

CẢI THIỆN BẢO MẬT LỚP VẬT LÝ TRONG MẠNG VÔ TUYẾN NOMA BẰNG MẢNG ANTEN

ENHANCING PHYSICAL LAYER SECURITY OF NOMA WIRELESS NETWORKS BY ARRAY ANTENNA

Trương Ngọc Hà*, Nguyễn Văn Phúc, Đặng Phước Hải Trang, Trần Thị Quỳnh Như

Trường Đại học Sư phạm Kỹ thuật TP. Hồ Chí Minh¹

*Tác giả liên hệ: hatn@hcmute.edu.vn

(Nhận bài: 26/7/2021; Chấp nhận đăng: 06/10/2021)

Tóm tắt - Trong bài báo này, nhóm tác giả đã đưa ra mô hình truyền thông vô tuyến với kỹ thuật NOMA kết hợp mảng Anten để cải thiện bảo mật lớp vật lý. Mô hình đưa ra gồm ba nút: Nguồn, đích và nút nghe lén. Nút nguồn là một mảng Anten sử dụng kỹ thuật NOMA để truyền đồng thời hai tín hiệu x_1 và x_2 . Bằng các lý thuyết đưa ra, đã chứng minh được bảo mật vật lý tỷ lệ thuận với số lượng Anten ở nút nguồn. Chúng ta kiểm chứng bằng quá trình mô phỏng và chứng minh điều kết luận ở lý thuyết là đúng. Ngoài ra, để có một hướng nhìn khác, nhóm tác giả đã tiến hành đánh giá tỷ lệ lỗi bit (BER) để thấy được mối quan hệ giữa BER và bảo mật lớp vật lý trong mạng truyền thông NOMA có kết hợp với mảng Anten.

Từ khóa - NOMA; mảng Anten; bảo mật lớp vật lý; xác suất dừng; BER

1. Giới thiệu

Ngày nay, cuộc cách mạng công nghiệp 4.0 đang diễn ra một cách mạnh mẽ trên toàn cầu, trong đó lĩnh vực viễn thông là đầu tàu của cuộc cách mạng đó. Hàng loạt các hệ thống vô tuyến và các chuẩn giao tiếp như Wifi, LTE, Wimax, HSPA+... đã ra đời [1], [2]. Tuy nhiên, tần số là tài nguyên có hạn và hiệu suất sử dụng phổ tần số còn thấp. Một kỹ thuật đa truy cập đầy tiềm năng và triển vọng đang được nghiên cứu đó là kỹ thuật đa truy cập phi trực giao (NOMA) [3], [4]. NOMA là kỹ thuật cho phép với cùng một người dùng gọi cùng lúc nhiều tín hiệu trên cùng một băng tần đến một hoặc nhiều người dùng khác. Điều đó được thực hiện bằng cách ghép tuyến tính các dữ liệu lại với nhau rồi gửi tín hiệu đã ghép tới các bên nhận. Ở phía thu dữ liệu, chúng sẽ được giải mã theo cơ chế khử nhiễu tuần tự (Successive Interference Cancellation (SIC)) [5].

Tuy nhiên, do tín hiệu truyền từ nguồn đến nơi nhận qua môi trường vô tuyến nên dễ bị tấn công hoặc nghe lén. Hiện tại, các phương pháp bảo mật thường được triển khai ở lớp ứng dụng: Các kỹ thuật mã hóa, xác thực (như WEP, WPA, ...). Bên cạnh đó, các phương thức tấn công mạng cũng thay đổi và phát triển không ngừng [6]. Ngày nay, một hướng nghiên cứu mới nhằm tìm ra các giải pháp tăng cường khả năng bảo mật cho mạng vô tuyến ở lớp vật lý [7]. Một hệ thống truyền thông không dây có khả năng bảo mật nếu dung lượng kênh truyền hợp pháp lớn hơn dung lượng kênh truyền nghe lén [7]. Một trong những hướng nghiên cứu về bảo mật lớp vật lý là dùng kỹ thuật

Abstract - In this paper, the authors proposed a wireless communication NOMA technique with antenna array to improve the security of the physical layer. The proposed model is composed of three nodes, namely the source node, the destination node, and the eavesdropping node. The source node is an antenna array that uses NOMA technology to transmit two signals x_1 and x_2 simultaneously. It was mathematically proved that the physical security is proportional to the number of antennas at the source node. This was also verified by the simulation results. In addition, for different perspective, the authors evaluated the bit error ratio (BER) to determine that BER is strongly related to the security of physical layer in NOMA communication network combined with antenna array.

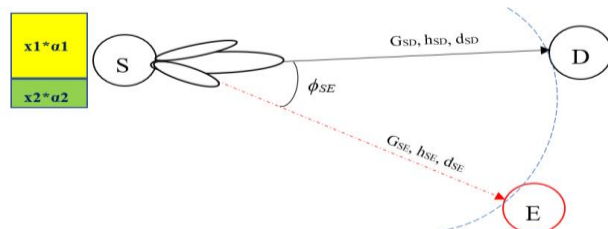
Key words - NOMA; array antenna; physical layer security; outage probability; BER

beamforming và mảng Anten [8], [9], [10], [11], [12]. Trong nghiên cứu này, các tác giả sẽ tập trung đi vào phân tích ảnh hưởng của mảng Anten đến xác suất dừng của bảo mật vật lý trong mạng NOMA này.

2. Mô hình hệ thống mạng

2.1. Mô hình nghiên cứu

Trong nghiên cứu này, nhóm tác giả đưa ra mô hình gồm 3 nút mạng như Hình 1. Mô hình này gồm nút nguồn S, nút đích D, và nút nghe lén E. Trong đó, nút nguồn S sử dụng công nghệ NOMA để truyền dữ liệu đến nút đích D. Nút nghe lén E cố gắng để nghe tín hiệu truyền từ S đến D.



Hình 1. Mô hình mạng NOMA gồm nút S là mảng Anten, nút đích D và nút nghe lén E

Các giả thuyết đưa ra trong mô hình như sau:

- Nút nguồn S có N Anten, nút đích và nút nghe lén chỉ sử dụng 1 Anten.
- Nguồn S có thể điều chỉnh búp sóng để nút D thu được tín hiệu cực đại của búp sóng.
- Tất cả các kênh truyền là kênh Rayleigh fading.

¹ Ho Chi Minh City University of Technology and Education (Trương Ngọc Hà, Nguyễn Văn Phúc, Đặng Phước Hải Trang, Trần Thị Quỳnh Như)

- Tất cả các tín hiệu nhiễu trắng (AWGN) tại bộ thu thu được có giá trị trung bình bằng 0 và phương sai tín hiệu nhiễu là N_0 .

Trong mô hình này, nút S đặt tại gốc tọa độ, các nút D và nút E được giả sử đều nằm trên đường tròn có tâm là gốc tọa độ và bán kính bằng 1.

2.2. Kỹ thuật NOMA

Kỹ thuật NOMA là kỹ thuật mà hai tín hiệu x_1 và x_2 sẽ được cộng tuyến tính lại với nhau dưới dạng sau [13]:

$$x_s = \sqrt{\alpha_1 P_s} x_1 + \sqrt{\alpha_2 P_s} x_2 \quad (1)$$

Trong đó, x_s là dữ liệu tổng hợp sẽ được gửi đi; α_1 và α_2 là hệ số phân chia công suất phát P_s cho các tín hiệu x_1 và x_2 . Trong đó, $\alpha_1 > \alpha_2$ và $\alpha_1 + \alpha_2 = 1$, có nghĩa là tín hiệu x_1 sẽ được phân công với công suất phát lớn hơn tín hiệu x_2 . Trong nghiên cứu này, hai dữ liệu x_1 và x_2 là hai dữ liệu khác nhau nhưng cùng được gửi đến cùng một nguồn đích.

2.3. Mảng anten

Mảng anten là một hệ thống gồm nhiều anten đặt gần nhau, cách nhau một khoảng cách, nhằm tạo ra chùm bức xạ cho mảng khác nhau ở những vị trí khác nhau [14]. Mảng anten có nhiều loại khác nhau hai chiều, một chiều, tuyến tính, không tuyến tính... [14]. Trong nghiên cứu này, mảng anten được xem xét là mảng tuyến tính [14]: Khi đó, hệ số sắp xếp (AF: array factor) của mảng là:

$$|AF(N, \phi)| = \left| \frac{\sin[N(kd \cos \phi + \beta)]}{\sin\left(\frac{kd \cos \phi + \beta}{2}\right)} \right| \quad (2)$$

Trong đó:

N : Số anten của nút nguồn S.

$k=2\pi/\lambda$: Thừa số bước sóng (với λ là bước sóng của tín hiệu).

d : Khoảng cách giữa các anten ($d = \lambda/2(1-1/N)$).

β : Hệ số pha của dòng cung cấp (trong nghiên cứu này $\beta = -k*d$).

ϕ : Hệ số pha tính theo đơn vị rad trên mặt phẳng tọa độ cực.

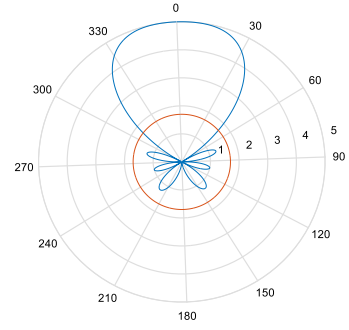
Theo công thức (2) giá trị $|AF(N, \phi)|$ phụ thuộc vào các biến: $\phi(0 \leq \phi \leq \pi)$, số lượng anten N . Như vậy, khi N và ϕ thay đổi thì giá trị $|AF(N, \phi)|$ cũng sẽ thay đổi theo. Hình 2a và Hình 2b là đồ thị của $|AF(N, \phi)|$ với $N=5$ trên tọa độ cực và tọa độ cầu.

Sau khi 2 tín hiệu x_1 và x_2 được ghép theo công thức (1), tín hiệu x_s này sẽ đưa đến một mảng anten có hệ số AF như trong công thức (2) để truyền đi, khi đó tín hiệu ngõ ra tại nút S có dạng như công thức (3).

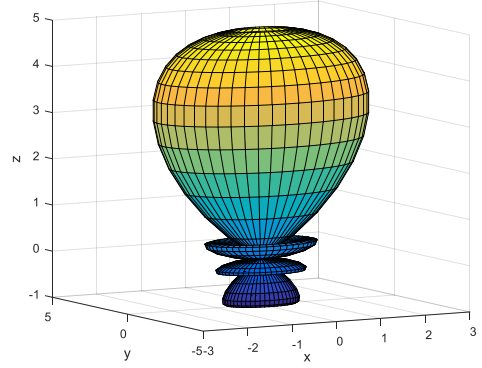
$$x_{S_AF} = |AF(N, \phi_{SD})| \sqrt{\alpha_1 P_s} x_1 + \sqrt{\alpha_2 P_s} x_2 \quad (3)$$

Với $|AF(N, \phi_{SD})|$ là hệ số của $|AF(N, \phi)|$ theo hướng nút D.

Tín hiệu x_{S_AF} này sẽ được truyền trong môi trường vô tuyến đến nút D.



Hình 2a. Đồ thị bức xạ 2 chiều của mảng gồm 5 anten



Hình 2b. Đồ thị bức xạ 3 chiều của mảng gồm 5 anten

3. Bảo mật lớp vật lý trong mảng NOMA kết hợp mảng anten

3.1. Lý thuyết bảo mật lớp vật lý trong mạng NOMA

Tín hiệu từ nguồn phát (nút S) sau khi đi qua môi trường vô tuyến sẽ đến bộ thu. Trong nghiên cứu này, nút đích được xem như là nằm ở vị trí trường vùng xa của mảng anten (khi đó ta không xem xét đến ảnh hưởng của từng anten đến tín hiệu thu được tại nút đích mà chỉ xét ảnh hưởng chung với một hệ số kênh truyền) [14]. Khi đó, tín hiệu tại nút D nhận được là:

$$y_D = \sqrt{\alpha_1} |AF(N, \phi_{SD})| \sqrt{P_s} x_1 h_{SD} + \sqrt{\alpha_2} |AF(N, \phi_{SD})| \sqrt{P_s} h_{SD} x_2 + n_{SD} \quad (4)$$

Trong đó, h_{SD} là hệ số kênh truyền fading Rayleigh giữa S và D, $|AF(N, \phi_{SD})|$ là giá trị của mảng anten theo hướng nút D, n_{SD} là nhiễu cộng tại D (là một biến ngẫu nhiên có phân phối Gauss với giá trị trung bình bằng 0 và phương sai bằng N_0).

Trong kỹ thuật NOMA, nút đích D sẽ giải mã dữ liệu x_1 trước (vì x_1 được phân bổ công suất cao hơn x_2). Sau khi giải mã thành công x_1 , kỹ thuật khử nhiễu tuần tự (SIC) được sử dụng [15] để tách lấy tín hiệu x_2 (nút đích sẽ loại bỏ thành phần $\sqrt{\alpha_1} |AF(N, \phi_{SD})| \sqrt{P_s} x_1 h_{SD}$ ra khỏi tín hiệu nhận được). Tín hiệu còn lại là dữ liệu x_2 cộng với nhiễu:

$$y_{D_x2} = \sqrt{\alpha_2} |AF(N, \phi_{SD})| \sqrt{P_s} h_{SD} x_2 + n_{SD} \quad (5)$$

Tương tự, nút E cũng thu được tín hiệu như sau:

$$y_E = \sqrt{\alpha_1} |AF(N, \phi_{SE})| \sqrt{P_s} x_1 h_{SE} + \sqrt{\alpha_2} |AF(N, \phi_{SE})| \sqrt{P_s} h_{SE} x_2 + n_{SE} \quad (6)$$

Trong đó, h_{SE} là hệ số kênh truyền fading Rayleigh giữa

S và E, $|AF(N, \phi_{SE})|$ là giá trị của mảng anten theo phương ϕ_{SE} (theo phương nút nghe lên E), n_{SE} là nhiễu cộng tại E (là một biến ngẫu nhiên có phân phối Gauss với giá trị trung bình bằng 0 và phương sai bằng N_0).

Nút nghe lên E cũng sẽ giải mã tín hiệu x_1 trước. Sau khi giải mã thành công x_1 , nút E sử dụng kỹ thuật SIC để giải mã tín hiệu của x_2 như sau:

$$y_{E-x_2} = \sqrt{\alpha_2} |AF(N, \phi_{SE})| \sqrt{P_s} h_{SE} x_2 + n_{SE} \quad (7)$$

Các đại lượng g_{SD} , g_{SE} , G_{SD} , G_{SE} , lần lượt được cho bởi các công thức bên dưới.

$$g_{SD} = |h_{SD}|^2 \quad (8)$$

$$g_{SE} = |h_{SE}|^2 \quad (9)$$

$$G_{SD} = |AF(N, \phi_{SD})|^2 \quad (10)$$

$$G_{SE} = |AF(N, \phi_{SE})|^2 \quad (11)$$

Từ công thức (4), (5), (8), (9), (10), (11), ta có tỷ số SNR đạt được tại D của x_1 và x_2 là:

$$SNR_{D,x_1} = \frac{G_{SD} P_S \alpha_1 g_{SD} / N_0}{G_{SD} P_S \alpha_2 g_{SD} / N_0 + 1} = \frac{G_{SD} Q \alpha_1 g_{SD}}{G_{SD} Q \alpha_2 g_{SD} + 1} \quad (12)$$

$$SNR_{D,x_2} = \frac{G_{SD} P_S \alpha_2 g_{SD}}{N_0} = G_1 Q \alpha_2 g_{SD} \quad (13)$$

Trong công thức (12) và (13), Q là tỷ số mức công suất tín hiệu trên công suất nhiễu và được xác định như sau:

$$Q = \frac{P_s}{N_0} \quad (14)$$

Trong mô hình này, ta xem xét trường hợp tệ nhất là nút E áp dụng nguyên lý SIC tốt nhất. Từ công thức (6), (7), (8), (9), (10), (11), ta có tỷ số SNR đạt được tại nút nghe lên E để lấy x_1 và x_2 là:

$$SNR_{E,x_1} = \frac{G_{SE} P_S \alpha_1 g_{SE} / N_0}{G_{SE} P_S \alpha_2 g_{SE} / N_0 + 1} = \frac{G_{SE} Q \alpha_1 g_{SE}}{G_{SE} Q \alpha_2 g_{SE} + 1} \quad (15)$$

$$SNR_{E,x_2} = \frac{G_{SE} P_S \alpha_2 g_{SE}}{N_0} = G_{SE} Q \alpha_2 g_{SE} \quad (16)$$

Xét kênh truyền trong mô hình hệ thống là kênh truyền fading Rayleigh, có CDF và PDF của các độ lợi kênh g_i lần lượt là [16]:

$$F_{g_i}(x) = 1 - e^{-\lambda_i x} \quad (17)$$

Với $\lambda_i = d_i^\beta$

$$f_{g_i}(x) = \lambda_i e^{-\lambda_i x} \quad (18)$$

Trong đó, β là hệ số suy hao kênh truyền, d là khoảng cách giữa điểm phát và điểm thu.

Dung lượng kênh truyền tại nút đích và nút nghe lên:

$$C_D^{x_i} = \log_2(1 + SNR_{D,x_i}) \quad (19)$$

$$C_E^{x_i} = \log_2(1 + SNR_{E,x_i}) \quad (20)$$

Với $i = 1, 2$.

Dung lượng kênh truyền bảo mật [16]:

$$C_i = [C_D^{x_i} - C_E^{x_i}]^+ \quad (21)$$

Trong đó $[x]^+ = \max\{x, 0\}$.

3.2. Xác suất dừng bảo mật lớp vật lý trong mạng NOMA kết hợp mảng anten

Xác suất dừng bảo mật là xác suất mà dung lượng bảo

mật C_i (trong công thức (21)) nhỏ hơn ngưỡng tốc độ C_{th} cho trước [17]. Các biểu thức dưới đây đưa ra nhằm đánh giá hiệu năng của xác suất dừng bảo mật trong mạng thứ cấp cũng như đánh giá khả năng nghe lên của nút nghe lên E.

Như vậy, xác suất dừng bảo mật lớp vật lý của dữ liệu x_1 là:

$$P_{out}^{x_1} = \Pr[C_1 < C_{th}] = \Pr[(C_D^{x_1} - C_E^{x_1}) < C_{th}] \quad (22)$$

Thay các công thức (19), (20) vào (22) được công thức cho $P_{out}^{x_1}$ như sau:

$$\begin{aligned} P_{out}^{x_1} &= \Pr[(\log_2(1 + SNR_{D,x_1}) - \log_2(1 + SNR_{E,x_1})) < C_{th}] \\ &= \Pr\left[\log_2\left(\frac{1 + SNR_{D,x_1}}{1 + SNR_{E,x_1}}\right) < C_{th}\right] \\ &= \Pr\left[\frac{1 + SNR_{D,x_1}}{1 + SNR_{E,x_1}} < 2^{C_{th}}\right] \end{aligned} \quad (23)$$

Đặt $\theta = 2^{C_{th}} - 1$. Công thức (23) được viết lại như sau:

$$P_{out}^{x_1} = P_r \left[\frac{G_{SD} Q \alpha_1 g_{SD}}{G_{SD} Q \alpha_2 g_{SD} + 1} < \theta + (\theta + 1) \frac{G_{SE} Q \alpha_1 g_{SE}}{G_{SE} Q \alpha_2 g_{SE} + 1} \right] \quad (24)$$

Với điều kiện xấu nhất, nút nghe lên E có thể giải mã tín hiệu x_1 một cách tốt nhất (tức là khi đó nút nghe lên có thể loại bỏ được nhiễu đồng kênh). Khi đó, xác suất dừng từ công thức (24) được viết lại như sau:

$$\begin{aligned} P_{out}^{x_1} &= P_r \left[\frac{G_{SD} Q \alpha_1 g_{SD}}{G_{SD} Q \alpha_2 g_{SD} + 1} < \theta + (\theta + 1) G_{SE} Q \alpha_1 g_{SE} \right] \\ &= P_r \left[\frac{g_{SE} > \frac{G_{SD} g_{SD}}{(\theta + 1) G_{SE} (G_{SD} Q \alpha_2 g_{SD} + 1)}}{\theta} \right] dx \\ &= \int_0^\infty f_{g_{SD}}(x) Pr \left[\frac{g_{SE} > \frac{G_{SD} x}{(\theta + 1) G_{SE} (G_{SD} Q \alpha_2 g_{SD} + 1)}}{\theta} \right] dx \\ &= \int_0^\infty f_{g_{SD}}(x) Pr \left[\frac{G_{SD} x}{(\theta + 1) G_{SE} (G_{SD} Q \alpha_2 g_{SD} + 1)} < \frac{\theta}{(\theta + 1) G_{SE} Q \alpha_1} \right] dx \\ &= \int_0^\infty f_{g_{SD}}(x) Pr \left[\frac{g_{SE} > \frac{G_{SD} g_{SD}}{(\theta + 1) G_{SE} (G_{SD} Q \alpha_2 g_{SD} + 1)}}{\theta} \right] dx \\ &= \int_0^\infty f_{g_{SD}}(x) Pr \left[\frac{G_{SD} x}{(\theta + 1) G_{SE} (G_{SD} Q \alpha_2 g_{SD} + 1)} > \frac{\theta}{(\theta + 1) G_{SE} Q \alpha_1} \right] dx \end{aligned} \quad (25)$$

Nếu $\alpha_1 \leq \theta \alpha_2$ thì:

$$\Pr[(\alpha_1 - \theta \alpha_2) x G_{SD} Q \leq \theta] = 1 \text{ và}$$

$$Pr \left[\frac{g_{SE} > \frac{G_{SD} g_{SD}}{(\theta + 1) G_{SE} (G_{SD} Q \alpha_2 g_{SD} + 1)} - \frac{\theta}{(\theta + 1) G_{SE} Q \alpha_1}}{\frac{G_{SD} x}{(\theta + 1) G_{SE} (G_{SD} Q \alpha_2 g_{SD} + 1)} > \frac{\theta}{(\theta + 1) G_{SE} Q \alpha_1}} \right] = 0 \quad (26)$$

$$\begin{aligned} \text{Nên: } P_{out}^{x_1} &= \int_0^\infty f_{g_{SD}}(x) \cdot 1 dx + \int_0^\infty f_{g_{SD}}(x) \cdot 0 dx \\ &= 1 + 0 = 1 \end{aligned}$$

Nếu $\alpha_1 > \theta \alpha_2$:

$$P_{out}^{x_1} = \int_0^{\infty} f_{g_{SD}}(x) Pr \left[x < \frac{\theta}{(\theta+1)G_{SD}Q\alpha_1} \right] dx + \int_0^{\infty} f_{g_{SD}}(x) Pr \left[\frac{g_{SE}}{(\theta+1)G_{SE}(G_{SD}Q\alpha_2 g_{SD} + 1)} > \frac{\theta}{(\theta+1)G_{SE}Q\alpha_1}, x > \frac{\theta}{(\theta+1)G_{SD}Q\alpha_1} \right] dx \quad (27)$$

$$\text{Với } m = \frac{\theta}{G_{SD}Q(\alpha_1 - \theta\alpha_2)}$$

$$P_{out}^{x_1} = 1 - e^{-\lambda_{SD}m} + \int_m^{\infty} \lambda_{SD} e^{-\lambda_{SD}x} e^{-\lambda_{SE}A} dx \quad (28)$$

Với

$$A = \frac{\alpha_1 - \theta\alpha_2}{\alpha_1\alpha_2(\theta+1)QG_{SE}} - \frac{1}{\alpha_2(\theta+1)G_{SE}Q(QG_{SD}\alpha_2x+1)}$$

Tương tự như công thức (22), xác suất dừng bảo mật lớp vật lý của dữ liệu x_2 là:

$$P_{out}^{x_2} = Pr[C_D^{x_2} - C_E^{x_2} < C_{th}] \quad (29)$$

Thay các công thức (19) và (20) vào (29), được:

$$\begin{aligned} P_{out}^{x_2} &= Pr \left[1 + G_{SD}g_{SD}Q\alpha_2 < 2^{C_{th}}(1 + G_{SE}g_{SE}Q\alpha_2) \right] \\ &= Pr \left[G_{SD}g_{SD}Q\alpha_2 < \theta + (\theta+1)G_{SE}g_{SE}Q\alpha_2 \right] \\ &= Pr \left[g_{SE} > \frac{G_{SD}g_{SD}Q\alpha_2 - \theta}{(\theta+1)G_{SE}Q\alpha_2} \right] \\ &= \int_0^{\infty} f_{g_{SD}}(x) Pr \left[g_{SE} > \frac{G_{SD}xQ\alpha_2 - \theta}{(\theta+1)G_{SE}Q\alpha_2} \right] dx \\ &= \int_0^{\infty} f_{g_{SD}}(x) Pr \left[G_{SD}xQ\alpha_2 < \theta \right] dx \\ &\quad + \int_0^{\infty} f_{g_{SD}}(x) Pr \left[g_{SE} > \frac{G_{SD}xQ\alpha_2 - \theta}{(\theta+1)G_{SE}Q\alpha_2}, G_{SD}xQ\alpha_2 > \theta \right] dx \\ &= \int_0^{\infty} \lambda_{SD} e^{-\lambda_{SD}x} Pr \left[G_{SD}xQ\alpha_2 < \theta \right] dx \\ &\quad + \int_0^{\infty} \lambda_{SD} e^{-\lambda_{SD}x} Pr \left[g_{SE} > \frac{G_{SD}xQ\alpha_2 - \theta}{(\theta+1)G_{SE}Q\alpha_2} \right] dx \\ &= \int_0^{\infty} \lambda_{SD} e^{-\lambda_{SD}x} \left[1 - \lambda_{SD} e^{-\lambda_{SD}n} \right] dx \\ &\quad + \int_n^{\infty} \lambda_{SD} e^{-\lambda_{SD}x} e^{-\frac{\lambda_{SE}}{(\theta+1)G_{SE}g_{SE}Q\alpha_2}} dx \\ &= 1 - e^{-\lambda_{SD}n} + \lambda_{SD} \frac{e^{-\lambda_{SD}n}}{\lambda_{SD} + \frac{G_{SD}\lambda_{SE}}{(\theta+1)G_{SE}}} \end{aligned} \quad (30)$$

$$\text{Với: } n = \frac{\theta}{QG_{SD}\alpha_2}$$

Ta biết rằng, xác suất dừng nằm trong khoảng từ 0 đến 1. Giá trị P_{out} càng nhỏ (tiến gần 0) thì tính bảo mật của hệ thống càng tốt (xác suất để xảy ra $(C_D^{x_1} - C_E^{x_1} < C_{th})$ nhỏ, tức là xác suất $(C_D^{x_1} - C_E^{x_1} > C_{th})$ lớn). Ngược lại, khi P_{out} càng tiến đến 1 thì tính bảo mật của hệ thống càng kém (xác suất để xảy ra $(C_D^{x_1} - C_E^{x_1} < C_{th})$ lớn, tức là xác suất $(C_D^{x_1} - C_E^{x_1} > C_{th})$ nhỏ). Công thức (28) cho thấy, xác suất này tỷ lệ nghịch với hệ số α_1, G_{SD}, Q . Ngược lại, xác suất dừng này tỷ lệ thuận với hệ số G_{SE} . Mặt khác, hệ số G_{SD} tỷ lệ thuận với bình phương số anten trong nút S. Do đó, khi số anten ở nút nguồn tăng lên thì xác suất dừng giảm đi. Trong khi đó, hệ số G_{SE} phụ thuộc vào hai thông số là vị trí của nút nghe lén và số lượng anten ở nút nguồn. Trong mô hình này, khoảng cách từ nút đích đến nút nguồn cũng như từ nút E đến nút

nguồn đều bằng 1 nên hệ số λ_{SD} bằng 1, nên sẽ không ảnh hưởng đến giá trị của xác suất dừng. Công thức (30) cho ta thấy, xác suất dừng $P_{out}^{x_2}$ tỷ lệ nghịch với hệ số α_2, G_{SD}, Q . Hệ số $P_{out}^{x_2}$ này tỷ lệ thuận với hệ số G_{SE} .

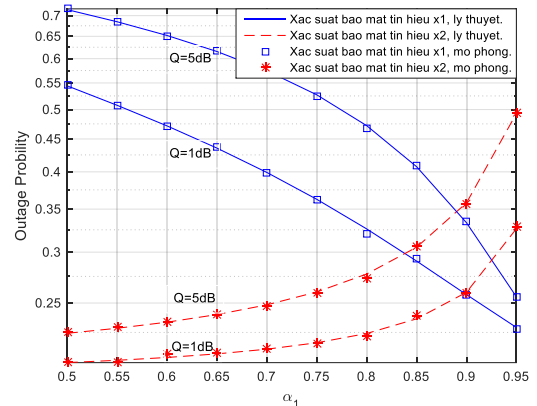
4. Kết quả mô phỏng và đánh giá

Các kết quả mô phỏng được thực hiện bằng phần mềm MatLab theo phương pháp Monte-Carlo với số phép thử 10000 lần. Công thức (28) và công thức (30) lần lượt là xác suất dừng bảo mật lớp vật lý theo lý thuyết của x_1 và x_2 .

4.1. Đánh giá theo hệ số anpha

Hình 3 thể hiện xác suất dừng bảo mật lớp vật lý theo hệ số phân chia công suất giữa 2 tín hiệu x_1 và x_2 .

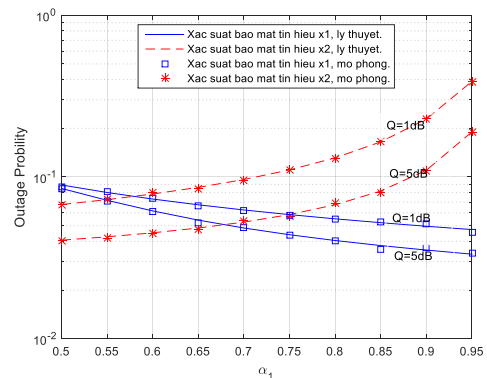
Các thông số mô phỏng, số anten của S là $N=5$; anten của D =1, của E =1; $Q=1$ và 5dB; $R_t=0,2$; $G_{SE}=1$ (hay $\phi_{SE}=80^\circ$); $\lambda_{SD}=1, \lambda_{SE}=1$.



Hình 3. Xác suất dừng theo hệ số phân chia công suất α_1 với $G_{SE}=1$

Kết quả trên Hình 3 thể hiện giữa lý thuyết và mô phỏng và phù hợp với nhau. Với hình này, khi hệ số α_1 tăng lên thì xác suất dừng của x_1 giảm còn của x_2 tăng lên.

Với cùng một tỷ lệ phân chia công suất α_1 , khi Q tăng lên xác suất dừng của x_1 tăng còn của x_2 giảm. Điều này được giải thích rằng, khi công suất tín hiệu tăng, nút nghe lén nghe được tín hiệu tốt hơn dẫn đến xác suất dừng sẽ tăng (bảo mật sẽ kém đi).



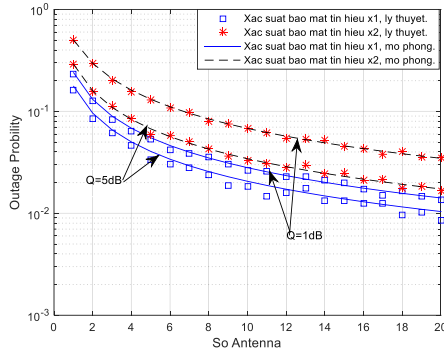
Hình 4. Xác suất dừng theo hệ số phân chia công suất α_1 với $G_{SE}=0,1$

Khi hệ số G_{SE} giảm xuống ($G_{SE}=0,1$ hay $\phi_{SE}=62^\circ$), còn các thông số khác vẫn giữ nguyên, kết quả mô phỏng được cho như Hình 4. Với Hình 4, xác suất dừng của x_1 và x_2

đều giảm khi α_1 tăng (giống Hình 3). Khi Q tăng lên, xác suất dừng x_2 sẽ giảm (giống Hình 3), còn của x_1 giảm (khác so với Hình 3).

4.2. Đánh giá theo số lượng anten

Hình 5 thể hiện xác suất dừng của x_1 và x_2 khi số lượng anten ở nút S được thay đổi. Các thông số mô phỏng còn lại: Q=1dB và 5dB; $\lambda_{SD}=1, \lambda_{SE}=1$; Số anten của D và E bằng 1; $R_t=0,2; G_{SE}=0,1$.

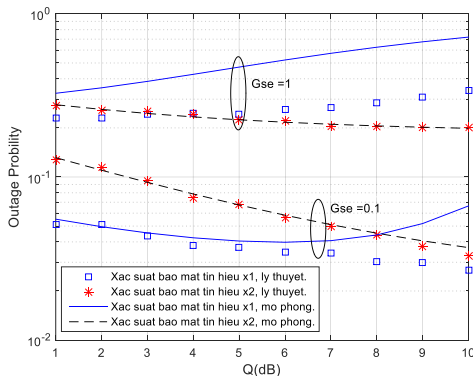


Hình 5. Xác suất dừng theo số lượng anten ở nút S

Kết quả ở Hình 5 đã chỉ ra rằng, khi số lượng anten trong mảng được tăng lên thì xác suất dừng của bảo mật lớp vật lý của x_1 và x_2 sẽ giảm. Ngoài ra, khi tăng hệ số Q_dB (với cùng một số lượng anten) thì xác suất dừng của x_1 và x_2 sẽ giảm. Khi số lượng anten tăng lên đồng nghĩa với nhiều vấn đề sẽ phát sinh (nhưng yếu tố này không được xét trong nghiên cứu này).

4.3. Đánh giá theo hệ số SNR (Q(dB))

Hình 6 thể hiện xác suất dừng của x_1 và x_2 khi hệ số Q_dB (mức công suất tín hiệu) thay đổi S được thay đổi. Các thông số mô phỏng còn lại: Số anten của S là N=5; Số anten của D =1, của E =1; $G_{SE}=0.1$ (hay $\phi_{SE}=62^\circ$) và 1; $\lambda_{SD}=1, \lambda_{SE}=1; R_t=0,2$.



Hình 6. Xác suất dừng theo hệ số Q(dB)

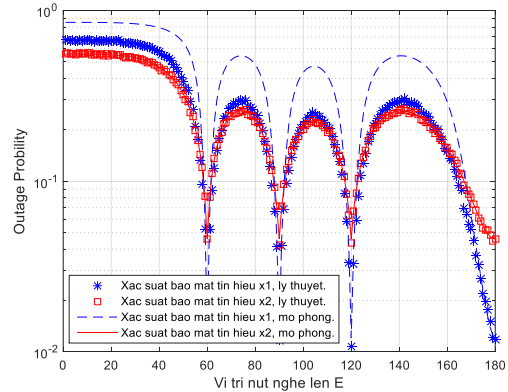
Kết quả ở Hình 6 chứng tỏ, xác suất dừng của tín hiệu x_2 là có sự phù hợp của lý thuyết và mô phỏng. Với tín hiệu x_1 : xác suất dừng giữa lý thuyết và mô phỏng có sự khác nhau khi Q_dB lớn hơn 5dB (với trường hợp $G_{SE}=0,1$), trường hợp $G_{SE}=1$ thì có sự khác nhau khá rõ. Sự khác biệt này là do từ công thức (24) xuống (25) giả sử mẫu số $[G_{SE}Q\alpha_2G_{SE}+1]$ được xem gần bằng 1. Giả sử này xem là đúng khi hệ số $G_{SE}Q\alpha_2G_{SE}$ là nhỏ hơn 1 nhiều. Tuy nhiên, khi Q tăng hay G_{SE} lớn thì giả sử này không còn đúng nữa. Khi đó, xác suất dừng bảo mật của x_1 theo lý thuyết sẽ lớn

hơn theo mô phỏng.

Kết quả từ Hình 6 còn giúp ta thấy rằng, khi G_{SE} lớn (nút nghe lén E ở gần nút D) thì khi Q_dB tăng nút nghe lén càng giải mã tín hiệu từ nút S tốt hơn dẫn đến việc bảo mật sẽ giảm (xác suất dừng bảo mật vật lý tăng lên).

4.4. Đánh giá theo vị trí nút nghe lén E

Trong mô phỏng ở dưới đây, nhóm tác giả sẽ cho vị trí nút E thay đổi trên toàn bộ mặt phẳng xung quanh điểm S. Khi đó, giữ nút E, nút S và nút D tạo ra một góc $0 \leq \phi_{SE} \leq 180^\circ$, kết quả được cho ở Hình 7. Các thông số mô phỏng còn lại: Số anten nút S =5; Số anten của D và E bằng 1; $Q=5dB; \lambda_{SD}=1, \lambda_{SE}=1; R_t=0,2$.



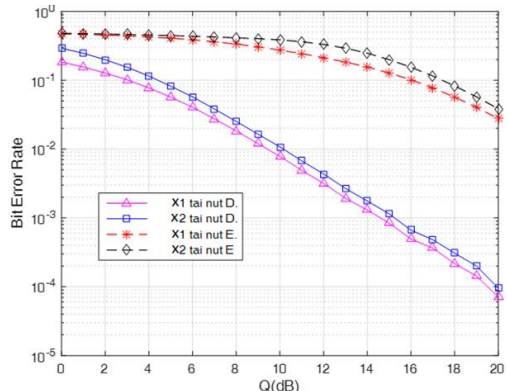
Hình 7. Xác suất dừng theo vị trí nút nghe lén E (đơn vị độ)

Kết quả ở Hình 7 chứng tỏ xác suất dừng của x_1 và x_2 giữa lý thuyết và mô phỏng là tương đối phù hợp nhau. Tuy nhiên, khi nút E thay đổi vị trí khi G_{SE} lớn thì có sự khác biệt giữa lý thuyết và mô phỏng của tín hiệu x_1 . Khi đó, xác suất dừng bảo mật của x_1 theo lý thuyết sẽ lớn hơn theo mô phỏng. Kết quả ở Hình 7 cũng chỉ ra rằng, ở những vị trí khác nhau của nút E, xác suất dừng bảo mật là khác nhau.

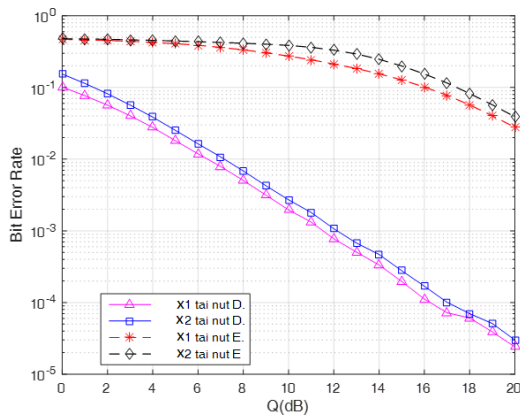
4.5. Đánh giá tỷ lệ lỗi bit BER của hệ thống

Trong nghiên cứu này, các tác giả còn mô phỏng xác suất lỗi BER (Bit Error Ratio) của từng tín hiệu. Trong các mô phỏng về tỷ lệ BER dưới đây, giá trị $G_{SE}=0,1, \alpha_1=0,6$. Phương pháp Monte-Carlo được sử dụng với tổng số bit được truyền trong mỗi trường hợp là 10^6 bit.

Bộ giải mã tuần tự SIC được sử dụng để giải mã tín hiệu tại nút D và nút E. Tín hiệu x_2 phụ thuộc vào việc giải mã của tín hiệu x_1 . Kết quả được cho ở Hình 8 và Hình 9.



Hình 8. Xác suất BER của hệ thống theo Q(dB) với bộ tách tín hiệu lý tưởng trên nút D và nút E (với anten tại nút S=2)



Hình 9. Xác suất BER của hệ thống theo Q (dB) với bộ tách tín hiệu lý tưởng trên nút D và nút E (với anten tại nút $S=4$)

Trong các Hình 8 và Hình 9, khi Q tăng lên thì BER của x_1 và x_2 giảm (cả nút S và nút E). BER trong Hình 9 của x_1 và x_2 tại nút D tốt hơn so với BER trong Hình 8 trong khi BER tại nút E của cả x_1 và x_2 trong hai Hình ít thay đổi. Điều đó chứng tỏ rằng, khi số anten tại nút S tăng lên tính bảo mật sẽ tốt hơn.

5. Kết luận

Trong nghiên cứu này, nhóm tác giả đã đưa ra mô hình truyền thông vô tuyến với kỹ thuật NOMA kết hợp với mảng anten và đánh giá vấn đề bảo mật vật lý trong mô hình. Nhóm tác giả đã phân tích từ lý thuyết đi đến một dạng công thức đơn giản hơn để thể hiện mối quan hệ giữa các đại lượng. Cuối cùng, tiến hành mô phỏng, đánh giá các kết quả đạt được, để từ đó thấy được sự đúng đắn của lý thuyết cũng như những vấn đề còn chưa đạt được khi đưa ra các giả thuyết để đơn giản trong tính toán. Nghiên cứu có thể là một tài liệu tham khảo cho những hướng nghiên cứu tiếp theo về các vấn đề liên quan đến bảo mật lớp vật lý và mảng anten.

TÀI LIỆU THAM KHẢO

- [1] J. G. Andrews et al., "What Will 5G Be?", *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065-1082, June 2014.
- [2] Y.-L. Tseng, "LTE-advanced enhancement for vehicular communication", *IEEE Wireless Commun.*, vol. 22, no. 6, pp. 4-7, Dec. 2015.
- [3] O. Maraqa, A. S. Rajasekaran, S. Al-Ahmadi, H. Yanikomeroglu and S. M. Sait, "A Survey of Rate-Optimal Power Domain NOMA

With Enabling Technologies of Future Wireless Networks", in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2192-2235, Fourthquarter 2020.

- [4] A. S. Marcano and H. L. Christiansen, "Performance of Non-Orthogonal Multiple Access (NOMA) in mmWave wireless communications for 5G networks", *2017 International Conference on Computing, Networking and Communications (ICNC)*, 2017, pp. 969-974.
- [5] T. E. A. Alharbi, K. Z. Shen and D. K. C. So, "Full-Duplex Cooperative Non-Orthogonal Multiple Access System with Feasible Successive Interference Cancellation", *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020, pp. 1-6.
- [6] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao and L. Hanzo, "Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access in Large-Scale Networks", in *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656-1672, March 2017
- [7] Yuanwei Liu, Zhiguo Ding, Yue Gao, and Maged Elkashlan, Zhijin Qin, "Physical Layer Security for 5G Non-orthogonal Multiple Access in Large-scale Networks", Queen Mary University of London, London, UK, 2016.
- [8] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming", *IEEE Trans. Signal Process.*, vol. 62, pp. 1850-1863, Apr. 2014.
- [9] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in mimo wiretap channels with imperfect CSI", *IEEE Trans. Signal Process.*, vol. 59, pp. 351-361, Jan. 2011.
- [10] Z. Sheng, H. D. Tuan, T. Q. Duong and H. V. Poor, "Beamforming Optimization for Physical Layer Security in MISO Wireless Networks", in *IEEE Transactions on Signal Processing*, vol. 66, no. 14, pp. 3710-3723, 15 July 2018.
- [11] E. Yaacoub and M. Al-Husseini, "Achieving physical layer security with massive MIMO beamforming", *2017 11th European Conference on Antennas and Propagation (EUCAP)*, 2017, pp. 1753-1757.
- [12] Ghous, Mujtaba, Ziaul H. Abbas, Ahmad K. Hassan, Ghulam Abbas, Thar Baker, and Dhiya Al-Jumeily. 2021. "Performance Analysis and Beamforming Design of a Secure Cooperative MISO-NOMA Network" *Sensors* 21, no. 12: 4180.
- [13] N. D. Anh and P. N. Son, "Performance Analysis and Evaluation of Underlay Two-Way Cooperative Networks with NOMA", *2020 5th International Conference on Green Technology and Sustainable Development (GTSD)*, 2020, pp. 103-108.
- [14] Constantine A. Balanis, *Antenna theory analysis and design, third edition*, Published by John Wiley & Sons, Inc, 2005.
- [15] B. C. Jung and S.-W. Jeon, S.-H. Lee, "Successive Interference Cancellation with Feedback for Random Access Networks", *IEEE Communications Letters.*, vol. 21, no. 4, pp. 825 - 828, 2017.
- [16] P. N. Son, V. P. Tuan, S. Park and H. Y. Kong, "Closed-form Analysis of a Decode-and-Forward Scheme under Physical Layer Security over General Fading Channels", *2018 5th NAFOSTED Conference on Information and Computer Science (NICS)*, 2018, pp. 1-5.
- [17] A. Hyadi, Z. Rezk and M. Alouini, "An Overview of Physical Layer Security in Wireless Communication Systems with CSIT Uncertainty", in *IEEE Access*, vol. 4, pp. 6121-6132, 2016.