PHÂN TÍCH HIỆU NĂNG BẢO MẬT CỦA MẠNG CHUYỂN TIẾP ĐA CHẶNG TRONG ĐIỀU KIỆN PHẦN CỨNG KHÔNG LÝ TƯỞNG

SECRECY PERFORMANCE ANALYSIS OF MULTI-HOP RELAY NETWORKS WITH HARDWARE IMPAIRMENTS

Chu Tiến Dũng[1], Võ Nguyễn Quốc Bảo[2]

[1]Trường Đại học Thông tin Liên lạc; chutiendung@tcu.edu.vn
[2]Học viện Công nghệ Bưu chính Viễn thông; baovnq@ptithcm.edu.vn

Tóm tắt - Trong bài báo này, chúng tôi đánh giá hiệu năng bảo mật của mạng vô tuyến chuyển tiếp trong điều kiện phần cứng của các nút chuyển tiếp không lý tưởng. Mô hình mạng bao gồm một nút nguồn, một nút đích và nhiều nút chuyển tiếp. Quá trình truyền thông tin từ nút nguồn đến nút đích được sự giúp đỡ của các nút chuyển tiếp và nghe lén bởi một nút nghe lén. Để đánh giá hiệu năng bảo mật của hệ thống, chúng tôi phân tích biểu thức tính chính xác dạng đóng và biểu thức xấp xỉ cho xác suất dừng bảo mật hệ thống cho hai giao thức chuyển tiếp, đó là ngẫu nhiên và chuyển tiếp (Randomize and Forward – RF) và giải mã và chuyển tiếp (Decode and Forward – DF) trên kênh truyền fading Rayleigh. Các kết quả phân tích được kiểm chứng bởi mô phỏng Monte-Carlo và chỉ ra ảnh hưởng của phần cứng không hoàn hảo lên hiệu năng bảo mật của hệ thống chuyển tiếp đa chặng.

Từ khóa - Dung lượng bảo mật khác không; xác suất dừng bảo mật; phần cứng không lý tưởng; kênh truyền fading; mạng chuyển tiếp.

Abstract - In this article, we evaluate secrecy performance of multi-hop relay networks with hardware performance. The system consists of one source, one destination and multiple immediate relays. The communication between the source and the destination is helped by relays and overheard by an eavesdropper. Specifically, we derive expressions of the system secrecy outage probability considering two relaying protocols including Randomize-and-Forward (RF) and Decode-and-Forward (DF). Finally, the Monte Carlo simulations is performed to verify the analysis expressions and to show the effect of hardware impairment on the system secrecy performance.

Key words - Non-zero secrecy capacity probability; secrecy outage probability; hardware impairments; rayleigh fading channels; relay networks.

1. Đặt vấn đề

Ngày nay, kỹ thuật chuyển tiếp [1] được sử dụng rộng rãi trong mạng vô tuyến để giảm bớt sự ảnh hưởng của hiện tượng fading và để mở rộng vùng phủ sóng của mạng. Mô hình cơ bản sử dụng kỹ thuật chuyển tiếp bao gồm: một nút nguồn, một nút đích và một hoặc nhiều nút chuyển tiếp ở giữa. Các nút chuyển tiếp sẽ hỗ trợ nút nguồn hoặc nút trước nó chuyển tiếp dữ liệu từ nguồn đến nút đích mong muốn. Trong mạng hai chặng thông thường [2], thông tin nguồn có thể được chuyển tới đích thông qua một nút chuyển tiếp tốt nhất. Trong chuyển tiếp đa chặng [3] - [4], việc truyền dữ liệu giữa nguồn và đích được thực hiện với sự giúp đỡ của nhiều nút chuyển tiếp khác nhau. Gần đây, kỹ thuật chuyển tiếp đã được áp dụng trong các mạng vô tuyến thế hệ mới như WiMax hoặc LTE [5]. Bên cạnh các ưu điểm nêu trên, nhược điểm của kỹ thuật chuyển tiếp là hiệu suất phổ tần thấp do số lượng khe thời gian trực giao sử dụng tỷ lệ với số chặng giữa nút nguồn và nút đích. Một trong những giải pháp cải thiện hiệu suất phổ tần cho mạng chuyển tiếp đa chặng là chế độ chuyển tiếp hai chiều [6] - [7], tuy nhiên các ứng dụng cho chế độ chuyển tiếp hai chiều là hạn chế trong thực tế.

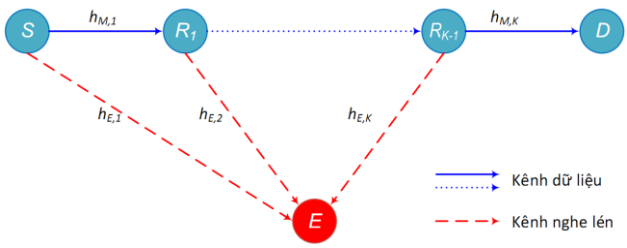
Bên cạnh hiệu năng và vùng phủ sóng, bảo mật là một trong những vấn đề quan trọng của mạng vô tuyến do tính chất mở của kênh truyền vô tuyến, cụ thể là tín hiệu được truyền đi có thể bị nghe trộm bởi các thiết bị nghe lén. Để đánh giá mức độ bảo mật của một giao thức liên lạc, Shannon đã đề ra khái niệm dung lượng bảo mật, là độ lệch giữa dung lượng kênh dữ liệu và kênh nghe lén [8] - [9]. Do đó, để nâng cao hiệu năng bảo mật của hệ thống, hoặc là tăng dung lượng kênh dữ liệu và/hoặc giảm dung lượng kênh nghe lén. Gần đây, rất nhiều nhà nghiên cứu đã tập trung vào lĩnh vực bảo mật lớp vật lý, ví dụ như [10] - [17].

Trong bài báo [10] - [11], các tác giả đưa ra mô hình chọn lựa nút chuyển tiếp tốt nhất để tăng cường dung lượng bảo mật của hệ thống. Trong bài báo [12], các tác giả quan tâm đến sự bảo mật lớp vật lý trong những mạng lưới chuyển tiếp hai chặng với chỉ một nút chuyển tiếp trung gian. Trong bài báo [13], các tác giả đề nghị các phương pháp chọn lựa nút chuyển tiếp và nút tạo nhiễu trong những mô hình chuyển tiếp hai chặng. Trong bài báo [14], tác giả tập trung nghiên cứu sự ảnh hưởng của phần cứng không lý tưởng đến bảo mật thông tin trong hệ thống MIMO nhận thức qua kênh truyền fading Rayleigh. Bài báo [15] đã nghiên cứu, đánh giá sự tác động phần cứng không lý tưởng lên mạng chuyển tiếp hai chiều cùng với kỹ thuật lựa chọn nút chuyển tiếp tốt nhất. Bài báo [16] phân tích, đánh giá, so sánh xác suất dừng và dung lượng kênh Shannon trung bình của mạng vô tuyến chuyển tiếp từng phần và toàn phần dưới sự tác động của phần cứng không lý tưởng. Trong bài báo [17], các tác giả đã phân tích hiệu năng của hệ thống vô tuyến chuyển tiếp từng phần theo phương thức khuếch đại và chuyển tiếp (Amplify and Forward – AF), nút chuyển tiếp được lựa chọn phụ thuộc vào trạng thái của kênh truyền từ nút nguồn đến nút chuyển tiếp. Với bài báo [18], các tác giả đánh giá xác suất dừng và dung lượng trung bình của kênh truyền fading Rayleigh sử dụng kỹ thuật chủ động lựa chọn nút chuyển tiếp dưới sự tác động của phần cứng không lý tưởng và nhiễu đồng kênh. Trong bài báo [19], tác giả đưa ra mô hình mạng lưới chuyển tiếp đa chặng, tác giả đánh giá rất chi tiết khả năng bảo mật của hệ thống, tuy nhiên chưa đặt hệ thống dưới sự ảnh hưởng của phần cứng không lý tưởng. Nghiên cứu [20], các tác giả phân tích khả năng bảo mật của mạng vô tuyến gây nhiễu hợp tác để đối phó với các cuộc tấn công của người nghe lén, trong khi hệ thống hợp pháp có thể loại bỏ được

hoàn toàn tín hiệu gây nhiễu và thu được thông tin bí mật. Bài báo [21], nhóm tác giả khảo sát xác suất dừng bảo mật của một hệ thống biến đổi thông tin và năng lượng đồng thời, trong hệ thống tồn tại nhiều nút nghe lén có khả năng thu thập năng lượng và tín hiệu. Bài báo [22], các tác giả khai thác giải pháp nhảy tần và hợp tác gây nhiễu để tạo ra được những chu kỳ truyền tin thuận lợi cho tạo khóa bí mật để chống lại sự tấn công của người nghe lén.

Như chúng ta đã biết, hầu hết các nghiên cứu đóng góp trong lĩnh vực chuyển tiếp cho rằng các phần cứng thu phát của các nút chuyển tiếp là hoàn hảo. Tuy nhiên, trong thực tế, phần cứng thu phát của các nút vô tuyến luôn luôn bị ảnh hưởng bởi suy yếu. Ví dụ, sự mất cân bằng chỉ số I/Q, bộ khuếch đại biên độ - biên độ không tuyến tính, và nhiễu pha [4] - [6]. Trong bài báo [23], các tác giả nghiên cứu nâng cao hiệu quả bảo mật của mạng cảm biến hợp tác RF đa đường và đa chặng dưới sự hiện diện của nhiều nút nghe trộm trong khi phần cứng của các nút cảm biến là không lý tưởng. Trong bài báo này, nhóm tác giả quan tâm đến sự bảo mật lớp vật lý trong mô hình chuyển tiếp đa chặng dưới sự ảnh hưởng của phần cứng không lý tưởng. Bài báo tập trung phân tích đánh giá tác động của phần cứng không lý tưởng ở nút nguồn, nút đích và nút chuyển tiếp trong giao thức RF và giao thức DF lên hiệu năng bao mật của hệ thống. Cụ thể hơn, chúng ta phân tích được chính xác xác suất dừng bảo mật (Secure outage probability – SOP) của hệ thống ở kênh truyền fading Rayleigh. Nhóm tác giả cũng thực hiện mô phỏng để khảo sát tác động của phần cứng không lý tưởng lên hiệu năng bảo mật của hệ thống.

2. Mô hình hệ thống



Hình 1. *Mô hình hệ thống*

Xem xét một mạng chuyển tiếp đa chặng như trình bày ở Hình 1. Mô hình mạng nghiên cứu bao gồm một nút nguồn (T_0), một nút đích (T_K), có sự tồn tại một nút nghe trộm (E). Giả sử không có sự kết nối trực tiếp từ nút nguồn đến nút đích, ví dụ do vùng phủ sóng của nút nguồn hạn chế hay do hiệu ứng bóng mờ. Do đó, quá trình trao đổi thông tin từ nút nguồn đến nút đích thông qua sự hỗ trợ của $K-1$ nút chuyển tiếp ký hiệu lần lượt là $T_1,\ldots,T_{K-1}$.

Tại các nút chuyển tiếp, nhóm tác giả xem xét hai kỹ thuật chuyển tiếp là DF và RF. Ở phương pháp RF, các nút chuyển tiếp trung gian thực hiện giải mã hoàn toàn các thông tin nhận được từ nút trước liền nó rồi thực hiện mã hóa lại sử dụng từ mã khác với từ mã đang sử dụng. Mục đích của phương pháp RF để tránh việc nút nghe lén kết hợp các thông tin nhận được từ nút nguồn và nút chuyển tiếp. Sau đó, nút chuyển tiếp chuyển dữ liệu vừa mới mã hoá đến nút kế tiếp. Ở phương pháp DF, các nút chuyển tiếp trung gian giải mã hoàn toàn các thông tin nhận được và sau đó mã hóa lại với từ mã cũ rồi chuyển tiếp đến các nút chuyển tiếp hợp pháp tiếp theo qua kênh vô tuyến fading. Rõ ràng phương pháp RF có khả năng bảo mật thông tin tốt hơn phương pháp DF, tuy nhiên do dùng các từ mã khác nhau cho mỗi chặng nên độ phức tạp và độ tiêu thụ năng lượng của phương pháp RF cũng sẽ cao hơn.

Giả sử kênh truyền xem xét trong hệ thống là kênh truyền fading Rayleigh. Ta gọi $h_{M,k}$ và $h_{E,k}$ lần lượt là hệ số kênh truyền của kênh chính và kênh nghe trộm ở chặng thứ k. Để đơn giản hóa bài toán phân tích, giả sử mức độ phần cứng không lý tưởng tại tất cả thiết bị thu phát, kể cả nghe trộm đều như nhau. Cụ thể, ta gọi κ là mức độ của phần cứng không lý tưởng tại tất cả các đầu cuối. Giả sử này là chấp nhận được trong thực tế, khi mà các nút mạng thường được chế tạo với cùng một thông số và công nghệ.

3. Đánh giá hiệu năng bảo mật

Để đánh giá hiệu năng bảo mật của hệ thống, chúng ta trước hết xem xét tỷ số tín hiệu trên tạp âm (SNR) của đường truyền từ nút T_n đến nút T_{n+1}, với $n = 0, 1, 2, ..., K-1$, dưới sự ảnh hưởng của phần cứng không lý tưởng [24]:

$$\Psi_{M,n} = \frac{P_n|h_{M,n}|^2}{P_n|h_{M,n}|^2\kappa + N_0} = \frac{\gamma_{M,n}}{\kappa\gamma_{M,n}+1}, \quad (1)$$

với $\gamma_{M,n} = \dfrac{P_n|h_{M,n}|^2}{N_0}$.

Ở kênh truyền fading RAyleign, $|h_{M,n}|^2$ là biến ngẫu nhiên hàm mũ với tham số . Do đó từ (1), ta có hàm CDF của $\Psi_{M,n}$ được biểu diễn bởi biểu thức sau:

$$F_{\Psi_{M,n}}(x) = \Pr(\Psi_{M,n} < x) = \Pr\left(\frac{\gamma_{M,n}}{\kappa\gamma_{M,n}+1} < x\right). \quad (2)$$

Để tính (2), ta sử dụng xác suất có điều kiện và xem xét hai trường hợp của κ, ta dễ dàng tính được $F_{\Psi_{M,n}}(x)$ như sau:

$$F_{\Psi_{M,n}}(x) = \begin{cases} 1; & x \geq \dfrac{1}{\kappa} \\ 1-\exp\left(-\lambda_{M,n}\dfrac{x}{1-\kappa x}\right); & x < \dfrac{1}{\kappa}. \end{cases}$$

Tiếp theo, chúng ta tính tỉ số tín hiệu trên tạp âm (SNR) của đường truyền giữa T_n và E dưới sự ảnh hưởng của phần cứng không lý tưởng như sau:

$$\Psi_{E,n} = \frac{P_n|h_{E,n}|^2}{P_n|h_{E,n}|^2\kappa + N_0} = \frac{\gamma_{E,n}}{\kappa\gamma_{E,n}+1}, \quad (3)$$

với $\gamma_{E,n} = \dfrac{P_n|h_{E,n}|^2}{N_0}$.

Ta nhận thấy rằng $\Psi_{M,n}$ và $\Psi_{E,n}$ có cùng một dạng, do

đó sử dụng kỹ thuật tương tự như với $F_{\Psi_{M,n}}(x)$, ta có được hàm CDF của $\Psi_{E,n}$ được biểu diễn bởi biểu thức:

$$F_{\Psi_{E,n}}(x) = \Pr\left(\gamma_{E,n}(1-\kappa x) < x\right) = \begin{cases} 1; & x \geq \frac{1}{\kappa} \\ 1-\exp\left(-\lambda_{E,n}\frac{x}{1-\kappa x}\right); & x < \frac{1}{\kappa}. \end{cases} \quad (4)$$

với $\lambda_{E,n}$ làm tham số của biến ngẫu nhiên hàm mũ $|h_{E,n}|^2$.

Từ các biểu thức hàm CDF của $\Psi_{M,n}$ và $\Psi_{E,n}$, ta tính được hàm PDF của $\Psi_{M,n}$ và $\Psi_{E,n}$ sử dụng mối quan hệ giữa hàm CDF và hàm PDF lần lượt như sau:

$$f_{\Psi_{M,n}}(x) = \begin{cases} 0; & x \geq \frac{1}{\kappa} \\ \frac{\lambda_{M,n}}{(1-\kappa x)^2}\exp\left(-\frac{\lambda_{M,n}x}{1-\kappa x}\right); & x < \frac{1}{\kappa}, \end{cases} \quad (5)$$

$$f_{\Psi_{E,n}}(x) = \begin{cases} 0; & x \geq \frac{1}{\kappa} \\ \frac{\lambda_{E,n}}{(1-\kappa x)^2}\exp\left(-\frac{\lambda_{E,n}x}{1-\kappa x}\right); & x < \frac{1}{\kappa}. \end{cases} \quad (6)$$

3.1. Ngẫu nhiên và chuyển tiếp (RF)

Với kỹ thuật ngẫu nhiên và chuyển tiếp, dung lượng bảo mật được biểu diễn bởi [25]:

$$C_n = \left[\log_2\left(\frac{1+\Psi_{M,n}}{1+\Psi_{E,n}}\right)\right]^+. \quad (7)$$

Khi các nút chuyển tiếp sử dụng từ mã khác nhau ở các chặng, dung lượng bảo mật từ đầu cuối đến đầu cuối của giao thức RF được tính như sau:

$$C_{RF}^{Sec} = \min_{n=0,1,..,K-1} C_n. \quad (8)$$

Chúng ta xét xác suất dừng bảo mật tại chặng thứ $n+1$. Xác suất dừng bảo mật được định nghĩa là xác suất dung lượng bảo mật ở chặng này C_n nhỏ hơn một giá trị dương R_{th}, là tốc độ bảo mật mạng mong muốn. Từ (7), ta có thể viết:

$$P_{RF}^{out,n} = \Pr\left(C_n < R_{th}\right) = \int_0^{+\infty} f_{\Psi_{E,n}}(x) F_{M,n}(\rho-1+\rho x)dx, \quad (9)$$

với $\rho = 2^{R_{th}}$.

Từ công thức (9), ta xét hai trường hợp như sau:

Trường hợp 1: $1+\frac{1}{\kappa} \leq \rho$.

Trong trường hợp này, sử dụng các phương trình (2), (4), (5) và (6), ta có thể tính $P_{RF}^{out,n}$ như sau:

$$P_{RF}^{out,n} = \int_0^{1/\kappa} \frac{\lambda_{E,n}}{(1-\kappa x)^2}\exp\left(-\frac{\lambda_{E,n}x}{1-\kappa x}\right)dx = 1. \quad (10)$$

Trường hợp 2: $1+\frac{1}{\kappa} > \rho$.

$$P_{RF}^{out,n} = \int_0^{\frac{1+1/\kappa-\rho}{\rho}} f_{\Psi_{E,n}}(x) F_{M,n}(\rho-1+\rho x)dx \int_{\frac{1+1/\kappa-\rho}{\rho}}^{1/\kappa} f_{\Psi_{E,n}}(x)dx. \quad (11)$$

Một lần nữa, ta thay các kết quả đạt được trong các phương trình (2) và (6) ta có công thức (12).

$$\begin{aligned} P_{RF}^{out,n} &= \int_0^{\frac{1+1/\kappa-\rho}{\rho}} \frac{\lambda_{E,n}}{(1-\kappa x)^2}\exp\left(\frac{-\lambda_{E,n}x}{1-\kappa x}\right)\left(1-\exp\left(-\lambda_{M,n}\frac{\rho-1+\rho x}{1-\kappa(\rho-1+\rho x)}\right)\right)dx + \int_{\frac{1+1/\kappa-\rho}{\rho}}^{1/\kappa} \frac{\lambda_{E,n}}{(1-\kappa x)^2}\exp\left(\frac{-\lambda_{E,n}x}{1-\kappa x}\right)dx \\ &= \left[\int_0^{\frac{1+1/\kappa-\rho}{\rho}} \frac{\lambda_{E,n}}{(1-\kappa x)^2}\exp\left(\frac{-\lambda_{E,n}x}{1-\kappa x}\right)dx + \int_{\frac{1+1/\kappa-\rho}{\rho}}^{1/\kappa} \frac{\lambda_{E,n}}{(1-\kappa x)^2}\exp\left(\frac{-\lambda_{E,n}x}{1-\kappa x}\right)dx\right] \\ &\quad - \int_0^{\frac{1+1/\kappa-\rho}{\rho}} \frac{\lambda_{E,n}}{(1-\kappa x)^2}\exp\left(\frac{-\lambda_{E,n}x}{1-\kappa x}\right)\exp\left(\frac{-\lambda_{M,n}(\rho-1+\rho x)}{1-\kappa(\rho-1+\rho x)}\right)dx \\ &= \int_0^{1/\kappa} \frac{\lambda_{E,n}}{(1-\kappa x)^2}\exp\left(\frac{-\lambda_{E,n}x}{1-\kappa x}\right)dx - \int_0^{\frac{1+1/\kappa-\rho}{\rho}} \frac{\lambda_{E,n}}{(1-\kappa x)^2}\exp\left(\frac{-\lambda_{E,n}x}{1-\kappa x}\right)\exp\left(\frac{-\lambda_{M,n}(\rho-1+\rho x)}{1-\kappa(\rho-1+\rho x)}\right)dx. \end{aligned} \quad (12)$$

Mặt khác, tích phân trong (12) không thể được đưa ra dưới dạng tường minh nên sử dụng các phần mềm toán học như Mathematica hay Matlab để tính. Và cuối cùng, P_{RF}^{out} của toàn chặng được tính như sau:

$$P_{RF}^{out} = 1 - \prod_{n=0}^{K-1}\left(1-P_{RF}^{out,n}\right). \quad (12)$$

Chúng ta cũng xem xét đến xác suất dung lượng bảo mật khác không - $P_{RF}^{non-zero}$, như vậy, từ (8) chúng ta có:

$$\begin{aligned} P_{RF}^{non-zero} &= \Pr\left(C_{RF}^{Sec} > 0\right) \\ &= \Pr\left(\min_{n=0,1,..,K-1} C_n > 0\right) \\ &= \prod_{n=0}^{K-1} \Pr\left(C_n > 0\right). \end{aligned} \quad (13)$$

Từ (7), chúng ta có:

$$\begin{aligned}\Pr(C_n>0)&=\Pr\left(\frac{1+\Psi_{M,n}}{1+\Psi_{E,n}}>1\right)\\&=\Pr(\Psi_{M,n}>\Psi_{E,n})\\&=\int_0^{+\infty} f_{\Psi_{M,n}}(y)F_{\Psi_{E,n}}(y)dy.\end{aligned}\tag{14}$$

Từ (4) và (5), chúng ta có:

$$\begin{aligned}\Pr(C_n>0)&=\int_0^{\frac{1}{\kappa}}\frac{\lambda_{M,n}}{(1-\kappa y)^2}\exp\left(-\frac{\lambda_{M,n}y}{1-\kappa y}\right)\left[1-\exp\left(-\frac{\lambda_{E,n}y}{1-\kappa y}\right)\right]dy\\&=1-\int_0^{\frac{1}{\kappa}}\frac{\lambda_{M,n}}{(1-\kappa y)^2}\exp\left(-\frac{(\lambda_{M,n}+\lambda_{E,n})y}{1-\kappa y}\right)dy.\end{aligned}\tag{15}$$

Để tính toán tích phân trong (15), sử dụng phương pháp đổi biến, cụ thể đặt $u=1-\kappa y$, ta có:

$$\begin{aligned}I&=\int_0^1\frac{\lambda_{M,n}}{u^2}\exp\left(-\frac{(\lambda_{M,n}+\lambda_{E,n})}{u}\frac{1-u}{\kappa}\right)\frac{du}{\kappa}\\&=\frac{\lambda_{M,n}}{\kappa}\exp\left(\frac{\lambda_{M,n}+\lambda_{E,n}}{\kappa}\right)\\&\quad\times\int_0^1\frac{1}{u^2}\exp\left(-\frac{\lambda_{M,n}+\lambda_{E,n}}{\kappa u}\right)du.\end{aligned}\tag{16}$$

Đặt $t=\frac{1}{u}$, ta có:

$$\begin{aligned}I&=\frac{\lambda_{M,n}}{\kappa}\exp\left(\frac{\lambda_{M,n}+\lambda_{E,n}}{\kappa}\right)\int_1^{+\infty}\exp\left(-\frac{\lambda_{M,n}+\lambda_{E,n}}{\kappa}t\right)dt\\&=\frac{\lambda_{M,n}}{\lambda_{M,n}+\lambda_{E,n}}.\end{aligned}\tag{17}$$

3.2. Giải mã và chuyển tiếp (DF)

Ở phương pháp này, dung lượng bảo mật từ đầu cuối đến đầu cuối của đường truyền dữ liệu được biểu diễn như sau:

$$C_{data}=\log_2\left(1+\min_{n=0,1,...,K-1}\Psi_{M,n}\right).\tag{18}$$

Dung lượng bảo mật từ đầu cuối đến đầu cuối của đường truyền nghe trộm ở phương pháp này sẽ là:

$$C_{eavesdropping}=\log_2\left(1+\sum_{n=0}^{K-1}\Psi_{E,n}\right).\tag{19}$$

Như vậy, dung lượng bảo mật của hệ thống được biểu diễn bởi biểu thức:

$$C_{DF}^{Sec}=\max\left(0,C_{data}-C_{eavesdropping}\right).\tag{20}$$

Đầu tiên ta xác định hàm phân bố xác suất của $X=\min_{n=0,1,...,K-1}(\Psi_{M,n})$ như sau:

$$\begin{aligned}F_X(x)&=\Pr\left(\min_{n=0,1,...,K-1}(\Psi_{M,n})<x\right)\\&=\begin{cases}1; & x\ge\frac{1}{\kappa}\\ 1-\exp\left(-\sum_{n=0}^{K-1}\frac{\lambda_{M,n}x}{1-\kappa x}\right); & x<\frac{1}{\kappa}.\end{cases}\end{aligned}\tag{21}$$

Vì vậy, xác suất dừng bảo mật trong mô hình DF được tính như sau:

$$\begin{aligned}P_{DF}^{out}&=\Pr\left(C_{DF}^{Sec}<R_{th}\right)\\&=\Pr\left(X<\rho-1+\rho\sum_{n=0}^{K-1}\Psi_{E,n}\right).\end{aligned}\tag{22}$$

Từ (22), ta có thể viết lại P_{DF}^{out} như sau:

$$P_{DF}^{out}=\int_0^{+\infty}F_X(\rho-1+\rho t)f_T(t)dt,\tag{23}$$

trong đó $f_T(t)$ là hàm mật độ xác suất của biến ngẫu nhiên T với $T=\sum_{n=0}^{K-1}\Psi_{E,n}$.

Bây giờ, chúng ta xét đến dung lượng bảo mật khác không của giao thức DF được thể hiện ở biểu thức sau:

$$\begin{aligned}P_{DF}^{non-zero}&=\Pr\left(C_{DF}^{Sec}>0\right)\\&=\Pr\left(\min_{n=0,1,...,K-1}(\Psi_{M,n})>\sum_{n=0}^{K-1}\Psi_{E,n}\right).\end{aligned}\tag{24}$$

Tương tự, chúng ta có được:

$$P_{DF}^{non-zero}=\int_0^{+\infty}\exp\left(-\left(\sum_{n=0}^{K-1}\lambda_{M,n}\right)t\right)f_T(t)dt.\tag{25}$$

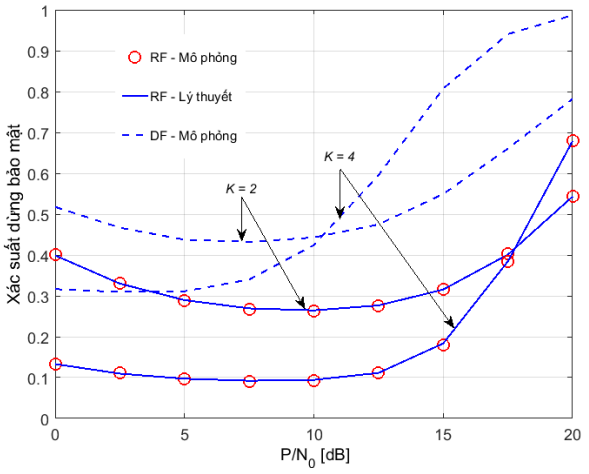
Bởi vì việc tính hàm mật độ xác suất $f_T(t)$ là phức tạp nên nhóm tác giả cũng sẽ không trình bày cách tính P_{DF}^{out}, $P_{DF}^{non-zero}$ trong bài báo này. Nhóm tác giả sử dụng phương pháp mô phỏng để so sánh P_{DF}^{out} với P_{RF}^{out} và $P_{DF}^{non-zero}$ với $P_{RF}^{non-zero}$.

4. Kết quả mô phỏng

Trong phần này, thực hiện mô phỏng Monte-Carlo để so sánh hiệu năng bảo mật của các mô hình đã được xét ở trên, cũng như so sánh giữa mô phỏng và các tính toán lý thuyết. Trong mặt phẳng hai chiều *Oxy*, nhóm tác giả giả sử các nút $T_n(n=0,1,2,...,K)$ có tọa độ là $(n/K;0)$ và nút E có tọa độ là $(0;1)$. Như vậy, khoảng cách giữa hai nút gần nhau T_n và T_{n+1} là $d_{M,n}=1/K$ và khoảng cách giữa T_n và E là $d_{E,n}=\sqrt{(n/K)^2+1}$. Giả sử hệ số suy hao đường truyền $\eta=3$, các tham số $\lambda_{M,n}$ và $\lambda_{E,n}$ lần lượt được biểu diễn theo khoảng cách như sau: $\lambda_{M,n}=d_{M,n}^3$ và $\lambda_{E,n}=d_{E,n}^3$. Nhóm tác giả cũng giả sử rằng công suất truyền của các nút phát T_n là bằng nhau và bằng P.

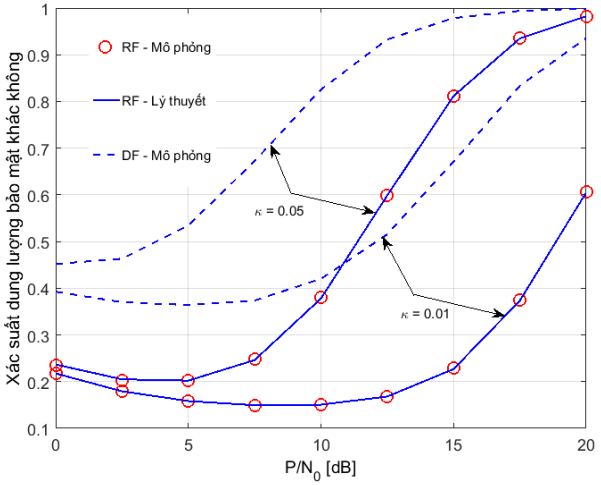
Trong Hình 2, biểu diễn xác suất dừng bảo mật theo giá trị của P/N_0 khi các thông số khác được cố định như $\kappa=0.01$ và $R_{th}=1$. Ta có thể thấy từ Hình 2 rằng mô hình RF đạt xác suất dừng thấp hơn mô hình DF với mọi giá trị của số chặng và P/N_0. Hơn thế nữa, xác suất dừng bảo mật có xu hướng tăng khi ta tăng giá trị của P/N_0. Chúng ta cũng thấy rằng khi thay đổi giá trị của số chặng từ 2 lên 4, xác suất dừng bảo mật cũng thay đổi. Tuy nhiên, tùy thuộc vào giá trị của P/N_0 mà xác suất dừng bảo mật của mô hình RF hay DF tăng hoặc giảm. Đặc biệt, tại mỗi đường cong chúng ta thấy tồn tại một giá trị xác suất dừng bảo mật nhỏ nhất, hiệu năng bảo mật của hệ thống lúc này là tốt nhất. Kết quả mô phỏng này có thể đưa vào ứng dụng

thực tế khi đặt công suất phát cho nút nguồn và nút chuyển tiếp cho hệ thống truyền thông vô tuyến đa chặng đa chặng. Ở Hình 2, tại đường cong mô phỏng RF, chúng ta thấy rằng khi $K = 4$ thì công suất phát của nút nguồn và nút chuyển tiếp ở mức 7.5 [dB] và khi $K = 2$ thì công suất phát của nút nguồn và nút chuyển tiếp ở mức 10[dB] thì hiệu năng bảo mật của hệ thống tối ưu nhất.



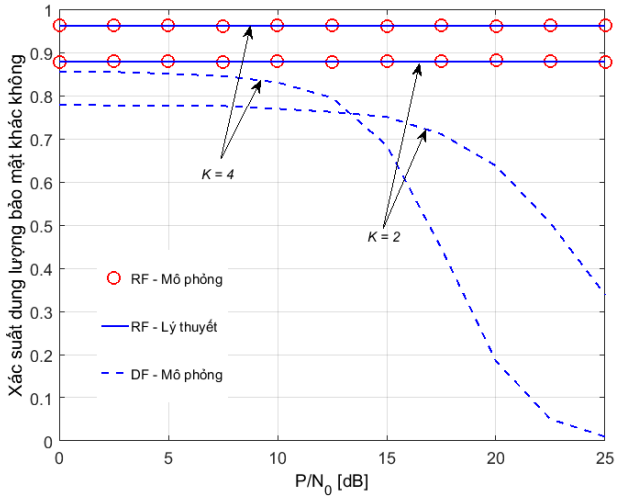
Hình 2. *Xác suất dừng bảo mật biểu diễn theo giá trị* P / N_0 *khi* $\kappa = 0.01$, $R_{th} = 1$, $K = 2$ *và* $K = 4$.

Trong Hình 3, cũng biểu diễn xác suất dừng bảo mật theo giá trị của P / N_0 và cố định $K = 3$ và $R_{th} = 1$. Tương tự như trong Hình 2, hiệu năng của các mô hình giảm khi giá trị P / N_0 lớn. Tuy nhiên, mô hình RF vẫn đạt hiệu năng tốt hơn mô hình DF. Ta cũng thấy được từ Hình 3 rằng, khi giá trị mức suy hao phần cứng tăng, hiệu năng của cả hai mô hình RF và DF suy giảm đáng kể. Tại các đường cong mô phỏng tồn tại giá trị mà hiệu năng bảo mật của hệ thống tối ưu nhất. Ví dụ, ở mô hình RF, khi $\kappa = 0.01$, hiệu năng bảo mật tốt nhất khi $P / N_0 = 8.75$ [dB] và khi $\kappa = 0.05$ thì hiệu năng bảo mật tốt nhất khi $P / N_0 = 10$ [dB]. Với kết quả mô phỏng này, chúng ta cần xem xét giá trị P / N_0 khi triển khai hệ thống truyền thông vô tuyến đa chặng với mỗi mức độ không lý tưởng của phần cứng hệ thống.



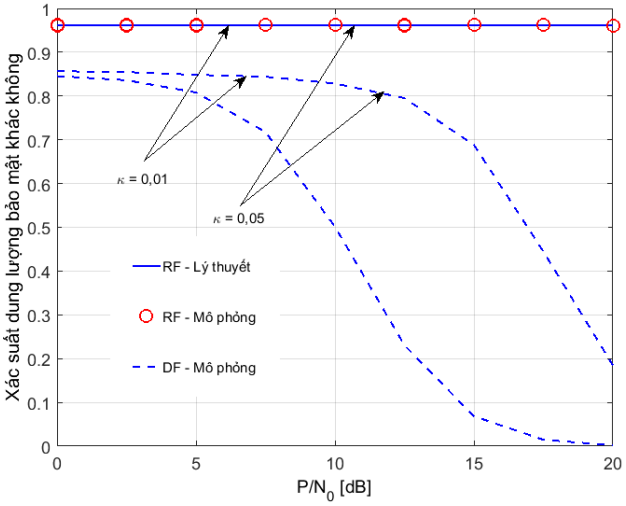
Hình 3. *Xác suất dừng bảo mật biểu diễn theo giá trị* P / N_0 *khi* $\kappa = 0.01$, $\kappa = 0.05$, $R_{th} = 1$ *và* $K = 3$

Trong Hình 4, thực hiện mô phỏng dung lượng bảo mật khác không của cả hai mô hình DF và RF theo giá trị P / N_0, $\kappa = 0.01$, thay đổi số chặng của mô hình chuyển tiếp với $K = 2$ và $K = 4$. Dung lượng bảo mật khác không của mô hình chuyển tiếp RF không thay đổi khi P / N_0 và K thay đổi, giá trị dung lượng bảo mật khác không của mô hình chuyển tiếp DF giảm khi P / N_0 tăng.



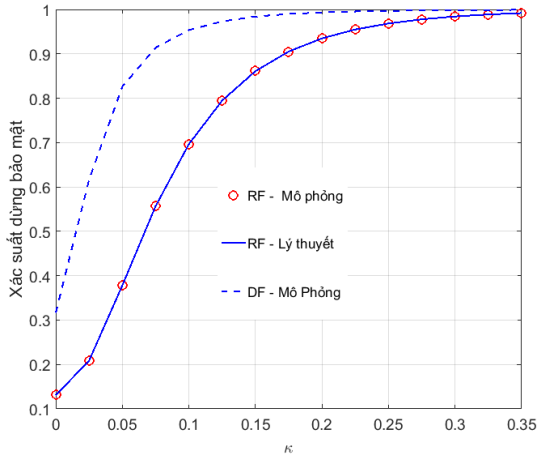
Hình 4. *Dung lượng bảo mật khác không biểu diễn theo giá trị* P / N_0, $\kappa = 0.01$, *khi* $K = 2$ *và* $K = 4$.

Trong Hình 5, biểu diễn xác suất dừng bảo mật theo giá trị của P / N_0, cố định $K = 4$ và $R_{th} = 1$, thay đổi hệ số phần cứng không lý tưởng $\kappa = 0.01$, và $\kappa = 0.05$. Dung lượng bảo mật khác không của mô hình DF giảm khi hệ số suy giảm κ tăng, dung lượng bảo mật khác không của mô hình RF không phụ thuộc vào κ và P / N_0.



Hình 5. *Dung lượng bảo mật khác không biểu diễn theo giá trị* P / N_0, $K = 4$ *khi* $\kappa = 0.01$ *và* $\kappa = 0.05$

Trong Hình 6, đánh giá xác suất dừng bảo mật của hệ thống theo giá trị của κ, cố định $K = 3$ và $R_{th} = 1$. Xác suất dừng bảo mật của hệ thống tăng khi κ tăng, kết quả mô phỏng cho thấy hiệu năng bảo mật của hệ thống vô tuyến truyền thông đa chặng chịu ảnh hưởng lớn từ sự thay đổi của suy hao phần cứng.



Hình 6. *Xác suất dừng bảo mật biểu diễn theo giá trị* κ, $K = 3$ *khi* $R_{th} = 1$.

5. Kết luận

Trong bài báo này, nhóm tác giả khảo sát hiệu năng bảo mật của các mô hình chuyển tiếp đa chặng dưới tác động của suy hao phần cứng. Cụ thể, đã đưa ra các biểu thức tính xác suất dừng bảo mật và xác suất dung lượng bảo mật khác không của các mô hình khảo sát trên kênh truyền fading Rayleigh. Các kết quả tính toán được kiểm chứng bằng những mô phỏng máy tính. Các kết quả đã thể hiện rằng độ suy hao phần cứng ảnh hưởng đáng kể lên hiệu năng bảo mật của hệ thống.

Lời cảm ơn: Nghiên cứu này được tài trợ bởi Quỹ Phát triển Khoa học và Công nghệ Quốc gia (NAFOSTED) trong đề tài mã số 102.02-2018.320.

TÀI LIỆU THAM KHẢO

[1] J. N. Laneman, D.N.C. Tse, G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior", *IEEE Trans. Inf. Theory*, vol. 50, pp. 3062-3080, 2004.

[2] T. T. Duy, H. Y. Kong, "Exact outage probability of cognitive two-way relaying scheme with opportunistic relay selection under interference constraint", *IET Commun.*, p. 2750–2759, 2012.

[3] V. N. Q. Bao, T. Q. Duong, "Outage analysis of cognitive multihop networks under interference constraints", *IEICE Trans. Commun.*, p. 1019–1022, 2012.

[4] T. T. Duy, V. N. Q. Bao, "Outage performance of cooperative multihop transmission in cognitive underlay networks", *Proc. ComManTel 2013*, pp. 123-127, 2013.

[5] Yang Yang, Honglin Hu, Jing Xu, Guoqiang Mao, "Relay technologies for WiMax and LTE-advanced mobile systems", *IEEE Communications Magazine*, pp. 100-105, 2009.

[6] Louie, H. Y. Raymond, Y. Li, B. Vucetic, "Practical physical layer network coding for two-way relay channels: performance analysis and comparison", *IEEE Trans. Wirel. Commun.*, pp. 764-777, 2010.

[7] Nan Yang, P.L. Yeoh, M. Elkashlan, I.B. Collings, Z. Chen, "Two-Way Relaying With Multi-Antenna Sources: Beamforming and Antenna Selection", *IEEE Trans. Veh. Technol.*, pp. 3996-4008, 2012.

[8] C. Shannon, "Communication theory of secrecy systems", *Bell System Technical Journal*, p. 656–715, 1949.

[9] Gopala, Praveen Kumar, Lifeng Lai, H. El Gamal, "On the Secrecy Capacity of Fading Channels", *IEEE Trans. Inf. Theory*, pp. 4687-4698, 2008.

[10] I. Krikidis, J.S. Thompson, S. Mclaughlin, "Relay selection for secure cooperative networks with jamming", *IEEE Trans. Wirel. Commun.*, pp. 5003-5011, 2009.

[11] D. H. Ibrahim, E. S. Hassan, S. A. El-Dolil, "A new relay and jammer selection schemes for secure one-way cooperative networks", *Wirel. Pers. Commun.*, pp. 1-21, 2013.

[12] J. Chen, R. Zhang, L. Song, Z. Han, B. Jiao, "Joint relay and jammer selection for secure decode-and-forward two-way relay communications", *IEEE Trans. Info. For. Sec.*, pp. 310-320, 2012.

[13] H.A. Suraweera, H.K. Garg, A. Nallanathan , "Performance Analysis of Two Hop Amplify-and-Forward Systems with Interference at the Relay", *IEEE Commun. Lett.*, pp. 692-694, 2010.

[14] T. T. Duy, V. N. Q. Bao and T.Q. Duong, "Secured communication in cognitive {MIMO} schemes under hardware impairments", *International Conference on Advanced Technologies for Communications (ATC)*, pp. 109-112, 2014.

[15] N. H. Nhat, V. N. Q. Bao, N. L. Trung, M. Debbah, "Relay selection in two-way relaying networks with the presence of hardware impairment at relay transceiver", *2014 International Conference on Advanced Technologies for Communications (ATC)*, pp. 616-620, 2014.

[16] K. Guo, J. Chen, Y. Huang, G. Li, N. Liu, "Outage and capacity analysis between opportunistic and partial relay cooperative network with hardware impairments", in *2014 International Workshop on High Mobility Wireless Communications (HMWC)*, 2014, pp. 78-83.

[17] G. Kefeng, J. Chen, G. Li, X. Wang, "Outage analysis of cooperative cellular network with hardware impairments", in *2014 International Conference on Information Science, Electronics and Electrical Engineering (ISEEE)*, 2014, pp. 1416-1420.

[18] T. T. Duy, T. Q. Duong, D.B. da Costa, V. N. Q. Bao, M. Elkashlan, "Proactive Relay Selection with Joint Impact of Hardware Impairment and Co-channel Interference", *IEEE Trans. Comm.*, pp. 1-1, 2015.

[19] 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*, 2012.

[20] J. K. J. L. a. J. P. C. J. Kim, "Physical-Layer Security Against Smart Eavesdroppers: Exploiting Full-Duplex Receivers", *IEEE Access*, vol. 6, pp. 32945-32957, 2018.

[21] W. S. J. N. S. A. J. C. K. J. Furqan, "On the Secrecy Performance of SWIPT Receiver Architectures with Multiple Eavesdroppers", *Wireless Commun. and Mobile Comput.*, vol. 2018, pp. 1-12, 2018.

[22] J. S. S. a. J. P. Vilela, "Uncoordinated Frequency Hopping for Wireless Secrecy Against Non-Degraded Eavesdroppers", *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 143-155, 2018.

[23] T. T. D. a. B. K. T. D. Hieu, "Performance Enhancement for Multihop Harvest-to-Transmit WSNs With Path-Selection Methods in Presence of Eavesdroppers and Hardware Noises", *IEEE Sensors Journal*, vol. 18, pp. 5173-5186, 2018.

[24] K. Guo, J. Chen, G. Li, X. Wang, "Outage analysis of cooperative cellular network with hardware impairments", in *2014 International Conference on Information Science, Electronics and Electrical Engineering (ISEEE)*, 2014, pp. 1416-1420.

[25] J. Barros, M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels", *2006 IEEE International Symposium on Inf. Theory*, pp. 356-360, 2006.

(BBT nhận bài: 28/9/2018, hoàn tất thủ tục phản biện: 18/10/2018)