Universidad de Málaga

Escuela Técnica Superior de Ingeniería de Telecomunicación

TESIS DOCTORAL POR COMPENDIO

PHYSICAL LAYER SECURITY TECHNIQUES FOR BEYOND 5G NETWORKS

Autor:

GONZALO JAVIER ANAYA LÓPEZ

Doctorado en Ingeniería de Telecomunicación

Ph.D. in Telecommunication Engineering

Directores:

FRANCISCO JAVIER LÓPEZ MARTÍNEZ

AÑO 2023

AUTOR: Gonzalo Javier Anaya López

https://orcid.org/0000-0002-8481-8496

EDITA: Publicaciones y Divulgación Científica. Universidad de Málaga

DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD DE LA TESIS PRESENTADA PARA OBTENER EL TÍTULO DE DOCTOR

D. **Gonzalo Javier Anaya López**

Estudiante del programa de doctorado en **Ingeniería de Telecomunicación** de la Universidad de Málaga, autor/a de la tesis presentada para la obtención del título de doctor por la Universidad de Málaga, titulada: **Physical Layer Security Techniques for Beyond 5G networks**.

Realizada bajo la tutorización y dirección de **Francisco Javier López Martínez**.

DECLARO QUE:

La tesis presentada es una obra original que no infringe los derechos de propiedad intelectual ni los derechos de propiedad industrial u otros, conforme al ordenamiento jurídico vigente (Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia), modificado por la Ley 2/2019, de 1 de marzo.

Igualmente asumo, ante a la Universidad de Málaga y ante cualquier otra instancia, la responsabilidad que pudiera derivarse en caso de plagio de contenidos en la tesis presentada, conforme al ordenamiento jurídico vigente.

En Málaga, a **06** de **Noviembre** de **2023**.

Fdo.: Gonzalo Javier Anaya López Doctorando	Fdo.: Francisco Javier López Martínez Tutor y director de tesis

AUTORIZACIÓN PARA LA LECTURA DE LA TESIS

Por la presente, el Dr. Francisco Javier López Martínez, profesor del Departamento de Teoría de la Señal, Telemática y Comunicaciones de la Universidad de Granada, profesor Titular de Universidad (en excedencia) del Departamento de Ingeniería de Comunicaciones de la Universidad de Málaga, y profesor perteneciente al programa de doctorado en Ingeniería de Telecomunicación de la Universidad de Málaga,

CERTIFICA

Que D. Gonzalo Javier Anaya López, ha realizado en el Departamento de Ingeniería de Comunicaciones de la Universidad de Málaga bajo su dirección, el trabajo de investigación correspondiente a su TESIS DOCTORAL titulada:

"**Physical Layer Security Techniques for Beyond 5G networks**"

En dicho trabajo, se han propuesto aportaciones originales para el análisis y diseño de sistemas de comunicaciones seguros desde el punto de vista de la capa física, con el potencial de ser considerados para su integración en futuros estándares de comunicaciones móviles e inalámbricas. Los resultados de dicha tesis han dado lugar a las diversas publicaciones en revista, así como a aportaciones a congresos, superando el requisito de 1 punto ANECA del programa de doctorado regulado por el Real Decreto 99/2011.

Por todo ello, y dada la unidad temática de las distintas contribuciones y la metodología común seguida en todas ellas, el director considera que esta tesis es apta para su presentación al Tribunal que ha de evaluarla y AUTORIZA la presentación de la tesis por COMPENDIO DE PUBLICACIONES en la Universidad de Málaga. Igualmente, certifica que las publicaciones que avalan la tesis no han sido empleadas en trabajos anteriores a la misma.

Málaga, 06 de Noviembre de 2023

El director:

Fdo.: Francisco Javier López Martínez

UNIVERSIDAD DE MÁLAGA

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN

Reunido el tribunal examinador en el día de la fecha, constituido por:

Presidente: Dr. D. _____

Secretario: Dr. D. _____

Vocal: Dr. D. _____

para juzgar la Tesis Doctoral titulada "*Physical Layer Security Techniques for Beyond 5G networks*", realizada por D. Gonzalo Javier Anaya Lópezy dirigida por el Dr. Francisco Javier López Martínez,

acordó por _____ otorgar la calificación de

_____

y, para que conste, se extiende firmada por los componentes del tribunal la presente diligencia.

Málaga, a _____ de _____ del _____

El presidente: El secretario: El vocal:

Fdo.: _____ Fdo.: _____ Fdo.: _____

Agradecimientos

En primer lugar, me gustaría darle las gracias a Javi por todo. Sin ti esto no habría sido posible. Gracias por tu paciencia, comprensión, pasión por lo que haces y por haberme dado la oportunidad de trabajar contigo. Lo que haces y lo que me has enseñado no tiene precio.

De igual forma, quiero darle las gracias a José. Ha sido un placer trabajar contigo. Siempre has estado ahí dispuesto a echar una mano en lo que sea y con infinitas ganas de trabajar. Especialmente gracias con la paciencia que has tenido para enseñarme un poquito del álgebra que tan bien se me da.

No puedo olvidar a las personas que me han dado su apoyo incondicional, mi familia. En los momentos más difíciles siempre he podido contar con vosotros para poder seguir adelante, gracias.

Finalmente, quiero dar las gracias a Elena. La persona que más me ha sufrido en todo este proceso y día a día me ayuda a ser mejor. Te quiero.

Resumen

El aumento en el número de conexiones inalámbricas debido al Internet de las cosas (IoT) y la llegada de la quinta generación de redes móviles (5G) ha propiciado un aumento en las preocupaciones sobre el rendimiento de las transmisiones y su seguridad. En esta tesis se pretende analizar la aportación que tiene la seguridad en capa física (PLS) en este tipo de entornos donde elevar el número de antenas viene siendo habitual. En primer lugar, se propone un nuevo esquema de selección de antena transmisora (TAS) centrado en impedir la posible fuga de información: ETAS. Se obtienen las métricas para poder evaluar su rendimiento en términos de máxima tasa de transmisión segura y se compara con otros esquemas habituales como el óptimo (OTAS) y el sub-óptimo basado en el usuario legítimo (BTAS). Los resultados muestran como el esquema sub-óptimo ETAS permite una mayor tasa de transmisión que el BTAS en escenarios donde los fisgones son dominantes. Por otro lado, se ha propuesto un ataque sobre sistemas basados en PLS, denominado ataque de canal producto con desvanecimientos sintéticos. Se fundamenta en la necesidad que estos sistemas tienen de obtener correctamente la información del canal (CSI) de los distintos usuarios. De esta forma, se propone un ataque que pretende hacer que la estación base (BS) transmita al usuario legítimo información segura a una tasa superior a la que su canal le permitiría y conseguir así interceptarla. Asi mismo, se presenta una propuesta para poder combatir este tipo de ataques: utilizando zonas de guarda o de seguridad. Finalmente, se ha analizado cómo afecta a PLS la tendencia de aumentar el número de antenas y reducir el tamaño de las celdas en busca de mayor capacidad en las comunicaciones. En concreto, se ha analizado el impacto de incorporar modelos de propagación más realistas para estos casos, como es la propagación esférica (SW), en lugar del clásico modelo de onda plana (PW), que deja de ser válido en estas condiciones. El resultado se refleja en una propuesta de modelo para PLS con propagación esférica y una estrategia de precodificación y selección de usuario conjunta, el *Leakage Subspace Precoding* (LSP), que incluye las particularidades de PLS y SW en su diseño. De esta forma, consigue aprovechar mejor las particularidades físicas del medio para mejorar el rendimiento entre un 20-40 % con respecto a esquemas tradicionales como el *zero forcing* (ZF).

Abstract

The increase in the number of wireless connections due to the Internet of Things (IoT) and the arrival of the fifth generation of mobile networks (5G) has led to an increase in concerns about transmission performance and security. This thesis aims to analyse the contribution of physical layer security (PLS) in such environments where increasing the number of antennas is commonplace. Firstly, a new approach to antenna selection methods (TAS) is proposed, focused on preventing possible information leakage: ETAS. Metrics are obtained in order to evaluate its performance in terms of maximum secure transmission rate and compared with other common schemes such as the optimal (OTAS) and the sub-optimal legitimate user-based (BTAS) schemes. The results show that the sub-optimal ETAS scheme allows a higher transmission rate than BTAS in scenarios where eavesdroppers are strong. On the other hand, an attack on PLS-based systems, called product channel attack with synthetic fading, has been proposed. It is based on the necessity of these systems to correctly acquire the channel state information (CSI) of the different users. Thus, an attack is proposed that aims to make the base station (BS) transmit secure information to the legitimate user at a higher rate its channel would allow and thus successfully intercept it. A strategy to combat this type of attack is also presented: using guard or security zones. Finally, we have analysed how PLS is affected by the trend to increase the number of antennas and reduce the size of the cells in order to increase communications capacity. Specifically, we have analysed the impact of considering more realistic propagation models for these cases, such as spherical-wave propagation (SW), instead of the classical plane-wave (PW) model, which is no longer valid under these conditions. The result result has led to a proposed model for PLS with spherical propagation and a joint scheduling and precoding, the Leakage Subspace Precoding (LSP), which includes the particularities of PLS and SW in its design. In this way, it manages to take advantage of the physical peculiarities of the channel to improve performance by 20-40 % with respect to traditional schemes such as *zero forcing* (ZF).

Índice general

1. Introducción **1**
1.1. Objetivos . . . 2
1.2. Organización . . . 3
1.3. Publicaciones . . . 3

2. Antecedentes **5**
2.1. Notación . . . 5
2.2. Seguridad en Capa Física . . . 8
2.2.1. Escenario de ejemplo . . . 9
2.2.2. Escalado con el número de antenas . . . 11
2.3. Modelo de propagación . . . 14

3. Resumen de los resultados **17**
3.1. Selección de antena . . . 17
3.1.1. TAS óptimo . . . 19
3.1.2. TAS basado en Bob . . . 20
3.1.3. TAS basado en Eve . . . 21
3.1.4. MRT . . . 22
3.1.5. ZF . . . 23
3.1.6. Resultados . . . 24
3.2. Ataque tipo canal producto . . . 29
3.3. Propagación esférica con un usuario . . . 35
3.3.1. Escenario 1 . . . 36
3.3.2. Escenario 2 . . . 39
3.3.3. Escenario 3 . . . 41
3.4. Leakage Subspace Precoding and Scheduling . . . 42
3.4.1. Escenario de cooperación total . . . 44
3.4.2. Escenario de cooperación parcial . . . 47
3.4.3. Complejidad . . . 50

4. Conclusiones y líneas futuras **53**
4.1. Conclusiones . . . 53
4.2. Líneas futuras . . . 54

A. Publications **57**

A.1. Leakage Subspace Precoding and Scheduling for Physical Layer Security in Multi-User XL-MIMO Systems 57
A.2. Spatial Degrees of Freedom for Physical Layer Security in XL-MIMO . . . 59
A.3. A New Transmit Antenna Selection Technique for Physical Layer Security with Strong Eavesdropping 61
A.4. A Product Channel Attack to Wireless Physical Layer Security 63
A.5. Ataques tipo Canal-Producto a Comunicaciones con Seguridad en Capa Física y Selección de Antena en Transmisión 65

Bibliografía **67**

Índice de figuras

2.1. Modelo de sistema del escenario de ejemplo con un usuario legítimo y un fisgón, ambos mono-antena. 9
2.2. Cantidad de información segura de Bob con $\overline{\gamma}_{\mathrm{E}} = 5$ dB. 11
2.3. Canales Rayleigh con 0 dB (Rayleigh 1) y 10 dB (Rayleigh 2) de media en su SNR con 2000 muestras de tiempo. 12
2.4. Escalado de la relación señal-ruido (SNR) en decibelios con el número de antenas, M, para los modelos PW y SW con 50 dB de P_{Tx} a una distancia de 15 m del centro del *array* sobre la frecuencia de $2{,}4$ GHz. 13
2.5. Correlación entre los canales del usuario legítimos y el fisgón con la distancia para los modelos PW y SW. 13
2.6. Modelo de sistema del escenario de ejemplo con SW, una BS de M elementos, un usuario legítimo mono-antena y varios fisgones todos mono-antena. 14

3.1. Modelo de sistema con selección de antena. El mensaje transmitido en DL z_{B} por la BS (Alice) a través de la antena k seleccionada según cierto criterio TAS. 18
3.2. $\overline{R}_{\mathrm{s}}$ en función de $\overline{\gamma}_{\mathrm{B}_0}$ para los esquemas O-TAS, B-TAS y E-TAS con $\overline{\gamma}_{\mathrm{E}_0} = 10$ dB. Los escenarios con $M = \{2, 8\}$ antenas se representan con líneas discontinuas con puntos y continuas respectivamente. Los marcadores corresponden con simulaciones de MC. 24
3.3. $\overline{R}_{\mathrm{s}}$ en función de $\overline{\gamma}_{\mathrm{E}_0}$ para los esquemas O-TAS, B-TAS y E-TAS con $\overline{\gamma}_{\mathrm{B}_0} = 10$ dB. Los escenarios con $M = \{2, 8\}$ antenas se representan con líneas discontinuas con puntos y continuas respectivamente. Los marcadores corresponden con simulaciones de Monte Carlo (MC). 25
3.4. $\overline{R}_{\mathrm{s}}$ normalizada a O-TAS en función de $\overline{\gamma}_{\mathrm{E}_0}/\overline{\gamma}_{\mathrm{B}_0}$ para diferentes valores de $\overline{\gamma}_{\mathrm{B}_0} = \{10, 20, 30\}$ dB y $M = 8$. Estos valores se corresponden con líneas continuas, discontinuas y discontinuas con puntos respectivamente. Los marcadores corresponden con simulaciones de MC. Los valores de SNR donde se cruzan los dos esquemas se identifican con puntos negros sólidos para cada pareja de curvas. 26

3.5. $\overline{R}_{\mathrm{s}}$ normalizada a MRT con en función de $\overline{\gamma}_{\mathrm{E}_0}/\overline{\gamma}_{\mathrm{B}_0}$ para diferentes valores de $\overline{\gamma}_{\mathrm{B}_0} = \{10, 20, 30\}$ dB y $M = 8$. Estos valores se corresponden con líneas continuas, discontinuas y discontinuas con puntos respectivamente. Los marcadores corresponden con simulaciones de MC. Los valores de SNR donde se cruzan los dos esquemas se identifican con puntos negros sólidos para cada pareja de curvas. 27
3.6. $\overline{R}_{\mathrm{s}}$ normalizada a ZF en función de $\overline{\gamma}_{\mathrm{E}_0}/\overline{\gamma}_{\mathrm{B}_0}$ para diferentes valores de $\overline{\gamma}_{\mathrm{B}_0} = \{10, 20, 30\}$ dB y $M = 8$. Estos valores se corresponden con líneas continuas, discontinuas y discontinuas con puntos respectivamente. Los marcadores corresponden con simulaciones de MC. Los valores de SNR donde se cruzan los dos esquemas se identifican con puntos negros sólidos para cada pareja de curvas. 28
3.7. $\overline{R}_{\mathrm{s}}$ en función de $\overline{\gamma}_{\mathrm{E}}$ para los esquemas TAS presentados, MRT y ZF con $M = 8$. Los escenarios con $\overline{\gamma}_{\mathrm{B}_0} = \{10, 30\}$ dB se representan con líneas continuas y discontinuas respectivamente. Los marcadores corresponden con simulaciones de MC. 28
3.8. Modelo de sistema bajo ataque con un usuario legítimo y un fisgón, ambos con una única antena. 29
3.9. Exceso de tasa segura $\mathcal{D}$ con MRT en función de $\overline{\gamma}_{\mathrm{B}}$ para diferentes número de antenas y distribuciones de los desvanecimientos sintéticos θ_{E} con $\overline{\gamma}_{\mathrm{E}} = 15$ dB para $M = 1$ y después reducido por $10 \log_{10} M$ (dB), ... 31
3.10. Máxima tasa segura media ($\overline{R}_{\mathrm{s}}$) vs. tasa media comprometida ($\overline{\mathfrak{R}}_{\mathrm{s}}$) en función de $\overline{\gamma}_{\mathrm{B}_0}$ con $M = 4$, $\overline{\gamma}_{\mathrm{E}_0} = \{5, 10, 15\}$ dB y desvanecimientos sintéticos uniformes. Los marcadores corresponden con simulaciones usando el método de MC. 32
3.11. Máxima tasa segura media ($\overline{R}_{\mathrm{s}}$) vs. tasa media comprometida ($\overline{\mathfrak{R}}_{\mathrm{s}}$) utilizando B-TAS en función de $\overline{\gamma}_{\mathrm{B}_0}$ con $\overline{\gamma}_{\mathrm{E}_0} = 5$ dB, $M = 1, 2, 4, 8$ y desvanecimientos sintéticos uniformes. Los marcadores corresponden con simulaciones usando el método de MC. 33
3.12. Exceso de tasa segura $\mathcal{D}$ utilizando MRT, ZF, B-TAS y E-TAS en función de $\overline{\gamma}_{\mathrm{B}_0}$ con $\overline{\gamma}_{\mathrm{E}} = 15$ dB y desvanecimientos sintéticos uniformes. Los casos de $M = 2, 4, 8$ antenas se representan con líneas continuas, discontinuas y discontinuas con puntos respectivamente. 34
3.13. Representación gráfica de la posición de los usuarios en el escenario 1. La posición de Bob en (5°, 200 m) se señala con un círculo azul y las del fisgón que varía su posición con cruces negras. 36
3.14. R_{s} en función de la posición de $\mathrm{Eve}_{\mathrm{A}}$ en el escenario 1 con Bob fijo en (10°, 200 m). 37
3.15. R_{s} en función de $r_{\mathrm{E_A}}$ para el escenario 1 con $\theta_{\mathrm{E_A}} = 5°$ donde se han representado con líneas sólidas, discontinuas con puntos y discontinuas los casos con $M = [500, 250, 100]$ antenas respectivamente. 38

3.16. R_{s} en función de $r_{\mathrm{E_A}}$ para el escenario 1 donde se han representado con líneas sólidas, discontinuas con puntos, punteadas y discontinuas los casos con $\theta_{\mathrm{E_A}} = [60, 70, 80, 90]^{\circ}$ respectivamente. 39
3.17. Representación gráfica de la posición de los usuarios en el escenario 2. La posición de Bob en (5°, 200 m) se señala con un círculo azul, los fisgones fijos en (10°, 75 m) y (5°, 800 m) con cruces rojas y las del fisgón que mueve su posición con cruces negras. 39
3.18. R_{s} en función de la posición de $\mathrm{Eve_A}$ en el escenario 2 con Bob fijo en (5°, 200 m) y dos Eve fijos en (10°, 75 m) y (5°, 800 m). 40
3.19. Representación gráfica de la posición de los usuarios en el escenario 3. La posición de Bob es móvil y se señala con círculos azules, mientras que los tres fisgones fijos se encuentran en (5°, 200 m), (10°, 75 m) y (5°, 800 m) y se señalan con cruces rojas. 41
3.20. R_{s} en función de la posición de Bob en el escenario 3 con tres Eve fijos en (5°, 200 m), (10°, 75 m) y (5°, 800 m). 42
3.21. Eficiencia espectral segura en el escenario TC, considerando propagación SW y PW y diferentes estrategias de precodificación. Las líneas continuas y discontinuas corresponden con ($K_{\mathrm{B}} = 10$) y ($K_{\mathrm{B}} = 20$) respectivamente. 47
3.22. Número de usuarios servidos en el escenario TC, considerando propagación SW y PW y diferentes estrategias de precodificación. Las líneas continuas y discontinuas corresponden con ($K_{\mathrm{B}} = 10$) y ($K_{\mathrm{B}} = 20$) respectivamente. 47
3.23. Eficiencia espectral segura en el escenario PC, considerando propagación SW y PW y diferentes estrategias de precodificación. Las líneas continuas y discontinuas corresponden con ($K_{\mathrm{B}} = 10$) y ($K_{\mathrm{B}} = 20$) respectivamente. 49
3.24. Número de usuarios servidos en el escenario PC, considerando propagación SW y PW y diferentes estrategias de precodificación. Las líneas continuas y discontinuas corresponden con ($K_{\mathrm{B}} = 10$) y ($K_{\mathrm{B}} = 20$) respectivamente. 50
3.25. Evolución de las métricas con TC con las iteraciones i considerando propagación SW. 51

Lista de Acrónimos

5G	Fifth **G**eneration
	Quinta generación
6G	Sixth **G**eneration
	Sexta generación
ASC	**A**verage **S**ecrecy **C**apacity
	Capacidad secreta media
AWGN	**A**dditive **W**hite **G**aussian **N**oise
	Ruido blanco Gaussiano
BS	**B**ase **S**tation
	Estación base
BTAS	**B**ob-based **T**ransmit **A**ntenna **S**election
	Selección de antena transmisora basada en Bob
CDF	**C**umulative **D**istribution **F**unction
	Función de distribución acumulada
CSI	**C**hannel **S**tate **I**nformation
	Información del estado del canal
DL	**D**own**L**ink
DMA	**D**ynamic **M**etasurface **A**ntenna
	Antena dinámica de metasuperficie
DoF	**D**egree **o**f **F**reedom
	Grado de libertad
ETAS	**E**ve-based **T**ransmit **A**ntenna **S**election
	Transmisión de antena transmisora basada en Eve
IoT	**I**nternet **o**f **T**hings
	Internet de las cosas

IRS	**I**ntelligent **R**eflecting **S**urface
	Superficie reflectante inteligente
IUI	**I**nter-**U**ser **I**nterference
	Interferencia entre usuarios
LINR	**L**eakage-to-**I**nterference-plus-**N**oise **R**atio
	Relación señal fugada-interferencia más ruido
LSP	**L**eakage **S**ubspace **P**recoding
MC	**M**onte **C**arlo
MIMO	**M**ultiple-**I**nput **M**ultiple-**o**utput
	Múltiples-entradas, múltiples-salidas
MIMOME	**M**ultiple-**I**nput **M**ultiple-**o**utput, **M**ulti-**E**avesdropper
	Múltiples-entradas, múltiples-salidas y múltiples-fisgones
MRC	**M**aximum **R**atio **C**ombining
MRT	**M**aximum **R**atio **T**ransmission
NOMA	**N**on-**O**rthogonal **M**ultiple **A**ccess
OTAS	**O**ptimal **T**ransmit **A**ntenna **S**election
	Selección de antena transmisora óptima
PC	**P**artial **C**ollusion
	Colaboración parcial
PDF	**P**robability **D**ensity **F**unction
	Función de densidad de probabilidad
PLS	**P**hysical **L**ayer **S**ecurity
	Seguridad en capa física
PW	**P**lanar-**W**avefront
	Frente de onda-plano
RF	**R**adio **F**requency
	Radiofrecuencia
RIS	**R**econfigurable **I**ntelligent **S**urface
	Superficie reconfigurable inteligente
RV	**R**andom **V**ariable
	Variable aleatoria

SINR	**S**ignal-to-**I**nterference-plus-**N**oise **R**atio
	Relación señal-interferencia más ruido
SNR	**S**ignal-to-**N**oise **R**atio
	Relación señal-ruido
SW	**S**pherical-**W**avefront
	Frente de onda-esférico
TAS	**T**ransmit **A**ntenna **S**election
	Selección de antena en transmisión
TC	**T**otal **C**ollusion
	Colaboración total
UL	**U**plink
ULA	**U**niform **L**inear **A**rray
	Array lineal uniforme
XL	E**x**tra-**L**arge
	Extra-grande
XL-MIMO	E**x**tra-**L**arge **M**ultiple-**I**nput **M**ultiple-**o**utput
	Múltiples-entradas, múltiples-salidas extra-grande
ZF	**Z**ero-**F**orcing

Capítulo 1

Introducción

El número de conexiones inalámbricas ha aumentado drásticamente [1] desde la llegada del internet de las cosas (IoT) y la quinta generación (5G) de redes móviles [2]. Esto, junto a la previsión de que sigan aumentando con la sexta generación (6G) y el resto de tecnologías emergentes [3], aumenta la necesidad de buscar nuevas formas de mejorar las prestaciones de las transmisiones. De igual importancia es asegurar que que estas comunicaciones siguen siendo seguras y libre de errores.

La criptografía ha sido tradicionalmente utilizada para asegurar unas comunicaciones seguras, pero desde los trabajos de [4], [5] las técnicas de seguridad en capa física (PLS) han cobrado importancia. Estas técnicas aprovechan la aleatoriedad inherente al canal radio para proveer de seguridad a las comunicaciones en presencia de fisgones. Se han realizado numerosos estudios de las técnicas de PLS desde diferentes frentes: escenarios con múltiples usuarios y *zero-forcing* (ZF) regularizado se presenta en [6]; una formulación general para los escenarios con múltiples-entradas, múltiples-salidas y múltiples-fisgones (MIMOME) se describe en [7]; el uso de ruido artificial se estudia en [8], [9]; como alternativa a estas técnicas de ruido artificial, el uso de zonas de protección o de guarda se discute en [10], [11] y [12].

De la misma forma que las técnicas de PLS buscan mejorar la seguridad en las comunicaciones radio, las prestaciones en las comunicaciones móviles se pretenden elevar, entre otras tendencias, aumentando el número de antenas [3], [13] y reduciendo el tamaño de las celdas [14]. Esto provoca que el tamaño del *array* de antenas pueda ser comparable a la distancia con los usuarios. Por tanto, la suposición de campo lejano deja de ser efectiva y, en consecuencia, dejemos de poder tener un frente de onda plano, *i. e.* con fase constante. En [15] y recientemente extendido en [16] se propone un modelo de onda esférica, que incluye como caso particular al frente de onda plano, para caracterizar este tipo de transmisiones. Este nuevo modelo de propagación más realista dota al sistema de nuevas herramientas para reducir la interferencia entre usuario: ya no depende únicamente del ángulo de propagación, sino que la distancia también debe tenerse en cuenta. En el ámbito de las técnicas de PLS, esta nueva atenuación en la interferencia con la distancia puede ser vista como una menor cantidad de información fugada hacia los fisgones que desean interceptar la señal.

El uso de *arrays* de antenas cada vez más grandes lleva a altos costes tanto en complejidad y hardware como en energía. Motivadas por la búsqueda de alternativas eficientes energéticamente y en hardware surgen las superficies reflectantes inteligentes (IRSs) [17], [18]. Estas metasuperficies compuestas por un gran número de elementos pasivos o no que permiten reconfigurar sus propiedades electromagnéticas mediante un controlador electrónico. Ajustando las fases y amplitudes de estos elementos reflectores se pueden mejorar las capacidades de las comunicaciones sin necesidad de introducir amplificación de la señal. Para ello, se buscará sumar constructivamente las señales deseadas o destructivamente las no deseadas [19]. El desafío de esta tecnología es, por un lado caracterizar correctamente estas superficies y, por otro lado, la búsqueda del diseño óptimo de los diferentes elementos de las IRS.

1.1. Objetivos

Aunque el interés por las técnicas PLS es evidente, hay varios aspectos que necesitan ser mejor estudiados antes de que puedan aspirar a su inclusión en futuros estándares inalámbricos. El objetivo de esta tesis es analizar algunos de estos aspectos, y cuantificar su impacto en despliegues prácticos.

En primer lugar, se pretende analizar posibles ataques PLS en comunicaciones móviles inalámbricas. De la misma manera que el criptoanálisis pretende encontrar vulnerabilidades en los sistemas criptográficos, se pretende determinar cómo pueden diseñarse ataques específicos a PLS para comprometer la seguridad.

En segundo lugar, se pretenden estudiar las implicaciones del uso de sistemas con múltiples-entradas, múltiples-salidas (MIMO) de forma masiva y su evolución desde la perspectiva de PLS. La tendencia a aumentar el número de antenas [13] y reducir el tamaño de la célula [14] conduce a un cambio de paradigma con respecto al tipo de frente de onda. Asimismo, en la literatura se encuentran soluciones como los esquemas de selección de antena transmisora (TAS) y las superficies reconfigurables inteligentes (RISs) como forma de aumentar considerablemente el número efectivo de antenas en los sistemas de comunicaciones sin elevar excesivamente el coste en energía y hardware. En este ámbito se definen los siguientes objetivos

- Estudiar mecanismos sencillos y/o de bajo coste para aumentar el número de antenas.
- Estudiar los verdaderos límites en el beneficio de aumentar el número de antenas, considerando leyes de propagación realistas conforme a la física.
- Estudiar nuevos modelos de propagación más apropiados para sistemas con múltiples-entradas, múltiples-salidas extra-grande (XL-MIMO) de forma masiva.

1.2. Organización

El documento, una tesis por compendio, está organizado como sigue:

- Un primer capítulo, en el que nos encontramos, que contiene una breve introducción y motivación del trabajo realizado, seguido de la definición de los objetivos de esta tesis, la organización del documento y, por último, las publicaciones que avalan la tesis.
- El capítulo 2 presenta todos los antecedentes necesarios para comprender la formulación y los escenarios propuestos en las distintas contribuciones de la tesis.
- El capítulo 3 resume la contribución científica de las distintas publicaciones.
- El capítulo 4 detalla las conclusiones y las posibles orientaciones futuras que podrían derivarse del trabajo realizado.
- Por último, el apéndice A contiene las publicaciones que componen esta tesis por compendio.

1.3. Publicaciones

A continuación se enumeran las publicaciones en revistas especializadas y actas de congresos incluidas en la elaboración de esta tesis:

- [20] G. J. Anaya-López, J. P. González-Coma y F. J. López-Martínez, «Leakage Subspace Precoding and Scheduling for Physical Layer Security in Multi-User XL-MIMO Systems», *IEEE Commun. Lett.*, vol. 27, n.º 2, págs. 467-471, 2023. DOI: 10.1109/LCOMM.2022.3225881.
- [21] G. J. Anaya-López, J. P. González-Coma y F. J. López-Martínez, «Spatial Degrees of Freedom for Physical Layer Security in XL-MIMO», en *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, 2022, págs. 1-5. DOI: 10.1109/VTC2022-Spring54318.2022.9860861.
- [22] G. J. Anaya-López, J. C. Ruiz-Sicilia y F. J. López-Martínez, «A New Transmit Antenna Selection Technique for Physical Layer Security with Strong Eavesdropping», en *2021 4th International Conference on Advanced Communication Technologies and Networking (CommNet)*, 2021, págs. 1-5. DOI: 10.1109/CommNet52204.2021.9641938.
- [23] G. J. Anaya-López, G. Gomez y F. J. López-Martínez, «Ataques tipo Canal-Producto a Comunicaciones con Seguridad en Capa Física y Selección de Antena en Transmisión», *XXXVI Simposium Nacional de la Unión Científica Internacional de Radio*, 2021.

- [24] G. J. Anaya-Lopez, G. Gomez y F. J. Lopez-Martinez, «A Product Channel Attack to Wireless Physical Layer Security», *IEEE Wireless Commun. Lett.*, vol. 10, n.º 5, págs. 943-947, 2021. DOI: 10.1109/LWC.2021.3050957.

Las publicaciones [20] y [21] recogen los resultados relacionados con la propagación frente de onda esférica (SW) desde un punto de vista de PLS, mientras que las publicaciones [22], [23] y [24] tratan posibles ataques a la seguridad en PLS.

Durante los estudios de doctorado se han logrado publicaciones adicionales, aunque no se consideran estrictamente parte del conjunto de publicaciones utilizadas para avalar esta tesis:

- [25] J. Lopez-Fernandez, G. J. Anaya-Lopez y F. J. Lopez-Martinez, «The Second Order Scattering Fading Model with Fluctuating Line-of-Sight», *submitted to IEEE Trans. Veh. Technol.*, 2023.
- [26] J. C. Ruiz-Sicilia, J. Gimenez de la Cuesta, G. J. Anaya-López y F. J. López-Martínez, «Configuring an Intelligent Reflecting Surface for Wireless Communications: the hUMAns at RISk approach», *XXXVI Simposium Nacional de la Unión Científica Internacional de Radio*, 2021.

Capítulo 2

Antecedentes

El propósito de este capítulo es definir el conjunto de variables y métricas previas a los resultados. Estas serán necesarias para comprender los resultados presentados en los capítulos posteriores.

La organización del capítulo consta de tres partes. Una primera Sección 2.1 en la que se recogerá toda la notación utilizada a lo largo del trabajo. Una segunda Sección 2.2 en la que se introducirá brevemente el concepto de PLS y se plantearán unas métricas generales de seguridad que se utilizarán a lo largo de este trabajo. Finalmente, en la Sección 2.3 se discutirá la validez del modelo de propagación clásico, basado en un frente de onda plana, y se propondrá un modelo de onda esférica válido tanto para campo lejano como cercano.

2.1. Notación

TABLA 2.1: Resumen de variables y notación.

Notación	Descripción
$\approx$	Aproximadamente
$\arg\max, \arg\min$	Argumento del máximo y del mínimo
K	Cantidad de usuarios
$\lvert\mathcal{C}\rvert$	Cardinal del conjunto
$\mathcal{V}$	Conjunto de fisgones
$\mathcal{E}_k$	Conjunto de fisgones del clúster k
$\mathbb{C}$	Conjunto de los números complejos
$\mathcal{S}$	Conjunto de los usuarios seleccionados
$\mathcal{U}$	Conjunto de usuarios
$\mathcal{B}$	Conjunto de usuarios legítimos
$\forall$	Cuantificador universal
D	Dimensión física de la antena
r_{Crit}	Distancia crítica
r_{Rayl}	Distancia de Rayleigh

Continúa en la siguiente página.

Notación	Descripción
r_{ref}	Distancia de referencia
r_{k}	Distancia del usuario k
$\mathcal{N}_{\mathbb{C}}(\mu, \sigma^2)$	Distribución normal con media μ y varianza σ^2
$\mathcal{R}(\sigma)$	Distribución Rayleigh con desviación típica σ
$\sim$	Distribuido estadísticamente como
$\mathcal{D}$	Exceso de tasa segura
$\mathrm{span}\,(\mathbf{X})$	Extensión de las columnas de la matriz
$f_X(x)$	Función de densidad de probabilidad de X
$F_X(x)$	Función de distribución acumulada de X
$\mathrm{erfc}(\cdot)$	Función de error complementaria
$K_1(\cdot)$	Función de Bessel modificada de segunda especie y primer orden
$\mathrm{E}_1(\cdot)$	Función exponencial integral
$\Gamma(\cdot)$	Función gamma
$(\cdot)^{\mathrm{H}}$	Hermítica
$\cap$	Intersección
λ	Longitud de onda
$\mathbf{A}$	Matriz conjunta de canales
$\mathbf{B}_{\mathrm{k}}$	Matriz conjunta de canales k-ésima
$\mathbf{W}$	Matriz de precodificación
$\mathrm{diag}\,(\mathbf{x})$	Matriz diagonal
$\mathrm{máx}, \mathrm{mín}$	Máximo y mínimo
s_{k}	Mensaje
$\|\cdot\|$	Módulo
M	Número de antenas
$\mathbb{E}[\cdot]$	Operador esperanza
$[X]^+$	Parte positiva de X
θ_{k}	Posición angular del usuario k
β_0	Potencia de referencia del canal
p_{k}	Potencia del usuario
q_{k}	Prioridad del usuario
$\mathbf{\Pi}$	Proyector ortogonal
r_q	Radio de zona protegida
$\hat{\gamma}_X$	Relación señal-ruido comprometida de X
γ_X	Relación señal-ruido de X
h_k	Respuesta impulsiva del canal
$\hat{h}_k$	Respuesta impulsiva del canal comprometido
n_k	Ruido
y_{k}	Señal recibida
x_{k}	Señal transmitida

Continúa en la siguiente página.

Notación	Descripción
d	Separación entre antenas
$\subseteq$	Subconjunto
$\mathfrak{L}$	Subespacio de fuga
$\mathfrak{I}_{\bar{k}}$	Subespacio de interferencia
$R_{\mathrm{s,k}}$	Tasa de transmisión segura
$\mathfrak{R}_{\mathrm{s,k}}$	Tasa de transmisión segura comprometida
$(\cdot)^{\mathrm{T}}$	Transpuesta
σ_w^2	Varianza del ruido
$\mathbf{w}_{\mathrm{k}}$	Vector de precodificación
$\mathbf{a}_{\mathrm{k}}$	Vector de respuesta
$\mathbf{z}, \mathbf{Z}$	Vectores y matrices

2.2. Seguridad en Capa Física

El escenario propuesto para el estudio pretende emular al de comunicaciones móviles celulares. En él, una estación base (BS), Alice, equipada con una antena de M elementos da servicio a una celda con un conjunto $\mathcal{U}$ de usuarios mono-antena, con $|\mathcal{U}| = K$, siendo K el número total de usuarios servidos. Se asume que la BS opera en dos modos: en un primer modo *normal*, la BS adquiere la información del estado del canal (CSI) de los K usuarios y los sirve bajo cierto criterio (i. e.: maximizar la tasa de transmisión global), se considera que esta CSI está libre de errores; en un segundo modo *seguro*, un grupo $\mathcal{B}$ de usuarios legítimos, Bobs, con $|\mathcal{B}| = K_{\mathrm{B}} < K$ se sirven bajo cierto criterio de seguridad (i. e.: maximizar la tasa de transmisión segura global). Para ello, se basa en la CSI para evitar que la información transmitida a estos K_{B} usuarios sea interceptada por otro grupo $\mathcal{V}$ de usuarios actuando como fisgones, Eves, con $|\mathcal{V}| = K_{\mathrm{E}} = K - K_{\mathrm{B}}$.

El objetivo de la BS bajo el modo *seguro* es transmitir una señal (el mensaje) $s_{\mathrm{k}} \sim \mathcal{N}_{\mathbb{C}}(0,1)$ a cada uno de los usuarios legítimos $k \in \mathcal{B}$. Para ello, la BS adapta el mensaje a la CSI adquirida en el modo *normal* para evitar que llegue a los fisgones. Esto se hace mediante las matrices de precodificación $\mathbf{W} \in \mathbb{C}^{M \times K_{\mathrm{B}}}$, donde la columna k es $\mathbf{w}_{\mathrm{k}}$, con $\|\mathbf{w}_{\mathrm{k}}\| = 1, \forall k \in \mathcal{B}$. Finalmente, se tiene que la señal transmitida es $\mathbf{x} = \sum_{k\in\mathcal{B}} p_{\mathrm{k}} \mathbf{w}_{\mathrm{k}} s_{\mathrm{k}}$, donde p_{k} son los factores de escala de la potencia asignada de forma que $P_{\mathrm{TX}} = \sum_{k\in\mathcal{B}} p_{\mathrm{k}}$ [W], siendo P_{TX} la potencia transmitida por la BS.

De esta forma, se puede definir la señal recibida por cada usuario y_{k} como:

$$y_{\mathrm{k}} = \sqrt{p_{\mathrm{k}}} s_{\mathrm{k}} \mathbf{w}_{\mathrm{k}}^{\mathrm{H}} \mathbf{a}_{\mathrm{k}} + \sum_{j\neq k; j\in\mathcal{B}} \sqrt{p_{\mathrm{j}}} s_{\mathrm{j}} \mathbf{w}_{\mathrm{j}}^{\mathrm{H}} \mathbf{a}_{\mathrm{k}} + n_{\mathrm{k}}, \tag{2.1}$$

donde $\mathbf{a}_{\mathrm{k}}$ es un coeficiente que define la propagación de la señal desde la BS hasta el usuario y $(\cdot)^{\mathrm{H}}$ denota la transposición hermítica. Este término puede incluir las pérdidas por propagación, las ganancias de las antenas, la polarización, etc. Nótese que el primer término de (2.1) corresponde con la señal deseada por el usuario legítimo, el segundo es la interferencia entre usuarios (IUI) debida a los demás usuarios legítimos distintos de k y el tercero es el ruido blanco Gaussiano (AWGN) $n_{\mathrm{k}} \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_w^2)$.

A partir de la expresión en (2.1), se puede obtener la relación señal-interferencia más ruido (SINR) para el usuario legítimo como [27]:

$$\mathrm{SINR}_{\mathrm{k}} = \frac{p_{\mathrm{k}} |\mathbf{w}_{\mathrm{k}}^{\mathrm{H}} \mathbf{a}_{\mathrm{k}}|^2}{\sigma_w^2 + \sum_{j\neq k; j\in\mathcal{B}} p_{\mathrm{j}} |\mathbf{w}_{\mathrm{j}}^{\mathrm{H}} \mathbf{a}_{\mathrm{k}}|^2} \tag{2.2}$$

y la SNR si eliminamos la interferencia del resto de usuarios:

$$\gamma_{\mathrm{k}} = \frac{p_{\mathrm{k}} |\mathbf{w}_{\mathrm{k}}^{\mathrm{H}} \mathbf{a}_{\mathrm{k}}|^2}{\sigma_w^2}. \tag{2.3}$$

De forma análoga, se puede definir la parte de la señal que llega a los fisgones. Esta

señal no se trata de interferencia, desde el punto de vista de los fisgones, sino de información fugada. Así pues, se puede definir la relación señal fugada-interferencia más ruido (LINR) como:

$$\mathrm{LINR_k}(v) = \frac{p_\mathrm{k}|\mathbf{w}_\mathrm{k}^\mathrm{H}\mathbf{a}_v|^2}{\sigma_w^2 + \sum_{j\neq k; j\in\mathcal{V}} p_\mathrm{j}|\mathbf{w}_\mathrm{j}^\mathrm{H}\mathbf{a}_v|^2}, \tag{2.4}$$

donde esta LINR puede ser vista como la SINR del mensaje s_k en el fisgón v. En el caso de existir más de un fisgón, se tendría que la cantidad de información fugada total es:

$$\mathrm{LINR_k} = \sum_{v\in\mathcal{V}} \frac{p_\mathrm{k}|\mathbf{w}_\mathrm{k}^\mathrm{H}\mathbf{a}_v|^2}{\sigma_w^2 + \sum_{j\neq k; j\in\mathcal{V}} p_\mathrm{j}|\mathbf{w}_\mathrm{j}^\mathrm{H}\mathbf{a}_v|^2}. \tag{2.5}$$

Esta expresión suele simplificarse al considerar el caso peor en el que los fisgones colaboran entre ellos para cancelar la interferencia sufrida [28]:

$$\mathrm{LINR_k} = \sum_{v\in\mathcal{V}} \gamma_\mathrm{k} = \sum_{v\in\mathcal{V}} \frac{p_\mathrm{k}|\mathbf{w}_\mathrm{k}^\mathrm{H}\mathbf{a}_v|^2}{\sigma_w^2}, \tag{2.6}$$

donde γ_k es la SNR de los fisgones considerando que la potencia recibida es la interferencia que se genera al transmitir al usuario legítimo k.

A partir de estas dos métricas (2.2) y (2.6), se puede obtener la cantidad de información segura que se puede transmitir a un usuario [6], [7]:

$$R_{\mathrm{s,k}} = \log_2\left[\frac{1+\mathrm{SINR_k}}{1+\mathrm{LINR_k}}\right]^+ \ [\mathrm{bps/Hz}], \tag{2.7}$$

donde $[X]^+$ representa la parte positiva de X.

2.2.1. Escenario de ejemplo

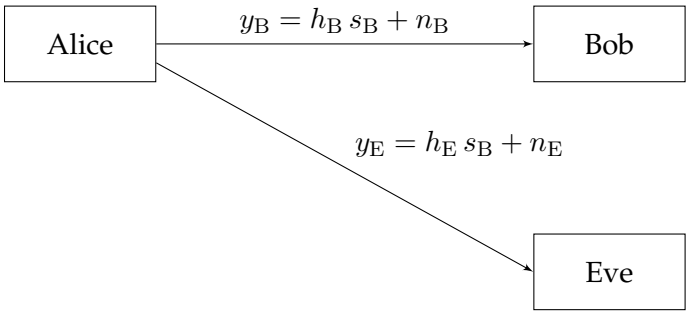


FIGURA 2.1: Modelo de sistema del escenario de ejemplo con un usuario legítimo y un fisgón, ambos mono-antena.

Con el fin de comprender mejor el concepto de PLS, se presenta un escenario simple de redes celulares con tres participantes: la BS, Alice, un usuario legítimo, Bob, y un fisgón, Eve. En este escenario, ver Fig. 2.1, Alice desea transmitir información de forma segura a Bob sabiendo que otro usuario de la misma red, Eve, del que conoce su CSI, pretende interceptar dicha comunicación. Para ello, calcula la cantidad de información

que les llegaría a cada uno de los usuarios. Simplificando (2.1) al escenario propuesto y fijándonos en una sola antena, se obtiene que la señal recibida por Bob es:

$$y_{\mathrm{u}} = h_{\mathrm{u}} s_{\mathrm{u}} + n_{\mathrm{u}}, \tag{2.8}$$

donde h_{u} $u \in \{\mathrm{B}, \mathrm{E}\}$ es la respuesta impulsiva del canal entre Alice y cada uno de los usuarios que incluye por simplicidad todas las características del canal radio: pérdidas por propagación, las ganancia de las antenas, las pérdidas por desadaptación y polarización, etc. En esta expresión no hay interferencia, puesto que al único usuario al que se le transmite información es a Bob. Por ello, se tiene que la SINR converge a SNR:

$$\gamma_{\mathrm{u}} = \overline{\gamma}_{\mathrm{u},0} \left| h_{\mathrm{u}}^{\mathrm{eq}} \right|^2 \left| s_{\mathrm{u}} \right|^2, \tag{2.9}$$

donde $\overline{\gamma}_{\mathrm{u},0}$ es el valor medio de la SNR y $h_{\mathrm{u}}^{\mathrm{eq}}$ no es más que la h_{u} normalizada con media unitaria, pero con su mismo comportamiento estadístico.

Actualizando las expresiones (2.2) y (2.6) en (2.7) se obtiene la cantidad de información segura que puede transmitir Alice a Bob libre de errores y segura [29] como:

$$R_{\mathrm{S}}(\gamma_{\mathrm{B}}, \gamma_{\mathrm{E}}) \underset{\gamma_{\mathrm{B}} > \gamma_{\mathrm{E}}}{=} \left[\log_2(1+\gamma_{\mathrm{B}}) - \log_2(1+\gamma_{\mathrm{E}}) \right]^+ \quad [\mathrm{bps/Hz}]. \tag{2.10}$$

La aleatoriedad de los canales radio hace que los valores de h_{u} cambien constantemente y, por consiguiente, se suela hablar de su valor estadístico, definido por su distribución de probabilidad. Por ende, la cantidad de información obtenida en (2.10) se trata de un valor instantáneo y para obtener su valor medio hay que obtener la media según [30, Ec. 5-29]:

$$\begin{aligned} \overline{R}_{\mathrm{s}} &= \iint R_{\mathrm{s}} \, f_{\mathrm{B}}(x) \, f_{\mathrm{E}}(x) \, d\gamma_B \, d\gamma_E \\ &= \frac{1}{\ln 2} \int_0^{\infty} \frac{F_{\gamma_E}(x) \left[1 - F_{\gamma_B}(x)\right]}{1+x} dx \quad [\mathrm{bps/Hz}], \end{aligned} \tag{2.11}$$

donde $f_{\mathrm{B}}(x)$ y $f_{\mathrm{E}}(x)$ son las funciones de densidad de probabilidad (PDFs) de γ_{B} y γ_{E} respectivamente, mientras que $F_{\mathrm{B}}(x)$ y $F_{\mathrm{E}}(x)$ son sus funciones de distribución acumulada (CDFs). Esta información forma parte de la CSI adquirida por Alice en el modo *normal* de operación descrito al comienzo de esta sección.

A continuación, se realiza una simulación en Matlab para mostrar gráficamente lo que ocurre. Para ello, se utiliza el canal AWGN [31] como referencia y se compara con un escenario como el mostrado en la Fig. 2.1 en el que se añade una simulación para comprobar las expresiones teóricas proporcionadas. En él, se asume que los canales son Rayleigh con desvanecimientos lentos y sin visión directa [32]. El canal del fisgón se fija con una media $\overline{\gamma}_{\mathrm{E}} = 5$ dB y se va variando la media del canal de Bob. El resultado se muestra en la Fig. 2.2, donde adicionalmente se ha representado un valor límite cuando se tiene que el canal de Bob es mucho mejor que el de Eve ($\overline{\gamma}_{\mathrm{B}} \gg \overline{\gamma}_{\mathrm{E}}$). En este caso, la

expresión en (2.11) converge a [33] $\overline{R}_{\mathrm{s}} = \overline{R}_{\mathrm{B}} - \overline{R}_{\mathrm{E}}$, donde $\overline{R}_{\mathrm{B}}$ y $\overline{R}_{\mathrm{E}}$ son la capacidad del canal de Bob e Eve respectivamente. En esta Fig. 2.2 se sombrea en verde la cantidad de información que se puede transmitir de forma segura y en rojo la zona donde se podría transmitir información, pero cuya seguridad estaría comprometida.

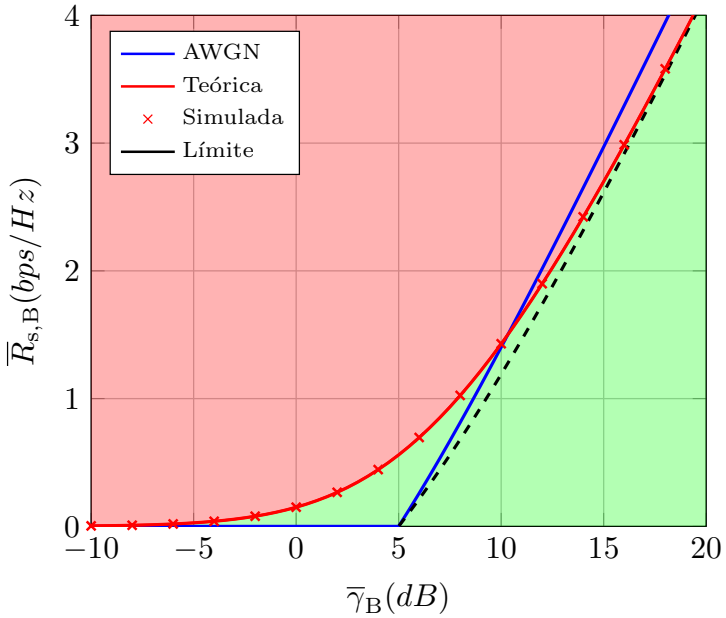


FIGURA 2.2: Cantidad de información segura de Bob con $\overline{\gamma}_{\mathrm{E}} = 5$ dB.

Cabe destacar la sección de la Fig. 2.2 desde los -10 dB hasta los 5 dB. En esta zona, y bajo un canal AWGN, no existe posibilidad de transmitir de forma segura. Sin embargo, esto no ocurre cuando se considera un canal Rayleigh con desvanecimientos. Esto se debe a que la métrica es un valor medio donde instantáneamente el canal del fisgón, con mejor media, puede obtener un nivel de señal inferior al del legítimo. Esto se ilustra en la Fig. 2.3. En ella se muestran dos ejemplos de canales Rayleigh con 2000 muestras (instantes temporales): un primer canal con media normalizada, representando el canal del usuario legítimo con 0 dB, y otro con una media superior de 10 dB representando al fisgón. Pese a la diferencia de potencia media, hemos destacado una de las zonas en las que durante una ventana de tiempo, entre las muestras 659 y 688, el canal con peor media podría recibir información segura.

2.2.2. Escalado con el número de antenas

Este escenario de ejemplo presentado en la sección anterior puede complicarse al incorporar la existencia de múltiples antenas en la BS. Debido a que no existe IUI, puesto que tan solo se transmite a un usuario legítimo, la aplicación de *maximum ratio transmission* (MRT) [34] para aprovechar la diversidad de antena modificaría levemente el escenario. En concreto, la expresión en (2.9) se vería modificada como sigue:

$$\gamma_{\mathrm{u}} = \overline{\gamma}_{\mathrm{u},0} G \left|h_{\mathrm{u}}^{\mathrm{eq}}\right|^2 \left|s_{\mathrm{u}}\right|^2, \tag{2.12}$$

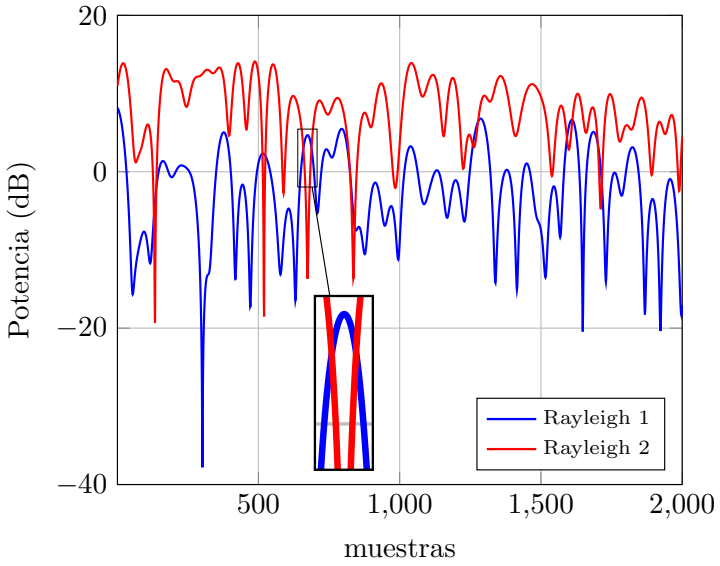


FIGURA 2.3: Canales Rayleigh con 0 dB (Rayleigh 1) y 10 dB (Rayleigh 2) de media en su SNR con 2000 muestras de tiempo.

donde ahora $\overline{\gamma}_{\mathrm{u},0}$ es el valor medio de SNR del canal cuando se transmite con una única antena, $h_{\mathrm{u}}^{\mathrm{eq}}$ es un parámetro que recoge todo el comportamiento estadístico de los canales, pero unitario en potencia, y G es la ganancia obtenida por usar MRT con M antenas en transmisión. Bajo el modelo de propagación habitual en comunicaciones móviles, frente de onda plano (PW), esta ganancia es idéntica al número de antenas empleadas. De esta forma, se tiene que la SNR del canal crece linealmente con el número de antenas, como se muestra en la Fig. 2.4. Este escalado que se aprecia en la figura parece crecer con la SNR indefinidamente con el número de antenas. Sin embargo, esto no es físicamente posible. El resultado es consecuencia de utilizar un modelo de propagación inadecuado para el sistema planteado, el modelo de propagación en campo lejano, modelo PW. Si la frecuencia se mantiene constante, **a medida que el número de antenas crece, la dimensión eléctrica del *array* de antenas se vuelve comparable a la distancia con los usuarios y, en consecuencia, la condición de campo lejano deja de cumplirse.** Este hecho no ha sido relevante debido a que los escenarios sobre los que se planteaba no consideraban un gran número de antenas, sin embargo esto ha dejado de ser así, viéndose sistemas de transmisión con centenas de antenas. En estas condiciones, la condición de campo lejano deja de cumplirse y es necesario buscar modelos de propagación que se ajusten mejor a estos nuevos escenarios. En [15] se propone un modelo más completo, el SW, que incorpora al PW como caso particular, que tiene un escalado con el número de antenas más realista (ver Fig. 2.4). Cabe destacar que tanto la dimensión eléctrica del array de antenas como la condición de campo lejano son dependientes de la frecuencia. Específicamente, si todos los demás parámetros se mantienen fijos, subir en frecuencia provoca que el tamaño eléctrico del *array* disminuye y también hace que la condición de campo lejano se cumpla a una distancia menor.

Además de un comportamiento físico más realista, este modelo de propagación presenta una característica muy interesante en el ámbito de PLS: permite decorrelar usuarios que se encuentren en la misma dirección (ver Fig. 2.5). Esto significa que se puede reducir IUI separándolos no solo angularmente, como sucede en PW, sino que también con la distancia. Desde un punto de vista de PLS esto significa que existen menos zonas donde la comunicación a un usuario pueda ser interceptada. Asimismo, en la Fig. 2.5 se muestra como esta interferencia puede ser reducida con el número de antenas.

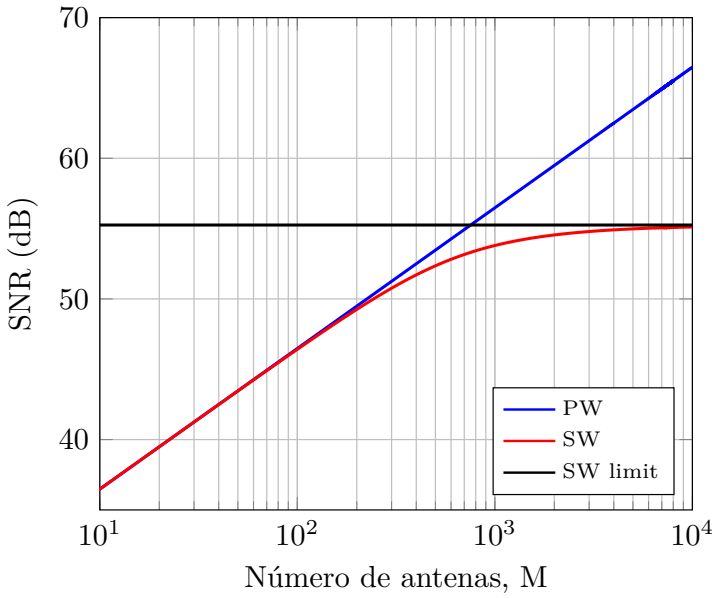


FIGURA 2.4: Escalado de la SNR en decibelios con el número de antenas, M, para los modelos PW y SW con 50 dB de P_{Tx} a una distancia de 15 m del centro del *array* sobre la frecuencia de 2,4 GHz.

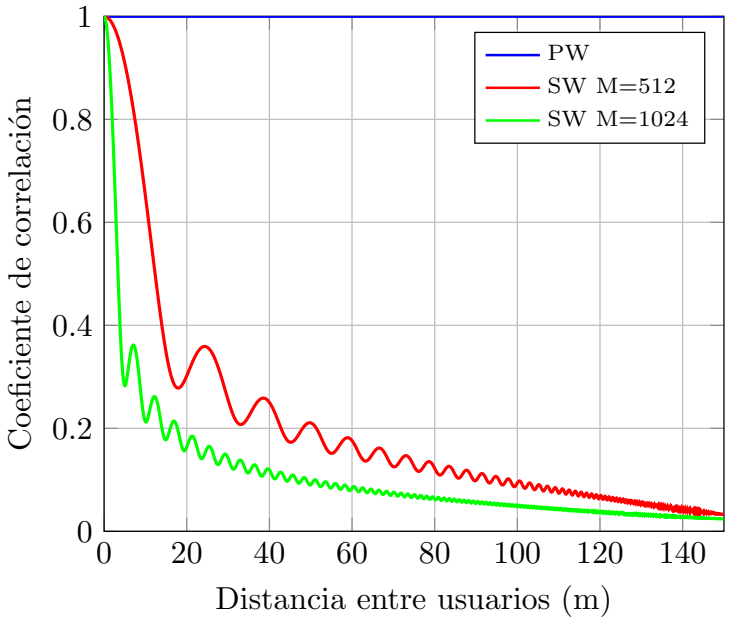


FIGURA 2.5: Correlación entre los canales del usuario legítimos y el fisgón con la distancia para los modelos PW y SW.

2.3. Modelo de propagación

La aparición del 5G y la inminente llegada del 6G lleva asociada un incremento en los requisitos de las redes móviles [2], [35], [36]. Entre otros objetivos, aumentar el volumen de datos transmitidos, como el número de usuarios conectados es crucial para estas tecnologías. Con el fin de alcanzar estos requisitos, aumentar el número de antenas de forma masiva, XL-MIMO [13], o reducir el tamaño de las celdas [14] son algunas de las soluciones propuestas. Sin embargo, esto provoca que el clásico modelo de propagación en campo lejano deje de tener validez [13], [15], [16]: tanto el aumento del tamaño de las antenas, como la reducción en el tamaño de las celdas, hacen que el tamaño físico de la antena en la BS y la distancia a los usuarios empiecen a ser comparables.

En [15] y, posteriormente extendido en [16], se propone un modelo de propagación esférica para modelar estos escenarios con XL-MIMO. Se presenta un modelo, que incluye al modelo de propagación de onda plana como caso particular, basado en tres regiones definidas por la diferencia de fase en los elementos del *array* de antenas. Una primera región de campo lejano definida por la distancia de *Rayleigh*, $r_{\text{Rayl}} = \frac{2D^2}{\lambda}$, donde $D = Md$ es el tamaño físico del *array*, λ es la longitud de onda y d es la separación entre los elementos del *array*. En esta región se tiene que la amplitud y la diferencia de fase es constante para todos los elementos del *array* y, por tanto, el frente de onda es plano. A continuación, se define una región intermedia, a la que llaman *upper near-field*, en la que la fase deja de ser constante. Finalmente, define una última región, llamada *lower near-field*, donde tanto la fase como la amplitud varían para cada uno de los elementos del *array*. Esta última región, delimitada por la distancia *crítica*, $r_{\text{Crit}} \approx 9D$ [15], es en la que centraremos el trabajo en este ámbito. La razón es que en ella se observa como la interferencia entre usuarios no sólo depende de la posición angular con respecto al *array*, sino que también depende de la distancia.

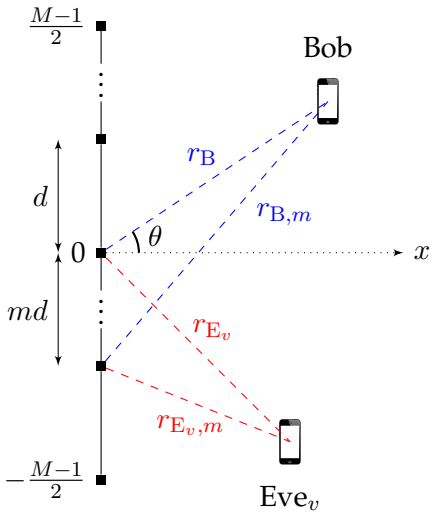


FIGURA 2.6: Modelo de sistema del escenario de ejemplo con SW, una BS de M elementos, un usuario legítimo mono-antena y varios fisgones todos mono-antena.

El cambio de paradigma en el modelo de propagación implica que se debe actualizar el escenario presentado en la sección anterior Sec. 2.2.1. En concreto, se propone un escenario sencillo como el de la Fig. 2.6, donde ahora se tienen en cuenta los elementos que conforman los $M \gg 1$ elementos de la antena, las distancias a los usuarios, $r_{\mathrm{k,m}}$, de estos elementos y la posición angular de los usuarios, θ_{k}, con respecto al centro del *array*. Se considera un *array* lineal uniforme (ULA) situado a lo largo del eje de ordenadas, y, donde la distancia a cada uno de los usuarios se puede definir como:

$$r_{\mathrm{k,m}} = r_{\mathrm{k}}\sqrt{1 - 2md_{\mathrm{k}}\sin\theta_{\mathrm{k}} + d_{\mathrm{k}}^2 m^2},\ m \in \left[-\tfrac{M}{2}, \tfrac{M}{2}\right], \tag{2.13}$$

donde $r_{\mathrm{k},0} = r_{\mathrm{k}}$ y $d_{\mathrm{k}} = \frac{d}{r_{\mathrm{k}}}$, siendo $d = \frac{\lambda}{2}$. De (2.13), podemos obtener el vector de respuesta del *array* para cada usuario k como:

$$\mathbf{a}_{\mathrm{k}} = [a_1(r_{\mathrm{k}}, \theta_{\mathrm{k}}), a_2(r_{\mathrm{k}}, \theta_{\mathrm{k}}), \ldots, a_{\mathrm{M}}(r_{\mathrm{k}}, \theta_{\mathrm{k}})]^{\mathrm{T}}, \tag{2.14}$$

donde el elemento m del vector se puede expresar, en función del modelo de propagación, como:

$$a_m^{\mathrm{SW}}(r_{\mathrm{k}}, \theta_{\mathrm{k}}) = \tfrac{\sqrt{\beta_0}}{r_{\mathrm{k,m}}}\mathrm{e}^{-\mathrm{j}\frac{2\pi}{\lambda}r_{\mathrm{k,m}}} \tag{2.15}$$

y

$$a_m^{\mathrm{PW}}(r_{\mathrm{k}}, \theta_{\mathrm{k}}) = \tfrac{\sqrt{\beta_0}}{r_{\mathrm{k}}}\mathrm{e}^{-\mathrm{j}\frac{2\pi}{\lambda}r_{\mathrm{k}}}\mathrm{e}^{-\mathrm{j}2\pi m\sin\theta_{\mathrm{k}}}, \tag{2.16}$$

respectivamente, y siendo β_0 la potencia del canal a la distancia de referencia $r_{\mathrm{ref}} = 1$ m [16]. A partir de estos vectores se puede obtener la señal recibida utilizando directamente (2.1) y, en consecuencia, el resto de métricas necesarias para el estudio desde una perspectiva de PLS.

Capítulo 3

Resumen de los resultados

Este capítulo presenta los principales resultados obtenidos en esta tesis. En el ámbito de las comunicaciones móviles y PLS se ha estudiado cómo el incremento en el número de antenas afecta a las redes celulares. Esto ha desembocado en una primera contribución que busca una forma sencilla y eficiente de aprovechar la diversidad de antena en transmisión. En concreto, el mecanismo de TAS basado en PLS que busca reducir la información fugada a los fisgones. En segundo lugar, se ha presentado una posible vulnerabilidad en estos sistemas basados en PLS. Esta consiste en que el usuario que pretende interceptar la comunicación puede engañar a la BS para que no pueda caracterizar correctamente el estado de su canal. Por último, el incremento en el número de antenas para dar servicio a cada vez más usuarios ha llevado a replantearse la validez del modelo de propagación en campo lejano. En este sentido, se ha presentado un modelo de sistema con PLS alternativo al clásico de propagación de onda plana en campo lejano. Este modelo, basado en un modelo de propagación esférico, contempla la propagación tanto en campo lejano como en campo cercano. Además de ser un modelo más completo, presenta ciertas características que dotan al sistema de mayor flexibilidad, grado de libertad (DoF), para diseñar los enlaces radio. Asimismo, se propone una estrategia de precodificación segura y, conjuntamente, selección de usuarios para redes móviles que incorpora las particularidades de este modelo de propagación.

El capítulo está organizado de la siguiente manera. En la Sección 3.1 se introduce el nuevo método de selección de antena propuesto basado en minimizar las fugas hacia el fisgón y se compara con los utilizados habitualmente en TAS. En la Sección 3.2 se presentan los fundamentos del ataque propuesto y cómo afectaría a un modelo de sistema con selección de antena, como el propuesto en la sección anterior. Finalmente, las aplicaciones a PLS del modelo de propagación esférica se presentan en la Sección 3.3.

3.1. Selección de antena

La gran cantidad de antenas disponibles en los sistemas celulares [13] ha llevado al diseño de complejas técnicas de *beamforming* [37], [38] para mejorar la seguridad de las comunicaciones móviles. Esto, sin embargo, conlleva un elevado incremento tanto en

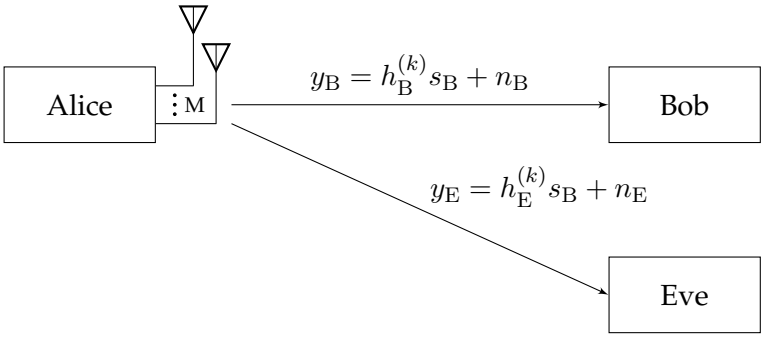


FIGURA 3.1: Modelo de sistema con selección de antena. El mensaje transmitido en DL z_{B} por la BS (Alice) a través de la antena k seleccionada según cierto criterio TAS.

computación y como en complejidad [39], [40]. Por consiguiente, se propone un modelo basado en TAS [39] que tan solo requiere una cadena de radiofrecuencia (RF) y, en consecuencia, se reduce la complejidad [41], [42]. Estos esquemas se han utilizado en el ámbito de PLS clásicamente bajo una estrategia sub-óptima basada únicamente en el canal del usuario legítimo [42]-[45]. Esto se debe a que la solución óptima requeriría un conocimiento perfecto de la CSI tanto del usuario legítimo como del fisgón [46] que, en la práctica, no siempre es posible. A pesar de ello, es habitual suponer el conocimiento de dicha CSI en escenarios como *non-orthogonal multiple access* (NOMA) [47] o al menos conocer su distribución estadística [48].

El primer resultado de esta tesis es la propuesta de un modelo TAS basado en el canal del fisgón. En concreto, se presenta para un escenario como el presentado en la Sección 2.2: un escenario de comunicaciones móviles, Fig. 3.1, donde la BS está equipada con una antena de M elementos, pero tan solo una cadena de RF y, por tanto, utiliza TAS para aprovechar su diversidad de antena. Asimismo, se consideran tan solo dos usuarios, como en el escenario propuesto en la Sección 2.2.1, donde los canales se consideran con desvanecimientos lentos cuasi-estáticos y distribución Rayleigh [33]. Además, se asume que la CSI de los usuarios puede ser adquirida durante el modo de funcionamiento *normal* de la BS, ver Sección 2.2. Utilizando la expresión en (2.3) se puede obtener la expresión de la SNR de los usuarios como:

$$\gamma_{\mathrm{B}} = \overline{\gamma}_{\mathrm{B},0} \left| h_{\mathrm{B}}^{\mathrm{TAS}} \right|^2 |s_{\mathrm{B}}|^2 \tag{3.1}$$

y

$$\gamma_{\mathrm{E}} = \overline{\gamma}_{\mathrm{E},0} \left| h_{\mathrm{E}}^{\mathrm{TAS}} \right|^2 |s_{\mathrm{B}}|^2 , \tag{3.2}$$

donde $\overline{\gamma}_{\mathrm{B},0}$ y $\overline{\gamma}_{\mathrm{E},0}$ son los valores medios de SNR si tan solo se utilizase una antena en transmisión y $h_u^{\mathrm{TAS}} = h_u^{(k)}, u \in \{\mathrm{B}, \mathrm{E}\}$ son los coeficientes del canal entre cada antena k y el receptor de cada usuario. Asimismo, se asume que los canales $h_u^{\mathrm{k}} \in \left[h_u^{(1)}, \ldots, h_u^{(M)} \right]$ están normalizados con media unidad $\mathbb{E}\{|h_{\mathrm{u}}^{(i)}|^2\} = 1, \forall i \in [1, \ldots, M]$ y la señal transmitida también $\mathbb{E}\{|s_{\mathrm{B}}|^2\} = 1$.

A partir de estas expresiones se puede obtener la cantidad de información segura que se puede transmitir usando (2.11). Es importante mencionar que la variación en esta métrica está directamente relacionada con la de los canales equivalentes h_u^{TAS}, puesto que el resto de términos son constantes. En el caso de utilizar una antena aleatoria, sin ningún criterio, no se obtendría ninguna ganancia de la diversidad de antenas en la BS y, por consiguiente, el escenario converge al mostrado en la Sección 2.2.1. A continuación, se muestra cómo afecta a la cantidad de información segura que se puede transmitir el hecho de utilizar otros criterios más inteligentes.

3.1.1. TAS óptimo

En primer lugar, se considera el criterio de selección de antena transmisora, TAS, que mayor cantidad de información segura permite transmitir [46]. Este método, en adelante selección de antena transmisora óptima (OTAS), se basa en obtener la antena k que maximiza la expresión en (2.10):

$$k = \underset{1\leq i\leq M}{\arg\max}\left\{ \log_2 \left(\underbrace{\frac{1+\overline{\gamma}_{\mathrm{B}_0}\left|h_{\mathrm{B}}^{(i)}\right|^2}{1+\overline{\gamma}_{\mathrm{E}_0}\left|h_{\mathrm{E}}^{(i)}\right|^2}}_{X_i} \right) > 0 \right\}, \tag{3.3}$$

donde la variable aleatoria a maximizar, X_i, requiere conocimiento perfecto de la CSI tanto del canal legítimo como del fisgón, puesto que se define como un ratio entre la SNR de los canales del usuario legítimo y del fisgón. A partir de este criterio, se puede obtener la máxima tasa de información segura como:

$$\overline{R}_{\mathrm{s}}^{\mathrm{O-TAS}} = \mathbb{E}\left\{ \log_2 \left(\frac{1+\overline{\gamma}_{\mathrm{B}_0}\left|h_{\mathrm{B}}^{(k)}\right|^2}{1+\overline{\gamma}_{\mathrm{E}_0}\left|h_{\mathrm{E}}^{(k)}\right|^2} \right) > 0 \right\} \quad [\mathrm{bps/Hz}]. \tag{3.4}$$

Para el cálculo de la tasa segura en OTAS se utilizan los resultados obtenidos en [46, eq. (13)], cuyas expresiones son algo complejas debido a la distribución estadística de la variable aleatoria (RV) X_i en (3.3):

$$\overline{R}_{\mathrm{s}}^{\mathrm{O-TAS}} = \int_0^\infty x\left(2^x \ln 2\right) M \left[1 - \frac{\bar{\gamma}_m \exp\left(\frac{1-2^x}{\bar{\gamma}_m}\right)}{\bar{\gamma}_m + \bar{\gamma}_w 2^x}\right]^{M-1} \times \tag{3.5}$$

$$\left[\exp\left(\frac{1-2^x}{\bar{\gamma}_m}\right) \frac{\bar{\gamma}_m + \bar{\gamma}_m\bar{\gamma}_w + \bar{\gamma}_w 2^x}{\left(\bar{\gamma}_m + \bar{\gamma}_w 2^x\right)^2}\right] \mathrm{d}x \quad [\mathrm{bps/Hz}], \tag{3.6}$$

donde $\bar{\gamma}_m$ y $\bar{\gamma}_w$ es lo que se ha denominado $\overline{\gamma}_{\mathrm{B}_0}$ y $\overline{\gamma}_{\mathrm{E}_0}$ respectivamente.

3.1.2. TAS basado en Bob

En la literatura, usualmente no se recurre al método de selección óptima debido a que el conocimiento perfecto de la CSI del canal del fisgón no siempre está disponible [42]-[45]. Por esta razón, se suele utilizar un criterio sub-óptimo basado tan solo en la información del canal del usuario legítimo, en adelante, selección de antena transmisora basada en Bob (BTAS). Este método TAS sub-óptimo [49] busca seleccionar la antena que mejor canal consigue para el usuario legítimo. Este método no requiere ninguna información de los fisgones, puesto que no intervienen en ningún momento en el criterio de decisión. Además, cabe destacar que la información completa del canal legítimo tampoco es necesaria, ya que el índice de la antena óptima sería suficiente. Este índice se puede obtener mediante un canal de realimentación o *feedback* de baja tasa, o ser estimado mediante un detector de energía [39]. De esta forma, el criterio de selección de antena en (3.3) se relaja:

$$h_{\mathrm{B}}^{\mathrm{B-TAS}} = \underset{i=1,\ldots,M}{\max} \left\{ \left| h_{\mathrm{B}}^{(i)} \right|^2 \right\}, \tag{3.7}$$

donde la distribución estadística de este nuevo canal equivalente, $h_{\mathrm{B}}^{\mathrm{B-TAS}}$, se puede obtener a partir de la distribución de los canales $h_{\mathrm{B}}^{(i)}$. En el caso de suponer que los canales son independientes e idénticamente distribuidos, $h_{\mathrm{B}}^{(i)}\, \forall i = 1, ..., M$, se puede aplicar el estadístico de orden M [50] para obtener la distribución del canal definido por el criterio (3.7) como:

$$F_{\mathrm{B}}^{M}(x) = F(x)^M, \tag{3.8}$$

donde $F(x)$ es la CDF que tienen los canales $h_{\mathrm{B}}^{(i)}$. Destacar que la distribución de los canales del usuario legítimo dependen del número de antenas M. Sin embargo, puesto que desde el punto de vista del fisgón la selección de antena puede considerarse aleatoria, su distribución del canal, $h_{\mathrm{E}}^{\mathrm{B-TAS}}$, no se ve alterada por el criterio de selección.

A fin de obtener una expresión para la tasa de información segura, se supone que los coeficientes del canal $h_{\mathrm{B}}^{(i)}$ siguen una distribución normal ($N(0, \sigma)$) compleja de forma que su módulo siga una distribución Rayleigh ($R(\sigma)$) [51, p. 148-149], donde este canal se utiliza en la literatura para modelar escenarios con desvanecimientos y sin visión directa en redes celulares [32]. A partir de esta distribución de $|h_{\mathrm{B}}^{(i)}|$, se puede obtener la de su SNR utilizando:

$$X \sim Exponencial(x|\lambda) \Rightarrow Y = \sqrt{2X\sigma^2\lambda} \sim Rayleigh(y|\sigma), \tag{3.9}$$

donde se tiene que la distribución de su SNR, definida por la potencia del canal, sigue una distribución exponencial:

$$F_{\mathrm{E}}(x, \beta) = 1 - \exp\left(\frac{-x}{\beta}\right), \tag{3.10}$$

donde $\beta = 1/\lambda$ es la media de la distribución exponencial.

Finalmente, se utiliza (2.11) con las expresiones de la CDF de Bob (3.8) e Eve (3.10) para obtener la máxima tasa de información segura media que se puede tener con el esquema BTAS:

$$\begin{aligned}\overline{R}_{\mathrm{s}}^{\mathrm{B-TAS}} =& \frac{1}{\ln 2}\int_0^\infty \frac{F_{\exp}(x,\overline{\gamma}_{\mathrm{E}_0})\left[1-F_{\exp}^M(x,\overline{\gamma}_{\mathrm{B}_0})\right]}{1+x}dx \\ =& \frac{1}{\ln 2}\sum_{k=1}^{M}\binom{M}{k}(-1)^{k+1}\Delta\mathcal{E}\left(\frac{k}{\overline{\gamma}_{\mathrm{B}_0}},\frac{1}{\overline{\gamma}_{\mathrm{E}_0}}+\frac{k}{\overline{\gamma}_{\mathrm{B}_0}}\right) \quad [\mathrm{bps/Hz}],\end{aligned} \tag{3.11}$$

donde $\Delta\mathcal{E}(\cdot)$ es una función auxiliar definida como

$$\Delta\mathcal{E}\left(A,B\right) = e^A\mathrm{E}_1(A) - e^B\mathrm{E}_1(B), \tag{3.12}$$

donde $\mathrm{E}_1(\cdot)$ es la función exponencial integral [52, eq. (5.1.1)].

3.1.3. TAS basado en Eve

A continuación, se presenta el método de selección de antena original de este trabajo: selección de antena transmisora basada en Eve (ETAS). El objetivo de este método es mejorar las prestaciones del sistema en el ámbito de PLS. Para ello, se centra únicamente en el canal del fisgón. La razón de este enfoque se detalla en la sección 3.1.6: se observa cómo el método sub-óptimo presentado anteriormente en la sección 3.1.2 y el óptimo 3.1.1 tienden a conseguir la misma tasa de transmisión segura cuando el canal del usuario legítimo es mucho mejor que la del fisgón: $1+\overline{\gamma}_{\mathrm{B}_0}\left|h_{\mathrm{B}}^{(i)}\right|^2 \gg 1$ en (3.4). Si el canal del fisgón no se ve afectado, se tiene que $X_i \approx 1+\overline{\gamma}_{\mathrm{B}_0}\left|h_{\mathrm{B}}^{(i)}\right|^2$. De esta forma, ambos métodos convergen. Sin embargo, existen escenarios donde los fisgones pueden recibir altos niveles de señal: véase el caso de escenarios con usuarios cercanos [53] o fisgones con mejores canal que los legítimos [54]. Estos casos se encuentran claramente alejados de la suposición anteriormente mencionada. De hecho, sería el denominador de X_i el que dominase en el criterio de selección de antena. Por esta razón, sugerir un método de selección de antena basado en el canal del fisgón parece legítimo.

En la búsqueda de maximizar X_i en (3.3) parece evidente que se puede aumentar el numerador o reducir el denominador. El esquema sub-óptimo presentado en la sección 3.1.2 busca lo primero y el que se propone, en adelante ETAS, busca lo segundo: maximizar la tasa de información segura reduciendo la capacidad del canal del fisgón. Para ello, debe determinar la antena que presente el peor canal de cara al fisgón:

$$h_{\mathrm{E}}^{\mathrm{E-TAS}} = \min_{i=1,\ldots,M}\left\{\left|h_{\mathrm{E}}^{(i)}\right|^2\right\}, \tag{3.13}$$

donde la distribución estadística de $h_{\mathrm{E}}^{\mathrm{E-TAS}}$ se puede obtener de forma análoga a la realizada anteriormente para $h_{\mathrm{B}}^{\mathrm{B-TAS}}$ utilizando el estadístico de primer orden [50]:

$$F_{\mathrm{E}}^{1}(x) = 1 - \left[1 - F(x)\right]^{M}, \tag{3.14}$$

donde $h_{\mathrm{E}}^{(i)}\, \forall i = 1, ..., M$ se suponen independientes e idénticamente distribuidos. De la misma forma que en BTAS, el canal fuera del criterio de selección no se ve alterado, puesto que la elección de antena desde su punto de vista es aleatoria y, por tanto, igual a la de una única antena.

Finalmente, se puede obtener la máxima tasa de información segura media para el esquema ETAS substituyendo (3.14) y (3.10) en (2.11):

$$\begin{aligned}\overline{R}_{\mathrm{s}}^{\mathrm{E-TAS}} =& \frac{1}{\ln 2}\int_{0}^{\infty} \frac{F_{\mathrm{E}}^{1}(x)\left[1 - F_{\exp}(x, \overline{\gamma}_{\mathrm{B}_0})\right]}{1+x} dx \\ =& \frac{1}{\ln 2}\Delta\mathcal{E}\left(\frac{1}{\overline{\gamma}_{\mathrm{B}_0}}, \frac{M}{\overline{\gamma}_{\mathrm{E}_0}} + \frac{1}{\overline{\gamma}_{\mathrm{B}_0}}\right) \quad [\mathrm{bps/Hz}],\end{aligned} \tag{3.15}$$

Se puede destacar como la expresión de (3.15) es prácticamente idéntica a la obtenida por Bloch en [55, eq. 5] para el caso de utilizar usuarios con una única antena y con desvanecimientos Rayleigh. La única diferencia observable en (3.15) es que la SNR media del fisgón se ve reducida por un factor M. Esto implica que la SNR efectiva del fisgón se ve reducida conforme aumenta el número de antenas, hecho que es evidentemente beneficioso para la PLS.

3.1.4. MRT

Alternativamente a los criterios de selección de antena, MRT [34] es un método ampliamente utilizado en la literatura para aprovechar la diversidad de antena en transmisión. Este método se basa en utilizar el vector de precodificación $\mathbf{w}_{\mathrm{B}}^{\mathrm{MRT}} \in \mathbb{C}^{M\times 1}$, visto en (2.1), durante la transmisión *downlink* (DL) en modo *seguro* para adaptar la señal transmitida al canal instantáneo de Bob [34] y maximizar la señal recibida:

$$\mathbf{w}_{\mathrm{B}}^{\mathrm{MRT}} = \frac{\mathbf{h}_{\mathrm{B}}}{||\mathbf{h}_{\mathrm{B}}||} = \frac{[h_{\mathrm{B}}^{(1)}, \ldots, h_{\mathrm{B}}^{(M)}]}{\sqrt{\sum_{i=1}^{M} |h_{\mathrm{B}}^{(i)}|^2}}, \tag{3.16}$$

donde $\mathbf{h}_{\mathrm{B}} \in \mathbb{C}^{M\times 1}$ son los coeficientes del canal legítimo de cada una de las antenas. De esta forma, se tiene que el canal equivalente de Bob, $h_{\mathrm{B}}^{\mathrm{eq}}$, es $\mathbf{h}_{\mathrm{B}}^{\mathrm{H}}\mathbf{w}_{\mathrm{B}}^{\mathrm{MRT}}$ y el de Eve, $h_{\mathrm{E}}^{\mathrm{eq}}$, es $\mathbf{h}_{\mathrm{E}}^{\mathrm{H}}\mathbf{w}_{\mathrm{B}}^{\mathrm{MRT}}$.

Debido a que el esquema MRT se ajusta al canal legítimo se puede demostrar que la distribución del canal del fisgón [56, ec. 24, Anexo A] no se ve alterada, es decir, sigue una distribución exponencial. Sin embargo, sí cambia la del usuario legítimo. Como se explicó en la Sección 3.1.2, la distribución de la SNR de los canales $|h_{\mathrm{B}}|^2$ sigue una distribución exponencial. De esta forma, se puede demostrar que el canal equivalente

$|h_{\mathrm{B}}^{\mathrm{eq}}|^2 = |\mathbf{h}_{\mathrm{B}}^{\mathrm{H}}\mathbf{w}_{\mathrm{B}}^{\mathrm{MRT}}|^2$ es una suma de M exponenciales. Esto resulta en una distribución Gamma con parámetros de escala y forma $\overline{\gamma}_{\mathrm{B}_0}$ y M, respectivamente [57]:

$$F_{\mathrm{B}}(x) = 1 - \exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{B}}}\right)\sum_{n=0}^{M-1}\left(\frac{x}{\overline{\gamma}_{\mathrm{B}}}\right)^n\frac{1}{n!}, \tag{3.17}$$

donde se tiene que la media de la distribución es $\overline{\gamma}_{\mathrm{B}} = M\overline{\gamma}_{\mathrm{B}_0}$.

El fisgón es incapaz de aprovechar la diversidad de antena del sistema, hecho que se refleja en las SNRs: la del fisgón al no variar es $\overline{\gamma}_{\mathrm{E}} = \mathbb{E}\{\gamma_{\mathrm{E}}\} = \overline{\gamma}_{\mathrm{E}_0}$ y la del usuario legítimo $\overline{\gamma}_{\mathrm{B}} = \mathbb{E}\{\gamma_{\mathrm{B}}\} = M\overline{\gamma}_{\mathrm{B}_0}$. Nótese que $\overline{\gamma}_{\mathrm{E}}$ no está influenciado por el número de antenas, M, ya que el vector de *beamforming*, $\mathbf{w}_{\mathrm{B}}^{\mathrm{MRT}}$, no está adaptado a su canal, puesto que la transmisión no se dirige hacia este usuario. La cantidad de información segura que se puede transmitir, como en los casos anteriores, se puede obtener sin más que sustituir (3.17) y (3.10) en (2.11).

3.1.5. ZF

Como alternativa al uso de MRT existe otra técnica para aprovechar la diversidad de antena en transmisión, ampliamente utilizado, cuyo objetivo es distinto: de igual forma que MRT busca maximizar la señal recibida, ZF [58] busca adaptar el mensaje mediante el vector de precodificación $\mathbf{w}_{\mathrm{B}}^{\mathrm{ZF}} \in \mathbb{C}^{M\times 1}$ para eliminar la interferencia entre usuarios:

$$\mathbf{w}_{\mathrm{B}}^{\mathrm{ZF}} = \frac{\mathbf{h}_{\mathrm{B}}}{\mathbf{h}_{\mathrm{B}}{}^{\mathrm{H}}\mathbf{h}_{\mathrm{B}}}. \tag{3.18}$$

Este vector de precodificación $\mathbf{w}_{\mathrm{B}}^{\mathrm{ZF}}$ se trata de una proyección ortogonal del canal h_{B} en el subespacio ortogonal con el resto de usuarios. De esta forma, se evita la interferencia entre usuario. Del mismo modo, puede emplearse ZF para conseguir un nulo de señal en Eve, a costa de tener que conocer su CSI.

Bajo la misma distribución de canal que en el caso anterior 3.1.4, una distribución exponencial, se puede obtener la del canal equivalente $|h_{\mathrm{B}}^{\mathrm{eq}}|^2 = |\mathbf{h}_{\mathrm{B}}^{\mathrm{H}}\mathbf{w}_{\mathrm{B}}^{\mathrm{ZF}}|^2$. En concreto, se demuestra en [59] que la distribución dicho canal equivalente usando ZF es:

$$F_{\mathrm{B}}(x,a,b) = \frac{1}{\Gamma(a)^b}x^{a-1}\exp -\frac{x}{b}, \tag{3.19}$$

donde $\Gamma(\cdot)$ es la función gamma, $a = M - K + 1$ y $b = \overline{\gamma}_{\mathrm{B}}$. Estos parámetros a y b son los parámetros de forma y escala respectivamente de una distribución gamma: $F_{\mathrm{B}}(x,a,b) \sim \Gamma(M-K+1,\overline{\gamma}_{\mathrm{B}})$.

3.1.6. Resultados

En esta sección se presentan los resultados obtenidos para los diferentes esquemas propuestos en esta sección con respecto a PLS. En todos los casos se incluyen simulaciones de MC para comprobar la validez de los resultados analíticos.

En la Fig. 3.2 se evalúa la capacidad secreta media (ASC) para los tres esquemas TAS presentados, en función de la SNR media en el receptor del usuario legítimo $\overline{\gamma}_{\mathrm{B}_0}$ y con un valor fijo de $\overline{\gamma}_{\mathrm{E}_0} = 10$ dB. Los casos con $M = 2$ y $M = 8$ antenas se han incluido con líneas discontinuas y continuas respectivamente. Se observa como el mejor resultado lo obtiene, evidentemente, el esquema OTAS y que su diferencia con los sub-óptimos aumenta con M. Cabe destacar que el esquema clásico, BTAS, tan solo obtiene mejores resultados que el esquema propuesto, ETAS, cuando $\overline{\gamma}_{\mathrm{B}_0}$ es lo suficientemente alta (en torno a los 15 dB). Esta pequeña diferencia de rendimiento entre ambos esquemas sub-óptimos apenas se modifica al aumentar el número de antenas. Sin embargo, existe un rango de valores de SNR (hasta los ≈ 12 dB) para el que ETAS funciona mejor que BTAS, donde la SNR del usuario legítimo y el del fisgón son comparables.

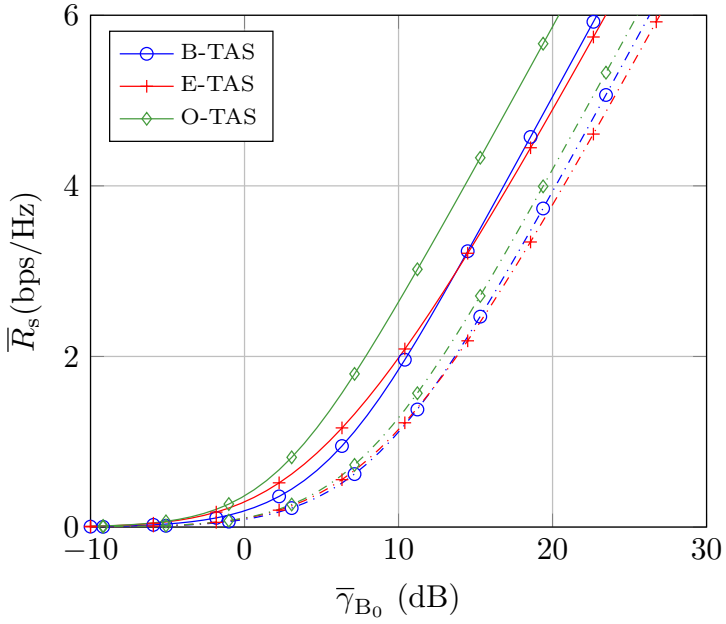


FIGURA 3.2: $\overline{R}_{\mathrm{s}}$ en función de $\overline{\gamma}_{\mathrm{B}_0}$ para los esquemas O-TAS, B-TAS y E-TAS con $\overline{\gamma}_{\mathrm{E}_0} = 10$ dB. Los escenarios con $M = \{2, 8\}$ antenas se representan con líneas discontinuas con puntos y continuas respectivamente. Los marcadores corresponden con simulaciones de MC.

Con el fin de destacar el efecto del fisgón, en la Fig. 3.3 se evalúa la ASC en función de $\overline{\gamma}_{\mathrm{E}_0}$ para un valor fijo de $\overline{\gamma}_{\mathrm{B}_0} = 10$ dB. De nuevo, se consideran los casos con $M = 2$ y $M = 8$. En esta nueva figura se puede ver cómo el esquema OTAS actúa como límite superior de los esquemas sub-óptimos. Además, se observa como a medida que crece la SNR del fisgón el esquema ETAS no sólo supera al BTAS convencional, sino que también empieza a comportarse de forma muy parecida al esquema OTAS. En los extremos, donde predomina la SNR de uno de los usuarios, el esquema sub-óptimo que mejor se

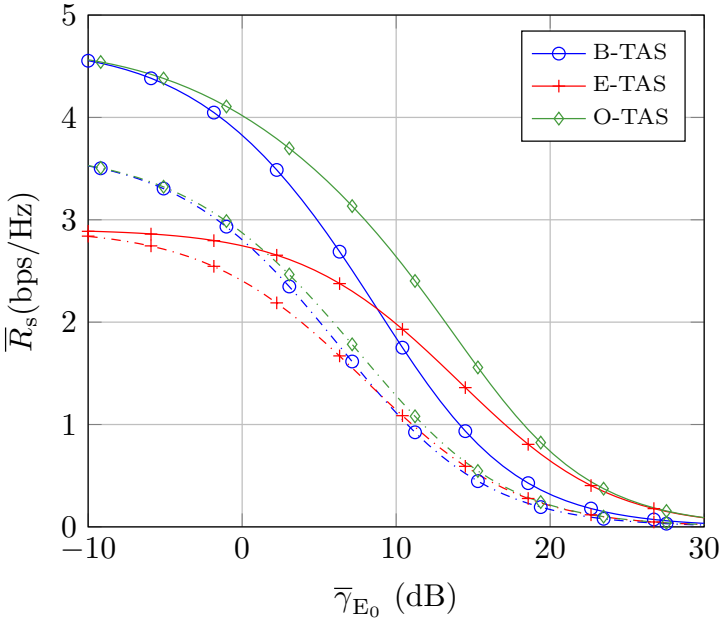


FIGURA 3.3: $\overline{R}_{\mathrm{s}}$ en función de $\overline{\gamma}_{\mathrm{E}_0}$ para los esquemas O-TAS, B-TAS y E-TAS con $\overline{\gamma}_{\mathrm{B}_0} = 10$ dB. Los escenarios con $M = \{2, 8\}$ antenas se representan con líneas discontinuas con puntos y continuas respectivamente. Los marcadores corresponden con simulaciones de MC.

aproxima a OTAS es aquel cuyo parámetro predominante es el utilizado en el criterio de selección de antena, véase (3.7) y (3.13). De hecho, la ASC disminuye en todos los casos a medida que crece la SNR del fisgón y aumenta cuando se utilizan más antenas.

A continuación, se pretende poner de manifiesto la pérdida de rendimiento relativa con respecto al esquema TAS óptimo de los esquemas propuestos. Para ello, en la Fig. 3.4 se representa la ASC normalizada al del caso OTAS en función de la relación $\overline{\gamma}_{\mathrm{E}_0}/\overline{\gamma}_{\mathrm{B}_0}$. El caso con $M = 8$ antenas se utiliza a modo de ejemplo junto con tres valores diferentes de $\overline{\gamma}_{\mathrm{B}_0}$. Como se ha mencionado anteriormente, el mejor esquema sub-óptimo varía considerablemente en función del canal dominante; por ello, se incluyen puntos negros para resaltar cuándo el mejor esquema cambia de BTAS a ETAS. De la figura se pueden extraer varias conclusiones:

- ETAS se aproxima más al esquema óptimo en un rango más amplio de valores de SNR.
- ETAS es el mejor esquema sub-óptimo cuando nos encontramos con fisgones que reciben un alto nivel de señal (régimen de *strong eavesdropper*).
- Aumentar el nivel de SNR de ambos usuarios es beneficioso para el esquema ETAS, mientras que el esquema BTAS ve degradado su rendimiento con cualquier mejora que sufra el fisgón, pese a que el valor relativo con el usuario legítimo permanezca constante.
- Se puede observar como un esquema de transmisión adaptativo capaz de alternar entre los criterios sub-óptimo ETAS y BTAS en función de la SNR media y del índice

de antena mejoraría sustancialmente la tasa de información segura que se puede transmitir.

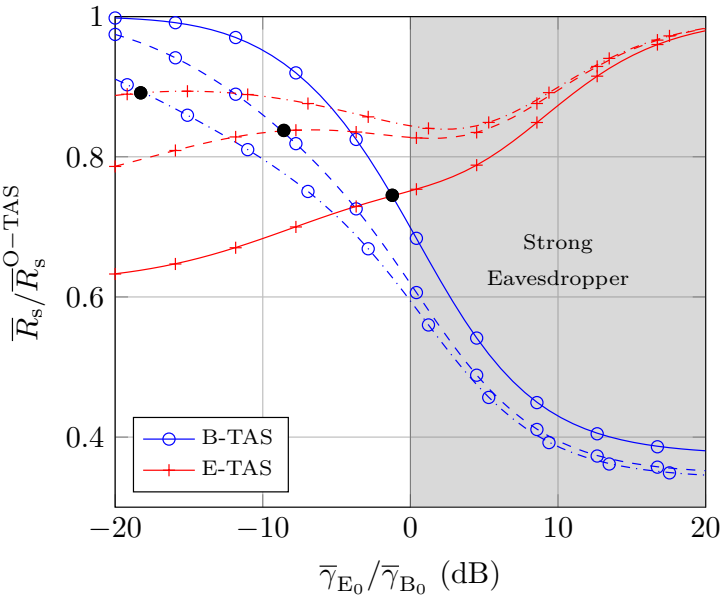


FIGURA 3.4: $\overline{R}_{\mathrm{s}}$ normalizada a O-TAS en función de $\overline{\gamma}_{\mathrm{E}_0}/\overline{\gamma}_{\mathrm{B}_0}$ para diferentes valores de $\overline{\gamma}_{\mathrm{B}_0} = \{10, 20, 30\}$ dB y $M = 8$. Estos valores se corresponden con líneas continuas, discontinuas y discontinuas con puntos respectivamente. Los marcadores corresponden con simulaciones de MC. Los valores de SNR donde se cruzan los dos esquemas se identifican con puntos negros sólidos para cada pareja de curvas.

Se repite la figura anterior, pero normalizando la ASC con respecto a otro esquema de diversidad de antena fuera de TAS. En concreto, al MRT que es ampliamente utilizado en la literatura cuando se desea maximizar la potencia recibida. De esta Fig. 3.5 se pueden destacar las siguientes características:

- ETAS sigue obteniendo resultados más cercanos al de referencia y durante un rango de valores de SNR más amplio.
- Pese a que ETAS sufre una gran degradación con el valor más bajo de nivel SNR (línea continua), sigue siendo bastante bueno cuando el canal de Eve es mucho mejor que el de Bob. Sin embargo, BTAS deja de comportarse como el esquema de referencia donde mejor resultados obtiene y, además, es muy parecido al ETAS cuando el nivel de SNR de ambos usuarios es alto.
- En esta ocasión, aumentar el nivel de señal supone una mejoría en las métricas normalizadas para ambos esquemas sub-óptimos. Esto es efecto de la normalización, puesto que las métricas sin normalizar siguen los mismos patrones que las anteriores.

A continuación, en la Fig. 3.6 se muestra la ASC normalizada con respecto al resultado que se obtiene al aplicar una estrategia ZF, cuyo objetivo es eliminar la interferencia al resto de usuarios o en este caso, la información fugada. Se puede observar como es el peor caso de todos, puesto que ningún esquema sub-óptimo se acerca al que proporciona

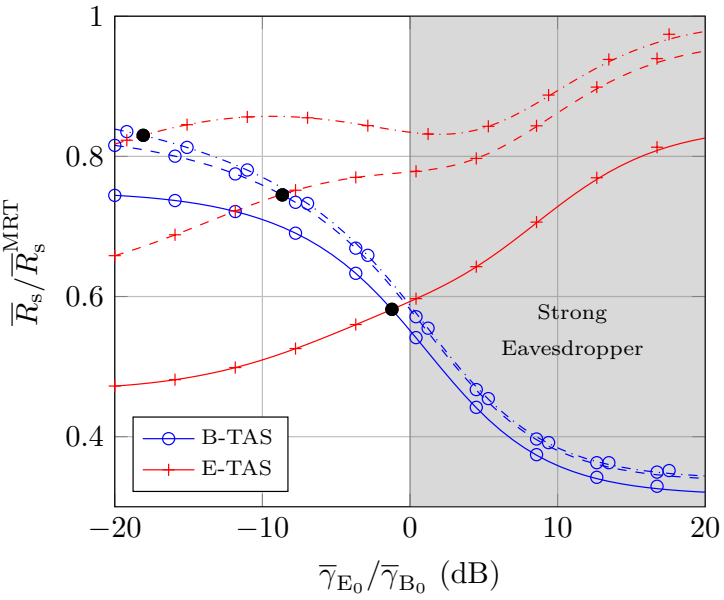


FIGURA 3.5: $\overline{R}_{\mathrm{s}}$ normalizada a MRT con en función de $\overline{\gamma}_{\mathrm{E}_0}/\overline{\gamma}_{\mathrm{B}_0}$ para diferentes valores de $\overline{\gamma}_{\mathrm{B}_0} = \{10, 20, 30\}$ dB y $M = 8$. Estos valores se corresponden con líneas continuas, discontinuas y discontinuas con puntos respectivamente. Los marcadores corresponden con simulaciones de MC. Los valores de SNR donde se cruzan los dos esquemas se identifican con puntos negros sólidos para cada pareja de curvas.

ZF. Asimismo, cualquier mejora de la SNR de Eve empeora el resultado. Esto se debe al carácter inherente al ZF: anular la interferencia. Conforme mejor canal tiene el fisgón, más importancia tendrá utilizar la diversidad de antena para anular la señal que le llegue, en lugar de maximizar la potencia transmitida hacia el usuario legítimo. Tan solo en la zona que no está sombreada, donde el fisgón tiene peor canal que el usuario legítimo, se observan comportamientos similares a los comentados anteriormente en esta sección. Aunque no se aprecie en la figura, cabe destacar que el comportamiento no se debe a que la $R_{\mathrm{s}}^{\mathrm{ZF}}$ aumente, pues permanece constante en todo el barrido (no se ve afectado por el fisgón). Se debe a que el resto de esquemas obtienen menor R_{s} conforme el canal del fisgón mejora con respecto al del usuario legítimo, como se observa en la Fig. 3.7.

Finalmente, en la Fig. 3.7 se muestra la ASC sin normalizar de todos los esquemas presentados en función de la SNR media del fisgón para dos valores de $\overline{\gamma}_{\mathrm{B}_0} = \{10, 30\}$ dB y $M = 8$. De esta figura se pueden extraer las siguientes conclusiones:

- Los esquemas MRT y ZF obtienen mejores resultados que los TAS, aunque estos requieren más conocimiento de los canales y son más complejos, puesto que tienen que diseñar los vectores de precodificación.
- ZF destaca claramente como el mejor esquema. Siempre obtiene mejores resultados que TAS, especialmente en la zona donde el fisgón es fuerte, y mejores que MRT en todo el barrido, salvo cuando el canal de Bob domina considerablemente y, por tanto, centrarse en mejorar su SNR es más beneficioso que empeorar la de Eve. Cabe destacar que la diferencia entre ZF y el resto se acentúa notablemente cuando

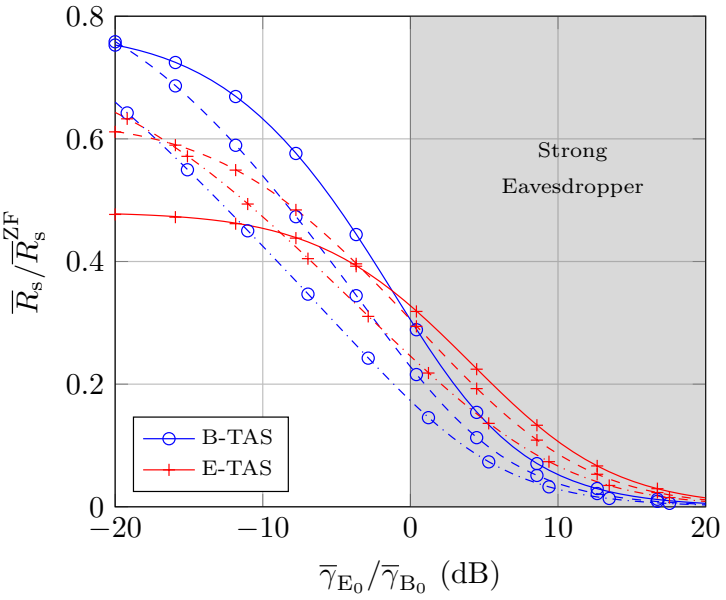


FIGURA 3.6: $\overline{R}_{\mathrm{s}}$ normalizada a ZF en función de $\overline{\gamma}_{\mathrm{E}_0}/\overline{\gamma}_{\mathrm{B}_0}$ para diferentes valores de $\overline{\gamma}_{\mathrm{B}_0} = \{10, 20, 30\}$ dB y $M = 8$. Estos valores se corresponden con líneas continuas, discontinuas y discontinuas con puntos respectivamente. Los marcadores corresponden con simulaciones de MC. Los valores de SNR donde se cruzan los dos esquemas se identifican con puntos negros sólidos para cada pareja de curvas.

la potencia transmitida al usuario legítimo aumenta. Esto se debe a que ZF prioriza siempre anular totalmente la información fugada al fisgón.

- Los esquemas TAS, pese a ser más sencillos, obtienen resultados similares a MRT cuando el fisgón recibe un gran nivel de señal.

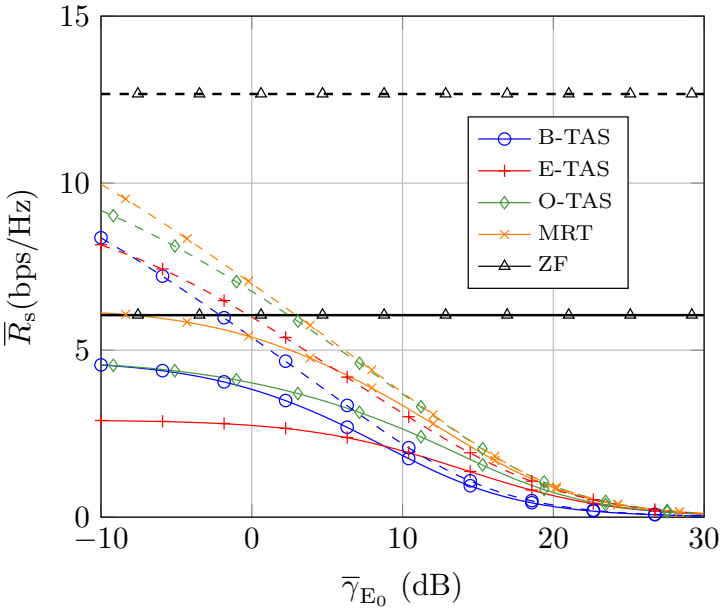


FIGURA 3.7: $\overline{R}_{\mathrm{s}}$ en función de $\overline{\gamma}_{\mathrm{E}}$ para los esquemas TAS presentados, MRT y ZF con $M = 8$. Los escenarios con $\overline{\gamma}_{\mathrm{B}_0} = \{10, 30\}$ dB se representan con líneas continuas y discontinuas respectivamente. Los marcadores corresponden con simulaciones de MC.

3.2. Ataque tipo canal producto

La seguridad en capa física tiene gran dependencia de la capacidad que tiene la BS de obtener la CSI del canal de los usuarios del sistema. En este sentido, los ataques como el *jamming* [60] que intentan entorpecer esta adquisición afectan directamente a la cantidad de información segura que se puede transmitir. Asimismo, en sistemas *massive* MIMO se han presentado otros ataques en la literatura, conocidos como *pilot contamination attack* [61] o *pilot spoofing* [62], en los que los fisgones engañan a la BS para que no pueda aprovechar su diversidad de antena. Esto lo consiguen haciendo creer a la BS que su canal mejora con el número de antenas. Con un enfoque distinto se presentó en [24] un ataque que busca hacer que la BS subestime su canal. El objetivo no es impedir que se transmita información, como en *pilot spoofing*, sino que busca que transmita más información de la que puede hacer de forma segura y, de esta forma, interceptarla.

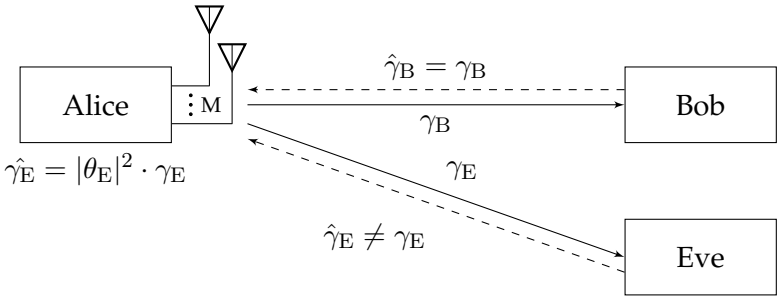


FIGURA 3.8: Modelo de sistema bajo ataque con un usuario legítimo y un fisgón, ambos con una única antena.

El ataque propuesto se realiza en la etapa de *uplink* (UL), durante el modo de operación *normal*. En esta etapa, el fisgón transmite todos sus símbolos, x_{E}, modificados por una variable sintética θ_{E} con media unitaria para evitar ser detectado el ataque. De esta forma, los símbolos transmitidos son $\tilde{x}_{\mathrm{E}} = x_{\mathrm{E}} \cdot \theta_{\mathrm{E}}$ con $\mathbb{E}\{|\tilde{x}_{\mathrm{E}}|^2\} = 1$ y la BS observará un canal $\hat{h}_{\mathrm{E}} \neq h_{\mathrm{E}}$ con la siguiente relación $\hat{h}_{\mathrm{E}} = \theta_{\mathrm{E}} \cdot h_{\mathrm{E}}$. El resultado es un modelo de sistema ligeramente distinto al presentado en la Fig. 3.1 donde el canal equivalente del usuario legítimo no se ve afectado, pero el del fisgón sí, ver Fig. 3.8. Debido a que se diseña el ataque para que $\hat{\gamma}_{\mathrm{E}} \geq \gamma_{\mathrm{E}}$ (se hace creer que el canal de Eve es peor de lo que realmente es), se tiene que la cantidad de información que cree la BS que puede transmitir de forma segura sea mayor o igual que la real $\overline{\mathfrak{R}}_{\mathrm{s}} \geq \overline{R}_{\mathrm{s}}$, donde $\overline{\mathfrak{R}}_{\mathrm{s}}$ corresponde con la $\overline{R}_{\mathrm{s}}$ en (2.11) cuando se utiliza $\hat{\gamma}_{\mathrm{E}}$ en lugar de γ_{E}. Esto significa que la BS diseñará la transmisión en DL, durante el modo *seguro*, en la zona roja de la Fig. 2.2.

Dependiendo de la distribución estadística de la variable sintética se tienen diferentes tipos de ataques. En esta tesis consideraremos dos casos: el ataque será uniforme si se asume que la variable sintética sigue distribución uniforme y unitaria en potencia, se tiene que debe cumplirse que $|\theta_{\mathrm{E}}|^2 \in [0, \sqrt{3}]$; por otro lado, se considera Rayleigh si se asume que la variable sintética sigue una distribución Rayleigh y unitaria en potencia, por lo que se tiene que cumplir que $|\theta_{\mathrm{E}}|^2 \sim Rayleigh(\sigma = \sqrt{2})$. A continuación, para

obtener la distribución del canal producto $\hat{\gamma}_{\mathrm{E}} = |\theta_{\mathrm{E}}|^2 \gamma_{\mathrm{E}}$ se usa la expresión:

$$F_{\hat{\mathrm{E}}}(z) = \int_0^\infty F_{\mathrm{E}}\left(\frac{z}{y}\right) f_{\mathrm{y}}(y)\, dy, \tag{3.20}$$

donde $f_{\mathrm{y}}(y)$ es la PDF de la variable sintética $y = |\theta_{\mathrm{E}}|$. Ahora, sin más que sustituir en (3.20) se obtiene que las CDFs de $\hat{\gamma}_{\mathrm{E}}$ son [24]:

$$F_{\hat{\mathrm{E}}}^{\mathrm{Uni}}(z) = 1 - \left[e^{-\frac{z}{3\overline{\gamma}_{\mathrm{E}}}} - \sqrt{\frac{z\pi}{3\overline{\gamma}_{\mathrm{E}}}}\mathrm{erfc}\left(\sqrt{\frac{z}{3\overline{\gamma}_{\mathrm{E}}}}\right)\right] \tag{3.21}$$

y

$$F_{\hat{\mathrm{E}}}^{\mathrm{Ray}}(z) = 1 - 2\sqrt{\frac{z}{\overline{\gamma}_{\mathrm{E}}}}\, K_1\left(\sqrt{\frac{4z}{\overline{\gamma}_{\mathrm{E}}}}\right), \tag{3.22}$$

donde la primera corresponde con el ataque uniforme, la segunda con el Rayleigh, $\mathrm{erfc}(\cdot)$ es la función de error complementaria y $K_1(\cdot)$ es la función de Bessel modificada de segunda especie y primer orden.

Se define el exceso de tasa segura, $\mathcal{D}$, como la diferencia entre la máxima tasa segura media y la máxima tasa segura comprometida media:

$$\mathcal{D} = \overline{\mathfrak{R}}_{\mathrm{s}} - \overline{R}_{\mathrm{s}} \geq 0 \quad [\mathrm{dB}]. \tag{3.23}$$

En la Fig. 3.9 se evalúa esta métrica $\mathcal{D}$ donde el eje x corresponde con la SNR media de Bob con MRT, es decir, $\overline{\gamma}_{\mathrm{B}}(\mathrm{d}B) = \overline{\gamma}_{\mathrm{B}_0}(\mathrm{d}B) + 10\log_{10} M$. Esto significa que para alcanzar un valor objetivo de $\overline{\gamma}_{\mathrm{B}}$, la potencia de transmisión se puede disminuir en un factor de M en comparación con el caso de utilizar una sola antena[1]. En otras palabras, establecer un valor fijo de $\overline{\gamma}_{\mathrm{B}}$ idealmente hace que $\overline{\gamma}_{\mathrm{E}}$ disminuya en un factor de M. Podemos extraer varias ideas importantes de la observación de la Fig. 3.9:

- El uso de desvanecimientos sintéticos uniformes parece la mejor opción desde la perspectiva del fisgón, ya que puede generarse de forma más sencilla y, al mismo tiempo, permite mayor exceso de tasa segura.
- El uso de un mayor número de antenas en Alice permite reducir $\mathcal{D}$ cuando la SNR es baja en Bob, principalmente debido a la reducción efectiva en $\overline{\gamma}_{\mathrm{E}}$ para un valor fijo de $\overline{\gamma}_{\mathrm{B}}$; sin embargo, como se ha comentado anteriormente, el escalado de $\overline{\gamma}_{\mathrm{B}}$ con M no se mantiene cuando el tamaño del conjunto de antenas crece [63]. Esto implica que el exceso de tasa segura no puede ser eliminado en la práctica haciendo $M \to \infty$.
- Se observa que, en el régimen de baja SNR, aumentar el número de antenas en Alice es en realidad perjudicial, ya que el exceso de tasa segura crece con M.

[1] Tenemos en cuenta que la escala de $\overline{\gamma}_{\mathrm{B}}$ con M no se mantiene en la práctica para antenas arbitrariamente grandes de M. Por lo tanto, si bien es útil para analizar el comportamiento de los conjuntos de antenas en la práctica, no debe utilizarse para fines asintóticos como $M \to \infty$ [63].

- Finalmente, cuando $\overline{\gamma}_{\mathrm{B}}$ aumenta llega a saturar el exceso de tasa segura, por lo tanto, no se obtiene ningún beneficio al acercar al usuario legítimo a Alice para reducir $\mathcal{D}$. Esto se puede apreciar si llevamos al límite la expresión en (3.23): $\mathcal{D} \underset{\overline{\gamma}_{\mathrm{B}}\to\infty}{\approx} \overline{\mathfrak{R}}_{\mathrm{E}} - \overline{R}_{\mathrm{E}}$, donde se observa que el resultado tan solo depende del fisgón. En concreto, depende de la diferencia entre la capacidad media del canal de Eve real, $\overline{R}_{\mathrm{E}}$, y la estimada o comprometida en Alice, $\overline{\mathfrak{R}}_{\mathrm{E}}$.

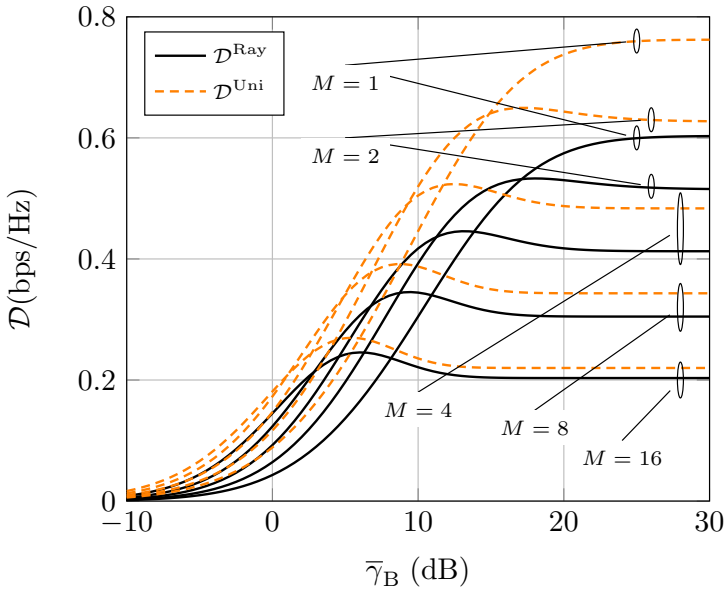


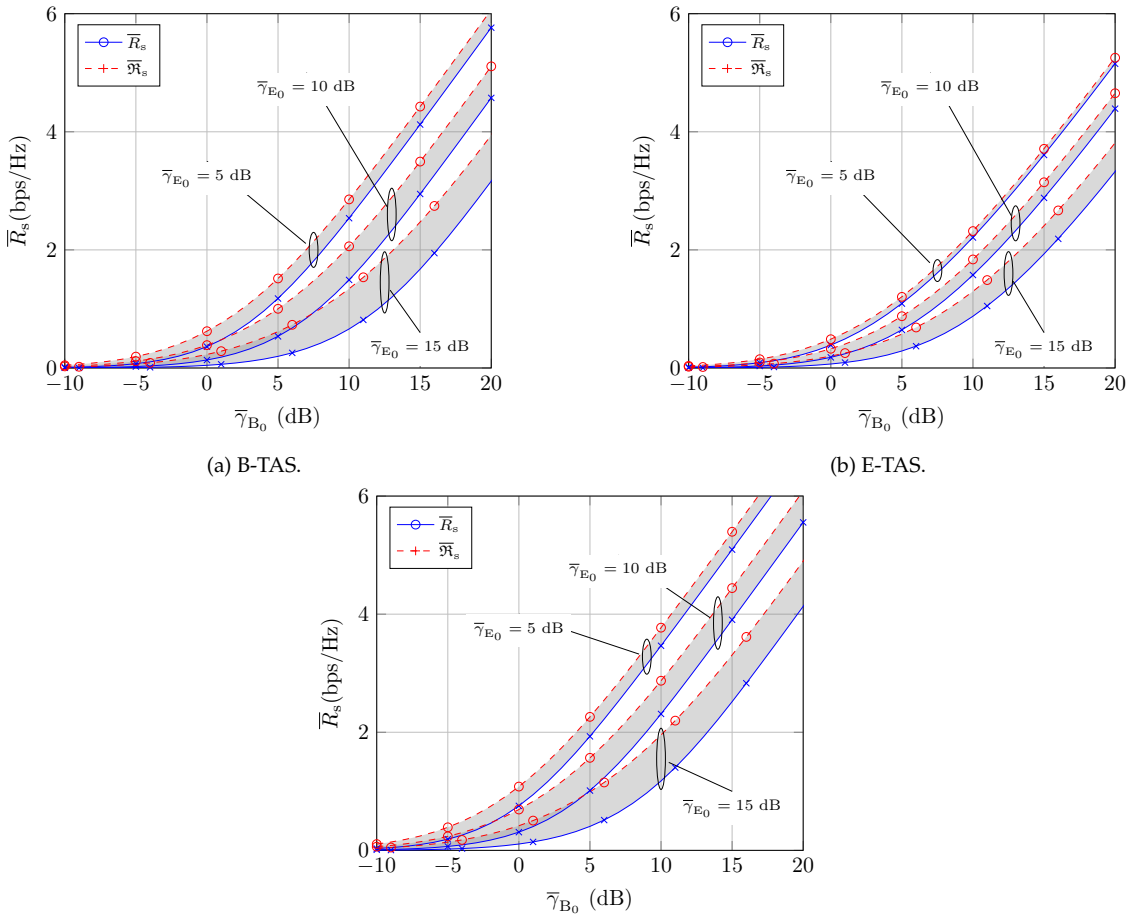
FIGURA 3.9: Exceso de tasa segura $\mathcal{D}$ con MRT en función de $\overline{\gamma}_{\mathrm{B}}$ para diferentes número de antenas y distribuciones de los desvanecimientos sintéticos θ_{E} con $\overline{\gamma}_{\mathrm{E}} = 15$ dB para $M = 1$ y después reducido por $10\log_{10} M$ (dB),

Con el fin de probar estos ataques, se compararán los resultados utilizando el esquema ETAS propuesto en la sección 3.1.3 frente a este tipo de ataques en términos de PLS bajo el desvanecimiento sintético más severo: el uniforme. Asimismo, se comparará con el esquema sub-óptimo utilizado habitualmente en la literatura, BTAS, y con MRT.

En la sección anterior se concluyó que, bajo una distribución de canal Rayleigh, la distribución del canal del fisgón sin ataque es exponencial tanto para MRT como para BTAS, mientras que para ETAS la distribución viene definida en la ecuación (3.14). Por otro lado, la distribución del canal legítimo también es exponencial para ETAS, mientras que para MRT y BTAS se definieron las CDF en (3.17) y (3.8) respectivamente. Si se aplica el cambio de variable $\overline{\gamma}_{\mathrm{E}}^{\mathrm{E-TAS}} = \overline{\gamma}_{\mathrm{E}}/M$ sobre (3.21) o (3.22), se tiene la expresión de la CDF del canal del fisgón bajo el ataque propuesto y utilizando ETAS.

A continuación se presentan los resultados obtenidos para los diferentes esquemas propuestos en la sección con respecto a PLS bajo un ataque con desvanecimientos sintéticos uniformes. En todos los casos se incluyen simulaciones MC para comprobar la validez de los resultados analíticos.

En la Fig. 3.10 se representa la máxima tasa secreta media, $\overline{R}_{\mathrm{s}}$, y la máxima tasa secreta comprometida media, $\overline{\mathfrak{R}}_{\mathrm{s}}$, para diferentes valores de $\overline{\gamma}_{\mathrm{E}}$ y un transmisor con múltiples



(a) B-TAS.

(b) E-TAS.

(c) MRT.

FIGURA 3.10: Máxima tasa segura media ($\overline{R}_s$) vs. tasa media comprometida ($\overline{\mathfrak{R}}_s$) en función de $\overline{\gamma}_{B_0}$ con $M = 4$, $\overline{\gamma}_{E_0} = \{5, 10, 15\}$ dB y desvanecimientos sintéticos uniformes. Los marcadores corresponden con simulaciones usando el método de MC.

antenas, $M = 4$, utilizando los dos esquemas TAS sub-óptimos analizados anteriormente y MRT. Se observa que en todos los casos la $\overline{\mathfrak{R}}_s$, que es la métrica con la que Alice diseña la transmisión en DL, excede el valor de $\overline{R}_s$. Por tanto,

Remark. *Cualquier tasa de transmisión, $\overline{R}$, dentro del área sombreada en gris, $\overline{R} \in \left[\overline{\mathfrak{R}}_s \leq \overline{R} < \overline{R}_s\right)$, es sensible a ser decodificada por el fisgón.*

Además, la diferencia entre $\overline{R}_s$ y $\overline{\mathfrak{R}}_s$ crece a medida que $\overline{\gamma}_E$ crece. Por lo tanto, para una configuración dada, el ataque es más efectivo cuanto mejor nivel de señal reciba el fisgón, es decir, cuanto más cerca de la BS se encuentre. Cabe destacar que para bajo nivel de señal en el fisgón, $\overline{\gamma}_{E_0} = 5$ dB, con ETAS prácticamente no afecta el ataque, mientras que en BTAS sigue existiendo un diferencia apreciable entre la tasa secreta real y la comprometida. El comportamiento con MRT es muy parecido al observado con BTAS donde el único cambio es un desplazamiento en el nivel medio de las métricas, puesto que MRT consigue mejores tasas de transmisión.

En la Fig. 3.11 se evalúa de nuevo la máxima tasa secreta media y la máxima tasa

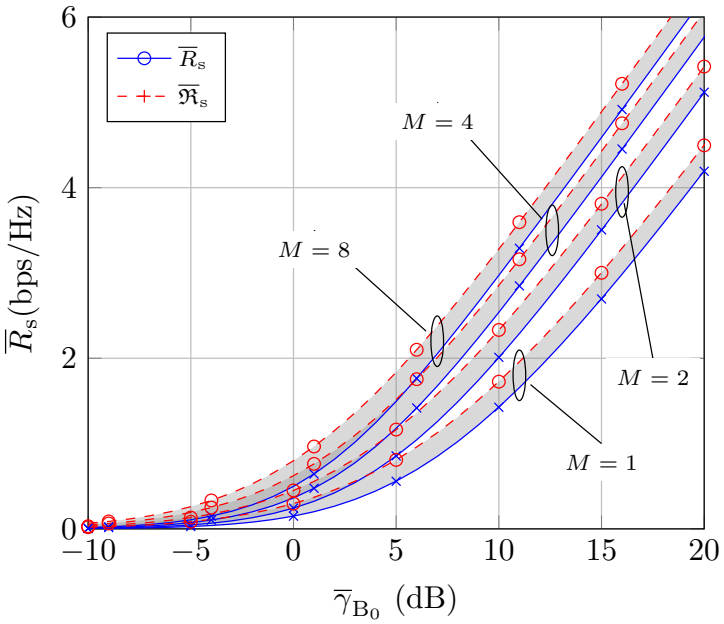


FIGURA 3.11: Máxima tasa segura media ($\overline{R}_{\mathrm{s}}$) vs. tasa media comprometida ($\overline{\mathfrak{R}}_{\mathrm{s}}$) utilizando B-TAS en función de $\overline{\gamma}_{\mathrm{B}_0}$ con $\overline{\gamma}_{\mathrm{E}_0} = 5$ dB, $M = 1, 2, 4, 8$ y desvanecimientos sintéticos uniformes. Los marcadores corresponden con simulaciones usando el método de MC.

secreta comprometida media, pero para diferentes configuraciones de antena y una SNR del fisgón fija en $\overline{\gamma}_{\mathrm{E}} = 5$ dB. Al contrario de lo que ocurre con la Fig. 3.10a, la diferencia entre las dos métricas, el exceso de tasa $\mathcal{D}$, aparentemente no varía con el número de antenas. Sin embargo, en la Fig. 3.12 se aprecia que esto no es cierto en todo el rango de SNR. En esta última figura se comparan los dos esquemas TAS sub-óptimos presentados junto al MRT y ZF para diferentes valores de antenas en transmisión y con una SNR del fisgón fija en $\overline{\gamma}_{\mathrm{E}} = 15$ dB. De la figura se pueden sacar las siguientes conclusiones:

- $\mathcal{D}$ tiende a quedarse en torno a $0{,}77$ bps/Hz independientemente del número de antenas para MRT y BTAS.
- MRT es considerablemente más sensible a este ataque que los esquemas TAS, efecto que aumenta con el número de antenas.
- El esquema ETAS es el que menos se ve afectado por este tipo de ataque, siendo bastante relevante su comportamiento con tan solo 8 antenas en transmisión.
- ZF no se ve afectado por los ataques. La alteración que sufre el canal debido al ataque es insuficiente para que ZF no consiga anular la señal que llega a los fisgones, es decir, $\overline{\mathfrak{R}}_{\mathrm{E}} = \overline{R}_{\mathrm{E}} = 0$ bps/Hz. En consecuencia, no existe ninguna diferencia entre el tasa secreta real y la comprometida.

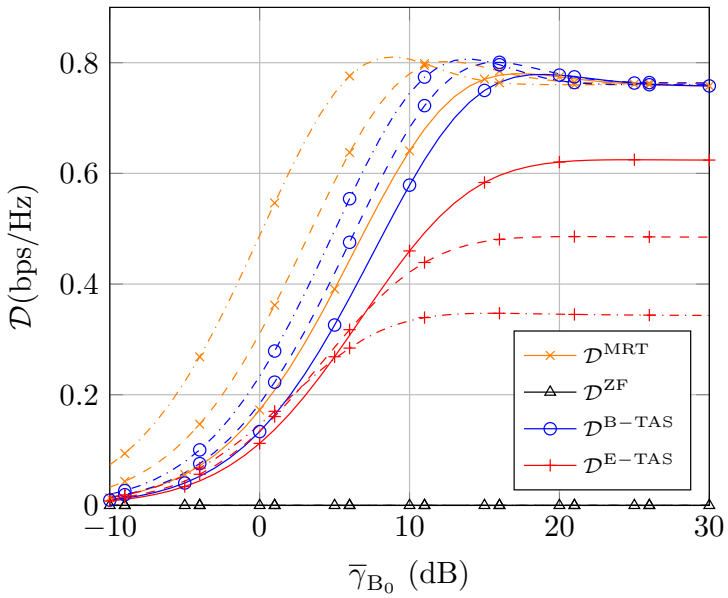


FIGURA 3.12: Exceso de tasa segura $\mathcal{D}$ utilizando MRT, ZF, B-TAS y E-TAS en función de $\overline{\gamma}_{\mathrm{B}_0}$ con $\overline{\gamma}_{\mathrm{E}} = 15$ dB y desvanecimientos sintéticos uniformes. Los casos de $M = 2, 4, 8$ antenas se representan con líneas continuas, discontinuas y discontinuas con puntos respectivamente.

3.3. Propagación esférica con un usuario

El cambio de paradigma en el modelo de propagación planteado en la sección 2.3 conlleva cambios en la forma de diseñar los enlaces hacia los usuarios. En concreto, en el denominado *campo cercano* aparecen nuevos grados de libertad a la hora de diseñar la transmisión a múltiples usuarios. Esto es debido a que la interferencia se ve reducida debida a la posición angular de los usuarios, como en el modelo clásico de propagación plana, pero también con la distancia. Esta interferencia, en el ámbito de la seguridad, puede ser vista como información fugada. Parece evidente el interés de estudiar cómo se puede aprovechar o cómo influye esto en el ámbito de PLS.

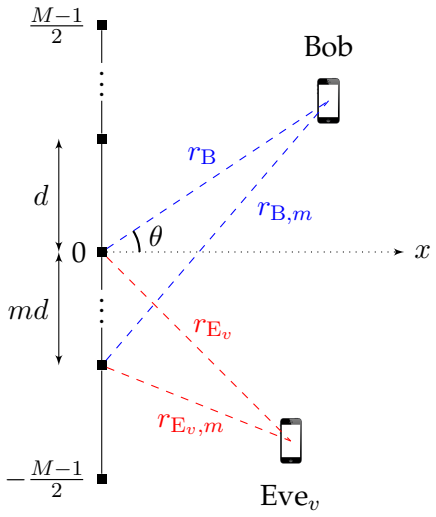


FIGURA 2.6: Modelo de sistema del escenario de ejemplo con SW, una BS de M elementos, un usuario legítimo mono-antena y varios fisgones todos mono-antena. (Repetida en la página 14).

En consecuencia, se propone un modelo sencillo como el de la Fig. 2.6 donde una BS equipada con una antena de $M \gg 1$ elementos da servicio de forma segura a un usuario legítimo en presencia de uno o varios fisgones. Con las expresiones de la sección 2.3 como base, se estudia el modelo con dos criterios diferentes de fisgones que afectarán a la métrica definida en (2.5). En primer lugar, uno en el que los fisgones no son capaces de colaborar, criterio *non-colluding*, entre ellos. Bajo esta condición, la información fugada viene determinada por el fisgón e que tiene la mayor LINR:

$$\mathrm{LINR}_{ncol}(v) = \mathrm{LINR}(e);\ e = \underset{j\in\mathcal{V};j\neq v}{\arg\,\max}\Big\{\mathrm{LINR}(j)\Big\} \quad [\mathrm{dB}]. \tag{3.24}$$

Por otro lado, se puede considerar un caso peor [6] donde los usuarios pueden colaborar entre ellos, criterio *colluding*:

$$\mathrm{LINR}_{col} = \sum_{v\in\mathcal{V}} \frac{p_{\mathrm{B}}|\mathbf{w}_{\mathrm{B}}^{\mathrm{H}}\mathbf{a}_v|^2}{\sigma_w^2} \quad [\mathrm{dB}], \tag{3.25}$$

TABLA 3.1: Configuración de los parámetros de simulación para un único usuario.

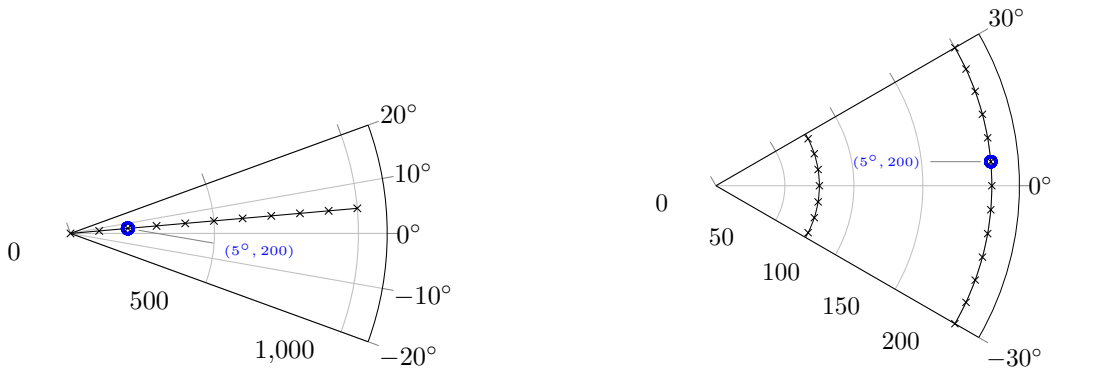
Parámetro	**Valor**
Longitud de onda	$\lambda = 0{,}1249$ m
Distancia entre antenas	$d = \frac{\lambda}{2}$ m
Número de antenas	$M = 1000$
SNR transmitida (β_0/σ_w^2)	25 dB
Distancia de referencia	$r_{\mathrm{B}} = 200$ m
Ángulo de referencia	$\theta_{\mathrm{B}} = \frac{\pi}{36}$ rad = 5°
Rango de distancias	$[1, 2(9Md) - 40]$ m
Rango angular	$[-\frac{\pi}{4}\frac{\pi}{4}]$ rad

donde se puede observar que debida a la colaboración entre los fisgones, también se considera que pueden cancelar la interferencia entre ellos mismos.

A continuación, se analizan tres escenarios donde se comparan los modelos PW y SW en términos de PLS. En estos tres escenarios se han definido una serie de parámetros comunes, ver Tabla 3.1, donde se ha considerado una simulación en distancia lo suficientemente amplia para observar la región de campo cercano definidas en la sección 2.3.

3.3.1. Escenario 1

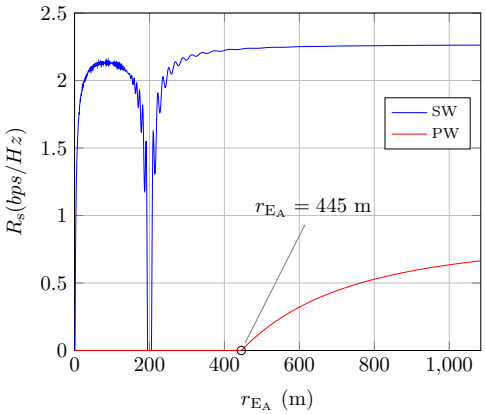
El primer escenario, ver Fig. 3.13, es un caso sencillo con sólo dos usuarios: uno de ellos actúa como Bob y el otro como $\mathrm{Eve}_{\mathrm{A}}$. En este caso, las distintas definiciones de LINR son equivalentes, ya que no existe la posibilidad de colaborar.



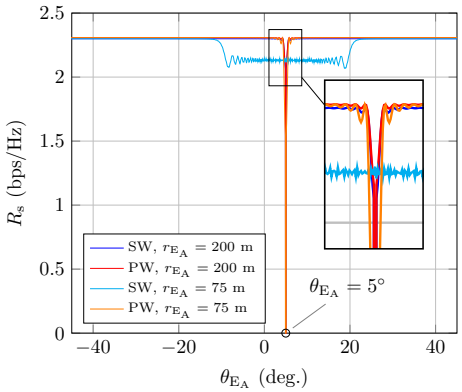
(a) Posición de los usuarios con Eve en 5° y distintas distancias.

(b) Posición de los usuarios con Eve a 75 y 200 m y distintas direcciones.

FIGURA 3.13: Representación gráfica de la posición de los usuarios en el escenario 1. La posición de Bob en (5°, 200 m) se señala con un círculo azul y las del fisgón que varía su posición con cruces negras.



(a) R_s en función de la distancia de Eve_A con la dirección fija a $\theta_{E_A} = 5°$.



(b) R_s en función de la dirección de Eve_A con la distancia fija a $r_{E_A} = [75, 200]$ m.

FIGURA 3.14: R_s en función de la posición de Eve_A en el escenario 1 con Bob fijo en $(10°, 200$ m).

La Fig. 3.14a muestra la máxima tasa de transmisión segura, R_s, para los modelos PW y SW en función de la distancia del fisgón a la BS, r_{E_A}, con ángulos fijos e idénticos $\theta_{E_A} = \theta_B = 5°$. En primer lugar, se observa como la tasa de transmisión segura es nula para el modelo PW hasta 445 m aproximadamente. Esto se debe a que la potencia de señal fugada hacia el fisgón, Eve, es mayor que la recibida por el propio usuario legítimo, Bob, hasta que este se encuentra más lejos de la estación base. Asimismo, no comienza justo en 400 m debido a que la interferencia entre usuarios cuando ambos están muy próximos es elevada. Cuando Eve está lo suficientemente lejos, tanto la interferencia entre usuarios como la información fugada a Eve disminuyen para producir valores positivos de tasa segura R_s. Además, en esta figura se observa como la reducción de interferencia con la distancia del modelo SW puede ser visto como un nuevo DoF aplicable a PLS, similar a la observación realizada en [15] para la tasa de transmisión libre de error: la interferencia en Eve al transmitir a Bob, es decir, la información fugada, se reduce con la distancia aunque Eve se encuentre en la misma dirección angular. Esto contrasta con lo observado para PW. Sin embargo, no es posible cancelar la interferencia si Eve está muy cerca de Bob, o en una región cercana a la BS independientemente del ángulo. Por último, tenemos que los modelos PW y SW no convergen cuando r_{E_A} crece. En cambio, tienden a permanecer separados en valores de $2,269$ bps/Hz para SW y $0,837$ bps/Hz para PW. Esta gran separación se debe a la distancia entre Bob y la BS, que no es suficiente para que se cumpla la hipótesis de campo lejano. Esto queda patente si se reduce el número de antenas del escenario, ver Fig. 3.15. Se puede obtener como la distancia de Rayleigh, distancia mínima para considerar campo lejano, es de $62,5$ km para los parámetros de la Tabla 3.1. Esta distancia se ve reducida en los casos mostrados en la Fig. 3.15 de la siguiente forma: $M = 500 \rightarrow 15,625$ km, $M = 250 \rightarrow 3,90625$ km y $M = 100 \rightarrow 625$ m. De esta forma, para el rango de distancias observado en la figura se observa como los modelos SW y PW se parecen cada vez más si se reduce el número de antenas.

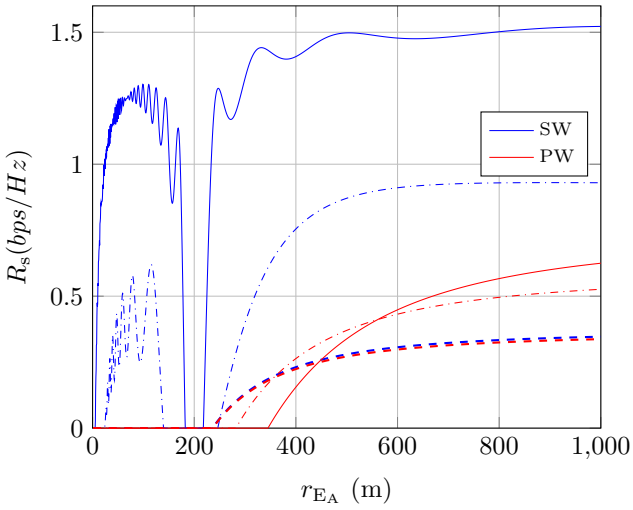


FIGURA 3.15: R_s en función de r_{E_A} para el escenario 1 con $\theta_{E_A} = 5°$ donde se han representado con líneas sólidas, discontinuas con puntos y discontinuas los casos con $M = [500, 250, 100]$ antenas respectivamente.

Fig. 3.14b muestra la tasa de transmisión segura para los modelos PW y SW en función del ángulo θ_{E_A} en grados (°) para un θ_B fijo. Además, comparamos la métrica cuando tenemos $r_{E_A} = r_B = 200$ m (líneas azul y roja) y $r_{E_A} = 75$ m y $r_B = 200$ m (líneas celeste y naranja). Cuando ambos usuarios, Eve y Bob, se encuentran a la misma distancia del *array* de antenas (líneas azul y roja), puede observarse que los modelos PW y SW ofrecen rendimientos similares. Una característica destacable de este escenario es que el ángulo es casi irrelevante, excepto si ambos usuarios están muy cerca el uno del otro ($\theta_B \approx \theta_{E_A}$), lo que hace imposible tener una tasa de transmisión segura positiva. Por el contrario, cuando ambos usuarios no están a la misma distancia (líneas celeste y naranja), el rendimiento en términos de seguridad para el modelo SW es inferior al presentado por el modelo PW. Sin embargo, la tasa de transmisión segura para SW es positiva incluso cuando los ángulos de Eve y Bob coinciden. Este comportamiento es una consecuencia directa del DoF adicional con la distancia mencionado en Fig 3.13a, es decir, la interferencia es en general subestimada para el supuesto PW excepto para $\theta_{E_A} = \theta_B$, donde la interferencia es sobrestimada. Por último, se observa una simetría con respecto al ángulo de Bob que se rompe a medida que se aleja del centro del conjunto de antenas.

En este escenario, la reducción de M provoca caídas más breves y profundas en el modelo SW. Este efecto también es apreciable a medida que aumenta el ángulo de Bob, ver Fig. 3.16: acercar Bob al borde del *array* de antenas provoca una reducción del número de antenas efectivas [64]. De nuevo, detrás de este fenómeno se encuentra la hipótesis de campo lejano: reducir el número efectivo de antenas, es decir, el tamaño físico del *array* ($D = Md$), permite alcanzar el campo lejano a una distancia menor. En esta figura, al contrario de lo que ocurría en la Fig. 3.15, se observa como el modelo PW presenta siempre el mismo resultado. Esto se debe a que el ángulo no afecta en PW al módulo del vector de respuesta del *array* (ver 2.16). Por último, se observa en la Fig. 3.16 como los modelos PW y SW tienden a parecerse de nuevo si se reduce el número efectivo de

antenas [15].

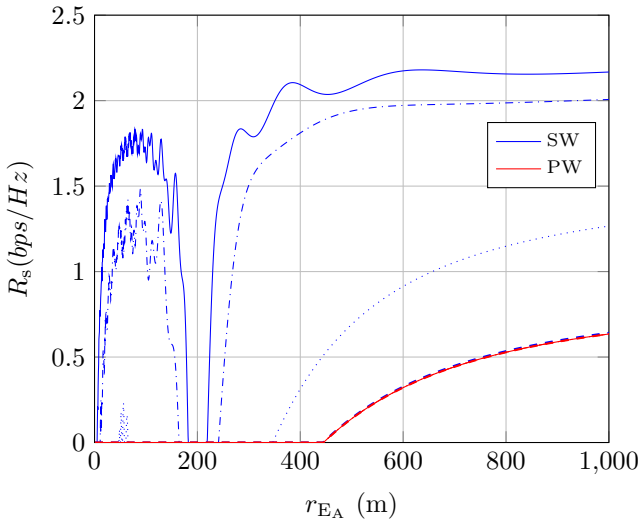
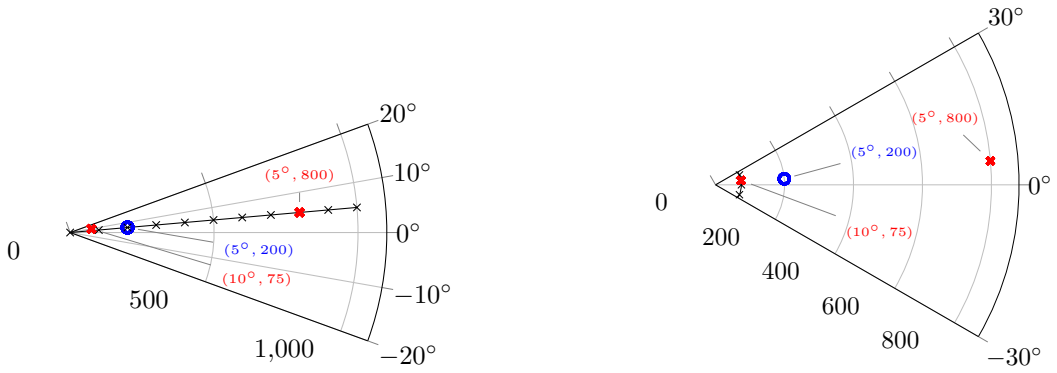


FIGURA 3.16: R_s en función de r_{E_A} para el escenario 1 donde se han representado con líneas sólidas, discontinuas con puntos, punteadas y discontinuas los casos con $\theta_{E_A} = [60, 70, 80, 90]^\circ$ respectivamente.

3.3.2. Escenario 2



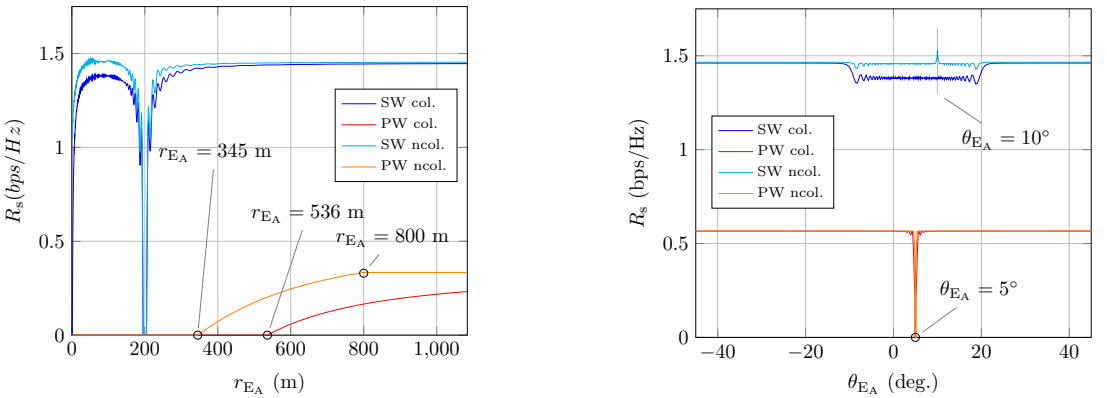
(a) Posición de los usuarios con el Eve móvil en 5° y distintas distancias.

(b) Posición de los usuarios con el Eve móvil a 75 m para distintas direcciones del mismo.

FIGURA 3.17: Representación gráfica de la posición de los usuarios en el escenario 2. La posición de Bob en (5°, 200 m) se señala con un círculo azul, los fisgones fijos en (10°, 75 m) y (5°, 800 m) con cruces rojas y las del fisgón que mueve su posición con cruces negras.

En este escenario, ver Fig. 3.17, se añaden dos nuevos Eves en ubicaciones fijas: $r_{E_B} = 800$ m, $\theta_{E_B} = 5^\circ$ y $r_{E_C} = 75$ m, $\theta_{E_C} = 10^\circ$. La configuración de los parámetros de simulación y el fisgón sobre el que se realiza el barrido, Eve_A, siguen siendo los mismos que en Escenario 1. La existencia de múltiples fisgones permitirá observar las diferencias entre los criterios *colluding* y *non-colluding* presentados al principio de la sección. Asimismo, la potencia de transmisión a Bob será menor, puesto se han añadido usuarios en un

sistema donde la potencia es limitada y se distribuye equitativamente. Esto tiene consecuencia directa en la Fig. 3.18a y la Fig. 3.18b como una disminución en los valores de R_{s}.



(a) R_{s} en función de la distancia de $\mathrm{Eve_A}$ con la dirección fija a $\theta_{\mathrm{E_A}} = 5°$.

(b) R_{s} en función de la dirección de $\mathrm{Eve_A}$ con la distancia fija a $r_{\mathrm{E_A}} = 75$ m.

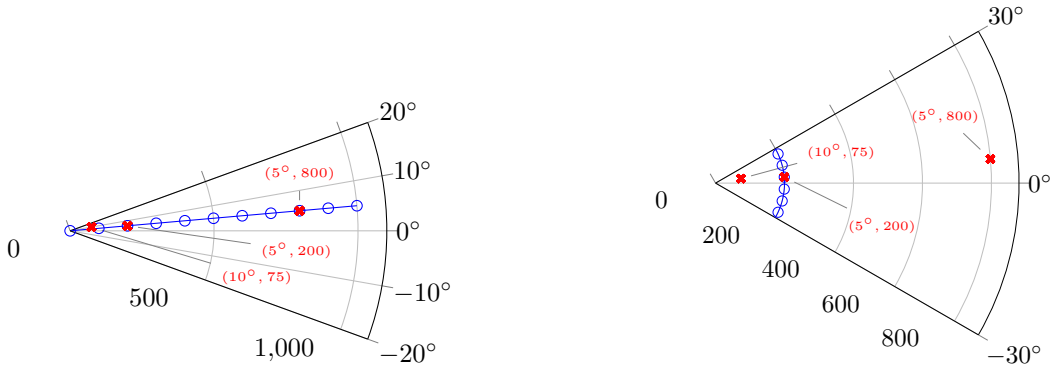
FIGURA 3.18: R_{s} en función de la posición de $\mathrm{Eve_A}$ en el escenario 2 con Bob fijo en (5°, 200 m) y dos Eve fijos en (10°, 75 m) y (5°, 800 m).

En la Fig. 3.18a se pretenden mostrar dos de las zonas más relevantes para los fisgones. En concreto, $\mathrm{Eve_C}$ ilustra un fisgón situado cerca del *array* de antenas, $r_{\mathrm{E_C}} = 75$ m, aunque en una dirección distinta a la de Bob, $\theta_{\mathrm{E_C}} = 10°$. El otro fisgón, $\mathrm{Eve_B}$, representa a un fisgón situado en la misma dirección que el usuario legítimo, pero con una distancia distinta $r_{\mathrm{E_B}} = 800$ m. De la Fig. 3.18a, se pueden destacar los siguientes aspectos:

- Transmitir menos potencia a cada usuario implica una menor interferencia entre usuarios (menor LINR) y, junto a la nueva interferencia que sufren los fisgones, hace que la máxima tasa de transmisión segura sea posible con una menor $r_{\mathrm{E_A}}$ que en el escenario anterior bajo el criterio *non-colluding*.
- El criterio *colluding* es el más perjudicial para el sistema, ya que los fisgones son capaces de anular sus interferencias y todas sus contribuciones se unen para romper la seguridad del sistema.
- El criterio *non-colluding* en el modelo PW satura cuando $\mathrm{Eve_A}$ alcanza la distancia $r_{\mathrm{E_A}} = r_{\mathrm{E_B}} = 800$ m. En este punto, ambos fisgones son igualmente perjudiciales, pero como $\mathrm{Eve_A}$ continúa alejándose de Bob, $\mathrm{Eve_B}$ pasa dominar la LINR.
- La influencia de $\mathrm{Eve_B}$ sobre SW es irrelevante porque la reducción de la interferencia con la distancia hace que ni reciba información de Bob ni Bob reciba interferencia. Esta es la misma razón detrás de la similitud entre los criterios *colluding* y *non-colluding* a medida que $\mathrm{Eve_A}$ se aleja de Bob.
- Finalmente, en el modelo PW $\mathrm{Eve_A}$ necesita estar más lejos para tener una tasa secreta positiva en el criterio *colluding*. Esto se debe a que la LINR recibida por el resto de fisgones es suficiente y, por tanto, $\mathrm{Eve_A}$ necesita recibir menos cantidad de información que en el escenario anterior para interceptar la señal hacia Bob.

En la Fig. 3.18b se puede observar mejor el impacto de Eve_C. En primer lugar, se observa un pico de R_s en el modelo SW cuando Eve_A pasa por el mismo lugar que Eve_C. La razón es que la interferencia que los fisgones se causan entre sí, existente únicamente cuando no cooperan, aumenta. Esto provoca que se reduzcan los niveles de LINR y, por tanto, aumente la R_s. Además, dado que la LINR Eve_C es superior o similar a la de Eve_A en todo el barrido, la tasa secreta se mantiene casi constante cuando consideramos el criterio *non-colluding* y el modelo SW. Por el contrario, cuando tenemos un criterio *colluding*, la tasa secreta cae en la zona en la que ambos fisgones tienen una LINR relevante. Finalmente, la influencia de Eve_B se aprecia principalmente en la caída de la tasa secreta en el modelo PW. Debido a que tiene el mismo ángulo que Bob, el parámetro más relevante para reducir la interferencia en PW, su presencia enmascara la de cualquier otro fisgón.

3.3.3. Escenario 3



(a) Posición de los usuarios con Bob móvil en 5° y distintas distancias.

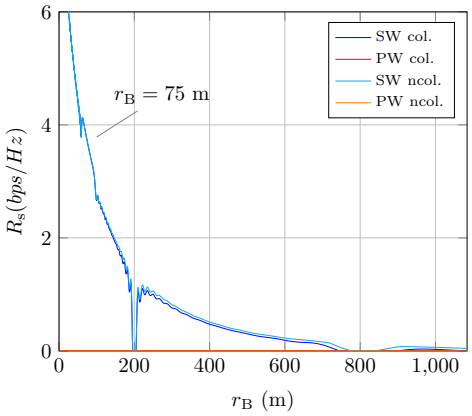
(b) Posición de los usuarios con Bob móvil a 75 m para distintas direcciones del mismo.

FIGURA 3.19: Representación gráfica de la posición de los usuarios en el escenario 3. La posición de Bob es móvil y se señala con círculos azules, mientras que los tres fisgones fijos se encuentran en (5°, 200 m), (10°, 75 m) y (5°, 800 m) y se señalan con cruces rojas.

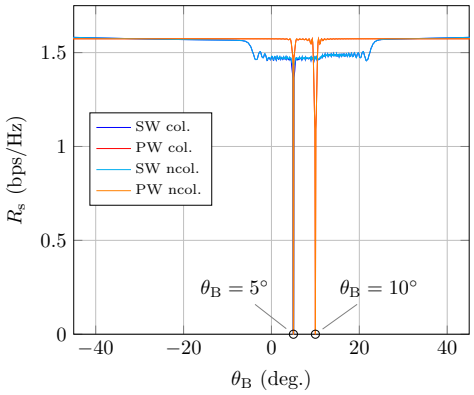
Para remarcar las diferencias entre SW y PW, incluimos un tercer escenario en el que tenemos los mismos fisgones que en Escenario 2, pero esta vez se realiza el barrido sobre diferentes distancias de Bob, mientras que mantenemos a Eve_A fija en $r_{\text{E}_\text{A}} = 200$ m y $\theta_{\text{E}_\text{A}} = 5°$. De las dos nuevas figuras, Fig. 3.20a y Fig. 3.20b, extraemos las siguientes conclusiones:

- El modelo PW nunca alcanza una tasa secreta positiva en el barrido de distancia, ya que hay dos fisgones en la misma dirección que Bob.
- La métrica SW muestra un decaimiento exponencial con la distancia alterado por la presencia de fisgones a sus respectivas distancias donde predomina su LINR. Sin embargo, dado que sólo predomina un fisgón en cada zona, y están en ubicaciones fijas, los criterios *colluding* y *non-colluding* son prácticamente idénticos.

- Bob no puede aprovecharse de la DoF con la distancia a partir de 800m en adelante, ya que le llega muy poca potencia.
- Alrededor de Eve_C la R_s aumenta. A esta distancia la diferencia angular es suficiente para decorrelar a los usuarios; por lo tanto, Eve_C deja de recibir información de Bob.
- Finalmente, en la Fig. 3.20b se muestra claramente que la tasa secreta en SW sólo cae a 0 bps/Hz si la ubicación coincide con la de un fisgón. Se puede observar como la R_s no llega a 0 bps/Hz con $\theta_\text{B} = 10°$ debido a que no se encuentran a la misma distancia el fisgón Eve_C y Bob.



(a) R_s en función de la distancia de Bob con la dirección fija a $\theta_\text{B} = 5°$.



(b) R_s en función de la dirección de Bob con la distancia fija a $r_\text{B} = 200$ m.

FIGURA 3.20: R_s en función de la posición de Bob en el escenario 3 con tres Eve fijos en (5°, 200 m), (10°, 75 m) y (5°, 800 m).

Todos los escenarios descritos en esta sección señalan determinados lugares donde los fisgones resultan muy perjudiciales para una comunicación segura. Esta idea encaja perfectamente con el concepto de zona de comunicación segura o zona protegida [10], [65]. Una zona protegida requiere conocer el escenario para especificar el área donde se deben evitar tener fisgones. Centrándonos en el problema presentado, **el uso del modelo SW permite definir zonas considerablemente más pequeñas que las del modelo PW**: SW sólo requiere delimitar una zona próxima al usuario legítimo y el área junto al *array* de antenas, mientras que PW requiere restringir toda el área con una dirección similar a la de Bob.

3.4. Leakage Subspace Precoding and Scheduling

A continuación, se extiende el trabajo realizado en la sección 3.3 permitiendo la existencia de múltiples usuarios legítimos en el escenario. Al igual que en el caso anterior, se consideran dos escenarios de fisgones: colaboración total (TC), en el que todos los fisgones $v \in \mathcal{V}$ colaboran en la decoficación del mensaje dirigido al usuario k y colaboración parcial (PC), en el que sólo los fisgones en las proximidades del usuario k colaboran, es

decir, $v \in \mathcal{E}_k$, donde $\mathcal{E}_k \subseteq \mathcal{V}$ es el conjunto de fisgones agrupados para interceptar al usuario k.

Haciendo uso de la expresión (2.7) y particularizando la LINR según el escenario bajo estudio, se tiene que la cantidad de información segura, medida como eficiencia espectral secreta, es [6], [7]:

$$R_{\mathrm{s}} = \sum\nolimits_{k\in\mathcal{B}} R_{\mathrm{s,k}} = \sum\nolimits_{k\in\mathcal{B}} \log_2 \left[\frac{1+\mathrm{SINR_k}}{1+\mathrm{LINR_k^{TC/PC}}} \right]^+ \quad [\mathrm{bps/Hz}], \tag{3.26}$$

donde se recuerda que $\mathcal{B}$ es el conjunto de usuarios legítimos. Asimismo, se considera que la LINR utilizada en la expresión corresponde con la del caso peor, (2.6), donde los fisgones colaboran entre sí y consiguen cancelar la interferencia [28].

La existencia de múltiples usuarios legítimos hace más complejo el problema de optimizar la cantidad de información segura. Ahora hay que diseñar las matrices de precodificación y cómo se distribuye la potencia a cada usuario, teniendo en cuenta que la BS sigue teniendo limitada su potencia de transmisión P_{TX}:

$$\underset{\{\mathbf{w}_\mathrm{k},p_k\}_{k\in\mathcal{B}}}{\operatorname{argmax}} \; R_{\mathrm{s}} \quad \text{s.t.} \quad \sum_{k\in\mathcal{B}} p_k \leq P_{\mathrm{TX}}. \tag{3.27}$$

La sección anterior puso de manifiesto cómo se puede reducir la IUI cuando nos encontramos en campo cercano y se utiliza un modelo de propagación más completo, como es el SW: separando los usuarios en el dominio angular (i.e, con θ_k) como se hace en PW y, como novedad, en el dominio de la distancia [16] (i.e, con r_k). Por lo tanto, esta nueva característica que permite reducir interferencias y, por tanto la información fugada, debe tenerse en cuenta a la hora de diseñar tanto el precodificador y como la asignación de potencia a los distintos usuarios, es decir, decidir en cada momento a qué usuarios se da servicio (*scheduling*).

Existen diferencias clave entre los diseños convencionales de *scheduling* y precodificación [27], [64] conjuntos, y sus homólogos en PLS orientados a una maximización de la R_{s} como los que aquí se abordan:

- La métrica clásica de eficiencia espectral es más simple.
- Tan sólo los usuarios seleccionados por el procedimiento de *scheduling* se consideran para calcular la IUI.
- La información fugada a los usuarios no servidos (es decir, Eves) es ignorada.

A continuación, se describe una propuesta, *Leakage Subspace Precoding* (LSP), para la realización de *scheduling* y precodificación de forma conjunta para comunicaciones seguras en este escenario (véase Alg. 1), considerando las estrategias para los fisgones descritas en la sección anterior: TC y PC. A continuación se detallan las diferencias:

Algorithm 1 Leakage Subspace Precoding

$i \leftarrow 0$, $\mathcal{S}^{(0)} \leftarrow \emptyset$
TC scenario
$\mathbf{\Pi} \leftarrow$ Compute the orthogonal projector into $\mathfrak{L}^{\perp}$
PC scenario
$\mathbf{\Pi}_{\mathrm{k}} \leftarrow$ Compute the orthogonal projector into $\mathfrak{L}_{\mathrm{k}}^{\perp}$, $\forall k \in \mathcal{B}$
$q_{\mathrm{k}}^{(0)} \leftarrow$ set initial priorities $\forall k \in \mathcal{B}$
repeat
  $k^{(i)} \leftarrow$ Find highest priority (3.29), $\mathcal{S}^{(i+1)} \leftarrow \mathcal{S}^{(i)} \cup \{k^{(i)}\}$
  TC scenario
  $\mathbf{A}^{(i)} \leftarrow$ Update using (3.31)
  $\boldsymbol{\omega}_{k^{(j)}} \leftarrow$ Compute TC-ZF precoders (3.30), $\forall k^{(j)} \in \mathcal{S}^{(i+1)}$
  PC scenario
  $\mathbf{B}_{k^{(j)}}^{(i)} \leftarrow$ Compute using (3.33), $\forall k^{(j)} \in \mathcal{S}^{(i+1)}$
  $\boldsymbol{\omega}_{k^{(j)}} \leftarrow$ Compute PC-ZF precoders (3.34), $\forall k^{(j)} \in \mathcal{S}^{(i+1)}$
  $\mathbf{w}_{k^{(j)}} \leftarrow$ Normalize $\boldsymbol{\omega}_{k^{(j)}}$, $\forall k^{(j)} \in \mathcal{S}^{(i+1)}$
  $p_{k^{(j)}} \leftarrow$ Power allocation using waterfilling, $\forall k^{(j)} \in \mathcal{S}^{(i+1)}$
  $q_{\mathrm{k}}^{(i+1)} \leftarrow$ Update user priorities with (3.32)
  $\mathcal{B} \leftarrow \mathcal{B} \setminus \{k^{(i)}\}$, $i \leftarrow i+1$
until $\mathcal{B} = \emptyset$ or stopping criterion is met

3.4.1. Escenario de cooperación total

Este corresponde al caso peor habitual en la que todos los fisgones colaboran para decodificar los datos de los usuarios legítimos. De acuerdo con la definición de LINR en (2.6), para evitar la intercepción del mensaje se propone definir un subespacio de fuga, $\mathfrak{L}$, compuesto por los vectores de canal de los fisgones, es decir $\mathfrak{L} = \mathrm{span}(\mathbf{a}_{v_1}, \mathbf{a}_{v_2}, \ldots, \mathbf{a}_{v_{K_{\mathrm{E}}}})$. Si se diseñan los vectores de precodificación asociados a cada usuario legítimo para que pertenezcan al subespacio ortogonal, $\mathfrak{L}^{\perp}$, se garantiza que $\mathrm{LINR}_{\mathrm{k}}^{\mathrm{TC}} = 0$ en (3.26). De esta forma, se puede decidir de forma más sencilla a qué usuarios asignar potencia en cada momento, puesto que ya se garantiza la seguridad de los usuarios servidos.

El proceso iterativo de selección de usuarios comienza estableciendo una prioridad inicial para cada uno de los usuarios legítimos, $q_{\mathrm{k}}^{(0)}$ con $\forall k \in \mathcal{B}$, calculada como

$$q_{\mathrm{k}}^{(0)} = \|\mathbf{\Pi}\mathbf{a}_{\mathrm{k}}\|, \tag{3.28}$$

donde $\mathbf{\Pi}$ es el proyector ortogonal en el subespacio $\mathfrak{L}^{\perp}$. A continuación, de forma similar a [27], se inicia un procedimiento iterativo tal que en la iteración i-ésima el usuario con mayor prioridad, es decir,

$$k^{(i)} = \underset{k \in \mathcal{B}}{\mathrm{argmax}}(q_{\mathrm{k}}^{(i)}) \tag{3.29}$$

se elige como candidato para recibir una determinada cantidad de potencia disponible P_{TX}. Para comprobar si servir al usuario candidato $k^{(i)}$ mejora la métrica objetivo, (3.26), se diseñan los vectores de precodificación TC-ZF para el conjunto de usuarios, $\mathcal{S}^{(i)} \subseteq \mathcal{B}$, compuesto por los usuarios previamente seleccionados en la iteración i y el usuario candidato $k^{(i)}$ como

$$[\boldsymbol{\omega}_{k^{(1)}}, \ldots, \boldsymbol{\omega}_{k^{(i)}}] = \mathbf{\Pi}^{*}(\mathbf{A}^{(i)})^{\mathrm{H}}(\mathbf{A}^{(i)}\mathbf{\Pi}^{*}(\mathbf{A}^{(i)})^{\mathrm{H}})^{-1}, \tag{3.30}$$

donde

$$\mathbf{A}^{(i)} = [\mathbf{a}_{k^{(1)}}, \mathbf{a}_{k^{(2)}}, \ldots, \mathbf{a}_{k^{(i)}}]^T, \forall k \in \mathcal{S}^{(i)}. \tag{3.31}$$

Nótese como el proyector $\mathbf{\Pi}$ se incluye en el diseño de los vectores de precodificación TC-ZF. Ahora, para k en $\mathcal{S}^{(i)}$ denotamos por $\mathfrak{I}_k^{(i)} = \mathrm{span}(\mathbf{a}_{j_1}, \mathbf{a}_{j_2}, \ldots, \mathbf{a}_{j_{i-1}})$ al subespacio constituido por los canales de los $i-1$ usuarios legítimos en $\mathcal{S}^{(i)}$, con $j_1, \ldots, j_{i-1} \neq k$. Por tanto, el subespacio posible para el vector de precodificación del usuario k viene dado por $(\mathfrak{I}_k^{(i)})^{\perp} \cap \mathfrak{L}^{\perp}$. Dado que las características espaciales de los canales dependen en gran medida del modelo de propagación [16], la reducción de interferencias *y* fugas que proporciona la distancia en el modelo SW [16] ofrece un grado de libertad adicional en el diseño del vector de precodificación en comparación con el caso PW. Finalmente, los vectores de precodificación para cada uno de los usuarios legítimos seleccionados es $\mathbf{w}_{\mathrm{k}} = \boldsymbol{\omega}_k / \|\boldsymbol{\omega}_k\|$, $\forall k \in \mathcal{S}^{(i)}$ y la potencia asignada $\mathbf{P}$ se elige según el procedimiento habitual de *waterfilling* [27], con $P_{\mathrm{TX}} = \sum_{k \in \mathcal{S}^{(i)}} p_{\mathrm{k}}$. Nótese que no utilizar ruido artificial en transmisión es óptimo para (3.26) en escenarios sin desvanecimiento o con múltiples fisgones cooperando [66], como es el escenario considerado. Además, en cada iteración i, es importante actualizar las prioridades en función de la interferencia causada por el usuario seleccionado en iteraciones anteriores, es decir

$$q_{\mathrm{k}}^{(i)} = \left\| \left(\mathbf{\Pi} - \sum\nolimits_{j=1}^{i-1} \mathbf{w}_{\mathrm{k_j}}^{(j)} (\mathbf{w}_{\mathrm{k_j}}^{(j)})^{\mathrm{H}} \right) \mathbf{a}_{\mathrm{k}} \right\|, \tag{3.32}$$

donde $\mathbf{w}_{\mathrm{k_j}}^{(j)}$ es el vector de precodificación obtenido en la iteración j para el usuario seleccionado k_j. El proceso iterativo continúa incorporando estos usuarios candidatos como usuarios seleccionados si el nuevo candidato mejora la eficiencia espectral secreta; en caso contrario, se descarta y finaliza el proceso iterativo. Se asume que los usuarios no seleccionados se asignarán en un recurso de tiempo/frecuencia diferente de la BS.

El esquema LSP se pone a prueba bajo un escenario XL-MIMO con SW y el caso de suponer erróneamente la propagación PW. Además, comparamos LSP con un esquema clásico en la literatura de PLS como el ZF con *waterfilling* [6]. Se simula un escenario como el de la Fig. 2.6 donde se da servicio a un conjunto de usuarios localizados aleatoriamente de la siguiente forma: los usuarios legítimos K_{B} se despliegan aleatoriamente a lo largo de la región de cobertura descrita en la Tabla 3.2 en las posiciones θ_{k} y r_{k}; a continuación, se despliega un número de fisgones k_{e} en las proximidades de cada usuario legítimo en las posiciones $\theta_{\mathrm{e,k}}$ y $r_{\mathrm{e,k}}$, con $e = 1 \ldots k_{\mathrm{e}}$, de forma que $K_{\mathrm{E}} = K_{\mathrm{B}} \cdot k_{\mathrm{e}}$. En concreto, un fisgón siempre está situado aproximadamente en la misma dirección angular que el usuario k (es decir, $\theta_{1,\mathrm{k}} = \theta_{\mathrm{k}} + \Delta_{\mathrm{k}}$, con $\Delta_{\mathrm{k}} \sim \mathcal{U}[\pm 0, 1^o]$), y r_{p} metros más cerca de la BS. Los demás fisgones $e = 2 \ldots k_{\mathrm{e}}$ se despliegan a una distancia $r_{\mathrm{q}} = r_{\mathrm{Crit}}$ m de Bob (es decir, r_{q} es el radio de una zona protegida, en la que no hay fisgones cerca de Bob) y a un cierto $\theta_{\mathrm{e,k}}$.

La eficiencia espectral secreta (Fig. 3.21) y el número de usuarios legítimos servidos (Fig. 3.22) se muestran para el caso del escenario TC, el caso peor [6] en el que todos los

TABLA 3.2: Configuración de los parámetros de simulación con múltiples usuarios.

Parámetro	**Valor**
Realizaciones del canal	1000
# usuarios legítimos	$K_{\mathrm{B}} = [10, 20]$
# fisgones por cada Bob	$k_{\mathrm{e}} = [2^{TC}, 6^{PC}]$
Longitud de onda	$\lambda = 0{,}1249$ m
Distancia entre antenas	$d = \frac{\lambda}{2}$ m
Número de antenas	$M = 100$
SNR transmitida	$[0, 5, 10, 15, 20, 25]$ dB
Distancia de Rayleigh	$r_{\mathrm{Rayl}} = \frac{2D^2}{\lambda}$ m
Distancia crítica [15]	$r_{\mathrm{Crit}} \approx 9D$ m
Rango de distancias	$[3\, r_{\mathrm{Crit}}, r_{\mathrm{Rayl}}]$ m
Rango angular	$[-\frac{\pi}{4}, \frac{\pi}{4}]$ rad

fisgones cooperan para decodificar los mensajes de lo usuarios legítimos, bajo los modelos de propagación PW y SW. Las líneas continuas y discontinuas denotan los casos con $K_{\mathrm{B}} = \{10, 20\}$ usuarios legítimos, respectivamente, y el resto del conjunto de parámetros del escenario son los que se presentan en la Tabla 3.2, con $r_{\mathrm{p}} = 2r_{\mathrm{q}}$ y $D = Md$.

De la Fig. 3.21 se pueden destacar los siguientes aspectos:

- En el modelo PW, la eficiencia espectral secreta se reduce debido a la posición de los fisgones, principalmente a los situados en direcciones angulares similares a las de los usuarios legítimos.
- La consideración del modelo SW permite mejorar las tasas de transmisión segura hasta $44\,\%$ y dar servicio a más usuarios, ya que los usuarios legítimos y los fisgones con direcciones angulares similares están decorrelados con la distancia [16].
- El aumento del número de usuarios legítimos mejora notablemente la eficiencia espectral secreta en el caso SW, cosa que no ocurre cuando se considera PW.
- Aunque el número de usuarios servidos no es la métrica a optimizar, vemos que en este escenario LSP consigue mejorar *tanto* la eficiencia espectral secreta como el número medio de usuarios servidos cuando $K_{\mathrm{B}} = 20$, en comparación con la precodificación ZF convencional [6].

Obsérvese que tanto ZF como LSP usan *waterfilling* para determinar la potencia asignada a cada usuario. En consecuencia, la asignación de potencia está directamente relacionada con el número de usuarios legítimos a los que se sirve. De hecho, los usuarios reciben potencia sólo si la ganancia efectiva de su canal, es decir, la ganancia obtenida cuando se eliminan la información fugada y las interferencias de los demás usuarios

legítimos, es superior a un determinado umbral, digamos μ. El valor de dicho umbral aumenta con el número de usuarios que reciben potencia, y disminuye con la SNR y las ganancias efectivas del canal. En consecuencia, se puede esperar que el número de usuarios servidos sea mayor cuando se utiliza ZF. Esto se debe a que el enfoque ZF obtiene, en general, ganancias efectivas más equilibradas, ya que los usuarios no son priorizados como en LSP. Sin embargo, esta intuición puede fallar cuando la SNR y/o las ganancias efectivas del canal no son suficientemente grandes, como podemos ver en la Fig. 3.22. Así, el incremento en μ debido al número de usuarios legítimos servidos no puede ser compensado debido a las bajas ganancias efectivas de canal obtenidas en este escenario.

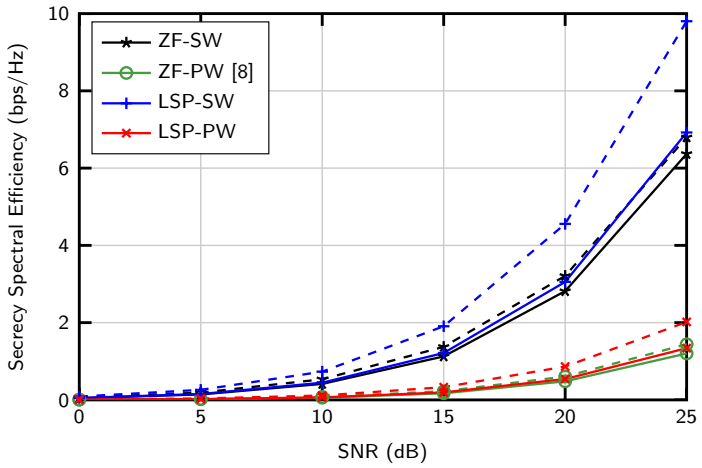


FIGURA 3.21: Eficiencia espectral segura en el escenario TC, considerando propagación SW y PW y diferentes estrategias de precodificación. Las líneas continuas y discontinuas corresponden con ($K_{\mathrm{B}} = 10$) y ($K_{\mathrm{B}} = 20$) respectivamente.

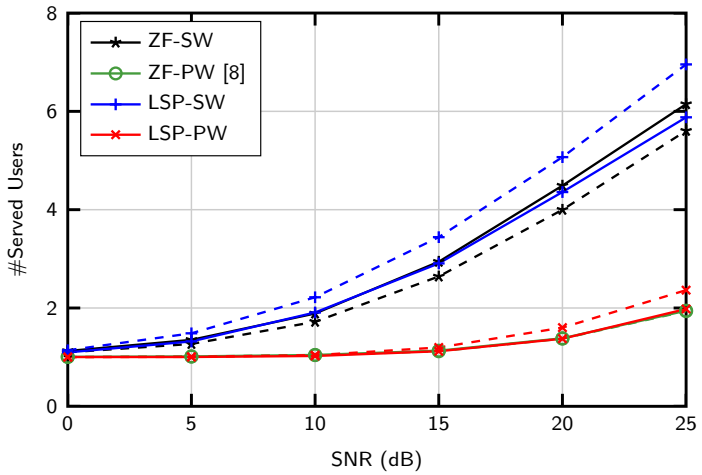


FIGURA 3.22: Número de usuarios servidos en el escenario TC, considerando propagación SW y PW y diferentes estrategias de precodificación. Las líneas continuas y discontinuas corresponden con ($K_{\mathrm{B}} = 10$) y ($K_{\mathrm{B}} = 20$) respectivamente.

3.4.2. Escenario de cooperación parcial

En esta sección se considera una situación más práctica en la que sólo el subconjunto de fisgones $\mathcal{E}_k \subseteq \mathcal{V}$ situados en las proximidades del usuario legítimo $k \in \mathcal{B}$ son capaces

de interceptar su mensaje, es decir, θ_{v} y r_{v} ($\forall v \in \mathcal{E}_k$) son similares a θ_k y r_k. Estos fisgones pertenecientes a $\mathcal{E}_k$ colaboran para descifrar la información del usuario legítimo k. Dado que el conjunto de fisgones capaces de cooperar es menor que en el caso TC, se puede aprovechar para el diseño de la matriz de precodificación.

En Alg. 1 se puede apreciar también el proceso seguido en este escenario, ya que sigue la misma estructura que en el caso TC. Sin embargo, las prioridades de los usuarios legítimos, q_{k}, y el diseño los vectores de precodificación tienen que incorporar las particularidades de (2.6). A diferencia de TC, en el caso PC cada usuario tiene su propio subespacio de información fugada definido por $\mathfrak{L}_{\mathrm{k}} = \mathrm{span}(\mathbf{a}_{v_1}, \mathbf{a}_{v_2}, \ldots, \mathbf{a}_{v_{|\mathcal{E}_k|}})$ y $v_1, v_2, \ldots, v_{|\mathcal{E}_k|} \in \mathcal{E}_k$. De esta forma, sólo se necesita garantizar que el vector de precodificación para el usuario k se encuentra en el subespacio $\mathfrak{L}_{\mathrm{k}}^{\perp}$ para asegurar la condición $\mathrm{LINR}_{\mathrm{k}}^{\mathrm{PC}} = 0$, simplificando así la función objetivo en (3.27). Para ello, se define el proyector ortogonal en el subespacio $\mathfrak{L}_{\mathrm{k}}^{\perp}$ como $\mathbf{\Pi}_{\mathrm{k}}$ y se establecen las prioridades iniciales como $q_{\mathrm{k}}^{(0)} = \|\mathbf{\Pi}_{\mathrm{k}}\mathbf{a}_{\mathrm{k}}\|$, de forma que sólo los fisgones en $\mathcal{E}_k$ afectan a si el usuario k es elegido o no. A continuación, se inicia el proceso iterativo y la selección del usuario candidato en la iteración i-ésima se realiza utilizando (3.29). Nótese que el diseño del vector de precodificación TC-ZF en (3.30) no es válido en este escenario, ya que el subespacio de fuga no es común a todos los usuarios. Así, para cada $k \in \mathcal{S}^{(i)}$ se define la matriz

$$\mathbf{B}_{\mathrm{k}}^{(i)} = [\mathbf{a}_k, \mathbf{a}_{j_1}, \mathbf{a}_{j_2}, \ldots, \mathbf{a}_{j_{i-1}}, \mathbf{a}_{v_1}, \mathbf{a}_{v_2}, \ldots, \mathbf{a}_{v_{|\mathcal{E}_k|}}]^T, \tag{3.33}$$

donde se incluye el vector del canal del usuario k para los usuarios $i-1$ en $\mathcal{S}^{(i)}$ tal que $j_1, \ldots, j_{i-1} \neq k$, y aquellos de los fisgones $v_1, v_2, \ldots, v_{|\mathcal{E}_k|} \in \mathcal{E}_k$. A continuación, se diseña el vector de precodificación PC-ZF como

$$\boldsymbol{\omega}_k = \left[(\mathbf{B}_{\mathrm{k}}^{(i)})^{\mathrm{H}} \left(\mathbf{B}_{\mathrm{k}}^{(i)} (\mathbf{B}_{\mathrm{k}}^{(i)})^{\mathrm{H}} \right)^{-1} \right]_{:,1}, \tag{3.34}$$

siendo esta la primera columna de la matriz de precodificación. De esta forma, se asegura que el vector de precodificación para cada usuario $k \in \mathcal{S}^{(i)}$ pertenece a la intersección de los subespacios $(\mathfrak{I}_k^{(i)})^{\perp} \cap \mathfrak{L}_{\mathrm{k}}^{\perp}$. De nuevo, los vectores de precodificación se normalizan por $\mathbf{w}_{\mathrm{k}} = \boldsymbol{\omega}_k / \|\boldsymbol{\omega}_k\|, \forall k \in \mathcal{S}^{(i)}$ y se utiliza *waterfilling* para la asignación de potencia $\mathbf{P}$. En cuanto a la actualización de las prioridades en (3.32), se puede utilizar la misma expresión pero ahora incluyendo el proyector $\mathbf{\Pi}_{\mathrm{k}}$.

La diferencia principal de este segundo escenario es que el usuario legítimo k sólo se ve obligado a protegerse de aquellos fisgones situados en su área más cercana, que son los más perjudiciales para la seguridad en capa física [67]. Por tanto, los grados de libertad disponibles para el diseño de la matriz de precodificación son mayores, en general, que en el escenario TC. Estos grados de liberad adicionales se suman a los proporcionados por la reducción de interferencias e información fugada con la distancia en el modelo SW.

Al igual que con el caso TC, la eficiencia espectral secreta (Fig. 3.23) y el número de

usuarios legítimos servidos (Fig. 3.24) se muestran para el caso del escenario PC, bajo los modelos de propagación PW y SW. Puesto que ahora no colaboran todos los fisgones desplegados, se ha aumentado $k_{\mathrm{e}} = 6$ para que cada usuario legítimo se vea afectado por un mayor número de fisgones potencialmente perjudiciales en comparación con el caso TC. Estos nuevos fisgones se despliegan a una distancia $\frac{r_{\mathrm{q}}}{2}$ de Bob con los ángulos $\theta_{\mathrm{e,k}}$ uniformemente distribuidos. De las dos nuevas figuras, Fig. 3.23 y Fig. 3.24, se extraen las siguientes conclusiones:

- Con el modelo PW, la R_{s} es baja porque los fisgones cercanos tienen un efecto dominante.
- Por el contrario, con el modelo de propagación SW la R_{s} mejora hasta $19\,\%$ aprovechando la reducción de información fugada con la distancia.
- La R_{s} es similar a la obtenida en TC para un número bajo de usuarios legítimos ($K_{\mathrm{B}} = 10$), pero mejora cuando aumentamos este valor ($K_{\mathrm{B}} = 20$). La razón es que la información fugada para cada usuario legítimo es alta con pocos usuarios, pero no aumenta drásticamente con el número de usuarios. Esto se debe a que se ha aumentado la influencia de los fisgones en las proximidades de cada usuario, pero estos no colaboran con los de otros usuarios.
- LSP consigue mejor R_{s} a pesar de servir a menos usuarios, un efecto que se aprecia mejor en regímenes de alta SNR. Esto se debe a que las ganancias efectivas de los canales son mayores que en el escenario anterior, puesto que existe menor información fugada que en el caso TC. Por tanto, LSP da prioridad a los usuarios con canales de gran ganancia efectiva para maximizar la métrica objetivo, mientras que ZF distribuye la potencia entre los usuarios legítimos cuyas ganancias efectivas están distribuidas de forma más uniforme, puesto que ZF se ve obligado a cancelar las interferencias para *todos* los usuarios, independientemente de que no se les asigne potencia con *waterfilling*.

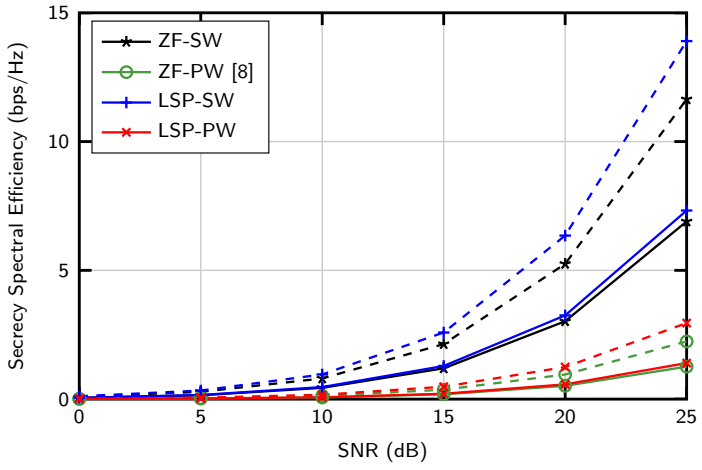


FIGURA 3.23: Eficiencia espectral segura en el escenario PC, considerando propagación SW y PW y diferentes estrategias de precodificación. Las líneas continuas y discontinuas corresponden con ($K_{\mathrm{B}} = 10$) y ($K_{\mathrm{B}} = 20$) respectivamente.

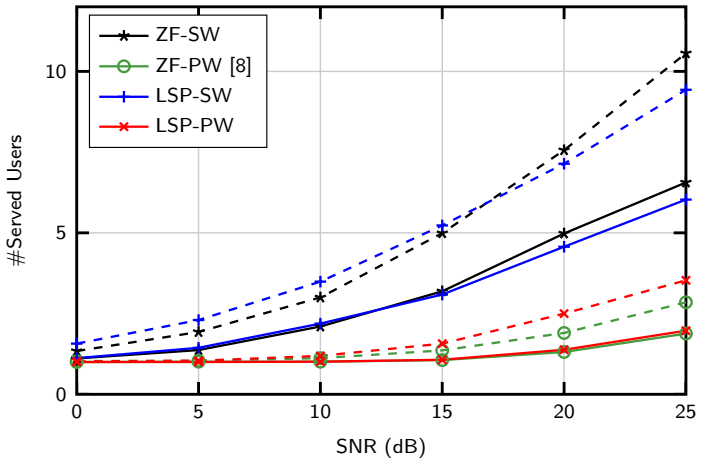


FIGURA 3.24: Número de usuarios servidos en el escenario PC, considerando propagación SW y PW y diferentes estrategias de precodificación. Las líneas continuas y discontinuas corresponden con ($K_{\mathrm{B}} = 10$) y ($K_{\mathrm{B}} = 20$) respectivamente.

3.4.3. Complejidad

Finalmente, se incorpora un estudio sobre la complejidad del algoritmo propuesto. Para ello, hay que fijarse en que el cálculo de los proyectores de ambos escenarios, $\mathbf{\Pi}$ y $\mathbf{\Pi}_k$, se computan antes de comenzar el proceso iterativo. Por ende, el coste computacional del algoritmo (1) queda definido por los pasos que exigen un mayor número de operaciones:

- Para el escenario TC, uno de estos pasos es el cálculo de los vectores de precodificación TC-ZF en (3.30). Estos tienen la siguiente complejidad computacional: $\mathcal{O}(2M|\mathcal{S}^{(i)}|^2 + |\mathcal{S}^{(i)}|^3)$. Obsérvese como las primeras iteraciones son menos costosas, ya que el número de usuarios seleccionados, $|\mathcal{S}^{(i)}|$, es igual al número de la iteración i. Además, se ha considerado que el producto de los vectores de canal, $\mathbf{a}_k$, con el proyector, $\mathbf{\Pi}$, se almacena cuando se calcula en el paso 3 del algoritmo. El otro gran coste computacional proviene de la actualización de las prioridades de los usuarios, $q_k^{(i)}$, en (3.32). Este está sujeto al límite $\mathcal{O}(3M(|\mathcal{B}| - |\mathcal{S}^{(i)}|))$ al evitar el cálculo repetido de términos utilizados en iteraciones anteriores.

- En el caso de PC, se aplican límites similares, pero con ligeras diferencias en el número de operaciones. Con respecto al cálculo de los vectores de precoficación PC-ZF en (3.34), el orden de complejidad viene dado por $\mathcal{O}(2M|\mathcal{S}^{(i)}|(|\mathcal{S}^{(i)}| + |\mathcal{E}_k|)^2 + |\mathcal{S}^{(i)}|(|\mathcal{S}^{(i)}| + |\mathcal{E}_k|)^3)$, que también depende del número de fisgones para el usuario k, i.e. $|\mathcal{E}_k|$. En cuanto al número de operaciones requerida para actualizar las prioridades de los usuarios, se tiene que es el mismo que en el escenario anterior $\mathcal{O}(3M(|\mathcal{B}| - |\mathcal{S}^{(i)}|))$.

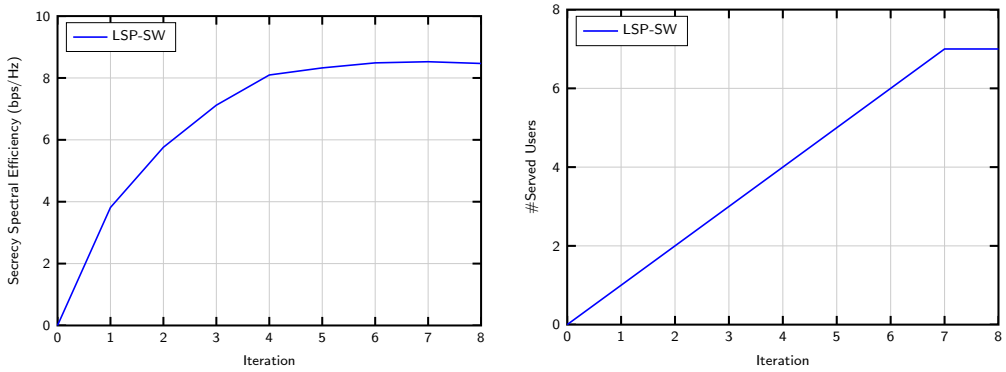
Dado el sistema XL-MIMO considerado en este trabajo, es importante destacar que la complejidad computacional de la solución propuesta depende linealmente del número de antenas en la BS: $\mathcal{O}(M)$. Nótese que otras soluciones en la literatura basadas en ZF, como por ejemplo [6], también presentan una dependencia lineal con M en la complejidad

computacional del algoritmo.

TABLA 3.3: Configuración de los parámetros de simulación de la complejidad.

Parámetro	**Valor**
# usuarios legítimos	$K_{\mathrm{B}} = 10$
# fisgones por cada Bob	$k_{\mathrm{e}} = 2$
Longitud de onda	$\lambda = 0{,}1249$ m
Distancia entre antenas	$d = \frac{\lambda}{2}$ m
Número de antenas	$M = 100$
SNR transmitida	25 dB
Distancia Rayleigh	$r_{\mathrm{Rayl}} = \frac{2D^2}{\lambda}$ m
Distancia crítica [15]	$r_{\mathrm{Crit}} \approx 9D$ m
Rango de distancias	$[3\, r_{\mathrm{Crit}}, r_{\mathrm{Rayl}}]$ m
Rango angular	$[-\frac{\pi}{4}, \frac{\pi}{4}]$ rad

En cuanto a la evolución de la función objetivo respecto al número de iteraciones i, se puede apreciar en la siguiente Fig. 3.25 donde evaluamos el algoritmo propuesto suponiendo propagación SW con los parámetros de simulación descritos en la Tabla 3.25, donde $D = Md$. Nótese que la última iteración, cuando el algoritmo se detiene, no mejora la eficiencia espectral alcanzable, de hecho, disminuye. Por lo tanto, la salida del algoritmo que presenta el método de *scheduling* y precodificación propuesto es obtenida en la iteración anterior, es decir, $i = 7$ en la Fig. 3.25.



(a) Eficiencia espectral.

(b) Número de usuarios servidos.

FIGURA 3.25: Evolución de las métricas con TC con las iteraciones i considerando propagación SW.

Capítulo 4

Conclusiones y líneas futuras

En este capítulo final, se exponen las principales conclusiones que se derivan de las aportaciones de esta tesis. Asimismo, se sugieren algunas líneas de trabajo futuras y posibles aplicaciones de los resultados obtenidos.

4.1. Conclusiones

En esta tesis se han propuesto diferentes escenarios de comunicaciones móviles, desde una perspectiva de PLS, y analizado cómo en dichos escenarios se ven alteradas las comunicaciones cuando se considera MIMO masivo y, por tanto, se eleva considerablemente el número de antenas. A partir de este trabajo, se pueden extraer las siguientes conclusiones:

- En primer lugar, se han estudiado métodos de selección de antena que permiten aprovechar la diversidad de antena con un bajo coste, tanto computacional como *hardware*. En este ámbito, se ha propuesto un método de selección de antena, enfocado en PLS, donde en lugar de buscar maximizar la transmisión al usuario legítimo, se busca reducir la información fugada a los fisgones.
- Este método sub-óptimo ETAS obtiene resultados considerablemente mejores al típico BTAS en escenarios con fuerte presencia de fisgones y aceptables donde BTAS funciona mejor. Asimismo, se ha comparado con otros métodos más complejos como OTAS y MRT donde se ha observado que en estos escenarios el método propuesto obtiene resultados bastante similares. Por otro lado, se ha observado como en el ámbito de la seguridad ZF es el mejor de todos los estudiados.
- Se ha propuesto un tipo de ataque a los sistemas basados PLS denominado ataque de canal producto con desvanecimientos sintéticos. Este se basa en la necesidad de los sistemas PLS de adquirir CSI de los fisgones. Se han probado dos tipos de ataques: Rayleigh y uniforme, nombrados así por la distribución estadística en la que basan su ataque. Se ha demostrado como el uniforme, además de ser más difícil de detectar, es más efectivo. Asimismo, se ha planteado una propuesta para combatirlos basado en establecer zonas de guarda o de seguridad.

- Este ataque se ha probado sobre los métodos de selección de antena anteriores y se ha observado como ETAS consigue combatirlos de forma indirecta reduciendo el impacto sobre el sistema.
- Por otro lado, se ha estudiado la aplicación del modelo de propagación SW, propuesto en [15], en el ámbito de PLS sobre un escenario con un único usuario legítimo. En este sentido, se ha demostrado como los nuevos DoF que aporta este modelo, que incluye al PW como caso particular, permiten reducir la información fugada y, por tanto, reducir las áreas donde un fisgón puede poner en peligro una comunicación segura.
- Se ha ampliado el estudio anterior sobre un escenario con un múltiples usuarios legítimos. Asimismo, sobre este escenario se ha propuesto un método de *scheduling* y precodificación conjunto, el LSP, que incorpora las características de PLS y SW en su diseño.
- Se ha comparado el método propuesto, LSP, con otro existente en la literatura de PLS como es el ZF con *waterfilling* y se ha observado como lo mejora entre un $20\,\%$ y un $40\,\%$ dependiendo de la configuración de fisgones que se considere: TC o PC dependiendo de la capacidad de colaboración que se le supongan a los mismos.

4.2. Líneas futuras

El modelo SW no ha sido muy explorado en el ámbito de PLS y permite seguir pensando y estudiando posibles escenarios de estudio y aplicaciones donde sacar partido a los nuevos DoF proporcionados por la distancia. Asimismo, en la literatura existen otros modelos de propagación entre el PW y el SW como el parabólico [68].

Una importante línea de trabajo futura es utilizar modelos de antenas más complejos: desde utilizar una antena 2D [16] en lugar del ULA utilizado, hasta ir incorporando las posible no idealidades que pueden surgir de trabajar en las zonas de campo cercano. Puesto que en las zonas de campo cercano la estructura de la antena tiene más relevancia, se podrían incorporar modelos de propagación más realistas y estudiar como las posibles no idealidades afectan a los resultados planteados. En este ámbito, el estudio de soluciones reales para las antenas como las RIS [17], las antenas líquidas [69] o las antena dinámica de metasuperficie (DMA) [70].

Asimismo, durante esta tesis se han analizado escenarios de comunicaciones móviles donde los usuarios forman parte del sistema y se supone conocido su CSI. Por tanto, analizar cómo afecta la existencia de CSI imperfecta [71] es interesante, especialmente con métodos como ZF donde anular por completo la interferencia o información fugada es crucial.

En esta tesis se ha planteado un posible ataque basado en PLS, pero se puede estudiar el impacto de otros tipos más comunes como el *jamming* [72] o métodos para combatir los fisgones de forma activa como la transmisión deliberada de ruido blanco [73].

Apéndice A

Publications

A.1. Leakage Subspace Precoding and Scheduling for Physical Layer Security in Multi-User XL-MIMO Systems

[20] G. J. Anaya-López, J. P. González-Coma y F. J. López-Martínez, «Leakage Subspace Precoding and Scheduling for Physical Layer Security in Multi-User XL-MIMO Systems», *IEEE Commun. Lett.*, vol. 27, n.º 2, págs. 467-471, 2023.

DOI: 10.1109/LCOMM.2022.3225881.

Abstract:
We investigate the achievable secrecy spectral efficiency in a multi-user extra-large multiple-input multiple-output (XL-MIMO) system. In these beyond-5G scenarios, seen as the natural evolution of conventional massive MIMO systems, the distances from the mobile users to the base station become comparable to the antenna array dimensions. We show that the consideration of spherical-wavefront propagation inherent to these set-ups is beneficial for physical-layer security, as it provides immunity against eavesdroppers located in similar angular directions that would otherwise prevent secure communication under classical planar-wavefront propagation. A leakage subspace precoding strategy is also proposed for joint secure precoding and user scheduling, which allows to improve the secrecy spectral efficiency over a 40 % compared to conventional zero-forcing methods, under different eavesdropper collusion strategies.

A.2. Spatial Degrees of Freedom for Physical Layer Security in XL-MIMO

[21] G. J. Anaya-López, J. P. González-Coma y F. J. López-Martínez, «Spatial Degrees of Freedom for Physical Layer Security in XL-MIMO», en *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, 2022, págs. 1-5.

DOI: 10.1109/VTC2022-Spring54318.2022.9860861.

Abstract:
This paper analyzes the key differences between the plane-wave (PW) and the spherical-wavefront (SW) models in the context of physical layer security (PLS) for extra-large (XL)-multiple-input multiple-output (MIMO) systems with multiple eavesdroppers. Both colluding and non-colluding strategies are considered for the different eavesdroppers. Results show that the propagation features associated to the SW model allow to reach higher secrecy rates, and to reduce the areas where an eavesdropper makes secure communication unfeasible.

A.3. A New Transmit Antenna Selection Technique for Physical Layer Security with Strong Eavesdropping

[22] G. J. Anaya-López, J. C. Ruiz-Sicilia y F. J. López-Martínez, «A New Transmit Antenna Selection Technique for Physical Layer Security with Strong Eavesdropping», en *2021 4th International Conference on Advanced Communication Technologies and Networking (CommNet)*, 2021, págs. 1-5.

DOI: 10.1109/CommNet52204.2021.9641938.

Abstract:
We propose a new transmit antenna selection (TAS) technique that can be beneficial for physical layer security purposes. Specifically, we show that the conventional TAS criterion based on the legitimate channel state information (CSI) is not recommended when the average signal-to-noise ratio for the illegitimate user becomes comparable or superior to that of the legitimate user. We illustrate that an eavesdropper's based antenna selection technique outperforms conventional TAS, without explicit knowledge of the eavesdropper's instantaneous CSI. Analytical expressions and simulation results to support this comparison are given, showing how this new TAS scheme is a better choice in scenarios with a strong eavesdropper.

A.4. A Product Channel Attack to Wireless Physical Layer Security

[24] G. J. Anaya-Lopez, G. Gomez y F. J. Lopez-Martinez, «A Product Channel Attack to Wireless Physical Layer Security», *IEEE Wireless Commun. Lett.*, vol. 10, n.º 5, págs. 943-947, 2021.

DOI: 10.1109/LWC.2021.3050957.

Abstract:
We propose a novel attack that compromises the physical layer security in wireless systems with eavesdropper's channel state information at the transmitter side. This technique is based on the transmission of a slowly-varying random symbol by the eavesdropper during its uplink transmission, so that the equivalent fading channel observed at the base station (BS) has a larger variance. Then, the BS designs the secure downlink transmission under the assumption that the eavesdropper's channel experiences a larger fading severity than in reality. We show that this approach can lead the BS to transmit to Bob at a rate larger than the secrecy capacity, thus compromising the system secure operation. Our analytical results, corroborated by simulations, show that the use of multiple antennas at the BS may partially alleviate but not immunize against these type of attacks.

A.5. Ataques tipo Canal-Producto a Comunicaciones con Seguridad en Capa Física y Selección de Antena en Transmisión

[23] G. J. Anaya-López, G. Gomez y F. J. López-Martínez, «Ataques tipo Canal-Producto a Comunicaciones con Seguridad en Capa Física y Selección de Antena en Transmisión», *XXXVI Simposium Nacional de la Unión Científica Internacional de Radio*, 2021.

Abstract:
We investigate the impact of a product-channel attack against wireless physical layer security with different diversity techniques. The attack proposed is based on introducing synthetic fading that aims to make the base station transmit at a rate higher than the secrecy capacity. We demonstrate that a low complex transmit antenna selection (TAS) criterion based on the eavesdropper channel improves the robustness against the attack better than the traditional maximal ratio transmission (MRT) scheme or the TAS based on the legitimate channel. Analytical results and simulations are provided to corroborate this fact.

Bibliografía

[1] Forecast, GMDT, «Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017–2022», *Update*, vol. 2017, pág. 2022, 2019.

[2] S. Chen y J. Zhao, «The Requirements, Challenges, and Technologies for 5G of Terrestrial Mobile Telecommunication», *IEEE Commun. Mag.*, vol. 52, n.º 5, págs. 36-43, 2014.

[3] J. Zhang, E. Björnson, M. Matthaiou, D. W. K. Ng, H. Yang y D. J. Love, «Prospective Multiple Antenna Technologies for Beyond 5G», *IEEE J. Sel. Areas Commun.*, vol. 38, n.º 8, págs. 1637-1660, 2020.

[4] M. Bloch, J. Barros, M. R. Rodrigues y S. W. McLaughlin, «Wireless Information-Theoretic Security», *IEEE Trans. Inf. Theory*, vol. 54, n.º 6, págs. 2515-2534, 2008.

[5] P. K. Gopala, L. Lai y H. El Gamal, «On the Secrecy Capacity of Fading Channels», en *2007 IEEE International Symposium on Information Theory*, IEEE, 2007, págs. 1306-1310.

[6] G. Geraci, M. Egan, J. Yuan, A. Razi e I. B. Collings, «Secrecy Sum-Rates for Multi-User MIMO Regularized Channel Inversion Precoding», *IEEE Trans. Commun.*, vol. 60, n.º 11, págs. 3472-3482, 2012.

[7] A. Khisti y G. W. Wornell, «Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel», *IEEE Trans. Inf. Theory*, vol. 56, n.º 7, págs. 3088-3104, 2010.

[8] X. Zhou y M. R. McKay, «Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation», *IEEE Trans. Veh. Technol.*, vol. 59, n.º 8, págs. 3831-3842, 2010.

[9] A. Khisti y G. W. Wornell, «Secure Transmission With Multiple Antennas—Part II: The MIMOME Wiretap Channel», *IEEE Trans. Inf. Theory*, vol. 56, n.º 11, págs. 5515-5532, 2010.

[10] Y. Yapıcı, N. Rupasinghe, I. Güvenç, H. Dai y A. Bhuyan, «Physical Layer Security for NOMA Transmission in mmWave Drone Networks», *IEEE Trans. Veh. Technol.*, vol. 70, n.º 4, págs. 3568-3582, 2021.

[11] G. Gomez, F. J. Martin-Vega, F. J. Lopez-Martinez, Y. Liu y M. Elkashlan, «Physical Layer Security in Uplink NOMA Multi-Antenna Systems With Randomly Distributed Eavesdroppers», *IEEE Access*, vol. 7, págs. 70 422-70 435, 2019.

[12] S. H. Chae, W. Choi, J. H. Lee y T. Q. Quek, «Enhanced Secrecy in Stochastic Wireless Networks: Artificial Noise With Secrecy Protected Zone», *IEEE Trans. Inf. Forensics Secur.*, vol. 9, n.º 10, págs. 1617-1628, 2014.

[13] E. D. Carvalho, A. Ali, A. Amiri, M. Angjelichinoski y R. W. Heath, «Non-Stationarities in Extra-Large-Scale Massive MIMO», *IEEE Wireless Commun.*, vol. 27, n.º 4, págs. 74-80, 2020.

[14] T. Han, X. Ge, L. Wang, K. S. Kwak, Y. Han y X. Liu, «5G Converged Cell-Less Communications in Smart Cities», *IEEE Commun. Mag.*, vol. 55, n.º 3, págs. 44-50, 2017.

[15] H. Lu e Y. Zeng, «How Does Performance Scale with Antenna Number for Extremely Large-Scale MIMO?», en *ICC 2021 - IEEE International Conference on Communications*, 2021, págs. 1-6.

[16] H. Lu e Y. Zeng, «Communicating with Extremely Large-Scale Array/Surface: Unified Modelling and Performance Analysis», *IEEE Trans. Wireless Commun.*, vol. 21, n.º 6, págs. 4039-4053, 2022.

[17] Q. Wu y R. Zhang, «Intelligent Reflecting Surface Enhanced Wireless Network via Joint Active and Passive Beamforming», *IEEE Trans. Wirel. Commun.*, vol. 18, n.º 11, págs. 5394-5409, 2019.

[18] O. Tsilipakos, A. C. Tasolamprou, A. Pitilakis, F. Liu, X. Wang, M. S. Mirmoosa, D. C. Tzarouchis, S. Abadal, H. Taghvaee, C. Liaskos y col., «Toward Intelligent Metasurfaces: The Progress from Globally Tunable Metasurfaces to Software-Defined Metasurfaces with an Embedded Network of Controllers», *Adv. Opt. Mater.*, vol. 8, n.º 17, pág. 2 000 783, 2020.

[19] M. Cui, G. Zhang y R. Zhang, «Secure Wireless Communication via Intelligent Reflecting Surface», *IEEE Wireless Commun. Lett.*, vol. 8, n.º 5, págs. 1410-1414, 2019.

[20] G. J. Anaya-López, J. P. González-Coma y F. J. López-Martínez, «Leakage Subspace Precoding and Scheduling for Physical Layer Security in Multi-User XL-MIMO Systems», *IEEE Commun. Lett.*, vol. 27, n.º 2, págs. 467-471, 2023.

[21] G. J. Anaya-López, J. P. González-Coma y F. J. López-Martínez, «Spatial Degrees of Freedom for Physical Layer Security in XL-MIMO», en *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, 2022, págs. 1-5.

[22] G. J. Anaya-López, J. C. Ruiz-Sicilia y F. J. López-Martínez, «A New Transmit Antenna Selection Technique for Physical Layer Security with Strong Eavesdropping», en *2021 4th International Conference on Advanced Communication Technologies and Networking (CommNet)*, 2021, págs. 1-5.

[23] G. J. Anaya-López, G. Gomez y F. J. López-Martínez, «Ataques tipo Canal-Producto a Comunicaciones con Seguridad en Capa Física y Selección de Antena en Transmisión», *XXXVI Simposium Nacional de la Unión Científica Internacional de Radio*, 2021.

[24] G. J. Anaya-Lopez, G. Gomez y F. J. Lopez-Martinez, «A Product Channel Attack to Wireless Physical Layer Security», *IEEE Wireless Commun. Lett.*, vol. 10, n.º 5, págs. 943-947, 2021.

[25] J. Lopez-Fernandez, G. J. Anaya-Lopez y F. J. Lopez-Martinez, «The Second Order Scattering Fading Model with Fluctuating Line-of-Sight», *submitted to IEEE Trans. Veh. Technol.*, 2023.

[26] J. C. Ruiz-Sicilia, J. Gimenez de la Cuesta, G. J. Anaya-López y F. J. López-Martínez, «Configuring an Intelligent Reflecting Surface for Wireless Communications: the hUMAns at RISk approach», *XXXVI Simposium Nacional de la Unión Científica Internacional de Radio*, 2021.

[27] Taesang Yoo y A. Goldsmith, «On the Optimality of Multiantenna Broadcast Scheduling Using Zero-Forcing Beamforming», *IEEE J. Sel. Areas Commun.*, vol. 24, n.º 3, págs. 528-541, 2006.

[28] G. Geraci, S. Singh, J. G. Andrews, J. Yuan e I. B. Collings, «Secrecy Rates in Broadcast Channels with Confidential Messages and External Eavesdroppers», *IEEE Trans. Wireless Commun.*, vol. 13, n.º 5, págs. 2931-2943, 2014.

[29] C. E. Shannon, «A Mathematical Theory of Communication», *Bell Syst. Tech. J.*, vol. 27, n.º 3, págs. 379-423, 1948.

[30] A. Papoulis y S Unnikrishna Pillai, *Probability, Random Variables and Stochastic Processes*. 2002.

[31] S Leung-Yan-Cheong y M Hellman, «The Gaussian Wire-Tap Channel», *IEEE Trans. Inf. Theory*, vol. 24, n.º 4, págs. 451-456, 1978.

[32] D. Tse y P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge university press, 2005.

[33] M.-S. Alouini y A. J. Goldsmith, «Capacity of Rayleigh Fading Channels Under Different Adaptive Transmission and Diversity-Combining Techniques», *IEEE Trans. Veh. Technol.*, vol. 48, n.º 4, págs. 1165-1181, 1999.

[34] T. K. Lo, «Maximum Ratio Transmission», en *1999 IEEE International Conference on Communications*, IEEE, vol. 2, 1999, págs. 1310-1314.

[35] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov y M. Ylianttila, «Security for 5G and Beyond», *IEEE Commun. Surveys Tuts.*, vol. 21, n.º 4, págs. 3682-3722, 2019.

[36] R. Chataut y R. Akl, «Massive MIMO Systems for 5G and beyond Networks–Overview, Recent Trends, Challenges, and Future Research Direction», *Sensors*, vol. 20, n.º 10, pág. 2753, 2020.

[37] A. Mukherjee y A. L. Swindlehurst, «Robust Beamforming for Security in MIMO Wiretap Channels With Imperfect CSI», *IEEE Trans. Signal Process.*, vol. 59, n.º 1, págs. 351-361, 2010.

[38] Z. Sheng, H. D. Tuan, T. Q. Duong y H. V. Poor, «Beamforming Optimization for Physical Layer Security in MISO Wireless Networks», *IEEE Trans. Signal Process.*, vol. 66, n.º 14, págs. 3710-3723, 2018.

[39] S. Sanayei y A. Nosratinia, «Antenna Selection in MIMO Systems», *IEEE Commun. Mag.*, vol. 42, n.º 10, págs. 68-73, 2004.

[40] A. Mohammadi y F. M. Ghannouchi, «Single RF Front-End MIMO Transceivers», en *RF Transceiver Design for MIMO Wireless Communications*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, págs. 265-288.

[41] H. Alves, R. D. Souza y M. Debbah, «Enhanced Physical Layer Security Through Transmit Antenna Selection», en *2011 IEEE GLOBECOM Workshops (GC Wkshps)*, IEEE, 2011, págs. 879-883.

[42] H. Alves, R. D. Souza, M. Debbah y M. Bennis, «Performance of Transmit Antenna Selection Physical Layer Security Schemes», *IEEE Signal Process. Lett.*, vol. 19, n.º 6, págs. 372-375, 2012.

[43] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober e I. B. Collings, «Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels», *IEEE Trans. Commun.*, vol. 61, n.º 1, págs. 144-154, 2012.

[44] L. Wang, M. Elkashlan, J. Huang, R. Schober y R. K. Mallik, «Secure transmission with antenna selection in MIMO Nakagami-m fading channels», *IEEE Trans. Wirel. Commun.*, vol. 13, n.º 11, págs. 6054-6067, 2014.

[45] J. M. Moualeu, D. B. da Costa, F. J. Lopez-Martinez, W. Hamouda, T. M. N. Nkouatchah y U. S. Dias, «Transmit Antenna Selection in Secure MIMO Systems Over α-μ Fading Channels», *IEEE Trans. Commun.*, vol. 67, n.º 9, págs. 6483-6498, 2019.

[46] N. Sadeque, I. Land y R. Subramanian, «Average Secrecy Rate under Transmit Antenna Selection for the Multiple-Antenna Wiretap Channel», en *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, IEEE, 2013, págs. 238-242.

[47] Y. Feng, S. Yan, Z. Yang, N. Yang y J. Yuan, «Beamforming Design and Power Allocation for Secure Transmission With NOMA», *IEEE Trans. Wirel. Commun.*, vol. 18, n.º 5, págs. 2639-2651, 2019.

[48] Z. Sheng, H. D. Tuan, A. A. Nasir, T. Q. Duong y H. V. Poor, «Power Allocation for Energy Efficiency and Secrecy of Wireless Interference Networks», *IEEE Trans. Wirel. Commun.*, vol. 17, n.º 6, págs. 3737-3751, 2018.

[49] J. Zhu, Y. Zou, G. Wang, Y.-D. Yao y G. K. Karagiannidis, «On Secrecy Performance of Antenna-Selection-Aided MIMO Systems Against Eavesdropping», *IEEE Trans. Veh. Technol.*, vol. 65, n.º 1, págs. 214-225, 2015.

[50] H. A. David y H. N. Nagaraja, *Order Statistics*. John Wiley & Sons, 2004.

[51] C. A. López, *Probabilidad, Variables Aleatorias y Procesos Estocásticos: una Introducción Orientada a las Telecomunicaciones*. Universidad de Valladolid, Secretariado de Publicaciones e Intercambio Editorial, 2004.

[52] M. Abramowitz e I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. US Government printing office, 1964, vol. 55.

[53] C. Zhang, F. Jia, Z. Zhang, J. Ge y F. Gong, «Physical Layer Security Designs for 5G NOMA Systems With a Stronger Near-End Internal Eavesdropper», *IEEE Trans. Veh. Technol.*, vol. 69, n.º 11, págs. 13 005-13 017, 2020.

[54] Z. Sheng, H. D. Tuan, A. A. Nasir y H. V. Poor, «PLS for Wireless Interference Networks in the Short Blocklength Regime with Strong Wiretap Channels», en *GLOBECOM 2020-2020 IEEE Global Communications Conference*, IEEE, 2020, págs. 1-6.

[55] M. Bloch, J. Barros, M. R. D. Rodrigues y S. W. McLaughlin, «Wireless Information-Theoretic Security», *IEEE Trans. Inf. Theory*, vol. 54, n.º 6, págs. 2515-2534, 2008.

[56] X. Jiang, C. Zhong, X. Chen y Z. Zhang, «Secrecy Outage Probability of Wirelessly Powered Wiretap Channels», en *2016 24th European Signal Processing Conference (EUSIPCO)*, IEEE, 2016, págs. 793-797.

[57] A. Shah y A. M. Haimovich, «Performance Analysis of Maximal Ratio Combining and Comparison with Optimum Combining for Mobile Radio Communications with Cochannel Interference», *IEEE Trans. Veh. Technol.*, vol. 49, n.º 4, págs. 1454-1463, jul. de 2000.

[58] M. Joham, W. Utschick y J. A. Nossek, «Linear Transmit Processing in MIMO Communications Systems», *IEEE Trans. Signal Process.*, vol. 53, n.º 8, págs. 2700-2712, 2005.

[59] O. Dizdar, Y. Mao y B. Clerckx, «Rate-Splitting Multiple Access to Mitigate the Curse of Mobility in (Massive) MIMO Networks», *IEEE Trans. Commun.*, vol. 69, n.º 10, págs. 6765-6780, 2021.

[60] Z. Shu, Y. Qian y S. Ci, «On Physical Layer Security for Cognitive Radio Networks», *IEEE Netw.*, vol. 27, n.º 3, págs. 28-33, mayo de 2013.

[61] D. Kapetanovic, G. Zheng y F. Rusek, «Physical Layer Security for Massive MIMO: An Overview on Passive Eavesdropping and Active Attacks», *IEEE Commun. Mag*, vol. 53, n.º 6, págs. 21-27, jun. de 2015.

[62] J. K. Tugnait, «Pilot Spoofing Attack Detection and Countermeasure», *IEEE Trans. Commun.*, vol. 66, n.º 5, págs. 2093-2106, mayo de 2018.

[63] E. Björnson y L. Sanguinetti, «Power Scaling Laws and Near-Field Behaviors of Massive MIMO and Intelligent Reflecting Surfaces», *IEEE Open J. Commun. Soc.*, vol. 1, págs. 1306-1324, 2020.

[64] J. P. González-Coma, F. J. López-Martínez y L. Castedo, «Low-Complexity Distance-Based Scheduling for Multi-User XL-MIMO Systems», *IEEE Wireless Commun. Lett.*, vol. 10, n.º 11, págs. 2407-2411, 2021.

[65] N. Romero-Zurita, D. McLernon, M. Ghogho y A. Swami, «PHY Layer Security Based on Protected Zone and Artificial Noise», *IEEE Signal Process. Lett.*, vol. 20, n.º 5, págs. 487-490, 2013.

[66] M. Khojastehnia y S. Loyka, «To Jam or Not to Jam in Gaussian MIMO Wiretap Channels ?: Invited Paper», en *2021 17th International Symposium on Wireless Communication Systems (ISWCS)*, 2021, págs. 1-6.

[67] Á. Vázquez-Castro y M. Hayashi, «Physical Layer Security for RF Satellite Channels in the Finite-Length Regime», *IEEE Trans. Inf. Forensics Secur.*, vol. 14, n.º 4, págs. 981-993, 2018.

[68] H. Do, N. Lee y A. Lozano, «Parabolic Wavefront Model for Line-of-Sight MIMO Channels», *IEEE Trans. Wirel. Commun.*, 2023.

[69] H Fayad y P Record, «Broadband Liquid Antenna», *Electron. Lett.*, vol. 42, n.º 3, págs. 133-134, 2006.

[70] D. R. Smith, O. Yurduseven, L. P. Mancera, P. Bowen y N. B. Kundtz, «Analysis of a Waveguide-Fed Metasurface Antenna», *Phys. Rev. Appl.*, vol. 8, n.º 5, pág. 054 048, 2017.

[71] K. Zhi, C. Pan, G. Zhou, H. Ren, M. Elkashlan y R. Schober, «Is RIS-Aided Massive MIMO Promising With ZF Detectors and Imperfect CSI?», *IEEE J. Sel. Areas Commun.*, vol. 40, n.º 10, págs. 3010-3026, 2022.

[72] I. Krikidis, J. S. Thompson y S. McLaughlin, «Relay Selection for Secure Cooperative Networks with Jamming», *IEEE Trans. Wirel. Commun.*, vol. 8, n.º 10, págs. 5003-5011, 2009.

[73] P.-H. Lin, S.-H. Lai, S.-C. Lin y H.-J. Su, «On Secrecy Rate of the Generalized Artificial-Noise Assisted Secure Beamforming for Wiretap Channels», *IEEE J. Sel. Areas Commun.*, vol. 31, n.º 9, págs. 1728-1740, 2013.