JTE HCM-UTE
ISSN: 1859-1272

TẠP CHÍ KHOA HỌC GIÁO DỤC KỸ THUẬT
Trường Đại học Công nghệ Kỹ thuật Thành phố Hồ Chí Minh
Website: https://jte.edu.vn
Email: jte@hcmute.edu.vn

Performance and Reliability, Security of One-Way Duplex Relay Network Using Artificial Noise

Quoc Bao Ho
Van Hien University, Vietnam

*Corresponding author. *Email: baohq@vhu.edu.vn*

ARTICLE INFO

Received: 15/09/2025
Revised: 31/12/2025
Accepted: 09/01/2026
Published: 28/02/2026

KEYWORDS

Outage Probability;
Intercept Probability;
Secrecy Outage Probability;
Artificial Noise;
One-Way Full-Duplex.

ABSTRACT

The authors employ the artificial noise (AN) technique to enhance physical layer security (PLS) in one-way full-duplex (OWFD) networks. Specifically, an OWFD network incorporating AN and operating over Rayleigh fading channels is considered. The system consists of five nodes: a source node, a destination node, a relay node, an eavesdropper node, and a jamming node. To evaluate security performance, the authors analyze and assess several metrics, including the secrecy outage probability (SOP), secrecy throughput (STP), and the trade-off between outage probability (OP) and intercept probability (IP). Closed-form expressions are derived in the paper. The analytical results are validated through Monte Carlo simulations implemented in MATLAB, the results are illustrated through four graphs: the impact of the artificial-noise node's position on the SOP under variations in the source node's transmit power; the effect of the eavesdropper's position; and the influence of the path-loss exponent on the system's OP, IP, and SOP. In addition, a comparative graph of the SOP between the proposed model and the reference model is presented. All graphs demonstrate a significant improvement in security performance compared with previous studies. The proposed model confirms the feasibility of implementing PLS solutions in OWFD networks.

Hiệu năng và độ tin cậy, bảo mật mạng chuyển tiếp song công một chiều sử dụng nhiễu nhân tạo

Hồ Quốc Bảo
Trường Đại học Văn Hiến, Việt Nam

*Tác giả liên hệ. *Email: baohq@vhu.edu.vn*

THÔNG TIN BÀI BÁO

Ngày nhận bài: 15/09/2025
Ngày hoàn thiện: 31/12/2025
Ngày chấp nhận đăng: 09/01/2026
Ngày đăng: 28/02/2026

TỪ KHÓA

Xác suất dừng;
Xác suất chặn;
Xác suất dừng bảo mật;
Nhiễu nhân tạo;
Song công một chiều.

TÓM TẮT

Tác giả sử dụng phương pháp gây nhiễu nhân tạo (AN) nhằm cải thiện các vấn đề bảo mật lớp vật lý (PLS) trong mạng song công một chiều (OWFD). Cụ thể, xem xét mạng OWFD có áp dụng AN và sử dụng các kênh truyền suy hao Rayleigh fading. Hệ thống bao gồm năm nút: nút nguồn, nút đích, nút chuyển tiếp, nút nghe lén và nút gây nhiễu. Để đánh giá hiệu suất bảo mật, tác giả tiến hành phân tích và đánh giá các thông số như: xác suất dừng bảo mật (SOP), thông lượng bảo mật (STP), sự đánh đổi giữa xác suất dừng (OP) và xác suất chặn (IP). Bài báo đã xây dựng các công thức dạng đóng. Kết quả phân tích toán học được kiểm chứng bằng phương pháp mô phỏng Monte-Carlo trên phần mềm MATLAB, thể hiện bằng bốn đồ thị: ảnh hưởng vị trí của nút gây nhiễu nhân tạo lên SOP khi thay đổi giá trị công suất phát tại nút nguồn, vị trí nút nghe lén, giá trị hệ số suy hao đường truyền lên OP, IP và SOP của hệ thống. Đồng thời, cũng đưa ra đồ thị so sánh SOP giữa mô hình đề xuất và tham chiếu. Tất cả các đồ thị đều cho thấy hiệu suất bảo mật được cải thiện đáng kể so với các nghiên cứu trước đây. Mô hình đề xuất chứng minh tính khả thi của việc triển khai các vấn đề PLS trong mạng OWFD.

Doi: https://doi.org/10.54644/jte.2026.2004

JTE
HCM-UTE
ISSN: 1859-1272

TẠP CHÍ KHOA HỌC GIÁO DỤC KỸ THUẬT
Trường Đại học Công nghệ Kỹ thuật Thành phố Hồ Chí Minh
Website: https://jte.edu.vn
Email: jte@hcmute.edu.vn

1. Giới thiệu

Các ứng dụng phổ biến của mạng không dây đã trở thành một phần không thể thiếu trong cuộc sống của chúng ta. Mạng không dây đòi hỏi ngày càng nhiều tài nguyên phổ tần số để hỗ trợ số lượng người sử dụng ngày càng tăng cao [1]. FD cho phép truyền và nhận đồng thời duy nhất trong một kênh thời gian và tần số, hứa hẹn sẽ tăng gấp nhiều lần hiệu suất phổ so với các hệ thống truyền thông bán song công (HD) [2]-[5]. Một trong những mối quan tâm ngày càng tăng của truyền thông không dây là tính bảo mật của tín hiệu được truyền đi. Do mạng không dây có tính chất mở, về bản chất thì thông tin truyền đi không được bảo mật [6]. Sự đơn giản của việc đạt được quyền truy cập vào phương tiện không dây làm cho dễ dàng nghe lén thông tin liên lạc qua phương tiện của thiết bị không hợp pháp [7]. Phương pháp tiếp cận AN– Goel và Negi [8], [9] đã đề xuất một kỹ thuật đảm bảo giao tiếp bảo mật tuyệt đối giữa các nút hợp pháp. Các tác giả đã thiết lập rằng bảo mật hoàn hảo có thể được thực hiện khi kênh của bộ thu bất hợp pháp nhiễu hơn kênh của bộ thu hợp pháp. AN được thêm vào không gian của kênh người nhận hợp pháp [10].

1.1. Công trình liên quan

Tác giả đã phân tích, đánh giá sự đánh đổi độ tin cậy và bảo mật của hệ thống, sử dụng kênh truyền Rayleigh fading, FD và dùng giao thức DF tại nút chuyển tiếp, PLS bằng cách gây AN đến nút nghe lén [11]. Trong [12], tác giả đánh giá SOP và STP của hệ thống, tính toán trên kênh truyền Rayleigh fading, dùng giao thức DF và FD tại nút chuyển tiếp, PLS bằng cách thu thập năng lượng tại nút chuyển tiếp của hệ thống. Nhóm tác giả cũng nghiên cứu, phân tích, đánh giá SOP và IP của hệ thống, kênh truyền Rayleigh fading được dùng trong mô hình, sử dụng giao thức AF và HD tại nút chuyển tiếp [13]. Trong [14], nhóm tác giả phân tích, đánh giá OP và IP của hệ thống, sử dụng kênh truyền Nakagami-m, hệ thống không dùng thiết bị FD, PLS bằng cách dùng bảng phản xạ để chuyển tiếp tín hiệu, vì tín hiệu được truyền thẳng nên không dùng giao thức AF hay DF. Đặc biệt, trong [15], các công thức toán học được áp dung để tính toán và phân tích ra kết quả dạng đóng, được các tác giả trình bày chi tiết [16], tác giả nghiên cứu phần cứng của RIS nhằm PLS một cách tốt nhất, giới thiệu các kịch bản tương ứng, các mô hình hệ thống được xem xét đều không có FD và thiết bị chuyển tiếp, tác giả thảo luận về các hướng nghiên cứu tiềm năng trong tương lai và những thách thức của truyền thông PLS được hỗ trợ bởi RIS. Các nghiên cứu trong nước cũng đã phân tích, đánh giá xác suất dừng, xác suất chặn cho mạng nhận thức, song công khi trạm chuyển tiếp có thu thập năng lượng và dùng kỹ thuật chuyển tiếp kênh [17-19].

Từ các nghiên cứu trên, tác giả của mô hình đề xuất cũng đã đưa ra những vấn đề mở cho nghiên cứu tiếp theo, chẳng hạn như: Đặt thêm thiết bị gây nhiễu vào hệ thống, song công tại thiết bị chuyển tiếp và thiết bị nhận tín hiệu hợp pháp, thêm đường trực tiếp từ thiết bị nguồn đến thiết bị nghe hợp pháp và nghe lén vào mô hình nghiên cứu, thay đổi mô hình kênh truyền và giao thức tại nút chuyển tiếp.

1.2. Đóng góp

Các nghiên cứu trong các công trình liên quan chưa đề cập đến nút đích trong hệ thống và nút ngoài hệ thống gây AN, đồng thời cũng chưa nghiên cứu đường truyền tín hiệu trực tiếp từ nút nguồn đến nút đích cho hệ thống này. Cụ thể là các công trình [11]-[15] tuy đã phân tích, đánh giá sự đánh đổi OP và IP, SOP, STP cho các mô hình bán song công, song công, có nút chuyển tiếp, gây nhiễu từ nút nguồn, kênh truyền Rayleigh fading, Nakagami-m ….

Nghiên cứu đề xuất đã làm giảm thiểu tối đa tỷ số tín hiệu trên nhiễu (SNR) tại nút nghe lén bằng cách gây nhiễu từ nút ngoài hệ thống và nút đích, có đường truyền trực tiếp từ nút nguồn đến nút đích, nhằm tăng cường độ bảo mật và cải thiện tốt hiệu năng bảo mật cho mạng chuyển tiếp OWFD. Mô hình có FD tại nút nghe hợp pháp và nút chuyển tiếp nhằm tiết kiệm băng thông và bảo vệ thông tin hữu ích khi truyền tín hiệu.

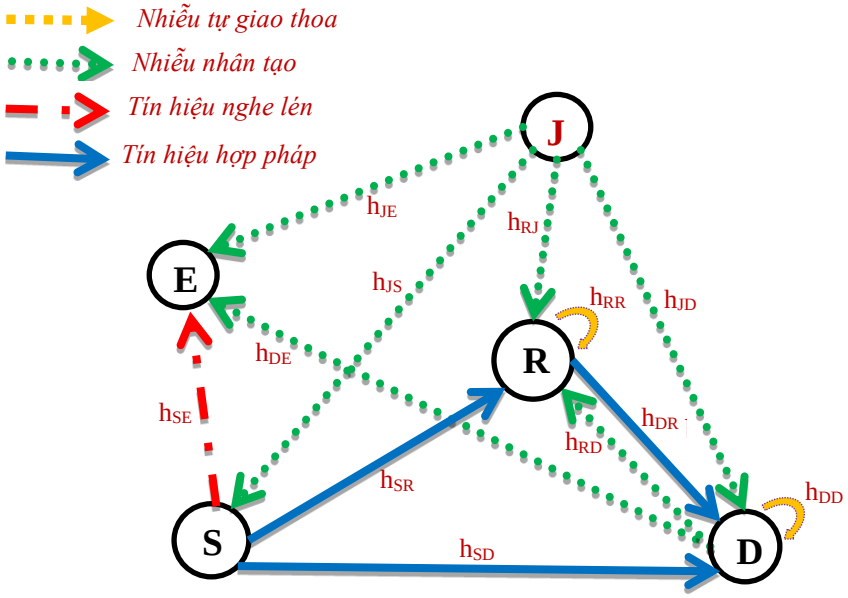
Các vấn đề chính được đóng góp trong bài báo này bao gồm:

Tại nút đích và nút chuyển tiếp sử dụng thiết bị FD nhằm bảo mật thông tin và tiết kiệm băng thông cho mạng chuyển tiếp OWFD. Đồng thời, bài báo đã đề xuất các bộ gây AN ngoài hệ thống và tại nút đích. Rút ra được dạng đóng sau khi phân tích các biểu thức SOP, STP, OP, IP một cách rõ ràng, chính xác cho mạng chuyển tiếp OWFD. Chứng minh một cách hiệu quả việc ảnh hưởng đáng kể đến hiệu năng hệ thống trong việc ngăn chặn thiết bị nghe lén khi có sự tác động của bộ gây AN. Đánh giá, phân tích các biểu thức SOP, STP, OP, IP được chứng minh hoàn toàn chính xác, thông qua việc thực hiện phần mềm Matlab và mô phỏng Monte Carlo.

1.3. Cấu trúc bài báo

Cấu trúc bài báo được chia làm 6 phần: Phần 1 giới thiệu tổng quan các công trình liên quan và sự đóng góp của bài báo. Phần 2 trình bày mô hình hệ thống đang được xem xét. Phần 3 phân tích và đánh giá sự đánh đổi OP và IP. Phần 4 phân tích và cung cấp chi tiết các biểu thức SOP, STP. Phần 5 trình bày kết quả và thảo luận. Phần 6 trình bày kết luận.

2. Mô hình hệ thống



Hình 1. *Mô hình mạng chuyển tiếp song công một chiều có mặt thiết bị nghe lén.*

Hệ thống truyền thông được xem xét bao gồm một nút nguồn S, một nút chuyển tiếp song công R, một nút đích song công D, một nút nghe lén thụ động E và một nút gây nhiễu J, như được mô tả trong Hình 1 của bài báo này. Giả sử rằng S, E và J mỗi nút có một anten duy nhất, trong khi R và D được trang bị hai anten để truyền và nhận tín hiệu. Nút chuyển tiếp R hoạt động theo giao thức DF, nút D nhận tín hiệu đồng thời từ S và R, trong khi nút E chỉ nghe lén tín hiệu từ S. Nút D và J gây nhiễu nhân tạo bằng cách phát đi sóng mang có các tần số khác với những tần số phát ra từ các nút khác trong hệ thống. Đồng thời, giữa nguồn gây nhiễu tại nút D, J và nguồn tin tại nút S, R luôn biết trước trạng thái thông tin kênh truyền với nhau. Giả sử rằng nút E không thể nghe lén tín hiệu từ nút R do các đặc điểm địa hình bị che chắn như cây cối, đồi núi, các tòa nhà cao tầng, v.v…, làm cản trở đường truyền tín hiệu từ nút chuyển tiếp R đến nút E. Cho $u \in \{S-R, S-E, R-D, S-D, D-R, D-E, J-E\}$ thì các hệ số kênh truyền trong hệ thống Rayleigh fading là h_u và được phân phối theo quy luật $h_u \sim CN(0, \lambda_u)$ với $\lambda_u = E\{|h_u|^2\}$ là độ lợi trung bình của kênh truyền u. Cho $v \in \{S, R, D, J\}$ thì công suất phát tại nút v là P_v. Cho $l \in \{R, D, E\}$, nhiễu Gaussian tại nút l là $n_l(t)$ được phân phối theo quy luật $n_l(t) \sim CN(0, \sigma_l)$, phương sai nhiễu Gaussian được chuẩn hóa $\sigma_l^2 = N_0$, SNR tại nút l được ký hiệu là γ_l. Các kênh trong

hệ thống sử dụng mô hình Rayleigh fading nên hàm mật độ xác suất (PDF) và hàm phân bố xác suất (CDF) của độ lợi kênh lần lượt được cho bởi: $f_{|h_u|^2}(x)=\frac{1}{\lambda_u}e^{-\frac{x}{\lambda_u}}$ và $F_{|h_u|^2}(x)=1-e^{-\frac{x}{\lambda_u}}$ với $x>0$.

Giả sử rằng tại thời điểm t, S phát tín hiệu $x_S(t)$ đến R và D. Trong khi đó, D, J gửi tín hiệu gây nhiễu $w_D(t), w_J(t)$ đến S, R và E, sau đó E nghe lén tín hiệu từ R. Việc gửi tín hiệu gây nhiễu nhằm làm giảm SNR tại E, từ đó tăng cường hiệu năng bảo mật cho hệ thống. $w_D(t), w_J(t)$ và $x_S(t)$ được chuẩn hóa sao cho: $E\left\{\left|w_D(t)\right|^2\right\}=E\left\{\left|w_J(t)\right|^2\right\}=E\left\{\left|x_S(t)\right|^2\right\}=1$, trong đó $E\{.\}$ là toán tử kỳ vọng.

Tại thời điểm t, tín hiệu thu được tại R được cho như sau:

$$y_R(t)=h_{SR}\sqrt{P_S}x_S(t)+h_{RR}\sqrt{P_R}x_R(t)+h_{DR}\sqrt{P_D}w_D(t)+h_{JR}\sqrt{P_J}w_J(t)+n_R(t) \quad (1)$$

Vì các can nhiễu nhân tạo có thể biết trước tại R và R có thể khử can nhiễu $h_{JR}w_J(t)$, $h_{DR}w_D(t)$. Do đó, tín hiệu thu được sau khi khử can nhiễu tại R được cho bởi:

$$\tilde{y}_R(t)=h_{SR}\sqrt{P_S}x_S(t)+h_{RR}\sqrt{P_R}x_R(t)+n_R(t) \quad (2)$$

Cũng tại thời điểm t, tín hiệu thu được tại E và D được cho như sau:

$$y_E(t)=h_{SE}\sqrt{P_R}x_R(t)+h_{DE}\sqrt{P_D}w_D(t)+h_{JE}\sqrt{P_J}w_J(t)+n_E(t) \quad (3)$$

$$y_D(t)=h_{SD}\sqrt{P_S}x_S(t)+h_{RD}\sqrt{P_R}x_R(t)+h_{DD}\sqrt{P_D}w_D(t)+h_{JD}\sqrt{P_J}w_J(t)+n_D(t) \quad (4)$$

Vì các can nhiễu nhân tạo có thể biết trước tại D và D có thể khử can nhiễu $h_{JD}w_J(t)$. Do đó, tín hiệu thu được sau khi khử can nhiễu tại D được cho bởi:

$$\tilde{y}_D(t)=h_{SD}\sqrt{P_S}x_S(t)+h_{RD}\sqrt{P_R}x_R(t)+h_{DD}\sqrt{P_D}w_D(t)+n_D(t) \quad (5)$$

Từ (1), (3) và (4), ta có SNR tại các nút R, E và D ở thời điểm t, lần lượt được cho như sau:

SNR tại nút R là:

$$\gamma_R=\frac{|h_{SR}|^2P_S}{|h_{RR}|^2P_R+N_0} \quad (6)$$

SNR tại nút E khi R giải mã $x_S(t)$ thành công, nghĩa là $x_R(t)=x_S(t)$:

$$\gamma_E=\frac{|h_{SE}|^2P_R}{|h_{DE}|^2P_D+|h_{JE}|^2P_J+N_0} \quad (7)$$

Vì giữa 2 nút R và E bị che chắn bởi địa hình như tác giả đã nêu trong mô hình, nên cho dù nút R có giải mã thành công hay bị lỗi thì đều không chuyển tiếp tín hiệu đến nút E được. Do vậy, SNR tại nút E khi giải mã $x_S(t)$ bị lỗi cũng bằng chính SNR tại nút E khi giải mã $x_S(t)$ thành công:

$$\gamma_E^*=\frac{|h_{SE}|^2P_R}{|h_{DE}|^2P_D+|h_{JE}|^2P_J+N_0}=\gamma_E \quad (8)$$

SNR tại nút D khi R giải mã $x_S(t)$ thành công, nghĩa là $x_R(t)=x_S(t)$:

$$\tilde{\gamma}_D = \frac{\left|h_{SD}P_S + h_{RD}P_R\right|^2}{\left|h_{DD}\right|^2 P_D + N_0} \le \gamma_D = \frac{\left|h_{SD}\right|^2 P_S + \left|h_{RD}\right|^2 P_R}{\left|h_{DD}\right|^2 P_D + N_0} \tag{9}$$

SNR tại nút D khi R giải mã $x_S(t)$ bị lỗi, nghĩa là $x_R(t) \neq x_S(t)$:

$$\gamma_D^* = \frac{\left|h_{SD}\right|^2 P_S}{\left|h_{RD}\right|^2 P_R + \left|h_{DD}\right|^2 P_D + N_0} \tag{10}$$

3. Phân tích hiệu năng bảo mật

SOP của hệ thống được đưa ra. Dung lượng bảo mật được định nghĩa là độ lệch giữa dung lượng kênh hợp pháp và dung lượng kênh nghe lén.

$$C_S = \left[C_D - C_E\right]^+ = \frac{1}{2}\left[\log_2 \frac{1+\gamma_D}{1+\gamma_E}\right]^+ \tag{11}$$

trong đó C_S , C_D và C_E lần lượt là dung lượng bảo mật của hệ thống, dung lượng nhận tín hiệu hợp pháp tại D và dung lượng nghe lén tín hiệu tại E, $\left[x\right]^+ = max(x,0)$.

Định lý 1: CDF và PDF của γ_R được cho bởi

$$F_{\gamma_R}(x) = 1 - a_0 \frac{e^{-b_0 x}}{a_0 + x} \tag{12}$$

$$f_{\gamma_R}(x) = \frac{a_0 b_0 e^{-b_0 x}}{a_0 + x} + \frac{a_0 e^{-b_0 x}}{(a_0 + x)^2} \tag{13}$$

trong đó, $a_0 = \frac{\lambda_{SR} P_S}{\lambda_{RR} P_R}$; $b_0 = \frac{N_0}{\lambda_{SR} P_S}$

Chứng minh:

Từ công thức (6) CDF của γ_R được cho bởi

$$F_{\gamma_R}(x) = \Pr\left(\frac{\left|h_{SR}\right|^2 P_S}{\left|h_{RR}\right|^2 P_R + N_0} < x\right) = \Pr\left(\frac{x_0 P_S}{x_1 P_R + N_0} < x\right) = 1 - a_0 \frac{e^{-b_0 x}}{a_0 + x} \tag{14}$$

trong đó, $x_0 = \left|h_{SR}\right|^2$ và $x_1 = \left|h_{RR}\right|^2$.

Từ (14), PDF của γ_R là đạo hàm bậc nhất của $F_{\gamma_R}(x)$, được tính như sau:

$$f_{\gamma_R}(x) = -a_0 \frac{-b_0 e^{-b_0 x}(a_0 + x) - e^{-b_0 x}}{(a_0 + x)^2} = \frac{a_0 b_0 e^{-b_0 x}}{a_0 + x} + \frac{a_0 e^{-b_0 x}}{(a_0 + x)^2} \tag{15}$$

Định lý 2: CDF của γ_D được cho bởi

$$F_{\gamma_D}(y) = 1 - \frac{e^{-a_1 y}}{b_1(y + c_1)}\left(1 + \frac{1}{d_1}\right) + \frac{e^{-f_1 y}}{e_1 d_1 (y + g_1)} \tag{16}$$

trong đó,

$$a_1=\frac{N_0}{\lambda_{RD}P_R};\ b_1=\frac{\lambda_{DD}P_D}{\lambda_{RD}P_R};\ c_1=\frac{\lambda_{RD}P_R}{\lambda_{DD}P_D};\ d_1=\lambda_{RD}\left(\frac{P_R}{P_S\lambda_{SD}}-\frac{1}{\lambda_{RD}}\right);\ e_1=\frac{\lambda_{DD}P_D}{P_S\lambda_{SD}};\ f_1=\frac{N_0}{P_S\lambda_{SD}};\ g_1=\frac{P_S\lambda_{SD}}{\lambda_{DD}P_D}.$$

Chứng minh:

Khi R giải mã thành công, ta có:

$$F_{\gamma_D}(y)=\Pr\left(\frac{|h_{SD}|^2P_S+|h_{RD}|^2P_R}{|h_{DD}|^2P_D+N_0}<y\right)=\Pr\left(\frac{Q}{|h_{DD}|^2P_D+N_0}<y\right) \quad (17)$$

trong đó, $Q=|h_{SD}|^2P_S+|h_{RD}|^2P_R$

Cho nên,

$$F_Q(q)=\Pr(Q<q)=1-e^{-\frac{q}{\lambda_{RD}P_R}}-\frac{e^{-\frac{q}{\lambda_{RD}P_R}}}{\lambda_{RD}\left(\frac{P_R}{P_S\lambda_{SD}}-\frac{1}{\lambda_{RD}}\right)}+\frac{e^{-\frac{q}{P_S\lambda_{SD}}}}{\lambda_{RD}\left(\frac{P_R}{P_S\lambda_{SD}}-\frac{1}{\lambda_{RD}}\right)} \quad (18)$$

Do đó,

$$F_{\gamma_D}(y)=\Pr\left(Q<y\left(|h_{DD}|^2P_D+N_0\right)\right)=1-\frac{e^{-a_1y}}{b_1(y+c_1)}\left(1+\frac{1}{d_1}\right)+\frac{e^{-f_1y}}{e_1d_1(y+g_1)} \quad (19)$$

trong đó, $y_0=|h_{DD}|^2$.

Định lý 3: CDF của γ_D^* được cho bởi

Khi R giải mã bị lỗi, ta có:

$$F_{\gamma_D^*}(z)=\Pr\left(\frac{|h_{SD}|^2P_S}{|h_{RD}|^2P_R+|h_{DD}|^2P_D+N_0}<z\right)=\Pr\left(\frac{z_0P_S}{z_1P_R+z_2P_D+N_0}<z\right)=1-\frac{1}{a_3}\left(\frac{e^{-b_3z}}{z+c_3}-\frac{e^{-b_3z}}{z+d_3}\right) \quad (20)$$

trong đó, $z_0=|h_{SD}|^2$, $z_1=|h_{RD}|^2$ và $z_2=|h_{DD}|^2$.

$$a_3=\frac{\lambda_{RD}P_R}{\lambda_{SD}P_S}-\frac{\lambda_{DD}P_D}{\lambda_{SD}P_S};\mathrm{b}_3=\frac{N_0}{\lambda_{SD}P_S};\mathrm{c}_3=\frac{\lambda_{SD}P_S}{\lambda_{RD}P_R};d_3=\frac{\lambda_{SD}P_S}{\lambda_{DD}P_D}$$

Định lý 4: CDF và PDF của γ_E được cho bởi

$$F_{\gamma_E}(t)=1-\frac{1}{b_2}\left(\frac{e^{-a_2t}}{(t+c_2)}-\frac{e^{-a_2t}}{(t+d_2)}\right) \quad (21)$$

Và

$$f_{\gamma_E}(t)=\frac{1}{b_2}\left(\frac{a_2e^{-a_2t}}{(t+c_2)}+\frac{e^{-a_2t}}{(t+c_2)^2}-\frac{a_2e^{-a_2t}}{(t+d_2)}-\frac{e^{-a_2t}}{(t+d_2)^2}\right) \quad (22)$$

trong đó, $a_2=\frac{N_0}{\lambda_{SE}P_R}$, $b_2=\frac{\lambda_{DE}P_D}{\lambda_{SE}P_R}-\frac{\lambda_{JE}P_J}{\lambda_{SE}P_R}$, $c_2=\frac{\lambda_{SE}P_R}{\lambda_{DE}P_D}$, và $d_2=\frac{\lambda_{SE}P_R}{\lambda_{JE}P_J}$.

Chứng minh:

Phân tích công thức (7), ta có CDF của γ_E bằng cách áp dụng ([16], eq. (3.352.4) and eq. (3.353.3)).

$$F_{\gamma_E}(t)=\Pr\left(\frac{|h_{SE}|^2 P_R}{|h_{DE}|^2 P_D+|h_{JE}|^2 P_J+N_0}<t\right)=\Pr\left(\frac{t_0 P_R}{t_1 P_D+t_2 P_J+N_0}<t\right)=1-\frac{1}{b_2}\left(\frac{e^{-a_2 t}}{t+c_2}-\frac{e^{-a_2 t}}{t+d_2}\right) \quad (23)$$

trong đó $t_0=|h_{SE}|^2$, $t_1=|h_{DE}|^2$ và $t_2=|h_{JE}|^2$.

Từ công thức (23), PDF của γ_E là đạo hàm bậc nhất của $F_{\gamma_E}(t)$, được tính như sau:

$$f_{\gamma_E}(t)=\frac{1}{b_2}\left(\frac{a_2 e^{-a_2 t}}{t+c_2}+\frac{e^{-a_2 t}}{(t+c_2)^2}-\frac{a_2 e^{-a_2 t}}{t+d_2}-\frac{e^{-a_2 t}}{(t+d_2)^2}\right) \quad (24)$$

Định lý 5: CDF và PDF của γ_E^* được cho bởi

Khi R giải mã bị lỗi (E cũng không phụ thuộc vào R), ta có:

$$F_{\gamma_E^*}(t)=F_{\gamma_E}(t) \quad (25)$$

và

$$f_{\gamma_E^*}(t)=f_{\gamma_E}(t) \quad (26)$$

Chứng minh:

Vì khi R giải mã bị lỗi, thì E vẫn chỉ nghe lén tín hiệu từ S. Nên tỷ số tín hiệu trên nhiễu tại E lúc này, bằng tỷ số tín hiệu trên nhiễu chính nó khi R giải mã thành công. Nghĩa là:

$$F_{\gamma_E^*}(t)=\Pr\left(\frac{|h_{SE}|^2 P_R}{|h_{DE}|^2 P_D+|h_{JE}|^2 P_J+N_0}<t\right)=F_{\gamma_E}(t) \quad (27)$$

Từ đó, suy ra:

$$f_{\gamma_E^*}(t)=\frac{1}{b_2}\left(\frac{a_2 e^{-a_2 t}}{t+c_2}+\frac{e^{-a_2 t}}{(t+c_2)^2}-\frac{a_2 e^{-a_2 t}}{t+d_2}-\frac{e^{-a_2 t}}{(t+d_2)^2}\right)=f_{\gamma_E}(t) \quad (28)$$

3.1. Xác suất dừng bảo mật của hệ thống

SOP của hệ thống là xác suất xảy ra khi và chỉ khi dung lượng bảo mật nhỏ hơn một ngưỡng cho trước và được cho bởi:

$$SOP=\Pr(C_S<C_{th}) \quad (29)$$

trong đó C_S là dung lượng bảo mật của hệ thống, C_{th} là ngưỡng cho trước của dung lượng tại nút nghe hợp pháp.

Áp dụng công thức (18) cho mô hình đang xem xét, khi nút R giải mã thành công và bị lỗi, xác suất dừng bảo mật lần lượt được tính như sau:

$$SOP_{Nerror}=\Pr\left(C_S^{Nerror}<C_{th}\right)=F_{\gamma_D}\left(2^{C_{th}}\gamma_E+2^{C_{th}}-1\right) \quad (30)$$

$$SOP_{Error}=\Pr\left(C_S^{Error}<C_{th}\right)=F_{\gamma_D^*}\left(2^{C_{th}}\gamma_E^*+2^{C_{th}}-1\right) \quad (31)$$

Do đó, SOP của hệ thống được cho bởi:

$$\begin{aligned} SOP &= SOP_{Nerror}\,\Pr\left(\gamma_R \geq 2^{C_{th}}-1\right)+SOP_{Error}\,\Pr\left(\gamma_R < 2^{C_{th}}-1\right) \\ &= SOP_{Nerror}\left(1-F_{\gamma_R}\left(2^{C_{th}}-1\right)\right)+SOP_{Error}F_{\gamma_R}\left(2^{C_{th}}-1\right) \end{aligned} \quad (32)$$

3.2. Thông lượng bảo mật của hệ thống

Thông lượng bảo mật của hệ thống chính là tích của tốc độ bảo mật với xác suất hoạt động bảo mật của hệ thống và được xác định như sau:

$$STP = R_s(1-SOP)\ \ (\text{bit/s/Hz}) \quad (33)$$

trong đó STP thông lượng bảo mật của hệ thống, R_S tốc độ bảo mật của hệ thống, SOP xác suất dừng bảo mật của hệ thống.

4. Phân tích, đánh giá sự đánh đổi độ tin cậy và bảo mật

4.1. Độ tin cậy

Độ tin cậy chính là xác suất dừng của hệ thống hay xác suất mà dung lượng Shannon của kênh dữ liệu nhỏ hơn một ngưỡng xác định trước, được định nghĩa:

$$\text{OP} = \Pr\left(C_D < C_{th}\right) \quad (34)$$

Áp dụng công thức (30), sau đó lần lượt thế $y = z = 2^{C_{th}}-1$ vào (16) và (20) cho mô hình đang xem xét, khi nút R giải mã thành công và bị lỗi, xác suất dừng của hệ thống lần lượt được tính như sau:

$$OP_{Nerror} = \Pr\left(C_D^{Nerror} < C_{th}\right) = 1-\frac{e^{-a_1\left(2^{C_{th}}-1\right)}}{b_1\left(2^{C_{th}}-1+c_1\right)}\left(1+\frac{1}{d_1}\right)+\frac{e^{-f_1\left(2^{C_{th}}-1\right)}}{e_1 d_1\left(2^{C_{th}}-1+g_1\right)} \quad (35)$$

$$OP_{Error} = \Pr\left(C_S^{Error} < C_{th}\right) = 1-\frac{1}{a_3}\left(\frac{e^{-b_3\left(2^{C_{th}}-1\right)}}{2^{C_{th}}-1+c_3}-\frac{e^{-b_3\left(2^{C_{th}}-1\right)}}{2^{C_{th}}-1+d_3}\right) \quad (36)$$

Do đó, OP của hệ thống được cho bởi:

$$\begin{aligned} OP &= OP_{Nerror}\,\Pr\left(\gamma_R \geq 2^{C_{th}}-1\right)+OP_{Error}\,\Pr\left(\gamma_R < 2^{C_{th}}-1\right) \\ &= OP_{Nerror}\left(1-F_{\gamma_R}\left(2^{C_{th}}-1\right)\right)+OP_{Error}F_{\gamma_R}\left(2^{C_{th}}-1\right) \end{aligned} \quad (37)$$

4.2. Độ bảo mật

Xác suất chặn (IP) hay xác suất nút nghe lén giải mã thành công dữ liệu nghe lén mà dung lượng Shannon của kênh nghe lén dữ liệu lớn hơn hoặc bằng một ngưỡng xác định trước, được định nghĩa:

$$\text{IP} = \Pr\left(C_E \geq C_{th}\right) = 1-\Pr\left(C_E < C_{th}\right) \quad (38)$$

Áp dụng công thức (34), sau đó thế $t = 2^{C_{th}}-1$ vào (21) cho mô hình đang xem xét, khi nút R giải mã thành công và bị lỗi, xác suất chặn của hệ thống lần lượt được tính như sau:

$$IP_{Nerror} = 1-\Pr\left(C_E^{Nerror} < C_{th}\right) = \frac{1}{b_2}\left(\frac{e^{-a_2\left(2^{C_{th}}-1\right)}}{\left(2^{C_{th}}-1+c_2\right)}-\frac{e^{-a_2\left(2^{C_{th}}-1\right)}}{\left(2^{C_{th}}-1+d_2\right)}\right) \quad (39)$$

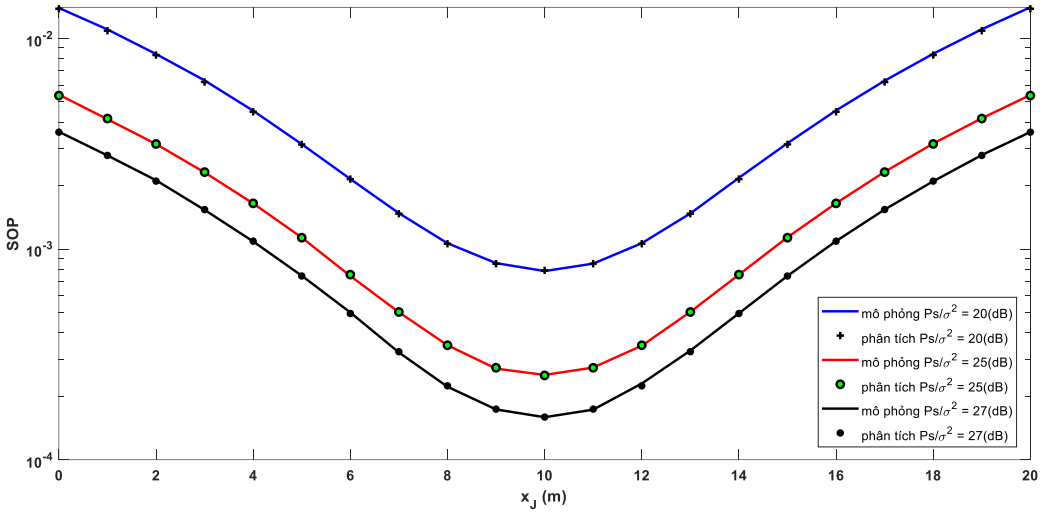
$$IP_{Error} = 1 - \Pr\left(C_E^{Error} < C_{th}\right) = IP_{Nerror} \tag{40}$$

Do đó, IP của hệ thống được cho bởi:

$$IP = IP_{Nerror} \Pr\left(\gamma_R \geq 2^{C_{th}} - 1\right) + IP_{Error} \Pr\left(\gamma_R < 2^{C_{th}} - 1\right) = IP_{Nerror} = IP_{Error} \tag{41}$$

5. Kết quả và thảo luận

Các kết quả số và mô phỏng để xác minh các biểu thức SOP, STP được đề xuất, đánh giá hiệu năng bảo mật của mạng chuyển tiếp OWFD được trình bày trong phần này. Sử dụng kênh truyền Rayleigh fading trong mô hình. SOP, STP, OP và IP được đánh giá trong các thông số vận hành chính, chẳng hạn như vị trí của nút E và J, số mũ suy hao đường truyền β, ngưỡng cho trước của dung lượng $C_{th} = \{0.01, 0.05, 0.1\}$ $(b/s/Hz)$. Để minh họa bài toán, tọa độ người dùng được chọn là S tại $(0.0,0.0)$, D tại $(8.0,8.0)$, R tại $(5.0,4.0)$, E tại $(10.0,14.0)$, J tại $(8.0,20.0)$, đặt x_S, x_D, x_E, x_J và y_S, y_D, y_E, y_J lần lượt là hoành độ và tung độ của S, D, E, J. Ngoài ra, $P_S = 20(dB)$, $P_R = -25(dB)$, $P_D = -25(dB)$, $P_J = 1(dB)$ cũng được thông qua. Tính toán suy hao đường truyền, công suất fading được mô hình hóa $d^{-\beta}$ với d là khoảng cách từ máy phát đến máy thu. Trong tất cả các kết quả thì có một kết quả xem xét cho tùy môi trường truyền dẫn nên giá trị β được chọn chạy từ 2 đến 6 và các kết quả còn lại đều được chọn $\beta = 3$.

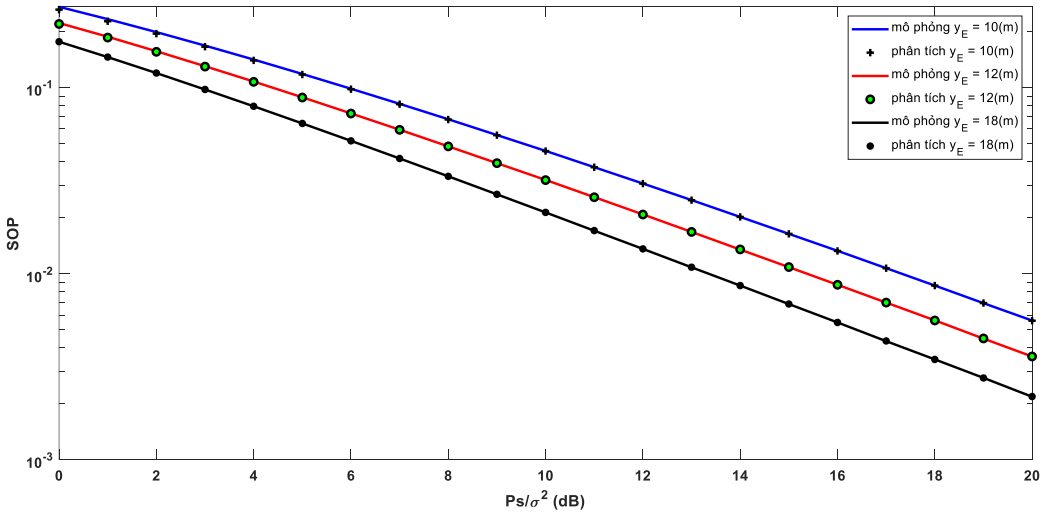


Hình 2. *Ảnh hưởng vị trí của nút J lên SOP khi thay đổi giá trị* P_S/σ^2.

Hình 2 mô tả ảnh hưởng vị trí của nút J lên SOP tại ba giá trị khác nhau của P_S/σ^2 với $P_S/\sigma^2 = \{20,25,27\}$ (dB), $C_{th} = 0.01$ $(b/s/Hz)$. Hình này cho thấy sự trùng khớp giữa mô phỏng và phân tích, xác thực các biểu thức SOP được đề xuất. Ta thấy rằng, khoảng cách nút J tăng từ 0 đến 10 mét thì SOP giảm dần đến cực tiểu, tiếp đó, khoảng cách nút J tăng từ 10 đến 20 mét thì SOP tăng dần từ giá trị cực tiểu. Điều này được lý giải như sau, nút J càng gần nút E thì công suất nhiễu tại nút E càng tăng, nên SOP càng giảm và ngược lại. Do đó, tại vị trí của nút J có hoành độ là 10 mét thì nút gần nút E nhất, lúc này, SOP đạt giá trị cực tiểu. Mặt khác, khi P_S/σ^2 càng tăng thì SNR tại E càng tăng và tỷ lệ tăng chậm hơn SNR tại D vì nút E nhận bốn kênh, trong đó có hai kênh phát nhiễu, do đó các thành phần nhiễu này làm giảm độ tăng của SNR tại E, nên c_s càng tăng, vì thế, SOP càng giảm.

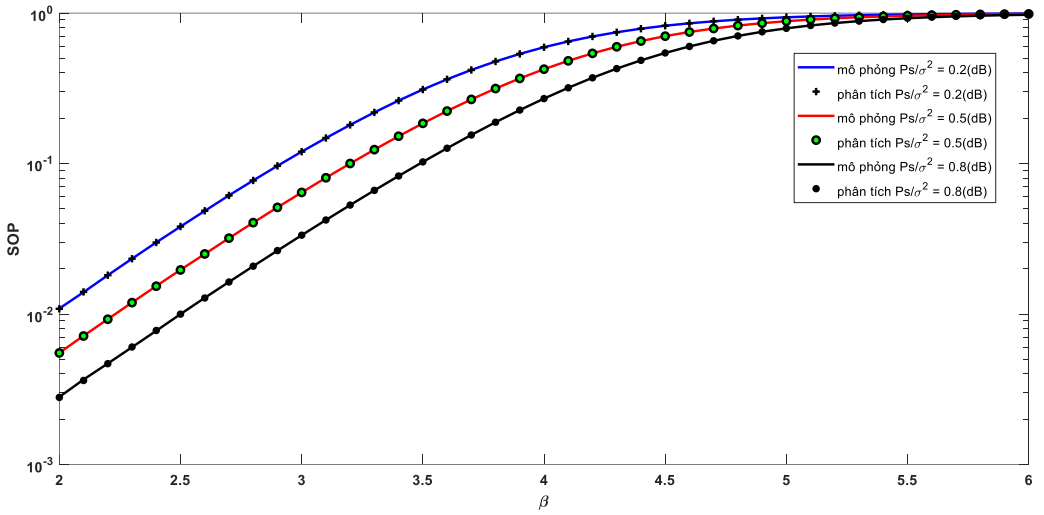
JTE
HCM-UTE
ISSN: 1859-1272

TẠP CHÍ KHOA HỌC GIÁO DỤC KỸ THUẬT
Trường Đại học Công nghệ Kỹ thuật Thành phố Hồ Chí Minh
Website: https://jte.edu.vn
Email: jte@hcmute.edu.vn



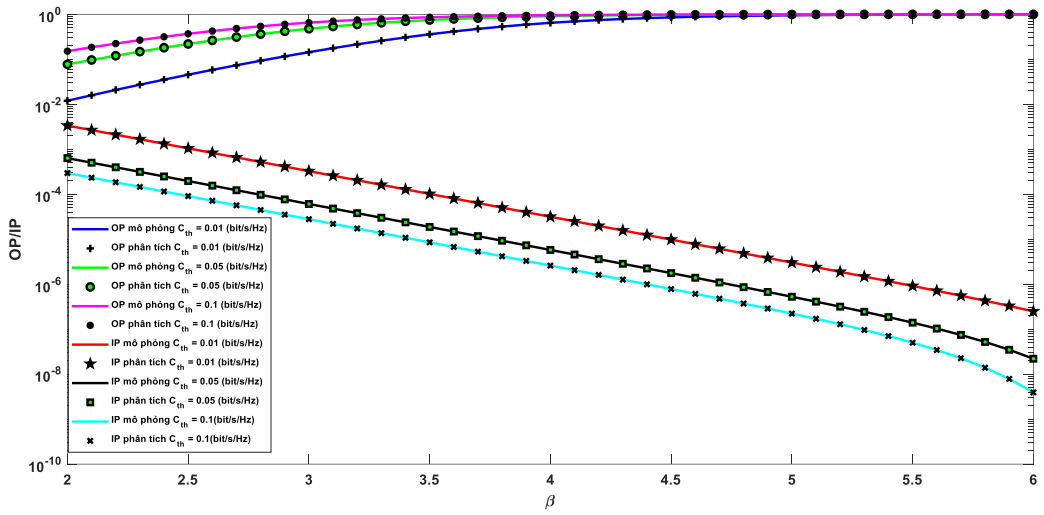
Hình 3. *Ảnh hưởng giá trị* P_S/σ^2 *lên* SOP *khi thay đổi vị trí của nút nghe lén E.*

Hình 3 mô tả ảnh hưởng giá trị P_S/σ^2 lên SOP khi thay đổi vị trí nút nghe lén E. Đồ thị cho thấy sự trùng khớp giữa mô phỏng và phân tích. Công suất phát nút S là P_S/σ^2 càng tăng thì SNR tại nút R, D càng tăng, từ đó độ bảo mật của hệ thống càng tăng, hay nói cách khác là SOP càng giảm, vì SNR tại nút D càng tăng, nghĩa là dung lượng bảo mật của hệ thống càng tăng, dẫn đến SOP càng giảm. Mặt khác, tung độ nút nghe lén E là y_E càng lớn thì SNR tại E càng giảm, trong khi đó không gây ảnh hưởng đến SNR tại D, nên C_S càng tăng, từ đó, làm cho SOP của hệ thống càng giảm.



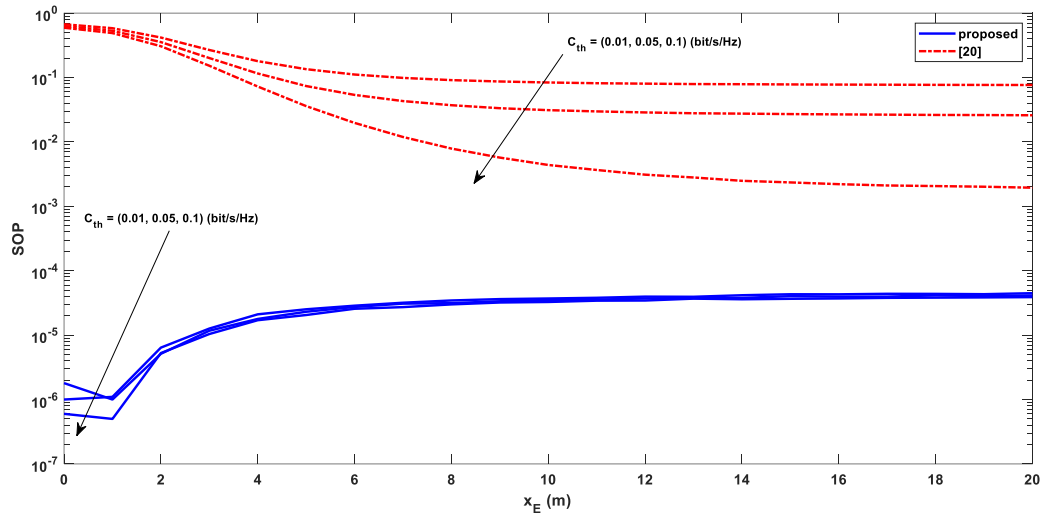
Hình 4. *Ảnh hưởng của* β *lên SOP khi thay đổi giá trị* P_S/σ^2 .

Hình 4 mô tả ảnh hưởng β lên SOP, hình này cũng đã cho thấy sự trùng khớp giữa mô phỏng và phân tích. Ta nhận thấy rõ rằng, β càng tăng thì công suất nhiễu nhận tại nút E và nút D càng tăng, nhưng công suất nhiễu nhận tại nút E tăng chậm hơn tại D, vì giá trị nhiễu tại nút E lớn hơn tại nút D. Từ đó, SNR tại nút E càng tăng, dẫn đến C_S càng giảm, nên SOP càng tăng. Kết quả mô phỏng cho thấy rõ, tại $\beta = 2$ thì SOP đạt cực tiểu. Mặt khác, P_S/σ^2 càng tăng thì SOP càng giảm, lý do là công suất nhiễu nhận tại nút D tăng nhanh hơn tại E, dẫn đến C_S càng tăng, nên SOP của hệ thống càng giả.



Hình 5. *Ảnh hưởng của* β *lên OP và IP tại 3 giá trị ngưỡng* C_{th}.

Hình 5 mô tả ảnh hưởng vị trí nút nguồn β lên OP và IP, đồ thị này cũng đã cho thấy sự trùng khớp giữa mô phỏng và phân tích. Khi β càng tăng thì OP càng tăng và IP càng giảm. Điều này được lý giải một cách dễ dàng, β càng tăng thì SNR tại D càng thấp và SNR tại E càng cao, từ đó dẫn đến OP càng cao và IP càng thấp. Hơn nữa, giá trị ngưỡng cho trước C_{th} càng tăng thì thì OP càng tăng, còn IP càng giảm, điều này được chứng minh từ định nghĩa của OP và IP. Từ sự đánh giá và phân tích cho Hình 5 ta thấy rõ được rằng khi OP tăng thì IP giảm và ngược lại. Trong mô hình đề xuất này, OP và IP luôn luôn đối ngược lại với nhau. Hay nói cách khác, được OP thì mất IP và ngược lại. Như vậy, giữa OP và IP có sự đánh đổi cho nhau. Nghĩa là, luôn tồn tại việc đánh đổi giữa độ tin cậy và bảo mật trong hệ thống đã xem xét.



Hình 6. *SOP của mô hình tham chiếu và mô hình đề xuất khi thay đổi vị trí nút* E.

Hệ thống tham chiếu [20] bao gồm năm nút, trong đó có một nút phản xạ tín hiệu nhận được từ nút nguồn và nút chuyển tiếp, dùng kênh truyền Rayleigh fading, kỹ thuật bán song công và giao thức DF tại nút chuyển tiếp, mô hình nghiên cứu OP và hiệu suất năng lượng bảo mật, cải thiện hệ thống bảo mật bằng bảng phản xạ thông minh.

Hình 6 mô tả đường mô phỏng nhằm so sánh SOP giữa mô hình tham chiếu và đề xuất. Hệ thống tham chiếu gồm năm nút: S, R, D, E và B (nút B phản xạ tín hiệu), trong khi đó, hệ thống đề xuất gồm năm nút: S, R, D, E và J (nút D và nút J gây nhiễu). Khi so sánh hiệu năng thì vị trí của các nút tương

ứng trong hai mô hình là bằng nhau, nút S(0.0, 0.0), R(0.5, 0.4), D(1.0, 0.2), E(x_E, 1.8) và mô hình đề xuất có thêm nút J(0.5, 2.0), mô hình tham chiếu có thêm nút B(0.5, 0.8). Khi so sánh, tác giả cho tổng công suất phát của hệ thống trong hai mô hình bằng nhau, cụ thể tổng công suất phát của hai hệ thống bằng 101,36 *(W)*. Kết quả cho thấy các đường mô phỏng SOP của mô hình đề xuất thấp hơn nhiều so với các đường SOP trong mô hình tham chiếu, hay nói cách khác hiệu năng của mô hình đề xuất nổi trội hơn so với mô hình tham chiếu.

6. Kết luận

Mô hình bài toán đã đưa ra một giao thức kết hợp gây AN cho hệ thống OWFD. AN được phát đi từ S và D nhằm bảo vệ thông tin tại R và làm giảm dung lượng tín hiệu mà E nhận được, từ đó làm tăng độ tin cậy R và cải thiện được c_s của hệ thống. Phân tích cho thấy rõ gây nhiễu luôn hiệu quả hơn nhiều so với không gây nhiễu cho hệ thống. Kết quả đồng thời cho thấy rằng SNR càng cao thì SOP của hệ thống càng thấp và dẫn đến STP của hệ thống càng cao. IP và OP của hệ thống đều phụ thuộc vào các thông số hệ thống, chứng tỏ chúng có mối tương quan. Hơn nữa, qua việc phân tích IP và OP đã cho thấy chúng tỷ lệ nghịch với nhau khi thay đổi các thông số của hệ thống, điều này minh chứng hệ thống có sự đánh đổi giữa độ tin cậy và bảo mật. Bằng cách sử dụng công cụ phần mềm Matlab và phương pháp mô phỏng Monte-Carlo đã thể hiện tính chính xác của việc phân tích các bài toán trong hệ thống thông qua sự trùng khớp giữa đường mô phỏng và đường phân tích. Ngoài ra, kết quả đã cho được sự lựa chọn giá trị hệ số phân chia công suất và ngưỡng dung lượng cho trước để hiệu năng bảo mật hệ thống được tốt nhất. Kết quả cũng đã đánh giá β ảnh hưởng đến SOP của hệ thống.

Lời cám ơn

Tác giả xin gửi lời cám ơn đến các Phòng, Ban, Khoa, cá nhân (Đặc biệt là Ban Quản Lý Khoa Học, Khoa Kỹ Thuật Công Nghệ) Trường Đại Học Văn Hiến đã đóng góp, tài trợ cho nghiên cứu. Công trình này thuộc "Đề tài nghiên cứu khoa học cấp trường năm 2025, được tài trợ kinh phí bởi Trường Đại Học Văn Hiến".

Xung đột lợi ích

Tác giả tuyên bố không có xung đột lợi ích trong bài báo này.

TÀI LIỆU THAM KHẢO

[1] C. Chen, S. J. Baek, R. Yin, S. Yang, X. Yu, and C. Li, "Practical and efficient coded transmission for full-duplex relay networks without CSI," *IEEE/ACM Trans. Netw.*, vol. 32, no. 3, pp. 2721–2735, Jun. 2024, doi: 10.1109/TNET.2024.3366697.

[2] J. T. Lim, T. Kim, and I. Bang, "Impact of outdated CSI on the secure communication in untrusted in-band full-duplex relay networks," *IEEE Access*, vol. 10, pp. 19825–19835, 2022, doi: 10.1109/ACCESS.2022.3151792.

[3] M. H. Khoshafa, T. M. N. Ngatched, M. H. Ahmed, and A. Ibrahim, "Improving physical layer security of cellular networks using full-duplex jamming relay-aided D2D communications," *IEEE Access*, vol. 8, pp. 53575–53586, 2020, doi: 10.1109/ACCESS.2020.2979848.

[4] X. Pei, H. Yu, M. Wen, Q. Li, and Z. Ding, "Secure outage analysis for cooperative NOMA systems with antenna selection," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4503–4507, Apr. 2020, doi: 10.1109/TVT.2020.2973726.

[5] C. Chen, S. J. Baek, R. Yin, S. Yang, X. Yu, and C. Li, "Practical and efficient coded transmission for full-duplex relay networks without CSI," *IEEE/ACM Trans. Netw.*, vol. 32, no. 3, pp. 2721–2735, Jun. 2024, doi: 10.1109/TNET.2024.3366697.

[6] I. Zabir, A. Maksud, G. Chen, B. M. Sadler, and Y. Hua, "Secrecy of multi-antenna transmission with full-duplex user in the presence of randomly located eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2060–2075, 2021, doi: 10.1109/TIFS.2020.3047763.

[7] F. U. Din and F. Labeau, "Artificial noise assisted in-band full-duplex secure channel estimation," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 6800–6813, Jul. 2021, doi: 10.1109/TVT.2021.3082810.

[8] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *Proc. IEEE MILCOM*, Atlantic City, NJ, USA, 2005, vol. 3, pp. 1501–1506, doi: 10.1109/MILCOM.2005.1605889.

[9] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008, doi: 10.1109/TWC.2008.060848.

[10] X. Zhang, D. Chen, J. Li, and Z. Wang, "Security-reliability tradeoff analysis of untrusted full-duplex relay networks," *Wireless Commun. Mobile Comput.*, Art. no. 2419430, pp. 1–12, Jul. 2022, doi: 10.1155/2022/2419430.

[11] Z. Cao *et al*., "Security-reliability trade-off analysis of AN-aided relay selection for full-duplex relay networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2362–2377, Mar. 2021, doi: 10.1109/TVT.2021.3057830.

[12] I. W. G. D. Silva, J. D. V. Sánchez, E. E. B. Olivo, and D. P. Moya Osorio, "Impact of self-energy recycling and cooperative jamming on SWIPT-based FD relay networks with secrecy constraints," *IEEE Access*, vol. 10, pp. 24132–24148, 2022, doi: 10.1109/ACCESS.2022.3155498.

[13] K. Venugopalachary, D. Mishra, and R. Saini, "Exact outage analysis for non-regenerative secure cooperation against double-tap eavesdropping," *Infocommunications J.*, vol. 14, no. 4, pp. 42–48, Jan. 2022, doi: 10.36244/ICJ.2022.4.6.

[14] J. Sun, X. Chuai, Y. Zeng, and X. Li, "Secrecy analysis and prediction of ambient backscatter NOMA systems with I/Q imbalance," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 2980–2990, 2024, doi: 10.1109/OJCOMS.2024.3395702.
[15] M. Guo *et al*., "Inspiring physical layer security with RIS: Principles, applications, and challenges," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 2903–2925, 2024, doi: 10.1109/OJCOMS.2024.3392359.
[16] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 6th ed. San Diego, CA, USA: Academic Press, 2000.
[17] N. A. Tuan, V. N. Q. Bao, "Phân tích xác suất dừng hệ thống vô tuyến nhận thức sử dụng kỹ thuật thu thập năng lượng vô tuyến", *Tạp chí Khoa học công nghệ Thông tin và Truyền thông,* no. 3&4, pp. 26-33, 2019. (in Vietnamese).
[18] N. A. Tuan, V. N. Q. Bao, "Performance analysis of energy harvesting full duplex relay system with power beacon," *Tạp chí Khoa học Công nghệ - Đại học Đà Nẵng*, vol 18, no 5.1, pp. 70-74, 2020 (in Vietnamese).
[19] T. A. Ngo, H. M. T. Tran, H. T. Pham, and N. T. Le, "Improving the operation of relay stationsto maintain the connections for handover calls in 4g lte system by channel relaying strategy," *Transport and Communications Science Journal*, vol. 73, no. 5, pp. 526–539, 2022 (in Vietnamese).
[20] X. Li *et al*., "Physical layer security for wireless-powered ambient backscatter cooperative communication networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 9, no. 4, pp. 927–939, 2023, doi: 10.1109/TCCN.2023.3270425.

Quoc Bao Ho received his Master's degree in Telecommunication Engineering in 2016 from the University of Transport and Communications, Hanoi, Vietnam, and another Master's degree in Environmental Resource Management in 2018 from Ho Chi Minh City University of Technology, Vietnam. Through his academic training and research activities, he has authored several national papers and contributed as a co-author to international publications. From 2015 to 2022, he was a lecturer at Thu Duc College of Technology, Ho Chi Minh City, Vietnam. Since 2023, he has been a lecturer at Van Hien University. His current research focuses on performance evaluation and analysis of full-duplex wireless communication systems, including physical layer security, outage probability, intercept probability, secrecy outage probability, and artificial noise techniques. Phone: +84 988 765 049. Address: 418/17/4 Le Van Tho Street, An Hoi Dong Ward, Ho Chi Minh City.

Email: baohq@vhu.edu.vn. ORCID: https://orcid.org/0009-0003-2063-4844