ĐÁNH GIÁ HIỆU NĂNG BẢO MẬT CỦA MẠNG VÔ TUYẾN CHUYỂN TIẾP ĐA CHẶNG

Chu Tiến Dũng*, **Võ Nguyễn Quốc Bảo**† **và Nguyễn Lương Nhật**†
* Đại Học Thông Tin Liên Lạc, Khánh Hòa
† Học Viện Công Nghệ Bưu Chính Viễn Thông Cơ Sở TP. Hồ Chí Minh

***Tóm tắt*—Truyền thông chuyển tiếp đã thể hiện được rất nhiều ưu điểm vượt trội trong hệ thống thông tin vô tuyến, đặc biệt là nâng cao khả năng bảo mật của hệ thống. Trong bài báo này, chúng tôi đánh giá hiệu năng bảo mật của mạng vô tuyến nhận thức chuyển tiếp đa chặng sử dụng kỹ thuật lựa chọn nút chuyển tiếp tốt nhất tại mỗi chặng. Cụ thể, chúng tôi đưa ra các biểu thức Xác suất dừng bảo mật - Secure Outage Probability (SOP) và Xác suất lượng bảo mật khác không - Probability of Non-zero Secrecy Capacity (PrNZ) cho giao thức chuyển tiếp ngẫu nhiên-và-chuyển tiếp - Randomize-and-Forward (RF) sử dụng kỹ thuật lựa chọn nút chuyển tiếp tốt nhất ở mỗi chặng. Cuối cùng, các kết quả mô phỏng Monte-Carlo sẽ được trình bày để kiểm chứng phương pháp phân tích và biểu thức phân tích đạt được.**

***Từ khóa*—Vô tuyến nhận thức, Chuyển tiếp có lựa chọn, Dung lượng bảo mật khác không, Xác suất dừng bảo mật, Dung lượng bảo mật.**

I. GIỚI THIỆU

Mạng thông tin vô tuyến đã trở thành một phần không thể thiếu của đời sống, đặc biệt trong lĩnh vực ngân hàng và quân đội, và ngày càng phát triển mạnh mẽ. Do đặc tính quảng bá của kênh truyền vô tuyến, người dùng không hợp pháp cũng có thể dễ dàng thu nhận được thông tin, hay thậm chí có thể tấn công và sửa đổi thông tin. Vì lý do đó, bảo mật trong thông tin vô tuyến đóng vai trò hết sức quan trọng. Theo quan điểm truyền thống, bản mật trong thông tin vô tuyến được thực hiện ở các lớp trên lớp vật lý, và tất cả các giao thức mật mã được sử dụng rộng rãi hiện nay (RSA, AES,...) đều được thiết kế và thực hiện với giả thiết là lớp vật lý đã được thiết lập và cung cấp một đường truyền không có lỗi [1].

Những năm gần đây, nhiều nghiên cứu cho thấy lớp vật lý có khả năng tăng cường độ bảo mật của hệ thống thông tin vô tuyến, vì vậy các nhà nghiên cứu đã tập trung nghiên cứu về bảo mật thông tin ở lớp vật lý. Lý thuyết bảo mật thông tin là nguyên lý cơ bản của bảo mật lớp vật lý, và chủ yếu được xây dựng dựa trên khái niệm bảo mật hoàn hảo của Shannon [2]. Khái niệm này cho thấy khả năng hệ thống thông tin vô tuyến vẫn đảm bảo an toàn khi kẻ nghe trộm có đầy đủ năng lực để giải mã, phân tích thông tin được truyền từ nguồn đến đích. Sau đó, năm 1975, trong [3], Wyner đã đưa ra mô hình kênh nghe trộm và chứng minh được rằng hệ thống có thể đạt được bảo mật hoàn toàn nếu tốc độ truyền nhỏ hơn hiệu dung lượng giữa kênh chính và kênh nghe trộm mà không cần phải mật mã cho dữ liệu. Sau đó, đến năm 1978, trong [4] đã mở rộng mô hình Wyner cho kênh Gaussian, kết quả cũng cho thấy độ bảo mật của hệ thống sẽ được đảm bảo nếu tốc độ truyền nhỏ hơn dung lượng bảo mật.

Trong bảo mật thông tin lớp vật lý, có ba tham số hiệu năng quan trọng dùng để đánh giá khả năng bảo mật của hệ thống thông tin vô tuyến, đó là: i) xác suất dừng bảo mật - Secrecy Outage Probability (SOP), ii) xác suất dung lượng bảo mật khác không - Probability of Non-zero Secrecy capacity (PrNZ) và iii) dung lượng bảo mật - Secrecy Capacity (CS) là các tham số để [5].

Tuy nhiên, khả năng bảo mật của hệ thống vô tuyến có thể không đảm bảo khi các điều kiện vật

Tác giả liên hệ: Chu Tiến Dũng, email: chutien-dung@tcu.edu.vn

Đến tòa soạn: , chỉnh sửa: , chấp nhận đăng: 19/12/2017.
Một phần kết quả của bài báo này đã được trình bày tại quốc gia ECIT'2015.

lý của kênh truyền hợp pháp kém hơn điều kiện vật lý của kênh truyền không hợp pháp. Để khắc phục tình trạng này, truyền thông chuyển tiếp hay truyền thông hợp tác thường là một giải pháp tốt mà ở đó các nút chuyển tiếp sẽ hợp tác và trợ giúp để cải thiện điều kiện vật lý của kênh truyền hợp pháp nhằm nâng cao khả năng bảo mật của hệ thống thông tin vô tuyến, ví dụ: [6], [7], [8]. Một xu hướng khác gần đây là sử dụng nhiễu nhân tạo nhằm tăng khả năng bảo mật của hệ thống, ví dụ [9], [10], [11], [12], [13].

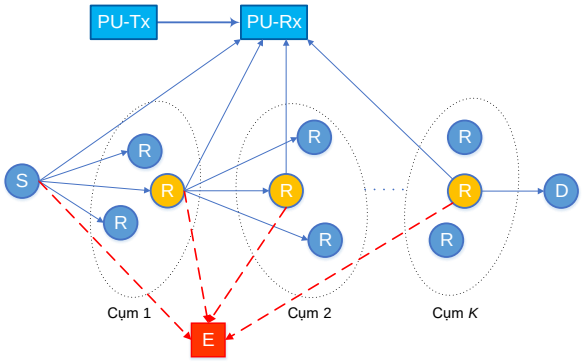
Trong khi các nghiên cứu nói trên chỉ đề cập đến hệ thống vô tuyến chuyển tiếp hai chặng thì bài báo [14] đã đánh giá khả năng bảo mật lớp vật lý của mạng thông tin vô tuyến với nhiều chặng chuyển tiếp. Các kết quả phân tích trong bài báo đã chỉ ra các ưu điểm vượt trội của kỹ thuật chuyển tiếp đa chặng trong bảo mật thông tin của hệ thống.

Ngày nay, với sự phát triển rất nhanh của thiết bị di động đã làm cho nhu cầu sử dụng phổ tần vô tuyến gia tăng nhanh chóng. Với chính sách phân bổ phổ tần hiện nay, các dải phổ được cấp phép theo từng nhóm thiết bị và có phần nào đó gây khó khăn cho việc triển khai các công nghệ vô tuyến mới [15]. Trong các giải pháp tiềm năng thì vô tuyến nhận thức là giải pháp tốt để giải quyết bài toán hạn chế về phổ tần [16], [17]. Trong hệ thống vô tuyến nhận thức, người dùng thứ cấp - Secondary Users (SUs) có thể sử dụng tạm thời tần số của người dùng sơ cấp - Primary Users (PUs) khi PUs không sử dụng. Với cơ chế này, các khoảng phổ trắng được tận dụng cho SUs và dẫn đến hiệu suất sử dụng của toàn bộ giải tần được cải thiện đáng kể. Kết hợp mạng vô tuyến nhận thức với truyền thông chuyển tiếp sẽ mang lại nhiều lợi ích như mở rộng phạm vi truyền tải thông tin, giảm can nhiễu cho các hệ thống khác mà vẫn đảm bảo được chất lượng truyền tải tin tức từ nguồn đến đích [18], [19], [20].

Trong bài báo này, chúng tôi quan tâm đến mô hình nghiên cứu tổng quát của bài [14] và khảo sát khả năng bảo mật lớp vật lý khi sử dụng kỹ thuật lựa chọn nút chuyển tiếp tốt nhất ở từng chặng. Để đánh giá khả năng bảo mật của hệ thống, chúng tôi phân tích và đánh giá các tham số SOP, PrNZ của hệ thống trên kênh truyền fading Rayleigh. Các kết quả phân tích được đánh giá thông qua mô phỏng Monte-Carlo trên phần mềm Matlab.

Phần còn lại của bài báo được tổ chức như sau. Mục II trình bày mô hình hệ thống; Mục III trình bày chi tiết các phân tích đánh giá hiệu năng bảo mật của hệ thống; Mục IV trình bày kết quả mô phỏng bằng phần mềm Matlab, và cuối cùng Mục V là tóm tắt kết luận thông qua các phân tích, đánh giá đã được trình bày ở trên.

II. MÔ HÌNH HỆ THỐNG



Hình 1. Mô hình hệ thống chuyển tiếp đa chặng sử dụng kỹ thuật lựa chọn nút chuyển tiếp từng phần.

Mô hình đề xuất xem xét của bài báo này là một hệ thống chuyển tiếp đa chặng trong môi trường vô tuyến nhận thức như trình bày ở Hình 1. Trong đó, hệ thống mạng thứ cấp bao gồm một nút nguồn (S) và một nút đích (D), có sự tồn tại một nút nghe trộm (E). Giả sử không có đường truyền trực tiếp từ nút nguồn đến nút đích, như vậy nút nguồn truyền thông tin đến nút đích thông qua nhiều cụm (cluster) chuyển tiếp tin cậy. Chúng tôi giả sử có K cụm giữa nút nguồn và nút đích. Mỗi cụm có số nút lần lượt là: $N_1, N_2, ..., N_K$. Nút chuyển tiếp trung gian tốt nhất được lựa chọn ở mỗi cụm giải mã hoàn toàn các thông tin bí mật nhận được và sau đó mã hóa lại rồi chuyển tiếp đến nút đích qua kênh vô tuyến fading. Giả sử rằng tất cả các nút được trang bị một antena và hoạt động ở chế độ bán song công. Trong khi đó, tại mỗi chặng, nút nghe trộm cũng cố gắng thu, giải mã thông tin qua kênh bất hợp pháp. Chúng tôi giả định rằng, nút phát (nút nguồn hoặc nút chuyển tiếp) có đầy đủ thông tin trạng thái - Channel Status Information (CSI) của cả hai kênh chính và kênh nghe trộm. Trong mô hình này chúng tôi sử dụng phương pháp chuyển tiếp RF để nút nghe trộm không kết hợp được dữ liệu ở các chặng.

III. ĐÁNH GIÁ HIỆU NĂNG HỆ THỐNG

Gọi R_b^{i+1} với $i = 0, 1, 2, \ldots, K$ là nút chuyển tiếp tốt nhất được chọn ở cụm thứ $i+1$. Với hai trường hợp đặc biệt: $i = 0$ thì R_b^0 là nút nguồn S, $R_b^0 \equiv$ S và $i = K$ thì R_b^{i+1} là nút đích D, $R_b^{i+1} \equiv$ D. Ta có thể viết

$$R_b^{i+1} = \underset{j=1,2,\ldots,N_{i+1}}{\arg\max}\ \gamma_{R_b^i, R_j^{i+1}}. \quad (1)$$

Xét chặng thứ i với $i = 1, 2, \ldots, K$, công suất phát của nút được chọn để chuyển tiếp là [21], [22]

$$P_{R_b^{i-1}} = \frac{I_{th}}{\gamma_{R_b^{i-1},P}}, \quad (2)$$

với I_{th} là mức can nhiễu tối đa cho trước mà máy thu sơ cấp có thể chịu đựng được.

Ta ký hiệu $\gamma_{R_b^{i-1},P}$ là độ lợi kênh truyền giữa R_b^{i-1} và PU, $\gamma_{R_b^{i-1},R_b^i}$ là độ lợi kênh truyền giữa R_b^{i-1} và R_b^i, và $\gamma_{R_b^{i-1},E}$ là độ lợi kênh truyền giữa R_b^i và E. Ở kênh truyền fading Rayleigh, các độ lợi kênh truyền $\gamma_{R_b^{i-1},P}$, $\gamma_{R_b^{i-1},R_b^i}$ và $\gamma_{R_b^{i-1},E}$ có phân phối mũ với thông số đặc trưng lần lượt là $\lambda_{i-1,P}$, $\lambda_{i-1,i}$ và $\lambda_{i-1,E}$.

Theo [2], dung lượng chuẩn hóa tức thời của kênh dữ liệu là

$$\begin{aligned} C_{R_b^{i-1},R_b^i} &= \log_2\left(1 + \frac{I_{th}\gamma_{R_b^{i-1},R_b^i}}{N_0\gamma_{R_b^{i-1},P}}\right) \\ &= \log_2\left(1 + Q\frac{\gamma_{R_b^{i-1},R_b^i}}{\gamma_{R_b^{i-1},P}}\right) \end{aligned} \quad (3)$$

với $Q = I_{th}/N_0$ và N_0 là phương sai của nhiễu cộng. Dung lượng chuẩn hóa tức thời của kênh nghe trộm là

$$C_{R_b^{i-1},E} = \log_2\left(1 + Q\frac{\gamma_{R_b^{i-1},E}}{\gamma_{R_b^{i-1},P}}\right). \quad (4)$$

Dung lượng bảo mật ở chặng thứ i 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 trộm, cụ thể [2]

$$\begin{aligned} C_{\text{sec}}^i &= \max\left(0, C_{R_b^{i-1},R_b^i} - C_{R_b^{i-1},E}\right) \\ &= \max\left[0, \log_2\left(\frac{1 + Q\frac{\gamma_{R_b^{i-1},R_b^i}}{\gamma_{R_b^{i-1},P}}}{1 + Q\frac{\gamma_{R_b^{i-1},E}}{\gamma_{R_b^{i-1},P}}}\right)\right]. \end{aligned} \quad (5)$$

Trong hệ thống truyền thông đa chặng, chặng yếu nhất sẽ quyết định hiệu năng của hệ thống [14]. Do đó, ta có thể viết dung lượng bảo mật của hệ thống như sau:

$$\begin{aligned} C_{\text{sec}} &= \min_{i=1,2,\ldots,K} C_{\text{sec}}^i \\ &= \min_{i=1,2,\ldots,K} \max\left[0, \log_2\left(\frac{1 + Q\frac{\gamma_{R_b^{i-1},R_b^i}}{\gamma_{R_b^{i-1},P}}}{1 + Q\frac{\gamma_{R_b^{i-1},E}}{\gamma_{R_b^{i-1},P}}}\right)\right]. \end{aligned} \quad (6)$$

A. Xác suất dừng bảo mật

Xác suất dừng bảo mật là một thông số quan trọng để đánh giá chất lượng của của hệ thống thứ cấp, SOP cho chúng ta biết chất lượng của hệ thống mà không cần biết hệ thống sử dụng phương pháp điều chế và giải điều chế nào. Bởi vì, SOP chỉ so sánh dung lượng bảo mật nhỏ hơn một giá trị dung lượng bảo mật dương cho trước C_{th}. Viết theo biểu thức toán học, ta có

$$\begin{aligned} \text{SOP} &= \Pr\left(C_{\text{sec}} < C_{th}\right) \\ &= \Pr\left(\min_{i=1,2,\ldots,K} C_{\text{sec}}^i < C_{th}\right). \end{aligned} \quad (7)$$

Giả sử rằng kênh truyền giữa các chặng là độc lập với nhau, ta viết lại (7) như (8) được trình bày ở đầu trang sau. Để tìm được SOP, ta cần phải tính I_i trong (8). Đặt $\rho = 2^{C_{th}}$, ta viết lại I_i như sau [23], [14]

$$\begin{aligned} I_i &= \Pr\left(\frac{1 + Q\frac{\gamma_{R_b^{i-1},R_b^i}}{\gamma_{R_b^{i-1},P}}}{1 + Q\frac{\gamma_{R_b^{i-1},E}}{\gamma_{R_b^{i-1},P}}} < 2^{C_{th}}\right) \\ &= \int_0^\infty F_{\gamma_{R_b^{i-1},R_b^i}}\left(\frac{\rho - 1}{Q}x + \rho y\right) \\ &\quad \times f_{\gamma_{R_b^{i-1},P}}(x)\, f_{\gamma_{R_b^{i-1},E}}(y)\, dxdy. \end{aligned} \quad (9)$$

Khi sử dụng kỹ thuật lựa chọn nút chuyển tiếp từng phần ở từng chặng [24], ta có thể viết

$$\gamma_{R_b^i,R_j^{i+1}} = \max_{j=1,2,\ldots,i+1} \gamma_{R_b^i,R_j^{i+1}} \quad (10)$$

nên hàm phân bố xác suất tích lũy của $\gamma_{R_b^{i-1},R_b^i}$, $F_{\gamma_{R_b^{i-1},R_b^i}}\left(\frac{\rho-1}{Q}x + \rho y\right)$, có dạng như (11) được trình bày ở đầu trang sau.

Thay thế (11) vào (9) và thực hiện tích phân, ta có biểu thức dạng đóng cho I_i như (12). Cuối

$$\begin{aligned}\mathrm{SOP} =& \Pr\left[\min_{i=1,2,\ldots,K} \max\left(0, \log_2\left(\frac{1+Q\frac{\gamma_{R_b^{i-1},R_b^i}}{\gamma_{R_b^{i-1},P}}}{1+Q\frac{\gamma_{R_b^{i-1},E}}{\gamma_{R_b^{i-1},P}}}\right)\right) < C_{th}\right] \\ =& 1-\prod_{i=1}^{K}\Bigg[1-\underbrace{\Pr\left(\max\left(0, \log_2\left(\frac{1+Q\frac{\gamma_{R_b^{i-1},R_b^i}}{\gamma_{R_b^{i-1},P}}}{1+Q\frac{\gamma_{R_b^{i-1},E}}{\gamma_{R_b^{i-1},P}}}\right)\right) < C_{th}\right)}_{I_i}\Bigg] \end{aligned} \tag{8}$$

$$\begin{aligned} I_i =& \int_0^{+\infty} \lambda_{i-1,P}\exp\left(-\lambda_{i-1,P}x\right)\lambda_{i-1,E}\exp\left(-\lambda_{i-1,E}y\right) \\ &\times\left[1+\sum_{n=1}^{N_i}(-1)^n C_{N_i}^n \exp\left(-n\lambda_{i-1,i}\frac{\rho-1}{Q}x\right)\exp\left(-n\lambda_{i-1,i}\rho y\right)\right]dxdy \\ =& 1+\sum_{n=1}^{N_i}(-1)^n C_{N_i}^n \int_0^{+\infty}\lambda_{i-1,P}\exp\left(-\lambda_{i-1,P}x\right)\lambda_{i-1,E} \\ &\times\exp\left(-\lambda_{i-1,E}y\right)\exp\left(-n\lambda_{i-1,i}\frac{\rho-1}{Q}x\right)\exp\left(-n\lambda_{i-1,i}\rho y\right)dxdy \\ =& 1+\sum_{n=1}^{N_i}(-1)^n C_{N_i}^n \frac{\lambda_{i-1,P}}{\lambda_{i-1,P}+n\lambda_{i-1,i}\frac{\rho-1}{Q}}\cdot\frac{\lambda_{i-1,E}}{\lambda_{i-1,E}+n\lambda_{i-1,i}\rho} \end{aligned} \tag{11}$$

$$\begin{aligned} I_i =& \int_0^{+\infty} \lambda_{i-1,P}\exp\left(-\lambda_{i-1,P}x\right)\lambda_{i-1,E}\exp\left(-\lambda_{i-1,E}y\right) \\ &\times\left[1+\sum_{n=1}^{N_i}(-1)^n \binom{N_i}{n} \exp\left(-n\lambda_{i-1,i}\frac{\rho-1}{Q}x\right)\exp\left(-n\lambda_{i-1,i}\rho y\right)\right]dxdy \\ =& 1+\sum_{n=1}^{N_i}(-1)^n \binom{N_i}{n} \frac{\lambda_{i-1,P}}{\lambda_{i-1,P}+n\lambda_{i-1,i}\frac{\rho-1}{Q}}\frac{\lambda_{i-1,E}}{\lambda_{i-1,E}+n\lambda_{i-1,i}\rho} \end{aligned} \tag{12}$$

$$\mathrm{SOP} = 1-\prod_{i=1}^{K}\left[\sum_{n=1}^{N_i}(-1)^{n+1}\binom{N_i}{n}\frac{\lambda_{i-1,P}}{\lambda_{i-1,P}+n\lambda_{i-1,i}\frac{\rho-1}{Q}}\frac{\lambda_{i-1,E}}{\lambda_{i-1,E}+n\lambda_{i-1,i}\rho}\right] \tag{13}$$

cùng, kết hợp (12) và (8), ta tìm được biểu thức dạng đóng của SOP như ở công thức (13). Tiếp theo, chúng tôi khảo sát hiệu năng xác suất dừng bảo mật ở các giá trị Q lớn. Thật vậy, khi Q đủ lớn, ta có thể xấp xỉ (3) và (4) như sau:

$$\begin{aligned} C_{R_b^{i-1},R_b^i} &\overset{Q\to+\infty}{\approx} \log_2\left(Q\frac{\gamma_{R_b^{i-1},R_b^i}}{\gamma_{R_b^{i-1},P}}\right), \\ C_{R_b^{i-1},E} &\overset{Q\to+\infty}{\approx} \log_2\left(Q\frac{\gamma_{R_b^{i-1},E}}{\gamma_{R_b^{i-1},P}}\right). \end{aligned} \tag{14}$$

Do đó, xác suất dừng bảo mật trong (9) có thể

xấp xỉ như sau:

$$I_i \overset{Q\to+\infty}{\approx} \Pr\left(\frac{Q\gamma_{R_b^{i-1},R_b^i}/\gamma_{R_b^{i-1},P}}{Q\gamma_{R_b^{i-1},E}/\gamma_{R_b^{i-1},P}} < \rho\right) \overset{Q\to+\infty}{\approx} \Pr\left(\gamma_{R_b^{i-1},R_b^i} < \rho\gamma_{R_b^{i-1},E}\right) \overset{Q\to+\infty}{\approx} \int_0^\infty f_{\gamma_{R_b^{i-1},E}}(x)\, F_{\gamma_{R_b^{i-1},R_b^i}}(\rho x)\, dx. \quad (15)$$

Tương tự như cách tính toán ở trên, ta có thể đạt được I_i bằng biểu thức sau:

$$\begin{aligned} I_i &\overset{Q\to+\infty}{\approx} 1 + \sum_{n=1}^{N_i} (-1)^n C_{N_i}^n \\ &\quad \times \int_0^{+\infty} \lambda_{i-1,E} \exp(-\lambda_{i-1,E}x) \\ &\quad \times \exp(-n\lambda_{i-1,i}\rho x) dx \\ &\overset{Q\to+\infty}{\approx} 1 + \sum_{n=1}^{N_i} (-1)^n C_{N_i}^n \frac{\lambda_{i-1,E}}{\lambda_{i-1,E} + n\lambda_{i-1,i}\rho} \end{aligned} \quad (16)$$

Cuối cùng, xác suất dừng bảo mật toàn trình có thể được dẫn ra như trong công thức số (17) bên dưới:

$$\mathrm{SOP} \overset{Q\to+\infty}{\approx} 1 - \prod_{i=1}^{K} \left[\sum_{n=1}^{N_i} (-1)^{n+1} \binom{N_i}{n} \frac{\lambda_{i-1,E}}{\lambda_{i-1,E} + n\lambda_{i-1,i}\rho}\right]. \quad (17)$$

Quan sát từ công thức số (17), ta thấy rằng, khi giá trị Q lớn, xác suất dừng bảo mật hội tụ về một giá trị không phụ thuộc vào Q. Hơn thế nữa, giá trị này chỉ phụ thuộc vào các tham số đặc trưng của kênh dữ liệu ($\lambda_{i-1,i}$) và kênh nghe lén ($\lambda_{i-1,E}$) mà không phụ thuộc vào tham số của kênh giữa mạng thứ cấp và mạng sơ cấp ($\lambda_{i-1,P}$).

B. Xác suất dung lượng bảo mật khác không

Xác suất dung lượng bảo mật khác không là thông số bảo mật của hệ thống thể hiện xác suất mà dung lượng Shannon của kênh truyền dữ liệu lớn hơn kênh truyền nghe trộm, cụ thể được biểu diễn ở biểu thức (18).

Sử dụng phương pháp tương tự như cho (7), ta có thể viết lại PrNZ như sau

$$\begin{aligned} &\mathrm{PrNZ} \\ &= \prod_{i=1}^{K} \Pr\left(1 + Q\frac{\gamma_{R_b^{i-1},R_b^i}}{\gamma_{R_b^{i-1},P}} > 1 + Q\frac{\gamma_{R_b^{i-1},E}}{\gamma_{R_b^{i-1},P}}\right) \\ &= \prod_{i=1}^{K} \Pr\left(\gamma_{R_b^{i-1},R_b^i} > \gamma_{R_b^{i-1},E}\right). \end{aligned} \quad (19)$$

Xét xác suất $\Pr\left(\gamma_{R_b^{i-1},R_b^i} > \gamma_{R_b^{i-1},E}\right)$ trong (19), sử dụng xác suất điều kiện, ta có [23]:

$$\begin{aligned} &\Pr\left(\gamma_{R_b^{i-1},R_b^i} > \gamma_{R_b^{i-1},E}\right) \\ &= \int_0^{+\infty} f_{\gamma_{R_b^{i-1},E}}(x) \left[1 - F_{\gamma_{R_b^{i-1},R_b^i}}(x)\right] dx \\ &= \sum_{n=1}^{N_i} (-1)^{n+1} \binom{N_i}{n} \int_0^{+\infty} \lambda_{i-1,E} \\ &\quad \times \exp\left(-\lambda_{i-1,E}x\right) \exp\left(-n\lambda_{i-1,i}x\right) dx \\ &= \sum_{n=1}^{N_i} (-1)^{n+1} \binom{N_i}{n} \frac{\lambda_{i-1,E}}{\lambda_{i-1,E} + n\lambda_{i-1,i}}. \end{aligned} \quad (20)$$

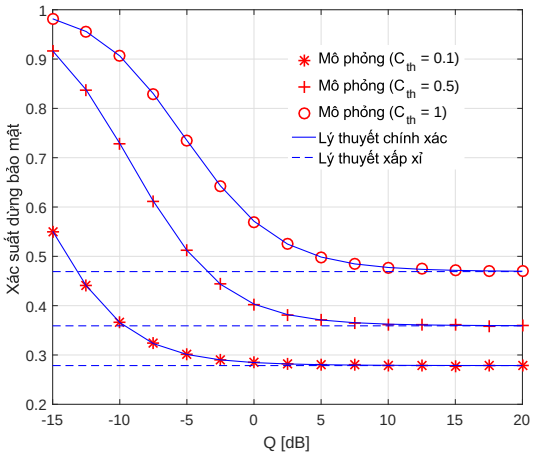
Thay thế (20) vào (19), ta được công thức dạng tường minh của xác suất dung lượng bảo mật khác không của hệ thống.

IV. KẾT QUẢ MÔ PHỎNG

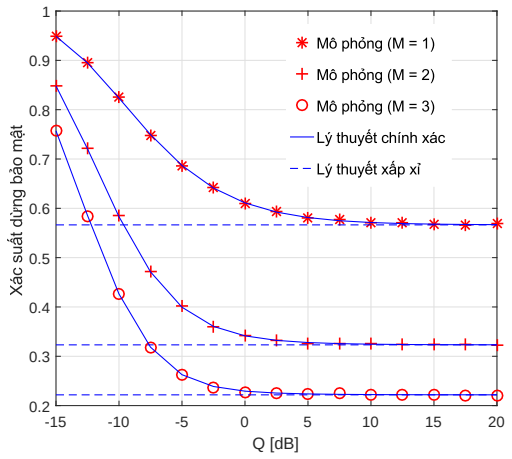
Trong phần này, chúng tôi sẽ thực hiện mô phỏng trên phần mềm Matlab để kiểm chứng các kết quả phân tích ở phần trên. Xem xét mô hình hệ thống ở không gian hai chiều với nút nguồn đặt ở vị trí (0, 0), nút đích đặt tại vị trí (1, 0), các nút chuyển tiếp của cụm i đặt ở vị trí (i/K, 0). Nút E được đặt tại vị trí (x_E, y_E), nút PU ở vị trí (x_P, y_P). Khoảng cách giữa hai nút R_b^{i-1} và R_b^i là $d_{i-1,i} = 1/K$, khoảng cách giữa nút R_b^{i-1} và P sẽ là $d_{i-1,P} = \sqrt{\left(\frac{i-1}{K} - x_P\right)^2 + (y_P)^2}$ và $d_{i-1,E} = \sqrt{\left(\frac{i-1}{K} - x_E\right)^2 + (y_E)^2}$. Độ lợi kênh truyền sử dụng mô hình suy hao đường truyền đơn giản như sau: $\lambda_{i-1,P} = (d_{i-1,P})^\beta$, $\lambda_{i-1,i} = (d_{i-1,i})^\beta$ và $\lambda_{i-1,E} = (d_{i-1,E})^\beta$ với β là hệ số suy hao đường truyền được cố định bằng 3.

Trong Hình 2, chúng tôi khảo sát xác suất dừng bảo mật theo giá trị của Q (dB). Trong mô phỏng này, số cụm được cố định bằng 2 (K=2) và số nút trong mỗi cụm bằng 2 ($N_1 = N_2 = 2$), vị

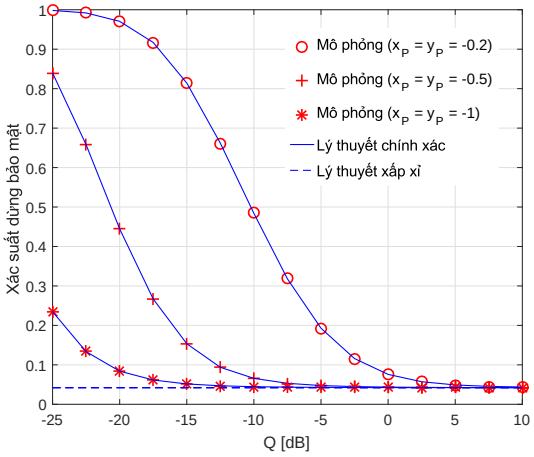
$$\mathrm{PrNZ} = \Pr\left(C_{\mathrm{sec}} > 0\right) = \Pr\left[\min_{i=1,2,\ldots,K} \max\left(0, \log_2\left(\frac{1+Q\frac{\gamma_{R_b^{i-1},R_b^i}}{\gamma_{R_b^{i-1},P}}}{1+Q\frac{\gamma_{R_b^{i-1},E}}{\gamma_{R_b^{i-1},P}}}\right)\right) > 0\right]. \quad (18)$$



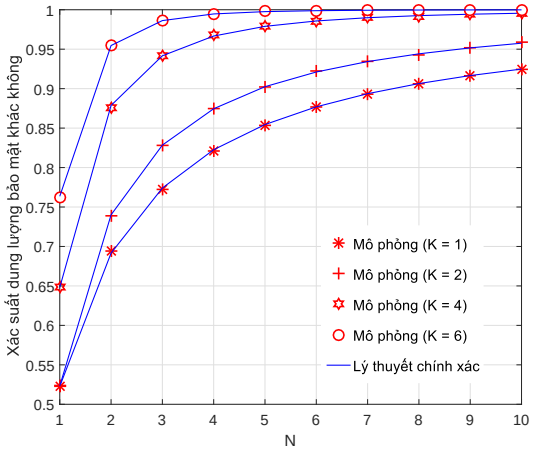
Hình 2. Xác suất dừng bảo mật biểu diễn theo giá trị Q [dB] khi $x_E = 1, y_E = 0.25, x_P = -0.5, y_P = -0.5$, $C_{th} = \{0.1, 0.5, 1\}$, $K = 2$, $N_1 = 2$, $N_2 = 2$.



Hình 3. Xác suất dừng bảo mật biểu diễn theo giá trị Q [dB] khi $x_E = 1, y_E = 0.25, x_P = -0.5, y_P = -0.5$, $C_{th} = 0.75$, $K = 3$, và $N_1 = N_2 = N_3 = N$.



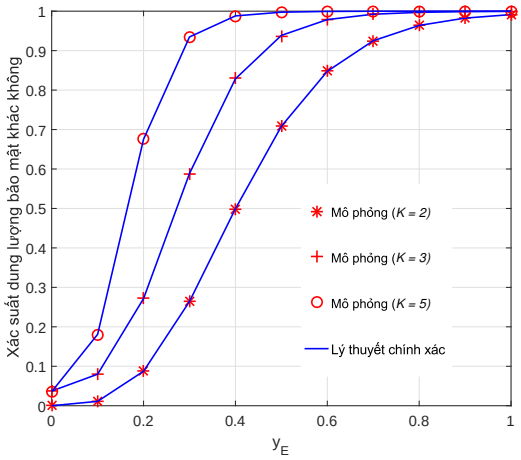
Hình 4. Xác suất dừng bảo mật biểu diễn theo giá trị Q (dB) khi $x_E = 0.5, y_E = 0.5$, $C_{th} = 0.25$, $K = 4$, $N_1 = 2$, $N_2 = 3$, $N_3 = 2$ và $N_4 = 3$.



Hình 5. Xác suất dung lượng bảo mật khác không biểu diễn theo giá trị N khi $x_E = 1, y_E = 0.25$, và $K = 1, 2, 4, 6$.

trí của nút nghe lén là (1, 0.25), vị trí của nút sơ cấp là (-0.5, -0.5); và giá trị của C_{th} thay đổi từ 0.1 đến 1. Từ hình vẽ, ta thấy rằng xác suất dừng bảo mật SOP giảm theo sự gia tăng của Q. Tuy nhiên, khi Q đủ lớn, SOP hội tụ về kết quả lý thuyết xấp xỉ (LT-XX). Ta cũng có thể thấy rằng, hiệu năng bảo mật SOP cũng giảm khi giá trị của C_{th} tăng. Cuối cùng, Hình 2 cho thấy rằng kết quả mô phỏng (MP) trùng khít với kết quả phân tích lý thuyết chính xác (LT-CX), điều này minh chứng cho sự chính xác trong các phân tích lý thuyết.

Trong Hình 3, chúng tôi khảo sát sự ảnh hưởng của số lượng nút trong mỗi cụm lên giá trị của SOP. Cụ thể, chúng tôi cố định giá trị số chặng



Hình 6. Xác suất dung lượng bảo mật khác không biểu diễn theo giá trị y_E khi $x_E = 0.5$, $N = 3$ và $K = 2, 3, 5$.

bằng 3 (K=3) và giả sử số nút trong mỗi cụm bằng nhau và bằng N ($N_1 = N_2 = N_3 = N$). Các thông số còn lại được xác lập như sau: $x_E = 1, y_E = 0.25, x_P = -0.5, y_P = -0.5$ và $C_{th} = 0.75$. Quan sát từ hình vẽ, ta thấy rằng giá trị của SOP giảm đáng kể khi ta tăng số lượng nút trong mỗi cụm. Điều này có thể được giải thích đơn giản bởi khi số lượng nút tăng cũng đồng nghĩa với việc tăng dung lượng cho kênh dữ liệu. Hình 4 Khảo sát sự ảnh hưởng vị trí nút PU lên hiệu năng SOP của mô hình khảo sát. Trong hình vẽ này, nút PU được đặt ở các vị trí (-0.2, -0.2), (-0.5, -0.5) và (-1, -1). Các thông số khác có thể được liệt kê như sau: $x_E = 0.5, y_E = 0.5$, $C_{th} = 0.25$, $K = 4$, $N_1 = 2$, $N_2 = 3$, $N_3 = 2$ và $N_4 = 3$. Quan sát từ hình vẽ ta thấy rằng, giá trị SOP giảm khi PU được đặt xa mạng thứ cấp (x_P và y_P lớn). Tuy nhiên, khi giá trị Q đủ lớn, hiệu năng SOP của mô hình khảo sát sẽ không phụ thuộc vào vị trí của nút PU, như đã chứng minh trong phần 3.

Hình 5 vẽ xác suất dung lượng bảo mật khác không theo số lượng nút chuyển tiếp trong mỗi cụm. Giả sử rằng mỗi cụm có số nút bằng nhau và bằng N ($N_i = N, \forall i$). Trong hình vẽ này, các thông số được thiết lập như sau: $x_E = 1, y_E = 0.25$, và $K = 1, 2, 4, 6$. Từ hình vẽ ta thấy rằng, xác suất dung lượng bảo mật khác không tăng khi ta tăng giá trị của N. Hơn thế nữa, giá trị của xác suất dung lượng bảo mật khác không cũng tăng khi số chặng tăng. Điều này có thể được giải thích như sau: việc tăng số chặng sẽ nâng cao tốc độ của kênh dữ liệu bởi tốc độ truyền trên những chặng có khoảng cách càng nhỏ sẽ càng lớn.

Trong Hình 6, chúng tôi cố định hoàng độ của nút E tại $x_E = 0.5$ và biểu diễn xác suất dung lượng bảo mật khác không theo giá trị của tung độ y_E (y_E thay đổi từ 0 đến 1). Các tham số còn lại được cố định như sau: $x_E = 0.5$, $N = 3$ và $K = 2, 3, 5$. Ta có thể thấy từ Hình 6 rằng khi giá trị xác suất dung lượng bảo mật khác không tăng khi E cách xa tuyến từ nguồn đến đích (y_E tăng). Một lần nữa, ta cũng thấy rằng giá trị PrNZ tăng với sự gia tăng của số chặng K.

Trong Hình 5 và Hình 6, các kết quả mô phỏng (MP) và lý thuyết tính chính xác xác suất dung lượng bảo mật khác không (LT-CX) trùng khít với nhau, điều này minh chứng cho sự chính xác của các biểu thức toán được đưa ra trong phần 3.

V. KẾT LUẬN

Trong bài báo này, chúng tôi đã khảo sát hiệu năng bảo mật của mạng vô tuyến nhận thức chuyển tiếp đa chặng sử dụng kỹ thuật lựa chọn nút chuyển tiếp ở từng chặng. Cụ thể, chúng tôi đã đưa ra các biểu thức dạng đóng tính xác suất dừng bảo mật và xác suất dung lượng bảo mật khác không của mô hình khảo sát trên kênh truyền Rayleigh fading. Các kết quả tính toán được kiểm chứng bằng những mô phỏng máy tính. Các kết quả đã thể hiện rằng số nút tại mỗi cụm ảnh hưởng đáng kể lên hiệu năng bảo mật của hệ thống.

LỜI CẢM ƠN

Cảm ơn Phòng Thí Nghiệm Thông Tin Vô Tuyến (WCOMM) đã hỗ trợ trong quá trình thực hiện bài báo này.

TÀI LIỆU THAM KHẢO

[1] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[2] C. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[3] A. Wyner, "The wire-tap channel," *Bell System Technical Journal, The*, vol. 54, no. 8, pp. 1355–1387, Oct 1975.

[4] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *Information Theory, IEEE Transactions on*, vol. 24, no. 4, pp. 451–456, Jul 1978.

[5] P. K. Gopala, L. Lifeng, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.
[6] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Communications*, vol. 4, no. 15, pp. 1787–1791, 2010.
[7] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Transactions on Information Theory*, vol. 57, no. 1, pp. 137–155, 2011.
[8] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 12, no. 12, pp. 6076–6085, 2013.
[9] I. Krikidis, J. S. Thompson, P. M. Grant, and S. McLaughlin, "Power allocation for cooperative-based jamming in wireless networks with secrecy constraints," in *Proc. of 2010 IEEE GLOBECOM Workshops (GC Wkshps)*, 2010, pp. 1177–1181.
[10] Z. Ding, K. Leung, D. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Transactions on Wireless Communications*, vol. 10, no. 6, pp. 1725 – 1729, 2011.
[11] T. Koike-Akino and D. Chunjie, "Secrecy rate analysis of jamming superposition in presence of many eavesdropping users," in *Proc. of 2011 IEEE Global Telecommunications Conference (GLOBECOM 2011)*, 2011, pp. 1–6.
[12] Y. Liu, J. Li, and A. Petropulu, "Destination assisted cooperative jamming for wireless physical layer security," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 682 – 694, 2013.
[13] T. Tran and H. Kong, "CSI-secured orthogonal jamming method for wireless physical layer security," *IEEE Communications Letters*, vol. 18, no. 5, pp. 841 – 844, 2014.
[14] V. N. Q. Bao and N. L. Trung, "Multihop decode-and-forward relay networks: Secrecy analysis and relay position optimization," *REV Journal on Electronics and Communication*, vol. 2, no. 1-2, 2012.
[15] I. F. Akyildiz, L. Won-Yeol, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks [cognitive radio communications and networks]," *IEEE Transactions on Communications*, vol. 46, no. 4, pp. 40–48, 2008, 0163-6804.
[16] R. Berry, M. L. Honig, and R. Vohra, "Spectrum markets: motivation, challenges, and implications," *IEEE Communications Magazine*, vol. 48, no. 11, pp. 146–155, 2010.
[17] W. Webb, "On using white space spectrum," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 145–151, 2012.
[18] V. N. Q. Bao and T. Q. Duong, "Outage analysis of cognitive multihop networks under interference constraints," *IEICE Trans Commun*, vol. E95-B, no. 03, pp. 1019–1022, 2012.
[19] V. N. Q. Bao, T. Q. Duong, and C. Tellambura, "On the performance of cognitive underlay multihop networks with imperfect channel state information," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 4864–4873, 2013.
[20] T.-T. Tran, V. N. Q. Bao, V. Dinh Thanh, and T. Q. Duong, "Performance analysis and optimal relay position of cognitive spectrum-sharing dual-hop decode-and-forward networks," in *Proc. of the 2013 International Conference on Computing, Management and Telecommunications (ComManTel)*, 2013, pp. 269–273.
[21] V. N. Q. Bao and B. Dang Hoai, "A unified framework for performance analysis of DF cognitive relay networks under interference constraints," in *Proc. 2011 International Conference on ICT Convergence (ICTC)*, 2011, pp. 537–542.
[22] T. Q. Duong, D. Benevides da Costa, M. Elkashlan, and V. N. Q. Bao, "Cognitive amplify-and-forward relay networks over Nakagami-m fading," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 5, pp. 2368–2374, 2012.
[23] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*, 4th ed. Boston: McGraw-Hill, 2002.
[24] V. N. Q. Bao and H. Y. Kong, "Diversity order analysis of dual-hop relaying with partial relay selection," *IEICE Trans Commun*, vol. E92-B, no. 12, pp. 3942–3946, 2009.

CHU TIẾN DŨNG Sinh ngày 18 tháng 11 năm 1976.
Nhận bằng kỹ sư ngành Vô tuyến điện và Thông tin Liên lạc tại Trường Sĩ Quan Thông Tin, Binh Chủng Thông Tin Liên Lạc và thạc sĩ ngành Điện - Điện tử tại Học Viện Công Nghệ Bưu Chính Viễn Thông lần lượt năm 1999 và 2011.
Hiện tại, đang giảng dạy tại Khoa Kỹ Thuật Viễn Thông, Trường Sĩ Quan Thông Tin và đang làm nghiên cứu sinh tại Học Viện Công Nghệ Bưu Chính Viễn Thông.
Hướng nghiên cứu hiện tại là: bảo mật thông tin ở lớp vật lý.
Điện thoại: 0905121260
E-mail: chutiendung@tcu.edu.vn

PGS. TS. VÕ NGUYỄN QUỐC BẢO Sinh ngày 03 tháng 6 năm 1979. Nhận bằng Tiến sỹ chuyên ngành Thông Tin Vô Tuyến tại Đại Học Ulsan Hàn Quốc vào năm 2010. PGS. TS. Bảo là thành viên Ban Biên Tập của nhiều tạp chí khoa học chuyên ngành bao gồm:
Hiện công tác tại Khoa Kỹ Thuật Viễn Thông, Học Viện Công Nghệ Bưu Chính Viễn Thông, Cơ Sở Thành Phố Hồ Chí Minh.
Lĩnh vực nghiên cứu: Thông tin vô tuyến và thông tin số, tập trung vào truyền thông hợp tác, hệ thống MIMO, năng lượng xanh, vô tuyến nhận thức và bảo mật lớp vật lý.
Điện thoại: 0913454446
E-mail: baovnq@ptithcm.edu.vn

TS. NGUYỄN LƯƠNG NHẬT Sinh ngày 20 tháng 01 năm 1969.
Nhận bằng Tiến sỹ chuyên ngành Viễn Thông tại Đại Học Thông Tin Liên Lạc Matxcova.
Hiện công tác tại Khoa Kỹ Thuật Điện Tử, Học Viện Công Nghệ Bưu Chính Viễn Thông, Cơ Sở Thành Phố Hồ Chí Minh.
Lĩnh vực nghiên cứu: Xử lý tín hiệu cho thông tin vô tuyến.
Điện thoại: 0913725530
E-mail: nhatnl@ptithcm.edu.vn