BẢO MẬT TRONG MẠNG VÔ TUYẾN NHẬN THỨC DẠNG PHỦ CÓ THU THẬP NĂNG LƯỢNG

Trần Trọng Hiếu[1*], Lê Thành Tới[1], Hồ Văn Khương[2]
[1]*Trường Đại học Công nghiệp Thực phẩm TP.HCM*
[2]*Trường Đại học Bách Khoa TP.HCM*
*Email: *hieutt@hufi.edu.vn*
Ngày nhận bài: 03/6/2022; Ngày chấp nhận đăng: 22/8/2022

TÓM TẮT

Bài báo này đề xuất giải pháp bảo mật cho mạng vô tuyến nhận thức dạng phủ có thu thập năng lượng. Giải pháp ứng dụng nhiễu nhân tạo để gây nhiễu tín hiệu thu tại thiết bị nghe lén. Hiệu năng bảo mật của mạng này được đánh giá thông qua tiêu chí xác suất dừng bảo mật. Nhiều kết quả được cung cấp để rút ra những hiểu biết sâu sắc về khả năng bảo mật của mạng này khi ứng dụng nhiễu nhân tạo, mà từ đó xác định được các thông số kỹ thuật tối ưu để mạng được bảo mật tối đa. Đáng chú ý, truyền thông sơ cấp/thứ cấp có thể được bảo mật với các mức độ khác nhau bằng cách kiểm soát linh hoạt nhiều thông số kỹ thuật của giải pháp được đề xuất.

Từ khóa: Xác suất dừng bảo mật, mạng vô tuyến nhận thức, thu thập năng lượng, nhiễu nhân tạo.

1. MỞ ĐẦU

Mạng truyền thông thế hệ thứ năm (Fifth Generation - 5G) cung cấp một lượng lớn các dịch vụ không dây mới nổi và do đó, gây áp lực đáng kể lên cơ sở hạ tầng viễn thông [1]. Thật vậy, một trong những dịch vụ quan trọng của mạng 5G là Internet vạn vật (Internet of Things - IoT) được ứng dụng rộng rãi từ dân sự (ví dụ: chăm sóc sức khỏe, giao thông, điện lực, an toàn công cộng, v.v.) đến quân sự (ví dụ: căn cứ thông minh, trinh sát chiến thuật, v.v.) [2]. Tuy nhiên, khi triển khai IoT, một lượng lớn các thiết bị được kết nối đồng thời sẽ tiêu tốn rất nhiều năng lượng và do đó, cần nâng cao hiệu quả sử dụng năng lượng để không chỉ kéo dài tuổi thọ của các thiết bị mà còn giảm thiểu nhu cầu năng lượng. Hơn nữa, IoT cũng cần băng thông rộng để phân bổ cho hoạt động đồng thời của một lượng lớn người dùng. Vì vậy, trong tình hình thiếu và khan hiếm phổ tần như hiện nay thì các giải pháp nâng cao hiệu quả sử dụng phổ tần cần được đề xuất. Tương tự như IoT, thông tin di động 5G phải phục vụ số lượng lớn các thiết bị di động và yêu cầu tốc độ dữ liệu ngày càng cao nên cũng cần các giải pháp sử dụng phổ tần và năng lượng hiệu quả để đáp ứng các yêu cầu đó [3]. Áp lực như vậy có thể được giải tỏa bằng các giải pháp công nghệ hiện đại có hiệu suất (năng lượng, sử dụng phổ tần, phổ) cao như sau.

Người dùng nhận thức (Cognitive User - CU), thường hoạt động theo cơ chế *phủ*, *nền* và *đan xen*, có thể sử dụng dải tần được cấp phép (Licensed Frequency Band - LFB) của người dùng sơ cấp (Primary User - PU) mà không gây hại cho việc nhận tín hiệu của PU; do đó, nâng cao đáng kể hiệu suất phổ và giảm thiểu vấn đề khan hiếm phổ tần [4]. Trong cơ chế nền, CU chỉ có quyền truy cập vào LFB nếu CU giới hạn công suất can nhiễu gây ra tại PU ở mức có thể chấp nhận được. Các CU làm việc trong cơ chế phủ truy cập đồng thời LFB với PU nhưng các tiêu chí hiệu năng của PU vẫn được duy trì hoặc nâng cao bằng các kỹ thuật xử lý tín hiệu phức tạp. Ngược lại, cơ chế đan xen chỉ để lại băng thông trống của PU cho CUs truy cập. Trong khi hầu hết các công bố đã nghiên cứu sâu về cơ chế nền và đan xen thì một số ít các

công trình đã tập trung vào cơ chế phủ. Vì cơ chế phủ đạt được tương nhượng tốt hơn về hiệu năng giữa truyền thông sơ cấp và truyền thông thứ cấp so với các cơ chế khác nên bài báo này tập trung vào cơ chế phủ.

Các giải pháp khả thi để cải thiện hiệu suất năng lượng của mạng truyền thông không dây có thể được liệt kê như quy hoạch mạng, giải pháp phần cứng, thu thập năng lượng tần số vô tuyến, v.v. Trong số các giải pháp này, thu thập năng lượng từ tín hiệu RF không đòi hỏi thiết bị thu thập năng lượng phức tạp cũng như không phụ thuộc vào các nguồn năng lượng biến thiên theo thời gian. Những ưu điểm như vậy của giải pháp thu thập năng lượng này làm cho nó trở thành một ứng viên sáng giá được triển khai cho thiết bị có kích thước nhỏ trong thông tin di động 5G hoặc IoT để cung cấp năng lượng, kéo dài thời gian sử dụng và nâng cao hiệu suất sử dụng năng lượng [5].

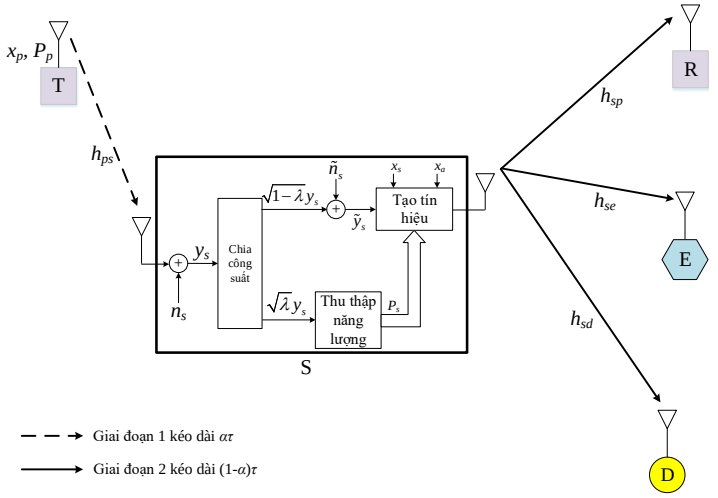
Mạng vô tuyến nhận thức (chế độ phủ) thu thập năng lượng (Energy Harvesting Overlay-based Cognitive Radio Network - EHON) có thể khai thác đồng thời các lợi thế của cả hai công nghệ khả dụng (thu thập năng lượng và vô tuyến nhận thức) để đáp ứng các tiêu chí thiết kế khác nhau của các mạng truyền thông tiên tiến bao gồm hiệu suất năng lượng và phổ cao [6]. Tuy nhiên, việc cả người dùng thứ cấp và người dùng sơ cấp trong các mạng này được phép truyền đồng thời trên LFB có thể tạo điều kiện cho những thiết bị nghe lén giả lập người dùng hợp pháp để nghe lén thông tin hợp pháp, từ đó cảnh báo nghiêm trọng về các vấn đề bảo mật. Để bổ sung và nâng cao hiệu năng bảo mật cho các giải pháp mã hóa và mật mã thông thường thì bảo mật lớp vật lý (Physical Layer Security - PLS) gần đây đã nổi lên như một ứng viên đầy hứa hẹn [7]. PLS có thể được triển khai với nhiều kỹ thuật bao gồm chuyển tiếp, gây nhiễu, v.v. Trong số các kỹ thuật này, gây nhiễu (hoặc tạo ra nhiễu nhân tạo) đã được khai thác rộng rãi nhờ việc triển khai hiệu quả, đơn giản và linh hoạt. Do đó, bài báo này tạo ra nhiễu nhân tạo trong EHONs để bảo mật thông tin cho cả người dùng sơ cấp và người dùng thứ cấp.

Bài báo này nghiên cứu tác động của nhiễu nhân tạo trong EHON, trong đó máy phát sơ cấp không thể kết nối trực tiếp với máy thu sơ cấp trong một số trường hợp (ví dụ: fading) và do đó, máy phát thứ cấp cần hỗ trợ truyền thông sơ cấp để đổi lấy quyền được truy cập vào LFB. Máy phát thứ cấp hoạt động theo cơ chế khuếch đại và chuyển tiếp (Amplify-and-Forward - AF) thu thập năng lượng RF trong tín hiệu của máy phát sơ cấp và phát không chỉ tín hiệu riêng mà còn cả tín hiệu của máy phát sơ cấp và nhiễu nhân tạo. Truyền thông của máy phát thứ cấp bị nghe lén bởi thiết bị nghe lén. Cần lưu ý rằng trong khi hầu hết các công bố đã nghiên cứu về PLS đối với mạng vô tuyến nhận thức (theo cơ chế đan xen hoặc nền) thu thập năng lượng thì một số ít công trình đã chú ý đến cơ chế phủ [4, 8-15]. Tuy nhiên, tác động của nhiễu nhân tạo trong EHON vẫn chưa được nghiên cứu.

2. MẠNG VÔ TUYẾN NHẬN THỨC DẠNG PHỦ CÓ THU THẬP NĂNG LƯỢNG

2.1. Mô hình hệ thống

Hình 1 minh họa EHON, trong đó cặp máy phát - máy thu sơ cấp, T - R, không thể giao tiếp trực tiếp với nhau do fading, shadowing, v.v. Do đó, máy phát thứ cấp S, nằm trong phạm vi phủ sóng của T, có thể hỗ trợ T bằng cách chuyển tiếp thông tin của T đến R. Hơn nữa, S hoạt động theo cơ chế phủ, nghĩa là chuyển tiếp thông tin của T đến R đồng thời với truyền dữ liệu riêng đến máy thu thứ cấp D. Truyền tin của S bị nghe lén bởi thiết bị nghe lén E (giả sử rằng E không thể nghe trực tiếp từ T do một số nguyên nhân như bị che chắn nghiêm trọng (strong shadowing), T và E cách quá xa nhau, fading, v.v.). Để giảm thiểu khả năng nghe lén của E thì S phát nhiễu nhân tạo cùng thông tin của T và S.



Hình 1. Mô hình hệ thống

Hình 1 ký hiệu $h_{sp}, h_{sd}, h_{se}, h_{ps}$ là các hệ số kênh truyền S→R, S→D, S→E, T→S. Bài báo này mô hình các hệ số kênh truyền này lần lượt là $h_{sp} \sim \mathcal{CN}(0, \mu_{sp})$ $h_{sd} \sim \mathcal{CN}(0, \mu_{sd})$, $h_{se} \sim \mathcal{CN}(0, \mu_{se})$ và $h_{ps} \sim \mathcal{CN}(0, \mu_{ps})$. Mô hình hệ số kênh truyền như vậy tương ứng với kênh truyền fading Rayleigh. Tích hợp suy hao đường truyền vào các đặc tính kênh truyền sẽ mô hình μ_{ab} với $a \in \{p, s\}$ và $b \in \{s, p, d, e\}$ là $\mu_{ab} = d_{ab}^{-\rho}$, trong đó ρ là số mũ suy hao đường truyền và d_{ab} là khoảng cách $a - b$.

Tổng thời gian truyền τ để cả T và S hoàn tất quá trình truyền dữ liệu đến các máy thu tương ứng bao gồm hai giai đoạn như trong Hình 1. Trong giai đoạn 1 kéo dài $\alpha\tau$ với $\alpha \in (0,1)$ là hệ số phân chia thời gian, T với công suất phát P_p gửi ký hiệu x_p cho S để thu thập năng lượng dựa trên giao thức phân chia công suất và khuếch đại tín hiệu của T. Giao thức như vậy chia tín hiệu nhận được thành hai phần: một phần $\sqrt{\lambda} y_s$ (y_s là tín hiệu nhận được của S và $\lambda \in (0,1)$ là hệ số phân chia công suất) để thu thập năng lượng và phần khác $\sqrt{1-\lambda} y_s$ để khuếch đại tín hiệu của T. Trong giai đoạn 2 kéo dài $(1-\alpha)\tau$, S phát đi tín hiệu xếp chồng của ba tín hiệu: tín hiệu sơ cấp được khuếch đại, tín hiệu thứ cấp và nhiễu nhân tạo.

2.2. Mô hình tín hiệu

Trong giai đoạn 1, S nhận được tín hiệu:

$$y_s = h_{ps} \sqrt{P_p} x_p + n_s \tag{1}$$

trong đó ăng-ten thu của S tạo ra nhiễu $n_s \sim \mathcal{CN}(0, \sigma_s^2)$, P_p là công suất của máy phát sơ cấp, x_p là tín hiệu phát của máy phát sơ cấp.

Dựa vào Hình 1, năng lượng thu thập được của S là

$$E_s = \eta \Xi \left\{ \left| \sqrt{\lambda} y_s \right|^2 \right\} \alpha\tau = \eta\lambda \left(P_p g_{ps} + \sigma_s^2 \right) \alpha\tau \approx \alpha\eta\lambda P_p g_{ps} \tau \tag{2}$$

trong đó $\eta \in (0,1)$ là hiệu suất chuyển đổi năng lượng và $\Xi\{\cdot\}$ là toán tử kỳ vọng. Từ

phần này, $g_{ab} = |h_{ab}|^2$ ký hiệu độ lợi công suất của kênh truyền với $a \in \{p, s\}$ và $b \in \{s, p, d, e\}$.

Trong giai đoạn 2, S có công suất phát là

$$P_s = \frac{E_s}{(1-\alpha)\tau} \approx A P_p g_{ps} \tag{3}$$

trong đó $A = \alpha\eta\lambda/(1-\alpha)$.

Một trong những đầu vào của bộ tạo tín hiệu trong Hình 1 là $\tilde{y}_s = \sqrt{1-\lambda}\, y_s + \tilde{n}_s$, trong đó $\tilde{n}_s \sim \mathcal{CN}\left(0, \tilde{\sigma}_s^2\right)$ là nhiễu do chuyển đổi tín hiệu thông dải sang tín hiệu băng gốc. Thay thế (1) vào $\tilde{y}_s$ tạo ra

$$\tilde{y}_s = \sqrt{(1-\lambda) P_p}\, h_{ps} x_p + \sqrt{1-\lambda}\, n_s + \tilde{n}_s \tag{4}$$

Bộ tạo tín hiệu khuếch đại $\tilde{y}_s$ trước khi kết hợp với tín hiệu thứ cấp và nhiễu nhân tạo. Cụ thể hơn, bộ tạo tín hiệu tạo ra tín hiệu $\bar{x}_s = \beta \tilde{y}_s + \sqrt{\theta(1-\kappa) P_s}\, x_s + \sqrt{(1-\theta) P_s}\, x_a$, trong đó β là hệ số khuếch đại, θ là hệ số phân bổ công suất cho tín hiệu mong muốn và nhiễu nhân tạo và κ là hệ số phân bổ công suất cho tín hiệu thứ cấp và tín hiệu sơ cấp, x_s là ký hiệu của S và x_a là nhiễu nhân tạo. Hệ số khuếch đại β được xác định để tổng công suất của S là P_s. Do đó, công suất để khuếch đại tín hiệu sơ cấp là $\theta\kappa P_s$ mà từ đó β được cho bởi

$$\beta = \sqrt{\frac{\theta\kappa P_s}{\Xi\left\{|\tilde{y}_s|^2\right\}}} = \sqrt{\frac{\theta\kappa P_s}{(1-\lambda) P_p g_{ps} + (1-\lambda)\sigma_s^2 + \tilde{\sigma}_s^2}} \tag{5}$$

Trong giai đoạn 2, các tín hiệu nhận được lần lượt tại R, D, E là

$$y_p = h_{sp}\bar{x}_s + n_p, \;\; y_d = h_{sd}\bar{x}_s + n_d, \;\; y_e = h_{se}\bar{x}_s + n_e \tag{6}$$

trong đó các ăng-ten thu của R, D, E lần lượt gây ra nhiễu $n_p \sim \mathcal{CN}\left(0, \sigma_p^2\right)$, $n_d \sim \mathcal{CN}\left(0, \sigma_d^2\right)$, $n_e \sim \mathcal{CN}\left(0, \sigma_e^2\right)$.

S cố tình tạo ra nhiễu nhân tạo x_a để chỉ làm giảm khả năng nghe lén của E nhưng không làm giảm hiệu năng của các máy thu hợp pháp (D, R). Việc tạo ra nhiễu nhân tạo như vậy có thể được thực hiện bằng cách cho phép S chia sẻ x_a với D và R. Do đó, các bộ thu hợp pháp (D, R) có thể tạo lại chính xác nhiễu nhân tạo và loại bỏ hoàn toàn nó để sau cùng tín hiệu không có nhiễu nhân tạo thu được tại R và D lần lượt là

$$\tilde{y}_p = h_{sp}\tilde{x}_s + n_p, \;\; \tilde{y}_d = h_{sd}\tilde{x}_s + n_d \tag{7}$$

trong đó $\tilde{x}_s = \beta\tilde{y}_s + \sqrt{\theta(1-\kappa) P_s}\, x_s$.

Thay $\tilde{y}_s$ ở (4) vào $\tilde{x}_s$ và sau đó thay $\tilde{x}_s$ vào (7), ta viết lại (7) như sau:

$$\tilde{y}_p = \sqrt{(1-\lambda) P_p}\, h_{sp}\beta h_{ps} x_p + h_{sp}\sqrt{\theta(1-\kappa) P_s}\, x_s + h_{sp}\beta\left(\sqrt{1-\lambda}\, n_s + \tilde{n}_s\right) + n_p \tag{8}$$

$$\tilde{y}_d = \sqrt{(1-\lambda) P_p}\, h_{sd}\beta h_{ps} x_p + h_{sd}\sqrt{\theta(1-\kappa) P_s}\, x_s + h_{sd}\beta\left(\sqrt{1-\lambda}\, n_s + \tilde{n}_s\right) + n_d \tag{9}$$

mà từ đó, SINR để khôi phục x_p tại R và x_s tại D lần lượt được cho bởi

$$\gamma_p = \frac{\Xi\left\{\left|\sqrt{(1-\lambda)P_p}h_{sp}\beta h_{ps}x_p\right|^2\right\}}{\Xi\left\{\left|h_{sp}\sqrt{\theta(1-\kappa)P_s}x_s + h_{sp}\beta\left(\sqrt{1-\lambda}n_s + \tilde{n}_s\right) + n_p\right|^2\right\}} = \frac{(1-\lambda)P_p g_{sp}g_{ps}\beta^2}{g_{sp}\theta(1-\kappa)P_s + g_{sp}\beta^2\left([1-\lambda]\sigma_s^2 + \tilde{\sigma}_s^2\right) + \sigma_p^2} \quad (10)$$

$$\gamma_d = \frac{\Xi\left\{\left|h_{sd}\sqrt{\theta(1-\kappa)P_s}x_s\right|^2\right\}}{\Xi\left\{\left|\sqrt{(1-\lambda)P_p}h_{sd}\beta h_{ps}x_p + h_{sd}\beta\left(\sqrt{1-\lambda}n_s + \tilde{n}_s\right) + n_d\right|^2\right\}} = \frac{\theta(1-\kappa)P_s g_{sd}}{(1-\lambda)P_p g_{ps}g_{sd}\beta^2 + g_{sd}\beta^2\left([1-\lambda]\sigma_s^2 + \tilde{\sigma}_s^2\right) + \sigma_d^2} \quad (11)$$

Thay thế P_s ở (3) và β ở (5) vào (10) và (11) và sau một số thao tác đơn giản hóa, ta rút gọn (10) và (11) như sau:

$$\gamma_p = \frac{Gg_{sp}}{Hg_{sp} + J} \quad (12)$$

$$\gamma_d = \frac{\bar{G}g_{sd}}{\bar{H}g_{sd} + \bar{J}} \quad (13)$$

trong đó $B = \sigma_s^2 + \frac{\tilde{\sigma}_s^2}{1-\lambda}$, $\bar{J} = \sigma_d^2$

$$G = \theta\kappa A P_p^2 g_{ps}^2 \quad (14)$$

$$H = \theta A\left[B + (1-\kappa)P_p g_{ps}\right]P_p g_{ps} \quad (15)$$

$$J = \left(P_p g_{ps} + B\right)\sigma_p^2 \quad (16)$$

$$\bar{G} = \theta(1-\kappa)AP_p g_{ps} \quad (17)$$

$$\bar{H} = \theta\kappa AP_p g_{ps} \quad (18)$$

Thay (4) vào $\bar{x}_s$ và sau đó thay $\bar{x}_s$ vào y_e ở (6), ta viết lại (6) cho E như sau

$$y_e = h_{se}\beta\sqrt{(1-\lambda)P_p}h_{ps}x_p + h_{se}\sqrt{\theta(1-\kappa)P_s}x_s + h_{se}\beta\left(\sqrt{1-\lambda}n_s + \tilde{n}_s\right) + h_{se}\sqrt{(1-\theta)P_s}x_a + n_e \quad (19)$$

Nhiễu nhân tạo x_a được biết tại R, D và S để bảo vệ x_s và x_p nhưng E không biết x_a. Do đó, SINR tại E để khôi phục x_s và x_p lần lượt được suy ra từ (19) như sau

$$\gamma_e^s = \frac{\Xi\left\{\left|h_{se}\sqrt{\theta(1-\kappa)P_s}x_s\right|^2\right\}}{\Xi\left\{\left|h_{se}\beta\sqrt{(1-\lambda)P_p}h_{ps}x_p + h_{se}\beta\left(\sqrt{1-\lambda}n_s + \tilde{n}_s\right) + h_{se}\sqrt{(1-\theta)P_s}x_a + n_e\right|^2\right\}} \quad (20)$$
$$= \frac{g_{se}\theta(1-\kappa)P_s}{(1-\lambda)P_p\beta^2 g_{se}g_{ps} + g_{se}\beta^2\left[(1-\lambda)\sigma_s^2 + \tilde{\sigma}_s^2\right] + g_{se}(1-\theta)P_s + \sigma_e^2}$$

$$\gamma_e^p = \frac{\Xi\left\{\left|h_{se}\beta\sqrt{(1-\lambda)P_p}h_{ps}x_p\right|^2\right\}}{\Xi\left\{\left|h_{se}\sqrt{\theta(1-\kappa)P_s}x_s + h_{se}\beta\left(\sqrt{1-\lambda}n_s + \tilde{n}_s\right) + h_{se}\sqrt{(1-\theta)P_s}x_a + n_e\right|^2\right\}} \quad (21)$$
$$= \frac{(1-\lambda)P_p\beta^2 g_{se}g_{ps}}{g_{se}\theta(1-\kappa)P_s + g_{se}\beta^2\left[(1-\lambda)\sigma_s^2 + \tilde{\sigma}_s^2\right] + g_{se}(1-\theta)P_s + \sigma_e^2}$$

Phương trình (20) và (21) cho thấy rằng S cố ý tạo ra lượng công suất nhiễu nhân tạo, $g_{se}(1-\theta)P_s$, để gây nhiễu cho thiết bị nghe lén. Do đó, tăng lượng công suất nhiễu nhân tạo này sẽ bảo mật truyền thông cho x_s và x_p.

Thay thế P_s trong (3) và β trong (5) thành (20) và (21) và sau một số thao tác đơn giản hóa, ta rút gọn (20) và (21) như sau

$$\gamma_e^s = \frac{\bar{G}g_{se}}{\bar{U}g_{se} + \bar{J}} \quad (22)$$

$$\gamma_e^p = \frac{Gg_{se}}{Ug_{se} + J} \quad (23)$$

trong đó

$$U = A\left[B + (1-\theta\kappa)P_p g_{ps}\right]P_p g_{ps} \quad (24)$$

$$\bar{U} = (1-\theta+\theta\kappa)AP_p g_{ps} \quad (25)$$

và $\sigma_s^2 = \sigma_e^2 = \sigma_d^2 = \sigma_p^2 = \tilde{\sigma}_s^2 = N_0$ được giả sử mà không mất tính tổng quát.

Dung lượng kênh truyền của D và R trong giai đoạn 2 lần lượt được cho bởi

$$C_d = (1-\alpha)\log(1+\gamma_d) \quad (26)$$

$$C_p = (1-\alpha)\log(1+\gamma_p) \quad (27)$$

trong đó giai đoạn 2 kéo dài $(1-\alpha)\tau$ tạo ra hệ số trước hàm log là 1 - α. Tương tự, dung lượng kênh truyền tại E để giải mã x_p và x_s trong giai đoạn 2 lần lượt được suy ra là

$$C_{Ep} = (1-\alpha)\log(1+\gamma_e^p) \quad (28)$$

$$C_{Es} = (1-\alpha)\log(1+\gamma_e^s) \quad (29)$$

Sự khác biệt về dung lượng giữa R và E để khôi phục x_p được định nghĩa là dung lượng bảo mật cho x_p:

$$\tilde{C}_p = (1-\alpha)\left[\log\frac{1+\gamma_p}{1+\gamma_e^p}\right]^+ \quad (30)$$

trong đó $[x]^+$ biểu thị max(x, 0).

Tương tự, sự khác biệt về dung lượng giữa D và E để khôi phục x_s là dung lượng bảo mật cho x_s:

$$\tilde{C}_s = (1-\alpha)\left[\log\frac{1+\gamma_d}{1+\gamma_e^s}\right]^+ \quad (31)$$

2.3. Hiệu năng bảo mật

Tiêu chí hiệu năng quan trọng để đánh giá hiệu năng bảo mật của truyền thông không dây là xác suất dừng bảo mật (Secrecy Outage Probability - SOP). SOP là xác suất mà dung lượng bảo mật nhỏ hơn mức bảo mật yêu cầu C_0.

SOP cho x_p được định nghĩa là

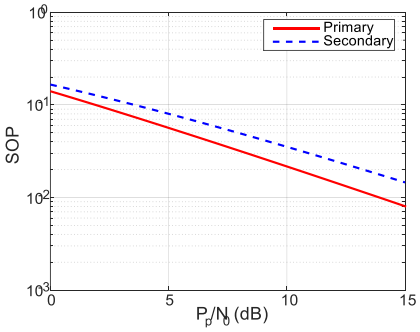
$$\mathcal{O}_p(C_0) = \Pr\{\tilde{C}_p < C_0\} \quad (32)$$

SOP cho x_s được biểu diễn như sau

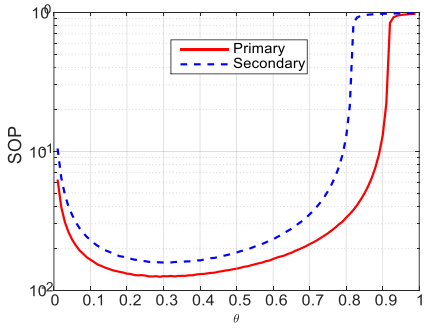
$$\mathcal{O}_s(C_0) = \Pr\{\tilde{C}_s < C_0\} \quad (33)$$

3. CÁC KẾT QUẢ MINH HỌA

SOP của cả truyền thông sơ cấp và truyền thông thứ cấp trong EHON được đánh giá theo các thông số kỹ thuật quan trọng. Vì mục đích minh họa nên một số thông số kỹ thuật được chọn ngẫu nhiên như máy thu sơ cấp R tại $(0.4, -0.2)$, máy phát sơ cấp T tại $(-0.2,\ 0.2)$, thiết bị nghe lén E tại $(0.5, -0.1)$, máy thu thứ cấp D tại $(0.5,\ 0.0)$, máy phát thứ cấp S tại $(d,\ 0.0)$, hiệu suất chuyển đổi năng lượng $\eta = 0.9$, số mũ suy hao đường truyền $\rho = 3$. Hơn nữa, những hình sau đây được tạo ra với tập hợp các thông số kỹ thuật (tỷ số công suất phát sơ cấp trên nhiễu $P_p = N_0 = 10$ dB, $d = 0.0$, hệ số phân chia công suất $\lambda = 0.6$, hệ số phân bổ công suất cho tín hiệu sơ cấp và tín hiệu thứ cấp $\kappa = 0.6$, hệ số phân bổ công suất cho tín hiệu mong muốn và nhiễu nhân tạo $\theta = 0.7$, mức bảo mật mục tiêu $C_0 = 0.1$ bits/s/Hz, hệ số phân chia thời gian $\alpha = 0.4$) trừ khi có trường hợp đặc biệt. Mô phỏng Monte-Carlo được dùng để tạo ra tất cả các kết quả trong phần này với số lần hiện thực (realization) là 10^7.



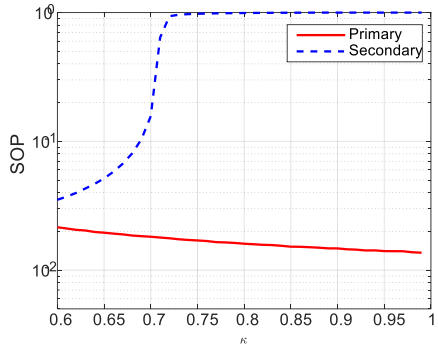
Hình 2. SOP theo P_p/N_0



Hình 3. SOP theo θ

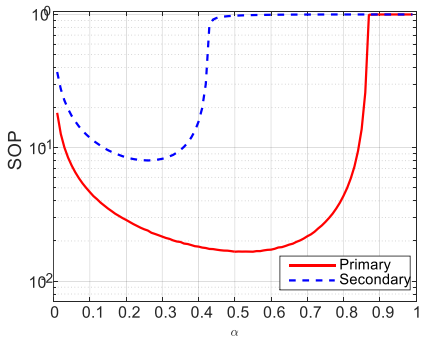
Hình 2 biểu diễn SOP theo P_p / N_0. Hình này cho thấy rằng hiệu năng bảo mật tỷ lệ thuận với P_p / N_0. Kết quả này được giải thích như sau. Tăng P_p / N_0 tạo điều kiện cho S thu thập thêm năng lượng từ T và do đó, làm tăng SINR trong giai đoạn 2 và giảm SOP. Hơn nữa, hiệu năng bảo mật của truyền thông sơ cấp tốt hơn hiệu năng bảo mật của truyền thông thứ cấp. Điều này là do trong tổng lượng công suất θP_s được dành để truyền dữ liệu hợp pháp thì S phân bổ 60% ($\kappa = 0.6$) lượng này để khuếch đại và chuyển tiếp tín hiệu sơ cấp và 40% $(1-\kappa = 0.4)$ để gửi dữ liệu thứ cấp.

Hình 3 cho thấy SOP theo θ. Hình này cho thấy rằng hiệu năng bảo mật của cả truyền thông thứ cấp và truyền thông sơ cấp được tối đa ở các giá trị tối ưu của θ, mà cân bằng công suất phát cho các thông điệp (sơ cấp và thứ cấp) hợp pháp và nhiễu nhân tạo. Ngoài ra, hiệu năng bảo mật tốt nhất của truyền thông sơ cấp cao hơn so với truyền thông thứ cấp. Điều này có thể được hiểu từ thực tế rằng $\kappa = 0.6$ sẽ phân bổ nhiều năng lượng hơn để S truyền thông điệp của T so với truyền thông điệp của S.

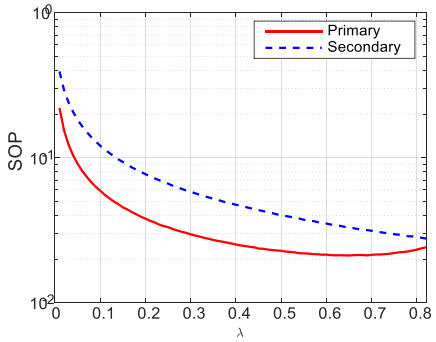


Hình 4. SOP theo κ

Hình 4 minh họa SOP theo κ. Các kết quả cho thấy rằng tăng κ nâng cao hiệu năng bảo mật của truyền thông sơ cấp (nghĩa là $\mathcal{O}_p$ giảm) trong khi làm giảm hiệu năng của truyền thông thứ cấp (nghĩa là $\mathcal{O}_s$ tăng). Điều này là hiển nhiên vì κ biểu diễn phần trăm công suất phát của S được phân bổ cho tín hiệu của T trong khi $1-\kappa$ tượng trưng cho phần trăm công suất phát của S được phân bổ cho tín hiệu của S. Do đó, tăng κ làm giảm $\mathcal{O}_p$ nhưng lại làm tăng $\mathcal{O}_s$. Hơn nữa, truyền thông thứ cấp luôn dừng hoạt động đối với một số phạm vi nào đó của κ. Ví dụ: $\mathcal{O}_s$ = 1 khi $\kappa \geq 0.75$ như trong Hình 4. Điều này được hiểu như sau. κ lớn có nghĩa là phần trăm công suất phát của S được phân bổ cho tín hiệu của S là nhỏ và do đó, D nhận được ít năng lượng hơn để giải mã thông tin của S, dẫn đến sự kiện dừng hoạt động.



Hình 5. SOP theo α



Hình 6. SOP theo λ

Hình 5 biểu diễn SOP theo α với $\kappa = 0.7$. Hình này cho thấy rằng khả năng bảo mật của cả truyền thông thứ cấp và truyền thông sơ cấp được tối đa với sự lựa chọn tối ưu của α. Giá trị tối ưu của α mà làm tối thiểu SOP được xác định và được giải thích tương tự như các hình trước. Hơn nữa, cả truyền thông thứ cấp và truyền thông sơ cấp bị dừng hoàn toàn với giá trị lớn của α. Ví dụ: $\alpha \geq 0.87$ gây ra $\mathcal{O}_p = 1$. Điều này là do giá trị lớn của α làm giảm đáng kể dung lượng bảo mật trong giai đoạn 2, gây ra sự kiện dừng bảo mật.

Hình 6 minh họa SOP theo λ. Các kết quả cho thấy rằng tăng λ sẽ cải thiện khả năng bảo mật của truyền thông thứ cấp. Nguyên nhân là do tăng λ làm tăng năng lượng thu thập nhưng lại làm giảm công suất phát tín hiệu của T trong tín hiệu thu tại S trước khi khuếch đại tín hiệu của T; do đó, công suất để truyền dữ liệu của S cao hơn trong giai đoạn 2, mà sau cùng làm giảm $\mathcal{O}_s$. Tuy nhiên, λ có thể được chọn một cách hợp lý để tối ưu hiệu năng bảo mật của truyền thông sơ cấp. λ tối ưu mà làm cho $\mathcal{O}_p$ tối thiểu là để cân bằng giữa năng lượng thu thập được và công suất phát tín hiệu của T trong tín hiệu thu tại S. Ngoài ra, hiệu năng bảo mật tốt nhất của truyền thông sơ cấp cao hơn so với truyền thông thứ cấp là do $\kappa = 0.6$. Đây là nhận xét tương tự được rút ra từ các hình trước đó.

4. KẾT LUẬN

Bài báo này đã nghiên cứu EHON, trong đó máy phát thứ cấp hoạt động theo cơ chế khuếch đại và chuyển tiếp nhằm chuyển tiếp tín hiệu của máy phát sơ cấp cũng như truyền tín hiệu riêng. Máy phát thứ cấp tự cung cấp năng lượng bằng cách thu thập năng lượng RF và tự bảo mật thông tin sơ cấp và thông tin thứ cấp chống lại những thiết bị nghe lén bằng cách tạo ra nhiễu nhân tạo. Hiệu năng bảo mật của cả truyền thông thứ cấp và truyền thông sơ cấp được đánh giá thông qua tiêu chí quan trọng SOP. Nhiều kết quả được cung cấp để hiểu rõ hơn về ảnh hưởng của nhiễu nhân tạo đối với hiệu năng bảo mật của EHON theo các thông số kỹ thuật quan trọng. Ngoài ra, các thông số kỹ thuật tối ưu đã được tìm thấy thông qua các tìm kiếm toàn diện. Các thông số kỹ thuật tối ưu này đóng vai trò quan trọng trong hướng dẫn thiết kế hệ thống.

TÀI LIỆU THAM KHẢO

1. Saad W.K., Shayea I., Hamza B.J., Azizan A., Ergen M. and Alhammadi A. - Performance evaluation of mobility robustness optimisation (MRO) in 5G network with various mobility speed scenarios. IEEE Access **10** (2022) 60955-60971.
2. Panjaitan S.D., Tjen J., Sanjaya B.W., Wigyarianto F.T.P. and Khouw S. - A forecasting approach for IoT-Based energy and power quality monitoring in buildings. IEEE Transactions on Automation Science and Engineering (2022) 1-9.
3. Boiko J., Pyatin I. and Eromenko O. - Analysis of signal synchronization conditions in 5G mobile information technologies. IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) (2022) 1-6.
4. Ho-Van K. and Do-Dac T. - Overlay networks with jamming and energy harvesting: security analysis. Arabian Journal for Science and Engineering **46** (2021) 9713-9724.
5. Ropokis G.A. and Bithas P.S. - Wireless powered relay networks: Rate optimal and power consumption-aware WPT/SWIPT. IEEE Transactions on Vehicular Technology **71** (8) (2022) 8574-8590.
6. Le-Thanh T. and Ho-Van K. - Effect of hardware imperfections and energy scavenging non-linearity on overlay networks in κ-μ shadowed fading. Arabian Journal for Science and Engineering **47** (2022) 14601-14616.

7. Wu Y., Ji G., Wang T., Qian L., Lin B. and Shen X. - Non-orthogonal multiple access assisted secure computation offloading via cooperative jamming. IEEE Transactions on Vehicular Technology **71** (7) (2022) 7751 - 7768 .
8. Dang-Ngoc H., Ho-Quoc B., and Ho-Van K. - Key secrecy performance metrics of overlay networks with energy scavenging and artificial noise. 2020 4th International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom) (2020) 77–81.
9. Xu M., Jing T., Fan X., Wen Y., and Huo Y. - Secure transmission solutions in energy harvesting enabled cooperative cognitive radio networks. 2018 IEEE Wireless Communications and Networking Conference (WCNC) (2018) 1-6.
10. Dang-Ngoc H., Ho-Van K., and Do-Dac T. - Secrecy analysis of overlay mechanism in radio frequency energy harvesting networks with jamming under Nakagami-m fading. Wireless Personal Communications **120** (2021) 447-479.
11. Su R., Wang Y., and Sun R. - Secure cooperative transmission in cognitive AF relay systems with destination-aided jamming and energy harvesting. 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC) (2019) 1-5.
12. Li M., Yin H., Huang Y., Wang Y., and Yu R. - Physical layer security in overlay cognitive radio networks with energy harvesting. IEEE Transactions on Vehicular Technology **67** (11) (2018) 11274-11279.
13. Pham-Thi-Dan N., Ho-Quoc B., Ho-Van K. et al. - Secrecy throughput analysis of energy scavenging overlay networks with artificial noise, 2020 International Conference on Advanced Technologies for Communications (ATC) (2020) 90-94.
14. Su R., Wang Y., and Sun R. - Destination-assisted jamming for physical-layer security in SWIPT cognitive radio systems. 2018 IEEE Wireless Communications and Networking Conference (WCNC) (2018) 1-6.
15. Wang D., Zhou F., and Leung V. C. - Primary privacy preserving with joint wireless power and information transfer for cognitive radio networks. IEEE Transactions on Cognitive Communications and Networking **6** (2) (2020) 683-693.

ABSTRACT

SECURITY IN ENERGY HARVESTING OVERLAY-BASED COGNITIVE RADIO NETWORKS

Tran Trong Hieu[1*], Le Thanh Toi[1], Ho Van Khuong[2]
[1]*Ho Chi Minh City University of Food Industry*
[2]*Ho Chi Minh City University of Technology*
*Email: *hieutt@hufi.edu.vn*

This paper proposes a security solution for an energy harvesting overlay-based cognitive radio network. The solution applies artificial noise to jam the received signal at the eavesdropper. The security performance of this network is evaluated through the secrecy outage probability. Multiple results are provided to derive insights into the security of this network when artificial noise is applied, thereby determining optimum system parameters for maximum network security. Remarkably, primary/secondary communications can be secured at different levels by dynamically adjusting many system parameters of the proposed solution.

Keywords: Secrecy outage probability, cognitive radio network, energy harvesting, artificial noise.