PHÂN TÍCH HIỆU NĂNG MẠNG VÔ TUYẾN ĐA TRUY CẬP KHÔNG TRỰC GIAO THU THẬP NĂNG LƯỢNG VỚI THIẾT BỊ GÂY NHIỄU

Đỗ Đắc Thiểm[(1)]
(1) Trường Đại học Thủ Dầu Một
Ngày nhận bài 21/01/2025; Chấp nhận đăng 02/02/2025
Liên hệ email: thiemdd@tdmu.edu.vn

Tóm tắt

Mạng vô tuyến đa truy cập không trực giao thu thập năng lượng đáp ứng tốt các yêu cầu về hiệu suất năng lượng, hiệu suất phổ và độ tin cậy thông tin trong truyền thông hiện đại. Bài báo này trình bày kết quả nghiên cứu mô hình đa truy cập không trực giao thu thập năng lượng với thiết bị gây nhiễu (EHNOMAwJ) nhằm cải thiện hiệu năng bảo mật bằng phương pháp mô phỏng Monter-Carlo xác suất dừng kết nối/bảo mật và xác suất dừng hoạt động cho cả thiết bị thu ở xa và gần. Các kết quả cho thấy có sự đánh đổi giữa độ tin cậy và độ bảo mật. Bài báo còn cho thấy khi lựa chọn hệ số phân chia thời gian/công suất phù hợp thì mô hình này đạt được hiệu năng bảo mật/độ tin cậy tối ưu. Ngoài ra, các kết quả còn cho thấy tồn tại các giới hạn về tốc độ truyền tin yêu cầu/dung lượng bảo mật để tránh mất kết nối hoàn toàn và đạt được bảo mật hoàn toàn. Hơn nữa, ảnh hưởng của tính phi tuyến thu thập năng lượng đến độ tin cậy truyền thông/bảo mật thông tin là đáng kể/nhỏ.

Từ khóa: *mạng vô tuyến đa truy cập không trực giao, thiết bị gây nhiễu, thu thập năng lượng, xác suất dừng kết nối/bảo mật*

Abstract

PERFORMANCE ANALYSIS OF ENERGY HARVESTING NON-ORTHOGONAL MULTI-ACCESS NETWORKS WITH JAMMER

Energy harvesting non-orthogonal multiple access (NOMA) networks effectively meet the demands for energy efficiency, spectral efficiency, and information reliability in modern communications. To enhance security performance, this paper studies an energy harvesting non-orthogonal multiple access model with eavesdropping devices (EHNOMAwJ). The paper employs a Monte Carlo simulation method to analyze the connection/security outage probability and the operational outage probability for both far and near receivers. The results indicate a trade-off between reliability and security. The paper further demonstrates that with an appropriate selection of the time/power splitting factor, this model achieves optimal security/reliability performance. Additionally, the results reveal that there are limits on the required transmission rate/security capacity to avoid complete disconnection and achieve full security. Furthermore, the impact of non-linear energy harvesting on communication reliability/information security is significant/small.

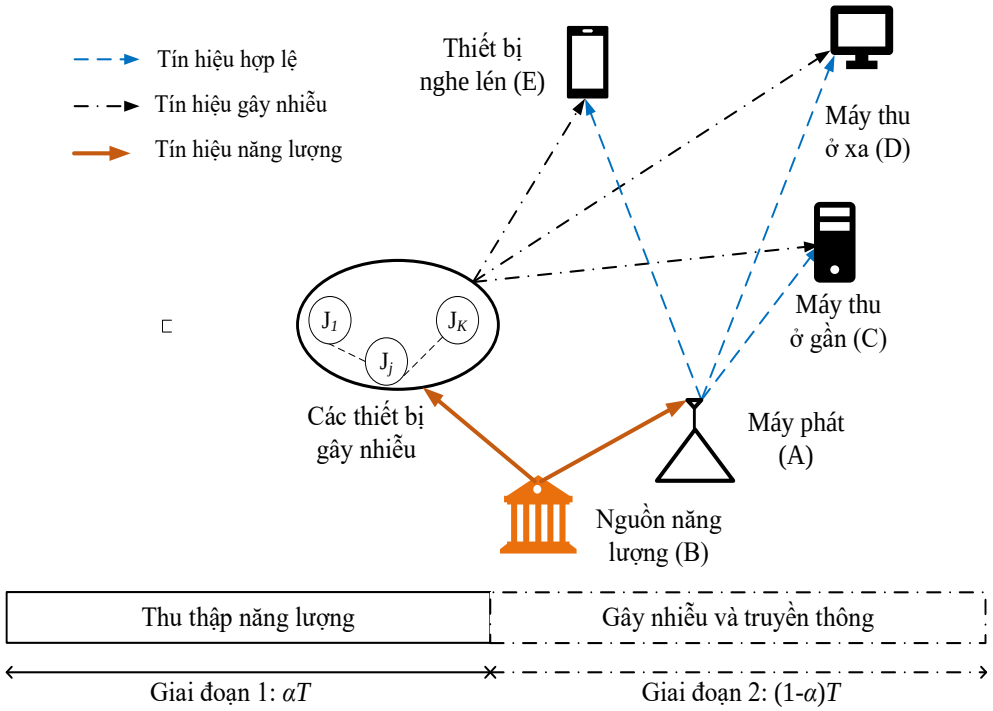
1. Giới thiệu

Trong các mạng vô tuyến thế hệ mới hiện nay, việc đảm bảo đường truyền cho một lượng lớn người dùng trước các thiết bị nghe lén gặp nhiều thách thức (Ngo và cộng sự, 2023). Do đó, các giải pháp cải thiện hiệu năng bảo mật và độ tin cậy cũng như hiệu quả về quang phổ và năng lượng ngày càng trở nên quan trọng hơn. Đa truy cập không trực giao (NOMA) được đề xuất là một giải pháp để cải thiện hiệu suất phổ là cho các mạng 5G (Li và cộng sự, 2024; Zang và cộng sự, 2024; Srinath và cộng sự, 2023). Bằng cách phân phối các mức công suất khác nhau cho những người dùng khác nhau, NOMA có thể giải mã thông tin người dùng bằng tính năng khử nhiễu liên tiếp, điều này hứa hẹn sẽ cải thiện hiệu năng độ tin cậy hơn nữa. Ngoài ra, NOMA còn có thể giúp nâng cao hiệu quả sử dụng năng lượng bằng cách thu năng lượng tần số vô tuyến (RF) trong môi trường xung quanh. Hiện nay, các mạch thu năng lượng (EH) đã được tích hợp thành công ở người dùng 5G/6G (Halimi và cộng sự., 2023). Tuy nhiên, EH đã được mô hình hóa tuyến tính cho khả năng điều khiển trong hầu hết các phân tích hiệu năng (Wang và cộng sự., 2020; Ge và cộng sự., 2020; Bouabdellah và cộng sự., 2019; Gosh và cộng sự., 2023). Hơn nữa, bảo mật lớp vật lý (PLS) sử dụng tính chất lan truyền của các kênh vô tuyến đã được chứng minh là một giải pháp hiệu quả để cải thiện hiệu năng bảo mật (Loukil và cộng sự., 2023; Kasuki và cộng sự., 2023). Do đó, PLS cho NOMA được hỗ trợ EH đã thu hút được sự quan tâm đáng kể từ cả trong công nghiệp và giới học thuật nhằm đáp ứng đồng thời các nhu cầu chính về hiệu năng bảo mật và bảo mật cao cũng như hiệu quả về năng lượng và quang phổ cho các mạng vô tuyến thế hệ tiếp theo. Một trong những kỹ thuật PLS hiệu quả để đảm bảo việc truyền thông an toàn là gây nhiễu nhân tạo, làm suy yếu việc nghe lén có chủ đích nhưng không gây hại cho việc truyền thông của người dùng mong muốn (Zheng và cộng sự., 2016; Hu và cộng sự., 2017). Khảo sát các công trình trên, tác giả đề xuất nghiên cứu hiệu năng của mô hình mạng đa truy cập không trực giao thu thập năng lượng với thiết bị gây nhiễu. Lưu ý rằng, bài báo này nghiên cứu hiệu năng của hệ thống EHNOMAwJ với kỹ thuật thu thập năng lượng phi tuyến tính (NLEH), đây là nhân tố mà các công trình trên chưa được tính đến. Phân tích hiệu năng của mô hình cho thấy những ưu điểm của hệ thống đó là hiệu năng có độ tin cậy và bảo mật cao cũng như hiệu quả về quang phổ và năng lượng. Sau đây là nội dung chính của công trình nghiên cứu này.

2. Mô hình hệ thống

Mô hình hệ thống EHNOMAwJ được minh họa như hình 1. Mô hình này cho phép truyền thông đồng thời từ máy phát NOMA (A) đến hai máy thu NOMA (C và D) để có hiệu suất phổ cao trong khi thiết bị gây nhiễu được chọn (J*j*) từ một nhóm thiết bị gây nhiễu J làm gián đoạn việc lấy cắp thông tin của thiết bị nghe lén (E) để mang lại hiệu năng bảo mật cao. A và J_j tự cấp nguồn cho hoạt động của mình bằng cách thu thập năng lượng từ nguồn (B), có thể là đài phát thanh/truyền hình có công suất phát cao và ổn định để nâng cao hiệu quả sử dụng năng lượng.

EHNOMAwJ như trên có thể biểu diễn đường xuống trong các mạng truyền thông di động. A và J*j* thu thập năng lượng từ B là bộ nguồn sẵn có (ví dụ: đài phát thanh, đài phát sóng truyền hình) để cấp nguồn hoạt động. Đối với EHNOMAwJ được đề xuất, B truyền năng lượng cho A và J_j trong khoảng thời gian α của khối truyền T, tức là giai đoạn 1, trong khi A thực hiện liên lạc đường xuống NOMA tới C và D và bộ gây nhiễu được chọn J_j trong số các thiết bị gây nhiễu J sẽ gây nhiễu việc nghe lén của E trong phần còn lại của T, tức là giai đoạn 2.



Hình 1. *Mô hình mạng EHNOMAwJ*

Các ký hiệu g_{ba}, g_{ac}, g_{ad} và g_{ae} là các độ lợi kênh giữa B và A, A và C, A và D, A và E, tương ứng trong khi g_{bj} , g_{jn}, g_{jf} , g_{je} là độ lợi kênh giữa B và J_j , J_j và C, J_j và D, J_j và E, tương ứng. Với giả sử các kênh fading Rayleigh phẳng. Do đó, g_{kl} với tr={*ba, ac, ad, ae, bj, jc, jd, je*} được phân phối theo hàm mũ với giá trị trung bình là $\varphi_{tr} = \Xi\{g_{tr}\}$. Để tính đến suy hao đường truyền, φ_{kl} được mô hình hóa thành ρd_{tr}^{-v} trong đó ρ là công suất pha đinh ở khoảng cách tham chiếu 1m, d_{kl} là khoảng cách từ máy phát đến máy thu tương ứng và υ là số mũ suy hao đường truyền. Lưu ý rằng các ký hiệu sau đây biểu thị $g_{tr} = |h_{tr}|^2$ trong đó h_{kl} là hệ số kênh.

Ở giai đoạn 1, B truyền năng lượng vô tuyến cho A và J_j. Do đó, A và J_j tích lũy lượng năng lượng là $W_u = \alpha T\beta P\, g_{bu}$ trong đó P là công suất của B và $\beta \in (0, 1)$ biểu thị hiệu suất chuyển đổi năng lượng; u ={*a,j*}. Vì giai đoạn 2 kéo dài *(1-α)T* nên công suất truyền thông ở giai đoạn 2 được chuyển đổi từ W_u là $W_u(1-\alpha)T$. Theo NLEH (Solanki và cộng sự., 2020), công suất A và J_j tiêu thụ ở giai đoạn 2 là

$$P_u = \begin{cases} \dfrac{\beta\alpha P}{1-\alpha} g_{bu} & , \alpha P g_{bu} \le \chi \\ \dfrac{\beta\alpha\chi}{1-\alpha} & , \alpha P g_{bu} > \chi \end{cases} = \begin{cases} \Delta g_{bu} & , g_{bu} \le \Theta \\ \Omega & , g_{bu} > \Theta \end{cases} \quad (1)$$

trong đó $\Delta = \dfrac{\beta\alpha P}{1-\alpha}$, $\Omega = \dfrac{\beta\alpha\chi}{1-\alpha}$, $\Theta = \dfrac{\chi}{\alpha P}$ và χ là ngưỡng bão hòa công suất. Điều đáng chú ý là NLEH rõ ràng được đặc trưng bởi (1). Cụ thể hơn, NLEH tạo ra công suất của Δg_{bu}, tỷ lệ tuyến tính với công suất đầu vào khi nó vượt quá χ; mặt khác, công suất đầu ra của nó bão hòa ở χ. Ngoài ra, NLEH trở thành thu thập năng lượng tuyến tính khi χ lớn ($\chi \to \infty$).

Trong giai đoạn 2, đường xuống NOMA và hoạt động gây nhiễu được thực hiện đồng thời, tức là A gửi đồng thời các ký hiệu (x_c và x_d) với công suất phát P_a trong biểu diễn NOMA của $\sqrt{\delta P_a}x_c+\sqrt{(1-\delta)P_a}x_d$ đến C và D trong khi thiết bị gây nhiễu được chọn, cụ thể là J_j, gửi tín hiệu gây nhiễu x_j để gây nhiễu E với công suất phát P_j trong đó $\Xi\left\{|x_c|^2\right\}=\Xi\left\{|x_d|^2\right\}=\Xi\left\{|x_j|^2\right\}=1$, x_c và xd lần lượt là các ký hiệu của tín hiệu mong muốn của C và D. Theo cơ chế NOMA, C được phân bổ ít năng lượng hơn D và do đó, $\delta < 0,5$. Do đó:

• Tín hiệu nhận được tại C là:

$$y_c=h_{ac}\left(\sqrt{\delta P_a}x_c+\sqrt{(1-\delta)P_a}x_d\right)+h_{jc}\sqrt{P_j}x_j+\varepsilon_c \qquad (2)$$

• Tín hiệu nhận được tại D là:

$$y_d=h_{ad}\left(\sqrt{\delta P_a}x_c+\sqrt{(1-\delta)P_a}x_d\right)+h_{jd}\sqrt{P_j}x_j+\varepsilon_d \qquad (3)$$

• Tín hiệu nhận được tại E là:

$$y_e=h_{ae}\left(\sqrt{\delta P_a}x_c+\sqrt{(1-\delta)P_a}x_d\right)+h_{je}\sqrt{P_j}x_j+\varepsilon_e \qquad (4)$$

trong đó $\varepsilon_c \sim \mathrm{N}\left(0,\sigma_c\right), \varepsilon_d \sim \mathrm{N}\left(0,\sigma_d\right)$ và $\varepsilon_e \sim \mathrm{N}\left(0,\sigma_e\right)$ lần lượt là nhiễu cộng tại C, D và E.

Chọn thiết bị gây nhiễu J_j sao cho nó gây nhiễu nhiều nhất trong số tất cả các thiết bị gây nhiễu tới E. Điều này có nghĩa là chỉ số j được biểu thị bằng $j=\max_{i\in[1,K]} g_{ie}P_i$. Việc lựa chọn J_j có thể được thực hiện theo nhiều cách. Ví dụ: mỗi thiết bị gây nhiễu J_i có thể đặt bộ đếm thời gian độc lập với ngưỡng tỷ lệ nghịch với $g_{ie}P_i$. Khi đó, J_j là đối tượng gây nhiễu có thời gian hết hạn sớm nhất.

2.1. Phát hiện tại C và D:

Bởi vì J_j gây nhiễu x_j để chỉ gây can nhiễu vào E mà không gây tổn hại đến liên lạc của C và D, nên máy thu mong muốn (C và D) có thể dự đoán chính xác tín hiệu gây nhiễu này, có thể được hiểu là được truyền qua khoảng trống đến C và D (Hu và cộng sự., 2017; Zou, 2017). Theo đó, C và D có thể triệt tiêu hoàn toàn tín hiệu gây nhiễu ra khỏi y_r, cuối cùng tạo ra tín hiệu không nhiễu.

$$\tilde{y}_v=h_{ad}\left(\sqrt{\delta P_a}x_c+\sqrt{(1-\delta)P_a}x_d\right)+\varepsilon_v \text{ với } v=\{c,d\} \qquad (5)$$

Theo $\tilde{y}_v$, C và D phát hiện x_c và x_d theo nguyên tắc phát hiện dựa trên NOMA. Vì $\delta<0,5$ nên C phát hiện x_d trước tiên bằng cách coi x_c là nhiễu. Sau đó, C phát hiện x_d từ $\tilde{y}_c$ với tỷ lệ tín hiệu trên nhiễu cộng với nhiễu (SINR) là

$$\Psi_c^d=\frac{(1-\delta)P_a g_{ac}}{g_{ac}\delta P_a+\sigma_c} \qquad (6)$$

Bằng cách triệt tiêu nhiễu do xd tạo ra, C tiếp tục khôi phục xc từ $\hat{y}_c=y_e-h_{ae}\sqrt{(1-\delta)P_a}x_d=h_{ae}\sqrt{\delta P_a}x_c+\varepsilon_e$. Do đó, dựa trên $\hat{y}_c$, C khôi phục x_c với tỷ lệ tín hiệu trên nhiễu (SNR) như sau:

$$\Psi_c^c = \frac{g_{ac}\delta P_a}{\sigma_c} \quad (7)$$

Trong khi đó, D phát hiện x_d bằng cách coi x_c là nhiễu. Theo đó, D phát hiện x_d trực tiếp từ $\tilde{y}_f$ với SINR.

$$\Psi_d^d = \frac{(1-\delta)P_a g_{ad}}{g_{ad}\delta P_a + \sigma_d} \quad (8)$$

2.2. Phát hiện tại E:

Thiết bị nghe lén không có thông tin về tín hiệu gây nhiễu x_j. Từ đó, dựa trên (4), E thực hiện việc phát hiện x_c và x_d theo nguyên tắc phát hiện dựa trên NOMA. Vì δ < 0,5, E phát hiện x_d trước tiên bằng cách coi x_c là nhiễu. Sau đó, E phát hiện x_d từ $y_e = h_{ae}\left(\sqrt{\delta P_a}x_c + \sqrt{(1-\delta)P_a}x_d\right) + h_{je}\sqrt{P_j}x_j + \varepsilon_e$ với SINR là

$$\Psi_e^d = \frac{(1-\delta)P_a g_{ae}}{g_{ae}\delta P_a + g_{je}P_j + \sigma_e} \quad (9)$$

Bằng cách triệt tiêu nhiễu gây ra bởi x_d, E tiếp tục phát hiện x_c từ $\hat{y}_e = y_e - h_{ae}\sqrt{(1-\delta)P_a}x_d = h_{ae}\sqrt{\delta P_a}x_c + \varepsilon_e$. Theo đó, tuân theo $\hat{y}_e$, E phát hiện x_c với SINR là:

$$\Psi_e^c = \frac{g_{ae}\delta P_a}{g_{je}P_j + \sigma_e} \quad (10)$$

Ta thấy từ (9)-(10) rằng J_j làm suy yếu E bằng công suất gây nhiễu là $g_{je}P_j$, điều này làm giảm đáng kể xác suất phát hiện thành công x_c và x_d tại E và do đó, cải thiện đáng kể hiệu năng bảo mật.

3. Phân tích hiệu năng EHNOMAwJ

Đầu tiên, phần này mô phỏng COP/SOP của EHNOMAwJ. COP được xác định là khả năng dung lượng kênh đạt được ở máy thu mong muốn nhỏ hơn tốc độ dữ liệu mục tiêu R_0. Trong khi đó, SOP được xác định là khả năng dung lượng kênh thu được ở thiết bị nghe lén nhỏ hơn tốc độ bảo mật dự phòng (R_0 -R_s) dành riêng cho việc nghe lén trong đó R_s là tốc độ bảo mật mục tiêu. Do đó, COP/SOP thể hiện độ tin cậy/bảo mật của việc truyền tải thông tin.

3.1. Độ tin cậy

Hiệu năng độ tin cậy được đặc trưng bởi COP tại C và D. Khi đó, COP có giá trị càng thấp thì hiệu năng độ tin cậy càng cao.

∗ *COP tại F*: COP tại D được biểu diễn dưới dạng:

$$COP_d = \Pr\left\{(1-\alpha)\log_2\left(1+\Psi_d^d\right) \le R_0\right\} = \Pr\left\{\Psi_d^d \le \Psi_0\right\} \quad (11)$$

trong đó $\Psi_0 = 2^{R_0/(1-\alpha)} - 1$. Hệ số của *(1-α)* trước logarit của (8) là do giai đoạn 2 diễn ra trong khoảng $(1-\alpha)T$.

∗ *COP tại N:* Hai sự kiện khiến C bị mất kết nối như sau:

• Sự kiện đầu tiên xảy ra khi C giải mã x_d không thành công, cụ thể là $(1-\alpha)\log_2\left(1-\Psi_c^d\right) \le R_0$.

• Sự kiện thứ hai xảy ra khi C giải mã x_d thành công (cụ thể là $(1-\alpha)\log_2\left(1-\Psi_c^d\right) > R_0$ nhưng khôi phục x_c không thành công (cụ thể là $(1-\alpha)\log_2\left(1-\Psi_c^d\right) \le R_0$.

Theo định luật xác suất tổng, COP tại C được biểu diễn dưới dạng

$$\begin{aligned} COP_c &= \Pr\left\{(1-\alpha)\log_2\left(1+\Psi_c^d\right) \le R_0\right\} \\ &\quad + \Pr\left\{(1-\alpha)\log_2\left(1+\Psi_c^d\right) > R_0, (1-\alpha)\log_2\left(1+\Psi_c^c\right) \le R_0\right\} \\ &= 1-\Pr\left\{\Psi_c^d \ge \Psi_0, \Psi_c^c \ge \Psi_0\right\} \end{aligned} \quad (12)$$

Nhận xét 1: Cả COP_c và COPd đều phụ thuộc vào các tham số (R_0, α, P, δ, χ, β), nghĩa là C và D có thể đạt được độ tin cậy mong muốn bằng cách thiết lập đúng các tham số này.

3.2. Phân tích bảo mật

Hiệu năng bảo mật được biểu diễn bằng SOP tại E. Theo đó, SOP tại E càng thấp thì hiệu năng bảo mật càng thấp. SOP tại E được xác định theo cách tương tự như COP tại C và D. Như vậy, SOP của C và D lần lượt được đưa ra bởi:

$$\begin{aligned} SOP_c &= \Pr\left\{(1-\alpha)\log_2\left(1+\Psi_e^d\right) \le R_0 - R_s\right\} \\ &\quad + \Pr\left\{(1-\alpha)\log_2\left(1+\Psi_e^d\right) > R_0 - R_s, (1-\alpha)\log_2\left(1+\Phi_e^n\right) \le R_b - R_s\right\} \\ &= 1-\Pr\left\{\Psi_e^d \ge \Psi_s, \Psi_e^c \ge \Psi_s\right\} \end{aligned} \quad (13)$$

và

$$SOP_d = \Pr\left\{(1-\alpha)\log_2\left(1+\Psi_e^d\right) \le R_0 - R_s\right\} = \Pr\left\{\Psi_e^d \le \Psi_s\right\} \quad (14)$$

trong đó $\Psi_s = 2^{(R_b-R_s)/(1-\alpha)} - 1$.

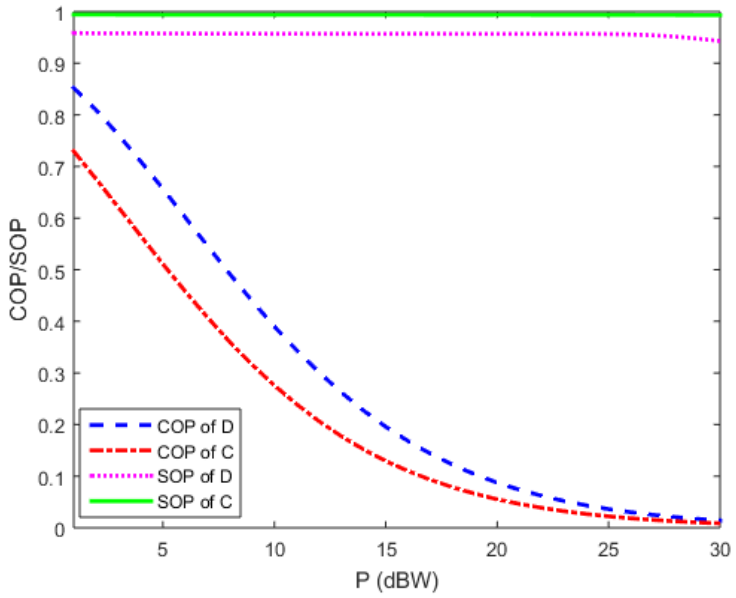
Nhận xét 2: Cả SOP_c và SOP_d đều phụ thuộc vào các tham số (R_0, R_s, α, P, δ, χ, J, β), nghĩa là C và D có thể đạt được hiệu quả bảo mật mong muốn bằng cách thiết lập đúng các tham số này.

4. Kết quả và thảo luận

Để minh họa, người dùng được đặt trong mặt phẳng 2D, với tọa độ lần lượt như sau: A(10, −10), B(0, 0), C(30, 0), D(45, −10), E(25, 0), J_j (10, 5). Các kết quả mô phỏng được trình bày để đo COP/SOP của C và D trong EHNOMAwJ theo các thông số kỹ thuật được áp dụng trong bảng 1, trừ khi có quy định khác.

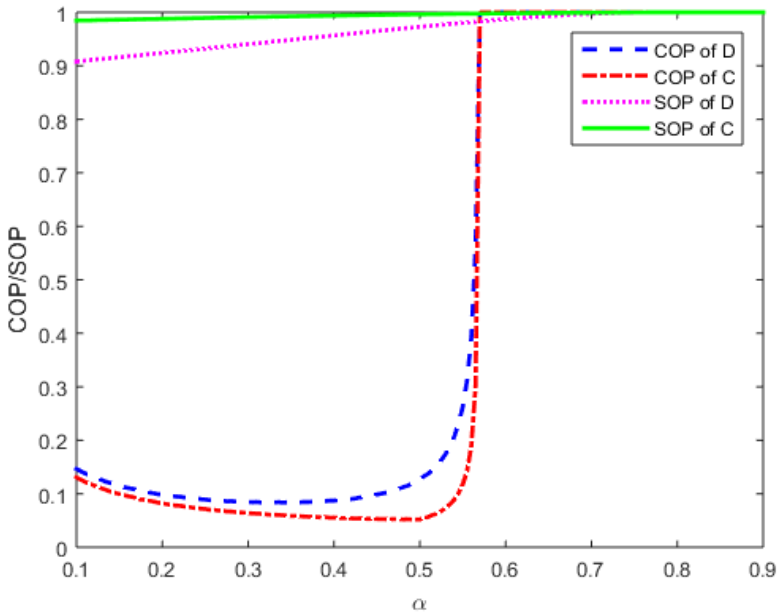
Bảng 1. *Các thông số hoạt động*

Tham số	Giá trị
Hệ số phân chia thời gian	$\alpha = 0,4$
Hiệu suất chuyển đổi năng lượng	$\beta = 0,7$
Công suất fading ở khoảng cách tham chiếu 1m	$\rho = 10^{-2}$
Công suất phát của B	$P = 20$ dBW
Công suất tạp âm	$\sigma_c = \sigma_d = \sigma_e = -90$ dBm
Hệ số phân chia công suất	$\delta = 0,2$
Ngưỡng bão hòa công suất	$\sigma = -20$ dBW
Tốc độ dữ liệu mục tiêu	$R_0 = 1$ bps/Hz
Tốc độ bảo mật mục tiêu	$R_s = 0,5$ bps/Hz
Số lượng thiết bị gây nhiễu	$J = 5$
Số mũ suy hao đường truyền	$\upsilon = 2,7$



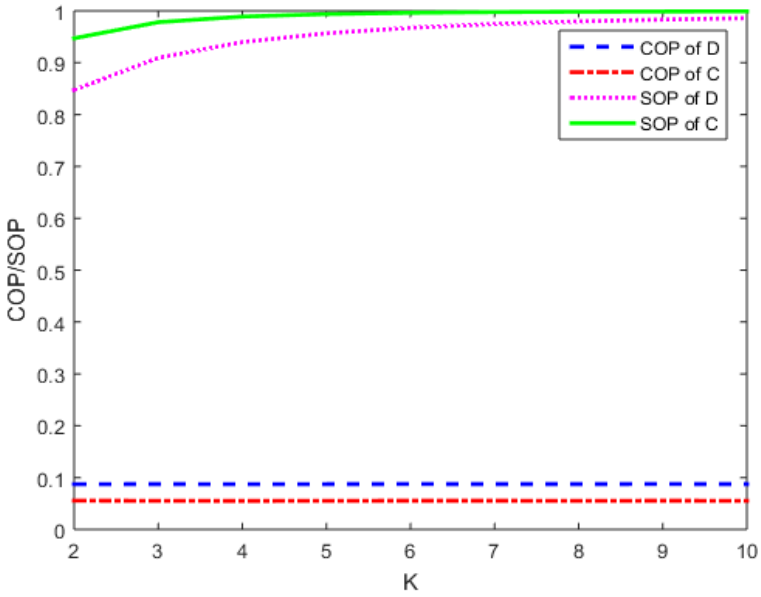
Hình 2. *COP/SOP theo công suất của B*

Hình 2 minh họa COP/SOP theo P (công suất phát của B). Kết quả này cho thấy độ tin cậy được nâng cao đáng kể (tức là COP thấp hơn) tính bảo mật gần như không đổi (tức là SOP thay đổi rất ít) cho cả C và D khi tăng công suất của B. Điều này bắt nguồn từ việc tăng năng lượng thu thập. Thật vậy, năng lượng thu được cao hơn (tức là công suất phát của A cao hơn) làm cho C và D nhận được tín hiệu mong muốn của chúng một cách đáng tin cậy hơn. Tuy nhiên, năng lượng thu được cao hơn không chỉ làm tăng công suất phát của A mà còn tích tụ công suất phát của J_j, khiến E nhận được nhiều hơn cả công suất tín hiệu mong muốn và công suất gây nhiễu. Do đó, SINR để E giải mã x_c và x_d thay đổi ít, cuối cùng làm hiệu năng bảo mật gần như không đổi. Hơn nữa, khi công suất của B tăng do sự gia tăng của cả COP và SOP, nên nảy sinh sự đánh đổi giữa độ tin cậy và tính bảo mật. Tuy nhiên, tính bảo mật thay đổi ít trong khi độ tin cậy được cải thiện đáng kể khi B tăng cho thấy hiệu quả của hoạt động gây nhiễu trong các thông tin liên lạc còn lại được bảo mật với độ tin cậy cao hơn.



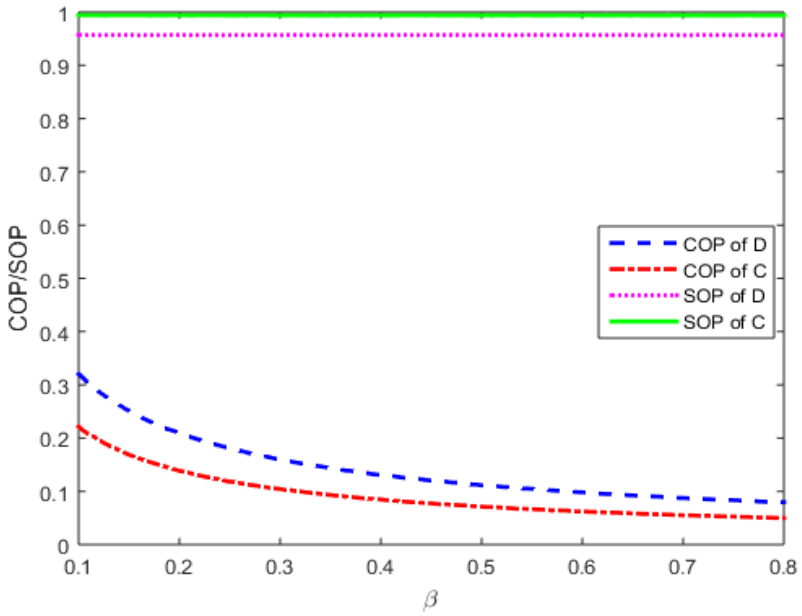
Hình 3. *COP/SOP so với hệ số phân chia thời gian α*

Hình 3 minh họa ảnh hưởng của hệ số phân chia thời gian α đến COP/SOP của C và D. Hình này cho thấy độ tin cậy tăng khi tăng α trong khoảng giá trị nhỏ (tức là COP giảm khi tăng α). Hơn nữa, khi α cao COP bằng 1 (mất kết nối hoàn toàn) khi $R_b \geq -(1-\alpha)\log_2 \delta$ hoặc $\alpha \geq 1 + R_b / \log_2 \delta$. Ngoài ra, kết quả còn cho thấy, tính bảo mật giảm (SOP tăng) khi α tăng. Rõ ràng kết quả cho thấy có sự cân bằng giữa bảo mật và độ tin cậy.



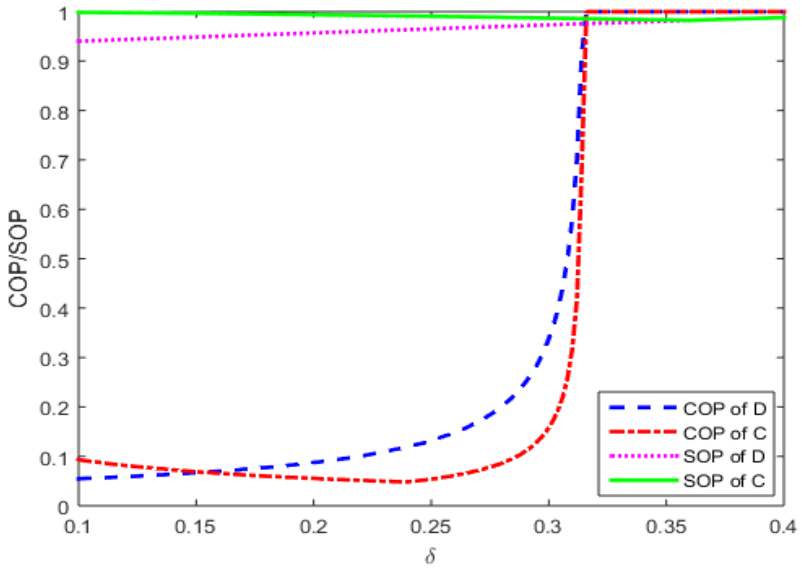
Hình 4. *COP/SOP theo số lượng thiết bị gây nhiễu K*

Hình 4 cho thấy ảnh hưởng của số lượng thiết bị gây nhiễu K đến COP/SOP của C và D. Kết quả này, cho thấy tính hiệu quả của việc lựa chọn thiết bị gây nhiễu được đề xuất trong việc cải thiện bảo mật thông tin. Hơn nữa, tính bảo mật được cải thiện khi tăng *K*, như mong đợi.



Hình 5. *COP/SOP so với hiệu năng chuyển đổi năng lượng*

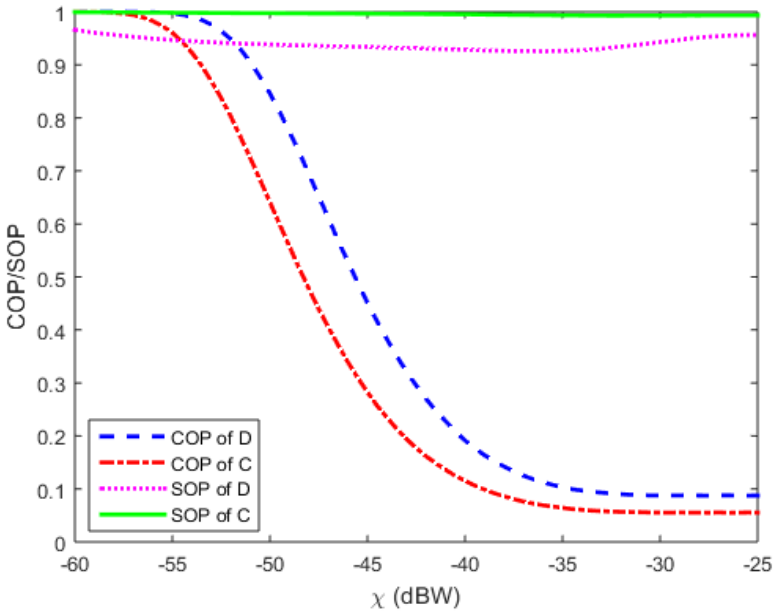
Hình 5 minh họa ảnh hưởng của hiệu năng chuyển đổi năng lượng β lên COP/SOP của C và D. Hình này cho thấy độ tin cậy truyền thông được cải thiện khi tăng β do năng lượng thu hoạch ngày càng tăng, cuối cùng làm tăng công suất nhận được ở C và D để giải mã x_c và x_d đáng tin cậy hơn. Tuy nhiên, hiệu quả bảo mật hầu như không thay đổi khi tăng β. Điều này là do năng lượng thu được ngày càng tăng do tăng β tích lũy cả công suất của tín hiệu mong muốn và tín hiệu gây nhiễu và do đó, SINR để E giải mã x_c và x_d gần như không đổi.



Hình 6. *COP/SOP so với hệ số phân chia công suất*

Hình 6 biểu diễn ảnh hưởng của hệ số phân chia công suất δ, đại diện cho phần công suất được phân bổ cho x_c, theo COP/SOP của C và D. Kết quả cho thấy độ tin cậy của D bị giảm thiểu khi tăng δ, đó là do công suất được phân bổ để truyền x_d ít hơn và giải mã

trực tiếp x_d tại D. Tuy nhiên, C trong sơ đồ đề xuất có thể đạt được COP cao nhất với mức tối ưu lựa chọn δ (ví dụ $\delta = 0,238$ làm cho COP của C cao nhất trong hình 6). Điều này là do C phải giải mã x_d trước khi giải mã x_c. Vì vậy, nên chọn δ một cách tối ưu để cân bằng giữa SINR cho việc giải mã x_d và SNR cho việc giải mã x_c. Ngoài ra, δ cao gây ra COP bằng 1 (hay mất kết nối hoàn toàn) đối với $R_0 \geq -(1-\alpha) log_2 \delta$ hoặc $\delta > 2^{-R_0/(1-\alpha)}$.



Hình 7. *COP/SOP so với ngưỡng bão hòa công suất*

Hình 7 cho thấy ảnh hưởng của ngưỡng bão hòa công suất χ đến COP/SOP của C và D. Kết quả cho thấy sự cải thiện đáng kể về độ tin cậy khi tăng χ, đó là do năng lượng thu thập ngày càng tăng. Ngoài ra, COP bão hòa ở mức χ cao vì χ cao làm cho bộ thu năng lượng trở nên tuyến tính. Tuy nhiên, SOP có thể được tối ưu hóa với việc lựa chọn χ thích hợp. Điều này là do việc tăng χ sẽ tích tụ cả công suất của tín hiệu gây nhiễu và tín hiệu mong muốn. Từ đó, E có thể đạt được SOP tốt nhất (mức bảo mật kém nhất cho C và D) bằng cách cân bằng giữa công suất gây nhiễu và công suất mong muốn với giá trị tối ưu là χ.

5. Kết luận

Bài viết này đề xuất lựa chọn thiết bị gây nhiễu trong NOMA được hỗ trợ EH để cải thiện hiệu năng về độ tin cậy và bảo mật cũng như hiệu quả về quang phổ và năng lượng cho truyền thông đường xuống. Để đánh giá hiệu năng bảo mật/độ tin cậy bài viết này đã mô phỏng COP/SOP tại các máy thu ở gần và ở xa. Kết quả đã cho thấy khi tăng công suất B hiệu năng bảo mật thay đổi ít trong khi độ tin cậy được cải thiện đáng kể. Tuy nhiên, có sự đánh đổi giữa độ tin cậy và tính bảo mật. Các kết quả còn cho thấy hiệu năng bảo mật/độ tin cậy tối ưu với việc lựa chọn δ và χ phù hợp. Ngoài ra, kết quả còn cho thấy rằng tính phi tuyến của EH, được đặc trưng bởi χ, ảnh hưởng đáng kể đến độ tin cậy của truyền thông nhưng ảnh hưởng không đáng kể đến an toàn thông tin.

TÀI LIỆU THAM KHẢO

[1] D. Wang et al. (2020). Primary Privacy Preserving With Joint Wireless Power and Information Transfer for Cognitive Radio Networks. *IEEE Transactions on Cognitive Communications and Networking, 6*(2), pp. 683-693.

[2] H. Grama Srinath et al. (2023). An Efficient NB-IoT Compatible GF-NOMA PHY Mechanism for mMTC. *IEEE Internet of Things Journal*, *10*(20), pp. 17949-17963.

[3] J. Hu et al. (2017). Artificial-noise-aided secure transmission scheme with limited training and feedback overhead. *IEEE Transactions on Wireless Communications, 16*(1), pp. 193-205.

[4] L. Ge et al. (2020). Performance Analysis for Multihop Cognitive Radio Networks With Energy Harvesting by Using Stochastic Geometry. *IEEE Internet of Things Journal, 7*(2), pp. 1154-1163.

[5] M. A. Halimi et al. (2023). Rectifier Circuits for RF Energy Harvesting and Wireless Power Transfer Applications: A Comprehensive Review Based on Operating Conditions. *IEEE Micro Magazines, 24*(1), pp. 46-61.

[6] M. A. Halimi et al. (2023). Rectifier Design Challenges for Wireless Energy Harvesting/Wireless Power Transfer Systems: Broadening Bandwidth and Extended Input Power Range. *IEEE Micro Magazines, 24*(6), pp. 54-67.

[7] M. Bouabdellah et al. (2019). Cooperative Energy Harvesting Cognitive Radio Networks With Spectrum Sharing and Security Constraints. *IEEE Access*, vol. 7, pp. 173329-173343.

[8] M. H. Loukil et al. (2023). Physical Layer Security at a Point-to-Point MIMO System With 1-Bit DACs and ADCs. *IEEE Wireless Communications Letters, 12*(8), pp. 1439-1443.

[9] Q. T. Ngo et al. (2023). Physical Layer Security in IRS-Assisted Cache-Enabled Satellite Communication Networks. *IEEE Transactions on Green Communications and Networking, 7*(4), pp. 1920-1931.

[10] S. Ghosh et al. (2023). On the Performance of End-to-End Cooperative NOMA-Based IoT Networks With Wireless Energy Harvesting. *IEEE Internet of Things Journal*, *10*(18), pp. 16253-16270.

[11] S. Solanki et al. (2020). Performance Analysis of Piece-Wise Linear Model of Energy Harvesting-Based Multiuser Overlay Spectrum Sharing Networks. *IEEE OJCS*, vol. 1, pp. 1820-1836.

[12] T. X. Zheng et al. (2016). Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers. *IEEE Transactions on Vehicular Technology, 65*(10), pp. 8812-8817.

[13] X. Hu et al. (2016). Secure Transmission via Jamming in Cognitive Radio Networks with Possion Spatially Distributed Eavesdroppers. *Proc. IEEE PIMRC*, vol. 4-7, pp. 1-6. Spain.

[14] X. Zhang et al. (2023). Generalized Approximate Message Passing Based Bayesian Learning Detectors for Uplink Grant-Free NOMA. *IEEE Transactions on Vehicular Technology, 72*(11), pp. 15057-15061.

[15] Y. Katsuki et al. (2023). Noncoherent Massive MIMO With Embedded One-Way Function Physical Layer Security. *IEEE Trans. Info. Forensics and Security*, vol. 18, pp. 3158-3170.

[16] Y. Li et al. (2024). NOMA Assisted Two-Tier VR Content Transmission: A Tile-Based Approach for QoE Optimization. *IEEE Transactions on Mobile Computing, 23*(5), pp. 3769-3784.

[17] Y. Zou (2017). Physical-Layer Security for Spectrum Sharing Systems. *IEEE Transactions on Wireless Communications, 16*(2), pp. 1319-132.