

**BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ KỸ THUẬT
THÀNH PHỐ HỒ CHÍ MINH**

VÕ TÁ TÝ

**THIẾT KẾ MẠNG VÔ TUYẾN SỬ DỤNG
BỀ MẶT PHẢN XẠ THÔNG MINH
VỚI KỸ THUẬT TẠO NHIỄU NHÂN TẠO
NHẪM NÂNG CAO KHẢ NĂNG BẢO MẬT**

Chuyên ngành: Kỹ thuật điện tử
Mã số: 9520203

TÓM TẮT LUẬN ÁN TIẾN SĨ

TP. Hồ Chí Minh, tháng 4/2026

Công trình được hoàn thành tại
Trường Đại học Công nghệ Kỹ thuật TP. HCM

Người hướng dẫn khoa học 1: PGS. TS. Trần Trung Duy
Người hướng dẫn khoa học 2: PGS. TS. Phạm Ngọc Sơn

Luận án sẽ được bảo vệ trước Hội đồng đánh giá luận án Cấp chuyên
môn (khoa) họp tại Trường Đại học Công nghệ Kỹ thuật TP. HCM
vào ngày tháng năm 2026

MỞ ĐẦU

Động lực nghiên cứu

Trong những năm gần đây, sự phát triển mạnh mẽ của các hệ thống truyền thông vô tuyến đã đóng vai trò quan trọng trong việc thúc đẩy tăng trưởng kinh tế-xã hội và đáp ứng nhu cầu kết nối ngày càng gia tăng trong kỷ nguyên số. Các hệ thống thông tin di động liên tục được nâng cấp qua nhiều thế hệ nhằm đáp ứng các yêu cầu về dung lượng, tốc độ truyền dữ liệu, độ trễ thấp và khả năng kết nối quy mô lớn. Đặc biệt, với sự ra đời của mạng di động thứ năm (5G) và định hướng phát triển lên mạng di động thứ sáu (6G), các hệ thống truyền thông đang hướng tới môi trường truyền dẫn thông minh, có khả năng thích ứng linh hoạt và tối ưu hóa hiệu năng. Tuy nhiên, sự gia tăng nhanh chóng của các thiết bị không dây cùng với các ứng dụng như IoT, thực tế ảo/ thực tế ảo tăng cường, mạng cảm biến... đã đặt ra nhiều thách thức cho các mạng vô tuyến. Những thách thức này bao gồm việc sử dụng hiệu quả tài nguyên phổ tần, đảm bảo độ tin cậy của liên kết truyền dẫn, nâng cao hiệu quả năng lượng cũng như tăng cường khả năng bảo mật trong môi trường truyền thông ngày càng phức tạp. Do đó, nhiều công nghệ tiên tiến đã được nghiên cứu nhằm cải thiện hiệu năng tổng thể của hệ thống. Trong số đó, bảo mật lớp vật lý (PLS) nổi lên như một hướng tiếp cận hiệu quả nhằm đảm bảo an toàn thông tin trong các hệ thống vô tuyến. Khác với các phương pháp mã hóa truyền thống, PLS khai thác đặc tính ngẫu nhiên của kênh truyền để đảm bảo rằng chất lượng kênh hợp pháp tốt hơn so với kênh nghe lén, từ đó cho phép truyền thông tin một cách an toàn mà không cần các thuật toán mã hóa phức tạp. Bên cạnh đó, mặt phản xạ thông minh (IRS) được xem là một công nghệ đầy tiềm năng cho các hệ thống truyền thông thế hệ mới. Với khả năng điều khiển chủ động môi trường truyền sóng thông qua việc điều chỉnh pha và biên độ của các phần tử phản xạ, IRS giúp cải thiện đáng kể chất lượng kênh truyền và hiệu năng hệ thống. Tuy nhiên, do đặc tính quảng bá của kênh vô tuyến, tín hiệu truyền vẫn có thể bị đánh chặn bởi các thiết bị nghe lén. Trong bối cảnh đó, tạo nhiễu nhân tạo (AJ) được xem là một giải pháp hiệu quả nhằm làm suy giảm chất lượng kênh tại thiết bị nghe lén trong khi vẫn duy trì hiệu năng tại người dùng hợp pháp. Do đó, việc kết hợp IRS và AJ mở ra một hướng tiếp cận đầy tiềm năng nhằm đồng thời nâng cao chất lượng truyền dẫn và tăng cường khả năng bảo mật. Xuất phát từ những vấn đề trên, đề tài **“Thiết kế mạng vô tuyến sử dụng bề mặt phản xạ thông minh với kỹ thuật tạo nhiễu nhân tạo nhằm nâng cao khả năng bảo mật”** mang tính

cấp thiết, có ý nghĩa khoa học cao và phù hợp với xu thế phát triển của thời đại. Kết quả nghiên cứu góp phần bổ sung cơ sở lý thuyết cũng như có ý nghĩa thực tiễn vào bảo đảm an toàn cho các mạng vô tuyến thế hệ mới.

Các đóng góp của luận án

Thứ nhất, mô hình mạng vô tuyến thu hoạch năng lượng kết hợp IRS và AJ trên kênh pha-đỉnh Rayleigh được đề xuất. Các biểu thức giải tích cho xác suất dừng (OP), xác suất đánh chặn (IP), dung lượng bảo mật trung bình (ASC) và xác suất dừng bảo mật (SOP) được dẫn xuất và kiểm chứng bằng mô phỏng Monte Carlo đối với cả mô hình có và không có AJ. Kết quả cho thấy hệ thống đề xuất đạt hiệu năng bảo mật vượt trội so với cấu hình không sử dụng AJ. Bên cạnh đó, ảnh hưởng của các tham số hệ thống lên hiệu năng bảo mật cũng được đánh giá toàn diện, qua đó cung cấp các chỉ dẫn thiết kế quan trọng nhằm nâng cao bảo mật cho các mạng vô tuyến thế hệ mới.

Thứ hai, đề xuất mô hình mạng vô tuyến tích hợp IRS-AJ trên kênh pha-đỉnh Nakagami- m , ảnh hưởng của khử AJ không hoàn hảo cũng được đánh giá nhằm phản ánh linh hoạt điều kiện thực tế. Các biểu thức ASC và hiệu quả năng lượng bảo mật (SEE) được thiết lập cho cả mô hình có và không có AJ, cho thấy sự cải thiện đồng thời về bảo mật và hiệu quả năng lượng của mô hình đề xuất. Bên cạnh đó, thuật toán tìm kiếm theo tỷ lệ vàng (GSS) được áp dụng để xác định công suất gây nhiễu tối ưu. Ngoài ra, ảnh hưởng của các tham số hệ thống lên ASC và SEE cũng được đánh giá toàn diện, làm rõ cơ chế đánh đổi giữa bảo mật và hiệu quả năng lượng, đồng thời khẳng định ưu thế của mô hình đề xuất so với mô hình đối sánh.

Thứ ba, mô hình mạng vô tuyến đa người dùng sử dụng kỹ thuật đa truy nhập không trực giao (NOMA) kết hợp IRS và AJ được đề xuất trên kênh pha-đỉnh Rayleigh, xét cả trường hợp khử giao thoa nối tiếp hoàn hảo pSIC và khử giao thoa nối tiếp không hoàn hảo (ipSIC), cũng như đánh giá ảnh hưởng của khử AJ không hoàn hảo. Các biểu thức tường minh cho ASC, SOP và SEE được dẫn xuất và kiểm chứng bằng mô phỏng Monte Carlo cho các kịch bản có và không có AJ. Kết quả cho thấy hệ thống đề xuất đạt hiệu năng bảo mật vượt trội so với các mô hình đối sánh như IRS-NOMA-không sử dụng AJ (Non Jammer), nút chuyển tiếp (Relay)-Jammer-NOMA, IRS-Jammer-đa truy nhập trực giao (OMA). Bên cạnh đó, ảnh hưởng của các tham số hệ thống lên hiệu năng bảo mật cũng được đánh giá toàn diện, qua đó rút ra các nguyên tắc thiết kế và khẳng định tính khả thi của mô hình trong các mạng vô tuyến đa người dùng thế hệ mới.

Chương 1: Tổng quan về vấn đề nghiên cứu

Trong những năm gần đây, PLS được xem là giải pháp hiệu quả nhằm nâng cao bảo mật cho các hệ thống vô tuyến 5G/6G. Bên cạnh đó, IRS cho phép điều khiển môi trường truyền dẫn nhằm tăng cường tín hiệu hợp pháp và suy giảm tín hiệu tại thiết bị nghe lén, trong khi AJ đóng vai trò làm suy giảm khả năng đánh chặn của thiết bị nghe lén. Tuy nhiên, các nghiên cứu hiện tại chủ yếu xem xét IRS hoặc AJ một cách độc lập, trong khi các công trình kết hợp đồng thời hai kỹ thuật này vẫn còn hạn chế ở các công trình quốc tế cũng như trong nước. Do đó, việc nghiên cứu PLS tích hợp IRS và AJ là cần thiết nhằm khai thác hiệu quả tiềm năng của chúng và nâng cao hiệu năng bảo mật trong các mạng vô tuyến thế hệ mới.

Chương 2: Cơ sở lý thuyết

Chương 2 trình bày các kiến thức nền tảng về PLS và các tham số đánh giá hiệu năng cơ bản như đánh đổi OP-IP, ASC, SOP. Ngoài ra, chương cũng giới thiệu tổng quan về IRS, AJ, cùng các lý thuyết cơ bản liên quan đến thu hoạch năng lượng (RF-EH) và NOMA.

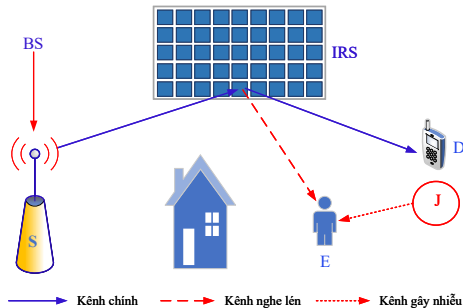
Chương 3: Phân tích bảo mật cho mạng vô tuyến thu hoạch năng lượng sử dụng IRS và AJ

3.1. Giới thiệu

Nội dung của Chương 3 được công bố trong công trình J1

Vo Ta Ty, Pham Ngoc Son, Tran Trung Duy, “Secrecy performance of RIS-assisted wireless-powered systems with artificial-jamming generation,” *Physical Communication* (SCIE, Q2), vol. 69, 102592, Jan. 2025.

3.2. Mô hình hệ thống



Hình 3.1: Mô hình hệ thống.

Mô hình mạng vô tuyến thu hoạch năng lượng tích hợp IRS và AJ được minh họa trong Hình 3.1. Trong đó nguồn phát (S) được cấp năng lượng thông qua thu hoạch từ trạm gốc và truyền tín hiệu tới thiết bị đích (D) thông qua IRS gồm L phần tử phản xạ thụ động. Do thiết bị nghe lén (E) có thể thu tín hiệu phản xạ từ IRS, một nút gây nhiễu (J) được triển khai nhằm làm suy giảm chất lượng tín hiệu tại E. Toàn bộ các nút đều sử dụng một ăng-ten và các kênh được mô hình hóa theo pha-đỉnh Rayleigh.

Trên cơ sở mô hình hệ thống, Luận án xác định được biểu thức tín hiệu thu tại D và E. Từ đó, tìm ra biểu thức SNR, làm cơ sở xác định các biểu thức phân tích phẩm chất bảo mật của hệ thống.

3.3. Phân tích hiệu năng bảo mật

3.3.1. Xác suất dừng và xác suất đánh chặn

Các biểu thức tường minh của OP và IP đối với mô hình đề xuất và mô hình không sử dụng AJ được xác định lần lượt như sau

$$OP = 1 - \sum_{n=1}^N v_n \Gamma(\theta, \Omega_D \sqrt{\gamma_{th}}). \quad (3.1)$$

$$IP = \sum_{n=1}^N \varepsilon_n \Gamma(\theta, \Omega_E \sqrt{\gamma_{th}}). \quad (3.2)$$

$$OP^{NJ} = 1 - \sum_{n=1}^N v_n \Gamma(\theta, \Omega_D^{NJ} \sqrt{\gamma_{th}}), \quad (3.3)$$

$$IP^{NJ} = \sum_{n=1}^N v_n \Gamma(\theta, \Omega_E^{NJ} \sqrt{\gamma_{th}}). \quad (3.4)$$

3.3.2. Dung lượng bảo mật trung bình

Giá trị ASC của mô hình đề xuất và mô hình không sử dụng AJ được biểu diễn lần lượt là

$$ASC = \frac{(1 - \alpha)}{\ln 2} \frac{(2^\theta - 1)}{\sqrt{\pi}} \left[\sum_{n=1}^N v_n G_{3,5}^{5,1} \left(\frac{\Omega_D^2}{4} \middle| \begin{matrix} 0, \frac{1}{2}, 1 \\ \frac{\theta}{2}, \frac{\theta+1}{2}, 0, \frac{1}{2}, 0 \end{matrix} \right) - \sum_{n=1}^N \varepsilon_n G_{3,5}^{5,1} \left(\frac{\Omega_E^2}{4} \middle| \begin{matrix} 0, \frac{1}{2}, 1 \\ \frac{\theta}{2}, \frac{\theta+1}{2}, 0, \frac{1}{2}, 0 \end{matrix} \right) \right]. \quad (3.5)$$

$$\text{ASC}^{\text{NJ}} = \frac{(1-\alpha)(2^\theta-1)}{\ln 2} \frac{\sum_{n=1}^N v_n}{\sqrt{\pi}} \left[G_{3,5}^{5,1} \left(\frac{(\Omega_{\text{D}}^{\text{NJ}})^2}{4} \middle| \begin{matrix} 0, \frac{1}{2}, 1 \\ \frac{\theta}{2}, \frac{\theta+1}{2}, 0, \frac{1}{2}, 0 \end{matrix} \right) - G_{3,5}^{5,1} \left(\frac{(\Omega_{\text{E}}^{\text{NJ}})^2}{4} \middle| \begin{matrix} 0, \frac{1}{2}, 1 \\ \frac{\theta}{2}, \frac{\theta+1}{2}, 0, \frac{1}{2}, 0 \end{matrix} \right) \right]. \quad (3.6)$$

3.3.3. Xác suất dừng bảo mật

Biểu thức SOP của mô hình đề xuất và mô hình không sử dụng AJ được xác định lần lượt như sau

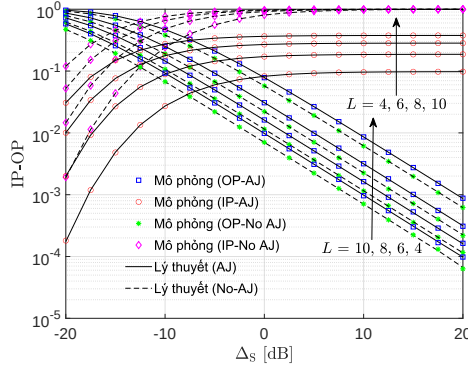
$$\text{SOP} = 1 - \sum_{m=1}^M \sum_{n=1}^N \sum_{q=1}^Q \frac{\pi^2 \xi_m \sqrt{1-y_n^2} \sqrt{1-y_q^2}}{4NQ\Gamma(\theta)} \left[\ln \left(\frac{2}{1+y_q} \right) \right]^{\theta-1} \times \Gamma \left(\theta, \frac{1}{\phi_{\text{D}}} \sqrt{\frac{[\ln(2/(1+y_q))]^2}{(\Phi_{\text{E}})^2} + \frac{\kappa \lambda_{\text{BS}}}{\ln(2/(1+y_n))}} \right). \quad (3.7)$$

$$\text{SOP}^{\text{NJ}} = 1 - \sum_{n=1}^N \sum_{m=1}^M \frac{\pi^2 \sqrt{1-y_n^2} \sqrt{1-y_m^2}}{4NM[\Gamma(\theta)]^2} \left[\ln \left(\frac{2}{1+y_n} \right) \right]^{\theta-1} \times \Gamma \left(\theta, \frac{1}{\phi_{\text{D}}} \sqrt{\rho_{\text{th}}(\phi_{\text{E}})^2 \left[\ln \left(\frac{2}{1+y_n} \right) \right]^2 + \frac{\kappa \lambda_{\text{BS}}}{\ln(2/(1+y_m))}} \right). \quad (3.8)$$

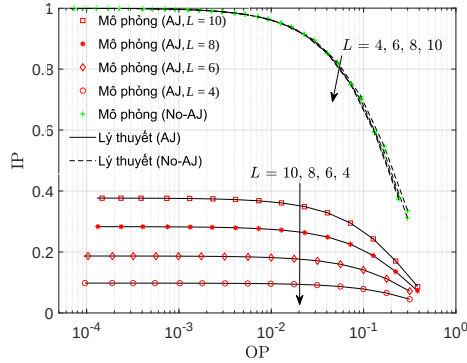
3.4. Kết quả mô phỏng

Trong phần này, phẩm chất hệ thống được đánh giá thông qua kết quả tính toán số kết hợp với mô phỏng Monte Carlo nhằm xác nhận tính đúng đắn của các kết quả phân tích. Để đảm bảo tính công bằng trong so sánh, công suất phát của hệ thống không sử dụng AJ là: $P_{\text{S}}^{\text{NJ}} = P_{\text{BS}} + P_{\text{I}} = (1+\mu)P_{\text{BS}}$.

Kết quả từ Hình 3.2 cho thấy khi Δ_{S} tăng, OP được cải thiện trong khi IP suy giảm, phản ánh sự đánh đổi giữa độ tin cậy và bảo mật do dung lượng của cả kênh dữ liệu và kênh nghe lén cùng tăng. Khi L tăng, OP tiếp tục cải thiện nhưng IP xấu đi, cho thấy sự đánh đổi theo L . So với mô hình không sử dụng AJ, hệ thống đề xuất có OP cao hơn không đáng kể nhưng IP được cải thiện, đặc biệt trong miền Δ_{S} cao. Ngoài ra, trong miền SNR cao, IP của hệ thống đề xuất hội tụ về một giá trị trần và không còn phụ thuộc vào Δ_{S} , cho phép cải thiện OP mà hầu như không làm suy giảm hiệu năng bảo mật.



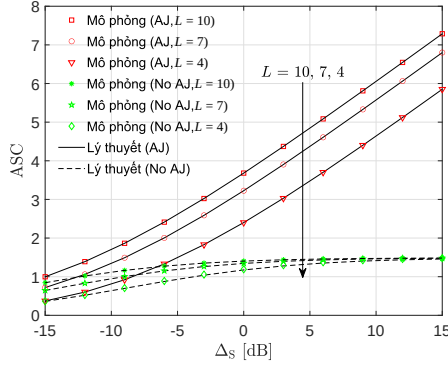
Hình 3.2: IP và OP theo Δ_S với $y_E = -0.5$, $\mu = 0.4$ và $\alpha = 0.5$.



Hình 3.3: Đánh đổi OP-IP với $y_E = -0.5$, $\mu = 0.4$ và $\alpha = 0.5$.

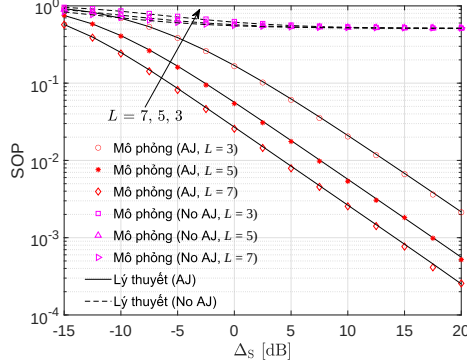
Hình 3.3 cho thấy IP tăng khi OP giảm, phản ánh rõ sự đánh đổi giữa độ tin cậy và bảo mật. Trong hệ thống đề xuất, tại miền OP thấp, IP hội tụ về giá trị bão hòa do đạt giới hạn trong miền SNR cao. So với hệ thống không sử dụng AJ, hệ thống đề xuất đạt IP thấp hơn đáng kể tại cùng một mức OP, cho thấy hiệu quả của mô hình đề xuất. Đồng thời, khi L tăng, sự đánh đổi OP-IP trong hệ thống đề xuất trở nên rõ rệt hơn, trong khi hệ thống không gây nhiều thay đổi không đáng kể.

Kết quả từ hình 3.4 cho thấy ASC của cả hai hệ thống tăng khi Δ_S và L tăng. Đáng chú ý, mô hình đề xuất luôn đạt ASC cao hơn so với mô hình



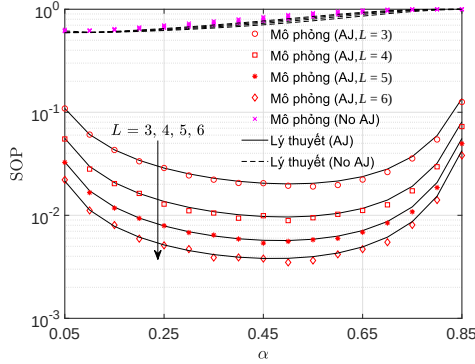
Hình 3.4: ASC theo Δ_S với $y_E = -0.5$, $\mu = 0.3$ và $\alpha = 0.25$.

không sử dụng AJ. Trong miền SNR cao, ASC của hệ thống đề xuất tiếp tục tăng, trong khi hệ thống không có AJ đạt trạng thái bão hòa do dung lượng chỉ phụ thuộc vào các liên kết qua IRS và không còn phụ thuộc vào Δ_S .



Hình 3.5: SOP theo Δ_S với $y_E = -0.4$, $\mu = 0.3$ và $\alpha = 0.4$.

Hình 3.5 cho thấy SOP giảm khi Δ_S và L tăng. Hệ thống đề xuất đạt hiệu năng vượt trội so với hệ thống không sử dụng AJ, đặc biệt trong miền SNR trung bình và cao. Trong miền SNR cao, SOP của hệ thống không có AJ đạt bão hòa, trong khi hệ thống đề xuất tiếp tục cải thiện nhờ tác động của bộ gây nhiễu. Đồng thời, khi L tăng, SOP của hệ thống đề xuất giảm đáng kể, còn hệ thống không gây nhiễu chỉ cải thiện nhẹ.



Hình 3.6: Ảnh hưởng của α lên SOP

Kết quả từ hình 3.6 cho thấy SOP của hệ thống đề xuất luôn tốt hơn so với hệ thống không sử dụng AJ. Đồng thời, tồn tại một giá trị tối ưu của α giúp hệ thống đạt hiệu năng bảo mật tốt nhất.

3.5. Kết luận

Chương 3 đề xuất mô hình mạng vô tuyến kết hợp RF-EH, IRS và AJ nhằm nâng cao hiệu năng bảo mật. Các biểu thức tường minh cho OP, IP, ASC và SOP được dẫn xuất và kiểm chứng bằng mô phỏng, đồng thời so sánh với cấu hình không sử dụng AJ. Kết quả cho thấy hệ thống đề xuất cải thiện đáng kể hiệu năng bảo mật, trong khi cấu hình đối sánh có IP cao và bão hòa ở miền SNR lớn, khẳng định hiệu quả của việc kết hợp IRS, AJ và RF-EH. Tuy nhiên, mô hình vẫn chưa xem xét khứ AJ không hoàn hảo và D, E có thể nhận được cả tín hiệu từ S. Do đó, Chương 4 mở rộng sang kịch bản tổng quát hơn với triệt nhiễu không hoàn hảo, tồn tại đường truyền trực tiếp và kênh pha-đỉnh Nakagami- m nhằm đánh giá sát thực tế hơn.

Chương 4: Phân tích dung lượng bảo mật và hiệu quả năng lượng cho mạng vô tuyến sử dụng IRS và AJ dựa trên MRC

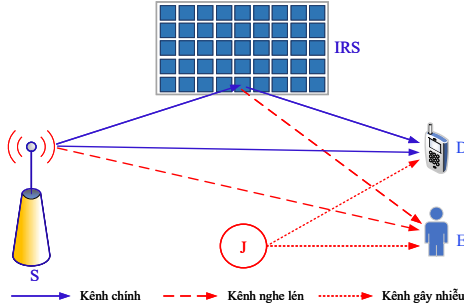
4.1. Giới thiệu

Nội dung của Chương 4 được công bố trong công trình J3

Vo Ta Ty, Tran Trung Duy, Tran Manh Hoang, Pham Ngoc Son, “Enhancing average secrecy capacity and secure energy efficiency of SISO system using RIS with artificial jamming over Nakagami- m fading channels,” *REV Journal on Electronics and Communications*, vol. 15, no. 3, Jul. 2025.

4.2. Mô hình hệ thống

Bảo mật thông tin cho mạng vô tuyến với sự hỗ trợ của IRS và AJ được minh họa trong Hình 4.1.



Hình 4.1: Mô hình hệ thống

Mô hình xem xét mạng vô tuyến tích hợp IRS và AJ, trong đó tín hiệu từ S đến D và E được truyền qua cả đường trực tiếp và đường phản xạ qua IRS. Để tăng cường bảo mật, một bộ gây nhiễu được triển khai nhằm làm suy giảm khả năng đánh chặn của E, đồng thời xem xét khả năng triệt nhiễu không hoàn hảo tại D nhằm phản ánh sát điều kiện thực tế. Ngoài ra, tất cả các nút đều sử dụng một ăng-ten.

Trên cơ sở mô hình hệ thống, Luận án xác định được biểu thức tín hiệu thu tại D và E. Từ đó, xác định được biểu thức SNR, làm cơ sở để phân tích phẩm chất bảo mật và SEE của hệ thống.

4.3. Phân tích hiệu năng bảo mật

4.3.1. Dung lượng bảo mật trung bình

ASC của mô hình đề xuất và mô hình không sử dụng AJ được biểu diễn lần lượt như sau

$$\begin{aligned} \text{ASC} = & \frac{1}{\ln 2} \sum_{n=1}^N \sum_{m=1}^M \varepsilon_n \varepsilon_m \Gamma\left(\omega_1, \phi_1 \sqrt{\frac{A_D}{P_S} \frac{1 - v_m}{1 + v_m}}\right) \\ & - \frac{1}{\ln 2} \sum_{w=1}^W \sum_{q=1}^Q \varepsilon_w \varepsilon_q \Gamma\left(\omega_2, \phi_2 \sqrt{\frac{A_E}{P_S} \frac{1 - v_q}{1 + v_q}}\right). \end{aligned} \quad (4.1)$$

$$\begin{aligned} \text{ASC}^{\text{NJ}} = & \frac{1}{\ln 2} \frac{1}{\Gamma(\omega_1)} \varepsilon_{k_1} \Gamma\left(\omega_1, \phi_1 \sqrt{\frac{\delta_D^2}{P_S^{\text{NJ}}} \frac{1 - v_{k_1}}{1 + v_{k_1}}}\right) \\ & - \frac{1}{\ln 2} \frac{1}{\Gamma(\omega_2)} \varepsilon_{k_2} \Gamma\left(\omega_2, \phi_2 \sqrt{\frac{\delta_D^2}{P_S^{\text{NJ}}} \frac{1 - v_{k_2}}{1 + v_{k_2}}}\right). \end{aligned} \quad (4.2)$$

4.3.2. Hiệu quả năng lượng bảo mật

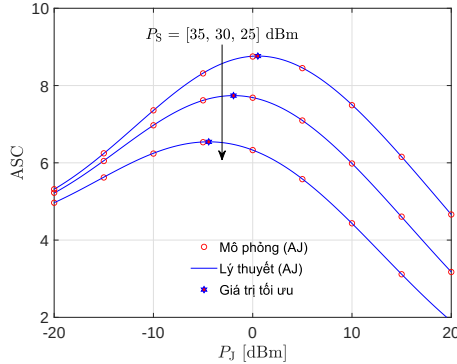
Công thức tính SEE của mô hình đề xuất và mô hình không sử dụng AJ được biểu diễn như sau

$$\eta = \frac{R_{\text{sec}}}{P_i}, \quad (4.3)$$

trong đó R_{sec} là tốc độ bảo mật của hệ thống. Tốc độ bảo mật của hệ thống đề xuất cũng như hệ thống không sử dụng AJ được xác định tương ứng từ (4.1) và (4.2). $P_i \in \{P_{\text{tol}}, P_{\text{tol}}^{\text{NJ}}\}$ biểu diễn tổng công suất tiêu thụ.

4.4. Kết quả mô phỏng

Trong phần này, phẩm chất hệ thống được đánh giá dựa trên các kết quả tính toán số kết hợp với mô phỏng Monte Carlo nhằm kiểm chứng tính chính xác của các phân tích lý thuyết. Để đảm bảo tính công bằng trong so sánh, công suất phát của hệ thống không sử dụng AJ là: $P_S^{\text{NJ}} = P_S + P_J = (1 + \mu)P_S$.



Hình 4.2: ASC theo P_J với $P_S = 25, 30, 35$ dBm, $f_c = 3$ GHz và $L = 40$.

Kết quả từ Hình 4.2 cho thấy ASC tăng theo P_J ở giai đoạn đầu, đạt cực đại tại một giá trị tối ưu, sau đó giảm do ảnh hưởng của AJ lên cả E và D. Ngoài ra, tồn tại giá trị P_J tối ưu để tối đa hóa ASC, được xác định hiệu quả bằng thuật toán GSS được thể hiện như Bảng 1. Kết quả cung cấp cơ sở quan

Bảng 1: Thuật toán tối ưu nhằm xác định P_J^*

Đầu vào: Thiết lập $P_{J_{\min}} = -20$ dBm, $P_{J_{\max}} = 20$ dBm, hệ số tìm kiếm vàng $\omega = \frac{\sqrt{5}-1}{2}$ và ngưỡng dừng $\delta = 10^{-3}$.

Đầu ra: Giá trị tối ưu P_J^* để ASC đạt cực đại.

Bắt đầu:

1. Xây dựng các điểm $\epsilon_1 = P_{J_{\min}} + (P_{J_{\max}} - P_{J_{\min}})\omega$ và $\epsilon_2 = P_{J_{\max}} - (P_{J_{\max}} - P_{J_{\min}})\omega$.

2. **Trong khi** $P_{J_{\max}} - P_{J_{\min}} \geq \delta$ **thì thực hiện**

Cập nhật: ASC(ϵ_1).

Cập nhật: ASC(ϵ_2).

Nếu ASC(ϵ_2) > ASC(ϵ_1) **thì**

Cập nhật: $P_{J_{\min}} \leftarrow \epsilon_1$.

Ngược lại

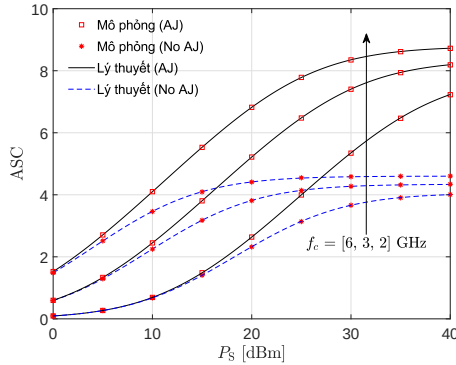
Cập nhật: $P_{J_{\max}} \leftarrow \epsilon_2$.

Kết thúc nếu.

3. **Kết thúc vòng lặp.**

4. Trả về $P_J^* = \frac{P_{J_{\max}} + P_{J_{\min}}}{2}$.

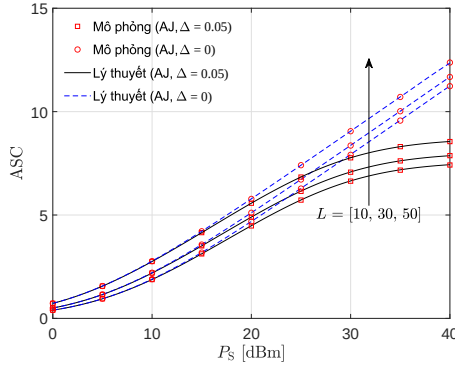
Kết thúc.



Hình 4.3: Ảnh hưởng của f_c lên ASC.

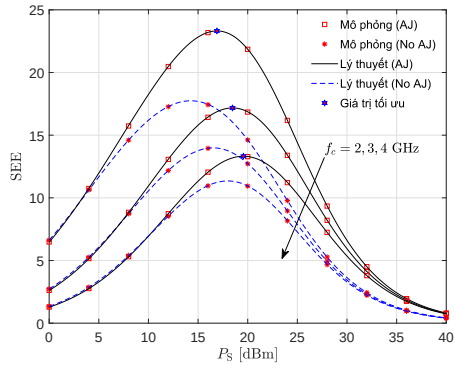
trọng cho thiết kế hệ thống nhằm cân bằng giữa hiệu năng bảo mật và SEE.

Hình 4.3 cho thấy ASC suy giảm khi tần số sóng mang f_c tăng. Bên cạnh đó, hệ thống đề xuất luôn đạt ASC cao hơn đáng kể so với hệ thống không sử dụng AJ trong toàn bộ dải tần số, khẳng định hiệu quả của AJ trong việc nâng cao bảo mật.



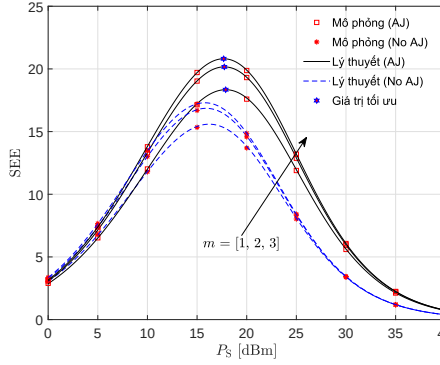
Hình 4.4: Ảnh hưởng của Δ đến ASC.

Kết quả từ Hình 4.4 cho thấy hiệu quả khử AJ ảnh hưởng rõ rệt đến ASC. Khi P_S nhỏ, sự khác biệt giữa khử nhiễu lý tưởng và không lý tưởng là không đáng kể, nhưng ở miền công suất lớn, khử nhiễu lý tưởng mang lại ASC cao hơn rõ rệt. Nguyên nhân là do P_J tăng theo P_S , làm suy giảm hiệu năng tại người dùng hợp pháp trong trường hợp khử nhiễu không hoàn hảo. Điều này khẳng định vai trò quan trọng của kỹ thuật khử nhiễu trong việc nâng cao hiệu năng bảo mật của hệ thống.



Hình 4.5: SEE theo P_S với $f_c = 2, 3, 4$ GHz và $L = 30$.

Hình 4.5 cho thấy SEE của hai hệ thống gần như tương đương ở miền công suất thấp, nhưng hệ thống đề xuất vượt trội rõ rệt khi P_S lớn. Đồng thời,



Hình 4.6: Ảnh hưởng của tham số m lên SEE.

với mỗi f_c tồn tại một giá trị P_S tối ưu để tối đa hóa SEE. Ngoài ra, SEE giảm khi f_c tăng tương tự như kết quả trong Hình 4.3.

Kết quả từ Hình 4.6 cho thấy m ảnh hưởng đáng kể đến SEE và ứng với mỗi m đều tồn tại một giá trị P_S tối ưu để tối đa hóa SEE. Đồng thời, hệ thống đề xuất luôn đạt SEE cao hơn so với hệ thống không sử dụng AJ.

Kết luận

Chương 4 đề xuất mô hình IRS-AJ nhằm nâng cao bảo mật cho mạng vô tuyến dưới sự hiện diện của thiết bị nghe lén. Các biểu thức tường minh cho ASC và SEE được xây dựng và kiểm chứng bằng mô phỏng, cho thấy hệ thống đề xuất đạt hiệu năng vượt trội so với cấu hình không gây nhiễu. Tuy nhiên, Chương 4 chỉ xét kịch bản đơn người dùng. Do đó, Chương 5 mở rộng sang hệ thống đa người dùng sử dụng kỹ thuật NOMA kết hợp IRS và AJ, đồng thời xem xét các trường hợp ipSIC cũng như khử AJ không hoàn hảo tại các người dùng hợp pháp nhằm đánh giá toàn diện hiệu năng bảo mật.

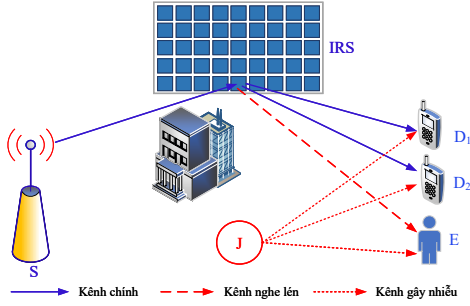
Chương 5: Phân tích mạng vô tuyến đa người dùng bảo mật sử dụng NOMA kết hợp với IRS và AJ

5.1. Giới thiệu

Nội dung của Chương 5 được công bố trong công trình J2

Vo Ta Ty, Tran Trung Duy, Pham Ngoc Son, “Enhancing the secrecy performance and secure energy efficiency of NOMA systems using RIS with artificial jamming,” *International Journal of Communication Systems* (SCIE, Q2), vol. 39, no. 7, p.e70474, Mar. 2026.

5.2. Mô hình hệ thống



Hình 5.1: Mô hình hệ thống.

Mô hình hệ thống IRS-Jammer-NOMA gồm S, J, IRS với L phần tử, hai người dùng D_1 , D_2 và E. Khả năng triệt nhiễu không hoàn hảo và ipSIC cũng được xem xét. Ngoài ra, tất cả các nút đều sử dụng một ăng-ten.

Trên cơ sở mô hình hệ thống, Luận án xác định được biểu thức tín hiệu thu tại D_1 , D_2 và E. Từ đó, xác định được biểu thức SINR, làm cơ sở để phân tích phẩm chất bảo mật của hệ thống.

5.3. Phân tích hiệu năng bảo mật

5.3.1. Dung lượng bảo mật trung bình

Giá trị ASC của mô hình đề xuất và mô hình không sử dụng AJ được biểu diễn là

$$\begin{aligned} \text{ASC}^{x_1} = & \frac{1}{\ln 2} \sum_{n=1}^N \sum_{u_1=1}^{U_1} \xi_n \xi_{u_1} \Gamma\left(\theta, \frac{\omega_{D_1}}{\sqrt{\alpha_2 P_S}} \sqrt{\frac{1+v_{u_1}}{1-v_{u_1}}}\right) \\ & - \frac{1}{\ln 2} \sum_{q=1}^Q \sum_{u_2=1}^{U_2} \xi_q \xi_{u_2} \Gamma\left(\theta, \frac{\omega_E}{\sqrt{\alpha_1 P_S}} \sqrt{\frac{1-v_{u_2}}{1+v_{u_2}}}\right). \end{aligned} \quad (5.1)$$

$$\begin{aligned}
\text{ASC}_{\text{ipSIC}}^{x_2} &= \frac{1}{\ln 2} \sum_{m=1}^M \sum_{u_{31}=1}^{U_{31}} \xi_m \xi_{u_{31}} \Gamma(\theta, \omega_{D_1^1} \sqrt{\frac{\varphi_{v_{u_{31}}}}{P_S(\alpha_2 - \varphi_{u_{31}} \alpha_1 \rho)}}) \\
&+ \frac{1}{\ln 2} \sum_{k=1}^K \sum_{u_{41}=1}^{U_{41}} \xi_k \xi_{u_{41}} \Gamma\left(\theta, \omega_{D_2^2} \sqrt{\frac{\varphi_{v_{u_{41}}}}{P_S(\alpha_1 - \varphi_{v_{u_{41}}} \alpha_2)}}\right) \\
&- \frac{1}{\ln 2} \sum_{q=1}^Q \sum_{u_2=1}^{U_2} \xi_q \xi_{u_2} \Gamma\left(\theta, \frac{\omega_E}{\sqrt{\alpha_2 P_S}} \sqrt{\frac{1 - v_{u_2}}{1 + v_{u_2}}}\right). \tag{5.2}
\end{aligned}$$

$$\begin{aligned}
\text{ASC}_{x_1}^{\text{NJ}} &= \frac{1}{\ln 2} \sum_{w_1=1}^{W_1} \xi_{w_1} \Gamma\left(\theta, \frac{\delta_{D_1}}{\phi_{D_1} \sqrt{\alpha_2 P_S^{\text{NJ}}}} \sqrt{\frac{1 + v_{w_1}}{1 - v_{w_1}}}\right) \\
&- \frac{1}{\ln 2} \sum_{w_2=1}^{W_2} \xi_{w_2} \Gamma\left(\theta, \frac{\delta_E}{\phi_E \sqrt{\alpha_1 P_S^{\text{NJ}}}} \sqrt{\frac{1 - v_{w_2}}{1 + v_{w_2}}}\right). \tag{5.3}
\end{aligned}$$

$$\begin{aligned}
\text{ASC}_{x_2}^{\text{NJ-ipSIC}} &= \frac{1}{\ln 2} \sum_{w_{31}=1}^{W_{31}} \xi_{w_{31}} \Gamma\left(\theta, \frac{\delta_{D_2}}{\phi_{D_2}} \sqrt{\frac{\varphi_{v_{w_{31}}}}{P_S^{\text{NJ}}(\alpha_2 - \alpha_1 \rho \varphi_{v_{w_{31}}})}}\right) \\
&+ \frac{1}{\ln 2} \sum_{w_{41}=1}^{W_{41}} \xi_{w_{41}} \Gamma\left(\theta, \frac{\delta_{D_2}}{\phi_{D_2}} \sqrt{\frac{\varphi_{v_{w_{41}}}}{P_S^{\text{NJ}}(\alpha_1 - \varphi_{v_{w_{41}}} \alpha_2)}}\right) \\
&- \frac{1}{\ln 2} \sum_{w_2=1}^{W_2} \xi_{w_2} \Gamma\left(\theta, \frac{\delta_E}{\phi_E \sqrt{\alpha_2 P_S^{\text{NJ}}}} \sqrt{\frac{1 - v_{w_2}}{1 + v_{w_2}}}\right). \tag{5.4}
\end{aligned}$$

5.3.2. Xác suất dừng bảo mật

Giá trị SOP của mô hình đề xuất và mô hình không sử dụng AJ được biểu diễn lần lượt như sau

$$\begin{aligned}
\text{SOP}^{x_1} &= 1 - \left[\sum_{n=1}^N \sum_{q=1}^Q \sum_{b_1=1}^{B_1} \xi_n \xi_q \xi_{b_1} \frac{A_{E_1}^\theta}{2} \mathcal{U}_{b_1}^{\frac{\theta}{2}-1} \exp(-A_{E_1} \sqrt{\mathcal{U}_{b_1}}) \right. \\
&\times \left. \Gamma\left(\theta, \omega_{D_1} \sqrt{\frac{2^{\mathcal{R}^{x_1}} \mathcal{U}_{b_1} + 2^{\mathcal{R}^{x_1}} - 1}{P_S(\alpha_1 - \alpha_2(2^{\mathcal{R}^{x_1}} \mathcal{U}_{b_1} + 2^{\mathcal{R}^{x_1}} - 1))}}\right) \right]. \tag{5.5}
\end{aligned}$$

$$\begin{aligned}
\text{SOP}_{\text{ipSIC}}^{x_2} = & 1 - \left[\sum_{m=1}^M \sum_{q=1}^Q \sum_{b_{21}=1}^{B_{21}} \xi_m \xi_q \xi_{b_{21}} \frac{A_{\text{E}_2}^\theta}{2} \mathcal{U}_{b_{21}}^{\frac{\theta}{2}-1} \exp(-A_{\text{E}_2} \sqrt{\mathcal{U}_{b_{21}}}) \right. \\
& \times \Gamma \left(\theta, \omega_{\text{D}_2^1} \sqrt{\frac{2\mathcal{R}^{x_2} \mathcal{U}_{b_{21}} + 2\mathcal{R}^{x_2} - 1}{P_{\text{S}}(\alpha_2 - \alpha_1 \rho (2\mathcal{R}^{x_2} \mathcal{U}_{b_{21}} + 2\mathcal{R}^{x_2} - 1))}} \right) \\
& + \sum_{k=1}^K \sum_{q=1}^Q \sum_{b_{31}=1}^{B_{31}} \xi_k \xi_q \xi_{b_{31}} \frac{A_{\text{E}_2}^\theta}{2} \mathcal{U}_{b_{31}}^{\frac{\theta}{2}-1} \exp(-A_{\text{E}_2} \sqrt{\mathcal{U}_{b_{31}}}) \\
& \left. \times \Gamma \left(\theta, \omega_{\text{D}_2^2} \sqrt{\frac{2\mathcal{R}^{x_2} \mathcal{U}_{b_{31}} + 2\mathcal{R}^{x_2} - 1}{P_{\text{S}}(\alpha_1 - \alpha_2 (2\mathcal{R}^{x_2} \mathcal{U}_{b_{31}} + 2\mathcal{R}^{x_2} - 1))}} \right) \right]. \quad (5.6)
\end{aligned}$$

$$\begin{aligned}
\text{SOP}_{x_1}^{\text{NJ}} = & 1 - \left[\sum_{b_4=1}^{B_4} \xi_{b_4} \frac{(A_{\text{E}_1}^{\text{NJ}})^\theta}{2} \mathcal{U}_{b_4}^{\frac{\theta}{2}-1} \exp(-A_{\text{E}_1}^{\text{NJ}} \sqrt{\mathcal{U}_{b_4}}) \right. \\
& \left. \times \Gamma \left(\theta, \frac{1}{\phi_{\text{D}_1}} \sqrt{\frac{(2\mathcal{R}^{x_1} \mathcal{U}_{b_4} + 2\mathcal{R}^{x_1} - 1) \delta_{\text{D}_1}^2}{P_{\text{S}}(\alpha_1 - \alpha_2 (2\mathcal{R}^{x_1} \mathcal{U}_{b_4} + 2\mathcal{R}^{x_1} - 1))}} \right) \right]. \quad (5.7)
\end{aligned}$$

$$\begin{aligned}
\text{SOP}_{x_2}^{\text{NJ-ipSIC}} = & 1 - \left[\sum_{b_{51}=1}^{B_{51}} \xi_{b_{51}} \frac{(A_{\text{E}_2}^{\text{NJ}})^\theta}{2} \mathcal{U}_{b_{51}}^{\frac{\theta}{2}-1} \exp(-A_{\text{E}_2}^{\text{NJ}} \sqrt{\mathcal{U}_{b_{51}}}) \right. \\
& \times \Gamma \left(\theta, \frac{1}{\phi_{\text{D}_2}} \sqrt{\frac{A_{b_{51}} \delta_{\text{D}_2}^2}{P_{\text{S}}(\alpha_2 - \alpha_1 \rho A_{b_{51}})}} \right) \\
& + \sum_{b_{61}=1}^{B_{61}} \xi_{b_{61}} \frac{(A_{\text{E}_2}^{\text{NJ}})^\theta}{2} \mathcal{U}_{b_{61}}^{\frac{\theta}{2}-1} \exp(-A_{\text{E}_2}^{\text{NJ}} \sqrt{\mathcal{U}_{b_{61}}}) \\
& \left. \times \Gamma \left(\theta, \frac{1}{\phi_{\text{D}_2}} \sqrt{\frac{A_{b_{61}} \delta_{\text{D}_2}^2}{P_{\text{S}}(\alpha_1 - \alpha_2 A_{b_{61}})}} \right) \right]. \quad (5.8)
\end{aligned}$$

5.3.3. Hiệu quả năng lượng bảo mật

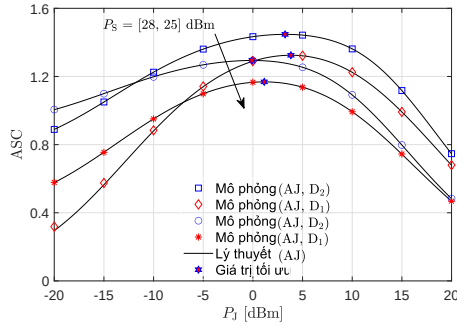
Công thức tính SEE của mô hình đề xuất và mô hình không sử dụng AJ được thể hiện như sau

$$\eta = \frac{R_{\text{sec}}}{P_i}, \quad (5.9)$$

trong đó tốc độ bảo mật của hệ thống đề xuất cũng như hệ thống không sử dụng AJ được xác định tương ứng từ (5.1)-(5.4).

5.4. Kết quả mô phỏng

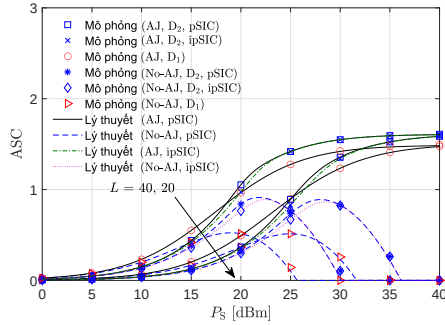
Trong phần này, hiệu năng hệ thống được đánh giá dựa trên các kết quả phân tích số, đồng thời được xác minh thông qua mô phỏng Monte Carlo nhằm đảm bảo tính nhất quán giữa phân tích lý thuyết và mô phỏng. Để đảm bảo tính công bằng trong so sánh, công suất phát của hệ thống không sử dụng AJ là: $P_S^{\text{NJ}} = P_S + P_J = (1 + \mu)P_S$.



Hình 5.2: ASC theo P_J với $P_S = 25, 28$ dBm, $L = 30$ và $\rho = 0$.

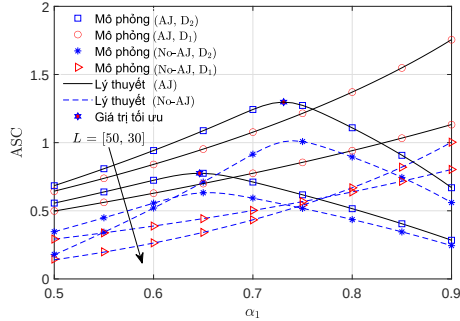
Kết quả từ Hình 5.2 cho thấy với mỗi P_S , tồn tại giá trị tối ưu của P_J để tối đa hóa ASC tại D_1 và D_2 . Giá trị ASC tăng khi P_J tăng do P_J làm suy giảm kênh nghe lén, nhưng giảm khi P_J quá lớn do ảnh hưởng của nhiễu AJ không hoàn hảo tại các người dùng hợp pháp. Vì khó xác định nghiệm giải tích, thuật toán GSS được áp dụng để tìm P_J tối ưu, với kết quả phù hợp với phân tích lý thuyết và cung cấp cơ sở cho thiết kế hệ thống.

Kết quả từ Hình 5.3 cho thấy hệ thống đề xuất đạt ASC vượt trội so với hệ thống không gây nhiễu, đồng thời ASC tăng đáng kể khi L tăng. Trong miền công suất cao, giá trị ASC của hệ thống đề xuất đạt bão hòa, trong khi



Hình 5.3: ASC tại D_1 và D_2 theo P_S với $L = 20, 40$

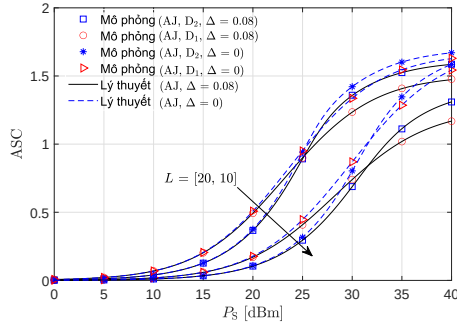
hệ thống không gây nhiễu suy giảm mạnh. Dưới điều kiện ipSIC, ASC thấp hơn so với pSIC, tuy nhiên sự khác biệt này trở nên không đáng kể trong miền công suất lớn.



Hình 5.4: Ảnh hưởng của α_1 lên ASC tại D_1 và D_2 .

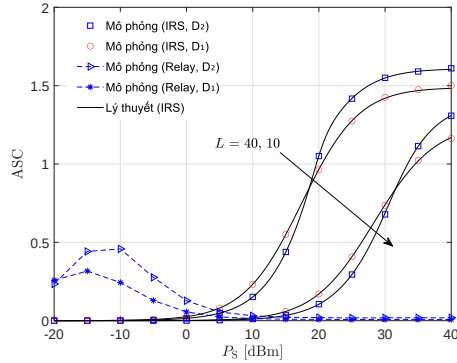
Kết quả từ Hình 5.4 cho thấy khi α_1 tăng, ASC tại D_1 tăng, trong khi ASC tại D_2 tăng đến một giá trị cực đại rồi giảm, cho thấy tồn tại hệ số phân bổ công suất tối ưu. Giá trị α_1 tối ưu được xác định hiệu quả bằng thuật toán GSS từ đó cung cấp cơ sở cho thiết kế hệ thống. Ngoài ra, hệ thống đề xuất luôn đạt ASC cao hơn so với cấu hình không gây nhiễu.

Hình 5.5 cho thấy ảnh hưởng của nhiễu là không đáng kể ở miền công suất thấp, nhưng trở nên rõ rệt khi P_S tăng. Ở miền công suất cao, nhiễu lý tưởng mang lại ASC vượt trội so với trường hợp không hoàn hảo. Nguyên nhân là do P_J tăng theo P_S , gây suy giảm hiệu năng tại người dùng



Hình 5.5: Ảnh hưởng của Δ lên ASC tại D_1 và D_2 .

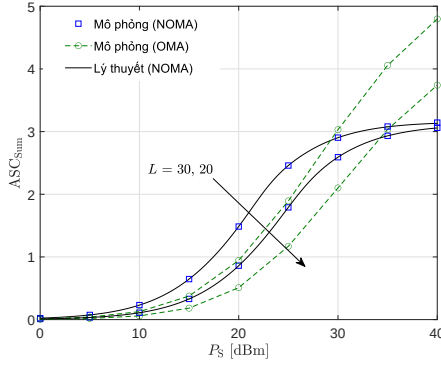
hợp pháp khi tồn tại nhiều dư, qua đó nhấn mạnh vai trò quan trọng của cơ chế khử AJ trong việc nâng cao hiệu năng bảo mật.



Hình 5.6: So sánh ASC của mô hình đề xuất với Relay.

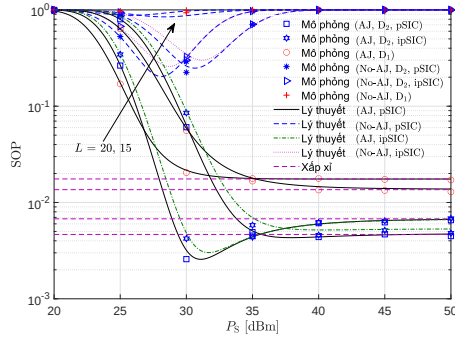
Kết quả từ Hình 5.6 cho thấy trong miền công suất thấp, hệ thống Relay-Jammer-NOMA đạt ASC cao hơn; tuy nhiên, khi P_S tăng, hệ thống IRS-Jammer-NOMA vượt trội do ASC tiếp tục tăng trong khi hệ thống chuyển tiếp bị bão hòa và suy giảm. Điều này khẳng định hiệu quả của IRS trong việc nâng cao hiệu năng bảo mật, đặc biệt ở miền công suất trung bình và cao.

Kết quả từ Hình 5.7 cho thấy trong miền công suất trung bình, hệ thống IRS-Jammer-NOMA đạt ASC vượt trội so với OMA. Tuy nhiên, ở miền công suất cao, ASC của NOMA dần bão hòa trong khi OMA tiếp tục tăng do không



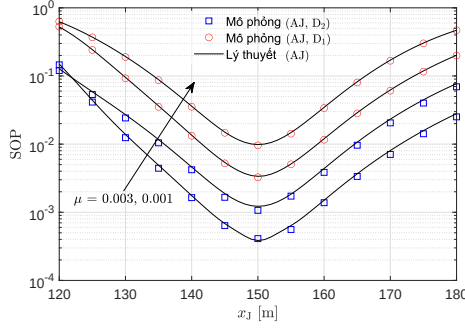
Hình 5.7: So sánh ASC của mô hình đề xuất với OMA.

chịu nhiều liên người dùng. Dù vậy, hệ thống đề xuất vẫn phù hợp hơn trong thực tiễn nhờ hiệu suất phổ cao, khả năng linh hoạt trong phân bổ công suất, cũng như khả năng cân bằng hiệu quả giữa bảo mật và SEE.



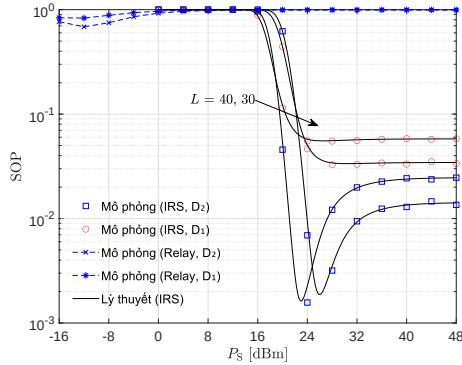
Hình 5.8: SOP theo P_S với $L = 15, 20$ và $\mu = 0.002$.

Hình 5.8 cho thấy việc sử dụng AJ giúp cải thiện đáng kể SOP so với cấu hình không gây nhiễu. Trong miền SNR cao, SOP của hệ thống không có AJ tiến gần 1, trong khi hệ thống đề xuất đạt giá trị sản thấp hơn, cho thấy khả năng bảo mật vượt trội. Bên cạnh đó, tăng L giúp cải thiện SOP. Trường hợp ipSIC cho hiệu năng SOP thấp hơn pSIC nhưng sự khác biệt giảm dần ở miền công suất lớn. Ở miền SNR cao, SOP hội tụ về một hằng số và không phụ thuộc vào P_S , cho thấy bậc đa dạng bảo mật của hệ thống bằng 0.



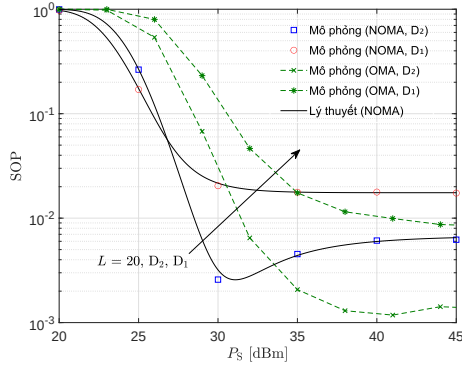
Hình 5.9: Ảnh hưởng của x_J lên SOP.

Hình 5.9 cho thấy vị trí của J ảnh hưởng đáng kể đến SOP, trong đó SOP đạt giá trị tối ưu khi J nằm gần thiết bị nghe lén, giúp tăng nhiễu tại E và giảm ảnh hưởng lên người dùng hợp pháp. Khi J di chuyển xa khỏi E, hiệu năng bảo mật suy giảm do nhiễu tại E giảm. Ngoài ra, việc tăng hệ số μ giúp cải thiện SOP nhờ tăng công suất gây nhiễu, qua đó làm suy giảm khả năng nghe lén.



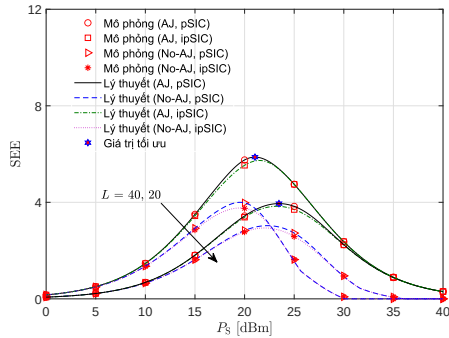
Hình 5.10: So sánh SOP của mô hình đề xuất với Relay.

Kết quả từ Hình 5.10 cho thấy trong miền công suất thấp, hệ thống Relay-Jammer-NOMA có SOP tốt hơn; tuy nhiên, khi P_S tăng, hệ thống IRS-Jammer-NOMA vượt trội rõ rệt về hiệu năng bảo mật. Ngoài ra, việc tăng L giúp cải thiện đáng kể SOP của hệ thống đề xuất.



Hình 5.11: So sánh SOP của mô hình đề xuất với OMA.

Hình 5.11 cho thấy trong miền công suất trung bình, hệ thống IRS-Jammer-NOMA đạt SOP vượt trội so với IRS-Jammer-OMA. Tuy nhiên, ở miền công suất rất cao, OMA có xu hướng cải thiện nhẹ hiệu năng bảo mật do loại bỏ nhiễu liên người dùng.



Hình 5.12: SEE theo P_S với $L = 20, 40$.

Kết quả từ Hình 5.12 cho thấy với mỗi giá trị L , tồn tại giá trị P_S tối ưu để tối đa hóa SEE, và giá trị này giảm khi L tăng. Điều này cho thấy có thể đạt SEE tối ưu với công suất thấp và L lớn. Ngoài ra, hệ thống đề xuất luôn đạt SEE cao hơn so với cấu hình không gây nhiễu, trong khi ipSIC cho hiệu năng thấp hơn pSIC. Bên cạnh đó, giá trị P_S tối ưu được xác định hiệu quả bằng thuật toán GSS.

Kết luận

Chương 5 đề xuất và phân tích mô hình mạng vô tuyến sử dụng kỹ thuật NOMA với sự hỗ trợ của IRS và AJ nhằm nâng cao bảo mật. Các biểu thức tường minh cho ASC, SOP và SEE được dẫn xuất và kiểm chứng cho mô hình đề xuất và mô hình không sử dụng AJ, xét trong các điều kiện pSIC và ipSIC cũng như loại bỏ AJ không hoàn hảo. Kết quả cho thấy hệ thống đề xuất đạt hiệu năng bảo mật tốt hơn so với các cấu hình đối sánh. Những kết quả này khẳng định tiềm năng của việc tích hợp IRS, AJ và NOMA trong các hệ thống vô tuyến bảo mật và hiệu quả cho mạng thế hệ mới.

Chương 6: Kết luận và hướng nghiên cứu tiếp theo

6.1. Kết luận của Luận án

1. Đề xuất và phân tích mạng vô tuyến có sự hỗ trợ của IRS kết hợp với RF-EH và AJ nhằm nâng cao hiệu năng bảo mật trên kênh pha-đỉnh Rayleigh. Biểu thức tường minh cho các tham số hiệu năng như OP, IP, ASC và SOP đã được dẫn xuất và kiểm chứng thông qua mô phỏng Monte Carlo. Kết quả cho thấy hệ thống đề xuất đạt hiệu năng bảo mật vượt trội so với cấu hình không sử dụng gây nhiễu, đặc biệt xét trên các mối quan hệ đánh đổi giữa OP-IP, ASC và SOP. Ngoài ra, hiệu năng bảo mật của hệ thống có thể được cải thiện đáng kể thông qua việc tăng số lượng phần tử phản xạ của IRS, tăng công suất gây nhiễu và tối ưu hóa quá trình thu thập năng lượng.

2. Phân tích hiệu năng bảo mật và hiệu quả năng lượng của mạng vô tuyến tích hợp IRS-AJ trên kênh pha-đỉnh Nakagami- m . Các biểu thức tường minh cho ASC và SEE đã được xây dựng và kiểm chứng thông qua mô phỏng Monte Carlo. Kết quả cho thấy việc kết hợp IRS và AJ mang lại cải thiện đáng kể về hiệu năng so với các cấu hình không sử dụng gây nhiễu. Đồng thời, ảnh hưởng của các tham số hệ thống quan trọng như: số phần tử phản xạ, khả năng khử nhiễu tại người dùng hợp pháp, tần số sóng mang, khoảng cách giữa các nút, công suất gây nhiễu đã được phân tích toàn diện, qua đó làm rõ đặc tính hoạt động của hệ thống. Bên cạnh đó, thuật toán GSS được áp dụng để xác định các tham số tối ưu, nhằm tối đa hiệu năng bảo mật và SEE.

3. Xây dựng và phân tích mô hình mạng vô tuyến sử dụng kỹ thuật NOMA với sự hỗ trợ của IRS và AJ trong môi trường pha-đỉnh Rayleigh, xét cả hai trường hợp pSIC và ipSIC. Các biểu thức tường minh cho ASC, SOP và SEE đã được dẫn xuất cho cả hai kịch bản có và không có AJ. Kết quả cho thấy hệ thống đề xuất đạt hiệu năng bảo mật vượt trội hơn so với các mô hình đối sánh như IRS-Non Jammer-NOMA, Relay-Jammer-NOMA và

IRS-Jammer-OMA. Đồng thời, ảnh hưởng của các tham số hệ thống như: số lượng phần tử phản xạ, vị trí bộ gây nhiễu, vị trí thiết bị nghe lén, khả năng khử nhiễu tại các người dùng hợp pháp, công suất nguồn và công suất gây nhiễu đã được phân tích chi tiết, cung cấp cơ sở cho việc thiết kế hệ thống trong thực tế. Bên cạnh đó, thuật toán GSS đã được áp dụng hiệu quả để xác định các tham số tối ưu nhằm cực đại hóa hiệu năng bảo mật và SEE.

Các kết quả của Luận án khẳng định tiềm năng của việc tích hợp IRS, AJ trong việc xây dựng các hệ thống truyền thông vô tuyến bảo mật, hiệu quả và bền vững cho các mạng thế hệ mới.

6.2. Hướng phát triển của Luận án

Trên cơ sở các kết quả đạt được, một số hướng nghiên cứu tiềm năng có thể tiếp tục phát triển như sau:

1. Mở rộng mô hình nghiên cứu theo hướng xét CSI không hoàn hảo và sai lệch pha tại IRS nhằm phản ánh sát hơn các điều kiện triển khai thực tế và đánh giá chính xác hiệu năng hệ thống.

2. Xem xét các kịch bản mạng phức tạp hơn như nhiều người dùng, nhiều thiết bị nghe lén, nhiều thiết bị gây nhiễu, nhằm đánh giá hiệu quả của hệ thống trong các môi trường thực tế.

3. Kết hợp IRS với các công nghệ như mmWave/THz, RSMA, mã Fountain nhằm nâng cao đồng thời hiệu năng bảo mật và hiệu quả năng lượng. Bên cạnh đó, sử dụng các công nghệ tiên tiến hơn của IRS như ARIS, IRS lai chủ động-thụ động, và STAR-RIS.

4. Ứng dụng các phương pháp học máy tiên tiến, đặc biệt là học tăng cường và học sâu tăng cường, nhằm giải quyết các bài toán tối ưu phức tạp trong hệ thống. Các phương pháp này cho phép tối ưu đồng thời nhiều tham số như phân bổ công suất, cấu hình IRS và điều khiển gây nhiễu, đồng thời khai thác dữ liệu kênh để nâng cao độ chính xác của CSI và hiệu quả phân bổ tài nguyên.

DANH MỤC CÁC CÔNG TRÌNH ĐÃ CÔNG BỐ

A. Các công trình sử dụng trong Luận án

[J1]. Vo Ta Ty, Pham Ngoc Son, Tran Trung Duy, “Secrecy performance of RIS-assisted wireless-powered systems with artificial-jamming generation,” *Physical Communication*, vol.69, 2025, 102592, <https://doi.org/10.1016/j.phycom.2024.102592> (SCIE - Q2).

[J2]. V. Ta Ty, T. Trung Duy, and P. Ngoc Son, “Enhancing the Secrecy Performance and Secure Energy Efficiency of NOMA Systems Using RIS with Artificial Jamming,” *International Journal of Communication Systems*, vol. 39, no. 7, p. e70474, 2026
<https://doi.org/10.1002/dac.70474> (SCIE - Q2).

[J3]. Vo Ta Ty, Tran Trung Duy, Tran Manh Hoang, Pham Ngoc Son, “Enhancing average secrecy capacity and secure energy efficiency of SISO system using RIS with artificial jamming over Nakagami-m fading channels,” *REV Journal on Electronics and Communications*, Vol. 15, No. 3, Jul. 2025, <http://dx.doi.org/10.21553/rev-jec.413>.

B. Các công trình không sử dụng trong Luận án

[C1]. Vo Ta Ty, Tran Trung Duy, Lam-Thanh Tu, Tien-Tung Nguyen, D.Trinh, Tan Hanh, “Security-reliability tradeoff of multi-hop secure communication networks using Fountain codes and RIS-aided cooperative communication,” in 2023 International Conference on Advanced Technologies For Communications (ATC), 2023, pp. 499-504, IEEE.

[C2]. Vo Ta Ty, Nguyen Van Hien, Tran Trung Duy, Lam-Thanh Tu, Pham Ngoc Son, “On performance evaluation of intelligent reflecting surface-aided NOMA systems using Fountain codes with presence of colluding eavesdroppers,” in 2025 International Conference on Advanced Technologies For Communications (ATC), 2025, pp. 1-6, IEEE.

[C3]. Vo Ta Ty, Le Thi Ngoc Diep, Tran Van Vinh, Tran Trung Duy, Pham Ngoc Son, “Secrecy performance analysis of RIS-assisted RSMA systems with Artificial Jamming,” the 8th International Conference on Green Technology and Sustainable Development (GTSD 2026). Đã được chấp nhận bản tóm tắt, NCS đang hoàn thiện đề nộp bản đầy đủ vào ngày 30.4.2026.

[J4]. Hieu T. Nguyen, Nguyen-Thi Hau, Nguyen Van Toan, Vo Ta Ty, and Tran Trung Duy, “Fountain Coding Based Two-Way Relaying Cognitive Radio Networks Employing Reconfigurable Intelligent Surface and Energy Harvesting”, vol.6, no.1., 2024, *Telecom*, được lập chỉ mục trong Web of Science (ESCI) và Scopus (Q2).

[J5]. Vo Ta Ty, Tran Trung Duy, Tran Manh Hoang, Pham Ngoc Son, “Physical-Layer Security Enhancement via RSMA-Enabled RIS with Artificial Jamming and RF Energy Harvesting,” *Digital Signal Processing*, 2026, (SCIE - Q2), (bản thảo đã nộp tạp chí ngày 26.01.2026, hiện đang trong quá trình phản biện).