NÂNG CAO HIỆU QUẢ BẢO MẬT CỦA HỆ THỐNG MIMO BẰNG PHƯƠNG PHÁP BEAMFORMING

Nguyễn Anh Đức, Chu Tiến Dũng, Trần Lương Hùng, Trần Mạnh Hoàng*

Tóm tắt: *Bài báo này đề xuất phương thức beamforming trong hệ thống (MIMO: Multiple-Input Multiple-Output), nhằm mục đích cải thiện hiệu quả xác suất dừng bảo mật của lớp vật lý (PLS: Physical Layer Security). Hệ thống đề xuất là mạng chuyển tiếp hai chặng, tại mỗi nút hợp pháp được trang bị nhiều ăng-ten, trong khi đó, nút nghe lén được trang bị một ăng-ten. Tham số phân tích để đánh giá khả năng bảo mật là xác suất dừng bảo mật. Phương thức xử lí ăng-ten sử dụng kĩ thuật phát phân tập cực đại (MRT: maximal ratio transmission) và thu kết hợp cực đại (MRC: Maximal Ratio Combining). Hàm phân bố tích lũy (CDF: Cumulative Distribution Function) và hàm phân bố xác suất (PDF: Probability Density Function) của SNR đối với hệ thống MIMO được xây dựng và vận dụng lần đầu tiên trong bài báo này. Sử dụng mô phỏng Monte-Carlo để đánh giá hiệu quả của hệ thống đề xuất và kiểm chứng các kết quả phân tích trong bài báo.*

Từ khóa: MIMO; MRT; PLS; SOP; Beamforming.

1. ĐẶT VẤN ĐỀ

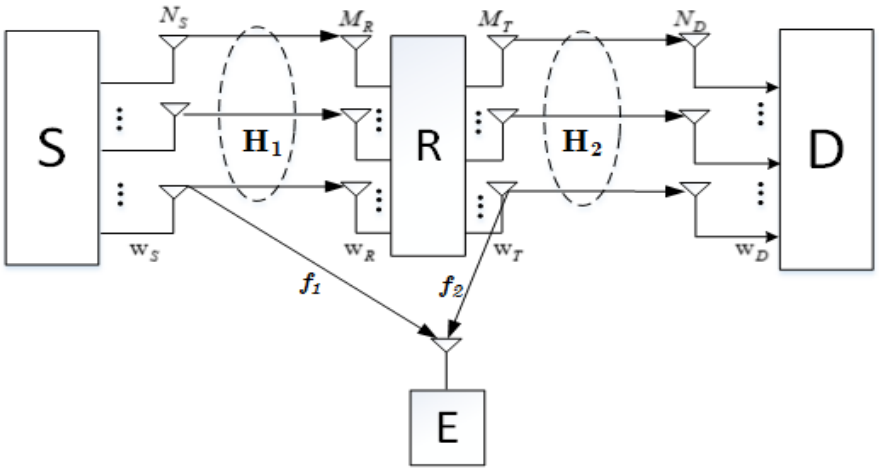
Hệ thống đa đầu vào đa đầu ra (MIMO: Multiple-Input Multiple-Output) được biết đến với khả năng cải thiện dung lượng trong các mạng viễn thông. Do đó, hiện nay có nhiều nghiên cứu đề xuất các phương pháp kết hợp phân tập trong MIMO để nâng cao hiệu quả bảo mật ở lớp vật lý (PLS: Physical Layer Security) [1, 2]. Tuy nhiên, các nghiên cứu này chỉ sử dụng phương thức lựa chọn ăng- ten phát (TAS: Transmit Antenna Selection) dẫn đến chỉ khai thác được độ lợi của mảng ăng-ten mà không đạt đến độ lợi phân tập. Hơn nữa, các nghiên cứu về PLS trên hệ thống MIMO chủ yếu tập trung cho các cấu hình điểm-điểm, khảo sát khả năng bảo mật của một nút phát đến một nút thu và có một nút nghe lén. Do đó, mô hình này sẽ đơn giản trong tính toán và mô phỏng hệ thống. Các khảo sát khả năng bảo mật cho hệ thống chuyển tiếp thường chỉ xem xét cấu hình đơn ăng-ten [3, 4], tuy nhiên, đây là những nghiên cứu nền tảng để mở rộng cho các hệ thống đa ăng-ten. Các đề xuất tiếp theo của hệ thống chuyển tiếp có nhiều ăng-ten và đánh giá khả năng bảo mật [5, 6] tập trung đề xuất các thuật toán cải thiện dung lượng bảo mật hệ thống. Nghiên cứu gần với mô hình đề xuất trong bài báo này là [7, 8], tuy nhiên, trong cả hai công trình này chỉ cấu hình nhiều ăng-ten tại nút chuyển tiếp, tại nút nguồn và nút đích chỉ sử dụng 1 ăng-ten.

Từ những công trình đã đề cập ở trên, bài báo của chúng tôi đề xuất cấu hình nhiều ăng-ten tại mỗi nút hợp pháp để tăng khả năng bảo mật của hệ thống. Ngoài ra, trong bài báo này đề xuất phương thức Beamforming để tăng độ lợi mảng khi sử dụng nhiều ăng-ten. Do đó, đóng góp của bài báo được tóm tắt như sau: Phân tích được hàm phân bố SNR của hệ thống MIMO tổng quát, đây là biểu thức có thể sử dụng để khảo sát các tham số khác của hệ thống MIMO, là cách tiếp cận mới để giải quyết những khó khăn về giải tích trong khảo sát phẩm chất hệ thống MIMO mà nhiều nhà nghiên cứu hiện nay chưa giải quyết được. Ngoài ra, kết quả của bài báo là xây dựng biểu thức tường minh của xác suất dừng bảo mật, đây là tham số cơ bản được sử dụng để đánh giá khả năng bảo mật của hệ thống vô tuyến. Sử dụng công cụ mô phỏng để kiểm chứng lại kết quả phân tích và đánh giá phẩm chất bảo mật của hệ thống MIMO chuyển tiếp. Cấu trúc bài báo thể hiện qua các phần như sau: Sau khi giới thiệu và đặt vấn đề ở Phần 1, mô hình hệ thống được đề xuất ở Phần 2; Phần 3 thực hiện phân tích biểu thức (SOP: Secrecy Outage Probability); Phần 4 trình bày kết quả mô phỏng để kiểm chứng hệ thống; Phần 5 là kết luận và đề xuất hướng nghiên cứu.

2. MÔ HÌNH HỆ THỐNG

Xem xét mô hình hệ thống MIMO đề xuất như trong hình 1, trong đó, nút nguồn (S: Source), nút chuyển tiếp (R: Relay) và nút đích (D: Destination) được trang bị nhiều ăng-ten. Như kí hiệu

trên hình N_S và N_D là số ăng-ten tại nút S và D tương ứng, trong khi đó, M_R và M_T tương ứng là số ăng-ten thu phát tại R. Hoạt động của hệ thống giả sử là bán song công. Trong quá trình thu/phát tín hiệu của hệ thống xuất hiện nút nghe lén (E: Eavesdropper) được trang bị một ăng-ten. Kênh truyền ở mỗi chặng giả sử có phân bố Rayleigh, tác động bởi pha đinh phẳng, tức là biên độ không thay đổi trong mỗi khung dữ liệu, nhưng sẽ thay đổi giữa các khung dữ liệu khác nhau [9]. Để giảm thiểu sự nghe lén của nút E, trong hệ thống này phương thức beamforming được thiết kế tại S và R. Beamforming là kỹ thuật biến đổi tín hiệu để phục vụ nhiều người dùng đồng thời trong các hệ thống đa ăng-ten. Ý tưởng chính của kỹ thuật beamforming là thiết kế trọng số các kênh truyền với điều kiện khử nhiễu đồng kênh dựa vào đặc tính trực giao của các kênh truyền với trọng số được thiết kế tại máy phát.



Hình 1. *Mô hình hệ thống.*

Các hệ số kênh truyền mỗi chặng kí hiệu là $\mathbf{H}_1 = [h_{i,j}]$ và $\mathbf{H}_2 = [h_{k,l}]$ là ma trận kênh truyền từ S đến R và từ R đến D tương ứng, trong đó, $i \in \{1,\cdots,N_S\}$, $j \in \{1,\cdots,M_R\}$, $k \in \{1,\cdots,M_T\}$ và $l \in \{1,\cdots,N_D\}$. Ngoài ra, vector kênh nghe lén từ S đến E và từ R đến E tương ứng là $\mathbf{f}_1 = [f_1,\cdots,f_{N_S}]^T$ và $\mathbf{f}_2 = [g_1,\cdots,g_{M_T}]^T$. Độ lợi kênh trung bình của mỗi đường kết nối từ ăng-ten phát đến ăng-ten thu trên chặng thứ nhất và chặng thứ hai được kí hiệu tương ứng là $\Omega_{i,j} = \mathbb{E}\{|h_{i,j}|^2\}$, $\Omega_{k,l} = \mathbb{E}\{|h_{k,l}|^2\}$, ngoài ra độ lợi kênh nghe lén từ S đến E và R đến E là $\Omega_i = \mathbb{E}\{|f_i|^2\}$. Công suất nhiễu trắng cộng tính tại các nút thu giả sử có phân bố chuẩn với trung bình không và phương sai σ_A^2, tức là $\mathbf{n}_A \sim CN(0,\sigma_A^2\mathbf{I})$. Hoạt động của hệ thống theo cơ chế bán song công (HD: Half duplex), nút chuyển tiếp thực hiện giao thức giải mã chuyển tiếp (DF: Decode and forward), do đó, mỗi chu kì tín hiệu từ S đến D thông qua 2 pha thời gian.

Trong pha thời gian thứ nhất, nút S phát kí hiệu $\mathbf{x} = [x_1, x_2, \cdots, x_{N_S}]^T$ sau khi đã được trọng số với vector phát MRT, $\mathbf{w}_S = \mathbf{u}_{\max}(\mathbf{H}_1^\dagger \mathbf{H}_1)$. Tín hiệu nhận được tại R được kết hợp từ mỗi nhánh ăng-ten theo phương pháp MRC, tức là trọng số với vector $\mathbf{w}_R = \mathbf{H}_1\mathbf{w}_S / \| \mathbf{H}_1\mathbf{w}_S \|$. Do đó, phương trình tín hiệu băng gốc tại R được biểu diễn là:

$$\mathbf{z}_R = \mathbf{w}_R^\dagger \mathbf{y}_R = \sqrt{P_S}\mathbf{H}_1\mathbf{w}_R^\dagger\mathbf{w}_S\mathbf{x} + \mathbf{w}_R^\dagger\mathbf{n}_R. \quad (1)$$

Do môi trường truyền lan vô tuyến, nút nghe lén E cũng thu được tín hiệu sau

$$\mathbf{y}_{SE} = \sqrt{P_S}\mathbf{f}_1\mathbf{w}_S\mathbf{x} + \mathbf{n}_E, \quad (2)$$

trong đó, P_S là công suất phát của S, $\mathbf{n}_R$ và $\mathbf{n}_E$ tương ứng là AWGN tại R và E.

Từ hai phương trình tín hiệu trên, chúng ta nhận được biểu thức tỉ số công suất tín hiệu trên công suất tạp âm tại R và E của pha truyền thứ nhất là

$$\gamma_{SR} = P_S \lambda_{\max}(\mathbf{H}_1^{\dagger}\mathbf{H}_1) / \sigma_R^2 = P_S \| \mathbf{H}_1 \|_F^2 / \sigma_R^2, \quad (3)$$

$$\gamma_{SE} = P_S \| \mathbf{f}_1 \|^2 / \sigma_E^2, \quad (4)$$

trong đó, $\lambda_{\max}(\mathbf{H}_\ell^{\dagger}\mathbf{H}_\ell)$, với $\ell = 1,2$ là giá trị riêng lớn nhất của vector riêng tương ứng.

Trong pha thời gian thứ 2 nút chuyển tiếp giải mã, mã hóa lại và trọng số với vector phát MRT tại R, $\mathbf{w}_T = \mathbf{u}_{\max}(\mathbf{H}_2^{\dagger}\mathbf{H}_2)$, tín hiệu sẽ được phát đến nút đích D, tại D thực hiện MRC của mỗi phần tử ăng-ten với vector trọng số $\mathbf{w}_D = \mathbf{H}_2\mathbf{w}_T / \| \mathbf{H}_2\mathbf{w}_T \|$, cùng lúc đó, nút nghe lén E nhận được tín hiệu do R phát, do đó, phương trình tín hiệu tại D và E được biểu diễn là

$$\mathbf{z}_D = \mathbf{w}_D^{\dagger}\mathbf{y}_D = \sqrt{P_R}\mathbf{H}_2\mathbf{w}_D^{\dagger}\mathbf{w}_T\mathbf{x} + \mathbf{w}_D^{\dagger}\mathbf{n}_D, \quad (5)$$

$$\mathbf{y}_{RE} = \sqrt{P_R}\mathbf{f}_2\mathbf{w}_T\mathbf{x} + \mathbf{n}_E, \quad (6)$$

trong đó, P_R là công suất phát của nút chuyển tiếp, $\mathbf{n}_D$ là AWGN tại D.

Từ (5) và (6) rút ra được SNR tức thời tại R và E là

$$\gamma_{RD} = P_R \lambda_{\max}(\mathbf{H}_2^{\dagger}\mathbf{H}_2) / \sigma_D^2 = P_R \| \mathbf{H}_2 \|_F^2 / \sigma_D^2, \quad (7)$$

$$\gamma_{RE} = P_R \| \mathbf{f}_2 \|^2 / \sigma_E^2. \quad (8)$$

Theo giao thức DF chúng ta có thể mô hình hóa SNR từ S đến D $\gamma_D = \min(\gamma_{SR}, \gamma_{RD})$. Ngoài ra, tại E có thể nhận biết được tín hiệu khi SNR dựa vào SNR mỗi chặng, tức là với SNR tại E được mô hình thành $\gamma_E = \max(\gamma_{SE}, \gamma_{RE})$.

Với phương thức phát MRT và thu MRC, hàm phân bố tích lũy (CDF: Cumulative Distribution Function) và hàm phân bố xác suất (PDF: Probability Density Function) của biên độ kênh truyền chuẩn hóa, $\lambda_{\max}(\mathbf{H}_\ell^{\dagger}\mathbf{H}_\ell) = \| \mathbf{H}_\ell \|^2$ theo đặc tính Rayleigh có dạng

$$F_{\lambda_{\max}}(z) = 1 - \sum_{k=1}^{s} \sum_{l=t-s}^{(t+s-2k)k} \sum_{m=0}^{l} \frac{\alpha'_{k,l} k^m z^m}{m! \Omega_\ell^m} \exp\left(-\frac{kz}{\Omega_\ell}\right), \quad (9)$$

$$f_{\lambda_{\max}}(z) = \sum_{k=1}^{s} \sum_{l=t-s}^{(t+s-2k)k} \frac{\alpha'_{k,l}}{l!} \left(\frac{k}{\Omega_\ell}\right)^{l+1} z^l \exp\left(-\frac{kz}{\Omega_\ell}\right). \quad (10)$$

trong đó, $s = \min(n_S, n_R)$, $t = \max(n_S, n_R)$ với n_S và n_R là số ăng-ten phát và thu ở mỗi chặng tương ứng, $\alpha'_{k,l} = \alpha_{k,l}(\prod_{i=1}^{s}(s-i)! \prod_{j=1}^{t}(t-j)!)^{-1} l! / k^{l+1}$.

Hai phương trình (9) và (10) được sử dụng để phân tích biểu thức tường minh tham số xác suất dừng bảo mật SOP của hệ thống theo phương thức phân tập MRT/MRC ở phần sau. Thêm vào đó, hàm CDF và PDF của SNR tại E khi S và R phát theo phương thức MRT được tính toán như sau:

$$F_{\gamma_\ell^E}(\gamma) = 1 - \exp\left(-\frac{\gamma}{\Omega_\ell}\right) \sum_{m=0}^{M-1} \frac{1}{m!} \left(\frac{\gamma}{\Omega_\ell}\right)^m, \quad (11)$$

$$f_{\gamma_\ell^E}(\gamma) = \frac{\gamma^{M-1}}{\Gamma(M)\Omega_\ell^M} \exp\left(-\frac{\gamma}{\Omega_\ell}\right), \quad (12)$$

trong đó, chỉ số *M* là số ăng- ten phát tại S và R.

3. PHÂN TÍCH HIỆU NĂNG HỆ THỐNG

Xác suất dừng bảo mật được định nghĩa là xác suất của tỉ số dung lượng tức thời của kênh chính (kênh hợp pháp) và kênh nghe lén C_{SD} nhỏ hơn tốc độ ngưỡng bảo mật cho trước R_0, mô hình toán học SOP được mô tả bởi

$$\mathrm{SOP}_{\mathrm{e2e}} = \Pr(\mathrm{C}_{\mathrm{SD}} < R_0), \tag{13}$$

trong đó, $\mathrm{C}_{\mathrm{SD}} = \left[\frac{1}{2}\log_2(1+\gamma_{\mathrm{D}}) - \frac{1}{2}\log_2(1+\gamma_{\mathrm{E}})\right]^+$.

Do đó, chúng ta có thể viết SOP thành

$$\mathrm{SOP}_{\mathrm{e2e}} = \Pr\left(\frac{1+\gamma_{\mathrm{D}}}{1+\gamma_{\mathrm{E}}} < 2^{2R_0}\right) = \int_0^\infty \Pr(\gamma_{\mathrm{D}} < \theta(1+y)-1)\, f_{\gamma_{\mathrm{E}}}(y)dy = \int_0^\infty F_{\gamma_{\mathrm{D}}}(z)\, f_{\gamma_{\mathrm{E}}}(y)dy, \tag{14}$$

với $z = \theta(1+y)-1$.

Để nhận được biểu thức tường minh trong phương trình (14) chúng ta cần có $F_{\gamma_{\mathrm{D}}}(z)$ và $f_{\gamma_{\mathrm{E}}}(y)$ của toàn chặng. Khi $\gamma_{\mathrm{D}} = \min(\gamma_{\mathrm{SR}}, \gamma_{\mathrm{RD}})$, chúng ta có thể viết thành

$$\begin{aligned} F_{\gamma_{\mathrm{D}}^{\mathrm{MRT}}}(\gamma) &= \Pr(\gamma_{\mathrm{D}}^{\mathrm{MRT}} \le \gamma) \\ &= \Pr\left(\min(\gamma_{\mathrm{SR}}, \gamma_{\mathrm{RD}}) < \gamma\right) = 1 - \Pr\left(\gamma_{\mathrm{SR}} > \gamma,\, \gamma_{\mathrm{RD}} > \gamma\right). \end{aligned} \tag{15}$$

Từ phương trình (9), sau một số biến đổi đơn giản chúng ta nhận được hàm CDF của SNR từ S đến D là

$$F_{\gamma_{\mathrm{D}}^{\mathrm{MRT}}}(\gamma) = 1 - \sum_{k=1}^{s}\sum_{l=t-s}^{(t+s-2k)k}\sum_{m=0}^{l}\frac{\alpha_{k,l}\,k^m}{m!(P_{\mathrm{S}}\Omega_{\mathrm{SR}})^m}\sum_{u=1}^{s_1}\sum_{q=t_1-s_1}^{(t_1+s_1-2u)u}\sum_{n=0}^{q}\frac{\alpha_{u,q}\,u^n\gamma^{m+n}}{n!(P_{\mathrm{R}}\Omega_{\mathrm{RD}})^n}\exp(-\psi\gamma), \tag{16}$$

trong đó, $\psi = u/P_{\mathrm{R}}\Omega_{\mathrm{RD}} + k/P_{\mathrm{S}}\Omega_{\mathrm{SR}}$, $s = \min(N_{\mathrm{S}}, M_R)$, $t = \max(N_{\mathrm{S}}, M_R)$, $s_1 = \min(M_T, N_{\mathrm{D}})$ và $t_1 = \max(M_T, N_{\mathrm{D}})$.

Ngoài ra, khi $\gamma_{\mathrm{E}} = \max(\gamma_{\mathrm{SE}}, \gamma_{\mathrm{RE}})$, sau một số tính toán đơn giản chúng ta nhận được PDF của SNR tại E là

$$\begin{aligned} f_{\gamma_{\mathrm{E}}^{\mathrm{MRT}}}(\gamma) &= \frac{1}{\Gamma(N_{\mathrm{S}})\Gamma(M_T)(P_{\mathrm{S}}\Omega_{\mathrm{SE}})^{N_{\mathrm{S}}}}\gamma^{N_{\mathrm{S}}-1}\exp\left(-\frac{\gamma}{P_{\mathrm{S}}\Omega_{\mathrm{SE}}}\right)\gamma\left(M_T, \frac{\gamma}{P_{\mathrm{R}}\Omega_{\mathrm{RE}}}\right) \\ &+ \frac{1}{\Gamma(M_T)\Gamma(N_{\mathrm{S}})(P_{\mathrm{R}}\Omega_{\mathrm{RE}})^{M_T}}\gamma^{M_T-1}\exp\left(-\frac{\gamma}{P_{\mathrm{R}}\Omega_{\mathrm{RE}}}\right)\gamma\left(N_{\mathrm{S}}, \frac{\gamma}{P_{\mathrm{S}}\Omega_{\mathrm{SE}}}\right). \end{aligned} \tag{17}$$

Thực hiện thay thế (16) và (17) vào biểu thức SOP ban đầu (14), và thay thế $\gamma = \theta(1+y)-1$ vào hàm CDF, $F_{\gamma_{\mathrm{D}}^{\mathrm{MRT}}}(\gamma)$, sau đó áp dụng khai triển nhị thức của thành phần số mũ sau đây thành tổng, tức là $(\theta(1+y)-1)^{n+m} = \sum_{v}^{m+n}\binom{m+n}{v}(\theta-1)^{m+n-v}\theta^v$. Sau các biến đổi tích phân

$$J_1(y) = \frac{1}{\Gamma(N_{\mathrm{S}})\Gamma(M_T)(P_{\mathrm{S}}\Omega_{\mathrm{SE}})^{N_{\mathrm{S}}}}\int_0^\infty y^{N_{\mathrm{S}}+v-1}\exp\left(-\frac{y}{P_{\mathrm{S}}\Omega_{\mathrm{SE}}} - \psi\theta y\right)\gamma\left(M_T, \frac{y}{P_{\mathrm{R}}\Omega_{\mathrm{RE}}}\right)dy. \tag{18}$$

$$J_2(y) = \frac{1}{\Gamma(M_T)\Gamma(N_{\mathrm{S}})(P_{\mathrm{R}}\Omega_{\mathrm{RE}})^{M_T}}\int_0^\infty y^{M_T+v-1}\exp\left(-\frac{y}{P_{\mathrm{R}}\Omega_{\mathrm{RE}}} - \psi\theta y\right)\gamma\left(N_{\mathrm{S}}, \frac{y}{P_{\mathrm{S}}\Omega_{\mathrm{SE}}}\right)dy. \tag{19}$$

Cuối cùng chúng ta nhận được biểu thức tường minh SOP là

$$\mathrm{SOP}_{\mathrm{e2e}}^{\mathrm{MRT}} = 1 - A_1 A_2 A_3 (J_1 + J_2), \tag{20}$$

trong đó:

$$A_1 = \sum_{k=1}^{s} \sum_{l=t-s}^{(t+s-2k)k} \sum_{m=0}^{l} \frac{\alpha_{k,l}^{'} k^m}{m!(P_{\mathrm{S}}\Omega_{\mathrm{SR}})^m}, \; A_2 = \sum_{u=1}^{s_1} \sum_{q=t_1-s_1}^{(t_1+s_1-2u)u} \sum_{n=0}^{q} \frac{\alpha_{u,q}^{'} u^n}{n!(P_{\mathrm{R}}\Omega_{\mathrm{RD}})^n},$$
$$A_3 = \sum_{v}^{m+n} \binom{m+n}{v} (\theta - 1)^{m+n-v} \theta^v \exp[-\psi(\theta - 1)] \tag{21}$$

$$J_1 = \frac{1}{\Gamma(N_{\mathrm{S}})\Gamma(M_T)(P_{\mathrm{S}}\Omega_{\mathrm{SE}})^{N_{\mathrm{S}}}} \frac{\alpha_1^{M_T}\Gamma(\mu_1 + M_T)}{\mu_1(\alpha_1 + \beta_1)^{\mu_1 + M_T}} {}_2F_1\left[1, \mu_1 + M_T; \mu_1 + 1; \frac{\beta_1}{\alpha_1 + \beta_1}\right]$$
$$J_2 = \frac{1}{\Gamma(M_T)\Gamma(N_{\mathrm{S}})(P_{\mathrm{R}}\Omega_{\mathrm{RE}})^{M_T}} \frac{\alpha_2^{N_S}\Gamma(\mu_2 + N_S)}{\mu_2(\alpha_2 + \beta_2)^{\mu_2 + N_S}} {}_2F_1\left[1, \mu_2 + N_S; \mu_2 + 1; \frac{\beta_2}{\alpha_2 + \beta_2}\right]. \tag{22}$$

$$\alpha_1 = \frac{1}{P_{\mathrm{R}}\Omega_{\mathrm{RE}}}, \alpha_2 = \frac{1}{P_{\mathrm{S}}\Omega_{\mathrm{SE}}}, \beta_1 = \frac{1}{P_{\mathrm{S}}\Omega_{\mathrm{SE}}} + \psi\theta, \beta_2 = \frac{1}{P_{\mathrm{R}}\Omega_{\mathrm{RE}}} + \psi\theta, \mu_1 = N_{\mathrm{S}} + v, \mu_2 = M_T + v$$

Hàm ${}_2F_1$[a, b, c, d] được gọi là hàm Hypergeometric Gauss. Tích phân trong (18) và (19) được tính toán dựa vào công thức có sẵn [10, Eq. (6. 455)]. Như vậy, (20) là biểu thức tường minh SOP của hệ thống được sử dụng để đánh giá SOP trên toàn chặng bằng phương pháp beamforming MRT tại S và R.

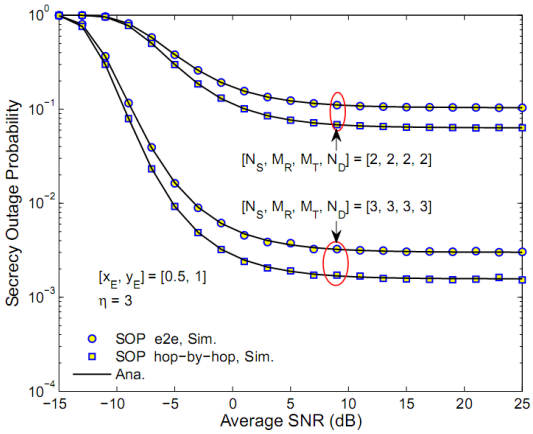
Ngoài ra, khi đánh giá SOP của mỗi chặng, tức là từ S đến R hoặc từ R đến D chúng ta chỉ việc thay thế (9) và (12) vào (14) sẽ nhận được công thức SOP của từng chặng. Do phạm vi của bài báo và sự đơn giản của phép toán nên không trình bày thêm ở bài báo này.

4. MÔ PHỎNG VÀ THẢO LUẬN

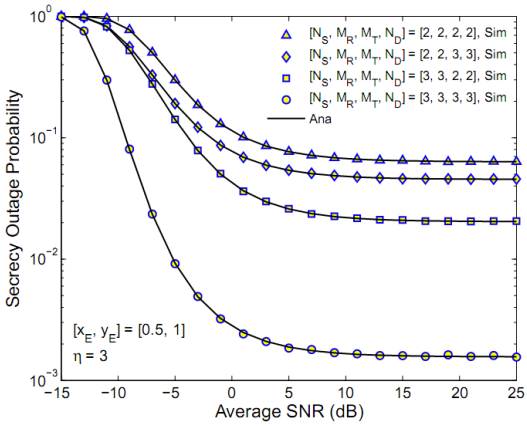
Trong phần này, bài báo trình bày kết quả mô phỏng nhằm kiểm chứng SOP của hệ thống. Ngoài ra, kết quả mô phỏng được trình bày để kiểm tra lại các phân tích ở phần 3. Số liệu mô phỏng được cài đặt như sau: số mẫu ngẫu nhiên thực hiện 2^{14} lần, hệ số suy hao môi trường truyền làn $\eta = 3$, hệ số này tương ứng với môi trường trong nhà (indoor), tần số hoạt động tại 1.9 GHz. Do mô hình hóa các kênh truyền dạng small-scale Reyleigh pha đinh, có thể coi các nút hợp pháp là tĩnh và chuẩn hóa khoảng cách là 1, tọa độ 2 chiều của các nút được cấu hình tại các vị trí tương ứng S(0, 0), R(0.5, 0) D(0, 1), và E(x_E, y_E) với $0 \le x_E \le 1, 0 \le y_E \le 1$. Độ lợi các kênh truyền $\Omega_{\mathrm{SR}} = d_{\mathrm{SR}}^{-\eta}$ và $\Omega_{\mathrm{RD}} = d_{\mathrm{RD}}^{-\eta}$, tương tự từ độ lợi từ nút S đến E và R đến R là $\Omega_{\mathrm{SE}} = d_{\mathrm{SE}}^{-\eta}$ $\Omega_{\mathrm{RE}} = d_{\mathrm{RE}}^{-\eta}$, trong đó, $d_{\mathrm{SE}} = \sqrt{(x_{\mathrm{E}} - x_{\mathrm{S}})^2 + (y_{\mathrm{E}} - y_{\mathrm{S}})^2}$ và $d_{\mathrm{RE}} = \sqrt{(x_{\mathrm{E}} - x_{\mathrm{R}})^2 + (y_{\mathrm{E}} - y_{\mathrm{R}})^2}$. AWGN được chuẩn hóa $\sigma_{\mathrm{R}}^2 = \sigma_{\mathrm{D}}^2 = \sigma_{\mathrm{E}}^2 = \sigma^2 = 1$.

Hình 2 trình bày SOP của hệ thống với số lượng ăng-ten được cấu hình tại S, R, D khác nhau. Vị trí nút nghe lén giả sử được đặt tại E(0.5, 1). Từ kết quả trên hình chúng ta thấy rằng, tăng số lượng ăng-ten của các nút hợp pháp có thể cải thiện được SOP. Nguyên nhân là do độ lợi kênh hợp pháp tăng theo độ lợi mảng dẫn đến tỉ số dung lượng kênh hợp pháp và kênh nghe lén lớn hơn. Ngoài ra, SOP của mỗi chặng nhỏ hơn SOP của toàn chặng, tức là khả năng nghe lén của nút E của từng chặng độc lập để giải mã khó khăn hơn khi kết hợp tín hiệu của cả hai chặng rồi thực hiện giải mã tín hiệu trường hợp này tương đương như việc mô hình hóa SNR tại E, $\gamma_{\mathrm{E}} = \max(\gamma_{\mathrm{SE}}, \gamma_{\mathrm{RE}})$ tương ứng với kết hợp cả 2 chặng để lấy năng lượng giải mã và $\gamma_{\mathrm{E}} = \min(\gamma_{\mathrm{SE}}, \gamma_{\mathrm{RE}})$ lấy năng lượng của một chặng bất kì để giải mã. Thêm vào đó, từ kết quả

nhận xét rằng, đồ thị mô phỏng trùng với đường đồ thị lí thuyết, thể hiện rằng, các phân tích toán học trong bài báo hoàn toàn chính xác.

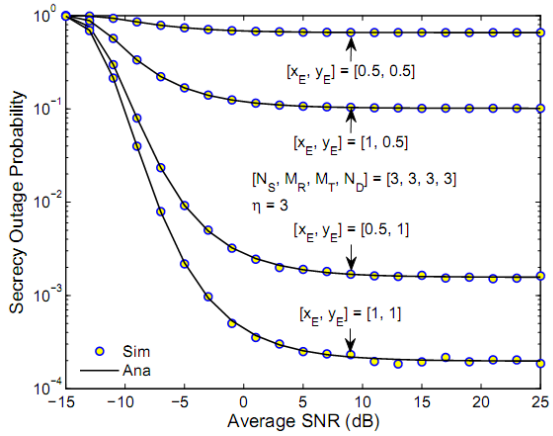


Hình 2. *SOP theo số ăng-ten được cấu hình của 2 kịch bản là SOP từ S-D và của mỗi chặng.*

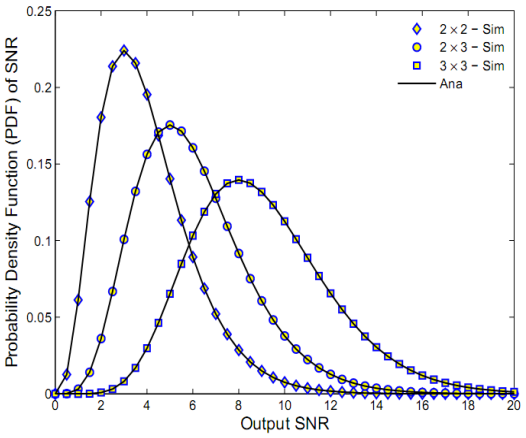


Hình 3. *SOP của hệ thống với số ăng-ten được cấu hình theo nhiều kịch bản.*

Hình 3 trình bày kết quả SOP của hệ thống theo các cấu hình ăng-ten khác nhau. Từ kết quả trên hình thấy rằng, khi số ăng- ten của kênh chính lớn dẫn đến SOP nhỏ, có nghĩa là khả năng bảo mật của hệ thống tốt lên. Điểm đặc biệt trong kết quả này là, khi cùng một chi phí tổng số lượng ăng- ten như nhau nhưng cấu hình tại mỗi nút khác nhau sẽ cho kết quả SOP khác nhau. Tức là với cấu hình $[N_S, M_R, M_T, N_D]=[2,2,3,3]$ có SOP xấu hơn cấu hình $[N_S, M_R, M_T, N_D]=[3,3,2,2]$. Điều này được lí giải bởi khi các nút S, R và D cố định và nút E đặt tại E(0.5, 1) cho độ lợi kênh từ S đến E khác độ lợi kênh từ R đến E, kết hợp với độ lợi mảng ăng- ten hai chặng khác nhau dẫn đến SOP khác nhau.



Hình 4. *SOP của hệ thống theo vị trí khác nhau của nút nghe lén.*



Hình 5. *Đặc điểm phân bố SNR của hệ thống MIMO với số ăng-ten khác nhau.*

Hình 4 biểu diễn kết quả SOP của hệ thống khi cùng cấu hình ăng-ten tại mỗi nút, và vị trí khác nhau của nút nghe lén. Từ kết quả trên hình thấy rằng, khi nút nghe lén đặt xa các nút hợp pháp dẫn đến SOP nhỏ, ngược lại khi E đặt gần với S, R và D dẫn đến khả năng bảo mật của hệ thống kém đi. Cụ thể khi E đặt gần nút R hệ thống gần như mất khả năng bảo mật. Một kết quả khác được quan tâm là khi vị trí E(0.5, 1) kết quả SOP khác hoàn toàn so với vị trí E(1, 0.5). Điều này do kết quả độ lợi kênh của mỗi nút biến đổi theo tọa độ của E, cụ thể như bảng sau:

x_E, y_E	Ω_{SE}	Ω_{RE}
0.5, 1	0.7155	1
1, 0.5	0.7155	2.8284

Có nghĩa là khi E(1, 0.5) mức năng lượng nhận được tại E sẽ lớn hơn và SOP tăng lên đáng kể so với E tại (0.5, 1).

Hình 5 kiểm chứng lại biểu thức (10) bằng kết quả mô phỏng và lí thuyết để đánh giá tính chính xác của biểu thức, vì đây là một công cụ được sử dụng như là hướng nghiên cứu mới để giải quyết những bài toán khó khăn trong việc phân tích phẩm chất hệ thống MIMO từ trước đến nay. Từ kết quả ở hình 5 thấy rằng, khi tăng số ăng- ten tại mỗi nút thu phát xác suất để nhận được SNR lớn hơn, tức là phẩm chất của hệ thống đạt tốt hơn. Đặc điểm này tương đương như việc mở rộng mẫu phương sai, nhằm mục đích đảm bảo cho các giá trị nhận trong đó luôn sát với giá trị kì vọng.

5. KẾT LUẬN

Bài báo này đã trình bày được công thức toán học tường minh cho tham số SOP của hệ thống MIMO chuyển tiếp 2 chặng bằng phương pháp beamforming MRT. Đặc biệt bài báo đã xác định được các hàm phân bố của độ lợi mảng với số ăng- ten tùy ý, đây là bước tiến mới có thể sử dụng để khảo sát các hệ thống MIMO khác ở những hướng nghiên cứu khác nhau. Mô hình phân tập ăng- ten sử dụng là kĩ thuật beamforming MRT, tuy nhiên, bài báo có thể mở rộng cho các phương thức phân tập phát khác. Các kết quả trình bày trong bài báo được kiểm chứng qua mô phỏng Monte-Carlo, trong điều kiện thông tin trạng thái kênh lí tưởng. Mô hình toán học trình bày trong bài báo có thể áp dụng phân tích cho hệ thống đa truy nhập không trực giao (NOMA: Non-Orthogonal Multiple-Access), hệ thống sử dụng thiết bị không người lái (UAV: Unmanned Aerial Vehicle) trong những công trình tiếp theo của các tác giả.

TÀI LIỆU THAM KHẢO

[1]. J. Zhang, C. Yuen, C.-K. Wen, S. Jin, K.-K. Wong, and H. Zhu, *"Large system secrecy Rate analysis for SWIPT MIMO wiretap channels,"* Information Forensics and Security, IEEE Transactions on, vol. 11, pp. 74-85, 2016.

[2]. J. Si, Z. Li, J. Cheng, and C. Zhong, *"Asymptotic Secrecy Outage Performance for TAS/MRC Over Correlated Nakagami-m Fading Channels,"* IEEE Transactions on Communications, vol. 67, pp. 7700-7714, 2019.

[3]. H. Zhao, Z. Liu, L. Yang, and M.-S. Alouini, *"Secrecy Analysis in DF Relay over Generalized-K Fading Channels,"* IEEE Transactions on Communications, 2019.

[4]. T. G. Nguyen, C. So-In, Z. A. Baig, and S. Sanguanpong, *"Secrecy Outage Performance Analysis for Energy Harvesting Sensor Networks With a Jammer Using Relay Selection Strategy,"* IEEE Access, 2018.

[5]. H. Lei, J. Zhang, K.-H. Park, P. Xu, Z. Zhang, G. Pan, et al., *"Secrecy Outage of Max-Min TAS Scheme in MIMO-NOMA Systems,"* IEEE Transactions on Vehicular Technology, 2018.

[6]. C. D. T. Thai, J. Lee, and T. Q. Quek, *"Physical-layer secret key generation with colluding untrusted relays,"* IEEE Transactions on Wireless Communications, vol. 15, pp. 1517-1530, 2016.

[7]. A. Salem, K. A. Hamdi, and K. M. Rabie, *"Physical layer security with RF energy harvesting in AF multi-antenna relaying networks,"* IEEE Transactions on Communications, vol. 64, pp. 3025-3038, 2016.

[8]. Y. Huang, J. Wang, C. Zhong, T. Q. Duong, and G. K. Karagiannidis, *"Secure transmission in cooperative relaying networks with multiple antennas,"* IEEE Transactions on Wireless Communications, vol. 15, pp. 6843-6856, 2016.

[9]. H. M. Tran, N. X. Tran, B. C. Nguyen, and D. T. Le, *"On the Performance of MIMO Full-Duplex Relaying System with SWIPT under Outdated CSI,"* IEEE Transactions on Vehicular Technology, 2020.

[10]. D. Zwillinger, Table of integrals, series, and products: Elsevier, 2014.

ABSTRACT

SECRECY OUTAGE PROBABILITY ANALYSIS
OF HOP-BY-HOP BEAMFORMING MIMO RELAYING SYSTEM

In this paper, we propose and analyze the secure performance of a dual hop beamforming MIMO system under the presence of an eavesdropper. To exploit the multi-antenna for improving the secrecy performance, we propose a linear processing maximal ratio transmission schemes at the transmitter and diversity combining technique using maximal ratio combining (MRC) at the receiver. We present the fundamental of the output SNR at legitimate users that is propagation over channel matrices and output SNR at eavesdropper. The probability density function (PDF) of the output SNR for arbitrary number of antenna elements configured at the transmitter and receiver are plotted and discussed. After that apply them to derive the closed-form expressions of secrecy performance of the proposed MIMO system for each linear processing scheme. The closed-form of secrecy outage probability expression (SOP) are derived in condition the channel having Rayleigh distribution. All analysis results are validated by Monte Carlo simulations.

Keywords: MIMO; MRT; PLS; SOP; Beamforming.

Nhận bài ngày 15 tháng 4 năm 2021
Hoàn thiện ngày 28 tháng 8 năm 2021
Chấp nhận đăng ngày 05 tháng 9 năm 2021

Địa chỉ: Đại học Thông tin liên lạc, Nha Trang, Khánh Hòa.
*Email: tranmanhhoang@tcu.edu.vn.