UNIVERSIDAD AUTONOMA DE MADRID

ESCUELA POLITECNICA SUPERIOR

PROYECTO FIN DE CARRERA

APLICACIÓN DE TÉCNICAS ANTI-*JAMMING* A UN SISTEMA DE COMUNICACIONES CONVENCIONAL PARA SU EXPLOTACIÓN EN ENTORNOS TÁCTICOS

Juan Francisco Díaz Bejarano

OCTUBRE 2012

APLICACIÓN DE TÉCNICAS ANTI-*JAMMING* A UN SISTEMA DE COMUNICACIONES CONVENCIONAL PARA SU EXPLOTACIÓN EN ENTORNOS TÁCTICOS

AUTOR: Juan Francisco Díaz Bejarano
TUTOR: Alberto Quintana Ocaña
PONENTE: Jorge Alfonso Ruiz Cruz

Dpto. de Ingeniería de Telecomunicación
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Octubre de 2012

Agradecimientos

Sin duda el primer lugar de esta lista de agradecimientos es para mi tutor Alberto que me propuso la elaboración de este proyecto, y no sólo me guió en su elaboración, sino también en los primeros pasos de mi carrera laboral. Quisiera agradecer también a mis compañeros de trabajo Antonio y Javi, auténticos gurús de los sistemas WiMAX que supieron responder a todas mis preguntas.

Como este proyecto no es sino el último paso de una larga caminata, no puedo dejar de recordar a todos los compañeros que he tenido durante la carrera. Entendiendo como carrera no unas horas en un centro de estudios sino una etapa de mi vida. Desde 2005 nos han unido incontables horas de clases, prácticas y estudio en biblioteca. Pero eso además conlleva innumerables historias, viajes y anécdotas dentro y fuera de la universidad.

Y como en las incontables horas de clases y prácticas no estábamos solos y no somos autodidactas, también he de agradecer a todos los profesores que he tenido durante la carrera. Además de la materia que imparten, de todos hemos aprendido algo. Quisiera agradecer a mi ponente, Jorge, cuyas asignaturas (las que impartía mientras yo estudiaba) formaron una importante base para el campo donde he comenzado mi experiencia laboral. Por ese motivo solicité que fuera el ponente de este proyecto.

“Es de bien nacido ser agradecido”. Suponiendo que con este dicho con “bien nacido” se quiera decir “bien educado”, me sirve para recordar en este punto a toda mi familia. En especial a mis padres que me dieron todo el apoyo necesario para que estudiara esta carrera a y me tuvieron becado a distancia (separados por un océano). También el resto de mi familia, hermanas, tíos y abuelos, que no dejaron de preocuparse e interesarse por mis estudios. También ellos agradecerán que termine este proyecto y cierre esta etapa.

Juan F. Díaz Bejarano

RESUMEN

El presente proyecto es un estudio de la aplicación de técnicas anti-*jamming* a un sistema de comunicaciones convencional para su explotación en entornos tácticos con presencia de *jammers*. Dicho sistema es elegido de acuerdo a su posible aplicabilidad a los entornos mencionados, así como su capacidad de incorporar técnicas y estrategias anti-*jamming*.

El proyecto se inicia con un estudio de los entornos tácticos y los distintos tipos de *jammer* que pueden aparecer en ellos. Tras ello se presenta y describe el sistema de comunicaciones en cuestión, haciendo hincapié en las áreas relacionadas con la aplicabilidad de técnicas anti-*jamming*.

El objetivo principal es el estudio del comportamiento del sistema en entornos tácticos con *jamming* y su posible mejora para dichos entornos utilizando técnicas anti-*jamming*. Para ello se realizarán simulaciones en distintos escenarios con una versión simplificada del sistema en la que se tendrá en cuenta únicamente la capa física.

PALABRAS CLAVE

Jamming, anti-*jamming*, entornos tácticos, capa física, sistema de comunicaciones, WiMAX, frequency hopping

ABSTRACT

The present project is a study of the application of anti-*jamming* techniques to a communications system in order to adapt it to tactical environments with *jamming*. The system is selected according to its usefulness in these environments, along with its flexibility to incorporate different anti-*jamming* techniques and strategies.

The project starts with the study of tactical environments and the different types of *jammers* that may be present in them. After that, the actual communications system selected is described, focusing in the areas related to the application of anti-*jamming* techniques.

The principal objective is the study of the performance of the system in tactical environments with *jamming* and its possible improvement applying anti-*jamming* strategies. To validate the decisions taken, there will be simulations of various scenarios with a simplified model of the system. This simplified model must focus in the physical layer of the system.

KEY WORDS

Jamming, anti-*jamming*, tactical environment, physical layer, communications system, WiMAX, frequency hopping

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE ECUACIONES

1 Introducción

1.1 Motivación

La demanda actual de los cuerpos de seguridad y defensa en el ámbito de las comunicaciones tiene una tendencia a la reutilización de sistemas de comunicaciones civiles. Sin embargo, los entornos en los que pueden operar los cuerpos de seguridad y defensa difieren de los escenarios típicos de los sistemas civiles convencionales. Por ello, es necesaria una fase de adaptación del sistema para su explotación en entornos tácticos.

A pesar de la necesidad de introducir modificaciones para adaptar el sistema a las necesidades de los cuerpos de seguridad y defensa, el coste se ve reducido frente al desarrollo de un sistema de comunicaciones a medida desde cero. Asimismo, el tiempo de comercialización (*Time to market*) se reduce en comparación con un desarrollo completo, lo cual es de gran importancia tanto para el usuario (los cuerpos de seguridad y defensa) como para la empresa proveedora del sistema.

Una de las complejidades de los entornos tácticos radica en la posible presencia de elementos que intencionadamente tratan de perturbar la comunicación (*jammers*) evitando la correcta recuperación de la señal en el receptor. Los sistemas que se despliegan en un entorno de tales características deben tener robustez frente a dichos ataques. Existen multitud de formas de atacar las comunicaciones mediante *jamming*, pero los mecanismos más sencillos pueden ser suficientes para cualquier sistema de comunicaciones convencional. Igualmente, existen técnicas para contrarrestar el efecto del *jamming*.

Estos elementos crean un interesante marco para analizar la viabilidad de adaptar un sistema de comunicaciones convencional aplicando técnicas y mecanismos que permitan reducir su vulnerabilidad frente a ataques de *jamming*.

1.2 Objetivos

El objetivo principal de este proyecto es analizar la adaptación de un sistema de comunicaciones convencional para su explotación en un entorno táctico. De cara a alcanzar este objetivo principal, el proyecto se divide en dos partes u objetivos parciales:

1) Analizar la vulnerabilidad de los sistemas de comunicaciones convencionales en entornos con interferencia como puede ser un entorno táctico con *jamming*.
2) Demostrar cómo la aplicación de sencillas técnicas anti-*jamming* pueden mejorar las prestaciones en estos sistemas en entornos hostiles.

Para cumplir este objetivo, será necesario identificar y caracterizar el entorno en el que se desplegará el sistema. Se presentarán y describirán los distintos tipos de *jammer* existentes, eligiendo aquellos más apropiados para crear ciertos escenarios de simulación.

El siguiente paso es la elección de un sistema de comunicaciones apropiado para su adaptación a entornos tácticos. Asimismo, el sistema elegido deberá ser compatible con las necesidades operativas de un entorno táctico.

Se modelará el sistema de comunicaciones seleccionado usando la herramienta Simulink permitiendo la parametrización de distintos escenarios tácticos que pondrán a prueba las prestaciones del sistema.

Con la información obtenida de las simulaciones se valorará la necesidad de aplicar técnicas de protección frente a *jamming*. Igualmente se simulará y analizará el impacto en las prestaciones de la introducción de dichas medidas.

Con la realización de este proyecto se pretende mostrar el funcionamiento de estas técnicas, su aplicabilidad a sistemas ya existentes, y su eficiencia en distintos escenarios de *jamming*.

1.3 Organización de la memoria

La memoria está organizada de modo que se presente primero información de contexto que ayuda a plantear el análisis que lleva a cumplir los objetivos (capítulos 2 y 3). Con esta información de contexto se puede plantear una metodología, hipótesis y herramientas para realizar el estudio. También los resultados se presentan de forma separada para poder analizarlos frente a los dos objetivos definidos en la sección anterior (capítulos 4 y 5). Al final de la memoria se presentan las conclusiones del estudio frente al objetivo principal del proyecto (capítulo 6) así como diversos anexos que complementan información presentada a lo largo del documento.

La memoria consta de los siguientes capítulos:

- **Capítulo 1:** Introducción.
- **Capítulo 2:** Definición de entornos tácticos con *jamming*.
- **Capítulo 3:** Identificación y descripción del sistema de comunicaciones bajo estudio.
- **Capítulo 4:** Análisis de prestaciones en entornos tácticos.
- **Capítulo 5:** Análisis de prestaciones con medidas anti-*jamming*.
- **Capítulo 6:** Conclusiones y trabajo futuro.
- **Capítulo 7:** Referencias.
- **Capítulo 8:** Glosario.
- **Capítulo 9:** Anexos e información adicional.

2 Definición de Entornos Tácticos con *Jamming*

El objetivo de esta sección es presentar las características que presenta un entorno táctico. En primer lugar se introducen las características generales, centrándose después en la definición de los tipos de *jamming* que se pueden encontrar. Cabe recordar, que el objetivo del proyecto es el estudio del *jamming* y técnicas anti-*jamming* (AJ) a nivel de capa física, referida de ahora en adelante como PHY.

2.1 Características Generales

2.1.1 Características del despliegue

Se puede definir entorno táctico como el conjunto de escenarios de despliegue u operación de un sistema con determinadas características propias que lo distinguen de otros entornos como, por ejemplo, el entorno civil o comercial. Esto quiere decir que tienen ciertas limitaciones, condiciones y parámetros determinados. A continuación se presentan algunas de las características que definen un entorno táctico. Sin embargo, sólo una parte de ellas serán tenidas en cuenta para el desarrollo de este proyecto.

2.1.2 Servicios y aplicaciones soportados

Los sistemas desplegados en entornos tácticos tienen que dar soporte a ciertos tipos de servicios y aplicaciones. Estos servicios tienen distintas características de tasa de datos, latencia, modelado de tráfico, etc. A continuación se muestra una lista con los servicios típicos que puede requerir un sistema en un entorno táctico:

- *Streaming* de vídeo.
- Mensajería instantánea.
- Servicios *web*.
- Transferencia de datos de mando y control.
- Transferencia de datos críticos en tiempo real.
- VoIP.
- Servicios de voz PTT (*Push to talk*).
- Transferencia de imágenes y mapas de alta resolución.
- Transferencia de datos genéricos (ficheros, mediciones, etc.).

La disponibilidad de los servicios dependerá directamente de las condiciones del entorno, ya que para poder proporcionar cada uno de los servicios se requiere que los enlaces proporcionen unas ciertas características de ancho de banda, tasa de error y retardo.

2.1.3 Movilidad

El sistema deberá proporcionar soporte a la movilidad tanto para las estaciones de usuario como para las estaciones base, sobretodo cuando éstas se encuentran en los niveles bajos de la jerarquía (nodos con gran movilidad). Los nodos pueden estar embarcados en vehículos en movimiento, hecho que se debe tener en cuenta en términos de velocidad y efecto Doppler.

2.1.4 Capacidades de Seguridad

En este tipo de escenarios y despliegues, uno de los aspectos a los que hay que prestar mayor atención y resulta de suma importancia son las capacidades de seguridad que debe presentar el sistema. Estas capacidades pueden ser aplicables a distintos niveles, aunque el caso relevante para este documento es a nivel PHY. TRANSEC se basa en la aplicación de medidas que tienen el objetivo de proteger a las transmisiones de la interceptación de la información que contienen. Los objetivos principales de estas medidas son garantizar que en las transmisiones se tiene una baja probabilidad de interceptación (LPI, *Low Probability of Interception*), una baja probabilidad de detección (LPD, *Low Probability of Detection*) y alta capacidad de resistencia al *jamming* (capacidad AJ o contramedidas electrónicas). En lo que respecta a la capacidad *AJ*, también se puede asimilar como una capacidad de robustez que se tratan en el siguiente punto.

El TRANSEC requiere la disponibilidad de un subsistema CRIPTO donde se encuentran los mecanismos de seguridad (generación se secuencias pseudoaleatorias, gestión de claves, etc.).

2.1.5 Robustez

El sistema debe garantizar que es robusto ante las interferencias intencionadas (*jamming*) que pueden ser provocadas por terceros. Para ello, se utilizan técnicas y estrategias AJ. Estas técnicas pueden estar presentes a distintos niveles OSI, como en los protocolos o en la propia PHY. En la sección 2.2 se presentan los distintos tipos de *jammers* que pueden estar presentes en un entorno táctico.

2.1.6 Bandas de frecuencia objetivo

Los sistemas de comunicaciones actualmente empleados se agrupan en una serie de bandas militares dispares. Existen sistemas en bandas de HF (de 3 a 30 MHz), de VHF (de 30 a 300 MHz) o incluso en bandas de UHF (de 300 MHz a 3 GHz).

Sin embargo, el objetivo planteado por los operativos es migrarse a medio/corto plazo a bandas OTAN. De lo cual se puede deducir que el nuevo sistema debe estar encuadrado dentro de una banda OTAN, en concreto de la banda NATO IV que va desde los 4.4 GHz a los 5 GHz. Esta es una banda reservada para uso militar y que por ahora se puede considerar que no tiene restricciones en cuanto a potencia emitida.

Aparte de la banda NATO IV, también podría resultar de interés realizar modos del sistema que pudieran ir sobre la banda de frecuencias NATO II con un margen de frecuencias que va desde los 225 MHz a los 400 MHz, y que está siendo la banda objetivo para nuevos sistemas de comunicaciones militares desarrollados en la actualidad. Dicha banda presenta una serie de restricciones en relación a la banda NATO IV, como por ejemplo la reducción de ancho de banda de canalización, pero se mantiene como posible opción debido a lo comentado con anterioridad y a la posibilidad de incrementar considerablemente el alcance de las comunicaciones.

2.1.7 Capacidad de cobertura

Una cobertura apropiada para el sistema de comunicaciones sería de entorno a los 20 Km.

No obstante, para cubrir ciertos casos especiales, el sistema debería ser diseñado para que en determinadas condiciones se pueda llegar a alcanzar una distancia de hasta 50 Km o incluso de hasta 100 Km, ya que puede haber unidades subordinadas a dichas distancias.

2.2 Identificación y caracterización de jammers

El *jamming* es la interferencia o perturbación intencionada de una comunicación con el fin de evitar o al menos entorpecer el intercambio de información. Para ello, se introduce energía en el receptor, en el momento en el que se va a recibir la señal objetivo. Por lo tanto, lo que se consigue es disminuir la SIR en recepción, haciendo que se cometan errores al recuperar la información. La energía necesaria para evitar o perjudicar significativamente la comunicación depende de la naturaleza de la señal objetivo, la señal de *jamming* y las técnicas o estrategias implementadas por el receptor para añadir robustez a la comunicación.

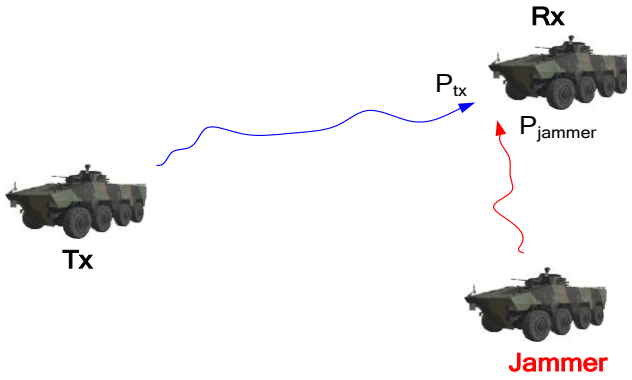


Figura 2-1: Disposición de un *jammer* en la comunicación

Existen muchas estrategias y técnicas que emplear contra un sistema de comunicaciones. Algunas son más efectivas que otras, y el hecho de que una determinada funcione correctamente depende del tipo de AJ empleado por el sistema. La clasificación de estrategias de *jamming* empleada en este documento consiste en: el tipo de modulación o forma de onda de la señal transmitida, el patrón de tiempo que utiliza el *jammer* en su transmisión y en como la potencia disponible del *jammer* se distribuye con la frecuencia [1].

2.2.1 Identificación por forma de onda interferente

Una posible clasificación de los distintos tipos de *jammer* es por la forma de onda de la señal interferente. La interferencia se reduce a introducir energía en la banda del espectro que utiliza la señal objetivo, teniendo en cuenta que la forma o distribución de esta energía puede ser más o menos eficiente o eficaz en función de las características de la transmisión. Según esta división, los *jammers* pueden ser:

- Ruido blanco

  La señal de *jamming* tiene forma de ruido aleatorio gaussiano y puede ocupar todo el ancho de banda de la señal a interferir o sólo una parte de él. No siempre es necesario atacar la señal completa para interrumpir de manera eficiente la comunicación [2]. La intención es elevar el nivel de ruido en el receptor para perturbar la comunicación. Es muy útil cuando no se tiene mucha información del tipo de señal a interferir. La complejidad de esta forma de onda interferente es mínima.

- Tono / Multitono

Esta estrategia consiste en colocar estratégicamente uno, single-tone (ST), o varios, multiple-tone (MT), tonos a lo largo del espectro que ocupa la señal objetivo. La eficiencia de esta técnica reside en la elección de lugar del espectro donde se coloquen los pulsos así como su número. Es por eso que se requiere estudiar y conocer la señal objetivo. Así mismo, si la potencia de *jammer* no es muy alta, se requiere que la fase del tono sea acorde con la transmisión para mayor eficacia [1].
El ST *jamming* es aplicable de forma efectiva a objetivos de banda muy estrecha y que no cambian de frecuencia.
En el caso de MT si los tonos se colocan en canales contiguos, el resultado será similar al de ruido de banda parcial, esta técnica con MT en particular se conoce como *comb jamming* [2].

- Repetidores (i.e: misma forma de onda a interferir)

Estos *jammers*, en lugar de generar ruido aleatorio o pulsos, utilizan replicas de la señal objetivo para interferir la comunicación. Se escucha la señal objetivo y se generan señales idénticas o de la misma naturaleza. El principal problema de estos *jammers* es que se requiere conocer en cierta medida como es la señal objetivo para poder recibirla y generar señales de la misma naturaleza de forma eficaz.

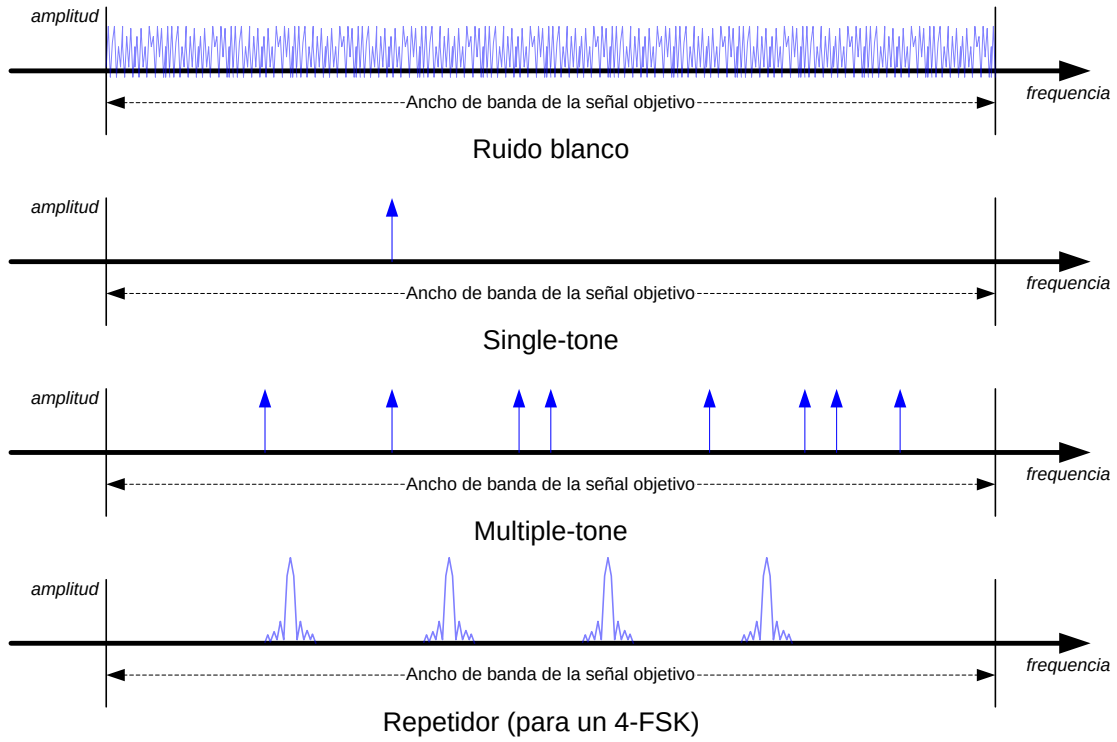


Figura 2-2: *Jammers* por forma de onda interferente

2.2.2 Identificación por el patrón tiempo usado en la interferencia

Otra posible división de los tipos de *jammer* es por su patrón de interferencia en el tiempo. Es decir, si interfieren continuamente o sólo en determinados momentos. Interferir incluso cuando la señal objetivo está en silencio puede provocar que se detecte fácilmente la presencia de *jammers*.

- Continuos

Este tipo de *jammers*, agrupa a todos aquellos que se mantienen constantes en el tiempo. Es decir, una vez conectados no dejan de emitir la señal interferente hasta que se desconectan. Pueden resultar ineficientes en el uso de la potencia ya que actúan incluso durante los posibles silencios de la señal objetivo.

- Pulsados

Esta estrategia consiste en no transmitir señal interferente durante todo el tiempo, sino en determinados momentos en los que se considera más necesario o eficaz. Pulsos de muy corta duración tienen un gran ancho de banda y por tanto son similares a *jamming* de ancho de banda total (descritos en el siguiente apartado). La eficiencia de potencia puede ser mucho mayor, pero el éxito depende en gran medida del correcto diseño del ciclo de trabajo. Es decir, se requiere conocer los instantes en los que se transmitirá información sensible o importante para actuar en esos momentos [1].

- Followers / Repetidores

Un *jammer* follower intenta localizar la frecuencia e instante en el que el objetivo transmite, identificar la señal como objetivo e interferirla. Este *jamming* puede ser en forma de ruido blanco, tonos o repetición (Ver 2.2.1). El problema de esta técnica reside en que primero se localiza la señal objetivo y después se intenta interferir; sin embargo, para cuando la señal de *jamming* llega al receptor, es posible que ya se haya entregado de forma correcta la información.

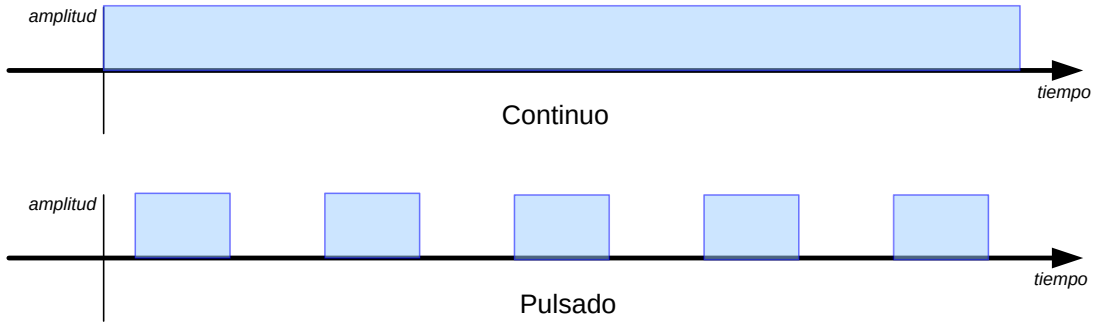


Figura 2-3: *Jammers* por tiempo usado en la interferencia

2.2.3 Por el ancho de banda cubierto (i.e: patrón frecuencia)

La tercera clasificación de *jammers* propuesta atiende al ancho de banda que cubren las señales interferentes. Cabe destacar que a mayor ancho de banda, se requiere mayor potencia para tener la misma amplitud de señal interferente. Es decir, si no aumenta la potencia y se amplía el ancho de banda cubierto, aumenta la SIR (*Signal to Interference Ratio*).

- Banda total

También conocido como ruido de banda ancha o BBN (*Broadband noise*), introduce energía a través de todo el espectro de frecuencias en el que opera la señal a interferir. Este tipo de *jamming* es aplicable a cualquier tipo de señal, sin embargo, el principal inconveniente es que la potencia es esparcida por un espectro ancho. Debido a esto, el

nivel de potencia de *jamming* es muy bajo (a menos que se use una potencia desmesurada) [2].
En esencia, este tipo de *jamming* eleva el nivel de ruido en el receptor, creando un entorno de ruido grande en el sistema objetivo. El ruido es el enemigo de cualquier sistema de comunicaciones, y si aumenta hace la comunicación más difícil (disminuyendo su rango, aumentando su BER o incluso negándola completamente).

- Banda parcial

Se conoce también como PBN (*Partial band noise*). En este caso, se introduce energía a través de una parte específica del espectro, cubriendo solamente algunos canales (contiguos o no). Este tipo de *jamming* desperdicia menos potencia, ya que no siempre se requiere interferir todo el espectro, sino ciertos lugares donde importa. Por ejemplo, si se interfiere la parte del espectro donde se localiza la información de sincronización o control se puede evitar por completo el éxito de la comunicación [2].

- Barrido

Se puede considerar una estrategia complementaria al *jamming* por PBN. Consiste en introducir ruido en una parte del espectro e ir desplazando dicha señal de ruido por todo el espectro que ocupe la señal objetivo. La principal ventaja frente al *jamming* por BBN es que optimiza el uso de la potencia. Esto se debe a que no se tiene que esparcir la potencia por todo el ancho del espectro, sino que se utiliza la máxima potencia en determinado lugar y determinado momento [2] . En cada instante, se interfiere una pequeña parte del espectro, pero debido al barrido, en un corto periodo de tiempo se puede abarcar un amplio rango de frecuencias. Esta estrategia permite además seleccionar solo las áreas del espectro por la que se hace el barrido, dejando aquellas que no usa el enemigo o pertenecen a comunicaciones amigas Esta técnica es especialmente eficiente contra sistemas con FH si se tiene una señal interferente de ancho de banda igual al que tienen los dwells de la señal objetivo [1].

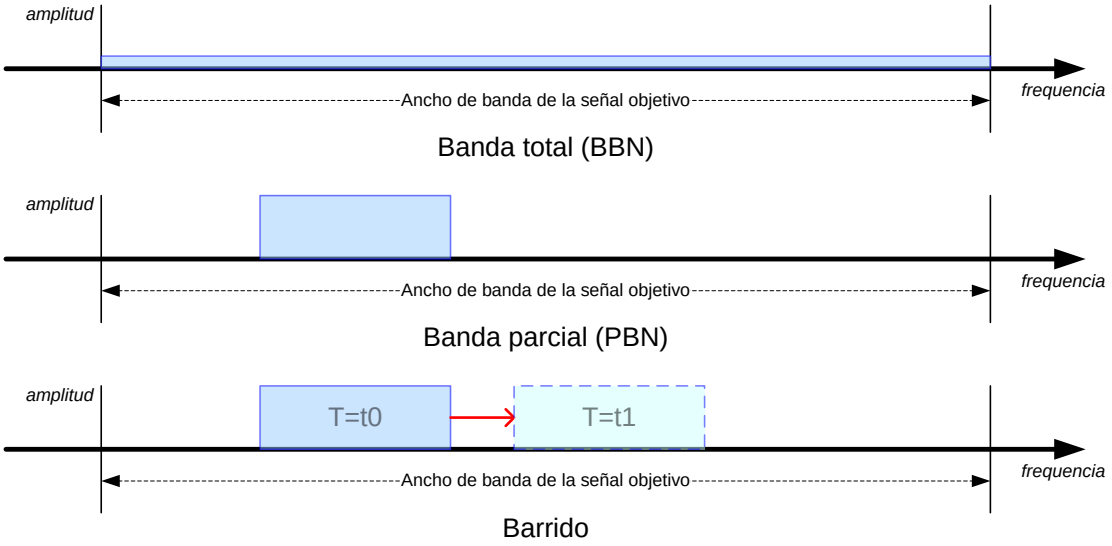


Figura 2-4: *Jammers* por ancho de banda cubierto

3 Identificación y descripción del sistema de comunicaciones bajo estudio

El sistema de comunicaciones elegido para su portabilidad a un entorno táctico es el WiMAX. A continuación se presenta la descripción general del sistema, así como la descripción de la capa física, objeto final del estudio.

3.1 Descripción general y aplicación

El desarrollo de las telecomunicaciones se está orientando en los últimos años a un uso intensivo de sistemas de banda ancha con altos niveles de calidad. Esto se consigue mediante el desarrollo de tecnologías de alta capacidad de transmisión, entre los cuales podemos destacar el xDSL (x *Digital Subscriber Line*), la fibra óptica o el cable coaxial, sistemas cableados que tienen un alto coste de instalación, construcción y puesta en servicio. Adicionalmente, el desarrollo de estos medios de transmisión en zonas rurales y de interés social, representan inversiones de difícil recuperación debido a las características inherentes de las demandas.

Frente a esta situación, y a otras limitaciones tecnológicas y topográficas, se han buscado alternativas inalámbricas que permitan un despliegue rápido de la infraestructura, mayor predictibilidad de la inversión en función de los lugares donde se instalan, así como menores costes de operación y mantenimiento. Dentro de este entorno se desarrolla la tecnología **WiMAX** (*Worldwide Interoperability for Microwave Access*) con el objetivo de dar cobertura a distintos tipos de usuario y ofrecer una alternativa competitiva a los medios de accesos de banda ancha por cable, introduciendo nuevos y mejores servicios de telecomunicaciones dentro del concepto "*Triple Play*" (voz, imagen y datos).

Actualmente WiMAX está siendo desarrollado y promovido por un gran consorcio de industrias que certifican la compatibilidad entre distintos equipos que utilizan esta tecnología, esta organización se conoce con el nombre de WiMAX Forum.

WiMAX está basado en el estándar para redes WMAN (*Wireless Metropolitan Area Network*) desarrollado por el IEEE 802.16, y adoptado por el IEEE y el grupo ETSI HIPERMAN. El grupo IEEE 802.16 fue formado en 1998 para desarrollar un estándar de banda ancha inalámbrica. Inicialmente, el grupo se centró en el desarrollo de un sistema de banda ancha LOS (*Line-Of-Sight*) basado en punto multipunto en una banda de onda milimétrica entre 10GHz y 66GHz. El estándar resultante 802.16 fue completado en diciembre del 2001, soportando una capa física (PHY) de una única portadora con una capa de control acceso al medio (MAC) basada en TDM (*Time Division Multiplexed*). Muchos de los conceptos referentes a la capa MAC fueron adaptados a *wireless* desde el estándar de modem cable DOCSIS (*Data Over Cable Service Interface Specification*).

Posteriormente, el IEEE 802.16 realizó una corrección del estándar para incluir aplicaciones NLOS (*Non-Line-Of-Sight*) en la banda de 2GHz y 11GHz, usando una capa física basada en OFDM (*Orthogonal Frecuency Division Multiplexing*) incluyéndose también soporte para OFDMA (*Orthogonal Frecuency Division Access*) en la capa MAC. Las siguientes revisiones dieron lugar a un nuevo estándar en el 2004, IEEE 802.16-2004, que remplazó a todas las versiones anteriores y estableció las bases de la primera solución WiMAX. Estas soluciones tenían como objetivo aplicaciones fijas, *fixed WiMAX*. En

diciembre del 2005, se completó y aprobó el IEEE 802.16e-2005 que establece las bases para las soluciones WiMAX para aplicaciones móviles, *mobile WiMAX*, y que es el objeto del presente documento.

Estos estándares fueron desarrollados para encajar en gran variedad de aplicaciones y escenarios, y ofrecen múltiples elecciones de diseño. En realidad, se podría decir que el IEEE 802.16 es una colección de estándares. Para realizar las elecciones de diseño, por razones de interoperabilidad, el WiMAX Forum especifica un número limitado de **perfiles de sistemas** y **perfiles de certificación**. Un perfil del sistema define el conjunto de características obligatorias y opcionales de la capa física y MAC para los estándares IEEE 802.16-2004 o IEEE 802.16e-2005. Actualmente, el WiMAX Forum tiene dos perfiles de sistema distintos; uno basado en el IEEE 802.16-2004, OFDM PHY, llamado *Fixed System Profile*, y el otro basado en IEEE 802.16e-205, escalable OFDMA PHY, llamado *Mobility System Profile*. Un perfil de certificación se define como una instancia particular de un perfil del sistema donde se especifican la frecuencia de operación, el ancho de banda del canal y el modo de duplexado.

El WiMAX Forum ha definido cinco perfiles fijos de certificación y catorce perfiles de certificación móviles empleando todos como capa física OFDMA y considerando, al menos inicialmente, que todos los perfiles móviles usarán una MAC punto-multipunto. Debemos apuntar que todos los perfiles candidatos están basados en TDD, aunque en un futuro los perfiles FDD pueden ser más necesarios para cumplir con las regulaciones complementarias y los requerimientos de coexistencia de interoperadores en ciertas bandas.

Dentro de los catorce perfiles mencionados con anterioridad, en este proyecto se seleccionará uno de los mismos para la validación de una implementación de la capa física OFDMA.

Las características que proporcionan a WiMAX una gran flexibilidad en las opciones de implementación son las que se indican a continuación:

- **Capa física basada en OFDM:** la capa física WiMAX (PHY) está basada en OFDM *(Ortogonal Frequency Division Multiplexing)*, un esquema que ofrece resistencia al multitrayecto y permite operar en condiciones NLOS.
- **Alta velocidad de transmisión de datos:** la velocidad de transmisión pico PHY puede llegar a 74 Mbps cuando opera a 20 MHz de ancho de banda. Usando un espectro de 10 MHz bajo un esquema TDD con un *ratio downlink-uplink* de 3:1 llega a 25 Mbps en el *downlink* y 6.7 Mbps en el *uplink*. Estas tasas se consiguen cuando se usa una modulación 64-QAM con un código de corrección de errores de tasa 5/6. Con buenas condiciones de señal, se podrían incluso conseguir mejores resultados usando multiplexación espacial y múltiples antenas.
- **Velocidad de transmisión y ancho de banda escalable:** la arquitectura de la capa física permite escalar rápidamente la velocidad de transmisión con el ancho de banda. Esta escalabilidad se soporta en el modo OFDMA, donde el tamaño de la FFT (*Fast Fourier Transform*) puede ser escogido basándose en el ancho de banda disponible. Por ejemplo, un sistema WiMAX puede usar FFTs de tamaño 128, 512 o 1.024 según sea el ancho de banda del canal de 1.25 MHz, 5 MHz o 10 MHz, respectivamente. Esta escalabilidad puede realizarse dinámicamente para soportar

la navegación del usuario sobre distintas redes que puedan tener distintas asignaciones de ancho de banda.

- **Soporta AMC:** WiMAX soporta un gran número de modulaciones y de esquemas de codificación FEC (*Forward Error Correction*), y permite cambiar el esquema para cada usuario o para cada trama, basándose en las condiciones del canal. AMC (*Adaptive Modulation and Coding*) es un mecanismo efectivo para maximizar el rendimiento en un canal variante en tiempo. El algoritmo ofrece al usuario, la modulación y el esquema de codificación más alto que puede ser admitido según la relación señal a ruido y el ratio de interferencia en el receptor, y la máxima velocidad de transmisión de datos que pueda ser soportada en sus respectivos enlaces.
- **Retransmisiones en la capa de enlace:** para conexiones que requieren aumentar la fiabilidad, WiMAX soporta ARQ en la capa de enlace, esto implica que cada paquete transmitido debe ser reconocido por el receptor, asumiéndose que se ha perdido y necesita ser retransmitido si el receptor no lo reconoce. WiMAX soporta opcionalmente *Hybrid-ARQ*, que es una combinación eficaz entre FEC y ARQ.
- **Soporte para TDD, FDD y *Half-duplex* FDD:** los estándares IEEE 802.16-2004 y IEEE 802.16e-2005 soportan TDD (*Time Division Duplexing*), FDD (*Frequency Division Duplexing*) y *Halfduplex* FDD, permitiendo éste último implementaciones de bajo coste. TDD es favorable para la mayoría de las implementaciones por su flexibilidad en la elección de velocidades de transmisión de datos en el *downlink* y en el *uplink*, su habilidad para explotar la reciprocidad del canal y su menor complejidad en el diseño del transceptor. Todos los perfiles iniciales de WiMAX están basados en TDD excepto dos perfiles fijos en la banda de frecuencia de 3.5 GHz.
- **Asignación de recursos flexible y dinámica:** la asignación de recursos en el *uplink* y el *downlink* están controlados por un planificador en la estación base. La capacidad a repartir es compartida entre múltiples usuarios en base a las demandas, usando un esquema de ráfagas TDM (*Time Division Multiplexing*). Cuando se usa el modo OFDMA-PHY, la multiplexación se hace en la dimensión de frecuencia, asignando distintos subconjuntos de subportadoras OFDM a distintos usuarios. De forma adicional, los recursos pueden ser asignados en el dominio espacial y cuando se utilizan los sistemas opcionales de antenas avanzadas (AAS). En conclusión, WiMAX permite asignar los recursos de ancho de banda en tiempo, frecuencia y espacio, y tiene un mecanismo flexible para transmitir la información de asignación de recursos trama a trama.
- **Soporte para técnicas avanzadas de antenas:** WiMAX posee gran cantidad de ideas incorporadas en el diseño de la capa física, que permiten el uso de técnicas multi-antena como el *beamforming*, la codificación espacio-temporal y la multiplexación espacial. Estos esquemas pueden ser usados para mejorar la capacidad general del sistema y la eficiencia espectral mediante el despliegue de múltiples antenas en transmisión y/o en recepción.
- **Calidad de servicio:** la capa de acceso al medio de WiMAX está diseñada para soportar un gran número de usuarios, con múltiples conexiones por terminal, cada una con sus propios requisitos de QoS *(Quality-of-Service)*. La arquitectura de la capa está diseñada para soportar distintas aplicaciones como voz o servicios multimedia y se ofrece soporte para una tasa de bit constante o variable, flujos de tráfico en tiempo real o no, y tráfico *Best-Effort*.
- **Seguridad:** el estándar incluye el estado del arte de métodos que aseguran al usuario la privacidad de sus datos y previenen de accesos no autorizados. La

seguridad es manejada por una primera subcapa dentro de la capa WiMAX MAC. Los principales aspectos de seguridad WiMAX son los siguientes:

  - Soporte para privacidad: los datos de los usuarios son cifrados usando esquemas criptográficos como son AES (*Advanced Encryption Standard*) y 3DES (*Triple Data Encryption Standard*). La mayoría de las implementaciones harán uso probablemente AES, al ser éste el nuevo estándar de cifrado aprobado conforme al FIPS (*Federal Information Processing Standard*) y resultar sencilla su implementación. La clave de 128 o 256 bits usada para obtener la información cifrada se genera durante la fase de autenticación y se actualiza periódicamente para incrementar la protección a los datos.
  - Autenticación usuario/dispositivo: WiMAX proporciona formas flexibles de autenticar estaciones base y usuarios para prevenir el acceso no autorizado. El *framework* de autenticación está basado en el EAP IETF (*Internet Engineering Task Force*), que soporta credenciales como *login/password*, certificados digitales, y tarjetas inteligentes (*smart cards*). Los terminales WiMAX suelen ir junto a un certificado X.509 que contiene su clave pública y dirección MAC.

- **Protocolo flexible de gestión de claves:** se emplea PKMv2 (*Privacy and Key Management Protocol Version2*) para transferir el material de las claves desde la estación base a la móvil, reautorizando y refrescando las claves periódicamente. PKM es un protocolo clienteservidor, actuando la MS (*Mobile Station*) como cliente y la BS (*Base Station*) como servidor. PKM usa el certificado digital X.509 y los algoritmos de cifrado de clave pública RSA (*Rivest-Shamer-Adleman*) para realizar el intercambio de claves entre las BS y las MS.
- **Protección de los mensajes de control:** La integridad de los mensajes de control "*over-theair*" se protege empleando esquemas de mensajes *digest*, como AES basado en CMAC (*Cipher-based Message Authentication Code*) o MD5 basado en HMAC (*Hash-based Message Authentication Codes*).
- **Soporte para entrega rápida:** WiMAX permite a la MS usar pre-autenticación para facilitar una reentrada acelerada a la red. Se tolera un esquema *handshake* para optimizar los mecanismos de re-autenticación con el objetivo de soportar entregas rápidas, y simultáneamente prevenir cualquier ataque externo.
- **Soporte para movilidad:** la variante *Mobile WiMAX* presenta mecanismos para soportar entregas transparentes y seguras para aplicaciones de movilidad completa tolerantes a retrasos, como por ejemplo puede ser VoIP. El sistema también integra mecanismos de ahorro de energía para ampliar la duración de la batería de los dispositivos móviles y se especifican mejoras de la capa física como la estimación del canal con más frecuencia, la subcanalización del *uplink* y el control de energía.
- **Arquitectura basada en IP**: el WiMAX Forum ha definido una arquitectura de red de referencia basada en una plataforma IP. Todos los servicios extremo a extremo se prestan mediante protocolos de transporte basados en IP, gestión de sesiones, seguridad y movilidad. La dependencia sobre IP permite a WiMAX disminuir los costes de procesamiento IP, facilitar la convergencia con otras redes y explotar el ecosistema existente para aplicaciones desarrolladas en IP.

3.2 Descripción detallada de la PHY

La capa física (PHY) de WiMAX está basada en lo especificado en los estándares IEEE 802.16-2004 y IEEE 802.16e-2005, y fue diseñada bajo la influencia de la tecnología WiFi (IEEE 802.11a). Aunque en muchos aspectos las dos tecnologías son muy diferentes, sobre

todo por su propósito y aplicaciones, algunos de sus aspectos básicos son comunes. Como WiFi, WiMAX está basado en los principios de modulación OFDM (*Orthogonal Frequency Division Multiplexing*), la cual es la técnica de modulación y de acceso más apropiada para escenarios donde se tenga alta tasa de datos y condiciones de no línea de visión directa (NLOS). Sin embargo, en WiMAX muchos de los parámetros referentes a la modulación OFDM difieren con WiFi (número de subportadoras, pilotos, bandas de guarda, etc), al trabajar en distintos entornos.

Los estándares IEEE 802.16 definen dentro de su *scope* cuatro capas PHY diferentes, pudiéndose emplear cada una de estos tipos diferentes de capa PHY con la capa MAC definida en el estándar.

Estas cuatro capas PHY diferentes son las siguientes:

- ***WirelessMAN SC***: capa física con modulación monoportadora para frecuencias por encima de los 11 GHz en condiciones LOS.
- ***WirelessMAN SCa***: capa física con modulación monoportadora para las frecuencias entre 2 y 11 GHz en operaciones punto - multipunto.
- ***WirelessMAN OFDM***: capa física OFDM con 256 puntos de FFT, empleada para operaciones punto-multipunto en condiciones NLOS y en frecuencias entre los 2 y los 11 GHz. Esta capa física ha sido aceptada por el WiMAX Forum para la certificación de equipos utilizados para aplicaciones fijas (*fixed* WiMAX).
- ***WirelessMAN OFDMA***: capa física basada en OFDM de 2048 puntos FFT para aplicaciones punto - multipunto entre las frecuencias de 2 y 11 GHz en condiciones NLOS. En el estándar IEEE 802.16e-2005 esta capa física ha sido modificada a SOFDMA (*scalable* OFDMA) donde el tamaño de la FFT es variable (128, 512, 1024 y 2048 puntos), de tal forma que se consiga una óptima relación entre la operación y la implementación de un sistema sobre un amplio rango de anchos de banda de canal y de condiciones radio. Esta capa física ha sido aceptada por el WiMAX Forum como la capa física para aplicaciones móviles (*mobile* WiMAX).

En la Figura 3-1 se muestra cuáles son las diferentes etapas funcionales presentes en una capa física de WiMAX.

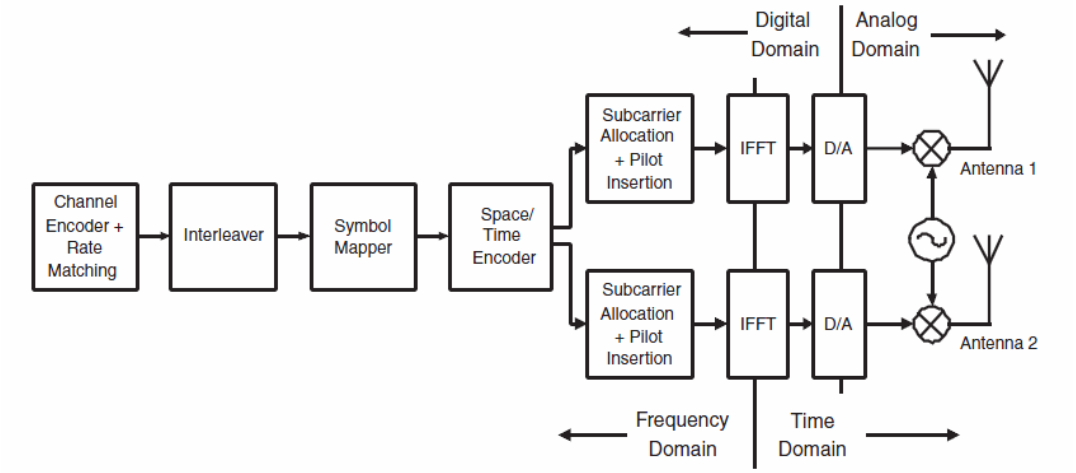


Figura 3-1: Etapas funcionales de la PHY de WiMAX

La primera etapa es el FEC (*Forward Error Correction*) que incluye la codificación de canal, el entrelazado de los datos, la aleatorización de los datos y el mapeo a símbolos.

La siguiente etapa funcional tiene que ver con la construcción de los símbolos OFDM en el dominio de la frecuencia, mapeándose en esta etapa los datos en los apropiados subcanales y subportadoras. En esta etapa también se realiza la inserción de los símbolos pilotos que permitirán la estimación y el *tracking* del estado del canal. En esta etapa también se lleva a cabo cualquier tipo de codificación espacio-temporal para la transmisión con diversidad o MIMO.

La última de las etapas se refiere a la conversión del símbolo OFDM desde el dominio de la frecuencia al dominio temporal, y a señal analógica para transmisión.

Aunque la Figura 3-1 sólo muestra los componentes lógicos para el transmisor, existen componentes similares en el receptor, en orden inverso, para reconstruir la secuencia de información transmitida. Además, se debe mencionar que como en otros estándares, sólo se especifican los componentes de transmisión en el estándar, dejándose abierta la especificación de los componentes en recepción.

3.2.1 Multiplexación OFDM

La capa física de WiMAX está basada en OFDM (Orthogonal Frequency Division Multiplexing), este esquema eficiente para entornos NLOS o multitrayecto, es usado en muchos sistemas comerciales de banda ancha, incluyendo DSL, Wi-Fi, DVB-H (Digital Video Broadcast-Handheld y MediaFLO.

OFDM pertenece a una familia de esquemas de transmisión llamada modulación multiportadora basada en la idea de dividir un flujo de datos de alta tasa de bit en varios flujos paralelos y modular cada uno en portadoras separadas, llamadas también subcanales. Los esquemas de modulación multiportadora eliminan o minimizan la interferencia intersimbólica (ISI) haciendo que el símbolo dure lo suficiente de forma que se mitigue el multitrayecto introducido por el canal. Por tanto, en sistemas con alta tasa de datos en los que la duración del símbolo es pequeña – siendo inversamente proporcional a la velocidad de transmisión de datos - dividir el flujo aumenta la duración del símbolo de cada uno de forma que el retardo de propagación es sólo una pequeña fracción de la duración del símbolo.

OFDM es una versión espectralmente eficiente de una modulación multiportadora, donde los subcanales son elegidos de forma que son todos ortogonales entre sí sobre la duración del símbolo. Así, evita la necesidad de tener canales subportadores no solapados para eliminar la interferencia entre portadoras, a costa de requerir una sincronización más fina. Con el objetivo de eliminar completamente la ISI, se usan intervalos de guarda mayores que el retardo de propagación entre los símbolos OFDM. Añadir un intervalo de guarda, implica sin embargo gasto de energía y una disminución de la eficiencia de ancho de banda. La cantidad de potencia perdida depende de la duración del tiempo de guarda sobre la duración del símbolo OFDM. Por lo tanto, cuanto mayor sea el periodo de símbolo para una velocidad de transmisión dada (más subcanales) más pequeña será la pérdida.

El tamaño de la FFT en un diseño OFDM debería elegirse cuidadosamente como un compromiso entre la protección frente al multitrayecto, el efecto Doppler y el coste/complejidad del diseño. Para un ancho de banda dado, seleccionar un tamaño de FFT

grande reduce el espacio entre subportadoras e incrementa la duración del símbolo, simplificando la protección contra el retardo de propagación multitrayecto. Sin embargo, un espacio reducido de subportadora hace al sistema más vulnerable a la interferencia entre portadoras producida por el efecto Doppler.

Para demodular una señal OFDM, el receptor tiene que realizar dos importantes tareas de sincronización. En primer lugar, deben determinarse el offset de tiempo del símbolo y los instantes de tiempo óptimos; esto se conoce como sincronización en tiempo. En segundo lugar, el receptor debe ajustar su frecuencia de portadora a la frecuencia de portadora del transmisor, sincronización en frecuencia. En comparación con los sistemas monoportadora, los requerimientos de sincronización en tiempo para OFDM son pequeños debido a la presencia del prefijo cíclico, ya que la estructura natural del símbolo OFDM da cabida a un grado razonable de error de sincronización. Por otra parte, los requerimientos en frecuencia son significativamente más estrictos, ya que la ortogonalidad de los símbolos depende de su discernibilidad individual en el dominio de la frecuencia. También es necesario aplicar técnicas de estimación e inversión del canal causado por el medio de propagación, aprovechándose de las portadoras piloto transmitidas en cada símbolo OFDM.

3.2.1.1 Principales características

- **Complejidad computacional reducida**: los requisitos de procesado crecen de forma ligeramente superior a la linealealidad con la velocidad de transmisión o ancho de banda. Esta complejidad es mucho menor que la cuadrática que ofrecen los sistemas basados en ecualización.
- **Ligera degradación del rendimiento con un gran retardo de propagación**: cuando el retardo de propagación es mayor que para el que está diseñado el sistema, el rendimiento de los sistemas OFDM se degrada de forma poco importante. Para obtener tasas alternativas que sean significativamente más robustas contra el retardo de propagación puede utilizarse una mayor tasa de codificación y tamaños de constelación más pequeños. OFDM está concebida para modulación y codificación adaptativa, lo que permite al sistema adaptarse a las condiciones de canal disponibles. Esto contrasta con la alta degradación debida a la propagación del error que sufren los sistemas monoportadora.
- **Explotación de la diversidad en frecuencia**: OFDM facilita la codificación y el entrelazado entre subportadoras en el dominio de la frecuencia, lo que ofrece robustez frente a los errores de ráfaga causados por porciones de espectro transmitido con desvanecimiento. En realidad, WiMAX define permutaciones de subportadoras que permiten al sistema explotar esto.
- **Utilización como esquema multiacceso**: OFDM puede usarse como esquema multiacceso, donde distintas portadoras se reparten entre múltiples usuarios. Este esquema conocido como OFDMA, ofrece la posibilidad de granularidad fina en la asignación del canal a los usuarios. En canales con variación en el tiempo lenta, es posible aumentar significativamente la capacidad adaptando la velocidad de transmisión de datos por abonado según la relación señal a ruido de cada subportadora.
- **Robustez ante las interferencias de banda estrecha**: OFDM es relativamente robusta ante las interferencias de banda estrecha, ya que dicha interferencias afectan sólo una fracción de las subportadoras.
- **Adecuado para demodulación coherente**: es relativamente simple en los sistemas OFDM hacer estimaciones de canal basadas en portadoras piloto, lo que los hace

adecuados para esquemas de demodulación coherente que son más eficientes en potencia.

- **Problema con las señales de PAR alto**: existe un problema asociado a que las señales OFDM tienen un PAR alto (*Peak-to-Average Ratio*) que causa no linealidades y distorsión *clipping*. Esto puede llevar a ineficiencias en potencia que deben ser tenidas en cuenta.
- **Susceptibilidad al ruido de fase y a la dispersión en frecuencia**: Las señales OFDM son muy susceptibles al ruido de fase y a la dispersión en frecuencia, con lo que el diseño debe mitigar estas imperfecciones. Esto también hace que sea fundamental una sincronización en frecuencia.

3.2.2 Capas físicas OFDM/OFDMA

Como ya se ha mencionado, las versiones fija y móvil de WiMAX tienen implementaciones ligeramente distintas en su capa física:

- **Fixed WiMAX OFDM-PHY**: para esta versión se fija el tamaño de la FFT a 256, de los cuales 192 subportadoras se usan para transmitir datos, 8 se usan como portadoras piloto para la estimación del canal y sincronización y el resto se usan como portadoras de guarda. Una vez fijado el tamaño FFT el espacio entre subportadoras varía con el ancho de banda, disminuir el tiempo de símbolo implica que una fracción más larga necesita ser asignada como tiempo de guarda para reducir el retardo de propagación. WiMAX permite un amplio rango de tiempos de guardas que permiten a los diseñadores de sistemas buscar un compromiso entre eficiencia espectral y robustez en el retardo de propagación.
- **Mobile WiMAX OFDMA-PHY**: el tamaño de la FFT es escalable desde 128 hasta 2.048. Aquí, cuando el ancho de banda disponible aumenta, el tamaño de FFT es también incrementado de forma que el espacio entre subportadoras sea siempre 10.94 KHz. El espacio entre subcanales de 10.94 KHz fue elegido como un buen compromiso entre el retardo de propagación y los requerimientos del efecto Doppler para operar tanto en entornos fijos como móviles. Esto mantiene la duración del símbolo OFDM fijo y por tanto minimiza el impacto de la escalabilidad en las capas más altas. Este espacio entre subportadoras puede soportar valores de retardo de propagación hasta los 20 microsegundos y movilidad de vehículos hasta 125 km/h operando a 3.5 GHz. Un espacio entre subportadoras de 10.94 KHz implica que FFTs de 128, 512, 1.024 y 2.048 son usadas cuando el ancho de banda del canal es 1.25MHz, 5MHz, 10MHz y 20 MHz respectivamente. Debemos apuntar que *mobile WiMAX* puede incluir también perfiles adicionales de ancho de banda.

Las subportadoras disponibles pueden ser divididas en varios grupos llamados subcanales. *Fixed* WiMAX basado en OFDM-PHY permite una forma limitada de subcanalización sólo en el *uplink*. El estándar define 16 subcanales, donde 1, 2, 4, 8 o todos los conjuntos pueden ser asignados a una estación abonada en el *uplink*, lo que permite subscribir estaciones para transmitir usando sólo una fracción (tan baja como 1/16) del ancho de banda asignado por la estación base, lo que proporciona mejoras en el coste del enlace que pueden ser usadas para aumentar el rango de rendimiento y/o mejorar la duración de la batería de las estaciones abonadas. Un factor de subcanalización 1/16 proporciona una mejora de 12 dB.

Mobile WiMAX basado en OFDMA-PHY, sin embargo, permite la subcanalización en el *uplink* y en el *downlink*, los subcanales pueden estar constituidos usando subportadoras contiguas o subportadoras distribuidas aleatoriamente a través del espectro de frecuencia.

Los subcanales formados usando subportadoras distribuidas ofrecen más diversidad en frecuencia, lo que es particularmente útil para aplicaciones móviles.

WiMAX define varios esquemas de subcanalización basados en portadoras distribuidas para el *uplink* y el *downlink*. Una, llamada PUSC (*Partial Usage Of Subcarries*), es obligatoria para todas las implementaciones WiMAX móvil. Los perfiles iniciales WiMAX definen 15 y 17 subcanales para el downlink y el uplink, respectivamente, para un ancho de banda de 5MHz. Para 10MHz, se define 30 y 35 canales, respectivamente. El esquema de subcanalización basada en subportadoras contiguas en WiMAX se llama AMC (*Adaptive Modulation and Coding*). Aunque la diversidad de frecuencia se pierda, AMC permite a los diseñadores de sistemas explotar la diversidad multiusuario, asignando subcanales a los usuarios basándose en su respuesta en frecuencia. La diversidad multiusuario puede proporcionar ganancias significativas en la capacidad total del sistema, si el sistema se esfuerza por proveer a cada usuario de un subcanal que maximice su SINR recibida. En general, los subcanales contiguos son más adecuados para aplicaciones fijas y de baja movilidad. Definimos una serie de estructuras básicas:

- **Subcanal**: conjunto de portadoras dentro de un símbolo que conforman una unidad mínima. Dependiendo de la zona, estas subportadoras pueden estar situadas de forma contigua o aleatoria dentro de cada símbolo.
- **Slot**: unidad mínima que se puede asignar a un usuario. Dependiendo de la zona el slot tiene distintas definiciones. Por ejemplo, en el caso de una zona FUSC (*Full Usage Of Subcarries*) es un subcanal durante un símbolo OFDM, y en el uplink PUSC es un subcanal durante tres símbolos OFDM adyacentes.
- **Región de datos**: es un conjunto de slots asignado a un usuario. Se define mediante una región formada por varios símbolos OFDM y varios subcanales adyacentes.

3.2.3 Descripción de la capa física OFDMA

3.2.3.1 Codificación de canal

En el estándar se indica que durante la codificación de canal se deben seguir las fases de: aleatorización, entrelazado, codificación de canal, modulación y HARQ (opcional). El esquema global del proceso de codificación se puede ver en la Figura 3-2.

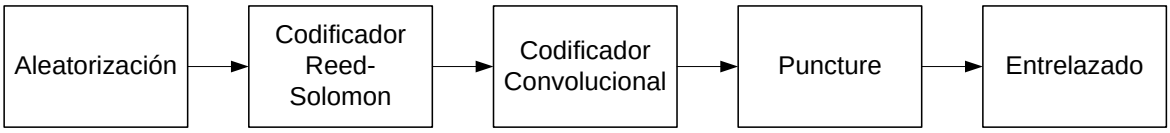


Figura 3-2: Esquema global de la codificación de canal

3.2.3.1.1 Aleatorización

Se realiza una multiplicación por una secuencia pseudo-aleatoria. En el punto 8.4.9.1 del estándar se especifica que esta secuencia se genera mediante un LFSR (*Linear Feedback Shift Register*) como en la Figura 3-3, utilizando como secuencia de inicialización la cadena 011011100010101. Este aleatorizador es necesario reinicializarlo para cada bloque FEC, y en el caso del mensaje FCH este módulo no se deberá utilizar. El número de bits a la entrada debe ser suficiente para rellenar slots OFDMA completos, y en caso contrario se hará un relleno con 1's.

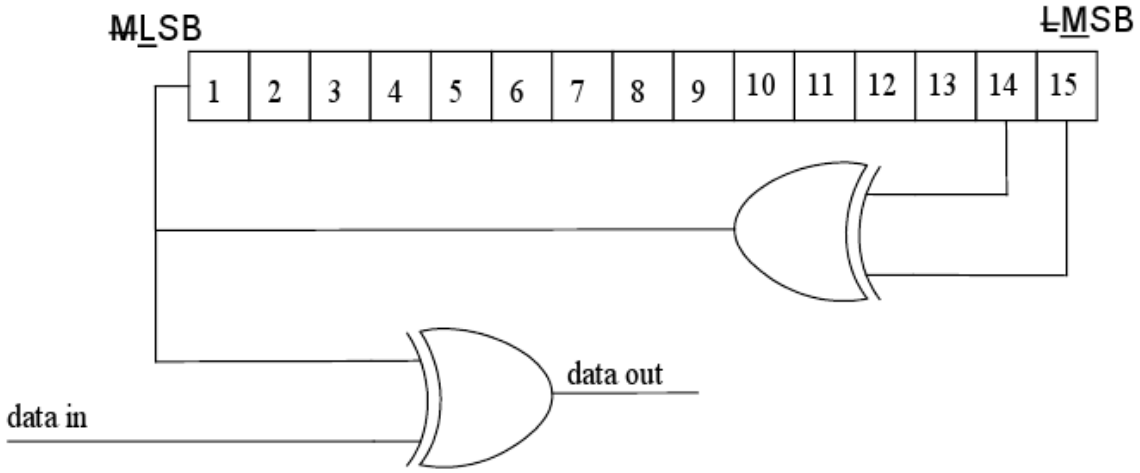


Figura 3-3: LFSR utilizado en la aleatorización

3.2.3.1.2 Codificación

El estándar de WiMAX permite distintos esquemas de codificación. A continuación se presenta una opción de FEC que consiste en una concatenación de un codificador Reed-Solomon (RS) y un codificador convolucional (CC). Esto significa que los datos primero pasan por el codificador RS y después por el convolucional. Es un proceso de codificación flexible debido al *puncturing* y permite distintas tasas de codificación [3]. Se conoce a esta codificación como RS-CC y sus posibles configuraciones se presentan en la siguiente tabla:

Modulación	Tamaño de bloque sin codificar (bytes)	Tamaño de bloque codificado (bytes)	Tasa de codificación global	Código RS (N',K',T')	Tasa CC
BPSK	12	24	1/2	(12,12,0)	1/2
QPSK	24	48	1/2	(32,24,4)	2/3
QPSK	36	48	3/4	(40,36,2)	5/6
16-QAM	48	96	1/2	(64,48,8)	2/3
64-QAM	72	96	3/4	(80,72,4)	5/6
64-QAM	96	144	2/3	(108,96,6)	3/4
64-QAM	108	144	3/4	(120,108,6)	5/6

Tabla 3-1: Formatos de codificación disponibles en WiMAX

- Codificador RS:

Las propiedades de los códigos RS los hacen apropiados para aplicaciones en los que los errores ocurren a ráfagas. Funciona construyendo polinomios a partir de los datos a transmitir, enviando una versión sobremuestreada del polinomio en lugar del original [3]. Los códigos RS tienen la máxima distancia posible para el FEC con los parámetros especificados N,K. Esto significa que pueden corregir el máximo número de errores para dichos parámetros.

El codificador RS tiene N=256, K=239, T=8 y soporta todas las tasas de codificación y requisitos de corrección de errores estipulados por las especificaciones de WiMAX. Para conseguir la tasa K' y capacidad de corrección de errores T' deseadas, el código es acortado y se hace un *puncturing*. El recorte se hace añadiendo K-K' ceros al inicio

del mensaje que tras la codificación son descartados. El *puncturing* se hace descartando los últimos 2(T-T') bits de paridad [4].

- Codificador convolucional:

Tras la codificación RS, los bits de datos pasan por un codificador convolucional, el cual acepta mensajes de k0 bits y genera palabras código de n0 bits. Generalmente se compone de registros de desplazamiento de L segmentos [3]. El codificador convolucional empleado tiene una tasa de 1/2 y L=7 y está definido por los polinomios generadores:

$$G_1 = 171_{OCT} \quad \text{for} \quad X,$$

$$G_2 = 133_{OCT} \quad \text{for} \quad Y.$$

Ecuación 3-1: Polinomios generadores del codificador convolucional

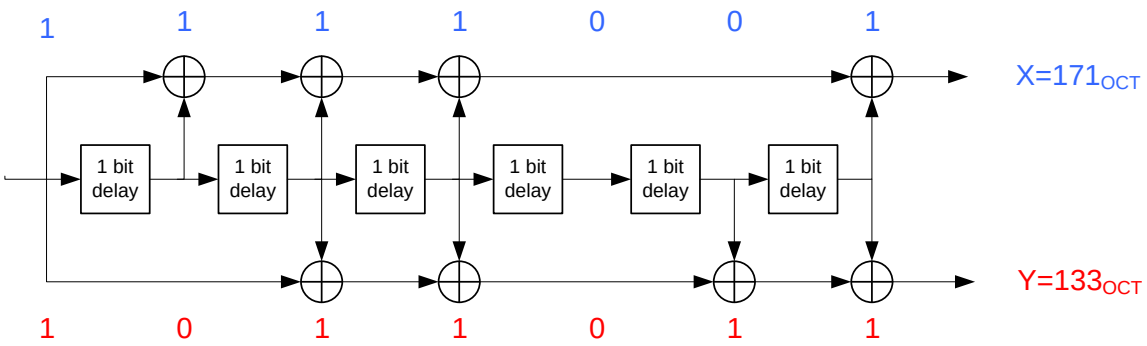


Figura 3-4: Codificador convolucional con tasa 1/2

Para acomodar todas las tasas definidas en el estándar WiMAX, la salida del CC recibe un *puncturing*. En la Tabla 3-2 se muestra los patrones de *puncturing* para cada una de las tasas del CC; donde las dos salidas del codificador están representadas por X e Y respectivamente [4].

Tasa	1/2	2/3	3/4	5/6
Patrón de salida con *puncturing*	X_1Y_1	$X_1Y_1Y_2$	$X_1Y_1Y_2X_3$	$X_1Y_1Y_2X_3Y_4X_5$

Tabla 3-2: Patrones de *puncturing* para cada tasa del CC

3.2.3.1.3 Entrelazado

Todos los bits codificados deben pasar por una fase de entrelazado. Este proceso se realiza en dos pasos, el primero asegura que los bits codificados adyacentes son mapeados en subportadoras no adyacentes lo que proporciona diversidad en frecuencia y mejora el rendimiento del decodificador. El segundo paso asegura que los bits adyacentes son mapeados alternativamente desde los bits menos significativos a los más significativos de la constelación de la modulación.

Las ecuaciones utilizadas para el entrelazado son:

$$m(k) = (N_{cbps}/d) \cdot mod(k,d) + floor(k/d)$$

$$j(k) = s \cdot floor(m(k)/s) + mod(m(k) + N_{cbps} - floor(d \cdot m(k)/N_{cbps}), s)$$

Ecuación 3-2: Ecuaciones aplicables al entrelazador

Siendo d igual a 16 en la implementación obligatoria (distancia), Ncbps el número de bits codificados del bloque, k la posición del bit antes del entrelazado, y s el número de bits por símbolo dividido por dos, esto es, 1 para 4-QAM, 2 para 16-QAM y 3 para 64-QAM. Se obtiene una primera permutación a través de la expresión de m(k), y posteriormente se realiza una segunda permutación j(k) para obtener la posición final de cada bit.

3.2.3.2 Conformación de trama

3.2.3.2.1 Modulación

Los datos codificados deben traducirse a símbolos IQ, siguiendo una modulación QAM de distintos niveles. Las modulaciones obligatorias son BPSK, QPSK y 16-QAM, siendo 64-QAM opcional. En la siguiente figura se muestran algunas de las constelaciones de las modulaciones (la de 64-QAM se forma de forma análoga).

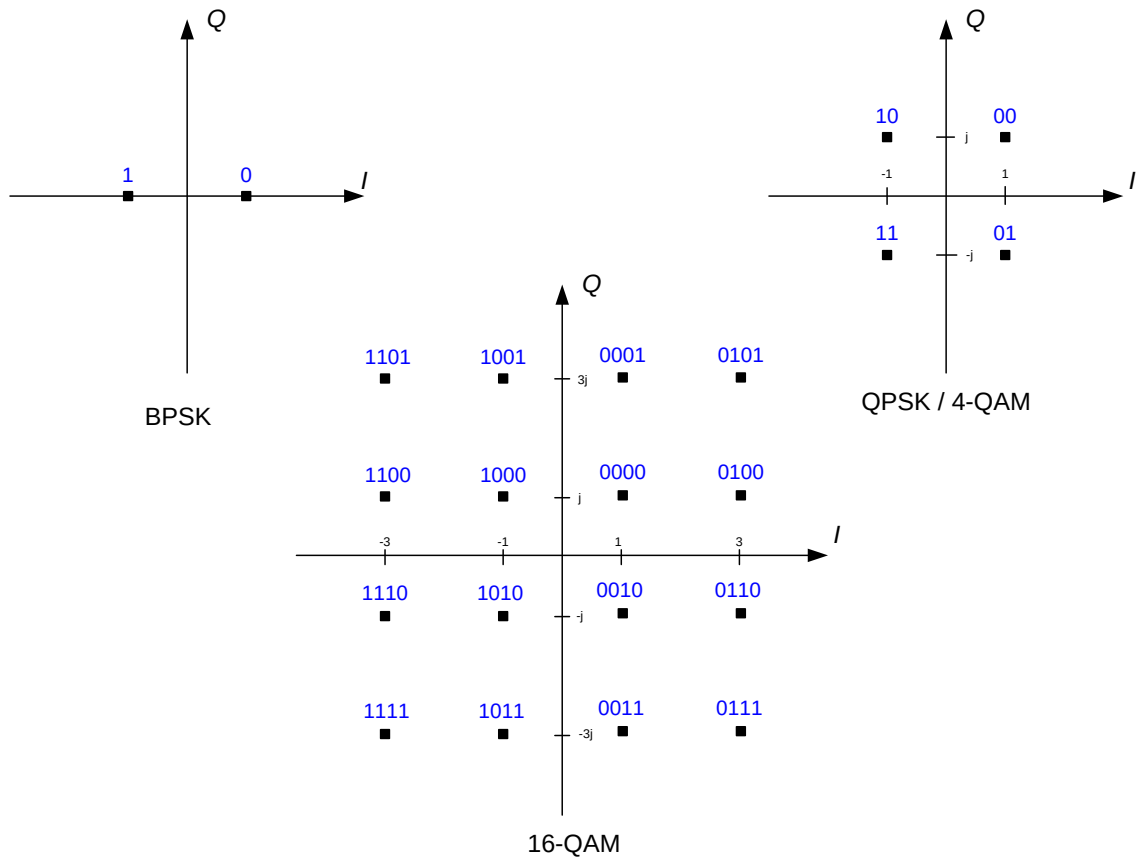


Figura 3-5: Constelaciones de las distintas modulaciones

Cabe resaltar que BPSK no es utilizado para datos, solo para el preámbulo y modulación de las señales piloto.

3.2.3.2.2 Estructura de trama

La estructura más grande a nivel físico es la trama (*frame*). Está compuesta por una serie de símbolos OFDM que se transmiten de forma continua. A nivel global se puede descomponer en preámbulo, subtrama de downlink y subtrama de *uplink*. Solo se permite la transferencia de estos tres elementos en modo TDD, a diferencia de otros niveles físicos en los que se permite la operación FDD. El ratio de subtrama *downlink*-to-*uplink* puede variar desde 3:1 a 1:1 para soportar distintos perfiles de tráfico.

El preámbulo se emite a intervalos regulares desde la estación base (5, 15, 25 ms...), y después de él va la subtrama de downlink. La estructura particular de esta subtrama es variable, y se transmite en los dos primeros símbolos de la misma (ver Subsección 7.3.2.3.1). A continuación, y después de un tiempo de guarda se transmite la subtrama de *uplink*, cuya estructura (UL-MAP) se ha comunicado a las estaciones móviles durante el downlink. Este proceso se inicia otra vez con la transmisión del preámbulo después de dejar un tiempo de guarda tras la subtrama de *uplink*.

Dentro de cada subtrama se pueden diferenciar a su vez zonas de permutación (*permutation zones*) y ráfagas (*bursts*). Las zonas de permutación son un conjunto de símbolos OFDM adyacentes en los que se utiliza un método concreto de asignación y estructuración de las portadoras. Las zonas especificadas son: PUSC (*Partial Usage of Subcarriers*), FUSC (*Full Usage of Subcarriers*), AMC (*Adaptative Modulation and Coding*) y TUSC (*Tile Usage of Subcarriers*). La única zona obligatoria es la zona PUSC, y la subtrama de downlink siempre contiene una al principio inmediatamente después del preámbulo.

Las ráfagas son conjuntos de portadoras dentro de una zona asignados a uno o varios usuarios, y que tienen en común tener la misma modulación, tasa de codificación y FEC. Estas ráfagas se asignan a las regiones de datos para su transmisión, siguiendo el siguiente esquema:

1) Se divide la ráfaga en slots.
2) Se sitúa el primer slot dentro de la región de datos en el subcanal y símbolo de menor índice. Como cada slot ocupa un subcanal durante una serie de símbolos OFDM consecutivos según la zona donde esté definida la región de datos, el slot se distribuirá a lo largo de un número mayor o menor de símbolos.
3) Cada slot se va situando en el subcanal siguiente. Cuando se alcanza el último subcanal de la región de datos, se vuelve al primer subcanal pero del siguiente símbolo OFDM sin asignar.

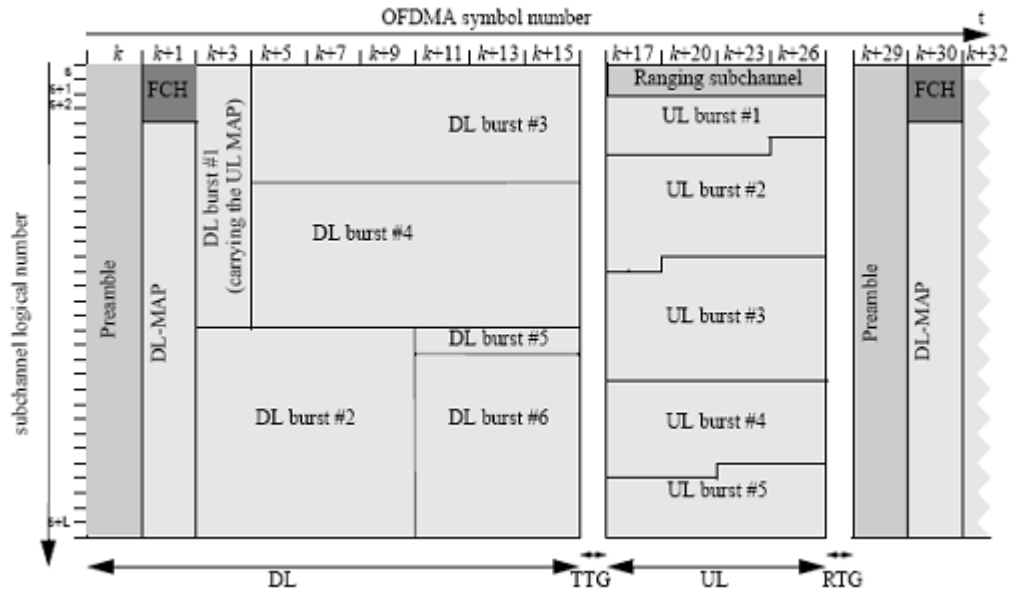


Figura 3-6: Estructura global de una trama

La subtrama de downlink es la transmisión desde la estación base a la estación móvil. El primer símbolo de downlink es el preámbulo (*preamble*), el cual es elegido basándose en el identificador de segmento y célula de la comunicación. Los datos e información de control se identifican como ráfagas (*bursts*). La primera ráfaga es de control y se conoce como *Frame Control Header* (FCH). El FCH proporciona información sobre el DL-MAP, que contiene información de las ráfagas de datos. Por lo tanto, cada estación móvil tiene que decodificar el DL-MAP para obtener información sobre la ráfaga de datos asignada a ella.

La subtrama de *uplink* (UL) es la transmisión de la estación móvil a la estación base. Cada estación móvil que desee establecer contacto con la estación base debe enviar una ráfaga de control en el subcanal *Ranging subchannel* junto con las ráfagas de datos (ver figura anterior) [5].

3.2.3.2.2.1 Preámbulo

El símbolo utilizado como preámbulo se obtiene mediante la modulación BPSK de una secuencia pseudo-aleatoria especificada en el estándar. Esta secuencia se sitúa en las portadoras, separando cada valor por dos portadoras a cero. La posición de las mismas también depende del segmento de la transmisión.

3.2.3.2.2.2 Estructura de símbolo OFDM: downlink PUSC

- Dominio del tiempo

La transformada inversa de Fourier (IFFT) crea la forma de onda OFDM; esta amplitud de tiempo se denomina periodo de símbolo útil (Tb). Una copia de duración Tg al final del símbolo es copiada al principio tal y como se muestra en la siguiente figura:

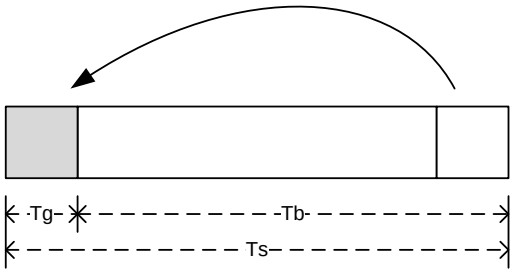


Figura 3-7: Estructura de símbolo OFDM en tiempo

Esta copia se denomina prefijo cíclico (CP) y se utiliza para determinar el canal antes de que comiencen los datos útiles en el receptor [6].

- Dominio de la frecuencia

Un símbolo OFDM (ver figura inferior) está formado por subportadoras o subcarriers, cuyo número determina el tamaño de FFT usado [6]. Hay tres tipos de subcarriers:

  - Data subcarriers: Para la transmisión de datos.
  - Pilot subcarriers: Utilizadas para estimaciones en el receptor.
  - Null subcarriers: No se transmite nada en ellas, se utilizan como bandas de guarda, subcarriers no activas y subportadora DC.

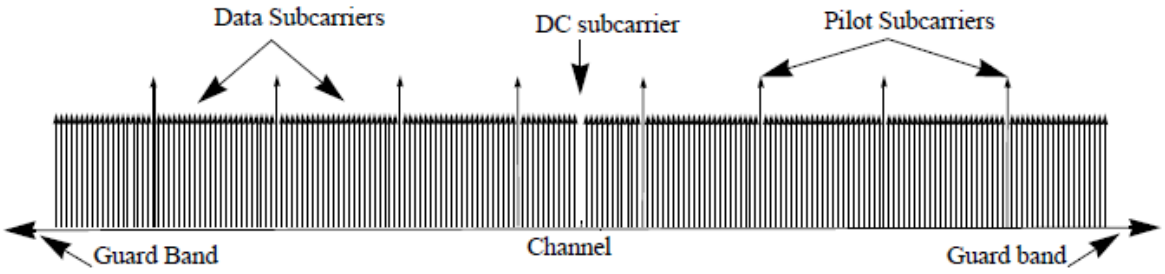


Figura 3-8: Estructura de símbolo OFDM en frecuencia

4 Análisis de prestaciones en entorno táctico

El primer objetivo de este estudio consiste en demostrar la vulnerabilidad del sistema de comunicaciones bajo estudio, WiMAX, cuando opera en entornos con presencia de *jammers*.

De cara a evidenciar esta vulnerabilidad, se consideraran una serie de escenarios a analizar. Estos escenarios, representan distintos despliegues de enlaces WiMAX y simulan el efecto que puede tener ciertos tipos de *jamming* en dicho escenario. Los *jammer* seleccionados para el análisis son de ruido blanco y con distintos anchos de banda. El motivo de la elección de estos tipos es que tienen poca complejidad y no requieren mucha información de la forma de onda a interferir, por lo que demuestran la supuesta vulnerabilidad del sistema.

4.1 Escenario táctico genérico

En primer lugar, los escenarios considerados se componen de 3 elementos:

- Un transmisor que se caracteriza por los siguientes parámetros:
  - fc: Frecuencia central de operación
  - BW: Ancho de banda de canal
  - P_{tx}: Potencia de transmisión
  - d: Distancia al receptor
- Un receptor que se supone en concordancia con el transmisor (misma frecuencia de operación y ancho de banda de canal.
- Un *jammer* de ruido blanco caracterizado por los siguientes parámetros:
  - fc_{jamm}: Frecuencia central de operación
  - BW_{jamm}: Ancho de banda atacado
  - P_{jamm}: Potencia de transmisión (en la banda de operación)
  - d_{jamm}: Distancia al receptor

En la siguiente figura se puede apreciar la relación entre los elementos que componen el escenario.

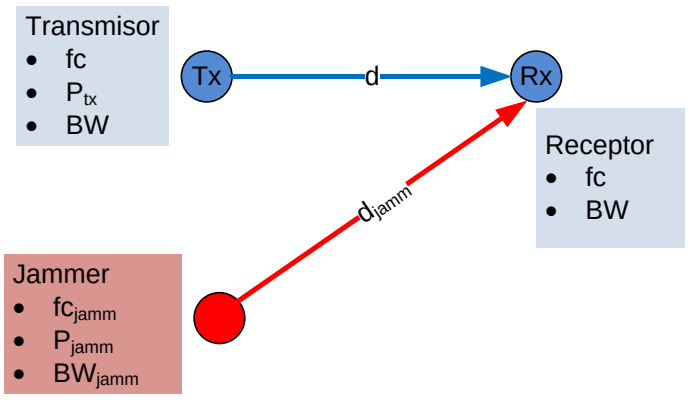


Figura 4-1: Elementos de un escenario genérico

Con estos elementos y parámetros básicos se pueden modelar y simular los efectos del *jamming* en todos los escenarios a considerar en este estudio.

La forma de simular el efecto de un *jammer* de ruido blanco en la comunicación es mediante el SIR en recepción. Ésto es la relación entre la potencia de señal y potencia de *jamming* en el receptor.

Dado que se considera que la comunicación se hace a través de un trayecto en espacio abierto sin obstáculos, las pérdidas de potencia (tanto para el transmisor como para el *jammer*) se calculan usando la ecuación de Friis para propagación en espacio libre [7]:

$$L = G_T G_R \left(\frac{\lambda}{4\pi d}\right)^2$$

Ecuación 4-1: Ecuación de Friis de propagación en espacio libre

Donde L es la ganancia (negativa, por lo tanto son pérdidas), G_T y G_R son las ganancias de las antenas de transmisión y recepción respectivamente, d es la distancia entre transmisor y receptor y lamba es la longitud de onda de la señal. Esta ecuación es aplicable si $d \gg \lambda$ y el ancho de banda de la señal es lo suficientemente estrecho como para considerar que una única longitud de onda λ para toda la banda. A veces se excluye la ganancia de las antenas en el cálculo de las pérdidas de propagación. La fórmula también se puede expresar en decibelios como (en este caso excluyendo la ganancia de las antenas:

$$L_{dB} = -20\, log_{10}\left(\frac{\lambda}{4\pi d}\right)$$

Ecuación 4-2: Ecuación de Friis de propagación en espacio libre en dB

4.1.1 Transmisor genérico considerado

A continuación se muestran una gráficas que representa la potencia en recepción en función de la distancia entre transmisor y receptor para varias potencias de transmisión. Estas figuras son importantes de cara a analizar la introducción de *jammers* y la SIR en el receptor. Se considera que las frecuencias de operación están en la banda de 4.4 a 5 GHz (NATO-IV) y centradas en 4.7 GHz. También se considera que los anchos de banda son lo suficientemente estrechos como para considerar que la atenuación es la misma en toda la banda.

En primer lugar, las estaciones móviles tienen una potencia de transmisión de unos 23dBm (200mW), por lo que en la gráfica se muestran potencias de 20 a 25dBm en intervalos de 1dBm.

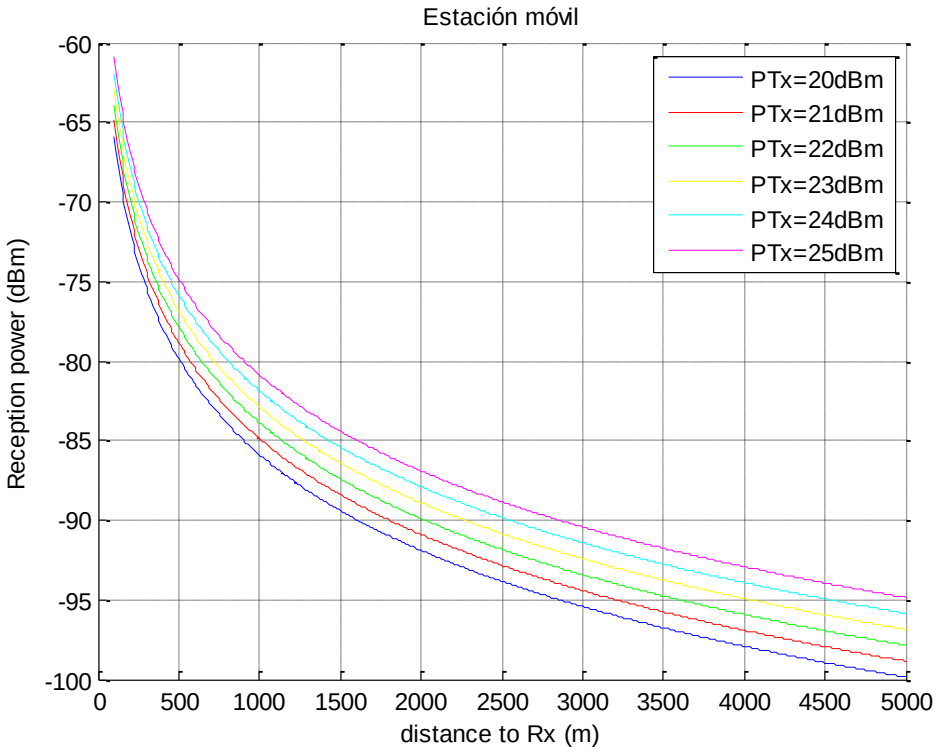


Figura 4-2: Potencia recibida en función de distancia Tx-Rx – Estación móvil

Las estaciones base de WiMAX tienen una potencia de transmisión de unos 43dBm (20W), por lo que en la gráfica se muestran potencias de 40 a 45dBm en intervalos de 1dBm.

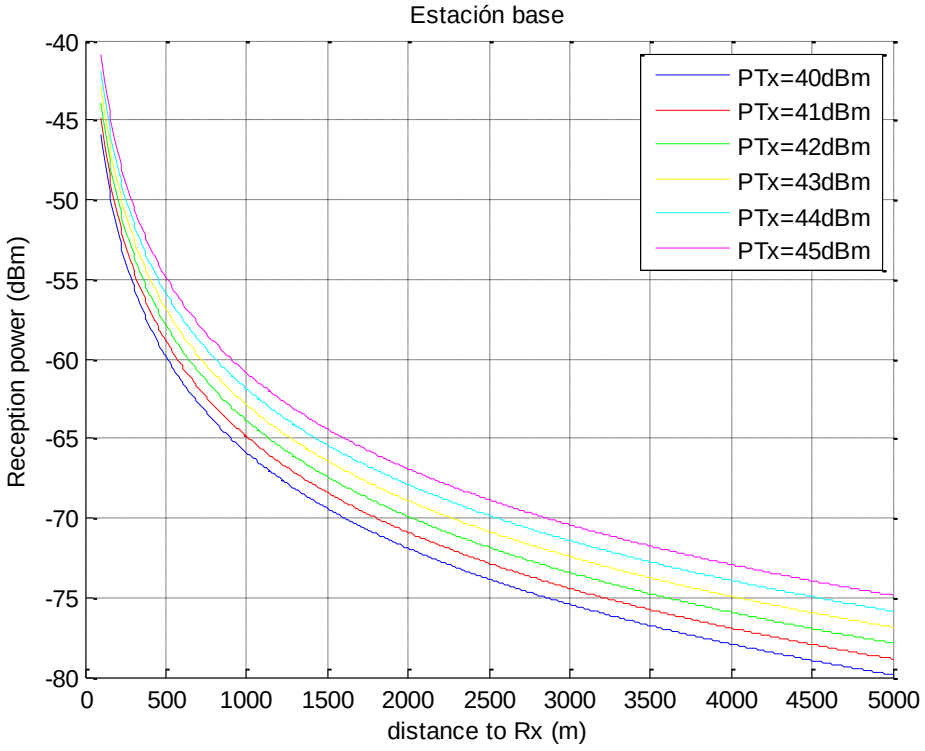


Figura 4-3: Potencia recibida en función de distancia Tx-Rx – Estación base

4.1.2 Tipos de *Jammer* considerados

4.1.2.1 Jammer de Banda ancha

Este tipo de *jamming* introduce energía en un amplio espectro aumentando el nivel de ruido en el receptor. La principal desventaja de este *jammer* de cara a perturbar la comunicación es que la potencia queda esparcida a lo largo de una amplia zona del espectro, disminuyendo su efectividad.

Por ejemplo, suponiendo que la banda de operación elegida para el sistema de WiMAX fuese la comprendida entre 4,4 y 5 GHz, es elegiría dicha banda como objetivo para el *jammer*.

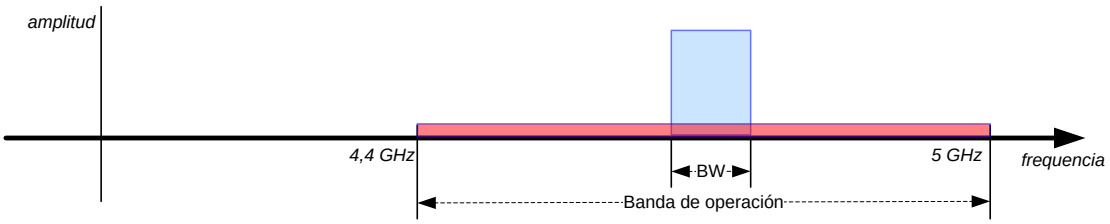


Figura 4-4: Disposición de *Jammer* de banda ancha

La potencia de transmisión del sistema es parametrizable así como la banda objetivo sobre la que se aplica dicha potencia.

Al igual que para la señal transmitida, también se obtiene la potencia de *jamming* en recepción usando el modelo de Friis y calculando el porcentaje que realmente cae sobre la señal objetivo.

En la siguiente gráfica se representa la potencia de *jamming* en recepción en función de la distancia entre el *jammer* y el receptor en función para algunas potencias de *jammer*. La banda objetivo es la NATO-IV completa, sobre la que opera el sistema WiMAX propuesto.

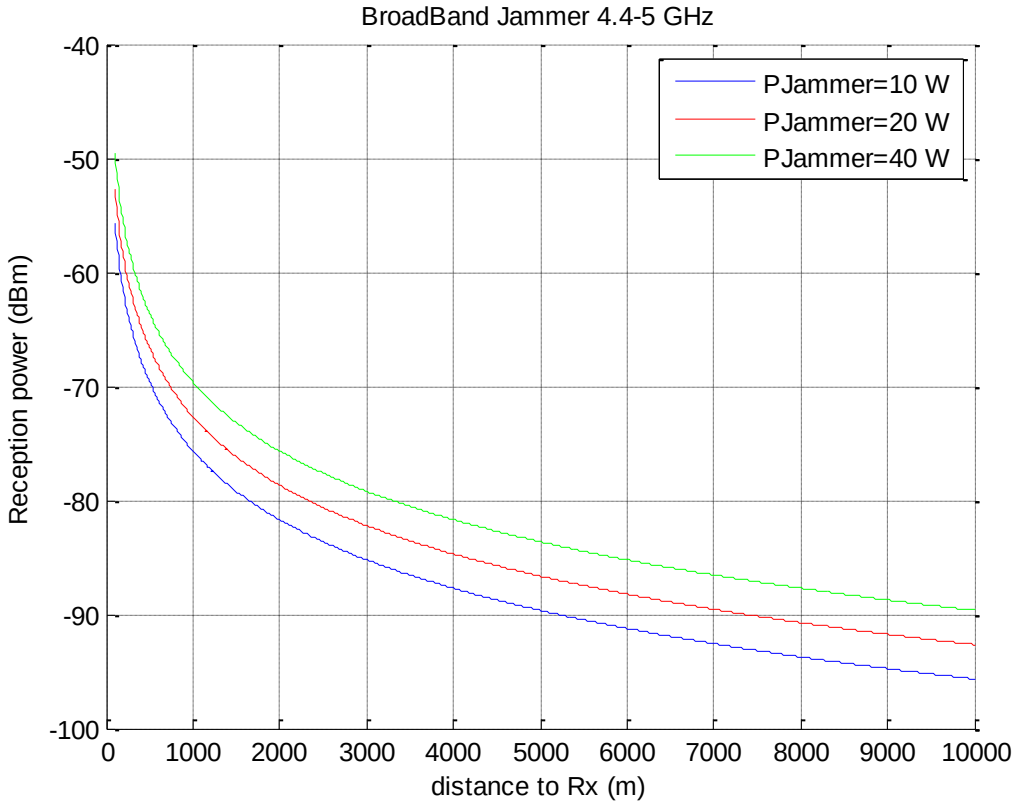


Figura 4-5: BroadBand *Jammer* – distancia a receptor

4.1.2.2 Jammer de Banda parcial

Este tipo de *jammer* funciona como el de banda ancha pero limitando la banda de operación, por lo que se consigue concentrar la energía de forma más efectiva en una zona del espectro. La desventaja de este tipo de *jammer* es que se debe conocer la banda de operación del sistema objetivo para concentrar su energía alrededor de ésta.

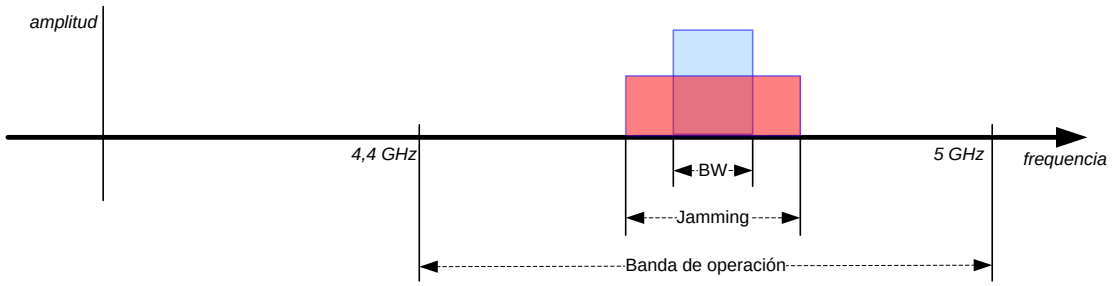


Figura 4-6: Disposición de *Jammer* de banda parcial

Los *jammers* de ruido se pueden caracterizar mediante los W/MHz; esto es, simplemente la potencia de ruido dividida por el ancho de banda que ocupa. Por ejemplo, un *jammer* de 500W transmitiendo con 200MHz de ancho de banda tiene 2.5 W/MHz.

La efectividad del *jammer* reside en el porcentaje de potencia que realmente cae sobre el ancho de banda que cae en la señal objetivo. Por ejemplo, considerando el *jammer* anterior y una señal objetivo con 3 MHz dentro de la banda de operación del *jammer* sufre una potencia de *jamming* en recepción:

$$2.5 \text{ W/MHz} \times 3 \text{ MHz} = 7.5\text{W} = 38.75 \text{ dBm}$$

Ecuación 4-3 : Ejemplo de potencia de *jamming* en recepción.

Por lo tanto, es vital optimizar la potencia de *jamming* ajustando la frecuencia central a la portadora de la señal objetivo y el ancho de banda mínimo para cubrir la señal o parte de ella. De este modo se minimiza la SIR y el efecto del *jammer* es más efectivo. Los *jammers* actuales permiten ajustar todos estos parámetros para atacar la señal de forma óptima [8].

Esta potencia de transmisión de los dispositivos de *jamming* también se ve atenuada por la propagación en el espacio libre según el modelo de Friis.

En las siguientes gráficas se representa la potencia de *jamming* en recepción en función de la distancia entre el *jammer* y el receptor para algunas potencias distintas. La banda objetivo está centrada sobre 4.7 GHz al igual que la señal transmitida y tendrá un ancho determinado sobre el que se reparte la potencia de transmisión. Para calcular la potencia de *jamming* en el receptor se asume que el ancho de banda de canal es de 10 MHz.

Gráfica considerando un *jammer* centrado en 4.7GHz y ancho de banda de 100MHz.

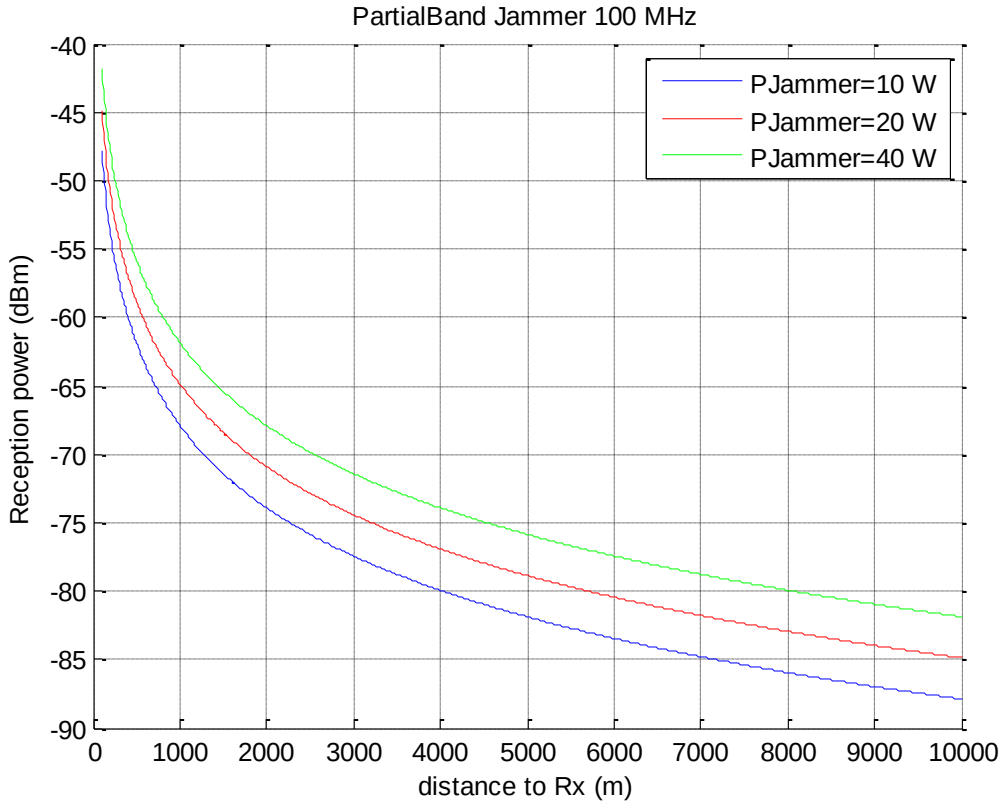


Figura 4-7: PartialBand *Jammer* 1 – distancia a receptor

Gráfica considerando un *jammer* centrado en 4.7GHz y ancho de banda de 20MHz.

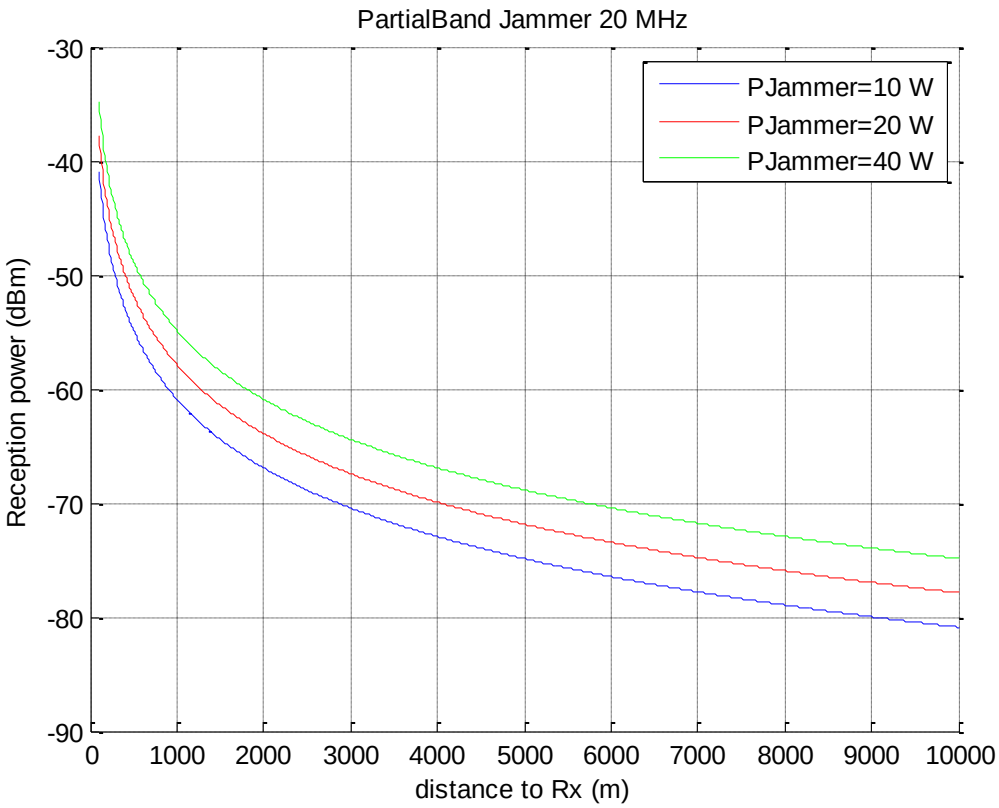


Figura 4-8: PartialBand *Jammer* 2 – distancia a receptor

Gráfica considerando un *jammer* centrado en 4.7GHz y ancho de banda de 10MHz.

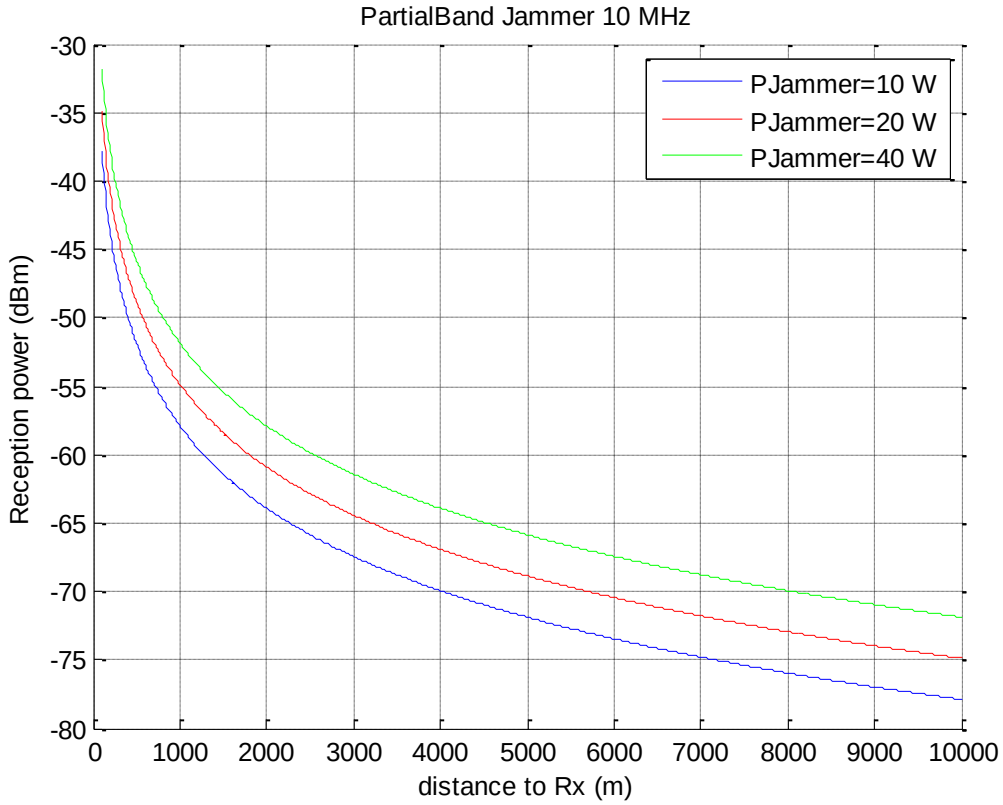


Figura 4-9: PartialBand *Jammer* 3 – distancia a receptor

4.2 Modelado de escenarios tácticos

La forma de simular los escenarios y caracterizarlos es usando un modelo simplificado de WiMAX en la herramienta Simulink. Como punto de partida para este estudio, se considera un sistema formado por un transmisor y un receptor compuestos únicamente por una capa física simplificada [3].

El transmisor de este sistema simplificado contiene la cadena de procesado desde los datos proporcionados por la capa superior hasta las muestras en banda base que alimentaría la cadena de conversión a frecuencia superior. El efecto de los *jammers* se modela en banda base, por lo que el transmisor del modelo no implementa la cadena de *upconversion* [3].

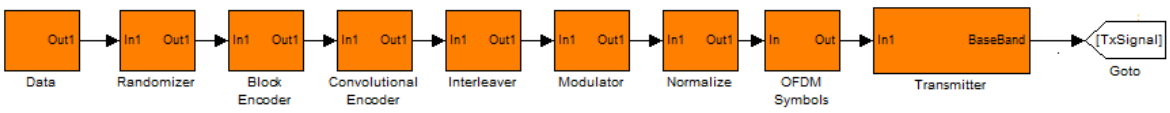


Figura 4-10: Diagrama de bloques del transmisor

Existen 4 parámetros primitivos que caracterizan el símbolo OFDM que se transmite:

- BW: Ancho de banda de la señal transmitida es 10 MHz
- N_{used}: El número de portadoras usado es 200 (192 de datos y 8 pilotos).
- n: Factor de muestreo. Este parámetro, junto con el ancho de banda (BW) y el número de subportadoras (N_{used}), determina el espacio entre subportadoras y el periodo de símbolo útil. Dado que el ancho de banda es 10MHz, n=144/125

- G: Es el ratio de tiempo de CP y tiempo útil. Se escoge 1/32.

De los parámetros primitivos, se derivan los siguientes:

- N_{FFT}: El número de portadoras usado es 192, lo que implica un tamaño de FFT de 256 (potencia de 2 inmediatamente mayor que N_{used}).
- Frecuencia de muestreo: F_s=floor(n·BW/8000)x8000
- Espacio entre subportadoras: $\Delta f=F_s/N_{FFT}$
- Periodo de símbolo útil: $Tb=1/\Delta f$
- Periodo de CP: $Tg=G \cdot Tb$
- Periodo de símbolo OFDM: $Ts=Tg+Tb$
- Periodo de muestreo: Tb/N_{FFT}

El receptor contiene la cadena de procesado desde las muestras en banda base hasta la entrega de datos a la capa superior.

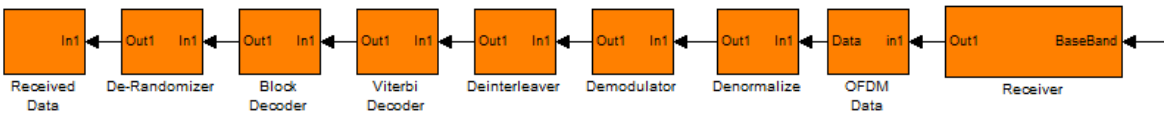


Figura 4-11: Diagrama de bloques del receptor

Se ha considerado un receptor simple sin ecualizador de canal ni sincronización [3].

Es en la frontera de la capa física con la capa superior donde se comprueba el BER que se produce en cada escenario.

4.2.1 Escenario de control

Dado que el objeto del estudio es el efecto de distintos tipos de *jammers* en el sistema, se decide eliminar variables como efectos de canal y ruido. Partiendo de esta idealidad del sistema, se considera que el BER de los datos decodificados y entregados al final de la capa física es 0, no se produce ningún error. Dicho dato es corroborado con el modelo de Simulink.

En la siguiente figura se puede ver el diagrama de bloques del simulador en el que el transmisor se conecta al receptor sin pasar por ningún canal ni añadir *jammers*:

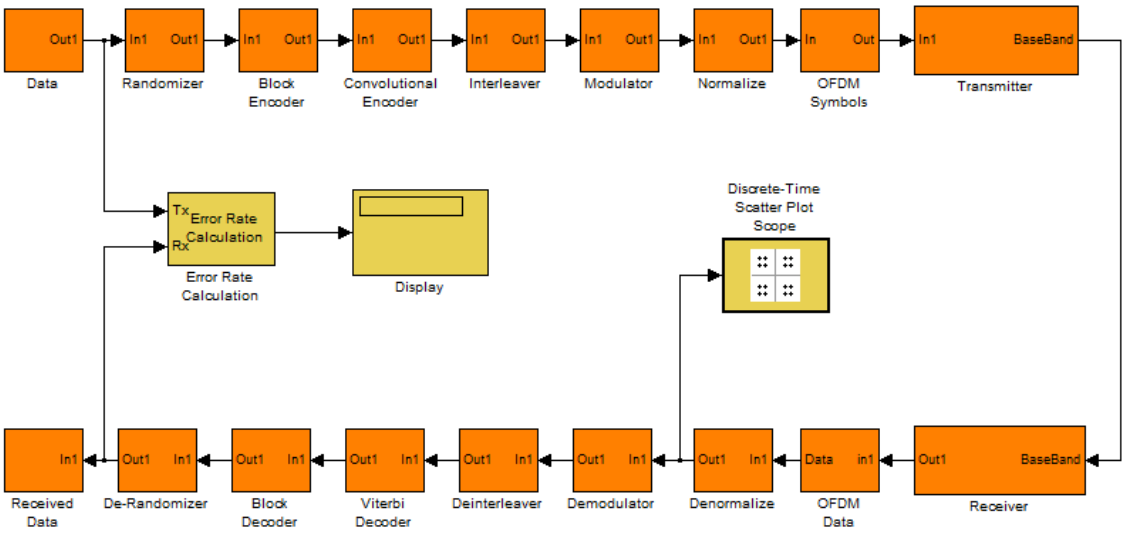
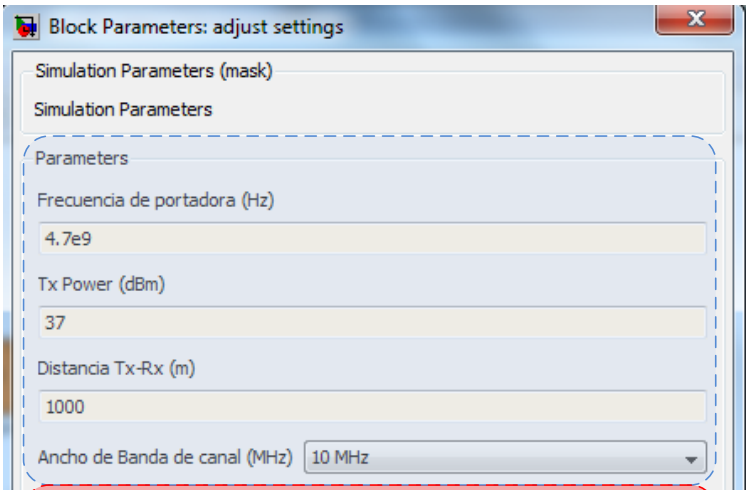


Figura 4-12: Diagrama de bloques: Escenario de control

El uso de este escenario de control permite aislar el efecto de los *jammers* tal y como se describe en los capítulos sucesivos. Sin embargo, si se introduce un modelado de atenuación de la señal de transmisión en espacio libre.

El transmisor se caracteriza mediante el diálogo de la figura inferior:



Parámetros de configuración de transmisor

Figura 4-13: Parámetros de configuración de transmisor

El transmisor se caracteriza por la frecuencia de portadora, la potencia de transmisión (en dBm), la distancia al receptor (en metros) y el ancho de banda de canal (5 o 10 MHz son los valores posibles).

4.2.2 Modelado de *jammers*

Partiendo del escenario de control, el paso lógico es modelar una serie de *jammers* y observar su impacto en las prestaciones. Para ello, se añade al modelo Simulink un bloque que introduce los efectos del canal con *jamming*.

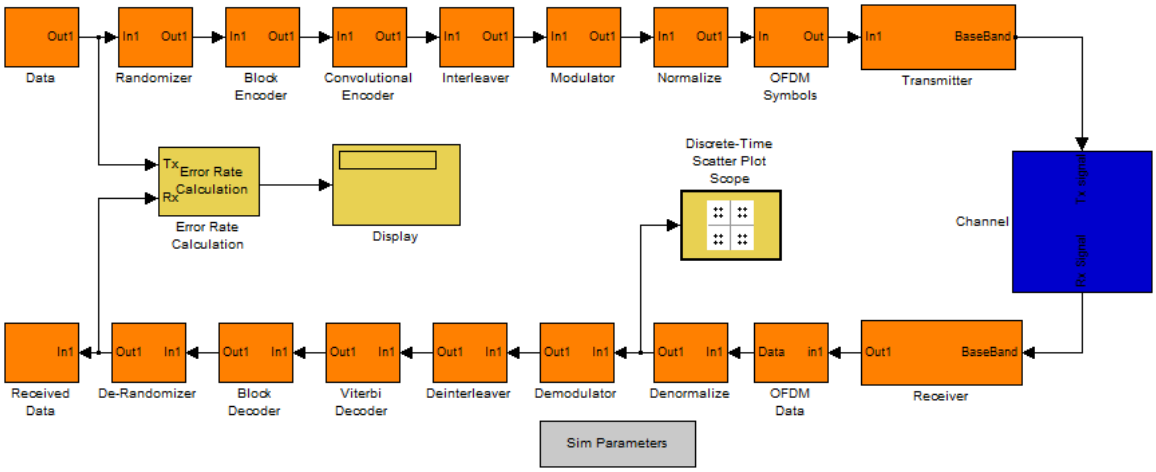
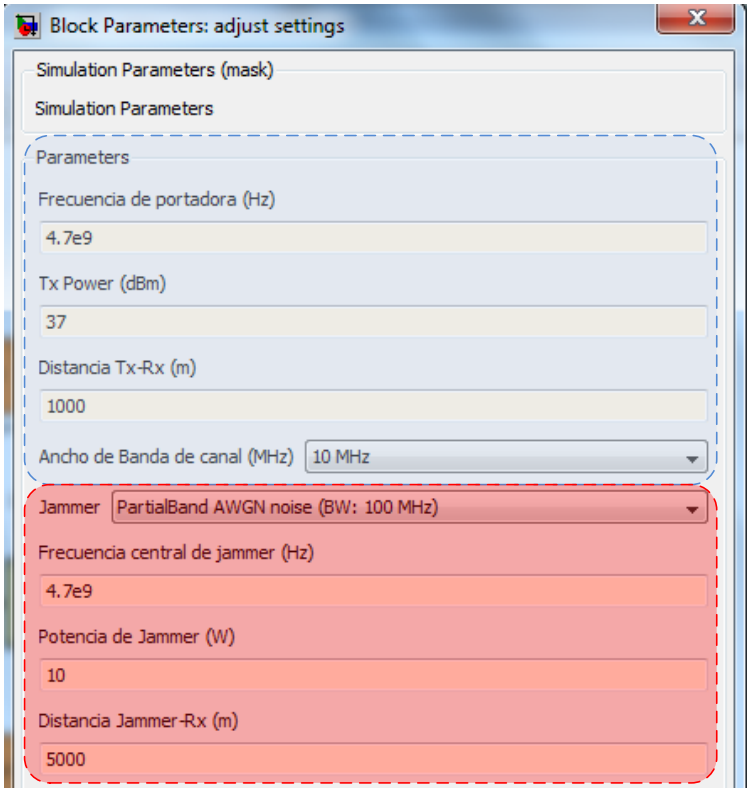


Figura 4-14: Diagrama de bloques: Modelado de *Jammers*

El escenario se caracteriza mediante el diálogo de la figura inferior. Los parámetros se pueden agrupar en dos campos: parámetros de configuración del transmisor y parámetros de configuración del *jammer*.



Parámetros de configuración de transmisor

Parámetros de configuración de jammer

Figura 4-15: Parámetros de configuración de *jamming*

Los parámetros que caracterizan el *jammer* son: el tipo de *jammer* (puede ser de banda ancha para toda la banda de operación, banda parcial de 100 MHz, 20 MHz o 10 MHz), la frecuencia central, la potencia (en vatios) y distancia al receptor (en metros).

La forma de modelar este *jammer* es haciendo pasar la señal transmitida por un canal AWGN que aplica una SNR de params.txPower-params.jammPower, donde:

- params.txPower es la potencia de señal transmitida en el receptor en dBm.
- params.jammPower es la potencia de *jamming* en recepción (calculando el porcentaje que realmente cae sobre el ancho de banda del canal).

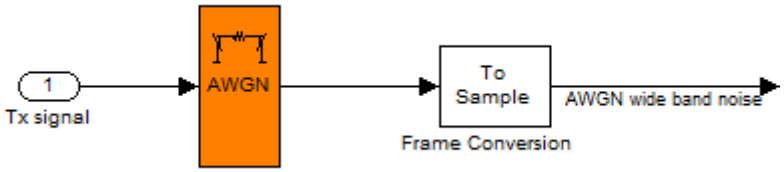


Figura 4-16: Diagrama de bloques: *Jammer* de banda ancha

Tanto la potencia de señal transmitida en recepción como la potencia de *jamming* en recepción se obtienen usando el modelo de Friis y calculando el porcentaje que realmente cae sobre la señal objetivo.

La potencia de transmisión del sistema es parametrizable así como la banda objetivo sobre la que se aplica dicha potencia.

Por un lado, el transmisor se caracteriza por la frecuencia de portadora, la potencia de transmisión (en dBm), la distancia al receptor (en metros) y el ancho de banda de canal (5 o 10 MHz son los valores posibles).
Los parámetros que caracterizan el *jammer* son: el tipo de *jammer* (puede ser de banda ancha para toda la banda de operación, banda parcial de 100 MHz, 20 MHz o 10 MHz), la frecuencia central, la potencia (en vatios) y distancia al receptor (en metros).

4.3 Resultados de simulación de escenarios

4.3.1 Escenario 1

En este escenario, se considera una base en una zona despoblada y de orografía plana (flat-terrain). A 1 kilómetro en dirección suroeste se encuentra un puesto avanzado en comunicación con la base con un terminal WiMAX vehicular (estación móvil). El puesto avanzado y la estación base intercambian información a través de este enlace (ordenes, imágenes, video, etc).

A 5 km del puesto avanzado y 6 km de la estación base se encuentra un adversario equipada con sistemas de guerra electrónica (EW). Debido a las características orográficas del terreno, todos los equipos se encuentran en línea de visión (aunque el adversario no ha sido divisado por el puesto avanzado).

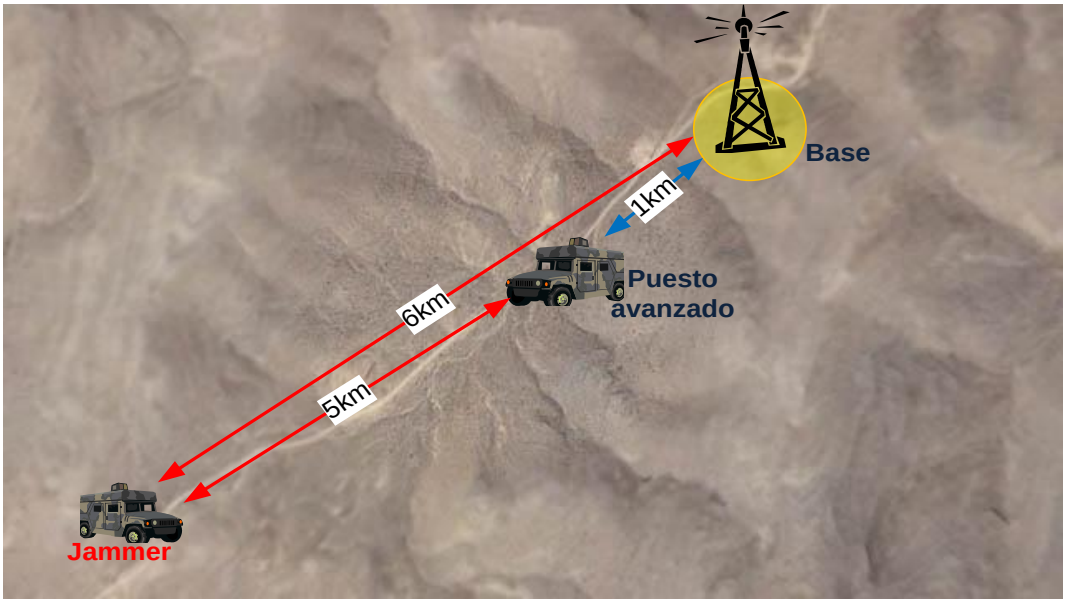


Figura 4-17: Escenario 1 - Disposición geográfica

El adversario enciende sus equipos de *jamming* para perturbar las comunicaciones entre la estación base y el puesto avanzado. Se consideran 4 variantes del escenario (A, B, C y D) en las que el adversario elige distintas estrategias de *jamming*.

Para todos los casos, se considera una estación base con potencia de transmisión de 37 dBm como la B1 descrita en el ANEXO B y un equipo móvil con una potencia de 25 dBm como el A1 descrito en el ANEXO A.

Las comunicaciones tienen lugar en la banda de 4.4 a 5 GHz (NATO-IV) y centradas en 4.7 GHz con ancho de banda de canal de 10 MHz.

4.3.1.1 Escenario 1-A

El adversario desconoce las características de la comunicación pero sabe que se utiliza la banda NATO-IV, que comprende entre 4.4 y 5 GHz. Por lo tanto, la banda objetivo tiene 600 MHz entre 4.4 y 5 GHz.

La tabla siguiente muestra el BER medido en comunicaciones entre la estación base (EB) y la estación móvil (EM) para distintas potencias de *jamming* (P_{jamm}).

BER obtenida para:	Comunicación EB-EM (*downlink*)	Comunicación EM-EB (*uplink*)
P_{jamm} = 5 W	0	0
P_{jamm} = 10 W	0	$7.02x10^{-4}$
P_{jamm} = 20 W	0	$3.14x10^{-2}$
P_{jamm} = 40 W	0	Bloqueada

Tabla 4-1: Escenario 1-A (*Jammer* de banda Ancha)

Tal y como se puede apreciar en los resultados, la comunicación desde la estación base no se ve perturbada. Sin embargo, cuando el adversario emite con potencias superiores a 5W la comunicación desde el puesto avanzado a la estación base sufre una degradación

considerable. Para potencias entre 5 y 10 W todavía se puede transmitir información con cierta calidad, como por ejemplo VoIP, pero para potencia superiores a 10W la integridad de los datos cae considerablemente dificultando la comunicación.

4.3.1.2 Escenario 1-B

En este caso, la amenaza marca como objetivo una banda de 100 MHz centrada en 4.7 GHz ya que ha detectado que las comunicaciones están teniendo lugar en frecuencias dentro de esa banda. La banda objetivo es por lo tanto de 4.65 a 4.75 GHz.

La tabla siguiente muestra el BER medido en comunicaciones entre la estación base (EB) y la estación móvil (EM) para distintas potencias de *jamming* (P_{jamm}).

BER obtenida para:	Comunicación EB-EM (*downlink*)	Comunicación EM-EB (*uplink*)
P_{jamm} = 5 W	0	0.16
P_{jamm} = 10 W	0	Bloqueada
P_{jamm} = 20 W	$1.27x10^{-3}$	Bloqueada
P_{jamm} = 40 W	$4.64x10^{-2}$	Bloqueada

Tabla 4-2: Escenario 1-B (*Jammer* de banda parcial 100MHz)

Cuando la banda atacada se estrecha a 100 MHz sobre la banda objetivo y aumenta su potencia en recepción, se bloquea la comunicación desde el puesto avanzado hacia la estación base.

Por otra parte, gracias a la mayor potencia de transmisión de la estación base, la comunicación hacia el puesto avanzado no se ve afectada para potencias de *jamming* menores a 10W. Se sufre degradación de los datos a medida que la potencia sube, perdiendo mucha cuando se acerca a los 20W.

4.3.1.3 Escenario 1-C

En este caso, la amenaza marca como objetivo una banda de 20 MHz centrada en 4.7 GHz ya que ha detectado que las comunicaciones están teniendo lugar en frecuencias dentro de esa banda. La banda objetivo es por lo tanto de 4.69 a 4.71 GHz.

La tabla siguiente muestra el BER medido en comunicaciones entre la estación base (EB) y la estación móvil (EM) para distintas potencias de *jamming* (P_{jamm}).

BER obtenida para:	Comunicación EB-EM (*downlink*)	Comunicación EM-EB (*uplink*)
P_{jamm} = 5 W	$4.9x10^{-3}$	Bloqueada
P_{jamm} = 10 W	0.11	Bloqueada
P_{jamm} = 20 W	Bloqueada	Bloqueada
P_{jamm} = 40 W	Bloqueada	Bloqueada

Tabla 4-3: Escenario 1-C (*Jammer* de banda parcial 20 MHz)

Para una banda atacada de 20 MHz centrada sobre la señal objetivo, los efectos son devastadores. La comunicación desde el puesto avanzado a la estación base queda bloqueada para cualquier potencia. La comunicación desde la estación base todavía es posible para potencias menores a 5W pero con cierta pérdida de calidad.

4.3.1.4 Escenario 1-D

En este caso, la amenaza marca como objetivo una banda de 10 MHz centrada en 4.7 GHz ya que ha detectado que las comunicaciones están teniendo lugar en frecuencias dentro de esa banda. La banda objetivo es por lo tanto de 4.695 a 4.705 GHz.

La tabla siguiente muestra el BER medido en comunicaciones entre la estación base (EB) y la estación móvil (EM) para distintas potencias de *jamming* (P_{jamm}).

BER obtenida para:	Comunicación EB-EM (*downlink*)	Comunicación EM-EB (*uplink*)
P_{jamm} = 5 W	0.11	Bloqueada
P_{jamm} = 10 W	Bloqueada	Bloqueada
P_{jamm} = 20 W	Bloqueada	Bloqueada
P_{jamm} = 40 W	Bloqueada	Bloqueada

Tabla 4-4: Escenario 1-D (*Jammer* de banda parcial 10 MHz)

Cuando la potencia de la señal perturbadora se centra sobre el objetivo con 10 MHz de ancho de banda el bloqueo de la comunicación es total.

4.3.2 Escenario 2

La celebración de un multitudinario evento se lleva a cabo en un parque a las afueras de una ciudad. Dicho parque tiene una orografía plana y está alejado de grandes edificios y obstáculos (flat-terrain).

El evento es declarado de riesgo y por lo tanto las fuerzas de seguridad llevan a cabo el despliegue de una red WiMAX móvil para coordinar las labores de vigilancia. Se despliega una estación base a 100 metros del acceso al recinto y estaciones móviles repartidas por el terreno, una de ellas en la entrada. Las estaciones móviles transmiten imágenes de videocámaras de seguridad. Desde la estación base se emiten órdenes a través de VoIP y, en caso necesario, imágenes de videocámaras de alguna de las estaciones móviles.

El acceso está vigilado por cámaras, cuya imagen se retransmite desde la estación móvil a la estación base donde se analizan en tiempo real.

Para todos los casos, se considera una estación base con potencia de transmisión de 35 dBm como la B2 descrita en el ANEXO B y un equipo móvil con una potencia de 27 dBm como el A2 descrito en el ANEXO A. Las comunicaciones tienen lugar en la banda de 2.2 a 2.4 GHz (NATO-IV) y centradas en 2.3 GHz con ancho de banda de canal de 5 MHz.

La disposición de los elementos mencionados se puede observar en la figura inferior:

Figura 4-18: Escenario 2 - Disposición geográfica

En un momento dado, un individuo con entrada no autorizada al recinto baja de un coche y camina hacia la entrada. El individuo porta oculto un dispositivo de *jamming* como el que especifica en el ANEXO C. El dispositivo emite 300 mW de potencia en la banda de 2395 MHz a 2500 MHz, por lo que actúa sobre todo el canal de comunicaciones entre el control de acceso y la estación base (5 MHz de ancho entre 2397.5 y 2402.5 MHz)

4.3.2.1 Escenario 2-A

Cuando está a 40 metros de la entrada y 140 metros de la estación base enciende el dispositivo con intención de perturbar la comunicación desde el control de acceso a la estación base y poder entrar sin ser detectado.

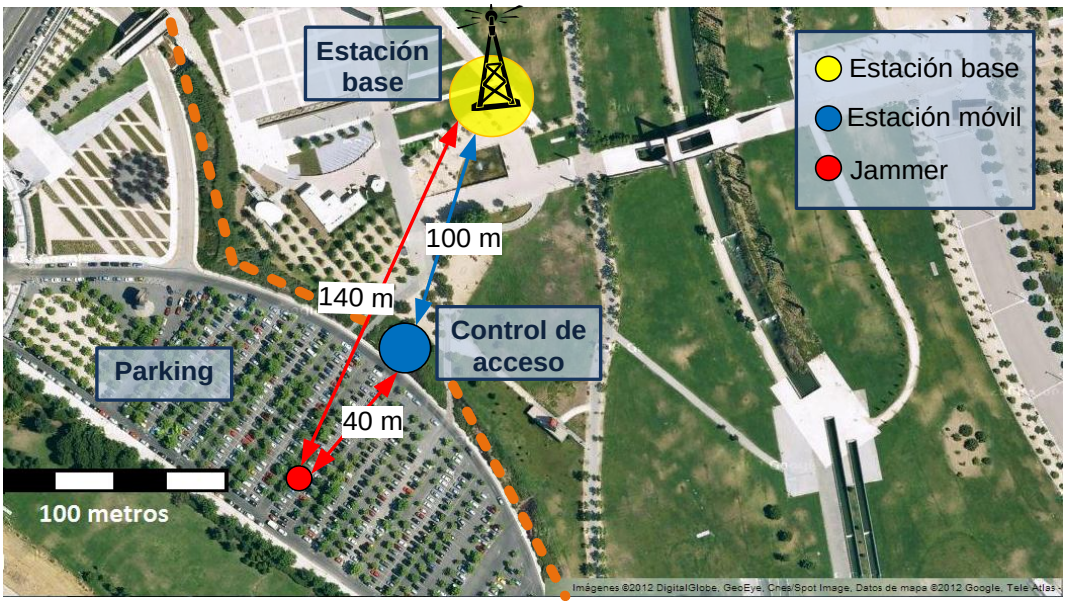


Figura 4-19: Disposición geográfica del escenario 2-A

Se definen las siguientes posiciones del individuo para analizar los efectos del dispositivo desde ellas:

- A0 – 40 metros de la entrada y 140 metros de la estación base.
- A1 – 20 metros de la entrada y 120 metros de la estación base.
- A2 – 10 metros de la entrada y 110 metros de la estación base.
- A3 – En la entrada (0 metros) y 100 metros de la estación base.

BER obtenida para:	Comunicación EB-EM (*downlink*)	Comunicación EM-EB (*uplink*)
Posición A0	$2.8x10^{-2}$	$7.31x10^{-4}$
Posición A1	Bloqueada	$4.99x10^{-3}$
Posición A2	Bloqueada	$1.2x10^{-2}$
Posición A3	Bloqueada	$2.93x10^{-2}$

Tabla 4-5: Escenario 2-A

Posición A0:
Cuando el individuo se sitúa en la posición A0 y enciende el dispositivo, perturba en gran medida la comunicación desde la estación base a la estación móvil del control de acceso. Por lo tanto dificulta o anula enormemente la posibilidad de enviar órdenes (y cualquier otro servicio). Las imágenes de video que se transmiten desde el control de acceso comienzan a llegar degradadas a la estación base.

Posición A1:
Desde la posición A1, a 20 metros de la entrada, el individuo bloquea completamente la comunicación desde la estación base. Las imágenes que se reciben en la estación base procedentes están bastante degradas, pero no se puede reaccionar y dar orden de cerrar el acceso.

Posición A2:
Con el individuo a 10 metros de la puerta, las imágenes recibidas en la estación base no permiten la analizar nada de lo que pasa en la entrada. La comunicación desde la estación base hacia el control de acceso sigue bloqueada.

Posición A3:
El individuo no autorizado está en el control de acceso. La estación base no ha recibido video con calidad para advertir la presencia del individuo. No se ha podido dar orden de cerrar la entrada, y el sujeto aprovecha la muchedumbre para acceder al recinto.

4.3.2.2 Escenario 2-B

Una vez dentro, el individuo planea dejar el dispositivo de *jamming* en un punto donde pueda bloquear completamente las comunicaciones en ambos sentidos.
Para ello, se definen las siguientes posiciones en las que el individuo puede dejar el dispositivo para analizar los efectos desde ellas:

- B1 – A 15 metros de la entrada y 85 metros de la estación base.
- B2 – A 25 metros de la entrada y 75 metros de la estación base.
- B3 – A 30 metros de la entrada y 70 metros de la estación base.

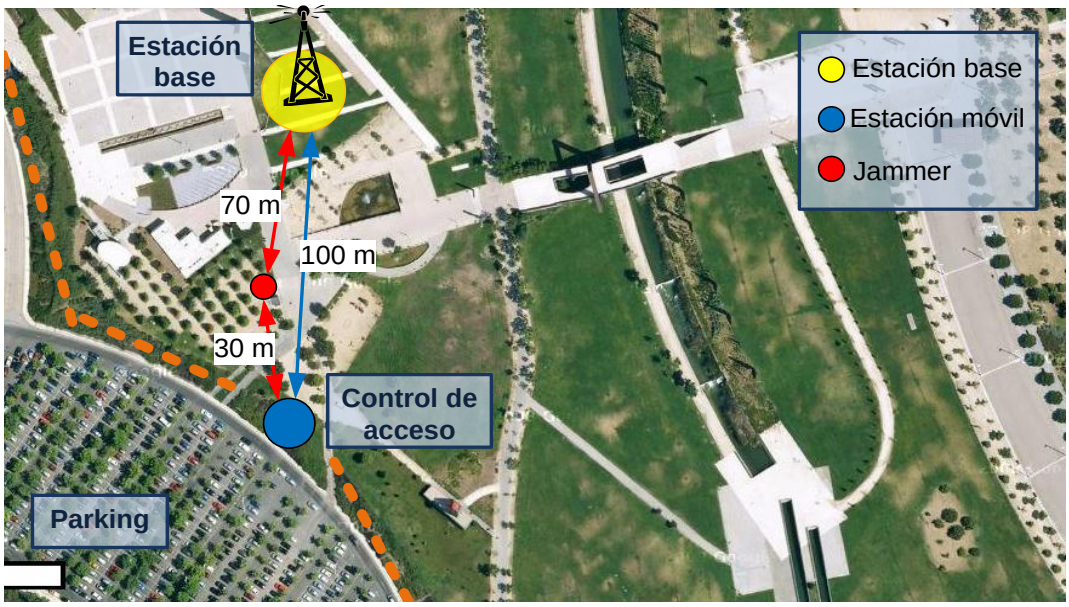


Figura 4-20: Disposición geográfica del escenario 2-B

En la siguiente tabla se muestran los resultados obtenidos desde las distintas posiciones definidas:

BER obtenida para:	Comunicación EB-EM (*downlink*)	Comunicación EM-EB (*uplink*)
Posición B1	Bloqueada	Bloqueada
Posición B2	Bloqueada	Bloqueada
Posición B3	Bloqueada	Bloqueada

Tabla 4-6: Escenario 2-B

Los resultados muestran que una vez dentro, el dispositivo puede ser depositado en cualquier sitio bloqueando completamente las comunicaciones en ambos sentidos.

4.3.3 Análisis de resultados

Con los resultados obtenidos para los escenarios propuestos se puede apreciar claramente que se ha evidenciado la vulnerabilidad del sistema WiMAX a un entorno táctico. Simulando unos *jammers* de muy poca complejidad se ha conseguido perturbar la comunicación y en algunos casos incluso bloquearla.

Se cumple así el primer objetivo del estudio que es demostrar la necesidad de aplicar algún tipo de medidas para contrarrestar el efecto de los *jammers* si se quiere poder desplegar comunicaciones WiMAX en un entorno táctico.

5 Análisis de prestaciones con medidas anti-*jamming*

En los resultados del escenario 1, se aprecia que los efectos del *jammer* de banda ancha son mínimos para potencias bajas, pero pueden afectar a las comunicaciones a medida que se aumenta la potencia. Esto se debe, tal y cómo se ha mencionado previamente, a que la energía queda esparcida a lo largo de una amplia banda del espectro.

Sin embargo, cuando la banda atacada comienza a estrecharse sobre la señal transmitida, los efectos aumentan gradualmente hasta bloquear completamente la comunicación. Al estrechar la banda atacada, algunas frecuencias quedan libres de sus efectos, por lo que se propone la introducción de la técnica de salto de frecuencia o Frequency Hopping (FH) de cara a explotar esas frecuencias.

Debido a que el *jammers* se centra en atacar determinadas frecuencias, se propone esta medida como explotación de la diversidad de frecuencias.

5.1 Definición Frequency Hopping

Esta técnica consiste en que transmisor y receptor no operan en una frecuencia fija, sino que cada cierto intervalo de tiempo (periodo de salto) se modifica la frecuencia en la que se está transmitiendo. Esto significa que la frecuencia de portadora cambia cada "salto" de forma pseudo-aleatoria. Transmisor y receptor utilizan una secuencia pseudo-aleatoria generada con un algoritmo y semilla conocidos para asegurar que en cada instante ambos estarán operando en la misma frecuencia. Esta técnica exige además un alto grado de sincronismo en tiempo a la hora de saltar de frecuencia.

El funcionamiento del FH es el siguiente:

- Se divide la banda de operación en un *grid* de frecuencias; esto es, frecuencias portadoras a las que se puede saltar en un momento dado.
- Se determina un periodo de salto; esto es, cada cuánto se salta a una frecuencia distinta.
- Se utiliza un algoritmo que genere una secuencia pseudo-aleatoria con una clave que conocen transmisor y receptor. A partir de esta secuencia se determina que frecuencia del *grid* se usa en un momento dado.

El FH se introduce en el modelo Simulink de la siguiente forma:

- Como parámetro de simulación se selecciona un *jammer* con una frecuencia central (fc_jamm) y ancho de banda (BW_jamm) determinados.
- Un generador de números aleatorios selecciona cada periodo de salta una frecuencia portadora (fc) dentro de la banda de operación. La señal transmitida tiene un ancho de banda BW.
- Se compara la banda que ocupará la señal en el espectro para esa frecuencia de portadora (de fc-BW/2 hasta fc+BW/2) con la banda objetivo del *jammer* (de fc_jamm-BW_jamm/2 a fc_jamm+BW/2).
    - Si existe solape entre las bandas, se considera que la señal ha sido perturbada.

- Si no existe solape entre las bandas, se considera que la señal se ha transmitido sin perturbación por parte del *jammer*.

- En el caso de que la frecuencia se considera perturbada, la señal transmitida se procesa tal y como se hace en el capítulo 4.2 para los escenarios con *jamming*. La señal transmitida se pasa por un canal AWGN con una SNR que depende la potencia de la señal transmitida y la potencia del *jammer*.

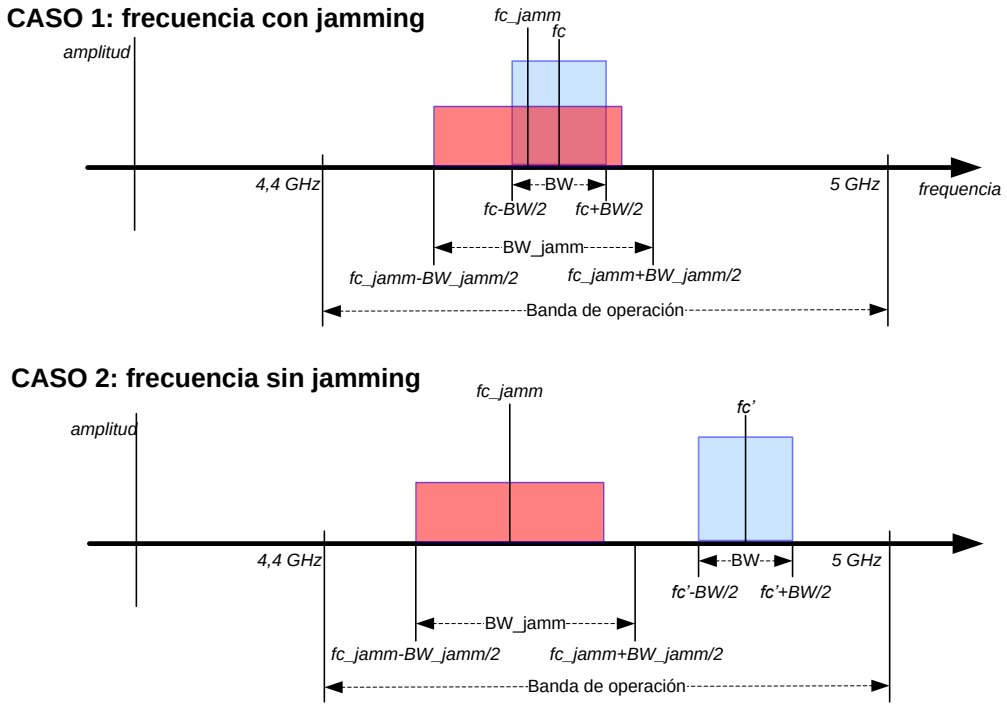


Figura 5-1: Comparación de frecuencia de FH con *jammer*

5.2 Modelado de Frequency Hopping

Como la simulación del escenario se hace en banda base, es necesario un bloque que analice los parámetros de simulación para determinar en cada momento como afecta el *jammer* a la señal en función de la banda objetivo del *jammer* y la frecuencia de portadora de la señal transmitida. Para ello se introduce un bloque que decide tal y como se ha descrito anteriormente si la señal es afectada por el *jamming* o no. En la siguiente figura se puede apreciar el diagrama de bloques correspondiente:

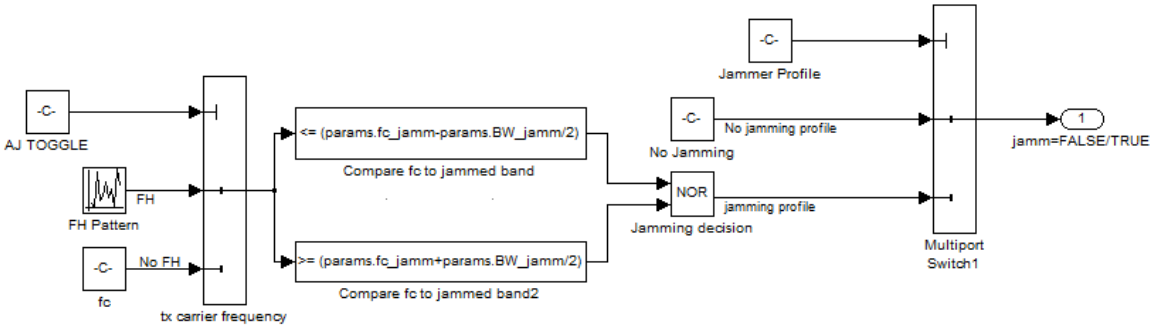


Figura 5-2: Diagrama de bloques: Comparación de frecuencia de FH con *jammer*

El primer multiplexador decide la frecuencia en la que se transmite la señal: la generada para el FH si el AJ está activado o la frecuencia de portadora elegida para la simulación si el AJ está desactivado.

Posteriormente se compara esa frecuencia con la banda objetivo del *jammer*, determinada por los parámetros de simulación params.fc_jamm (frecuencia central) y params.BW_jamm (ancho de banda).

Si la frecuencia de la señal transmitida cae en la banda objetivo del *jammer*, se considera que la señal es afectada por el *jamming* (TRUE) y se simula tal y como se describió en el apartado de *jammers* (4.2). Si por el contrario la frecuencia queda fuera de la banda atacada por el *jammer*, se considera que la señal transmitida no ha sido perturbada y llega intacta al receptor.

Este cálculo cambia cada vez que el generador de frecuencias de salto cambia la frecuencia de portadora.

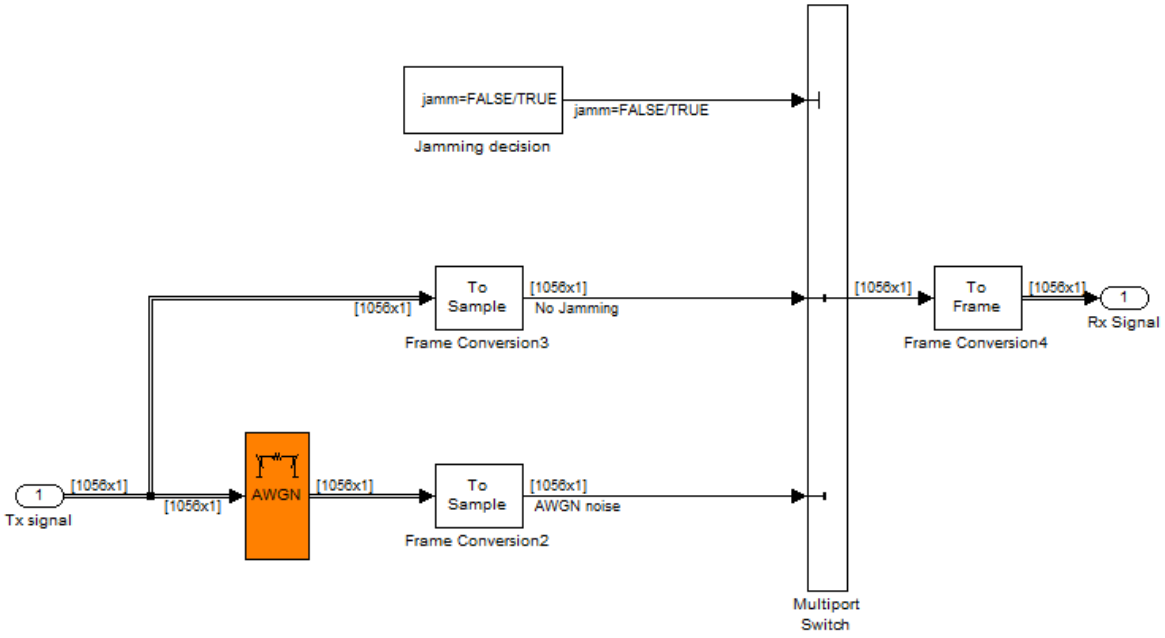


Figura 5-3: Diagrama de bloques: Introducción de *jamming* en la señal recibida

En la figura anterior se puede observar el diagrama de bloques de la introducción de *jamming* en función de la salida del bloque decisor.

Mediante el siguiente diálogo se puede caracterizar el escenario para un transmisor y *jammer* determinados y activar o desactivar las medidas AJ.

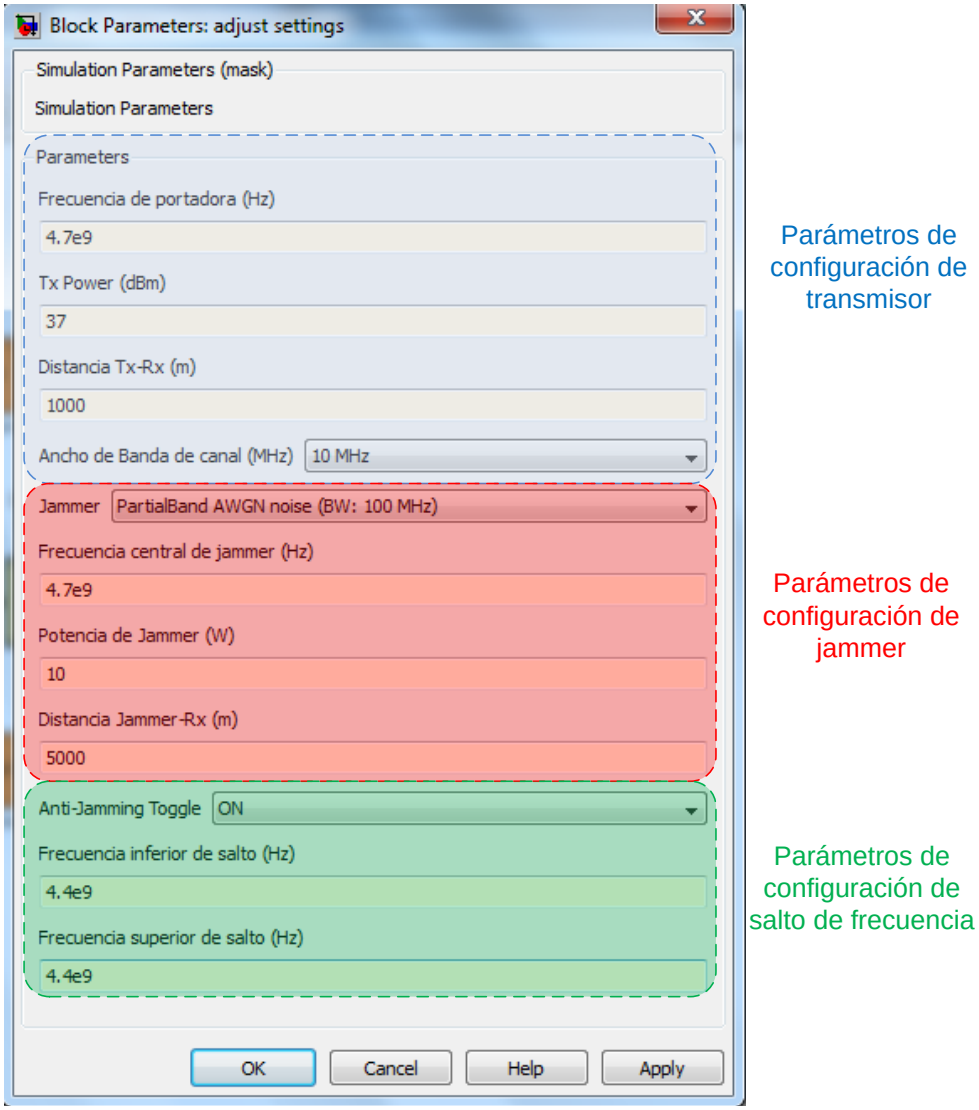


Figura 5-4: Parámetros de configuración con AJ

Por un lado, el transmisor se caracteriza por la frecuencia de portadora, la potencia de transmisión (en dBm), la distancia al receptor (en metros) y el ancho de banda de canal (5 o 10 MHz son los valores posibles).

Los parámetros que caracterizan el *jammer* son: el tipo de *jammer* (puede ser de banda ancha para toda la banda de operación, banda parcial de 100 MHz, 20 MHz o 10 MHz), la frecuencia central, la potencia (en vatios) y distancia al receptor (en metros).

Las medidas AJ se pueden activar mediante el parámetro Anti-*jamming* Toggle (ON/OFF) y se caracterizan definiendo la banda sobre la que puede saltar el sistema con una frecuencia portadora de salto inferior y superior.

5.3 Resultados de simulación con Frequency Hopping

Dado que todas las frecuencias de salto son equiprobables (distribución probabilística uniforme), la decisión del *jammer* es elegir una frecuencia cualquiera dentro de la banda de operación. El porcentaje de saltos con éxito (salto a una frecuencia libre de *jamming*) depende del número de frecuencias del grid que abarca la banda objetivo del *jammer*.

Esta técnica no ofrece mejora de prestaciones frente al *jammer* de banda ancha debido a que se asume que en dicho escenario el *jamming* abarca toda la banda de operación del sistema (todas las frecuencias tienen *jamming*). Los resultados serán los mismos que los obtenidos en el capítulo 4.

Sin embargo, frente al *jammer* de banda parcial, dado que solo abarca parte de las frecuencias de salto, se debe analizar el comportamiento del sistema con FH para determinar las nuevas prestaciones.

5.3.1 Escenario 1

Se considera que el sistema puede saltar a cualquier frecuencia dentro de la banda de operación (4.4 a 5 GHz).

A continuación se muestra la simulación para los escenarios 1-B, 1-C, 1-D, 2-B, 2-C y 2-D activando las medidas AJ en el sistema.

5.3.1.1 Escenario 1-B

En este caso, la amenaza marca como objetivo una banda de 100 MHz centrada en 4.7 GHz ya que ha detectado que las comunicaciones están teniendo lugar en frecuencias dentro de esa banda. La banda objetivo es por lo tanto de 4.65 a 4.75 GHz.

La tabla siguiente muestra el BER medido en comunicaciones entre la estación base (EB) y la estación móvil (EM) para distintas potencias de *jamming* (P_{jamm}).

BER obtenida para:	Comunicación EB-EM (*downlink*)	Comunicación EM-EB (*uplink*)
P_{jamm} = 5 W	0	$2.59x10^{-2}$
P_{jamm} = 10 W	0	16.7% Bloqueada
P_{jamm} = 20 W	$2.62x10^{-4}$	16.7% Bloqueada
($1P_{jamm}$ = 40 W	$7.99x10^{-3}$	16.7% Bloqueada

Tabla 5-1: Escenario 1-B con FH (*Jammer* de banda parcial 100MHz)

Dado que la frecuencia de portadora de la comunicación entre la estación base y el puesto avanzado no es fija, no todas las transmisiones se ven afectadas. Dada la relación entre rango de frecuencias de salto (600 MHz) y el porcentaje de esas frecuencias que están bajo los efectos del perturbador, solo el 16.7% de los saltos se verán afectados. Esto se ve reflejado en los resultados de la tabla anterior. Es importante identificarlo como tal y no con un valor de BER porque con ciertos mecanismos se puede conseguir una comunicación aceptable para algunos servicios (ver capítulo 6).

5.3.1.2 Escenario 1-C

En este caso, la amenaza marca como objetivo una banda de 20 MHz centrada en 4.7 GHz ya que ha detectado que las comunicaciones están teniendo lugar en frecuencias dentro de esa banda. La banda objetivo es por lo tanto de 4.69 a 4.71 GHz.

La tabla siguiente muestra el BER medido en comunicaciones entre la estación base (EB) y la estación móvil (EM) para distintas potencias de *jamming* (P_{jamm}).

BER obtenida para:	Comunicación EB-EM (*downlink*)	Comunicación EM-EB (*uplink*)
P_{jamm} = 5 W	$1.76x10^{-4}$	3.33% Bloqueada
P_{jamm} = 10 W	$3.8x10^{-3}$	3.33% Bloqueada
P_{jamm} = 20 W	3.33% Bloqueada	3.33% Bloqueada
P_{jamm} = 40 W	3.33% Bloqueada	3.33% Bloqueada

Tabla 5-2: Escenario 1-C con FH (*Jammer* de banda parcial 20 MHz)

Con un ancho de banda atacado de 20 MHz y rango de frecuencias de salto de 600 MHz, el porcentaje de frecuencias que están bajo los efectos del perturbador son solo el 3.33% de los saltos se verán afectados. Esto se ve reflejado en los resultados de la tabla anterior. Al igual que en el caso anterior, es importante identificarlo como tal y no con un valor de BER porque con ciertos mecanismos se puede conseguir una comunicación aceptable para algunos servicios (ver capítulo 6).

5.3.1.3 Escenario 1-D

En este caso, la amenaza marca como objetivo una banda de 10 MHz centrada en 4.7 GHz ya que ha detectado que las comunicaciones están teniendo lugar en frecuencias dentro de esa banda. La banda objetivo es por lo tanto de 4.695 a 4.705 GHz.

La tabla siguiente muestra el BER medido en comunicaciones entre la estación base (EB) y la estación móvil (EM) para distintas potencias de *jamming* (P_{jamm}).

BER obtenida para:	Comunicación EB-EM (*downlink*)	Comunicación EM-EB (*uplink*)
P_{jamm} = 5 W	$1.6x10^{-3}$	1.67% Bloqueada
P_{jamm} = 10 W	1.67% Bloqueada	1.67% Bloqueada
P_{jamm} = 20 W	1.67% Bloqueada	1.67% Bloqueada
P_{jamm} = 40 W	1.67% Bloqueada	1.67% Bloqueada

Tabla 5-3: Escenario 1-D con FH (*Jammer* de banda parcial 10 MHz)

Con un ancho de banda atacado de 10 MHz y rango de frecuencias de salto de 600 MHz, el porcentaje de frecuencias que están bajo los efectos del perturbador son solo el 1.67% de los saltos se verán afectados. Esto se ve reflejado en los resultados de la tabla anterior. Al igual que en el caso anterior, es importante identificarlo como tal y no con un valor de BER porque con ciertos mecanismos se puede conseguir una comunicación aceptable para algunos servicios (ver capítulo 6).

5.3.2 Escenario 2

Se considera que el sistema puede saltar a cualquier frecuencia dentro de la banda de operación (2.2 a 2.4 GHz).

A continuación se muestra la simulación para los escenarios 2-A y 2-B activando las medidas AJ en el sistema.

5.3.2.1 Escenario 2-A

BER obtenida para:	Comunicación EB-EM (*downlink*)	Comunicación EM-EB (*uplink*)
Posición A0	$7.69x10^{-4}$	$1.4x10^{-5}$
Posición A1	2.5% Bloqueada	$1.3x10^{-4}$
Posición A2	2.5% Bloqueada	$3.46x10^{-4}$
Posición A3	2.5% Bloqueada	$8.22x10^{-4}$

Tabla 5-4: Escenario 2-A

Con la banda de frecuencias de salto del sistema y la banda atacada por el dispositivo, solo el 2.5% de frecuencias están bajo los efectos del *jammer*. El 97.5% de los saltos serán a frecuencias libres de perturbación y la comunicación se verá afectada pero en ningún caso bloqueada.

La comunicación se verá interrumpida cada cierto tiempo durante un corto intervalo debido a salto a una frecuencia atacada. Sin embargo, ajustando adecuadamente el periodo de salto se pueden conseguir largos intervalos de tiempo en los que la comunicación está libre de errores. Por lo que se reciben imágenes que se pueden analizar en la estación base y se pueden dar ordenes al respecto al control de acceso. Esta situación se da en cualquier posición del individuo que lleva el dispositivo mientras se acerca a la entrada. Por lo tanto, ante la sospecha de la cierta degradación de las comunicaciones, se puede elevar el nivel de alerta y dar órdenes de cerrar la entrada o analizar exhaustivamente a los sujetos que entran. Se ha dificultado o impedido el acceso del individuo no autorizado al recinto.

5.3.2.2 Escenario 2-B

BER obtenida para:	Comunicación EB-EM (*downlink*)	Comunicación EM-EB (*uplink*)
Posición B1	2.5% Bloqueada	2.5% Bloqueada
Posición B2	2.5% Bloqueada	2.5% Bloqueada
Posición B3	2.5% Bloqueada	2.5% Bloqueada

Tabla 5-5: Escenario 2-B

Al igual que para el escenario 2-A, la comunicación se verá interrumpida cada cierto tiempo, pero durante intervalos de tiempo la comunicación será correcta, lo que permite

cierto margen de maniobra. En el capítulo 6 se mencionan mecanismos que permiten aprovechar estos periodos de correcto funcionamiento de las comunicaciones.

5.3.1 Análisis de resultados

Con los resultados obtenidos tras la aplicación de salto de frecuencia al sistema WiMAX se puede apreciar la mejora en las prestaciones para los mismos escenarios de entorno táctico que se consideraron en el capítulo 4.

Se cumple así el segundo objetivo del estudio que es demostrar la efectividad de unas sencillas medidas anti-*jamming* para contrarrestar la vulnerabilidad del sistema en entornos tácticos.

6 Conclusiones y trabajo futuro

6.1 Efecto de las medidas Anti-Jamming

De cara a ofrecer una clara visión del efecto de las medidas anti-*jamming* introducidas en el sistema se ofrecen a continuación tablas resumen con todos los resultados de los dos escenarios considerados con medidas anti-*jamming* y sin ellas. Asimismo, se ofrecen unas conclusiones de cada escenario analizando las prestaciones del sistema WiMAX en cada caso.

Para obtener estos resultados se ha usado un modelado de equipos y escenarios que se describe detalladamente en los capítulos 4 y 5. Destaca el uso de un proyecto de Simulink para modelar transmisor, receptor y perturbador caracterizándolos para distintos escenarios. También con Simulink se modela la adaptación del sistema para entornos tácticos con la inclusión de salto de frecuencia. El modelo de Simulink usado está descrito en los capítulos 4 y 5.

6.1.1 Escenario 1

En el escenario 1 se analiza el efecto de un perturbador situado a cierta distancia de una estación base y un equipo móvil. Las comunicaciones de la estación base al equipo móvil (*downlink*) representan principalmente ordenes concisas mediante mensajes cortos a través de servicios VoIP y transferencias de datos esporádicas (por ejemplo imágenes). Las comunicaciones desde el equipo móvil a la estación base (*uplink*) representan envío de mensajes VoIP como contestación a órdenes y tráfico más pesado de que pueden ser en tiempo real (por ejemplo imágenes de video) o no (por ejemplo información de sensores).

Primero se analizan las prestaciones del enlace considerando que las medidas anti-*jamming* están desconectadas de cara al primer objetivo del proyecto (demostrar la vulnerabilidad del sistema convencional en entornos tácticos). Para ello se utilizan distintos perturbadores sencillos pero efectivos y con distintas potencias de transmisión.

Tanto los perturbadores como los equipos seleccionados son representativos de los que podrían encontrarse en un entorno táctico típico. En los anexos A1 y B1 se incluyen las hojas de especificación de equipos reales comercializados por empresas del sector. Dichas especificaciones se utilizan para caracterizar los transmisores y receptores del escenario considerado.

A continuación se analizan las prestaciones del enlace tras la inclusión del mecanismo de salto de frecuencia para demostrar el aumento de robustez con sencillas adaptaciones.

La siguiente tabla muestra una comparativa de prestaciones entre el sistema sin modificar (AJ OFF) y el uso del salto de frecuencia (AJ ON) para todos los tipos de *jammer* considerados (ver capítulo 4.3.1):

BER obtenida para: (Tipo/potencia)		Comunicación EB-EM (*downlink*)		Comunicación EM-EB (*uplink*)	
		AJ OFF	AJ ON	AJ OFF	AJ ON
Banda Ancha (4.4 – 5 GHz)	5 W	0	0	0	0
	10 W	0	0	$7.02x10^{-4}$	$7.02x10^{-4}$
	20 W	0	0	$3.14x10^{-2}$	$3.14x10^{-2}$
	40 W	0	0	Bloqueada	Bloqueada
Banda parcial 100 MHz (4.65 – 4.75 GHz)	5 W	0	0	0.16	$2.59x10^{-2}$
	10 W	0	0	Bloqueada	16.7 % Bloqueada
	20 W	$1.27x10^{-3}$	$2.62x10^{-4}$	Bloqueada	16.7 % Bloqueada
	40 W	$4.64x10^{-2}$	$7.99x10^{-3}$	Bloqueada	16.7 % Bloqueada
Banda parcial 20 MHz (4.69 – 4.71 GHz)	5 W	$4.9x10^{-3}$	$1.76x10^{-4}$	Bloqueada	3.3 % Bloqueada
	10 W	0.11	$3.8x10^{-3}$	Bloqueada	3.3 % Bloqueada
	20 W	Bloqueada	3.3 % Bloqueada	Bloqueada	3.3 % Bloqueada
	40 W	Bloqueada	3.3 % Bloqueada	Bloqueada	3.3 % Bloqueada
Banda parcial 10 MHz (4.695 – 4.705 GHz)	5 W	0.11	$1.6x10^{-3}$	Bloqueada	1.67 % Bloqueada
	10 W	Bloqueada	1.67 % Bloqueada	Bloqueada	1.67 % Bloqueada
	20 W	Bloqueada	1.67 % Bloqueada	Bloqueada	1.67 % Bloqueada
	40 W	Bloqueada	1.67 % Bloqueada	Bloqueada	1.67 % Bloqueada

Tabla 6-1 : Resumen de prestaciones en escenario 1

Se considera que una comunicación está bloqueada cuando las prestaciones no permiten la realización de los servicios que se requieren de ella debido a la tasa de error. Por otra parte, se puede considerar que una comunicación está bloqueada con un porcentaje y el significado de esto se explica en las conclusiones presentadas a continuación.

Por ejemplo, se considera que no se puede proporcionar servicio de audio o video en *streaming* (servicios principales considerados en estos escenarios) si la BER es mayor del orden de 10^{-4}.

Las conclusiones están agrupadas para detallar las prestaciones del sistema frente a los distintos perturbadores propuestos:

Jammer de banda ancha (4.4 – 5 GHz)

El *jammer* de banda ancha tiene poco efecto sobre la comunicación para las potencias más bajas consideradas dado que reparte su energía a lo largo de un amplio espectro. Sin embargo, para las potencias más altas se consigue hacer disminuir la calidad de la comunicación desde el puesto avanzado hacia la estación base, llegando incluso a bloquearlas. Dado que las frecuencias de salto están todas incluidas dentro de la banda atacada por el adversario, no se mejoran las prestaciones con la inclusión de esta medida AJ contra este *jammer* (todos los saltos son a frecuencias atacadas).

Jammer de banda parcial de 100 MHz (4.65 – 4.75 GHz)

Cuando el *jammer* estrecha la banda a 100 MHz, la potencia está más concentrada sobre la banda ocupada por las comunicaciones entre la estación base y el puesto avanzado (dado que la banda atacada está centrada sobre ésta). Para las potencias más bajas consideradas la comunicación desde la estación base no se ve afectada debido a la gran potencia de transmisión. Las potencias de *jamming* más altas si degradan la calidad de la señal recibida y el valor de BER resultante hace que algunos servicios dejen de estar disponibles. Sin

embargo, las comunicaciones del puesto avanzado, que cuenta con menor potencia de transmisión, se ven gravemente afectadas y quedan bloqueadas.

Con la introducción de salto de frecuencia se observa que la calidad de la comunicación desde la estación base hacia el puesto avanzado mejora de forma considerable, permitiendo así la reanudación de servicios que podrían haber quedado bloqueados por la degradación. Las comunicaciones desde el puesto avanzado hacia la estación base, que antes estaban completamente bloqueadas pasan a funcionar sin errores el 83.3% de las veces. Esto se debe a que el 83.3% de los saltos son a frecuencias fuera de los efectos del perturbador. Esto puede ser insuficiente para algunos servicios en tiempo real, pero algunos servicios pueden seguir funcionando (transferencia de datos "*best-effort*" por ejemplo). Otra forma de permitir algún servicio de tiempo real como voz o video es aumentar el tiempo de salto de tal forma que una vez se puedan hacer ráfagas largas sin perturbación (hasta que se vuelve a saltar a una frecuencia con *jamming*. Esto permite envío de órdenes breves y concisas a través de VoIP o transferencia de video a ráfagas.

Jammer de banda parcial de 20 MHz (4.69 – 4.71 GHz)
A medida que se sigue disminuyendo el ancho de banda objetivo hasta los 20MHz, aumentan los efectos perturbadores sobre la comunicación. Solo para potencias inferiores a 5 W es posible la comunicación desde la estación base hacia el puesto avanzado. Algunos servicios quedan en cualquier caso anulados. Las comunicaciones desde el puesto avanzado hacia la estación base quedan de nuevo bloqueadas.
Frente a este *jammer*, la introducción de salto de frecuencia hace que vuelva a ser posible la realización de algunos servicios en tiempo real para las potencias más bajas de perturbador. El resto de comunicaciones entre estación base y puesto avanzado (en ambas direcciones) pasan de estar completamente bloqueadas a funcionar sin errores el 96.7% de las veces. Esto se debe a que solo el 3.3% de los saltos son a frecuencias bajo los efectos del perturbador. Al igual que se ha descrito para el caso anterior, esto permite la realización de algunos servicios que antes estaban anulados. También modificando el periodo de salto se pueden conseguir ráfagas largas sin perturbación que permiten servicios en tiempo real durante periodos de tiempos.

Jammer de banda parcial de 10 MHz (4.695 – 4.705 GHz)
Cuando el *jammer* concentra toda su potencia sobre la banda ocupada por las comunicaciones entre la base y el puesto avanzado, sus efectos son devastadores. Todas las comunicaciones en ambos sentidos quedan bloqueadas incluso para las potencias de *jamming* más bajas que se han considerado.

Al aplicar salto de frecuencia en este caso, se consigue que el 98.3% de las transmisiones sean fuera de la banda afectada por el adversario, que ocupa solo 1.67% de los saltos. De nuevo, esto permite algunos tipos de comunicación que antes estaban completamente anulados.

6.1.2 Escenario 2

En el escenario 2 se analiza el efecto de un perturbador que se sitúa en distintas posiciones y distancias respecto a una estación base y un equipo móvil. Las comunicaciones de la estación base al equipo móvil (*downlink*) representan principalmente ordenes concisas mediante mensajes cortos a través de servicios VoIP y transferencias de datos esporádicas (por ejemplo imágenes o video). Las comunicaciones desde el equipo móvil a la estación

base (*uplink*) representan envío más pesado y constante de datos en tiempo real (por ejemplo imágenes de video).

Primero se analizan las prestaciones del enlace considerando que las medidas anti-*jamming* están desconectadas de cara al primer objetivo del proyecto (demostrar la vulnerabilidad del sistema convencional en entornos tácticos). Para ello se consideran distintas posiciones del perturbador, ya que debido a su tamaño tiene gran portabilidad (ver anexo C).

A continuación se analizan las prestaciones del enlace tras la inclusión del mecanismo de salto de frecuencia para demostrar el aumento de robustez con sencillas adaptaciones. Este escenario es muy interesante ya que demuestra la vulnerabilidad del sistema inicial con un dispositivo de *jamming* con características similares a otros dispositivos que se pueden adquirir con gran facilidad a través de internet.

La siguiente tabla muestra una comparativa de prestaciones entre el sistema sin modificar (AJ OFF) y el uso del salto de frecuencia (AJ ON) para todas las posiciones consideradas (ver capítulo 4.3.2):

BER obtenida para:	Comunicación EB-EM (*downlink*)		Comunicación EM-EB (*uplink*)	
	AJ OFF	AJ ON	AJ OFF	AJ ON
Posición A0	$2.8x10^{-2}$	$7.69x10^{-4}$	$7.31x10^{-4}$	$1.4x10^{-5}$
Posición A1	Bloqueada	2.5% Bloqueada	$4.99x10^{-3}$	$1.3x10^{-4}$
Posición A2	Bloqueada	2.5% Bloqueada	$1.2x10^{-2}$	$3.46x10^{-4}$
Posición A3	Bloqueada	2.5% Bloqueada	$2.93x10^{-2}$	$8.22x10^{-4}$
Posición B1	Bloqueada	2.5% Bloqueada	Bloqueada	2.5% Bloqueada
Posición B2	Bloqueada	2.5% Bloqueada	Bloqueada	2.5% Bloqueada
Posición B3	Bloqueada	2.5% Bloqueada	Bloqueada	2.5% Bloqueada

Tabla 6-2: Resumen de prestaciones en escenario 2

Al igual que para el escenario anterior, se considera que no se puede proporcionar servicio de audio o video en *streaming* (servicios principales considerados en estos escenarios) si la BER es mayor del orden de 10^{-4}.

Se puede obtener de la tabla anterior que el dispositivo de *jamming* portátil, a pesar de su potencia limitada puede afectar gravemente a las comunicaciones gracias a su portabilidad. Cuando el dispositivo se acerca lo suficiente al receptor, la comunicación queda totalmente bloqueada.

Introducir el mecanismo de salto de frecuencia supone un aumento significativo de las prestaciones tal y como se refleja en las mejoras de BER de la tabla. Asimismo, comunicaciones que estaban completamente bloqueadas pasan a estarlo solo 2.5% del tiempo (porcentaje de saltos que son a frecuencias atacadas por el dispositivo). Esto permite cierto margen de maniobra para conseguir mantener algunos servicios funcionando.

Al igual que el escenario es interesante debido a la evidencia de la vulnerabilidad del sistema ante un *jamming* de fácil adquisición, se demuestra que la aplicación de una

sencilla técnica como el salto de frecuencia tiene grandes efectos positivos de cara a contrarrestar el efecto del *jammer*.

6.2 Conclusiones generales

De los resultados en ambos escenarios sin medidas AJ se aprecia que las comunicaciones mediante WiMAX móvil son vulnerables a ataques mediante *jamming*. En el primer escenario se comprueba como mediante el uso de potentes *jammers* se puede dificultar o bloquear las comunicaciones entre una base de operaciones y un puesto avanzado desde una distancia considerable. En el segundo escenario se comprueba como se puede bloquear las comunicaciones de un enlace WiMAX mediante un simple dispositivo portátil. Se puede adquirir un dispositivo de similares características con facilidad por internet, lo que pone claramente de manifiesto la vulnerabilidad del sistema. Éste era el primer objetivo del proyecto.

El segundo objetivo consiste en la demostración de que el sistema se puede adaptar para ganar robustez en los entornos tácticos. Tras la aplicación de salto de frecuencia, se puede observar mejora de las prestaciones en todos los casos de ambos escenarios propuestos. En unos casos se disminuye la BER dando así la posibilidad de establecer servicios de comunicación que de otra forma quedaban anulados. En los casos en los que la comunicación había quedado totalmente anulada, tras aplicar el salto de frecuencia se conseguía establecer en cierto grado la comunicación. Por lo tanto, queda cubierto el segundo objetivo planteado.

Por contrapartida, el uso de salto de frecuencia tiene dos desventajas principales:

- El mayor uso de ancho de banda que de otra manera quedaba libre para otras comunicaciones.
    - Dicha desventaja se puede contrarrestar haciendo que todos los enlaces hagan salto en frecuencia ortogonal. Esto es, que todos saltan a la vez y nunca una frecuencia es usada por dos comunicaciones distintas en un mismo instante. Los saltos de frecuencias ortogonales se consiguen mediante algoritmos de generación de patrones de salto que utilizan semillas y claves conocidas por todos los nodos de la red.
- El salto en frecuencia requiere un alto grado de sincronismo en tiempo entre todos los nodos de modo que transmisor y receptor/es estén en la misma frecuencia en el instante adecuado y durante un intervalo de tiempo suficiente para escuchar toda la señal.
    - Esta complejidad está tenida en cuenta en sistemas que utilizan salto de frecuencia como medida de protección frente a perturbaciones intencionadas.

La conclusión que se puede obtener del análisis es que la aplicación de técnicas anti-*jamming* como el salto de frecuencia a un sistema de comunicaciones WiMAX es viable y facilita su operación en entornos tácticos. De cara a mejorar las prestaciones del sistema se podría complementar el salto de frecuencia con medidas adicionales más complejas.

Un sistema de comunicaciones de tales características ofrece una gran flexibilidad y capacidad de transferencia de información con robustez suficiente como para operar en entornos con presencia de *jamming*. Este resultado cumple el objetivo principal del

proyecto ya que se demuestra la viabilidad de una sencilla adaptación del sistema WiMAX para robustecer sus prestaciones en entornos tácticos.

6.3 Trabajo futuro

Considerando un receptor más complejo con ecualización y estima de canal y sincronización se podría analizar la posible mejora de prestaciones frente a otros tipos de *jammer* más complejos. Esto conllevaría el uso de las subportadoras piloto al principio de la cadena de recepción.

El uso de portadoras piloto para estimar el canal y sincronismo hace el sistema vulnerable a un *jamming* de los pilotos como un multitono posicionado sobre ellos. Aplicar una simple medida de protección como la aleatorización de los pilotos dentro de la trama OFDM usando una secuencia pseudo-aleatoria con parámetros conocidos en transmisión y recepción ofrece una protección frente a *jamming* multitono.

Otra forma de perturbar la señal es usar *jammers* pulsados en lugar de los de forma de onda continua. Esto permite utilizar la potencia de forma más eficiente atacando solo parte de la trama que lleva información de cabeceras y control. Frente a este tipo de *jamming* se puede introducir una aleatorización del comienzo en tiempo de la trama o *jitter*. Dado que la trama no empieza siempre con el mismo periodo, esta medida protege la comunicación de un *jammer* pulsado muy selectivo.

El conjunto de medidas de protección de la señal transmitida se denomina TRANSEC (por las siglas del término en inglés *Transmission Security*). Los algoritmos de TRANSEC requieren generadores de números pseudo-aleatorios equivalentes en transmisión y recepción para poder comunicarse. De este modo, el receptor se puede adaptar correctamente a la señal transmitida aunque ésta aparente tener ciertas aleatoriedades para un observador externo que desconoce las características del TRANSEC o las secuencias pseudo-aleatorias (frecuencia de portadora, posición de pilotos dentro de la trama OFDM, etc.).

A fin de cuentas, tal y como se describe en el capítulo 2, existen múltiples formas de perturbar una comunicación. Por lo tanto, la guerra electrónica (EW) se convierte en un juego de estrategia en el que los sistemas de comunicaciones que operan en entornos tácticos deben implementar medidas que cubran sus vulnerabilidades o puedan contrarrestar el *jamming* que se espera encontrar en dichos entornos. Asimismo, existen complejos equipos de *jamming* capaces de bloquear o perturbar diversos sistemas de comunicaciones. Para ello emplean diversos algoritmos y mecanismos capaces incluso de adaptarse de forma continua a las condiciones.

7 Referencias

[1] J. M. Nocedal, “RF *Jamming*”, Universidad de las Américas Puebla, 2006

[2] Richard Poisel , "Modern communications *jamming* principles and techniques", Artech House, 2004

[3] Amalia Roca, “Implementation of a WiMAX simulator in Simulink”, Institute of Communications and Radio-frequency Engineering, Vienna University of Engineering, 2007

[4] Sean Stamplecoskie, “A Study of the Concatenated Reed Solomon - Convolutional Coding Performance used in WiMAX”, Defence R&D Canada-Ottawa, 2007

[5] Naveen M B, Nidhish N, Prasanna M, Varun V, “WiMax”, Department of Electrical, Computer, and Energy Engineering at the University of Colorado at Boulder

[6] IEEE Standard for Air Interface for Broadband Wireless Access Systems, IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, 2012

[7] John S. Seybold, “Introduction to Propagation”, John Wiley & Sons Ltd, 2005

[8] Electronic Warfare And Radar System Engineering Handbook, Naval Air Systems Command, 1999

8 Glosario

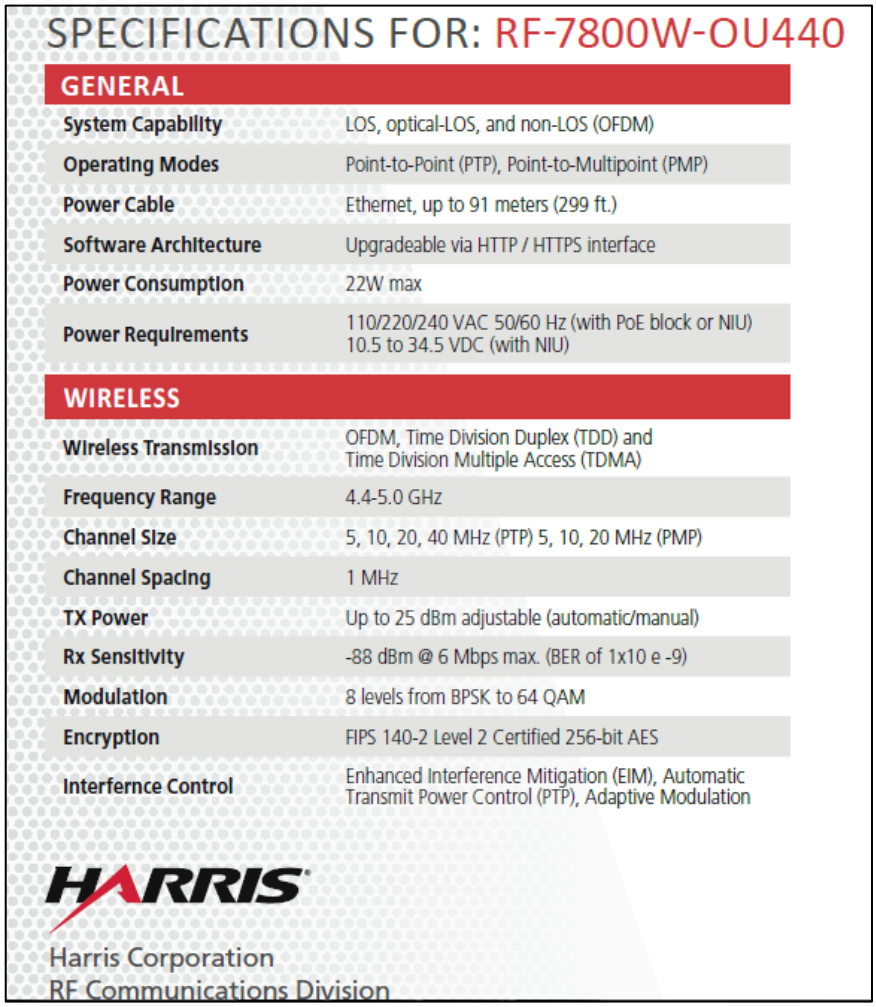
AJ	Anti-*Jamming*
BER	Bit Error Rate
BBN	BroadBand Noise
BW	BandWidth (Ancho de Banda)
CP	Cyclic Prefix (Prefijo Cíclico)
DL	DownLink
EB	Estación Base
EM	Estación Móvil
EW	Electronic Warfare
FCH	Frame Control Header
FEC	Forward Error Correction
FFT	Fast-Fourier Transform (Transformada rápida de Fourier)
FH	Frequency Hopping
LSFR	Linear Shift Finite Register
LPD	Low Probability of Detection
LPI	Low Probability of Interception
OFDM	Orthogonal Frequency Division Multiplexing
PBN	Partial-Band Noise
PHY	PHYsical layer
PSK	Phase Shift Keying
QAM	Quadrature and Amplitude Modulation
Rx	Receptor/Recepción
SIR	Signal to Interference Ratio
TRANSEC	TRANsmission SECurity
Tx	Transmisor/Transmisión
UL	UpLink
VoIP	Voice over IP
WiMAX	Worldwide Interoperability for Microware Access

9 Anexos

Anexo A – Terminales móviles WiMAX

A1 – Terminal móvil de Harris

La compañía estadounidense HARRIS Corporation desarrolla equipos electrónicos y de comunicaciones destinados al sector civil y de defensa. Entre sus productos cuenta con equipos móviles de WiMAX para desplegar redes de comunicaciones en lugares remotos. A continuación se muestra la hoja de especificaciones técnicas para un terminal de usuario móvil para equiparlo por ejemplo en vehículos.



SPECIFICATIONS FOR: RF-7800W-OU440

GENERAL	
System Capability	LOS, optical-LOS, and non-LOS (OFDM)
Operating Modes	Point-to-Point (PTP), Point-to-Multipoint (PMP)
Power Cable	Ethernet, up to 91 meters (299 ft.)
Software Architecture	Upgradeable via HTTP / HTTPS interface
Power Consumption	22W max
Power Requirements	110/220/240 VAC 50/60 Hz (with PoE block or NIU) 10.5 to 34.5 VDC (with NIU)
WIRELESS	
Wireless Transmission	OFDM, Time Division Duplex (TDD) and Time Division Multiple Access (TDMA)
Frequency Range	4.4-5.0 GHz
Channel Size	5, 10, 20, 40 MHz (PTP) 5, 10, 20 MHz (PMP)
Channel Spacing	1 MHz
TX Power	Up to 25 dBm adjustable (automatic/manual)
Rx Sensitivity	-88 dBm @ 6 Mbps max. (BER of 1x10 e -9)
Modulation	8 levels from BPSK to 64 QAM
Encryption	FIPS 140-2 Level 2 Certified 256-bit AES
Interfernce Control	Enhanced Interference Mitigation (EIM), Automatic Transmit Power Control (PTP), Adaptive Modulation

HARRIS

Harris Corporation
RF Communications Division

Figura A-1: Características estación móvil HARRIS RF-7800W-OU440

Los parámetros necesarios para su caracterización en el modelo de Simulink son:

- Banda de frecuencia de operación: 4.4 a 5 GHz (banda NATO-IV)
- Ancho de banda de canal: 10 MHz
- Potencia de transmisión: 25 dBm (~316 mW)

Este equipo se considera en el escenario 1 como estación móvil desplegada en el puesto avanzado. Tal y como se aprecia en la imagen inferior, por su tamaño se puede desplegar con facilidad montándolos en vehículos o soportes fijos.

Figura A-2: Fotografía estación móvil HARRIS RF-7800W-OU440

La imagen inferior, extraída del folleto comercial del dispositivo de HARRIS, muestra el despliegue del equipo en un puesto avanzado tal y como podría ser el propuesto en el escenario 1.

Figura A-3: Fotografía despliegue del móvil en soporte fijo

A2 – Terminal móvil de Amper

La compañía española AMPER Programas, especialista en el mercado de las radiocomunicaciones para entornos tácticos, está involucrada también en el desarrollo de productos y soluciones WiMAX. En la imagen inferior se muestran algunas de las

características técnicas extraídas de uno de sus folletos comerciales de un terminal de usuario móvil de WiMAX

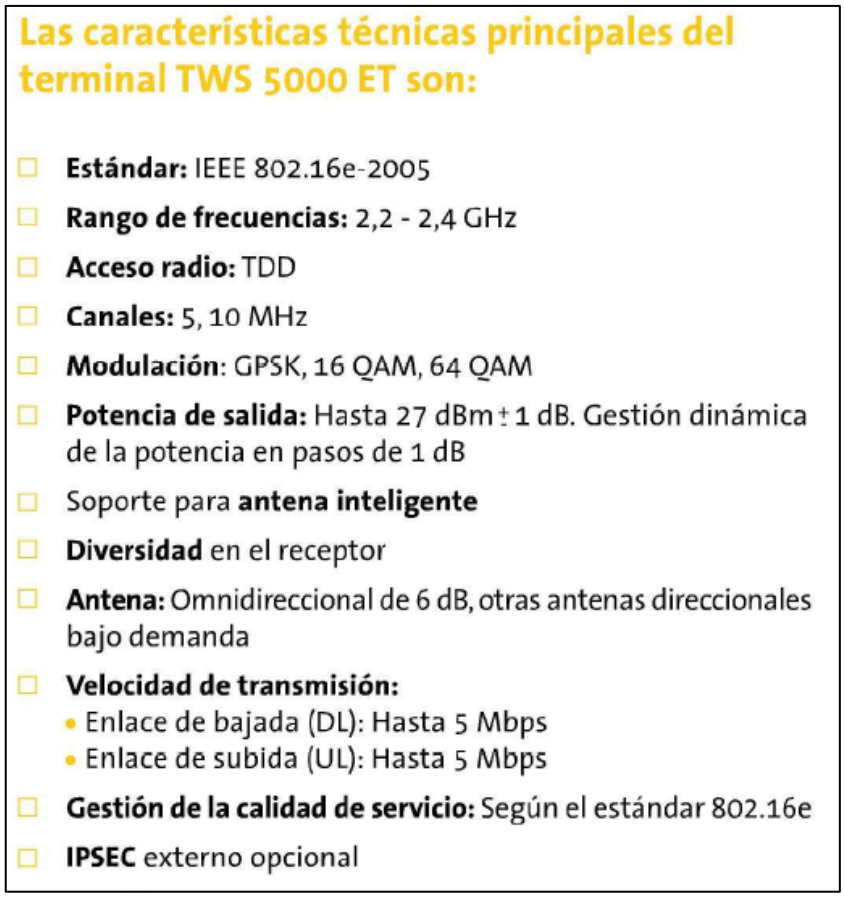


Figura A-4: Características estación móvil AMPER TWS-5000-ET

Los parámetros necesarios para su caracterización en el modelo de Simulink son:

- Banda de frecuencia de operación: 2.2 a 2.4 GHz
- Ancho de banda de canal: 5 MHz
- Potencia de transmisión: 27 dBm (~500 mW)

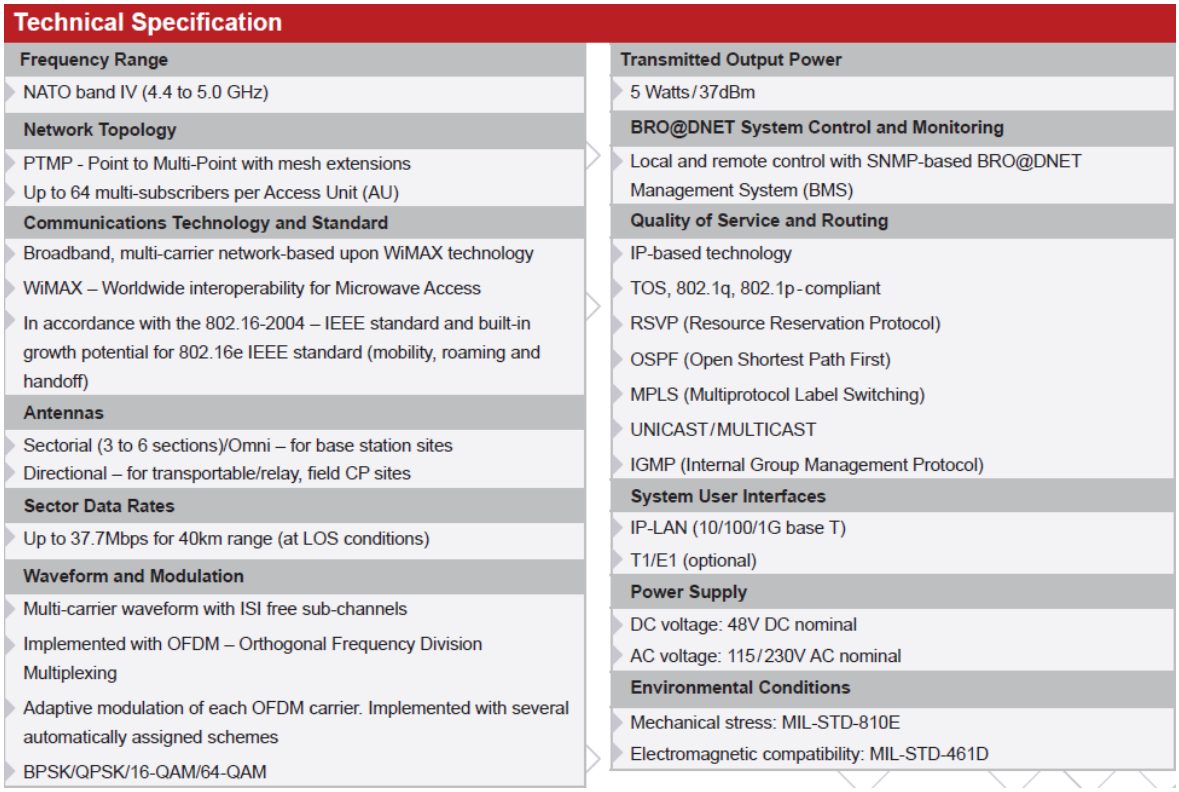
Este equipo se considera en el escenario 2 como estación móvil desplegada en el puesto de acceso. Tal y como se aprecia en la imagen inferior, por su tamaño se puede desplegar con facilidad montándolos en vehículos o soportes fijos.

Figura A-5: Fotografía estación móvil AMPER TWS-5000-ET

Anexo B – Estaciones base WiMAX

B1 – Estación base de TELEFUNKEN RACOMS

La compañía alemana Telefunken Racoms desarrolla productos y soluciones de radiocomunicaciones para el sector de defensa y seguridad. Uno de sus productos relacionados con WiMAX es el sistema Bro@dnet, una solución para el despliegue de redes WiMAX en entornos tácticos. A continuación se muestra la ficha técnica extraída de uno de los folletos comerciales para uno de sus equipos, una estación base de WiMAX:



Technical Specification

Frequency Range
- NATO band IV (4.4 to 5.0 GHz)

Network Topology
- PTMP - Point to Multi-Point with mesh extensions
- Up to 64 multi-subscribers per Access Unit (AU)

Communications Technology and Standard
- Broadband, multi-carrier network-based upon WiMAX technology
- WiMAX – Worldwide interoperability for Microwave Access
- In accordance with the 802.16-2004 – IEEE standard and built-in growth potential for 802.16e IEEE standard (mobility, roaming and handoff)

Antennas
- Sectorial (3 to 6 sections)/Omni – for base station sites
- Directional – for transportable/relay, field CP sites

Sector Data Rates
- Up to 37.7Mbps for 40km range (at LOS conditions)

Waveform and Modulation
- Multi-carrier waveform with ISI free sub-channels
- Implemented with OFDM – Orthogonal Frequency Division Multiplexing
- Adaptive modulation of each OFDM carrier. Implemented with several automatically assigned schemes
- BPSK/QPSK/16-QAM/64-QAM

Transmitted Output Power
- 5 Watts/37dBm

BRO@DNET System Control and Monitoring
- Local and remote control with SNMP-based BRO@DNET Management System (BMS)

Quality of Service and Routing
- IP-based technology
- TOS, 802.1q, 802.1p-compliant
- RSVP (Resource Reservation Protocol)
- OSPF (Open Shortest Path First)
- MPLS (Multiprotocol Label Switching)
- UNICAST/MULTICAST
- IGMP (Internal Group Management Protocol)

System User Interfaces
- IP-LAN (10/100/1G base T)
- T1/E1 (optional)

Power Supply
- DC voltage: 48V DC nominal
- AC voltage: 115/230V AC nominal

Environmental Conditions
- Mechanical stress: MIL-STD-810E
- Electromagnetic compatibility: MIL-STD-461D

Figura B-1: Características estación base TELEFUNKEN BRO@DNET

Los parámetros necesarios para su caracterización en el modelo de Simulink son:

- Banda de frecuencia de operación: 4.4 a 5 GHz (banda NATO-IV)
- Ancho de banda de canal: 5 MHz
- Potencia de transmisión: 37 dBm (~5 W)

Por estas características, se utiliza como estación base para el escenario 2. Tal y como se aprecia en la imagen inferior, por su tamaño se puede desplegar con facilidad montándolos en vehículos o soportes fijos.

B2 – Estación base de Amper Programas

La compañía española AMPER Programas, especialista en el mercado de las radiocomunicaciones para entornos tácticos, está involucrada también en el desarrollo de productos y soluciones WiMAX. En la imagen inferior se muestran algunas de las

características técnicas extraídas de uno de sus folletos comerciales de un terminal de estación base de WiMAX:

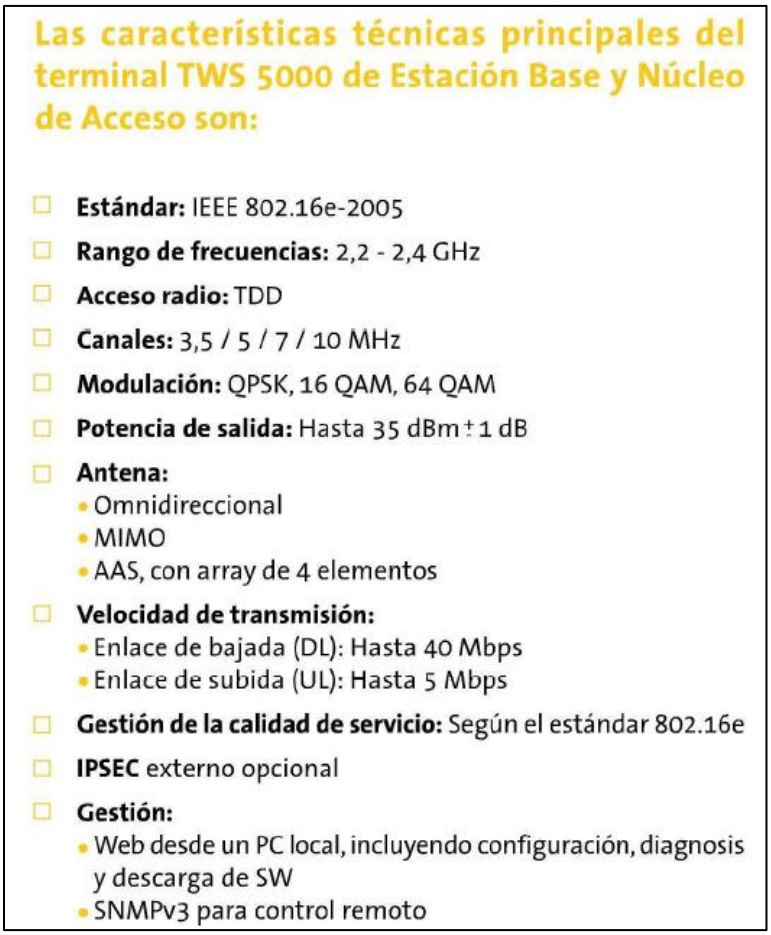


Figura B-2: Características estación base AMPER TWS-5000-EB

Los parámetros necesarios para su caracterización en el modelo de Simulink son:

- Banda de frecuencia de operación: 2.2 a 2.4 GHz
- Potencia de transmisión: 35 dBm (~3 W)

Por estas características, se utiliza como estación base para el escenario 2.

Figura B-3: Fotografía estación base AMPER TWS-5000-EB

Anexo C – Jammer portátil de baja potencia

La compañía taiwanesa Winpower, desarrolladora de productos y soluciones para el ámbito de la guerra electrónica y equipos de radiofrecuencia posee en su cartera una serie de dispositivos de *jamming* portátiles. A continuación se muestran las especificaciones del modelo JM-2010VP, extraídas de uno de sus folletos comerciales:

Specification

TX Frequency	(C) TX frequency 895/900 ~ 1000 MHz
	(D) TX frequency 1195/1200 ~ 1300 MHz
	(E) TX frequency 2395/2400 ~ 2500MHz
Output power	(A): +25dBm / 300mW
	(B): +25dBm / 300mW
Battery	Ni-MH battery DC12V / 1600mA/h
	Continue using time: 90 minute
	First time battery charge need 2 hours up
Dimension	110mm (H) ×62mm (L) ×30mm (D) (exclude antenna)
Weight	300g
Operating temperature	-10°C ~ +60°C
Humidity	5% ~ 80%
OEM or ODM for specially request	Yes

Figura C-1: Características *Jammer* portátil WINPOWER JM-2010VP

Los parámetros necesarios para su caracterización en el modelo de Simulink son:

- Banda de frecuencia de operación: 2395 MHz a 2.5 MHz
- Potencia de transmisión: 25 dBm (~300 mW)

Por estas características, se utiliza como dispositivo de *jamming* portátil en el escenario 2. Tal y como se aprecia en la imagen inferior, por su tamaño (110x62x30 mm) se puede portar sin llamar la atención en una mochila, bajo la ropa o incluso en un bolsillo.

Figura C-2: Fotografía *jammer* portátil WINPOWER JM-2010VP

Este producto encaja en la descripción que se hace del escenario 2, en la que un individuo lleva un dispositivo de *jamming* portátil que intenta introducir sin ser visto en un recinto.

Anexo D – PRESUPUESTO

1) Ejecución Material

- Compra de ordenador personal (Software incluido)..... ..... 2.000 €
- Alquiler de impresora láser durante 6 meses ..... 50 €
- Material de oficina ..... 150 €
- Total de ejecución material ..... 2.200 €

2) Gastos generales

- 21 % sobre Ejecución Material ..... 462 €

3) Beneficio Industrial

- 6 % sobre Ejecución Material ..... 132 €

4) Honorarios Proyecto

- 640 horas a 15 € / hora ..... 9.600 €

5) Material fungible

- Gastos de impresión y encuadernación ..... 250 €

6) Subtotal del presupuesto

- Subtotal Presupuesto ..... 12.644 €

7) I.V.A. aplicable

- 21% Subtotal Presupuesto ..... 2.655,24 €

8) Total presupuesto

- Total Presupuesto ..... 15.299,24 €

Madrid, Octubre de 2012

El Ingeniero Jefe de Proyecto

Fdo.: Juan Francisco Díaz Bejarano
Ingeniero Superior de Telecomunicación

Anexo E – PLIEGO DE CONDICIONES

Este documento contiene las condiciones legales que guiarán la realización, en este proyecto, de *Aplicación de técnicas Anti-Jamming a un sistema de comunicaciones convencional para su explotación en entornos tácticos*. En lo que sigue, se supondrá que el proyecto ha sido encargado por una empresa cliente a una empresa consultora con la finalidad de realizar dicho sistema. Dicha empresa ha debido desarrollar una línea de investigación con objeto de elaborar el proyecto. Esta línea de investigación, junto con el posterior desarrollo de los programas está amparada por las condiciones particulares del siguiente pliego.

Supuesto que la utilización industrial de los métodos recogidos en el presente proyecto ha sido decidida por parte de la empresa cliente o de otras, la obra a realizar se regulará por las siguientes:

Condiciones generales

1. La modalidad de contratación será el concurso. La adjudicación se hará, por tanto, a la proposición más favorable sin atender exclusivamente al valor económico, dependiendo de las mayores garantías ofrecidas. La empresa que somete el proyecto a concurso se reserva el derecho a declararlo desierto.

2. El montaje y mecanización completa de los equipos que intervengan será realizado totalmente por la empresa licitadora.

3. En la oferta, se hará constar el precio total por el que se compromete a realizar la obra y el tanto por ciento de baja que supone este precio en relación con un importe límite si este se hubiera fijado.

4. La obra se realizará bajo la dirección técnica de un Ingeniero Superior de Telecomunicación, auxiliado por el número de Ingenieros Técnicos y Programadores que se estime preciso para el desarrollo de la misma.

5. Aparte del Ingeniero Director, el contratista tendrá derecho a contratar al resto del personal, pudiendo ceder esta prerrogativa a favor del Ingeniero Director, quien no estará obligado a aceptarla.

6. El contratista tiene derecho a sacar copias a su costa de los planos, pliego de condiciones y presupuestos. El Ingeniero autor del proyecto autorizará con su firma las copias solicitadas por el contratista después de confrontarlas.

7. Se abonará al contratista la obra que realmente ejecute con sujeción al proyecto que sirvió de base para la contratación, a las modificaciones autorizadas por la superioridad o a las órdenes que con arreglo a sus facultades le hayan comunicado por escrito al Ingeniero Director de obras siempre que dicha obra se haya ajustado a los preceptos de los pliegos de condiciones, con arreglo a los cuales, se harán las modificaciones y la valoración de las diversas unidades sin que el importe total pueda exceder de los presupuestos aprobados. Por consiguiente, el número de unidades que se consignan en el proyecto o en el presupuesto, no podrá servirle de fundamento para entablar reclamaciones de ninguna clase, salvo en los casos de rescisión.

8. Tanto en las certificaciones de obras como en la liquidación final, se abonarán los trabajos realizados por el contratista a los precios de ejecución material que figuran en el presupuesto para cada unidad de la obra.

9. Si excepcionalmente se hubiera ejecutado algún trabajo que no se ajustase a las condiciones de la contrata pero que sin embargo es admisible a juicio del Ingeniero Director de obras, se dará conocimiento a la Dirección, proponiendo a la vez la rebaja de precios que el Ingeniero estime justa y si la Dirección resolviera aceptar la obra, quedará el contratista obligado a conformarse con la rebaja acordada.

10. Cuando se juzgue necesario emplear materiales o ejecutar obras que no figuren en el presupuesto de la contrata, se evaluará su importe a los precios asignados a otras obras o materiales análogos si los hubiere y cuando no, se discutirán entre el Ingeniero Director y el contratista, sometiéndolos a la aprobación de la Dirección. Los nuevos precios convenidos por uno u otro procedimiento, se sujetarán siempre al establecido en el punto anterior.

11. Cuando el contratista, con autorización del Ingeniero Director de obras, emplee materiales de calidad más elevada o de mayores dimensiones de lo estipulado en el proyecto, o sustituya una clase de fabricación por otra que tenga asignado mayor precio o ejecute con mayores dimensiones cualquier otra parte de las obras, o en general, introduzca en ellas cualquier modificación que sea beneficiosa a juicio del Ingeniero Director de obras, no tendrá derecho sin embargo, sino a lo que le correspondería si hubiera realizado la obra con estricta sujeción a lo proyectado y contratado.

12. Las cantidades calculadas para obras accesorias, aunque figuren por partida alzada en el presupuesto final (general), no serán abonadas sino a los precios de la contrata, según las condiciones de la misma y los proyectos particulares que para ellas se formen, o en su defecto, por lo que resulte de su medición final.

13. El contratista queda obligado a abonar al Ingeniero autor del proyecto y director de obras así como a los Ingenieros Técnicos, el importe de sus respectivos honorarios facultativos por formación del proyecto, dirección técnica y administración en su caso, con arreglo a las tarifas y honorarios vigentes.

14. Concluida la ejecución de la obra, será reconocida por el Ingeniero Director que a tal efecto designe la empresa.

15. La garantía definitiva será del 4% del presupuesto y la provisional del 2%.

16. La forma de pago será por certificaciones mensuales de la obra ejecutada, de acuerdo con los precios del presupuesto, deducida la baja si la hubiera.

17. La fecha de comienzo de las obras será a partir de los 15 días naturales del replanteo oficial de las mismas y la definitiva, al año de haber ejecutado la provisional, procediéndose si no existe reclamación alguna, a la reclamación de la fianza.

18. Si el contratista al efectuar el replanteo, observase algún error en el proyecto, deberá comunicarlo en el plazo de quince días al Ingeniero Director de obras, pues transcurrido ese plazo será responsable de la exactitud del proyecto.

19. El contratista está obligado a designar una persona responsable que se entenderá con el Ingeniero Director de obras, o con el delegado que éste designe, para todo relacionado con ella. Al ser el Ingeniero Director de obras el que interpreta el proyecto, el contratista deberá consultarle cualquier duda que surja en su realización.

20. Durante la realización de la obra, se girarán visitas de inspección por personal facultativo de la empresa cliente, para hacer las comprobaciones que se crean oportunas. Es obligación del contratista, la conservación de la obra ya ejecutada hasta la recepción de la misma, por lo que el deterioro parcial o total de ella, aunque sea por agentes atmosféricos u otras causas, deberá ser reparado o reconstruido por su cuenta.

21. El contratista, deberá realizar la obra en el plazo mencionado a partir de la fecha del contrato, incurriendo en multa, por retraso de la ejecución siempre que éste no sea debido a causas de fuerza mayor. A la terminación de la obra, se hará una recepción provisional previo reconocimiento y examen por la dirección técnica, el depositario de efectos, el interventor y el jefe de servicio o un representante, estampando su conformidad el contratista.

22. Hecha la recepción provisional, se certificará al contratista el resto de la obra, reservándose la administración el importe de los gastos de conservación de la misma hasta su recepción definitiva y la fianza durante el tiempo señalado como plazo de garantía. La recepción definitiva se hará en las mismas condiciones que la provisional, extendiéndose el acta correspondiente. El Director Técnico propondrá a la Junta Económica la devolución de la fianza al contratista de acuerdo con las condiciones económicas legales establecidas.

23. Las tarifas para la determinación de honorarios, reguladas por orden de la Presidencia del Gobierno el 19 de Octubre de 1961, se aplicarán sobre el denominado en la actualidad "Presupuesto de Ejecución de Contrata" y anteriormente llamado "Presupuesto de Ejecución Material" que hoy designa otro concepto.

Condiciones particulares

La empresa consultora, que ha desarrollado el presente proyecto, lo entregará a la empresa cliente bajo las condiciones generales ya formuladas, debiendo añadirse las siguientes condiciones particulares:

1. La propiedad intelectual de los procesos descritos y analizados en el presente trabajo, pertenece por entero a la empresa consultora representada por el Ingeniero Director del Proyecto.

2. La empresa consultora se reserva el derecho a la utilización total o parcial de los resultados de la investigación realizada para desarrollar el siguiente proyecto, bien para su publicación o bien para su uso en trabajos o proyectos posteriores, para la misma empresa cliente o para otra.

3. Cualquier tipo de reproducción aparte de las reseñadas en las condiciones generales, bien sea para uso particular de la empresa cliente, o para cualquier otra aplicación, contará con autorización expresa y por escrito del Ingeniero Director del Proyecto, que actuará en representación de la empresa consultora.

4. En la autorización se ha de hacer constar la aplicación a que se destinan sus reproducciones así como su cantidad.

5. En todas las reproducciones se indicará su procedencia, explicitando el nombre del proyecto, nombre del Ingeniero Director y de la empresa consultora.

6. Si el proyecto pasa la etapa de desarrollo, cualquier modificación que se realice sobre él, deberá ser notificada al Ingeniero Director del Proyecto y a criterio de éste, la empresa consultora decidirá aceptar o no la modificación propuesta.

7. Si la modificación se acepta, la empresa consultora se hará responsable al mismo nivel que el proyecto inicial del que resulta el añadirla.

8. Si la modificación no es aceptada, por el contrario, la empresa consultora declinará toda responsabilidad que se derive de la aplicación o influencia de la misma.

9. Si la empresa cliente decide desarrollar industrialmente uno o varios productos en los que resulte parcial o totalmente aplicable el estudio de este proyecto, deberá comunicarlo a la empresa consultora.

10. La empresa consultora no se responsabiliza de los efectos laterales que se puedan producir en el momento en que se utilice la herramienta objeto del presente proyecto para la realización de otras aplicaciones.

11. La empresa consultora tendrá prioridad respecto a otras en la elaboración de los proyectos auxiliares que fuese necesario desarrollar para dicha aplicación industrial, siempre que no haga explícita renuncia a este hecho. En este caso, deberá autorizar expresamente los proyectos presentados por otros.

12. El Ingeniero Director del presente proyecto, será el responsable de la dirección de la aplicación industrial siempre que la empresa consultora lo estime oportuno. En caso contrario, la persona designada deberá contar con la autorización del mismo, quien delegará en él las responsabilidades que ostente.