Secrecy Capacity Bounds Analysis for Physical Layer Security based on Game Theory

N. M. Ortega and C. Valencia

***Abstract*—A wireless communication aided with Cooperative Jamming in order to enhance Physical Layer security is modeled with Game Theory, using Secrecy Capacity as payment function. To completely take in account the inherent randomness of the wireless channel, a Second Order Cone Programming deterministic equivalent is derived from the game resulting probabilistic optimization problem. Results show how upper and lower bounds of the secrecy capacity, associated to the game values, can be used to characterize the system. Suggested mixed strategies are implemented and compared with pure strategies, and it's shown that performance of mixed strategies, in terms of outage probability, lays exactly between the performances of pure strategies.**

***Keywords*— Physical Layer Security, Second Order Cone Programming, Wireless Communications.**

I. INTRODUCCION

LA NATURALEZA abierta de los sistemas de comunicación inalámbricos ha permitido la generación de incontables aplicaciones escalables y de fácil acceso, resultando en un uso masivo de las tecnologías asociadas, transformándolos en un amplio e interesante campo de estudio. Sin embargo, esta misma naturaleza y el desarrollo de tendencias como Internet de las Cosas (IoT), Ciudades Inteligentes, Redes de Sensores Inalámbricos (WSN), Redes de Comunicación Vehicular, entre otras, ha llevado a los investigadores al desarrollo de nuevos protocolos, infraestructura y mecanismos de seguridad para comunicaciones, dada la naturaleza de la información transmitida en este tipo de redes.

El enfoque tradicional de seguridad es el uso de sistemas Criptográficos. Este tipo de mecanismos impiden que un receptor ilegitimo pueda obtener la información que está siendo transmitida en el canal, incluso si este es capaz de recibirla sin distorsión. Sin embargo, la creciente capacidad computacional global y la pronta llegada de procesadores cuánticos, que podrían descifrar un sistema criptográfico en un tiempo razonable, ha transformado la búsqueda de sistemas de seguridad complementarios o alternativos, tales como la Seguridad de Capa Física (PLS), en una prioridad absoluta.

La teoría de comunicaciones seguras fue desarrollada en [1]. Aquí, Shannon mostró que un secreto perfecto es alcanzado cuando la longitud de la llave secreta es al menos del mismo tamaño que el mensaje que está siendo transmitido.

Este resultado se basa en el supuesto que el receptor ilegítimo posee exactamente la misma información que el receptor legítimo, a excepción de la llave secreta [1], [2].

N. M. Ortega, Departamento de Ingeniería Eléctrica, Universidad de Chile, Santiago, Chile, nortega@ing.uchile.cl

C. Valencia, Departamento de Ingeniería Eléctrica, Universidad de Santiago, de Chile, Santiago, Chile, claudio.valenciac@usach.cl.

Corresponding author: nortega@ing.uchile.cl

El modelo de canal *wire-tap* fue propuesto en [3]. Este es ampliamente utilizado por la literatura para describir el problema de PLS [4], [5]. Este esquema asume que el canal del receptor ilegitimo es una versión degradada del canal de transmisión legitimo [2].

Años después, el escenario donde ambos, receptor legitimo e ilegitimo, poseen canales independientes, como en el caso de una transmisión tipo *broadcast*, fue estudiado en [6]. Csiszar probo que una comunicación segura es lograble si y solo si, la capacidad del canal de escucha ilegítimo es menor a la capacidad del canal legítimo, generalizando lo planteado inicialmente por [3]. En [6] se define la capacidad de secreto, la cual está dada por la máxima tasa de transmisión alcanzable sin que el receptor ilegítimo sea capaz de decodificar la información transmitida. Sin embargo, si por alguna circunstancia el receptor ilegitimo posee mejores condiciones de canal que el receptor legítimo, la capacidad de secreto se hace igual a cero [2].

Varios autores han mostrado que condiciones de canal optimas son capaces de garantizar una transmisión con secreto perfecto [7], [8]. Este planteamiento es llamado el Enfoque de la Teoría de Información para Seguridad. El objetivo de este enfoque es alcanzar altas tasas de secreto, impidiendo que el receptor ilegítimo obtenga la información que está siendo transmitida. La forma de lograrlo es a través de una degradación selectiva del canal del receptor ilegítimo, haciendo que la señal transmitida este tan distorsionada, que este último no pueda obtener información desde ella.

Para obtener estas condiciones de canal optimas, en [2] se propone la manipulación activa del canal mediante la incorporación de incertidumbre intencional en la señal transmitida, incorporando ruido artificial en la misma, con el objetivo de distorsionarla, de forma que el receptor ilegitimo no pueda obtener información de la misma [2], [9]. Este esquema es llamado *Jamming* Cooperativo (CJ).

En [10], el uso de CJ es propuesto para mejorar la PLS de una red que incorpora una serie de *relays* no confiables. Por otro lado, [11] estudia el uso de CJ en una red basada en Solicitud de Repetición Automática (ARQ) con los mismos propósitos que el estudio realizado en [10].

Habitualmente, cuando se habla de la presencia de un *jammer,* se entiende como la existencia de un ataque de interferencia. Considerando que un ataque tipo *jamming* de denegación de servicio, involucra agentes racionales con objetivos opuestos, la Teoría de Juegos resulta ser una herramienta prometedora para modelar tales situaciones de conflicto [12], [13]. Por ejemplo, en [14] proponen estrategias para desactivar un ataque *jamming*, de forma que la energía del atacante sea drenada lo más rápido posible. Aquí, la interacción entre el atacante y la red es modelada como un Juego No Cooperativo. Una estructura teórica de los juegos no cooperativos de suma cero, para la detección y prevención de

ataques tipo *jamming* se presentan en [15]. La función de pago utilizada para el juego es la Relación Señal a Ruido más Interferencia (SINR). En [16] se estudia un ataque *jamming* a una WSN como un juego no cooperativo de suma cero, donde las estrategias de los jugadores están dadas por sus potencias de transmisión disponibles. Este trabajo considera la naturaleza aleatoria del canal inalámbrico utilizando un modelo de optimización estocástico para la resolución del problema.

Por la descripción anteriormente presentada, se puede observar que un *jammer* puede ser utilizado como un elemento que limita la comunicación o un elemento que colabore en la comunicación segura desde la perspectiva de PLS. Entonces se puede aplicar la Teoría de Juegos para estudiar la PLS. En ese sentido en [17] se estudian problemas de tipo PLS y derivan modelos utilizando teoría de juegos.

Adicionalmente, la capacidad de secreto se presenta como una métrica apropiada para el estudio de PLS con teoría de juegos en [18]. El trabajo propone modelos de PLS mediante juegos no cooperativos utilizando la capacidad de secreto como función de pago y la distribución de la potencia total de transmisión como estrategias, cuando se utiliza CJ. El desempeño de varias distribuciones de potencia entre la señal de información y la de *jamming* cooperativo son estudiadas con el fin de mejorar la seguridad de la comunicación.

Debido a la aleatoriedad inherente al medio inalámbrico, es necesaria la utilización de modelos estocásticos que tomen en cuenta esta característica particular. En [17] se deriva un problema de optimización de Programación Cónica de Segundo Orden (SOCP), que incluye matrices de covarianza resultantes de variables aleatorias, las cuales utilizan la ganancia del canal para el cálculo del pago del juego. Lo anterior es posible, transformando el problema de optimización lineal inicial, en uno probabilístico. Este mismo modelo se utiliza en [19] para analizar la Capacidad de Secreto de un sistema que utiliza CJ. El presente artículo busca profundizar lo mostrado en [19], extendiendo los resultados de las estrategias mixtas a fin de validarlas en función de la Probabilidad de *Outage* versus la Capacidad de *Outage*, mostrando explícitamente las cotas de la Capacidad de Secreto para el modelo de juego, las cuales pueden ser utilizadas para caracterizar un sistema de comunicación asumiendo condiciones particulares en su tasa de transmisión.

El resto del trabajo sigue como se describe a continuación. La sección II describe en detalle el esquema de CJ. La sección III aborda el modelo de juego utilizado y sus problemas de optimización derivados. La sección IV muestra los resultados numéricos obtenidos a partir del modelamiento del juego y el desempeño de la implementación de estas estrategias. Finalmente, en la sección V se señalan las conclusiones más relevantes asociadas al trabajo.

II. DESCRIPCIÓN DEL SISTEMA

La figura 1 muestra el esquema PLS utilizado. Un nodo transmisor de múltiples antenas (S) busca transmitir un mensaje secreto a un nodo receptor (D). Sin embargo, un nodo pasivo (que no ejecuta ninguna transmisión) (E) busca realizar una escucha no autorizada de la información que está siendo transmitida desde el nodo S al nodo D. E se identifica como un agente malicioso *eavesdropper*, que podría dar un mal uso a la información obtenida de manera ilegítima. Se asumen canales de desvanecimiento plano y conocimiento perfecto del estado del canal (CSI).

Para evitar que el nodo E tenga éxito, ruido artificial tipo *jamming* es insertado a través de alguna de las antenas transmisoras (J), generando incertidumbre intencional en la recepción. La degradación selectiva solo del canal del nodo E es lograble si se asume que las antenas generan el ruido artificial en el espacio nulo del canal legítimo. Esto es realizable mediante técnicas de *beamforming* [4].

Tanto el nodo D como el E reciben la misma señal, la cual sufre de desvanecimiento y ruido aditivo. Se asume que el transmisor posee N_T antenas, y tanto el receptor como el *eavesdropper* poseen una antena de recepción cada uno. El canal entre el transmisor y el receptor, en el instante k, se denota por el vector de dimensiones $1xN_T$, H_k. Si x_k es la señal transmitida y z_k es la señal recibida en el instante k, se tiene entonces:

$$z_k = H_k x_k + n_k \tag{1}$$

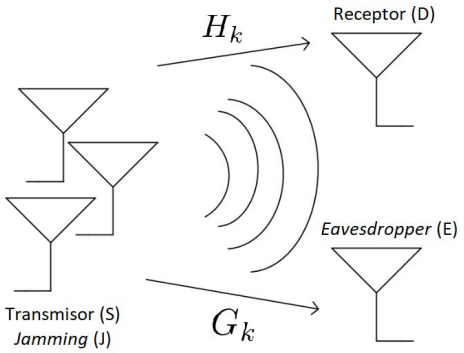


Figura 1. Descripción del sistema.

donde n_k son muestras de ruido blanco gaussiano aditivo (AWGN) con varianza σ_n^2. Similarmente, el canal del transmisor hacía el *eavesdropper* está dado por el vector de dimensiones $1xN_T$, G_k, y la señal recibida en el instante k, y_k, está dada por:

$$y_k = G_k x_k + e_k, \tag{2}$$

donde e_k son muestras AWGN con varianza σ_e^2.

Para que el receptor legítimo solo reciba la señal de información y que el canal del *eavesdropper* sea degradado selectivamente, la señal transmitida es modelada como la suma de la señal de información y la señal de ruido artificial:

$$x_k = s_k + w_k, \tag{3}$$

donde s_k es la señal de información y w_k es la señal de ruido artificial. Dado que la señal de *jamming* cooperativo se calcula

en el espacio nulo Z_k del canal del receptor legítimo H_k, $H_k \cdot W_k = 0$. Así, z_k está dado por:

$$z_k = H_k x_k + n_k = H_k(s_k + w_k) + n_k = H_k s_k + n_k \quad (4)$$

La potencia de transmisión utilizada para la para señal de información $P_{Inf} = E[s_k^\dagger s_k]$ es menor a la potencia total de transmisión P_0, dado que una porción de la potencia es utilizada para señal de ruido artificial.
El *eavesdropper* recibe la señal y_k dada por:

$$y_k = G_k s_k + G_k w_k + e_k. \quad (5)$$

Lo anterior se logra diseñando la señal de ruido como se muestra en [20].
Finalmente, la potencia de ruido efectiva del canal del *eavesdropper* está dada por $E[|G_k w_k|]^2 + \sigma_E^2$. La capacidad de secreto del sistema está dada por [2]:

$$C_s = (I(Z;U) - I(Y;U))^+ \quad (6)$$

$$C_s = \left(\log\left(1 + \frac{H_k H_k^\dagger \sigma_u^2}{\sigma_v^2}\right) - \log\left(1 + \frac{G_k G_k^\dagger \sigma_u^2}{E[|G_k w_k|]^2 + \sigma_E^2}\right)\right)^+, \quad (7)$$

donde $(\cdot)^+ = \max(\cdot, 0)$ y σ_u^2 representa la fracción de potencia utilizada en la señal de información.

El estudio del efecto de la posición del *eavesdropper* en la capacidad de secreto del sistema es propuesto en [2]. Si el *eavesdropper* se ubica lo suficientemente cerca del transmisor, se pueden asumir condiciones de canales favorables al mismo, i.e., $\sigma_E^2 = 0$. En este caso particular, la Mínima Capacidad de Secreto Garantizada se deriva de la ecuación 7, de forma que:

$$C_{s,min} = \left(\log\left(1 + \frac{H_k H_k^\dagger \sigma_u^2}{\sigma_v^2}\right) - \log\left(1 + \frac{G_k G_k^\dagger \sigma_u^2}{(G_k G_k^\dagger \sigma_u^2 + \sigma_v^2)}\right)\right)^+, \quad (8)$$

Donde σ_v^2 representa la potencia entregada a la señal de ruido artificial. Las posibles posiciones adoptadas por el *eavesdropper* son usadas como estrategias para la formulación del juego en la siguiente sección.

Dado el conocimiento del canal, y la elección de σ_u^2 y σ_v^2, de forma que maximicen la mínima capacidad de secreto promedio garantizada, el problema de optimización de interés está dado por:

$$\overline{C_{s,avg}} = \max_{f(\sigma_u^2, \sigma_v^2) | \sum P_k} E_{H_k, G_k}[C_{s,avg}] \quad (9)$$

III. MODELO DEL JUEGO Y PROBLEMAS DE OPTIMIZACIÓN

Con el objetivo de analizar en profundidad el comportamiento de la capacidad de secreto del sistema cuando se utiliza CJ, se aplica Teoría de Juegos para modelar la situación. Puesto que cuanto se beneficia un jugador, es cuanto se perjudica el otro, la situación se modela como un juego No Cooperativo de Suma Cero, donde uno de los jugadores busca maximizar su ganancia, mientras que el otro busca minimizar su pérdida.

El transmisor se denomina Jugador A y el *eavesdropper* se denomina Jugador B. Las estrategias del Jugador A están dadas por utilizar un 70% de la potencia total de transmisión en la señal de información (α_1) o utilizar un 50% de la potencia en la señal de información (α_2). El resto de la potencia de transmisión se utiliza para la señal *jamming*, de forma que $\frac{\sigma_u^2}{P_0} + \frac{\sigma_v^2}{P_0} = 1$. Las estrategias del Jugador B están dadas por su localización de forma tal que $\sigma_E^2 = 0$ (β_1) ó $\sigma_E^2 = \sigma_u^2/2$ (β_2). La función de pago está dada por la capacidad de secreto definida en la ecuación 7. La forma matricial del juego se muestra en la tabla 1.

Tabla 1. Matriz de pago del Juego.

	Jugador B	
Jugador A	β_1 $\sigma_E^2 = 0$	β_2 $\sigma_E^2 = \sigma_u^2/2$
α_1 $\frac{\sigma_u^2}{P_0} = 0.7$ $\frac{\sigma_v^2}{P_0} = 0.3$	$\overline{C_{s_{11}}}$	$\overline{C_{s_{12}}}$
α_2 $\frac{\sigma_u^2}{P_0} = 0.5$ $\frac{\sigma_v^2}{P_0} = 0.5$	$\overline{C_{s_{21}}}$	$\overline{C_{s_{22}}}$

Los juegos de suma cero se pueden describir como problemas de programación lineal Primal-Dual para el Jugador A y B respectivamente. Transformando estos problemas de la misma forma que en [18], los problemas equivalentes explícitos están dados por:

Jugador A

Minimizar $\sum_{i=1}^{n} p_i$

Sujeto a $\sum_{i=1}^{n} C_{s_{ij}} p_i \geq 1$

(10)

$j = 1, \ldots, m, \quad p_i \geq 0$

Jugador B

Maximizar $\sum_{j=1}^{m} q_j$

Sujeto a $\sum_{j=1}^{m} C_{s_{ij}} q_j \leq 1$

(11)

$i = 1, \ldots, n, \quad q_j \geq 0$

El problema 11 es el dual del problema primal 10. Aquí, $p_i = \alpha_i / V_A$, donde V_A es el valor medio del juego para el Jugador A y α_i es su estrategia i-ésima con $1 \leq i \leq n$. Para el Jugador B, $q_j = \beta_j / V_B$ donde V_B es el valor medio del juego y β_j es su estrategia j-ésima con $1 \leq j \leq m$.

A consecuencia de que la función de pago incluye variables aleatorias, una mejor forma de lidiar con el problema de optimización, es tomar las restricciones lineales y transformarlas en restricciones probabilísticas, de forma que:

Jugador A

Minimizar $\sum_{i=1}^{n} p_i$

Sujeto a $1 - Prob\left(\sum_{i=1}^{n} C_{s_{ij}} p_i \geq 1\right) \geq \rho_A$ (12)

$j = 1, \ldots, m, \quad p_i \geq 0$

Jugador B

Maximizar $\sum_{j=1}^{m} q_j$

Sujeto a $Prob\left(\sum_{j=1}^{m} C_{s_{ij}} q_j \leq 1\right) \geq \rho_B$ (13)

$i = 1, \ldots, n, \quad q_j \geq 0$

Donde ρ_A y ρ_B son los valores de confiabilidad con que las condiciones de los problemas de optimización probabilísticos se cumplen. Como resultado de lo anterior, los problemas 12 y 13 resultan del tipo *Chance Constrained*. Al igual que en [16], los valores de confiabilidad se deben encontrar entre $0.5 < \rho_A < 1$ y $0.5 < \rho_B < 1$. Mediante el proceso expuesto en [17], los problemas 12 y 13 se transforman en problemas equivalentes determinísticos. Para el problema de estudio se tiene:

Jugador A

Minimizar $p_1 + p_2$

Sujeto a $\left\| \sqrt{covar\left(C_{s_{1i}}, C_{s_{1j}}\right)} \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \right\| \leq \frac{\overline{C_{s_{1i}}} p_1 + \overline{C_{s_{1j}}} p_2 - 1}{\phi^{-1}(\rho_A)}$

$\left\| \sqrt{covar\left(C_{s_{2i}}, C_{s_{2j}}\right)} \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \right\| \leq \frac{\overline{C_{s_{2i}}} p_1 + \overline{C_{s_{2j}}} p_2 - 1}{\phi^{-1}(\rho_A)}$

$p_1, p_2 \geq 0$ (14)

Jugador B

Maximizar $q_1 + q_2$

Sujeto a $\left\| \sqrt{covar\left(C_{s_{1i}}, C_{s_{1j}}\right)} \begin{bmatrix} q_1 \\ q_2 \end{bmatrix} \right\| \leq \frac{-\overline{C_{s_{1i}}} q_1 - \overline{C_{s_{1j}}} q_2 + 1}{\phi^{-1}(\rho_B)}$

$\left\| \sqrt{covar\left(C_{s_{2i}}, C_{s_{2j}}\right)} \begin{bmatrix} q_1 \\ q_2 \end{bmatrix} \right\| \leq \frac{-\overline{C_{s_{2i}}} q_1 - \overline{C_{s_{2j}}} q_2 + 1}{\phi^{-1}(\rho_B)}$

$q_1, q_2 \geq 0$ (15)

Los problemas 14 y 15 son problemas tipo SOCP, donde $covar(\cdot,\cdot)$ es la matriz de covarianza de los elementos en el paréntesis y ϕ^{-1} es la función inversa de probabilidad acumulada.

V_A y V_B se definen ahora como los valores de juego para los problemas 14 y 15 respectivamente. V_A establece la ganancia mínima del jugador A y V_B se define como la pérdida máxima para el jugador B, de forma que V_A y V_B actúan como cotas inferiores y superiores para el valor del juego, respectivamente.

IV. RESULTADOS NÚMERICOS Y DESEMPEÑO DE LAS ESTRATEGIAS

A. Resultados del juego

Para facilitar la lectura, se muestran los resultados y el análisis de los juegos modelados en [19], desde los cuales se obtiene el desempeño de las estrategias en términos de su probabilidad de *outage* en la sub-sección siguiente. Tanto los problemas lineales como los SOCP se resolvieron utilizando MATLAB, mediante el *toolbox* CVX [21], con un millón de muestras para las variables aleatorias de la ecuación 7.

Las tablas II y III muestran los resultados de resolver los problemas 10 y 14, y sus respectivos duales. La tabla II muestra los resultados del problema lineal: su matriz de pago promedio, el valor medio de juego y las estrategias puras resultantes. Se muestra que para el problema lineal $V_A = V_B = V_L$. Sumado a lo anterior, se puede observar que el juego resulta en estrategias puras. Lo anterior es producto de que este problema puede ser resuelto incluso por simple inspección visual. Este resultado muestra lo poco interesante que resulta estudiar el problema cuando solamente se calculan los valores promedio del juego. Sin embargo, los problemas tipo SOCP, toman en consideración la aleatoriedad de la ecuación 7, utilizando las matrices de covarianza asociadas, permitiendo estudiar de forma efectividad la variabilidad de la capacidad de secreto del sistema. Lo anterior permite un estudio más detallado del comportamiento, en términos de sus estrategias, que deberían adoptar el Jugador A y B para distintos niveles de confiabilidad.

Tabla 2. Matriz de pago promedio, valores de juego y estrategias resultantes para cada jugador.

	Jugador B	
Jugador A	β_1	β_2
α_1	1.1329	1.2551
α_2	1.3200	1.3976

$V_L = V_U = V_E = 1.3200$	
Jugador A	**Jugador B**
$\alpha_1 = 0$	$\beta_1 = 1$
$\alpha_2 = 1$	$\beta_2 = 0$

La tabla 3 muestra los resultados del problema SOCP: cotas inferiores y superiores para el valor de juego lineal calculado y las estrategias mixtas resultantes, para distintos niveles de confiabilidad.

Tabla 3. Valores de juego SOCP y estrategias asociadas, para distintos niveles de confiabilidad.

$V_L = 1.3200$	Jugador A			Jugador B		
$\rho_A = \rho_B$	V_A	α_1	α_2	V_B	β_1	β_2
0.55	1.2216	0	1	1.4146	0.8270	0.1730
0.60	1.1219	0.0513	0.9487	1.4923	0.6289	0.3711
0.65	1.0343	0.2508	0.7492	1.5661	0.5764	0.4236
0.70	0.9506	0.3237	0.6763	1.6426	0.5508	0.4492
0.75	0.8633	0.3640	0.6360	1.7248	0.5353	0.4647
0.80	0.7677	0.3907	0.6093	1.8161	0.5247	0.4753
0.85	0.6562	0.4104	0.5896	1.9223	0.5166	0.4834
0.90	0.5189	0.4263	0.5737	2.0559	0.5100	0.4900
0.95	0.3149	0.4411	0.5589	2.2536	0.5038	0.4962

De la tabla 3 se observa que cuando el problema es restringido a un nivel de confiabilidad, se sugiere la utilización de estrategias mixtas, con una excepción en el nivel de confiabilidad 0.55 en el jugador A. La desigualdad $V_A \leq V_L \leq V_B$ se mantiene para todos los valores de ρ. Para niveles de poca confiabilidad, los valores de V_A y V_B se acercan bastante al valor calculado de V_L pero manteniendo la desigualdad señalada. Para valores superiores al 80% de confiabilidad, se observa que el valor de V_A puede caer bastante, disminuyendo considerablemente la posible capacidad de secreto del sistema, incluso si se utiliza CJ. No obstante, el valor de V_B se incrementa a medida que de nivel de confiabilidad se eleva. De lo anterior se puede concluir que

para condiciones óptimas del canal, pueden alcanzarse altas tasas de secreto, dadas por el valor de V_2. Adicionalmente, de la tabla 3 se advierte que utilizando las estrategias mixtas sugeridas por el nivel de confiabilidad 0.95, se puede alcanzar tasas de secreto de hasta 2.2536 bps.

Los resultados muestran que para maximizar la certeza acerca del comportamiento de la capacidad de secreto, el Jugador A debe disminuir la frecuencia con la que la potencia total de transmisión es distribuida de forma equivalente (α_2) y aumentar la frecuencia con la cual el 70% de la potencia es para la señal de información (α_1). Se observa que a medida que se incrementa el nivel de confiabilidad, se sugiere la utilización en forma casi completamente aleatoria de ambas estrategias. Para el nivel de confiabilidad $\rho_A = \rho_B = 0.95$, por ejemplo, se sugiere la utilización de la estrategia α_2 en aproximadamente un 10% más de frecuencia que la estrategia α_1.

Para el caso del Jugador B, para bajos niveles de confiabilidad, se sugiere que este se localice más cerca del transmisor (β_1) con más frecuencia que más lejos (β_2). Sin embargo, al subir el nivel de confiabilidad, rápidamente se sugiere una aleatoriedad casi total entre las estrategias. Puesto que para ρ_B se sugiere utilizar la estrategia β_1 solo con un 10% más de frecuencia que la estrategia β_2. Este análisis permite concluir que sin importar que tan bien se localice el *eavesdropper*, la utilización de CJ reduce la capacidad de recepción del *eavesdropper*.

Finalmente, de la figura 2 se puede observar que el comportamiento descrito por el juego modelado en las tablas 2 y 3, se mantiene para diferentes simulaciones. En el eje horizontal se muestra el número de simulación realizada y en el eje vertical, el valor de juego asociado a la misma. Desde esta figura es posible concluir que los valores establecidos como cotas para la capacidad de secreto, mediante los problemas tipo SOCP 14 y 15, permiten establecer de manera confiable la región en la cual se moverá la función de capacidad de secreto para distintos niveles de confiabilidad.

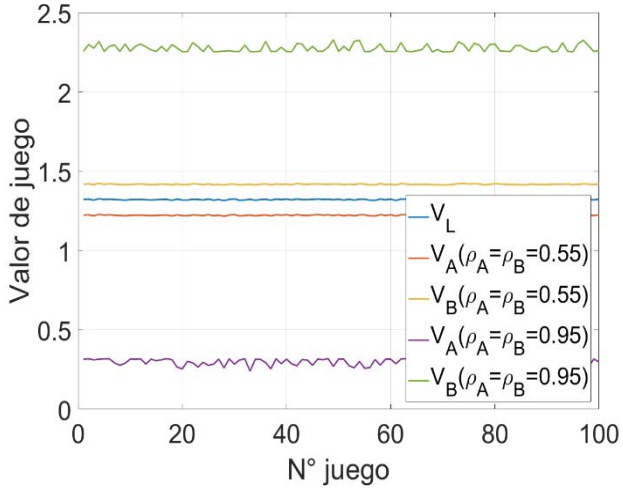


Figura 2. Cotas de la capacidad de secreto para diferentes juegos.

Como es de esperar, para un $\rho_A = \rho_B = 0.95$, no se logra captar toda la variabilidad asociada al medio inalámbrico, obteniéndose como resultado, valores de cota bastante cercanos al valor promedio de juego V_L utilizando estrategias puras. Sin embargo, al utilizar las estrategias mixtas sugeridas por el nivel de confiabilidad del 95%, las matrices de covarianza incluidas en los problemas 14 y 15 logran captar con mayor fidelidad la variabilidad del canal inalámbrico, ampliando la región en la que se comporta la capacidad de secreto para el 95% de los casos, cuando se utilizan las estrategias mixtas asociadas, pudiendo decaer la capacidad de secreto a valores menores que 0.5 bps, pero alcanzando, para condiciones óptimas del canal, valores cercanos a 2.5 bps.

B. Desempeño de las estrategias

La figura 3 muestra el desempeño de diferentes estrategias del Jugador A cuando el Jugador B utiliza la estrategia β_1 como estrategia pura, en términos de la probabilidad de *outage* del sistema. En ella se muestra la utilización de las estrategias α_1 y α_2 como estrategias puras y como estrategias mixtas para los niveles de confiabilidad del 75%, 85% y 95% con las distribuciones de probabilidad sugeridas por la tabla 3 para los ρ correspondientes.

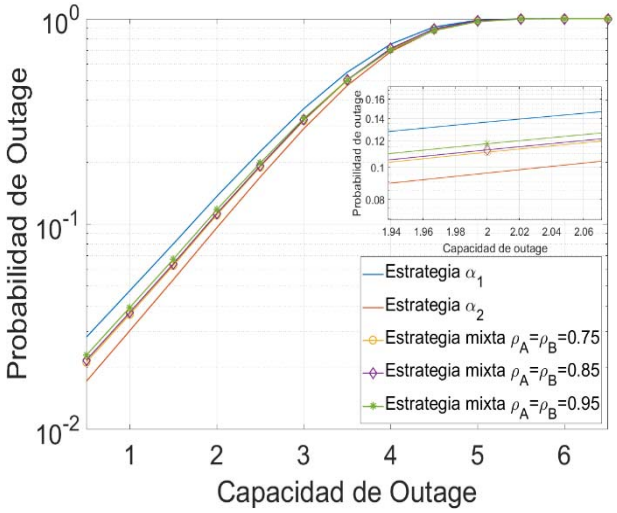


Figura 3. Probabilidad de *outage* para distintas estrategias del Jugador A, cuando el Jugador B utiliza la estrategia β_1 como estrategia pura.

Notar que, de las estrategias puras, la estrategia α_2 posee un mejor desempeño que α_1. Este resultado de simulación es congruente con el obtenido en la tabla 2, donde el resultado del juego lineal que entrega un mayor pago promedio, está dado por la utilización de α_2 como estrategia pura. En el caso de las estrategias mixtas, es interesante observar cómo estas caen justo en medio de los límites establecidos por las estrategias puras. Se puede ver cómo desde la estrategia con 75% de confiabilidad, hacía la estrategia de 95% de confiabilidad, la curva de desplaza gradualmente desde la estrategia pura α_2 hacía la estrategia pura α_1.

Por otro lado, notar que las estrategias asociadas a valores de $\rho_A = \rho_B = 0.95$ soy muy cercanas al rendimiento dado por la estrategia α_1. Esto es coherente con los resultados que se

muestran en la tabla 3, donde la distribución de probabilidades establecida para ese nivel de confiabilidad es cercana a la completa aleatoriedad ($\alpha_1 = 0.4411$ y $\alpha_2 = 0.5589$).

La figura 4 muestra el desempeño de diferentes estrategias del Jugador A cuando el Jugador B utiliza la estrategia β_2 como estrategia pura, en términos de la probabilidad de *outage* del sistema. En ella se muestra la utilización de las estrategias α_1 y α_2 como estrategias puras y también como estrategias mixtas para los niveles de confiabilidad del 75%, 85% y 95% con las distribuciones de probabilidad sugeridas por la tabla 3 para los ρ correspondientes.

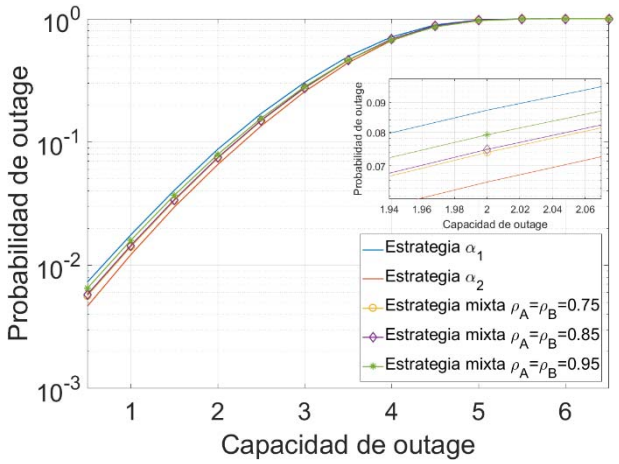


Figura 4. Probabilidad de *outage* para distintas estrategias del Jugador A, cuando el Jugador B utiliza la estrategia β_2 como estrategia pura.

Desde la figura 4, se puede observar que el comportamiento de las curvas de probabilidad de *outage* es básicamente el mismo que para cuando la estrategia pura utilizada por el Jugador B es β_1. No obstante, y como es de esperar, el sistema, en cada una de sus curvas, tiene un mejor desempeño. Lo anterior es coherente con que las condiciones de canal de la estrategia β_2 sean peores que las dadas por la estrategia β_1. Se observa en el *zoom* de la figura 4, que las diferencias de desempeño entre las distintas estrategias mixtas son bastante más pequeñas que en la figura 3. De esto se puede concluir, que para malas condiciones de canal del *eavesdropper*, el rendimiento de las diferentes estrategias mixtas es bastante parecido.

V. CONCLUSIONES

Una transmisión inalámbrica donde se emplea CJ para fortalecer la seguridad de capa física fue analizada. Se utilizó un modelo de Juego de Suma Cero, mediante el cual se derivó un problema de optimización probabilístico. Para abordar este último, se utilizó un equivalente determinístico tipo SOCP. Para un juego en particular, se calcularon las estrategias y valores de juego asociados. Se mostró que el comportamiento de los valores de juego calculados se mantiene para distintas simulaciones, y que estos se comportan como valores de cota para la función de pago utilizada, la capacidad de secreto. El desempeño de distintas estrategias mixtas fue analizado en términos de la capacidad de *outage* del sistema, mostrando que estas se ubican en un rango de comportamiento delimitado por las estrategias puras. Las estrategias mixtas tienen un peor rendimiento que la estrategia pura sugerida por el juego lineal, pero mejor que la estrategia pura desechada por el mismo.

El análisis expuesto ratifica lo mostrado en [19]: las estrategias resultantes del análisis con teoría de juegos, utilizando los problemas SOCP 14 y 15, y la capacidad de secreto como función de pago, no permiten mejorar el desempeño del sistema en términos de su probabilidad de *outage*. Sin embargo, su utilización nos permite un estudio acabado de las cotas alcanzables de la capacidad de secreto. Lo anterior adquiere relevancia a la hora de analizar sistemas de comunicaciones con condiciones particulares en las cuales haya alguna tasa de transmisión fija la cual no se pueda bajar. En este tipo de casos, el valor inferior de juego V_L puede ser utilizado para caracterizar la viabilidad de la comunicación. Por otra parte, el valor de juego superior V_B puede utilizarse para analizar las tasas de transmisión máximas alcanzables, asociadas a condiciones óptimas de canal.

AGRADECIMIENTOS

Los autores agradecen el apoyo financiero al Proyecto DICYT Asociativo, 061513VC DAS de la Universidad de Santiago de Chile.

REFERENCIAS

[1] C.E. Shannon, “Communication Theory of Secrecy Systems,” pp. 657-715, 1949.

[2] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180-2189, 2008.

[3] A.D. Wyner, “The Wire-Tap Channel,” *Bell System Technical Journal,* vol. 54, no. 8, pp. 1355-1387, 1975.

[4] M. Ghaderi, D. Goeckel, A. Orda and M. Dehghan, “Efficient wireless security through jamming, coding and routing,” *2013 IEEE International Conference on Sensing, Communications and Networking, SECON 2013,* pp. 505-513, 2013.

[5] A. Goldsmith, *Wireless Communications.* Cambridge University Press, 2005.

[6] I. Csiszár and J. Körner, “Broadcast Channels with Confidential Messages,” *IEEE Transactions on Information Theory,* vol. 24, no. 4, pp. 451-456, 1978.

[7] S.K. Leung-Yan-Cheong and M.E. Hellman, “The Gaussain Wire-Tap Channel,” *IEEE Transactions on Information Theory,* vol. 24, no. 4, pp. 451-456, 1978.

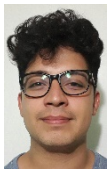
[8] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoric security,” *IEEE Transactions on Information Theory,* vol. 54, no. 6, pp. 2515-2534, 2008.

[9] R. Negi and S. Goel, “Secret communication using artificial noise,” *VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005.,* vol. 3, pp. 1906-1910, 2005.

[10] L. Lv, J. Chen, L. Yang, and Y. Kuo, “Improving physical layer security in untrusted relay networks: cooperative jamming and power allocation,” *IET Communications*, vol. 11, pp. 393-399, 2017.

[11] D. Wang, S. Member, and P. Ren, “Secure Cooperative Transmission Against Jamming-Aided Eavesdropper for ARQ Based Wireless Networks,” *IEEE* Access, vol. 5, pp. 3763-3776, 2017.

[12] E.N. Barron, *Game Theory,* Wiley Series in Operations Research and Management Science, 2002.
[13] O. Perez Barrios, G. De Ita Luna and L. M. Polanco Balcazar, "Designo f an efficient algorithm to find pure Nash equilibria on strategic games," *IEEE Latin America Transactions*, vol. 14, no 1, pp. 320-324, Jan. 2016.
[14] L. Chen and J. Leneutre, "Fight jamming with jamming – A game theoretic analysis of jamming attack in wireless networks and defense strategy," *Computer Networks,* vol. 55, no. 9, pp. 2259-2270, 2011.
[15] Xingkun Xu, Kunlun Gao, Xiaokun Zheng, and Ting Zhao, "A zero-sum game theoretic framework for jamming detection and avoidance in Wireless Sensor Networks," *2012 International Conference on Computer Science and Information Processing (CSIP),* pp. 265-270, 2012.
[16] Claudio Valencia Cordero and A. Lisser, "Jamming Attacks Reliable Prevention in a Clustered Wireless Sensor Network," *Wireless Personal Communications,* vol. 85, no. 3, pp. 925-936, 2015.
[17] W. Xiao, K. Huang, X. Luo, and Y. Hong, "Study on Physical Layer Security with Game Theory," *2013 4th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, pp. 697-700, 2013.
[18] K. Cumanan, H. Xing, P. Xu, G. A. N. Zheng, X. Dai, A. Nallanathan, Z. Ding, G. K. Karagiannidis, "Physical Layer Security Jamming: Theoretical Limits and Practical Designs in Wireless Networks," *IEEE Access,* vol. 5, pp. 3603-3611, 2017.
[19] Nicolás M. Ortega Silva and Claudio Valencia Cordero, "Towards physical layer security systems design using game theory approaches," in *Proc. CHILEAN Conf. Elect., Electron., Eng., Inf. Commun. Technol. (CHILECON),* Pucón, Chile, Oct. 2017, pp. 1-6.
[20] R. Liu and T. Wade, Eds., *Securing Wireless Communications at the Physical Layer*. Springer US, 2010.
[21] M. C. Grant and S. P. Boyd, "The CVX User Guide Release 2.1," 2017.



Nicolás Matías Ortega Silva es estudiante del programa de Magister en Ciencias de la Ingeniería, mención Eléctrica, de la Universidad de Chile, Chile. Obtuvo el título de Ingeniero Civil en Electricidad en la Universidad de Santiago el 2017. Sus investigaciones han estado enfocadas en seguridad de capa física y teoría de juegos aplicada a comunicaciones inalámbricas. Actualmente investiga en el área de capa física para redes vehiculares, modelamiento y estimación de canal.

Claudio Valencia Cordero es profesor jornada completa del Departamento de Ingeniería Eléctrica de la Universidad de Santiago de Chile, Chile. Obtuvo el Doctorado en Ciencias de Ingeniería y Magister en Telecomunicaciones en la Universidad de Santiago de Chile, el 2009 y 2005 respectivamente. El 2012 fue Postdoctoral Fellow en el Laboratoire de Recherche en Informatique en la Universidad Paris Sud, Orsay, Francia. Sus intereses de investigación se enfocan en seguridad de capa física, ataques de canal lateral, codificación y teoría de juegos para aplicaciones en sistemas de comunicación inalámbrico.