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

Gonzalo J. Anaya-López, Gerardo Gómez, F. Javier López-Martínez
{gjal, ggomez, fjlopezm}@ic.uma.es
Dpto. de Ingeniería de Comunicaciones, Instituto de Telecomunicación (TELMA)
Universidad de Málaga, Málaga, España 29071.

***Resumen*—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.**

I. Introducción

La investigación en seguridad sobre canales inalámbricos ha experimentado un cambio de paradigma en los últimos años debido a la llegada de las técnicas de seguridad en capa física (PLS). Aunque podría pensarse que la naturaleza *broadcast* del canal inalámbrico es perjudicial para la seguridad, los trabajos realizados en [1, 2] allanaron el camino para aprovechar la naturaleza aleatoria de los canales inalámbricos y proporcionar seguridad a las comunicaciones en presencia de fisgones. Al igual que las técnicas convencionales para la provisión de seguridad en capas superiores, la capa física en entornos inalámbricos también es sensible a los ataques.

Además del *jamming* [3], que afecta a la capacidad de Alice para adquirir la información del estado del canal (CSI) de Bob, hay otros enfoques propuestos en la literatura para realizar ataques desde una perspectiva de PLS. Por ejemplo, el utilizado en este trabajo [4], un ataque destinado a comprometer la seguridad en capa física para escenarios donde los fisgones forman parte del sistema. En este ataque, el fisgón diseña su transmisión de manera que el canal equivalente observado por la estación base (BS) es el producto del desvanecimiento real y una secuencia aleatoria que varía lentamente, es decir, un coeficiente de desvanecimiento sintético. De este modo, la BS diseña la transmisión de su enlace descendente (DL) al usuario legítimo considerando que el fisgón experimenta un desvanecimiento más severo que el real, eligiendo así una tasa de transmisión mayor que la capacidad secreta *real*.

En paralelo, la llegada del *internet de las cosas* con dispositivos de energía y potencia limitada exige estrategias que no incurran en una alta carga computacional ni en complejos protocolos de distribución de claves. Por esta razón, los enfoques basados en PLS se han convertido en una buena alternativa a las técnicas criptográficas utilizadas tradicionalmente para proporcionar seguridad en entornos inalámbricos [1, 5]. Los esquemas de selección de antena en transmisión (TAS), que sólo requieren una cadena de radiofrecuencia (RF), son útiles para reducir la complejidad del hardware de los transmisores, conservando al mismo tiempo algunos de los beneficios de transmitir con múltiples antenas [6]. En concreto, la selección de un criterio subóptimo basado únicamente en la CSI del enlace legítimo es usado habitualmente [7, 8] en detrimento del criterio óptimo que requiere conocimiento perfecto de CSI.

En este trabajo, se investiga el impacto del ataque con canal producto y desvanecimiento sintético uniforme sobre un modelo de sistema con múltiples antenas en transmisión comparando el uso de *maximal ratio transmission* (MRT) y dos esquemas TAS subóptimos. En concreto, demostramos que un criterio de selección basado en el canal del fisgón mejora considerablemente al esquema convencional de TAS como el de [7, 8] y al MRT.

II. Modelo del Sistema

Se considera un escenario de comunicaciones móviles donde una BS, equipada con M antenas, transmite información a los usuarios, equipados con una sola antena, en su área de cobertura. La BS utiliza un protocolo de duplexación por división de tiempo (TDD) para comunicarse con los $\mathcal{V}$ usuarios y, por tanto, la CSI puede ser estimada para cada usuario durante la fase de transmisión en el enlace ascendente (UL). Adicionalmente, se asume que los diferentes canales inalámbricos se ven afectados por desvanecimientos cuasi-estáticos independientes que permanecen constantes durante la transmisión de toda la palabra código.

En el DL, la BS opera en dos modos durante la transmisión definidos como modo *estándar* y *seguro*. Durante el modo *estándar* la BS envía un conjunto de mensajes z_v con $\mathbb{E}\{|z_v|^2\} = 1$ y $v \in \mathcal{V}$ a cada uno de los usuarios. En el modo *seguro*, la BS desea establecer una comunicación segura con el usuario legítimo, $v_{\mathrm{i}} = \mathrm{B}$, asumiendo que un usuario distinto e ilegítimo, $v_{\mathrm{j}} = \mathrm{E}$, quiere interceptar la comunicación.

Durante el UL, la señal recibida por la BS desde el usuario legítimo y del fisgón, $\mathrm{u} = \{\mathrm{B}, \mathrm{E}\}$, en la i-ésima antena puede ser expresada como:

$$y_{\mathrm{u}}^{(\mathrm{i})} = \sqrt{P_T R_{\mathrm{u}}^{-\alpha}} h_{\mathrm{u}}^{(\mathrm{i})} z_{\mathrm{u}} + n_{\mathrm{u}}, \tag{1}$$

donde P_T es la potencia de transmisión equivalente; n_{u} es la componente de ruido blanco gaussiano aditivo (AWGN) en cada receptor, con $\mathbb{E}\{|n_{\mathrm{u}}|^2\} = N_0$; R_{u} es la distancia entre la BS y Bob/Eve; α es el exponente de pérdidas de propagación; y el coeficiente del canal $h_{\mathrm{u}}^{(\mathrm{i})}$ es una variable aleatoria compleja gaussiana circularmente simétrica y normalizada con $\mathbb{E}\{|h_{\mathrm{u}}^{(i)}|^2\} = 1$. A partir de la expresión (1) se pueden obtener las expresiones de las relaciones señal-ruido (SNRs) instantáneas del usuario legítimo y del fisgón como:

$$\gamma_{\mathrm{u}} = \frac{P_T R_{\mathrm{u}}^{-\alpha}}{N_0} |h_{\mathrm{u}}^{\mathrm{eq}}|^2 |z_{\mathrm{u}}|^2 \tag{2}$$

donde $h_{\mathrm{u}}^{\mathrm{eq}}$ corresponde con los coeficientes del canal equivalente que se produce al aplicar alguno de los métodos para aprovechar la diversidad de antena que se detallan en las secciones A y B.

A. Maximal Ratio Transmission

Un método ampliamente utilizado para aprovechar la diversidad de antena en transmisión es el esquema MRT [9]. En esta configuración, durante la transmisión DL en modo seguro, la BS crea el mensaje z_{B} con $\mathbb{E}\{|z_{\mathrm{B}}|^2\} = 1$ adaptando la señal transmitida con un vector de *beamforming*, $\mathbf{w}_{\mathrm{B}} \in \mathbb{C}^{\mathbf{M}\times\mathbf{1}}$, al canal instantáneo de Bob. Debido a que el esquema MRT se ajusta al canal legítimo, $|h_{\mathrm{B}}^{\mathrm{eq}}|^2$ sigue una distribución Gamma con parámetros de escala y forma M y M, respectivamente, mientras que $|h_{\mathrm{E}}^{\mathrm{eq}}|^2$ sigue una distribución exponencial con media unitaria [10]:

$$F_{\mathrm{B}}(x) = 1 - \exp\left(-\frac{Mx}{\overline{\gamma}_{\mathrm{B}}}\right) \sum_{n=0}^{M-1} \left(\frac{Mx}{\overline{\gamma}_{\mathrm{B}}}\right)^n \frac{1}{n!} \tag{3}$$

y

$$F_{\mathrm{E}}(x,\beta) = 1 - \exp\left(\frac{-x}{\beta}\right), \tag{4}$$

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

El usuario ilegítimo es incapaz de aprovechar la diversidad de antena del sistema, hecho que se refleja en las SNRs:

$$\gamma_{\mathrm{u}} = \frac{P_T R_{\mathrm{u}}^{-\alpha}}{N_0} |h_{\mathrm{u}}^{\mathrm{eq}}|^2 |z_{\mathrm{u}}|^2 = \overline{\gamma}_{\mathrm{u}_0} |h_{\mathrm{u}}^{\mathrm{eq}}|^2 |z_{\mathrm{u}}|^2 \tag{5}$$

donde las medias son $\overline{\gamma}_{\mathrm{B}} = \mathbb{E}\{\gamma_{\mathrm{B}}\} = M\overline{\gamma}_{\mathrm{B}_0}$ y $\overline{\gamma}_{\mathrm{E}} = \mathbb{E}\{\gamma_{\mathrm{E}}\} = \overline{\gamma}_{\mathrm{E}_0}$, siendo $\overline{\gamma}_{\mathrm{B}_0}$ y $\overline{\gamma}_{\mathrm{E}_0}$ las medias en el caso de transmitir con una sola antena. Nótese que $\overline{\gamma}_{\mathrm{E}}$ no está influenciado por el número de antenas, M, ya que el vector de *beamforming*, $\mathbf{w}_{\mathrm{B}}$, no está adaptado al canal de Eve.

B. TAS basado en Bob

Cuando se selecciona una antena aleatoria para la transmisión, los coeficientes h_B^{eq} y h_E^{eq} tienen la misma distribución que considerar la transmisión con una única antena en la BS, es decir, no hay ganancia por tener múltiples antenas. Sin embargo, esta situación cambia cuando se considera un criterio TAS distinto al aleatorio.

El esquema de selección de antena en transmisión basado en Bob (B-TAS) es el esquema que en el estado del arte suele asociarse a TAS [7, 8] en la literatura de PLS. Bajo este criterio, se selecciona la antena que maximiza la tasa de transmisión del canal legítimo, en lugar de maximizar la capacidad secreta. Por este motivo, se considera un esquema subóptimo [11]. A pesar de no seleccionar la mejor antena posible desde el punto de vista de la seguridad, este esquema es popular en la práctica porque no requiere CSI del fisgón. Además, tampoco se requiere la información completa de Bob para implementar este esquema TAS, ya que la información del índice de antena puede ser recuperada de Bob usando un canal de retroalimentación de baja velocidad, o estimada en Alice usando un detector de energía. Así pues, se trata de un criterio de selección de antena de bajo coste, ya que tan solo es función de los coeficientes del canal legítimo:

$$h_{\mathrm{B}}^{\mathrm{eq}} = \underset{i=1,\ldots,M}{\max} \left\{ \left| h_{\mathrm{B}}^{(i)} \right|^2 \right\}, \tag{6}$$

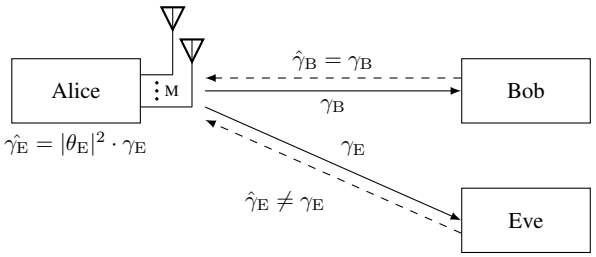

Fig. 1. Modelo del sistema bajo consideración. Por simplicidad, solo se han representado los usuarios de interés.

donde la distribución de $h_{\mathrm{B}}^{\mathrm{eq}}$ está definida por el estadístico del máximo (o M-ésimo orden) [12] como sigue:

$$F_{\mathrm{B}}^{M}(x) = F(x)^M, \tag{7}$$

donde $F(x)$ es la función de distribución acumulada (FDA) de los coeficientes si se seleccionase una antena aleatoriamente. Obsérvese que la distribución en (7) depende del número de antenas M entre las que se hace la selección. Por el contrario, la distribución de $h_{\mathrm{E}}^{\mathrm{eq}}$ no se ve alterada por el criterio de selección B-TAS, de la misma forma que ocurre con MRT.

C. TAS basado en Eve

El último esquema a analizar se denomina selección de antena en transmisión basado en Eve (E-TAS) y pretende mejorar las prestaciones de seguridad del sistema seleccionando la antena de transmisión únicamente en función del canal del fisgón. El fundamento de este esquema proviene del hecho de que la capacidad secreta puede mejorarse aumentando la capacidad del canal legítimo o disminuyendo la capacidad del canal del fisgón. Este último enfoque es interesante en casos donde el fisgón es fuerte, es decir, cuando el canal del fisgón tiene una SNR media mejor que la del canal legítimo [13][14]. Por lo tanto, el esquema E-TAS pretende mejorar la capacidad secreta seleccionando la antena que presenta el peor canal para el fisgón. De este modo, la CSI del canal legítimo no es necesaria en el criterio de selección:

$$h_{\mathrm{E}}^{\mathrm{eq}} = \underset{i=1,\ldots,M}{\mathrm{mín}} \left\{ \left| h_{\mathrm{E}}^{(i)} \right|^2 \right\}, \tag{8}$$

donde la distribución de $h_{\mathrm{E}}^{\mathrm{eq}}$ viene definida por el estadístico del mínimo (o primer orden) [12] como sigue:

$$F_{\mathrm{E}}^{1}(x) = 1 - [1 - F(x)]^M, \tag{9}$$

mientras que la distribución de $h_{\mathrm{B}}^{\mathrm{eq}}$ no se ve modificada por el criterio de selección E-TAS.

III. Ataque con Canal Producto

Como se ha mencionado previamente, la BS diseña la transmisión en DL para cada usuario usando alguno de los esquemas presentados anteriormente. Para ello, estima la CSI durante la fase de transmisión del UL. Por tanto, se tiene que la máxima tasa de transmisión segura, la capacidad secreta media (ASC), viene definida por:

$$\overline{C}_{\mathrm{S}} = \mathbb{E}\{C_{\mathrm{S}}(\gamma_{\mathrm{B}}, \gamma_{\mathrm{E}})\}, \tag{10}$$

donde $C_{\mathrm{S}}(\gamma_{\mathrm{B}}, \gamma_{\mathrm{E}})$ es la capacidad secreta instantánea

$$C_{\mathrm{S}}(\gamma_{\mathrm{B}}, \gamma_{\mathrm{E}}) \underset{\gamma_{\mathrm{B}} > \gamma_{\mathrm{E}}}{=} [\log_2(1+\gamma_{\mathrm{B}}) - \log_2(1+\gamma_{\mathrm{E}})]^+, \tag{11}$$

donde $[\cdot]^+$ se usa para indicar que $C_{\mathrm{S}} = 0$ cuando el argumento entre paréntesis es negativo.

El ataque en capa física considerado en este trabajo pretende engañar a la BS en la fase de UL [4]. Para ello, el fisgón transmite los símbolos modificados $\tilde{x}_{\mathrm{E}} = x_{\mathrm{E}} \cdot \theta_{\mathrm{E}}$ con $\mathbb{E}\{|\tilde{x}_{\mathrm{E}}|^2\} = 1$. La variable sintética θ_{E} se genera de forma que varíe con la misma tasa que los desvanecimientos propios del canal. Bajo esta situación, la BS estima el canal de Eve como $\hat{\mathbf{h}}_{\mathrm{E}} = \theta_{\mathrm{E}}\mathbf{h}_{\mathrm{E}}$, mientras que la estimación del canal de Bob no sufre ninguna alteración.

La transmisión entre Alice y Bob, ver Fig. 1, se diseña en base a las SNRs $\hat{\gamma}_{\mathrm{B}}$ y $\hat{\gamma}_{\mathrm{E}}$. Puesto que el canal de Bob no se ve alterado, tenemos que $\hat{\gamma}_{\mathrm{B}} = \gamma_{\mathrm{B}}$, mientras que $\hat{\gamma}_{\mathrm{E}} = |\theta_{\mathrm{E}}|^2\gamma_{\mathrm{E}}$. Sin embargo, la SNR media de Eve no cambia, puesto que el ataque se definió con media unitaria. Esto se hace para evitar ser detectado, ya que la SNR media está fuertemente influenciada por las pérdidas de propagación entre cada usuario y la BS. Este cambio en la SNR pretende provocar que la BS estime una capacidad secreta del canal distinta a la *real* y, por tanto, diseñe la transmisión con una tasa superior a la permitida para una comunicación segura:

$$\begin{aligned} R_{\mathrm{S}}(\gamma_{\mathrm{B}}, \hat{\gamma}_{\mathrm{E}}) &\underset{\gamma_{\mathrm{B}} > \hat{\gamma}_{\mathrm{E}}}{=} C_{\mathrm{B}}(\gamma_{\mathrm{B}}) - \hat{C}_{\mathrm{E}}(\hat{\gamma}_{\mathrm{E}}) \\ &\underset{\gamma_{\mathrm{B}} > \hat{\gamma}_{\mathrm{E}}}{=} [\log_2(1+\gamma_{\mathrm{B}}) - \log(1+\hat{\gamma}_{\mathrm{E}})]^+. \end{aligned} \tag{12}$$

Comparando las ecuaciones (11) y (12) se observa como la capacidad secreta real del canal y la que la BS utiliza para su diseño no coinciden; en adelante, nos referiremos a ella como capacidad secreta comprometida, R_{S}, y a su diferencia como exceso de tasa segura, $\mathcal{D}$. A partir de la ecuación (12), se tiene que la capacidad secreta comprometida media es:

$$\overline{R}_{\mathrm{S}} = \mathbb{E}\{R_{\mathrm{S}}\left(\gamma_{\mathrm{B}}, \hat{\gamma}_{\mathrm{E}}\right)\}. \tag{13}$$

Cuando la SNR de Bob es lo suficientemente grande, la capacidad secreta media se puede aproximar por [8]

$$\overline{C}_{\mathrm{S}} \underset{\overline{\gamma}_{\mathrm{B}} \to \infty}{\approx} \mathbb{E}\{C_{\mathrm{B}}\left(\gamma_{\mathrm{B}}\right)\} - \mathbb{E}\{C_{\mathrm{E}}\left(\gamma_{\mathrm{E}}\right)\}, \tag{14}$$

y de la misma forma, cuando la SNR de Bob es lo suficientemente grande, la capacidad secreta comprometida es

$$\overline{R}_{\mathrm{S}} \underset{\overline{\gamma}_{\mathrm{B}} \to \infty}{\approx} \mathbb{E}\{C_{\mathrm{B}}\left(\gamma_{\mathrm{B}}\right)\} - \mathbb{E}\{\hat{C}_{\mathrm{E}}\left(\hat{\gamma}_{\mathrm{E}}\right)\}. \tag{15}$$

Debido a que la $\hat{h}_{\mathrm{E}}^{\mathrm{eq}}$ tiene una mayor varianza que $h_{\mathrm{E}}^{\mathrm{eq}}$, se tiene que $\mathbb{E}\{C_{\mathrm{E}}\left(\gamma_{\mathrm{E}}\right)\} > \mathbb{E}\{\hat{C}_{\mathrm{E}}\left(\hat{\gamma}_{\mathrm{E}}\right)\}$ y, por tanto, $\overline{R}_{\mathrm{S}} > \overline{C}_{\mathrm{S}}$. De esta forma, la BS está estimando un canal para Eve con un desvanecimiento más severo del que realmente es y, en consiguiente, una tasa de transmisión, $\overline{R}_{\mathrm{S}}$, por encima de la capacidad secreta media *real* del canal. El resultado es que la seguridad del canal queda comprometida.

Para evaluar cómo afecta este ataque a la capacidad secreta, se usa la formulación de ASC definida en [15, eq. (12)]:

$$\overline{C}_{\mathrm{S}}\left(\overline{\gamma}_{\mathrm{B}}, \overline{\gamma}_{\mathrm{E}}\right) = \frac{1}{\ln 2}\int_0^\infty \frac{F_{\mathrm{E}}(x)\left[1 - F_{\mathrm{B}}(x)\right]}{1+x} dx, \tag{16}$$

donde, si en lugar de utilizar $F_{\mathrm{E}}(x)$, se utiliza la FDA de Eve bajo el ataque, $F_{\hat{\mathrm{E}}}(x)$, se obtiene la expresión para $\overline{R}_{\mathrm{S}}$. Esta formulación permite evaluar la ASC mediante paquetes estándar de integración numérica únicamente con las FDA de los canales de Eve y Bob.

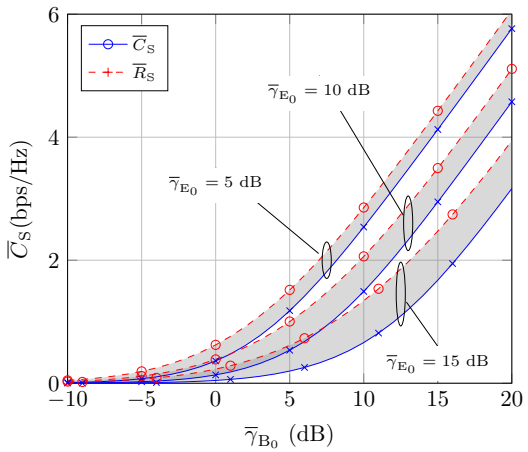

Fig. 2. Capacidad secreta media ($\overline{C}_{\mathrm{S}}$) vs. tasa media comprometida ($\overline{R}_{\mathrm{S}}$) utilizando B-TAS en función de $\overline{\gamma}_{\mathrm{B}_0}$, con $M = 4$ y $\overline{\gamma}_{\mathrm{E}_0} = \{5, 10, 15\}$ dB. Los marcadores corresponden con simulaciones usando el método de MC.

La distribución del canal del fisgón es exponencial tanto para MRT como para B-TAS sin tener en cuenta el ataque, mientras que para E-TAS la distribución viene definida en la ecuación (9). Por otro lado, la distribución del canal legítimo es exponencial para E-TAS, mientras que para MRT y B-TAS se han definido en la ecuaciones (3) y (7) respectivamente. Para utilizar la ecuación (16) se necesita la distribución del canal con la variable sintética, $|\theta_{\mathrm{E}}|$, que se obtiene resolviendo la distribución de $\hat{\gamma}_{\mathrm{E}} = |\theta_{\mathrm{E}}|^2\gamma_{\mathrm{E}}$ como sigue:

$$F_{\hat{\mathrm{E}}}(z) = \int_0^\infty F_{\mathrm{E}}\left(\frac{z}{y}\right) f_{\mathrm{y}}\left(y\right) dy, \tag{17}$$

donde $f_{\mathrm{y}}\left(y\right)$ es la función de densidad de probabilidad (FDP) de la variable $y = |\theta_{\mathrm{E}}|$.

La distribución uniforme, para que sea unitaria en potencia, debe tener el parámetro $|\theta_{\mathrm{E}}|^2 \in [0, \sqrt{3}]$. Con esta premisa, la distribución del producto de γ_{E}, siendo Exponencial, y esta variable Uniforme [4] es:

$$F_{\hat{\mathrm{E}}}^{\mathrm{Uni}}(z) = 1 - \left[e^{-\frac{z}{3\overline{\gamma}_{\mathrm{E}}}} - \sqrt{\frac{z\pi}{3\overline{\gamma}_{\mathrm{E}}}}\mathrm{erfc}\left(\sqrt{\frac{z}{3\overline{\gamma}_{\mathrm{E}}}}\right)\right], \tag{18}$$

donde $\mathrm{erfc}(\cdot)$ es la función de error complementaria. Para obtener la expresión de E-TAS tan solo hay que aplicar un cambio de variable $\overline{\gamma}_{\mathrm{E}}^{\mathrm{E-TAS}} = \overline{\gamma}_{\mathrm{E}}/M$.

IV. Resultados Numéricos

A continuación, se evalúan las métricas de rendimiento introducidas en la sección anterior para una serie de escenarios de interés. Se utilizan simulaciones de MC para comprobar la validez de los resultados analíticos presentados.

En la Fig. 2 representamos la capacidad secreta media y la capacidad secreta comprometida media para diferentes valores de $\overline{\gamma}_{\mathrm{E}}$ y un transmisor B-TAS con múltiples antenas, $M = 4$. Observamos que en todos los casos la capacidad secreta comprometida, $\overline{R}_{\mathrm{S}}$, que es la métrica con la que Alice diseña la transmisión en DL, excede la capacidad secreta *real*, $\overline{C}_{\mathrm{S}}$. Por tanto, cualquier tasa de transmisión dentro del área sombreada en gris es sensible a ser decodificada por el fisgón. Además, la diferencia entre $\overline{R}_{\mathrm{S}}$ y $\overline{C}_{\mathrm{S}}$ crece a medida que $\overline{\gamma}_{\mathrm{E}}$ crece. Por lo tanto, para una configuración dada, el ataque es más efectivo cuanto más cerca esté el fisgón de la BS.

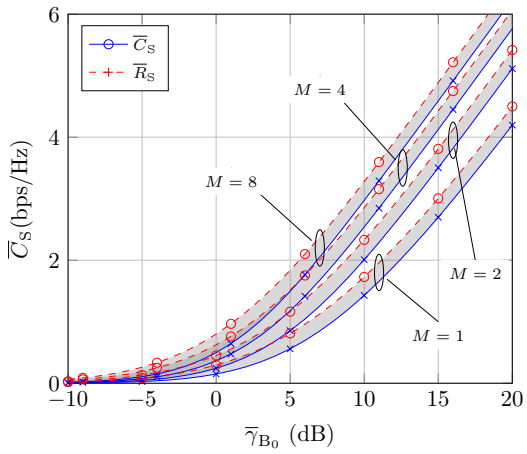

Fig. 3. Capacidad secreta media ($\overline{C}_{\mathrm{S}}$) vs. tasa media comprometida ($\overline{R}_{\mathrm{S}}$) utilizando B-TAS en función de of $\overline{\gamma}_{\mathrm{B}_0}$, con $\overline{\gamma}_{\mathrm{E}_0} = 5$ dB y $M = 1, 2, 4, 8$. Los marcadores corresponden con simulaciones usando el método de MC.

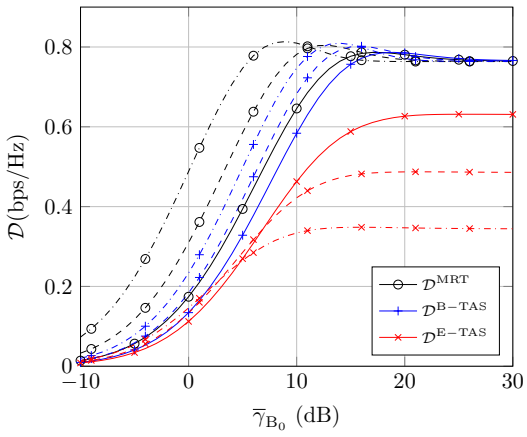

Fig. 4. Exceso de tasa segura $\mathcal{D}$ utilizando MRT, B-TAS y E-TAS en función de $\overline{\gamma}_{\mathrm{B}_0}$ y con $\overline{\gamma}_{\mathrm{E}} = 15$ dB. Los casos de $M = 2, 4, 8$ antenas se representan con líneas continuas, discontinuas y discontinuas-punteadas respectivamente.

En la Fig. 3 se evalúa la capacidad secreta media y la capacidad secreta comprometida media 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. 2, 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. 4 se aprecia que esto no es cierto en todo el rango de SNRs. En esta última figura se comparan los tres esquemas utilizados para aprovechar la diversidad de antena 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: (*i*) $\mathcal{D}$ tiende a quedarse entorno a 0.77 bps/Hz independientemente del número de antenas para *maximal ratio combining* (MRC) y B-TAS; (*ii*) MRT es considerablemente más sensible a este ataque que los esquemas TAS, efecto que aumenta con el número de antenas; (*iii*) el esquema E-TAS es el que menos se ve afectado por este tipo de ataque, siendo bastante destacable su comportamiento con tan solo 8 antenas en transmisión.

Por motivos de espacio no se presentan las Fig. 2 y 3 con MRT y E-TAS. El efecto observado con MRT es prácticamente idéntico al de B-TAS, mientras que con E-TAS la capacidad secreta comprometida y de capacidad secreta *real* se van acercan conforme se aumenta el número de antenas, efectos que se reflejan también en la Fig. 4.

V. Conclusiones

Se ha analizado el efecto de ataques con desvanecimientos sintéticos frente a los métodos MRT y TAS. En concreto, se observa cómo utilizar un método con bajo coste enfocado a minimizar el canal del fisgón, E-TAS, consigue una gran robustez frente a este tipo de ataques. Los resultados demuestran un claro perjuicio al aumentar el número de antenas en un régimen con baja SNR en el canal legítimo para todos los esquemas presentados. Sin embargo, cuando se utiliza E-TAS se observa una clara mejoría frente al ataque conforme se aumenta el número de antenas cuando la SNR del canal legítimo es positiva.

VI. Agradecimientos

Este trabajo ha sido parcialmente financiado por la Iniciativa de Empleo Juvenil y el Fondo Social Europeo, el Fondo Europeo de Desarrollo Regional (FEDER), la Junta de Andalucía bajo el proyecto P18-RT-3175 y por la Universidad de Málaga.

Referencias

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[2] P. K. Gopala, L. Lai, and H. El-Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[3] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 28–33, May 2013.

[4] G. J. Anaya-Lopez, G. Gomez, and F. J. Lopez-Martinez, "A product channel attack to wireless physical layer security," *IEEE Wireless Communications Letters*, vol. 10, no. 5, pp. 943–947, 2021.

[5] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[6] S. Sanayei and A. Nosratinia, "Antenna selection in MIMO systems," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 68–73, 2004.

[7] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, 2012.

[8] J. M. Moualeu, D. B. da Costa, F. J. Lopez-Martinez, W. Hamouda, T. M. N. Nkouatchah, and U. S. Dias, "Transmit Antenna Selection in Secure MIMO Systems Over α-μ Fading Channels," *IEEE Trans. Commun.*, vol. 67, no. 9, pp. 6483–6498, 2019.

[9] T. K. Lo, "Maximum ratio transmission," in *1999 IEEE International Conference on Communications (Cat. No. 99CH36311)*, vol. 2. IEEE, 1999, pp. 1310–1314.

[10] A. Shah and 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, no. 4, pp. 1454–1463, July 2000.

[11] J. Zhu, Y. Zou, G. Wang, Y.-D. Yao, and G. K. Karagiannidis, "On secrecy performance of antenna-selection-aided mimo systems against eavesdropping," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 214–225, 2015.

[12] H. A. David and H. N. Nagaraja, "Order statistics," *Encyclopedia of statistical sciences*, 2004.

[13] C. Zhang, F. Jia, Z. Zhang, J. Ge, and F. Gong, "Physical layer security designs for 5g noma systems with a stronger near-end internal eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13 005–13 017, 2020.

[14] Z. Sheng, H. D. Tuan, A. A. Nasir, H. Vincent Poor, and E. Dutkiewicz, "Physical layer security aided wireless interference networks in the presence of strong eavesdropper channels," *IEEE Transactions on Information Forensics and Security*, pp. 1–1, 2021.

[15] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in Two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247–258, Feb 2014.