Transport and Communications Science Journal

SECRECY PERFORMANCE ANALYSIS FOR COOPERATIVE NETWORK APPLYING NOMA

Pham Hong Quan[1], Nguyen Yen Chi[1]

[1]*University of Transport and Communications, No 3 Cau Giay Street, Hanoi, Vietnam.*

ARTICLE INFO

TYPE: Research Article
Received: 17/08/2019
Revised: 17/09/2019
Accepted: 24/09/2019
Published online: 16/12/2019
https://doi.org/10.25073/tcsj.70.4.13
[*]*Corresponding author*
Email: phamhongquan@utc.edu.vn

Abstract. Non-orthogonal Multiple Access (NOMA) has emerged as a key technique in 5G wireless communication networks. This paper studies physical layer security of a NOMA relaying system with a full-duplex relay. This system suffers from the attack of both an eavesdropper and a jammer. The secrecy outage probability is derived in this paper to characterize the performance system of the considered system. The simulation demonstrates that the secrecy outage probability (SOP) of the system increase when increasing the transmit power of the source, the relay and the jammer. The paper also demonstrates the effect of power allocation and channel gains on the secrecy performance of the system.

Keywords: physical layer security, secrecy outage probability, NOMA, full-duplex relaying, 5G wireless networks.

Tạp chí Khoa học Giao thông vận tải

PHÂN TÍCH CHẤT LƯỢNG BẢO MẬT CHO MẠNG VÔ TUYẾN HỢP TÁC ÁP DỤNG ĐA TRUY NHẬP PHI TRỰC GIAO

Phạm Hồng Quân[1], Nguyễn Yến Chi[1]

[1]*Trường Đại học Giao thông vận tải, Số 3 Cầu Giấy, Hà Nội.*

THÔNG TIN BÀI BÁO

Chuyên mục: Công trình khoa học
Ngày nhận bài: 17/08/2019
Ngày nhận bài sửa: 17/09/2019
Ngày chấp nhận đăng: 24/09/2019
Ngày xuất bản Online: 16/12/2019
https://doi.org/10.25073/tcsj.70.4.13
[*]*Tác giả liên hệ*
Email: phamhongquan@utc.edu.vn

Tóm tắt. Đa truy nhập phi trực giao đang nổi lên như một kỹ thuật chính trong các mạng vô tuyến 5G. Bài báo này nghiên cứu bảo mật lớp vật lý cho hệ thống chuyển tiếp sử dụng kỹ thuật đa truy nhập phi trực giao với một chuyển tiếp song công. Hệ thống này chịu sự tấn công từ một thiết bị nghe lén và một thiết bị gây nhiễu. Cụ thể, xác suất rớt bảo mật được đưa ra trong bài báo này để đánh giá chất lượng bảo mật của hệ thống được xem xét. Kết quả mô phỏng chỉ ra rằng xác suất rớt bảo mật của hệ thống tăng nếu tăng các giá trị công suất phát của nguồn, của chuyển tiếp và của thiết bị nghe lén. Bài báo cũng chỉ ra sự ảnh hưởng của hệ số phân bổ công suất và các độ lợi kênh truyền đến chất lượng bảo mật của hệ thống.

Từ khóa: Bảo mật lớp vật lý, xác suất rớt bảo mật, đa truy nhập phi trực giao, chuyển tiếp song công, hệ thống thông tin di động 5G.

1. ĐẶT VẤN ĐỀ

Kỹ thuật đa truy nhập phi trực giao là một công nghệ đầy hứa hẹn nhằm tăng cường thông lượng hệ thống và tạo độ tin cậy cao cho mạng vô tuyến di động 5G [1]. Kỹ thuật đa truy nhập này khai thác việc ghép kênh miền công suất tại các trạm phát và kỹ thuật giải mã tuần tự tại các máy thu phục vụ nhiều người sử dụng cùng một thời gian, tần số và mã. Tuy nhiên, về bản chất, việc truyền sóng của hệ thống thông tin di động 5G lại làm giảm khả năng bảo mật của hệ thống vì nó cho phép nghe những tín hiệu của các thiết bị hợp pháp qua các kênh truyền không hợp pháp. Để giải quyết vấn đề bảo mật cho mạng 5G, bảo mật lớp vật lý

ra đời như là một giải pháp vì nó bảo vệ dữ liệu hợp pháp ngay ở mức truyền dẫn. So với các kỹ thuật bảo mật bằng mật mã hóa truyền thống, bảo mật lớp vật lý làm giảm đáng kể các quá trình tính toán và có khả năng ứng dụng cho các mạng cỡ lớn. Vì thế, bảo mật lớp vật lý phù hợp cho các mạng 5G [2].

Hầu hết các nghiên cứu về bảo mật lớp vật lý trong các mạng 5G sử dụng công nghệ truy nhập phi trực giao (non-orthogonal multiple access – NOMA) tập trung vào đánh giá sự tấn công của thiết bị nghe lén, một trong những hình thức tấn công nguy hiểm nhất của mạng vô tuyến. Nhiều nghiên cứu khác tập trung phân tích chất lượng bảo mật của các hệ thống sử dụng kỹ thuật đa truy nhập phi trực giao với sự có mặt của thiết bị nghe lén thụ động, luôn luôn giữ im lặng và lắng nghe kênh truyền giữa các thiết bị hợp pháp của hệ thống. Trong [3], một giải pháp phân bổ công suất tối ưu được sử dụng để tối đa hóa tổng tốc độ bảo mật của hệ thống sử dụng kỹ thuật đa truy nhập phi trực giao với cả hai trường hợp một ăng ten phát một ăng ten thu và nhiều ăng ten phát nhiều ăng ten thu.

Tuy nhiên, không có nhiều nghiên cứu về bảo mật lớp vật lý cho mạng sử dụng truy nhập phi trực giao tập trung vào những thiết bị nghe lén chủ động. Những thiết bị nghe lén chủ động là những thiết bị điều khiển môi trường để nâng cao khả năng nghe lén thông qua việc gián tiếp làm tăng công suất phát hoặc điều chỉnh các dữ liệu. Ở [4], một cơ chế phân bổ công suất được đề xuất để đối mặt với một thiết bị nghe lén chủ động có thể hoặc là nghe lén hoặc là tạo ra các tín hiệu nhiễu. Hai mô hình của thiết bị nghe lén chủ động cũng được đề cập trong [5] sử dụng lý thuyết trò chơi. Trong [6], một cơ chế nghe lén hợp pháp được đề xuất để điều khiển các kênh truyền đáng nghi ngờ mà ở đó các thiết bị hợp pháp phát nhiễu để nâng cao chất lượng của thiết bị nghe lén. Ở [7], một thiết bị nghe lén chủ động có thể lựa chọn chuyển tiếp tốt nhất để nâng cao tốc độ tin tức của nó. Một cơ chế lựa chọn chuyển tiếp được đã được đề xuất để chống lại sự tăng tốc độ truyền tin của thiết bị nghe lén. Ở [8], một thiết bị nghe lén chủ động hợp tác với một thiết bị phát nhiễu để nâng cao chất lượng đường truyền của thiết bị nghe lén. Cũng trong nghiên cứu này, một cơ chế chống tấn công được đề xuất để chống lại sự phối hợp này. Tuy nhiên, các nghiên cứu trên mặc dù được sử dụng cho các mạng chuyển tiếp nhưng các mạng này chưa sử dụng kỹ thuật đa truy nhập phi trực giao. Ở [9], một cơ chế chống tấn công được đề xuất cho một hệ thống đa truy nhập phi trực giao. Bài báo này đưa ra mô hình toán học của tốc độ bảo mật ở trong miền tỷ số tín hiệu trên nhiễu cao. Tuy nhiên, trong bài báo này, hệ thống đa truy nhập phi trực giao mới chỉ dừng lại ở mô hình có hai thiết bị nhận trực tiếp tín hiệu từ nguồn, ở đó một trong hai thiết bị đóng vai trò như là một chuyển tiếp. Ở [10] phân tích chất lượng bảo mật của hệ thống đa truy nhập phi trực giao với chuyển tiếp đơn công và chuyển tiếp song công. Tuy nhiên, mô hình trong nghiên cứu này chỉ có tác động của thiết bị nghe lén và chưa xét đến tác động của thiết bị phát nhiễu riêng biệt.

Từ những nghiên cứu trên, bài báo này tập trung phân tích chất lượng bảo mật cho một hệ thống sử dụng kỹ thuật đa truy nhập phi trực giao với một chuyển tiếp riêng biệt dưới sự tấn công của cả thiết bị nghe lén và thiết bị phát tín hiệu nhiễu. Cụ thể, hệ thống vô tuyến hợp

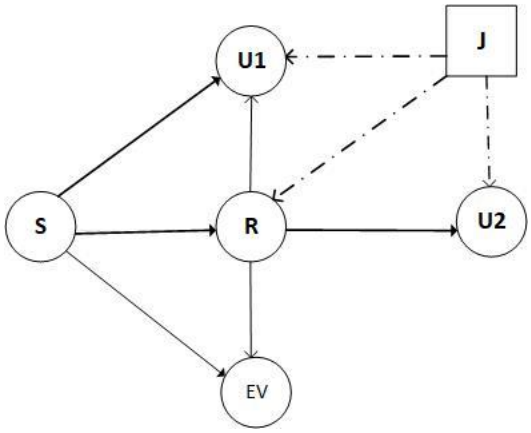
tác bao gồm một trạm phát truyền tin với hai người sử dụng qua một chuyển tiếp song công. Trong khi đó, cả thiết bị nghe lén và thiết bị phát nhiễu đều cố gắng kết hợp lấy thông tin từ các kênh truyền hợp pháp. Đầu tiên, kẻ gây nhiễu sẽ tạo tín hiệu nhiễu để tấn công chuyển tiếp và hai thiết bị nhận bằng cách tăng công suất của nhiễu. Để duy trì chất lượng của hệ thống, cả nguồn tín hiệu và chuyển tiếp sẽ phải tăng công suất phát. Nhờ việc tăng công suất phát của nguồn và chuyển tiếp, thiết bị nghe lén có thể nâng cao khả năng nghe được các tín hiệu hữu ích. Bài báo phân tích chất lượng bảo mật của hệ thống dưới sự hợp tác tấn công của cả hai thiết bị bất hợp pháp này. Từ đó, đưa ra các miền giá trị hợp lý cho các tham số để đảm bảo chất lượng bảo mật của hệ thống.

2. MÔ HÌNH HỆ THỐNG

Trong hệ thống này, nguồn S ứng dụng kỹ thuật mã hóa xếp chồng trong miền công suất và phát tín hiệu được xếp chồng tới các thiết bị nhận U1, U2 và E. Giả sử rằng U1 là người sử dụng gần nguồn hơn U2. Nguồn S có kết nối trực tiếp với U1 nhưng không có kết nối trực tiếp nào với U2. Do đó, chuyển tiếp R sẽ hỗ trợ S truyền tín hiệu tới U2 nhờ sử dụng kỹ thuật giải mã và chuyển tiếp. Ở bài báo này, chuyển tiếp được giả sử hoạt động ở chế độ song công. Trong chế độ này, chuyển tiếp R sẽ nhận tín hiệu từ nguồn S ở thời gian t và đồng thời ở thời gian t này, chuyển tiếp R cũng phát đi tín hiệu đã giải mã ở khe thời gian (t-1) ngay trước đó. Ở nghiên cứu này, các thiết bị hợp pháp bao gồm U1, U2 và R sử dụng kỹ thuật giải mã tuần tự (SIC) để giải mã các tín hiệu. Với kỹ thuật giải mã tuần tự này, tín hiệu của thiết bị nhận xa hơn sẽ được giải mã trước và tín hiệu của thiết bị ở gần hơn bị coi là nhiễu. Vì chuyển tiếp R hoạt động ở chế độ song công, như vậy R sẽ vừa nhận và vừa truyền tín hiệu ở thời điểm t. Việc truyền nhận cùng một thời điểm sẽ gây ra hiện tượng nhiễu tự phát. Trong bài báo này, chuyển tiếp R được giải sử có khả năng triệt tiêu hoàn toàn nhiễu tự phát. Thiết bị nghe lén E cũng được giả sử sử dụng kỹ thuật giải mã tuần tự để giải mã các tín hiệu nhận. Bằng cách sử dụng kỹ thuật giải mã này, thiết bị nghe lén sẽ giải mã tín hiệu của U2 trước khi giải mã tín hiệu của U1. Tất cả các kênh vô tuyến đều được giả sử là kênh truyền với fading phân bố Rayleigh và nhiễu trắng (AWGN) $n(t)$với $CN_0{\sim}(0, N_0)$. Các hệ số kênh truyền từ $S \to U_1$, $S \to U_2$, $S \to R$, $R \to U_2$, $S \to$ E, $R \to E$, $J \to U_1$, $J \to U_2$ và $J \to R$ tương ứng ký hiệu là $h_{S1}, h_{S2}, h_{SR}, h_{R1}, h_{R2}, h_{SE}, h_{RE}, h_{J1}, h_{J2}$ và h_{JR}. Giả sử rằng các kênh truyền $|h_{m,n}|$ có phân bố độc lập thống kê với các biến ngẫu nhiên có độ lợi kênh truyền trung bình là $\lambda_{m,n}$. Hàm mật độ xác suất và hàm phân bố tích lũy của độ lợi kênh truyền được biểu diễn như sau:

$$f_{|h_{m,n}|^2}(x) = \frac{1}{\lambda_{m,n}} exp\left(-\frac{x}{\lambda_{m,n}}\right) \quad (1)$$

$$F_{|h_{m,n}|^2}(x) = 1 - exp\left(-\frac{x}{\lambda_{m,n}}\right) \quad (2)$$



Hình 1. *Mô hình hệ thống vô tuyến hợp tác sử dụng chuyển tiếp song công (full-duplex) áp dụng kỹ thuật truy nhập phi trực giao NOMA.*

Nguồn tín hiệu S sẽ quảng bá tín hiệu $x(t)$ là tín hiệu xếp chồng của hai tín hiệu $x_1(t)$ và $x_2(t)$ tới U1, R và E ở thời điểm t với công suất phát P_s. Chúng ta giả sử rằng U1 là thiết bị thu gần với nguồn hơn U2, do đó theo nguyên lý của truy nhập phi trực giao, hệ số công suất phân bổ cho tín hiệu của U1 là α_1 sẽ nhỏ hơn hệ số công suất phân bổ cho tín hiệu của U2 là α_2, ở đó $\alpha_1 + \alpha_2 = 1$.

Tín hiệu nhận được tại R là:

$$y_R(t) = \sqrt{P_S\,\alpha_1}\,x_1(t)h_{SR}(t) + \sqrt{P_S\,\alpha_2}\,x_2(t)h_{SR}(t) + \sqrt{P_J}\,h_{JR}(t) + n(t) \quad (3)$$

Vì chuyển tiếp R hoạt động ở chế độ song công và sử dụng kỹ thuật giải mã và chuyển tiếp nên cùng thời điểm t, chuyển tiếp R sẽ giải mã tín hiệu nhận $x(t)$ và đồng thời chuyển tiếp đi tín hiệu $x_2(t-1)$. Do đó tín hiệu nhận tại U1 ở thời điểm t được biểu diễn như sau:

$$y_{u1}(t) = \sqrt{P_S\,\alpha_1}\,x_1(t)h_{S1}(t) + \sqrt{P_S\,\alpha_2}\,x_2(t)h_{S1}(t) + \sqrt{P_R}\,x_2(t-1)h_{R1}(t) + \sqrt{P_J}\,h_{J1}(t) + n(t) \quad (4)$$

Tương tự tín hiệu nhận được tại thời điểm t tại thiết bị nghe lén E là:

$$y_E(t) = \sqrt{P_S\,\alpha_1}\,x_1(t)h_{SE}(t) + \sqrt{P_S\,\alpha_2}\,x_2(t)h_{SE}(t) + \sqrt{P_R}\,x_2(t-1)h_{RE}(t) + \sqrt{P_J}\,h_{J1}(t) + n(t) \quad (5)$$

Theo nguyên lý của giải mã tín hiệu tuần tự tín hiệu $x_2(t)$ sẽ được giải mã trước tín hiệu $x_1(t)$. Tỷ số tín hiệu trên nhiễu để giải mã tín hiệu $x_2(t)$ tại R là:

$$\gamma_{2,R} = \frac{P_S\,\alpha_2\,|h_{SR}|^2}{P_S\,\alpha_1\,|h_{SR}|^2 + P_J|h_{JR}| + N_0} \quad (6)$$

Tỷ số tín hiệu trên nhiễu để giải mã tín hiệu $x_1(t)$ tại R là:

$$\gamma_{1,R} = \frac{P_S\ \alpha_1\ |h_{SR}|^2}{P_J|h_{JR}|+N_0} \quad (7)$$

Giả sử U1 và E đã giải mã thành công các tín hiệu ở khe thời gian (t-1). Do đó tỷ số tín hiệu trên nhiễu để giải mã tín hiệu $x_2(t)$ tại U1 là:

$$\gamma_{2,U1} = \frac{P_S\ \alpha_2\ |h_{S_1}|^2 + P_R\ |h_{R_1}|^2}{P_S\ \alpha_1\ |h_{S_1}|^2 + P_J|h_{J_1}|+N_0} \quad (8)$$

Tỷ số tín hiệu trên nhiễu để giải mã tín hiệu $x_1(t)$ tại U1 là:

$$\gamma_{1,U1} = \frac{P_S\ \alpha_1\ |h_{S_1}|^2}{P_J|h_{J_1}|+N_0} \quad (9)$$

Giả sử thiết bị nghe lén sử dụng kỹ thuật giải mã tuần tự. Tỷ số tín hiệu trên nhiễu để giải mã tín hiệu $x_2(t)$ tại E là:

$$\gamma_{2,E} = \frac{P_S\ \alpha_2\ |h_{S_1}|^2 + P_R\ |h_{RE}|^2}{P_S\ \alpha_1\ |h_{S_1}|^2 + N_0} \quad (10)$$

Tỷ số tín hiệu trên nhiễu để giải mã tín hiệu $x_1(t)$ tại E là:

$$\gamma_{1,E} = \frac{P_S\ \alpha_1\ |h_{S_1}|^2}{N_0} \quad (11)$$

Tín hiệu nhận được tại người nhận thứ hai U2 là:

$$y_{u2}(t-1) = \sqrt{P_r}\ h_{r,2}(t)\ x_2(t-1) + \sqrt{P_J}\ h_{J,2}(t) + n(t) \quad (12)$$

Tỷ số tín hiệu trên nhiễu để giải mã tín hiệu $x_2(t)$ là:

$$\gamma_{2,u2} = \frac{P_r|h_{r,2}|^2}{P_J|h_{J,2}|^2+N_0} \quad (13)$$

3. PHÂN TÍCH XÁC SUẤT RỚT BẢO MẬT CỦA HỆ THỐNG

3.1. Dung lượng bảo mật

Dung lượng bảo mật được định nghĩa như sau:

$$C_S = [C_U - C_E]^+ \quad (14)$$

Ở đó $[x]^+ = max\{x, 0\}$, và C_U và C_E là dung lượng truyền dẫn của kênh truyền chính và kênh truyền bị nghe lén.

Xác suất mất bảo mật của tín hiệu $x_1(t)$ được biểu diễn như sau:

$$C_{1,sec} = B\log_2\{(1+\gamma_{1,U1})/(1+\gamma_{1,E})\} \quad (15)$$

Xác suất mất bảo mật của tín hiệu $x_2(t)$ được biểu diễn như sau:

$$C_{2,sec} = B\log_2\{(1+\gamma_{2,2})/(1+\gamma_{2,E})\} \quad (16)$$

Ở đó:

$$\gamma_{2,2} = min(\gamma_{2,U1}, \gamma_{2,U2}, \gamma_{2,R}) \quad (17)$$

3.2. Xác suất mất bảo mật

Xác suất rớt bảo mật của hệ thống xảy ra khi dung lượng bảo mật của kênh truyền nhỏ hơn tốc độ bảo mật r và được định nghĩa là:

$$O_{sec} = Pr\{C_S < r\} \quad (18)$$

Giả sử tốc độ bảo mật của người nhận thứ nhất và người nhận thứ hai tương ứng là r_1 và r_2. Xác suất rớt bảo mật của U1 được biểu diễn như sau:

$$SOP_1 = Pr\{C_{1,sec} < r_1\} \quad (19)$$

Và xác suất rớt bảo mật của U2 được biểu diễn bởi công thức:

$$SOP_2 = Pr\{C_{2,sec} < r_2\} \quad (20)$$

Xác suất rớt bảo mật của hệ thống được tính như sau:

$$SOP = (1 - SOP_1)(1 - SOP_2) \quad (21)$$

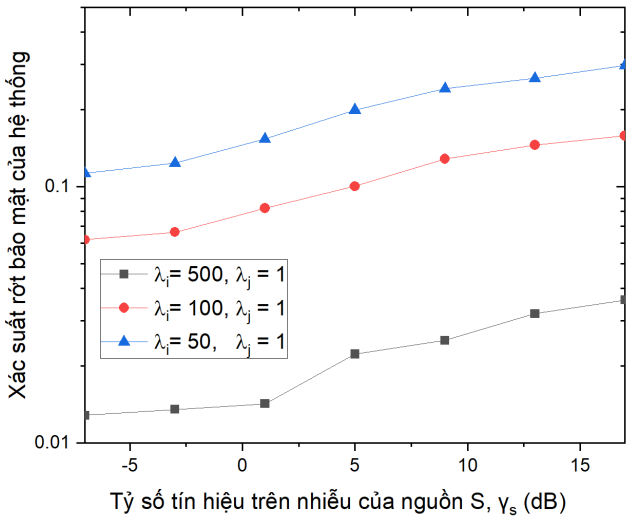
4. KẾT QUẢ MÔ PHỎNG

Trong phần này, bài báo mô phỏng để xác định ảnh hưởng của các tham số lên hệ thống truy nhập phi trực giao sử dụng chuyển tiếp song công R. Cụ thể các tham số của hệ thống được cài đặt như sau:

+ Băng thông của hệ thống: B = 5 MHz

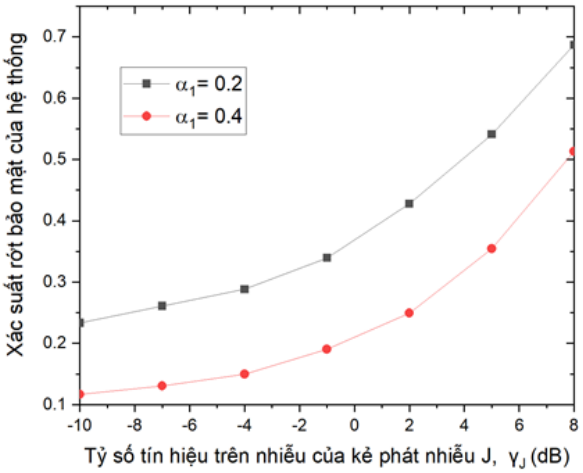
+ Tốc độ bảo mật của hai thiết bị nhận hợp pháp U1 và U2: $R_1 = R_2 = 1kpbs$

+ Giả sử $\gamma_s = \frac{P_s}{N_0}$, $\gamma_J = \frac{P_J}{N_0}$ và $\gamma_R = \frac{P_R}{N_0}$ tương ứng là các giá trị tỷ số tín hiệu trên nhiễu của các nguồn, thiết bị gây nhiễu và chuyển tiếp R.



Hình 2. *Xác suất rớt bảo mật của hệ thống theo tỷ số tín hiệu trên nhiễu của nguồn với hệ số phân bổ công suất* $\alpha_1 = 0.4$.

Bài báo khảo sát xác suất bảo mật của hệ thống theo tỷ số tín hiệu trên nhiễu của nguồn với hệ số phân bổ công suất cho U1 là 0.4 và với các độ lợi kênh truyền khác nhau như ở hình 2. Các độ lợi kênh truyền của các kênh truyền có ích được ký hiệu là λ_i và độ lợi kênh truyền của các kênh truyền bất hợp pháp được ký hiệu là λ_j. Xác suất rớt bảo mật được khảo sát khi tăng độ lợi của kênh truyền hợp pháp lên so với kênh truyền bất hợp pháp. Kết quả mô phỏng cho thấy khi tăng độ lợi kênh truyền của các kênh truyền hợp pháp thì xác suất rớt bảo mật của hệ thống được giảm đáng kể, với giả sử là độ lợi kênh truyền của các kênh truyền bất hợp pháp không thay đổi. Khi độ lợi kênh truyền hợp pháp gấp 500 lần độ lợi kênh truyền bất hợp pháp thì xác suất rớt bảo mật của hệ thống nhỏ hơn 0.1 và có thể tiệm cận về 0.01. Kết quả mô phỏng cũng chỉ ra rằng, khi tăng tỷ số tín hiệu trên nhiễu của công suất phát của nguồn thì xác suất bảo mật giảm. Điều này có thể giải thích là vì khi tăng công suất của nguồn đồng nghĩa với việc thiết bị nghe lén có nhiều cơ hội giải mã được thông tin qua đường truyền từ S đến E. Do đó, tăng công suất của nguồn làm giảm khả năng bảo mật của hệ thống.

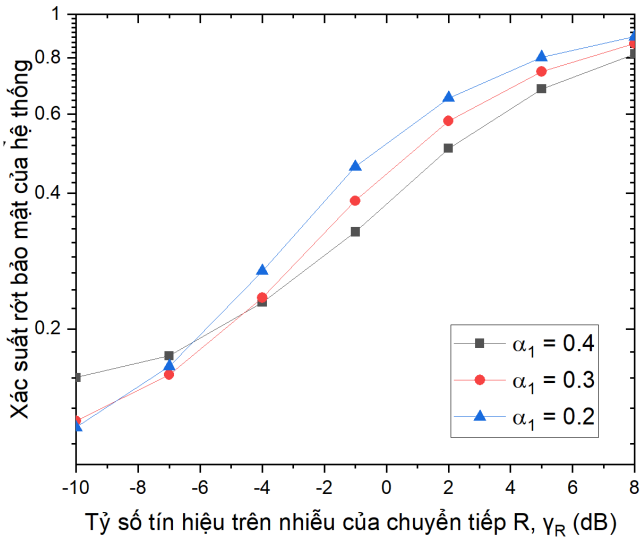


Hình 3. *Xác suất rớt bảo mật của hệ thống theo tỷ số tín hiệu trên nhiễu của kẻ phát nhiễu với hệ số phân bổ công suất* α_1.

Ở hình 3, xác suất rớt bảo mật của hệ thống được khảo sát theo tỷ số tín hiệu trên nhiễu của kẻ phát nhiễu và hệ số phân bổ công suất cho thiết bị thứ nhất. Ở đây, giá trị $\lambda_i = 50$ và giá trị $\lambda_j = 1$. Khi công suất phát của kẻ phát nhiễu càng tăng thì xác suất rớt bảo mật của hệ thống tăng tuyến tính theo công suất và hệ thống sẽ bị mất bảo mật. Việc tăng nhiễu làm ảnh hưởng nghiêm trọng đến tỷ số tín hiệu trên nhiễu khi giải mã tín hiệu, làm giảm tỷ số tín hiệu trên nhiễu và dẫn đến không giải mã được tín hiệu có ích. Khi tỷ số tín hiệu trên nhiễu của thiết bị phát nhiễu tăng đến 8 dB với $\alpha_1 = 0.2$, xác suất rớt bảo mật của hệ thống tiệm cận về giá trị 0.7, một giá trị rất lớn và gần như hệ thống mất khả năng bảo mật. Khi giá trị α_1 tăng thì xác suất rớt bảo mật của hệ thống giảm và ngược lại. Khi hệ số phân bổ công suất cho U1 lớn (khoảng 0.4) thì hệ số phân bổ công suất cho U2 giảm. Công suất tín hiệu dành cho U2 giảm và làm giảm xác suất rớt bảo mật của cả hệ thống.

Tương tự, xác suất rớt bảo mật của hệ thống được khảo sát theo tỷ số tín hiệu trên nhiễu của chuyển tiếp R và hệ số phân bổ công suất cho tín hiệu của thiết bị nhận thứ nhất

(hình 4). Giả sử giá trị $\lambda_i = 50$ và giá trị $\lambda_j = 1$. Kết quả mô phỏng cho thấy khi tăng công suất của chuyển tiếp thì khả năng bảo mật của hệ thống giảm. Khi tăng công suất của chuyển tiếp R thì thiết bị nghe lén hoàn toàn có khả năng giải mã được tín hiệu của hai người sử dụng. Khi tăng giá trị phân bổ công suất cho thiết bị U1, tương tự như mô phỏng ở hình 3, xác suất rớt bảo mật của hệ thống giảm.



Hình 4. *Xác suất rớt bảo mật của hệ thống theo tỷ số tín hiệu trên nhiễu của chuyển tiếp R và hệ số phân bổ công suất* α_1.

Khi giá trị tỷ số tín hiệu trên nhiễu của chuyển tiếp R tăng lên 8 dB với các giá trị phân bổ công suất cho U1 khác nhau thì xác suất rớt bảo mật của hệ thống đều tiệm cận về 0.9 và hệ thống gần như đã mất bảo mật.

5. KẾT LUẬN

Bài báo nghiên cứu về bảo mật lớp vật lý cho hệ thống sự dụng chuyển tiếp song công. Đặc biệt mô hình hệ thống trong bài báo sử dụng kỹ thuật đa truy nhập phi trực giao, một kỹ thuật tiềm năng cho hệ thống 5G. Bài báo đã đưa ra mô hình hệ thống và khảo sát khả năng bảo mật của hệ thống với sự thay đổi của các tham số. Kết quả bài báo chỉ ra rằng, hệ thống có thể cải thiện khả năng bảo mật khi tăng độ lợi của kênh truyền hợp pháp lớn gấp nhiều lần so với kênh truyền bất hợp pháp. Việc điều chỉnh công suất phát của các thiết bị phát hợp pháp như nguồn S và chuyển tiếp R đóng vai trò quan trọng trong việc giữ bảo mật của hệ thống. Kết quả bài báo cũng chỉ ra các giá trị hợp lý để điều chỉnh công suất của nguồn S và thiết bị R. Ngoài ra bài báo cũng khảo sát khả năng bảo mật của hệ thống theo hệ số phân bổ công suất, với hệ số phân bổ công suất cho thiết bị ở gần nhỏ dẫn đến làm tăng xác suất rớt bảo mật của hệ thống. Khi kẻ phát nhiễu tăng công suất phát nhiễu đến một giới hạn nào đó thì hệ thống sẽ mất bảo mật.

LỜI CẢM ƠN

Cám ơn tập thể Bộ môn Kỹ thuật Thông tin đã tư vấn hỗ trợ trong quá trình thực hiện nghiên cứu. Cảm ơn trường Đại học Giao thông Vận tải đã tài trợ cho nghiên cứu này trong khuôn khổ đề tài mã số T2019-DT-007.

TÀI LIỆU THAM KHẢO

[1]. S. M. Riazul Islam, Nurilla Avazov, Octavia A. Dobre, Kyung-sup Kwak, Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges, IEEE Communications Surveys & Tutorials, 19 (2017) 721-742. https://doi.org/10.1109/COMST.2016.2621116

[2]. Nan Yang, Lifeng Wang, Giovanni Geraci, Maged Elkashlan, Jinhong Yuan, Marco Di Renzo, Safeguarding 5G wireless communication networks using physical layer security, IEEE Communications Magazine, 53 (2015) 20-27. https://doi.org/10.1109/MCOM.2015.7081071.

[3]. Zhiguo Ding, Xianfu Lei, George K. Karagiannidis, Robert Schober, Jinhong Yuan, Vijay K. Bhargava, A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends, IEEE Journal on Selected Areas in Communications, 35 (2017) 2181-2195. https://doi.org/10.1109/JSAC.2017.2725519

[4]. George T. Amariucai, Shuangqing Wei, Half-duplex active eavesdropping in fast-fading channels: A block-Markov Wyner secrecy encoding scheme, IEEE Transactions on Information Theory, 58 (2012) 4660-4677. https://doi.org/10.1109/TIT.2012.2191672

[5]. Amitav Mukherjee, A. Lee Swindlehurst, Jamming games in the MIMO wiretap channel with an active eavesdropper, IEEE Transactions on Signal Processing, 61 (2012) 82-91. https://doi.org/10.1109/TSP.2012.2222386

[6]. Jie Xu, Lingjie Duan, Rui Zhang, Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels, IEEE Wireless Communications Letters, 5 (2015) 80-83. https://doi.org/10.1109/LWC.2015.2498610.

[7]. Sarbani Ghose, Chinmoy Kundu, Octavia A. Dobre, Secrecy outage of proactive relay selection by eavesdropper, GLOBECOM 2017-2017 IEEE Global Communications Conference, 2017. DOI: 10.1109/GLOCOM.2017.8254183

[8]. Tung Pham Huu, Truong Xuan Quach, Hung Tran, Hans-Jürgen Zepernick, Louis Sibomana, On proactive attacks for coping with cooperative attacks in relay networks, 2017 23rd Asia-Pacific Conference on Communications (APCC), 2017. DOI: 10.23919/APCC.2017.8303981

[9]. Chaoying Yuan, Xiaofeng Tao, Na Li, Wei Ni, Ren Ping Liu, Ping Zhang, Analysis on secrecy capacity of cooperative non-orthogonal multiple access with proactive jamming, IEEE Transactions on Vehicular Technology, 68 (2019) 2682-2696. https://doi.org/10.1109/TVT.2019.2895911

[10]. Omid Abbasi, Afshin Ebrahimi, Secrecy analysis of a NOMA system with full duplex and half duplex relay, 2017 Iran Workshop on Communication and Information Theory (IWCIT), 2017. DOI: 10.1109/IWCIT.2017.7947676