ĐÁNH GIÁ HIỆU NĂNG BẢO MẬT CỦA MẠNG VÔ TUYẾN CHUYỂN TIẾP VÀ GÂY NHIỄU CÓ LỰA CHỌN HAI CHẶNG

Chu Tiến Dũng[1*], Võ Nguyễn Quốc Bảo[2], Nguyễn Tùng Hưng[3]

Tóm tắt: *Bảo mật thông tin ở lớp vật lý đang thu hút được nhiều sự quan tâm của các nhà nghiên cứu. Cụ thể, gây nhiễu nhân tạo đang là một cách tiếp cận hiệu quả trong truyền thông hợp tác, kỹ thuật này được gọi là hợp tác gây nhiễu. Cho đến nay, hầu hết các nghiên cứu đều sử dụng kỹ thuật Khuếch đại và Chuyển tiếp (Decode and Forward - DF). Trong bài báo này, chúng tôi quan tâm đến giao thức Ngẫu nhiên và Chuyển tiếp (Random and Forward - RF), nút chuyển tiếp dữ liệu đến đích là nút được chọn. Để đánh giá hiệu năng bảo mật của mô hình đề xuất, chúng tôi đưa ra biểu thức dạng đóng của Xác suất dừng bảo mật (Secrecy Outage Probability - SOP), Xác suất bảo mật khác không (Non-zero Secrecy Capacity Probability - PrNZ) và Dung lượng bảo mật trung bình (Average Secure Capacity - ASC). Cuối cùng, chúng tôi thực hiện mô phỏng Monte-Carlo để chứng minh các phân tích.*

Từ khóa: Xác suất dừng bảo mật, Xác suất bảo mật khác không, Dung lượng bảo mật trung bình, Chuyển tiếp và gây nhiễu có lựa chọn.

1. ĐẶT VẤN ĐỀ

Ngày nay, hệ thống thông tin vô tuyến cũng được mở rộng và phát triển không ngừng, các thiết bị di động được người dùng sử dụng rộng rãi với nhiều dịch vụ được cung cấp bởi các nhà cung cấp dịch vụ viễn thông. Do đặc tính quảng bá của kênh truyền vô tuyến, các thiết bị phát đều có thể bị nghe lén bởi bất kỳ thiết bị thu nào trong vùng phủ sóng nên người sử dụng hệ thống thông tin vô tuyến đứng trước nguy cơ mất an toàn dữ liệu. Để đảm bảo an toàn thông tin cho hệ thống truyền thông vô tuyến, các hệ thống truyền thông truyền thống thường thực hiện mã mật tín hiệu bằng các thuật toán mã đối xứng, mã không đối xứng, các thuật toán này thường được áp dụng ở lớp ứng dụng. Tuy nhiên, do hệ thống truyền thông vô tuyến được phân bố trên địa bàn rộng, các thiết bị đầu cuối có tính di động cao và thông tin được truyền lan trong môi trường vô tuyến pha đinh nhanh... Do đó, sử dụng kỹ thuật mã hóa và giải mã sẽ khó khăn và kém hiệu quả.

Để khắc phục những hạn chế về bảo mật của hệ thống truyền thông vô tuyến, gần đây các nhà nghiên cứu trên thế giới tập trung nghiên cứu, khảo sát các đặc tính vật lý của hệ thống truyền thông vô tuyến để cải thiện hiệu năng bảo mật của hệ thống.

Tiên phong trong nghiên cứu về bảo mật lớp vật lý phải nói đến phân tích lý thuyết về lý thuyết bảo mật thông tin của Shannon [1], theo đó mức độ bảo mật của

hệ thống thông tin vô tuyến phụ thuộc vào số lượng thông tin những người nghe lén biết được. Hệ thống chỉ có thể đạt được bảo mật hoàn toàn khi người nghe lén không thu được thông tin. Sau đó, trong nghiên cứu [2], Wyner chỉ ra rằng khi kênh truyền của người sử dụng hợp pháp có điều kiện truyền lan tốt hơn so với người nghe trộm thì có thể đạt được bảo mật hoàn hảo mà không cần phải mật mã hóa dữ liệu. Kết luận này cũng đã được mở rộng trong [3] qua kênh Gaussian, tác giả chỉ ra rằng dung lượng bảo mật là sự khác nhau giữa dung lượng của kênh hợp pháp và kênh nghe lén. Tuy nhiên, khi các điều kiện kênh trong mạng thông tin vô tuyến không thuận lợi cho người dùng hợp pháp, tỷ lệ bảo mật có thể rất thấp hoặc thậm chí giảm xuống không.

Trong các nghiên cứu về bảo mật lớp vật lý, giải pháp truyền thông hợp tác đang được nhiều nghiên cứu và được đánh giá là một trong những giải pháp hiệu quả. Mục đích của bảo mật lớp vật lý trong truyền thông hợp tác là ngăn chặn quá trình nghe lén thông tin lan truyền từ nút nguồn sang nút đích, quá trình hợp tác chuyển tiếp thông tin thông thường là ngẫu nhiên. Để đạt được mức độ bảo mật cao hơn, một số giải pháp như: i) lựa chọn nút chuyển tiếp đã được đề xuất nhằm tăng độ lợi của kênh hợp pháp; ii) hợp tác gây nhiễu làm hạn chế khả năng thu nhận và giải mã thông tin của nút nghe lén.

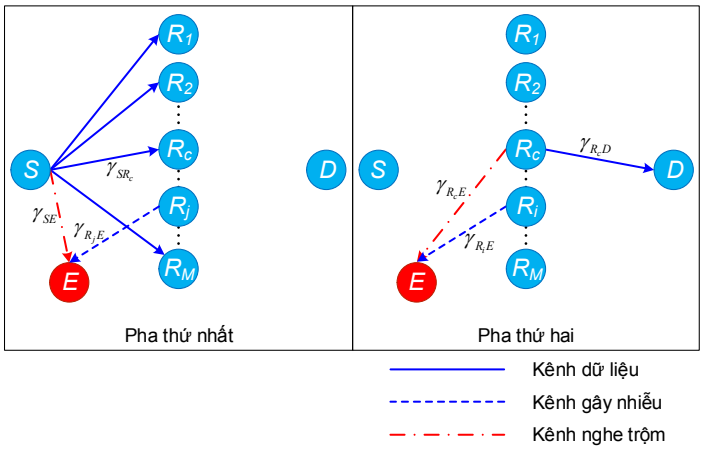
Trong bài báo [4], tác giả và các cộng sự nghiên cứu hiệu năng bảo mật của mạng vô tuyến hợp tác hai chặng sử dụng kỹ thuật DF, có sự hiện diện của một nút nghe lén. Kết quả của bài báo, tác giả đưa ra được biểu thức dạng đóng của dung lượng bảo mật egodic. Trong [5], Wang lại tiếp tục khảo sát với cùng mô hình trong [4] với những phân tích sâu hơn như ảnh hưởng của trạng thái kênh truyền không hoàn hảo lên mô hình và có sự hiện diện của nhiều nút nghe lén, tuy nhiên, bài báo cũng chỉ dừng lại ở kết quả dung lượng bảo mật trung bình và tối ưu hệ số phân bổ công suất tại các nút chuyển tiếp. Trong [6], tác giả đề xuất mô hình mạng truyền thông hợp tác hai chiều bằng kỹ thuật chuyển tiếp DF. Trong bài báo [7], khảo sát một mạng vô tuyến chuyển tiếp hai chặng sử dụng kỹ thuật Khuếch đại và Chuyển tiếp (Amplify and Forward - AF), có sự hiện diện của một nút nghe lén. Kết quả bài báo, tác giả đề xuất ba kịch bản để so sánh, đó là: kỹ thuật lựa chọn nút theo giá trị SNR tức thời; lựa chọn nút chuyển tiếp thông thường; lựa chọn nút gây nhiễu thông thường và lựa chọn nút chuyển tiếp tối ưu. Trong [8], bài viết đề xuất mô hình mạng vô tuyến hợp tác gồm bốn nút, đánh giá hiệu năng bảo mật của mô hình đề xuất khi nút chuyển tiếp đóng vai trò là chuyển tiếp hay gây nhiễu. Hai kịch bản đã được khảo sát và so sánh trong [8], đó là kịch bản truyền thông trực tiếp kết hợp với gây nhiễu và kịch bản truyền thông chuyển tiếp. Trong [9], kỹ

thuật chuyển tiếp RF đã được nghiên cứu đối với hệ thống truyền thông vô tuyến hợp tác, tuy nhiên vấn đề bảo mật chưa được đề cập tới.

Trong bài báo này, chúng tôi nghiên cứu khả năng bảo mật của hệ thống hệ thống truyền thông vô tuyến hợp tác sử dụng kỹ thuật chuyển tiếp RF để nút nghe lén không kết hợp được dữ liệu ở các chặng. Giả thiết mô hình kênh là pha đinh Rayleigh, bài báo sẽ khảo sát và phân tích xác suất dừng và xác suất dung lượng bảo mật khác không, dung lượng bảo mật trung bình nhằm đánh giá hiệu năng bảo mật của hệ thống. Bên cạnh đó, tác giả cũng thực hiện so sánh hiệu năng bảo mật của hệ thống truyền thông vô tuyến hợp tác gây nhiễu và chuyển tiếp có lựa chọn với gây nhiễu và chuyển tiếp ngẫu nhiên.

Phần còn lại của bài báo được tổ chức như sau: Mục 2 mô tả mô hình hệ thống. Trong mục 3, chúng tôi phân tích tính toán tham số đánh giá hiệu năng bảo mật của mô hình đề xuất. Kết quả mô phỏng được trình bày trong mục 4. Cuối cùng, chúng tôi thực hiện kết luận kết quả đạt được của bài báo trong mục 5.

2. MÔ HÌNH HỆ THỐNG



Hình 1. *Mô hình hệ thống.*

Xem xét một mạng vô tuyến hợp tác được minh họa theo hình 1. Trong mô hình, gồm có một nút nguồn - S và một nút đích - D. Giả sử, không có sự kết nối trực tiếp từ nút nguồn đến nút đích, việc truyền thông giữa hai nút phụ thuộc hoàn toàn vào sự giúp đỡ của M nút chuyển tiếp R_n với $n = 1,2,\ldots,M$. Tồn tại một nút nghe lén - E - cố gắng thu thập thông tin được phát ra của nút nguồn và nút chuyển tiếp trong quá trình truyền dữ liệu. Tất cả các nút trong mô hình được trang bị một anten và hoạt động ở chế độ bán song công. Chúng tôi giả định rằng, nút phát có đầy đủ thông tin trạng thái – CSI – của cả hai kênh chính và kênh nghe trộm. Như vậy, quá trình truyền dữ liệu từ nguồn đến đích xảy ra trong hai pha.

Trong pha đầu tiên, nút nguồn thực hiện phát quảng bá thông tin, lúc này $M-1$ nút chuyển tiếp và kể cả nút nghe lén đều thu nhận được thông tin. Cũng trong pha này, để ưu tiên cho việc gây nhiễu nhằm hạn chế nút nghe lén thu được dữ liệu từ nút nguồn, nút chuyển tiếp có độ lợi kênh truyền cao nhất đến nút nghe lén sẽ được lựa chọn để thực hiện gây nhiễu cho nút nghe lén, ký hiệu là R_J. Ta ký hiệu R_c là nút chuyển tiếp được lựa chọn để chuyển tiếp thông tin từ nguồn đến đích ở pha tiếp theo với $R_c \in (1,2,\ldots,M-1)$, γ_{SR_c} là độ lợi kênh truyền từ S đến R_c và γ_{R_JE} là độ lợi kênh truyền từ R_J đến E.

Vì vậy, $\gamma_{R_JE} = \arg\max_{n=1,2,\ldots,M} \gamma_{R_nE}.$ (1)

Với toàn bộ công suất phát của nút nguồn là P, ta có thể phân bổ công suất cho nút S và nút chuyển tiếp R_J tương ứng là αP và $(1-\alpha)P$, giá trị α để đảm bảo công suất thu tại nút nghe lén không vượt quá P, với $0 < \alpha \le 1$. Do đó, tương tự như trong [10], dung lượng kênh truyền của đường truyền từ S đến R_c, và của R_J đến E được biểu diễn như sau:

$$C_1^{\text{Data}} = \frac{1}{2}\log_2\left(1+\frac{\alpha P\gamma_{SR_c}}{N_0}\right), \quad (2)$$

$$C_1^{Eve} = \frac{1}{2}\log_2\left(1+\frac{\alpha P\gamma_{SE}}{N_0+(1-\alpha)P\gamma_{R_JE}}\right), \quad (3)$$

trong đó, N_0 là biến ngẫu nhiên của tạp âm Gaussian, giá trị $1/2$ cho biết quá trình truyền tin được diễn ra trong hai khe thời gian.

Dung lượng bảo mật của pha đầu tiên là một đại lượng lớn hơn không và được định nghĩa là sự chênh lệch giữa dung lượng chuẩn hóa tức thời của kênh dữ liệu và kênh nghe lén trong pha đầu tiên [11], cụ thể được biểu diễn như biểu thức sau:

$$C_1^{Sec} = \max\left(0, C_1^{\text{Data}} - C_1^{Eve}\right). \quad (4)$$

Trong pha thứ hai, để ưu tiên cho việc chuyển tiếp dữ liệu đến đích, nút chuyển tiếp có độ lợi kênh truyền cao nhất đến đích được lựa chọn để hợp tác chuyển tiếp dữ liệu đến đích. Nút chuyển tiếp tốt nhất đó không phải là nút gây nhiễu R_J tại pha thứ nhất. Sau khi lựa chọn được nút chuyển tiếp tốt nhất để chuyển dữ liệu, nút chuyển tiếp có độ lợi kênh truyền tốt nhất đến nút nghe lén trong số $M-1$ nút chuyển tiếp còn lại được lựa chọn làm nút gây nhiễu cho nút nghe lén (ký hiệu là R_i). Lưu ý rằng, tất cả các hệ số kênh truyền bị thay đổi sau mỗi pha, vì vậy nút gây nhiễu R_i tại pha này có thể là giống hoặc khác với nút gây nhiễu tại pha thứ

nhất. Trong pha này, ta quan tâm đến độ lợi kênh truyền từ R_c đến D, và từ R_i đến E, chúng được biểu diễn tương ứng như hai biểu thức dưới đây:

$$\gamma_{R_cD} = \max_{\substack{n=1,2,\ldots,M \\ n\neq J}} \gamma_{R_nD}, \tag{5}$$

$$\gamma_{R_iE} = \max_{\substack{n=1,2,\ldots,M-1 \\ n\neq c}} \gamma_{R_nE}. \tag{6}$$

Tương tự như trên, công suất phát của nút R_c được phân bố giống như công suất phát của nút nguồn là αP, trong khi đó công suất phát của nút R_i là $(1-\alpha)P$. Do đó, dung lượng kênh truyền từ R_c đến D, và từ R_i đến E là:

$$C_2^{D\text{ata}} = \frac{1}{2}\log_2\left(1+\frac{\alpha P\gamma_{R_cD}}{N_0}\right), \tag{7}$$

$$C_2^{Eve} = \frac{1}{2}\log_2\left(1+\frac{\alpha P\gamma_{R_cE}}{N_0+(1-\alpha)P\gamma_{R_iE}}\right). \tag{8}$$

Như vậy, dung lượng bảo mật của pha thứ hai được biểu diễn như biểu thức sau:

$$C_2^{\text{Sec}} = \max(0, C_2^{Data} - C_2^{Eve}). \tag{9}$$

3. PHÂN TÍCH HIỆU NĂNG BẢO MẬT

3.1. Xác suất dừng bảo mật - Secrecy Outage Probability (SOP)

Để đưa suy hao đường truyền vào trong tính toán, ta mô hình hóa λ_{SR_c} bởi $\lambda_{SR_c} = d_{SR_c}^{\beta}/\overline{\gamma}$ với $\overline{\gamma} = P/N_0$ và $d_{SR_c}^{\beta}$ là khoảng cách từ S đến R_c và β là hệ số suy hao đường truyền.

Trước hết, xác suất dừng bảo mật của pha đầu tiên được tính tương tự như các nghiên cứu [10, 12, 13].

$$P_{out}^{1} = \Pr\left(C_1^{Sec} < R_{th}\right) = \Pr\left(\frac{1+\alpha\overline{\gamma}\gamma_{SR_c}}{1+\dfrac{\alpha\overline{\gamma}\gamma_{SE}}{1+(1-\alpha)\overline{\gamma}\gamma_{R_JE}}} < \rho\right) = \Pr\left(X_1 < \frac{\rho-1}{\alpha} + \rho X_2\right), \tag{10}$$

trong đó, $\rho = 2^{2R_{th}}$ với R_{th} là ngưỡng tối đa để nút chuyển tiếp có thể giải mã tín hiệu. $X_1 = \overline{\gamma}\gamma_{SR_c}$, $X_2 = \dfrac{\overline{\gamma}\gamma_{SE}}{1+(1-\alpha)\overline{\gamma}\gamma_{R_JE}}$ là các biến ngẫu nhiên phân bố mũ với trung bình là $\lambda_{SR_c} = d_{SR_c}^{\beta}/\overline{\gamma}$.

Do đó,

$$P_{out}^{1} = \int_0^{+\infty} \left[1 - \exp\left(-\lambda_{SR_c} \frac{\rho - 1}{\alpha} \right) \exp\left(-\lambda_{SR_c} \rho x_2 \right) \right] f_{X_2}(x_2) dx_2 \\ = 1 - \exp\left(-\lambda_{SR_c} \frac{\rho - 1}{\alpha} \right) \int_0^{+\infty} \exp\left(-\lambda_{SR_c} \rho x_2 \right) f_{X_2}(x_2) dx_2, \quad (11)$$

trong đó, $f_{X_2}(x_2)$ là hàm phân bố xác suất (PDF) của X_2. Để tính được biểu thức (11) chúng ta tìm PDF của X_2.

Trước hết, ta viết lại: $X_2 = \frac{\overline{\gamma}\gamma_{SE}}{1 + (1-\alpha)\overline{\gamma}\gamma_{R_jE}} = \frac{Y_1}{1 + (1-\alpha)Y_2}$, với $Y_1 = \overline{\gamma}\gamma_{SE}, Y_2 = \overline{\gamma}\gamma_{R_jE}$.

Y_1 là biến ngẫu nhiên phân bố mũ với trung bình là $\lambda_{SE} = d_{SE}^{\beta} / \overline{\gamma}$, do đó:

$$F_{X_2}(x_2) = \int_0^{+\infty} \left[1 - \exp\left(-\lambda_{SE} x_2 \right) \exp\left(-\lambda_{SE} (1-\alpha) x_2 y_2 \right) \right] f_{Y_2}(y_2) dy_2, \quad (12)$$

trong đó, PDF của Y_2, được ký hiệu là $f_{Y_2}(y_2)$, được đưa ra như sau:

$$f_{Y_2}(y_2) = \frac{\partial F_{Y_2}(y_2)}{\partial y_2} \\ = \sum_{m=1}^{M} (-1)^{m+1} \binom{M}{m} m \lambda_{R_jE} \exp\left(-m \lambda_{R_jE} y_2 \right), \quad (13)$$

trong đó, $\lambda_{R_jE} = d_{R_jE}^{\beta} / \overline{\gamma}$.

Thay thế (13) vào (12), ta được:

$$F_{X_2}(x_2) = 1 - \exp\left(-\lambda_{SE} x_2 \right) \int_0^{+\infty} \exp\left(-\lambda_{SE} (1-\alpha) x_2 y_2 \right) f_{Y_2}(y_2) dy_2 \\ = 1 - \sum_{m=1}^{M} (-1)^{m+1} \binom{M}{m} \frac{\omega_m}{\omega_m + x_2} \exp\left(-\lambda_{SE} x_2 \right), \quad (14)$$

trong đó, $\omega_m \equiv \frac{m \lambda_{R_jE}}{\lambda_{SE}(1-\alpha)}$.

Chúng ta có được biểu thức (15) như sau:

$$f_{X_2}(x_2) = \sum_{m=1}^{M} (-1)^{m+1} \binom{M}{m} \left[\frac{\omega_m \exp\left(-\lambda_{SE} x_2 \right)}{\left(\omega_m + x_2 \right)^2} + \frac{\omega_m \lambda_{SE} \exp\left(-\lambda_{SE} x_2 \right)}{\omega_m + x_2} \right]. \quad (15)$$

Thay thế biểu thức (15) vào (11), ta có được xác suất dừng bảo mật của pha đầu tiên là:

$$\begin{aligned}P_{out}^{1} &= 1-\exp\left(-\lambda_{SR_c}\frac{\rho-1}{\alpha}\right)\sum_{m=1}^{M}(-1)^{m+1}\binom{M}{m}\Big[1-\left(\lambda_{SR_c}\rho+\lambda_{SE}\right)\omega_m\exp\left(\left(\lambda_{SR_c}\rho+\lambda_{SE}\right)\omega_m\right)\\ &\times E_1\left(\left(\lambda_{SR_c}\rho+\lambda_{SE}\right)\omega_m\right)+\omega_m\lambda_{SE}\exp\left(\left(\lambda_{SR_c}\rho+\lambda_{SE}\right)\omega_m\right)E_1\left(\left(\lambda_{SR_c}\rho+\lambda_{SE}\right)\omega_m\right)\Big]\\ &= 1-\exp\left(-\lambda_{SR_c}\frac{\rho-1}{\alpha}\right)\sum_{m=1}^{M}(-1)^{m+1}\binom{M}{m}\\ &\times\Big[1-\lambda_{SR_c}\rho\omega_m\exp\left(\left(\lambda_{SR_c}\rho+\lambda_{SE}\right)\omega_m\right)E_1\left(\left(\lambda_{SR_c}\rho+\lambda_{SE}\right)\omega_m\right)\Big],\end{aligned} \tag{16}$$

với $E_1(.)$ là tích phân hàm mũ.

Xác suất dừng bảo mật ở chặng thứ hai là:

$$\begin{aligned}P_{out}^{2} &= \Pr\left(C_2^{\text{Sec}} < R_{th}\right)\\ &= \Pr\left(\frac{1+\alpha\overline{\gamma}_{R_cD}}{1+\dfrac{\overline{\gamma}_{R_cE}}{1+(1-\alpha)\overline{\gamma}_{R_iE}}} < \rho\right)\\ &= \int_0^{+\infty} F_{Z_1}\left(\frac{\rho-1}{\alpha}+\rho x_2\right)f_{Z_2}\left(z_2\right)dz_2\end{aligned} \tag{17}$$

trong đó, $Z_2 = \dfrac{\overline{\gamma}_{R_cE}}{1+(1-\alpha)\overline{\gamma}_{R_iE}}$ và $Z_1 = \overline{\gamma}_{R_cD}$ là biến ngẫu nhiên phân bố mũ của hàm phân bố tích lũy (CDF), được cho bởi:

$$\begin{aligned}F_{Z_1}\left(x\right) &= \left(1-\exp\left(-\lambda_{R_cD}x\right)\right)^{M-1}\\ &= 1-\sum_{u=1}^{M-1}(-1)^{u+1}\binom{M-1}{u}\exp\left(-u\lambda_{R_cD}x\right).\end{aligned} \tag{18}$$

Vì vậy, ta có thể tính biểu thức (17) như sau:

$$P_{out}^{2} = 1-\sum_{u=1}^{M-1}(-1)^{u+1}\binom{M-1}{u}\exp\left(-u\lambda_{R_cD}\frac{\rho-1}{\alpha}\right)\int_0^{+\infty}\exp\left(-u\lambda_{R_cD}\rho z_2\right)f_{Z_2}\left(z_2\right)dz_2, \tag{19}$$

Tương tự như (15), ta tính được PDF của Z_2 như sau:

$$f_{Z_2}\left(z_2\right) = \sum_{m=1}^{M-1}(-1)^{m+1}\binom{M-1}{m}\left[\frac{\varphi_m\exp\left(-\lambda_{R_cE}z_2\right)}{\left(\varphi_m+z_2\right)^2}+\frac{\varphi_m\lambda_{R_cE}\exp\left(-\lambda_{R_cE}z_2\right)}{\varphi_m+z_2}\right], \tag{20}$$

trong đó, $\varphi_m \equiv \dfrac{m\lambda_{R_iE}}{(1-\alpha)\lambda_{R_cE}}$.

Thay thế (20) vào (19), chúng ta nhận được biểu thức xác suất dừng bảo mật của chặng thứ hai như biểu thức (21).

$$P_{out}^{2} = 1 - \sum_{u=1}^{M-1} (-1)^{u+1} \binom{M-1}{u} \exp\left(-u\lambda_{R_c D} \frac{\rho - 1}{\alpha}\right) \times \sum_{m=1}^{M-1} (-1)^{m+1} \binom{M-1}{m} \left[1 - u\lambda_{R_c D} \rho \varphi_m \exp\left(\left(\lambda_{R_I E} + \lambda_{R_c D} u\rho\right)\varphi_m\right) E_1\left(\left(\lambda_{R_I E} + \lambda_{R_c D} u\rho\right)\varphi_m\right)\right]. \quad (21)$$

Dung lượng bảo mật toàn hệ thống truyền thông hợp tác là dung lượng bảo mật nhỏ nhất của các chặng chuyển tiếp, được biểu diễn bởi biểu thức sau:

$$C_{e2e}^{Sec} = \min\left(C_1^{Sec}, C_2^{Sec}\right), \quad (22)$$

Từ (22), xác suất dừng bảo mật của toàn hệ thống được tính bởi:

$$P_{out}^{e2e} = 1 - \left(1 - P_{out}^{1}\right)\left(1 - P_{out}^{2}\right). \quad (23)$$

Thay thế (16) và (21) vào (23), ta có được kết quả của P_{out}^{e2e}.

3.2. Xác suất dung lượng bảo mật khác không - None-zero secrecy capacity probability (PrNZ)

Xác suất dung lượng bảo mật khác không là xác suất mà giá trị $C_{e2e}^{Sec} > 0$. Cụ thể, theo mô hình bài toán, P_{non}^{e2e} được biểu diễn như (24):

$$\begin{aligned} P_{non}^{e2e} &= \Pr\left(C_{e2e}^{Sec} > 0\right) \\ &= \Pr\left(\min\left(C_1^{Sec}, C_2^{Sec}\right) > 0\right) \\ &= \Pr\left(C_1^{Sec} > 0\right)\Pr\left(C_2^{Sec} > 0\right). \end{aligned} \quad (24)$$

Trước hết, ta tính xác suất dung lượng bảo mật khác không của pha thứ nhất $\Pr\left(C_1^{Sec} > 0\right)$, từ các biểu thức (2), (3) và (10), ta có:

$$\Pr\left(C_1^{Sec} > 0\right) = \Pr\left(\overline{\gamma}_{SR_c} > \frac{\overline{\gamma}_{SE}}{1 + (1-\alpha)\overline{\gamma}_{R_J E}}\right) = \int_0^{+\infty} \exp\left(-\lambda_{SR_c} x_2\right) f_{X_2}(x_2)\, dx_2, \quad (25)$$

Thay thế (15) vào (25), tương tự như tính toán ở trên, ta có:

$$\Pr\left(C_1^{Sec} > 0\right) = \sum_{m=1}^{M} (-1)^{m+1} \binom{M}{m} \left[1 - \lambda_{SR_c}\omega_m \exp\left(\left(\lambda_{SR_c} + \lambda_{SE}\right)\omega_m\right) E_1\left(\left(\lambda_{SR_c} + \lambda_{SE}\right)\omega_m\right)\right], \quad (26)$$

Xác suất dung lượng bảo mật khác không của pha thứ hai:

$$\begin{aligned} \Pr\left(C_2^{Sec} > 0\right) &= \Pr\left(\overline{\gamma}_{R_c D} > \frac{\overline{\gamma}_{R_c E}}{1 + (1-\alpha)\overline{\gamma}_{R_I E}}\right) \\ &= \sum_{u=1}^{M-1} (-1)^{u+1} \binom{M-1}{u} \int_0^{+\infty} \exp\left(-u\lambda_{R_c D} x\right) f_{Z_2}(z_2)\, dz_2. \end{aligned} \quad (27)$$

Thay thế (20) vào (27), ta có được biểu thức của dung lượng bảo mật khác không của pha thứ hai:

$$\Pr\left(C_2^{Sec}>0\right)=\sum_{u=1}^{M-1}(-1)^{u+1}\binom{M-1}{u}\sum_{m=1}^{M-1}(-1)^{m+1}\binom{M-1}{m}\left[1-u\lambda_{R_cD}\varphi_m\exp\left(\left(\lambda_{R_iE}+\lambda_{R_cD}u\right)\varphi_m\right)E_1\left(\left(\lambda_{R_iE}+\lambda_{R_cD}u\right)\varphi_m\right)\right] \quad (28)$$
$$\times\sum_{m=1}^{M-1}(-1)^{m+1}\binom{M-1}{m}\left[1-u\lambda_{R_cD}\varphi_m\exp\left(\left(\lambda_{R_iE}+\lambda_{R_cD}u\right)\varphi_m\right)E_1\left(\left(\lambda_{R_iE}+\lambda_{R_cD}u\right)\varphi_m\right)\right].$$

3.3. Dung lượng bảo mật trung bình - The average secrecy capacity (ACS)

Giá trị dung lượng bảo mật trung bình được tính bởi biểu thức

$$\bar{C}=\int_1^{+\infty}\frac{1-P_{out}^{e2e}}{\rho}d\rho. \quad (29)$$

Trước hết, ta viết lại biểu thức (23):

$$\begin{aligned}P_{out}^{e2e}=1-&\sum_{m=1}^{M}(-1)^{m+1}\binom{M}{m}\left[\exp\left(\frac{\lambda_{SR_c}}{\alpha}\right)\exp\left(-\frac{\lambda_{SR_c}}{\alpha}\rho\right)-\lambda_{SR_c}\rho\omega_m\exp\left(\frac{\lambda_{SR_c}}{\alpha}+\lambda_{SE}\omega_m\right)\right.\\&\left.\times\exp\left(-\lambda_{SR_c}\left(\omega_m-\frac{1}{\alpha}\right)\rho\right)E_1\left(\left(\lambda_{SR_c}\rho+\lambda_{SE}\right)\omega_m\right)\right]\sum_{u=1}^{M-1}(-1)^{u+1}\binom{M-1}{u}\\&\times\sum_{m=1}^{M-1}(-1)^{m+1}\binom{M-1}{m}\left[\exp\left(\frac{u\lambda_{R_cD}}{\alpha}\right)\exp\left(-\frac{u\lambda_{R_cD}}{\alpha}\rho\right)-u\lambda_{R_cD}\rho\varphi_m\exp\left(\frac{u\lambda_{R_cD}}{\alpha}+\lambda_{R_iE}\varphi_m\right)\right.\\&\left.\times\exp\left(-u\lambda_{R_cD}\left(\varphi_m-\frac{1}{\alpha}\right)\rho\right)\exp\left(\left(\lambda_{R_iE}+\lambda_{R_cD}u\rho\right)\varphi_m\right)E_1\left(\left(\lambda_{R_iE}+\lambda_{R_cD}u\rho\right)\varphi_m\right)\right].\end{aligned} \quad (30)$$

Thay thế P_{out}^{e2e} vào biểu thức (30), ta có được biểu thức chính xác của dung lượng bảo mật trung bình $\bar{C}$.

3.4. So sánh với phương pháp gây nhiễu và chuyển tiếp ngẫu nhiên

Tương tự như khảo sát với kịch bản chuyển tiếp và gây nhiễu có lựa chọn đã được giới thiệu ở phần trên. Tuy nhiên, kịch bản được phân tích theo phương pháp chuyển tiếp và gây nhiễu ngẫu nhiên.

3.4.1. Xác suất dừng bảo mật

Cũng tương tự như kịch bản chuyển tiếp và gây nhiễu có lựa chọn, giả sử công suất phát của nút S là αP, và công suất phát của nút gây nhiễu ngẫu nhiên R_k là $(1-\alpha)P$. Vậy, xác suất dừng bảo mật của pha thứ nhất được biểu diễn bởi:

$$\begin{aligned}P_{out}^{1}&=\Pr\left(C_1^{Sec}<R_{th}\right)\\&=\Pr\left(\frac{1+\alpha\bar{\gamma}\gamma_{SR_c}}{1+\frac{\alpha\bar{\gamma}\gamma_{SE}}{1+(1-\alpha)\bar{\gamma}\gamma_{R_kE}}}<\rho\right)\\&=\int_0^{+\infty}\left(1-\exp\left(-\lambda_{SR_c}\frac{\rho-1}{\alpha}-\lambda_{SR_c}\rho x_3\right)\right)f_{X_3}(x_3)dx_3,\end{aligned} \quad (31)$$

trong đó, $X_3 = \dfrac{\overline{\gamma\gamma}_{SE}}{1+(1-\alpha)\overline{\gamma\gamma}_{R_kE}}$.

Tính hàm PDF của X_3 ta được:

$$f_{X_3}(x_3) = \frac{\omega_0}{(\omega_0 + x_3)^2}\exp(-\lambda_{SE}x_3) + \frac{\omega_0\lambda_{SE}}{\omega_0 + x_3}\exp(-\lambda_{SE}x_3), \quad (32)$$

trong đó, $\omega_0 \equiv \dfrac{\lambda_{R_kE}}{\lambda_{SE}(1-\alpha)}$.

Do đó, xác suất dừng bảo mật tại pha thứ nhất của kịch bản này là:

$$P_{out}^1 = 1 - \exp\left(-\lambda_{SR_c}\frac{\rho-1}{\alpha}\right)\left[1 - \lambda_{SR_c}\rho\omega_0\exp\left(\left(\lambda_{SR_c}\rho + \lambda_{SE}\right)\omega_0\right)E_1\left(\left(\lambda_{SR_c}\rho + \lambda_{SE}\right)\omega_0\right)\right] \quad (33)$$

Tiếp theo, chúng tôi khảo sát pha thứ hai trong quá trình truyền tin của kịch bản chuyển tiếp và gây nhiễu ngẫu nhiên. Trong $M-1$ nút chuyển tiếp còn lại, hệ thống ngẫu nhiên lựa chọn một nút chuyển tiếp hoạt động với vai trò là nút gây nhiễu, ký hiệu là R_l. Giả sử như trên, nếu công suất phát của nút R_c là αP, khi đó công suất phát của nút gây nhiễu R_l sẽ là $(1-\alpha)P$. Do đó, xác suất dừng bảo mật của pha thứ hai được tính bởi biểu thức:

$$\begin{aligned} P_{out}^2 &= \Pr\left(C_2^{Sec} < R_{th}\right) \\ &= \Pr\left(\frac{1+\alpha\overline{\gamma\gamma}_{R_cD}}{1+\dfrac{\alpha\overline{\gamma\gamma}_{R_cE}}{1+(1-\alpha)\overline{\gamma\gamma}_{R_lE}}} < \rho\right). \end{aligned} \quad (34)$$

Tương tự như tính toán ở pha thứ nhất, ta có được xác suất dừng bảo mật của pha thứ hai theo biểu thức (35).

$$P_{out}^2 = 1 - \exp\left(-\lambda_{R_cD}\frac{\rho-1}{\alpha}\right)\left[1 - \lambda_{R_cD}\rho\omega_4\exp\left(\left(\lambda_{R_cD}\rho + \lambda_{R_cE}\right)\omega_4\right)E_1\left(\left(\lambda_{R_cD}\rho + \lambda_{R_cE}\right)\omega_4\right)\right], \quad (35)$$

trong đó, $\omega_4 \equiv \dfrac{\lambda_{R_lE}}{\lambda_{R_cE}(1-\alpha)}$.

Cuối cùng, ta có được dung lượng bảo mật của toàn trình là dung lượng bảo mật nhỏ nhất của hai pha.

$$C_{e2e}^{Sec} = \min\left(C_1^{Sec}, C_2^{Sec}\right). \quad (36)$$

Vì vậy, xác suất dừng bảo mật toàn trình được tính theo biểu thức:

$$P_{out}^{e2e} = 1 - \left(1 - P_{out}^{1}\right)\left(1 - P_{out}^{2}\right). \quad (37)$$

3.4.2. Dung lượng bảo mật khác không

Dung lượng bảo mật khác không là xác suất mà dung lượng bảo mật toàn trình C_{e2e}^{Sec} được tính bởi công thức:

$$\begin{aligned} P_{non}^{e2e} &= \Pr(C_{e2e}^{\mathrm{Sec}} > 0) \\ &= \Pr(C_{1}^{\mathrm{Sec}} > 0)\Pr(C_{2}^{\mathrm{Sec}} > 0) \end{aligned} \quad (38)$$

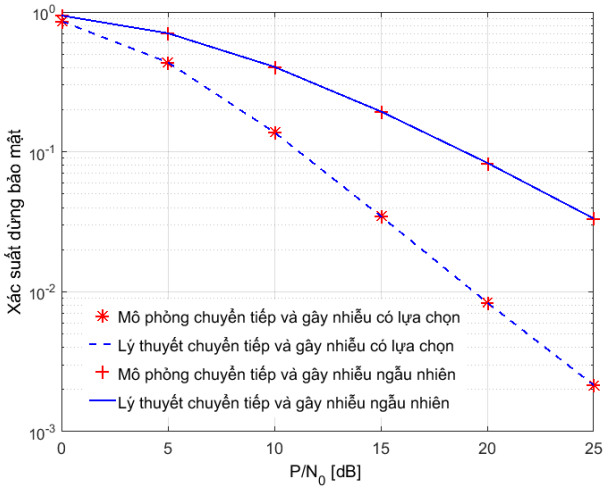
với $\Pr\left(C_1^{Sec} > 0\right)$ và $\Pr\left(C_2^{Sec} > 0\right)$ được biểu diễn như sau:

$$\Pr\left(C_1^{Sec} > 0\right) = 1 - \lambda_{SR_c}\omega_0 \exp\left(\left(\lambda_{SR_c} + \lambda_{SE}\right)\omega_0\right) E_1\left(\left(\lambda_{SR_c} + \lambda_{SE}\right)\omega_0\right), \quad (39)$$

$$\Pr\left(C_2^{Sec} > 0\right) = 1 - \lambda_{R_cD}\omega_4 \exp\left(\left(\lambda_{R_cD} + \lambda_{R_cE}\right)\omega_4\right) E_1\left(\left(\lambda_{R_cD} + \lambda_{R_cE}\right)\omega_4\right). \quad (40)$$

4. MÔ PHỎNG VÀ ĐÁNH GIÁ KẾT QUẢ

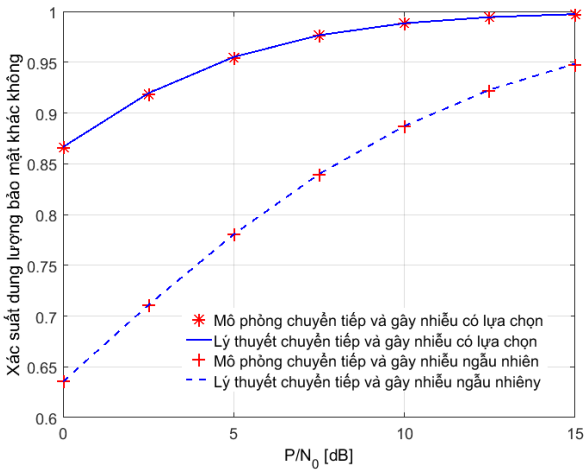
Trong phần này, chúng tôi thực hiện mô phỏng Monte-Carlo bằng phần mềm Matlab để kiểm chứng các kết quả đã được phân tích ở trên. Chúng tôi thực hiện mô phỏng đánh giá các tham số SOP, PrNZ và ACS của mô hình đề xuất trong các kịch bản khác nhau. Để minh họa cho mô hình hệ thống, ta xét trong không gian hai chiều Oxy với các nút được bố trị tại những vị trí sau: $R(0,0.4)$; $E(0.5,0.5)$; $S(0,0)$; $D(1,0)$; và hệ số suy hao đường truyền $\beta = 3$.



Hình 2. *Xác suất dừng bảo mật biểu diễn theo giá trị P/N_0, khi $M = 3$, $\alpha = 0,5$.*

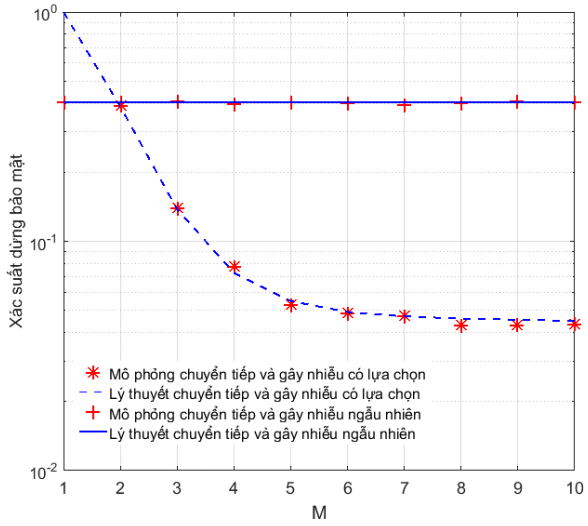
Trong hình 2, chúng tôi khảo sát ảnh hưởng của chuyển tiếp và gây nhiễu có lựa chọn lên mô hình hệ thống truyền thông hợp tác vô tuyến, và đánh giá tham số xác suất dừng bảo mật toàn trình của mô hình hệ thống P_{out}^{e2e} qua xác suất dừng P_{out}^{1} và

P_{out}^2 của hai pha. Khi khảo sát với $R_{th} = 1$, ta thấy xác suất dừng bảo mật của kịch bản chuyển tiếp và gây nhiễu có lựa chọn tốt hơn so với kịch bản chuyển tiếp và gây nhiễu ngẫu nhiên.



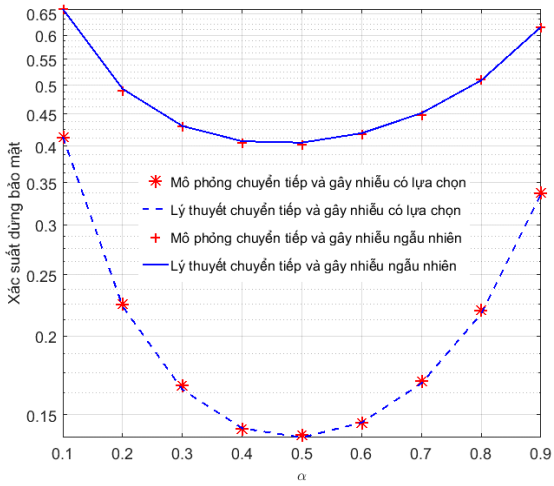
Hình 3. *Dung lượng bảo mật khác không biểu diễn theo giá trị P/N_0 khi $M = 3$, $\alpha = 0,5$ và $R_{th} = 1$.*

Trong hình 3, chúng tôi khảo sát, so sánh xác suất dung lượng bảo mật khác không của hai kịch bản. Khi giá trị tỉ số tín hiệu trên tạp âm P/N_0 thấp, lúc này xác suất dung lượng bảo mật khác không của kịch bản chuyển tiếp và gây nhiễu có lựa chọn tốt hơn xác suất dung lượng bảo mật khác không của kịch bản chuyển tiếp và gây nhiễu ngẫu nhiên. Tuy nhiên, khi giá trị P/N_0 tăng thì xác suất dung lượng bảo mật khác không của cả hai kịch bản tiến gần lại với nhau.



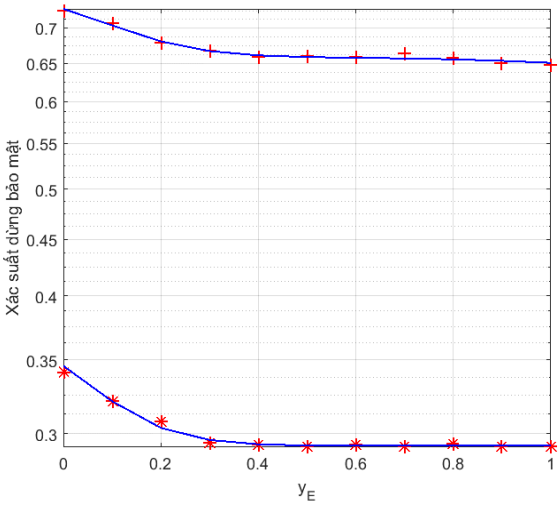
Hình 4. *Xác suất dừng bảo mật biểu diễn theo giá trị M khi $\alpha = 0,5$ và $R_{th} = 1$.*

Trong hình 4, chúng tôi mô phỏng dung lượng bảo mật của hai kịch bản. Quá trình mô phỏng cũng cho ta kết luận rằng phương pháp chuyển tiếp và gây nhiễu có lựa chọn có xác suất mất bảo mật giảm khi số lượng nút chuyển tiếp tăng. Kết quả mô phỏng cũng cho thấy xác suất dừng bảo mật ở gây nhiễu và chuyển tiếp ngẫu nhiên không thay đổi khi số nút chuyển tiếp thay đổi.



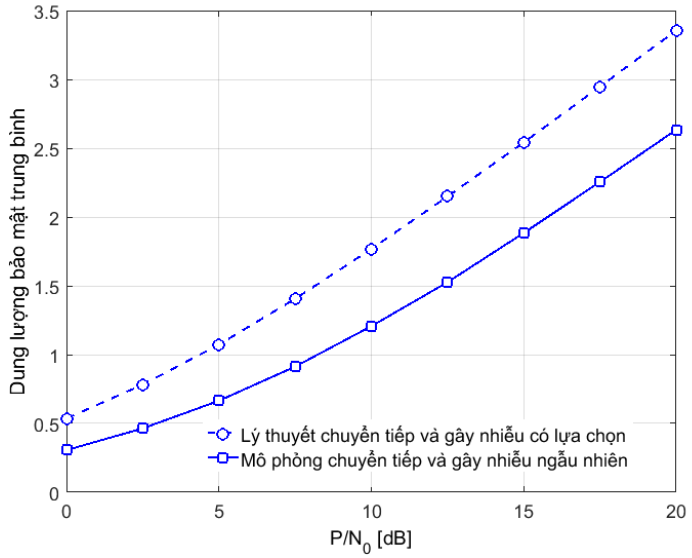
Hình 5. *Xác suất dừng bảo mật biểu diễn theo giá trị α khi M = 3 và R_{th} = 1.*

Trong hình 5, chúng tôi mô phỏng dung lượng bảo mật của hai kịch bản. Kết quả mô phỏng cho thấy xác suất dừng bảo mật của gây nhiễu và chuyển tiếp có lựa chọn thấp hơn so với gây nhiễu và chuyển tiếp ngẫu nhiên. Ở giá trị $\alpha = 0.5$ thì xác suất dừng bảo mật là tốt nhất, vì vậy việc phân bổ công suất cho nút phát và nút chuyển tiếp bằng nhau thì hiệu năng bảo mật của hệ thống là tốt nhất.



Hình 6. *Xác suất dừng bảo mật biểu diễn theo giá trị y_E khi α = 0,5, M = 3 và R_{th} = 1.*

Trong hình 6, chúng tôi mô phỏng dung lượng bảo mật của hai kịch bản. Kết quả mô phỏng cũng cho thấy kịch bản gây nhiễu và chuyển tiếp có lựa chọn có xác suất dừng bảo mật thấp hơn so với kịch bản gây nhiễu và chuyển tiếp ngẫu nhiên. Kết quả mô phỏng cũng cho thấy tồn tại một giá trị khoảng cách từ hệ thống đến nút nghe lén thì xác xuất dừng của hệ thống bằng không.



Hình 7. *Dung lượng bảo mật biểu diễn theo giá trị P/N_0 với $M = 3$, $\alpha = 0,5$.*

Trong hình 7, chúng tôi mô phỏng dung lượng bảo mật của hai kịch bản. Quá trình mô phỏng cũng cho ta kết luận rằng phương pháp chuyển tiếp và gây nhiễu có lựa chọn có dung lượng bảo mật trung bình tốt hơn so với phương pháp chuyển tiếp và gây nhiễu ngẫu nhiên, đặc biệt khi giá trị P/N_0 càng tăng thì dung lượng bảo mật trung bình của phương pháp chuyển tiếp và gây nhiễu có lựa chọn thể hiện rõ hiệu năng vượt trội.

5. KẾT LUẬN

Các nghiên cứu trước đây thường tập trung chủ yếu vào truyền dữ liệu đơn thuần mà không có sự hiện diện của người nghe lén hoặc sử dụng kỹ thuật lựa chọn nút chuyển tiếp và gây nhiễu ngẫu nhiên. Trong mô hình chúng tôi đề xuất, dữ liệu được chuyển tiếp bằng cách chọn nút tốt nhất và nút nghe lén bị gây nhiễu bởi nút chuyển tiếp được lựa chọn để tăng hiệu năng bảo mật của hệ thống, các nút chuyển tiếp trong mô hình sử dụng kỹ thuật RF.

Sự hợp tác giữa các nút chuyển tiếp trong mạng truyền thông vô tuyến được sử dụng cho truyền dữ liệu trong hai pha để tăng dung lượng bảo mật. Nút chuyển tiếp được lựa chọn để truyền dữ liệu giữa nguồn và đích, trong khi đó nút gây

nhiễu thực hiện gây nhiễu cho nút nghe lén. Kết quả bài báo cho thấy hiệu năng bảo mật vượt trội hơn hẳn của mô hình chuyển tiếp và gây nhiễu có lựa chọn với mô hình chuyển tiếp và gây nhiễu ngẫu nhiên.

TÀI LIỆU THAM KHẢO

[1]. H. Delfs and H. Knebl, *"Introduction to cryptography: Principles and applications," Springer (2nd edn)*, 2007.

[2]. A. D. Wyner, *"The wire-tap channel,"* Bell System Technical Journal, pp. 1355–1387, 1975.

[3]. S. K. Leung-Yan-Cheong and M. E. Hellman, *"The gaussian wire-tap channel,"* IEEE Trans. Inform. Theory, no. 1, pp. 451–456, 1978.

[4]. W. Chao, Wang Hui-Ming, *"Joint relay selection and artificial jamming power allocation for secure DF relay networks,"* in Communications Workshops (ICC), 2014 IEEE International Conference, pp. 819–824, 2014.

[5]. C. Wang, H.-M. Wang, and X.-G. Xia, *"Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks,"* Wirel. Commun., IEEE Trans., vol. 14, no. 2, pp. 589–605, 2015.

[6]. J. Wang, J. Chen, H. Duan, H. Ba, and J. Wu, *"Jammer selection for secure two-way DF relay communications with imperfect CSI," in* Advanced Communication Technology (ICACT), 2014 16th International Conference, pp. 300–303, 2014.

[7]. S. Ghose and R. Bose, *"Outage optimal relay selection strategy using destination-based jamming for secure communication in amplify-andforward relay networks,"* in Statistical Signal Processing (SSP), 2014 IEEE Workshop, pp. 404–407, 2014.

[8]. H. Deng, H.-M. Wang, W. Guo, and W. Wang, *"Secrecy transmission with a helper: To relay or to jam,"* Information Forensics and Security, IEEE Transaction, vol. 10, no. 2, pp. 293–307, 2015.

[9]. Jianhua Mo, Meixia Tao, and Yuan Liu, *"Relay Placement for Physical Layer Security: A Secure Connection Perspective"* IEEE Communications Letters, vol. 16, no.6, pp. 878-881, 2012.

[10]. V. N. Q. Bao and N. L. Trung, *"Multihop decode-and-forward relay networks: Secrecy analysis and relay position optimization,"* Journal on Electronics and Communication, vol. 2, 2012.

[11]. J. Barros and M. Rodrigues, *"Secrecy capacity of wireless channels,"* in Information Theory, 2006 IEEE International Symposium, pp. 356–360, Jul. 2006.

[12]. M. Z. I. Sarkar and T. Ratnarajah, *"Secrecy capacity and secure outage performance for rayleigh fading SIMO channel,"* IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 1900–1903, 2011.

[13]. H. M. F. He and W. Wang, *"Maximal ratio diversity combining enhanced security,"* IEEE Communications Letters, pp. 1–3, 2011.

ABSTRACT

SECRECY OUTAGE ANALYSIS OF DUAL-HOP NETWORKS WITH RELAY AND JAMMER SELECTION

In recent years, ensuring security of communications at the physical layer has attracted considerable attention. Particularly, transmitting artificial jamming signals to eavesdropper is one of effective approaches in multi-relay schemes, which is called cooperative jamming (CJ). Up to now, almost published literature on CJ have studied on the scenario in which the source transmits a single data stream to a single legitimate user in the existence of an eavesdropper. In this paper, we consider a cooperative relay protocol where one of achievable relays (R) is selected to help the communication between a source (S) and a destination (D) and some relays are used to generate artificial noises to a eavesdropper (E). In the proposed protocol, we assume that the jamming signals can be canceled from the received signals at D and R, except E. For performance evaluation, we derive expressions of Secure Outage Probability (SOP), Non-zero Secrecy Capacity Probability (PrNZ) and Average Secrecy Capacity (ASC) over Rayleigh fading channels. Finally, we present Monte Carlo simulations to verify the derivations.

Keywords: Probability of Non-zero Secrecy Capacity, Secrecy Outage Probability, Average Secrecy Capacity, Jammer selection.

Nhận bài ngày 10 tháng 3 năm 2017
Hoàn thiện ngày 10 tháng 4 năm 2017
Chấp nhận đăng ngày 01 tháng 5 năm 2017

Địa chỉ: [1] Đại học Thông tin liên lạc;
[2] Học viện Công nghệ Bưu chính Viễn thông;
[3] Phòng Thí nghiệm Trọng điểm An toàn thông tin.
[*] Email: chutiendung@tcu.edu.vn.