Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Capacidad secreta en sistema de comunicaciones MIMO con múltiples usuarios

Grado en Ingeniería Mecánica

ALUMNO: Alberto Sánchez Soriano

DIRECTORES: José González Coma

CURSO ACADÉMICO: 2023-2024

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Capacidad secreta en sistema de comunicaciones MIMO con múltiples usuarios

Grado en Ingeniería Mecánica

Intensificación en Tecnología Naval

Cuerpo General / Infantería de Marina

Universidade Vigo

RESUMEN

Los sistemas MIMO (*Multiple-Input Multiple-Output*) utilizan múltiples antenas en el transmisor y/o en el receptor para mejorar la eficiencia espectral y la calidad de la comunicación inalámbrica. Además, esta tecnología permite controlar el diagrama de radiación de la antena, cualidad fundamental para mejorar la confidencialidad de las comunicaciones. En este contexto, la capacidad secreta se refiere a la máxima cantidad de información que puede ser transmitida sin posibilidad de interceptación por *eavesdroppers* ("fisgones"). El uso de esta métrica es fundamental para garantizar la seguridad de las comunicaciones inalámbricas en entornos sensibles. Por consiguiente, este Trabajo de Fin de Grado pretende poner de manifiesto la relevancia de este tema de investigación para una institución como la Armada.

Para conseguir maximizar la capacidad secreta, en este TFG se combinan la diversidad espacial que ofrece el uso de múltiples antenas, y el empleo de las siguientes técnicas de *precoding*: MRT (*Maximum Ratio Transmission*) y ZF (*Zero-Forcing*). La evaluación teórica inicial sugiere que ZF reduce la capacidad del *eavesdropper* para decodificar la información más eficazmente que MRT, ya que es un *precoder* con capacidad de cancelación de señal, factor más que relevante en el ámbito de la Seguridad en la Capa Física.

PALABRAS CLAVE

MIMO, Capacidad secreta, *Eavesdropper*, *Precoder*, SINR.

AGRADECIMIENTOS

Quiero comenzar agradeciendo a mi tutor durante la realización del Proyecto, José González Coma. Gracias por ayudarme y guiarme en todo momento, ha sido fundamental y todos los días he aprendido de usted y sus conocimientos.

Siempre estaré agradecido de compartir momentos brillantes, y no tan brillantes junto a mis compañeros de Brigada y de Promoción de Infantería de Marina, que hoy puedo llamar hermanos. Gracias 424-154, siempre os llevaré en el corazón.

A mis padres, mi hermana, mis abuelas, toda mi familia, porque han sido mi formación permanente, y nunca habrá agradecimiento suficiente por ello. A mis abuelos Pepe y Cándido, que me continúan impulsando a dar lo mejor de mí cada día desde el Cielo. Gracias a todos.

Y a mi compañera de equipo, Andrea. Gracias por acompañarme y apoyarme en todo momento, has sido y seguirás siendo incondicional para mí. Siempre te estaré agradecido.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Contextualización

MIMO (*Multiple-Input Multiple-Output*; Entrada Múltiple, Salida Múltiple) es una tecnología inalámbrica que utiliza varios transmisores y receptores.

Los sistemas de telecomunicaciones de múltiples usuarios basados en modelos MIMO están formados por una estación base (BS, *Base Station*) que posee más de una antena, y pueden ser analizados en diversos aspectos. Uno de ellos es la capacidad secreta. La capacidad secreta de un sistema de telecomunicaciones se define como la relación entre la capacidad de recepción de señal de un usuario legítimo y la capacidad de recepción de señal de un usuario ilegítimo o *eavesdropper* (también llamado "fisgón"); y es un término altamente relacionado con la Seguridad en la Capa Física (PHY, *Physical Layer*). Como su propio nombre indica, la Seguridad en la Capa Física pretende adoptar las medidas necesarias para evitar intercepción de señal indeseada a nivel físico (recepción de ondas). La Seguridad en la Capa Física complementa a la seguridad inalámbrica mediante la explotación de las características de los canales inalámbricos, entre las que se incluyen el desvanecimiento, ruido e interferencia [1]. La comunicación inalámbrica es un elemento base de la sociedad moderna, pues es un apoyo incondicional a Internet, y forma parte de la estructura de conexión.

El Instituto Nacional de Estadística (INE) [2] muestra datos que refuerzan la indispensabilidad del uso de las TIC en España, como se refleja en la Figura 1-1. El 98,99% de las empresas con más de 10 empleados tiene conexión a Internet, por lo que en el ámbito empresarial casi la totalidad de las entidades depende de la conectividad a esta red.

Indicadores sobre uso TIC en las empresas - Años 2022-2023

		Empresas con menos de 10 empleados	Empresas con más de 10 empleados
Disponen de ordenadores	1	88,74	99,50
Tiene conexión a internet	1	85,03	98,99
Tiene conexión a internet y página web	2	30,63	78,53
Utilizan medios sociales	2	33,92	63,57
Realizan ventas por comercio electrónico	1	14,16	31,69
Realizan compras por comercio electrónico	1	21,73	41,78

1. Datos medidos en porcentaje sobre el total de empresas de cada tipo
2. Datos medidos en porcentaje sobre el total de empresas con conexión a internet de cada tipo

Figura 1-1: Uso de TIC en empresas [2].

En el ámbito familiar, la mayoría de los hogares también cuentan con conexión a Internet, como se muestra en la Figura 1-2. En la Figura 1-3 también es observable una tendencia creciente de hogares que implementan la conexión a Internet a sus características.

Equipamiento y uso de TIC en los hogares - Año 2023

		Valor	Variación
Hogares con conexión de banda ancha	1	96,4	0,3
Viviendas con algún tipo de ordenador	1	82,6	-0,3
Personas que han usado Internet (últimos 3 meses)	2	95,4	0,9
Usuarios diarios de Internet	2	90,0	2,9
Personas que han comprado por Internet (últimos 3 meses)	2	55,9	0,6

Valor en porcentaje. Variación: diferencia respecto a la tasa del año anterior
1. Hogares con al menos un miembro de 16 a 74 años de edad
2. Personas de 16 a 74 años de edad

Figura 1-2: Uso de las TIC en hogares [2].

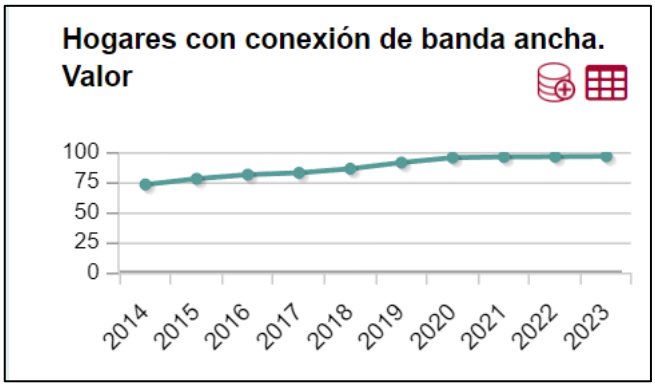


Figura 1-3: Gráfica evolución de hogares con conexión de banda ancha [2].

Dada la importancia de la conexión inalámbrica, es necesaria su estandarización. El IEEE (*Institute of Electrical and Electronics Engineers*, Instituto de Ingenieros Eléctricos y Electrónicos) regula las redes tanto inalámbricas como por medio guiado, de los tipos LAN (*Local Area Networks*, Redes de Área Local) y MAN (Metropolitan Area Networks, Redes de Área Metropolitana) mediante el protocolo estándar IEEE Std 802. Estas redes están enfocadas a conexiones como Ethernet, WiFi, o Bluetooth. A pesar de no tratar Internet, sin este paso previo el sistema no funcionaría.

El protocolo IEEE Std 802.15.4 – 2011 [3] define la capa física, de enlace y red para proporcionar servicios en una red inalámbrica, y también reseña la dificultad de hacer de dicha red inalámbrica una red segura. En dicho protocolo se hace responsable de ofrecer seguridad al sistema a la subcapa MAC, sin mencionar a la capa física en este ámbito, por lo que esta última es potencialmente mejorable.

Por otra parte, el uso de tecnología MIMO inalámbrica tiene como principales atributos: gran capacidad, gran diversidad y supresión de interferencia. Es un sistema implementado en los últimos 20 años relacionado con el estándar IEEE 802.11 [4], protocolo que tiene por objetivo definir un control de acceso al medio (MAC, *Medium Access Control*) y definir varias especificaciones de la capa física para conexiones inalámbricas para estaciones fijas, portátiles, o en movimiento dentro de un área local.

El estudio de la tecnología MIMO comenzó en escenarios de un solo usuario, en los que intervienen un emisor y un receptor. Dichos escenarios son denominados sistemas SU-MIMO (*Single-User* MIMO, MIMO de un usuario), y utilizan todas las antenas de las que dispone para transmitir a un usuario e incrementan la tasa de datos ya que dispone de mayor ancho de banda y potencia disponible.

Por otra parte, los sistemas MU-MIMO (*Multi-User* MIMO, MIMO de múltiples usuarios) distribuyen la transmisión de datos a múltiples usuarios a la vez, pero dicha transmisión depende del espacio que ocupe cada usuario. Aumenta la capacidad del sistema, es decir, el número de usuarios que actúan como receptores de la BS.

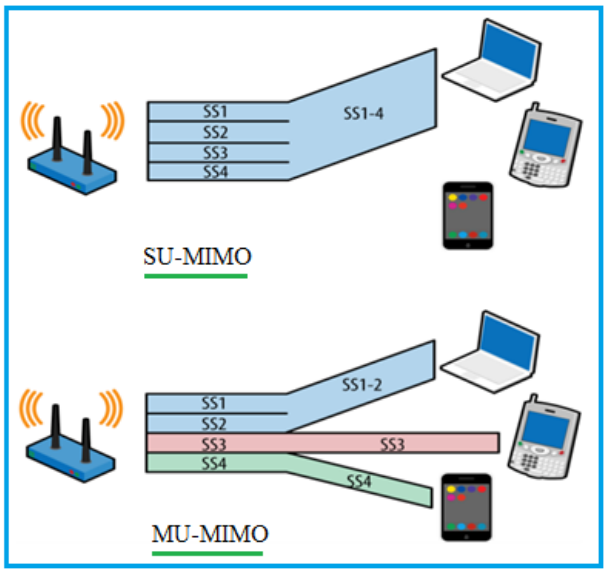


Figura 1-4: Diferencias entre SU-MIMO y MU-MIMO [5].

La última evolución de los sistemas MIMO fue el mMIMO (*massive* MIMO, MIMO masivo). Esta consiste en aumentar más aún el número de antenas a emplear, para potenciar cualidades anteriormente vistas. El modelo 5G se basa en este tipo de sistemas, mientras los modelos 3G o 4G se basan en los sistemas MU-MIMO.

1.2 Motivación

El estudio de los sistemas MIMO comenzó como innovación y alternativa a lo ya conocido, y ha evolucionado notablemente a lo largo de los años. Desde sus comienzos en SU-MIMO, hasta su evolución a mMIMO, los sistemas han conseguido evolucionar exponencialmente en el tiempo, y la tendencia ascendente da motivos para continuar estudiando dichos sistemas y aprovechar al máximo su potencial, sea en el ámbito de Defensa o relacionado.

Por otra parte, la Seguridad en la Capa Física es un ámbito en completo desarrollo, por lo que conseguir la capacidad secreta más beneficiosa en un sistema MU-MIMO es un reto más que ambicioso.

La razón principal de este Proyecto es la posibilidad de implementar los sistemas MIMO haciendo énfasis en la seguridad que ofrecen, es decir, su capacidad secreta; en el sector de Defensa y a un bajo nivel, para así hacer enfoque en el detalle del sistema y poder continuar su desarrollo.

El incremento de medidas de Seguridad en la Capa Física es necesario, ya que las comunicaciones militares basan su seguridad mayoritariamente en criptografía; y este factor conlleva consecuentes problemas de interoperabilidad, ya sea entre equipos debido a la empresa productora, o distintas unidades que no tienen relación orgánica directa para permitir enlaces de comunicaciones.

Para probar la eficacia de las medidas de seguridad que podrían implementarse en el sector militar, es necesario corroborar que dichas medidas cumplirán distintos objetivos, por ello la motivación de este Proyecto no es más que demostrar enlaces de comunicaciones seguros e imposibles de interceptar en distintos escenarios lo más realistas y parecidos posibles a situaciones tácticas que se puedan dar en el ámbito militar, más específicamente en la Infantería de Marina.

1.3 Objetivos

El objetivo principal en este Proyecto es desarrollar un análisis profundo del mayor número de escenarios posibles, en los que coexistan diferentes usuarios tanto legítimos como ilegítimos y se implementen métodos de Seguridad en la Capa Física mediante la herramienta más apta para ello: el empleo de Múltiples Antenas, convirtiendo los escenarios en sistemas de comunicaciones MIMO.

Para lograrlo, el objetivo es realizar previamente diferentes simulaciones empleando únicamente el *software Matlab*, para afianzar el fundamento teórico tras el escenario real que se desarrollará.

De tal forma, se pretende demostrar un buen rendimiento de estos sistemas en el ámbito militar, de forma que se ofrezca al sector una nueva herramienta y un amplio rango de nuevas capacidades que puedan ser tenidas en consideración, en cuanto a la especialidad de Tecnologías, Comunicación e Información se refiere.

Los objetivos generales que tiene este Proyecto son los siguientes:

- Indagar en el moderno sector de la Seguridad en la Capa Física, desarrollando sus bases y su posible impacto en el escenario militar.

- Ofrecer una actualización del ámbito de sistemas de comunicaciones MIMO, así como sus fundamentos y tendencia en el futuro.

- Adquisición de conocimientos avanzados de herramientas *software* ampliamente empleadas en el ámbito de las Telecomunicaciones, como son *Matlab* o *GNU Radio*; programando códigos interpretables por equipos radio, o programando simulaciones de escenarios de comunicaciones sin necesidad de tener un experimento real, para así afianzar conceptos puramente teóricos.

- Revisar los diseños de *precoding* más habituales en la literatura y su aplicación al escenario estudiado.

- Plantear diferentes escenarios de simulación prácticos, empleando el sistema de *array* de antenas desplegado en el laboratorio de radar y comunicaciones del CUD-ENM.

- Explotación de los conocimientos adquiridos durante el transcurso de la Ingeniería Mecánica, haciendo énfasis en importantes asignaturas como Álgebra y Estadística, Cálculo II, Sistemas de Radiocomunicaciones, o Sensores Navales.

1.4 Estructura del Proyecto

La estructura del Proyecto es la siguiente:

- En el Capítulo 1 se introduce el contexto del Proyecto, así como la motivación y objetivos de este.

- En el Capítulo 2 se detalla el Estado del Arte del Proyecto. Dicho Capítulo está dividido en los siguientes ámbitos: comunicación inalámbrica, Sistemas MIMO y Seguridad en la Capa Física.

- En el Capítulo 3 comienza el Desarrollo del TFG. En este Capítulo se realizan diferentes simulaciones en *software*, explicando el funcionamiento del sistema, y se introducen las características de los experimentos reales que se llevarán a cabo.

- En el Capítulo 4 se detallan los resultados y validación. En este Capítulo se realiza un análisis profundo de los resultados obtenidos en los experimentos reales, que se dividen en dos tipos según el escenario en el que se realizan. Se incluyen en total cinco análisis: tres experimentos del primer tipo de escenario, y dos experimentos del segundo tipo de escenario.

- En el Capítulo 5 se expresan las conclusiones extraídas durante la realización del Proyecto, así como las líneas futuras que se recomiendan, complementarias al Proyecto.

- En el Capítulo 6 se incluye la bibliografía empleada durante la realización del Proyecto

  Finalmente, el Proyecto concluye con siete anexos.

2 ESTADO DEL ARTE

2.1 Comunicación inalámbrica

2.1.1 Definición y fundamentos

Según el medio que utiliza para la transmisión, los tipos de sistemas de comunicaciones se dividen en: sistemas de comunicaciones guiados y sistemas de comunicaciones no guiados o inalámbricos.

La comunicación inalámbrica o comunicación a través de medios no guiados se define como la transmisión de datos originada por un transmisor con ondas electromagnéticas que viajan a través de un medio no guiado llamado canal, que normalmente es el aire o el agua; y recibida por un receptor. Su estructura general es similar a la mostrada en la Figura 2-1.

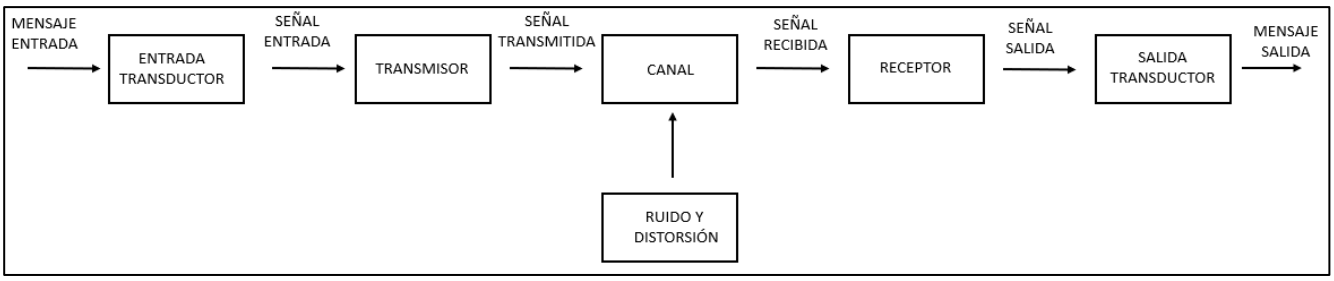


Figura 2-1: Estructura de sistema de comunicaciones [Elaboración propia].

La comunicación inalámbrica cuenta con los siguientes componentes [6]:

- La fuente originadora del mensaje, que es convertida en una onda electromagnética en banda base (sin modificar) a través del transductor de entrada.
- El transmisor, que modifica la banda base para una transmisión eficiente.
- El canal, definido como el medio a través del cual se transmiten las ondas electromagnéticas.
- El receptor, cuya función consiste en extraer el mensaje de la transmisión recibida con ruido.
- El transductor de salida, que convierte la señal recibida en la señal original.

Según el procesamiento de señal, la comunicación inalámbrica puede ser de señal analógica o digital [7].

- La señal analógica es continuamente variable en el tiempo, y recibe el nombre de analógica debido a que esta toma valores análogos entre magnitudes. Por ejemplo, una señal analógica de audio toma valores de voltaje en relación con la presión de la onda sonora de dicho audio. Es típicamente representada en forma sinusoidal.
- La señal digital es toda señal no continua en el tiempo. Esta es representada en forma discreta y toma valores de voltaje alternos pero constantes en un corto período de tiempo.

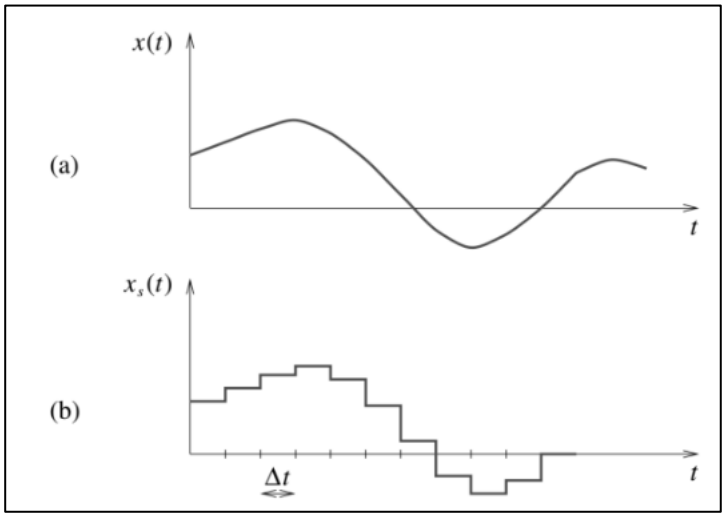


Figura 2-2: Señal analógica (a) vs. Señal digital (b) [8].

En términos de comunicación [9], las diferencias entre la comunicación digital y analógica son las siguientes:

PARÁMETRO	COMUNICACIÓN DIGITAL	COMUNICACIÓN ANALÓGICA
Representación	Ondas cuadradas.	Onda sinusoidal.
Inmunidad al ruido	Alta.	Baja.
Probabilidad de error	Alta.	Baja.
Ancho de banda	Requiere mayor ancho de banda.	Requiere menor ancho de banda.
Multiplexación [10]	Frecuencial (división de frecuencias en un canal).	Temporal (separación de paquetes).
Ejemplos	Audio (teléfono), video.	Ordenadores, discos duros.

Figura 2-3: Diferencias entre comunicación analógica y digital [9].

2.1.2 Historia

La comunicación inalámbrica por onda electromagnética tiene sus orígenes en la demostración de la teoría electromagnética que realizaron Maxwell y Hertz, y el primer sistema de comunicación inalámbrica fue establecido por Tesla. En 1898, Marconi demostró una comunicación inalámbrica desde un barco a la isla de Wight en el Canal de la Mancha. Por ello, ganó el premio Nobel de 1909 al ser nombrado inventor de la comunicación inalámbrica, a pesar de que Tesla lo realizase previamente. Tras el nacimiento de la comunicación inalámbrica unidireccional, esta continuó desarrollándose por todo el

mundo incentivando el uso de la radio y posteriormente de la televisión, con origen en 1925. El desarrollo de dicha comunicación se centró en radiodifusión de entretenimiento, y al final de los 1930 ya se había establecido una red de comunicación inalámbrica de difusión de entidad WAN.

Pero entonces llegó la necesidad de bidireccionalidad. Tanto el sector de Defensa como el policial requerían de sistemas de comunicaciones bidireccionales, y lideraron las líneas de investigación en este ámbito, motivados por la mejora militar frente a la Segunda Guerra Mundial. A su vez, Claude Shannon publicó *La teoría matemática de las comunicaciones* en 1948, y demostró la posibilidad de comunicación inalámbrica sin errores restringiendo la tasa de transmisión de datos y la Relación Señal-Ruido (SNR, *Signal to noise ratio*).

Durante los años 1940 y 1950 continuaron en desarrollo las comunicaciones inalámbricas destacando la primera instalación de sistema de telefonía móvil en Estados Unidos. Este sistema no contaba con interfaz automatizada, pero en su lugar esta labor era realizada por personas. Se trata de un sistema limitado, pues se disponía de seis canales para toda una ciudad, lo que suponía bastante colapso en la red. En la investigación para solventar este problema se dio con la clave que cambiaría el futuro de las comunicaciones inalámbricas: las células. Este principio permite el uso de frecuencias por células definidas por áreas físicas, multiplicando las posibilidades de frecuencias en cada célula, ya que distintas células pueden utilizar mismas frecuencias.

La comunicación analógica (1G, Primera Generación) continuó en desarrollo y, aunque el transporte a mano de los teléfonos era de severa dificultad, la funcionalidad de estos era intachable. Aun así, se estudió realizar esta comunicación con señal digital. En Europa en los años 1990, el ETSI (*European Telecommunications Standards Institute*, Instituto de Estándares de Telecomunicaciones Europeo) publicó el estándar celular digital GSM (*Global System for Mobile Communications,* Sistema Global para Comunicaciones Móviles), conocido como sistema de Segunda Generación (2G). Este sistema ofrecía calidad de audio, así como redes seguras; por lo que sobrepasó a las comunicaciones analógicas y provocó una conversión masiva a comunicación digital.

El siguiente gran paso fue implementar el sistema de comunicaciones de transmisión de datos. Tanto 1G (comunicación analógica) como 2G (comunicación digital estandarizada) centraron el esfuerzo en mejorar la comunicación inalámbrica en cuanto a voz y mensaje se refiere. El siguiente reto era implementar tasas de transmisión de datos por encima de 2 Mbit/s, y para ello comenzaría el desarrollo de las redes 3G (Tercera Generación). Estas redes tienen sus orígenes en dos estándares: *Third Generation Partnership Project* (3GPP) y 3GPP2. La implementación de 3G requería de nueva asignación de espectro, aspecto que bien pudieron explotar económicamente distintos países. También se trabajó en la implementación de técnicas preventivas de colisión de datos, como CDMA (*Code Division Multiple Access,* Acceso Múltiple por División de Código) y sus variantes como FDMA o OFDMA **(***Orthogonal Frequency Division Multiple Access***,** Acceso Múltiple por División de Frecuencia Ortogonal**).**

El estudio de estas técnicas derivó en respuestas como intervenir en la propia estructura física de las comunicaciones inalámbricas para mitigar efectos negativos como la interferencia, creando a partir de 1995 los sistemas de múltiples antenas, también conocidos como MIMO, los cuales se desarrollarán en el apartado 2.2. Estos sistemas junto con más medidas permitirían las incorporaciones de las siguientes generaciones: 4G (Cuarta Generación) y 5G (Quinta Generación) [11].

2.1.3 Comunicación inalámbrica en la Armada

Los sistemas CIS (Comunicación, Información y Sistemas) son un pilar para apoyar la función táctica de Mando y Control (C2) junto al jefe y Órganos Auxiliares, los procedimientos y las conexiones. Así los sistemas CIS son definidos, según la doctrina *ACP-176 SP NAVY SUPP-2* [12] como medios

materiales, métodos, procedimientos y personal, organizado de tal forma que permita la recepción, transmisión, tratamiento, presentación y almacenamiento de la información.

La comunicación inalámbrica, a su vez, es un pilar de los sistemas CIS en la Armada y en el ámbito militar y policial. Presenta enfoques distintos a los medios civiles, pues en el ámbito militar el ámbito de la seguridad y exclusividad de red en todas las capas o niveles es vital. La Armada cuenta con Sistemas de Radiofrecuencia (sistemas de comunicaciones, sistemas satelitales y sistemas radar) permanentes o desplegables, y trabaja en un amplio espectro de frecuencias que está gestionado por la Orden ETD/1449/2021, de 16 de diciembre, por la que se aprueba el Cuadro Nacional de Atribución de Frecuencias [13].

Según la frecuencia de trabajo en la que se encuentre un medio empleado por la Armada, la propagación se realiza de distinta manera [14]:

Símbolo	Frecuencias	Modelo de propagación
VLF	3 a 30 kHz	Guía-ondas tierra ionosfera
LF	30 a 300 kHz	Onda de superficie
MF	300 a 3000 kHz	Onda de superficie Onda ionosférica
HF	3 a 30 MHz	Onda ionosférica Onda de superficie
VHF	30 a 300 MHz	Onda espacial Dispersión ionosférica(f<50MHz)
UHF	300 a 3000 MHz	Onda espacial Dispersión ionosférica(f<500MHz)
SHF	3 a 30 GHz	Onda espacial

Figura 2-4: Frecuencias y sus modos de propagación [14].

Un buque de la Armada puede contener sistemas internos, para el servicio interno de la plataforma, y externos, para permitir interrelacionar a la plataforma con el exterior. Haciendo énfasis en los sistemas externos, un buque de la Armada puede contener los siguientes sistemas de comunicaciones [15]:

- Antenas HF (*High Frequency*) para transmisión, TRX para transmisión y recepción, y HF para recepción.
- Antenas UHF (*Ultra High Frequency*) y VHF (*Very High Frequency*).
- Antenas SATCOM (*Satellite Communications*).

Asimismo, una unidad de Infantería de Marina dispone de equipos permanentes y desplegables. Los equipos permanentes son generalmente estaciones radio para enlace entre unidades. Los equipos de comunicaciones desplegables se dividen por frecuencias de empleo.

- *Equipos HF*

Los equipos de Infantería de Marina que emplean el margen de frecuencias HF pueden emplear cifrado AES, que es comercial, o cifrado OTAN. AES es empleado por los equipos RF-5800H (Figura 2-5) y RF-7800H, mientras que los equipos AN/PRC-150 y PRC-160 emplean el cifrado OTAN. Cabe destacar que AN/PRC-150 y PRC-160 (Figura 2-6) son los mismos equipos que RF-5800H y RF-7800H respectivamente, pero cambian su denominación según su cifrado.

Figura 2-5: RF-5800H o AN/PRC 150 [16].

Figura 2-6: RF-7800H o AN/PRC 160 [17].

El empleo de este margen de frecuencias es comúnmente utilizado en transmisiones a distancias largas, que a su vez permiten menos transferencia de datos. La propagación por onda ionosférica debe ser estudiada, pues su calidad es dependiente del momento del día, y es necesario conocer la FOT (Frecuencia Óptima de Trabajo) y MUF (*Maximum Usable Frequency*, Máxima Frecuencia de Uso) para obtener un rendimiento eficaz de los equipos.

El hecho de emplear distintos cifrados refleja incompatibilidad entre unidades, problema que tiende a solucionarse estandarizando los equipos al menos a nivel nacional.

- *Equipos VHF*

El equipo militar VHF por excelencia es el PR4G. En [18] se realiza un estudio a fondo de las capacidades de estos equipos en todas sus versiones. En Infantería de Marina se ha firmado el traspaso de equipos a la familia HARRIS, es decir, los equipos PR4G se mantendrán hasta su obsolescencia, pero los futuros lotes de material incluirán sistemas HARRIS para así ofrecer interoperabilidad con las unidades de la Fuerza. El equipo más demandado para reemplazar el PR4G es el RF-7800M (Figura 2-7), un equipo multibanda que abarca hasta UHF SATCOM.

VHF es utilizado para transmisión a media distancia, y las ondas se propagan por onda de superficie, por lo que contar con LOS (*Line Of Sight*, línea de visión directa) mejora la calidad de la conexión notablemente, y viceversa.

Figura 2-7: RF-7800M multibanda [17].

- *Equipos UHF*

Los equipos UHF se dividen en terminales satélite, y equipos intrapatrulla.

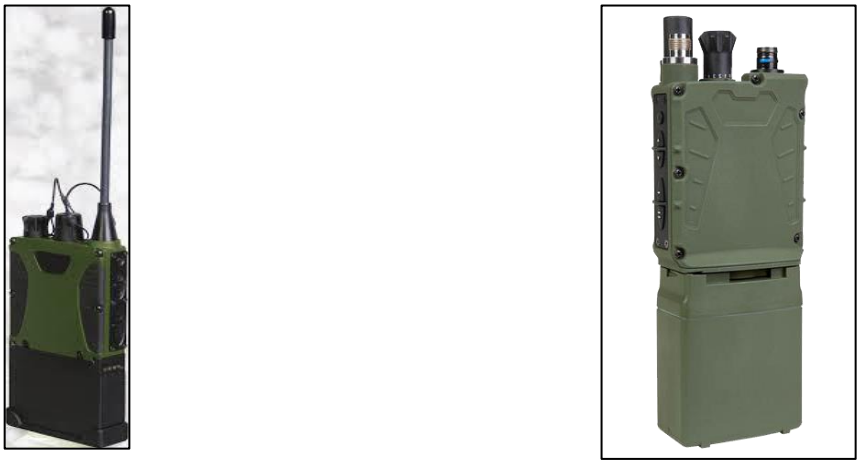
Los terminales satélites emplean UHF SATCOM para gran transmisión de datos, y los empleados en Infantería de Marina son el TLB-50 (terminal fijo, Figura 2-8), el TLX-5 DAMA (terminal móvil, Figura 2-9) y los terminales comerciales (como la tecnología TETRAPOL de FCSE).

Figura 2-8: TLB-50 [19].

Figura 2-9: TLX-5 DAMA [20].

Figura 2-10: Tecnología TETRAPOL [*locura digital*].

Los equipos intrapatrulla a nivel nacional se resumen al equipo RF-7800S (Figura 2-11), con cifrado AES, pero será reemplazado en el futuro por el equipo RF-7850 SPR (Figura 2-11), un equipo SDR (*Software-defined radio*, radio definida por Software) multibanda de gran capacidad, ya que permite transmisión de FMV (*Full Motion Video*, vídeo de movimiento completo).



a) **b)**

Figura 2-11: a) RF-7800S y b) RF-7850 SPR [17].

- *Seguridad en las comunicaciones militares*

Como se ha explicado anteriormente, las comunicaciones en el Ejército Español deben garantizar tres aspectos vitales para un correcto funcionamiento:

1. Fiabilidad: es la esperanza firme de que la comunicación o transmisión de la información será recibida y comprendida.

2. Rapidez: Es la cualidad que permite la llegada de un mensaje o comunicación a los destinatarios en el menor tiempo posible.
3. Seguridad: Es el resultado de la adopción de medidas que permitan las transmisiones libres del riesgo de poder ser interceptadas, analizadas o confundidas por el enemigo, presunto o real.

Haciendo énfasis en la seguridad de las comunicaciones militares, las medidas adoptadas por el Ejército español consisten en el cifrado automático de la información, realizado por el propio equipo radio. A nivel táctico y de unidades de acción, no se tiene en cuenta el ámbito de las comunicaciones a nivel físico, es decir, la Seguridad en la Capa Física. Al poseer equipos radio ya configurados previamente, la interoperabilidad, que es la capacidad de operar cohesionados distintos medios o equipos, entre unidades sólo es posible si ambos poseen el mismo equipo radio.

Cuantas más medidas de seguridad a nivel físico se puedan adoptar, mayor sería tanto la capacidad de operar entre distintos equipos, como la flexibilidad y poder de adaptación de equipos radio programables para distintas situaciones. Sin embargo, la Seguridad en la Capa Física es un ámbito escasamente explorado en el sector de Defensa.

2.2 Sistemas MIMO

2.2.1 Definición y fundamentos

Los sistemas MIMO son sistemas de comunicaciones inalámbricas que se basan en el uso de múltiples antenas en ambos extremos de un canal. Un sistema que utiliza múltiples antenas en uno de los extremos se denomina Sistema de Antenas Inteligentes [11]. A pesar de dichas definiciones, el ámbito de los sistemas MIMO utiliza el principio de Antenas Inteligentes para el estudio de sus diferentes escenarios, por lo que se puede incluir el término Antenas Inteligentes dentro de sistemas MIMO. Estos sistemas tienen los siguientes objetivos:

- Aumentar la cobertura mediante conformado de haz, técnica empleada con *arrays* de antenas.
- Incrementar la capacidad del sistema, como cualidad más destacada, aumentando la SINR (*Signal-to-Interference and Noise Ratio*, Relación Señal-Interferencia-Ruido) que se define como la relación entre la señal y la suma del ruido e interferencia de otros usuarios, siendo ambos factores que actúan en detrimento de la calidad de un canal. Como resultado del aumento de la SINR, es posible incorporar un mayor número de usuarios al sistema.
- Aumentar la calidad de la conexión, como consecuencia directa de la reducción de la potencia de interferencia recibida.
- Mejora de estimación de posición del usuario gracias al conocimiento de las DOAs (*Direction of Arrival*, dirección de llegada) de un usuario, especialmente en aquellos que se encuentran en LOS.

Asimismo, los sistemas MIMO cuentan con las siguientes limitaciones:

- Interferencias entre usuarios: en sistemas MIMO es probable que la comunicación sea interferida en mayor o menor medida por otro usuario por proximidad de canales en uso, o similar direccionalidad de canal.

- La gestión de distintos canales puede ser compleja debido a que distintos usuarios emplearán canales de comunicación en mismos instantes de tiempo, así como en frecuencias similares. Es por ello por lo que se estudian diferentes técnicas como multiplexación temporal o frecuencial. Dichas técnicas serán desarrolladas en futuros apartados.
- La multiplexación espacial (Apartado 2.2.3) para estudios como el presente requiere conocimiento de CSI (*Channel State Information*, Información del Estado del Canal), información que es de complicado conocimiento en estaciones en movimiento. CSI se puede dar tanto en el transmisor (CSIT, *Channel State Information at the transmitter*, Información del Estado del Canal en Transmisor) como en el receptor (CSIR, *Channel State Information at the receiver*, Información del Estado del Canal en Receptor).

Los sistemas de comunicaciones MIMO se analizan en base a la forma de comunicación. Su funcionamiento depende de si se trata de un sistema MIMO de un usuario (punto a punto), de múltiple acceso, o de difusión. En Figura 2-12, Figura 2-13 y Figura 2-14 se pueden apreciar ejemplos de los distintos sistemas respectivamente.

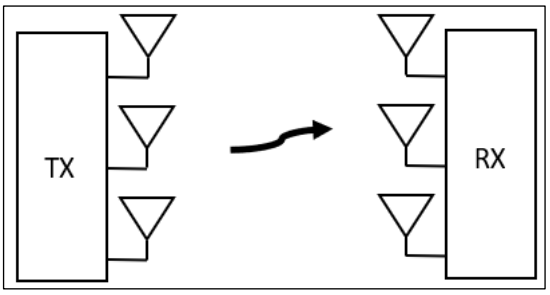


Figura 2-12: MIMO punto a punto [Elaboración propia].

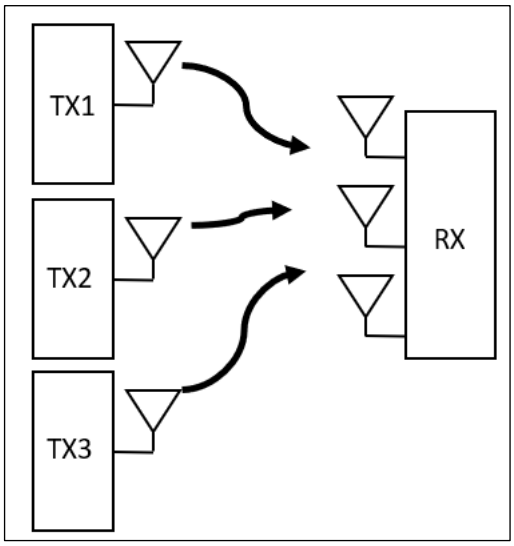


Figura 2-13: MIMO múltiple acceso [Elaboración propia].

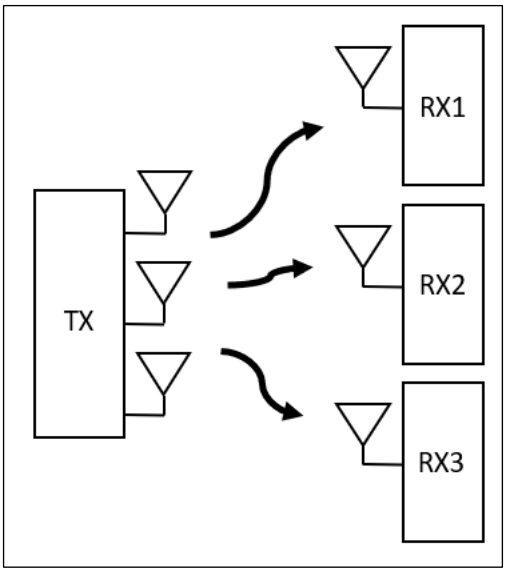


Figura 2-14: MIMO de difusión [Elaboración propia].

Los sistemas MIMO buscan explotar sus capacidades mediante técnicas como la diversidad. La diversidad es un método empleado en Telecomunicaciones como reacción a uno de los mayores problemas del ámbito: la atenuación de señal (*fading*). En un canal inalámbrico formado por un transmisor y un receptor, ambos con una antena, los paquetes de información viajarían a través de un canal, el cual tiene una probabilidad de atenuación suficientemente severa como para impedir decodificar los datos en la recepción, es decir, que a través de él cabe la posibilidad de que los paquetes de información se "pierdan", como se muestra en la Figura 2-15.

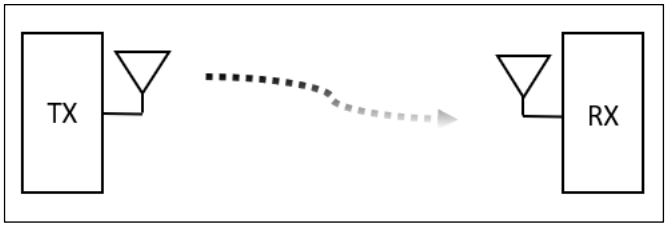


Figura 2-15: Atenuación en sistema SISO [Elaboración propia].

Para solventar dicho problema, se utiliza la diversidad [21]. El concepto de la diversidad en sistemas MIMO es básico, y puramente estadístico: a mayor número de transmisores, mayor será la probabilidad de que los paquetes transmitidos sean recibidos con éxito, como se muestra en la Figura 2-16.

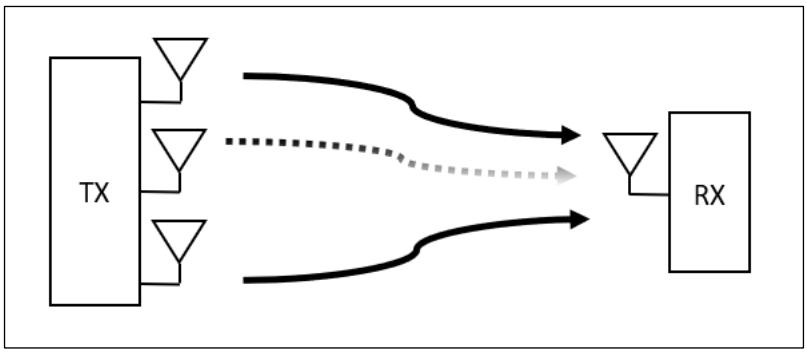


Figura 2-16: Diversidad de canales (3) con atenuación en uno de ellos [Ilustración propia].

La forma en la que los sistemas MIMO suelen compararse con otros escenarios de sistemas de comunicaciones inalámbricas es analizando la capacidad de información del sistema, y estos análisis se realizan matemáticamente. Al ser una métrica de tipo, el canal a emplear es el modelo Gaussiano [22]. En dicho modelo matemático, siempre interviene una señal de entrada, ruido (Gaussiano, independiente) *n* y una señal de salida. Los canales Gaussianos pueden estar sometidos a *fading* estadístico, como es el caso del *Rayleigh fading*, y a restricciones de potencia. De lo contrario, el modelo sería de capacidad ilimitada.

2.2.2 Capacidad en sistemas punto a punto

La capacidad de información de un canal (Ecuación 2-1) se define como la máxima información mutua entre dos variables (entrada y salida) que puede ofrecer una potencia determinada afectada por el resto de los factores que intervienen en la comunicación [22].

$$C = \max I(x; y)$$

Ecuación 2-1

La información mutua, que como parte de teoría de la información utiliza entropías (cantidad de información que contiene un símbolo), es la cantidad de información que se obtiene de una variable a partir de otra variable. En un canal inalámbrico, la representación de la información mutua se puede asemejar a un diagrama de Venn (Figura 2-17) en el que *H(x)* es la entropía de la variable *x* (entrada), *H(y)* es la entropía de la variable y (salida), *H(x|y)* es la entropía de *x* condicionada por el valor de *y*, ocurriendo al contrario en *H(y|x)*. *I(x;y)* es la Información Mutua entre ambas variables *x* e *y*.

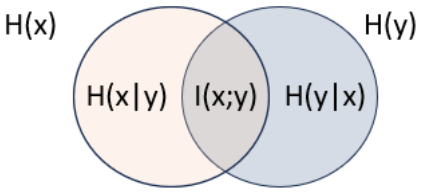


Figura 2-17: Diagrama de Venn, Teoría de la Información [Elaboración Propia].

En la Figura 2-18 se puede apreciar una comunicación en la que se transmite x y se recibe y. A pesar de *H(y)* recibido a la salida (*output*), al depender de *x*, la Información Mutua de las dos variables es menor, como se puede observar en la Ecuación 2-2.

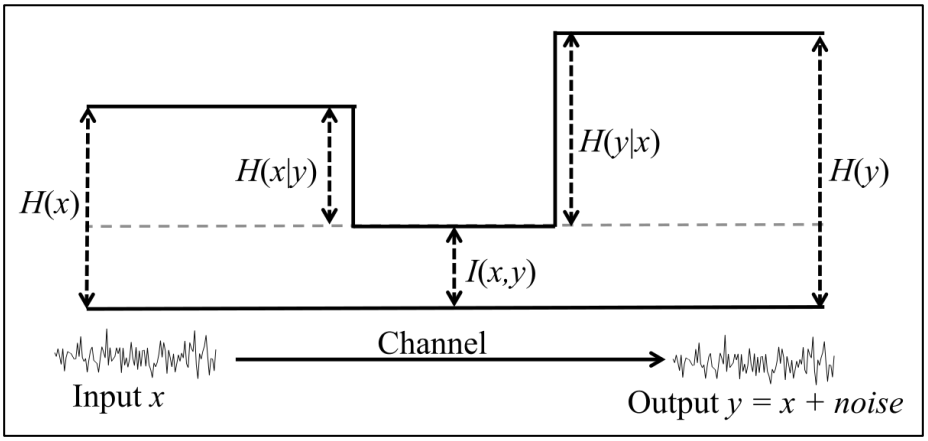


Figura 2-18: Información mutua I(x,y) de un canal SISO básico [23].

$$I(x;y) = H(y) - H(y|x) = H(x) - H(x|y)$$

Ecuación 2-2

La capacidad es dependiente de la SINR. La SINR relaciona la potencia de transmisión y la potencia del ruido, al que se debe sumar la posible interferencia en caso de existir otros usuarios en la comunicación. En Telecomunicaciones, la capacidad es calculada logarítmicamente, utilizando la base logarítmica 2 comúnmente asociada al bit. El empleo de múltiples antenas aumenta la capacidad del sistema de comunicaciones considerablemente como se demuestra a continuación.

- *Capacidad en sistema SISO punto a punto*

Para un sistema de comunicaciones SISO (*Single-Input Single-Output*, Una Entrada Una Salida) se definirá la comunicación previamente codificada como se presenta en la Ecuación 2-3 y Figura 2-19, donde *x* es la señal a la salida, *h* es el canal, *p* es el *precoder* o codificación previa, *s* es la información a la entrada y *n* es el ruido [24].

El modelo matemático que se va a estudiar supone que h es una variable aleatoria compleja y gaussiana de potencia unitaria.

$$y = hpx + n$$

Ecuación 2-3

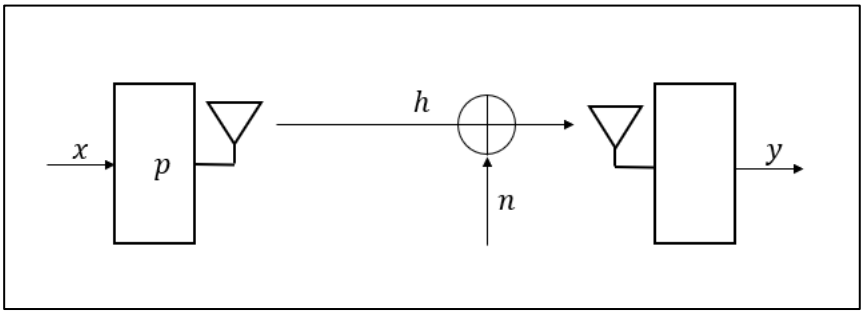


Figura 2-19: canal (valor escalar) en SISO [Elaboración propia].

La capacidad en un sistema de comunicaciones SISO se define como en la Ecuación 2-4. En dicha ecuación se define la SINR como la relación entre $|h|^2 p$ y σ_n^2. El numerador es el producto entre la norma del canal como número complejo ($|h|^2$) y la potencia transmitida p, que es escalar. El denominador es la potencia esperada del ruido (σ_n^2), y equivale al valor esperado de la norma del vector potencia de ruido, como se muestra en la Ecuación 2-5.

$$C_{SISO} = log_2(1 + SINR) = log_2(1 + \frac{|h|^2 p}{\sigma_n^2})$$

Ecuación 2-4

$$\sigma_n^2 = E[|n|^2]$$

Ecuación 2-5

Cabe destacar que en caso de tratarse de un sistema de comunicaciones SISO entre un transmisor y un receptor, la SINR equivaldría a la SNR ya que no existe interferencia de otros usuarios.

Con este modelo de capacidad se puede apreciar el uso de un único canal, y una única potencia transmitida. Este factor proporciona capacidad limitada al sistema, que se demostrará en los próximos apartados.

- *Capacidad en sistema MISO punto a punto*

Para un sistema de comunicaciones MISO (*Multiple-Input Single-Output*, Múltiples Entradas Una Salida) se definirá la comunicación previamente codificada como se presenta en la Ecuación 2-6 y Figura 2-20 en la que *y* es la señal a la salida, $\boldsymbol{h} = [h_1, \dots, h_N]$ es el vector canal representado, $\boldsymbol{p}[p_1, \dots, p_N]$ es el vector *precoder*, x es la información a la entrada y *n* es el ruido aleatorio que afecta a la antena receptora [24].

En este caso las componentes de $\boldsymbol{h}$ pueden estar correladas o incorreladas espacialmente entre sí, ya que la correlación permite analizar o suponer patrones entre componentes. Por ejemplo, el retardo al recibir un frente de onda por parte de un *array* de antenas permite determinadas suposiciones basadas en la colocación espacial de cada antena del *array*.

$$\boldsymbol{y = h^H p x + n}$$

Ecuación 2-6

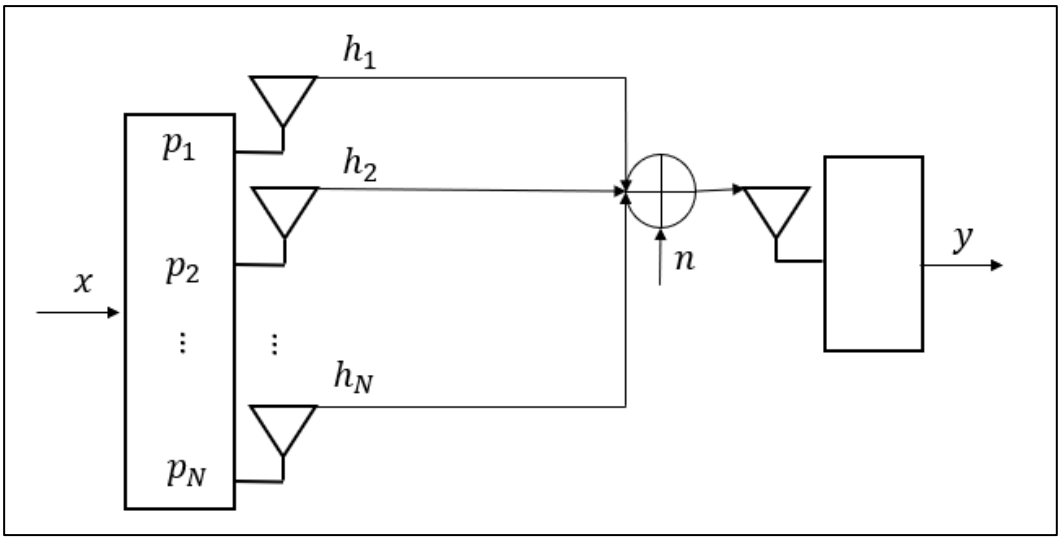


Figura 2-20: Comunicación MISO [Elaboración propia].

En un sistema MISO, el número de antenas transmisoras es igual al número de canales disponibles para realizar la transmisión, empleando así la diversidad de canales. A su vez, para cada canal se puede realizar su correspondiente *precoding*. Es por ello por lo que un sistema MISO es más sofisticado que un sistema SISO.

En cuanto a la capacidad de un sistema MISO (Ecuación 2-7), en este caso el numerador en la SINR contiene la norma del sumatorio de los productos entre tantos canales como *precoder* existan. Como consecuencia directa, la SINR aumenta con el uso de más canales y *precoders* [25]. Al disponer de mayor número de antenas, existe mayor flexibilidad para el *precoding* del mensaje a transmitir, y es por ello por lo que en sistemas MISO $\boldsymbol{p}$ se trata de una matriz de dimensión, no un escalar. Cabe destacar que sólo la antena receptora se ve afectada por el ruido Gaussiano, pero como se muestra en la Ecuación 2-7, la capacidad se sigue viendo aumentada en relación con el número de antenas empleadas para transmitir (N).

$$C_{MISO} = log_2(1 + SINR) = log_2\left(1 + \frac{|\sum_{i=1}^{N} h_i^* p_i|^2}{\sigma_n^2}\right)$$

Ecuación 2-7

2.2.3 Sistemas multiusuario

Los sistemas multiusuario son ampliamente estudiados tanto en el empleo de múltiples antenas como en sistemas más simples, ya que implican mayor complejidad de funcionamiento y fundamentos.

Dichos sistemas tienen dos principales problemas: el distribuir la información con capacidad suficiente, que se trata parcialmente en el apartado 2.2.2, y el gestionar la interferencia entre usuarios [21].

- *Uplink y Downlink*

El canal *uplink* (Canal de subida), también conocido como MAC (*Multiple Access Channel*, Canal de Acceso Múltiple) es el canal asociado a un dispositivo o estación a través del cual recibe datos de otros usuarios, por ejemplo, la conexión de diversos usuarios a una red WiFi se realiza mediante el canal *uplink* del *router* (enrutador) WiFi.

El canal *downlink* (Canal de bajada), también conocido como BC (*Broadcast*, Difusión), es el canal asociado a un dispositivo a través del cual transmite datos a otros usuarios, por ejemplo, una estación radio difunde información a diversos usuarios mediante el canal *downlink.*

Ante la problemática de gestionar ambos canales por parte de las estaciones transmisoras y receptoras, se diferenciaron ambos canales mediante el empleo de distintas frecuencias, o distintos instantes de tiempo; gestionando así los recursos para servir a todos los usuarios. En este Proyecto, se definirán las técnicas de gestión en el canal de acceso múltiple de una estación.

- *FDMA*

Frequency Division Multiple Access (Acceso Múltiple por División de Frecuencia) es una técnica de multiplexación en la que se dividen los canales según el ancho de banda disponible, en tantas partes como el número de usuarios requiera, pudiendo ser empleado cada canal en el mismo instante temporal como se indica en la Figura 2-21.

FDMA es un método eficaz pero que está limitado por el ancho de banda disponible para cada usuario.

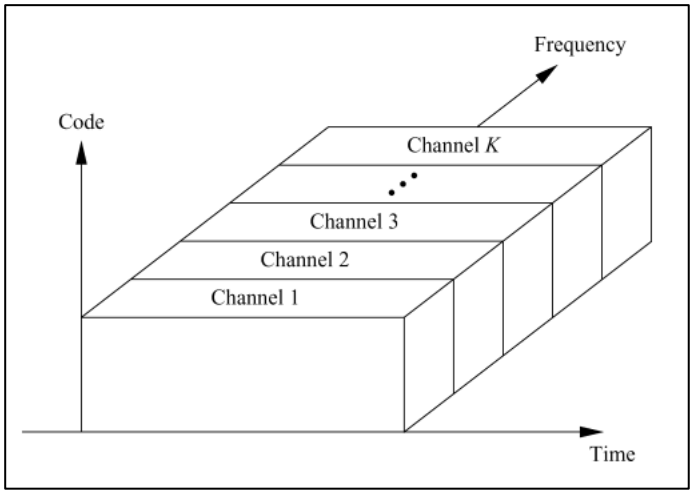


Figura 2-21: Representación gráfica FDMA [21].

- *TDMA*

Time Division Multiple Access (Acceso Múltiple por División Temporal) es una técnica de multiplexación en la que cada canal ocupa al completo el ancho de banda disponible durante un corto periodo de tiempo denominado *slot*, como se muestra en la Figura 2-22. Cuanto mayor sea el número de usuarios, y por lo tanto de canales, mayor será el tiempo que transcurra hasta que el mismo canal vuelva a ocupar todo el ancho de banda.

A pesar de ser un método efectivo, si un canal está formado por demasiados usuarios, TDMA provocará una conexión de baja calidad, ya que la tasa de datos disponible sería insuficiente.

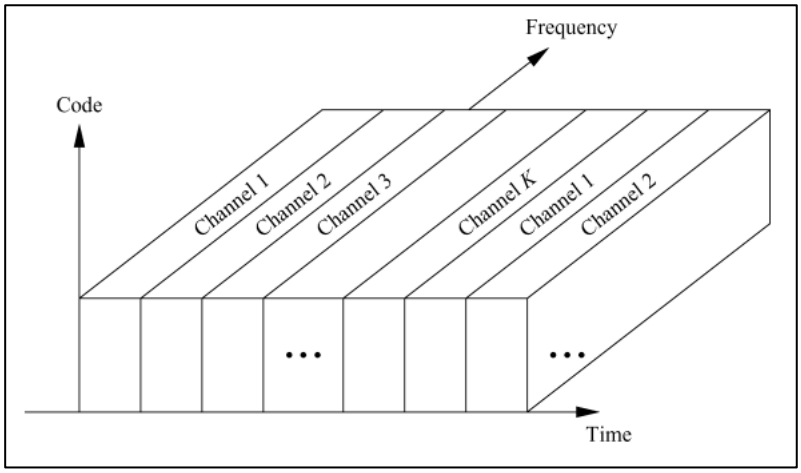


Figura 2-22: Representación gráfica TDMA [21].

- *CDMA*

Code Division Multiple Access (Acceso Múltiple por División de Código) es una técnica de mayor complejidad que las anteriores, ya que cada usuario emplea el ancho de banda total del canal en mismos instantes temporales, como se muestra en la Figura 2-23. La diferencia es que cada transmisión incluye un código, que, al ser recibido, permite al receptor decodificar dicha transmisión mediante diferentes técnicas. El nivel de complejidad en CDMA es superior ya que permite mayor número de opciones que supongan una solución en comparación a TDMA o FDMA.

A pesar de la eficacia de CDMA, la posterior decodificación tras recibir el mensaje ya supone el empleo de tiempo por parte del receptor. Además, esta técnica es más susceptible de provocar interferencias entre usuarios, ya que la coincidencia en tiempo y frecuencia provoca una acumulación de datos que pueden interferir a pesar de diversos métodos de codificación.

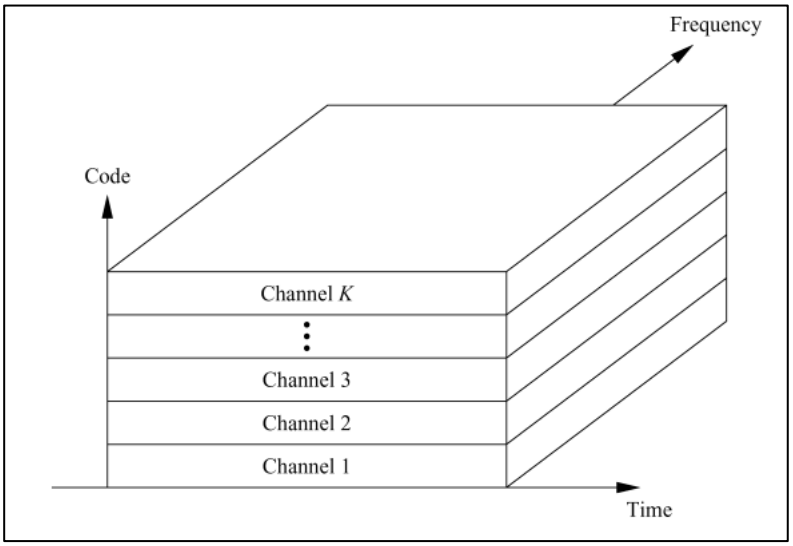


Figura 2-23: Representación gráfica CDMA [21].

- *SDMA*

Space Division Multiple Access (Acceso Múltiple por División Espacial) es una técnica que trata de conseguir gestionar el acceso múltiple a un servicio mediante separación espacial de canales, como se muestra en la Figura 2-25. Este método es una gran opción ya que las medidas empleadas se realizan a nivel físico, es decir, los factores involucrados en SDMA son la direccionalidad de una antena, así como el empleo de *arrays* de antenas (múltiples antenas) con el propósito de gestionar de la manera más eficaz dicha direccionalidad para obtener el mayor beneficio posible.

En términos de capacidad, la direccionalidad de la antena está relacionada con el *precoder*, mientras que el empleo de *arrays* de antenas aumenta directamente el número de canales. Ambos factores demuestran en la Ecuación 2-7 que su potenciación beneficia a la SINR considerablemente. La tecnología de múltiples antenas enfoca su estudio en conseguir mayor capacidad de información y en abarcar el mayor número de usuarios posible con enlaces de calidad.

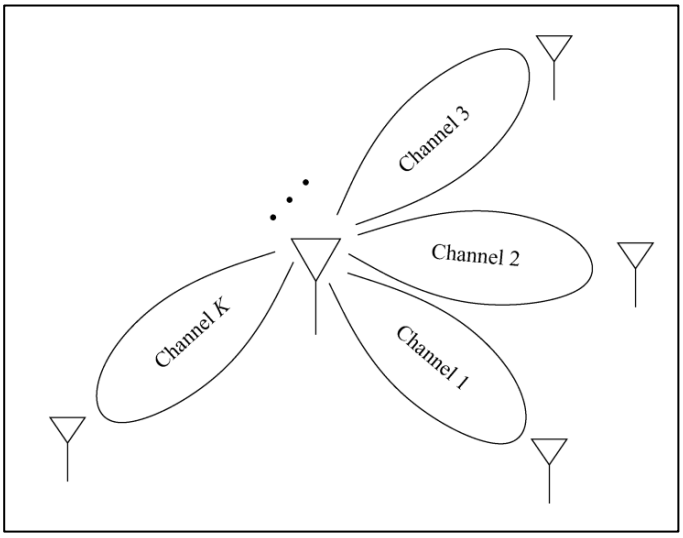


Figura 2-24: Representación gráfica SDMA [21].

2.2.4 Capacidad en sistemas multiusuario

La capacidad de información en un sistema depende en gran parte de la SNR de la que disponga el sistema como se demostró en el Apartado 2.2.2, en el que este factor se veía afectado por el ruido. En los sistemas multiusuario el término a emplear es la SINR, ya que en este caso afecta negativamente tanto el ruido como la interferencia que causen el resto de los usuarios sobre el canal entre dos usuarios.

A continuación, se mostrarán distintos escenarios de comunicación multiusuario y su relación con la capacidad del sistema.

- *Capacidad en SISO multiusuario*

El primer escenario para estudiar es la comunicación entre un usuario transmisor y $\boldsymbol{u} = (u_1, u_2, \dots, u_U)$ usuarios receptores, como se muestra en la Figura 2-25. Este escenario ejemplifica el canal *downlink*, realizando *Broadcast* por parte del transmisor.

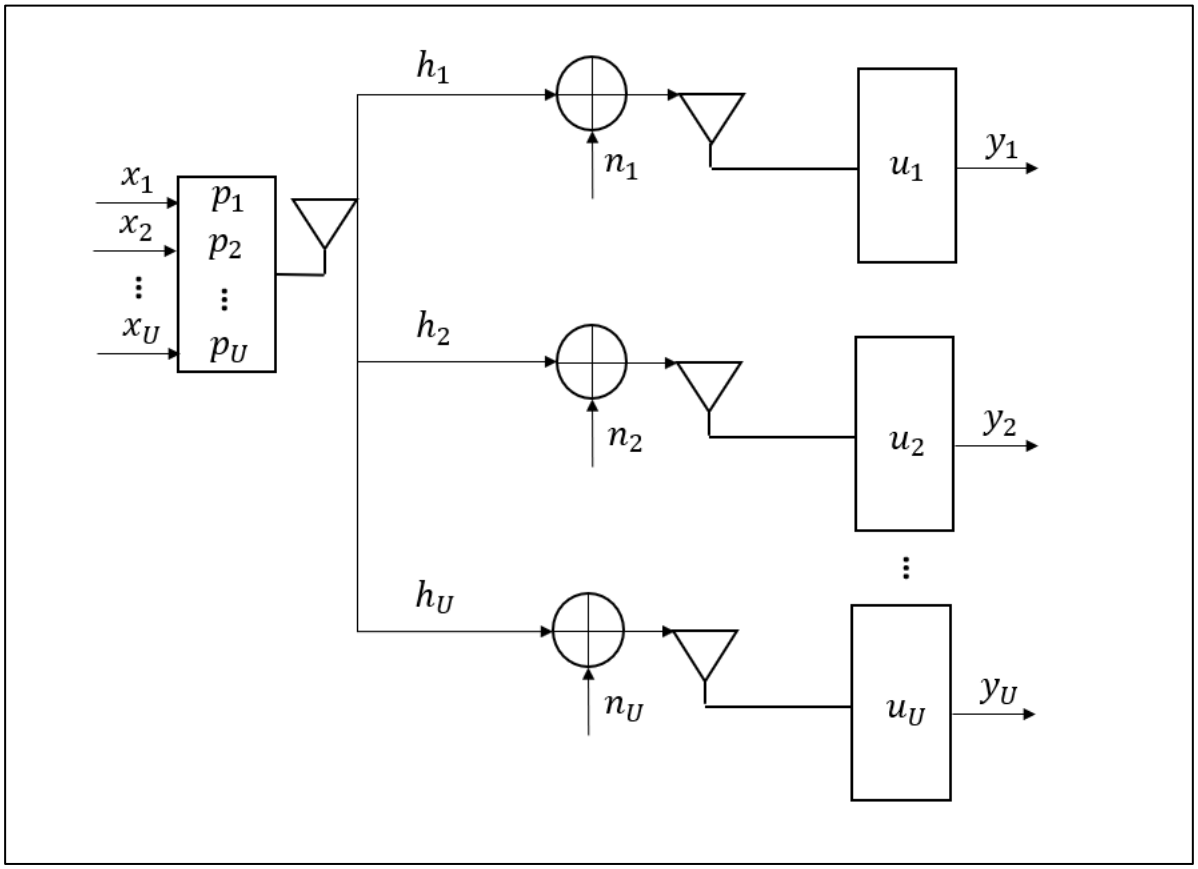


Figura 2-25: SISO multiusuario [Elaboración propia].

En dicha comunicación, se asume que el transmisor no utiliza ninguna técnica de multiplexación, es decir, no controla la potencia de transmisión en base al usuario destinatario de determinada información; y que cada receptor espera un mensaje distinto $\boldsymbol{x} = (x_1, x_2, \dots, x_U)$, es decir, no se trata de una estación radio que difunde información destinada a todos los usuarios por igual (*Common Data*, Datos Comunes). El ruido recibido es distinto para cada antena receptora, aunque no es un factor para tener en cuenta ya que ambos valores comparten similitudes. El *precoding* es muy limitado, ya que la potencia máxima que puede ser utilizada por la antena para transmitir debe ser dividida para cada usuario. En otras palabras, $p = \sum_{i=1}^{U} p_i$. El *precoding* $\boldsymbol{p}$ visto en el apartado anterior es vectorial debido a sus múltiples componentes, pero en este caso los valores de $\boldsymbol{p}$ provienen de la gestión de la potencia que permite una antena. Por lo tanto, la capacidad de u_1 y u_2 es la correspondiente a la Ecuación 2-8 y Ecuación 2-9, respectivamente; mientras que la capacidad para u_U sería la respectiva a la Ecuación 2-10.

$$C_{SISO,u_1} = log_2(1 + SINR_{u_1}) = log_2(1 + \frac{|h_1|^2 p_1}{\sigma_{n_1}^2 + (\sum_{i=1}^{U} |h_1|^2 p_i) - |h_1|^2 p_1})$$

Ecuación 2-8

$$C_{SISO,u_2} = log_2(1 + SINR_{u_2}) = log_2(1 + \frac{|h_2|^2 p_2}{\sigma_{n_2}^2 + (\sum_{i=1}^{U} |h_2|^2 p_i) - |h_2|^2 p_2})$$

Ecuación 2-9

$$C_{SISO,u_U} = log_2(1 + SINR_{u_U}) = log_2(1 + \frac{|h_U|^2 p_U}{\sigma_{n_U}^2 + (\sum_{i=1}^{U} |h_U|^2 p_i) - |h_U|^2 p_U})$$

Ecuación 2-10

Aunque no se tenga en cuenta la dificultad que supondría decodificar la señal recibida, la SINR es insuficiente, ya que la potencia transmitida a un usuario causa interferencia sobre el resto, y es muy poco modificable puesto que la potencia de una única antena es de un grado de libertad (*Degrees of Freedom*, DoF), es decir, un solo haz es más difícil de adecuar a distintos usuarios que varios haces. El mayor contraste en comparación con los sistemas punto a punto es que la potencia $\boldsymbol{p}$ interviene tanto en la señal recibida como en la interferencia que causa a otros usuarios, por lo que la capacidad no aumenta. Este problema es la principal causa de la aparición de las técnicas de multiplexación vistas en el Apartado 2.3.3, las cuales permitirían aumentar la SINR reduciendo la interferencia que se causaría entre usuarios.

- *Capacidad en MISO multiusuario*

Los sistemas MISO multiusuario emplean múltiples antenas para realizar *broadcast*. El escenario que se analizará en este apartado incluye una estación base con *N* antenas transmisoras, y $\boldsymbol{u}$ usuarios receptores con una antena cada uno, como se aprecia en la Figura 2-26.

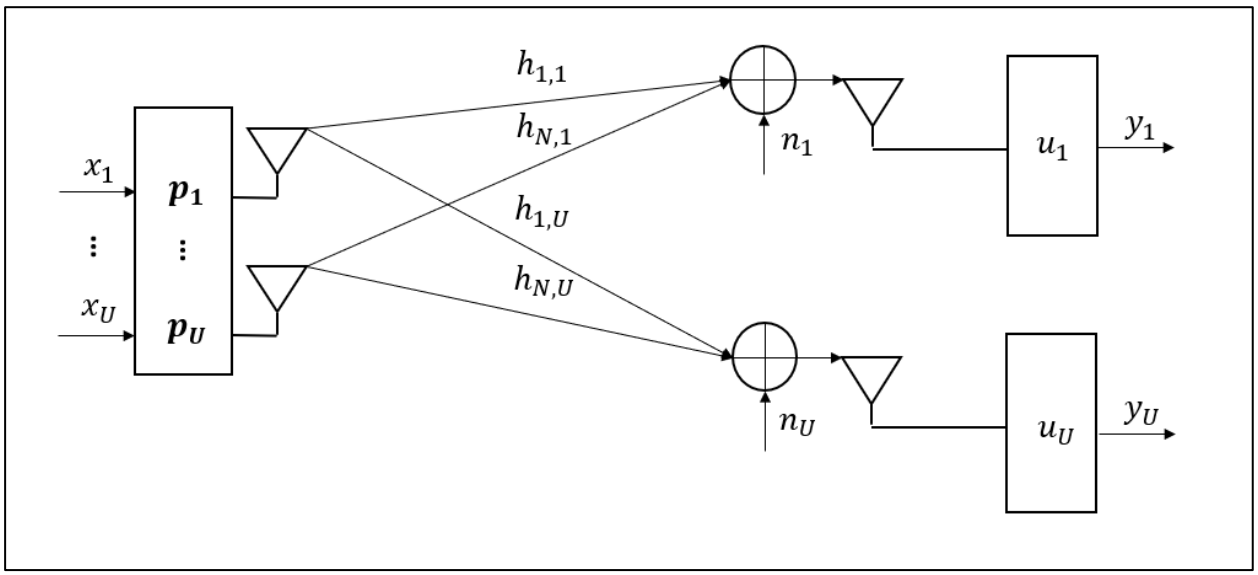


Figura 2-26: MISO multiusuario [Elaboración propia]

En la Figura 2-26 es apreciable tanto la ganancia en diversidad de canales como la posibilidad de transmitir el producto de datos ($\boldsymbol{x}$) y *precoder* ($\boldsymbol{P}$) a través de N antenas, lo que permite mayor dimensión para $\boldsymbol{P}$, es decir, mayor flexibilidad de transmisión. El número de canales empleados es dependiente del

número de antenas transmisoras y el número de usuarios receptores. En este caso, u_1 cuenta con $\boldsymbol{h_1} = (h_{1,1}, \dots, h_{N,1})$ y, en consecuencia, u_U con $\boldsymbol{h_U} = (h_{1,U}, \dots, h_{N,U})$.

Los canales de cada usuario se recogen en $\boldsymbol{H_{UxN}} = \begin{pmatrix} \boldsymbol{h_1} \\ \boldsymbol{h_2} \\ \vdots \\ \boldsymbol{h_U} \end{pmatrix}$, mientras que el *precoder* se define como $\boldsymbol{P_{UxN}} = \begin{pmatrix} \boldsymbol{p_1} \\ \boldsymbol{p_2} \\ \vdots \\ \boldsymbol{p_U} \end{pmatrix}$.

El *precoder* es dependiente del número de antenas transmisoras y el número de canales existentes, pero la señal a transmitir ($\boldsymbol{Px}$) podrá ser recibida con mejor calidad cuanto mayor DoF tenga, ya que el *precoder* puede ser más flexible al tener mayor dimensión.

La capacidad para el primer usuario u_1 será la reflejada en la Ecuación 2-11.

$$C_{MISO,u_1} = log_2(1 + SINR_{u_1}) = log_2(1 + \frac{|\boldsymbol{h_1^H p_1}|^2}{\sigma_{n_1}^2 + \left(\sum_{i=1}^{U} |\boldsymbol{h_1^H p_i}|^2\right) - |\boldsymbol{h_1^H p_1}|^2})$$

Ecuación 2-11

En la Ecuación 2-11 se aprecia la interferencia causada por el resto de los usuarios, por lo que el objetivo consiste en conseguir un sumatorio de productos con el menor valor posible, para así beneficiar el valor total de la SINR. La capacidad para u_U sería la reflejada en la Ecuación 2-12.

$$C_{MISO,u_U} = log_2(1 + SINR_{u_U}) = log_2(1 + \frac{|\boldsymbol{h_U^H p_U}|^2}{\sigma_{n_U}^2 + \left(\sum_{i=1}^{U} |\boldsymbol{h_U^H p_i}|^2\right) - |\boldsymbol{h_U^H p_U}|^2})$$

Ecuación 2-12

En la Ecuación 2-12, cada vector *precoder* debe ser diseñado para adaptarse matemáticamente a cada vector canal $\boldsymbol{H_{UxN}} = \begin{pmatrix} \boldsymbol{h_1} \\ \boldsymbol{h_2} \\ \vdots \\ \boldsymbol{h_U} \end{pmatrix}$, para así conseguir valores de capacidad de información más eficaces. En otras palabras, un mensaje x_1 destinado a u_1 deberá ser precodificado ($\boldsymbol{p_1}$) para que el producto de $|\boldsymbol{h_1^H p_1}|^2$ tenga un valor considerablemente superior a la interferencia $\left(\sum_{i=1}^{U} |\boldsymbol{h_1^H p_i}|^2\right) - |\boldsymbol{h_1^H p_1}|^2$, la cual debería tratar de obtener el efecto contrario: un valor bajo para así causar la menor interferencia posible. En caso de no ser así, la posterior decodificación por parte del receptor sería de extrema dificultad, puesto que recibe en similares proporciones tanto los datos destinados a dicho receptor como aquellos destinados a otros receptores, como se muestra en la Ecuación 2-13.

$$y_1 = \boldsymbol{h_1}\left(\sum_{i=1}^{U} p_i x_i\right) + n_1$$

Ecuación 2-13

A continuación, tras analizar la capacidad en distintos escenarios con múltiples antenas, se profundizará en el canal y el *precoding*.

2.2.5 Comparación de escenarios

Los diferentes escenarios analizados anteriormente pueden ser simulados mediante la herramienta *Matlab*. Inicialmente se realizarán simulaciones de los sistemas punto a punto.

- *Simulación en sistemas punto a punto*

Los sistemas punto a punto que se analizaron en el Apartado 2.2.3 son SISO y MISO. Para realizar la simulación en *Matlab*, es necesario formular el código a emplear, el cual se muestra a continuación:

```
clc;

close all;
clear all;

ITER = 2500;
SNRdB = 0:25;
SNR = 10.^(SNRdB/10);
C_SISO = zeros(1,length(SNR));
C_MISO2 = zeros(1,length(SNR));
C_MISO3 = zeros(1,length(SNR));
C_MISO4 = zeros(1,length(SNR));

    for ite = 1:ITER
        h_SISO = (randn +1i*randn);
        h_MISO2 = (randn(1,2)+1i*randn(1,2));
        h_MISO3 = (randn(1,3)+1i*randn(1,3));
        h_MISO4 = (randn(1,4)+1i*randn(1,4));

        for K = 1:length(SNR)
            C_SISO(K) = C_SISO(K) + log2(1+ SNR(K)*norm(h_SISO)^2);
            C_MISO2(K) = C_MISO2(K) + log2(1+ SNR(K)*norm(h_MISO2)^2);
            C_MISO3(K) = C_MISO3(K) + log2(1+ SNR(K)*norm(h_MISO3)^2);
            C_MISO4(K) = C_MISO4(K) + log2(1+ SNR(K)*norm(h_MISO4)^2);
        end

    end
C_SISO = C_SISO/ITER;
C_MISO2 = C_MISO2/ITER;
C_MISO3 = C_MISO3/ITER;
C_MISO4 = C_MISO4/ITER;

plot(SNRdB,C_SISO,'r',SNRdB,C_MISO2,'m',SNRdB,C_MISO3,'g',SNRdB,C_MISO4,'k')
legend('SISO','MISO2','MISO3','MISO4')
xlabel('SNR en dB')
ylabel('Capacidad (b/s/Hz)')
title('Capacidad Vs. SNR')
grid;
```

Dicho código es una modificación realizada al código de [26] y proporciona la capacidad en bps/Hz según la SNR. El código establece el vector SNR (1x26) en el que se incluye el ruido que afectará a cada canal. Tras definir los vectores de capacidad de cada escenario, se generan los vectores canal, con tantas componentes como antenas transmisoras contiene el transmisor. Para obtener un resultado más estable, se realiza el cálculo de las capacidades mediante la media de 2500 iteraciones. En la Figura 2-27 se muestra la gráfica con los resultados obtenidos.

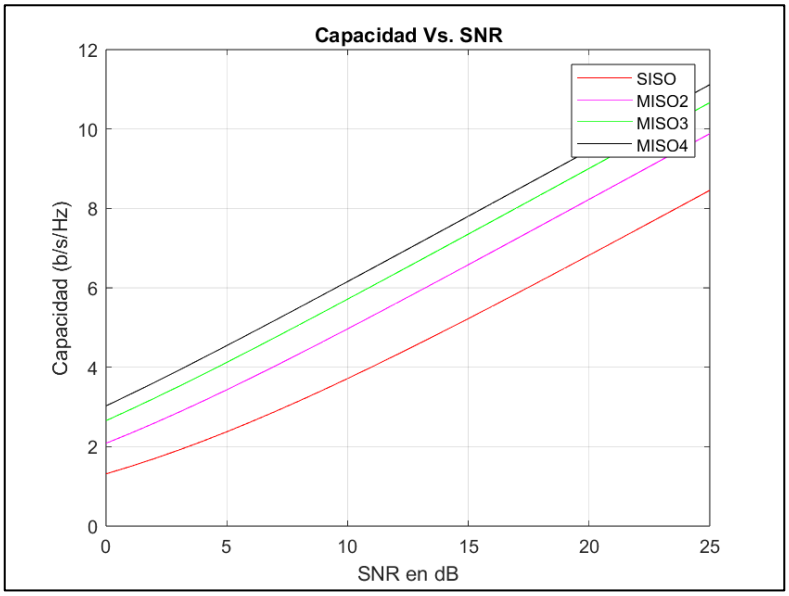


Figura 2-27: Capacidad en distintos escenarios punto a punto [Elaboración propia].

El resultado del análisis concluye que cuanto mayor sea el número de antenas transmisoras en un sistema MISO, mayor será la capacidad de información del sistema. La capacidad de un sistema SISO es inferior a la obtenida en cualquier sistema MISO en las condiciones establecidas.

Los resultados obtenidos son los esperados según el Apartado 2.2.2, pero los sistemas SISO cuentan con clara desventaja a la hora de ser analizados, puesto que el hecho de realizar sumatorios a valores de capacidad sólo indica los beneficios relacionados con el incremento del número de antenas. La siguiente simulación se realiza con una modificación en el código, de tal forma que el código empleado es el siguiente:

```
clc;

close all;
clear all;

ITER = 2500;
SNRdB = 0:25;
SNR = 10.^(SNRdB/10);
C_SISO = zeros(1,length(SNR));
C_MISO2 = zeros(1,length(SNR));
C_MISO3 = zeros(1,length(SNR));
C_MISO4 = zeros(1,length(SNR));

    for ite = 1:ITER
        h_SISO = (randn +1i*randn);
        h_MISO2 = (randn(1,2)+1i*randn(1,2));
        h_MISO3 = (randn(1,3)+1i*randn(1,3));
        h_MISO4 = (randn(1,4)+1i*randn(1,4));

        for K = 1:length(SNR)
            C_SISO(K) = C_SISO(K) + log2(1+ SNR(K)*norm(h_SISO)^2);
            C_MISO2(K) = C_MISO2(K) + log2(1+ SNR(K)*norm(h_MISO2)^2/2);
            C_MISO3(K) = C_MISO3(K) + log2(1+ SNR(K)*norm(h_MISO3)^2/3);
            C_MISO4(K) = C_MISO4(K) + log2(1+ SNR(K)*norm(h_MISO4)^2/4);
        end

    end
```

```
C_SISO = C_SISO/ITER;
C_MISO2 = C_MISO2/ITER;
C_MISO3 = C_MISO3/ITER;
C_MISO4 = C_MISO4/ITER;

plot(SNRdB,C_SISO,'r',SNRdB,C_MISO2,'m',SNRdB,C_MISO3,'g',SNRdB,C_MISO4,'k')
legend('SISO','MISO2','MISO3','MISO4')
xlabel('SNR en dB')
ylabel('Capacidad (b/s/Hz)')
title('Capacidad Vs. SNR')
grid;
```

En este caso se trata de obtener un resultado adaptado a una de las antenas, con el objetivo de comprobar si cada antena independiente obtiene un valor de capacidad superior al que obtiene SISO.

Como se puede comprobar en la Figura 2-28, la diferencia entre los resultados obtenidos es menor que en el caso anterior, y entre sistemas MISO es mínima. Los parámetros modificados y empleados en esta simulación no explotan las capacidades de estos sistemas ya que no se está haciendo uso del *precoding*, por lo que a pesar de demostrar las ventajas en sistemas MISO, existe margen de mejora.

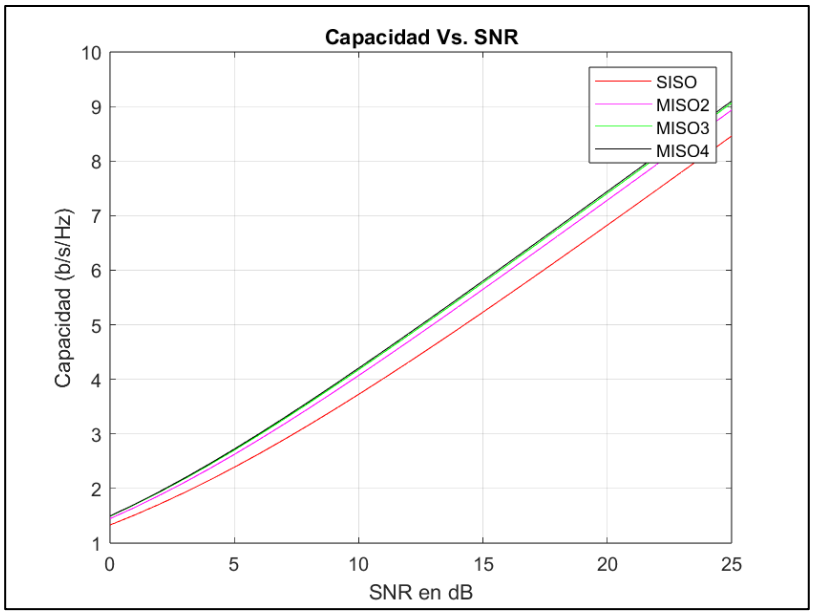


Figura 2-28: Capacidad en distintos escenarios punto a punto [Elaboración propia].

2.3 Canal inalámbrico con frente de ondas plano

Un frente de ondas se define como el lugar geométrico que une todos los puntos que, en un instante dado, se encuentran en idéntico estado de vibración, es decir, tienen igual fase. Existen distintas maneras de considerar los frentes de ondas: frente de ondas plano y frente de ondas esférico. Un frente de ondas plano es comúnmente asumido en situaciones en las que se recibe un frente de ondas esférico a una distancia determinada, a partir de la cual es considerado plano.

Al definir un modelo de canal asumiendo que su frente de ondas es plano, se tienen en cuenta consideraciones que facilitan el estudio de dicho canal. La recepción de una onda plana por parte de un *array* de antenas centra el estudio en el retardo existente entre la recepción (o transmisión) de la onda por parte de todas las antenas, y en la posición geométrica de las antenas.

En la Figura 2-29 se aprecia la vista en planta de un *array* de tres antenas recibiendo un frente de ondas plano, así como líneas con distinto patrón de trazado que indican el momento de recepción de la onda por parte de cada antena, es decir, el retardo τ. En la Figura 2-29 también se indica el comportamiento de la onda a medida que avanza espacialmente, adoptando la forma de frente de ondas plano antes de ser recibida por el *array* de antenas. En este caso, la señal recibida $\boldsymbol{y}$ sería

$$y(t) = \begin{pmatrix} y(t) \\ y(t+\tau_1) \\ y(t+\tau_2) \end{pmatrix}$$

de acuerdo con la Figura 2-29. Según el ángulo de incisión de la onda (θ), el resto de las antenas del *array* recibirán la onda con un determinado período τ.

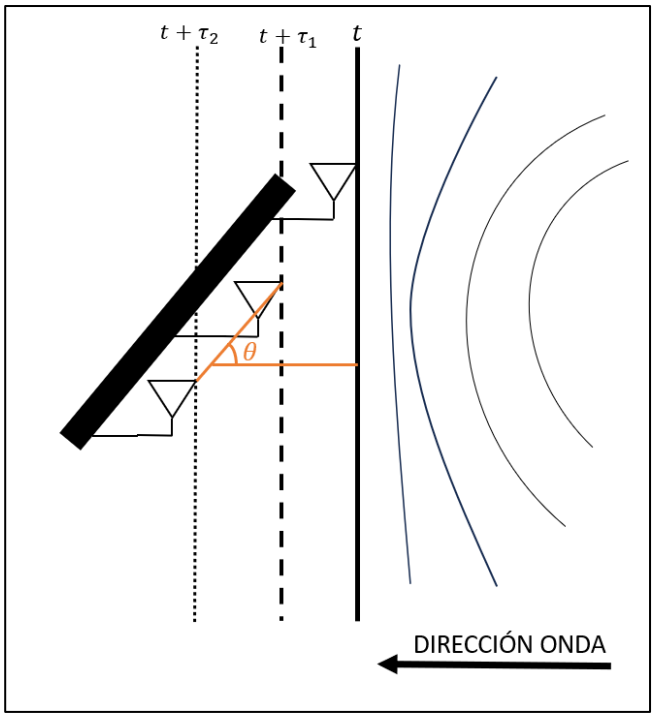


Figura 2-29: Recepción de frente de ondas plano con retardos [Elaboración propia].

La fase de la señal recibida $\boldsymbol{y}$ variará en cada recepción, y esta variación se nombra respecto a la antena principal, es decir, la antena con función $y(t)$. En el caso de la Figura 2-29, el cambio de fase es representado tal que

$$y(t)\begin{bmatrix} 1 \\ e^{-jW_c\tau_1} \\ e^{-jW_c\tau_2} \end{bmatrix}$$

y dicho vector es el vector canal recibido por un usuario, por lo que el vector canal contendrá tantas columnas como usuarios transmitan información al *array* de antenas.

El frente de ondas plano puede incidir de forma ortogonal, como se expresa en la Figura 2-30, pero en este caso la información que se recibirá será similar, obteniendo menos datos contrastables entre sí, es decir, la recepción de un frente de ondas perpendicular al eje de antenas de un *array* ofrece menor información tras ser procesada.

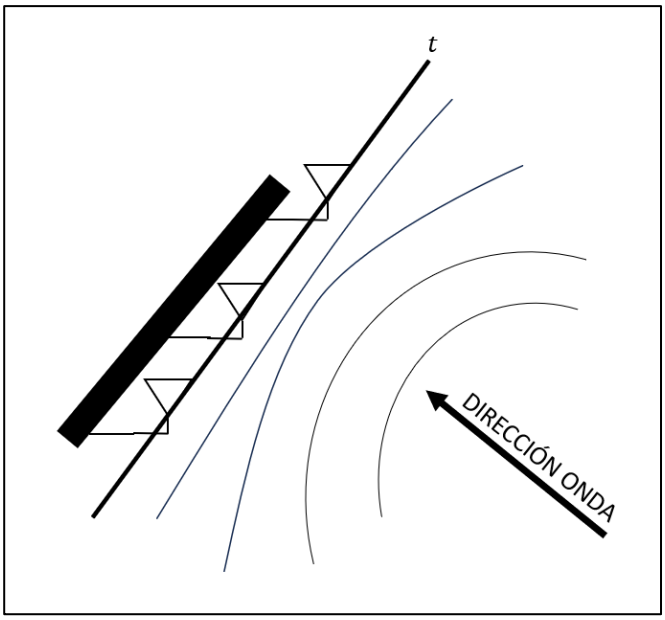


Figura 2-30: Recepción de frente de ondas plano perpendicular a eje de antenas [Elaboración propia].

2.4 *Precoding* en la transmisión MIMO

En los últimos años, el estudio sobre aplicar *precoding* en el transmisor (MUTP, *multiuser transmitter preprocessing*, procesamiento en el transmisor en multiusuario) ha incrementado notablemente, ya que se trata de técnicas de baja complejidad y gran eficiencia de potencia [27]. Las técnicas empleadas en este Proyecto son el *Zero-Forcing* o ZF, y el MRT (*Maximum Ratio Transmission*, Transmisión de tasa máxima).

2.4.1 Zero-Forcing

El *precoding* en el transmisor mediante *Zero-Forcing* es un método empleado para reducir interferencias por completo, y para ello emplea un algoritmo [28]. Cabe destacar que para un *precoder* ZF es necesario CSIT. El diseño de *precoding* de ZF tiene por objetivo principal mitigar la interferencia entre los símbolos transmitidos para mejorar la calidad de la señal recibida en el receptor.

De manera más práctica y de acuerdo con el presente Proyecto, el propósito de ZF consiste en realizar el producto de la matriz que contiene los canales de todos los usuarios por la matriz de *precoding* que contiene los *precoder* de dichos usuarios, y que dicho producto resulte en una matriz de identidad, identificando la diagonal principal como la señal deseada para cada usuario, y el resto de los elementos de la matriz como causantes de interferencia entre los usuarios. Por ejemplo, en un sistema de dos usuarios receptores y dos antenas transmisoras el *precoding* ZF sería como se muestra en la Ecuación 2-14. Para el caso de dos usuarios, el sistema contaría con $\boldsymbol{h_1}$ y $\boldsymbol{h_2}$, así como con *precoders* $\boldsymbol{p_1}$ y $\boldsymbol{p_2}$; y la condición del *precoding* ZF sería $\boldsymbol{h_1^H p_2 = 0}$ y $\boldsymbol{h_2^H p_1 = 0}$.

$$\begin{bmatrix} \boldsymbol{h_1^H} \\ \boldsymbol{h_2^H} \end{bmatrix} [\boldsymbol{p_1} \quad \boldsymbol{p_2}] = \begin{bmatrix} \boldsymbol{h_1^H p_1} & \boldsymbol{h_1^H p_2} \\ \boldsymbol{h_2^H p_1} & \boldsymbol{h_2^H p_2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \boldsymbol{I}$$

Ecuación 2-14

Tanto para este caso como para un caso con número arbitrario de usuarios y antenas transmisoras, se puede afirmar que $\boldsymbol{H^H P = I}$; y por tanto el *precoding* ZF resultaría $\boldsymbol{P = H(H^H H)^{-1}}$. Para modelar el *precoding*, se realiza la matriz pseudoinversa de H con el fin de poder realizar *precoding* con matrices no cuadradas, ya que la inversa de una matriz requiere que sea cuadrada y esto ofrece poca flexibilidad de parámetros, en cuanto a número de antenas transmisoras y usuarios se refiere.

2.4.2 Maximum Ratio Transmission

Un *precoding* MRT es una técnica empleada para múltiples antenas que pretende aumentar la tasa de transmisión de datos, y puede realizarse tanto en transmisión como en la recepción (MRC, *máximum ratio combining*, combinación de tasa máxima) de datos.

En [29] se demuestra que, para obtener la mejor tasa de transmisión de datos, el *precoder* debe ser programado en base a la matriz canal, es decir, teniendo CSIT el *precoder* más efectivo sería empleando los mismos elementos que contiene la matriz canal para maximizar el producto de matrices y obtener el efecto deseado; de tal forma que, conocida la matriz canal H, el *precoder* resultaría $\boldsymbol{P = H^*}$.

El empleo de MRT en sistemas multiusuario conlleva la desventaja de maximizar la señal deseada, pero ignorando la interferencia que dicha señal puede causar a otros usuarios, por lo que la efectividad plena de este *precoder* se daría en sistemas de comunicaciones MISO o MIMO punto a punto.

2.5 Seguridad en la Capa Física

2.5.1 Fundamentos

La Seguridad en la Capa Física se define como las transmisiones de capa física que garantizan una baja probabilidad de intercepción basada en las propiedades de transmisión, tales como modulación, señales y canales, sin recurrir al cifrado de la información, proporcionando un grado de confidencialidad [30].

La Seguridad en la Capa Física en un sistema de comunicaciones es medida por la capacidad secreta, que es la relación entre la capacidad en los canales legítimos y los canales ilegítimos [31]. En los canales ilegítimos los usuarios son comúnmente denominados “fisgones” o *eavesdroppers*. El valor de capacidad secreta debe ser positivo, y en caso de no conseguir capacidad secreta su valor es cero (*eavesdropper* recibe toda la información).

Los dos tipos de *precoding* normalmente empleados para obtener la máxima capacidad secreta posible son el ZF (*Zero-Forcing*, Cero-Forzado), también denominado *Channel Inversion* (Inversión de canal); y el RCI (*Regularized Channel Inversion*, Inversión de Canal Regularizada).

Hoy en día, la Seguridad en la Capa Física no tiene un empleo táctico para aumentar la confidencialidad, rapidez y fiabilidad en las unidades de Infantería de Marina. Dichas unidades requieren de equipos radio cifrados, es decir, se asume que el enemigo tiene la capacidad de interceptar información de las fuerzas propias, y se intenta que dicha intercepción sea en vano.

Si una situación requiere comunicación entre equipos radio con distinta cifra incluida de serie, sería imposible lograr dicha comunicación, y es en este ámbito en el que la Seguridad en la Capa Física cobra importancia. Cabe destacar que no es necesario acudir a un escenario extremo en el que no exista cifrado, sino que una combinación de ambas técnicas de seguridad (cifrado de información y Seguridad en la Capa Física) puede resultar tremendamente eficaz.

2.5.2 Ejemplo de escenario de operación militar

En la Figura 2-31 se muestra un ejemplo de una situación en la que dos unidades aliadas necesitan comunicarse, y dicha comunicación es interceptada por el enemigo.

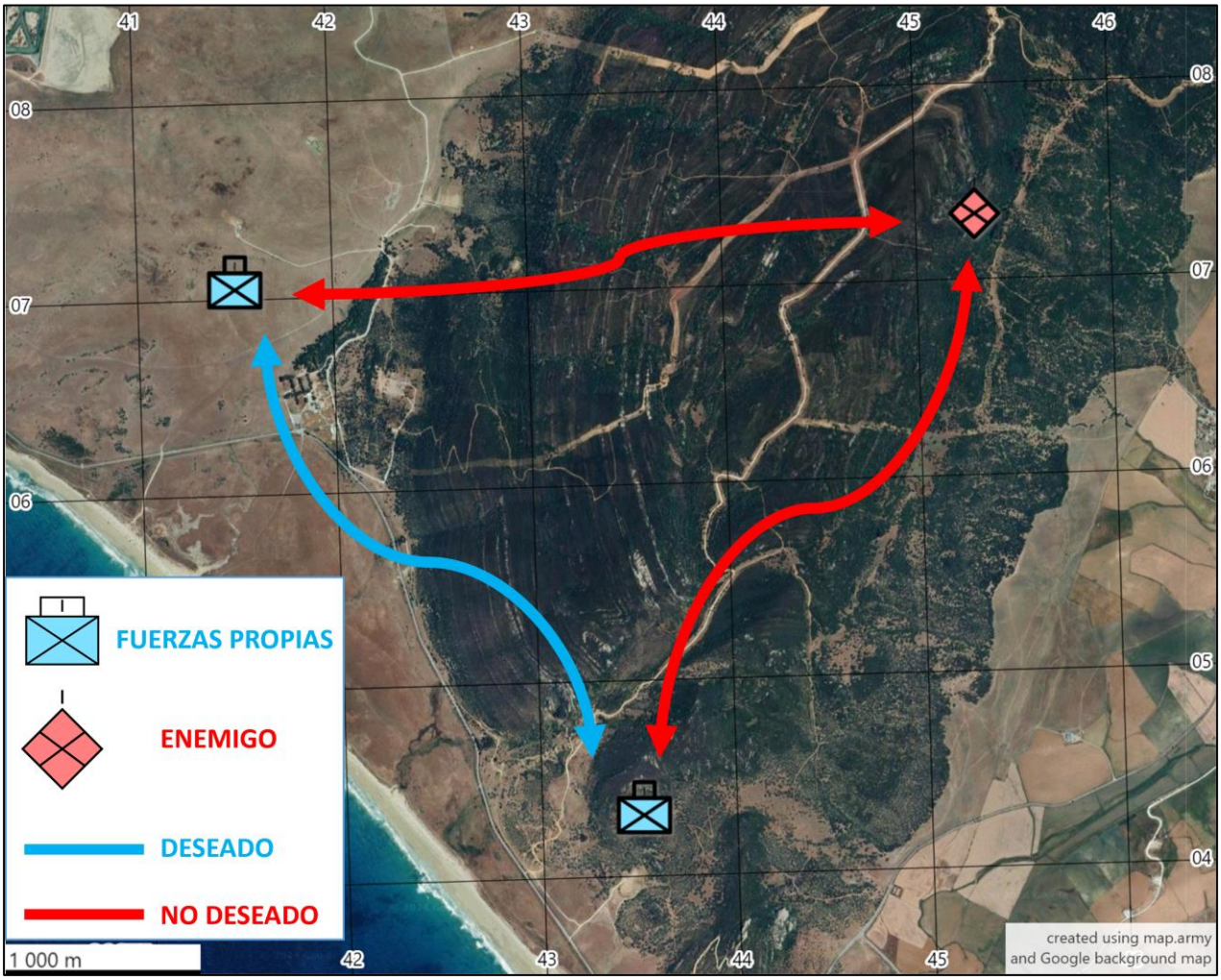


Figura 2-31: Situación táctica en la que el enemigo intercepta comunicaciones aliadas [Elaboración propia].

Para solucionar dicha situación implementando medidas de Seguridad en la Capa Física, las unidades aliadas son capaces de anular direcciones de propagación con el propósito de evitar intercepciones, como se muestra en la Figura 2-32. De esta manera, las unidades aliadas son capaces de comunicarse a nivel físico, obviando cualquier medida de seguridad que se encuentre en distintas capas, como puede ser el cifrado de información.

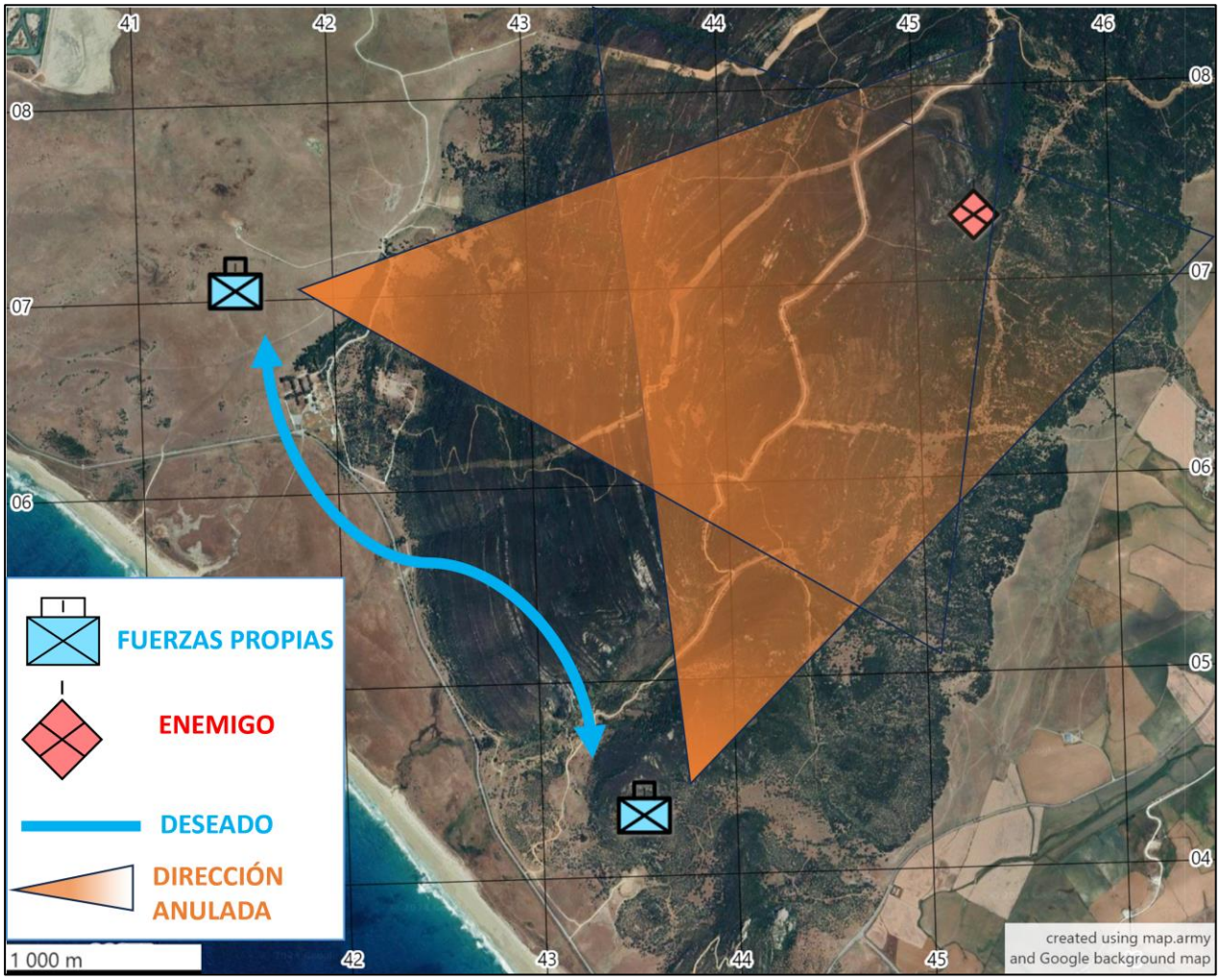


Figura 2-32: Fuerzas aliadas anulan su transmisión en la dirección del enemigo, evitando intercepción [Elaboración propia].

2.5.3 Capacidad secreta en MISO

Según el número de *eavesdroppers* que se encuentren en el sistema, los sistemas MISO pueden clasificarse como MISOSE (*Multiple-Input Multiple-Output Single-Eavesdropper*, Entrada Múltiple Salida Múltiple de un "Fisgón") o MISOME (*Multiple Input Multiple Output Multiple Eavesdroppers*, Entrada Múltiple Salida Múltiple "Fisgones" Múltiples).

El modelo de sistema MISO en el que intervienen uno o varios *eavesdroppers* es representado en la Figura 2-33, en la que existen U usuarios (RX) y S *eavesdroppers* (E), y se representa la comunicación por parte de la estación base (TX) tanto con los usuarios deseados como con los usuarios no deseados.

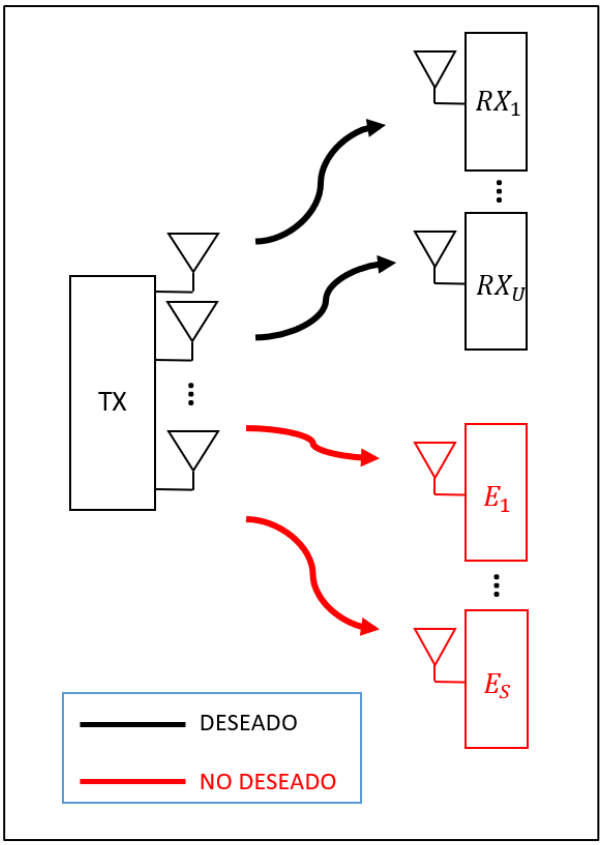


Figura 2-33: Sistema MISO con U usuarios (RX) y N *eavesdroppers* (E) [Elaboración propia].

En un sistema de comunicaciones que no está preparado para actuar contra *eavesdroppers*, es decir, que no cuenta con medidas de protección de Seguridad en la Capa Física; los usuarios ilegítimos tienen la capacidad de interceptar parte de la señal destinada a otro usuario. El valor de dicha señal es determinado por la LINR (*Leakage to interference plus noise ratio*, Relación Intercepción-Interferencia-Ruido) [32], de tal forma que un S-ésimo usuario ilegítimo que trata de interceptar la señal de un usuario U cuenta con la LINR mostrada en la Ecuación 2-15.

$$LINR_{E_S} = \frac{|\boldsymbol{h}_{\boldsymbol{E_S}}^{\boldsymbol{H}} \boldsymbol{p}_{\boldsymbol{U}}|^2}{\sigma_{n_{E_S}}^2}$$

Ecuación 2-15

.

El objetivo de las medidas de Seguridad en la Capa Física es incrementar la capacidad secreta. La manera de conseguirlo es directamente reduciendo lo máximo posible el valor del producto $\boldsymbol{h}_{\boldsymbol{S}}^{\boldsymbol{H}} \boldsymbol{p}_{\boldsymbol{U}}$, mediante el conocimiento del canal del *eavesdropper* (sería útil conocer la dirección angular en la que se encuentra dicho usuario) y el *precoder* adaptado a dicho fin.

El empleo de sistemas MISO permite alterar el valor de LINR mediante la direccionalidad de antenas, así como la diversidad. Sin dichos sistemas sería imposible anular o reducir la LINR y a la vez mantener la SINR necesaria para el usuario legítimo. Cuanto mayor sea el número de elementos transmisores (o receptores), mayor direccionalidad podrá tener la transmisión, y mayores nulos se podrán generar con el propósito de estos ángulos "muertos" (nulos) y dirigirlos hacia el *eavesdropper*, reduciendo así su LINR.

De hecho, al aumentar el número de antenas, la separación angular entre usuario legítimo y *eavesdropper* puede ser menor garantizando un ángulo "muerto" o nulo para el *eavesdropper* y un ángulo con suficiente ganancia para el usuario legítimo, como se puede apreciar en la Figura 2-34, con ejemplos para 4, 8 y 16 antenas transmisoras.

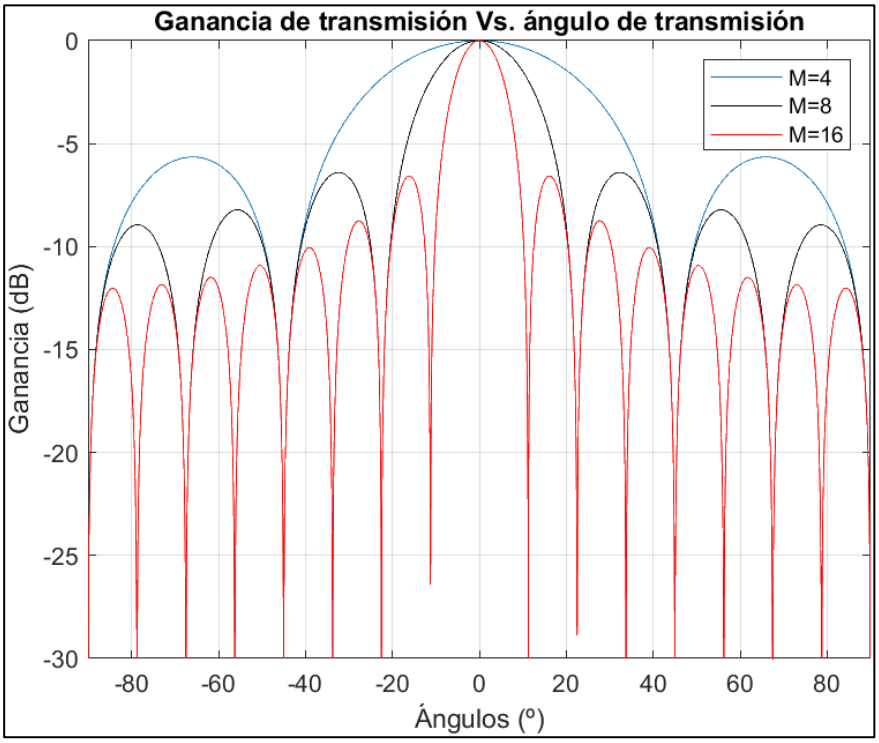


Figura 2-34: Ganancia de transmisión según ángulo de transmisión para M antenas [Elaboración propia].

Por lo tanto, la capacidad secreta de un U-ésimo usuario u_U será tal y como se muestra en la Ecuación 2-16, y dependerá tanto de la señal que obtenga de la transmisión por parte de la BS ($SINR_{u_U}$ de la Ecuación 2-12) como de la intercepción por parte de un *eavesdropper* (Ecuación 2-15, para un solo *eavesdropper* E_1).

$$C_{S,u_U} = log_2\left(\frac{1 + SINR_{u_U}}{1 + LINR_{E_1}}\right)$$

Ecuación 2-16

La capacidad secreta de un sistema equivaldría a la suma de las capacidades secretas de todos los usuarios del sistema, como se muestra en la Ecuación 2-17.

$$C_{S,total} = \sum_{i=1}^{U} C_{S,u_i}$$

Ecuación 2-17

La capacidad secreta es un factor complicado de mejorar, puesto que para poder centrar los esfuerzos en evitar la intercepción de información por parte de *eavesdropper*, es necesario haber conseguido cierta eficacia en el canal de comunicaciones; y a medida que el número de usuarios ilegítimos aumenta, más difícil será conseguir valores eficientes de capacidad secreta, ya que la adaptación del *precoder* deberá ser más exigente [33].

3 DESARROLLO DEL TFG

3.1 Simulaciones en *Software*

Las simulaciones en el s*oftware Matlab* se han realizado con dos tipos de *precoding*: *Zero-forcing* y *Maximum Ratio Transmission,* empleados de forma separada.

3.1.1 Funciones auxiliares empleadas en el código

Las simulaciones que se realizarán en *Matlab* tienen diferentes parámetros establecidos mediante funciones que complementan al código principal.

- *MISOchannel*

La función *MISOchannel* (Anexo IV) es la función que genera matrices canal (*MISO_H*) según el número de antenas transmisoras y número de usuarios.

Esta función "recoge" dos parámetros del código principal: número de antenas transmisoras *M* y ángulo de incisión del frente de onda *theta*. *MISOchannel* pretende generar canales determinando inicialmente un vector simétrico ***m*** que simula la posición de las antenas en el *array*. Posteriormente, genera un vector ***a*** en el que ya se incluye el desfase y atenuación que afecta a cada antena con posición ***m***. Dicho vector ***a*** es "devuelto" al código principal como *MISO_P*.

- *SINR_DL*

La función *SINR_DL* (Anexo V) es la función que calcula la SINR para cada usuario. Los valores de entrada para esta función son las matrices de canal y *precoding* (*MISO_H* y *MISO_P* respectivamente), y el ruido, que es expresado como $\frac{1}{\boldsymbol{SNR}(i)}$ con $\boldsymbol{i} = [1,2,\dots,25]$, es decir, que cada simulación de capacidad se realiza con mejores condiciones de SNR.

SINR_DL calcula un valor escalar de interferencia utilizando bucles para así tener en cuenta a todos los usuarios, salvo el que pretende recibir la señal (no causa interferencia a sí mismo). El cálculo de la SINR para cada usuario consiste en el producto por columnas de *MISO_P* y *MISO_H*, y su división entre el valor de interferencia sumada al ruido. Como resultado se obtiene un vector que ofrece el valor de SINR para cada usuario.

- *ZFprecoder*

La función *ZFprecoder* (Anexo VI) es la función que calcula la matriz de *precoding MISO_P*, en caso de utilizar el método de *precoding Zero-Forcing*, a partir de la matriz canal *MISO_H* ya calculada anteriormente. Cabe destacar que, en el código principal, el empleo del *precoder* MRT no está incluido en ninguna función, sino en el propio código.

ZFprecoder calcula una matriz (***A***) que consiste en el producto de la matriz canal por la matriz de correlación inversa del canal, que es una matriz cuadrada simétrica cuya función (sin invertir) es proporcionar información sobre el estado del canal (CSI, CSIT en este caso) para así poder emplear un *precoding* adecuado y eficiente. A la matriz de correlación se le suma un valor mínimo (1^{-10}) a la diagonal principal ya que el producto de matrices puede no ser invertible, factor que evitaría el funcionamiento del *precoder*, por lo que es necesario realizar una regularización, es decir, dar un valor mínimo.

El empleo de *ZFprecoder* implica sacrificar parte de la ganancia en SNR del sistema, ya que la cancelación de interferencia limita dicha ganancia, algo que no ocurre en el *precoder* con el modelo MRT

Por último, las filas de ***A*** *s*on normalizadas dividiéndolas por la raíz cuadrada de la diagonal de ***A***, obteniendo así la matriz de *precoding.*

3.1.2 Código principal

El código principal sobre el que se realizarán diferentes simulaciones mediante el empleo del *software Matlab* se encuentra disponible en el Anexo III. Dicho código define variables, entre las cuales se encuentran el número de antenas transmisoras (*A*) y el número de usuarios en el canal inalámbrico (*U*), y ambos parámetros son modificables para así realizar simulaciones en diferentes escenarios que permitan afianzar conclusiones y resultados efectivos.

Inicialmente, se definen el número de experimentos que se realizarán (y se promediarán posteriormente), el vector creciente ***SNR*** de valores logarítmicos para definir la SNR, el vector ***nusers***, y se inicializan las matrices de canal, *precoding* y capacidad tanto por usuario como la suma de todas.

El vector ***SNR*** de 26 elementos es empleado de manera que el factor que difiere los elementos sea la potencia del ruido, y la potencia de transmisión se considera invariable, de valor unitario e independiente del número de antenas transmisoras.

Cada experimento se realizará con un ángulo de incisión de frente de onda *theta* generado aleatoriamente, y comienza con la generación de canales (*MISO_H*) por parte de la función *MISOchannel.*

Una vez generados los canales, el código contiene dos ramas de acción: una de ellas consiste en general la matriz de *precoding* de igual manera que se generó la matriz canal, por lo que no se intenta cancelar ninguna interferencia; y la otra consiste en emplear la función *ZFprecoder* con el propósito de cancelar la interferencia que pueden causar los usuarios entre sí. Para aplicar el *precoder* MRT es necesario descomentar la línea 26, mientras que para aplicar el *ZFprecoder* se debe descomentar la línea 29. No se pueden aplicar ambos *precoder* en la misma simulación.

Una vez se han obtenido las matrices de canal y *precoding*, se procede al cálculo de la SINR que afectará a cada usuario, mediante la función *SINR_DL*, y posteriormente se calcula la capacidad para cada usuario mediante la fórmula de capacidad mostrada en la Ecuación 2-12.

El proceso explicado hasta este momento se repetirá en tantas ocasiones como se haya establecido en la variable *nexperiments*. Una vez realizados todos los experimentos, se promediarán los resultados para cada usuario (la matriz ***C_MISO*** tiene dimensión $nexperiments\ x\ U$) y se sumarán para obtener

la capacidad total del sistema (***C_SUMA_MISO***). Este proceso se realizará para cada valor establecido en el vector ***SNR***, es decir, 26 veces.

Por último, el resultado ***C_SUMA_MISO*** es representado en una gráfica en la que el eje de abscisas contiene los valores de SNR en dB (de 0 a 25 dB), y el eje de ordenadas representa la capacidad sumada expresada en bps/Hz.

3.1.3 Simulaciones y resultados

A continuación, se analizarán distintos escenarios alternando parámetros, así como diferentes *precoder* para realizar una comparación de escenarios. El primer apartado contiene los análisis de cuatro escenarios diferentes en los que se empleará el *precoder* MRT, mientras que el segundo realizará lo mismo, pero con el *precoder* ZF.

- *Escenarios con precoder MRT*

Los parámetros establecidos para la primera simulación son los siguientes:

```
A=5; %ANTENAS TRANSMISORAS --> MODIFICABLE

U=5; %NÚMERO DE USUARIOS --> MODIFICABLE

nexperiments = 10000; %NÚMERO DE EXPERIMENTOS PARA PROMEDIAR
```

En la Figura 3-1 se representan los valores de Capacidad Suma Vs. SNR en dB obtenidos en la simulación del primer escenario.

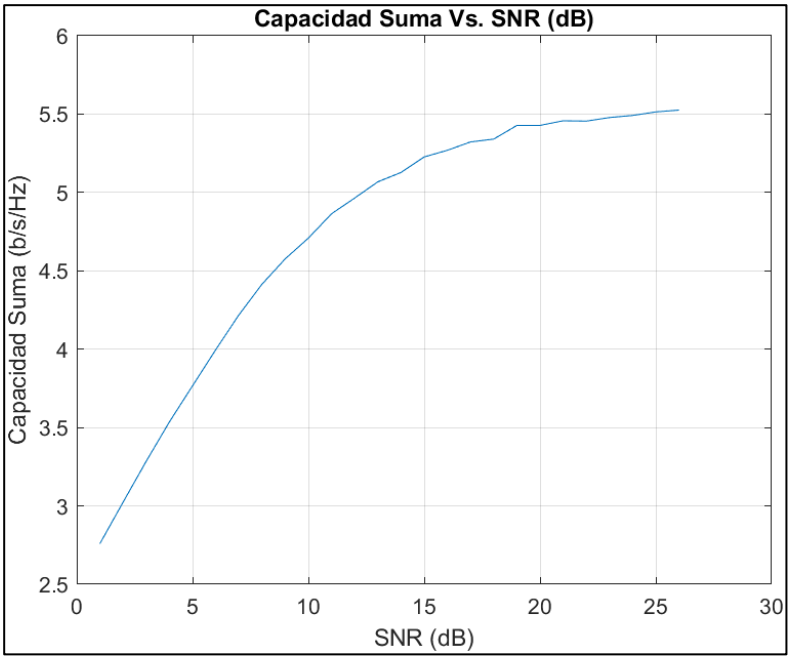


Figura 3-1: Capacidad Suma Vs. SNR; A=5 y U=5 [Elaboración propia].

El primer escenario será objeto de comparación para el resto de los escenarios, de modo que la variación de parámetros determinará un mejor o peor sistema en cada escenario según los parámetros que se hayan establecido para cada escenario previamente.

El segundo escenario para analizar contendrá los siguientes parámetros:

```
 A=8; %ANTENAS TRANSMISORAS --> MODIFICABLE
U=5; %NÚMERO DE USUARIOS --> MODIFICABLE
nexperiments = 10000; %NÚMERO DE EXPERIMENTOS PARA PROMEDIAR
```

En la Figura 3-2 se representan los valores de Capacidad Suma Vs. SNR en dB obtenidos en la simulación del segundo escenario.

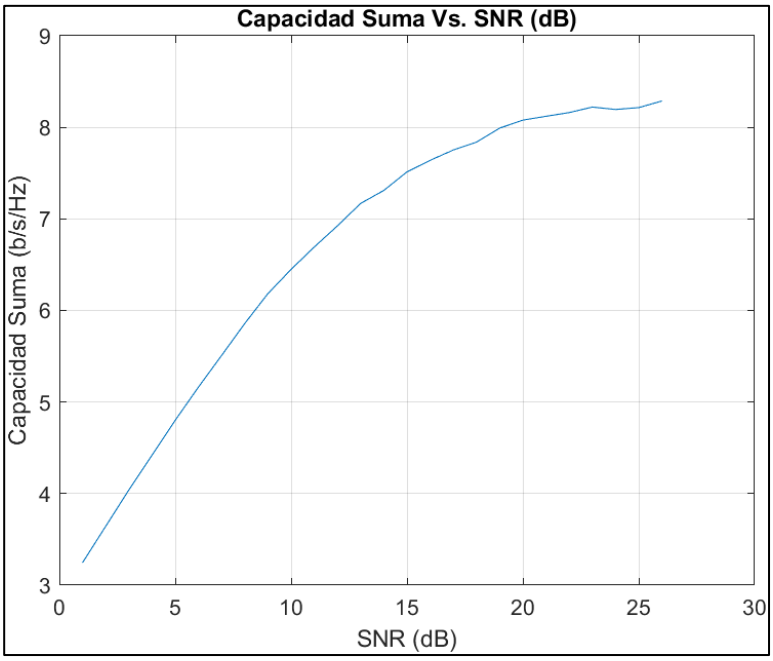


Figura 3-2: Capacidad Suma Vs. SNR; A=8 y U=5 [Elaboración propia].

Como se puede comprobar, al aumentar el número de antenas transmisoras la Capacidad Suma aumenta considerablemente. El resultado respalda el estudio realizado en el Apartado 2.2.5 y lo que ocurre matemáticamente al aumentar el número de antenas transmisoras, es realizar productos de matrices canal y *precoding* de mayor dimensión. Concretamente, al aumentar el número de antenas transmisoras aumentarán las filas tanto en MISO_H como en MISO_P; y también el número de columnas de ***C_MISO***, por lo que finalmente en ***C_MISO_SUMA*** se sumarán 8 valores en vez de 5 (Figura 3-1).

En la Figura 3-2 también es apreciable que, al aumentar el número de antenas, éstas pueden aumentar su capacidad de direccionalidad, es decir, se podrán precodificar de modo que cada usuario reciba menor interferencia por parte del resto de usuarios.

El tercer escenario para analizar contendrá los siguientes parámetros:

```
A=5; %ANTENAS TRANSMISORAS --> MODIFICABLE

U=8; %NÚMERO DE USUARIOS --> MODIFICABLE

nexperiments = 10000; %NÚMERO DE EXPERIMENTOS PARA PROMEDIAR
```

En la Figura 3-3 se representan los valores de Capacidad Suma Vs. SNR en dB obtenidos en la simulación del tercer escenario.

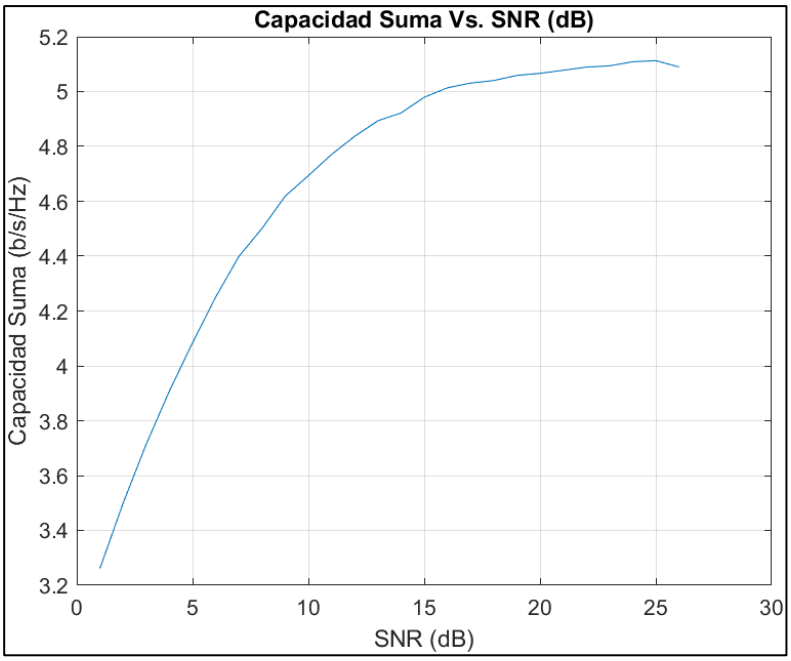


Figura 3-3: Capacidad Suma Vs. SNR; A=5 y U=8 [Elaboración propia].

En este caso (Figura 3-3), se ha aumentado el número de usuarios receptores en el sistema. Este factor implica que la interferencia que se causará entre usuarios será mayor, es decir, un usuario recibirá interferencia procedente de siete usuarios, respecto a los cuatro usuarios que interfieren en el primer escenario.

Es por ello por lo que la Capacidad Suma es menor que en el primer escenario, ya que matemáticamente el valor que recoge la suma de interferencias (x) en la función *SINR_DL* es mayor que en el primer escenario puesto que el bucle de la función se repite $U - 1$ veces. Por lo tanto, si el valor de x aumenta, la SINR será generalmente menor para cada usuario, repercutiendo directamente en el posterior cálculo de la capacidad.

Los parámetros del cuarto escenario para analizar son los siguientes:

```
A=8; %ANTENAS TRANSMISORAS --> MODIFICABLE

U=8; %NÚMERO DE USUARIOS --> MODIFICABLE

nexperiments = 10000; %NÚMERO DE EXPERIMENTOS PARA PROMEDIAR
```

En la Figura 3-4 se representan los valores de Capacidad Suma Vs. SNR en dB obtenidos en la simulación del cuarto escenario.

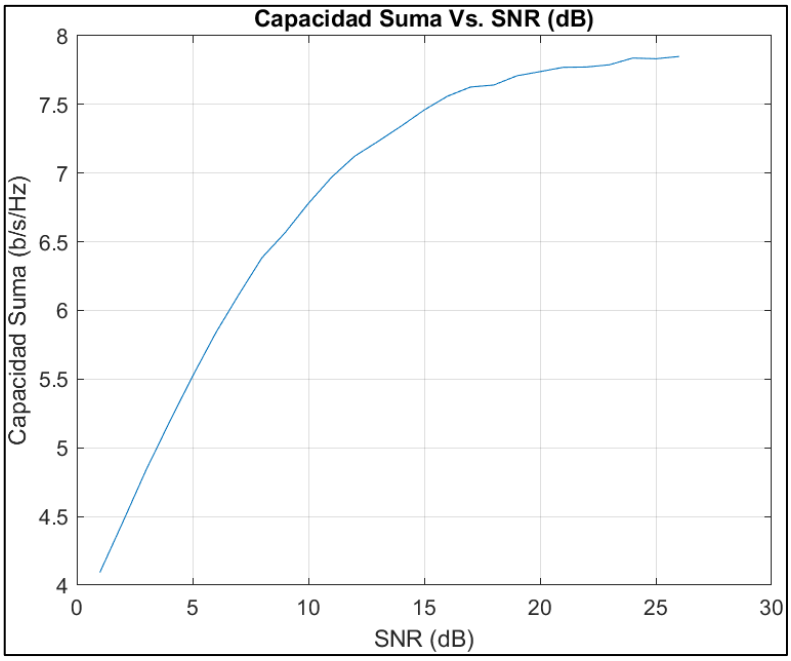


Figura 3-4: Capacidad Suma Vs. SNR; A=8 y U=8 [Elaboración propia].

La simulación del cuarto escenario se realiza con mismo número de antenas transmisoras y usuarios receptores, al igual que el primer escenario. La diferencia se encuentra en que dicho número es mayor. Los resultados obtenidos (Figura 3-4) demuestran que, a pesar de recibir mayor interferencia, es eficiente aumentar tanto las antenas transmisoras como el número de usuarios, es decir, en la transmisión tiene mayor "peso" la cantidad de antenas que se empleen que la interferencia que cause un número elevado de usuarios receptores.

Como se puede comprobar, las simulaciones de los cuatro escenarios comparten la característica de que a medida que aumenta la SNR, la Capacidad Suma disminuye su pendiente, hasta que en los valores finales de ***SNR*** la Capacidad Suma varía escasamente. Este suceso se debe a que los elementos del vector ***SNR*** aumentan logarítmicamente, es decir, la diferencia entre valores consecutivos aumenta a lo largo del vector. Como el vector ***SNR*** es empleado como divisor en la función *SINR_DL*, provoca el efecto contrario en la SINR: los valores de sus elementos serán más similares a medida que el vector es calculado. Finalmente, la SINR es el principal actor en el cálculo de la capacidad, por lo que afecta directamente al resultado de la Capacidad Suma.

- *Escenarios con precoder ZF*

En este Apartado se simularán los mismos (cuatro) escenarios que en el Apartado anterior, pero realizando el *precoding* con el modelo ZF, realizado por la función auxiliar *ZFprecoder*.

Los parámetros establecidos para la primera simulación son los siguientes:

```
A=5; %ANTENAS TRANSMISORAS --> MODIFICABLE

U=5; %NÚMERO DE USUARIOS --> MODIFICABLE

nexperiments = 10000; %NÚMERO DE EXPERIMENTOS PARA PROMEDIAR
```

En la Figura 3-5 se representan los valores de Capacidad Suma Vs. SNR en dB obtenidos en la simulación del primer escenario, tanto para el empleo de MRT como de ZF.

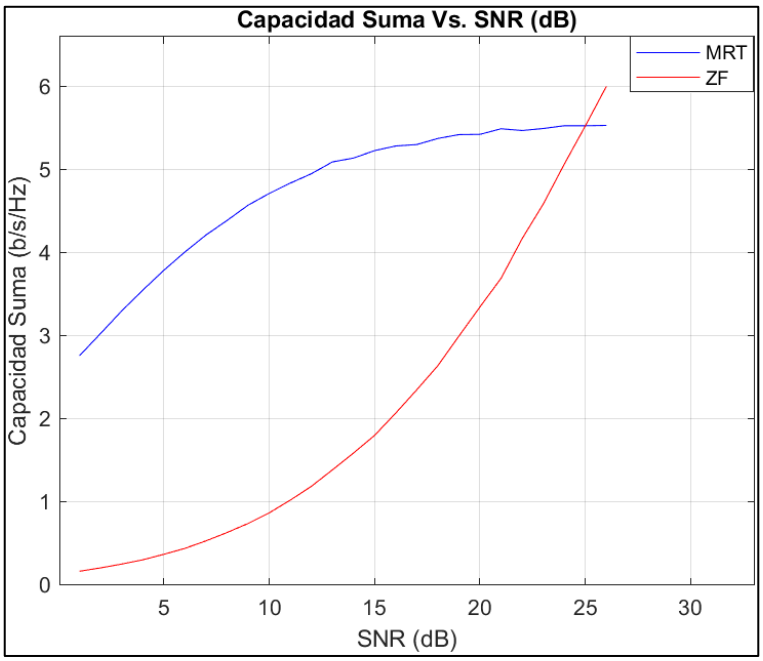


Figura 3-5: Capacidad Suma Vs. SNR; A=5 y U=5 [Elaboración propia].

Como en las simulaciones anteriores, la simulación del primer escenario empleando ZF servirá de referencia a la hora de analizar distintas características. En comparación con el empleo de MRT, el *precoder* ZF (Figura 3-5) influye directamente en la Capacidad Suma, siendo esta última mucho más dependiente del valor de SNR que en el empleo de MRT.

A partir de 25 dB de SNR la Capacidad Suma es mayor en ZF, y es debido a que la pendiente de ZF es mucho mayor que en MRT, por lo que el empleo recomendable de ZF es en escenarios con valores de SNR más altos.

El segundo escenario para analizar contendrá los siguientes parámetros:

```
 A=8; %ANTENAS TRANSMISORAS --> MODIFICABLE

U=5; %NÚMERO DE USUARIOS --> MODIFICABLE

nexperiments = 10000; %NÚMERO DE EXPERIMENTOS PARA PROMEDIAR
```

En la Figura 3-6 se representan los valores de Capacidad Suma Vs. SNR en dB obtenidos en la simulación del primer escenario, tanto para el empleo de MRT como de ZF.

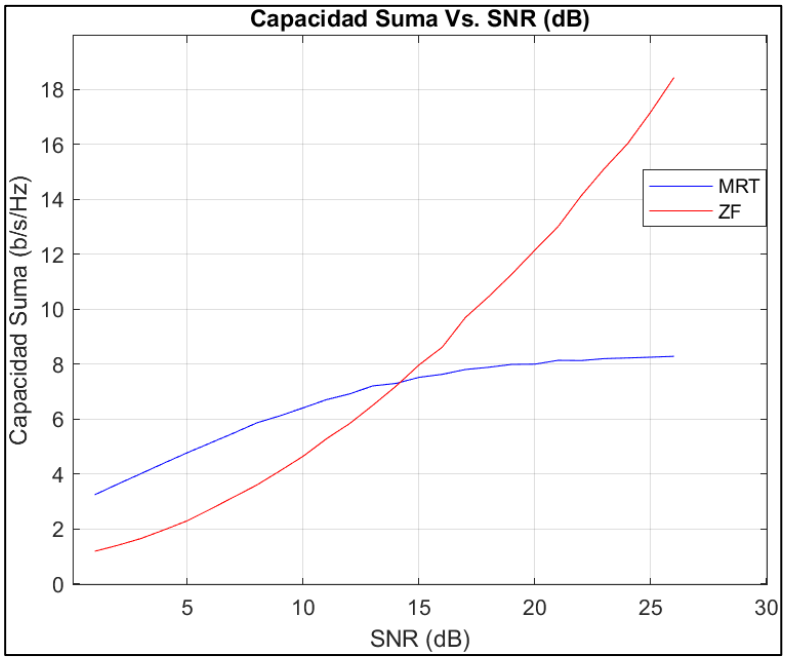


Figura 3-6: Capacidad Suma Vs. SNR; A=8 y U=5 [Elaboración propia].

El resultado de la segunda simulación (Figura 3-6) es claramente superior al equivalente empleando *precoder* MRT. Este factor indica que el utilizar un mayor número de antenas que de usuarios en el sistema es muy beneficioso para el empleo de ZF.

Además, la Capacidad Suma obtenida en la segunda simulación es muy superior a la obtenida en la primera simulación (Figura 3-5), por lo que empleando ZF se respalda la idea de mantener mayor número de antenas transmisoras que de usuarios en el sistema. La capacidad se triplica empleando ZF, mientras que en el empleo de MRT la diferencia es claramente menor. Por ejemplo, a 25 dB de SNR si se emplea MRT la diferencia de Capacidad Suma entre los dos primeros escenarios es de aproximadamente 3 bps/Hz. Sin embargo, empleando ZF dicha diferencia aumenta hasta 12 bps/Hz, aproximadamente.

En conclusión, para un sistema en el que el número de antenas es mayor que el número de usuarios, el empleo de un *precoder* ZF maximizará la capacidad del sistema.

El tercer escenario para analizar contendrá los siguientes parámetros:

```
A=5; %ANTENAS TRANSMISORAS --> MODIFICABLE

U=8; %NÚMERO DE USUARIOS --> MODIFICABLE

nexperiments = 10000; %NÚMERO DE EXPERIMENTOS PARA PROMEDIAR
```

En la Figura 3-7 se representan los valores de Capacidad Suma Vs. SNR en dB obtenidos en la simulación del primer escenario, tanto para el empleo de MRT como de ZF.

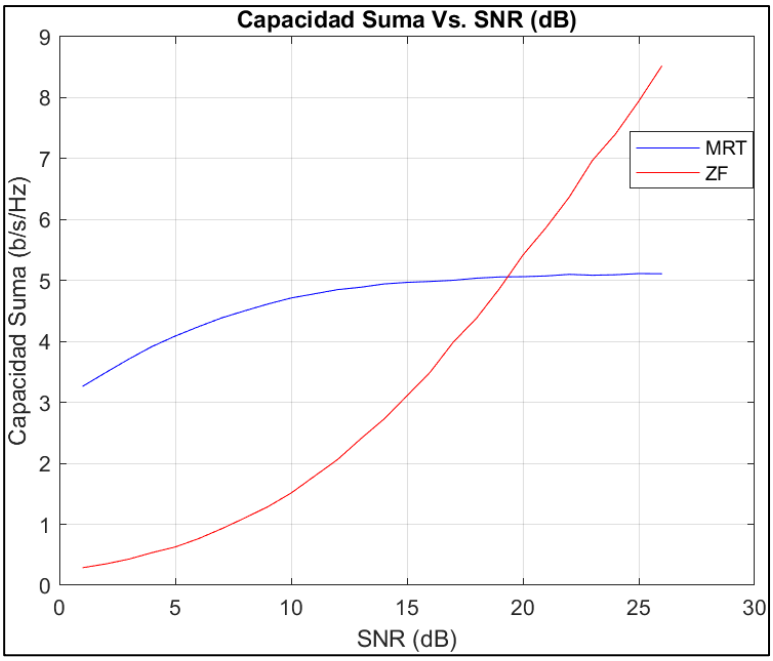


Figura 3-7: Capacidad Suma Vs. SNR; A=5 y U=8 [Elaboración propia].

El resultado de la tercera simulación (Figura 3-7) también beneficia al sistema. En este caso, la interferencia que debería afectar a cada usuario es mayor, ya que en el primer escenario un usuario es interferido por otros cuatro, mientras que en este caso es interferido por siete. Sin embargo, en la tercera simulación se aprecia mayor capacidad que en la primera (Figura 3-5). Esto se debe a que el empleo de ZF consigue evitar las interferencias entre usuarios, y a pesar de sacrificar parte de señal deseada, el resultado mejora la Capacidad Suma respecto al primer escenario (Figura 3-5).

En comparación con el empleo de MRT, el resultado de la tercera simulación con ZF es claramente superior, puesto que con MRT la Capacidad Suma disminuyó levemente, concluyendo en que para sistemas con mayor número de usuarios que de antenas transmisoras, es más eficiente el empleo de *precoder* ZF en vez de *precoder* MRT.

Los parámetros del cuarto escenario para analizar son los siguientes:

```
A=8; %ANTENAS TRANSMISORAS --> MODIFICABLE

U=8; %NÚMERO DE USUARIOS --> MODIFICABLE

nexperiments = 10000; %NÚMERO DE EXPERIMENTOS PARA PROMEDIAR
```

En la Figura 3-8 se representan los valores de Capacidad Suma Vs. SNR en dB obtenidos en la simulación del primer escenario, tanto para el empleo de MRT como de ZF.

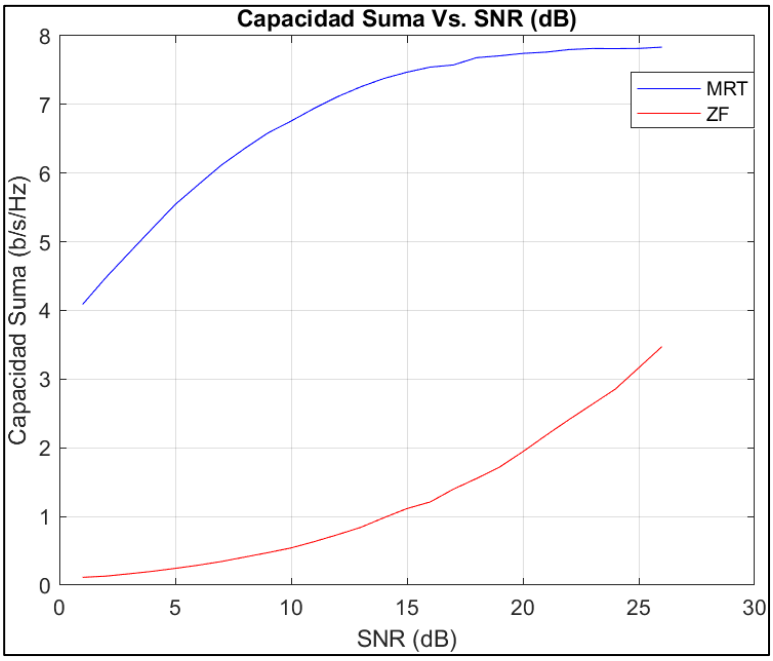


Figura 3-8: Capacidad Suma Vs. SNR; A=8 y U=8 [Elaboración propia].

El resultado de la cuarta simulación (Figura 3-8) demuestra que el empleo de ZF no siempre es más beneficioso para el sistema. En este caso, el *precoder* ha sacrificado excesiva señal deseada intentando reducir la interferencia. El resultado obtenido es el más bajo de todas las simulaciones, y es indicio de que el *precoder* no es capaz de cubrir todas las situaciones posibles en las que se puede crear un sistema de comunicaciones.

Existen factores que pueden alterar la capacidad de este *precoder*, como son la colocación espacial de los usuarios receptores, los distintos ángulos de incisión del frente de ondas… y el caso $A = U$ es un caso específico en el que ZF no se consigue adaptar al sistema, por lo que, concluyendo, el empleo de MRT es más recomendable para situaciones en las que el número de usuarios es el mismo que de antenas transmisoras.

De forma alternativa, otra posible solución es recurrir a técnicas como FDMA o TDMA en un subconjunto de determinados usuarios, para emplear el *precoder* ZF en un escenario en el que de nuevo se cuenten con más antenas que usuarios, y maximizar la Capacidad Suma del sistema.

Como se puede observar en las simulaciones de los cuatro escenarios empleando ZF, la pendiente de las gráficas aumenta a medida que aumenta la SNR, al contrario que en los escenarios en los que se

emplea MRT. Esto se debe a que empleando MRT la interferencia causada por los usuarios se sumaba a la componente del vector ***SNR*** que le correspondía, y de esa manera disminuía la SINR generalmente; es decir, el valor del sumatorio de interferencias (variable *x*) en *SINR_DL* aumentaba considerablemente. En ZF se evita dicha interferencia, y el único factor que influye en cada componente de ***SINR*** es el ruido, mientras que la señal deseada sí es multiplicada. En otras palabras, el valor de la variable *x* aumenta poco porque sólo se ve influido por el vector ***SNR,*** mientras que la señal deseada sí aumenta considerablemente. De esta manera aumenta la SINR, con mayor facilidad a medida que aumenta la SNR.

3.2 Experimentos reales

Tras comprobar diferentes valores teóricos en las simulaciones realizadas en el *software Matlab*, a continuación, se presentarán los distintos escenarios propuestos sobre los que se experimentará, así como los diferentes equipos empleados para realizar dichos experimentos.

3.2.1 Medios empleados

Los medios que se han empleado en la realización de los experimentos prácticos son los siguientes: *array* de antenas del laboratorio del CUD, USRP X310, ADALM-PLUTO, HACK RF, y los *softwares Matlab* y *GNU Radio*. En la Figura 3-9, Figura 3-10 y Figura 3-11 se muestran imágenes de los dispositivos.

a) **b)**

Figura 3-9: a) *array* de cuatro antenas [Elaboración propia], y b) USRP X310 [Elaboración propia].

El *array* de cuatro antenas será la BS, actuará recibiendo datos de los distintos usuarios y dichos datos serán procesados por el USRP X310. Ambos dispositivos se muestran en la Figura 3-9.

a) **b)**

Figura 3-10: a) montaje de ADALM-PLUTO y antena [Elaboración propia], y b) ADALM-PLUTO [34].

El *software* empleado para programar los dispositivos ADALM-PLUTO (Figura 3-10) y HACK RF (Figura 3-11) es *GNU Radio*, de forma que transmitirán señales que serán recibidas por la BS.

a) **b)**

Figura 3-11: a) dispositivo HACK RF [35] y b) antena conectada a HACK RF [Elaboración propia]

3.2.2 Contextualización

En el presente Proyecto se emplearán dos tipos de escenarios: el primero constará de un usuario transmisor y dos usuarios receptores (Figura 3-12), de los cuales uno de ellos será ilegítimo; y el segundo se diferenciará en que habrá tres usuarios receptores, de los cuales uno será ilegítimo (Figura 3-13).

Como se puede observar, los experimentos reales han sido llevados a cabo en las inmediaciones de la pista militar de la Escuela Naval Militar y el laboratorio de investigación del CUD (coordenadas en MGRS: 29T NG 24104 93939).

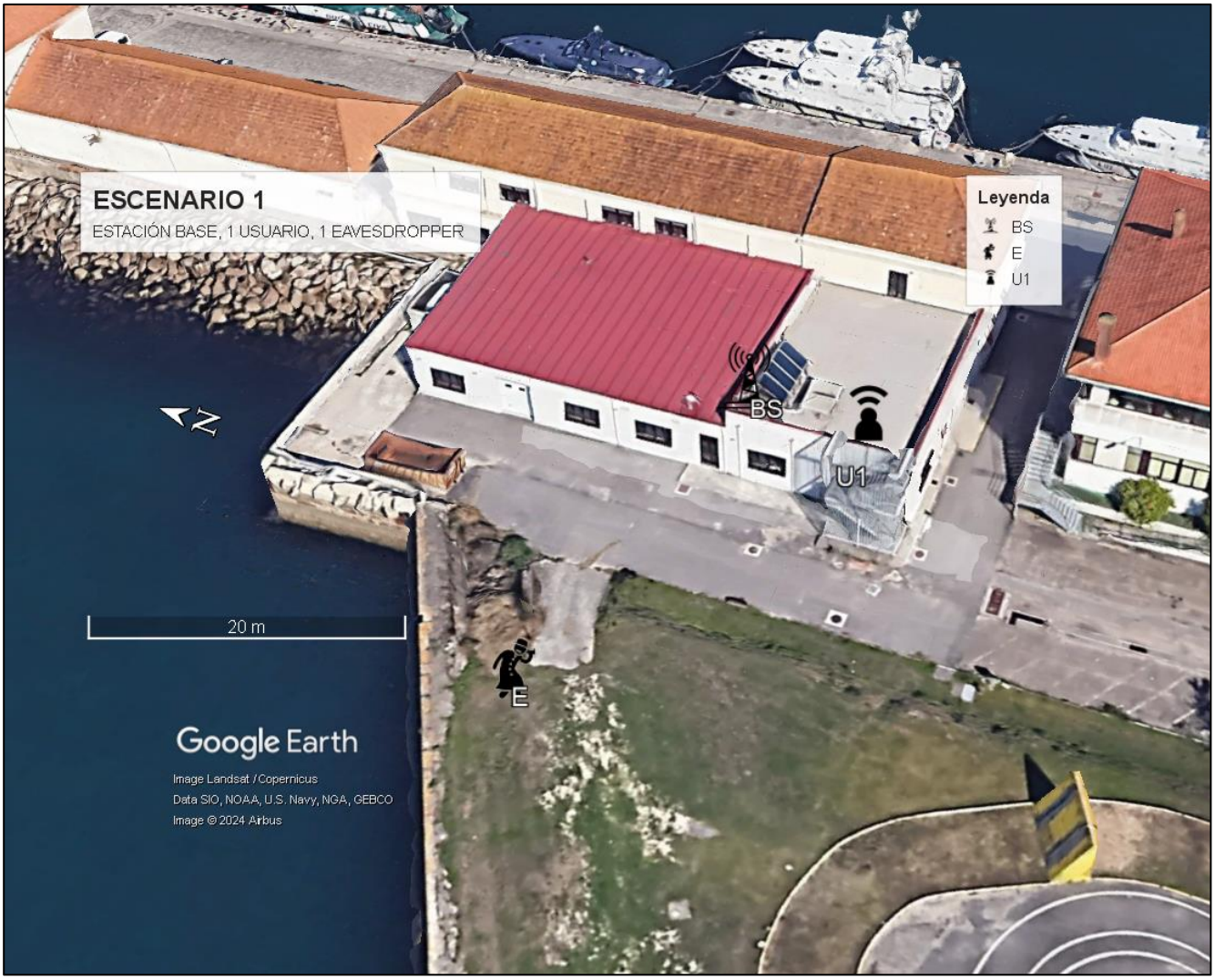


Figura 3-12: Representación gráfica del primer escenario [Elaboración propia].

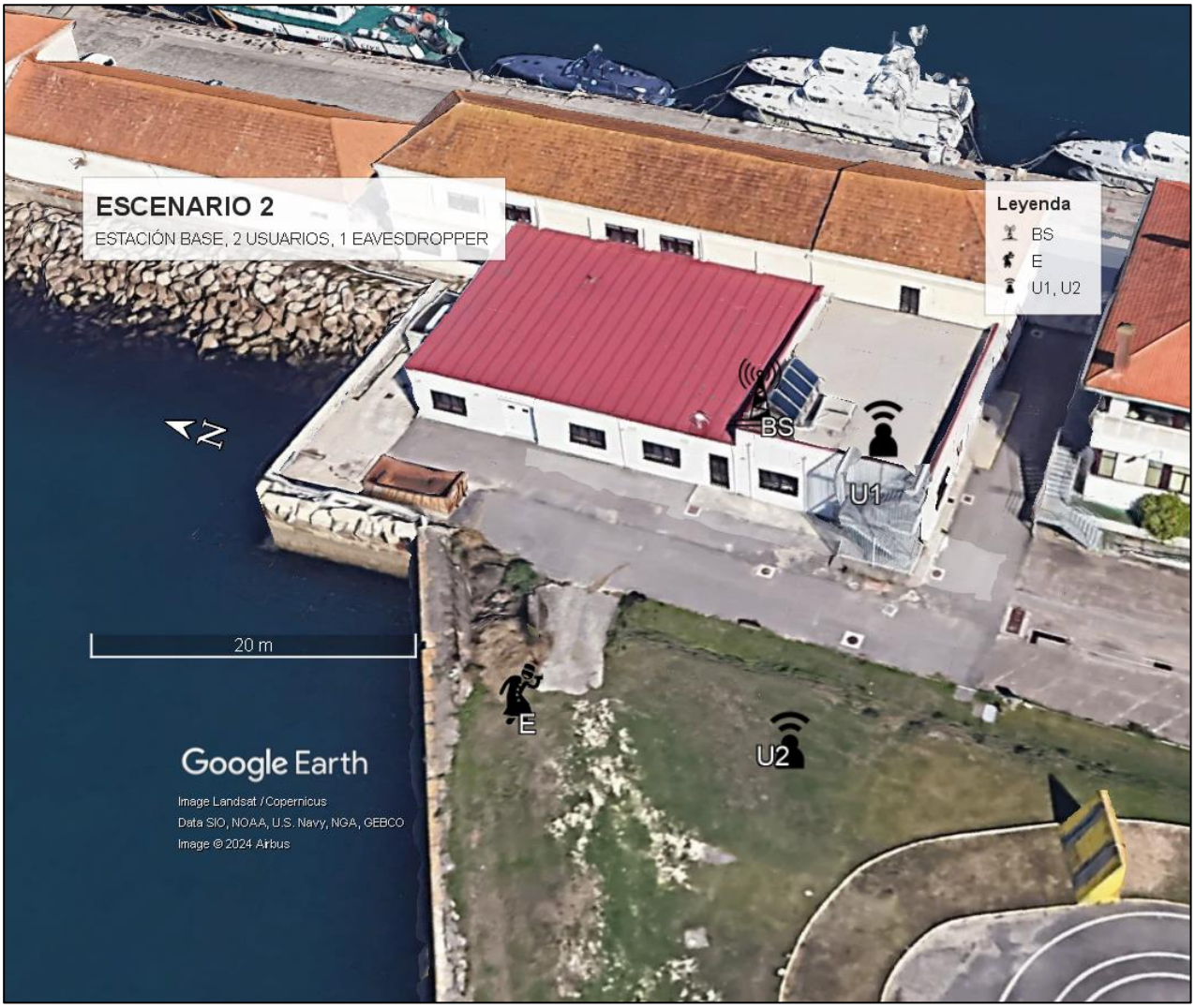


Figura 3-13: Representación gráfica del segundo escenario [Elaboración propia].

El propósito de los experimentos es conseguir la máxima capacidad secreta, pero por motivos físicos de *hardware* no es posible analizar el canal *downlink* de la Estación Base (Figura 3-9). Como solución, basando el Proyecto en el principio de dualidad demostrado en [36], los resultados obtenidos para el canal *uplink* se consideran válidos, y sustituibles por los que se obtendrían analizando el canal *downlink*.

Según los escenarios propuestos, los resultados obtenidos por el dispositivo USRP X310 (Figura 3-9) y procesados por el código desarrollado para el *software Matlab* serán analizados en el Apartado 4: Resultados.

4 RESULTADOS Y VALIDACIÓN

4.1 Primer escenario

Para el primer escenario (Figura 3-12), se realizarán tres experimentos alternando posiciones de los usuarios, para tener la posibilidad de contrastar datos y afianzar las capacidades del sistema propuesto. Es necesario tener en cuenta que, en este escenario, al no haber más de un usuario legítimo, no existen interferencias; por lo que los datos de SINR que se mostrarán serán equivalentes a la SNR.

Es necesario tener en cuenta que los datos que se muestran son del canal *uplink* de la BS, y se asume la dualidad de SINR o LINR con el *downlink* [36]. Como consecuencia, el uso de *precoders*, visto a lo largo del Proyecto; se sustituirá por el empleo de dos filtros o *equalizers*: ZF, que no varía respecto al *precoder* ZF; y MRC, que es el filtro que sustituye al *precoder* MRT. En resumen, los resultados obtenidos en el *uplink* son equivalentes a los que se obtendrían en el *downlink.*

4.1.1 Primer experimento

En este experimento, los usuarios E y U1 se encuentran en los ángulos 8º y -85º, respectivamente, como se muestra en la Figura 4-1.

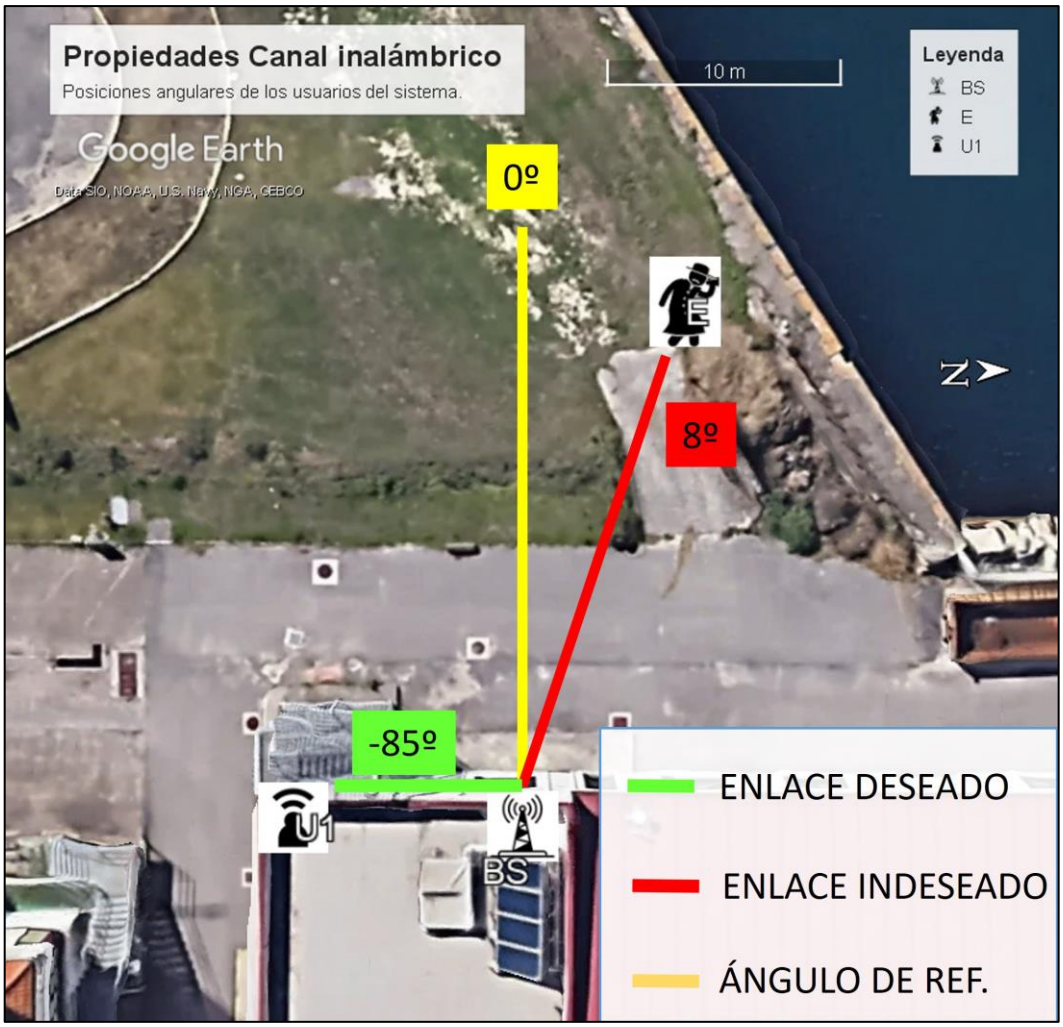


Figura 4-1: Vista en planta de posición angular de los usuarios [Elaboración propia].

La disposición de los usuarios queda demostrada en la Figura 4-2 y Figura 4-3, en las que se recibe la señal de interés (499595600 Hz por parte del *eavesdropper*, y 498000000 Hz por parte del usuario legítimo) y se muestra la ganancia en el dominio angular en valores teórico y real, según la disposición espacial respecto al *array* de antenas mostrada anteriormente.

El empleo de diferentes frecuencias no restringe la posibilidad real de realizar experimentos con las mismas frecuencias, es decir, es posible realizar pruebas emitiendo en las mismas frecuencias; pero en el caso de este Proyecto se emplean diferentes frecuencias para facilitar el control del escenario.

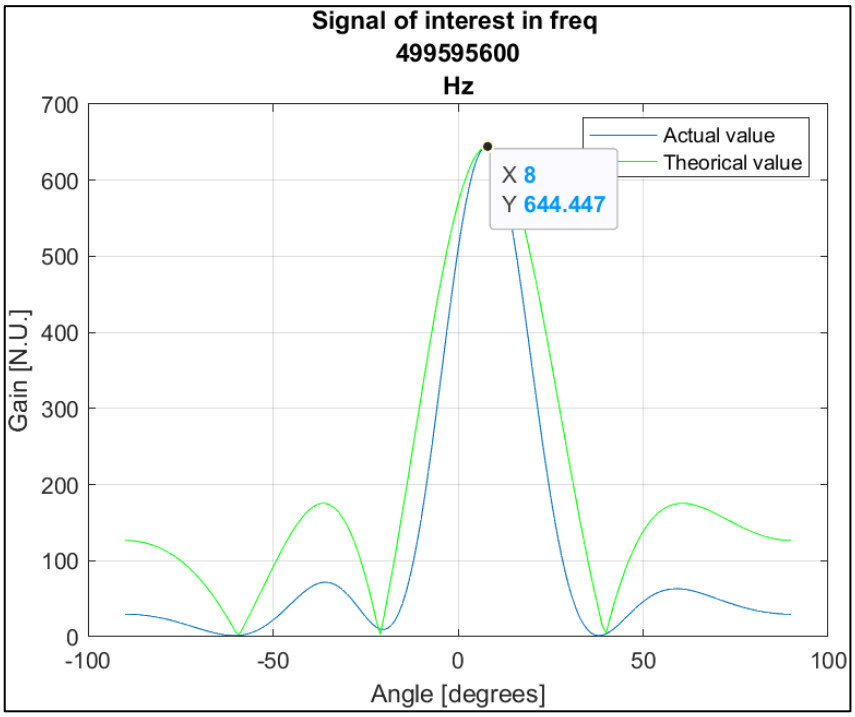


Figura 4-2: Ganancia del *array* de antenas para frecuencia del *eavesdropper* [Elaboración propia].

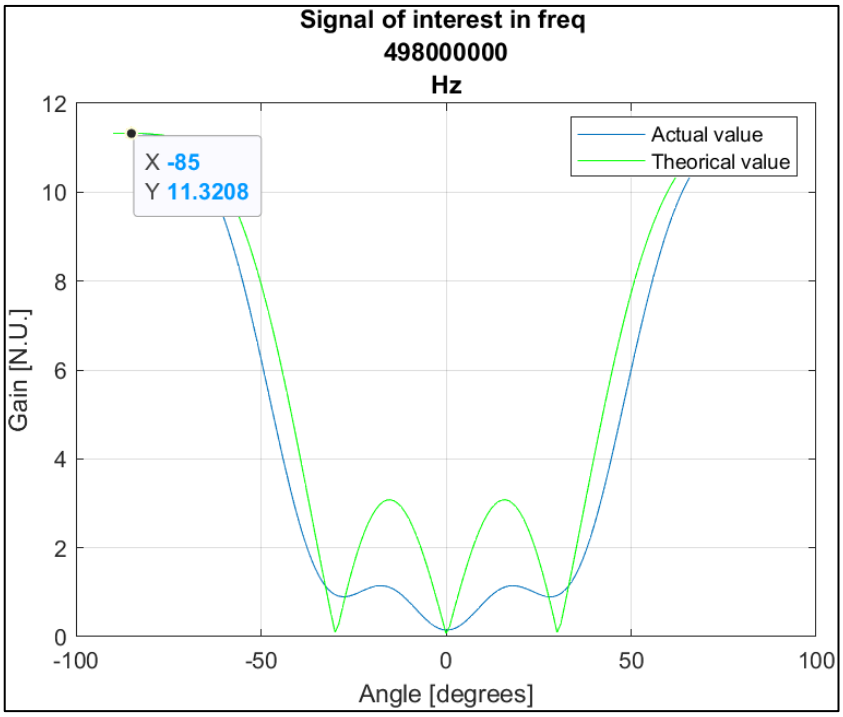


Figura 4-3: Ganancia del *array* de antenas para frecuencia del usuario legítimo [Elaboración propia].

La Figura 4-2 y Figura 4-3 demuestran a su vez que en este experimento el *eavesdropper* cuenta con la mayor ventaja, que es una antena con potencia de transmisión muy superior al usuario legítimo. De esta manera, el experimento se lleva al peor escenario posible, lo que a su vez ayudará a obtener conclusiones y preparar el sistema frente a amenazas menos exigentes.

Para el primer experimento, los datos que cada antena de la BS recibe son los mostrados en la Figura 4-4. De esta manera, se comprueba el correcto funcionamiento del sistema, ya que se recibe la señal de los dos usuarios del sistema, en las frecuencias y potencias esperadas.

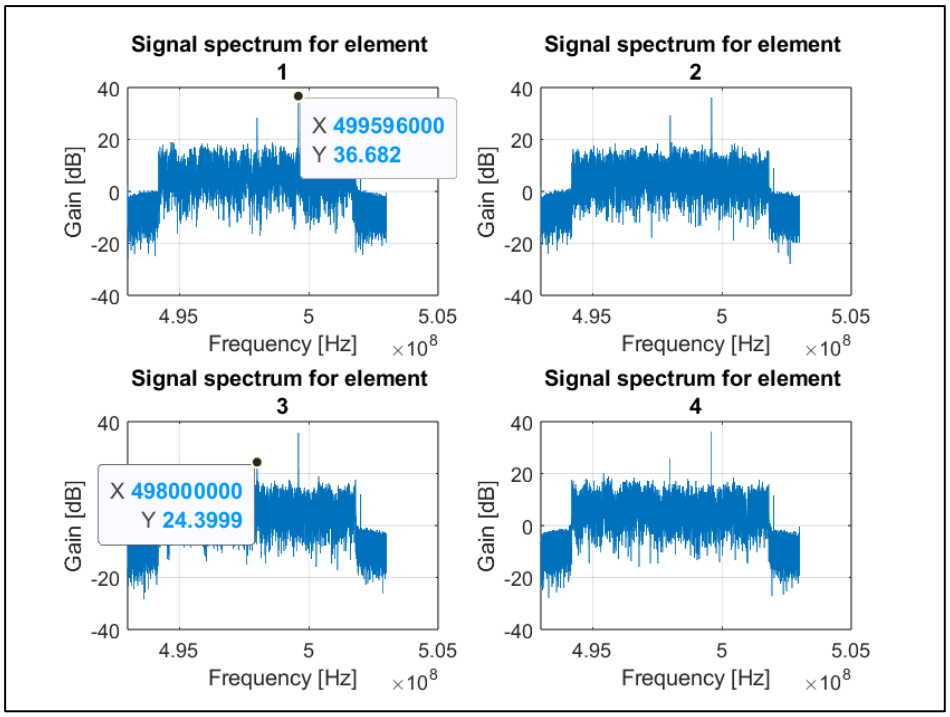


Figura 4-4: Recepción de datos para cada antena de la BS [Elaboración propia].

Como se puede comprobar, la situación es desfavorable para el usuario legítimo, pues el *eavesdropper* ya cuenta con superioridad en ganancia (36 dB vs. 24 dB), y se intentará reducir al máximo la ganancia para el *eavesdropper*, e intentar aumentar la ganancia del usuario legítimo.

Para ello, se realizan dos filtros: ZF configurado para forzar un nulo entre los ángulos 6º y 10º y apuntar en la dirección del usuario legítimo, y MRC orientado a -85º. En la Figura 4-5 se observan las ganancias aplicadas por el receptor para cada dirección espacial tras emplear el filtro ZF, en cuanto al dominio angular.

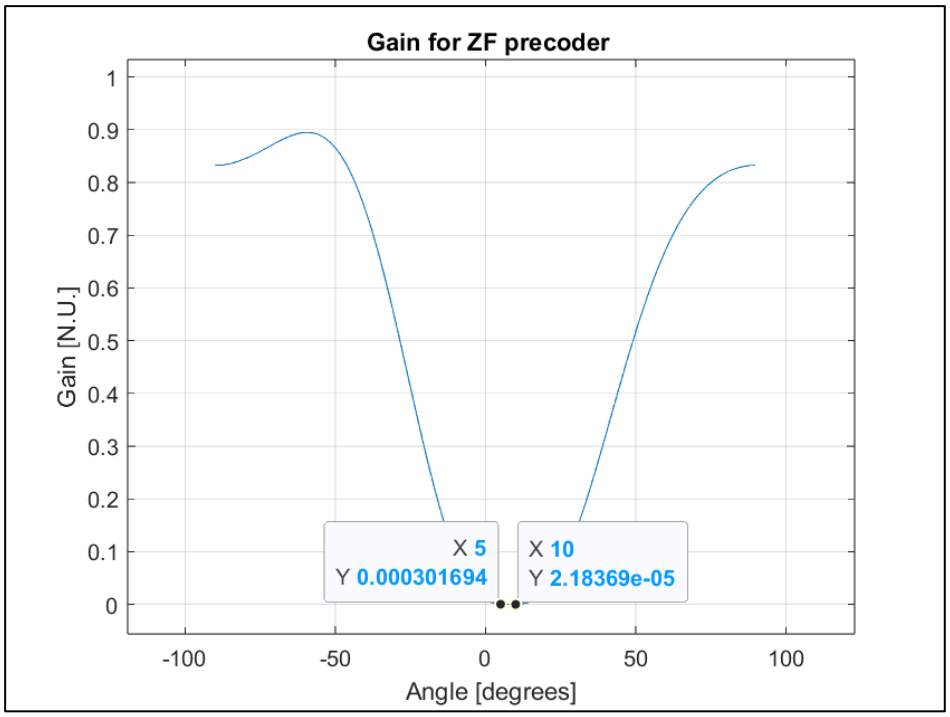


Figura 4-5: Ganancia obtenida al aplicar ZF, en el dominio angular [Elaboración propia].

En este experimento, el filtro ZF ha conseguido atenuar la dirección de interferencia, por lo que el resultado final de ganancia para un usuario en dicha dirección anulada debería ser considerablemente menor. En la Figura 4-6 se muestran los resultados obtenidos para cada filtro.

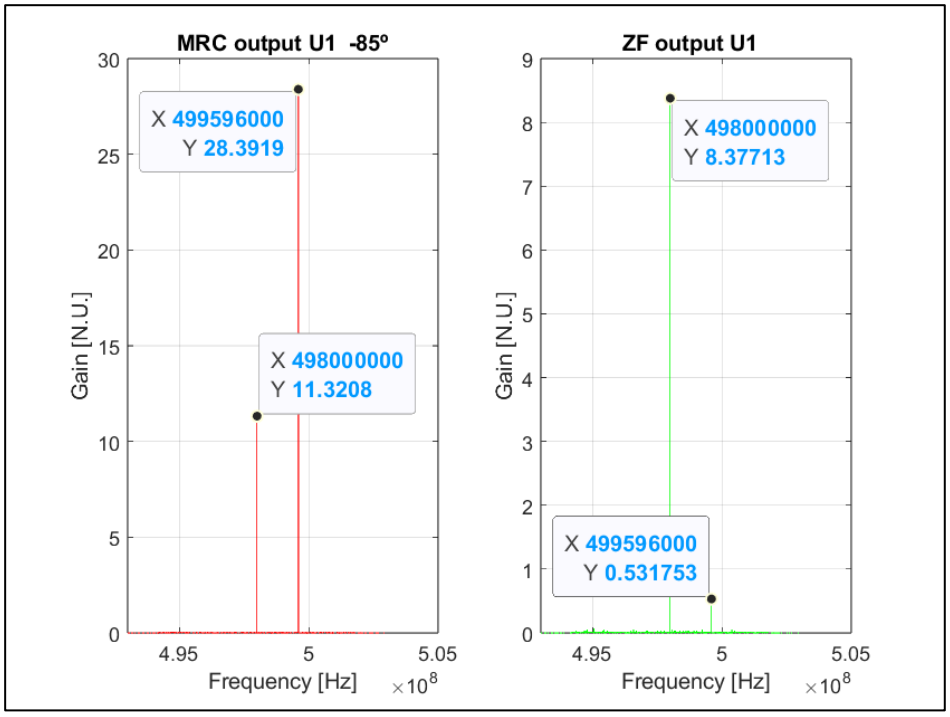


Figura 4-6: Ganancias obtenidas para cada filtro en el espectro frecuencial [Elaboración propia].

Como se puede comprobar en la Figura 4-6, aplicando el filtro MRC se obtiene un valor de potencia para la señal del usuario legítimo (11.3208) idéntico al obtenido en la Figura 4-3, pero el *eavesdropper* tiene una potencia superior (28.3919), por lo que es imposible que la capacidad secreta en esta situación sea positiva. El filtro MRC ha conseguido reducir la ganancia del *eavesdropper* (de 644.447 a 28.3919), pero no ha sido suficiente.

Al aplicar ZF entre 6º y 10º, la ganancia del *eavesdropper* se reduce en un 99.92% (de 644.447 a 0.531753), un porcentaje muy cercano a la cancelación de la señal interferente; y ha reducido levemente la ganancia del usuario legítimo (de 11.3208 a 8.37713). Por lo tanto, previsiblemente, el filtro ZF provocará un aumento en la capacidad secreta del sistema.

Los valores de SINR para el usuario legítimo, LINR para el *eavesdropper*, y capacidad secreta se muestran en la Tabla 4-1 en bps, para los dos tipos de filtros.

	MRC	**ZF**
SINR [bps]	122.7435	90.8271
LINR [bps]	307.8328	5.7654
CAPACIDAD SECRETA	0	3.7627

Tabla 4-1: Comparativa entre filtros del primer experimento [Elaboración propia].

Como se puede comprobar en la Tabla 4-1, al emplear el filtro MRC la capacidad secreta es negativa, por lo tanto, es nula, ya que su valor requiere ser superior que 0. Sin embargo, el empleo de ZF permite al usuario legítimo reducir en mayor medida la LINR del *eavedropper*, aunque también se reduce ligeramente la SINR respecto al empleo de MRC. Este factor repercute directamente en el cálculo de capacidad secreta aplicando ZF, que es correcto; al contrario que el valor obtenido al aplicar MRC. En otras palabras, a pesar de la diferencia en la potencia de transmisión de los usuarios, gracias al uso de ZF es posible transmitir al usuario legítimo sin que el *eavesdropper* pueda interceptar la comunicación.

El hecho de que la SINR sea superior al emplear MRC debería cumplirse en todos los experimentos que se realicen, ya que la acción que el filtro ZF lleva a cabo es aplicar un filtro MRC y restringir la ganancia, en cuanto al dominio angular de la interferencia se refiere.

En comparación con MRC, aplicando ZF se consigue reducir la LINR de 307.8328 a 5.7654 y, a pesar de la ligera reducción (de 122.7435 a 90.8271) de SINR, aumentar decisivamente la capacidad secreta. Dicho aumento marca la diferencia entre la intercepción de la comunicación por parte del *eavesdropper*, o el fallo en el intento.

En conclusión, en una situación de mismas características que las analizadas en este escenario, aplicar un *precoder* ZF evitará, mediante diversas técnicas como la introducción artificial de ruido, que el *eavesdropper* intercepte la transmisión entre la BS y el usuario legítimo, proporcionando al sistema un determinado grado de Seguridad en la Capa Física.

4.1.2 Segundo experimento

El segundo experimento se realizará con una ligera modificación en el escenario del anterior. En este caso, la posición del *eavesdropper* (E) se desplazará a la anterior posición que ocupaba el usuario legítimo (-85º), y el usuario legítimo se situará en el ángulo de referencia de la antena (0º) y transmitirá con una antena de mayor ganancia; de manera que se pueda analizar la flexibilidad del sistema ante diferentes posiciones de los usuarios. La disposición de los usuarios se detalla en la Figura 4-7.

Figura 4-7: Vista en planta de posición angular de los usuarios [Elaboración propia].

Para el segundo experimento, los datos que cada antena de la BS recibe son los mostrados en la Figura 4-8. De esta manera, se comprueba el correcto funcionamiento del sistema, ya que se recibe la señal de los dos usuarios del sistema, en las frecuencias y potencias esperadas. En la Figura 4-8 también se aprecia la superioridad en ganancia del usuario legítimo sin aplicar filtros.

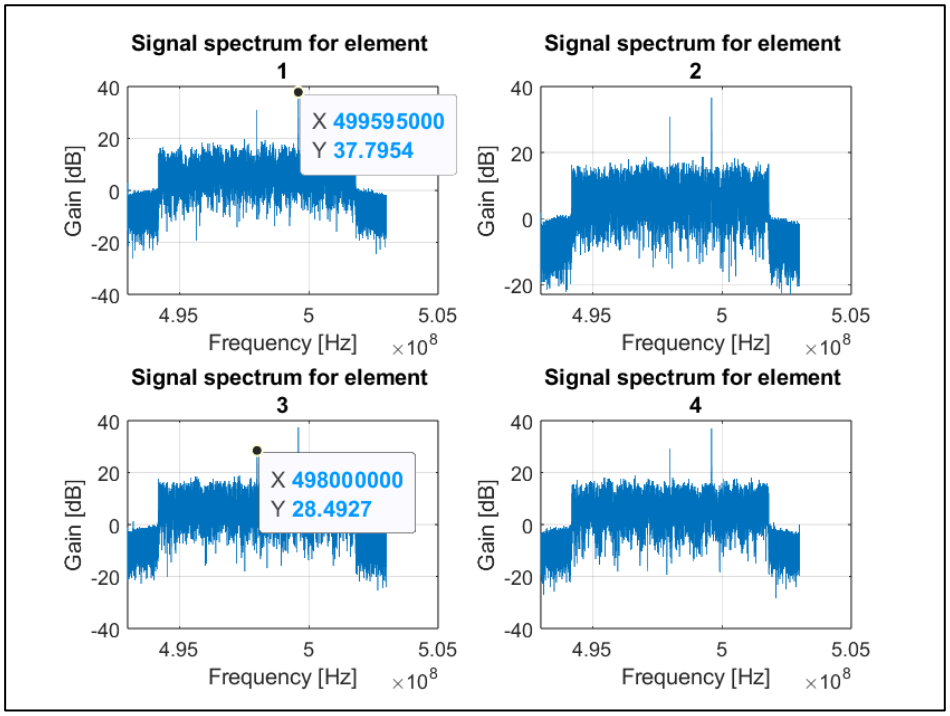


Figura 4-8: Recepción de datos para cada antena de la BS [Elaboración propia].

La disposición de los usuarios queda corroborada en la Figura 4-9 y Figura 4-10, en las que se recibe la señal de interés (499595600 Hz por parte del usuario legítimo, y 498000000 Hz por parte del *eavesdropper*) y se muestra la ganancia en el dominio angular en valores teórico y real, según la disposición del *array* de antenas mostrada anteriormente.

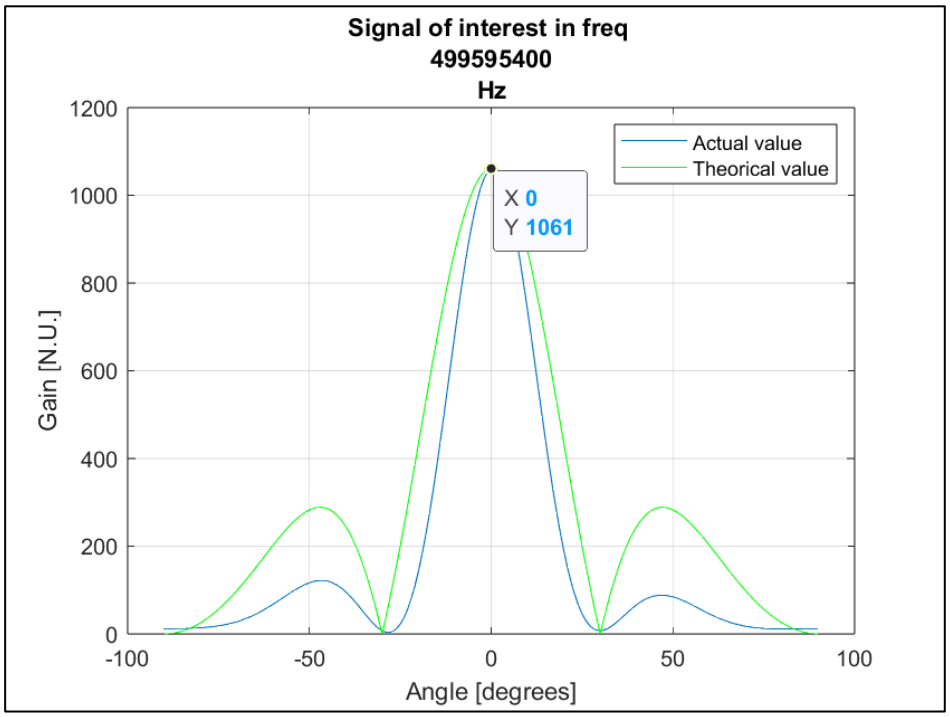


Figura 4-9: Ganancia del *array* de antenas para frecuencia del usuario legítimo [Elaboración propia].

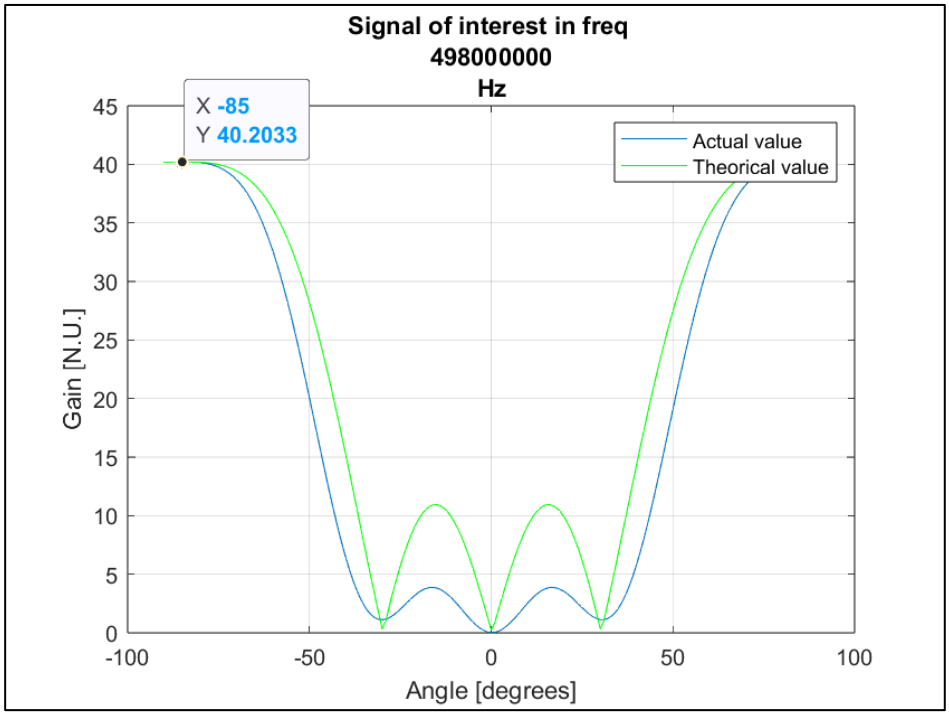


Figura 4-10: Ganancia del *array* de antenas para frecuencia del *eavesdropper* [Elaboración propia].

Como se puede comprobar en la Figura 4-9, en este caso el usuario legítimo cuenta con una ganancia mayor (1061) que la del *eavesdropper*, lo cual es un factor para tener en cuenta en los resultados que se obtengan, que presuntamente deberían ser superiores a los del anterior experimento.

Para intentar conseguir la máxima capacidad secreta, se han aplicado los mismos dos filtros que en el caso anterior: MRC dirigido al ángulo de referencia (0º) y ZF configurado para atenuar al máximo la señal de los ángulos comprendidos entre -86º y -84º, y tratar de aumentar la señal proveniente del ángulo 0º.

En la Figura 4-11 se detalla la respuesta del ZF ante la programación establecida, y se puede comprobar el correcto funcionamiento de este, estableciendo la ganancia máxima en la dirección del usuario legítimo, y la mínima en la dirección del *eavesdropper*.

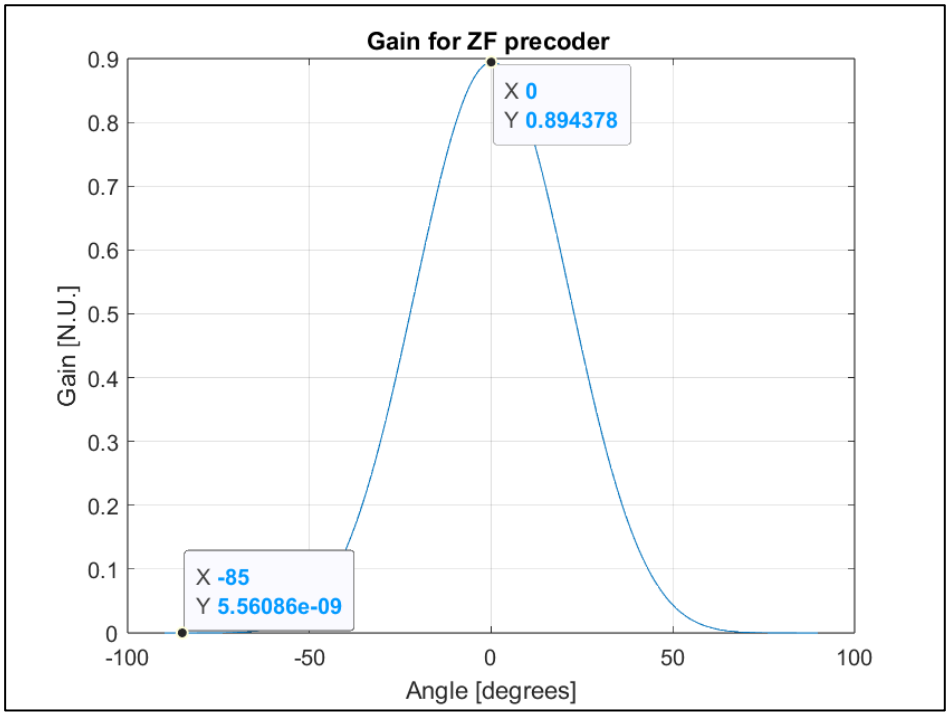


Figura 4-11: Ganancia obtenida al aplicar ZF, en el dominio angular [Elaboración propia].

En la Figura 4-12 se muestran los resultados obtenidos por cada filtro.

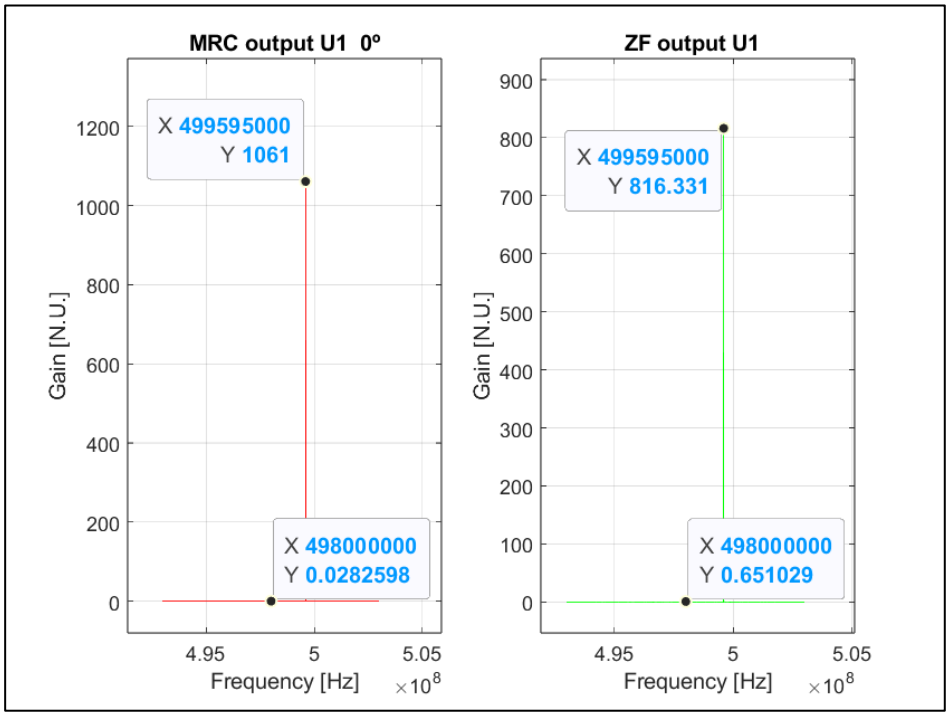


Figura 4-12: Ganancias obtenidas para cada filtro en el espectro frecuencial [Elaboración propia].

El filtro MRC orientado a la dirección del usuario legítimo demuestra resultados muy beneficiosos para el sistema, ya que ha conseguido mantener la ganancia del usuario legítimo (1061, comparando Figura 4-9 y Figura 4-12) y ha reducido casi al completo la potencia del *eavesdropper* (de 40.2033 a 0.0282598), comparando la Figura 4-10 y Figura 4-12.

Por otro lado, el filtro ZF ha reducido levemente la ganancia del usuario legítimo (1061 Vs. 816.331) y ha atenuado en gran medida la señal del *eavesdropper*, comparando la Figura 4-10 y Figura 4-12 (de 40.2033 a 0.6510); pero los valores de ganancia obtenidos por el filtro MRC superan a los obtenidos por ZF, y la capacidad secreta resultará previsiblemente mayor aplicando el filtro MRC.

Los valores de SINR para el usuario legítimo, LINR para el *eavesdropper*, y capacidad secreta se muestran en la Tabla 4-2 en bps, para los dos tipos de filtros.

	MRC	**ZF**
SINR [bps]	9035.8683	6952.1666
LINR [bps]	0.24067	5.5444
CAPACIDAD SECRETA	12.8305	10.0532

Tabla 4-2: Comparativa entre filtros del segundo experimento [Elaboración propia].

Como se puede comprobar en la Tabla 4-2, al emplear el filtro MRC la capacidad secreta es superior que al emplear ZF (12.8305 Vs. 10.0532), aunque ambos valores son válidos para que la comunicación entre la BS y el usuario legítimo pueda no ser interceptada por el *eavesdropper*.

Entrando más en detalle, MRC tiene más capacidad que ZF para conservar la SINR del usuario legítimo, y debería ser siempre así. Por ello, aplicando ZF se obtiene un valor reducido de SINR (9035.8683 Vs. 6952.1666), lo que en este caso supone un factor diferencial en el posterior cálculo de la capacidad secreta.

Por otro lado, la LINR obtenida es menor con el filtro MRC (0.24067) que con el filtro ZF (5.5444). Esto ocurre porque la efectividad de ZF está totalmente condicionada por el grado de ortogonalidad de los canales correspondientes a cada usuario o, en otras palabras, la posición en que se encuentren los usuarios. Es por ello por lo que, en este caso particular, aplicando el filtro ZF la LINR es mayor y resulta más ventajoso aplicar MRC.

En comparación con el primer experimento, la capacidad secreta obtenida en el segundo experimento se debe a la superioridad del usuario legítimo en cuanto a ganancia frente al *eavesdropper*, al contrario que ocurre en el primer experimento; por lo que los resultados son los esperados y corroboran el correcto funcionamiento de ambos experimentos.

En conclusión, en una situación de mismas características que las analizadas en este escenario, la aplicación de un *precoder* ZF evitará en casi total medida que la comunicación entre la BS y el U1 pueda ser interceptada por el *eavesdropper*.

4.1.3 Tercer experimento

El tercer experimento alternará la posición del *eavesdropper* con la del usuario legítimo, complicando el escenario ya que en este caso la antena de mayor ganancia pertenece al *eavesdropper*. En la Figura 4-13 se detallan las posiciones de ambos usuarios.

Figura 4-13: Vista en planta de posición angular de los usuarios [Elaboración propia].

Para el tercer experimento, los datos recibidos por la BS son los mismos que en el segundo experimento, por lo que en la Figura 4-8 se puede comprobar el correcto funcionamiento del sistema.

La recepción de las señales transmitidas por los usuarios se muestra en la Figura 4-9 y Figura 4-10, con la diferencia de que en este experimento la frecuencia de transmisión del usuario legítimo es 498000000 Hz (Figura 4-10) y la del *eavesdropper* es 499595600 Hz (Figura 4-9).

Previsiblemente, la dificultad para conseguir valores beneficiosos de capacidad secreta aumenta en gran medida; por lo que a continuación se aplicarán los dos filtros: MRC orientado a -85º, y ZF configurado para atenuar lo máximo posible las direcciones comprendidas entre los ángulos -1º y 1º, y potenciar la señal proveniente de la dirección -85º.

En la Figura 4-14 se detalla la respuesta del ZF ante la programación establecida, y se puede comprobar el correcto funcionamiento de este, estableciendo la ganancia máxima en la dirección del usuario legítimo, y la mínima en la dirección del *eavesdropper*.

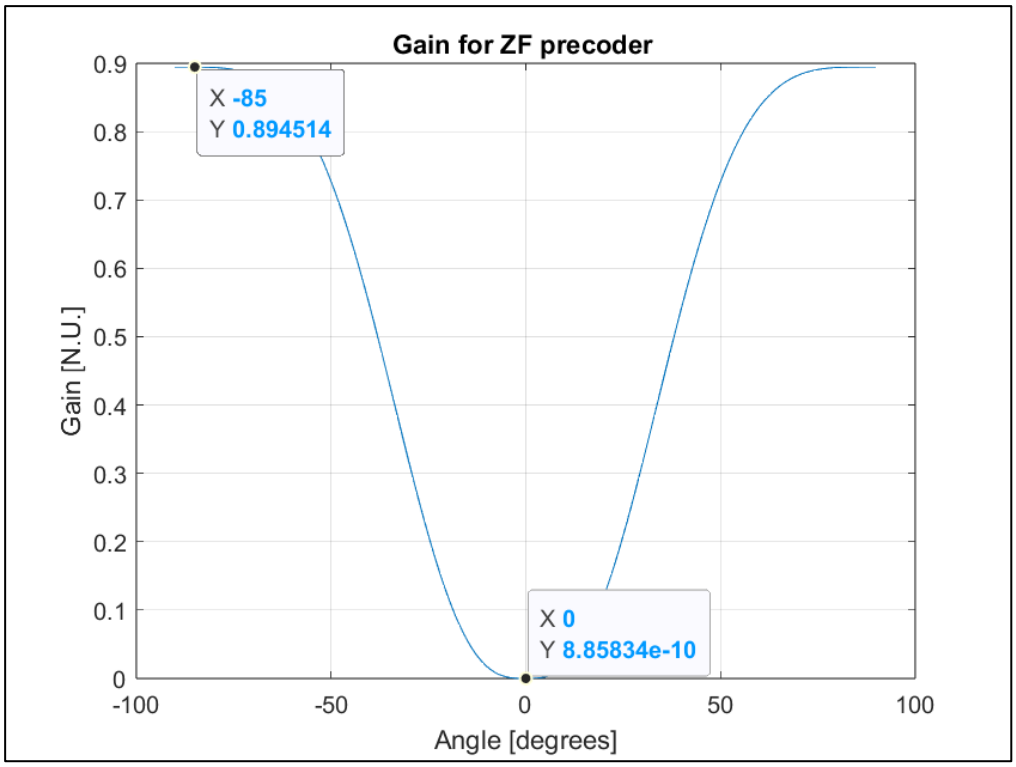


Figura 4-14: Ganancia obtenida al aplicar ZF, en el dominio angular [Elaboración propia].

Los resultados aplicando los filtros MRC y ZF se muestran a continuación, en la Figura 4-15.

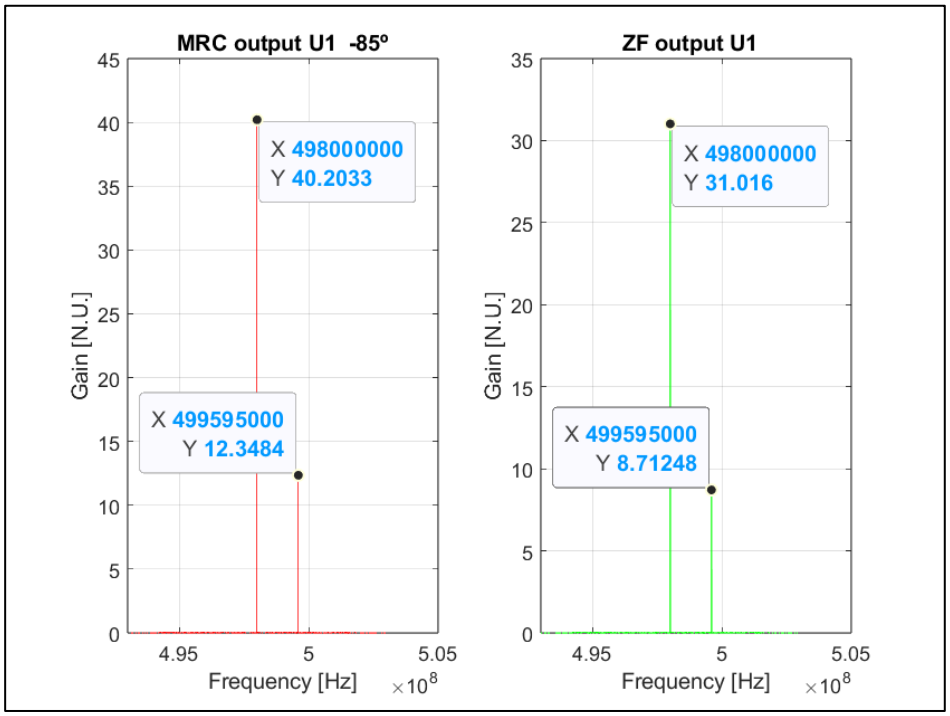


Figura 4-15: Ganancias obtenidas para cada filtro en el espectro frecuencial [Elaboración propia].

Como se puede comprobar en la Figura 4-15, en el tercer experimento se obtiene un resultado que aparentemente consigue el objetivo: tanto al aplicar MRC como ZF la ganancia obtenida del *eavesdropper* (12.3484 en MRC y 8.71248 en ZF) es inferior a la obtenida del usuario legítimo (40.2033 en MRC y 31.016 en ZF); por lo que es muy probable que la capacidad secreta aplicando ambos filtros resulte positiva.

Además, el filtro MRC reduce en gran medida la ganancia del *eavesdropper*, comparando la Figura 4-9 y Figura 4-15 (de 1061 a 12.3484) y recibe la señal de interés (40.2033) sin atenuación; por lo que su funcionamiento es más que correcto.

Por otra parte, el filtro ZF consigue reducir la ganancia del *eavesdropper* en un 99.18% (de 1061 a 8.71248), pero reduce también la ganancia del usuario legítimo: de 40.2033 a 31.016. Analizando ambas reducciones, la aplicación del filtro ZF es exitosa, ya que se obtiene con mayor ganancia la señal del usuario legítimo (31.016) que la del *eavesdropper* (8.71248), e inicialmente ocurría lo contrario.

Los valores de SINR para el usuario legítimo, LINR para el *eavesdropper*, y capacidad secreta se muestran en la Tabla 4-3 en bps, para los dos tipos de filtros.

	MRC	**ZF**
SINR [bps]	338.6903	261.293
LINR [bps]	104.0283	73.3978
CAPACIDAD SECRETA	1.6934	1.8178

Tabla 4-3: Comparativa entre filtros del segundo experimento [Elaboración propia].

Como se puede comprobar en la Tabla 4-3, al emplear el filtro MRC se consigue la capacidad secreta positiva (1.6934), pero aplicando ZF la capacidad secreta es incluso mayor (1.8178). Esto implica que, en este experimento, ambos filtros son válidos para establecer una comunicación segura.

En la Tabla 4-3 se puede comprobar que, inicialmente, el valor de SINR es superior en MRC (338.6903) que aplicando ZF (261.293); por lo que se vuelve a cumplir lo esperado.

El dato determinante en este experimento es la LINR. Como se muestra en la Tabla 4-3, en MRC se obtiene un valor de LINR (104.0283) más alto que empleando el filtro ZF (73.3978). Dicha diferencia es el resultado de aplicar correctamente la restricción del filtro ZF, en cuanto al dominio angular se refiere.

En el cálculo de capacidades secretas para ambos filtros, tiene mayor relevancia la restricción que aplica ZF para reducir la LINR, que la potenciación que aplica el filtro MRC para aumentar la SINR; por lo que el cálculo de capacidad secreta es superior para el filtro ZF.

No obstante, los resultados de capacidad secreta obtenidos en el tercer experimento son menores que en el primer y segundo experimento; pero teniendo en cuenta las ganancias iniciales de los usuarios, es decir, la ventaja inicial del *eavesdropper*, los resultados empleando ZF y MRC son exitosos.

En conclusión, en una situación de mismas características que las analizadas en este escenario, el empleo de un *precoder* ZF puede evitar en gran medida que la transmisión por parte de la BS al usuario legítimo sea interceptada por el *eavesdropper*. Pese a obtener el peor resultado de capacidad secreta, la capacidad de atenuar ganancias tan superiores es un indicativo de que, con una condición del usuario legítimo más equitativa (como ocurriría en el *downlink* de un sistema de comunicaciones), es posible conseguir una comunicación muy difícil de interceptar por un *eavesdropper*.

4.2 Segundo escenario

Para el segundo escenario (Figura 3-13), se realizarán dos experimentos. En este caso, al contar con más de un usuario legítimo, cada usuario legítimo causa interferencia al otro; por lo que la SINR se verá afectada, y ya no equivaldrá a la SNR, como ocurría en los casos anteriores. Por lo tanto, la SINR empleando MRC a partir de ahora puede ser inferior a la SINR empleando ZF, en función de la cantidad de interferencia que reciban los usuarios.

De nuevo, los datos mostrados son experimentos realizados en el canal *uplink* de la BS, y se continúa asumiendo la dualidad de SINR o LINR con el *downlink* [36]; así como el empleo de filtros en vez de *precoders*.

4.2.1 Primer experimento

En el primer experimento, los usuarios E, U1 y U2 se encuentran en los ángulos 37º, -85º y -7º, respectivamente, como se muestra en la Figura 4-16.

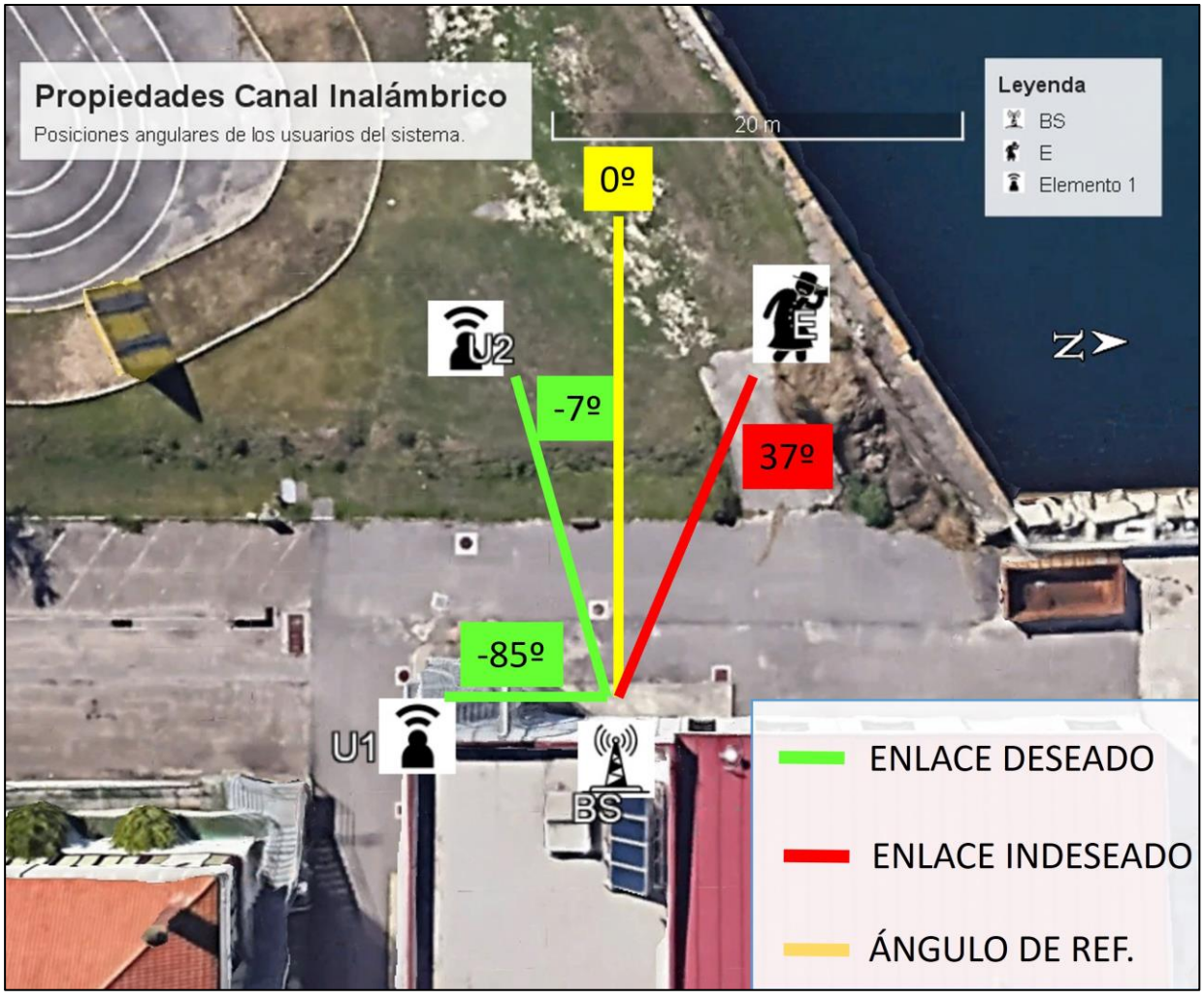


Figura 4-16: Vista en planta de posición angular de los usuarios [Elaboración propia].

Los datos recibidos por la BS se muestran en la Figura 4-17. Las tres señales se reciben correctamente, en las frecuencias deseadas: 498000000 Hz en el caso de U1, 499595000 Hz en el caso de U2 y 496394000 Hz en el caso del *eavesdropper* (E). En unidades logarítmicas, el usuario con más potencia en transmisión es U2 (37.3647 dB), seguido del U1 (27.9948 dB) y por último el *eavesdropper* (26.2958). Esto implica que el experimento se ha ideado para analizar una situación favorable, de manera que se pueda corroborar el correcto funcionamiento del sistema.

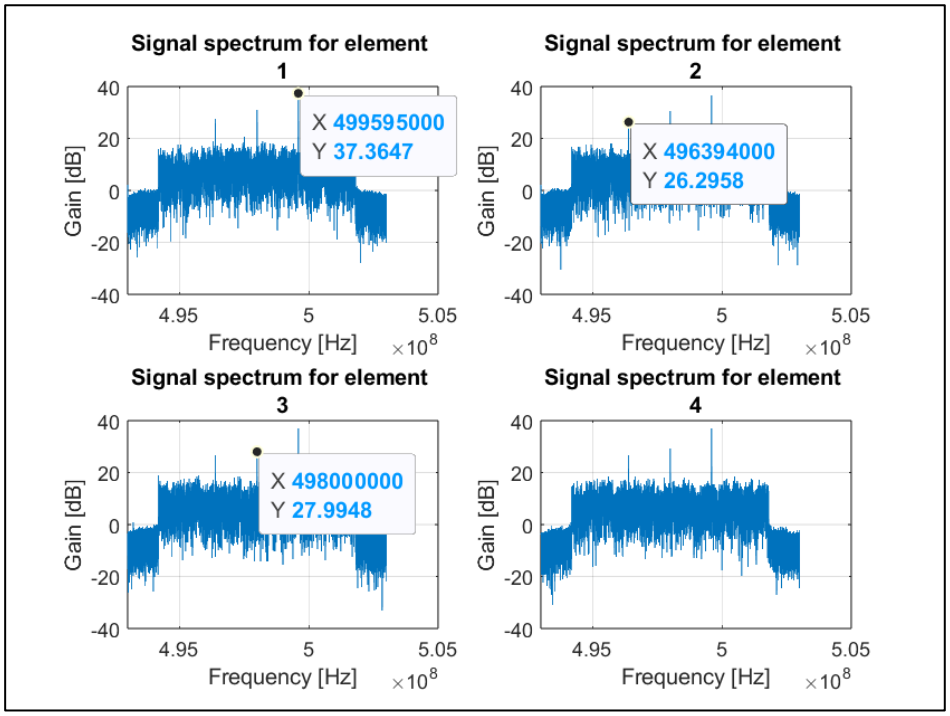


Figura 4-17: Recepción de datos para cada antena de la BS [Elaboración propia].

En la Figura 4-18, Figura 4-19 y Figura 4-20 se muestran las ganancias de cada usuario en el dominio angular.

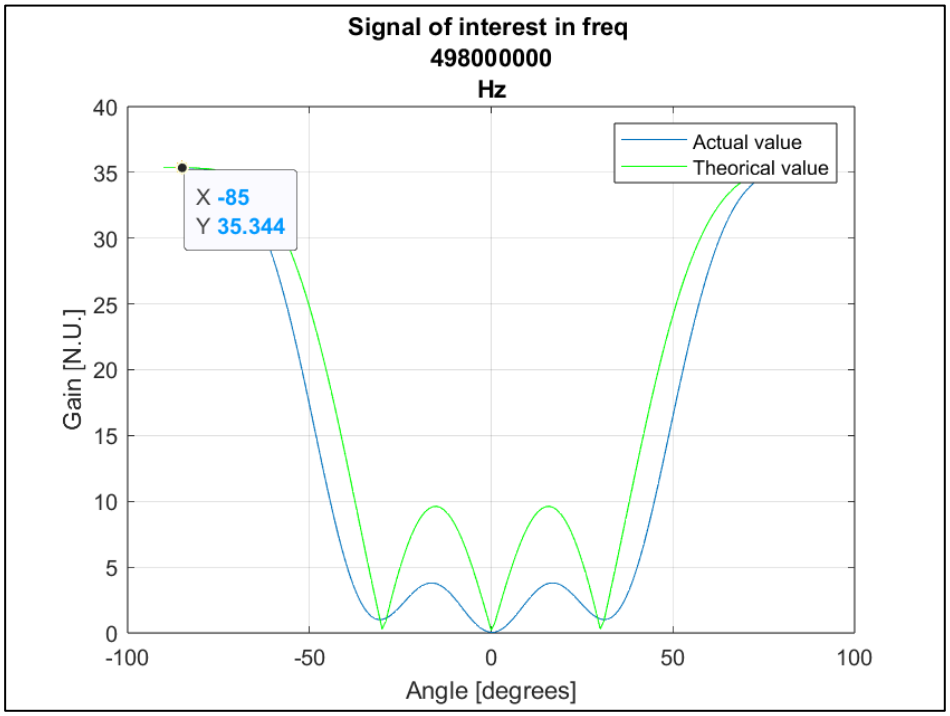


Figura 4-18: Ganancia del *array* de antenas para frecuencia del primer usuario legítimo, U1 [Elaboración propia].

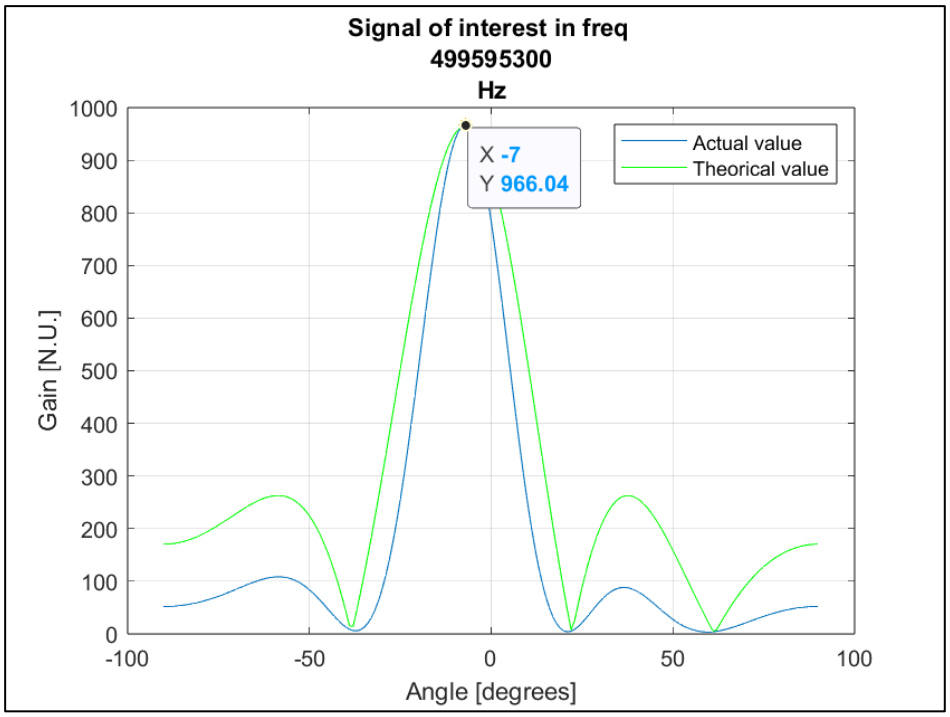


Figura 4-19: Ganancia del *array* de antenas para frecuencia del segundo usuario legítimo, U2 [Elaboración propia].

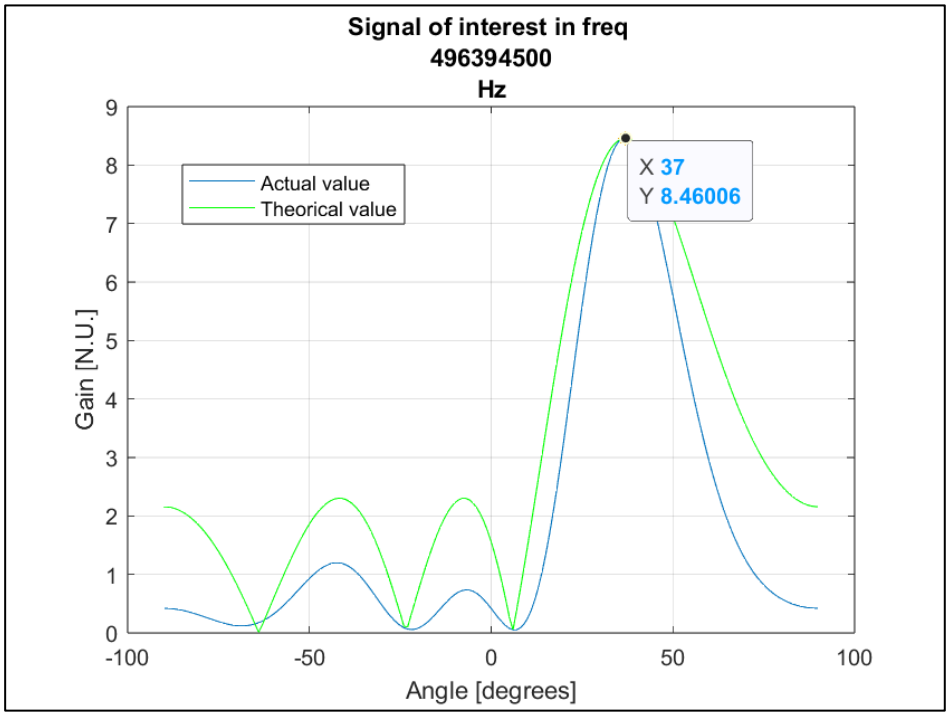


Figura 4-20: Ganancia del *array* de antenas para frecuencia del *eavesdropper* [Elaboración propia].

En este experimento se han aplicado los filtros MRC y ZF a cada usuario legítimo, es decir, en total se han aplicado dos filtros de MRC (a U1 y U2) y dos filtros de ZF (a U1 y U2). El filtro MRC aplicado a U1 ha sido programado para potenciar la ganancia en la dirección angular -85º, mientras que el segundo filtro MRC aplicado a U2 ha sido configurado para el mismo propósito en la dirección angular -7º.

Por otra parte, el filtro ZF aplicado a U1 ha sido configurado para aumentar la ganancia en la dirección angular -85º y atenuar la dirección angular comprendida entre -8º y 38º, con el propósito de evitar la potente interferencia que causaría U2 e intentar cancelar lo máximo posible la ganancia del *eavesdropper*.

Para U2, ZF ha sido configurado para aumentar la ganancia en la dirección angular -7º, y para intentar atenuar la dirección angular comprendida entre 36º y 38º, es decir, intenta cancelar exclusivamente el *eavesdropper*; aprovechando el comportamiento de dicha configuración, ya que la respuesta atenúa considerablemente la ganancia en la dirección de U1de forma natural. En la Figura 4-21 y Figura 4-22 se muestran las respuestas de los filtros ZF para ambos usuarios.

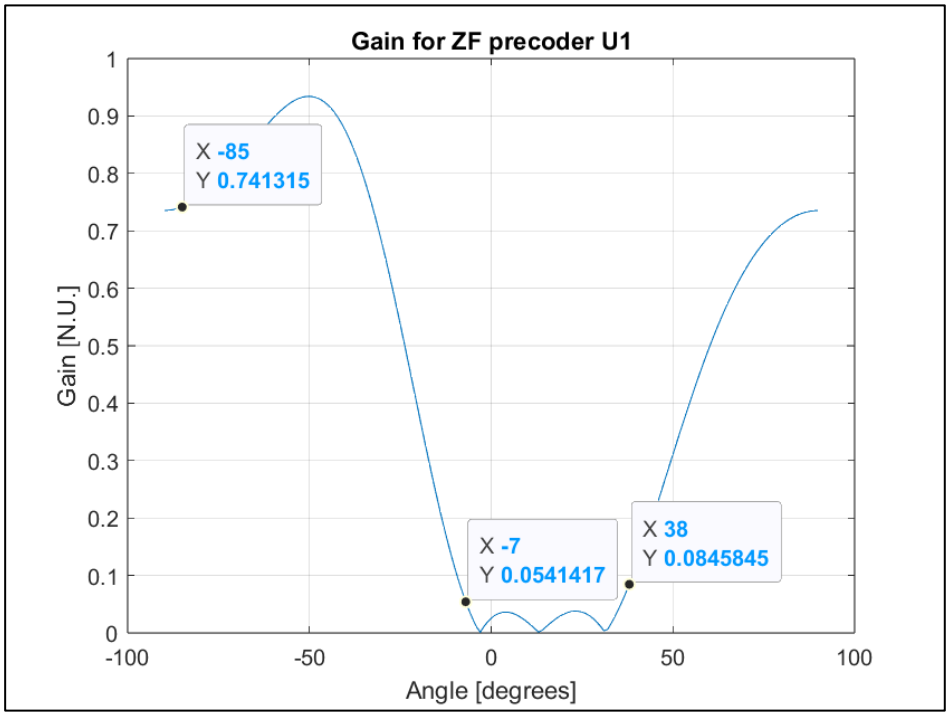


Figura 4-21: Ganancia obtenida al aplicar ZF al U1, en el dominio angular [Elaboración propia].

Como se puede comprobar en la Figura 4-21 y Figura 4-22, las respuestas de los dos filtros ZF son diferentes, como era de esperar. De ambas respuestas se puede deducir que, en cuanto al comportamiento del filtro, el filtro ZF prioriza atenuar la ganancia en la dirección angular establecida; dejando en un segundo plano la configuración que trata de potenciar la dirección angular en la que se encuentra la señal deseada, que en este caso son -85º y -7º, respectivamente.

Si el rango angular configurado para anular es demasiado amplio, el filtro sacrifica cancelación permitiendo pequeños lóbulos de ganancia, pero es algo inevitable si no se emplean más antenas.

Las respuestas del filtro ZF obtenidas en este experimento ofrecen menor ganancia en las direcciones angulares de interés que las obtenidas en escenarios con un usuario legítimo y un *eavesdropper*, por lo que inicialmente los sistemas con más de un usuario legítimo y un *eavesdropper* parten de esta desventaja.

En relación con dicha desventaja, se ve más afectado U2 ya que la respuesta de ZF en su dirección angular (-7º) reduce su ganancia por un factor de 0.668015 (Figura 4-22), mientras que para U1 la respuesta de ZF en su dirección angular (-85º) reduce su ganancia por un factor de 0.741315; es decir, ZF atenuará en mayor medida la señal de U2.

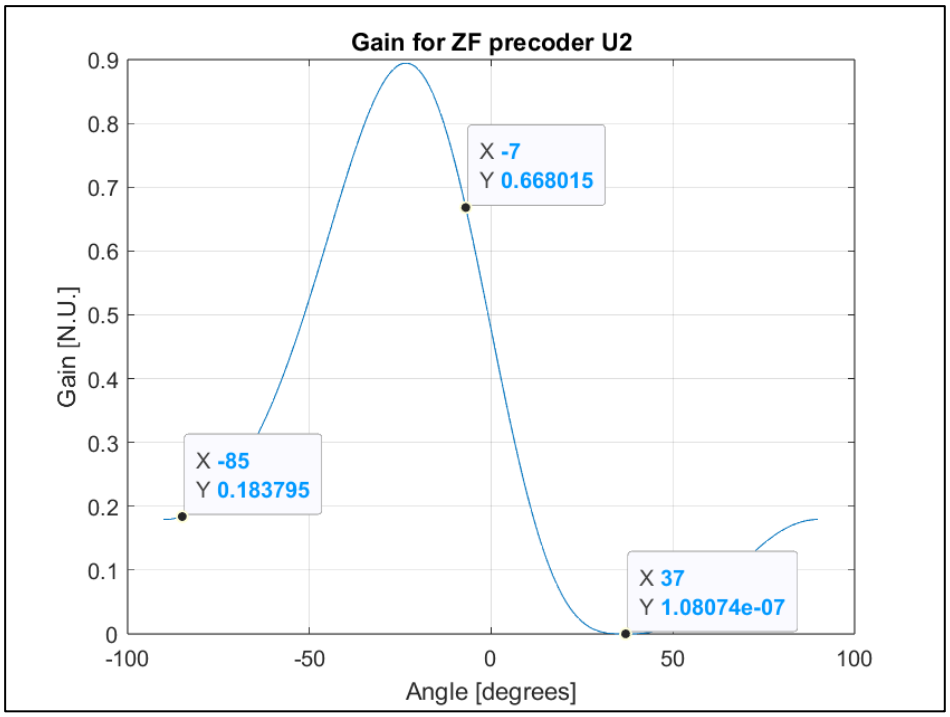


Figura 4-22: Ganancia obtenida al aplicar ZF al U2, en el dominio angular [Elaboración propia].

En la Figura 4-23 se muestra la comparación entre la aplicación de MRC y ZF para U1.

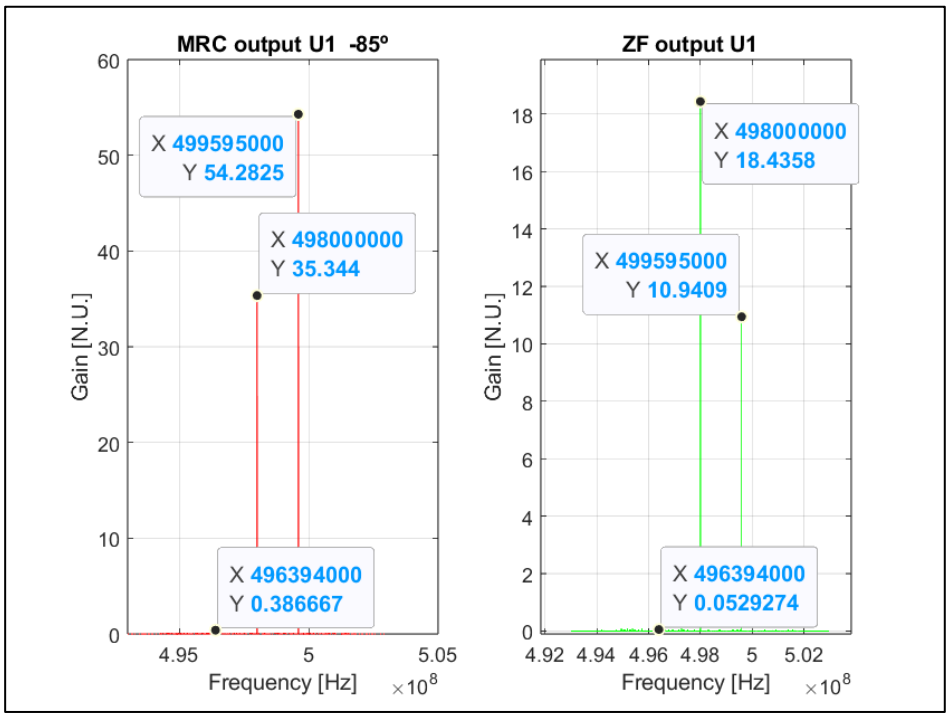


Figura 4-23: Ganancias obtenidas por cada filtro aplicado a U1 en el espectro frecuencial [Elaboración propia].

Recordemos la asignación de usuarios por frecuencias: 498000000 Hz en el caso de U1, 499595000 Hz en el caso de U2 y 496394000 Hz en el caso del *eavesdropper* (E). A continuación, se realizará un análisis del entorno de U1.

Como se puede comprobar en la Figura 4-23, la aplicación de MRC para U1 (-85º) provoca que se reciba con gran potencia la señal de U2. Este suceso es debido a la gran potencia que tenía U2

inicialmente mostrada en la Figura 4-19 (966.04). Con MRC se consigue mantener la potencia de U1 (35.344) y reducir en gran medida la potencia de U2 (de 966.04 a 54.2825), pero dicha reducción no es suficiente. La potencia obtenida de U2 afectará negativamente a la SINR, ya que será interferencia y se sumará al ruido del canal, pero será muy improbable que el *eavesdropper* intercepte la comunicación.

Aplicando MRC también se observa en la Figura 4-23 que la señal del *eavesdropper* ha sido cancelada casi al completo (de 8.46006 a 0.386667), por lo que el funcionamiento de MRC es válido para atenuar potencias inicialmente bajas, pero insuficiente para evitar interferencias de usuarios con alta potencia de transmisión.

Al aplicar ZF, se puede comprobar que la potencia obtenida para el U1 es reducida (de 35.344 a 18.4358) debido a la restricción adicional que aplica ZF, pero superior a la potencia recibida de U2 (10.9409). Se ha conseguido reducir en gran medida tanto la señal de U2 (de 966.04 a 10.9409) como la del *eavesdropper* (de 8.46006 a 0.0529274); por lo que previsiblemente la SINR de U1 se verá beneficiada empleando ZF y será muy improbable que el *eavesdropper* intercepte la comunicación.

En la Figura 4-24 se muestran los resultados aplicando ambos filtros para U2.

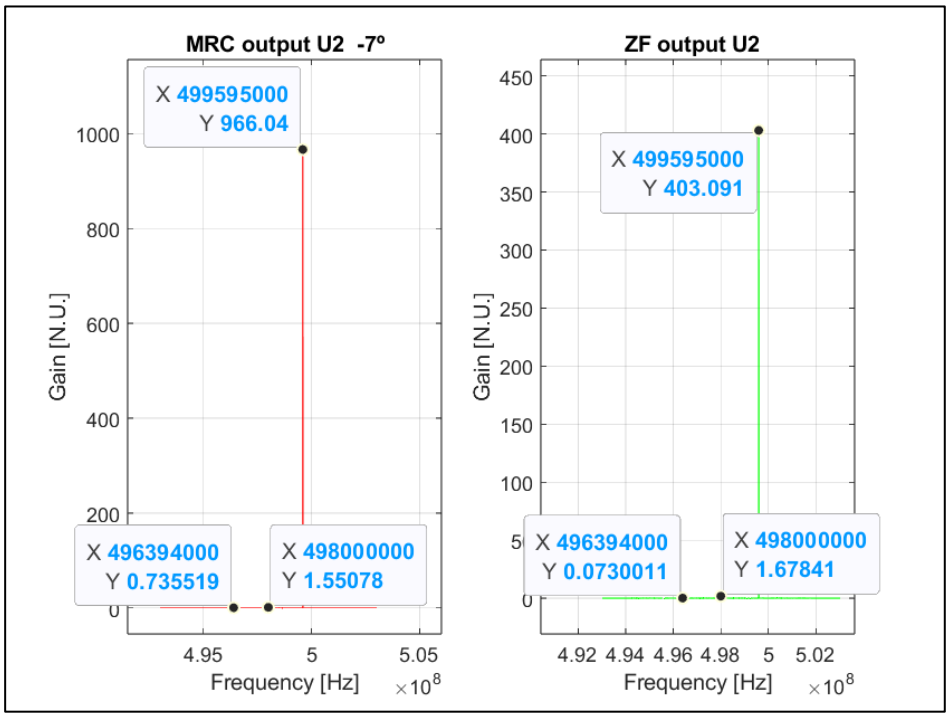


Figura 4-24: Ganancias obtenidas por cada filtro aplicado a U2 en el espectro frecuencial [Elaboración propia].

A continuación, se realizará un análisis del entorno de U2.

Como se puede comprobar en la Figura 4-24, la aplicación de MRC para U2 (-7º) provoca que su señal sea recibida con la misma ganancia (966.04), y el resto de las señales son atenuadas considerablemente: de 45.344 a 1.55078 en el caso de U1 y de 8.46006 a 0.0730011 en el caso del *eavesdropper*. Las reducciones son exitosas, ya que las ganancias de U1 y *eavesdropper* distan considerablemente, en cuanto a valor, de U2; y este factor beneficiará tanto a la SINR de U2 como a establecer comunicación con baja probabilidad de intercepción por parte del *eavesdropper*.

Al aplicar ZF, las ganancias obtenidas son una consecuencia de la importante restricción que aplica el filtro. La ganancia de U2 ha sido muy reducida (de 966.04 a 403.091) y se demuestra que esta disposición de los usuarios en particular no es beneficiosa para U2. A pesar de ello, ZF cancela casi al completo la ganancia del *eavesdropper* (de 8.46006 a 0.0730011), eliminando casi toda la probabilidad de que la comunicación pudiese ser interceptada por el *eavesdropper*.

MRC reduce más la ganancia en la dirección de U1 (-85º) que ZF (1.55078 Vs. 1.67841), y esto se debe al comportamiento del filtro, ya que no ha sido configurado para dirigir la cancelación de ganancia hacia U1. Consecuentemente, aplicando ZF, U2 sufrirá mayor interferencia, aunque la diferencia sea mínima.

Los valores de SINR para los usuarios U1 y U2, LINR para el *eavesdropper*, y capacidad secreta se muestran en la Tabla 4-4 en bps, aplicando el filtro MRC.

	U1	**U2**
SINR MRC [bps]	0.64984	582.8092
LINR MRC [bps]	3.6214	6.8885
CAPACIDAD SECRETA MRC	0	6.2096
$\sum C_S$	6.2096	

Tabla 4-4: Comparativa entre usuarios aplicando MRC [Elaboración propia].

Como se puede comprobar en la Tabla 4-4, en el entorno de U1, la LINR obtenida supera a la SINR (3.6214 Vs. 0.64984), como era esperado visualizando los resultados de la Figura 4-23. El factor determinante es la interferencia causada por U2, ya que reduce casi al completo la SINR de U1. En consecuencia, la LINR puede superar con facilidad a la SINR obteniendo un valor bajo; y la capacidad secreta es nula.

Por otro lado, en el entorno de U2, la SINR obtenida supera claramente a la SINR (582.8092 Vs. 6.8885), de acuerdo con lo esperado visualizando la Figura 4-24. Al ser el usuario con mayor ganancia inicialmente, MRC potencia beneficiosamente su dirección angular (-7º), dejando en segundo plano al resto de usuarios (U1 y E), los cuales tienen valores de ganancia que están muy por debajo del que obtiene U2. En consecuencia, la capacidad secreta es positiva, con un valor válido (6.2096) para evitar en gran medida la intercepción de señal por parte del *eavesdropper* y la interferencia por parte de U1.

El cómputo de capacidades secretas resulta positivo (6.2096) por la importancia y gran seguridad que ofrece el entorno de U2 al sistema, pero el objetivo se consigue parcialmente; ya que la comunicación en el entorno de U1 no es seguro.

Los valores de SINR para los usuarios U1 y U2, LINR para el *eavesdropper*, y capacidad secreta se muestran en la Tabla 4-5 en bps, aplicando el filtro ZF.

	U1	**U2**
SINR ZF [bps]	1.6688	225.7981
LINR ZF [bps]	0.4957	0.6837
CAPACIDAD SECRETA ZF	0.83535	7.0736
$\sum C_s$	7.909	

Tabla 4-5: Comparativa entre usuarios aplicando ZF [Elaboración propia].

Como se puede comprobar en la Tabla 4-5, en el entorno de U1, la SINR obtenida supera a la LINR (1.6688 Vs. 0.4957), como era esperado visualizando los resultados de la Figura 4-23. El factor determinante es que se ha conseguido evitar suficientemente la interferencia causada por U2, al contrario que MRC en este entorno. Además, se obtiene una leve LINR, que permite que aún con poca SINR, se consiga un valor positivo de capacidad secreta (0.83535).

En consecuencia, el entorno de U1 se convierte en un entorno seguro, ya que es poco probable que el *eavesdropper* intercepte la comunicación entre U1 y U2, y la interferencia causada por U2 no es suficiente como para afectar negativamente a la capacidad secreta.

Por otro lado, en el entorno de U2, la SINR obtenida supera claramente a la LINR (225.7981 Vs. 0.6837), de acuerdo con lo esperado visualizando la Figura 4-24. Cabe destacar que a pesar de obtener menor SINR que aplicando MRC (582.8092), ha habido una mayor reducción de LINR (de 6.8885 a 0.6837); por lo que la capacidad secreta aplicando ZF es superior (7.0736) que aplicando MRC (6.2096). En consecuencia, con el alto valor obtenido de capacidad secreta, se puede evitar en gran medida la intercepción de señal por parte del *eavesdropper* y la interferencia por parte de U1.

El cómputo de capacidades secretas resulta positivo (7.909) y muy superior al obtenido aplicando MRC (4.7236), por lo que continúa predominando la importancia y gran seguridad que ofrece el entorno de U2 al sistema, pero el objetivo se consigue completamente; ya que la comunicación en el entorno de U1 es seguro, aunque en menor medida que el entorno de U2.

La conclusión general en este experimento es que en un escenario en el que interviene más de un usuario legítimo, cobra severa importancia tanto la interferencia existente, como la disposición espacial de los usuarios; y el empleo del filtro ZF consigue mejores resultados, en cuanto a capacidad secreta se refiere, que el empleo del filtro MRC.

4.2.2 Segundo experimento

En el segundo experimento, los usuarios E, U1 y U2 se encuentran en los ángulos 1º, -85º y 23º, respectivamente, como se muestra en la Figura 4-25.

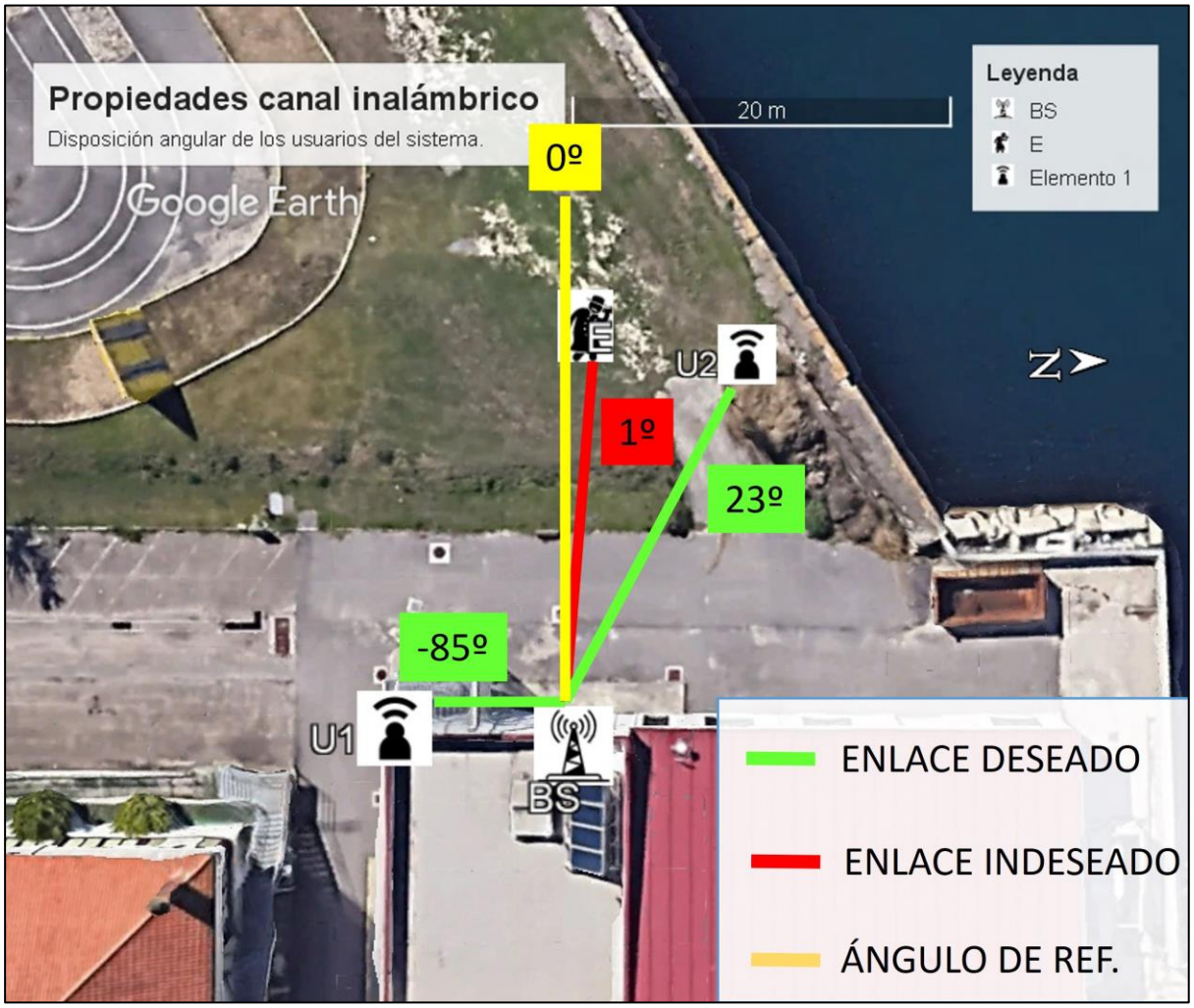


Figura 4-25: Vista en planta de posición angular de los usuarios [Elaboración propia].

Al modificar el escenario, es necesario volver a corroborar que las tres señales se reciben correctamente; y estas son: 498000000 Hz en el caso de U1, 499595000 Hz en el caso del *eavesdropper* (E) y 496395000 Hz en el caso de U2 (comprobables en la Figura 4-26).

La situación que se analizará en este experimento es de mayor complejidad al anterior, debido a dos factores. El primero es que, analizando la Figura 4-26, en este caso es el *eavesdropper* es el usuario que ha sido recibido con mayor ganancia (38.2584); por lo que esta situación es más desfavorable, en cuanto a potencia de transmisión por parte de los usuarios se refiere.

El segundo factor es que, en este caso, el *eavesdropper* se encuentra en la parte central (entre los dos usuarios legítimos) del escenario; por lo que forzará al filtro ZF a responder de forma no simétrica en cuanto a curvas de ganancia, en vez de uno como se ha visto en la mayoría de los casos anteriores. También es reseñable que la distancia angular entre el *eavesdropper* y el usuario más próximo es la menor (22º) de todos los experimentos realizados.

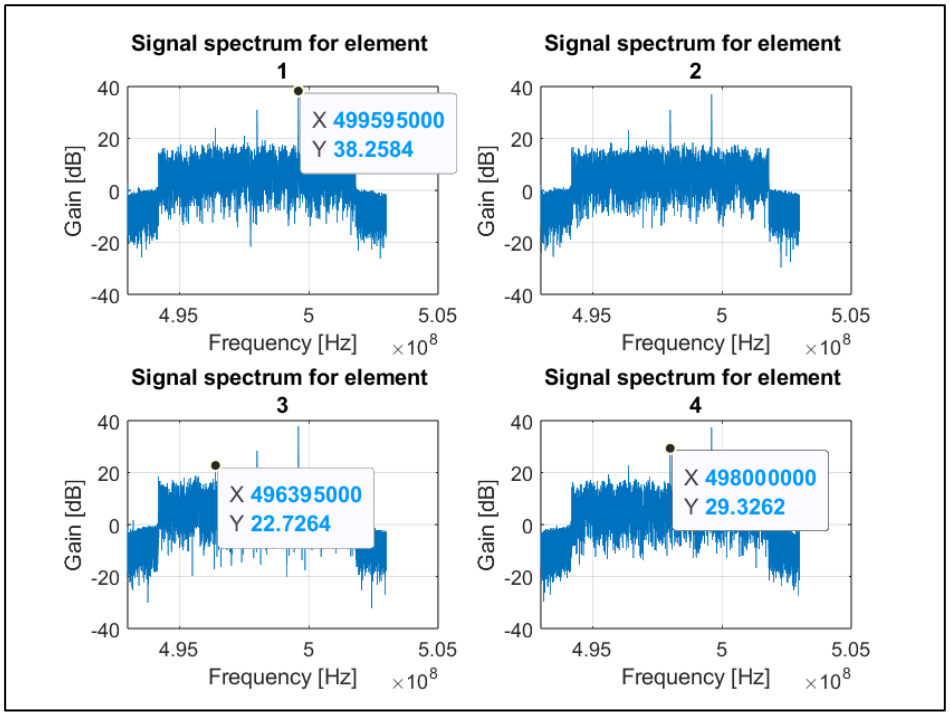


Figura 4-26: Recepción de datos para cada antena de la BS [Elaboración propia].

En la Figura 4-27, Figura 4-28 y Figura 4-29 se muestran las ganancias de cada usuario en el dominio angular. Como se puede comprobar, la mayor ganancia se recibe por parte del eavesdropper (1311.51), seguido de U1 (39.0797) y por último, U2 (1.59425).

A diferencia del anterior experimento, los usuarios legítimos cuentan con una gran desventaja (sobre todo U2), en cuanto a potencia de transmisión se refiere. Es por ello por lo que se tratará de solventar la situación mediante los filtros empleados en este Proyecto.

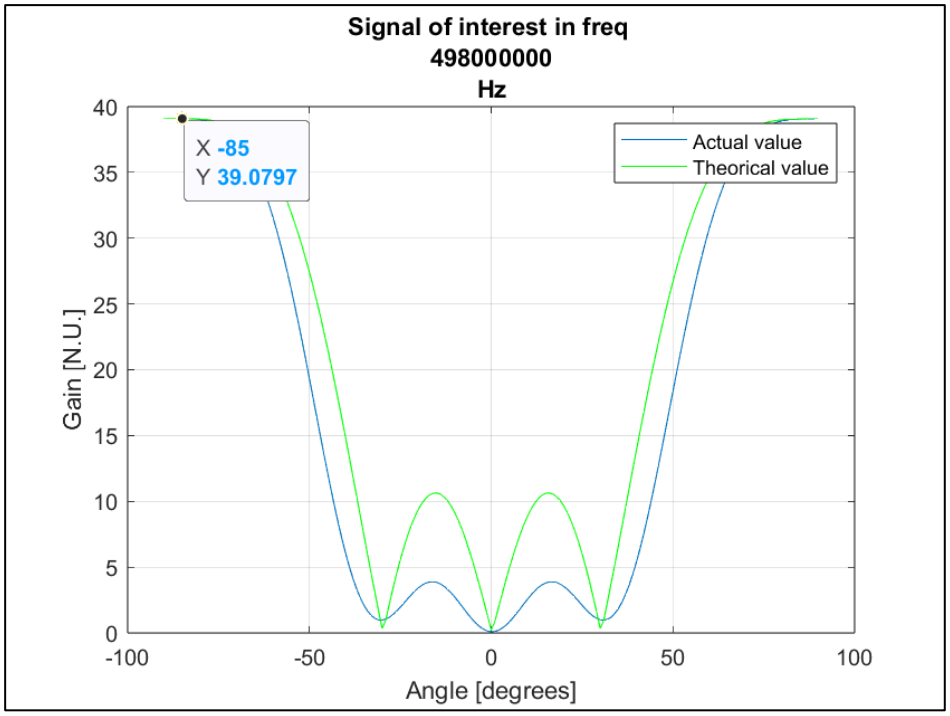


Figura 4-27: Ganancia del *array* de antenas para frecuencia del primer usuario legítimo, U1 [Elaboración propia].

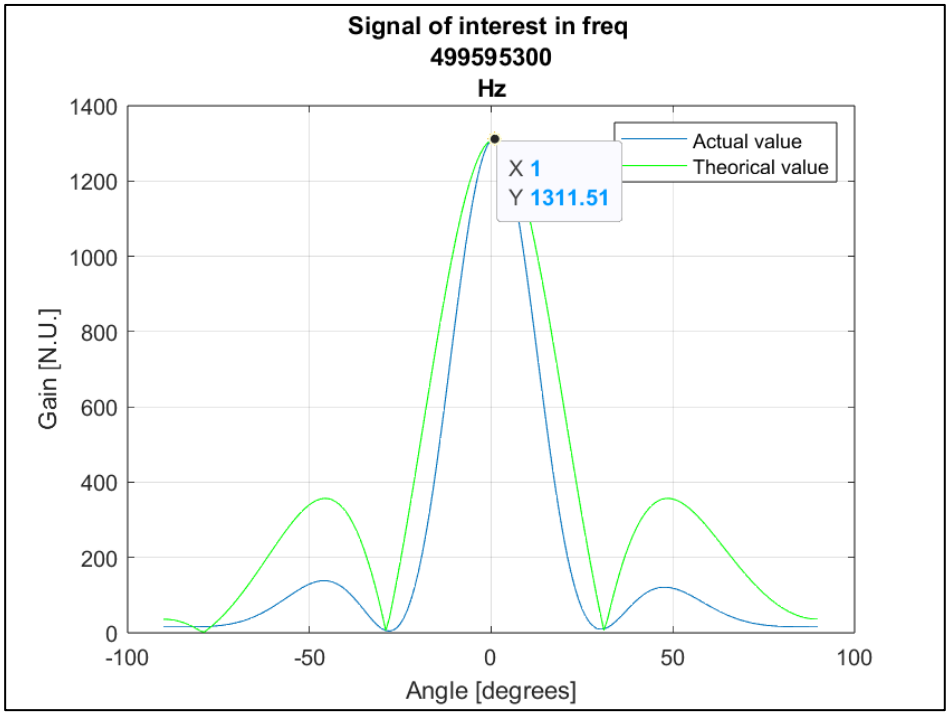


Figura 4-28: Ganancia del *array* de antenas para frecuencia del *eavesdropper* [Elaboración propia].

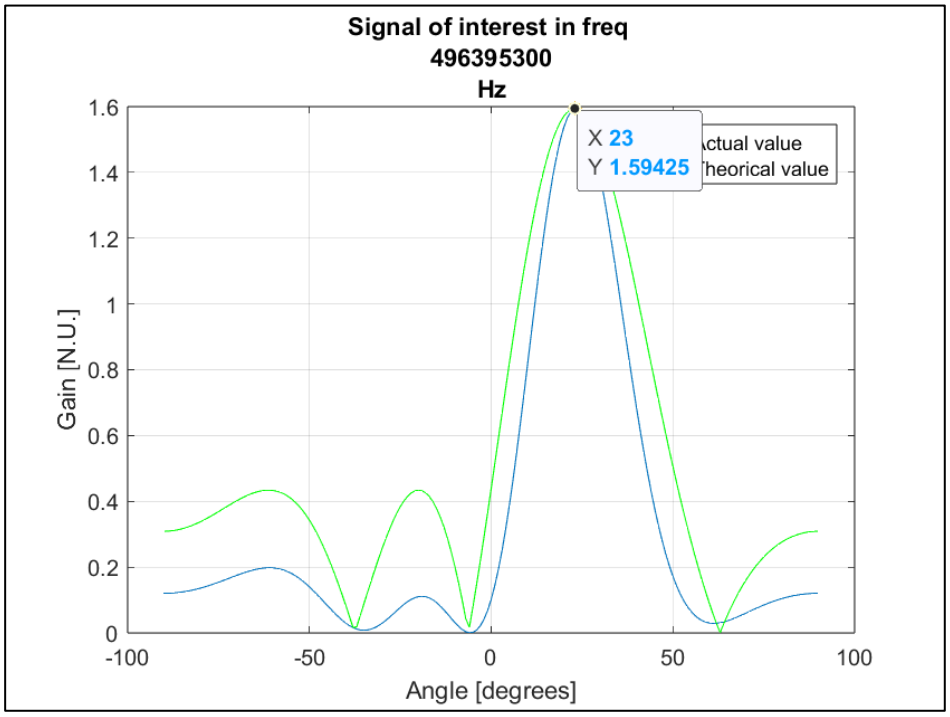


Figura 4-29: Ganancia del *array* de antenas para frecuencia del segundo usuario legítimo, U2 [Elaboración propia].

En este experimento se han aplicado los filtros MRC y ZF de igual manera que en el anterior experimento, dos filtros de cada tipo a cada usuario. Los filtros ZF han sido configurado de forma distinta, permitiendo el contraste de distintas configuraciones

El filtro MRC aplicado a U1 ha sido programado para potenciar la ganancia en la dirección angular -85º, mientras que el segundo filtro MRC aplicado a U2 ha sido configurado para el mismo propósito en la dirección angular 23º.

Por otra parte, el filtro ZF aplicado a U1 ha sido configurado para aumentar la ganancia en la dirección angular -85º y atenuar la dirección angular 1º y 23º, con el propósito de evitar la interferencia que causaría U2 e intentar cancelar la señal recibida por parte del *eavesdropper*.

Para U2, ZF ha sido configurado para aumentar la ganancia en la dirección angular 23º, y para intentar atenuar la dirección angular 85º y 1º, con el propósito de evitar la interferencia que causaría U1 e intentar cancelar la señal recibida por parte del *eavesdropper*; y a su vez no cancelar toda la dirección angular que separa a ambos usuarios, U1 y E. En la Figura 4-30 y Figura 4-31 se muestran las respuestas de los filtros ZF para ambos usuarios.

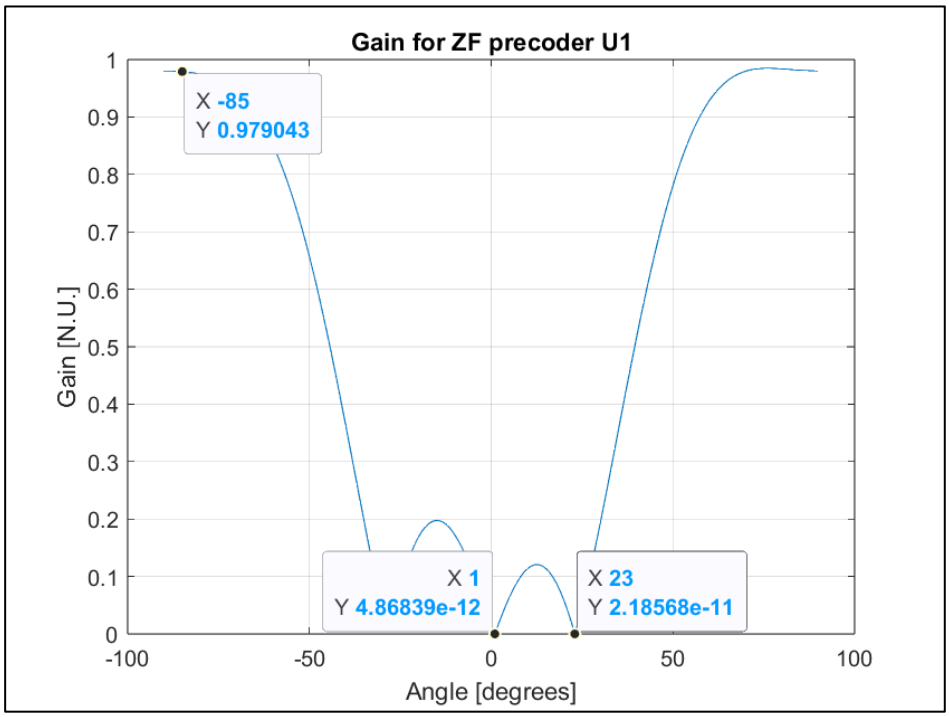


Figura 4-30: Ganancia obtenida al aplicar ZF al U1, en el dominio angular [Elaboración propia].

En el caso de U1, en la Figura 4-30, se obtiene un resultado beneficioso, ya que ZF reduce en gran medida las dos direcciones que se habían configurado, mostrando compatibilidad con la situación. La ganancia de U1 (0.979043) supera a la obtenida para el anterior experimento (0.741315), por lo que los resultados son más ventajosos en todas las direcciones angulares.

En el caso de U2, en la Figura 4-31, el resultado es menos exitoso que para U1; pero a pesar de ello se consigue superar la principal dificultad, que era configurar el filtro de manera que se cancelaran dos direcciones entre las que se pretendía que existiese un lóbulo de ganancia de forma que, si fuera necesario, o un usuario nuevo se introduce en el sistema y se coloca en dicha dirección, o un usuario legítimo se coloca en dicha dirección.

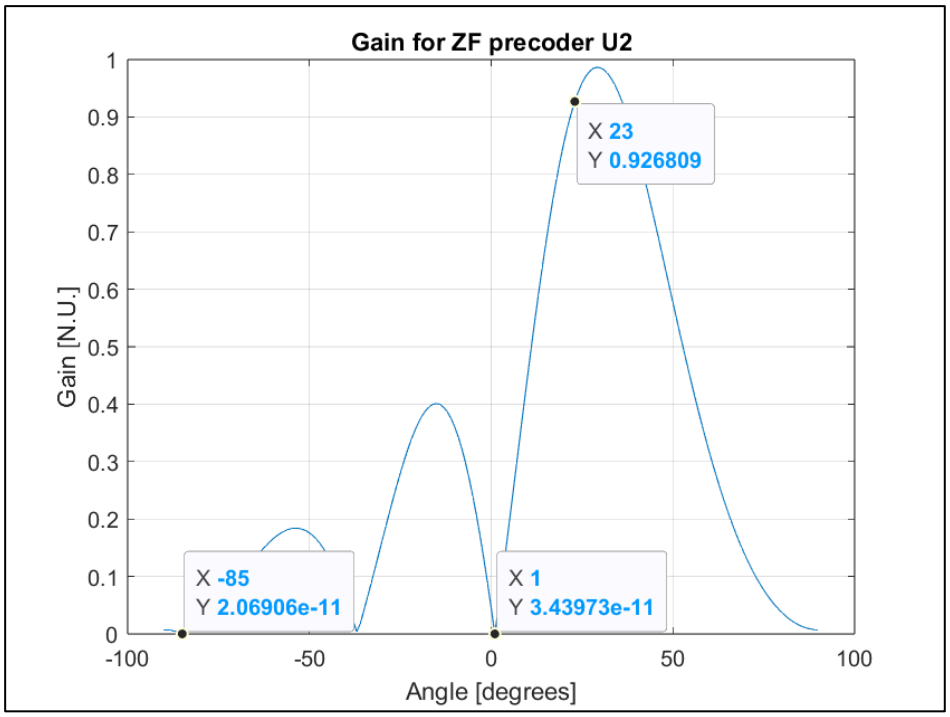


Figura 4-31: Ganancia obtenida al aplicar ZF al U2, en el dominio angular [Elaboración propia].

En la Figura 4-32 se muestra la comparación entre la aplicación de MRC y ZF para U1.

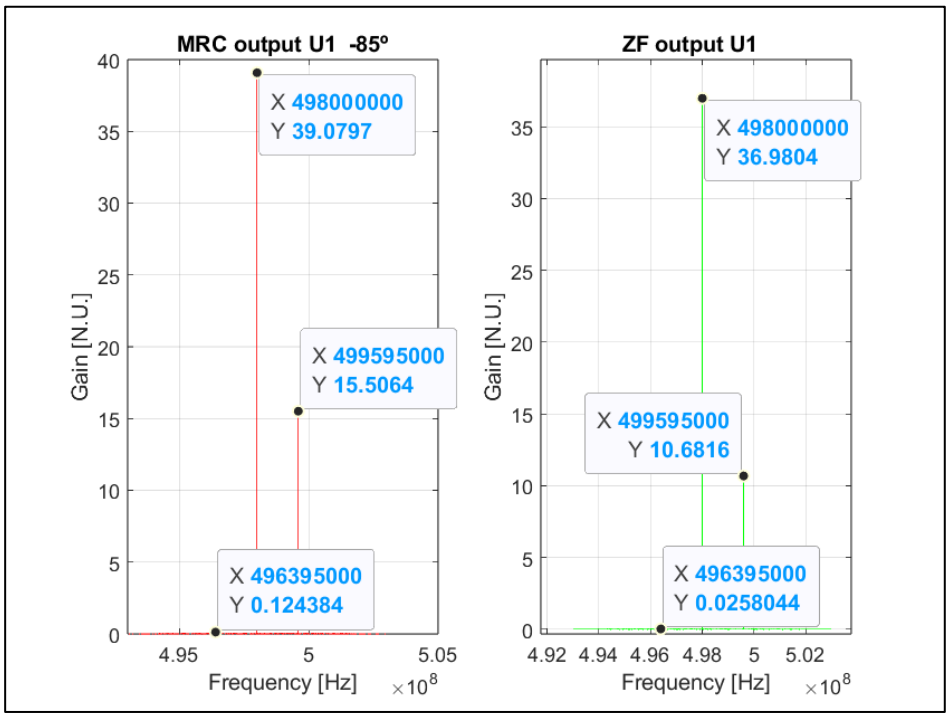


Figura 4-32: Ganancias obtenidas por cada filtro aplicado a U1 en el espectro frecuencial [Elaboración propia].

Recordemos la asignación de usuarios por frecuencias: 498000000 Hz en el caso de U1, 499595000 Hz en el caso de U2 y 496394000 Hz en el caso del *eavesdropper* (E). A continuación, se realizará un análisis del entorno de U1.

Como se puede comprobar en la Figura 4-32, la aplicación de MRC para U1 (-85º) provoca que se reciba con gran potencia su señal (39.0797), y a su vez se ha atenuado considerablemente la señal del *eavesdropper* (de 1311.51 a 15.5064), por lo que se puede conseguir determinada capacidad secreta. La señal de U2 ha sido atenuada casi al completo (de 1.59425 a 0.124384), por lo que causará leve interferencia a U1 y ayudará a que la SINR aumente.

Por otra parte, al aplicar ZF, se atenúa muy levemente la señal de U1 de 39.0797 a 36.9804, y se atenúa en mayor medida la señal del *eavesdropper* (10.6816). En cuanto a U2, su señal es atenuada en mayor medida que empleando ZF (0.0258044), por lo que el impacto en la SINR será más ventajoso que empleando MRC. Aparentemente, el resultado de capacidad secreta mejorará el obtenido mediante MRC.

En la Figura 4-33 se muestran los resultados aplicando ambos filtros para U2.

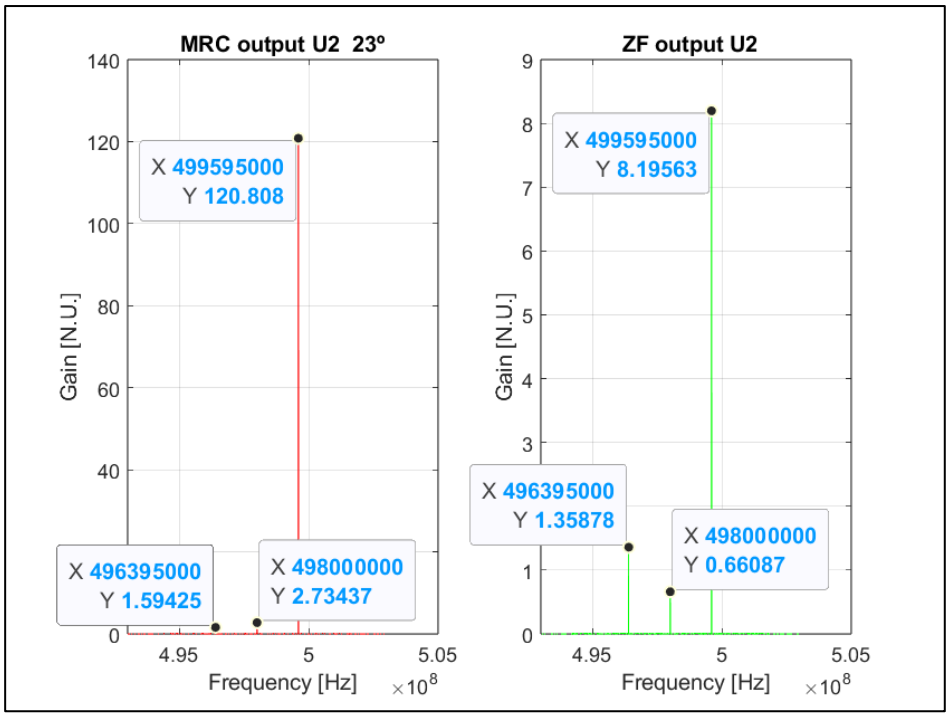


Figura 4-33: Ganancias obtenidas por cada filtro aplicado a U2 en el espectro frecuencial [Elaboración propia].

Es necesario recordar la reducida potencia de transmisión de U2 (1.59425). Como se puede comprobar en la Figura 4-33, empleando MRC, la potencia con la que se recibe la señal del *eavesdropper* es muy superior al resto (120.808). Este resultado se debe a la poca potencia del usuario que se intenta potenciar, U2, y a la cercanía del *eavesdropper*, que se ve suficientemente beneficiado de la situación, a pesar de que su señal ha sido atenuada de 1311.51 a 120.808. Como aspecto positivo, la interferencia que causa U1 también es reducida (de 39.0797 a 2.73437) y afectará positivamente a la SINR.

Por otra parte, al emplear ZF se consigue minimizar la diferencia de ventaja que tenía el *eavesdropper*. Como se puede comprobar, la señal del *eavesdropper* es atenuada de 1311.51 a 8.19563; un valor muy considerable pero que no consigue el objetivo. Como aspecto positivo, el empleo de ZF ha reducido en gran medida la interferencia de U1 y favorecerá la SINR de U2.

A pesar de no conseguir mayor potencia por parte de las señales de los usuarios legítimos, la mejoría que aportan los dos filtros al sistema es reseñable.

Los valores de SINR para los usuarios U1 y U2, LINR para el *eavesdropper*, y capacidad secreta se muestran en la Tabla 4-6 en bps, aplicando el filtro MRC.

	U1	**U2**
SINR MRC [bps]	171.2311	0.56171
LINR MRC [bps]	149.3233	1163.3559
CAPACIDAD SECRETA MRC	0.19628	0
$\sum C_s$	0.19628	

Tabla 4-6: Comparativa entre usuarios aplicando MRC [Elaboración propia].

Como se puede comprobar en la Tabla 4-6, al aplicar MRC en el entorno de U1 se ha conseguido obtener un valor de SINR superior a la LINR (171.2311 Vs. 149.3233), por lo que la capacidad secreta resulta ligeramente positiva. Conociendo el contexto y la ventaja con la que contaba el *eavesdropper*, el filtro MRC resuelve el problema de forma adecuada y permite la comunicación entre la BS y U1 con probabilidad de que el *eavesdropper* no intercepte la señal, un resultado de capacidad secreta óptimo (0.19628).

Por otra parte, en el entorno de U2, la gran desventaja con la que cuenta, en términos de potencia de transmisión, no puede ser revertida; ya que la SINR es muy reducida (0.56171) debido a que se recibe demasiada interferencia por parte de U1, y la LINR es absolutamente superior (1163.3559) a dicha SINR. En consecuencia, el entorno de U2 es un entorno no seguro y muy interferido, con capacidad secreta nula.

La capacidad secreta del sistema se ve gravemente afectada por el entorno de U2, pero el entorno de U1 es seguro y poco interferido. En conclusión, el objetivo ha sido conseguido parcialmente empleando MRC.

Los valores de SINR para los usuarios U1 y U2, LINR para el *eavesdropper*, y capacidad secreta se muestran en la Tabla 4-7 en bps, aplicando el filtro ZF.

	U1	**U2**
SINR ZF [bps]	285.235	1.7768
LINR ZF [bps]	102.861	78.9221
CAPACIDAD SECRETA ZF	1.4625	0
$\sum C_s$	1.4625	

Tabla 4-7: Comparativa entre usuarios aplicando ZF [Elaboración propia].

Como se puede comprobar en la Tabla 4-7, al aplicar ZF en el entorno de U1 se ha conseguido obtener un valor de SINR superior a la LINR (285.235 Vs. 102.861), y la diferencia es mayor que al aplicar MRC. Esto implica que se consigue una beneficiosa capacidad secreta en el entorno de U1 (1.4625), ya que, en comparación con el empleo de MRC, se ha conseguido tanto reducir la interferencia de U2 como la LINR del *eavesdropper*.

Por otra parte, en el entorno de U2, el resultado no consigue capacidad secreta positiva debido a que las restricciones de ZF no han sido suficientes como para revertir la situación que se había dado aplicando MRC. Sin embargo, se mejora muy notoriamente la situación, ya que la LINR resultada de aplicar MRC ha sido reducida de 1163.3559 a 78.9221 bps, y la interferencia que causa U1 es reducida considerablemente, de manera que el valor de SINR obtenido es mayor que empleando MRC (0.56171).

De nuevo, la capacidad secreta se ve mermada por el entorno de U2, pero se ha conseguido un escenario más seguro y menos interferido en el entorno de U1, de manera que se permite la comunicación entre la BS y U1 evitando en gran medida que el *eavesdropper* intercepte la señal.

En conclusión, el segundo experimento consigue parcialmente el objetivo propuesto en un escenario muy desfavorable, de manera que las medidas adoptadas en el experimento pueden tener éxito rotundo en una situación más igualitaria.

En cuanto a este tipo de escenario, las condiciones en las que se realizan los experimentos son muy desfavorables para los objetivos marcados, ya que se está evaluando el *downlink* mediante un *uplink* y, mientras que en el *downlink* las potencias de los usuarios se controlar de forma centralizada por el transmisor, en los experimentos realizados vienen determinadas por el *hardware* disponible en el laboratorio. Es decir, estamos evaluando una situación límite y muy conservadora si se compara con el rendimiento que se puede obtener para el sistema planteado.

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones

En este apartado se resumirán las conclusiones extraídas del desarrollo del Proyecto, así como de los resultados y validación de este.

5.1.1 Simulaciones en Matlab y análisis teórico

El ámbito de investigación de este Proyecto es de cierta complejidad, pero la aproximación hacia los experimentos reales mediante simulaciones en *Matlab* es un método que permite anticipar los resultados que se obtendrán en los escenarios reales, ya que la programación en *Matlab* es más sencilla de interpretar y manipular, y el completo entendimiento del funcionamiento de los sistemas MIMO requiere de la realización de pruebas empleando una gran variedad de parámetros y variables que, en un experimento real, puede suponer poco práctico o incluso imposible de llevar a cabo.

Dichas simulaciones se realizaron para demostrar tanto el aumento de capacidad a medida que aumenta el número de elementos transmisores, como las diferencias que conlleva emplear un *precoder* MRT, o un ZF.

Por lo tanto, la conclusión extraída es que, salvo en casos particulares, se corrobora la suposición inicial: generalmente, un mayor número de elementos transmisores ayudará a aumentar la capacidad del sistema, permitiendo tanto mayores tasas de transmisión como mayor número de usuarios en un sistema. Además, el empleo de *precoder* ZF es más recomendable que MRT, ya que empleando ZF la tendencia de la capacidad suma del sistema es creciente; y, en un escenario en el que se encuentran usuarios ilegítimos, el empleo de un *precoder* que centra su esfuerzo en cancelar la señal de estos usuarios será más eficaz que MRT.

5.1.2 Experimentos reales

Los experimentos reales se han dividido en dos tipos de escenario: comunicación entre BS y un usuario legítimo, y un *eavesdropper* que trata de interceptar dicha comunicación; y comunicación entre BS y dos usuarios legítimos, y un *eavesdropper* que trata de interceptar ambos canales de comunicación.

Para el primer tipo de escenario, tras realizar tres experimentos alternando tanto las potencias de transmisión de cada usuario como sus posiciones espaciales, se han extraído diferentes conclusiones.

El empleo del filtro MRT en situaciones en las que el *eavesdropper* cuenta con mayor potencia de transmisión que el usuario legítimo, perjudica gravemente a la capacidad secreta, siendo esta baja o nula.

En situaciones contrarias a la anterior, en las que el usuario legítimo cuenta con mayor potencia de transmisión, como es el caso del segundo experimento; emplear ZF puede resultar contraproducente, debido a la posición espacial (como caso particular) de los usuarios o debido a que MRC consigue el efecto buscado y ZF no contribuye a la mejora de este.

Los experimentos realizados basan su éxito en la comparación entre la situación previa, y la misma situación tras aplicar las medidas correspondientes, es decir, el éxito radica en la transformación de un entorno en completa desventaja en un entorno aceptable, con probabilidad de evitar intercepciones e interferencias indeseadas.

Es necesario no confundir el éxito con un entorno completamente seguro y fiable, ya que dichas características pueden conseguirse empleando medios más sofisticados y adquiriendo conocimientos muy avanzados del ámbito.

En conclusión, se han conseguido al completo los objetivos propuestos para este tipo de escenario, estableciendo comunicación entre la BS y el usuario legítimo sin que el *eavesdropper* intercepte la comunicación.

Para el segundo tipo de escenario, tras realizar dos experimentos alternando tanto las potencias de transmisión de cada usuario como sus posiciones espaciales, se han extraído diferentes conclusiones.

El principal problema que supone este tipo de escenario es la aparición de la interferencia entre usuarios legítimos. Este factor es ajeno al *eavesdropper*, por lo que sólo supone una desventaja para los usuarios legítimos y es necesario mitigarla, aumentando el nivel de exigencia del sistema.

La configuración del filtro ZF conlleva mayor dificultad en situaciones en las que se requiere cancelación de señal proveniente de más de una dirección angular. Todas las respuestas de los filtros coinciden en un aspecto: la ganancia máxima que atribuyen es menor que en todos los escenarios con un solo usuario legítimo.

En cuanto al rendimiento del filtro ZF, todos los resultados de capacidad secreta se han maximizado en este tipo de escenario. Esto es debido a la correcta adaptabilidad del filtro, o al no tan beneficioso rendimiento que ofrece el filtro MRC en este tipo de escenarios.

Al igual que en el anterior tipo de escenario, los resultados son exitosos porque corrigen de manera eficaz situaciones muy desfavorables para los usuarios legítimos. El nivel de Seguridad en la Capa Física no es perfecto, ya que para ello sería necesario reducir la LINR a un valor cercano a 0; pero en este Proyecto se establece un nivel de Seguridad en la Capa Física adaptado a los medios y tiempo disponible.

Debido a las dificultades implementadas en este tipo de escenario en comparación con el anterior, en determinados entornos no ha sido posible ofrecer un nivel de Seguridad en la Capa Física válido, pero dichos entornos no constituyen el sistema al completo. De hecho, los resultados desfavorables se han dado en los entornos que más probabilidad de fracaso tenían por condiciones iniciales desfavorables, por lo que los resultados obtenidos son los esperados.

En conclusión, se han conseguido parcialmente los objetivos propuestos para este tipo de escenario, estableciendo comunicación entre la BS y uno o dos usuarios legítimos sin que el *eavesdropper* intercepte dicha comunicación.

5.2 Líneas futuras

A continuación, se plantean líneas futuras complementarias al presente Proyecto.

- Desarrollo de un sistema de comunicaciones MIMO táctico. Este dispositivo, transportable, podría suponer una revolución en el sector de Defensa, al implementar un sistema con tasas de transmisión de datos superiores a las presentes en los equipos de comunicaciones actuales, así como un nuevo ámbito de seguridad: la Seguridad en la Capa Física.

- Creación de simulador de comunicaciones manipulable en *software*, ofreciendo una interfaz interpretable y sencilla, en la que personal militar sea capaz de realizar simulaciones de situaciones tácticas, así como identificar el grado de seguridad del que disponen; con el propósito de mejorar la percepción de la capacidad de las comunicaciones en distintas situaciones de planeamiento.

- Tratar de conseguir los medios *hardware* necesarios para poder realizar experimentos en un *downlink* real, sin tener que recurrir a la dualidad. Esto proporcionará resultados más cercanos a una situación práctica y, a la vista de los experimentos realizados, unas capacidades secretas más elevadas que en los casos evaluados.

- Empleo de Múltiples Antenas en los transmisores y receptores, de manera que se pueda implementar el empleo de *precoding* en la realidad. De esta manera, los resultados de capacidad secreta podrían ser más altos que los obtenidos en este Proyecto, ya que se combinarían técnicas de *precoding* y de filtrado (como en este Proyecto).

- Realizar tantos experimentos como sea necesario para estandarizar el funcionamiento de los medios empleados en este Proyecto, en cualquier situación.

6 BIBLIOGRAFÍA

[1] D. W. K. W. H. G. H.-H. C. Xiaoming Chen, «A Survey on Multiple-Antenna Techniques,» *IEEE*, vol. 19, nº 2, p. 27, 2017.

[2] INE, «INE,» [En línea]. Available: https://www.ine.es/index.htm. [Último acceso: 16 enero 2024].

[3] R. F. Heile, IEEE Std 802.15.4™-2011, New York: IEEE, 2011.

[4] J. W. R. R. S. S. M. Dorothy V. Stanley, IEEE Std 802 Part 11: Wireless LAN Medium Access Control, New York: IEEE, 2020.

[5] YTD2525, «YTD2525,» Wordpress, 2020. [En línea]. Available: https://ytd2525.wordpress.com/. [Último acceso: 16 enero 2024].

[6] T. Li, «Michigan State University, Dept. Electrical and Computer Engineering,» [En línea]. Available: egr.msu.edu.

[7] M. K. Saini, «Difference between Analog and Digital Signal,» 2 septiembre 2023. [En línea]. Available: https://www.tutorialspoint.com/difference-between-analog-and-digital-signal. [Último acceso: 17 enero 2024].

[8] P. M. G. Bernard Mulgrew, Digital Signal Processing: Concepts and Applications, Bristol: J. W. Arrowsmith Ltd, 2003.

[9] M. K. Saini, «Difference between Analog Communication and Digital Communication,» 2 septiembre 2023. [En línea]. Available: https://www.tutorialspoint.com/difference-between-analog-communication-and-digital-communication. [Último acceso: 17 enero 2024].

[10] TechTarget, «TechTarget,» [En línea]. Available: https://www.techtarget.com/whatis/definition/time-division-multiplexing-TDM. [Último acceso: 18 enero 2024].

[11] A. F. Molisch, Wireless Communications, Chennai, India: Laserwords Private Limited, 2011.

[12] OTAN, ACP-176 SP NAVY SUPP-2, 2017.

[13] M. d. A. E. y. T. Digital, «Orden ETD/1449/2021, de 16 de diciembre, por la que se aprueba el Cuadro Nacional de Atribución de Frecuencias.,» BOE, 2021.

[14] J. M. H. Rábanos, Transmisión por radio, Madrid: PUBLIDISA, 2013.

[15] C. L. F. S. Álvarez, *Sensores Navales,* 2023.

[16] E. d. Tierra, «Ejército de Tierra,» Defensa, [En línea]. Available: https://ejercito.defensa.gob.es/materiales/transmisiones/Harris_5800.html. [Último acceso: 27 febrero 2024].

[17] HARRIS, «l3harris,» HARRIS, [En línea]. Available: https://www.l3harris.com/all-capabilities/an-prc-160v-wideband-hf-vhf-manpack-radio. [Último acceso: 27 febrero 2024].

[18] J. Laguna, «Zaguan (CUD AGM),» 2016. [En línea]. Available: https://zaguan.unizar.es/record/99037?ln=es. [Último acceso: 27 febrero 2024].

[19] EMAD, «Twitter/X,» Meta, 11 marzo 2019. [En línea]. Available: https://twitter.com/EMADmde/status/1105111656340865025. [Último acceso: 2 febrero 2024].

[20] «Federación de asociaciones de Veteranos Boinas Verdes Españoles,» [En línea]. Available: https://fedavbve.com/material-y-armamento/.

[21] A. Goldsmith, Wireless Communications, Cambridge University Press, 2020.

[22] I. Universidad de Verona, *Gaussian Channel introduction,* Verona.

[23] J. Stone, Principles of Neural Information Theory: Computational Neuroscience and Metabolic Efficiency, Sheffield: Sebtel Press, 2018.

[24] D.-I. M. Joham, MIMO Systems, Munich: Technische Universit¨at M ¨unchen, 2014.

[25] J. P. G. Coma, *Quality of Service Optimization in the Broadcast Channel with Imperfect Transmit Channel State Information,* A Coruña: Universidad de A Coruña, 2015.

[26] Hussam, «MIMO Channel Capacity,» 2024. [En línea]. Available: https://www.mathworks.com/matlabcentral/fileexchange/30588-mimo-channel-capacity. [Último acceso: 21 febrero 2024].

[27] L.-L. Yang, «A Zero-Forcing Multiuser Transmitter Preprocessing Scheme for Downlink Communications,» *IEEE,* vol. 56, nº 6, p. 4, 2008.

[28] F. C. Vilar, «IMPLEMENTATION OF ZERO FORCING AND MMSE EQUALIZATION TECHNIQUES IN OFDM,» Universidad de Fortaleza, Fortaleza, 2014.

[29] T. K. Y. Lo, «Maximum Ratio Transmission,» *IEEE TRANSACTIONS ON COMMUNICATIONS,* vol. 47, nº 10, p. 4, 1999.

[30] J. L. Q. H. K. G. Q. Claudio valencia, «SEGURIDAD EN LA CAPA FÍSICA Y TEORÍA DE JUEGOS EN REDES DE SENSORES INALÁMBRICOS: ACTUALIDAD Y PERSPECTIVA.,» *CONGRESO INTERNACIONAL DE TELECOMUNICACIONES SENACITEL,* 2014.

[31] J. X. N. L. Xiaofeng Tao, «Artificial Noise Assisted Communication in the Multiuser Downlink: Optimal Power Allocation,» *IEEE,* vol. 19, nº 2, p. 4, 2015.

[32] G. J. A.-L. F. J. L.-M. José P. González-Coma, «Leakage Subspace Precoding and Scheduling for Physical Layer Security in Multi-User XL-MIMO Systems,» *IEEE COMMUNICATIONS LETTERS,* vol. 27, nº 2, p. 5, 2023.

[33] M. E. J. Y. A. R. I. B. C. Giovanni Geraci, «Secrecy Sum-Rates for Multi-User MIMO Regularized Channel Inversion Precoding,» *IEEE TRANSACTIONS ON COMMUNICATIONS,* vol. 60, nº 11, p. 11, 2012.

[34] THA, «THA,» [En línea]. Available: https://www.tha.de/en/library/ADALM-PLUTO.html. [Último acceso: 24 marzo 2024].

[35] [En línea]. Available: https://es.alasartech-security.com/software-defined-radio/hackrf-one/hackrf-one-h1.html. [Último acceso: 24 marzo 2024].

[36] M. R. A. K. Yue Rong, «On Uplink-Downlink Duality of Multi-Hop MIMO Relay Channel,» *IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS,* vol. 10, nº 6, p. 9, 2011.

[37] M. N. N. I. A. P. L. Abdolrasoul Sakhaei Gharagezlou, «Secrecy Sum Rate Analysis and Power Allocation,» *IEEE,* p. 5, 2022.

[38] C. B. P. A. L. S. M. H. Quentin H. Spencer, «An Introduction to the Multi-User MIMO Downlink,» *IEEE Communications Magazine,* p. 8, Octubre 2004.

[39] M. V. Muñoz, «Una historia de las telecomunicaciones navales,» *Revista de Marina,* vol. 120, nº 875, p. 10, 2003.

ANEXO I: IMPLICACIONES SOCIALES, Y/O ECONÓMICAS, Y/O AMBIENTALES

La investigación sobre la maximización de la capacidad secreta en sistemas de comunicaciones MIMO tiene un impacto relevante en los ámbitos social, medioambiental y económico.

Socialmente, este Proyecto contribuye directamente a mejorar la privacidad y seguridad en las comunicaciones, no solo en el sector de Defensa, sino también en otros campos como la protección de datos sensibles. incrementar la seguridad de las comunicaciones en entornos sensibles puede tener un impacto vital en la protección de la privacidad individual y en la prevención de posibles amenazas en el ciberespacio.

En cuanto al impacto medioambiental, el desarrollo de tecnologías que permitan maximizar la capacidad secreta en sistemas de comunicaciones MIMO puede tener efectos beneficiosos en la eficiencia energética de las redes de comunicación. La optimización de la transmisión de datos puede reducir el consumo de energía y los daños medioambientales asociados a la infraestructura de comunicaciones, factor que contribuye a la mitigación del cambio climático y a la sostenibilidad ambiental.

En el ámbito económico, este Proyecto puede impulsar el desarrollo tecnológico y la innovación en el sector de la seguridad de las comunicaciones. Las empresas dedicadas a la implementación de tecnologías seguras y eficientes pueden ganar una ventaja competitiva en el mercado global. Además, el aumento de la demanda de expertos en seguridad de la información y comunicaciones puede generar oportunidades de empleo y contribuir al crecimiento económico en este sector.

En resumen, la maximización de la capacidad secreta en sistemas de comunicaciones MIMO tiene un impacto significativo en los aspectos social, medioambiental y económico. Mejorar la seguridad y eficiencia de las comunicaciones no solo beneficia la protección de la privacidad y la seguridad de la información, sino que también contribuye a la conservación del medio ambiente y al desarrollo económico a través de la innovación tecnológica.

ANEXO II: REFLEXIONES ÉTICAS Y SOCIALES

La investigación sobre la mejora de la seguridad en comunicaciones mediante sistemas MIMO plantea cuestiones éticas y sociales significativas.

Inicialmente, se debe tener en cuenta el equilibrio entre la seguridad y la privacidad en las comunicaciones. La implementación de medidas de seguridad debe mantener la integridad de la información sin violar la privacidad de los individuos ni discriminar su libertad de expresión.

Además, se debe tener en cuenta la igualdad en el acceso a estas tecnologías. Es imprescindible que los avances en seguridad estén disponibles de manera igualitaria para todos los usuarios, evitando así la creación de desigualdades sociales y la exclusión de determinados grupos.

Otro aspecto vital es el impacto en la seguridad nacional y las relaciones internacionales. Por una parte, la mejora en la seguridad puede beneficiar a una nación; pero también puede generar tensiones con otras que perciban estas tecnologías como una amenaza potencial.

En conclusión, la seguridad en comunicaciones mediante sistemas MIMO plantea desafíos importantes, en cuanto a ética. Es fundamental considerar estos desafíos para garantizar un uso justo y responsable de estas tecnologías en beneficio de la sociedad en su conjunto.

ANEXO III: CÓDIGO PRINCIPAL CAPACIDAD SUMA

```
clear all;
close all
clc

A=4;  %ANTENAS TRANSMISORAS --> MODIFICABLE
U=6;  %NÚMERO DE USUARIOS --> MODIFICABLE
nexperiments = 10000; %NÚMERO DE EXPERIMENTOS PARA PROMEDIAR
SNRdB = 0:25;
SNR = 10.^(SNRdB/10);

nusers=1:U;

MISO_P = zeros(A,U);
MISO_H = zeros(A,U);
C_MISO = zeros(nexperiments,U);
C_SUMA_MISO = zeros(1,length(SNRdB));

for i=1:length(SNR)

    for n=1:nexperiments

        theta = rand(1,U)*pi; % ÁNGULO DE INCISIÓN DE LA ONDA --> MODIFICABLE

        for k = 1:U
            MISO_H(:,k) = MISOchannel(A,theta(k));
          % MISO_P(:,k) = MISOchannel(A,theta(k)); %DESCOMENTAR PARA APLICAR
        end

          % MISO_P = ZFprecoder(MISO_H); %DESCOMENTAR PARA APLICAR

        SINR=SINR_DL(MISO_H,MISO_P,1/SNR(i));

        for Q = 1:U

            C_MISO(n,Q) = log2(1+ SINR(:,Q));

        end

    end

    C_SUMA_MISO(i) = sum (mean(C_MISO,1));
end

plot(C_SUMA_MISO)

hold on;
xlabel('SNR (dB)')
ylabel('Capacidad Suma (b/s/Hz)');
title('Capacidad Suma Vs. SNR (dB)');
grid on;
```

Published with MATLAB® R2023b

ANEXO IV: FUNCIÓN GENERADORA DE CANAL (*MISOCHANNEL*)

```
 function [a] = MISOchannel(M,theta)
% M número de antenas
% theta ángulo de incisión de frente de onda, en radianes
% generación de canal
m =-(M-1)/2:(M-1)/2;
a = 1/sqrt(M)*exp(-1.j*pi*m*sin(theta)).';
```

Published with MATLAB® R2023b

ANEXO V: FUNCIÓN CALCULADORA DE SINR (*SINR_DL*)

```
function [SINR] = SINR_DL (H,P,N)
% H multi-user channel vector A x U
% P user precoding A x U
% N noise power

[~,U] = size(H);
SINR = zeros(1,U);
for u=1:U
    x = N;
    for j=1:U
        if (u~=j)
            x = x + abs(P(:,j)'*H(:,u))^2;
        end
    end
    SINR(u) = abs(P(:,u)'*H(:,u))^2/x;
end
```

Published with MATLAB® R2023b

ANEXO VI: FUNCIÓN CALCULADORA DE *PRECODING* (*ZFPRECODER*)

```
function [MISO_P] = ZFprecoder(MISO_H)
% MISO_H MxU multiuser channel matrix
[M,U] = size(MISO_H);
A = MISO_H/(MISO_H'*MISO_H+1e-10*eye(U));
MISO_P = (A.'./sqrt(diag(A'*A))).';
```

Published with MATLAB® R2023b

ANEXO VII: SIGLAS Y ACRÓNIMOS

3GPP. *Third Generation Partnership Project*

BC. *Broadcast*

BS. *Base Station*

CDMA. *Code Division Multiple Access*

CIS. *Comunicación, Información y Sistemas*

CSI. *Channel State Information*

CSIR. *Channel State Information at the receiver*

CSIT. *Channel State Information at the transmitter*

C2. *Mando y Control*

DOAs. *Directions of Arrival*

DoF. *Degrees of Freedom*

ETSI. *European Telecommunications Standards Institute*

FDMA. *Frequency Division Multiple Access*

FOT. *Frecuencia Óptima de Trabajo*

FMV. *Full Motion Video*

GSM. *Global System for Mobile Communications*

HF. *High Frequency*

IEEE. *Institute of Electrical and Electronics Engineers*

LAN. *Local Area Networks*

LINR. *Leakage to interference plus noise ratio*

LOS. *Line Of Sight*

MAC. *Medium Access Control*

MAN. *Metropolitan Area Networks*

MIMO. *Multiple-Input Multiple-Output*

MISOME. *Multiple-Input Multiple-Output Multiple-Eavesdroppers*

MISO. *Multiple-Input Single-Output*

MISOSE. *Multiple-Input Multiple-Output Single-Eavesdropper*

mMIMO. *Massive MIMO*

MRC. *Maximum Ratio Combining*

MRT. *Maximum Ratio Transmitter*

MUTP. *Multiuser transmitter preprocessing*

PHY. *Physical Layer*

RCI. *Regularized Channel Inversion*

SATCOM. *Satellite Communications*

SDR. *Software-defined radio*

SINR. *Signal-to-Interference and Noise Ratio*

SISO. *Single-Input Single-Output*

SNR. *Signal to noise ratio*

SU-MIMO. *Single-User MIMO*

TDMA. *Time Division Multiple Access*

UHF. *Ultra High Frequency*

VHF. *Very High Frequency*

ZF. *Zero-Forcing*