Dung lượng bảo mật của hệ thống MIMO cỡ rất lớn khi có thiết bị nghe lén thụ động

Invited article

Vũ Lê Quỳnh Giang[1,2], Trương Trung Kiên[2]

[1]Khoa Công nghệ Thông tin, Học viện Quản lý Giáo dục

[2]Phòng thí nghiệm Hệ thống Vô tuyến và Ứng dụng, Học viện Công nghệ Bưu chính Viễn thông

Tác giả liên hệ: Trương Trung Kiên, kientt@ptit.edu.vn

Ngày nhận bài: 21/12/2018, ngày sửa chữa: 26/12/2018, ngày duyệt đăng: 27/12/2018

Xem sớm trực tuyến: 28/12/2018, định danh DOI: 10.32913/rd-ict.vol3.no40.845

Biên tập lĩnh vực điều phối phản biện và quyết định nhận đăng: PGS. TS. Nguyễn Linh Trung

Tóm tắt: Bảo mật ở lớp vật lý có thể kết hợp với các giải pháp bảo mật ở lớp trên để đảm bảo an ninh thông tin trong mạng thông tin vô tuyến. Các kết quả nghiên cứu trước đây đã chỉ ra rằng với điều kiện kênh truyền Rayleigh, việc sử dụng rất nhiều ăng-ten ở trạm gốc giúp hệ thống thông tin MIMO (Multiple-Input Multiple-Output) cỡ rất lớn tự được bảo mật trước thiết bị nghe lén thụ động. Tuy nhiên, bài báo này sau khi đề xuất các biểu thức dạng đóng cho dung lượng bảo mật cho hệ thống MIMO cỡ rất lớn trong điều kiện kênh truyền Rice có xem xét thành phần truyền tầm nhìn thẳng đã chứng minh được rằng thiết bị nghe lén thụ động có thể ảnh hưởng lớn đến dung lượng bảo mật của hệ thống. Các kết quả mô phỏng được cung cấp để kiểm chứng tính chính xác của các kết quả phân tích giải tích và để rút ra một số chỉ dẫn thiết kế quan trọng.

Từ khóa: *Dung lượng bảo mật, MIMO cỡ rất lớn, nghe lén thụ động, bảo mật lớp vật lý.*

Title: **Secret Capacity of Massive MIMO Systems with a Passive Eavesdropper**

Abstract: Physical layer security may be combined with other approaches to make wireless transmissions more secured. Much prior work showed that, thanks to the excessive number of antennas at the base station, massive MIMO (Multiple-Input Multiple-Output) systems themselves are inherently robust against passive eavesdropping attacks under the Rayleigh fading channel. After providing closed-form expressions to secret capacity of massive MIMO under the Rician fading channel with line-of-sight transmission, this manuscript, however, showed that passive eavesdroppers may affect negatively the secret capacity. Simulation and numerical results are provided to validate the analytical results and to gain interesting insights into the system design.

Keywords: *Secret capacity, massive MIMO, eavesdropper, physical layer security.*

I. GIỚI THIỆU

Đảm bảo an toàn thông tin là một vấn đề quan trọng và thiết yếu trong các hệ thống thông tin, đặc biệt các hệ thống hoạt động ở môi trường vô tuyến [1]. Do đặc tính mở của môi trường truyền dẫn sóng vô tuyến, các thiết bị xâm nhập không hợp lệ có thể làm ảnh ảnh hưởng đến tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin bằng một trong hai phương pháp sau: (i) nghe lén thụ động (passive eavesdropping) và (ii) tấn công chủ động (active attacking/jamming) [2]. Cụ thể, thiết bị nghe lén thụ động chỉ cố gắng tách tín hiệu từ sóng vô tuyến mang thông tin nhận được từ thiết bị phát. Về nguyên lý, thiết bị nghe lén thụ động không thể bị phát hiện. Ngược lại, thiết bị tấn công chủ động không chỉ cố gắng tách tín hiệu được truyền từ thiết bị phát mà còn tự phát đi tín hiệu để gây nhiễu và làm ảnh hưởng đến quá trình huấn luyện và ước lượng kênh và/hoặc quá trình truyền dữ liệu giữa các thiết bị hợp lệ. Sự tác động này làm giảm hiệu năng hoạt động của hệ thống hợp lệ, thậm chí khiến hệ thống không thể hoạt động được.

Bảo mật lớp vật lý (Physical Layer Security) là một cách tiếp cận đang được quan tâm rộng rãi cho các mạng vô tuyến do có hiệu quả cao và do khả năng sẵn sàng kết hợp với các giải pháp bảo mật khác như mật mã hóa [1, 3, 4]. Ý tưởng chính của bảo mật lớp vật lý trong các hệ thống thông tin vô tuyến là xem xét các yếu tố ở lớp vật lý như tạp âm nhiệt, hệ số pha-đinh của kênh truyền và các kỹ thuật xử lý tín hiệu ảnh hưởng như thế nào đến khả năng

bảo mật thông tin được truyền qua kênh vật lý khi có mặt các thiết bị xâm nhập. Trên cơ sở đó, các giải pháp bảo mật lớp vật lý có thể được đề xuất để thiết bị thu hợp lệ có khả năng tách chính xác tín hiệu mong muốn bất chấp sự gây nhiễu của thiết bị tấn công chủ động trong khi thiết bị nghe lén thụ động không thể tách được tín hiệu mong muốn.

Hệ thống thông tin vô tuyến cỡ rất lớn (massive Multiple-Input Multiple-Output) là một công nghệ mới được đề xuất từ năm 2010 [5] và đã được chấp nhận là một trong các công nghệ chủ chốt của bộ tiêu chuẩn của 3GPP cho mạng thông tin di động thế hệ thứ 5 (5G: the fifth generation) Vô tuyến mới (NR: New Radio) [6]. Trong hệ thống này, trạm gốc được trang bị rất nhiều ăng-ten để phục vụ một hoặc nhiều thuê bao được trang bị chỉ một ăng-ten. Các nghiên cứu trước đây chủ yếu tập trung vào nghiên cứu các tiềm năng trong việc cải thiện hiệu quả sử dụng phổ tần số vô tuyến điện và hiệu quả sử dụng năng lượng hệ thống này [5, 7]. Bảo mật cho hệ thống thông tin vô tuyến MIMO mới chỉ được nghiên cứu trong vài năm gần đây [2, 8]. Các kết quả nghiên cứu đã công bố trên thế giới đến nay cho hệ thống thông tin MIMO cỡ rất lớn xem xét cả ba trường hợp sau đây: (i) chỉ có thiết bị tấn công chủ động [9–14], (ii) chỉ có thiết bị nghe lén thụ động [15–21] và (iii) có cả hai loại thiết bị trên [22, 23].

Bài báo này tập trung nghiên cứu dung lượng bảo mật lớp vật lý trong hệ thống thông tin MIMO cỡ rất lớn khi chỉ có mặt thiết bị nghe lén thụ động trong điều kiện kênh pha-đinh Rice không tương quan về không gian. Theo định nghĩa, dung lượng bảo mật của hệ thống bằng hiệu số của tốc độ dữ liệu đạt được ở thiết bị thu hợp lệ và tốc độ dữ liệu nghe lén được ở thiết bị nghe lén thụ động nếu hiệu số này không âm và bằng không nếu hiệu số này âm. Chú ý rằng, đa số các kết quả nghiên cứu trước đây liên quan đến hệ thống chỉ có một thiết bị nghe lén thụ động giả thiết mô hình kênh Rayleigh, tức là giả thiết hệ số kênh truyền chỉ có thành phần không tầm nhìn thẳng (NLOS: Non-Line-Of-Sight) [15–19]. Đáng chú ý, các kết quả phân tích và mô phỏng với mô hình kênh pha-đinh Rayleigh khẳng định thiết bị nghe lén thụ động gần như không thể tách được tín hiệu truyền từ trạm gốc, tức là tốc độ dữ liệu nghe lén rất nhỏ và có thể bỏ qua, nếu số lượng ăng-ten tại trạm gốc đủ lớn. Nói cách khác, dung lượng bảo mật của hệ thống sẽ tăng theo số lượng ăng-ten tại trạm gốc. Về lý thuyết, mô hình kênh pha-đinh Rice được giả thiết trong bài báo này tổng quát hơn mô hình kênh pha-đinh Rayleigh vì có thêm thành phần truyền tầm nhìn thẳng (LOS: Line-Of-Sight) [24, 25]. Tuy nhiên, mô hình kênh truyền Rice phức tạp lại gây khó khăn cho việc phân tích giải tích dung lượng bảo mật của hệ thống [11, 26]. Trong phạm vi hiểu biết của các tác giả, mới chỉ có một kết quả nghiên cứu được công bố đưa ra kế quả phân tích giải tích cho hệ thống thông tin MIMO cỡ rất lớn trong điều kiện mô hình kênh truyền Rice [21]. Tuy nhiên, công trình [21] xem xét mô hình hệ thống thông tin có nhiều cặp thu-phát chia sẻ một trạm khuếch đại-chuyển tiếp có rất nhiều ăng-ten. Ngoài ra, các tác giả của công trình [21] đã sử dụng phương pháp phân tích tiệm cận số lớn khi số ăng-ten tại trạm gốc rất lớn để phân tích giải tích dung lượng bảo mật của hệ thống. Trong bài báo này, chúng tôi đã đưa ra các kết quả phân tích giải tích dung lượng bảo mật của hệ thống truyền dẫn điểm-điểm với số lượng ăng-ten hữu hạn tại trạm gốc. Đặc biệt, kết quả phân tích giải tích của chúng tôi cho thấy trong điều kiện mô hình kênh truyền pha-đinh Rice thì tốc độ dữ liệu nghe lén được tăng theo số lượng ăng-ten tại trạm gốc trong khi dung lượng bảo mật của hệ thống tiến dần tới một giá trị bão hoà khi số lượng ăng-ten tại trạm gốc tiến tới vô cùng. Khẳng định tương tự như trên đã được quan sát dựa trên kết quả đo tốc độ dữ liệu nghe lén và dung lượng bảo mậ sử dụng một hệ thống MIMO cỡ rất lớn thử nghiệm hoạt động ở trong môi trường truyền dẫn vô tuyến thực tế [20]. Cần nhấn mạnh rằng trong phạm vi hiểu biết của các tác giả thì đây là kết quả công bố đầu tiên trên thế giới đưa ra các kết quả phân tích giải tích cho khẳng định trên. Các kết quả mô phỏng và tính toán số được cung cấp để kiểm chứng các nhận định trên.

Phần tiếp theo của bài báo được bố cục như sau. Mục II mô tả mô hình hệ thống được xem xét. Mục III đưa ra một phân tích giải tích cho dung lượng bảo mật của hệ thống. Mục IV cung cấp một số kết quả mô phỏng và tính toán số để kiểm chứng các kết quả phân tích giải tích và để khảo sát và đánh giá dung lượng bảo mật của hệ thống trong một số kịch bản cụ thể. Mục V kết luận bài báo và đưa ra một số hướng nghiên cứu tiếp theo.

Một số ký hiệu sử dụng trong bài báo này như sau: a là đại lượng vô hướng, $\mathbf{a}$ là đại lượng véc-tơ, $\mathbf{A}$ là ma trận, $[\mathbf{A}]_{i,j}$, $\mathbf{A}^H$, $\|\mathbf{A}\|_F$, $|\mathbf{A}|$ lần lượt là phần tử (i,j), ma trận chuyển vị liên hợp phức (Hermitian), chuẩn Frobenius, và định thức của ma trận $\mathbf{A}$, $\mathbb{E}[\cdot]$ là toán tử tính giá trị trung bình.

II. MÔ HÌNH HỆ THỐNG

Xem xét một hệ thống MIMO với trạm gốc (ký hiệu là A) đang phục vụ một thuê bao hợp lệ (ký hiệu là nút B) với sự có mặt của một thiết bị nghe trộm thụ động (ký hiệu là E), tức là thiết bị này không phát tín hiệu trong suốt thời gian được xem xét của hệ thống. Trong khi trạm gốc A có N_{t} ăng-ten thì thuê bao B và thiết bị nghe trộm E chỉ có một ăng-ten. Để tiện trình bày, chúng ta ký hiệu $\mathcal{X} = \{\mathrm{B}, \mathrm{E}\}$ là tập chỉ số nút. Giả thiết hệ thống hoạt động ở chế độ song công phân chia theo thời gian (TDD: Time Division Duplexing) với khung truyền dẫn vô tuyến dài τ ký hiệu. Giả thiết cấu trúc khung vô tuyến đã được định trước và

gồm có hai phần: (i) phần đầu gồm τ_p dành cho quá trình huấn luyện và ước lượng hệ số kênh truyền đường lên và (ii) phần còn lại dài $\tau_d = \tau - \tau_p$ ký hiệu được dùng để truyền dữ liệu đường xuống từ trạm gốc A tới thuê bao B.

Giả thiết kênh truyền vô tuyến có dạng pha-đinh khối phẳng trên miền tần số, trong đó hệ số kênh truyền không thay đổi trong thời gian của một khung vô tuyến nhưng có thể thay đổi một cách độc lập từ khung vô tuyến này sang khung vô tuyến khác. Ký hiệu $\mathbf{h}_B \in \mathbb{C}^{N_t \times 1}$ là vector hệ số kênh truyền đường lên từ thuê bao tới trạm gốc và $\mathbf{h}_E \in \mathbb{C}^{N_t \times 1}$ là vector hệ số kênh truyền đường lên từ thiết bị nghe lén tới trạm gốc. Giả thiết hệ số kênh truyền ở đường lên và đường xuống đối xứng hoàn hảo, tức là $\mathbf{h}_B^H, \mathbf{h}_E^H \in \mathbb{C}^{1 \times N_t}$ là các vector hệ số kênh truyền đường xuống tương ứng. Trong bài báo này, chúng ta giả thiết hệ số kênh truyền tuân theo mô hình pha-đinh Rice không tương quan về không gian. Ký hiệu κ_X là hệ số Rice và β_X là hệ số pha-đinh phạm vi rộng (large-scale fading) của kênh truyền từ trạm gốc tới nút $X \in \mathcal{X}$. Các hệ số pha-đinh phạm vi rộng ứng với thành phần truyền LOS $\beta_{X,L}$ và thành phần truyền NLOS $\beta_{X,N}$ được tính như sau:

$$\beta_{X,L} = \sqrt{\frac{\kappa_X}{\kappa_X + 1}}\beta_X, \tag{1}$$

$$\beta_{X,N} = \sqrt{\frac{1}{\kappa_X + 1}}\beta_X. \tag{2}$$

Khi đó vector hệ số kênh truyền từ trạm gốc tới nút X, ký hiệu $\mathbf{h}_X$, có phân bố $\mathcal{CN}(\mathbf{g}_X, \beta_{X,N}\mathbf{I}_N)$ với $X \in \mathcal{X}$ và được biểu diễn dưới dạng

$$\mathbf{h}_X = \mathbf{g}_X + \beta_{X,N}^{1/2}\mathbf{w}_X, \tag{3}$$

trong đó $\mathbf{g}_X$ là vector hệ số kênh truyền ứng với thành phần truyền LOS và $\mathbf{w}_X \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_t})$ là vector hệ số kênh truyền pha-đinh phạm vi nhỏ (small-scale fading). Để tiện tính toán, giả thiết mảng anten tại trạm gốc A được phân bố tuyến tính đều (ULA: Uniform Linear Array). Việc mở rộng ra các dạng hình học khác của mảng anten này không quá phức tạp. Khi đó, vector hệ số truyền LOS từ trạm gốc tới nút $X \in \mathcal{X}$ được tính như sau

$$\mathbf{g}_X = \beta_{X,L}^{1/2}\left[1 \;\; e^{j2\pi d \sin\phi_X} \;\; \cdots \;\; e^{j2\pi d(N-1)\sin\phi_X}\right]^T, \tag{4}$$

trong đó ϕ_X là góc tới từ nút X tới trạm gốc và d là tỷ số giữa khoảng cách giữa các phần tử ăng-ten kề nhau ở trạm gốc chia cho bước sóng. Chú ý rằng $\mathbf{g}_X^H\mathbf{g}_X = N_t\beta_{X,L}$ với mọi $X \in \mathcal{X}$. Để tiện trình bày, ta định nghĩa một số tham số như sau:

$$\psi(\phi_B, \phi_B) = \pi d(\sin\phi_B - \sin\phi_E), \tag{5}$$

$$\alpha(\phi_B, \phi_E, N_t) = \frac{\sin(N_t\psi(\phi_B, \phi_B))}{\sin(\psi(\phi_B, \phi_B))}. \tag{6}$$

Sau một số phép biến đổi, ta có

$$\mathbf{g}_E^H\mathbf{g}_B = \beta_{B,L}^{1/2}\beta_{E,L}^{1/2}e^{j\psi(\phi_B,\phi_B)}\alpha(\phi_B, \phi_E, N_t). \tag{7}$$

Trong pha huấn luyện và ước lượng kênh, nút B truyền một tín hiệu hoa tiêu với công suất phát p_p. Tín hiệu huấn luyện sau khi tiền xử lý là

$$\mathbf{y}_A = \sqrt{p_p}\tau_p\mathbf{h}_B + \mathbf{n}_A, \tag{8}$$

trong đó $\mathbf{n}_A \sim \mathcal{CN}(\mathbf{0}, \sigma_A^2\mathbf{I}_{N_t})$ là tạp âm Gauss trắng cộng tính (AWGN: Additive white Gaussian noise) có công suất σ_A^2. Giả thiết trạm gốc áp dụng kỹ thuật ước lượng kênh tối thiểu trung bình lỗi bình phương (MMSE: Minimum Mean Squared Error) để nhận được một ước lượng hệ số kênh truyền tới nút B là

$$\hat{\mathbf{h}}_B = \mathbf{g}_B + \frac{\sqrt{p_p}\beta_{B,N}}{p_p\tau_p\beta_{B,N} + \sigma_A^2}(\mathbf{y}_A - \sqrt{p_p}\tau_p\mathbf{g}_B). \tag{9}$$

Theo tính chất trực giao của phương pháp MMSE, sai số ước lượng tương ứng là

$$\tilde{\mathbf{h}}_B = \mathbf{h}_B - \hat{\mathbf{h}}_B. \tag{10}$$

Chú ý rằng $\hat{\mathbf{h}}_B \sim \mathcal{CN}(\mathbf{g}_B, \hat{\beta}_{B,N}\mathbf{I}_{N_t})$ và $\tilde{\mathbf{h}}_B \sim \mathcal{CN}(\mathbf{0}, \tilde{\beta}_{B,N}\mathbf{I}_{N_t})$ độc lập thống kê với nhau, trong đó

$$\hat{\beta}_{B,N} = \frac{p_p\tau_p\beta_{B,N}^2}{p_p\tau_p\beta_{B,N} + \sigma_A^2}, \tag{11}$$

$$\tilde{\beta}_{B,N} = \frac{\beta_{B,N}\sigma_A^2}{p_p\tau_p\beta_{B,N} + \sigma_A^2}. \tag{12}$$

Bên cạnh đó, ta có thể biểu diễn $\hat{\mathbf{h}}_B$ và $\tilde{\mathbf{h}}_B$ như sau:

$$\begin{aligned}\hat{\mathbf{h}}_B &= \mathbf{g}_B + \hat{\beta}_{B,N}^{1/2}\hat{\mathbf{w}}_B,\\ \tilde{\mathbf{h}}_B &= \tilde{\beta}_{B,N}^{1/2}\tilde{\mathbf{w}}_B,\end{aligned} \tag{13}$$

trong đó $\hat{\mathbf{w}}_B$ và $\tilde{\mathbf{w}}_B$ có cùng phân bố $\mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_t})$ và độc lập thống kê với nhau.

Trong pha truyền dữ liệu đường xuống, trạm gốc truyền tín hiệu x_B, trong đó $\mathbb{E}[x_B] = 0$, $\mathbb{E}[|x_B|^2] = 1$, tới nút B, nhưng bị nút E nghe lén. Ký hiệu p_d là công suất phát ở đường xuống. Giả thiết trạm gốc sử dụng bộ tiền mã hóa kết hợp phát cực đại (MRT: Maximal Ratio Transmission) được cho bởi

$$\mathbf{f}_B = \frac{\hat{\mathbf{h}}_B}{\xi}, \tag{14}$$

trong đó $\xi^2 = \mathbb{E}[\hat{\mathbf{h}}_B^H\hat{\mathbf{h}}_B] = (\beta_{B,L} + \hat{\beta}_{B,N})N_t$ là hệ số chuẩn hoá nhằm thỏa mãn điều kiện công suất phát trung bình cực đại tại trạm gốc $\mathbb{E}[|\mathbf{f}_B x_B|^2] \le p_d$. Tín hiệu thu được ở nút B và nút E lần lượt là

$$y_B = \sqrt{p_f}\mathbf{h}_B^H\mathbf{f}_B x_B + n_B, \tag{15}$$

$$y_E = \sqrt{p_f}\mathbf{h}_E^H\mathbf{f}_B x_B + n_B, \tag{16}$$

trong đó $n_B \sim \mathcal{CN}(0, \sigma_B^2)$ và $n_E \sim \mathcal{CN}(0, \sigma_E^2)$ là tạp âm Gauss trắng cộng độc lập thống kê với nhau.

III. PHÂN TÍCH DUNG LƯỢNG BẢO MẬT

1. Định nghĩa và cách tiếp cận

Dung lượng bảo mật của hệ thống là tốc độ dữ liệu tối đa có thể truyền từ trạm gốc tới thuê bao hợp lệ, tức là nút B, một cách tin cậy và bảo mật mà không cần dùng thêm các biện pháp mã hoá. Theo định nghĩa, dung lượng bảo mật (SC: Secret Capacity) được xác định như sau

$$C_{\mathrm{SC}} = [R_{\mathrm{B}} - R_{\mathrm{E}}]^{+}, \tag{17}$$

trong đó $[x]^{+} = \max\{x, 0\}$, R_{B} là tốc độ dữ liệu hợp lệ đạt được ở nút B và R_{E} là tốc độ dữ liệu nghe lén đạt được ở nút E. Dưới đây, mục III-2 trình bày chi tiết phân tích tốc độ dữ liệu đạt được ở nút B, mục III-3 trình bày chi tiết phân tích tốc độ dữ liệu đạt được ở nút E.

Chú ý rằng trạm gốc không truyền tín hiệu hoa tiêu đường xuống nên nút B và nút E không thể ước lượng hệ số kênh đường xuống tức thời. Trong bài báo này, chúng ta chấp thuận phương pháp tiếp cận thường được sử dụng trong các tài liệu trước đây trong đó các nút này chỉ ước lượng được hệ số kênh truyền đường xuống hiệu dụng trung bình [27]. Cụ thể, nút B chỉ có được thông tin trạng thái kênh ở dạng $\mathbb{E}[\mathbf{h}_{\mathrm{B}}^{H}\mathbf{f}_{\mathrm{B}}]$. Tương tự, nút E chỉ có được thông tin trạng thái kênh ở dạng $\mathbb{E}[\mathbf{h}_{\mathrm{E}}^{H}\mathbf{f}_{\mathrm{B}}]$.

Ngoài ra, bổ đề sau đây sẽ được sử dụng nhiều trong quá trình xây dựng công thức giải tích dạng tường minh cho tốc độ dữ liệu đạt được ở nút B và nút E.

Bổ đề 1: Cho $\mathbf{a} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$ và ma trận chuẩn tắc $\mathbf{B}$ (tức là $\mathbf{B}$ thoả mãn điều kiện $\mathbf{BB^H} = \mathbf{B}^H\mathbf{B}$). Khi đó ta có

$$\mathbb{E}[\mathbf{a}^H\mathbf{B}\mathbf{a}] = \mathrm{tr}\mathbf{B}, \tag{18}$$

$$\mathbb{E}[|\mathbf{a}^H\mathbf{B}\mathbf{a}|^2] = |\mathrm{tr}(\mathbf{B})|^2 + \mathrm{tr}(\mathbf{B}\mathbf{B}^H). \tag{19}$$

Chứng minh: Ký hiệu kết quả phân rã kỳ dị (Eigenvalue Decomposition) của $\mathbf{B}$ như sau $\mathbf{B} = \mathbf{U}^H\mathbf{\Lambda}\mathbf{U}$ trong đó $\mathbf{U}$ là một ma trận unita (tức là $\mathbf{U}\mathbf{U}^H = \mathbf{U}^H\mathbf{U} = \mathbf{I}_N$) và $\mathbf{\Lambda} = \mathrm{diag}\lambda_1, \lambda_2, \cdots, \lambda_N$. Chú ý rằng $\mathbf{c} = \mathbf{U}\mathbf{a} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$. Giả thiết là $\mathbf{c} = [c_1 \ c_2 \ \cdots \ c_N]^T$. Ta có

$$\mathbb{E}[\mathbf{a}^H\mathbf{B}\mathbf{a}] = \mathbb{E}[\mathbf{c}^H\mathbf{\Lambda}\mathbf{c}] = \sum_{n=1}^{N}\lambda_n\mathbb{E}[|c_n|^2] = \mathrm{tr}(\mathbf{B}).$$

Tương tự, ta có

$$\mathbb{E}[|\mathbf{a}^H\mathbf{B}\mathbf{a}|^2] = \mathbb{E}\left[\left|\sum_{n=1}^{N}\lambda_n|c_n|^2\right|^2\right] \tag{20}$$

$$= \sum_{m=1}^{N}\sum_{n=1}^{N}\mathbb{E}[|c_m|^2|c_n|^2]\lambda_m\lambda_n^* \tag{21}$$

$$= |\mathrm{tr}(\mathbf{\Lambda})|^2 + \mathrm{tr}(\mathbf{\Lambda}\mathbf{\Lambda}^H) \tag{22}$$

$$= |\mathrm{tr}(\mathbf{B})|^2 + \mathrm{tr}(\mathbf{B}\mathbf{B}^H), \tag{23}$$

trong đó chúng ta đã áp dụng tính chất $\mathbb{E}[|c_n|^2] = 1$ và $\mathbb{E}[|c_n|^4] = 2$ khi $c_n \sim \mathcal{CN}(0, 1)$. □

2. Tốc độ dữ liệu hợp lệ

Từ công thức (15) ta có thể viết lại biểu thức tín hiệu thu tại nút B như sau:

$$y_{\mathrm{B}} = \sqrt{p_{\mathrm{d}}}\mathbb{E}[\mathbf{h}_{\mathrm{B}}^H\mathbf{f}_{\mathrm{B}}]x_{\mathrm{B}} + \sqrt{p_{\mathrm{d}}}(\mathbf{h}_{\mathrm{B}}^H\mathbf{f}_{\mathrm{B}} - \mathbb{E}[\mathbf{h}_{\mathrm{B}}^H\mathbf{f}_{\mathrm{B}}])x_{\mathrm{B}} + n_{\mathrm{B}}, \tag{24}$$

trong đó số hạng đầu tiên đóng vai trò là tín hiệu mong muốn để tách sóng kết hợp, số hạng thứ hai đóng vai trò nhiễu gây ra do sai số ước lượng hệ số kênh truyền đường xuống hiệu dụng và số hạng cuối cùng là tạp âm nhiệt. Để tìm một giới hạn dưới cho tỷ số công suất tín hiệu trên tổng công suất nhiễu và tạp âm (SINR: Signal-to-Interference-plus-Noise Ratio), ta xét trường hợp xấu nhất xảy ra khi số hạng thứ hai và số hạng thứ ba là các tín hiệu không tương quan. Khi đó, một giới hạn dưới của SINR tại nút B được ký hiệu là η_{B} và được xác định như sau:

$$\eta_{\mathrm{B}} = \frac{p_{\mathrm{d}}|\mathbb{E}[\mathbf{h}_{\mathrm{B}}^H\mathbf{f}_{\mathrm{B}}x_{\mathrm{B}}]|^2}{p_{\mathrm{d}}\mathbb{E}[|(\mathbf{h}_{\mathrm{B}}^H\mathbf{f}_{\mathrm{B}} - \mathbb{E}[\mathbf{h}_{\mathrm{B}}^H\mathbf{f}_{\mathrm{B}}])x_{\mathrm{B}}|^2] + \sigma_{\mathrm{B}}^2}$$
$$= \frac{p_{\mathrm{d}}|\mathbb{E}[\mathbf{h}_{\mathrm{B}}^H\mathbf{f}_{\mathrm{B}}]|^2}{p_{\mathrm{d}}(\mathbb{E}[|\mathbf{h}_{\mathrm{B}}^H\mathbf{f}_{\mathrm{B}}|^2] - |\mathbb{E}[\mathbf{h}_{\mathrm{B}}^H\mathbf{f}_{\mathrm{B}}]|^2) + \sigma_{\mathrm{B}}^2}. \tag{25}$$

Bổ đề 2: Giá trị SINR hợp lệ η_{B} tỷ lệ tuyến tính với số ăng-ten tại trạm gốc N_{t}.

Chứng minh: Thay các biểu thức (14) và (10) vào (25) và sau đó áp dụng các tính chất xác suất của $\hat{\mathbf{h}}_{\mathrm{B}}$ và $\tilde{\mathbf{h}}_{\mathrm{B}}$, ta thu được

$$\mathbb{E}[\mathbf{h}_{\mathrm{B}}^H\mathbf{f}_{\mathrm{B}}] = \frac{\mathbb{E}[(\hat{\mathbf{h}}_{\mathrm{B}}^H + \tilde{\mathbf{h}}_{\mathrm{B}}^H)\hat{\mathbf{h}}_{\mathrm{B}}]}{\xi} = \frac{\mathbb{E}[\hat{\mathbf{h}}_{\mathrm{B}}^H\hat{\mathbf{h}}_{\mathrm{B}}]}{\xi} = \xi. \tag{26}$$

Bằng cách tương tự, ta có

$$\mathbb{E}[|\mathbf{h}_{\mathrm{B}}^H\mathbf{f}_{\mathrm{B}}|^2] = \frac{1}{\xi^2}(\mathbb{E}[|\hat{\mathbf{h}}_{\mathrm{B}}^H\hat{\mathbf{h}}_{\mathrm{B}}|^2] + \mathbb{E}[|\tilde{\mathbf{h}}_{\mathrm{B}}^H\hat{\mathbf{h}}_{\mathrm{B}}|^2]). \tag{27}$$

Thay (13) vào (27), ta thu được

$$\mathbb{E}[|\hat{\mathbf{h}}_{\mathrm{B}}^H\hat{\mathbf{h}}_{\mathrm{B}}|^2] = \mathbb{E}[|(\mathbf{g}_{\mathrm{B}}^H + \hat{\beta}_{\mathrm{B,N}}^{1/2}\hat{\mathbf{w}}_{\mathrm{B}}^H)(\mathbf{g}_{\mathrm{B}} + \hat{\beta}_{\mathrm{B,N}}^{1/2}\hat{\mathbf{w}}_{\mathrm{B}})|^2]$$
$$= \mathbb{E}[|a_1 + b_1 + c_1 + d_1|^2], \tag{28}$$

trong đó

$$a_1 = \mathbf{g}_{\mathrm{B}}^H\mathbf{g}_{\mathrm{B}} = \beta_{\mathrm{B,L}}N_{\mathrm{t}},$$
$$b_1 = \hat{\beta}_{\mathrm{B,N}}^{1/2}\hat{\mathbf{w}}_{\mathrm{B}}^H\mathbf{g}_{\mathrm{B}},$$
$$c_1 = \hat{\beta}_{\mathrm{B,N}}^{1/2}\mathbf{g}_{\mathrm{B}}^H\hat{\mathbf{w}}_{\mathrm{B}},$$
$$d_1 = \hat{\beta}_{\mathrm{B,N}}\hat{\mathbf{w}}_{\mathrm{B}}^H\hat{\mathbf{w}}_{\mathrm{B}}.$$

Áp dụng bổ đề 1 và tính chất đối xứng tròn của $\hat{\mathbf{w}}$, chúng ta tính được các thành phần thuộc vế phải của (28) như sau:

$$\mathbb{E}[a_1a_1^*] = \beta_{\mathrm{B,L}}^2N_{\mathrm{t}}^2,$$
$$\mathbb{E}[b_1b_1^*] = \mathbb{E}[c_1c_1^*] = \hat{\beta}_{\mathrm{B,N}}\beta_{\mathrm{B,L}}N_{\mathrm{t}},$$
$$\mathbb{E}[a_1d_1^*] = \mathbb{E}[d_1a_1^*] = \hat{\beta}_{\mathrm{B,N}}\beta_{\mathrm{B,L}}N_{\mathrm{t}}^2,$$
$$\mathbb{E}[d_1d_1^*] = \hat{\beta}_{\mathrm{B,N}}^2(N_{\mathrm{t}}^2 + N_{\mathrm{t}}),$$

trong khi các thành phần còn lại bằng 0. Từ các kết quả trên và sau một số phép biến đổi ta có

$$\mathbb{E}[|\hat{\mathbf{h}}_{\mathrm{B}}^H \hat{\mathbf{h}}_{\mathrm{B}}|^2] = \xi^4 + \hat{\beta}_{\mathrm{B,N}}\xi^2 + \hat{\beta}_{\mathrm{B,N}}\beta_{\mathrm{B,L}}N_{\mathrm{t}}. \quad (29)$$

Thay (13) vào (27), ta thu được

$$\begin{aligned}\mathbb{E}[|\tilde{\mathbf{h}}_{\mathrm{B,N}}^H \hat{\mathbf{h}}_{\mathrm{B}}|^2] &= \mathbb{E}[|\tilde{\beta}_{\mathrm{B,N}}^{1/2}\tilde{\mathbf{w}}_{\mathrm{B}}^H(\mathbf{g}_{\mathrm{B}} + \hat{\beta}_{\mathrm{B,N}}^{1/2}\hat{\mathbf{w}}_{\mathrm{B}})|^2] \\ &= \tilde{\beta}_{\mathrm{B,N}}\mathbb{E}[|\tilde{\mathbf{w}}_{\mathrm{B}}^H\mathbf{g}_{\mathrm{B}} + \hat{\beta}_{\mathrm{B,N}}^{1/2}\tilde{\mathbf{w}}_{\mathrm{B}}^H\hat{\mathbf{w}}_{\mathrm{B}})|^2] \\ &= \tilde{\beta}_{\mathrm{B,N}}\mathbb{E}[\tilde{\mathbf{w}}_{\mathrm{B}}^H\mathbf{g}_{\mathrm{B}}\mathbf{g}_{\mathrm{B}}^H\tilde{\mathbf{w}}_{\mathrm{B}}] + \hat{\beta}_{\mathrm{B,N}}\mathbb{E}[|\tilde{\mathbf{w}}_{\mathrm{B}}^H\hat{\mathbf{w}}_{\mathrm{B}}|^2] \\ &= \tilde{\beta}_{\mathrm{B,N}}[\beta_{\mathrm{B,L}}N_{\mathrm{t}} + \hat{\beta}_{\mathrm{B,N}}N_{\mathrm{t}}] \\ &= \tilde{\beta}_{\mathrm{B,N}}\xi^2. \end{aligned} \quad (30)$$

Thay các kết quả vừa tính được vào (25) và sau một số phép biến đổi, ta thu được

$$\eta_{\mathrm{B}} = \bar{\eta}_{\mathrm{B}}N_{\mathrm{t}}, \quad (31)$$

trong đó

$$\bar{\eta}_{\mathrm{B}} = \frac{p_{\mathrm{d}}(\beta_{\mathrm{B,L}} + \hat{\beta}_{\mathrm{B,N}})^2}{(p_{\mathrm{d}}\beta_{\mathrm{B,N}} + \sigma_{\mathrm{B}}^2)(\beta_{\mathrm{B,L}} + \hat{\beta}_{\mathrm{B,N}}) + p_{\mathrm{d}}\hat{\beta}_{\mathrm{B,N}}\beta_{\mathrm{B,L}}}. \quad (32)$$

Nhận thấy rằng $\bar{\eta}_{\mathrm{B}}$ chỉ phụ thuộc vào các tham số pha-đinh phạm vi lớn và các tham số công suất mà không phụ thuộc vào N_{t}, do đó η_{B} tỷ lệ tuyến tính với N_{t}. □

Tốc độ dữ liệu đạt được tương ứng ở nút B hay thuê bao hợp lệ được định nghĩa như sau:

$$R_{\mathrm{B}} = \log_2(1 + \eta_{\mathrm{B}}) = \log_2(1 + \bar{\eta}_{\mathrm{B}}N_{\mathrm{t}}). \quad (33)$$

3. Tốc độ dữ liệu nghe lén đạt được

Từ công thức (16) ta có thể viết lại biểu thức tín hiệu thu tại nút B như sau:

$$y_{\mathrm{E}} = \sqrt{p_{\mathrm{d}}}\mathbb{E}[\mathbf{h}_{\mathrm{E}}^H\mathbf{f}_{\mathrm{B}}]x_{\mathrm{B}} + \sqrt{p_{\mathrm{d}}}(\mathbf{h}_{\mathrm{E}}^H\mathbf{f}_{\mathrm{B}} - \mathbb{E}[\mathbf{h}_{\mathrm{E}}^H\mathbf{f}_{\mathrm{B}}])x_{\mathrm{B}} + n_{\mathrm{B}}. \quad (34)$$

Khi đó, một giới hạn dưới của SINR tại nút E được ký hiệu là η_{E} và được xác định bởi

$$\begin{aligned}\eta_{\mathrm{E}} &= \frac{p_{\mathrm{d}}|\mathbb{E}[\mathbf{h}_{\mathrm{E}}^H\mathbf{f}_{\mathrm{B}}x_{\mathrm{B}}]|^2}{p_{\mathrm{d}}\mathbb{E}[|(\mathbf{h}_{\mathrm{E}}^H\mathbf{f}_{\mathrm{B}} - \mathbb{E}[\mathbf{h}_{\mathrm{E}}^H\mathbf{f}_{\mathrm{B}}])x_{\mathrm{B}}|^2] + \sigma_{\mathrm{B}}^2} \\ &= \frac{p_{\mathrm{d}}|\mathbb{E}[\mathbf{h}_{\mathrm{E}}^H\mathbf{f}_{\mathrm{B}}]|^2}{p_{\mathrm{d}}(\mathbb{E}[|\mathbf{h}_{\mathrm{E}}^H\mathbf{f}_{\mathrm{B}}|^2] - |\mathbb{E}[\mathbf{h}_{\mathrm{E}}^H\mathbf{f}_{\mathrm{B}}]|^2) + \sigma_{\mathrm{B}}^2}. \end{aligned} \quad (35)$$

Bổ đề 3: Giá trị SINR nghe lén η_{E} được xác định bởi

$$\eta_{\mathrm{E}} = \bar{\eta}_{\mathrm{E}}\frac{|\alpha(\phi_{\mathrm{B}}, \phi_{\mathrm{E}}, N_{\mathrm{t}})|^2}{N_{\mathrm{t}}}, \quad (36)$$

trong đó

$$\bar{\eta}_{\mathrm{E}} = \frac{p_{\mathrm{d}}\beta_{\mathrm{E,L}}\beta_{\mathrm{B,L}}}{p_{\mathrm{d}}\rho_{\mathrm{E}} + \sigma_{\mathrm{E}}^2(\beta_{\mathrm{B,L}} + \hat{\beta}_{\mathrm{B,N}})}. \quad (37)$$

Chứng minh: Sử dụng phương pháp tính toán tương tự ở mục III-2, ta có thể tính được

$$\begin{aligned}|\mathbb{E}[\mathbf{h}_{\mathrm{E}}^H\mathbf{f}_{\mathrm{B}}]|^2 &= \frac{|\mathbb{E}[(\mathbf{g}_{\mathrm{E}} + \beta_{\mathrm{E,N}}^{1/2}\mathbf{w}_{\mathrm{E}})^H(\mathbf{g}_{\mathrm{B}} + \hat{\beta}_{\mathrm{B,N}}^{1/2}\hat{\mathbf{w}}_{\mathrm{B}})]|^2}{\xi^2} \\ &= \frac{|\mathbf{g}_{\mathrm{E}}^H\mathbf{g}_{\mathrm{B}}|^2}{\xi^2} \\ &= \frac{\beta_{\mathrm{E,L}}\beta_{\mathrm{B,L}}|\alpha(\phi_{\mathrm{B}}, \phi_{\mathrm{E}}, N_{\mathrm{t}})|^2}{\xi^2}. \end{aligned} \quad (38)$$

Tương tự, áp dụng bổ đề 1 ta cũng có

$$\begin{aligned}\mathbb{E}[|\mathbf{h}_{\mathrm{E}}^H\mathbf{f}_{\mathrm{B}}|^2] &= \frac{\mathbb{E}[|(\mathbf{g}_{\mathrm{E}} + \beta_{\mathrm{E,N}}^{1/2}\mathbf{w}_{\mathrm{E}})^H(\mathbf{g}_{\mathrm{B}} + \hat{\beta}_{\mathrm{B,N}}^{1/2}\hat{\mathbf{w}}_{\mathrm{B}})|^2]}{\xi^2} \\ &= \frac{\mathbb{E}[|a_2 + b_2 + c_2 + d_2|^2]}{\xi^2} \end{aligned} \quad (39)$$

trong đó

$$\begin{aligned}a_2 &= \mathbf{g}_{\mathrm{E}}^H\mathbf{g}_{\mathrm{B}}, \\ b_2 &= \hat{\beta}_{\mathrm{B,N}}^{1/2}\mathbf{g}_{\mathrm{E}}^H\hat{\mathbf{w}}_{\mathrm{B}}, \\ c_2 &= \beta_{\mathrm{E,N}}^{1/2}\mathbf{w}_{\mathrm{E}}^H\mathbf{g}_{\mathrm{B}}, \\ d_2 &= \beta_{\mathrm{E,N}}^{1/2}\hat{\beta}_{\mathrm{B,N}}^{1/2}\mathbf{w}_{\mathrm{E}}^H\hat{\mathbf{w}}_{\mathrm{B}}. \end{aligned}$$

Sau khi khai triển vế phải của (39) và áp dụng bổ đề 1, ta thu được

$$\begin{aligned}\mathbb{E}[a_2a_2^*] &= \beta_{\mathrm{E,L}}\beta_{\mathrm{B,L}}|\alpha(\phi_{\mathrm{B}}, \phi_{\mathrm{E}}, N_{\mathrm{t}})|^2, \\ \mathbb{E}[b_2b_2^*] &= \beta_{\mathrm{E,L}}\hat{\beta}_{\mathrm{B,N}}N_{\mathrm{t}}, \\ \mathbb{E}[c_2c_2^*] &= \beta_{\mathrm{E,N}}\beta_{\mathrm{B,L}}N_{\mathrm{t}}, \\ \mathbb{E}[d_2d_2^*] &= \beta_{\mathrm{E,N}}\hat{\beta}_{\mathrm{B,N}}N_{\mathrm{t}}, \end{aligned}$$

trong khi các thành phần khác bằng 0 do tính chất đối xứng vòng và độc lập của $\hat{\mathbf{w}}_{\mathrm{B}}$ và $\mathbf{w}_{\mathrm{E}}$. Như vậy, ta có

$$\mathbb{E}[|\mathbf{h}_{\mathrm{E}}^H\mathbf{f}_{\mathrm{B}}|^2] = \frac{\beta_{\mathrm{E,L}}\beta_{\mathrm{B,L}}|\alpha(\phi_{\mathrm{B}}, \phi_{\mathrm{E}}, N_{\mathrm{t}})|^2 + \rho_{\mathrm{E}}N_{\mathrm{t}}}{\xi^2}, \quad (40)$$

trong đó $\rho_{\mathrm{E}} = \beta_{\mathrm{E,L}}\hat{\beta}_{\mathrm{B,N}} + \beta_{\mathrm{E,N}}\beta_{\mathrm{B,L}} + \beta_{\mathrm{E,N}}\hat{\beta}_{\mathrm{B,N}}$ chỉ phụ thuộc vào các tham số pha-đinh phạm vi lớn và các tham số công suất mà không phụ thuộc vào N_{t}, ϕ_{B} và ϕ_{E}. Thay (38) và (40) vào (35) ta thu được (36). □

Tốc độ dữ liệu đạt được tương ứng ở nút B hay thuê bao hợp lệ được định nghĩa như sau:

$$R_{\mathrm{E}} = \log_2(1 + \eta_{\mathrm{E}}). \quad (41)$$

4. Thảo luận

Mục này tập trung khảo sát và thảo luận một số tính chất của tốc độ dữ liệu hợp lệ đạt được tại nút B (tức là R_{B} được xác định bởi (33)) và tốc độ dữ liệu nghe lén đạt được tại nút E (tức là R_{E} được xác định bởi (41)) cũng như dung lượng bảo mật của hệ thống C_{SC} được xác định bởi (17). Cụ thể, bổ đề 4 trình bày tính chất của giá trị SINR tại

thiết bị nghe trộm η_E và bổ đề 5 trình bày dung lượng bảo mật của hệ thống C_{SC} trong các điều kiện khác nhau về quan hệ giữa ϕ_E và ϕ_B. Để tiện cho việc thảo luận, ký hiệu chênh lệch góc tới của thuê bao hợp lệ B và thiết bị nghe trộm B là $\Delta\phi = |\phi_B - \phi_E|$.

Bổ đề 4: Nếu $\Delta\phi = 0$ thì η_E tỷ lệ tuyến tính với N_t. Ngoài ra thêm điều kiện, nếu N_t đủ lớn thì dung lượng bảo mật của hệ thống được xấp xỉ như sau:

$$C_{SC} \approx \log_2(\bar{\eta}_B/\bar{\eta}_E). \tag{42}$$

Chứng minh: Ta có khi $x \to 0$ thì $\sin(x) \approx x$ có độ chính xác cao. Thực tế chỉ cần $x < 0,2$ thì xấp xỉ này đã có độ chính xác cao [28]. Áp dụng biểu thức xấp xỉ này vào (6) ta có $\alpha(\phi_B, \phi_E, N_t) \approx N_t$. Thay giá trị này vào (36) ta có

$$\eta_E \approx \bar{\eta}_E N_t, \tag{43}$$

trong đó $\bar{\eta}_E$ được cho trong (37). Vì $\bar{\eta}_E$ chỉ phụ thuộc vào các tham số pha-đinh phạm vi lớn và các tham số công suất nên η_E có thể xấp xỉ bằng một hàm tuyến tính của N_t. Thay (43) vào (41) ta có $R_E \approx \log_2(1 + \bar{\eta}_E N_t)$. Kết hợp kết quả trên với (33), ta thu được một giá trị xấp xỉ của dung lượng bảo mật của hệ thống như sau:

$$C_{SC} \approx \log_2\left(\frac{1 + \bar{\eta}_B N_t}{1 + \bar{\eta}_E N_t}\right). \tag{44}$$

Tính giới hạn của biểu thức trên khi $N_t \to 0$ ta được (42). □

Có thể thấy rằng khi thiết bị nghe lén và thiết bị thu hợp lệ có cùng góc tới đến trạm gốc (trên không gian hai chiều), tức là $\phi_E = \phi_B$, thì dung lượng bảo mật của hệ thống C_{SC} chỉ phụ thuộc vào các tham số pha-đinh phạm vi lớn và các tham số công suất nhưng không phụ thuộc vào số lượng ăng-ten tại trạm gốc N_t hay các góc tới ϕ_B và ϕ_E. Hiện tượng này xảy ra do thành phần truyền LOS $\mathbf{g}_E$ và $\mathbf{g}_B$ chỉ sai khác hệ số pha đinh phạm vi lớn nên $\mathbf{h}_E$ và $\mathbf{h}_E$ có tương quan chéo đủ lớn, khiến cho công suất tín hiệu mong muốn hiệu dụng mà thiết bị nghe lén nhận được từ trạm gốc đủ lớn để tách tín hiệu.

Bổ đề 5: Nếu $\Delta\phi \neq 0$ thì $\eta_E \to 0$ và $R_E \to 0$ khi $N_t \to \infty$. Khi đó dung lượng bảo mật $C_{SC} \to R_B = \log_2(1 + \bar{\eta}_B)$ khi N_t đủ lớn.

Chứng minh: Ta có

$$|\alpha(\phi_B, \phi_E, N_t)| \leq |\sin(\psi(\phi_B, \phi_E))|^{-1}, \ \forall N_t \geq 1.$$

Thay bất đẳng thức này vào (36) ta có $0 \leq |\eta_E| \leq g(N_t) = \bar{\eta}_E |\sin(\psi(\phi_B, \phi_E))|^{-2}/N_t$ trong đó $\bar{\eta}_E$ được cho trong (37). Vì $\bar{\eta}_E$ và $\psi(\phi_B, \phi_E)$ không phụ thuộc vào N_t nên $\lim_{N_t\to\infty} g(N_t) = 0$. Vì vậy, $\lim_{N_t\to\infty} \eta_E = 0$. Từ đó ta có $\lim_{N_t\to\infty} R_E = 0$ và $\lim_{N_t\to 0} C_{SC} = R_B$. □

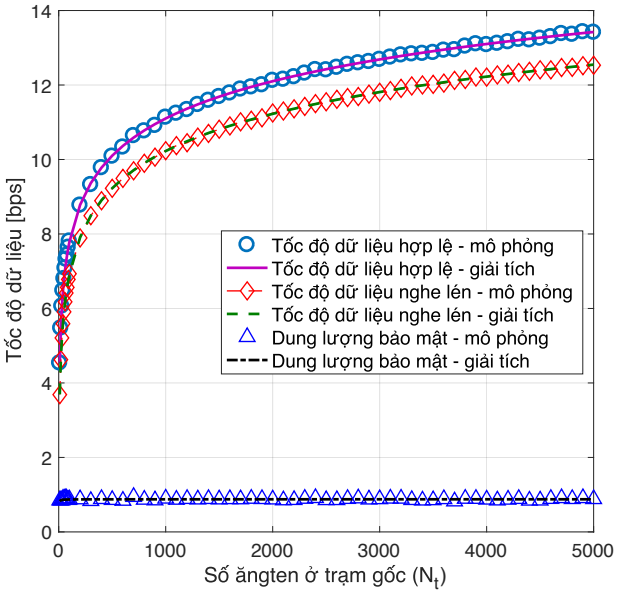
Nhớ lại rằng, các kết quả nghiên cứu trước đây cho điều kiện kênh pha-đinh Rayleigh đã khẳng định rằng thiết bị nghe lén thụ động gần như không thể tách được thông tin phát từ trạm gốc tới thuê bao hợp lệ. Nói cách khác, thiết bị nghe lén thụ động gần như không ảnh hưởng tới dung lượng bảo mật của hệ thống. Lý do cho hiện tượng này là trong điều kiện kênh pha-đinh Rayleigh với N_t đủ lớn thì $\mathbf{h}_B$ và $\mathbf{h}_E$ không chỉ có hệ số tương quan chéo thấp mà thậm chí còn trực giao với nhau. Chú ý rằng bổ đề 5 cũng đưa ra một khẳng định hoàn toàn tương đồng trong điều kiện kênh pha-đinh Rice nếu cả $\Delta\phi \neq 0$ và N_t đủ lớn. Có thể giải thích hiện tượng này như sau. Khi cả N_t đủ lớn thì độ phân giải không gian của mảng ăng-ten tại trạm gốc đủ nhỏ, điều này kết hợp với điều kiện $\Delta\phi \neq 0$ thì các vector hệ số kênh truyền $\mathbf{h}_B$ và $\mathbf{h}_E$ cũng sẽ có tương quan chéo thấp, khiến cho thiết bị nghe lén gần như không thu được tách được tín hiệu truyền từ trạm gốc.

IV. MÔ PHỎNG VÀ TÍNH TOÁN SỐ

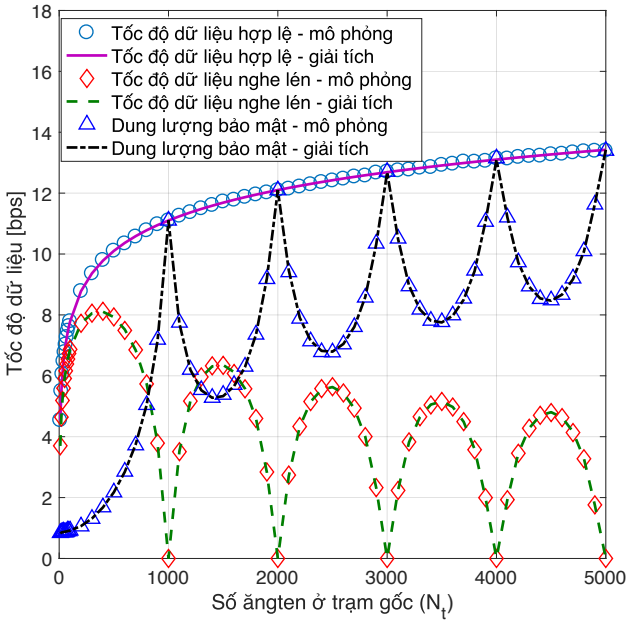
Mục này của bài báo cung cấp một số kết quả mô phỏng và tính toán số để kiểm chứng các kết quả phân tích giải tích đã trình bày ở mục III. Xét một mạng di động chỉ có một tế bào trong đó trạm gốc được đặt ở chính giữa tế bào trong khi thiết bị đầu cuối hợp lệ (nút B) và thiết bị nghe lén thụ động (nút E) được bố trí ngẫu nhiên trong tế bào. Giả thiết ảnh hưởng của hiệu ứng che chắn bị bỏ qua, khi đó hệ số suy hao đường truyền phạm vi lớn được tính như sau: [29–31]

$$\beta_{X,Y} = 32,4 + 10 n_Y \log_{10}(d_{3D,X}) + 20\log_{10}(f_c),$$

trong đó $X \in \mathcal{X}$, $Y \in \mathcal{Y} = \{L, N\}$, $d_{3D,X}$ là khoảng cách tính theo mét từ trạm gốc đến nút X trong không gian 3 chiều, $f_c = 3,5$ GHz là tần số sóng mang, n_Y là hệ số mũ suy hao đường truyền (path-loss exponent). Ngoài ra, $d_{3D,X}$ được tính như sau $d_{3D,X} = \sqrt{d_{2D,X}^2 + (h_A - h_X)^2}$ trong đó $d_{2D,X}$ là khoảng cách từ trạm gốc tới nút X trong không gian 2 chiều, h_A là chiều cao của trạm gốc A và h_X là chiều cao của nút X [29]. Không mất tính tổng quát, giả thiết $h_A = 10$ m và $h_B = h_E = 1,5$ m. Bài báo xem xét môi trường tế bào lớn ở đô thị (UMa: Urban Macro), khi đó $n_L = 2$ cho thành phần truyền LOS và $n_N = 2,9$ cho thành phần truyền NLOS [30, 31]. Theo [29], đối với môi trường UMa thì κ tính theo dB là một biến ngẫu nhiên Gauss $\mathcal{N}(9; 3, 5)$. Để đơn giản, chúng ta giả thiết $\kappa_B = \kappa_E = 9$ dB. Giả thiết hệ thống hoạt động với băng thông 10 MHz, công suất phát ở trạm gốc là $p_d = 46$ dBm, công suất phát ở thiết bị đầu cuối hợp lệ là $p_p = 24$ dBm và mật độ công suất tạp âm nhiệt là $N_0 = -174$ dBm/Hz. Tốc độ dữ liệu được tính cho một sóng mang con băng thông 15 kHz. Giả thiết khoảng cách giữa các ăng-ten lân cận tại trạm gốc bằng nửa bước sóng, tức là $d = 0,5$. Giả thiết hệ số tạp âm tại



Hình 1. Kết quả mô phỏng và kết quả phân tích giải tích của R_B, R_B và C_{SC} dưới dạng hàm số của N_t khi $\Phi_E = \Phi_B = 0$ rad.

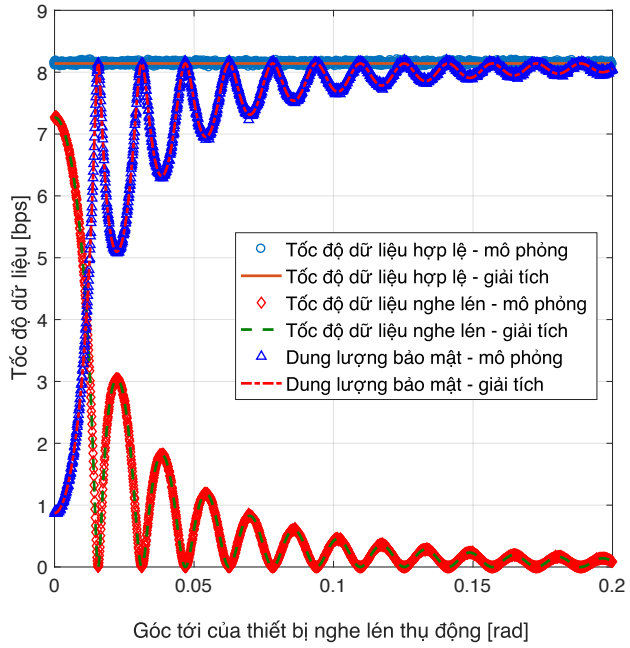


Hình 2. Kết quả mô phỏng và kết quả phân tích giải tích của R_B, R_B và C_{SC} dưới dạng hàm số của N_t khi $\Phi_E = \Phi_B = 0{,}002$ rad.

trạm gốc là 9 dB/Hz trong khi hệ số tạp âm tại nút B và tại nút E là 5 dB/Hz. Không mất tính tổng quát, giả thiết rằng $\Phi_B = 0$ rad.

Trước hết, chúng ta xem xét một kịch bản mô phỏng trong đó thiết bị nghe lén thụ động, hay nút E, đặt khá sát thiết bị đầu cuối hợp lệ, hay nút B. Một số các tham số mô phỏng của kịch bản này như sau: (i) khoảng cách từ nút E và từ nút B đến trạm gốc đều là 300 m, (ii) hệ số mô hình kênh Rice là $\kappa_B = \kappa_E = 9$ dB, và (iii) kết quả mô phỏng được lấy trung bình của 100.000 mẫu. Các hình 1 và 2 trình bày kết quả mô phỏng và kết quả phân tích giải tích của tốc độ dữ liệu hợp lệ R_B, tốc độ dữ liệu nghe lén R_B và dung lượng bảo mật C_{SC} dưới dạng hàm số của N_t tương ứng với khi $\Phi_E = 0$ rad và $\Phi_E = 0{,}002$ rad. Có thể thấy rằng các kết quả mô phỏng gần như nằm trên đường biểu diễn các kết quả phân tích giải tích tương ứng, tức là kết quả phân tích giải tích được đề xuất có độ chính xác cao và có thể được dùng thay thế cho kết quả mô phỏng. Trong cả hai hình trên, R_B luôn tăng theo hàm lôgarít của N_t, đúng như kết quả phân tích trong mục III-2. Hình 1 cho thấy R_E đều tăng theo hàm lôgarít đối với N_t trong khi C_{SC} gần như không đổi. Kết quả mô phỏng này hoàn toàn phù hợp với các khẳng định trong bổ đề 4.

Hình 2 cho thấy khi $\Phi_E \neq \Phi_B$ thì cả R_E và C_{SC} thay đổi không đơn điệu theo N_t. Khi số ăng-ten ở trạm gốc nhỏ thì tốc độ dữ liệu nghe lén gần sát với tốc độ dữ liệu hợp lệ, khiến cho dung lượng bảo mật thấp. Khi số ăng-ten ở trạm gốc tăng lên thì tốc độ dữ liệu nghe lén giảm dần. Đáng chú ý, có một số giá trị số ăng-ten ở trạm gốc khiến cho tốc độ dữ liệu nghe lén tiến sát bằng không và dung



Hình 3. Kết quả mô phỏng và kết quả phân tích giải tích của R_B, R_B và C_{SC} dưới dạng hàm số của Φ_E rad khi $N_t = 128$.

lượng bảo mật gần bằng tốc độ dữ liệu hợp lệ. Lý do là tại các giá trị N_t trên các vector hệ số kênh truyền trực giao với nhau.

Hình 3 trình bày kết quả mô phỏng và kết quả phân tích giải tích của R_B, R_B và C_{SC} dưới dạng hàm số của Φ_E rad khi $N_t = 128$. Có thể thấy rằng khi góc tới Φ_E càng lớn, tức

là $\Delta\Phi$ càng lớn, thì tốc độ dữ liệu nghe lén có xu hướng càng giảm. Điều này hợp lý vì khi $\Delta\Phi$ càng lớn thì tương quan chéo giữa các vector hệ số kênh truyền càng nhỏ.

V. KẾT LUẬN

Bài báo này đề xuất các biểu thức giải tích dạng tường minh cho dung lượng bảo mật của hệ thống thông tin vô tuyến MIMO cỡ rất lớn khi có mặt thiết bị nghe lén thụ động và dưới điều kiện kênh truyền pha-đinh Rice. Kết quả cho thấy của thành phần truyền tầm nhìn thẳng có thể làm cho tương quan chéo giữa các vector hệ số kênh truyền giữa trạm gốc và các thiết bị đủ lớn, từ đó cho phép thiết bị nghe lén thụ động có thể ảnh hưởng lớn đến dung lượng bảo mật của hệ thống. Các kết quả trên được kiểm chứng bởi mô phỏng Monte Carlo trong các điều kiện mô phỏng khác nhau. Một số hướng nghiên cứu tiếp theo liên quan là nghiên cứu ảnh hưởng của thiết bị nghe lén thụ động khi trạm gốc sử dụng các phương pháp xử lý tín hiệu khác hoặc nghiên cứu ảnh hưởng của thiết bị tấn công chủ động trong điều kiện kênh truyền pha-đinh Rice.

LỜI CẢM ƠN

Nghiên cứu này được tài trợ bởi Quỹ phát triển khoa học và công nghệ quốc gia (NAFOSTED) trong đề tài mã số 102.02-2013.09. Nhóm tác giả trân trọng cám ơn sự tài trợ nghiên cứu của Học viện Công nghệ Bưu chính Viễn thông thông qua Phòng thí nghiệm Hệ thống Vô tuyến và Ứng dụng.

TÀI LIỆU THAM KHẢO

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[2] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21–27, 2015.

[3] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[4] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct. 2015.

[5] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3590–3600, 2010.

[6] 3GPP TR 38.912, "Study on new radio (NR) access technology (Release 15)," 3GPP, Technical Report v.15.0.0, Jun. 2018.

[7] T. L. Marzetta, "Massive MIMO: An introduction," *Bell Labs Technical Journal*, vol. 20, pp. 11–22, 2015.

[8] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, 2018.

[9] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[10] D. Kapetanović, G. Zheng, K. Wong, and B. Ottersten, "Detection of pilot contamination attack using random training and massive MIMO," in *Proc. of IEEE Int. Symp. Personal, Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2013, pp. 13–18.

[11] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," *IEEE Transactions on Wireless Communications*, vol. 14, no. 12, pp. 6854–6868, Dec. 2015.

[12] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 3880–3900, Jul. 2016.

[13] D. Hu, W. Zhang, L. He, and J. Wu, "Secure transmission in multi-cell multi-user massive MIMO systems with an active eavesdropper," *to appear in IEEE Wireless Communications Letters*, Jul. 2019.

[14] H. Akhlaghpasand, S. M. Razavizadeh, E. Björnson, and T. T. Do, "Jamming detection in massive MIMO systems," *IEEE Wireless Communications Letters*, vol. 7, no. 2, pp. 242–245, Apr. 2018.

[15] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 4766–4781, 2014.

[16] ——, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2245–2261, 2016.

[17] Y. Long, Z. Chen, L. Li, and J. Fang, "Non-asymptotic analysis of secrecy capacity in massive MIMO system," in *Proceedings of the IEEE International Conference on Communications (ICC)*, Jun. 2015, pp. 4587–4592.

[18] A. Bereyhi, S. Asaad, R. R. Müller, R. F. Schaefer, and A. M. Rabiei, "On robustness of massive MIMO systems against passive eavesdropping under antenna selection," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, Abu Dhabi, UAE, Dec. 2018.

[19] T. Yang, R. Zhang, X. Cheng, and L. Yang, "Secure massive MIMO under imperfect CSI: Performance analysis and channel prediction," *to appear in IEEE Transactions on Information Forensics and Security*, 2018.

[20] C.-Y. Yeh and E. W. Knightly, "Feasibility of passive eavesdropping in massive MIMO: An experimental approach," in *Proceedings of the IEEE Conference on Communications and Network Security (CNS)*, Beijing, China, May 2018.

[21] X. Zhang, D. Guo, and K. Guo, "Secure performance analysis for multi-pair AF relaying massive MIMO systems in Ricean channels," *IEEE Access*, vol. 6, pp. 57 708–57 720, 2018.

[22] A. Mukherjee and A. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *Proceedings of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, Pacific Grove, U.S.A., Nov. 2011, pp. 265–269.

[23] D. B. Rawat, K. Neupane, and M. Song, "A novel algorithm for secrecy rate analysis in massive MIMO system with target SINR requirements," in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, Apr. 2016, pp. 53–58.

[24] O. Ozdogan, E. Bjornson, and E. G. Larsson, "Massive MIMO with spatially correlated rician fading channels,"

Submitted to IEEE Transactions on Communications, 2018.
[25] Y. Hu, Y. Hong, and J. Evans, "Angle-of-arrival-dependent interference modeling in Rician massive MIMO," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 7, pp. 6171–6183, Jul. 2017.
[26] L. Sanguinetti, A. Kammoun, and M. Debbah, "Theoretical performance limits of massive MIMO with uncorrelated Rician fading channels," *to appear in IEEE Transactions on Communications*, 2018.
[27] J. Jose, A. Ashikhmin, T. L. Marzetta, and S. Vishwanath, "Pilot contamination and precoding in multi-cell TDD systems," *IEEE Transactions on Wireless Communications*, vol. 10, no. 8, pp. 2640–2651, Aug. 2011.
[28] E. Bjornson, J. Hoydis, and L. Sanguinetti, *Massive MIMO Networks: Spectral, Energy, and Hardware Efficiency*. Foundations and Trends in Signal Processing, 2017, vol. 11, no. 3-4.
[29] 3GPP TR 38.901, "Study on channel model for frequencies from 0.5 to 100 GHz," 3GPP, Technical Report v.15.0.0, Jun. 2018.
[30] T. S. Rappaport, S. Sun, and M. Shafi, "Investigation and comparison of 3GPP and NYUSIM channel model for 5G wireless communications," in *Proceedings of the IEEE 86th Vehicular Technology Conference (VTC-Fall)*, Toronto, Canada, Sep. 2017.
[31] S. Sun, T. S. Rappaport, T. A. Thomas, A. Ghosh, H. C. Nguyen, I. Z. Kovacs, I. Rodriguez, O. Koymen, and A. Partyka, "Investigation of prediction accuracy, sensitivity, and parameter stability of large-scale propagation path loss models for 5G wireless communications," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 5, pp. 2843–2860, May 2016.

Vũ Lê Quỳnh Giang nhận bằng thạc sĩ và bằng kỹ sư ngành Khoa học máy tính tại Đại học Tổng hợp Kỹ thuật Quốc gia Vongagrat, Liên bang Nga lần lượt vào năm 2007 và năm 2005. Hiện tại, tác giả đang là nghiên cứu sinh và là thành viên của Phòng thí nghiệm Hệ thống Vô tuyến và Ứng dụng thuộc Học viện Công nghệ Bưu chính Viễn thông. Hướng nghiên cứu hiện tại của tác giả là bảo mật lớp vật lý cho hệ thống MIMO cỡ rất lớn.

Trương Trung Kiên nhận bằng tiến sĩ và bằng thạc sĩ ngành Điện tử Viễn thông tại Đại học Tổng hợp bang Texas cơ sở ở thành phố Austin, Texas, Hoa Kỳ lần lượt vào năm 2012 và năm 2008; nhận bằng kỹ sư ngành Điện tử Viễn thông tại Trường Đại học Bách khoa Hà Nội năm 2002. Hướng nghiên cứu hiện tại của tác giả bao gồm một số công nghệ cho mạng 5G như hệ thống FD-MIMO, hệ thống thông tin ở dải bước sóng milimét (mmWave) và hệ thống Internet kết nối vạn vật (Internet of Things). TS. Kiên đã được trao một số giải thưởng nghiên cứu khoa học như Bài báo xuất sắc nhất năm 2013 của tạp chí EURASIP Journal on Wireless Communications and Networking (JWCN), Bài báo xuất sắc nhất năm 2014 của tạp chí KICS Journal of Communications and Networks, Bài báo xuất sắc nhất của Hội nghị International Conference on Advanced Technologies for Communications năm 2018 và Bài báo xuất sắc nhất của Hội thảo Quốc gia về Điện tử, Truyền thông và Công nghệ Thông tin (REV-ECIT) các năm 2015 và 2018. TS. Kiên đang phụ trách Phòng thí nghiệm Hệ thống Vô tuyến và Ứng dụng thuộc Học viện Công nghệ Bưu chính Viễn thông và là Thành viên Cao cấp (Senior Member) của IEEE.