BỘ GIÁO DỤC VÀ ĐÀO TẠO BỘ QUỐC PHÒNG

HỌC VIỆN KỸ THUẬT QUÂN SỰ

ĐẶNG THẾ HÙNG

NGHIÊN CỨU HIỆU NĂNG BẢO MẬT LỚP VẬT LÝ CỦA MỘT SỐ HỆ THỐNG THÔNG TIN VÔ TUYẾN SỬ DỤNG MÃ FOUNTAIN

TÓM TẮT LUẬN ÁN TIẾN SĨ KỸ THUẬT

Chuyên ngành: KỸ THUẬT ĐIỆN TỬ

Mã số: 9 52 02 03

HÀ NỘI - 2021

CÔNG TRÌNH ĐƯỢC HOÀN THÀNH TẠI
HỌC VIỆN KỸ THUẬT QUÂN SỰ - BỘ QUỐC PHÒNG

Người hướng dẫn khoa học: 1. TS Trần Trung Duy
2. PGS.TS Đỗ Quốc Trinh

Phản biện 1: PGS.TS Lê Nhật Thăng

Phản biện 2: PGS.TS Nguyễn Xuân Quyền

Phản biện 3: PGS.TS Trần Đức Tân

Luận án sẽ được bảo vệ tại Hội đồng đánh giá luận án cấp Học viện theo quyết định số 221/QĐ-HV, ngày 21 tháng 01 năm 2021 của Giám đốc Học viện Kỹ thuật Quân sự.

Có thể tìm hiểu luận án tại:

- Thư viện Quốc gia Việt Nam
- Thư viện của Học viện Kỹ thuật Quân sự

DANH MỤC CÁC CÔNG TRÌNH ĐÃ CÔNG BỐ

A. Các công trình sử dụng kết quả trong luận án

1. **Đặng Thế Hùng**, Trần Trung Duy và Đỗ Quốc Trinh, "Nghiên Cứu Hiệu Năng Truyền Bảo Mật Sử Dụng Mã Fountain Trong Mạng Vô Tuyến Nhận Thức Dưới Sự Tác Động Của Khiếm Khuyết Phần Cứng," *Tạp Chí Nghiên Cứu Khoa Học và Công Nghệ Quân Sự,* số 59, trang 58-69, 02/2019, ISSN: 1859-1043.

2. **Đặng Thế Hùng**, Trần Trung Duy và Đỗ Quốc Trinh, "Đánh Giá Khả Năng Giải Mã và Bảo Mật Dữ Liệu Thành Công Trong Mạng MIMO TAS/SC Sử Dụng Mã Fountain Dưới Tác Động Của Giao Thoa Đồng Kênh," *Tạp Chí Khoa Học và Kỹ Thuật, Học Viện Kỹ Thuật Quân Sự,* số 192, trang 89-102, 08/2018, ISSN: 1859-0209.

3. **D. T. Hung**, T. T. Duy, T. T. Phuong, D. Q. Trinh, and T. Hanh, "Performance Comparison between Fountain Codes-Based Secure MIMO Protocols With and Without Using Non-Orthogonal Multiple Access," *Entropy*, vol. 21, no. 10, (928), Oct. 2019, SCIE/Q2, IF: 2.494, DOI: https://doi:10.3390/e21100982, ISSN: 1099-4300.

4. **D. T. Hung**, T. T. Duy, D. Q. Trinh, V. N. Q. Bao, and T. Hanh, "Security-Reliability Analysis of Power Beacon-Assisted Multi-hop Relaying Networks Exploiting Fountain Codes with Hardware Imperfection," in *The International Conference on Advanced Technologies for Communications (ATC)*, 2018, Ho Chi Minh city, Vietnam, pp. 354-359, Oct. 2018, DOI: 10.1109/ATC.2018.8587493.

5. **D. T. Hung**, T. T. Duy, and D. Q. Trinh, "Security-Reliability Analysis of Multi-hop LEACH Protocol with Fountain Codes and Cooperative Jamming," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 6, no. 18, pp. 1-7, Mar. 2019, DOI: http://dx.doi.org/10.4108/eai.28-3-2019.157120, ISSN: 2410-0218.

B. Các công trình công bố khác trong thời gian thực hiện luận án

1. **Đặng Thế Hùng**, T. T. Duy, V. N. Q. Bảo, Đ. Q. Trinh và T. Hạnh, "Phân Tích Hiệu Năng Mô Hình Truyền Đường Xuống Sử Dụng Kỹ Thuật Chọn Lựa Ăng-ten Phát và Mã Fountain Dưới Sự Ảnh Hưởng Của Nhiễu Đồng Kênh," *REV-ECIT 2017*, trang 270-274, TP. Hồ Chí Minh, Việt Nam, 12/2017.

2. P. T. Tin, **D. T. Hung**, T. T. Duy, and M. Voznak, "Security-Reliability Analysis of NOMA-based Multi-Hop Relay Networks in Presence of an Active Eavesdropper with Imperfect Eavesdropping CSI," *Advances in Electrical and Electronic Engineering (AEEE)*, vol. 15, no. 4, pp. 591-597, Nov. 2017, (Scopus).

3. **D. T. Hung**, T. T. Duy, D. Q. Trinh, and V. N. Q. Bao, "Secrecy Performance Evaluation of TAS Protocol Exploiting Fountain Codes and Cooperative Jamming under Impact of Hardware Impairments," in *SigTelCom 2018*, Ho Chi Minh city, Vietnam, pp. 164-169, Jan. 2018.

4. **Đặng Thế Hùng**, T. T. Duy, L. C. Khẩn và Đ. Q. Trinh, "Đánh Giá Hiệu Năng Xác Suất Dừng Mạng Thông Tin Vệ Tinh Chuyển Tiếp Hai Chiều Sử Dụng Mã Fountain," *REV-ECIT 2019*, trang 152-156, Hà Nội, Việt Nam, 12/2019.

5. B. Q. Đức, **Đặng Thế Hùng**, T. T. Duy và N. T. Bình, "Phân Tích Hiệu Năng Mạng Khuếch Đại Chuyển Tiếp Đa Chặng Dưới Sự Ảnh Hưởng Chung Của Nhiễu Đồng Kênh Và Nhiễu Phần Cứng," *REV-ECIT 2019*, trang 247-252, Hà Nội, Việt Nam, 12/2019.

6. Đ. V. Phương, N. T. Đông, **Đặng Thế Hùng** và H. V. Toàn, "Xác Suất Dừng Hệ Thống FD-NOMA Với Nút Chuyển Tiếp Sử Dụng Công Nghệ Thu Thập Năng Lượng," *REV-ECIT 2019*, trang 283-288, Hà Nội, Việt Nam, 12/2019.

7. P. T. Tin, **D. T. Hung**, N. N. Tan, T. T. Duy, and M. Voznak, "Secrecy Performance Enhancement for Underlay Cognitive Radio Networks Employing Cooperative Multi-hop Transmission With and Without Presence of Hardware Impairments," *Entropy*, vol. 21, no. 2, (217), Feb. 2019, SCIE/Q2, IF: 2.494.

8. **Đặng Thế Hùng** và N. T. Dũng, "Phân Tích Hiệu Năng Truyền Bảo Mật Sử Dụng Mã Fountain Với Kỹ Thuật Lựa Chọn Ăng-ten Phát," *REV-ECIT 2020*, trang 108-113, Hà Nội, Việt Nam, 12/2020.

9. **Đặng Thế Hùng**, L. C. Khẩn, N. V. Toàn và Đ. Q. Trinh, "Nghiên Cứu Hiệu Năng Bảo Mật Lớp Vật Lý Cho Mạng Chuyển Tiếp Lai Ghép Vệ Tinh-Mặt Đất Dưới Sự Tác Động Của Nhiễu Đồng Kênh Và Nhiễu Phần Cứng," *Tạp Chí Khoa Học Công Nghệ Thông Tin và Truyền Thông, Học Viện Công Nghệ Bưu Chính Viễn Thông,* số …, trang …, 12/2020, ISSN: 2525-2224, (Đã được chấp nhận đăng).

MỞ ĐẦU

1. Tính cấp thiết của đề tài

Ngày nay, với sự bùng nổ của truyền thông không dây đã mang lại cho con người nhiều tiện ích. Tuy nhiên, do đặc tính quảng bá của kênh truyền vô tuyến, những nút nghe lén có thể dễ dàng thu thập hoặc tấn công hay sửa đổi thông tin. Do đó, bảo mật thông tin là vấn đề rất quan trọng trong thiết kế các hệ thống thông tin hiện đại. Để bảo mật hệ thống, các thuật toán như DES, RSA được sử dụng và phát triển rộng rãi. Nhưng yêu cầu độ phức tạp cao và khi năng lực tính toán của hệ thống bẻ khóa ngày càng cao, sẽ rất khó hiệu quả để bảo đảm an toàn thông tin.

Bảo mật lớp vật lý (PLS) khai thác các đặc tính kênh truyền, như nhiễu và pha đinh, khoảng cách giữa các nút mạng, để nâng cao bảo mật hệ thống. PLS không phụ thuộc độ phức tạp tính toán, bảo mật đạt được không bị thỏa hiệp khi các thiết bị nghe lén có khả năng tính toán mạnh mẽ.

Mã Fountain không đưa ra tốc độ cố định, phù hợp các điều kiện kênh thay đổi theo thời gian, triển khai với độ phức tạp thấp, số gói mã hóa tạo ra từ dữ liệu nguồn có khả năng không giới hạn. Để truyền bảo mật, máy thu nhận đủ số gói mã hóa cần thiết để phục hồi bản tin gốc và tốc độ giải mã cao hơn nút nghe lén. Qua khảo sát các công trình trong nước và quốc tế có liên quan, chưa có nhiều công trình nghiên cứu các giao thức sử dụng FC từ quan điểm bảo mật. Do đó, việc nghiên cứu đề xuất các mô hình hệ thống sử dụng FC để bổ sung những khoảng trống bảo mật là vấn đề rất quan trọng, cần thiết, có ý nghĩa khoa học và thực tiễn.

2. Mục tiêu nghiên cứu của luận án

• Nghiên cứu khả năng bảo đảm an toàn thông tin ở lớp vật lý, đề xuất và phân tích hiệu quả bảo mật thông tin của giao thức đề xuất trong các hệ thống vô tuyến sử dụng FC, như MISO TAS, MIMO TAS/SC, MIMO-NOMA TAS/SC/MRC, giao thức chuyển tiếp đa chặng dựa vào thu thập năng lượng và giao thức LEACH đa chặng với gây nhiễu cộng tác.

• Phân tích hiệu năng bảo mật hệ thống với các giao thức đề xuất trên kênh truyền pha đinh Rayleigh.

• Xây dựng mô hình tính toán, phương pháp phân tích, chương trình mô phỏng để đánh giá các tham số hiệu năng bảo mật hệ thống.

3. Phạm vi và đối tượng nghiên cứu

• Nghiên cứu lý thuyết an toàn thông tin, giao thức PLS sử dụng FC, mô hình tính toán các loại kênh truyền như pha đinh Rayleigh và pha đinh Rice.

• Nghiên cứu ảnh hưởng của nhiễu đồng kênh, suy giảm phần cứng, sử dụng các công cụ toán học để phân tích hiệu năng và mô phỏng hệ thống.

• Nghiên cứu các hệ thống sử dụng FC như MISO, MIMO với kỹ thuật TAS, kết hợp phân tập thu SC hoặc MRC, kỹ thuật chuyển tiếp tín hiệu DF hoặc AF, mạng đa chặng thu thập năng lượng và giao thức LEACH với gây nhiễu cộng tác để cải thiện hiệu quả bảo mật lớp vật lý.

4. Các đóng góp chính của luận án

• Đề xuất và phân tích hiệu năng bảo mật sử dụng FC như MISO TAS trong mạng vô tuyến nhận thức dạng nền, mạng MIMO TAS/SC, dựa vào các biểu thức chính xác của SS và IP được đưa ra.

• Đề xuất và đánh giá hiệu năng FC với giao thức truyền bảo mật trong hệ thống MIMO-NOMA TAS/SC/MRC, dựa vào các biểu thức dạng tường minh TS và IP được đưa ra.

• Đề xuất và đánh giá hiệu năng bảo mật và độ tin cậy của các mạng đa chặng sử dụng FC như giao thức đa chặng dựa vào trạm phát sóng vô tuyến (Beacon) để thu thập năng lượng và giao thức phân cấp theo cụm thích ứng năng lượng thấp (LEACH) với gây nhiễu cộng tác trong WSN. Hiệu năng hệ thống được đánh giá dựa vào biểu thức chính xác OP và IP được đưa ra.

5. Bố cục luận án

Luận án được cấu trúc bao gồm phần mở đầu, 4 chương và kết luận, kiến nghị hướng nghiên cứu tiếp theo.

Phần mở đầu: Tập trung làm rõ các lý do cơ bản lựa chọn đề tài, xác định mục tiêu, phạm vi, đối tượng và phương pháp nghiên cứu của luận án.

• Chương 1: Những vấn đề chung

• Chương 2: Hiệu năng bảo mật trong các mạng MISO TAS và MIMO TAS/SC sử dụng mã Fountain

• Chương 3: Hiệu năng bảo mật trong mạng MIMO-NOMA TAS/SC/MRC sử dụng mã Fountain

• Chương 4: Hiệu năng bảo mật trong các mạng chuyển tiếp đa chặng sử dụng mã Fountain

Chương 1
NHỮNG VẤN ĐỀ CHUNG

1.1. Bảo mật trong hệ thống MIMO lựa chọn ăng-ten phát

Hệ thống MIMO với nhiều ăng-ten tại cả máy phát và máy thu làm tăng đáng kể dung lượng và độ tin cậy hệ thống. Tuy nhiên, sử dụng đa ăng-ten dẫn đến độ phức tạp phần cứng, kích thước, công suất tiêu thụ lớn và chi phí triển khai tốn kém. Kỹ thuật TAS với chi phí, độ phức tạp thấp, nhằm khai thác các ưu điểm của hệ thống MIMO, sử dụng ít chuỗi RF hơn để nâng cao dung lượng hệ thống. PLS sử dụng TAS để tăng dung lượng kênh hợp pháp càng lớn hơn kênh nghe lén nhằm nâng cao hiệu năng bảo mật của hệ thống.

1.2. Bảo mật với kỹ thuật phân tập thu

Trong thông tin vô tuyến, các kỹ thuật phân tập thu (SC, MRC hoặc EGC) được sử dụng rộng rãi để giảm ảnh hưởng của pha đinh đa đường, cải thiện độ tin cậy truyền dẫn mà không phải tăng công suất phát hoặc mở rộng băng thông. Phương pháp này cho phép nâng cao dung lượng kênh thông tin, do đó dung lượng bảo mật hệ thống được cải thiện đáng kể.

1.3. Bảo mật trong mạng vô tuyến nhận thức

Để giải quyết sự khan hiếm phổ tần và sử dụng phổ tần hiệu quả hơn, mạng vô tuyến nhận thức (CRN) được đề xuất bởi Mitola vào năm 1999. Trong CRN, mạng sơ cấp (được cấp phép sử dụng tần số) có thể chia sẻ phổ tần với người dùng thứ cấp (không được phép sử dụng tần số), theo các kịch bản như dạng nền, chồng hoặc xen kẻ, để tận dụng các khoảng phổ tần nhàn rỗi. Trong CRN dạng nền đã thu hút được nhiều sự quan tâm nghiên cứu, do trong mạng này cho phép mạng thứ cấp hoạt động song song với mạng sơ cấp, nhưng công suất phát thứ cấp phải hiệu chỉnh để không làm ảnh hưởng đến chất lượng dịch vụ mạng sơ cấp. Bảo mật trong CRN dạng nền là vấn đề rất quan trọng và đã được khảo sát dưới nhiều góc độ khác nhau.

1.4. Bảo mật trong mạng NOMA

Đa truy nhập không trực giao (NOMA) là công nghệ tiềm năng cho mạng di động thế hệ tiếp theo. NOMA cải thiện hiệu quả phổ tần bằng cách cung cấp nhiều người dùng đồng thời thông qua ghép kênh miền công suất (PDM). Ý tưởng của PDM-NOMA là sử dụng miền công suất để đồng thời

phục vụ nhiều người dùng trong cùng một khe thời gian, dải tần và mã, bằng mã hóa xếp chồng tại máy phát. Mức công suất cho một người dùng được quyết định dựa trên độ lợi kênh, người dùng có độ lợi kênh cao hơn được gán mức công suất thấp hơn, cụ thể $|h_1|^2 > |h_2|^2$ thì $0 < a_1 < a_2$. Tại máy thu thực hiện SIC, tín hiệu người dùng được giải mã dựa vào mức công suất phân bổ khác nhau giữa các người dùng. Gần đây, cả NOMA và PLS là công nghệ đầy hứa hẹn cho các hệ thống vô tuyến trong tương lai.

1.5. Bảo mật trong mạng đa chặng

Mạng chuyển tiếp được sử dụng rộng rãi trong thông tin vô tuyến, do có thể mở rộng vùng phủ sóng, giảm giá thành triển khai, giảm can nhiễu, nâng cao độ tin cậy, nhưng hạn chế về khoảng cách truyền dẫn, độ trễ xử lý tín hiệu và hiệu quả sử dụng phổ tần. Hơn nữa, các nút mạng thường bị hạn chế về nguồn pin, do đó rất phù hợp với thu thập năng lượng sóng vô tuyến (RF-EH), nhằm cải thiện hiệu năng. Bảo mật là vấn đề quan trọng trong các giao thức đa chặng. PLS không dựa vào mã hóa phức tạp, triển khai đơn giản, nên phù hợp với mạng đa chặng bị hạn chế năng lượng và sử dụng các giao thức chuyển tiếp đa chặng, gây nhiễu cộng tác (CJ) để nâng cao bảo mật.

1.6. Bảo mật trong hệ thống sử dụng mã Fountain

Hệ thống sử dụng FC, máy phát có thể tạo ra số lượng không giới hạn các gói mã hóa độc lập, máy thu cố gắng nhận các gói mã hóa và khi nhận đủ số gói mã hóa cần thiết để khôi phục bản tin gốc, máy thu có thể ngắt kết nối, do đó tiết kiệm thời gian và năng lượng truyền dẫn.

$$n = k(1+\varepsilon), \tag{1.1}$$

trong đó, k và n là symbol bản tin gốc và symbol mã hóa, ε $(\varepsilon \geq 0)$ là phần thông tin được bổ sung.

FC có thể thích ứng với các điều kiện kênh cụ thể, mà không cần ước lượng kênh tại máy phát. Ý tưởng của PLS dựa vào FC là khi nút đích dự định có thể nhận đủ số gói mã hóa trước nút nghe lén, truyền dữ liệu là thành công và bảo mật, ngược lại dữ liệu gốc bị thu chặn.

1.6. Kết luận chương 1

Chương 1 trình bày những vấn đề cơ bản về bảo mật thông tin và hệ thống sử dụng mã Fountain, làm cơ sở giải quyết các nội dung tiếp theo.

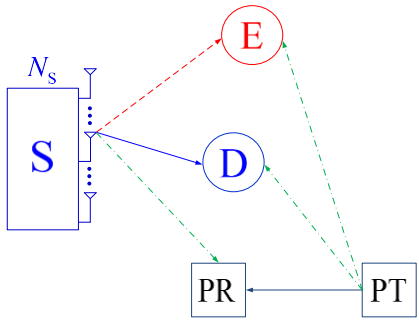
Chương 2

HIỆU NĂNG BẢO MẬT TRONG CÁC MẠNG MISO TAS VÀ MIMO TAS/SC SỬ DỤNG MÃ FOUNTAIN

Chương 2, Luận án đề xuất hai mô hình để phân tích hiệu năng bảo mật của các mạng MISO TAS và MIMO TAS/SC sử dụng FC trên kênh pha đinh Rayleigh, dưới tác động của nhiễu đồng kênh (CCI), gồm có: Phần 2.1 phân tích mô hình truyền dữ liệu của mạng MISO sử dụng FC, với kỹ thuật TAS trong môi trường vô tuyến nhận thức dạng nền, dưới sự tác động của chung giao thoa đồng kênh từ mạng sơ cấp và suy giảm phần cứng. Phần 2.2 nghiên cứu mô hình MIMO TAS/SC nhằm nâng cao độ tin cậy của truyền các gói mã hóa trên kênh chính sử dụng FC dưới tác động của CCI.

2.1. Mô hình 1: Mạng MISO TAS sử dụng mã Fountain trong môi trường vô tuyến nhận thức dạng nền

2.1.1. Mô hình hệ thống



Hình 2.1: Mô hình hệ thống đề xuất.

Hình 2.1 miêu tả hai mạng sơ cấp và thứ cấp cùng sử dụng chung một băng tần. Máy phát sơ cấp (PT) gửi dữ liệu đến máy thu sơ cấp (PR). Cùng lúc, nút nguồn thứ cấp (S) cũng truyền dữ liệu đến nút đích thứ cấp (D), xuất hiện nút nghe lén thứ cấp (E) cố gắng thu dữ liệu mà S gửi đến D. Do hai mạng sơ cấp và thứ cấp cùng hoạt động trên một dải tần, các máy phát sơ cấp và thứ cấp sẽ gây nhiễu đồng kênh lên các thiết bị thu thứ cấp và sơ cấp. Để đảm bảo chất lượng dịch vụ cho mạng sơ cấp (mạng được cấp phép sử dụng băng tần), S phải hiệu chỉnh công suất phát một cách thích hợp.

Giả sử PT, PR, D và E chỉ có 01 ăng-ten, S trang bị N_S ăng-ten phát và TAS để gửi gói dữ liệu đến D sử dụng FC. S chia dữ liệu gốc thành L gói nhỏ bằng nhau. Một số các gói nhỏ này được chọn ngẫu nhiên và XOR với nhau để tạo những gói mã hóa. S lần lượt gửi các gói mã hóa đến D sử dụng những khe thời gian trực giao theo TDMA. Bởi tính chất quảng bá của kênh vô tuyến, E cũng nhận được các gói mã hóa của S. Xem xét hệ thống giới hạn thời gian trễ, số gói mã hóa tối đa mà S có thể gửi đến D cố định bởi $N_{\max}$. Theo nguyên lý FC, D và E giải mã các gói mã hóa và lưu trữ dữ liệu vào bộ đệm. Để khôi phục dữ liệu gốc của S, thì D và E nhận thành công ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa, với $N_{\text{req}}^{\text{pkt}} = (1+\varepsilon)L$ và $\varepsilon(\varepsilon > 0)$ là thông tin bổ sung, $N_{\text{req}}^{\text{pkt}} \le N_{\max}$. Nếu D nhận đủ $N_{\text{req}}^{\text{pkt}}$ gói mã hóa trước khi S phát đủ $N_{\max}$ gói, D ngay lập tức gửi thông điệp ACK đến S để S dừng truyền. Nếu E không nhận đủ $N_{\text{req}}^{\text{pkt}}$ gói mã hóa từ S thì E sẽ không thể giải mã được dữ liệu gốc của S, truyền dữ liệu giữa S và D là thành công và bảo mật (SS). Ngược lại, nếu E nhận được ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa, dữ liệu gốc bị thu chặn (IP).

Hệ thống ràng buộc độ trễ, số khe thời gian sử dụng phát các gói mã hóa bị giới hạn bởi $N_{\max}$. Ký hiệu $N\left(N_{\text{req}}^{\text{pkt}} \le N \le N_{\max}\right)$ là số khe thời gian sử dụng bởi S, $N_{\text{D}}^{\text{pkt}}$ và $N_{\text{E}}^{\text{pkt}}$ là số gói mã hóa nhận được bởi D và E sau khi S dừng truyền. Biểu thức tính xác suất giải mã và bảo mật thông tin thành công (SS) của quá trình truyền từ S đến D như sau:

$$\text{SS} = \Pr\left(N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}},\ N_{\text{E}}^{\text{pkt}} < N_{\text{req}}^{\text{pkt}} \mid N \le N_{\max}\right). \tag{2.1}$$

Biểu thức (2.1) ngụ ý rằng D nhận đủ số gói mã hóa $\left(N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}}\right)$ trước E $\left(N_{\text{E}}^{\text{pkt}} < N_{\text{req}}^{\text{pkt}}\right)$ khi số khe thời gian được sử dụng $\left(N \le N_{\max}\right)$.

Kế tiếp, biểu thức xác suất thu chặn (IP), định nghĩa là xác suất mà E có thể đạt được thành công $N_{\text{req}}^{\text{pkt}}$ gói mã hóa trước hoặc cùng lúc với D.

$$\text{IP} = \Pr\left(N_{\text{E}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}},\ N_{\text{D}}^{\text{pkt}} \le N_{\text{req}}^{\text{pkt}} \mid N \le N_{\max}\right). \tag{2.2}$$

Biểu thức (2.2) thể hiện khi E đạt được $N_{\text{req}}^{\text{pkt}}$ gói mã hóa, E không cần nhận thêm số gói mã hóa nữa, E bắt đầu giải mã dữ liệu gốc của S.

2.1.2. Phân tích hiệu năng

2.1.2.1. Xác suất giải mã và bảo mật thông tin thành công (SS)

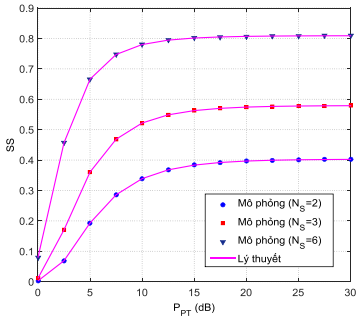
$$\mathrm{SS}=\sum_{w=N_{\mathrm{req}}^{\mathrm{pkt}}}^{N_{\max}}\left[C_{w-1}^{w-N_{\mathrm{req}}^{\mathrm{pkt}}}\left(1-\rho_{\mathrm{D}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}}\left(\rho_{\mathrm{D}}\right)^{w-N_{\mathrm{req}}^{\mathrm{pkt}}}\times\sum_{q=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1}C_{w}^{q}\left(1-\rho_{\mathrm{E}}\right)^{q}\left(\rho_{\mathrm{E}}\right)^{w-q}\right]. \tag{2.3}$$

2.1.2.2. Xác suất thu chặn (IP)

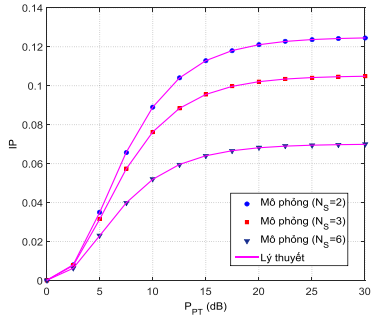
$$\mathrm{IP}=\sum_{w=N_{\mathrm{req}}^{\mathrm{pkt}}}^{N_{\max}}C_{w-1}^{w-N_{\mathrm{req}}^{\mathrm{pkt}}}\left(1-\rho_{\mathrm{E}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}}\left(\rho_{\mathrm{E}}\right)^{w-N_{\mathrm{req}}^{\mathrm{pkt}}}$$

$$\times\left[C_{w-1}^{w-N_{\mathrm{req}}^{\mathrm{pkt}}}\left(1-\rho_{\mathrm{D}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}}\left(\rho_{\mathrm{D}}\right)^{w-N_{\mathrm{req}}^{\mathrm{pkt}}}+\sum_{r=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1}C_{w}^{r}\left(1-\rho_{\mathrm{D}}\right)^{r}\left(\rho_{\mathrm{D}}\right)^{w-r}\right]. \tag{2.4}$$

2.1.3. Các kết quả mô phỏng



Hình 2.2: SS vẽ theo P_{PT} (dB) khi $N_{\max}=10$ và $\kappa_{\mathrm{D}}^2=\kappa_{\mathrm{E}}^2=0$.



Hình 2.3: IP vẽ theo P_{PT} (dB) khi $N_{\max}=10$ và $\kappa_{\mathrm{D}}^2=\kappa_{\mathrm{E}}^2=0$.

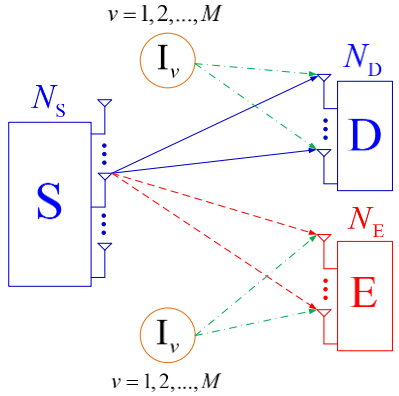
Hình 2.2, SS tăng khi P_{PT} tăng, SS tiến về hằng số khi P_{PT} đủ lớn, khi tăng số ăng-ten phát N_{S}, xác suất dữ liệu nguồn có thể nhận thành công và bảo mật tại D cũng tăng đáng kể. Hình 2.3, IP của hệ thống giảm khi nút nguồn trang bị nhiều ăng-ten hơn. Tương tự giá trị SS, IP cũng tăng khi P_{PT} tăng và bão hòa khi P_{PT} đủ lớn.

2.2. Mô hình 2: Mạng MIMO TAS/SC sử dụng mã Fountain

2.2.1. Mô hình hệ thống

Hình 2.4 miêu tả mô hình hệ thống đề xuất, nút nguồn (S) trang bị N_{S} ăng-ten phát, sử dụng TAS để gửi từng gói mã hóa đến nút đích (D) có N_{D}

ăng-ten thu. Cùng lúc, nút nghe lén (E) có N_E ăng-ten thu, đang cố gắng nhận những gói mã hóa để giải mã dữ liệu gốc của S. Cả D và E đều sử dụng kỹ thuật SC để giải mã những gói mã hóa nhận được. Hơn nữa, cả D và E đều chịu ảnh hưởng bởi nhiễu gây ra từ M nguồn giao thoa đơn ăng-ten, ký hiệu là $I_1, I_2, ..., I_{M-1}$ và I_M. Tác giả xem xét hai trường hợp: 1) D và E không có CSI đến các nguồn giao thoa; 2) D và E có thể ước lượng chính xác CSI đến các nguồn giao thoa.



Hình 2.4: Mô hình nghiên cứu đề xuất.

Tương tự, hệ thống sử dụng FC, S chia dữ liệu gốc thành L gói nhỏ bằng nhau và thực hiện phép XOR để tạo ra các gói mã hóa. Tiếp theo, S gửi các gói mã hóa đến D trong những khe thời gian trực giao theo phương pháp TDMA và do tính chất mở của kênh vô tuyến, E cũng có thể nhận được những gói mã hóa này. Dữ liệu gốc có thể được khôi phục nếu D (E) nhận thành công ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa, khi D nhận đủ số gói mã hóa cần thiết cho giải mã dữ liệu gốc thì D gửi thông điệp ACK để S dừng truyền. Nếu E không nhận đủ $N_{\text{req}}^{\text{pkt}}$ gói mã hóa thì E sẽ không thể giải mã được dữ liệu nguồn, do đó quá trình truyền dữ liệu là thành công và bảo mật.

Ký hiệu N_{TS} là tổng số gói mã hóa mà S phải gửi đến D để D có thể nhận đủ $N_{\text{req}}^{\text{pkt}}$ gói mã hóa để khôi phục thông tin gốc. Tác giả cũng ký hiệu $N_{\text{D}}^{\text{pkt}}$ và $N_{\text{E}}^{\text{pkt}}$ là số gói mã hóa mà D và E đã nhận thành công trong N_{TS}

khe thời gian truyền. Như đã đề cập, xác suất giải mã và bảo mật thông tin thành công (SS) có thể được định nghĩa bởi

$$\mathrm{SS} = \Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}},\ N_{\mathrm{E}}^{\mathrm{pkt}} < N_{\mathrm{req}}^{\mathrm{pkt}}\right). \tag{2.5}$$

Mô hình TAS/SC số 1 (MH1), giả sử D và E không biết CSI giữa các ăng-ten của chúng và các nguồn giao thoa. MH1 không đạt SINR tối đa cho kênh truyền giữa S và D do thiếu thông tin CSI từ các kênh giao thoa.

Mô hình TAS/SC số 2 (MH2), giả sử D và E có thể ước lượng chính xác CSI giữa các ăng-ten của chúng và các nguồn giao thoa.

Tiếp theo, tác giả sẽ đưa ra công thức tính chính xác của SS trong mô hình 1 (MH1) và mô hình 2 (MH2) bằng các biểu thức dưới đây.

2.2.2. Phân tích hiệu năng

2.2.2.1. Xác suất giải mã và bảo mật thông tin thành công chính xác trong mô hình TAS/SC số 1 (SS/MH1)

$$\mathrm{SS}_{\mathrm{MH1}} = \sum_{N_{\mathrm{TS}}=N_{\mathrm{req}}^{\mathrm{pkt}}}^{+\infty}\left[C_{N_{\mathrm{TS}}-1}^{N_{\mathrm{TS}}-N_{\mathrm{req}}^{\mathrm{pkt}}}\left(1-\rho_{1,\mathrm{D}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}}\left(\rho_{1,\mathrm{D}}\right)^{N_{\mathrm{TS}}-N_{\mathrm{req}}^{\mathrm{pkt}}}\right] \times\left[\sum_{q=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} C_{N_{\mathrm{TS}}}^{q}\left(1-\rho_{1,\mathrm{E}}\right)^{q}\left(\rho_{1,\mathrm{E}}\right)^{N_{\mathrm{TS}}-q}\right], \tag{2.6}$$

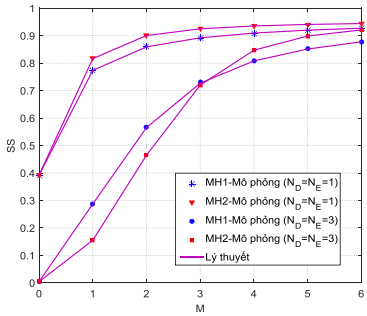
với $C_{N_{\mathrm{TS}}-1}^{N_{\mathrm{TS}}-N_{\mathrm{req}}^{\mathrm{pkt}}}\left(1-\rho_{1,\mathrm{D}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}}\left(\rho_{1,\mathrm{D}}\right)^{N_{\mathrm{TS}}-N_{\mathrm{req}}^{\mathrm{pkt}}}$ là xác suất D nhận đủ $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa, $C_{N_{\mathrm{TS}}}^{q}\left(1-\rho_{1,\mathrm{E}}\right)^{q}\left(\rho_{1,\mathrm{E}}\right)^{N_{\mathrm{TS}}-q}$ là xác suất E nhận thành công q gói mã hóa.

2.2.2.2. Xác suất giải mã và bảo mật thông tin thành công chính xác trong mô hình TAS/SC số 2 (SS/MH1)

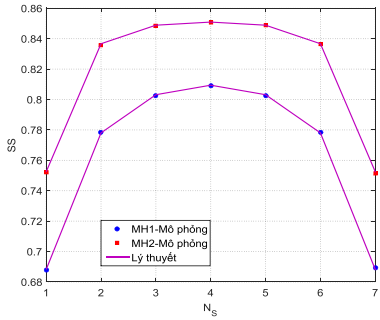
$$\mathrm{SS}_{\mathrm{MH2}} = \sum_{N_{\mathrm{TS}}=N_{\mathrm{req}}^{\mathrm{pkt}}}^{+\infty}\left[C_{N_{\mathrm{TS}}-1}^{N_{\mathrm{TS}}-N_{\mathrm{req}}^{\mathrm{pkt}}}\left(1-\rho_{2,\mathrm{D}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}}\left(\rho_{2,\mathrm{D}}\right)^{N_{\mathrm{TS}}-N_{\mathrm{req}}^{\mathrm{pkt}}}\right] \times\left[\sum_{q=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} C_{N_{\mathrm{TS}}}^{q}\left(1-\rho_{2,\mathrm{E}}\right)^{q}\left(\rho_{2,\mathrm{E}}\right)^{N_{\mathrm{TS}}-q}\right]. \tag{2.7}$$

2.2.3. Các kết quả mô phỏng

Luận án thực hiện mô phỏng Monte Carlo để kiểm chứng các công thức lý thuyết đã trình bày. Trong các mô phỏng, chuỗi vô cùng được cắt bởi giá trị bằng 1000.



Hình 2.5: SS vẽ theo M khi $Q_S = Q_I = 10$ (dB), $N_S = 3$, $\lambda_{SD} = 1$, $\lambda_{SE} = 1$, $\lambda_{ID} = 3$, $\lambda_{IE} = 3$, $\gamma_{th} = 1$ và $N_{req}^{pkt} = 5$.



Hình 2.6: SS vẽ theo N_S khi $Q_S = 5$ (dB), $Q_I = 10$ (dB), $N_E = 3$, $M = 1$, $\lambda_{SD} = 1$, $\lambda_{SE} = 1$, $\lambda_{ID} = 5$, $\lambda_{IE} = 5$, $\gamma_{th} = 1.75$ và $N_{req}^{pkt} = 4$.

Hình 2.5, SS của hai mô hình đều tăng khi tăng số nguồn giao thoa M. Khi D và E là đơn ăng-ten $(N_D = N_E = 1)$, SS/MH2 lớn hơn MH1, tăng số ăng-ten thu tại D và E $(N_D = N_E = 3)$, SS/MH1 tại $(M > 3)$ lớn hơn MH2 và ngược lại. SS giảm nhanh khi tăng số ăng-ten tại E, do E khai thác độ lợi phân tập thu nhờ sử dụng kỹ thuật SC.

Hình 2.6, giả sử rằng tổng số ăng-ten tại S và D là không đổi và bằng 8 $(N_S + N_D = 8)$, vẽ SS khi tăng N_S từ 01 đến 07. Giá trị SS biến thiên theo N_S và SS lớn nhất khi $(N_S = N_D = 4)$. Để đạt hiệu năng truyền thông và bảo mật tốt nhất, cần thiết kế (phân phối) phù hợp số ăng-ten tại S và D.

2.3. Kết luận chương

Các kết quả mô hình 1, hiệu năng tốt hơn khi S trang bị số ăng-ten phát phù hợp và phần cứng thiết bị thứ cấp tốt hơn. Để nâng cao hiệu năng bảo mật cần giảm số lần truyền gói mã hóa. Trong mô hình 2, hiệu năng chịu ảnh hưởng bởi các tham số đặc trưng kênh truyền và số nguồn giao thoa. Cần phân phối số ăng-ten tại máy thu/phát thích hợp, tăng số gói mã hóa yêu cầu để khôi phục dữ liệu gốc. Tùy thuộc vào điều kiện và tham số hệ thống cụ thể, chọn lựa mô hình thích hợp (MH1 hoặc MH2) để đạt được hiệu năng hệ thống tốt hơn.

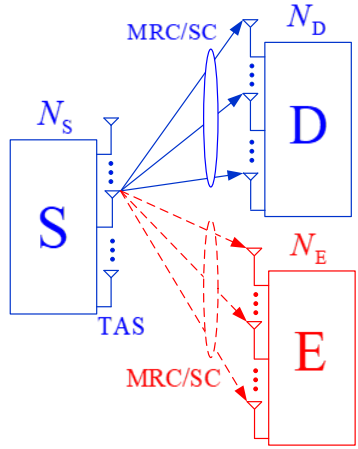
Chương 3

HIỆU NĂNG BẢO MẬT TRONG MẠNG MIMO-NOMA TAS/SC/MRC SỬ DỤNG MÃ FOUNTAIN

Chương 3 đã đề xuất hệ thống MIMO-NOMA sử dụng FC. Nút nguồn (S) đa ăng-ten sử dụng TAS để phát các gói mã hóa đến nút đích (D) đa ăng-ten, trong sự xuất hiện của nút nghe lén (E) đa ăng-ten. Các máy thu D và E sử dụng MRC hoặc SC để nâng cao độ tin cậy giải mã. Quá trình truyền kết thúc khi D nhận đủ gói mã hóa yêu cầu để khôi phục dữ liệu gốc. Tương tự, E cũng có khả năng khôi phục dữ liệu gốc nếu nhận đủ số gói mã hóa cần thiết. Do đó, bảo mật được bảo đảm khi E không nhận đủ số gói mã hóa. Để giảm số khe thời gian truyền được sử dụng, S có thể sử dụng NOMA để gửi hai gói mã hóa đến D tại mỗi khe thời gian.

So sánh hiệu năng giao thức đề xuất trong hai trường hợp với S sử dụng NOMA (NOMA) và không sử dụng NOMA (Wo-NOMA), dựa vào số khe thời gian trung bình (TS) và xác suất thu chặn (IP). Sử dụng NOMA có thể giảm cả TS và IP, so với giao thức Wo-NOMA. Các biểu thức chính xác của TS, IP được đưa ra cho giao thức NOMA và Wo-NOMA trên kênh pha đinh Rayleigh và mô phỏng để kiểm chứng kết quả phân tích lý thuyết.

3.1. Mô hình hệ thống



Hình 3.1: Mô hình hệ thống của giao thức đề xuất.

Mô hình hệ thống đề xuất như Hình 3.1, S trang bị N_S ăng-ten sử dụng FC phát dữ liệu đến D có N_D ăng-ten, trong sự xuất hiện của E với N_E ăng-ten. Tương tự như Chương 2, hệ thống sử dụng FC, dữ liệu gốc của S chia thành L gói, được mã hóa thích hợp để tạo các gói mã hóa. Tại mỗi khe thời gian, S lựa chọn ăng-ten tốt nhất để phát hai (hoặc một) gói mã hóa đến D, những gói mã hóa này cũng được nhận bởi E. Cả D và E cố gắng giải mã gói mã hóa. Để giải mã được dữ liệu gốc, D và E phải nhận chính xác ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa, với $N_{\text{req}}^{\text{pkt}} = (1+\varepsilon)L.$ Khi nhận đủ số gói mã hóa để khôi phục dữ liệu gốc, D gửi thông báo ACK đến S và sau đó S dừng truyền dữ liệu. Nếu E nhận thành công ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa, E cũng có thể phục hồi dữ liệu gốc và do đó dữ liệu nguồn bị thu chặn.

3.2. Phân tích hiệu năng

3.2.1. Số khe thời gian trung bình (TS)

3.2.1.1. Không sử dụng NOMA (Wo-NOMA)

$$\text{TS}= \sum_{N_{\text{TS}}=N_{\text{req}}^{\text{pkt}}}^{+\infty} N_{\text{TS}} \times \Pr\left(N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}} \mid N_{\text{TS}}\right), \tag{3.1}$$

với $\Pr\left(N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}} \mid N_{\text{TS}}\right)$ là xác suất mà D đạt được $N_{\text{req}}^{\text{pkt}}$ gói mã hóa sau N_{TS} khe thời gian. Từ (3.1), ta có biểu thức chính xác TS được tính là

$$\text{TS}= \frac{N_{\text{req}}^{\text{pkt}}}{\rho_{\text{D}}}. \tag{3.2}$$

3.2.1.2. Sử dụng NOMA

$$\text{TS}= \sum_{N_{\text{TS}}=\left\lceil N_{\text{req}}^{\text{pkt}}/2 \right\rceil}^{+\infty} N_{\text{TS}} \times \Pr\left(N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}} \cup N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}}+1 \mid N_{\text{TS}}\right), \tag{3.3}$$

với $\Pr\left(N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}} \cup N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}}+1 \mid N_{\text{TS}}\right)$ là xác suất mà nút đích có thể nhận được $N_{\text{req}}^{\text{pkt}}$ hoặc $N_{\text{req}}^{\text{pkt}}+1$ gói mã hóa sau N_{TS} khe thời gian.

Đặt T_1 và T_2 là số khe thời gian mà D có thể nhận chính xác một và hai gói mã hóa. Để tính $\Pr\left(N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}} \cup N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}}+1 \mid N_{\text{TS}}\right)$, ta xem xét ba

trường hợp: (1) Sau $N_{\mathrm{TS}}-1$ khe thời gian, D đạt được $N_{\mathrm{req}}^{\mathrm{pkt}}-2$ gói mã hóa và tại khe thời gian cuối cùng, D nhận được cả hai gói mã hóa.

$$\theta_{\mathrm{D},1}=\sum_{\mathrm{T}_2=1}^{\left\lfloor N_{\mathrm{req}}^{\mathrm{pkt}}/2\right\rfloor} C_{N_{\mathrm{TS}}-1}^{\mathrm{T}_1} C_{N_{\mathrm{TS}}-\mathrm{T}_1-1}^{\mathrm{T}_2-1}\left(\chi_{\mathrm{D},2}\right)^{\mathrm{T}_2}\left(\chi_{\mathrm{D},1}\right)^{\mathrm{T}_1}\left(\chi_{\mathrm{D},0}\right)^{N_{\mathrm{TS}}-\mathrm{T}_2-\mathrm{T}_1}. \tag{3.4}$$

(2) Sau $N_{\mathrm{TS}}-1$ khe thời gian, D đạt được $N_{\mathrm{req}}^{\mathrm{pkt}}-1$ gói mã hóa và tại khe thời gian cuối cùng, D chỉ nhận được một gói mã hóa.

$$\theta_{\mathrm{D},2}=\sum_{\mathrm{T}_2=0}^{\left\lfloor N_{\mathrm{req}}^{\mathrm{pkt}}/2\right\rfloor} C_{N_{\mathrm{TS}}-1}^{\mathrm{T}_2} C_{N_{\mathrm{TS}}-\mathrm{T}_2-1}^{\mathrm{T}_1-1}\left(\chi_{\mathrm{D},2}\right)^{\mathrm{T}_2}\left(\chi_{\mathrm{D},1}\right)^{\mathrm{T}_1}\left(\chi_{\mathrm{D},0}\right)^{N_{\mathrm{TS}}-\mathrm{T}_2-\mathrm{T}_1}. \tag{3.5}$$

(3) Sau $N_{\mathrm{TS}}-1$ khe thời gian, nút đích đạt được $N_{\mathrm{req}}^{\mathrm{pkt}}-1$ gói mã hóa và tại khe thời gian cuối cùng, D nhận được cả hai gói mã hóa.

$$\theta_{\mathrm{D},3}=\sum_{\mathrm{T}_2=1}^{\left\lceil N_{\mathrm{req}}^{\mathrm{pkt}}/2\right\rceil} C_{N_{\mathrm{TS}}-1}^{\mathrm{T}_1} C_{N_{\mathrm{TS}}-\mathrm{T}_1-1}^{\mathrm{T}_2-1}\left(\chi_{\mathrm{D},2}\right)^{\mathrm{T}_2}\left(\chi_{\mathrm{D},1}\right)^{\mathrm{T}_1}\left(\chi_{\mathrm{D},0}\right)^{N_{\mathrm{TS}}-\mathrm{T}_2-\mathrm{T}_1}. \tag{3.6}$$

Từ (3.3), ta có số khe thời gian trung bình sử dụng trong NOMA là

$$\mathrm{TS}=\sum_{N_{\mathrm{TS}}=\left\lceil N_{\mathrm{req}}^{\mathrm{pkt}}/2\right\rceil}^{+\infty} N_{\mathrm{TS}}\times\left(\theta_{\mathrm{D},1}+\theta_{\mathrm{D},2}+\theta_{\mathrm{D},3}\right). \tag{3.7}$$

Nhận xét: *Từ (3.2) và (3.7), khi SNR phát đủ lớn, $\Delta\to+\infty$, tất cả sự truyền tại các khe thời gian đều thành công, TS giao thức Wo-NOMA và NOMA hội tụ đến $N_{\mathrm{req}}^{\mathrm{pkt}}$ và $\left\lceil N_{\mathrm{req}}^{\mathrm{pkt}}/2\right\rceil$. Sử dụng NOMA có thể giảm một nữa số khe thời gian sử dụng cho truyền các gói mã hóa.*

3.2.2. Xác suất thu chặn (IP)

3.2.2.1. Không sử dụng NOMA (Wo-NOMA)

$$\mathrm{IP}=\sum_{N_{\mathrm{TS}}^{\mathrm{E}}=N_{\mathrm{req}}^{\mathrm{pkt}}}^{+\infty}\left[\begin{array}{l}\left(\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}\mid N_{\mathrm{TS}}^{\mathrm{E}}\right)+\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}}<N_{\mathrm{req}}^{\mathrm{pkt}}\mid N_{\mathrm{TS}}^{\mathrm{E}}\right)\right)\\ \times\Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}\mid N_{\mathrm{TS}}^{\mathrm{E}}\right)\end{array}\right]. \tag{3.8}$$

Công thức (3.8) ngụ ý E có thể nhận được $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa sau $N_{\mathrm{TS}}^{\mathrm{E}}$ khe thời gian, trong khi D có thể nhận đủ hoặc không. Sau khi nhận $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa, E dừng nghe lén dữ liệu truyền và bắt đầu khôi phục dữ liệu, bất kể S vẫn phát các gói mã hóa đến D. Biểu thức IP được tính chính xác là

$$\text{IP}=\sum_{N_{\text{TS}}^{\text{E}}=N_{\text{req}}^{\text{pkt}}}^{+\infty}\left[\begin{array}{l}\left(\begin{array}{l}C_{N_{\text{TS}}^{\text{E}}-1}^{N_{\text{req}}^{\text{pkt}}-1}\left(\rho_{\text{D}}\right)^{N_{\text{req}}^{\text{pkt}}}\left(1-\rho_{\text{D}}\right)^{N_{\text{TS}}^{\text{E}}-N_{\text{req}}^{\text{pkt}}}\\+\sum_{N_{\text{D}}^{\text{pkt}}=0}^{N_{\text{req}}^{\text{pkt}}-1}C_{N_{\text{TS}}^{\text{E}}}^{N_{\text{D}}^{\text{pkt}}}\left(\rho_{\text{D}}\right)^{N_{\text{D}}^{\text{pkt}}}\left(1-\rho_{\text{D}}\right)^{N_{\text{TS}}^{\text{E}}-N_{\text{D}}^{\text{pkt}}}\end{array}\right)\\\times C_{N_{\text{TS}}^{\text{E}}-1}^{N_{\text{req}}^{\text{pkt}}-1}\left(\rho_{\text{E}}\right)^{N_{\text{req}}^{\text{pkt}}}\left(1-\rho_{\text{E}}\right)^{N_{\text{TS}}^{\text{E}}-N_{\text{req}}^{\text{pkt}}}\end{array}\right]. \tag{3.9}$$

3.2.2.2. Sử dụng NOMA

$$\text{IP}=\sum_{N_{\text{TS}}^{\text{E}}=\left\lceil N_{\text{req}}^{\text{pkt}}/2\right\rceil}^{+\infty}\left[\begin{array}{l}\left(\begin{array}{l}\Pr\left(N_{\text{D}}^{\text{pkt}}=N_{\text{req}}^{\text{pkt}}\cup N_{\text{D}}^{\text{pkt}}=N_{\text{req}}^{\text{pkt}}+1\,|\,N_{\text{TS}}^{\text{E}}\right)\\+\Pr\left(N_{\text{D}}^{\text{pkt}}<N_{\text{req}}^{\text{pkt}}\,|\,N_{\text{TS}}^{\text{E}}\right)\end{array}\right)\\\times\Pr\left(N_{\text{E}}^{\text{pkt}}=N_{\text{req}}^{\text{pkt}}\cup N_{\text{E}}^{\text{pkt}}=N_{\text{req}}^{\text{pkt}}+1\,|\,N_{\text{TS}}^{\text{E}}\right)\end{array}\right]. \tag{3.10}$$

Trong (3.10), lưu ý rằng $\theta_{\text{D},1}$, $\theta_{\text{D},2}$ và $\theta_{\text{D},3}$ đạt được bằng cách thay N_{TS} trong (3.4)-(3.6) bởi N_{TS}^{E}. Đối với $\theta_{\text{E},1}$, $\theta_{\text{E},2}$ và $\theta_{\text{E},3}$, phương pháp tương tự được đưa ra như trong $\theta_{\text{D},1}$, $\theta_{\text{D},2}$, $\theta_{\text{D},3}$, ta có thể đạt được

$$\theta_{\text{E},1}=\sum_{\text{V}_2=1}^{\left\lfloor N_{\text{req}}^{\text{pkt}}/2\right\rfloor}C_{N_{\text{TS}}^{\text{E}}-1}^{\text{V}_1}C_{N_{\text{TS}}^{\text{E}}-\text{V}_1-1}^{\text{V}_2-1}\left(\chi_{\text{E},2}\right)^{\text{V}_2}\left(\chi_{\text{E},1}\right)^{\text{V}_1}\left(\chi_{\text{E},0}\right)^{N_{\text{TS}}^{\text{E}}-\text{V}_2-\text{V}_1}, \tag{3.11}$$

$$\theta_{\text{E},2}=\sum_{\text{V}_2=0}^{\left\lfloor N_{\text{req}}^{\text{pkt}}/2\right\rfloor}C_{N_{\text{TS}}^{\text{E}}-1}^{\text{V}_2}C_{N_{\text{TS}}^{\text{E}}-\text{V}_2-1}^{\text{V}_1-1}\left(\chi_{\text{E},2}\right)^{\text{V}_2}\left(\chi_{\text{E},1}\right)^{\text{V}_1}\left(\chi_{\text{E},0}\right)^{N_{\text{TS}}^{\text{E}}-\text{V}_2-\text{V}_1}, \tag{3.12}$$

$$\theta_{\text{E},3}=\sum_{\text{V}_2=1}^{\left\lceil N_{\text{req}}^{\text{pkt}}/2\right\rceil}C_{N_{\text{TS}}^{\text{E}}-1}^{\text{V}_1}C_{N_{\text{TS}}^{\text{E}}-\text{V}_1-1}^{\text{V}_2-1}\left(\chi_{\text{E},2}\right)^{\text{V}_2}\left(\chi_{\text{E},1}\right)^{\text{V}_1}\left(\chi_{\text{E},0}\right)^{N_{\text{TS}}^{\text{E}}-\text{V}_2-\text{V}_1}, \tag{3.13}$$

V_1 và V_2 là số khe thời gian mà E nhận chính xác một và hai gói mã hóa.

Xác suất D không thu được $N_{\text{req}}^{\text{pkt}}$ gói mã hóa sau N_{TS}^{E} khe thời gian là $\Pr\left(N_{\text{D}}^{\text{pkt}}<N_{\text{req}}^{\text{pkt}}\,|\,N_{\text{TS}}^{\text{E}}\right)\square\ \theta_{\text{D},4}$

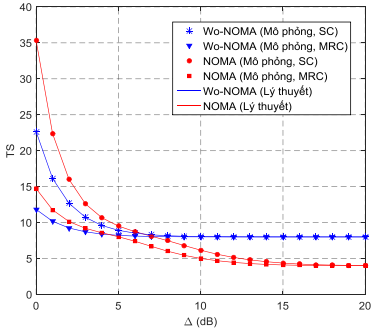
$$=\sum_{N_{\text{D}}^{\text{pkt}}=0}^{N_{\text{req}}^{\text{pkt}}-1}\sum_{\text{T}_2=0}^{\left\lfloor N_{\text{D}}^{\text{pkt}}/2\right\rfloor}C_{N_{\text{TS}}^{\text{E}}}^{\text{T}_2}C_{N_{\text{TS}}^{\text{E}}-\text{T}_2}^{\text{T}_1}\left(\chi_{\text{D},2}\right)^{\text{T}_2}\left(\chi_{\text{D},1}\right)^{\text{T}_1}\left(\chi_{\text{D},0}\right)^{N_{\text{TS}}^{\text{E}}-\text{T}_2-\text{T}_1}. \tag{3.14}$$

IP trong giao thức NOMA được viết lại như sau:

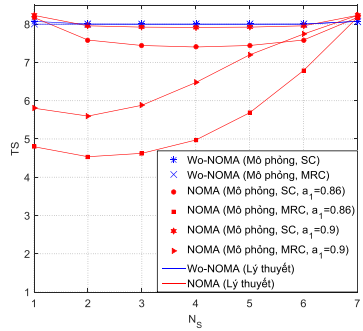
$$\text{IP}=\sum_{N_{\text{TS}}^{\text{E}}=\left\lceil N_{\text{req}}^{\text{pkt}}/2\right\rceil}^{+\infty}\left[\left(\theta_{\text{D},1}+\theta_{\text{D},2}+\theta_{\text{D},3}+\theta_{\text{D},4}\right)\times\left(\theta_{\text{E},1}+\theta_{\text{E},2}+\theta_{\text{E},3}\right)\right]. \tag{3.15}$$

3.3. Các kết quả mô phỏng

Tác giả sử dụng mô phỏng Monte Carlo để kiểm chứng kết quả lý thuyết, chuỗi vô hạn trong công thức tính toán cắt bởi 500 số hạng đầu tiên.



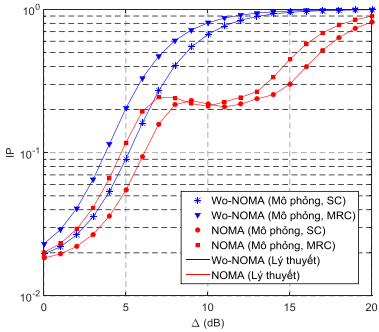
Hình 3.2: TS là hàm của $\Delta(\mathrm{dB})$ khi $N_S = 1,\ N_D = 3,\quad \lambda_{SD} = 2,\ N_{req}^{pkt} = 8,$ $a_1 = 0.9,\ \gamma_{th} = 1.$



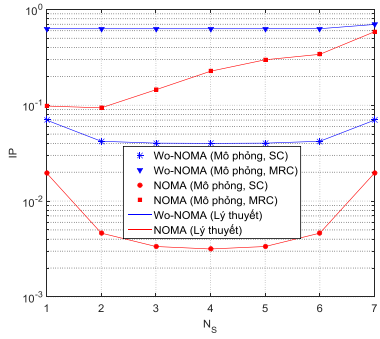
Hình 3.3: TS là hàm của N_S khi $\Delta = 8(\mathrm{dB}),\ N_D + N_S = 8,$ $\lambda_{SD} = 3,\ N_{req}^{pkt} = 8,\ \gamma_{th} = 1.5.$

Hình 3.2, giá trị của a_1 phải thỏa mãn điều kiện: $a_1 > (1+\gamma_{th})a_2$ hoặc $a_1 > (1+\gamma_{th})/(2+\gamma_{th}) = 2/3,$ nên ta chọn $a_1 = 0.9$ $(a_2 = 0.1).$ TS của Wo-NOMA và NOMA giảm khi tăng Δ và thấp hơn khi D sử dụng MRC. Tại Δ cao, TS của Wo-NOMA hội tụ đến N_{req}^{pkt}, trong khi NOMA đạt $N_{req}^{pkt}/2.$ Khi SNR phát cao, D trong NOMA có thể nhận hai gói mã hóa tại mỗi khe thời gian, S chỉ sử dụng $N_{req}^{pkt}/2$ khe thời gian truyền. Tuy nhiên, NOMA không tốt tại Δ thấp khi NOMA dùng nhiều khe thời gian hơn Wo-NOMA.

Hình 3.3, Wo-NOMA gần như sử dụng 8 khe thời gian cho truyền gói mã hóa, với tất cả N_S. Giao thức NOMA, TS biến đổi khi thay đổi số ăng-ten N_S từ 1 đến 7. Sử dụng SC, TS của NOMA giống nhau khi số ăng-ten tại S là N_S và $8 - N_S$. TS thấp nhất khi $N_S = N_D = 4,$ khi D sử dụng MRC, giá trị tối ưu N_S là 2 $(N_D = 6)$, và TS kém nhất khi $N_S = 7,$ do MRC là tốt hơn SC. Cuối cùng, có thể thấy TS của giao thức NOMA với $a_1 = 0.86$ $(a_2 = 0.14)$ thấp hơn giá trị $a_1 = 0.9$ $(a_2 = 0.1).$



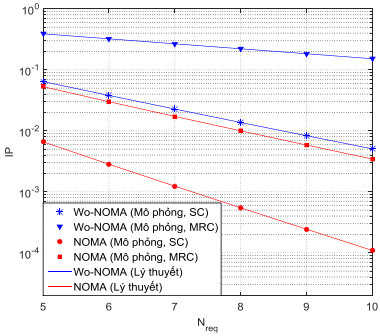
Hình 3.4: IP là hàm $\Delta(\text{dB})$ khi $N_S = 3,\ N_D = N_E = 2,\ \lambda_{SD} = 2.5,$ $\lambda_{SE} = 2.5,\quad N_{req}^{pkt} = 8,\ a_1 = 0.9$ và $\gamma_{th} = 1.$



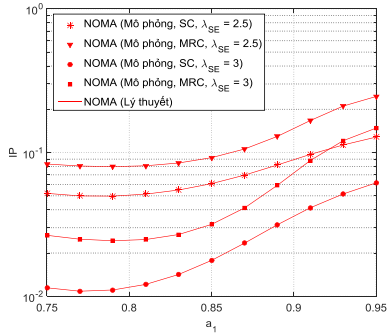
Hình 3.5: IP là hàm của N_S khi $\Delta = 5(\text{dB}),\quad N_D + N_S = 8,\ N_E = 4,$ $\lambda_{SD} = 2,\ \lambda_{SE} = 3,\ N_{req}^{pkt} = 8,$ $a_1 = 0.9$ và $\gamma_{th} = 1.5.$

Hình 3.4, IP của Wo-NOMA và NOMA tăng khi tăng SNR phát. NOMA thuộc khoảng $(8\text{ dB},\ 10\text{ dB})$, IP giảm nhẹ khi tăng Δ, tồn tại một khoảng hiệu năng cao giữa Wo-NOMA và NOMA trong đoạn này. Bởi vì IP tại E phụ thuộc vào trạng thái giải mã tại D và nhiễu giữa các tín hiệu, thay đổi IP trong NOMA phức tạp hơn Wo-NOMA, xét trên Δ. Khi Δ đủ lớn, các gói mã hóa có thể nhận chính xác bởi D và E. Trường hợp này, D và E có thể đạt N_{req}^{pkt} gói mã hóa tại cùng thời điểm, IP hội tụ tới 1. Khi D và E sử dụng MRC, IP giao thức đề xuất cao hơn, do khả năng thu chặn của E tốt hơn khi trang bị MRC. Cuối cùng, NOMA đạt hiệu năng IP tốt hơn Wo-NOMA.

Hình 3.5, D và E sử dụng SC, IP thấp nhất $N_S = N_D = 4,$ và sử dụng MRC, giá trị tối ưu của N_S là 2. Hiệu năng IP của Wo-NOMA biến đổi nhẹ khi thay đổi $N_S,$ nhưng NOMA biến đổi đáng kể. NOMA đạt hiệu năng tốt hơn Wo-NOMA và khi E sử dụng MRC thì IP không tốt. Nếu giá trị mong muốn IP là (dưới) 0.1, cả Wo-NOMA và NOMA không thể triển khai. Trường hợp này, để giảm IP, S có thể giảm công suất phát hoặc thiết kế các tham số hệ thống N_{req}^{pkt} và a_1 phù hợp.



Hình 3.6: IP là hàm của $N_{\text{req}}^{\text{pkt}}$ khi $\Delta = 5(\text{dB}),\ N_{\text{S}} = N_{\text{D}} = 3,\ N_{\text{E}} = 3,$ $\lambda_{\text{SD}} = 2,\ \lambda_{\text{SE}} = 3,\ a_1 = 0.85,$ $\gamma_{\text{th}} = 1.5.$



Hình 3.7: IP là hàm của a_1 khi $\Delta = 7.5(\text{dB}),\quad N_{\text{S}} = N_{\text{D}} = N_{\text{E}} = 2,$ $\lambda_{\text{SD}} = 2,\ N_{\text{req}}^{\text{pkt}} = 8,\ \gamma_{\text{th}} = 1.5.$

Hình 3.6, IP giảm khi $N_{\text{req}}^{\text{pkt}}$ tăng, với giả sử D và E trang bị MRC, NOMA có thể được sử dụng để đạt bảo mật cao hơn hoặc trường hợp nút nguồn trong giao thức Wo-NOMA có thể tăng số gói $N_{\text{req}}^{\text{pkt}}$ để giảm IP.

Hình 3.7, a_1 phải được thiết kế sao cho $a_1 > (1+\gamma_{\text{th}})/(2+\gamma_{\text{th}}) = 0.7143.$ nên lựa chọn khoảng a_1 là $(0.75,\ 0.95)$ và có thể thấy rằng tồn tại các giá trị tối ưu của a_1 để IP đạt thấp nhất.

3.4. Kết luận chương

Giao thức NOMA sử dụng FC không chỉ giảm số khe thời gian truyền dẫn mà còn nâng cao bảo mật. NOMA có thể giảm một nữa số khe thời gian so với Wo-NOMA. Truyền bảo mật, IP giảm đáng kể khi S sử dụng NOMA để phát hai gói mã hóa đến D tại mỗi khe thời gian. Các biểu thức chính xác của TS và IP được đưa ra, xác nhận bằng mô phỏng. Hiệu năng của Wo-NOMA và NOMA được nâng cao bằng cách tăng hoặc thiết kế số ăng-ten tối ưu tại S và D, lựa chọn thích hợp khoảng công suất phát phân bổ các tín hiệu NOMA và tăng số gói mã hóa yêu cầu khôi phục dữ liệu.

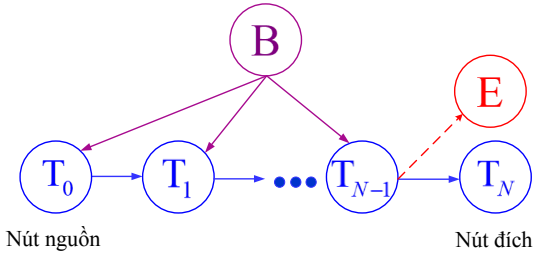
Chương 4

HIỆU NĂNG BẢO MẬT TRONG CÁC MẠNG CHUYỂN TIẾP ĐA CHẶNG SỬ DỤNG MÃ FOUNTAIN

Trong Chương 4, Luận án đề xuất hai mô hình để phân tích sự đánh đổi giữa hiệu quả bảo mật và độ tin cậy trong các mạng chuyển tiếp đa chặng sử dụng FC, bao gồm: Phần 4.1 trình bày mô hình đề xuất mạng chuyển tiếp đa chặng sử dụng mã Fountain với kỹ thuật thu thập năng lượng sóng vô tuyến từ trạm Beacon (EH-Beacon) dưới tác động của suy giảm phần cứng và Phần 4.2 đánh giá mô hình đề xuất của giao thức đa chặng LEACH sử dụng mã Fountain và gây nhiễu cộng tác.

4.1. Mô hình 1: Mạng chuyển tiếp đa chặng sử dụng mã Fountain với thu thập năng lượng sóng vô tuyến

4.1.1. Mô hình hệ thống



Hình 4.1: Mô hình hệ thống của giao thức đề xuất.

Như thể hiện trong Hình 4.1, nút nguồn (T_0) gửi dữ liệu tới nút đích (T_N) dựa vào $N-1$ nút chuyển tiếp, $T_1, T_2, ..., T_{N-1}$. Giả sử các máy phát như nút nguồn và nút chuyển tiếp là các thiết bị vô tuyến ràng buộc mức năng lượng, nên phải thu thập năng lượng từ trạm phát sóng vô tuyến (Beacon: B) được triển khai trong mạng. Trong mạng này, nút nghe lén (E) xuất hiện xung quanh T_N, do đó E có thể nghe lén dữ liệu phát đến nút này. Bởi vì E gần với T_N, nên giả sử E chỉ nhận được dữ liệu được phát từ nút chuyển tiếp T_{N-1}. Giả sử các thiết bị đầu cuối là đơn ăng-ten và hoạt động ở chế độ bán song công, sử dụng phương pháp TDMA để gửi các gói mã hóa từ nút nguồn đến nút đích dựa vào N khe thời gian trực giao.

Sử dụng FC, nút nguồn chia dữ liệu gốc thành L gói và XOR để tạo các gói Fountain. Hệ thống ràng buộc độ trễ, số khe thời gian tối đa phát các gói mã hóa giới hạn bởi $N_{\max}$, nút nguồn sẽ dừng truyền sau khi gửi $N_{\max}$ gói Fountain tới nút đích. Để khôi phục dữ liệu, nút đích và nút nghe lén phải nhận thành công ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa trong $N_{\max}$ khe thời gian, với $N_{\text{req}}^{\text{pkt}} = (1+\varepsilon)L$ và $N_{\text{req}}^{\text{pkt}} \le N_{\max}$. Ta có $N_{\text{D}}^{\text{pkt}}$ và $N_{\text{E}}^{\text{pkt}}$ là số gói mã hóa mà nút đích và nút nghe lén có thể thu được sau $N_{\max}$ khe thời gian. Nếu $N_{\text{D}}^{\text{pkt}} \ge N_{\text{req}}^{\text{pkt}}$, nút đích có thể khôi phục dữ liệu gốc. Nếu $N_{\text{D}}^{\text{pkt}} < N_{\text{req}}^{\text{pkt}}$, xác suất dừng xảy ra và trường hợp tại nút E, nếu $N_{\text{E}}^{\text{pkt}} \ge N_{\text{req}}^{\text{pkt}}$, dữ liệu bị thu chặn và nếu $N_{\text{E}}^{\text{pkt}} < N_{\text{req}}^{\text{pkt}}$, truyền dữ liệu được bảo mật.

Giả sử kênh pha đinh không đối xứng, với kênh dữ liệu và kênh nghe lén là pha đinh Rice, trong khi kênh thu thập năng lượng sóng vô tuyến (EH) từ trạm Beacon là kênh pha đinh Rayleigh, hệ thống sử dụng kỹ thuật giải mã và chuyển tiếp (DF) để chuyển tiếp tín hiệu. Thực tế, do nhiễu pha, không cân bằng I/Q và bộ khuếch đại không tuyến tính, tác giả khảo sát ảnh hưởng suy giảm phần cứng các thiết bị trong mạng lên hiệu năng hệ thống.

Xác suất dừng (OP) tại T_N và xác suất thu chặn (IP) tại E được tính bởi

$$\text{OP} = \Pr\left(N_{\text{D}}^{\text{pkt}} < N_{\text{req}}^{\text{pkt}} \mid N_{\max}\right), \quad \text{IP} = \Pr\left(N_{\text{E}}^{\text{pkt}} \ge N_{\text{req}}^{\text{pkt}} \mid N_{\max}\right). \tag{4.1}$$

4.1.2. Phân tích hiệu năng

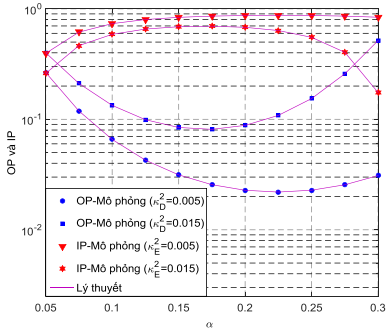
Từ (4.1), biểu thức chính xác của OP được cho bởi như sau:

$$\text{OP} = \sum_{N_{\text{D}}^{\text{pkt}}=0}^{N_{\text{req}}^{\text{pkt}}-1} C_{N_{\max}}^{N_{\text{D}}^{\text{pkt}}} \rho_{\text{D}}^{N_{\text{D}}^{\text{pkt}}} \left(1-\rho_{\text{D}}\right)^{N_{\max}-N_{\text{D}}^{\text{pkt}}}. \tag{4.2}$$

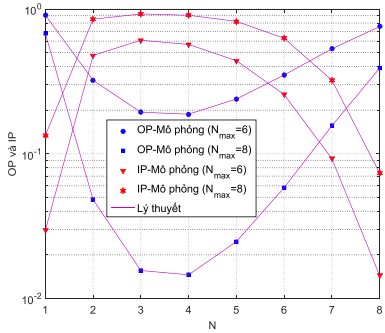
Biểu thức (4.2) có nghĩa rằng nút đích không thể khôi phục dữ liệu gốc của nút nguồn bởi vì số gói Fountain nhận được ít hơn $N_{\text{req}}^{\text{pkt}}$, các giá trị có khả năng của $N_{\text{D}}^{\text{pkt}}$ là từ 0 đến $N_{\text{req}}^{\text{pkt}}-1$ và có $C_{N_{\max}}^{N_{\text{D}}^{\text{pkt}}}$ khả năng cho mỗi giá trị của $N_{\text{D}}^{\text{pkt}}$. Cũng vậy, xác suất thu chặn (IP) có thể được tính là

$$\text{IP} = \sum_{N_{\text{E}}^{\text{pkt}}=N_{\text{req}}^{\text{pkt}}}^{N_{\max}} C_{N_{\max}}^{N_{\text{E}}^{\text{pkt}}} \rho_{\text{E}}^{N_{\text{E}}^{\text{pkt}}} \left(1-\rho_{\text{E}}\right)^{N_{\max}-N_{\text{E}}^{\text{pkt}}}. \tag{4.3}$$

4.1.3. Các kết quả mô phỏng



Hình 4.2: OP và IP là hàm của α khi $\Delta = 5(\text{dB})$, $N = 4$, $K_D = 20$, $K_E = 1$, $C_{th} = 1$, $N_{max} = 8$ và $N_{req}^{pkt} = 5$.



Hình 4.3: OP và IP là hàm của N khi $\Delta = 3(\text{dB})$, $K_D = 20$, $K_E = 1$, $\kappa_D^2 = \kappa_E^2 = 0$, $C_{th} = 0.9$ và $N_{req}^{pkt} = 5$.

Hình 4.2 thể hiện tồn tại các giá trị α để OP nhỏ nhất và IP lớn nhất. Ví dụ, khi $\kappa_D^2 = \kappa_E^2 = 0.015$, OP tốt nhất và IP cao nhất đạt được tại $\alpha = 0.175$. Mặt khác, OP cao hơn và IP thấp hơn khi mức suy giảm phần cứng κ_D^2 và κ_E^2 tăng.

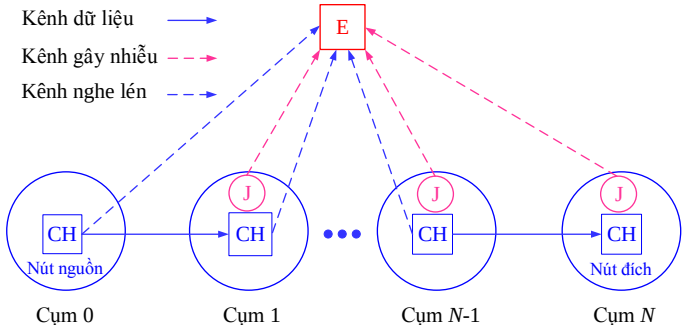
Hình 4.3, giá trị tối ưu của OP đạt được tại $N = 4$ và khi tăng giá trị N_{max} từ 6 đến 8, OP giảm. Khi tăng số khe thời gian sử dụng truyền các gói Fountain (N_{max}) làm tăng IP, do E có nhiều cơ hội hơn nhận đủ gói mã hóa.

4.2. Mô hình 2: Giao thức chuyển tiếp đa chặng LEACH sử dụng mã Fountain và nút gây nhiễu cộng tác

4.2.1. Mô hình hệ thống

Hình 4.4 thể hiện mô hình hệ thống giao thức đề xuất, nút nguồn (CH cụm 0) truyền dữ liệu đến nút đích (CH cụm *N*) dựa vào giao thức đa chặng LEACH với sự hỗ trợ của nhiều nút chuyển tiếp. Sử dụng FC, dữ liệu nguồn chia *L* gói rồi được mã hóa thích hợp để tạo các gói mã hóa. Tiếp theo, nút nguồn phát các gói mã hóa đến nút đích. Giả sử tất cả các CH trang bị đơn ăng-ten, do đó truyền dữ liệu của mỗi gói mã hóa thực hiện thông qua *N* khe thời gian trực giao, theo phương pháp TDMA. Để bảo đảm an toàn truyền

dữ liệu dưới sự tấn công của nút nghe lén, mỗi cụm (cluster) lựa chọn ngẫu nhiên một nút cụm để thực hiện hoạt động gây nhiễu cộng tác.



Hình 4.4: Mô hình hệ thống của giao thức đề xuất.

Trong giao thức đề xuất, nút nghe lén (E) cố gắng nhận các gói mã hóa để khôi phục dữ liệu nguồn. Đặt $N_{\max}$ là số gói mã hóa tối đa mà nút nguồn có thể gửi đến nút đích, với $N_{\max} \geq N_{\text{req}}^{\text{pkt}}$, sau khi gửi $N_{\max}$ gói, nút nguồn sẽ dừng truyền. Nếu đích không nhận thành công ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa thì không thể khôi phục dữ liệu gốc, xảy ra dừng hệ thống. Ngược lại, truyền dữ liệu giữa nguồn và đích là thành công. Đối với E, nếu E nhận ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa, dữ liệu nguồn bị thu chặn. Giả sử các kênh truyền là pha đinh Rayleigh, sử dụng chuyển tiếp DF. Hơn nữa, khi sử dụng gây nhiễu cộng tác (CJ), giả sử CH cụm thứ n có thể loại bỏ hoàn toàn nhiễu tạo ra bởi các nút gây nhiễu được lựa chọn, trong khi E không thể loại bỏ được nhiễu.

4.2.2. Phân tích hiệu năng

Như được đề cập ở trên, xác suất dừng (OP) của kênh dữ liệu là xác suất mà nút đích không thể nhận thành công ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa sau khi nút nguồn phát $N_{\max}$ khe thời gian. Do đó, OP có thể được tính bởi

$$\text{OP} = \sum_{r=0}^{N_{\text{req}}^{\text{pkt}}-1} C_{N_{\max}}^{r} \left(\rho_{\text{D}}\right)^{r} \left(1-\rho_{\text{D}}\right)^{N_{\max}-r}. \tag{4.4}$$

Biểu thức (4.4) ngụ ý rằng sau khi nút nguồn dừng truyền, nút đích chỉ nhận được r gói mã hóa, với $0 \leq r \leq N_{\text{req}}^{\text{pkt}} - 1$.

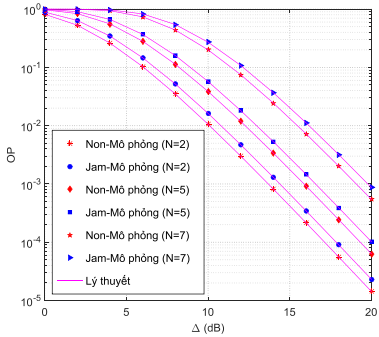
Xác suất thu chặn (IP), có thể được tính toán là

$$\mathrm{IP} = \sum_{w=N_{\mathrm{req}}^{\mathrm{pkt}}}^{N_{\max}} C_{N_{\max}}^{w} \left(\rho_{\mathrm{E}}\right)^{w} \left(1-\rho_{\mathrm{E}}\right)^{N_{\max}-w}. \tag{4.5}$$

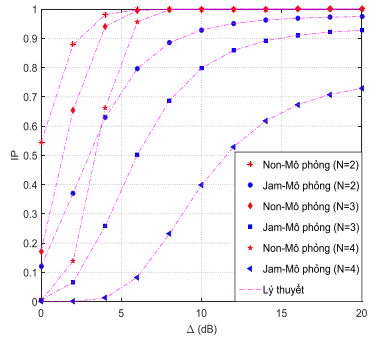
Trong (4.5), khi E có thể đạt được w gói mã hóa, với $N_{\mathrm{req}}^{\mathrm{pkt}} \le w \le N_{\max}$, E có thể khôi phục dữ liệu gốc và do đó dữ liệu nguồn bị thu chặn.

4.2.3. Các kết quả mô phỏng

Trong phần này, mô phỏng Monte Carlo được thực hiện để kiểm chứng các kết quả lý thuyết, so sánh hiệu năng của giao thức đề xuất (Jam) và giao thức LEACH truyền thống (Non).



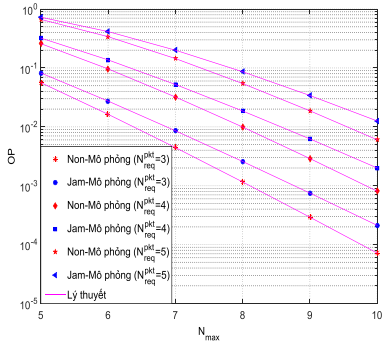
Hình 4.5: OP là hàm của Δ (dB) khi $\alpha = 0.85$, $N_{\mathrm{req}}^{\mathrm{pkt}} = 5$ và $N_{\max} = 7$.



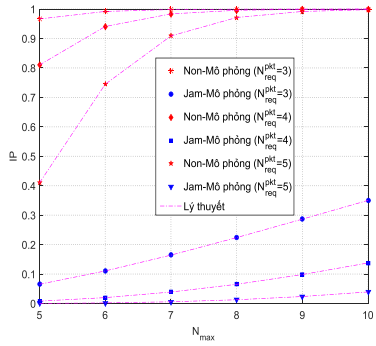
Hình 4.6: IP là hàm của Δ (dB) khi $\alpha = 0.85$, $N_{\mathrm{req}}^{\mathrm{pkt}} = 5$ và $N_{\max} = 7$.

Trong các Hình 4.5 và Hình 4.6, khoảng α cố định bằng 0.85 và giá trị của $N_{\mathrm{req}}^{\mathrm{pkt}}$ và $N_{\max}$ được gán bởi 5 và 7. Hình 4.5, OP giảm khi tăng Δ và OP của giao thức đề xuất (Jam) cao hơn giao thức không gây nhiễu (Non), do công suất phát các CH trong giao thức (Non) lớn hơn. Cũng nhận thấy từ Hình 4.5, OP các giao thức kém hơn khi tăng số chặng. Hình 4.6, IP tăng nhanh khi tăng Δ và IP của giao thức (Jam) thấp hơn nhiều so với (Non). Thêm vào đó, IP giảm khi tăng số chặng giữa nút nguồn và nút đích (N).

Hình 4.7, OP các giao thức xem xét tốt hơn khi $N_{\mathrm{req}}^{\mathrm{pkt}}$ giảm và $N_{\max}$ tăng. Thật vậy, với giá trị thấp hơn của $N_{\mathrm{req}}^{\mathrm{pkt}}$ và cao hơn của $N_{\max}$, xác suất mà nút đích nhận đủ số gói mã hóa tăng, điều này làm giảm xác suất dừng.



Hình 4.7: OP là hàm của $N_{\max}$ khi $\Delta = 7.5\text{dB},\ \alpha = 0.85$ và $N = 5$.



Hình 4.8: IP là hàm của $N_{\max}$ khi $\Delta = 7.5\text{dB},\ \alpha = 0.85$ và $N = 5$.

Tuy nhiên, Hình 4.8, các giá trị IP cũng tăng khi $N_{\text{req}}^{\text{pkt}}$ giảm và $N_{\max}$ tăng. Do đó, các giá trị của $N_{\text{req}}^{\text{pkt}}$ và $N_{\max}$ nên được thiết kế phù hợp để bảo đảm chất lượng dịch vụ (QoS) (OP) và bảo mật (IP). Ví dụ, trong giao thức đề xuất, để thỏa mãn yêu cầu QoS của $\text{OP} \le 0.01$ và mức độ bảo mật $\text{IP} \le 0.1$, ta phải thiết lập các giá trị của $N_{\text{req}}^{\text{pkt}}$ và $N_{\max}$ bằng 4 và 9.

4.3. Kết luận chương

Đề xuất trong mô hình 1 khảo sát sự đánh đổi giữa bảo mật và độ tin cậy trong mạng chuyển tiếp đa chặng sử dụng FC thu thập năng lượng sóng vô tuyến dựa vào trạm Beacon dưới tác động của suy giảm phần cứng. Hiệu năng xác suất dừng được nâng cao bằng cách tăng SNR phát, lựa chọn số chặng phù hợp và thiết kế khoảng tối ưu cho pha thu thập năng lượng. Tuy nhiên, các kết quả cũng thể hiện xác suất thu chặn tăng khi giảm xác suất dừng. Do đó, các tham số hệ thống nên được thiết kế phù hợp để giao thức đề xuất có thể đạt được QoS mong muốn và xác suất thu chặn là nhỏ nhất có thể.

Các kết quả trong mô hình đề xuất 2 đã đánh giá hiệu năng hệ thống thông qua các biểu thức OP và IP và thể hiện rằng tồn tại sự đánh đổi giữa bảo mật và độ tin cậy của truyền dữ liệu. Do vậy, các tham số hệ thống như số chặng, khoảng công suất phát được phân bổ để tạo nhiễu giả, số gói mã hóa yêu cầu khôi phục dữ liệu nguồn và số lần truyền tối đa tại nút nguồn nên được thiết kế thích hợp để có thể bảo đảm cả bảo mật và QoS.

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN CỦA LUẬN ÁN

1. Một số kết quả đạt được của luận án

Luận án đã đề xuất một số mô hình để cải thiện hiệu năng bảo mật trong các mạng vô tuyến. Một số đóng góp chính có thể được liệt kê như sau:

• Nghiên cứu hiệu năng bảo mật lớp vật lý của các giao thức đề xuất sử dụng FC, bao gồm: i) MISO TAS trong mạng vô tuyến nhận thức dạng nền dưới tác động chung của giao thoa đồng kênh từ mạng sơ cấp và suy giảm phần cứng; ii) MIMO TAS/SC dưới tác động của nhiều nguồn giao thoa đồng kênh, với kịch bản có và không có CSI đến các nguồn giao thoa.

• Đề xuất và phân tích hiệu năng của FC dựa vào giao thức bảo mật trong hệ thống MIMO-NOMA TAS/SC/MRC và thể hiện sử dụng NOMA đạt hiệu năng bảo mật tốt hơn tại SNR trung bình và cao so với Wo-NOMA.

• Phân tích độ tin cậy và bảo mật trong mạng chuyển tiếp đa chặng sử dụng FC với các mô hình đề xuất. Các tham số như số chặng, khoảng thời gian thu thập năng lượng, công suất phát nhiễu giả, số gói mã hóa yêu cầu, số lần truyền tối đa nên thiết kế phù hợp để bảo đảm cả bảo mật và QoS.

• Hơn nữa, một trong những đóng góp quan trọng nhất của luận án là phân tích hiệu năng bảo mật giao thức đề xuất bằng cách đưa ra các biểu thức chính xác trên kênh truyền pha đinh Rayleigh. Những đóng góp này giúp các nhà nghiên cứu hoặc thiết kế hệ thống thực hiện so sánh giao các thức mạng, kỹ thuật phân tập, mã hóa,… xác định những lựa chọn tối ưu dưới những điều kiện ràng buộc được đưa ra trong mạng.

2. Hướng phát triển của luận án

Xuất phát từ những kết quả đạt được của luận án, để phát triển hướng nghiên cứu của đề tài trong hệ thống sử dụng FC, một số vấn đề cần được tiếp tục mở rộng để thực hiện khảo sát trong tương lai.

• Mở rộng các giao thức này trong những kịch bản khác nhau, như mối quan hệ giữa IP (OP) và trong môi trường vô tuyến nhận thức.

• Phân tích hiệu năng mạng dưới tác động đồng thời của giao thoa đồng kênh và suy giảm phần cứng hoặc thu thập năng lượng sóng vô tuyến để tạo nhiễu giả đến nút nghe lén.

• Phân tích với các giao thức cộng tác, lựa chọn nút chuyển tiếp.

• Phân tích giao thức trên các kênh truyền khác như Nakagami-*m*.