajo de la cabina del piloto.

Otra de las hipótesis que se asumió es que las antenas de los nodos son omnidireccionales. El motivo de esta suposición es que se ha intentado modelar y simular el sistema en el peor caso posible, de esta manera el sistema recibe todas las interferencias existentes, tanto ambientales como artificiales. Al mismo tiempo se asume que las antenas y los receptores están adaptados a las frecuencias de trabajo, así se descarta el ruido fuera de la banda de transmisión.

3.2 Requerimientos

Este apartado recoge las especificaciones marcadas por las normativas vigentes que el sistema debe cumplir una vez terminado, así como las especificaciones autoimpuestas y que marcan el diseño del sistema.

En los siguientes puntos se recogen todos los requerimientos que se le exigirán al sistema final y que por tanto se tienen en cuenta a la hora del diseño.

- Bit error rate (BER) menor de 10^{-6}. El sistema final deberá asegurar este requerimiento en todo momento [4].

- Baja potencia. La potencia de emisión del sistema está todavía por determinar, pero se busca que sea un sistema que funcione con la mínima potencia posible (menor de 1 W)

- Alcance 100 metros. Se buscará un sistema que sea capaz comunicar nodos que se encuentren hasta una distancia máxima de 100 metros .

- El sistema debe ser capaz de transmitir la información de todos los actuadores (224 bits cada milisegundo) en todo momento y sin retrasos.

Estos requerimientos vienen en parte marcados por las sociedades de certificación que darían validez al sistema una vez finalizado. En este apartado se recogen sólo los requerimientos que afectan al presente proyecto, a la hora de la validación las sociedades de certificación exigen una gran cantidad de pruebas que abarcan muchos mas campos.

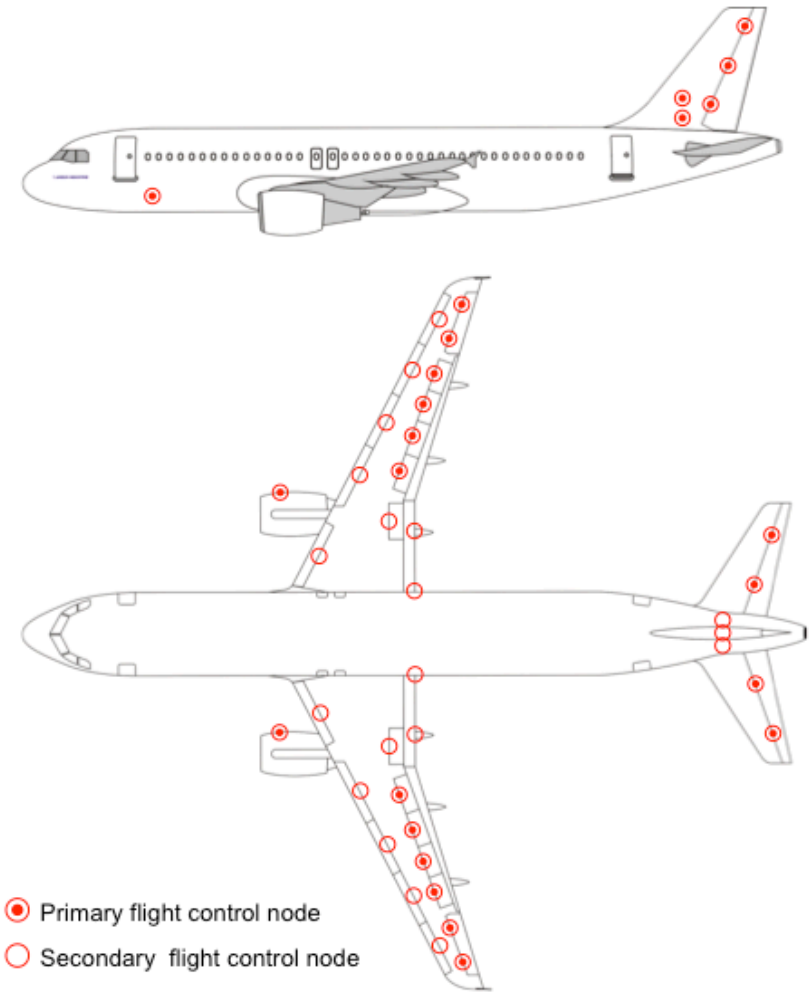


Figura 5: Posición de los nodos en el avión. Para este ejemplo se ha tomado un avión Airbus A320.

4. DISEÑO

Vistos los requerimientos en el apartado anterior, en este capítulo se van a explicar las diferentes partes de las que se compone el sistema creado en el presente proyecto final de carrera.

En la figura 6 se puede observar el diagrama de bloques de un enlace basado en OFDM. Para este proyecto se han diseñado todos los bloques representados en dicha figura y en este capítulo se procederá a explicar cada uno de ellos.

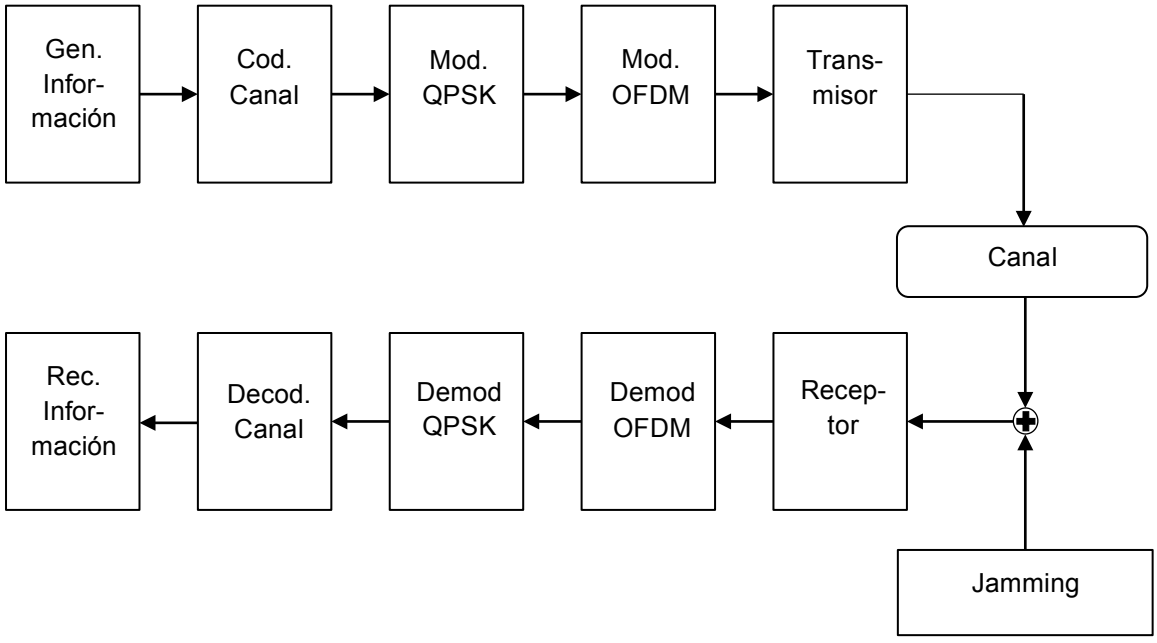


Figura 6: Diagrama de un enlace de comunicaciones como el diseñado en este proyecto

4.1 Throughput

El diseño de un sistema de comunicaciones es altamente dependiente de la cantidad de información por unidad de tiempo que se necesite transmitir (bits por segundo). Para el cálculo de este parámetro se parte de la necesidad de transmitir 224 bits por mensaje. Tener una topología en estrella obliga a transmitir con cada mensaje una cabecera, la cual no ha sido todavía determinada. Como algo orientativo se ha tomado como un tamaño de cabecera válido, el tamaño de las cabeceras que se han diseñado para sistemas críticos en seguridad aplicados a sistemas ferroviarios [5]. Por tanto, para este proyecto se asume una cabecera de 32 bytes por mensaje, lo que hacen 480 bits por mensaje transmitido. Si cada uno de los 43 nodos transmite un mensaje cada milisegundo la cantidad de información que debe soportar el sistema será de 20.64 Mbps.

4.2 Modulación digital

Un paso importante en el diseño es la elección de la codificación digital a utilizar. En un enlace, existe siempre un compromiso entre la cantidad de información que se transmite por unidad de tiempo, el ancho de banda necesario y la potencia necesaria y es labor del diseñador asignar valores a estos parámetros de manera que se cumplan los objetivos y las especificaciones deseadas de la manera más eficiente.

En general, en el diseño de un sistema de comunicaciones uno de esos parámetros será el factor limitante del sistema (máxima potencia disponible, ancho de banda máximo permitido o un data rate mínimo) y las técnicas de codificación permiten al diseñador jugar con los otros dos parámetros restantes para poder alcanzar los objetivos fijados.

En enlaces OFDM las codificaciones usadas son la modulación en fase (*phase shift keying* PSK) y la modulación en amplitud y cuadratura (*quadrature amplitude modulation* QAM). En el caso de este proyecto el factor más limitante es la potencia disponible (ya que uno de los requisitos era usar un sistema que usara una potencia muy baja), por tanto se escogió un orden de modulación (M) pequeño para poder llegar a alcanzar valores de bit error rate bajos aún cuando el ratio de señal a ruido no fuera elevado. Las modulaciones PSK y QAM son iguales para un orden bajo (M=2, 4) , y además está demostrado que el BER de la modulación de orden 2 (BPSK) y la de orden 4 (QPSK) es el mismo. Por tanto, finalmente se eligió una codificación QPSK. Las comprobacionas y demostraciones referentes a estas afirmaciones, así como la teoría referente a la modulación en fase quedan fuera de los objetivos de este proyecto, para ello puede consultarse [6].

4.3 Técnicas de acceso al medio

Dado que en el sistema existen 43 usuarios que comparten los mismos recursos se hace necesario el uso de una técnica de acceso al medio. Las posibles técnicas que se barajaron fueron TMDA (*time division multiple access*), FDMA (*frequency division multiple Access*) y CDMA (*code division multiple access*).

De entre estas técnicas CDMA fue descartada por dos razones. La primera fue que el hecho de que todos los usuarios transmitan al mismo tiempo se traduce en un empobrecimiento de la señal a ruido, puesto que para un usuario concreto todos los demás usuarios son ruido. Este problema se acentúa en el caso de sistemas de baja potencia y donde todos los enlaces tienen un nodo común. La segunda razón es a la hora de la sincronización, que haya que remodular una comunicación (ya de por sí generalmente de alta velocidad) con un código hace que los tiempos de símbolos (llamados tiempos de chip) sean muy pequeños y por tanto parámetros como el sincronismo de trama, o de símbolo sean complicados de adquirir.

La elección entre TMDA y FDMA se decanta a favor del primero por varias razones. La primera es por la naturaleza de la transmisión. Como se ha comentado en el capítulo 3 la información que generan los actuadores es un mensaje de 224 bits cada milisegundo, el uso de FDMA implica reservar un tiempo para que los usuarios transmitan, aunque no tengan nada que transmitir. En TDMA en cambio cada nodo tiene una ventana (*slot*) de transmisión asignada, de manera que, cuando a un nodo le llega su slot ya ha tenido tiempo de generar la información que necesita transmitir. La segunda (y principal) razón por la cual se escoge TDMA sobre FDMA es que está demostrado en la bibliografía que TDMA permite transmitir más información que FDMA en un tiempo y un ancho de banda fijados [6].

En este proyecto se decidió usar una multiplexación en tiempo (TDMA). Se ha elegido una trama TDMA de duración 1 ms, la cual está dividida en 43 ventanas (*slots*) de duración 23.25 μs cada una.

4.4 Técnicas de corrección de errores

Los códigos de protección contra errores conforman en todos los sistemas de comunicaciones una parte importante del diseño. La elección del código más adecuado no es trivial y conlleva un estudio de todos las posibles técnicas y de sus efectos en el sistema. Los beneficios que cada código aporta dependen también de cómo tienen lugar los errores durante la transmisión y la naturaleza de estos (ráfagas, uniformemente distribuidos, etc.). Esta información es todavía desconocida para el caso de un enlace fijo en un avión.

Durante la realización de este proyecto no ha habido el tiempo necesario para realizar un estudio correcto de todas las posibles opciones. Sin embargo, sí se ha querido implementar algún tipo de sistema de corrección de errores con el fin de crear un modelo que contenga todos los componentes finales del diseño.

Para ello se ha tomado como referencia la técnica de corrección de errores implementada en el estándar 802.11a. El cual es similar a este proyecto [7].

La codificación de canal usada en este diseño se compone por un código convolucional reducido (*punctured convolutional code*) de ratio ¾ seguido de un entrelazado aleatorio. El código convolucional reducido se construye a partir de un código convolucional de ratio ½ compuesto por un registro de dimensión 7 y ecuaciones de conexión g_1 y g_2:

$$\begin{aligned} g_1 &= 1011011 \\ g_2 &= 1111001 \end{aligned} \tag{1}$$

Para conseguir el ratio ¾ deseado se ha reducido con el siguiente esquema: 111001. Lo que representa que de cada 6 bits generados se descartan el 4 y el 5.

4.5 Sistemas de mejora

En este apartado se van a explicar los añadidos que se han hecho al sistema de comunicaciones básico con el fin de combatir el jamming y de mejorar el BER en entornos desfavorables (entornos con muchas interferencias, fading, etc.). Se han seleccionado tres maneras de abordar estas mejoras: radios cognitivas, redundancia en frecuencia y redundancia en tiempo y datos.

4.5.1 Radios cognitivas

Las radios cognitivas son una evolución de las radios definidas por software (*software defined radio* SDR). Las SDR son transmisores cuyos parámetros de emisión (potencia, codificación, frecuencia central, etc.) son configurables por software lo que permite adaptar la transmisión a entornos cambiantes, la limitación de estas radios es que dichos parámetros son configurables únicamente bajo demanda.

La innovación que aportan las radios cognitivas (*cognitive radios* CR) frente a las SDR es que son capaces de tomar decisiones por ellas mismas y modificar los parámetros de transmisión según convenga. Las radios cognitivas son capaces de observar y aprender del entorno, de reconocer patrones y ofrecer la mejor respuesta frente una situación nueva.

De esta manera un sistema basado en radios cognitivas es capaz de detectar cuándo el SNR del enlace disminuye y actuar en consecuencia (aumentando la potencia de transmisión, cambiando la frecuencia de transmisión, disminuyendo el orden de la modulación, etc.). En este proyecto lo que se quiere comprobar si las técnicas de defensa basadas en radios cognitivas son una solución viable como defensa contra el jamming y contra otros problemas que puedan surgir en el enlace, y por tanto merece la pena su estudio e implementación.

En este proyecto se van a emular ciertos comportamientos que pueden aportar las radios cognitivas, estos son: detección de jamming y evasión de jamming.

4.5.1.1 Detección de jamming

La detección de jamming tiene como objetivo detectar cuándo el sistema está siendo víctima de un ataque o de algún tipo de interferencia en la banda de transmisión. El reto de esta mejora es diferenciar cuándo la caída de la SNR es debida a un jamming y cuándo es debida al canal.

La detección de jamming se va a realizar mediante la comparación de dos estimaciones diferentes de la SNR en el receptor, el esquema puede observarse en la figura 7.

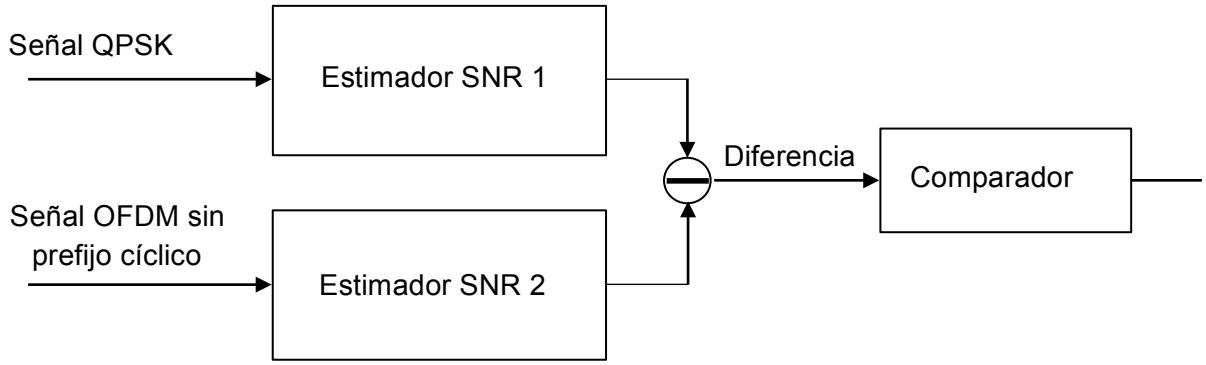


Figura 7: Esquema del sistema de detección de jamming situado en el receptor.

El primer estimador (estimador de SNR 1) consiste en tras el demodulador OFDM, demodular la señal QPSK recibida y posteriormente re-modularla (figura 8). Después se resta la señal re-modulada (que está limpia de ruido) de la señal recibida obteniendo así una estimación del ruido.

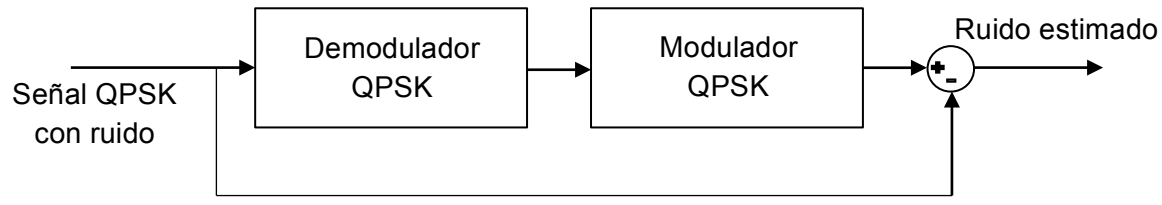
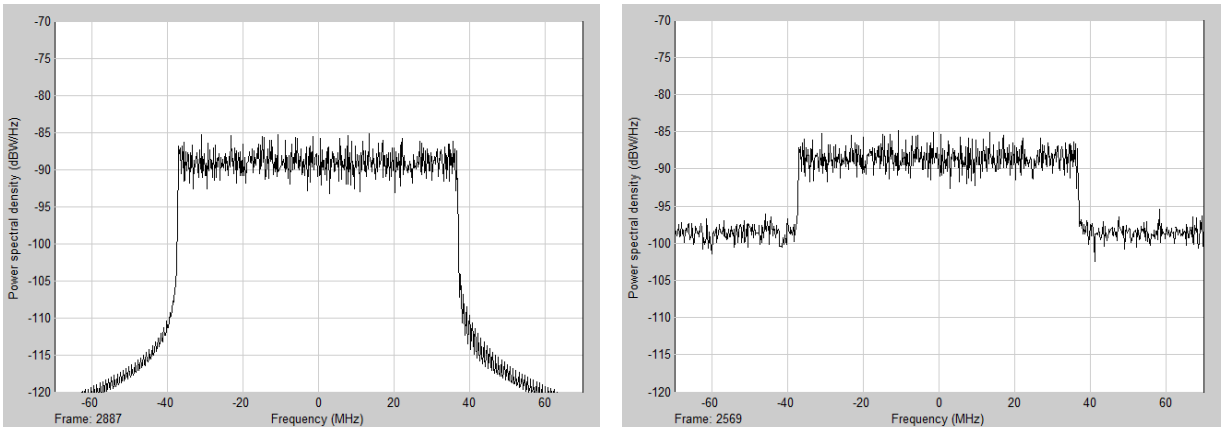


Figura 8: Esquema del estimador de SNR 1

Este sistema asume que la gran mayoría de los símbolos recibidos son estimados correctamente, lo cual no se cumple para SNR muy bajas, por tanto (y como se comprobará más adelante) se puede suponer que este estimador deja de ser fiable para E_b/N_0 bajas.

El segundo estimador (estimador de SNR 2) aprovecha el hecho de que en la generación de la señal OFDM se use el zero padding. Como se ha comentado, el zero padding consiste en rellenar con ceros los subsímbolos necesarios para alcanzar un numero que sea potencia de dos, por esta razón existen un espacio adyacente a la señal OFDM dónde se transmiten las subportadoras moduladas por los símbolos pertenecientes al zero padding (figura 9). Dado que los símbolos del zero padding son cero no se transmite nada en ese espacio y por tanto toda la potencia que se reciba en esa banda en el receptor pertenece al ruido.

Si consideramos que toda la potencia que se transmite en la banda de transmisión es debida a la señal y que toda la banda que se transmite en la banda de zero padding es debida al ruido podemos hacer una estimación de la señal a ruido de manera muy sencilla (tal y como se describe en [8])



a) Densidad espectral de potencia de la señal transmitida libre de ruido

b) Densidad espectral de potencia de la señal recibida

Figura 9: Densidades espectrales de potencia de la señal OFDM en transmisión y en recepción.

Tal y como se expone en el artículo relacionado el estimador de SNR se basa en el cálculo de la siguiente ecuación:

$$SNR_{est} = \frac{\sum_{j\in J}\sum_{k\in K}|Y(j,k)|^2}{\sum_{j\in J}\sum_{q\in Q}|Y(j,q)|^2}\eta - 1 \qquad \eta = \frac{||Q||}{||K||} \qquad (2)$$

Donde *Y* es la transformada de Fourier de la señal OFDM sin el prefijo cíclico. J

es el intervalo de estimación, K el conjunto de subportadoras de interés y Q el conjunto de subportadoras moduladas por el zero-padding. La operación ||·|| simboliza el número total de subportadoras del respectivo conjunto.

La desventaja que presenta este estimador es que si por alguna razón existiera una potencia en la banda de transmisión que no perteneciera a la señal (como por ejemplo un jamming), dicha potencia sería considerada como potencia de la señal y la señal a ruido aumentaría en vez de disminuir. Esta característica es la que se va a aprovechar para detectar el jamming.

Hay que destacar que este sistema no detectaría un ataque cuyo ancho de banda ocupara todo el ancho de banda de la señal OFDM y además la banda del zero padding, puesto que en ese caso el SNR estimado disminuiría como si de ruido AWGN normal se tratara.

La detección de jamming se va a basar en la característica del estimador 2, por la que la SNR estimada aumenta cuándo existe un jamming en la banda de transmisión, mientras que en el estimador 1 la SNR disminuye. De esta manera ante la presencia de un jamming en la banda OFDM existe una diferencia entre ambas estimaciones que marca la existencia de un ataque. En la figura 10 puede observarse un ejemplo del principio en el que se basa funcionamiento de la detección.

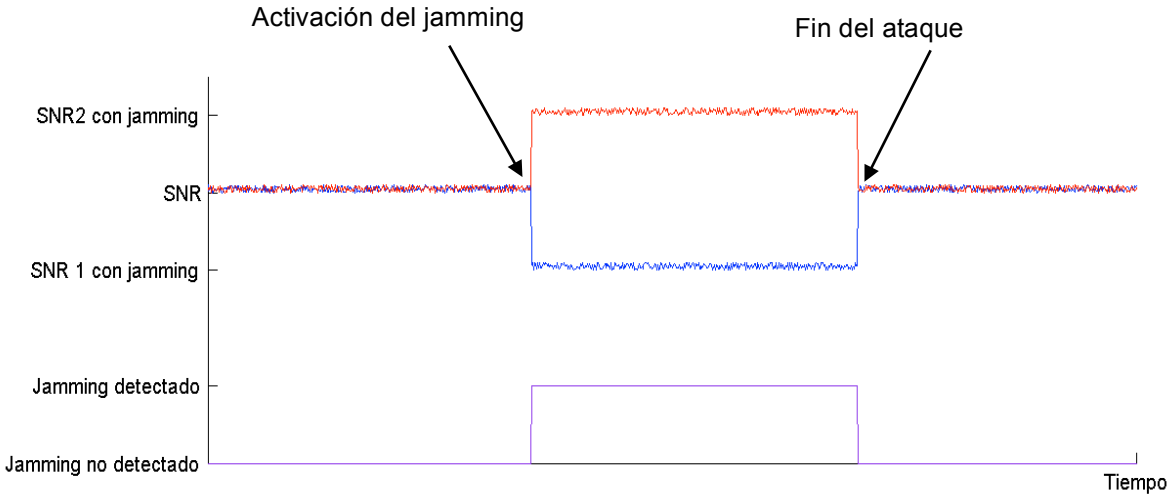


Figura 10: Descripción del funcionamiento del detector de jamming

4.5.1.2 Evasión de jamming

Tras la detección de jamming la siguiente operación que realizan las radios cognitivas es combatir dicho ataque. Dado que el sistema trabajará con potencias muy bajas (probablemente menos de 1 W) y encontrar un jammer que sea capaz de realizar su función con más de 1 W es relativamente sencillo (tal y como se describe en el capítulo 2) la defensa más efectiva contra este tipo de ataques es la evasión.

La evasión de jamming consiste en, una vez detectado el jamming, aplicar algún sistema para evadirlo. Esta tarea la realizarían las radios cognitivas y consistiría en un cambio de la frecuencia de transmisión a otra frecuencia seleccionada de manera aleatoria donde el jammer no este activo. Si el jammer es dinámico y puede localizar la nueva frecuencia de trabajo y reengancharse, el sistema se volvería a activar tras volver a detectar el jamming y saltaría de nuevo a otra frecuencia.

Un ejemplo puede verse en la figura 11, una vez el jamming es detectado, la frecuencia de central de transmisión se cambia y el jammer tarda un tiempo en volver a localizar la nueva frecuencia. En un sistema con radios cognitivas este proceso puede mejorarse, de manera que si el sistema detecta que el jammer tarda *t* segundos en detectar la nueva frecuencia, las radios cognitivas pueden anticiparse al jammer y trasladar la banda de transmisión antes de que la comunicación se vea afectada.

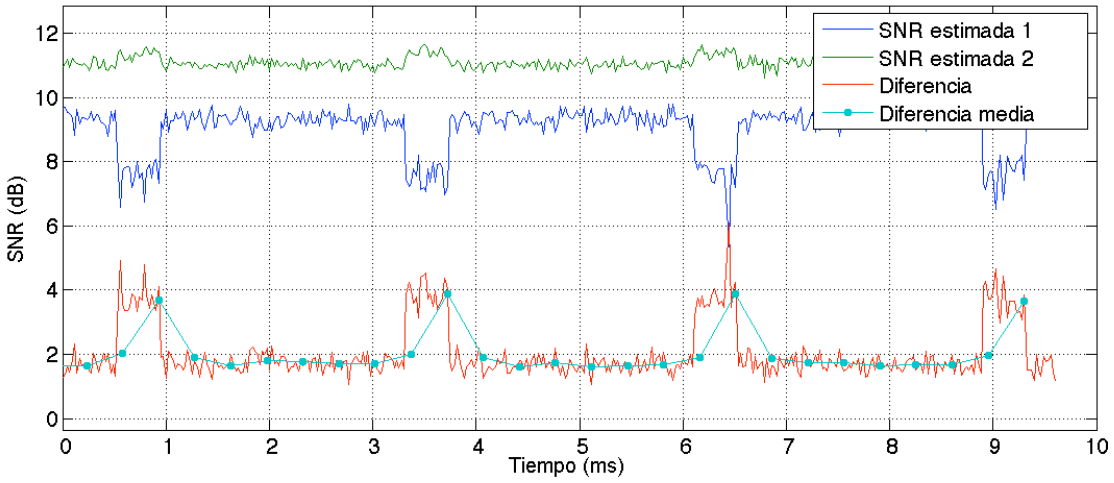


Figura 11: Sistema de evasión de jamming en funcionamiento. Se observa cuándo el ataque comienza al aumentar la diferencia

4.5.2 Redundancia frecuencial

En adición a las técnicas presentadas en el apartado anterior el sistema implementará una redundancia en frecuencia, esto es, la información se transmite en paralelo a través de dos frecuencias diferentes, las cuales están lo suficientemente separadas entre si como para poder considerar los efectos del canal independientes.

Existen varios motivos por los que se ha decidido implementar esta redundancia en frecuencia. Uno es que diseñar un sistema con frecuencias muy diferentes implica que en caso de tener un canal variable con el tiempo, los efectos de éste no serían iguales en ambas frecuencias (especialmente interesante en el caso de los fadings). Igualmente, el uso de la doble frecuencia añade un nivel de protección

adicional frente al jamming. De esta manera se obliga al jammer a atacar dos frecuencias diferentes ambas protegidas con sistemas de defensa basados en radios cognitivas.

La mejora de la doble frecuencia se consigue en el receptor gracias a los estimadores de SNR1, en este modelo se seleccionará la frecuencia que no esté siendo víctima de un ataque por considerar la frecuencia atacada como no fiable por no poderse detectar el tipo de ataque. En caso de que ambas se encuentre en la misma situación (ambas jammeadas o ambas libres de ataques) se seleccionará aquella con mejor SNR estimado. En la tabla 1 se puede observar la tabla de decisión entre las frecuencias.

$SNR_{f1} > SNR_{f2}$				$SNR_{f1} < SNR_{f2}$			
$Jamming_{f1}$ = ON		$Jamming_{f1}$ = OFF		$Jamming_{f1}$ = ON		$Jamming_{f1}$ = OFF	
J_{f2}=ON	J_{f2}=OFF	J_{f2}=ON	J_{f2}=OFF	J_{f2}=ON	J_{f2}=OFF	J_{f2}=ON	J_{f2}=OFF
Frec. 1	Frec. 2	Frec. 1	Frec. 1	Frec. 2	Frec. 2	Frec. 1	Frec. 2

Tabla 1: Tabla de decisión en el sistema de redundancia frecuencial

4.5.3 Redundancia en tiempo y datos

La última mejora a implementar en el sistema es una redundancia en datos y tiempo. Consiste en repetir el mensaje original 3 veces. Esta repetición se realiza a nivel de mensaje y se aplica posteriormente al código convolucional y antes del entrelazado. A todos los efectos, este tipo de defensa se comporta como un código de repetición de ratio 1/3.

Con esta última mejora se cierra la sección de mejoras del sistema, aun así, como protección se ha diseñado un protocolo de acción para situaciones hostiles o desfavorables que deberá ser implementado más adelante en las radios cognitivas. Dicho protocolo puede consultarse en el anexo C.

4.6 OFDM

La elección de la modulación a utilizar se basó en diferentes factores. Un factor fue la cantidad de información a transmitir. Como se ha visto en el apartado 4.1, hay que transmitir un mínimo de 20.64 Mbps (cifra que aumenta una vez se incluya la codificación de canal). Otro factor importante a tener en cuenta es la restricción que impone la normativa de un bit error rate máximo de 10^{-6} en todo momento. Esto implica que la modulación usada debe tener una resistencia natural contra ataques e interferencias, lo que reduce las posibilidades a técnicas de espectro ensanchado. El tercer factor determinante es el entorno, dado que el lugar de operación del sistema

será un avión, es asumible que el multicamino estará muy presente y sería acertado elegir una modulación que por definición fuera robusta en este tipo de entornos. Por estos motivos, se eligió OFDM (*Orthogonal Frequency Division Multiplexing*).

Como último paso dentro del proceso de diseño y una vez diseñados todos los demás sistemas se han asignado valores a las variables de la modulación OFDM.

La cantidad total de datos que se transmiten configura la conformación de la señal OFDM. Para calcular esta cantidad se parte de los 480 bits que cada nodo necesita transmitir (224 bits de información procedente de los actuadores y los 256 bits de cabeceras). El sistema aplica un código de repetición de ratio 1/3 y un código convolucional de ratio ¾, por tanto el enlace OFDM debe transmitir 1920 kbits por cada mensaje, equivalentes a 960 símbolos QPSK. Igualmente en la elección del sistema de acceso al medio, se ha especificado que la ventana de transmisión que corresponde a cada nodo es de 23.25 μs.

Antes de continuar con el cálculo de los parámetros de OFDM existe una particularidad del diseño OFDM que debe ser presentada para entender ciertos aspectos de este proyecto. En este apartado sólo se va a comentar lo necesario para entender el resto del proyecto, en caso de mayor interés recurrir al anexo E.

Dicha particularidad es el diseño de la estimación de canal. En este sistema se va a hacer uso de una estimación de canal basada en símbolos de entrenamiento, en concreto se van a enviar dos símbolos previamente al resto del mensaje, los cuales son a priori conocidos por el receptor. Se ha elegido este método frente a otros porque los mensajes son muy cortos y por tanto se puede asumir que las variaciones del canal serán mínimas durante ese lapso de tiempo. Para implementar el ecualizador se ha decidido usar una ecualización que minimice el error cuadrático (*least-sqaure equalization* LS), la elección de este ecualizador frente a otros más sofisticados (como *minimum mean square error* MMSE) se debió a su sencillez y a que no requiere de ninguna suposición y/o información previa a la ecualización.

Para la elección de los parámetros OFDM se ha partido del prefijo cíclico necesario. Para determinar este parámetro se ha asumido un retardo debido al multicamino máximo de 0.65 μs, lo que equivale aproximadamente a una diferencia de caminos entre el rayo principal y el primer multicamino de 160 metros. Si tenemos en cuenta el factor de roll off del filtro conformador (β=0.2) el prefijo cíclico se reduce a 160x0.8=128 metros. En la actualidad el avión comercial mas grande fabricado (Airbus A380) puede encuadrarse en un cuadrado de 80x80m [9], teniendo además en cuenta que el sistema trabaja con potencias bajas, no es arriesgado suponer que un retardo multicamino superior a 0.65 μs es altamente improbable. Para este sistema se ha elegido dividir el tiempo de guarda calculado (0.65 μs) en dos y aplicar un sufijo y un prefijo cíclico de igual longitud a cada símbolo OFDM. En esta

memoria, por simplicidad y de aquí en adelante, cuándo se mencione el prefijo cíclico hará referencia a ambos tiempos de guarda.

Partiendo del prefijo cíclico es asumible que el símbolo OFDM tenga una duración de entre 5 o 6 veces la duración del prefijo [10]. De esta manera se ha elegido que el número de símbolos sea N=4, que sumados a los símbolos de training hace un total de 6 símbolos OFDM por cada mensaje, de esta manera también nos aseguramos aprovechar al máximo la ventana temporal. En la tabla 2 se resumen los parámetros finales del enlace.

Para adaptar la transmisión al canal y mejorar la eficiencia espectral fuera de la banda de transmisión se ha elegido como filtro transmisor una pareja de filtros adaptados con forma de raíz de coseno realzado con un factor de roll-off de 0.2. En la figura 12 se puede observa el resultado final de la transmisión.

Duración de un mensaje	23.25 μs
Tamaño del mensaje original	224 bits + 256 bits de cabecera
Códigos de corrección de errores	Cód. de repetición (1/3) + cód. convolucional (3/4)
Número de símbolos OFDM	4 + 2 símbolos de entrenamiento
Duración del símbolo OFDM	3.875 μs
Prefijo cíclico	0.646 μs
Tiempo de integración	3.229 μs
Espaciado entre portadoras	309.693 kHz
Nº subportadoras con información	240
Tamaño de la IFFT	512
Ancho de banda de la señal OFDM	74.326 MHz
Factor de roll-off β	0.2

Tabla 2: Resumen de los parámetros del enlace

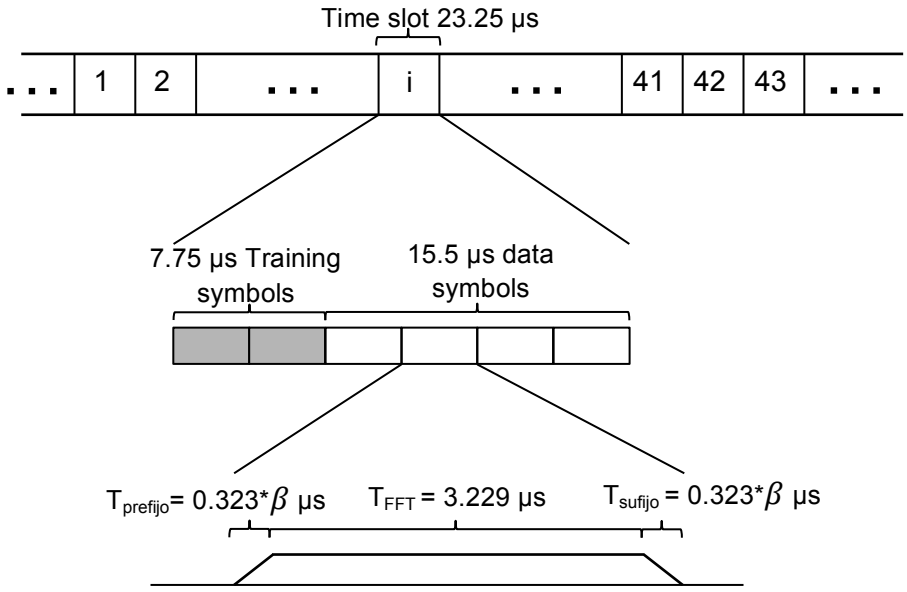


Figura 12: Descripción completa de la fisonomía del mensaje.

4.7 Jammigs

Una de las partes del proyecto es simular ataques contra el sistema basados en jamming, para este propósito se estudiaron los tipos de posibles ataques que pueden darse (capítulo 2). Igualmente se realizó un estudio acerca de las posibles situaciones de peligro que se podrían dar de acuerdo con las fases de vuelo que tienen lugar en un vuelo estándar, dicho estudio puede consultarse en el anexo C.

En la bibliografía están documentados estudios dónde se han realizado pruebas del comportamiento de un enlace OFDM en presencia de jamming [11] [12] [13]. Cada estudio ha arrojado diferentes resultados. Esto se debe a que la efectividad del jamming depende no solo del tipo de ataque sino además del sistema víctima. Igualmente la efectividad del atacante depende de la información que este posea acerca del sistema atacado, para este proyecto se realizaron una serie de suposiciones acerca de la información que el jammer posee, las cuales se recogen en el Anexo C.

En este proyecto se han simulado los siguientes tipos de jamming: jamming de banda ancha, jamming de banda parcial, jamming de banda estrecha, tone jamming (1 tono), multitone jamming (multiples tonos) y smart jamming. De esta manera se simulan todos los tipos de jamming y se buscará aquel que sea más perjudicial para cada situación.

Como se comentó en el apartado 2.4, el objetivo de los jammings de cobertura es aumentar el ruido en el receptor. Para el caso de los noise jammings (los 3 casos)

se ha generado un ruido blanco de un ancho de banda superior al de la señal OFDM y posteriormente se filtrado para simular los diferentes formatos (jamming de banda ancha, jamming de banda parcial y jamming de banda estrecha). En el caso de los tone jamming se han generado uno o varios tonos de fase aleatoria por cada paquete transmitido coincidiendo con las frecuencias de la subportadoras.

En el caso del Smart jamming se ha simulado un ataque en el que el jammer explota uno de los puntos débiles del sistema OFDM: la estimación de canal. Dicho jamming atacará únicamente los símbolos de entrenamiento, empeorando así la estimación de canal.

4.8 Selección de frecuencias

Asignar las frecuencias de transmisión para estos sistemas es algo que no depende únicamente del diseñador. Es más, el diseñador debe adaptar sus sistemas a las frecuencias del espectro que estén asignadas para el tipo de dispositivo que esté desarrollando. En el caso de sistemas como el que ocupa este proyecto la banda de frecuencias está todavía sin asignar y por esta razón únicamente se van a sugerir varios rangos de frecuencias en los que se podrían situar las frecuencias de transmisión. Posteriormente, corresponderá a las autoridades competentes reservar unos rangos de frecuencia para los sistemas de control de vuelo inalámbricos.

Los rangos sugeridos son: la banda de los 4 GHz y la banda de los 20 GHz. Dado que esta cuestión no es esencial en el desarrollo del proyecto se aborda con más detalle en el anexo G.

4.9 Canal

Uno de los factores más determinantes a la hora de simular el sistema es el canal que se va a modelar. En la bibliografía se pueden encontrar estudios realizados acerca de propagación electromagnética en la cabina del avión [14], [15], [16]. Estos estudios concluyen en que el modelo de canal puede ser aproximado por una distribución Rician o un canal Rayleigh multicamino. Dichos artículos tienen en común que van orientados al usuario, es decir, existe un emisor y un receptor situado en la cabina del avión pero en una posición variable.

Para el caso que nos ocupa los enlaces son fijos y conocidos. Por tanto sería necesario realizar un estudio apropiado acerca de la propagación dentro del avión entre dos puntos conocidos y estudiar las posibilidades de ecualización del

multicamino. Por otra parte, el sistema aquí planteado no exije que la comunicación sea por dentro del avión, sino que puede ser realizada por el exterior.

Se ha concluido que los datos actuales no son suficientes como para realizar un modelo correcto del canal para el sistema aquí presentado y por tanto en este proyecto se implementarán 3 canales diferentes: canal AWGN, canal Rayleigh con fading selectivo y canal Rayleigh con fading plano.

5. MODELADO

Una vez diseñado el sistema se procedió a su modelado. Para ello se ha hecho uso de la herramienta de Mathworks: MATLAB/Simulink. En especial se han usado las librerías básicas de simulink, la librería de *communications systems* y de *DSP system*.

En este capítulo se van a explicar los modelos creados a fin de dar una visión global de la simulación. Una descripción más detallada de dichos modelos puede verse en el anexo E. En este capítulo igualmente, se explicarán los métodos de validación del modelo y se mostrará el funcionamiento del mismo.

En definitva lo que se ha hecho en los modelos de simulink ha sido implementar el diagrama de bloques de un sistema de comunicaciones representado en la figura 6, añadiendo los elementos necesarios para simular el jamming y los sistemas de defensa. Debido a la carga computacional que conlleva simular los sistemas en banda frecuencial todos los modelos se simulan en banda base.

Para explicar los modelos creados, este capítulo se divide en los siguientes apartados:

- Enlace OFDM: en este apartado se explicará el funcionamiento de los bloques que conforman el enlace simple, simulando una transmisión estándar basada en una modulación OFDM.

- Jamming: en esta sección se explicará como se han simulado los diferentes jammings.

- Sistemas de mejora: en esta última parte se describirá el funcionamiento de los sistemas de mejora incluidos en la sección 4.5, a excepción del código de repetición.

5.1 Enlace OFDM

En este modelo se incluyen únicamente los elementos que pertenecen al enlace básico, los cuales se corresponden con el diagrama de bloques de la figura 6, a excepción del bloque de jamming. El enlace se divide en tres bloques principales: transmisor, canal y receptor.

El transmisor lo componen: el generador de información, el bloque de codificación de canal, el modulador QPSK, el modulador OFDM y el filtro transmisor.

El canal está formado por un bloque capaz de seleccionar el tipo de canal a simular.

El receptor esta construido por los bloques inversos del transmisor, estos son: el filtro receptor adaptado, el demodulador OFDM, el demodulador QPSK, el decodificador de canal, el receptor de información y un bloque para calcular el BER.

En la figura 14 se puede observar el modelo completo (incluyendo los bloques que se describen más adelante).

5.1.1 Transmisor

El primer bloque corresponde al generador de información. Dicho bloque es un generador aleatorio de bits (P(0)=P(1)=0.5), expuesto en la tabla 2 queda que el tiempo de bit debe ser :

$$\frac{23.25x10^{-6}}{480} = 4.844x10^{-8}\ s.$$

El siguiente bloque es el codificador de canal, en él se encuentra el código convolucional de ratio ¾, el código de repetición de ratio 1/3 y los bloques que aplican el entrelazado.

Los siguientes bloques son los moduladores. Primero se encuentra el modulador QPSK, el cual modula los bits en una constelación QPSK seleccionada (figura 13).

El siguiente bloque es el modulador OFDM, en este bloque la señal QPSK se transforman en un mensaje OFDM formado por 2+4 símbolos OFDM (2 símbolos de entrenamiento y 4 símbolos de información). En este bloque se añade igualmente el prefijo cíclico calculado en la sección de diseño. Antes de la salida los símbolos OFDM se transforman a formato serie.

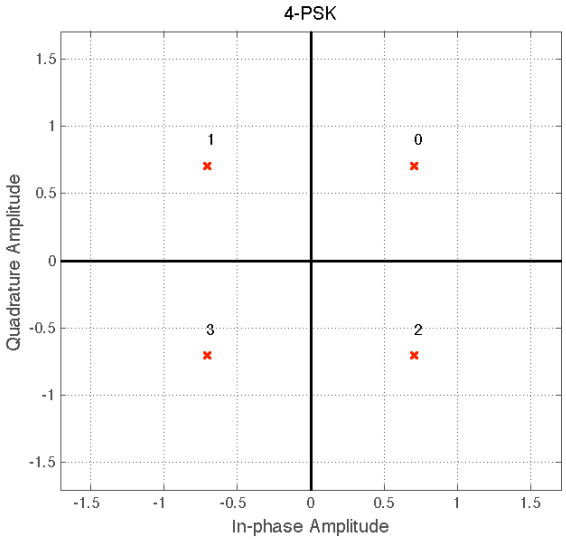


Figura 13: Constelación QPSK modelada

Por último encontramos el bloque del filtro transmisor, formado por un filtro de raíz de coseno realzado. Este bloque también realiza un upsampling de 10 a la señal OFDM. Este bloque también regula la potencia de la señal de salida.

5.1.2 Canal

El bloque del canal consta de los bloques de simulink necesarios para simular los efectos de 3 canales diferentes: AWGN, Rayleigh con efecto multicamino y Rayleigh con fading plano. La imagen del subsistema puede verse en la figura 16.

La elección entre los 3 canales se realiza a través de la máscara del bloque, la cual selecciona la salida del switch a través de la variabla *channel_select*.

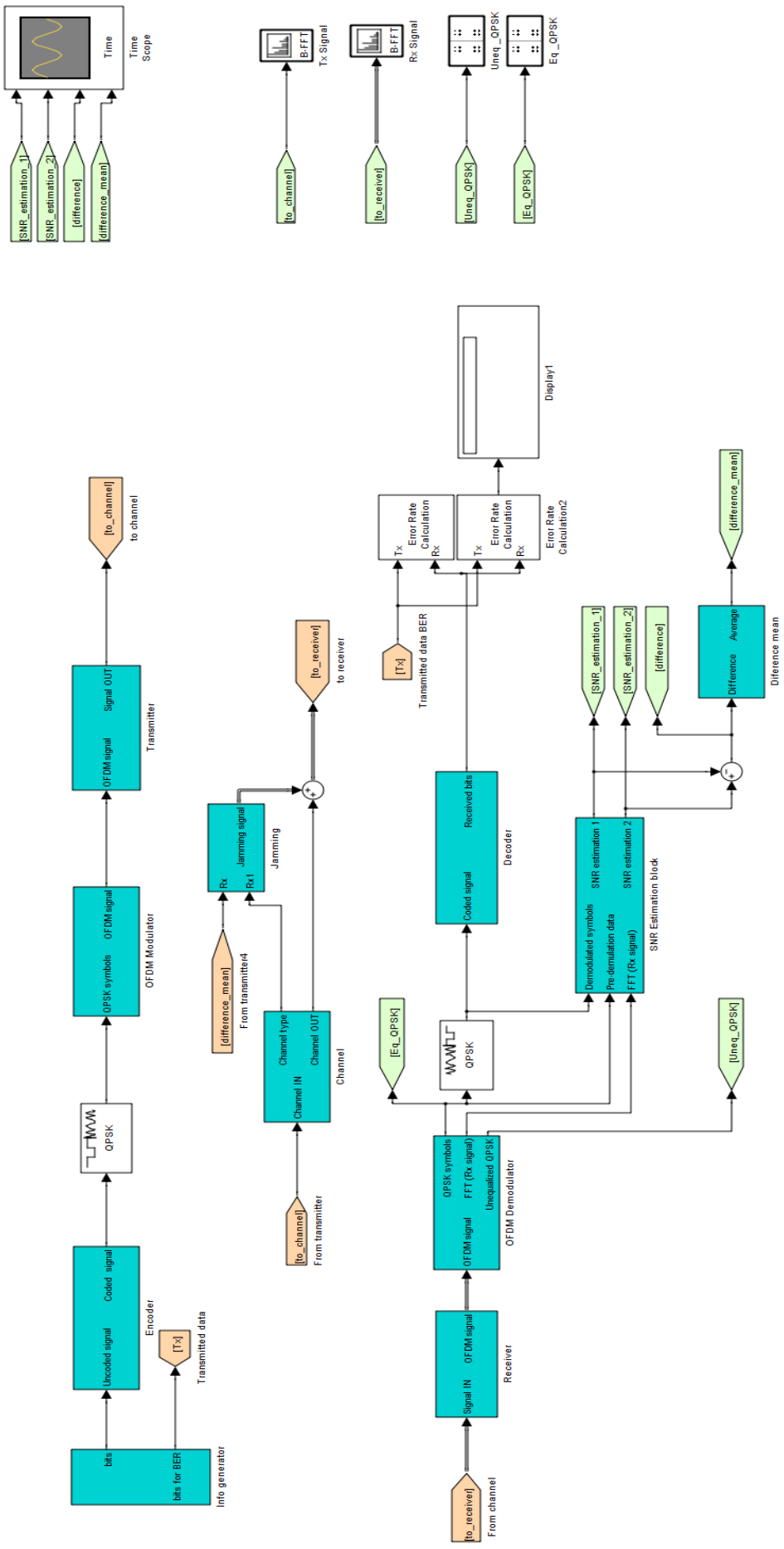


Figura 14: Modelo completo creado en Simulink

Especial atención merece el bloque AWGN, el cual regula el parámetro E_b/N_0, dicho parámetro se introduce en el modelo a través del workspace de MATLAB. El bloque AWGN genera un ruido de potencia N en función de la potencia de la señal a la entrada, de manera que a la salida del canal la señal tenga esa relación energía de bit a ruido (E_b/N_0). Destacar que modificar E_b/N_0 no modifica la relación señal-jamming (S/J) porque, como se puede constatar en la figura 14, el jamming se introduce a la salida del canal. De esta manera el BER obtenido mejorará conforme aumente E_b/N_0 porque los errores debidos al ruido gaussiano disminuirán, pero al no mejorar el S/J los errores que produce el jamming se mantienen.

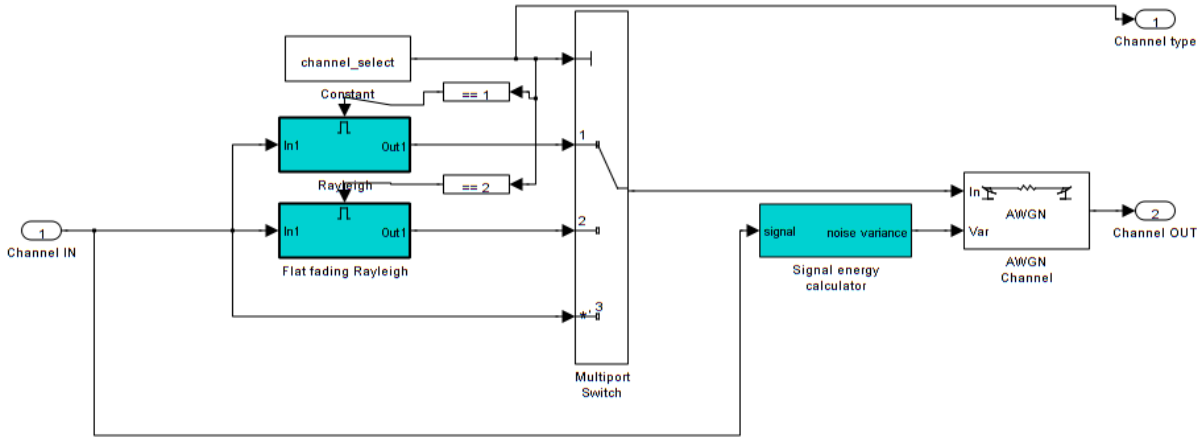


Figura 15: Diagrama del sub-sistema que forma el bloque de canal

5.1.3 Receptor

En el receptor encontramos los bloques contrarios al emisor. En primer lugar tenemos el filtro receptor adaptado al filtro transmisor, formado por un filtro raíz de coseno realzado, el cual realiza un downsampling de 10 muestras.

El siguiente bloque es el demodulador OFDM, aquí se extrae el prefijo cíclico, así como se extraen y se estudian los símbolos de entrenamiento para realizar la estimación del canal. A la salida de este bloque tenemos de nuevo la señal QPSK. Ésta se demodula en el siguiente bloque y así se obtienen los bits transmitidos.

El siguiente paso es deshacer la codificación canal, para ello está el bloque de decodificación, el cual contiene un decodificador de viterbi para el código convolucional, el voter para deshacer el código de repetición y los bloques de desentrelezado.

Por último se encuentra el bloque calculador del BER, donde los bits recibidos se comparan con los enviados.

5.1.4 Validación del enlace

La validación de los modelos hasta este punto se ha realizado a través de las curvas de BER de una modulación QPSK. OFDM se comporta de manera transparente para la transmisión QPSK, por tanto, para comprobar que el sistema se comporta como debería, basta con comparar la curva de BER de una modulación QPSK con la obtenida en el enlace OFDM modelado [10].

En la figura 16 pueden observarse diferentes simulaciones para el caso de un canal gaussiano. En ella se puede observar que para el caso de una transmisión en un canal AWGN sin codificación de canal obtenemos exactamente la curva de BER teórica de QPSK. Añadiendo el código convolucional se observa una notable mejora respecto al sistema sin codificación de canal (tal como era de esperar). Por el contrario, tras añadir el estimador de canal el BER empeora, esto se debe a que el ruido es incorrelado, por lo tanto calcular la estimación para dos símbolos y luego aplicarla a los siguientes no implica que necesariamente sea beneficioso. También se observa que dicho empeoramiento se traslada al modelo con código convolucional por la misma razón.

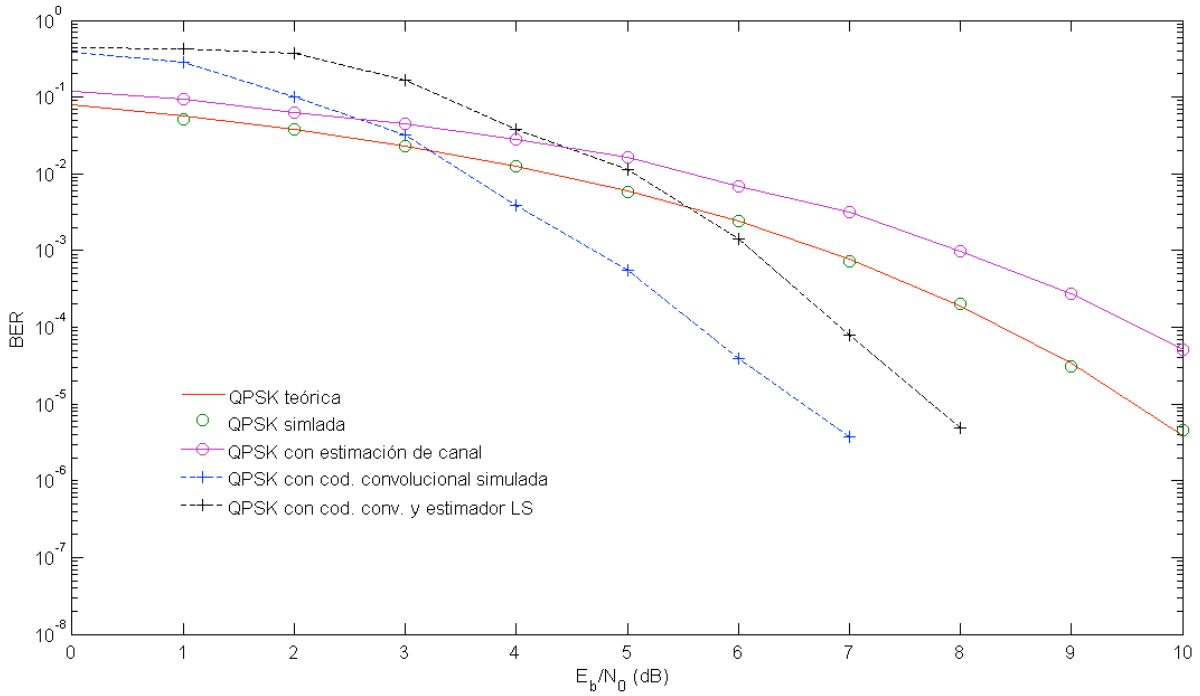


Figura 16: Comparación del BER en un canal AWGN. obtenido tras la simulación del sistema sencillo (sin codificación de canal) y con codificación de canal (código convolucional) con la curva teórica de una modulación QPSK. Igualmente se representa el empeoramiento que produce en el BER el uso de la estimación de canal.

Por otra parte, para comprobar que el modelo se comporta como debe en cuanto a los anchos de banda, potencias y tiempos representamos la densidad espectral de

potencia de la señal OFDM a la salida del filtro transmisor (figura 17). En esta figura podemos comprobar que el ancho de banda utilizado coincide con el calculado en el capítulo anterior. Así como la constelación QPSK se puede comprobar representando la constelación enviada y la recibida (figura 18).

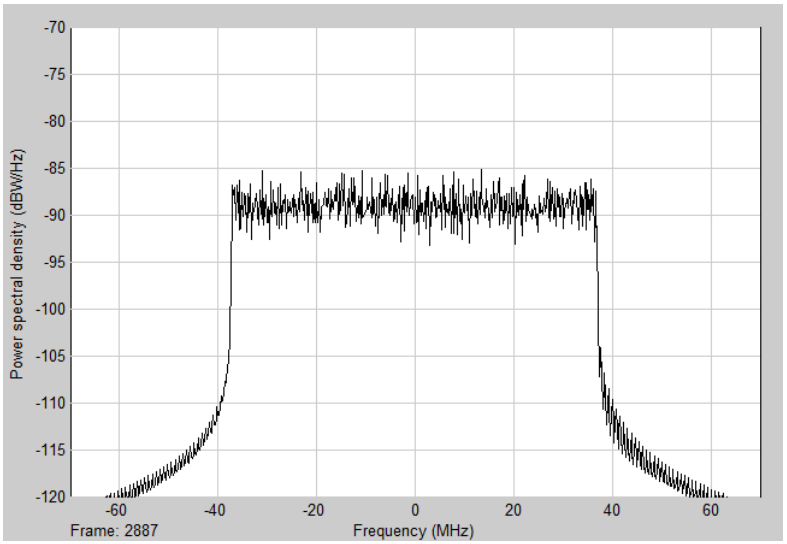


Figura 17: Señal OFDM a la salida del filtro transmisor.

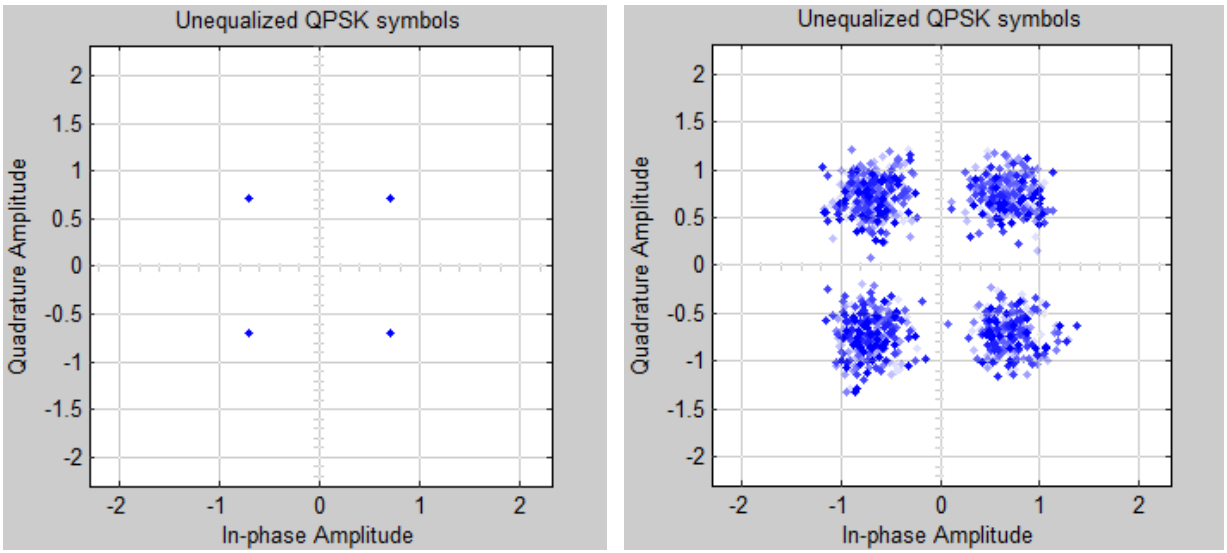


Figura 18: Comparación de la constelación QPSK enviada (figura de la izq.) y con la constelación recibida (figura d ela dcha.).

Para comprobar el comportamiento del sistema en canales no gaussianos, (i.e. Rayleigh con fading plano), realizaremos las mismas representaciones.

En la figura 19 podemos observar BER en un canal Rayleigh con fading plano. Podemos ver que los resultaos se quedan algo distantes respecto a la curva teórica

(cosa que no sucedía en el caso de canal AWGN), esto se debe a que en la curva teórica se asume una estimación de canal perfecta y esa situación no se da en el sistema simulado. Este hecho puede verse en la figura 20, donde a pesar de que se ha simulado con un E_b/N_0 muy alta (superior a los 100 dB) la estimación no es perfecta y se aprecia una pequeña desviación en la constelación ecualizada.

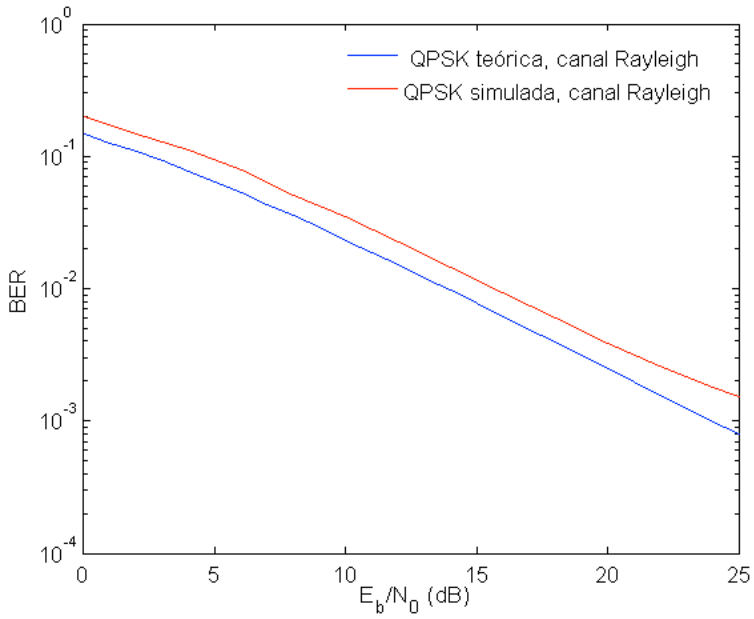
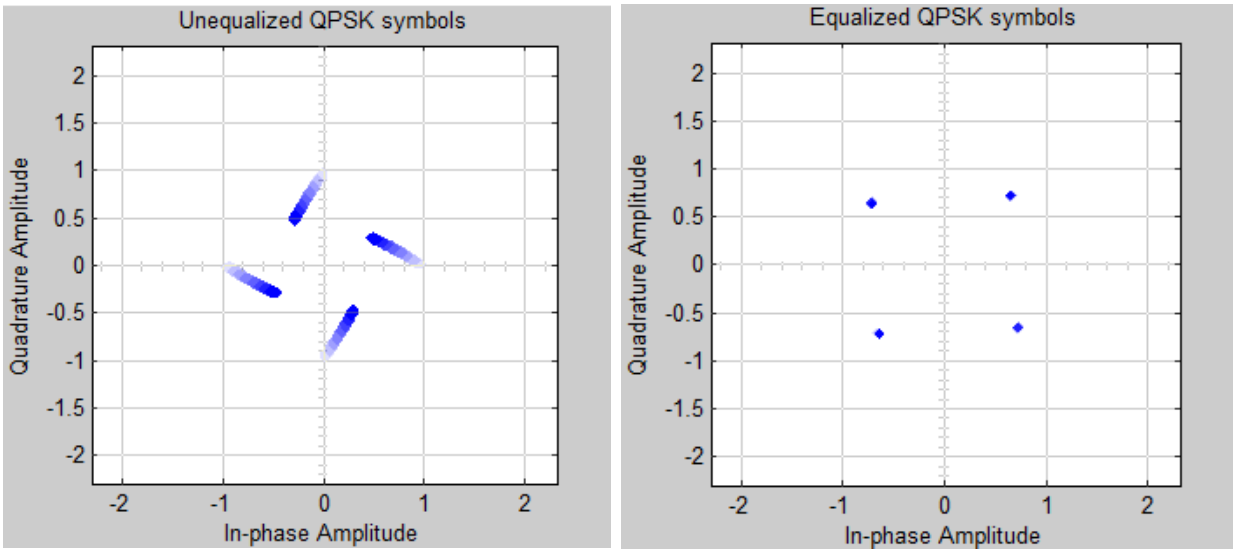


Figura 19: BER obtenido para un canal Rayleigh con fading plano.



a) b)

Figura 20: Comprobación del estimador de canal. La figura a) representa la constelación tal y como se recibe en el receptor (sin ecualizar). La figura b) es la constelación QPSK tras la ecualización.

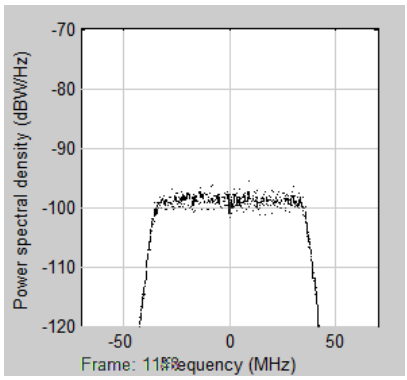
5.2 Jammings

El siguiente paso es la simulación de los jammings. En este modelo se han simulado 6 tipos de jamming, los cuales pueden verse en la tabla 3.

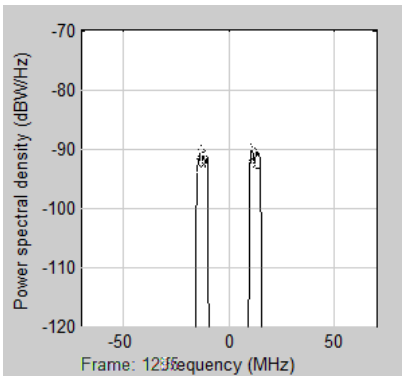
Jamming	Ancho de banda (MHz)	Frecuencia central (MHz)	Tiempo	S/J
Jamming de banda ancha	32	0	Toda la señal	10
Jamming de banda parcial	10	12.5	Toda la señal	10
Jamming de banda estrecha	1	10.5	Toda la señal	10
Tone jamming	-	10	Toda la señal	10
Multi-tone jamming	32	0	Toda la señal	10
Jamming inteligente	32	0	Sólo símbolos de entrenamiento	10

Tabla 3: Jammings simulados y sus parámetros.

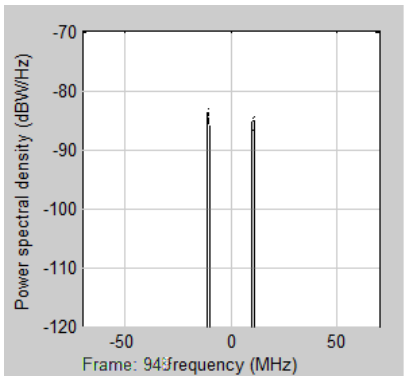
En las siguientes gráficas (figura 21) se observan las densidades espectrales de potencia para cada uno de los modelos de jamming. Por último se suma el jamming a la señal transmitida después de que ésta haya pasado por el canal. Se ha decidido hacerlo así para simular el peor caso posible, el cual sería que el jammer estuviera tan cerca de uno de los nodos que no le afectan los efectos del canal.



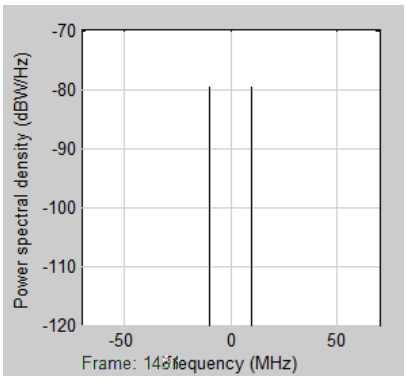
a) Banda ancha



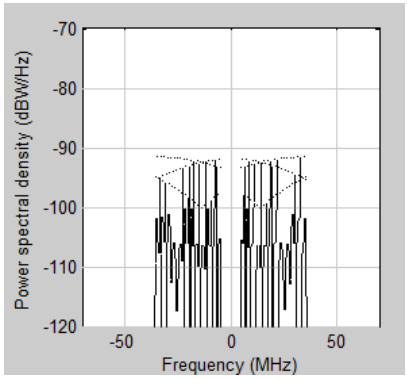
b) Banda parcial



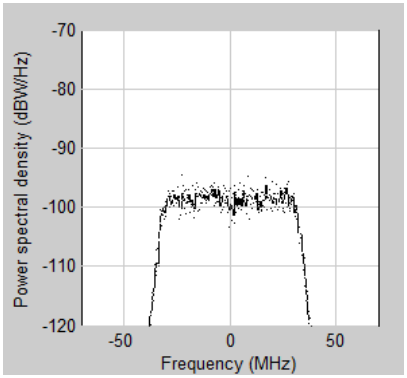
c) Banda estrecha



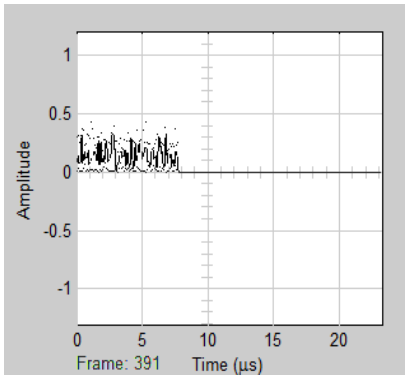
d) Tone



e) Multitone[1]



f) Jamming inteligente



g) Jamming inteligente (tiempo)

Figura 21: Espectros de los jammings simulados. Para el jamming inteligente se representa igualmente la distribución temporal, se puede observar que sólo los dos primeros símbolos son atacados.

1. La figura 22.e no es lo que cabría esperar de una SPD de una señal formada por varios tonos. Esto se debe a los filtros que utiliza MATLAB para dibujar y la resolución de la FFT usada.

5.3 Sistemas de mejora

En este apartado se van a describir los bloques que forman los sistemas de mejora comentados en la sección 4.5.

5.3.1 Detección y evasión de jamming

Para implementar la detección de jamming se ha recurrido a los 2 estimadores del ratio de señal a ruido comentados previamente.

Para crear el estimador de SNR 1 se ha seguido el esquema mostrado en la figura 11. El resultado se puede observar en la figura 22. La salida del estimador es directamente la SNR porque la potencia de los símbolos QPSK está normalizada.

Para modelar el estimador de SNR 2 se ha implementado la ecuación (6), para ello primero se separa la señal OFDM (sin el prefijo cíclico) recibida en dos partes: la banda de transmisión y la banda de zero-padding. Hecho esto se reproduce la ecuación (6) con un multiplicador. En el caso concreto de este sistema los valores de los parámetros son K=240 y Q=272. El estimador completo puede verse en la figura 24.

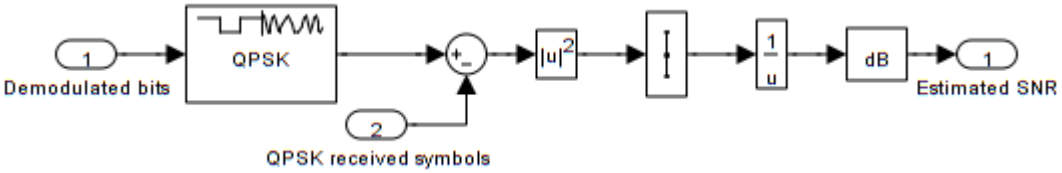


Figura 22: Estimador de SNR 1

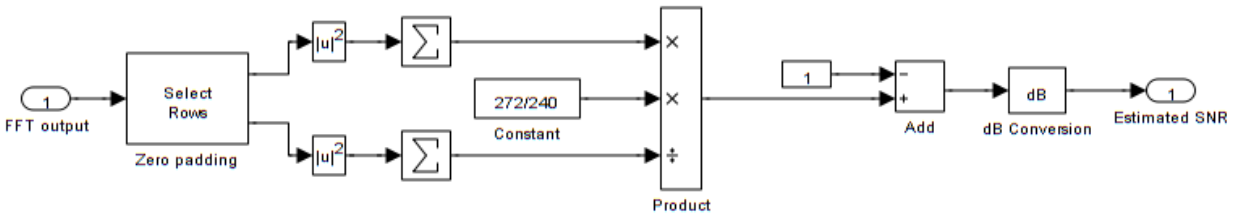


Figura 23: Estimador de SNR 2

A continuación se van a comentar ciertas particularidades de estos estimadores.

En la figura 24.a se puede observar la precisión de ambos estimadores en el caso de un canal AWGN. Se puede constatar que el estimador de SNR 1 posee un offset constante respecto al estimador SNR 2 y respecto a la SNR real de 1.78 dB. Igualmente y como era de esperar el estimador de SNR 1 no es fiable para valores de E_b/N_0 bajos, en concreto para menos de 5 dB.

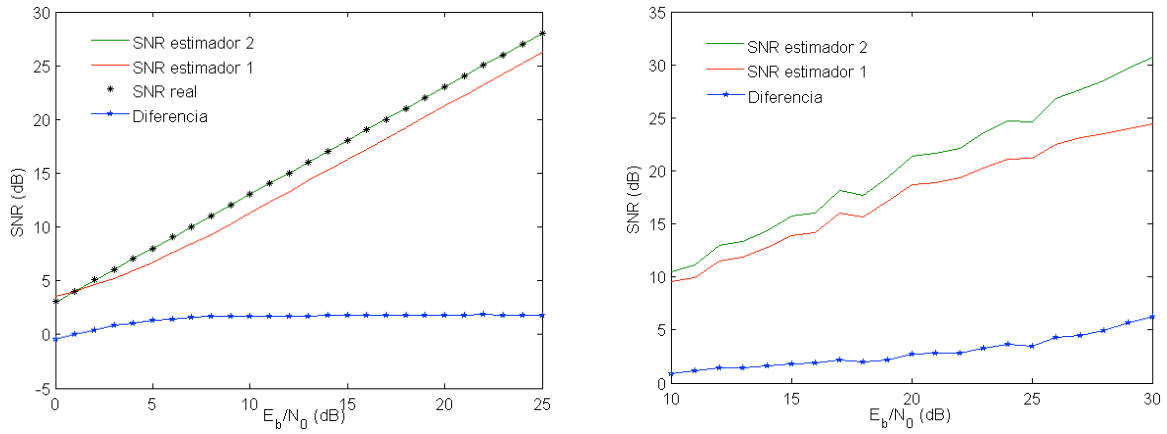


Figura 24: Comparación entre ambos estimadores y la SNR real. La figura a) representa dicha comparación en un canal AWGN. La figura b) refleja la variación del offset entre el estimador 1 y el 2 en un canal Rayleigh.

Para implementar el proceso de detección basta con restar ambas estimaciones y comparar el resultado con un umbral. En el caso de canales AWGN el nivel de ruido es constante y las estimaciones de SNR mantienen una diferencia constante, pero en el caso de un canal Rayleigh no es así (figura 24.b), la señal recibida se ve afectada por desvanecimientos que modifican rápidamente la SNR (figura 25), dado que los estimadores no son ideales existe la posibilidad de que la diferencia entre ambas estimaciones supere por un instante el umbral cuando no hay jamming activo, en tal caso se produce una falsa alarma. Para evitar estas falsas alarmas se ha implementado un bloque que hace la media de los últimos 15 valores de la diferencia, de manera que si la salida del restador supera en un instante el umbral no dispare los sistemas de defensa.

La longitud de la media gobierna la probabilidad de una falsa alarma pero también la velocidad de respuesta del sistema ante la aparición de un jamming. Cuantos más valores se usen para calcular la media la probabilidad de falsa alarma disminuye, pero también disminuye la velocidad de respuesta del sistema puesto que se tarda más en calcular el valor.

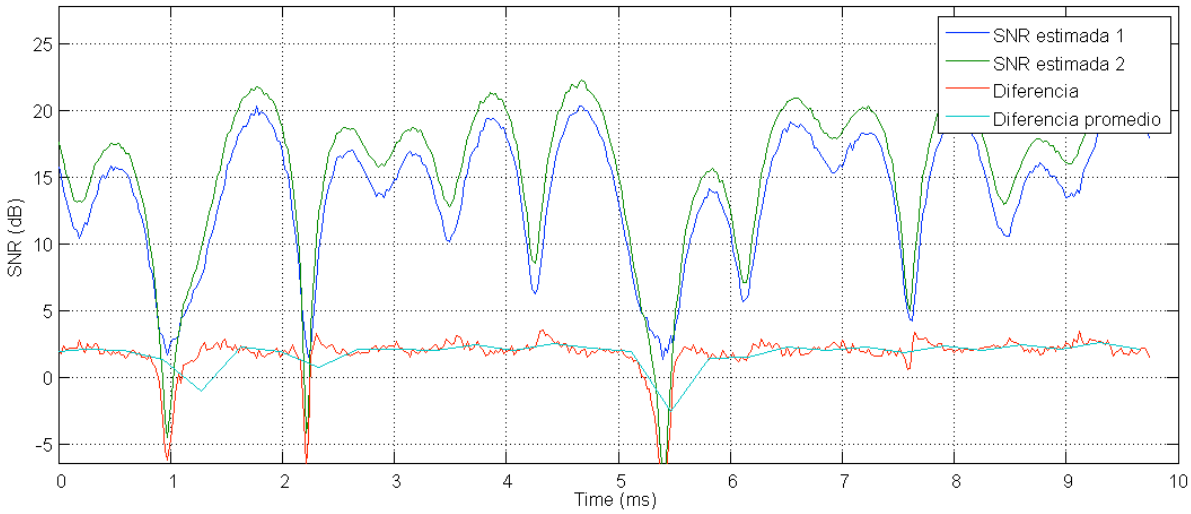


Figura 25: Sistema de detección de jamming en un canal Rayleigh con fading plano.

El umbral que marca la detección de jamming se ha calculado de manera empírica, para ello se han simulado 1.6 Mbits en un entorno sin jamming (tanto para un canal AWGN como para un canal Rayleigh con fading plano) y en un entorno con jamming. Se ha seleccionado como umbral un valor superior a la mayor diferencia de SNR promedio detectada durante ese tiempo y menor que la menor diferencia existente al introducir un jamming. En la figura 26 se puede apreciar la relación que existe entre la diferencia calculada en un entorno libre jamming y en un entorno con jamming.

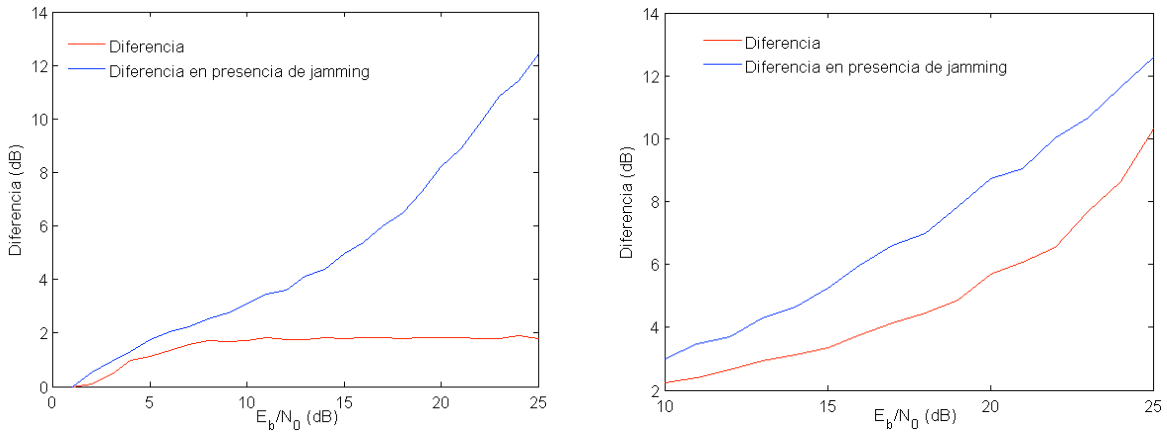


Figura 26: Estudio de la evolución de la diferencia de SNR. La figura a) es la comparación entre la diferencia promedio calculada en un canal AWGN sin jamming frente a la diferencia calculada en presencia de jamming. La figura b) representa lo mismo pero para el caso de un canal Rayleigh con fading plano.

A la hora de elegir el umbral hay que tener en cuenta dos factores, primero que el estimador de SNR 1 no es fiable por debajo de 5 dB, y segundo que para alcanzar un BER<10^{-6} en un canal AWGN hay que trabajar con E_b/N_0>8 dB (cómo se verá en en capítulo 6). Teniendo en cuenta estos factores para el caso de un canal AWGN un valor de umbral válido es de 3 dB. En este caso el umbral es constante puesto que la diferencia entre las SNR estimadas no varía conforme aumenta E_b/N_0. En un canal Rayleigh esto no ocurre y esa diferencia sí varía conforme aumenta E_b/N_0. Por esta razón en canales Rayleigh se calculó un umbral diferente para cada E_b/N_0 siguiendo el mismo proceso que el descrito para un canal AWGN.

EL cálculo de la media así como de las estimaciones de señal a ruido se realiza en los bloques “difference mean” y “SNR estimator” respectivamente. En cambio, la operación de comprar con un umbral se realiza en un subbloque dentro del bloque de jamming llamado “jamming detector”.

Dentro del bloque de jamming se encuentra también el bloque “cognitive radio simulator”. Este bloque es el encargado de simular parte de los sistemas de defensa basados en radios cognitivas, especialmente la función de evasión de jamming.

En el sistema real una vez detectado el jamming, el emisor cambiaría su frecuencia central de trabajo con el fin de escapar del ataque. En este modelo los sistemas se han simulado en banda base de modo que no es posible aplicar este cambio de frecuencia. Para simular los efectos que tendría dicha defensa se ha creado un bloque que desactiva el jamming una vez es detectado (simulando así el cambio en frecuencia) y que lo vuelve a activar pasado un tiempo *t* (recreando lo que sería un reenganche del jamming a la nueva frecuencia). Dicho parámetro *t* es configurable a través de la máscara del bloque de jamming. Para consultar el funcionamiento interno de estos bloques recurrir al anexo E.

5.3.2 Redundancia frecuencial

La segunda mejora planteada en el diseño es la redundancia en frecuencia. Como se ha comentado al comienzo de este capítulo el enlace se simula en banda base. Por eso, para poder simular el sistema con redundancia frecuencial se han creado dos enlaces diferentes que parten de un mismo transmisor. Cada uno de los enlaces posee todos los bloques que se encuentran en el sistema con una sola frecuencia. En la figura 28 se puede observar la forma del sistema completo con la redundancia en frecuencia.

La diferencia más significativa se encuentra tras la recepción individual. A la derecha del modelo está el voter frecuencial. Este sistema se encarga de analizar la información que se posee acerca del enlace en cada frecuencia (SNR y existencia

de jamming) y seleccionar la información que ha sido transmitida por la frecuencia más fiable. El criterio de selección de la frecuencia se realiza de acuerdo con los criterios expuestos en la tabla 1 en la sección 4.5.2**.**

5.3.3 Redundancia en tiempo y datos

Otra de las mejoras que se han planteado es la redundancia en tiempo y datos, la cual es un código de repetición de ratio 1/3. Dicha repetición se aplica (como se ha comentado en el apartado 5.1.1) en el bloque de codificación de canal y posteriormente en el receptor, concretamente en el bloque de decodificación, se deshace la repetición mediante un voter que toma los 3 bits recibidos en paralelo y elije el valor más probable (es decir, aquel valor presente en al menos 2 de los bits). De esta manera la probabilidad de error en el bit queda representada por la ecuación 3.

$$P_b = P_{b_1}P_{b_2}P_{b_3} + \overline{P_{b_1}}\,P_{b_2}P_{b_3} + P_{b_1}\overline{P_{b_2}}P_{b_3} + P_{b_1}P_{b_2}\overline{P_{b_3}} \qquad (3)$$

Donde P_b representa la probibalidad de error en el bit total, P_{b_i} la probabilidad de error en el bit *i* (*i*=1, 2, 3) en el enlace sin código de repetición y $\overline{P_{b_i}}$ la probabilidad de que el bit *i* posea el valor correcto. Suponiendo las probabilidades de error en el bit independientes e iguales podemos reescribir la ecuación 3 como:

$$P_b = P_{b_i}^3 + 3\overline{P_{b_i}}P_{b_i}^2 \qquad (4)$$

En la ecuación 4 se puede observar la mejora que implementa el código. La figura 27 representa la ecuación 4 de forma gráfica junto con los resultados obtenidos en las simulaciones.

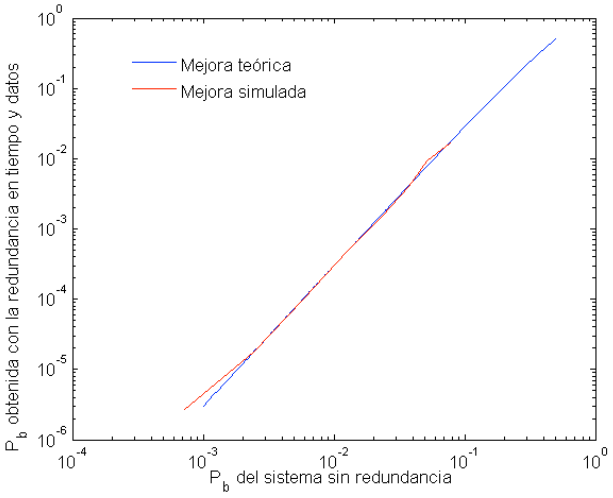


Figura 27: Mejora en el BER aportada por la redundancia. Curvas teóricas y simlada.

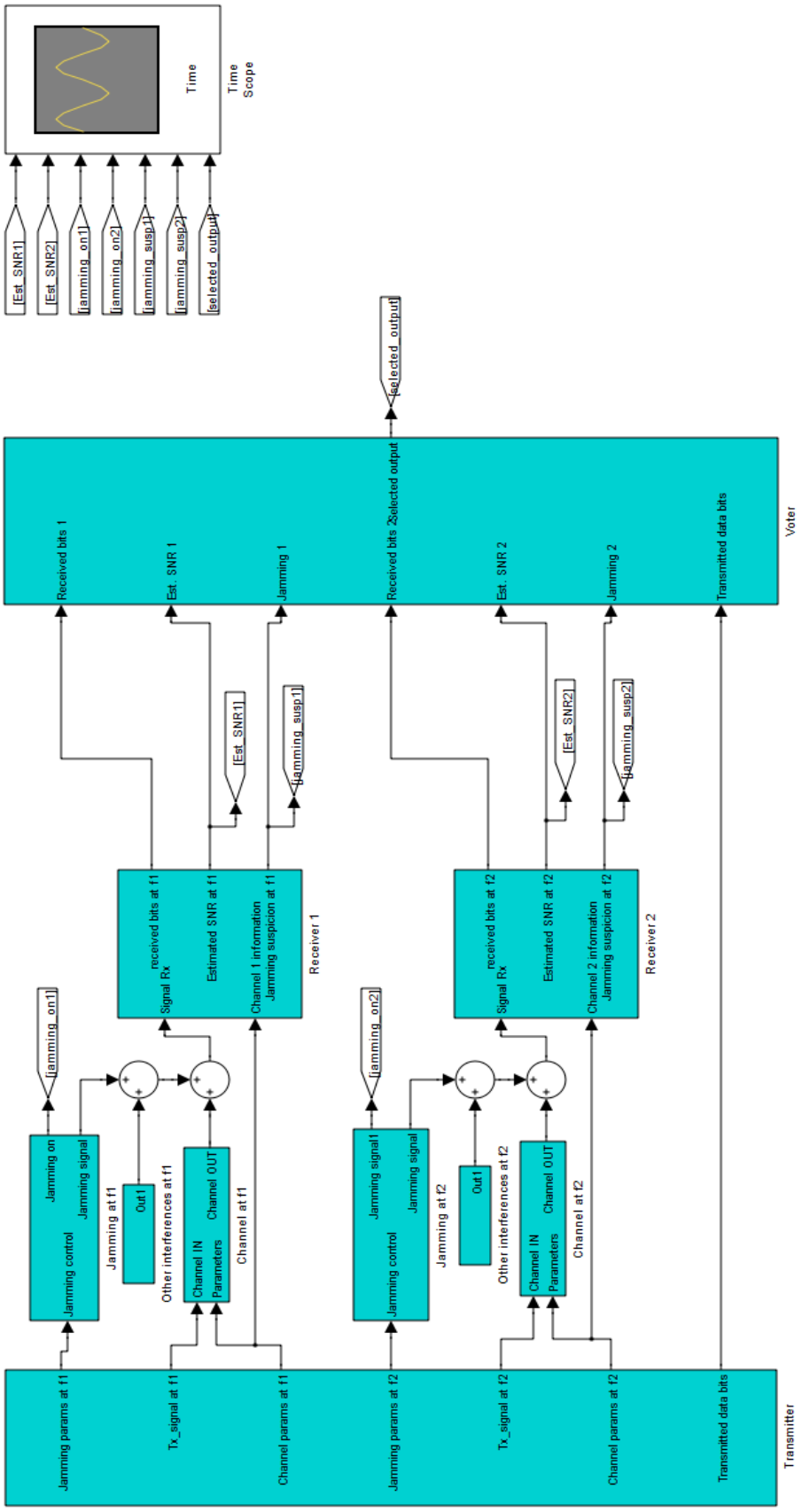


Figura 28: Modelo del sistema con redundancia en frecuencia

6. RESULTADOS

En este apartado se van a presentar y discutir los resultados obtenidos en las simulaciones.

Tras la validación del sistema comentada en el capítulo anterior, en este capítulo se expondrán únicamente los resultados más interesantes para los objetivos del presente proyecto.

Los objetivos buscados con las simulaciones son:

- Comprobar el BER alcanzado con el sistema en estado normal (sin ataques), para dos canales (AWGN y Rayleigh con fading plano).
- Comprobar el BER alcanzado cuando el sistema sufre un ataque, en dos canales (AWGN y Rayleigh con fading plano).
- Detectar el jamming más perjudicial para el sistema.
- Comprobar el comportamiento de la defensa basada en radios cognitivas en presencia del ataque más destructivo.
- Comprobar la mejora introducida por la redundancia en frecuencia para ambos canales (AWGN y Rayleigh con fading plano).

Para testear dichos objetivos se presentan las siguientes simulaciones:

- Comportamiento del sistema monofrecuencia en un canal AWGN sin presencia de jamming.
- Comportamiento del sistema monofrecuencia en un canal Rayleigh con fading plano sin presencia de jamming.
- Comportamiento del sistema (sin sistemas de defensa) en un canal AWGN en presencia de jamming.

- Comportamiento del sistema (sin sistemas de defensa) en un canal Rayleigh con fading plano en presencia de jamming.
- Comportamiento del sistema con evasión de jamming en un canal AWGN en presencia del jamming más destructivo.
- Comportamiento del sistema con evasión de jamming en un canal Rayleigh con fading plano en presencia del jamming más destructivo.
- Comportamiento del sistema con redundancia en frecuencia en un canal AWGN y sin jamming.
- Comportamiento del sistema con redundancia en frecuencia en un canal Rayleigh con fading plano y sin jamming

Las simulaciones se han realizado con los parámetros mostrados en la tabla 4.

	Canal AWGN			Canal Rayleigh con fading plano		
	No jamming	Jamming	2 frecuencias	No jamming	Jamming	2 frecuencias
Rango Eb/No (dB)	0-10	0-20	0-10	10-25	10-25	10-20
Max. Bits transmitidos	10^8	10^8	10^8	10^9	10^9	10^9
Max. Bits erróneos	10^3	$5x10^3$	10^3	$5x10^5$	$5x10^5$	$5x10^5$
S/J (dB)	10	10	10	10	10	10
Tamaño de la media	15	15	15	15	15	15
Tiempo de reenganche del jammer	-	400 mensajes	-	-	400 mensajes	-

Tabla 4: Relación de parámetros usados en las simulaciones

En la figura 29 se presenta los resultados pertenecientes a las simulaciones en un canal AWGN obtenidos con un sistema monofrecuencial y con el sistema con redundancia en frecuencia.

Se puede observar que el sistema alcanza el BER requerido de 10^{-6} con una relación señal a ruido por bit (E_b/N_0) de aproximadamente 6 dB. También se observa

que la mejora introducida por la redundancia en frecuencia es casi inapreciable. Esto se debe a que ambas frecuencias poseen la misma SNR y no hay variaciones en el canal, por tanto la elección de una u otra frecuencia no aporta prácticamente ninguna mejora. Si denominaos P_b a la probabilidad de error en el bit, podemos afirmar que para el caso de 2 frecuencias:

$$P_b = P_{b_1} P(SNR_1 > SNR_2) + P_{b_2} P(SNR_2 > SNR_1) \qquad (5)$$

Donde P_{b_i} representa la probabilidad de error en la frecuencia *i* (*i*=1,2). Si asumimos que la probabilidad de que $P(SNR_i>SNR_j)=0.5$, puesto que ambos canales son iguales, y que $P_{b_1}=P_{b_2}$ ya que ambos enlaces poseen la misma E_b/N_0. La ecuación (5) se puede reescribir como:

$$P_b = P_{b_i} \qquad i = 1,2 \qquad (6)$$

De esta última ecuación se desprenede que el uso de dos frecuencias no aporta ninguna mejora en un canal AWGN (tal y como se muestra en la figura 29). Para realizar estas igualdades se ha asumido que P_{bi} y $P(SNR_i>SNR_j)$ son independientes y constantes. La probabilidad de error en el bit tiene una relación directa con la SNR. Si bien, en el caso que nos ocupa las variaciones de SNR son mínimas y no varían apenas la probalidad de error para una E_b/N_0 dado, lo que nos permite considerar P_{bi} constante.

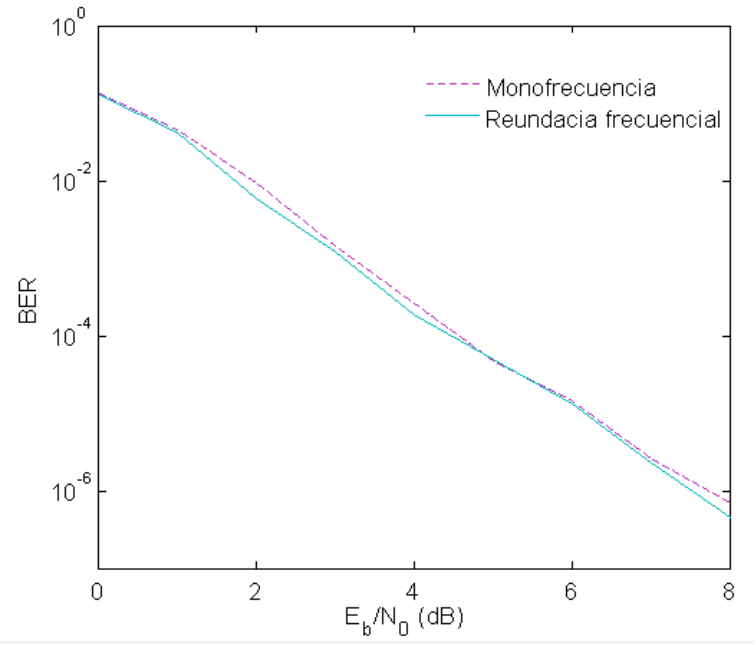
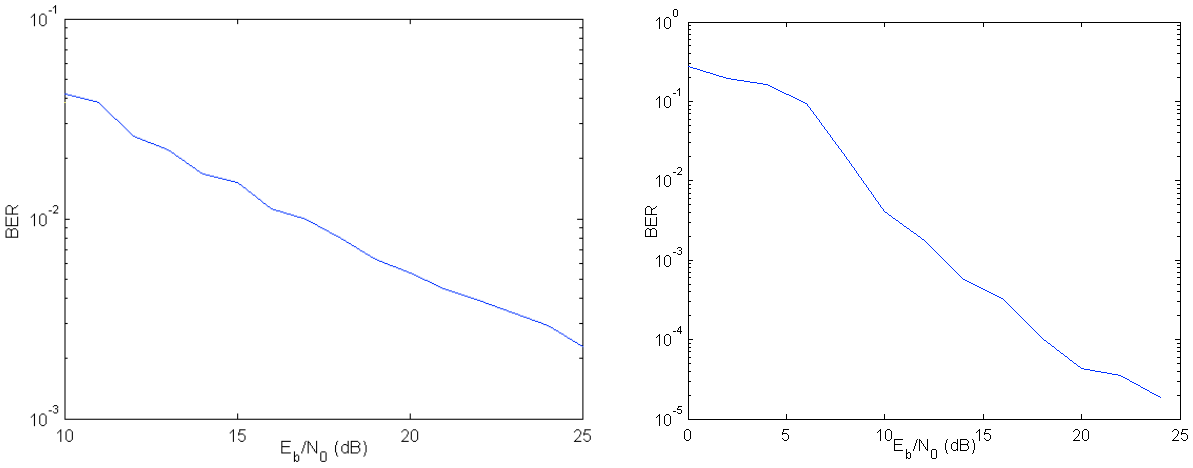


Figura 29: Resultados arrojados por el modelo monofrecuencial y con redundancia en frecuencia para un canal AWGN sin jamming

La siguiente figura (figura 30) muestra los resultados obtenidos por la simulación del sistema en un canal Rayleigh con fading plano.



a) b)

Figura 30: Resultados para canales Rayleigh con fading plano. En la figura a) se representan los resultados del sistema monofrecuencial. En la figura b) se encuentran los resultados para un sistema con redundancia en frecuencia.

Comparando la figura 30.a con la figura 19, se puede ver que añadir los códigos de corrección de errores no aporta una mejora al BER, esto se debe a que los fadings son mucho más largos que la longitud del paquete (figura 31). Esto implica que el paquete que se transmite durante un fading profundo no es demodulado correctamente y la redundancia que añade el código convolucional solamente empeora el BER.

En la figura 30 también se representa la mejora en el BER obtenida por la redundancia en frecuencia. En la simulación del sistema con dos frecuencias, se han querido considerar los efectos del canal independientes y diferentes para cada una de las frecuencias, por eso para el enlace en la frecuencia 1 se ha simulado el mismo canal en el caso del sistema simple, pero para el segundo enlace se han disminuido la frecuencia y aumentado la duración de los fadings (figura 31). Fácilmente se puede observar que la redundancia en frecuencia introduce una notable mejora en el BER obtenido. Como se observa en la figura 31, debe haber un fading simultáneo en ambas frecuencias para que se produzcan errores en la transmisión.

Los siguientes resultados que se presentan reflejan el comportamiento del sistema (sin mecanismos de defensa, a excepción del código de repetición) en presencia de los diferentes jammings. El objetivo de esta simulación es no solo estudiar el BER obtenido sino además localizar que tipo de jamming es el más peligroso. Dichos resultados se pueden observar en la figura 32.

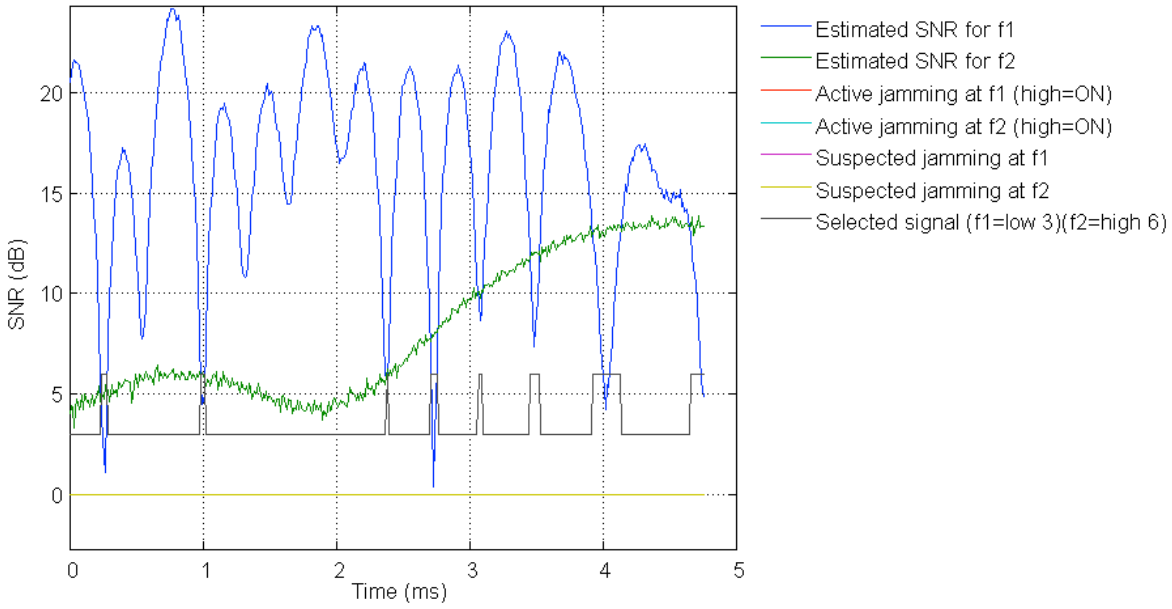


Figura 31: Variaciones de los canales para ambas frecuencias.

En la figura 32.a se puede observar que para un canal gaussiano el jamming más peligroso para E_b/N_0>8 dB es el jamming de banda parcial. En la gráfica se puede ver que las curvas de BER tienen forma asintótica. Esto se debe a lo comentado en el apartado referido al canal del capítulo 5, donde se explicaba que aumentar E_b/N_0 indefinidamente no mejora el BER debido a que la relación S/J se mantiene constante.

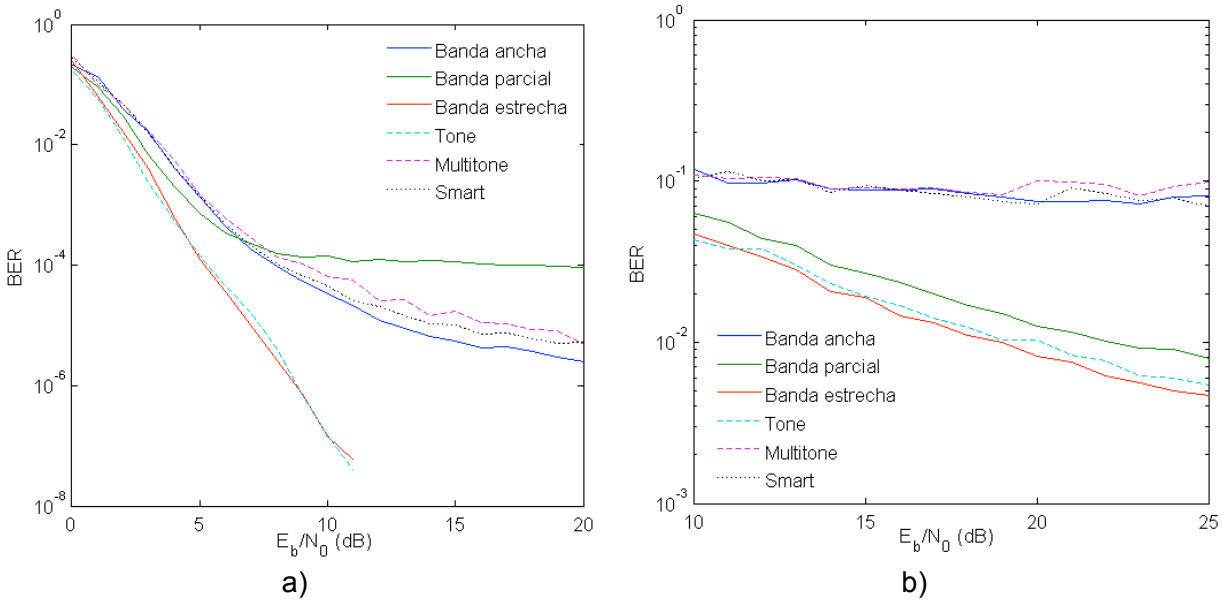


Figura 32: Comportamiento del sistema en presencia de jamming. La figura a) arroja los resultados correspondientes a un canal AWGN, b) se corresponde con un canal Rayleigh

En presencia de jamming se puede afirmar que:

$$\frac{S}{N} = \frac{S}{N_0 + J} \tag{7}$$

Donde J representa la potencia del jammer. Por tanto si asumimos que para valores de E_b/N_0 altos, el valor de N_0 disminuye hasta cumplir que: $N_0 << J$. Podemos aproximar la ecuación 7:

$$\frac{S}{N} = \frac{S}{J} \tag{8}$$

Si tal y como se ha explicado anteriormente ni S ni J varía al aumentar E_b/N_0, es de esperar el resultado asintótico de las figuras 32.a.

Para el caso de un canal Rayleigh (figura 32.b) se puede ver que los jammings más efectivos son: el jamming de banda ancha, el jamming multitono y el Smart jamming (o jamming inteligente). Estos tres jammings son tan efectivos en el canal Rayleigh porque atacan todo el ancho de banda de la señal, esto quiere decir que atacan los símbolos de entrenamiento que controlan la estimación del canal, punto débil de la transmisión OFDM.

El siguiente paso es simular las defensas frente al jamming implementadas. En la figura 33 puede verse el BER que se obtiene cuando el sistema usa la defensa basada en la detección y evasión del jamming. El sistema se simula de manera que el jammer tarda 400 tramas en reengancharse a la nueva frecuencia. Como era de esperar el BER mejora sustancialmente, de igual manera que pasaba antes, el resultado es asintótico, puesto que los errores que se producen debidos al jamming siempre están ahí. Hay que destacar los escalones que se forman en la curva de BER, dicho escalones se deben al sistema de detección.

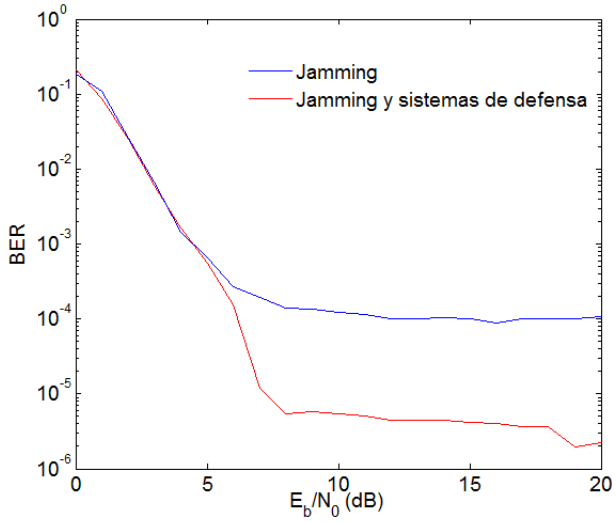


Figura 33: BER obtenido en un sistema con evasión de jamming y un canal AWGN. El jamming simulado fue un jamming de banda parcial y el tiempo de reenganche del jammer fue de aproximadamente 9.3 ms.

Como se observa en la figura 34 el sistema calcula un valor de “difference mean” en el que en parte de sus tramas el jamming ya estaba activo. Si los valores de diferencia son los bastante grandes como para hacer que la media supere el umbral el jamming será detectado en ese instante, sino el sistema detectará el jamming tras la siguiente ventana de 15 tramas. Los valores de la variable diferencia aumentan cuanto más grande es el E_b/N_0 simulado (como se puede observar en la figura 26). Por eso el mejor caso (en el que el sistema se detecta el jamming en la primera ventana) aparece para valores más altos de E_b/N_0. Como se ha comentado anteriormente el número de errores es quasiconstante y depende del tiempo en el que el jamming está activo, si ese tiempo disminuye porque el jamming es detectado antes, entonces el BER disminuye.

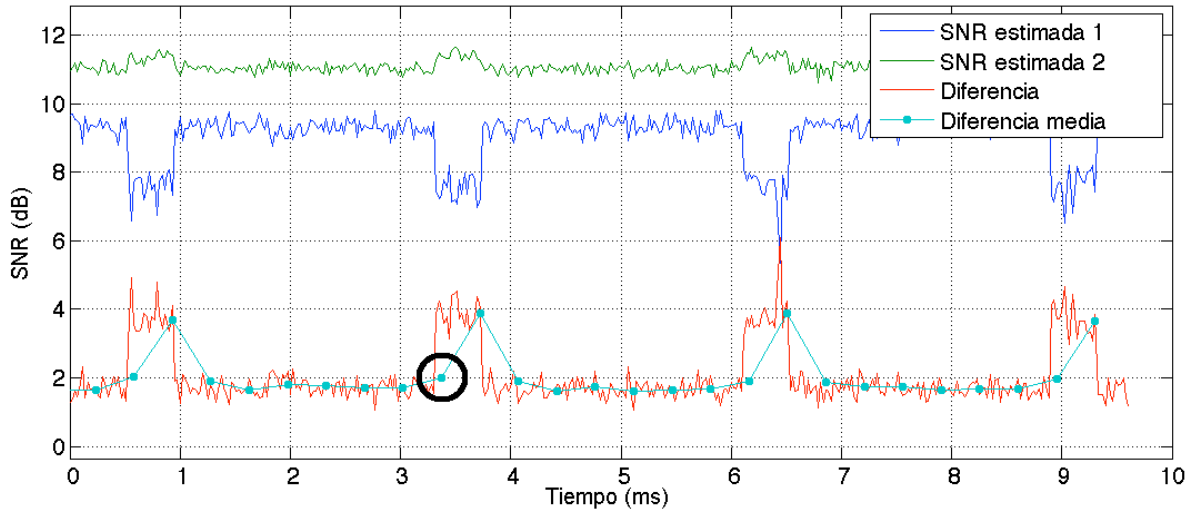


Figura 34: Proceso de evasión de jamming donde se muestra que un valor de la media da un valor menor que el umbral aún cuando el jamming está activo.

Es importante constatar el hecho de que el sistema de evasión transforma el jamming en un jamming pulsado de longitud igual al tiempo que tarda el sistema en detectar el jamming. En esta situación la probabilidad de error en el bit responde a la ecuación (9):

$$P_b = P_J P_{b_J} + P_{AWGN} P_{b_{AWGN}} \tag{9}$$

Donde definimos cada parámetro como:

P_J: Probabilidad de que exista jamming
P_{b_J}: Probailidad de error en el bit en presencia de jamming
P_{AWGN}: Probabilidad de que no exista jamming
$P_{b_{AWGN}}$: Probabilidad de error en el bit sin jamming

Si en la ecuación (9) hacemos el cambio:

$$P_{AWGN} = 1 - P_J \tag{10}$$

Obtenemos:

$$P_b = \left(P_{b_j} - P_{b_{AWGN}}\right) P_J + P_{b_{AWGN}} \tag{11}$$

Analizando la ecuación (8) se puede deducir que para valores de E_b/N_0 altos donde se cumpla que $P_{b_j} >> P_{b_{AWGN}}$ la ecuación (8) se puede aproximar por:

$$P_b = P_J P_{b_J} \tag{12}$$

La ecuación (12) muestra que la mejora aportada por las radios cognitivas es directamente dependiente del nivel de defensa, es decir, del tiempo que tarde el jamming en reengancharse a la señal.

Para un canal Rayleigh con fading plano los resultados en presencia de un jamming inteligente pueden observarse en la figura 35.

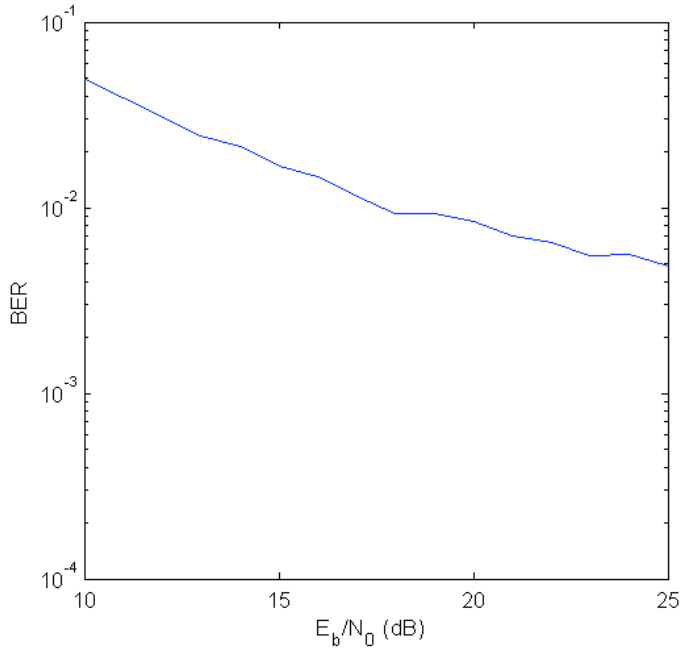


Figura 35: BER obtenido en un canal Rayleigh con fading plano, jamming inteligente y sistemas de evasión activos.

7. CONCLUSIONES Y POSIBLES MEJORAS

7.1 Conclusiones

En este proyecto se ha desarrollado la base para la creación de un sistema de control de vuelo inalámbrico que cumpla los requisitos que las organizaciones de certificación exigen. Al mismo tiempo, se han estudiado las posibles formas que toma la guerra electrónica y se han estudiado los posibles amenazas en forma de ataques intencionados que existen para este tipo de sistemas.

Como se comentó en el capítulo 1, el fin de este proyecto no es diseñar el sistema definitivo, sino un punto de partida desde el que poder avanzar y que arroje los primeros resultados. Teniendo en cuenta esto último, los resultados obtenidos y presentados en el capítulo anterior son esperanzadores. Si bien el sistema no cumple todos los requisitos (por ejemplo, mantener un BER<10^{-6} en todo momento), se ha marcado un camino a seguir.

De los resultados obtenidos se observa que para canales AWGN el sistema es capaz de alcanzar en entornos amigables (sin jamming o desvanecimientos profundos) el BER de 10^{-6}, para canales Rayleigh el comportamiento del sistema es ineficiente y debe mejorarse. Comparando las figuras 19 y 30.a se puede ver que con el sistema con codificación de canal se obtiene peor BER que con el enlace sin códigos de corrección de errores. Como se ha dicho anteriormente los códigos de corrección de errores no son los óptimos para este sistema, es necesario por tanto estudiar y analizar las diferentes opciones. Es igualmente importante estudiar el canal y como éste introduce los errores en el sistema para poder elegir el código más apropiado.

Igualmente, los resultados arrojados por la simulación de contramedidas basadas en el uso de radios cognitivas muestran, que en este caso concreto (dado que la evasión siempre se realiza a posteriori) la mejora es muy dependiente del tiempo que tarda el jammer en relocalizar la frecuencia de emisión. Sin embargo, las radios cognitivas pueden implementar el método de detección y evasión de una manera mucho más eficiente, tardando mucho menos en detectar el jamming e incluso llegando a conocer al jammer de tal manera que puedan adelantarse a sus movimientos cambiando la frecuencia de trabajo antes de que el jammer se reenganche. Por tanto la conclusión que este proyecto es que las radios cognitivas marcan un rumbo prometedor y que merece la que pena que sea estudiado para poder implementarlo en futuras versiones del sistema.

También se ha visto que el uso de una redundancia en frecuencia aporta otro nivel de defensa frente a jamming y frente a desvanecimientos selectivos en frecuencia. Para este proyecto se ha decidido elegir una u otra frecuencia de manera suplementaria a la hora de la demodulación, porque se ha considerado que en el caso de existir un jamming la frecuencia jammeada no es fiable. Esto hace que cuándo el sistema esté libre de jamming se descarte el 50% de la potencia total transmitida (puesto que una de las dos frecuencias es descartada) innecesariamente.

Igualmente se ha comprado que la redundancia en tiempo y datos (código de repetición de ratio 1/3) aporta una mejora importante al BER. Aún así es necesario valorar si dicha mejora compensa la cantidad de redundancia que introduce (multiplica por 3 la cantidad de bits transmitidos). Este aspecto queda resuelto nn la bibliografía, donde está documentado que los códigos de repetición son altamente ineficientes [17]. Por tanto esta mejora debe ser desechada y substituida por un código de corrección de errores más eficiente.

Por otra parte, el estudio de la guerra electrónica ha mostrado que el éxito de un ataque electrónico es una combinación entre el tipo de ataque perpetrado y el sistema atacado. También se ha visto que cuánta más información posea el atacante acerca del sistema víctima más sencillo es realizar un ataque exitoso. Para el caso concreto expuesto en este proyecto los resultados concluyen que el punto débil del sistema OFDM es la estimación del canal necesaria para los canales que introducen defases y por tanto los ataques más efectivos son los que atacan directamente esta función del sistema (jamming inteligente). En cambio en un canal AWGN (dónde la estimación de canal no es importante) el jamming más destructivo se corresponde con un jamming de banda parcial. Igualmente en las ecuaciones (9,10,11) y (12) se ha demostrado analíticamente que un jamming pulsado funciona para un nivel de potencia dado, tan bien o mejor(en el caso de que la potencia sea poca) que la versión continua.

7.1 Posibles mejoras

Los resultados del proyecto son prometedores, pero aún así existen puntos de mejora en el diseño que deben ser abordados en futuras versiones del proyecto, algunos de estos puntos se relatan a continuación.

- **Topología de la red:** la topología actual en estrella es muy ineficiente. Este tipo de topología multiplica los tiempos de guarda del TDMA (se necesita un periodo de guarda por cada mensaje transmitido), obliga a usar mensajes muy cortos, lo que multiplica los símbolos de entrenamiento de OFDM y limita el uso de técnicas de corrección de errores más eficientes (como los códigos *low density parity check* LDPC). Igualmente se multiplica el número de cabeceras transmitidas al tener que transmitir una por cada mensaje.

  Para solucionar estas desventajas se sugiere una topología como la de la figura 36. En esta nueva topología además de un método de acceso al medio TDMA se hace una división espacial. Se dividen los nodos en tres grupos diferentes, donde cada grupo no interfiere en los demás. Dentro de cada grupo se encuentra un nodo principal el cual es el encargado de recopilar la información de los nodos y transmitirla al ordenador central. Conseguimos así una comunicación de larga distancia entre menos nodos (4 principales nodos en total), haciendo el enlace más eficiente.

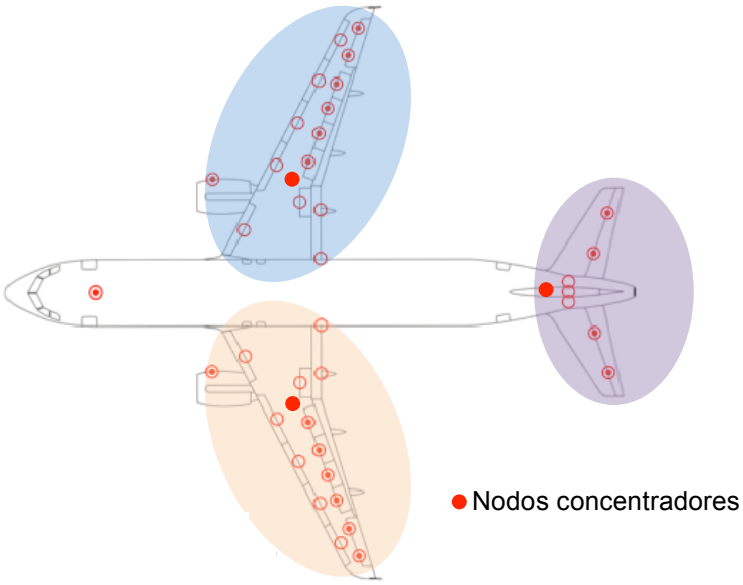


Figura 36: Ejemplo de una topología híbrida usando división espacial

- **Antenas:** En este sistema se han supuesto antenas omnidireccionales. Esta suposición no tiene sentido en el sistema final. Puesto que los enlaces son fijos y conocidos es mucho más conveniente el uso de antenas directivas para

un mayor aprovechamiento de la energía disponible y evitar al mismo interferencias provenientes de direcciones no deseadas.

- **Código de corrección de errores:** En la descripción del proyecto se expuso que el código de corrección de errores fue escogido por similitud con el sistema 802.11a. Sería necesario diseñar un código que se adapte mejor a este sistema concreto para poder sacar el máximo provecho.

- **Redundancia frecuencial:** El hecho de descartar una de las frecuencias es energéticamente muy ineficiente puesto que se desaprovecha mucha potencia transmitida. Sería adecuado buscar algún método que consiga combinar la potencia transmitida por ambas frecuencias.

7.3 Lineas de futuro

Como se ha expuesto al comienzo de esta memoria, este proyecto fin de carrera forma parte de una tesis doctoral. Por tanto existen todo un abanico de acciones futuras a realizar, estos son algunos de los puntos relacionados con el presente proyecto que podrían desarrollarse en un futuro:

- Investigar las mejoras propuestas anteriormente, con el fin de mejorar el sistema y acercarse a los requisitos.

- Realizar estudios acerca del nivel de ruido en un avión, así como estudios del canal para modelarlo correctamente y poder estimar la potencia necesaria para la transmisión.

- Usar radios cognitivas para implementar las ideas planteadas en este proyecto.

- Realizar un estudio de otras posibles interferencias no intencionadas que puedan darse en un escenario como el aquí planteado.

- Realizar un estudio de las posibles interferencias naturales que puedan existir y su impacto en el sistema (radiación solar, impacto de un rayo en el avión, etc.)

- Construir un banco de pruebas donde se pueda simular el enlace así como todos los parámetros del sistema, con el fin de testear el comportamiento real.

BIBLIOGRAFÍA

[1] NATO, "Nato Glossary of terms and definitios (English and French)," North Atlantic Treaty Organization, APP-6 2008.

[2] Richard Poisel, *Modern Communication Jamming Principles and Techniques*, 2nd ed.: Artech House, 2011.

[3] Liebherr-Aerospace Lindenberg GmbH, Specification for Aileron ACE.

[4] Oroitz Elgezabal Gómez, "Fly-by-Wireless (FBWSS): Benefits, risks and technical challenges," in *CANEUS Fly-by-Wireless Workshop*, Orono, ME, USA, Aug. 2010.

[5] Thorben Kupke, "Funkbasierte energieautarke Kommunikation für Eisenbahngüterzüge," Technischen Universität Carolo-Wilhelmina, Braunschweig, 2007.

[6] Bernard Sklar, *Digital Communications: Fundamentals and applications*, 2nd ed.: Prentice Hall.

[8] Yunxin Li, "Blind SNR estimation for OFDM signals," NICTA, Australia,.

[7] IEEE, "IEEE Std. 802.11a," IEEE, 1999.

[9] Airbus. www.aribus.com. [Online]. http://www.airbus.com/aircraftfamilies/passengeraircraft/a380family/a380-800/specifications/

[10] Ramjee Prasad, *OFDM for wireless communications systems*.: Artech House, 2004.

[11] T. Charles Clancy, "Efficient OFDM Denial: Pilot Jamming and Pilot Nulling," IEEE, 2011.

[12] Jun Luo, Jean H. Andrian, and Chi Zhou, "Bit Error Rate Analysis of Jamming for OFDM Systems," IEEE, 2007.

[13] Chirag S. Patel, Gordon L. Stüber, and Thomas G. Pratt, "Analysis of OFDM/MC-CDMA under imperfect channel estimation and jamming,".

[14] Nektarios Moraitis, Philip Constantinou, Fernando Perez Fontan, and Pavel Valtr, "Propagation Measurements inside Different Civil Aircrafts and Comparison with EM Techniques,".

[15] Alexandros Kaouris, Matthaios Zaras, Maria Revithi, Nektarios Moraitis, and

Constantinou Philip, "Propagation Measurements inside a B737 Aircraft for In-Cabin Wireless Networks," Mobile Radiocommunications Laboratory, Natiaonal Technical University of Athens,.

[16] Núria Riera Díaz and Juan E. Jiménez Esquitino, "Wideband Channel Characterization for Wireless Communications inside a Short Haul Aircraft," German Aerospace Center (DLR), Oberpfaffenhofen, Germany,.

[18] International air transport association. www.iata.org. [Online]. http://www.iata.org/whatwedo/passenger/passenger_baggage/Pages/check_bag.aspx

[17] Jorge Castiñeira Moreira and Patrick Guy Farrel, *Essentials of Error-Control Coding*.: John Wiley & Sons, Ltd, 2006.

[19] Richard van Nee and Ramjee Prasad, *OFDM for wireless multimedia communications*.: Artech House.

[20] Nathan Yee, Jean-Paul Linnartz, and Fettweis Gerhard, "Multi-Carrier CDMA in indoor wireless radio networks," in *The Fourth International Symposium on Personal, Indoor and Mobile Radio Communications*, Yokohama, Japan, 1993.

[21] Fuqin Xiong, *Digital modulation techniques*, 2nd ed.: Artech House, 2006.

[22] David Adamy, *EW 101: A first course in electronic warfare*.: Artech House, 2000.

[23] C. Fielding and R. Luckner, "Industrial considerations for flight control Flight Control Systems," in *Practical issues in design and implementation*, Roger W. Pratt, Ed., 2000.

[24] Christian Gehrmann, Joakim Persson, and Ben Smeets, *Bluetooth Security*.: Artech House, 2004.

[25] Adrian Graham, *Communications, Radar and Electronic Warfare*.: Wiley and Sons, 2011.

[26] Allan Seabridge Ian Moir, *Aircraft systems: mechanical, electrical and avionics subsystem integration*, Second edition ed.: Professional engineering publishing.

[28] Cho Yong Soo, Kim Jaekwon, Yang Won Young, and Kang Chung G., *MIMO-OFDM wireless communications with MATLAB*.: John Wiley & Sons (Asia), 2010.

[27] Richard A. Poisel, *Introduction to communication electronic warfare systems*.: Artech House, Inc, 2002.

[29] MathWorks, MATLab. Help Communication Toolbox. [Online]. http://www.mathworks.de/help/toolbox/comm/ug/bsvzixi.html#bsvziy0

[30] International air transport asociation. www.iata.org. [Online]. http://www.iata.org/whatwedo/passenger/passenger_baggage/Pages/check_bag.aspx