NGHIÊN CỨU HIỆU NĂNG MẠNG QUẢNG BÁ ĐA NGƯỜI DÙNG SỬ DỤNG MÃ FOUNTAIN VÀ KỸ THUẬT TẠO NHIỄU NHÂN TẠO TRÊN KÊNH NAKAGAMI-M

Nguyễn Văn Hiền, **Trần Trung Duy**, **Lê Quang Phú**, **Tân Hạnh**
Học Viện Công Nghệ Bưu Chính Viễn Thông Cơ Sở Tại Thành Phố Hồ Chí Minh

Tóm tắt— Bài báo này nghiên cứu hiệu năng mạng quảng bá đa người dùng sử dụng mã Fountain. Trong mô hình đề xuất, nút nguồn sử dụng mã Fountain để gửi cùng một dữ liệu đến một nhóm các nút đích. Hơn nữa, nhiều nút nghe lén xuất hiện trong mạng và cố gắng giải mã dữ liệu của nguồn. Do đó, kỹ thuật tạo nhiễu nhân tạo được áp dụng để làm giảm chất lượng của kênh nghe lén. Cụ thể, các nút ở gần các đích sẽ được dùng để tạo nhiễu lên các nút nghe lén. Chúng tôi đưa ra các công thức tường minh đánh giá chính xác xác suất dừng và xác suất mất bảo mật của mô hình đề xuất trên kênh Nakagami-*m*. Các kết quả mô phỏng Monte Carlo được thực hiện để kiểm chứng các công thức toán học, cũng như để phân tích sự tác động của các tham số hệ thống như số nút đích, số nút nghe lén, số nút tạo nhiễu và hệ số phân bổ công suất phát lên các hiệu năng hệ thống.

Từ khóa— Mã Fountain, mạng quảng bá đa người dùng, bảo mật lớp vật lý, xác suất dừng, xác suất mất bảo mật.

I. GIỚI THIỆU

Bảo mật lớp vật lý PLS (Physical-layer security) [1]-[3] là một kỹ thuật bảo mật đơn giản, trong đó dữ liệu có thể bảo mật nếu chất lượng của kênh dữ liệu (data channel) tốt hơn kênh nghe lén (eavesdropping channel). Vì vậy, các nhà nghiên cứu đã đưa ra các giải pháp nhằm nâng cao chất lượng của kênh dữ liệu và làm giảm chất lượng của kênh nghe lén. Một trong những kỹ thuật phổ biến để nâng cao chất lượng kênh dữ liệu là các kỹ thuật truyền/nhận phân tập (transmitting/receiving diversity), trong đó các thiết bị phát và thu hợp pháp trang bị nhiều anten để thực hiện truyền/nhận dữ liệu [4]-[6]. Đối với các thiết bị không thể trang bị nhiều anten (do giới hạn về kích thước như các thiết bị cảm biến, điện thoại di động, v.v.), các kỹ thuật chuyển tiếp kết hợp với chọn lựa nút chuyển tiếp cũng nâng cao chất lượng và độ lợi phân tập cho kênh dữ liệu [7]-[11]. Bên cạnh đó, kỹ thuật tạo nhiễu lên nút nghe lén sẽ làm giảm đáng kể chất lượng của kênh nghe lén, và do đó sẽ đạt được hiệu quả bảo mật cao. Kỹ thuật này với tên gọi là tạo nhiễu cộng tác CJ (Cooperative Jamming), trong đó nút tạo nhiễu (jammer) sẽ phát nhiễu lên nút nghe lén, đồng thời hợp tác với các máy thu hợp pháp để khử giao thoa mà nút này gây ra [12]-[13]. Trong các công trình [14]-[15], hiệu năng của mạng PLS được đánh giá thông qua xác suất dừng OP (Outage Probability) và xác suất mất bảo mật IP (Intercept Probability). Các kết quả đạt được từ các công trình [14]-[15] cho thấy có sự đánh đổi giữa OP và IP. Ví dụ, hệ thống nâng cao chất lượng dịch vụ (giảm OP) bằng cách tăng công suất cho máy phát. Tuy nhiên, hệ thống lại kém bảo mật hơn (tăng IP) do khả năng nghe lén tăng khi công suất phát lớn. Ngược lại, máy phát muốn giảm công suất phát để nâng cao hiệu quả bảo mật thông tin, nhưng lúc này OP của hệ thống lại tăng lên. Để có thể giảm IP mà vẫn đảm bảo được chất lượng dịch vụ OP, các công trình [16]-[17] đề xuất các kỹ thuật truyền/nhận phân tập, các kỹ thuật chọn lựa nút chuyển tiếp kết hợp với kỹ thuật tạo nhiễu nhân tạo.

Mã Fountain [18]-[19] có thể dễ dàng triển khai trong các hệ thống thông tin vô tuyến, trong đó một máy phát gửi liên tục các gói mã hóa đến các máy thu, cho đến khi các máy thu nhận đủ số lượng gói mã hóa để khôi phục dữ liệu gốc. Ta cũng lưu ý rằng các máy thu chỉ cần nhận đủ số lượng gói mã hóa mà không cần quan tâm gói nhận được cụ thể là gói nào. Vì vậy, mã Fountain tránh được việc máy phát phải gửi lại những gói mã hóa mà các máy thu không thể nhận được hoặc giải mã bị lỗi. Chính vì đặc điểm này, mã Fountain rất phù hợp với các mô hình mạng quảng bá đa người dùng. Tuy nhiên, bảo mật sẽ là một vấn đề cốt yếu trong các hệ thống vô tuyến sử dụng mã Fountain. Gần đây, các nhà nghiên cứu trong và ngoài nước đã đề xuất các mô hình hiệu quả nhằm nâng cao hiệu quả bảo mật [20]-[22]. Trong các tài liệu [20]-[21], các tác giả đề xuất các mô hình bảo mật lớp vật lý áp dụng cho mạng truyền thông vô tuyến sử dụng mã Fountain. Để bảo mật được thông tin, nút đích cần phải nhận đủ số gói mã hóa để khôi phục dữ liệu gốc trước nút nghe lén. Công trình [22] đưa ra mô hình chuyển tiếp cộng tác để nâng cao chất lượng kênh dữ liệu, nhằm giúp nút đích đạt được đủ số gói mã hóa sớm hơn nút nghe lén. Đồng thời, công trình [22] cũng áp dụng kỹ thuật tạo nhiễu hợp tác CJ để giảm khả năng giải mã của thiết bị nghe lén. Các tác giả trong tài liệu [23]-[24] áp dụng kỹ thuật chọn lựa anten phát tốt nhất để đạt được tỷ số SNR tối đa tại nút đích. Đồng thời, các nút tạo nhiễu trong các tài liệu [23]-[24] đặt gần các nút đích để phối hợp với các nút đích trong việc khử nhiễu gây ra. Các công trình [25]-[26] sử dụng kỹ thuật đa truy nhập phi trực giao NOMA

Tác giả liên hệ: Trần Trung Duy,
Email: trantrungduy@ptithcm.edu.vn
Đến tòa soạn: 11/2021, chỉnh sửa: 03/2022, chấp nhận đăng: 04/2022.

(Non-Orthogonal Multiple Access) để rút ngắn thời gian truyền các gói mã hóa đến các nút đích. Như đã đề cập trong các công trình [25]-[26], việc giảm số lần truyền các gói mã cũng nâng cao hiệu quả bảo mật thông tin.

Bài báo này đề xuất mô hình bảo mật lớp vật lý sử dụng mã Fountain cho mạng quảng bá đa người dùng. Trong mô hình đề xuất, một nút nguồn gửi cùng dữ liệu đến một nhóm các nút đích, với sự xuất hiện của nhiều nút nghe lén. Để giảm chất lượng kênh nghe lén, một nhóm các nút tạo nhiễu ở gần các nút đích sẽ được sử dụng để gây nhiễu lên các nút nghe lén. Sau đây, chúng tôi tóm tắt những điểm mới và những đóng góp chính của bài báo:

- Khác với các công trình [20]-[26], bài báo này nghiên cứu mạng quảng bá đa người dùng, trong đó nút nguồn sử dụng mã Fountain để truyền dữ liệu đến nhiều người dùng cùng lúc. Thật vậy, các công trình liên quan [20]-[26] chỉ xét mô hình có 01 người dùng. Trong thực tế, một nhóm các người dùng sẽ yêu cầu cùng một loại dữ liệu, và trong trường hợp này, việc áp dụng mã Fountain sẽ đơn giản trong việc truyền dữ liệu cũng như giảm thời gian trễ, khi so sánh với phương pháp truyền dữ liệu truyền thống.

- Khác với các công trình [20]-[26], các tác giả chỉ xét mô hình bảo mật lớp vật lý với chỉ 01 nút nghe lén. Trong thực tế, nhiều nút nghe lén có thể xuất hiện cùng lúc trong mạng, và đây là mô hình tổng quát được nghiên cứu trong bài báo này.

- Khác với các công trình [23]-[24] và [28], chúng tôi xem xét mô hình nhiều nút tạo nhiễu cộng tác, trong đó một nhóm các nút xuất hiện gần các nút đích sẽ phối hợp để gây nhiễu lên các nút nghe lén.

- Mặc dù công trình [29] cũng nghiên cứu mô hình truyền thông quảng bá đa người dùng, tuy nhiên công trình [29] không xem xét mô hình bảo mật lớp vật lý sử dụng kỹ thuật tạo nhiễu cộng tác (CJ). Hơn nữa, các tác giả trong [29] nghiên cứu về hiệu năng mạng quảng bá thứ cấp trong vô tuyến nhận thức (Cognitive Radio).

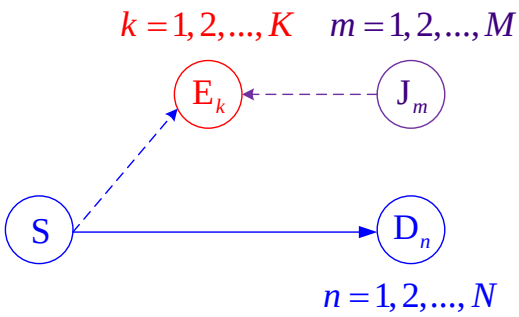
- Bài báo này đề xuất phương pháp phân bổ công suất phát đơn giản giữa nguồn và các nút tạo nhiễu, để so sánh một cách công bằng giữa các mô hình với số nút tạo nhiễu khác nhau, giữa mô hình sử dụng kỹ thuật tạo nhiễu cộng tác (CJ) và mô hình không sử dụng kỹ thuật này.

- Chúng tôi đưa ra các công thức tính chính xác OP và IP của mô hình đề xuất trên kênh Nakagami-*m*. Các biểu thức đưa ra đều dưới dạng tường minh (closed form), và được kiểm chứng tính chính xác thông qua mô phỏng Monte Carlo. Hơn nữa, kênh truyền Nakagami-*m* là kênh truyền tổng quát nên các kết quả phân tích trong bài báo này có thể áp dụng để thiết kế và quy hoạch mạng trong nhiều trường hợp thực tế.

- Các kết quả mô phỏng và lý thuyết được đưa ra để so sánh hiệu năng giữa các mô hình, cũng như đánh giá sự ảnh hưởng các tham số hệ thống lên hiệu năng OP và IP, sự đánh đổi giữa độ tin cậy (OP) và khả năng bảo mật thông tin (IP).

Phần còn lại của bài báo được cấu trúc như sau: Phần II trình bày nguyên lý hoạt động, trong khi Phần III đánh giá hiệu năng OP và IP của mô hình. Phần IV đưa ra các kết quả mô phỏng và lý thuyết. Các kết luận và hướng phát triển được thảo luận trong Phần V.

II. MÔ HÌNH HỆ THỐNG



Hình 1. Mô hình hệ thống.

Hình 1 mô tả mô hình hệ thống đề xuất, trong đó nguồn S muốn gửi cùng dữ liệu đến một nhóm *N* nút đích D. Cùng lúc đó, *K* nút nghe lén E đang cố gắng nghe lén dữ liệu của nguồn S. Để chống lại các nút nghe lén, *M* nút tạo nhiễu J sẽ hợp tác với các nút đích để gây nhiễu lên các nút E. Hơn nữa, các nút tạo nhiễu này ở gần các nút đích D và sẽ phối với các nút đích để khử nhiễu gây ra. Giả sử rằng tất cả các nút S, D_n, J_m và E_k đều có 01 anten, và hoạt động theo chế độ bán song công (half-duplex mode), với $n=1,2,...,N$, $m=1,2,...,M$ và $k=1,2,...,K$.

Sử dụng mã Fountain, nguồn S chia dữ liệu gốc thành các gói có kích thước bằng nhau, và chọn ngẫu nhiên một số các gói này để tạo ra các gói mã hóa (ví dụ như XOR các gói được chọn này lại [20]-[26]). Nguồn S sẽ liên tục gửi các gói mã hóa đến các đích D, và mỗi nút đích D_n phải nhận ít nhất *H* gói mã hóa để có thể khôi phục thành công dữ liệu gốc [28]. Hơn nữa, số lần truyền các gói mã hóa tối đa của nguồn S được ký hiệu là $N_{\max}$, $N_{\max} \geq H$ [28]. Cụ thể hơn, nguồn S sẽ liên tục gửi $N_{\max}$ gói mã hóa đến các nút đích, và sau đó sẽ ngưng truyền. Nếu nút đích D_n không thể nhận thành công ít nhất *H* gói, thì nút này không thể đạt được dữ liệu gốc. Cũng vậy, nếu nút nghe lén E_k không thể đạt được ít nhất *H* gói mã hóa thì E_k cũng không thể khôi phục được thông tin gốc.

2.1 Mô hình kênh truyền

Trong bài báo, kênh truyền giữa máy phát X và máy thu Y là kênh Nakagami-*m*, với $(\mathrm{X},\mathrm{Y}) \in \{\mathrm{S},\mathrm{D}_n,\mathrm{J}_m,\mathrm{E}_k\}$. Ta ký hiệu $h_{\mathrm{X,Y}}$ là hệ số kênh truyền giữa hai nút X và Y, và $\gamma_{\mathrm{X,Y}} = |h_{\mathrm{X,Y}}|^2$ là độ lợi kênh tương ứng. Giả sử rằng hệ số kênh truyền không thay đổi trong suốt quá trình truyền 01 gói mã hóa, và sẽ thay đổi độc lập giữa những lần truyền các gói mã hóa khác nhau. Do đó, độ lợi kênh $\gamma_{\mathrm{X,Y}}$ sẽ có hàm mật độ xác suất (Probability Density Function) như sau (xem tài liệu [30]):

$$f_{\gamma_{\mathrm{X,Y}}}(x) = \frac{\left(m_{\mathrm{X,Y}}\lambda_{\mathrm{X,Y}}\right)^{m_{\mathrm{X,Y}}}}{\left(m_{\mathrm{X,Y}}-1\right)!} x^{m_{\mathrm{X,Y}}-1} \exp\left(-m_{\mathrm{X,Y}}\lambda_{\mathrm{X,Y}}x\right). \quad (1)$$

Trong (1), $m_{\mathrm{X,Y}}$ là hệ số Nakagami-*m*, và $\lambda_{\mathrm{X,Y}}$ bằng nghịch đảo giá trị trung bình của $\gamma_{\mathrm{X,Y}}$: $\lambda_{\mathrm{X,Y}} = 1/\bar{\gamma}_{\mathrm{X,Y}}$, ở đây $\bar{\gamma}_{\mathrm{X,Y}}$ là giá trị trung bình của $\gamma_{\mathrm{X,Y}}$. Khi $m_{\mathrm{X,Y}}$ là số nguyên,

ta có hàm phân phối tích lũy CDF (Cumulative Distribution Function) của $\gamma_{\mathrm{X,Y}}$ như trong tài liệu [30]:

$$F_{\gamma_{\mathrm{X,Y}}}(x)=1-\exp\left(-m_{\mathrm{X,Y}}\lambda_{\mathrm{X,Y}}x\right)\sum_{u=0}^{m_{\mathrm{X,Y}}-1}\frac{1}{u!}\left(m_{\mathrm{X,Y}}\lambda_{\mathrm{X,Y}}x\right)^{u}. \quad (2)$$

Khi $m_{\mathrm{X,Y}}=1$, kênh Nakagami-*m* sẽ trở thành kênh fading Rayleigh, và hàm PDF và CDF của $\gamma_{\mathrm{X,Y}}$ sẽ là:

$$\begin{aligned} f_{\gamma_{\mathrm{X,Y}}}(x)&=\lambda_{\mathrm{X,Y}}\exp\left(-\lambda_{\mathrm{X,Y}}x\right),\\ F_{\gamma_{\mathrm{X,Y}}}(x)&=1-\exp\left(-\lambda_{\mathrm{X,Y}}x\right). \end{aligned} \quad (3)$$

Ta có thể giả sử rằng các kênh truyền $\mathrm{S}\to\mathrm{D}_n$, $\mathrm{S}\to\mathrm{E}_k$ và $\mathrm{J}_m\to\mathrm{E}_k$ là độc lập và đồng nhất, cụ thể:

$$\begin{aligned} &\lambda_{\mathrm{S,D}_n}=\lambda_{\mathrm{S,D}},\ \lambda_{\mathrm{S,E}_k}=\lambda_{\mathrm{S,E}},\lambda_{\mathrm{J}_m,\mathrm{E}_k}=\lambda_{\mathrm{J,E}},\\ &m_{\mathrm{S,D}_n}=m_{\mathrm{S,D}},\ m_{\mathrm{S,E}_k}=m_{\mathrm{S,E}},m_{\mathrm{J}_m,\mathrm{E}_k}=m_{\mathrm{J,E}}\left(\forall n,k,m\right). \end{aligned} \quad (4)$$

2.2 Xây dựng các biểu thức SNR (SINR)

Xét sự truyền 01 gói mã hóa bất kỳ giữa nguồn S và các nút đích D_n. Cũng trong lúc đó, các nút tạo nhiễu J_m cũng phát nhiễu lên các nút nghe lén E_k.

Tín hiệu nhận được tại đích D_n và nút nghe lén E_k được biểu diễn như sau:

$$\begin{aligned} y_{\mathrm{D}_n}&=\sqrt{P_{\mathrm{S}}}h_{\mathrm{S,D}_n}x_{\mathrm{S}}+\sum_{m=1}^{M}P_{\mathrm{J}_m}h_{\mathrm{J}_m,\mathrm{D}_n}x_{\mathrm{J}_m}+g_{\mathrm{D}_n},\\ y_{\mathrm{E}_k}&=\sqrt{P_{\mathrm{S}}}h_{\mathrm{S,E}_k}x_{\mathrm{S}}+\sum_{m=1}^{M}P_{\mathrm{J}_m}h_{\mathrm{J}_m,\mathrm{E}_k}x_{\mathrm{J}_m}+g_{\mathrm{E}_k}, \end{aligned} \quad (5)$$

với P_{S} và P_{J_m} lần lượt là công suất phát của S và J_m, x_{S} và x_{J_m} lần lượt là tín hiệu được gửi đi bởi S và J_m, và g_{D_n} và g_{E_k} lần lượt là nhiễu Gauss tại D_n và E_k. Để đơn giản về mặt trình bày, ta giả sử tất cả nhiễu Gauss đều có giá trị trung bình bằng 0 và phương sai là σ_0^2.

Các nút D_n sẽ hợp tác với các nút J_m để khử các thành phần giao thoa $\sum_{m=1}^{M}P_{\mathrm{J}_m}h_{\mathrm{J}_m,\mathrm{D}_n}x_{\mathrm{J}_m}$ ra khỏi tín hiệu nhận được. Sau phép khử, tín hiệu nhận được tại đích D_n còn lại là:

$$y_{\mathrm{D}_n}=\sqrt{P_{\mathrm{S}}}h_{\mathrm{S,D}_n}x_{\mathrm{S}}+g_{\mathrm{D}_n}. \quad (6)$$

Từ công thức (6), tỷ số SNR ở các đích D_n sẽ là:

$$\psi_{\mathrm{S,D}_n}=\frac{P_{\mathrm{S}}\gamma_{\mathrm{S,D}_n}}{\sigma_0^2}. \quad (7)$$

Để bảo mật việc trao đổi các thông tin liên quan đến hoạt động tạo nhiễu và các thông tin về x_{J_m}; các nút J_m thường ở gần các nút D_n để việc trao đổi này là hoàn toàn bảo mật đối với các nút nghe lén E_k [17], [23]-[24]. Do đó, các nút E_k không thể loại bỏ nhiễu gây ra bởi các nút tạo nhiễu J_m, nên từ công thức (5), tỷ số SINR (Signal-to-Interference-plus-Noise Ratio) tại E_k sẽ là

$$\psi_{\mathrm{S,E}_k}=\frac{P_{\mathrm{S}}\gamma_{\mathrm{S,E}_k}}{\sum_{m=1}^{M}P_{\mathrm{J}_m}\gamma_{\mathrm{J}_m,\mathrm{E}_k}+\sigma_0^2}. \quad (8)$$

2.3 Bài Toán Phân Bổ Công Suất Phát

Để so sánh công bằng giữa các mô hình với số lượng nút tạo nhiễu khác nhau, và giữa mô hình sử dụng kỹ thuật tạo nhiễu CJ và không sử dụng kỹ thuật tạo nhiễu CJ, chúng tôi đưa ra bài toán phân bổ công suất phát như sau:

Trước tiên, tổng công suất phát của nguồn S và tất cả các nút tạo nhiễu được cố định bằng *Q*, đó là:

$$P_{\mathrm{S}}+\sum_{m=1}^{M}P_{\mathrm{J}_m}=Q. \quad (9)$$

Giả sử rằng các nút tạo nhiễu phát cùng công suất, bài toán phân bổ công suất được viết lại như sau:

$$P_{\mathrm{S}}=\mu Q,\ P_{\mathrm{J}_m}=P_{\mathrm{J}}=\frac{1-\mu}{M}Q. \quad (10)$$

với μ là hệ số phân bổ công suất, ở đây $0<\mu\le 1$.

Trong trường không sử dụng kỹ thuật CJ, hay $\mu=1$, và bài toán trong công thức (10) được viết lại như sau:

$$P_{\mathrm{S}}=Q,\ P_{\mathrm{J}}=0. \quad (11)$$

Do đó, thay (10) vào (7) và (8), ta lần lượt đạt được các biểu thức tính SNR và SINR như sau:

$$\psi_{\mathrm{S,D}_n}=\frac{\mu Q\gamma_{\mathrm{S,D}_n}}{\sigma_0^2}=\mu\Psi\gamma_{\mathrm{S,D}_n}, \quad (12)$$

$$\begin{aligned} \psi_{\mathrm{S,E}_k}&=\frac{\mu Q\gamma_{\mathrm{S,E}_k}}{\frac{1-\mu}{M}\sum_{m=1}^{M}Q\gamma_{\mathrm{J}_m,\mathrm{E}_k}+\sigma_0^2}\\ &=\frac{\mu\Psi\gamma_{\mathrm{S,E}_k}}{\frac{1-\mu}{M}\Psi X_{k,\mathrm{sum}}+1}, \end{aligned} \quad (13)$$

với

$$\Psi=\frac{Q}{\sigma_0^2},\ X_{k,\mathrm{sum}}=\sum_{m=1}^{M}\gamma_{\mathrm{J}_m,\mathrm{E}_k}. \quad (14)$$

Trong trường hợp không sử dụng kỹ thuật CJ, thay (11) vào (7) và (8), ta có:

$$\psi_{\mathrm{S,D}_n}=\Psi\gamma_{\mathrm{S,D}_n},\psi_{\mathrm{S,E}_k}=\Psi\gamma_{\mathrm{S,E}_k}. \quad (15)$$

Trước khi đi vào phân tích các hiệu năng của mô hình đề xuất, chúng ta đi tìm hàm PDF của biến ngẫu nhiên $X_{k,\mathrm{sum}}$ trong công thức (14).

2.4 PDF của $X_{k,\mathrm{sum}}$

Sử dụng định nghĩa hàm sinh moment (MGF: Moment Generating Function) [31], từ các công thức (1) và (4), ta đạt được MGF của biến ngẫu nhiên $\gamma_{\mathrm{J}_m,\mathrm{E}_k}$ như sau:

$$\begin{aligned} \mathrm{MGF}_{\gamma_{\mathrm{J}_m,\mathrm{E}_k}}(s)&=\int_0^{+\infty}f_{\gamma_{\mathrm{J}_m,\mathrm{E}_k}}(x)\exp\left(-sx\right)dx\\ &=\frac{\left(m_{\mathrm{J,E}}\lambda_{\mathrm{J,E}}\right)^{m_{\mathrm{J,E}}}}{\left(s+m_{\mathrm{J,E}}\lambda_{\mathrm{J,E}}\right)^{m_{\mathrm{J,E}}}}. \end{aligned} \quad (16)$$

Vì vậy, MGF của $X_{k,\mathrm{sum}}$ được viết ra như sau:

$$\mathrm{MGF}_{X_{k,\mathrm{sum}}}(s)=\prod_{m=1}^{M}\mathrm{MGF}_{\gamma_{\mathrm{J}_m,\mathrm{E}_k}}(s)=\frac{\left(m_{\mathrm{J,E}}\lambda_{\mathrm{J,E}}\right)^{m_{\mathrm{J,E}}M}}{\left(s+m_{\mathrm{J,E}}\lambda_{\mathrm{J,E}}\right)^{m_{\mathrm{J,E}}M}}. \quad (17)$$

Sử dụng phép biến đổi Laplace ngược cho công thức (17), ta đạt được hàm PDF của $X_{k,\mathrm{sum}}$ như sau:

$$f_{X_{k,\text{sum}}}(x)=\frac{\left(m_{\text{J,E}}\lambda_{\text{J,E}}\right)^{m_{\text{J,E}}M}}{\left(m_{\text{J,E}}M-1\right)!}x^{m_{\text{J,E}}M-1}\exp\left(-m_{\text{J,E}}\lambda_{\text{J,E}}x\right). \quad (18)$$

III. PHÂN TÍCH HIỆU NĂNG OP VÀ IP HỆ THỐNG

3.1 Xác Suất Giải Mã Một Gói Mã Hóa

Nếu tỷ số SNR (hoặc SINR) đạt được tại một thiết bị thu lớn hơn một ngưỡng xác định trước ψ_{th}, thì thiết bị thu này sẽ giải mã thành công (không lỗi) gói mã hóa nhận được. Ngược lại, ta giả sử rằng thiết bị thu không thể giải mã thành công gói mã hóa nhận được.

Từ định nghĩa trên, xác suất mà nút đích D_n nhận thành công một gói mã hóa được tính như sau:

$$\rho_{\text{D}}=\Pr\left(\psi_{\text{S,D}_n}\geq\psi_{\text{th}}\right). \quad (19)$$

Sử dụng các công thức (2) và (12), ta tính được chính xác xác suất giải mã ρ_{D} trong công thức (19) như sau:

$$\begin{aligned}\rho_{\text{D}}&=\Pr\left(\gamma_{\text{S,D}_n}\geq\frac{\psi_{\text{th}}}{\mu\Psi}\right)=1-F_{\gamma_{\text{S,D}_n}}\left(\frac{\psi_{\text{th}}}{\mu\Psi}\right)\\&=\exp\left(-\frac{m_{\text{S,D}}\lambda_{\text{S,D}}\psi_{\text{th}}}{\mu\Psi}\right)\sum_{u=0}^{m_{\text{S,D}}-1}\frac{1}{u!}\left(\frac{m_{\text{S,D}}\lambda_{\text{S,D}}\psi_{\text{th}}}{\mu\Psi}\right)^{u}.\end{aligned} \quad (20)$$

Ta lưu ý rằng xác suất giải mã thành công một gói mã hóa tại tất cả các nút đích là giống nhau, do giả thiết các kênh truyền giữa nguồn S và các nút đích là đồng nhất. Hơn nữa, xác suất mà nút đích D_n không thể giải mã thành công 01 gói mã hóa sẽ là

$$\begin{aligned}&1-\rho_{\text{D}}=\\&1-\exp\left(-\frac{m_{\text{S,D}}\lambda_{\text{S,D}}\psi_{\text{th}}}{\mu\Psi}\right)\sum_{u=0}^{m_{\text{S,D}}-1}\frac{1}{u!}\left(\frac{m_{\text{S,D}}\lambda_{\text{S,D}}\psi_{\text{th}}}{\mu\Psi}\right)^{u}.\end{aligned} \quad (21)$$

Xét khả năng giải mã của nút nghe lén E_k; sử dụng công thức (13), ta có:

$$\begin{aligned}\rho_{\text{E}}&=\Pr\left(\psi_{\text{S,E}_k}\geq\psi_{\text{th}}\right)=\Pr\left(\gamma_{\text{S,E}_k}\geq\theta_1X_{\text{sum}}+\theta_2\right)\\&=\int_0^{+\infty}\left(1-F_{\gamma_{\text{S,E}_k}}\left(\theta_1x+\theta_2\right)\right)f_{X_{\text{sum}}}(x)\,dx,\end{aligned} \quad (22)$$

với

$$\theta_1=\frac{(1-\mu)\psi_{\text{th}}}{M\mu},\theta_2=\frac{\psi_{\text{th}}}{\mu\Psi}.$$

Thay các hàm CDF và PDF đã đạt được trong các công thức (2) và (18) vào trong công thức (22), ta đạt được:

$$\begin{aligned}\rho_{\text{E}}=&\frac{\left(m_{\text{J,E}}M\lambda_{\text{J,E}}\right)^{m_{\text{J,E}}M}}{\left(m_{\text{J,E}}M-1\right)!}\exp\left(-m_{\text{S,E}}\lambda_{\text{S,E}}\theta_2\right)\times\\&\sum_{u=0}^{m_{\text{S,E}}-1}\frac{\left(m_{\text{S,E}}\lambda_{\text{S,E}}\right)^{u}}{u!}\left[\begin{array}{l}\int_0^{+\infty}\left(\theta_1x+\theta_2\right)^{u}x^{m_{\text{J,E}}M-1}\\\times\exp\left(-\left(m_{\text{J,E}}M\lambda_{\text{J,E}}+m_{\text{S,E}}\lambda_{\text{S,E}}\theta_1\right)x\right)dx\end{array}\right].\end{aligned} \quad (23)$$

Sử dụng khai triển nhị phân: $\left(\theta_1x+\theta_2\right)^{u}=\sum_{v=0}^{u}C_u^v\left(\theta_1x\right)^{v}\left(\theta_2\right)^{u-v}$, ta viết tiếp công thức (23) dưới dạng sau:

$$\begin{aligned}\rho_{\text{E}}=&\frac{\left(m_{\text{J,E}}\lambda_{\text{J,E}}\right)^{m_{\text{J,E}}M}}{\left(m_{\text{J,E}}M-1\right)!}\exp\left(-m_{\text{S,E}}\lambda_{\text{S,E}}\theta_2\right)\\&\times\sum_{u=0}^{m_{\text{S,E}}-1}\sum_{v=0}^{u}\frac{\left(m_{\text{S,E}}\lambda_{\text{S,E}}\right)^{u}}{u!}C_u^v\left(\theta_1\right)^{v}\left(\theta_2\right)^{u-v}\\&\times\int_0^{+\infty}x^{m_{\text{J,E}}M+v-1}\exp\left(-\left(m_{\text{J,E}}\lambda_{\text{J,E}}+m_{\text{S,E}}\lambda_{\text{S,E}}\theta_1\right)x\right)dx.\end{aligned} \quad (24)$$

Sau khi thực hiện phép tính tích phân, ta có được biểu thức chính xác của ρ_{E} như sau:

$$\begin{aligned}\rho_{\text{E}}=&\frac{\left(m_{\text{J,E}}M\lambda_{\text{J,E}}\right)^{m_{\text{J,E}}M}}{\left(m_{\text{J,E}}M-1\right)!}\exp\left(-m_{\text{S,E}}\lambda_{\text{S,E}}\theta_2\right)\times\\&\sum_{u=0}^{m_{\text{S,E}}-1}\sum_{v=0}^{u}\frac{C_u^v\left(m_{\text{S,E}}\lambda_{\text{S,E}}\right)^{u}}{u!}\frac{\left(m_{\text{J,E}}M+v-1\right)!\left(\theta_1\right)^{v}\left(\theta_2\right)^{u-v}}{\left(m_{\text{J,E}}M\lambda_{\text{J,E}}+m_{\text{S,E}}\lambda_{\text{S,E}}\theta_1\right)^{m_{\text{J,E}}M+v}}.\end{aligned} \quad (25)$$

Tương tự như ρ_{D}, xác suất giải mã thành công một gói mã hóa tại tất cả các nút nghe lén là giống nhau, và xác suất mà nút nghe lén E_k không giải mã thành công 01 gói mã hóa sẽ là $1-\rho_{\text{E}}$.

Xét trường hợp đặc biệt: hệ thống không sử dụng kỹ thuật tạo nhiễu cộng tác CJ. Trong trường hợp này, các giá trị ρ_{D} và ρ_{E} được viết lại như sau:

$$\rho_{\text{D}}^{*}=\exp\left(-\frac{m_{\text{S,D}}\lambda_{\text{S,D}}\psi_{\text{th}}}{\Psi}\right)\sum_{u=0}^{m_{\text{S,D}}-1}\frac{1}{u!}\left(\frac{m_{\text{S,D}}\lambda_{\text{S,D}}\psi_{\text{th}}}{\Psi}\right)^{u}. \quad (26)$$

$$\rho_{\text{E}}^{*}=\exp\left(-\frac{m_{\text{S,E}}\lambda_{\text{S,E}}\psi_{\text{th}}}{\Psi}\right)\sum_{u=0}^{m_{\text{S,E}}-1}\frac{1}{u!}\left(\frac{m_{\text{S,E}}\lambda_{\text{S,E}}\psi_{\text{th}}}{\Psi}\right)^{u}. \quad (27)$$

3.2 Xác Suất Dừng Hệ Thống

Ký hiệu L_{D_n} là số gói mã hóa mà đích D_n nhận được sau khi nguồn đã gửi hết $N_{\max}$ gói mã hóa. Nếu $L_{\text{D}_n}\geq H$ thì nút đích D_n sẽ khôi phục thành công dữ liệu gốc.

Xét hiệu năng xác suất dừng hệ thống là xác suất tồn tại một nút đích không thể nhận đủ H gói mã hóa để khôi phục thông tin gốc. Trước hết, ta xét xác suất mà tất cả các nút đích đều có thể nhận được ít nhất H gói mã hóa:

$$\begin{aligned}\overline{\text{OP}}&=\prod_{n=1}^{N}\Pr\left(L_{\text{D}_n}\geq H\right)\\&=\prod_{n=1}^{N}\left[\sum_{L_{\text{D}_n}=H}^{N_{\max}}C_{N_{\max}}^{L_{\text{D}_n}}\left(\rho_{\text{D}}\right)^{L_{\text{D}_n}}\left(1-\rho_{\text{D}}\right)^{N_{\max}-L_{\text{D}_n}}\right]\\&=\left[\sum_{L=H}^{N_{\max}}C_{N_{\max}}^{L}\left(\rho_{\text{D}}\right)^{L}\left(1-\rho_{\text{D}}\right)^{N_{\max}-L}\right]^{N}.\end{aligned} \quad (28)$$

Trong công thức (28), xác suất tất cả các đích khôi phục thành công dữ liệu sẽ bằng tích xác suất thành công của mỗi nút đích. Nguyên nhân là vì hoạt động giải mã ở các nút đích là độc lập với nhau.

Từ công thức (28), ta đạt được công thức tính xác suất dừng hệ thống như sau:

$$\begin{aligned}\text{OP}&=1-\overline{\text{OP}}\\&=1-\left[\sum_{L=H}^{N_{\max}}C_{N_{\max}}^{L}\left(\rho_{\text{D}}\right)^{L}\left(1-\rho_{\text{D}}\right)^{N_{\max}-L}\right]^{N}.\end{aligned} \quad (29)$$

Thay giá trị của ρ_D trong công thức (20) vào công thức (29), ta đạt được biểu thức dạng tường minh của OP. Hơn nữa, thay ρ_D bằng ρ_D^* (xem công thức (26)), ta có được công thức tính OP hệ thống khi không sử dụng kỹ thuật tạo nhiễu nhân tạo CJ.

3.3 Xác Suất Mất Bảo Mật

Ký hiệu L_{E_k} là số gói mã hóa mà nút nghe lén E_k đạt được sau khi nguồn S kết thúc quá trình truyền dữ liệu. Ta thấy rằng chỉ cần một trong các nút nghe lén nhận ít nhất H gói mã hóa, thì dữ liệu sẽ bị mất bảo mật. Do đó, xác suất mà tất cả các nút nghe lén không nhận đủ số H gói là:

$$\begin{aligned}\overline{\text{IP}} &= \prod_{k=1}^{K} \Pr\left(L_{E_k} < H\right) \\ &= \prod_{k=1}^{K}\left[\sum_{L_{E_k}=0}^{H-1} C_{N_{\max}}^{L_{E_k}} \left(\rho_E\right)^{L_{E_k}} \left(1-\rho_E\right)^{N_{\max}-L_{E_k}}\right] \\ &= \left[\sum_{L=0}^{H-1} C_{N_{\max}}^{L} \left(\rho_E\right)^{L} \left(1-\rho_E\right)^{N_{\max}-L}\right]^K .\end{aligned} \quad (30)$$

Trong công thức (30), $0 \le L_{E_k} \le H-1$ vì thế nút E_k không thể khôi phục được thông tin gốc. Hơn nữa, bởi vì các nút nghe lén hoạt động độc lập và có vai trò như nhau nên xác suất $\overline{\text{IP}}$ bằng tích xác suất giải mã dữ liệu nguồn không thành công của mỗi nút nghe lén.

Vì vậy, xác suất mất bảo mật hệ thống sẽ là:

$$\text{IP} = 1-\overline{\text{IP}} = 1-\left[\sum_{L=0}^{N_{\max}-1} C_{N_{\max}}^{L} \left(\rho_E\right)^{L} \left(1-\rho_E\right)^{N_{\max}-L}\right]^K . \quad (31)$$

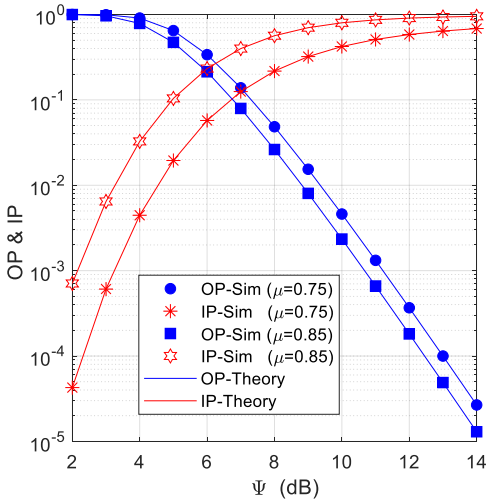
Thay giá trị của ρ_E trong công thức (25) vào công thức (31), ta đạt được biểu thức dạng tường minh của IP. Cuối cùng, thay ρ_E bằng ρ_E^* (xem công thức (27)), ta có được công thức tính IP hệ thống khi không sử dụng kỹ thuật CJ.

IV. KẾT QUẢ MÔ PHỎNG VÀ LÝ THUYẾT

Phần này đưa ra các kết quả mô phỏng và lý thuyết của các tham số hiệu năng OP và IP. Trong các kết quả mô phỏng, kênh truyền Nakagami-*m* giữa các nút được tạo ra bằng hàm Matlab *gamrnd*. Ngoài ra, để kết quả mô phỏng hội tụ về kết quả lý thuyết, chúng tôi thực hiện $5*10^6$ phép thử cho mỗi mô phỏng. Tất cả các kết quả cho ta thấy rằng các giá trị mô phỏng (Sim) và lý thuyết (Theory) trùng với nhau. Điều này kiểm chứng tính chính xác của các công thức OP và IP đưa ra trong Phần III.

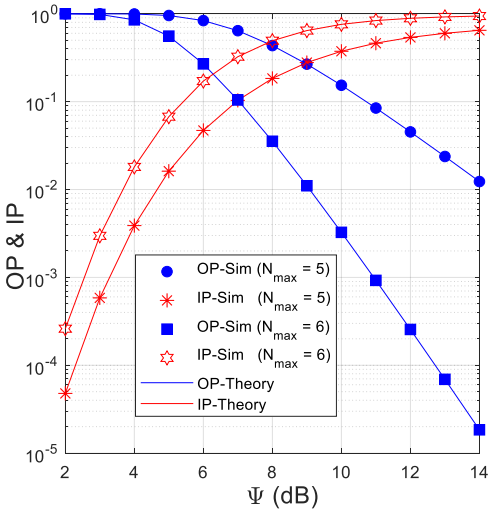
Trong các hình vẽ, ngưỡng dừng ψ_{th} được cố định bằng 1, số gói mã hóa (H) để khôi phục dữ liệu gốc bằng 5, và tham số của các kênh truyền được thiết lập như sau: $\lambda_{S,D}=1$, $\lambda_{S,E}=2$, $m_{S,D}=3$, $m_{S,E}=2$ và $m_{J,E}=1$.

Hình 2 biểu diễn xác suất dừng hệ thống (OP) và xác suất mất bảo mật hệ thống (IP) theo giá trị Ψ(dB) với các giá trị khác nhau của hệ số phân bổ công suất phát (μ), và với $N=5$, $M=2,$, $K=2$, $N_{\max}=6$, $\lambda_{J,E}=1.5$. Hình 2 cho thấy sự đánh đổi giữa chất lượng dịch vụ của mạng (giá trị OP) và khả năng bảo mật thông tin (giá trị IP). Thật vậy, khi tăng Ψ (hay tăng công suất phát Q), xác suất dừng giảm nhưng xác suất mất bảo mật lại tăng. Ta cũng thấy rằng khi $\mu=0.85$ thì giá trị OP nhỏ hơn khi so với $\mu=0.75$. Đó là vì μ càng lớn thì công suất phát của nguồn S càng lớn, điều này sẽ dẫn đến OP thấp. Tuy nhiên, μ càng lớn thì công suất phát của các nút tạo nhiễu sẽ giảm, dẫn đến khả năng nghe lén của các nút E_k tăng, và điều này làm giá trị IP hệ thống tăng.

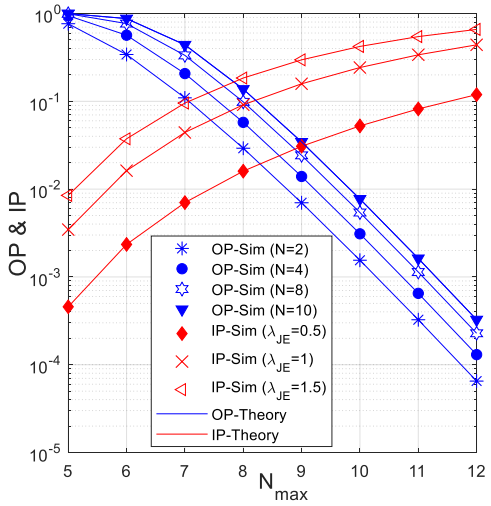


Hình 2. OP và IP vẽ theo Ψ (dB) với $N=5$, $M=2$, $K=2$, $N_{\max}=6$, $\lambda_{J,E}=1.5$.

Hình 3 biểu diễn xác suất dừng hệ thống (OP) và xác suất mất bảo mật hệ thống (IP) theo giá trị của Ψ(dB) với các giá trị khác nhau của $N_{\max}$, và với $N=5$, $M=3$, $K=3$, $\mu=0.8$, $\lambda_{J,E}=1.5$. Tương tự Hình 2, khi tăng Ψ, mô hình đề xuất đạt được giá trị OP thấp hơn nhưng lại chịu giá trị IP cao hơn. Hình 3 cũng cho thấy OP giảm đáng kể khi tăng $N_{\max}$ từ 5 lên 6. Bởi vì khi tăng $N_{\max}$ sẽ tăng thêm cơ hội cho các nút đích nhận đủ H gói mã hóa để khôi phục dữ liệu. Tuy nhiên, ta có thể thấy rằng $N_{\max}$ tăng cũng làm tăng giá trị IP. Qua các Hình 2 và 3, ta thấy được sự đánh đổi giữa OP và IP. Do đó, công suất phát của các nút, hệ số phân bổ công suất và số lần truyền của nút nguồn cần được thiết kế kỹ lưỡng.

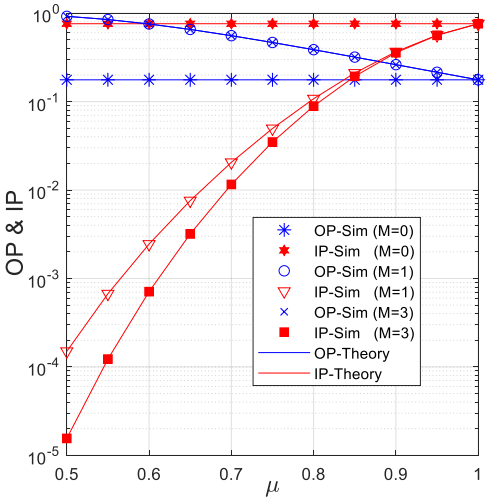


Hình 3. OP và IP vẽ theo Ψ (dB) với $N=5$, $M=3$, $K=3$, $\mu=0.8$, $\lambda_{J,E}=1.5$.

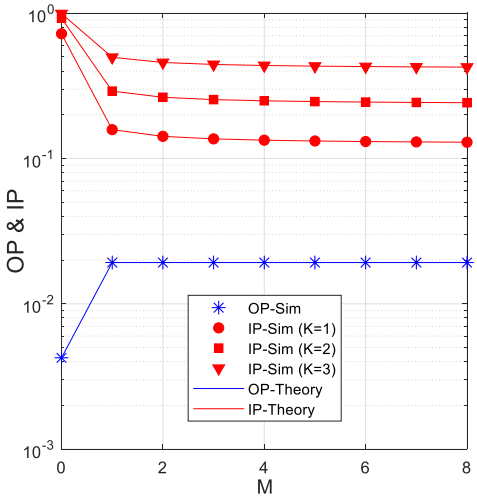


Hình 4. OP và IP vẽ theo $N_{\max}$ *với* $\Delta = 5\,(dB)$, $M = 1$, $K = 3$, $\mu = 0.75$.

Hình 4 vẽ OP và IP theo số lần truyền tối đa của nút nguồn $(N_{\max})$ với các giá trị khác nhau của số nút đích (N), và với $\Delta = 5\,(\text{dB})$, $M = 1$, $K = 3$, $\mu = 0.75$. Trước tiên, ta lưu ý rằng xác suất mất bảo mật (IP) sẽ không phụ thuộc vào số nút đích (N). Tuy nhiên, IP sẽ thay đổi theo $\lambda_{J,E}$. Bởi vì $\lambda_{J,E}$ bằng nghịch đảo giá trị trung bình của độ lợi kênh, nên $\lambda_{J,E}$ càng nhỏ thì trung bình độ lợi kênh giữa các nút J và các nút E càng lớn, và vì thế sự tác động của nhiễu do các nút J gây nên các nút E càng lớn. Đó là lý do tại sao trong Hình 4 khi giá trị $\lambda_{J,E}$ giảm thì giá trị IP cũng giảm theo. Tiếp đến, nhìn vào Hình 4, ta thấy xác suất dừng (OP) giảm mạnh khi $N_{\max}$ tăng bởi vì các nút đích có nhiều cơ hội hơn để khôi phục thành công dữ liệu nguồn. Tương tự, các nút nghe lén E cũng tăng thêm cơ hội giải mã dữ liệu nguồn, điều này dẫn đến giá trị IP tăng. Tiếp đến, ta thấy rằng giá trị OP tăng khi số người dùng (N) tăng. Bởi vì khi N tăng thì xác suất có ít nhất 01 nút đích không nhận đủ H gói mã hóa cũng tăng theo.



Hình 5. OP và IP vẽ theo μ *với* $\Delta = 5\,(dB)$, $N = 3$, $K = 4$, $N_{\max} = 6$, $\lambda_{J,E} = 1.5$.



Hình 6. OP và IP vẽ theo M *với* $\Delta = 6\,(dB)$, $N = 2$, $\mu = 0.8$, $N_{\max} = 7$, $\lambda_{J,E} = 1.5$.

Hình 5 khảo sát sự ảnh hưởng của hệ số phân bổ công suất (μ) lên các hiệu năng hệ thống, với các giá trị khác nhau của số nút tạo nhiễu (M) và với $\Delta = 5\,(\text{dB})$, $N = 3$, $K = 4$, $N_{\max} = 6$, $\lambda_{J,E} = 1.5$. Tương tự như Hình 2, Hình 5 cho ta thấy rằng tăng giá trị của μ sẽ làm giảm xác suất dừng (OP) nhưng lại tăng xác suất mất bảo mật (IP). Trong trường hợp $\mu = 1$, đây là mô hình không sử dụng kỹ thuật tạo nhiễu cộng tác CJ, và ta có thể thấy mặc dù giá trị OP đạt được là thấp hơn nhưng đổi lại giá trị IP lại rất cao. Tương tự, trường hợp M=0 cũng mô tả mô hình không sử dụng kỹ thuật CJ, và các giá trị của OP và IP trong trường hợp này không phụ thuộc vào μ. Hình 5 cũng cho thấy giá trị OP không phụ thuộc vào số nút tạo nhiễu M bởi vì công suất phát của nguồn S không phụ thuộc vào M (xem công thức (10)). Tuy nhiên, công suất phát của các nút tạo nhiễu lại phụ thuộc vào số lượng nút tạo nhiễu (M). Cụ thể, khi M càng lớn thì công suất phát của mỗi nút tạo nhiễu càng nhỏ. Ở chiều ngược lại, số lượng nút tạo nhiễu càng nhiều thì tổng thành phần giao thoa gây lên các nút nghe lén càng tăng. Quan sát từ Hình 5, ta có thể thấy khi M tăng từ 1 lên 3 thì giá trị IP giảm. Tuy nhiên, khi μ quá lớn thì sự chênh lệch giá trị IP trong hai trường hợp M=1 và M=3 là không đáng kể vì lúc này công suất phát của các nút tạo nhiễu là quá nhỏ.

Hình 6 khảo sát sự ảnh hưởng của số lượng nút tạo nhiễu (M) lên các giá trị OP và IP hệ thống, với các giá trị khác nhau của số nút nghe lén (K), và với $\Delta = 6\,(\text{dB})$, $N = 2$, $\mu = 0.8$, $N_{\max} = 7$, $\lambda_{J,E} = 1.5$. Ta có thể thấy rằng khi kỹ thuật tạo nhiễu nhân tạo không được sử dụng (M=0) thì nguồn S sẽ phát với công suất $P_S = Q$ nên OP có giá trị thấp nhất. Với các giá trị khác của M, bởi vì nguồn S phát với cùng công suất $P_S = \mu Q$ và với giả thiết các nút đích có thể khử nhiễu gây ra bởi các nút J, nên giá trị của OP không thay đổi. Đối với IP, khi M=0, giá trị IP là lớn nhất bởi vì kỹ thuật CJ không được sử dụng. Khi $M \geq 1$, giá trị IP nhỏ hơn nhiều khi so sánh với M=0. Tuy nhiên, với $M \geq 2$, giá trị IP chỉ giảm nhẹ khi số lượng nút tạo nhiễu tăng. Bởi vì khi có nhiều nút tạo nhiễu tham gia thì công

suất phát của các nút này giảm (xem công thức (10)) nên hiệu quả gây nhiễu tăng không đáng kể.

V. KẾT LUẬN

Bài báo đã đề xuất và đánh giá các thông số hiệu năng hệ thống cho mô hình truyền quảng bá đa người dùng sử dụng mã Fountain, với sự xuất hiện của nhiều nút nghe lén. Các kết quả cũng cho thấy có sự đánh đổi giữa bảo mật thông tin và độ tin cậy của việc truyền tin. Do đó, trong quá trình thiết kế hệ thống, các tham số quan trọng như công suất phát, hệ số phân bổ công suất phát, số lần truyền gói mã hoá tối đa hay số nút đích và số nút tạo nhiễu cần được thiết kế để tối ưu các hiệu năng hệ thống.

Công việc tiếp theo của nhóm nghiên cứu là sẽ phát triển mô hình trong bài báo này theo hướng chuyển tiếp bán song công/ song công trong mạng quảng bá đa người dùng, sử dụng các kỹ thuật chọn lựa nút chuyển tiếp và chọn lựa nút tạo nhiễu để nâng cao các hiệu năng mạng.

LỜI CẢM ƠN

Nghiên cứu này được tài trợ bởi Học Viện Công Nghệ Bưu Chính Viễn Thông Cơ Sở Thành Phố Hồ Chí Minh với mã số đề tài 02-HV-2021-RD_ĐT2.

REFERENCES

[1] A. D. Wyner, “The Wire-Tap Channel,” The Bell System Technical Journal vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] R. Liu, I. Maric, P. Spasojevic, R. D. Yates, "Discrete Memoryless Interference and Broadcast Channels With Confidential Messages: Secrecy Rate Regions," IEEE Transactions on Information Theory, vol. 54, no. 6, pp. 2493-2507, Jun. 2008.

[3] J. Zhang, Trung Q. Duong, R. Woods, A. Marshall, “Securing Wireless Communications of the Internet of Things From The Physical Layer, An Overview,” Entropy, vol. 19, no. 8, (420) Aug. 2017.

[4] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, I. B. Collings, "Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels," IEEE Transactions on Communications, vol. 61, no. 1, pp. 144-154, Jan. 2013.

[5] N. Yang, H. A. Suraweera, I. B. Collings, C. Yuen, "Physical Layer Security of TAS/MRC With Antenna Correlation," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 254-259, Jan. 2013.

[6] H. Zhao, Y. Tan, G. Pan, Y. Chen, N. Yang, "Secrecy Outage on Transmit Antenna Selection/Maximal Ratio Combining in MIMO Cognitive Radio Networks," IEEE Transactions on Vehicular Technology, vol. 65, no. 12, pp. 10236-10242, Dec. 2016.

[7] J. N. Laneman, D. N. C. Tse and G. W. Wornell, "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior," IEEE Transactions on Information Theory, vol. 50, no. 12, pp. 3062-3080, Dec. 2004.

[8] C. Cai, Y. Cai, W. Yang, W. Yang, "Secure Connectivity Using Randomize-and-Forward Strategy in Cooperative Wireless Networks," IEEE Communications Letters, vol. 17, no. 7, pp. 1340-1343, Jul. 2013.

[9] P. N. Son, H. Y. Kong, "Cooperative Communication with Energy-Harvesting Relays Under Physical Layer Security," IET Communications, vol. 9, no. 17, pp. 2131-2139, Nov. 2015.

[10] T. T. Duy, T. Q. Duong, T. L. Thanh, V. N. Q. Bao, "Secrecy Performance Analysis with Relay Selection Methods under Impact of Co-channel Interference," IET Communications, vol. 9, no. 11, pp. 1427-1435, Jul. 2015.

[11] L. Fan, X. Lei, N. Yang, T. Q. Duong, G. K. Karagiannidis, "Secure Multiple Amplify-and-Forward Relaying With Cochannel Interference," IEEE Journal of Selected Topics in Signal Processing, vol. 10, no. 8, pp. 1494-1505, Dec. 2016.

[12] L. Dong, Z. Han, A. P. Petropulu, H. V. Poor, “Improving Wireless Physical Layer Security via Cooperating Relays,” IEEE Transactions on Signal Processing, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[13] S. Jia, J. Zhang, H. Zhao, R. Zhang, “Relay Selection for Improved Security in Cognitive Relay Networks with Jamming,” IEEE Wireless Communications Letters, vol. 6, no. 5, pp. 662-665, Oct. 2017.

[14] X. Ding, T. Song, Y. Zou, X. Chen, L. Hanzo, "Security-Reliability Tradeoff Analysis of Artificial Noise Aided Two-Way Opportunistic Relay Selection," IEEE Transactions on Vehicular Technology, vol. 66, no. 5, pp. 3930-3941, May 2017.

[15] X. Ding, Y. Zou, F. Ding, D. Zhang, G. Zhang, "Opportunistic Relaying Against Eavesdropping for Internet-of-Things: A Security-Reliability Tradeoff Perspective," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8727-8738, Oct. 2019.

[16] P. T. Tin, T. T. Duy, "Power Allocation Strategies for Dual-hop Relay Protocols with Best Relay Selection under Constraint of Intercept Probability," ICT Express, vol. 5, no. 1, pp. 52-55, March 2019.

[17] N. T. Anh, N. C. Minh, T. T. Duy, T. Hanh and H. D. Hai, "Reliability-Security Analysis for Harvest-to-Jam based Multi-hop Cluster MIMO Networks Using Cooperative Jamming Methods Under Impact of Hardware Impairments," EAI Transactions on Industrial Networks and Intelligent Systems, vol. 8, no. 28, pp. 1-14, Sept. 2021.

[18] M. Luby, "LT Codes," in Proc. of the 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings., Vancouver, BC, 2002, pp. 271-280.

[19] A. Shokrollahi, "Raptor Codes," IEEE Transactions on Information Theory, vol. 52, no. 6, pp. 2551-2567, Jun. 2006.

[20] H. Niu, M. Iwai, K. Sezaki, L. Sun and Q. Du, "Exploiting Fountain Codes for Secure Wireless Delivery," IEEE Communications Letters, vol. 18, no. 5, pp. 777-780, May 2014.

[21] W. Li, Q. Du, L. Sun, P. Ren, Y. Wang, "Security Enhanced via Dynamic Fountain Code Design for Wireless Delivery," in Proc. of 2016 IEEE WCMC, Doha, 2016, pp. 1-6.

[22] L. Sun, P. Ren, Q. Du, and Y. Wang, “Fountain-Coding Aided Strategy for Secure Cooperative Transmission in Industrial Wireless Sensor Networks,” IEEE Trans. Industrial Inform., vol. 12, no. 1, pp. 291-300, Feb. 2016.

[23] D. T. Hung, T. T. Duy, D. Q. Trinh and V. N. Q. Bao, "Secrecy Performance Evaluation of TAS Protocol Exploiting Fountain Codes and Cooperative Jamming under Impact of Hardware Impairments," in Proc. of SigTelCom, pp. 164-169, Jan. 2018.

[24] P. T. Tin, N. N. Tan, N. Q. Sang, T. T. Duy, T. T. Phuong, M. Voznak, "Rateless Codes based Secure Communication Employing Transmit Antenna Selection and Harvest-To-Jam under Joint Effect of Interference and Hardware Impairments," Entropy, vol. 21, no. 7, (700), Jul. 2019.

[25] D. T. Hung, T. T. Duy, T. T. Phuong, D. Q. Trinh, T. Hanh, "Performance Comparison between Fountain Codes-Based Secure MIMO Protocols with and without Using Non-Orthogonal Multiple Access," Entropy, vol. 21, no. 10, (928), Oct. 2019.

[26] H. D. Hung, T. T. Duy, P. N. Son, L. T. Thuong and M. Voznak, "Security-Reliability Trade-off Analysis for

Rateless Codes-Based Relaying Protocols Using NOMA, Cooperative Jamming and Partial Relay Selection," IEEE Access, vol. 9, pp. 1-22, Sept. 2021.
[27] H. Khuong, V. Q. Son, L. T. Tra and P. H. Lien, "On the outage performance of relaying cognitive networks with reactive relay selection and selection combining," in Proc. of NICS 2015, 2015, pp. 333-338.
[28] N. V. Hien, T. T. Duy, T. D. Thuan, "Nghiên Cứu Hiệu Năng Bảo Mật Mạng Vô Tuyến Nhận Thức Dạng Nền Cộng Tác Sử Dụng Mã Fountain," Tạp chí Khoa Học Công Nghệ Thông Tin và Truyền Thông (JSTIC), vol. 1, no. 4A, pp. 112-120, 12/2020.
[29] T. L. Thanh, N. N. Tan, T. T. Duy, T. T. Phuong, M. Voznak, A. I. Aravanis, "Broadcasting in Cognitive Radio Networks: A Fountain Codes Approach," IEEE Transactions on Vehicular Technology, vol. 71, no. 10, pp. 11289-11294, Oct. 2022.
[30] P. T. Tin, D. T. Hung, T. T. Duy and M. Voznak, "Analysis of Probability of Non-zero Secrecy Capacity for Multi-hop Networks in Presence of Hardware Impairments over Nakagami-m Fading Channels," RadioEngineering, vol. 25, no. 4, pp. 774-782, Dec. 2016.
[31] I. S. Gradshteyn, I. M. Ryzhik. Table of integrals, series, and products. Academic press, 2014.

PERFORMANCE EVALUATION OF MULTI-CAST NETWORKS USING FOUNTAIN CODES AND COOPERATIVE JAMMING TECHNIQUE

Abstract: In this paper, we study outage probability and intercept probability of multi-cast networks using Fountain codes. In the proposed scheme, a source uses Fountain codes to send the same data to a group of destinations. In addition, multiple eavesdroppers also attempt to overhear Fountain packets that are sent be the source. To protect the source data, jammer nodes that are near the destinations are employed to generate jamming noises over the eavesdroppers. We derive exact closed-form expressions of outage probability and intercept probability of the proposed scheme over Rayleigh fading channels. The simulated results are then performed to verify the theoretical results, as well as to evaluate impact of the system parameters on the system performance.

Nguyễn Văn Hiền nhận bằng Thạc sỹ vào năm 2022 tại Học Viện Công Nghệ Bưu Chính Viễn Thông. Hiện đang công tác tại Khoa Viễn Thông 2, Học Viện Công Nghệ Bưu Chính Viễn Thông cơ sở tại TP. Hồ Chí Minh. Hướng nghiên cứu đang quan tâm bao gồm: truyền thông vô tuyến, mạng IoT.

Trần Trung Duy hiện đang công tác tại Học Viện Công Nghệ Bưu Chính Viễn Thông cơ sở tại TP. Hồ Chí Minh. Hướng nghiên cứu hiện tại bao gồm: truyền thông cộng tác, vô tuyến nhận thức, NOMA, Mã Fountain.

Lê Quang Phú, trưởng Phòng Đào tạo và Khoa học công nghệ, Học Viện Công Nghệ Bưu Chính Viễn Thông, cơ sở tại TP. Hồ Chí Minh. Lĩnh vực nghiên cứu và giảng dạy bao gồm: điện tử, mạng cảm biến, mạng IoT.

Tân Hạnh, Phó giám đốc Học Viện Công Nghệ Bưu Chính Viễn Thông, phụ trách cơ sở tại TP.HCM, nhận bằng Tiến Sỹ tại Grenoble Institute of Technology, Pháp. Lĩnh vực nghiên cứu bao gồm: học máy, truy xuất thông tin, xử lý ảnh.