ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

PHẠM HỮU TÙNG

ĐÁNH GIÁ HIỆU NĂNG BẢO MẬT TẦNG VẬT LÝ TRONG MẠNG NOMA

LUẬN ÁN TIẾN SĨ
MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG DỮ LIỆU

Tập thể hướng dẫn khoa học:
1. PGS.TS Nguyễn Đình Việt
2. TS. Trần Hùng

Hà Nội - 2024

LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu do tôi thực hiện. Các kết quả nghiên cứu, số liệu và kết luận trong luận án này là trung thực và chưa từng được công bố trên bất kỳ công trình nào khác. Các nội dung tham khảo từ các nguồn tài liệu đã được thực hiện trích dẫn và ghi nguồn gốc tài liệu tham khảo đúng quy định.

Hà Nội, tháng 06 năm 2024

Tác giả

Phạm Hữu Tùng

LỜI CẢM ƠN

Luận án tiến sĩ này được thực hiện tại trường Đại học Công nghệ - Đại học Quốc gia Hà Nội dưới sự hướng dẫn tận tình của tập thể cán bộ hướng dẫn PGS.TS Nguyễn Đình Việt và TS Trần Hùng. Tác giả xin được bày tỏ lòng biết ơn tới các thầy hướng dẫn đã định hướng, truyền đạt kiến thức, kinh nghiệm nghiên cứu, chỉ bảo tận tình, hỗ trợ và tạo điều kiện thuận lợi trong suốt quá trình tác giả thực hiện luận án.

Tác giả xin được trân trọng cảm ơn TS Võ Nhân Văn, TS Quách Xuân Trưởng, Ths Ninh Thị Thanh Tâm, Ths Nguyễn Yến Chi đã hỗ trợ, giúp đỡ, cộng tác, trao đổi thảo luận về mặt chuyên môn. Ngoài ra Tôi xin cảm ơn các tác giả của các công trình khoa học được trích dẫn trong luận án đã cung cấp kiến thức liên quan và là nguồn học liệu quan trọng trong quá trình nghiên cứu và hoàn thành luận án này.

Tác giả xin chân thành cảm ơn các Thầy/cô lãnh đạo Trường Đại học Công Nghệ - Đại học Quốc gia Hà Nội, các phòng ban chức năng, Khoa Công nghệ thông tin và tập thể các giảng viên Bộ môn Mạng và truyền thông máy tính đã luôn quan tâm giúp đỡ, tạo các điều kiện thuận lợi, có những ý kiến đóng góp quý báu cho tác giả trong quá trình học tập, và nghiên cứu tại trường.

Tác giả xin gửi lời cảm ơn đến tập thể Lãnh đạo, các đồng nghiệp Trường Đại học Xây dựng Hà Nội đã luôn tạo điều kiện thuận lợi, giúp đỡ tác giả trong quá trình học tập và nghiên cứu.

Cuối cùng, tác giả xin được bày tỏ lòng biết ơn tới gia đình hai bên nội ngoại, đặc biệt là vợ và hai con của Tôi đã luôn đồng hành, động viên và tạo mọi điều kiện tốt nhất để Tôi có thể chuyên tâm nghiên cứu. Tôi xin chân thành cảm ơn người thân và bạn bè thân thiết đã thường xuyên động viên, chia sẻ và hỗ trợ về mọi mặt trong cuộc sống để tác giả có thể hoàn thành luận án.

MỤC LỤC

Danh sách hình vẽ

DANH MỤC CÁC KÝ HIỆU

$f_X(x)$	Hàm PDF của biến ngẫu nhiên X
$F_X(x)$	Hàm CDF của biến ngẫu nhiên X
$E[X]$	Giá trị kỳ vọng của biến ngẫu nhiên X
$exp(x)$	e^x
$Pr\{.\}$	Biểu thức xác suất
R_s	Tốc độ truyền tin bảo mật
R	Ngưỡng tốc độ truyền tin tối thiểu
W	Băng thông của kênh truyền
N_0	Công suất nhiễu AWGN
P	Công suất truyền tin
Ω	Độ lợi trung bình của kênh truyền
γ	Tỉ số tín hiệu trên tạp âm hoặc trên nhiễu và tạp âm (SNR hoặc SINR)
C	Dung lượng của kênh truyền
C_m	Dung lượng kênh hợp pháp
C_e	Dung lượng kênh nghe lén
C_s	Dung lượng bảo mật của kênh truyền
$\mathcal{CN}(0, \sigma^2)$	Nhiễu Gaussian phức đối xứng vòng giá trị trung bình bằng 0 và phương sai bằng σ^2
$\mathcal{N}(0, \sigma^2)$	Nhiễu Gaussian thực giá trị trung bình bằng 0 và phương sai bằng σ^2
$\mathcal{O}_{sec}$	Xác suất dừng bảo mật
$\mathcal{O}_{suc}$	Xác suất nghe lén thành công
$\mathcal{O}_{int}$	Xác suất bị nghe lén
$\mathcal{O}_{out}^P$	Xác suất dừng hoạt động mạng sơ cấp
$\mathcal{O}_{out}$	Xác suất dừng hoạt động mạng thứ cấp
$\mathcal{O}_{otm}$	Xác suất rớt gói tin
$\inf R$	Cận dưới đúng của tập các giá trị R
$arg\{x\}$	Hàm trả về chỉ số của giá trị trong dãy
$\{.\}^+$	Lấy giá trị dương

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Từ gốc	Giải nghĩa - Tạm dịch
5G	The Fifth Generation	Mạng di động thế hệ thứ năm
AF	Amplify-and-Forward	Khuếch đại và chuyển tiếp
AES	Advanced Encryption Standard	Chuẩn mã hóa tiên tiến
APS	Active Protection Scheme	Cơ chế đối phó chủ động
AWGN	Additive White Gaussian Noise	Tạp âm Gauss trắng cộng
BS	Base station	Trạm cơ sở
CC	Cooperative Communication	Truyền thông hợp tác
CD-NOMA	Code-Domain NOMA	Mạng NOMA nghép kênh theo miền mã
CDF	Cumulative Distribution Function	Hàm phân phối xác suất tích lũy
CRN	Cognitive Radio Network	Mạng vô tuyến nhận thức
CSI	Channel State Information	Thông tin trạng thái kênh truyền
DF	Decode-and-Forward	Giải mã và chuyển tiếp
DMC	Discrete Memoryless Channel	Kênh rời rạc không nhớ
EAP	Extensible Authentication Protocol	Giao thức xác thực mở
Eve	Eavesdropper	Thiết bị nghe lén
IoT	Internet of Things	Internet vạn vật
IP	Intercepted Probability	Xác suất bị nghe lén
LoS	Line of Sight	Đường truyền thẳng
MIMO	Multi-Input Multi-Output	Đa đầu vào - Đa đầu ra
MUST	Multiuser Superposition Transmission	Truyền dẫn xếp chồng đa người dùng
MRT	Maximum Ratio Transmission	Truyền tỷ lệ cực đại
NOMA	Non-Orthogonal Multiple Access	Đa truy cập không trực giao

Từ viết tắt	Từ gốc	Giải nghĩa - Tạm dịch
NPS	Non-Protection Scheme	Mô hình không có cơ chế bảo vệ
OSI	Open Systems Interconnection	Mô hình tham chiếu kết nối các hệ thống mở
OP	Outage Probability	Xác suất dừng hoạt động
PIC	Parallel Interference Cancellation	Loại bỏ nhiễu song song
PDM-NOMA	Power-Domain NOMA	Mạng NOMA nghép kênh theo miền công suất
PDF	Probability Density Function	Hàm mật độ xác suất
PLS	Physical Layer Security	Bảo mật tầng vật lý
PN	Primary Network	Mạng sơ cấp
PU	Primary User	Người dùng sơ cấp
QoS	Quality of Service	Chất lượng dịch vụ
RFEH	Radio Frequency Energy Harvesting	Thu hoạch năng lượng qua sóng vô tuyến
RV	Random Variable	Biến ngẫu nhiên
SC	Selection Combining	Kết hợp lựa chọn
SDR	Semi-Definite Relaxation	Kỹ thuật tối ưu SDR
SIC	Successive Interference Cancellation	Loại bỏ nhiễu nối tiếp
SIMO	Single-Input Multiple-Output	Đơn đầu vào - Đa đầu ra
SINR	Signal-to-Interference-Plus-Noise Ratio	Tỉ số tín hiệu trên nhiễu và tạp âm
SISO	Single-Input Single-Output	Đơn đầu vào, đơn đầu ra
SLEP	Successful Legitimate Eavesdropping Probability	Xác suất nghe lén hợp pháp thành công
SU	Secondary Network	Mạng thứ cấp
SNR	Signal-to-Noise Radio	Tỉ số tín hiệu trên tạp âm
SOP	Secrecy Outage Probability	Xác suất dừng bảo mật
SU	Secondary User	Người dùng thứ cấp

Từ viết tắt	Từ gốc	Giải nghĩa - Tạm dịch
SWIPT	Simultaneous Wireless Information and Power Transfer	Truyền tải thông tin và năng lượng đồng thời
TAS	Transmit Antenna Selection	Lựa chọn ăng-ten phát
UAV	Unmanned Aerial Vehicle	Thiết bị bay không người lái
VLC	Visible Light Communication	Truyền thông tin không dây bằng ánh sáng nhìn thấy
DoS	Denial of Service	Từ chối dịch vụ

MỞ ĐẦU

1. Lý do lựa chọn đề tài

Trong những năm gần đây, sự phát triển mạnh mẽ của công nghệ mạng không dây đã mang lại cho con người cơ hội tiếp cận nhiều loại hình dịch vụ, tiện ích khác nhau. Các thế hệ mạng truyền thông không dây đã không ngừng cải tiến và phát triển cả về phần cứng cũng như phần mềm, thế hệ sau luôn kế thừa những ưu điểm trên nền tảng thế hệ trước đó và tích hợp những công nghệ tiên tiến để đáp ứng yêu cầu chất lượng dịch vụ ngày càng cao của người dùng như tốc độ truy cập nhanh, dung lượng lớn và chi phí hợp lý [95]. Tuy nhiên, cùng với sự phát triển của công nghệ mạng không dây cộng thêm với đặc tính tự nhiên của truyền thông không dây như tính mở, tính quảng bá, v.v. đã làm gia tăng các hoạt động bất hợp pháp như đánh cắp thông tin, ngăn cản hoạt động của người dùng hợp pháp trong mạng. Do đó đảm bảo truyền thông an toàn là một trong những yêu cầu bắt buộc, cấp thiết, là ưu tiên hàng đầu trong quá trình thiết kế các hệ thống truyền thông không dây, đặc biệt trong các lĩnh vực hoạt động như quân đội, tài chính - ngân hàng, chứng khoán, bảo hiểm và thông tin cá nhân. So với mạng có dây, mạng không dây dễ bị tấn công hơn do đặc tính quảng bá của môi trường truyền tin, có thể chia thành hai kiểu tấn công trong môi trường mạng không dây là tấn công chủ động và tấn công thụ động. Tấn công chủ động có thể gây ra sự can thiệp đáng kể vào hoạt động bình thường của mạng. Các hình thức phổ biến nhất của các cuộc tấn công chủ động bao gồm tấn công từ chối dịch vụ (DoS), tấn công giả mạo thông tin, tiết lộ thông tin hoặc sửa đổi làm sai lệch thông tin. Đối với kiểu tấn công thụ động nó không gây ra cản trở cho hoạt động của mạng, mục tiêu của kẻ tấn công là thu thập thông tin truyền trên các kênh không dây. Thường có hai loại tấn công thụ động được sử dụng, đó là xâm nhập nghe lén và phân tích lưu lượng mạng [136] [137].

Giải pháp bảo mật để chống lại các hoạt động bất hợp pháp ở trên là dựa theo cách tiếp cận từng lớp của mô hình tham chiếu kết nối các hệ thống mở (OSI). Trong đó, theo phương pháp truyền thống đã áp dụng ở các lớp trên tầng vật lý

như phương pháp giao thức xác thực mở rộng (EAP) trong tầng liên kết, mạng riêng ảo (VPN) ở tầng mạng, lớp liên kết bảo mật (SSL) ở tầng giao vận, sử dụng thuật toán mã hóa và giải mã dữ liệu như thuật toán mã hóa khối (DES), thuật toán mã hóa nâng cao (AES), thuật toán mã hóa khóa công khai (RSA) ở tầng ứng dụng. Các giải pháp bảo mật này có ưu điểm thực hiện bảo mật trực tiếp và đang được sử dụng phổ biến trong các hệ thống thông tin hiện nay. Tuy nhiên, với sự phát triển mạnh mẽ về năng lực tính toán của các hệ thống máy tính thì các phương pháp bảo mật dựa trên thời gian tính toán và bộ nhớ cần thiết để phá mã có thể không còn phù hợp trong tương lai khi năng lực tính toán của hệ thống máy tính bẻ khóa ngày càng cao và có khả năng không còn bị giới hạn [91]. Mặt khác, phương pháp bảo mật dựa trên độ phức tạp của thuật toán mã hóa gặp nhiều khó khăn, hạn chế trong việc quản lý và phân phối khóa đối với các mô hình mạng phân tán, và là thách thức lớn đối với các thiết bị trong mạng Internet vạn vật (IoT) vốn có tài nguyên hạn chế.

Để giải quyết vấn đề trên, các nhà nghiên cứu cả trong và ngoài nước đã tập trung nghiên cứu đưa ra các giải pháp bảo mật tầng vật lý (PLS) dựa trên cơ sở lý thuyết thông tin do Shannon đề xuất từ năm 1949. Trong đó Wyner là người tiên phong trong lĩnh vực này với công trình đầu tiên được công bố vào năm 1975 [30]. Ý tưởng cơ bản của phương pháp bảo mật tầng vật lý là khai thác các đặc tính vật lý của kênh truyền không dây như fading, tạp âm, nhiễu, khoảng cách, tính linh động của các nút mạng để đảm bảo truyền tin an toàn, bảo mật. Bảo mật tầng vật lý không dựa trên độ phức tạp tính toán, có nghĩa là mức độ bảo mật đạt được sẽ không bị vượt qua ngay cả khi các thiết bị bất hợp pháp có năng lực tính toán mạnh mẽ. Bảo mật tầng vật lý có độ phức tạp, độ trễ thấp và tiết kiệm tài nguyên, cũng như khả năng tích hợp với các cơ chế bảo mật mã hóa ở các tầng trên [97,99]. Bảo mật tầng vật lý có thể thực hiện việc truyền tin bảo mật trực tiếp mà không cần sử dụng các khóa bí mật. Tuy nhiên bảo mật tầng vật lý trong trường hợp cần thiết có thể sinh ra khóa bí mật chia sẻ giữa các thiết bị bằng cách sử dụng tính chất ngẫu nhiên của kênh truyền không dây và các đặc tính của kênh không dây như cường độ tín hiệu, pha của tín hiệu sóng mang, điều chế góc, biên độ kênh, tham số ngẫu nhiên Gaussian,v.v. [13, 17, 18, 21, 32, 33, 93, 94]. Bảo mật tầng vật lý có nhiều ưu điểm độc đáo và nhiều triển vọng đầy hứa hẹn. Do đó, bảo mật tầng

vật lý có thể được sử dụng như một phương pháp bảo mật bổ sung hiệu quả cho phương pháp bảo mật sử dụng các thuật toán mã hóa truyền thống để nâng cao khả năng an toàn, an ninh thông tin trên môi trường mạng không dây.

Hơn nữa, cùng với sự phát triển của khoa học công nghệ trong những năm qua, lĩnh vực mạng không dây đã thu hút được sự quan tâm rất lớn của các nhà nghiên cứu và đã có nhiều công nghệ mới được ra đời như mạng đa truy cập không trực giao, milimeter-Wave, massive MIMO, công nghệ búp sóng, IoT, truyền thông ánh sáng nhìn thấy, thiết bị bay không người lái, truyền thông hợp tác, thu hoạch năng lượng vô tuyến, mạng vô tuyến nhận thức, mạng cảm biến không dây v.v. Mạng không dây đã trở thành một lĩnh vực nghiên cứu quan trọng và phát triển mạnh. Trong đó mạng đa truy cập không trực giao là một công nghệ rất tiềm năng cho mạng thế hệ thứ 5 và tương lai, NOMA cho phép đồng thời nhiều người dùng cùng truy cập dựa trên cơ chế sử dụng chung khối tài nguyên không trực giao trong mạng vô tuyến như cùng khe thời gian, cùng tần số,v.v., trái ngược với cơ chế hoạt động của hệ thống đa truy cập trực giao thường dựa trên chia sẻ tài nguyên trực giao. NOMA làm tăng hiệu quả sử dụng dải tần số, tăng thông lượng, mật độ kết nối lớn, độ trễ thấp và đảm bảo tính công bằng giữa các người dùng. Bảo mật tầng vật lý trong mạng NOMA nhận được nhiều sự quan tâm của các nhà nghiên cứu trên thế giới. Giai đoạn đầu các nhà nghiên cứu tập trung vào các hệ thống NOMA đơn đầu vào đơn đầu ra [57,58,63,65,70]. Mặt khác, kỹ thuật đa ăng-ten kết hợp với kỹ thuật lựa chọn ăng-ten phát đã được chứng minh là giải pháp hiệu quả để cải thiện hiệu năng bảo mật của hệ thống [59,87,89,90]. Ngoài ra, các nhà nghiên cứu gần đây đã xem xét hệ thống trong kịch bản máy phát được trang bị số lượng lớn ăng-ten. Các kết quả nghiên cứu đã chỉ ra rằng số lượng người dùng có thể kết nối cũng như khả năng bảo mật tăng lên đáng kể khi máy thu/phát được trang bị số lượng lớn ăng-ten [72–75]. Đặc biệt nhiễu nhân tạo có thể được tạo ra để bảo đảm tính an toàn thông tin trước đối tượng nghe lén [88,89]. Hơn nữa, PLS còn được xem xét trên các hệ thống kết hợp giữa NOMA với các công nghệ truyền thông tiên tiến như truyền thông hợp tác, song công, thu hoạch năng lượng qua sóng vô tuyến, UAV, truyền tin và năng lượng đồng thời, và milimeter-Wave [44,77,79,80,82].

Với sự phổ biến và phát triển không ngừng của công nghệ mạng không dây,

vấn đề bảo mật trong truyền thông không dây sẽ có nhiều thách thức hơn nữa trong tương lai, làm cho chủ đề này trở thành một trong những lĩnh vực nghiên cứu quan trọng và liên tục. Mặc dù đã có nhiều các công trình nghiên cứu với cách tiếp cận khác nhau, song truyền thông bảo mật trong mạng NOMA vẫn đang là một vấn đề mở. Do đó luận án đề xuất các mô hình mạng NOMA với các kỹ thuật truyền thông tiên tiến như chủ động gây nhiễu, đa ăng-ten, truyền thông cộng tác kết hợp với các kỹ thuật lựa chọn ăng-ten phát (TAS), lựa chọn kết hợp (SC). Sau đó thực hiện phân tích, đánh giá hiệu năng bảo mật hệ thống, góp phần mở rộng thêm các kết quả nghiên cứu cũng như làm phong phú và sáng tỏ sự hiểu biết về bảo mật thông tin tầng vật lý trong mạng NOMA. Đây là vấn đề quan trọng, cấp thiết và chính là mục tiêu nghiên cứu của luận án.

Xuất phát từ những phân tích trên đây, tác giả đã lựa chọn và thực hiện đề tài "Đánh giá hiệu năng bảo mật tầng vật lý trong mạng NOMA" cho luận án Tiến sĩ của mình.

2. Mục tiêu nghiên cứu

Mục tiêu của luận án là nghiên cứu, đánh giá và đề xuất giải pháp nhằm nâng cao khả năng bảo mật thông tin tại tầng vật lý trong mạng NOMA, nhằm ngăn chặn hình thức tấn công nghe lén thông tin và đảm bảo QoS cho hệ thống. Luận án gồm các mục tiêu cụ thể sau:

- Đề xuất các mô hình mạng NOMA sử dụng các kỹ thuật truyền thông tiên tiến như truyền thông cộng tác, vô tuyến nhận thức, gây nhiễu cộng tác.
- Phân tích, đánh giá khả năng đảm bảo an toàn thông tin tầng vật lý, đề xuất các chiến lược nâng cao khả năng bảo mật và phân tích hiệu quả bảo mật của chiến lược được đề xuất trên kênh truyền Rayleigh và $\alpha - \mu$ fading.
- Xây dựng biểu thức toán học, chương trình mô phỏng để đánh giá tác động của các tham số hệ thống lên hiệu năng bảo mật của hệ thống.

3. Đối tượng nghiên cứu

- Các kênh truyền Rayleigh fading và α-μ fading. Các kiểu tấn công trên mạng không dây.

- Truyền thông cộng tác, đa ăng-ten, kỹ thuật gây nhiễu cộng tác.
- Cơ sở lý thuyết bảo mật thông tin tầng vật lý và các kỹ thuật đảm bảo an toàn thông tin tầng vật lý trong mạng không dây.
- Các phép đo, phương pháp phân tích, đánh giá hiệu năng bảo mật tầng vật lý.
- Mạng NOMA, mạng NOMA nhận thức dạng nền (Cognitive NOMA).

4. Phạm vi nghiên cứu

Trước xu hướng nghiên cứu của thế giới cũng như trong nước về bảo mật tầng vật lý trong mạng NOMA, luận án được giới hạn nghiên cứu trong phạm vi như sau:

- Nghiên cứu, đánh giá khả năng bảo mật thông tin trong truyền thông không dây tại tầng vật lý trong mạng NOMA bị tấn công nghe lén thông tin, trong đó các đối tượng nghe lén hoạt động ở chế độ thụ động.
- Nghiên cứu, đánh giá hiệu năng bảo mật tầng vật lý của một số mô hình mạng NOMA nghép kênh người dùng theo miền công suất.
- Sử dụng các phép đo: Xác suất dừng bảo mật, xác suất nghe lén hợp pháp thành công, xác suất bị nghe lén, xác suất dừng hoạt động, xác suất rớt gói tin, thời gian truyền gói tin trung bình để đánh giá hiệu năng bảo mật, hiệu suất hoạt động của hệ thống.
- Các kênh truyền không dây có mô hình thống kê tuân theo phân bố Rayleigh và phân bố α-μ.
- Mô hình mạng NOMA cộng tác sử dụng giao thức giải mã và chuyển tiếp (DF) tín hiệu.

5. Phương pháp nghiên cứu

Trong luận án, nghiên cứu sinh đã sử dụng những phương pháp nghiên cứu như sau:

- Phương pháp nghiên cứu lý thuyết: Thu thập tài liệu, khảo sát và tổng hợp các công trình đã công bố liên quan đến hướng nghiên cứu của đề tài.
- Phương pháp phân tích toán học: Mô tả bằng toán học các mô hình mạng NOMA được đề xuất, xây dựng các biểu thức toán học nhằm phân tích, đánh giá hiệu năng bảo mật, hiệu suất của hệ thống thông qua các phép đo: Xác suất dừng bảo mật, xác suất nghe lén hợp pháp thành công, xác suất bị nghe lén, xác suất rớt gói tin, thời gian truyền tin trung bình.
- Dựa trên các mô hình đã đề xuất, sử dụng phần mềm Matlab để mô phỏng theo phương pháp Monte Carlo nhằm kiểm chứng các kết quả phân tích lý thuyết.

6. Các đóng góp chính của luận án

Những đóng góp chính của luận án được tóm tắt như sau:

- Một là đã đề xuất và đánh giá chiến lược bảo mật thông tin cho mạng NOMA cộng tác trên kênh truyền α-μ fading bị thiết bị gây nhiễu và nghe lén hợp tác tấn công thông qua phép đo xác suất dừng bảo mật trong kịch bản hệ thống có chiến lược đối phó chủ động và không có chiến lược đối phó chủ động. Các kết quả mô phỏng đã chỉ ra rằng hiệu năng bảo mật của hệ thống được cải thiện đáng kể trong kịch bản có chiến lược đối phó chủ động. Kết quả này được công bố trong công trình số $A1$.
- Hai là đã đề xuất và đánh giá hiệu năng bảo mật của mô hình mạng NOMA có chiến lược chủ động nghe lén dựa trên các biểu thức dạng đóng (closed-form) của phép đo xác suất nghe lén hợp pháp thành công, xây dựng chính sách điều chỉnh công suất truyền tin trong kịch bản trạng thái kênh truyền xác định và không xác định vừa đảm bảo hiệu suất nghe lén vừa thỏa mãn ràng buộc về xác suất dừng hoạt động của hệ thống truyền tin bất hợp pháp. Các kết quả phân tích lý thuyết và mô phỏng chỉ ra rằng hiệu năng bảo mật của hệ thống tăng đáng kể khi số lượng ăng-ten của thiết bị chuyển tiếp tăng lên. Kết quả này được công bố trong công trình số $A3$.
- Ba là đã đề xuất và đánh giá khả năng bảo mật thông tin mô hình mạng SISO NOMA với các kịch bản khác nhau về thiết bị nghe lén Eve. Hiệu

năng bảo mật được phân tích, đánh giá thông qua phép đo xác suất dừng bảo mật của từng người dùng, của toàn bộ hệ thống với kịch bản Eve sử dụng các kỹ thuật SIC, PIC để xử lý tín hiệu thu được, kịch bản Eve được trang bị một và nhiều ăng-ten. Các kết quả phân tích lý thuyết và mô phỏng đã chỉ ra rằng hiệu năng bảo mật của hệ thống trong trường hợp Eve sử dụng PIC kém hơn so với trường hợp Eve sử dụng kỹ thuật SIC. Hơn nữa, hệ thống sẽ bảo mật hơn khi Eve chỉ được trang bị một ăng-ten so với trường hợp thiết bị nghe lén được trang bị nhiều ăng-ten. Kết quả này được công bố trong công trình số $A2$.

- Bốn là đã khảo sát, đánh giá được mối quan hệ giữa khả năng bảo mật thông tin và độ tin cậy của mô hình mạng NOMA nhận thức dạng nền dưới ràng buộc mức can nhiễu của mạng sơ cấp và công suất phát mức đỉnh của mạng thứ cấp. Các kết quả đã chỉ ra rằng giữa bảo mật và độ tin cậy có mối quan hệ tỷ lệ nghịch. Đồng thời đưa ra chính sách điều chỉnh công suất của mạng thứ cấp để vừa đảm bảo an toàn thông tin của mạng thứ cấp vừa đảm bảo hiệu suất hoạt động của mạng sơ cấp. Hiệu năng của hệ thống được đánh giá dựa trên các biểu thức dạng đóng của các phép đo xác suất dừng hoạt động và xác suất bị nghe lén. Kết quả này được công bố trong công trình số $A4$.

7. Ý nghĩa khoa học và thực tiễn của luận án

Ý nghĩa khoa học: Bảo mật thông tin tầng vật lý trong truyền thông không dây nói chung và mạng NOMA nói riêng là một vấn đề quan trọng mà các nhà nghiên cứu trên thế giới đang quan tâm. Các đóng góp của luận án góp phần mở rộng và làm phong phú thêm các kết quả nghiên cứu trong lĩnh vực bảo mật thông tin tầng vật lý trong mạng NOMA.

Ý nghĩa thực tiễn: Các kết quả nghiên cứu của luận án là nguồn tài liệu tham khảo cho các nhà nghiên cứu quan tâm đến lĩnh vực đánh giá hiệu năng bảo mật thông tin tầng vật lý trong mạng NOMA. Ngoài ra, các kết quả của luận án có thể sử dụng để đánh giá hiệu năng bảo mật của các hệ thống tương tự trong thực tế góp phần giúp các nhà quản lý có định hướng, giải pháp trong việc đề xuất phương án thiết kế mạng NOMA đảm bảo khả năng an toàn, bảo mật thông tin.

8. Cấu trúc của luận án

Luận án được bố cục bao gồm các phần như sau: Mở đầu, 04 chương, Kết luận và định hướng nghiên cứu, Danh mục công trình khoa học và Tài liệu tham khảo.

Phần mở đầu: Tập trung làm rõ các lý do lựa chọn đề tài nghiên cứu, xác định rõ mục tiêu, đối tượng, phạm vi nghiên cứu, phương pháp nghiên cứu, các đóng góp chính của luận án, ý nghĩa khoa học và thực tiễn của luận án.

Chương 1: Tổng quan về các kiến thức cơ bản của mô hình kênh truyền không dây, mô hình đầu vào/đầu ra của kênh truyền không dây, mô hình thống kê của kênh truyền fading, mạng NOMA. Cơ sở lý thuyết bảo mật tầng vật lý trong mạng không dây, trình bày khả năng bảo mật tầng vật lý trên kênh rời rạc, không nhớ, kênh Gaussian, kênh fading có nghe lén, mã wiretap, các phép đo hiệu năng bảo mật. Bên cạnh đó, trong chương này luận án đã khảo sát và trình bày các công trình nghiên cứu liên quan đến các hướng nghiên cứu của luận án và đề xuất hướng nghiên cứu của luận án. Các kiến thức này sẽ là cơ sở cho việc nghiên cứu, phân tích, đánh giá những kết quả chính được trình bày ở các chương sau của luận án.

Chương 2: Nghiên cứu, đánh giá hiệu năng bảo mật của mạng NOMA sử dụng kỹ thuật truyền thông cộng tác thông qua một thiết bị chuyển tiếp với sự hiện diện của một thiết bị nghe lén cộng tác với thiết bị gây nhiễu lên thiết bị chuyển tiếp và thiết bị cuối trên kênh truyền fading theo phân bố α-μ. Do ảnh hưởng của tín hiệu gây nhiễu nên thiết bị chuyển tiếp buộc phải tăng công suất truyền tin mà không biết sự hiện diện của thiết bị nghe lén và khi máy phát tăng công suất phát thì thiết bị nghe lén có khả năng thu thập được thông tin tốt hơn. Từ hình thức tấn công cộng tác đó, luận án đã đề xuất chiến lược đối phó chủ động để chống lại việc nghe lén thông tin trên mô hình này. Sau đó, luận án tính toán và so sánh xác suất dừng bảo mật của hệ thống trong hai kịch bản. Ngoài ra, luận án đã khảo sát, đánh giá tác động của một số tham số hệ thống lên hiệu năng bảo mật của hệ thống.

Chương 3: Nghiên cứu khả năng đảm bảo an toàn thông tin của mô hình mạng NOMA chủ động nghe lén, trong đó các thiết bị bất hợp pháp sử dụng mạng NOMA để truyền tin từ thiết bị cuối về trạm cơ sở, hệ thống thực hiện

việc gây nhiễu lên máy phát để buộc máy phát tăng công suất nhằm cải thiện hiệu suất quá trình nghe lén thông tin. Luận án trình bày quá trình xây dựng biểu thức công suất gây nhiễu dựa trên các kịch bản trạng thái kênh truyền và với ràng buộc không làm giảm hiệu suất hoạt động của hệ thống truyền tin bất hợp pháp. Tiếp theo, luận án tính toán xác suất nghe lén hợp pháp thành công để đánh giá hiệu năng bảo mật của hệ thống và tính toán xác suất nghe lén hợp pháp thành công đối với người dùng bất hợp pháp có tín hiệu mạnh nhất và yếu nhất.

Chương 4: Nghiên cứu, đánh giá hiệu năng bảo mật, độ tin cậy, hiệu suất của mô hình mạng SISO NOMA và mạng NOMA nhận thức dạng nền. Trong đó luận án đề xuất nghiên cứu hai mô hình. Mô hình thứ nhất (Mô hình 4.1), tác giả nghiên cứu hiệu năng bảo mật của hệ thống trong các trường hợp thiết bị nghe lén được trang bị một và nhiều ăng-ten, thiết bị nghe lén được giả thiết có thể sử dụng kỹ thuật loại bỏ nhiễu SIC hoặc PIC. Luận án trình bày quá trình xây dựng biểu thức tính toán xác suất dừng bảo mật của từng người dùng và của toàn bộ hệ thống. Bên cạnh đó, luận án còn đánh giá hiệu suất hoạt động của hệ thống qua phép đo xác suất rớt gói tin, thời gian truyền tin trung bình và trình bày thuật toán tìm hệ số phân bổ công suất với điều kiện ràng buộc về thời gian truyền tin giữa những người dùng trong một nhóm được nghép kênh theo miền công suất. Mô hình thứ hai (Mô hình 4.2) được mở rộng từ mô hình thứ nhất, mô hình mạng SISO NOMA trong môi trường vô tuyến nhận thức dạng nền dưới ràng buộc mức can nhiễu và công suất phát mức đỉnh của mạng thứ cấp. Trong mô hình này, luận án khảo sát mối quan hệ giữa hiệu suất bảo mật thông tin và độ tin cậy của mạng thứ cấp với ràng buộc mức can nhiễu của mạng sơ cấp và công suất phát tối đa của mạng thứ cấp. Từ đó, luận án trình bày quá trình phân tích, xây dựng biểu thức tính toán công suất phát của mạng thứ cấp, đánh giá sự ảnh hưởng của các tham số hệ thống lên hiệu năng bảo mật, độ tin cậy, công suất phát của mạng thứ cấp.

Phần kết luận và định hướng nghiên cứu của luận án sẽ trình bày tóm lược những kết quả nghiên cứu, những đóng góp của luận án đã được công bố trên các tạp chí và các hội thảo khoa học. Đồng thời đề xuất các hướng nghiên cứu tiếp theo của luận án.

Chương 1

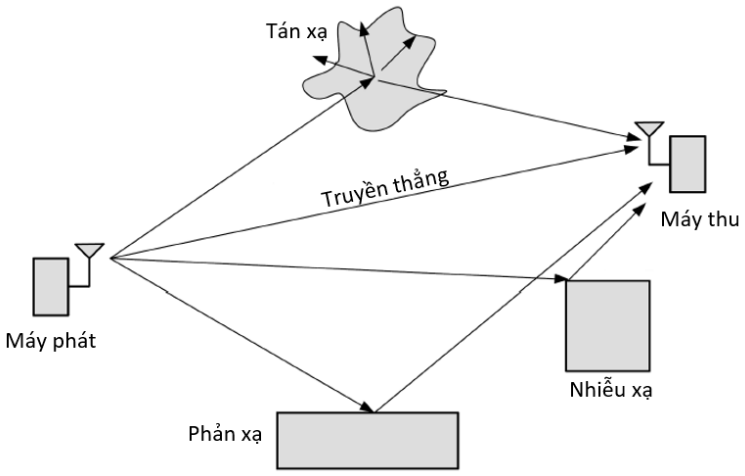
KIẾN THỨC CƠ SỞ VÀ TỔNG QUAN

Chương này trình bày các kiến thức cơ sở sẽ được sử dụng trong các chương sau, bao gồm: Tổng quan về mô hình kênh truyền không dây, mô hình đầu vào/ra của kênh truyền không dây, mô hình thống kê của kênh truyền fading và các phân bố thống kê của kênh fading được sử dụng trong các nghiên cứu của luận án. Nguyên lý hoạt động của mạng NOMA, đánh giá dung lượng kênh đường lên, đường xuống của mạng NOMA. Cơ sở lý thuyết của lĩnh vực bảo mật thông tin tại tầng vật lý trong truyền thông không dây, trình bày khả năng bảo mật tầng vật lý trên kênh rời rạc không nhớ, kênh Gaussian, kênh fading có nghe lén, các phép đo bảo mật hệ thống. Bên cạnh đó, trong phần này cũng trình bày tổng quan tình hình nghiên cứu, một số công trình nghiên cứu liên quan và một số các hướng nghiên cứu tiêu biểu của lĩnh vực bảo mật tầng vật lý trong mạng NOMA.

1.1 Mô hình kênh truyền không dây

Kênh truyền không dây truyền các tín hiệu từ ăng-ten máy phát tới ăng-ten của máy thu thông qua môi trường điện từ trường. Trong thực tế, điều kiện về không gian trống cho truyền tin không dây hiếm khi tồn tại do sự hiện diện của các chướng ngại vật như mô tả trong hình 1.1, bao gồm trong nó các đối tượng vật lý có thể ảnh hưởng đến sự lan truyền tín hiệu dưới dạng sóng điện từ từ máy phát đến máy thu. Do đó, tín hiệu bị suy giảm theo khoảng cách truyền sóng hoặc biến dạng do độ trễ thời gian truyền sóng của kênh đa đường hoặc do sự chuyển động của thiết bị thu phát, của các vật thể ở xung quanh v.v.. Vì vậy, kênh không dây trở nên ngẫu nhiên và khó dự đoán hơn so với kênh có dây.

Sự thay đổi của cường độ tín hiệu theo thời gian và tần số của kênh không dây



Hình 1.1: *Mô hình kênh truyền không dây*

gọi là hiện tượng fading và gây ra bởi 3 hiện tượng đó là path loss, shadowing, multipath. Trong đó path loss là hiệu ứng suy giảm công suất của tín hiệu nhận khi truyền qua một khoảng cách giữa máy phát và máy thu. Shadowing là hiện tượng công suất tín hiệu bị suy hao do các vật cản giữa máy phát và máy thu. Multipath là hiện tượng tín hiệu được truyền tới máy thu qua nhiều đường khác nhau do các hiện tượng phản xạ, tán xạ và nhiễu xạ từ các vật thể trong môi trường truyền sóng, sóng nhận được tại máy thu là sự chồng chập của các sóng đến từ nhiều hướng, tín hiệu thu được là tổng hợp các bản sao tín hiệu phát, tín hiệu này bị suy hao, trễ, dịch pha và ảnh hưởng lẫn nhau. Hiệu ứng fading có thể được chia làm hai loại cơ bản như sau [27]:

Hiệu ứng fading hẹp (Small-scale fading): Hiệu ứng này gây ra bởi hiện tượng đa đường, biên độ và pha của tín hiệu nhận được bị thay đổi nhanh trong một khoảng thời gian ngắn hoặc do sự di chuyển vị trí trong một khoảng cách ngắn giữa máy phát và máy thu. Nó là sự kết hợp hoặc triệt tiêu lẫn nhau của nhiều phiên bản tín hiệu được truyền theo nhiều đường khác nhau đến thiết bị thu.

Hiệu ứng fading rộng (Large-scale fading): Hiệu ứng này xảy ra do hiện tượng path loss và shadowing. Nó miêu tả đặc trưng về công suất trung bình của tín hiệu thu bị suy hao khi tín hiệu truyền qua một khoảng cách lớn hoặc bị chắn bởi các vật thể như tòa nhà, đồi núi.

Các mô hình để tính toán suy hao công suất tín hiệu trên kênh truyền không

dây đóng vai trò quan trọng trong việc thiết kế hệ thống, nó xác định các thông số chính của hệ thống như công suất truyền, tần số, chiều cao ăng-ten, v.v. Một số mô hình đã được đề xuất cho các hệ thống di động hoạt động trong các môi trường khác nhau (trong nhà, ngoài trời, thành thị, ngoại ô, nông thôn). Một số mô hình này được xây dựng theo phương pháp thống kê dựa trên các phép đo thực địa và một số khác được phát triển theo phương pháp phân tích dựa trên hiệu ứng nhiễu xạ. Hai mô hình thực nghiệm được sử dụng rộng rãi là Okumura/ Hata và COST 231 [11]. Tuy nhiên do tính chất phức tạp của quá trình truyền tín hiệu nên khó có thể có một mô hình duy nhất mô tả chính xác hiệu ứng path loss trên nhiều môi trường khác nhau. Các mô hình tính toán suy hao kênh truyền có thể thu được từ các mô hình phân tích phức tạp hoặc từ các phép đo thực nghiệm khi các tham số của hệ thống phải được đáp ứng đầy đủ hoặc các vị trí tốt nhất cho các trạm cơ sở hoặc sơ đồ bố trí các điểm truy cập phải được xác định. Vì vậy, để cân bằng chung của các thiết kế khác nhau giữa các hệ thống, chúng ta có thể sử dụng một mô hình đơn giản để thu được bản chất của việc truyền tín hiệu mà không cần các mô hình path loss phức tạp, chỉ cần xấp xỉ với kênh truyền thực tế. Do đó, một mô hình path loss đơn giản, coi nó như là một hàm của khoảng cách, thường được sử dụng trong thiết kế hệ thống, có dạng như sau [10].

$$P_r = P_t K \left[\frac{d_0}{d}\right]^{\eta} \tag{1.1}$$

trong đó P_r và P_t lần lượt là công suất của tín hiệu thu và phát. K là một hằng số đơn vị phụ thuộc vào tính chất của ăng-ten, độ suy hao kênh trung bình, và các yếu tố vật ký khác. Kí hiệu d và d_0 biểu diễn độ dài đường truyền tín hiệu và khoảng cách tham chiếu cho vùng trường xa của ăng-ten. η là hệ số path loss và giá trị của nó phụ thuộc vào môi trường truyền sóng (Bảng 1.1). Các mô hình tính toán suy hao đường truyền cho phép ước đoán cường độ tín hiệu trung bình giữa máy phát và máy thu tại một khoảng cách xác định. Các mô hình này có ý nghĩa trong việc tính toán, thiết kế và quy hoạch vùng phủ sóng.

Môi trường truyền	η
Không gian trống	2.0
Các cell nhỏ trong đô thị	2.7 - 3.5
Các cell lớn trong đô thị	3.7 - 6.5
Tòa nhà văn phòng (cùng tầng)	1.6 - 3.5
Tòa nhà văn phòng (các tầng khác nhau)	2.0 - 6.0
Cửa hàng	1.8 - 2.2
Nhà máy	1.6 - 3.3
Nhà riêng	3.0

Bảng 1.1: *Hệ số path loss trong môi trường truyền khác nhau [10].*

1.2 Mô hình đầu vào/đầu ra của kênh truyền không dây

Trên kênh truyền không dây, tín hiệu được truyền với độ lệch pha ban đầu bằng không được mô hình hóa như sau [10]

$$s(t) = \Re\left\{u(t)e^{j2\pi f_c t}\right\} = \Re\left\{u(t)\right\}\cos\left(2\pi f_c t\right) - \Im\left\{u(t)\right\}\sin\left(2\pi f_c t\right), \quad (1.2)$$

trong đó $u(t)$ là tín hiệu phức ở băng tần cơ bản của $s(t)$, B là băng thông và f_c là tần số sóng mang. $\Re\{.\}$ và $\Im\{.\}$ tương ứng là phần thực và phần ảo của tín hiệu phức. Tín hiệu được truyền đi thường đi qua nhiều đường khác nhau trước khi đến máy thu. Hiện tượng này là do phản xạ, tán xạ, nhiễu xạ và các yếu tố khác trong môi trường truyền sóng vô tuyến (xem Hình- 1.1). Ảnh hưởng của đa đường dẫn đến các biến thể khác nhau của tín hiệu nhận được. Do đó, ở phía máy thu, tín hiệu nhận được là tổng của các thành phần truyền thẳng và các thành phần đa đường, được diễn tả như sau

$$r(t) = \Re\left\{\left[\sum_{n=0}^{N(t)} \alpha_n(t)u(t-\tau_n(t))\right] e^{j2\pi f_c(t-\tau_n(t))+\Phi_{D_n}}\right\}, \quad (1.3)$$

trong đó $n = 0$ tương ứng với đường truyền thẳng, $\tau_n(t), \Phi_{D_n}$ và $\alpha_n(t)$ là độ trễ của thành phần đa đường, dịch pha Doppler và biên độ.

Để đơn giản, chúng ta đặt $\Phi_n(t) = 2\pi f_c\tau_n(t) - \Phi_{D_n}$ và viết lại công thức tín hiệu nhận được như sau

$$r(t) = \Re\left\{\left[\sum_{n=0}^{N(t)} \alpha_n(t)e^{-j\Phi_n(t)}u(t-\tau_n(t))\right] e^{j2\pi f_c t}\right\} \quad (1.4)$$

Giả thiết rằng độ trải trễ (delay spread) của kênh truyền nhỏ hơn rất nhiều so với nghịch đảo băng thông của tín hiệu B và $u(t-\tau_n(t)) \approx u(t)$. Khi đó, tín hiệu nhận được mô tả trong công thức (1.3) có dạng như sau [[10],Eq. (3.14)]

$$r(t) = r_I(t)\cos(2\pi f_c t) + r_Q(t)\sin(2\pi f_c t), \tag{1.5}$$

trong đó $r_I(t)$ và $r_Q(t)$ là các thành phần đồng pha và vuông góc, được tính như sau

$$r_I(t) = \sum_{n=1}^{N(t)} \alpha_n(t)\cos\Phi_n(t) \tag{1.6}$$

$$r_Q(t) = \sum_{n=1}^{N(t)} \alpha_n(t)\sin\Phi_n(t) \tag{1.7}$$

Nếu số lượng thành phần đa đường đủ lớn, $r_I(t)$ và $r_Q(t)$ có thể xấp xỉ như là quá trình ngẫu nhiên Gaussian [10].

1.3 Mô hình thống kê của kênh truyền fading

Như đã trình bày ở trên, fading là hiện tượng tín hiệu trên kênh truyền không dây luôn bị biến đổi do ảnh hưởng bởi các yếu tố vật lý trong môi trường truyền sóng. Trong đó fading rộng để mô tả cường độ tín hiệu nhận được và mức suy hao của nó khi được truyền qua một vùng không gian rộng hoặc khoảng cách dài. Ngược lại, fading hẹp mô tả quá trình biến đổi nhanh của cường độ tín hiệu thu được và pha dao động của nó khi tín hiệu truyền trong một khoảng cách gần hoặc một khoảng thời gian ngắn. Việc xây dựng một mô hình toán học đủ tổng quát để mô tả chính xác các kênh truyền fading là không khả thi hoặc rất phức tạp. Vì vậy, các mô hình thống kê trở nên thích hợp để sử dụng mô tả đặc tính của kênh truyền fading. Các mô hình thống kê thông dụng bao gồm các phân bố Rayleigh, phân bố mũ, Rician, Nakagami-m, Weibull và phân bố $\alpha-\mu$ [10, 27, 31]. Việc áp dụng mô hình thống kê nào phụ thuộc vào từng loại môi trường truyền sóng vô tuyến cụ thể. Trong luận án này, tác giả áp dụng mô hình phân bố Rayleigh và $\alpha-\mu$ cho các mô hình mạng NOMA được nghiên cứu trong luận án này, Rayleigh là mô hình phân bố được sử dụng phổ biến để mô tả tín hiệu của kênh truyền thay đổi theo thời gian của đường bao tín hiệu fading đa đường, còn $\alpha-\mu$ là mô

hình phân bố tổng quát, khi thay đổi các tham số chúng ta có các phân bố như Rayleigh, phân bố mũ, Rician, Nakagami-m, Weibull và phân bố Gaussian một phía [31].

1.3.1 Phân bố Rayleigh fading

Khi pha $\Phi_n(t)$ được phân bố đều, các thành phần $r_I(t)$ và $r_Q(t)$ là các biến ngẫu nhiên Gaussian có giá trị trung bình bằng 0 và phương sai σ^2. Khi đó biên độ của tín hiệu sẽ là

$$z(t) = |r(t)| = \sqrt{r_I^2(t) + r_Q^2(t)} \tag{1.8}$$

và $|r(t)|$ là một biến ngẫu nhiên theo phân bố Rayleigh với hàm mật độ và phân bố xác suất lần lượt như sau

$$f_Z(z) = \frac{2z}{\Omega} \exp\left(\frac{-z^2}{\Omega}\right), \tag{1.9}$$

$$F_Z(z) = 1 - \exp\left(\frac{z^2}{\Omega}\right), \tag{1.10}$$

trong đó $\Omega = \sum_{n=1} \mathbb{E}[\alpha_n^2] = 2\sigma^2$ là công suất trung bình của tín hiệu nhận được.

Hơn nữa, chúng ta có thể tìm được hàm mật độ phân bố xác suất của công suất bằng cách thay thế biến $h = z^2(t) = |r(t)|^2$ như sau

$$f_h(x) = \frac{1}{\Omega} \exp\left(-\frac{x}{\Omega}\right), x \geq 0, \tag{1.11}$$

h gọi là độ lợi công suất kênh truyền hay độ lợi kênh truyền. Hàm phân phối xác suất của h dễ dàng tìm được như sau

$$F_h(x) = 1 - \exp\left(-\frac{x}{\Omega}\right) \tag{1.12}$$

1.3.2 Phân bố $\alpha - \mu$ fading

Gần đây, một phân bố tổng quát mới dùng để mô hình hóa kênh truyền fading được giới thiệu bởi M. D Yacoub, có tên là phân bố $\alpha - \mu$ [46]. Nó được coi như là một mô hình tổng quát, linh hoạt và dễ quản lý. Hơn nữa, nó bao gồm các phân phối quan trọng như Rayleigh, Nakagami-m, Weibull, Gaussian một phía,

Gamma và phân bố mũ. Trên kênh truyền có tín hiệu fading với biên độ là x, hàm mật độ xác suất của phân bố $\alpha - \mu$ được mô tả theo công thức như sau

$$f_X(x) = \frac{\alpha \mu^{\mu} x^{\alpha\mu - 1}}{\Gamma(\mu)\hat{x}^{\alpha\mu}} \exp\left[-\mu\left(\frac{x}{\hat{x}}\right)^{\alpha}\right], \tag{1.13}$$

trong đó α là tham số bất kỳ > 0 và $\mu \geq 1/2$ là giá trị nghịch đảo của phương sai chuẩn x^{α} và được tính theo công thức sau $\mu = \mathbb{E}^2[r^{\alpha}]/\mathbb{V}[r^{\alpha}]$. Ở đây $\mathbb{E}[\cdot]$ và $\mathbb{V}[\cdot]$ là ký hiệu phép toán tính kỳ vọng và phương sai. Hơn nữa, $\Gamma(\cdot)$ là hàm Gamma và $\hat{x}$ là giá trị trung bình bậc α và được định nghĩa như sau $\hat{x} = \sqrt[\alpha]{\mathbb{E}[X^{\alpha}]}$ [56, (8.310.1)]. Mô men thứ k của X được mô tả là

$$\mathbb{E}[x^k] = \frac{\hat{x}^k}{\mu^{\frac{k}{\alpha}}} \frac{\Gamma(\mu + \frac{k}{\alpha})}{\Gamma(\mu)}. \tag{1.14}$$

Hàm phân bố xác suất tích lũy của X được tính như sau

$$F_X(x) = \frac{\Gamma\left[\mu, \mu\left(\frac{x}{\hat{x}}\right)^{\alpha}\right]}{\Gamma(\mu)}, \tag{1.15}$$

trong đó $\Gamma[\cdot,\cdot]$ là hàm Gamma không hoàn chỉnh [56, (8.350.1)]. Bằng cách thay đổi các tham số fading (α; μ trong (1.13)), chúng ta sẽ nhận được các phân bố khác nhau như Rayleigh ($\alpha = 2; \mu = 1$), Nakagami-m ($\alpha = 2; \mu = m$), Weibull ($\mu = 1$), phân phối mũ ($\alpha = 1; \mu = 1$), và phân phối Gaussian một phía ($\alpha = 1; \mu = 0.5$).

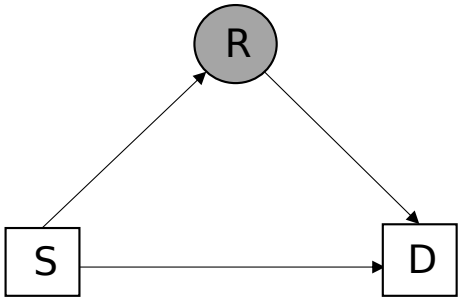
1.4 Mạng truyền thông không dây cộng tác

Công nghệ truyền thông không dây đã có bước phát triển nhảy vọt trong hai thập kỷ qua, nhiều thế hệ mạng được ra đời như mạng thế hệ thứ 3 (3G), mạng thế hệ thứ tư (4G), mạng thế hệ thứ năm (5G). Thế hệ sau kế thừa những ưu điểm của thế hệ trước đã đem lại nhiều dịch vụ tiện ích cho người dùng, tốc độ truyền dữ liệu ngày càng nhanh với chi phí hợp lý. Một trong những vấn đề mạng truyền thông không dây phải đối mặt đó là sự suy hao tín hiệu do các tác động của các yếu tố tự nhiên trong môi trường truyền sóng như phản xạ, nhiễu xạ và tán xạ và các hiện tượng fading khác. Để giải quyết vấn đề suy hao tín hiệu, đã có một số giải pháp được sử dụng như tăng công suất phát, tăng băng thông, sử dụng kỹ thuật điều chế như OFDM, CDMA, kỹ thuật Beamforming, kỹ thuật yêu cầu

lặp lại tự động (ARQ), kỹ thuật MIMO, kỹ thuật chuyển tiếp. Trong đó kỹ thuật chuyển tiếp nhận được sự quan tâm của các nhà nghiên cứu.

Mạng truyền thông cộng tác không dây sử dụng kỹ thuật chuyển tiếp để tăng khả năng

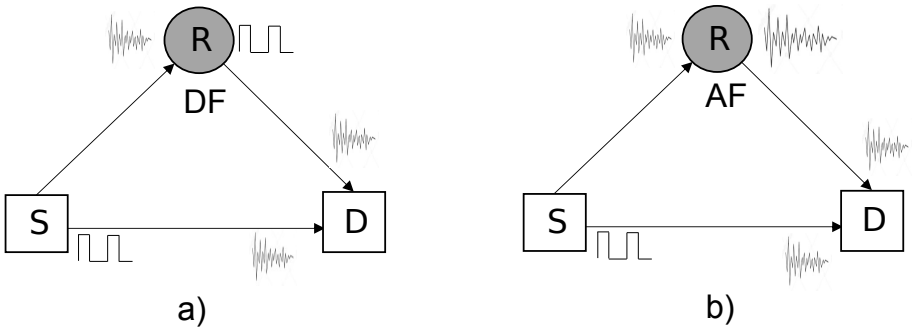
truyền tin giữa máy phát và máy thu. Mạng này thường được sử dụng trong các tình huống mà việc truyền thông trực tiếp giữa máy phát và máy thu gặp khó khăn hoặc không hiệu quả. Trong mạng truyền thông cộng tác, có ba thành phần chính: Máy phát (nguồn), máy thu (đích) và một hoặc nhiều nút (thiết bị) chuyển tiếp. Nút nguồn: Là thành phần tạo dữ liệu cần truyền và khởi tạo việc truyền tin. Nút chuyển tiếp là thành phần trung gian nhận và chuyển tiếp dữ liệu từ nguồn đến đích. Nút đích là thành phần cuối cùng nhận dữ liệu được gửi từ nút nguồn. Như trong hình 1.2 nút nguồn ký hiệu là S, nút chuyển tiếp là R và nút đích là



Hình 1.2: *Mô hình mạng truyền thông cộng tác có một nút chuyển tiếp*

D. Nói chung, có hai loại thiết bị chuyển tiếp, đó là chuyển tiếp bán song công và chuyển tiếp song công. Trong đó chuyển tiếp song công có thể truyền và nhận tín hiệu đồng thời trên cùng một kênh. Trái lại, với chuyển tiếp bán song công, cần hai kênh trực giao để thiết bị chuyển tiếp có thể truyền và nhận tín hiệu.

Chuyển tiếp song công tiết kiệm tài nguyên tần số và hiệu quả sử dụng gấp đôi khả năng sử dụng tần số so với chuyển tiếp bán song công. Tuy nhiên, với chuyển tiếp song công, tín hiệu đầu vào tại một ăng-ten sẽ bị nhiễu bởi tín hiệu đầu ra của chính nó, gọi là tự nhiễu. Thách thức đối với việc loại bỏ tự nhiễu này là do sự khác biệt đáng kể về mức công suất giữa tín hiệu vào và tín hiệu ra. Do đó, mặc dù chuyển tiếp bán song công có sử dụng tần số thấp hơn so với chuyển tiếp song công, nhưng nó vẫn được sử dụng trong các hệ thống không dây thực tế do tính đơn giản trong việc triển khai. Mạng truyền thông cộng tác không dây



Hình 1.3: *Mô hình mạng truyền thông cộng tác sử dụng giao thức DF, AF*

sử dụng một trong hai giao thức là: Khuếch đại và chuyển tiếp (AF) hoặc giải mã và chuyển tiếp (DF) như trong hình 1.3. Trong giao thức khuếch đại và chuyển tiếp, các nút chuyển tiếp khuếch đại tín hiệu sau đó chuyển tiếp tín hiệu nhận được đến nút nhận. Đối với giao thức giải mã và chuyển tiếp, các nút chuyển tiếp giải mã tín hiệu nhận được và chuyển tiếp nó đến nút đích. Giao thức khuếch đại và chuyển tiếp có ưu điểm là dễ cài đặt, vì nút chuyển tiếp tín hiệu nhiễu đã nhận mà không cần phải thực hiện việc giải mã tín hiệu. Mặt khác, nhược điểm chính của giao thức khuếch đại và chuyển tiếp là tín hiệu nhiễu nhận được tại nút chuyển tiếp cũng có thể được khuếch đại và chuyển tiếp đến nút đích. Điều này có thể dẫn đến sự suy giảm hiệu suất trong việc giải mã tín hiệu nguồn tại nút đích. Giả sử có một nguồn truyền tín hiệu x với công suất là P, tín hiệu nhận được tại nút chuyển tiếp có dạng như sau:

$$\gamma_r = \sqrt{P} h_{sr} x + n_r, \tag{1.16}$$

trong đó h_{sr} là hệ số kênh truyền từ nút nguồn tới nút đích và n_r nhiễu Gaussian trắng cộng với giá trị trung bình bằng 0 và phương sai là N_0. Trong giao thức khuếch đại và chuyển tiếp, nút chuyển tiếp sẽ khuếch đại tín hiệu nhận được γ_r với hệ số tỷ lệ $\alpha = 1/(\sqrt{P}|h_{sr}|)$ và chuyển tiếp tín hiệu đến điểm đích. Do đó, tín hiệu nhận được tại điểm đích có thể được biểu diễn như sau:

$$\gamma_d^{AF} = \sqrt{P} \alpha h_{rd} \gamma_r + n_d, \tag{1.17}$$

trong đó h_{rd} là hệ số kênh truyền từ nút chuyển tiếp tới nút đích và n_d là nhiễu Gaussian trắng cộng có giá trị trung bình bằng 0 và phương sai N_0. Từ phương trình (1.16) và (1.17), chúng ta có dung lượng của kênh truyền trong giao thức

khuếch đại và chuyển tiếp như sau:

$$C_{srd}^{AF} = \frac{1}{2}\log_2\left(1 + \frac{|h_{sr}|^2|h_{rd}|^2}{|h_{sr}|^2 + |h_{rd}|^2}\gamma\right), \tag{1.18}$$

trong đó $\gamma = P/N_0$ và hệ số $1/2$ xuất phát từ việc cần 2 khe thời gian để hoàn thành việc truyền tín hiệu từ nút nguồn tới nút đích thông qua nút chuyển tiếp. Từ phương trình (1.18) cho thấy dung lượng kênh truyền trong giao thức khuếch đại và chuyển tiếp phụ thuộc vào cả kênh truyền từ nút nguồn tới nút chuyển tiếp và từ nút chuyển tiếp tới nút đích.

Khác với giao thức khuếch đại và chuyển tiếp, trong giao thức giải mã và chuyển tiếp, nút chuyển tiếp giải mã tín hiệu nhận được từ nút nguồn trước khi chuyển tiếp đến nút đích. Chúng ta có thể tính toán dung lượng kênh truyền dựa vào giao thức giải mã và khuếch đại như sau [135]:

$$\gamma_{srd}^{DF} = \frac{1}{2}\log_2(1 + \gamma\min\{|h_{sr}|^2, |h_{rd}|^2\}). \tag{1.19}$$

Như vậy dung lượng kênh truyền trong giao thức giải mã và chuyển tiếp là giá trị nhỏ nhất giữa dung lượng kênh từ nút nguồn tới nút chuyển tiếp và dung lượng kênh từ nút chuyển tiếp tới nút đích. So sánh hai công thức (1.18) và (1.19) có thể dễ dàng kết luận rằng dung lượng kênh dựa trên giao thức giải mã và chuyển tiếp lớn hơn so với kênh dựa trên giao thức khuếch đại và chuyển tiếp, đây là ưu điểm của giao thức giải mã và chuyển tiếp so với giao thức khuếch đại và chuyển tiếp về hiệu suất dung lượng kênh truyền [28]. Tuy nhiên nhược điểm của giao thức giải mã và chuyển tiếp so với giao thức khuếch đại và chuyển tiếp là độ trễ trong quá trình truyền tin tăng lên do diễn ra hoạt động giải mã tín hiệu.

1.5 Mạng NOMA

1.5.1 Nguyên lý hoạt động

Các thế hệ mạng không dây hiện nay cấp phát tài nguyên vô tuyến cho người dùng cuối đều dựa trên nguyên lý đa truy cập trực giao. Tuy nhiên khi số lượng người dùng tăng lên, các phương pháp tiếp cận dựa trên đa truy cập trực giao (OMA) có thể không đáp ứng được các yêu cầu nghiêm ngặt như hiệu suất sử dụng phổ tần cao, độ trễ thấp và kết nối nhiều thiết bị. Nói cách khác, hiệu suất

của OMA không thể đáp ứng được trong các hệ thống thông tin truyền thông không dây trong tương lai. Do đó, từ năm 2003 các nhà khoa học đã bắt đầu nghiên cứu về NOMA và đề xuất NOMA như một ứng cử viên sáng giá về kỹ thuật đa truy cập cho các thế hệ mạng tiếp theo để cải thiện hiệu quả phổ đồng thời cho phép nhiễu đa truy cập ở một mức độ nào đó tại các máy thu. Trong mạng NOMA chia người dùng thành từng nhóm để thực hiện việc truyền và nhận thông tin. Nhìn chung, các phương pháp nhóm ghép người dùng thành các nhóm trong mạng NOMA hiện tại được chia thành hai loại chính là ghép kênh miền công suất (PDM-NOMA) và ghép kênh miền mã (CD-NOMA) [48]. Trong đó, ghép kênh miền mã có tiềm năng để tăng cường hiệu quả phổ nhưng kỹ thuật này đòi hỏi băng thông truyền dẫn cao và khó áp dụng vào các hệ thống thông tin hiện tại. Mặt khác, ghép kênh miền công suất có cách thực thi đơn giản vì các hệ thống mạng hiện có không cần phải triển khai những thay đổi đáng kể. Ngoài ra, ghép kênh miền công suất không yêu cầu băng thông bổ sung để cải thiện hiệu quả phổ tần [86]. Vì thế NOMA miền công suất đã trở thành mô hình hiệu quả và được nghiên cứu phổ biến nhất trong số các mô hình mạng NOMA. Cơ chế hoạt động của PDM-NOMA là sử dụng hiệu quả miền công suất cho đa truy cập để đồng thời phục vụ nhiều người dùng trong cùng một khe thời gian, cùng một dải tần số bằng phương pháp mã hóa xếp chồng tại máy phát. Trong đó, mức công suất cấp phát cho một người dùng được quyết định dựa trên độ lợi kênh, với người dùng có độ lợi kênh cao hơn được gán mức công suất thấp hơn và ngược lại. Tại máy thu, các tín hiệu người dùng khác nhau được phân tách bằng cách khai thác sự khác biệt về công suất tín hiệu của mỗi người dùng dựa trên kỹ thuật loại bỏ nhiễu nối tiếp (SIC) hoặc loại bỏ nhiễu song song (PIC). So với OMA, NOMA có những ưu điểm sau:

- Cải thiện hiệu quả phổ và thông lượng: Trong OMA, chẳng hạn như trong mạng ghép kênh phân chia tần số trực giao (OFDMA), một tài nguyên tần số cụ thể được chỉ định cho mỗi người dùng mà không phụ thuộc vào trạng thái kênh truyền tốt hay xấu, do đó hiệu suất và thông lượng phổ tổng thể của hệ thống thấp. Ngược lại, trong NOMA, tài nguyên tần số giống nhau được gán cho nhiều người dùng đồng thời với các điều kiện kênh truyền tốt, xấu khác nhau. Do đó, tài nguyên được cấp phát cho người dùng có

kênh truyền xấu cũng được sử dụng bởi người dùng có kênh truyền tốt và nhiễu có thể giảm thiểu thông qua các quá trình SIC tại máy thu.

- Tăng sự công bằng của người dùng, độ trễ thấp và hỗ trợ nhiều kết nối: Trong OMA, người dùng có kênh truyền tốt hơn có mức ưu tiên được phục vụ cao hơn trong khi người dùng có kênh truyền kém hơn phải chờ để được truy cập, dẫn đến một vấn đề về tính công bằng và độ trễ cao. Cách tiếp cận này không thể hỗ trợ nhiều kết nối. Ngược lại, NOMA có thể phục vụ đồng thời nhiều người dùng với các điều kiện kênh khác nhau. Do đó, nó có thể cải thiện sự công bằng cho người dùng, độ trễ giảm đi và khả năng thực hiện nhiều kết nối cao hơn.

- Khả năng tương thích cao: NOMA cũng tương thích với các hệ thống truyền thông hiện tại và tương lai vì nó không yêu cầu sửa đổi đáng kể trên kiến trúc hiện có. Lưu ý rằng NOMA miền công suất đường xuống đã được chuẩn hóa trong 3GPP, gọi là truyền dẫn xếp chồng đa người dùng [126].

Mặc dù NOMA có nhiều tính năng có thể hỗ trợ các thế hệ tiếp theo, nhưng nó có một số hạn chế cần được giải quyết để khai thác toàn bộ lợi thế của nó. Đó là, trong NOMA, người dùng được xếp thành từng nhóm, khi truyền tín hiệu, máy phát sẽ trộn tín hiệu của tất cả người dùng trong một nhóm thành tín hiệu hỗn hợp. Tại máy thu, tín hiệu của mỗi người dùng sẽ được lần lượt giải mã sau khi đã giải mã tín hiệu của những người dùng khác trong nhóm nên tính phức tạp của máy thu sẽ tăng lên khi so sánh với OMA, dẫn đến độ trễ lâu hơn. Hơn nữa, thông tin về độ lợi kênh truyền của tất cả người dùng phải được phản hồi về máy phát, điều này dẫn đến chi phí xử lý thông tin phản hồi tăng lên đáng kể. Hơn nữa, nếu bất kỳ lỗi nào xảy ra trong quá trình SIC ở bất kỳ người dùng nào, thì xác suất lỗi của quá trình giải mã nối tiếp sẽ tăng lên. Do đó, số lượng người dùng trong một nhóm nên được giảm bớt để tránh lỗi như vậy. Một lý do khác để hạn chế số lượng người dùng trong một nhóm là cần có sự khác biệt đáng kể về độ lợi kênh giữa những người dùng để có hiệu suất hoạt động tốt hơn [127]. Ngoài ra, đường xuống trong mạng NOMA, kỹ thuật SIC thực hiện trên thiết bị người dùng cuối và nó đòi hỏi tiêu thụ nhiều năng lượng để xử lý khi có nhiều người dùng trong một nhóm. Vì vậy, nhóm hai người dùng được chấp nhận rộng

rãi như là giải pháp phân nhóm hiệu quả trong mạng NOMA đường xuống [128].

1.5.2 Đường truyền xuống trong mạng NOMA

1.5.2.1 Dung lượng kênh truyền xuống trong mạng NOMA

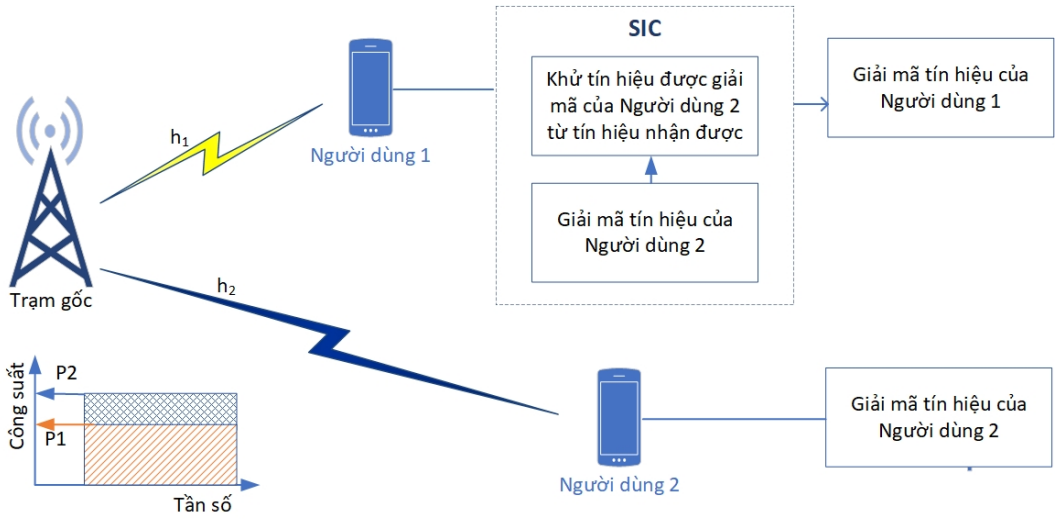
Xét trường hợp mạng NOMA đường xuống gồm có một trạm cơ sở (BS) và hai người dùng cuối U_i $(i = 1, 2)$ như trong hình 1.4. Băng thông hệ thống giả thiết là 1 Hz. BS truyền tín hiệu x_i tới U_i, trong đó P_i là công suất truyền và $P_1 + P_2 = P$. Tín hiệu của hai người dùng U_i là x_1 và x_2, được xếp chồng như sau:

$$x = \sqrt{P_1}x_1 + \sqrt{P_2}x_2. \tag{1.20}$$

Tín hiệu nhận được tại U_i được biểu diễn như sau

$$y_i = h_i x + w_i, \tag{1.21}$$

trong đó h_i là hệ số kênh phức giữa U_i và BS, w_i là nhiễu Gaussian trắng cộng (AWGN). Mật độ phổ công suất của w_i là $N_{0,i}$. Giả thiết rằng quá trình truyền tín



Hình 1.4: *Minh họa đường truyền xuống trong mạng NOMA sử dụng SIC tại máy thu*

hiệu không xảy ra lỗi và tín hiệu được giải mã thành công, dung lượng kênh của U_i là R_i được biểu diễn như sau

$$R_1 = \log_2\left(1 + \frac{P_1|h_1|^2}{N_{0,1}}\right), R_2 = \log_2\left(1 + \frac{P_2|h_2|^2}{P_1|h_2|^2 + N_{0,2}}\right). \tag{1.22}$$

Từ phương trình (1.22) chúng ta nhận thấy rằng, công suất phân bổ cho mỗi người dùng sẽ ảnh hưởng rất lớn đến dung lượng của người dùng đó. Bằng cách điều chỉnh tỷ lệ phân bổ công suất $\frac{P_1}{P_2}$, BS có thể điều khiển linh hoạt dung lượng của từng người dùng sao cho tín hiệu của từng người dùng có thể giải mã được tại máy thu tương ứng của nó.

1.5.2.2 So sánh dung lượng kênh truyền xuống giữa NOMA và OMA

Theo nguyên lý OMA, người dùng được cấp phát tài nguyên vô tuyến trực giao, do đó lượng băng thông là α gán cho U_1 ($0 \leq \alpha \leq 1$) thì lượng băng thông còn lại (1-α) Hz được gán cho U_2. Gọi R_i là dung lượng kênh của người dùng U_i, được biểu diễn như sau

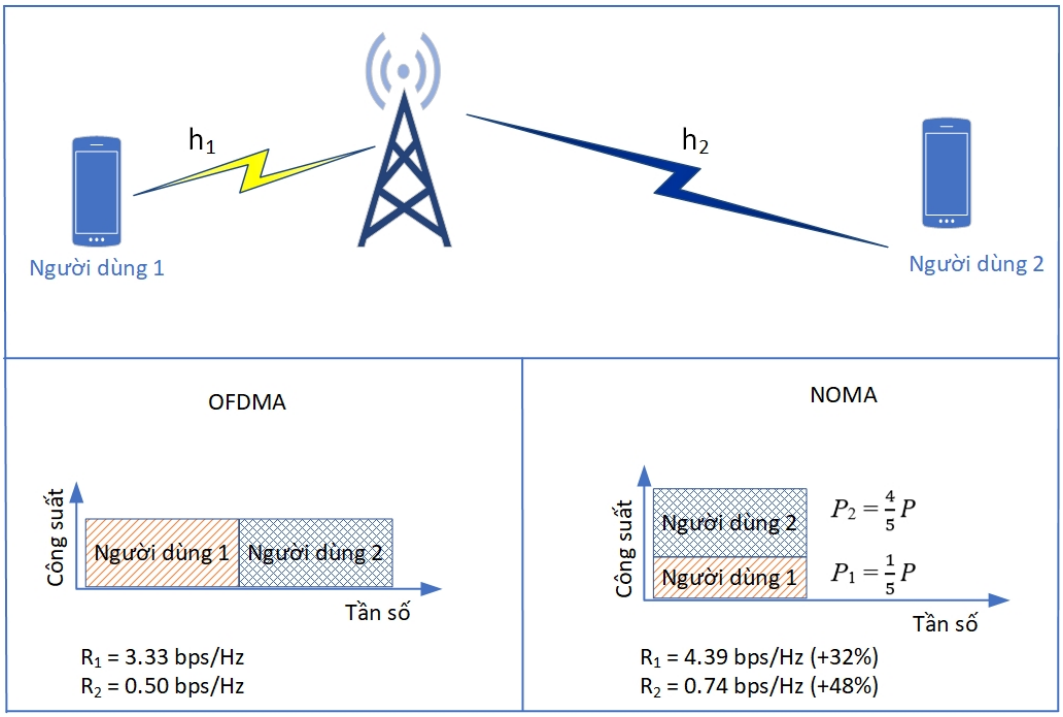
$$R_1 = \alpha \log_2 \left(1 + \frac{P_1|h_1|^2}{\alpha N_{0,1}}\right), R_2 = (1-\alpha) \log_2 \left(1 + \frac{P_2|h_2|^2}{(1-\alpha)N_{0,2}}\right). \quad (1.23)$$

Hiệu suất của NOMA so với OMA tăng lên khi độ lợi kênh truyền của U_i có sự khác biệt lớn. Chúng ta xem xét trường hợp có hai người dùng như trong hình 1.5, với U_1 là người dùng trung tâm và U_2 là người dùng ở biên xa máy phát BS hơn so với U_1, trong đó $\frac{|h_1|^2}{N_{0,1}}$ và $\frac{|h_2|^2}{N_{0,1}}$ có giá trị lần lượt là 20 dB và 0 dB tương ứng. Trong OMA thì băng thông và công suất truyền cấp phát cho hai người dùng là như nhau (α = 0.5, $P_1 = P_2 = \frac{1}{2}P$), tốc truyền tin của từng U_i được tính toán theo phương trình (1.23) lần lượt là R_1 = 3.33 bps và R_2 = 0.50 bps. Mặt khác, trong mạng NOMA giả thiết công suất được phân bổ cho U_i lần lượt là $P_1 = \frac{1}{5}P$ và $P_2 = \frac{4}{5}P$, tốc độ truyền tin được tính theo công thức (1.22) tương ứng là $R_1 = 4.39$ bps và $R_2 = 0.74$ bps. Tốc độ truyền tin trong NOMA tăng so với OMA là 32% đối với U_1 và 48% đối với U_2. Từ trường hợp hệ thống có hai người dùng đơn giản này, chúng ta thấy rằng tổng dung lượng của mạng NOMA cao hơn OMA [29].

1.5.3 Đường truyền lên trong mạng NOMA

1.5.3.1 Dung lượng kênh truyền lên trong mạng NOMA

Xem xét mô hình mạng NOMA đường lên như trong hình 1.6 với hai người dùng cuối U_i truyền tín hiệu về trạm cơ sở BS trên cùng tần số tại cùng một thời điểm và BS sử dụng SIC bóc tách tín hiệu của từng người dùng. Tương tự như



Hình 1.5: *So sánh dung lượng đường truyền xuống trong mạng NOMA và OMA*

đường xuống, chúng ta giả thiết băng thông toàn hệ thống là 1 Hz. Tín hiệu được truyền bởi U_i ký hiệu là x_i, công suất truyền là P_i. Trong mạng NOMA đường lên, tín hiệu nhận được tại BS là tín hiệu xếp chồng của hai người dùng U_i là x_1 và x_2 như sau

$$y = h_1\sqrt{P_1}x_1 + h_2\sqrt{P_2}x_2 + w, \tag{1.24}$$

trong đó h_1 là hệ số kênh phức giữa U_i và BS. w là nhiễu Gaussian trắng cộng (AWGN) tại BS với mật độ phổ công suất là N_0. U_1 là người dùng ở trung tâm, U_2 là người dùng nằm ở biên xa BS hơn so với U_1, $\frac{|h_1|^2}{N_0} > \frac{|h_2|^2}{N_0}$. BS sử dụng SIC để tách tín hiệu theo thứ tự độ lợi kênh truyền giảm dần. Giả thiết quá trình truyền tin không có lỗi xả ra, khi đó dung lượng R_i của U_i được tính như sau

$$R_1 = \log_2\left(1 + \frac{P_1|h_1|^2}{P_2|h_2|^2 + N_0}\right), R_2 = \log_2\left(1 + \frac{P_2|h_2|^2}{N_0}\right). \tag{1.25}$$

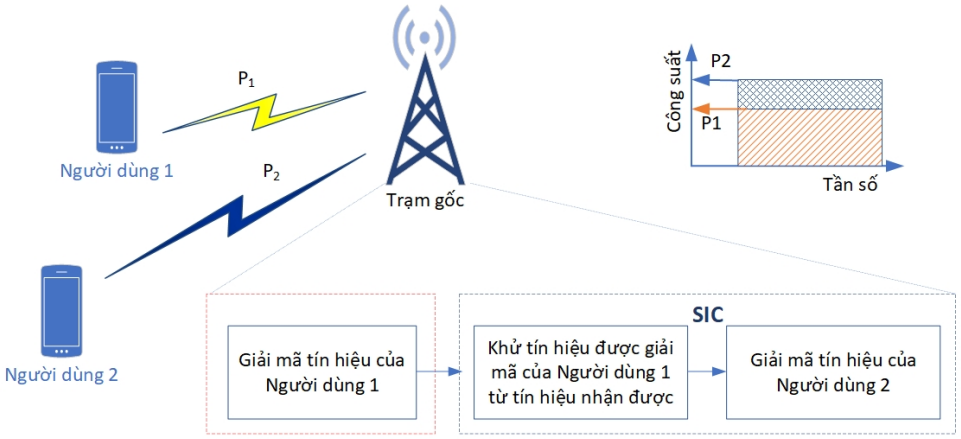
Nếu BS sử dụng SIC để tách tín hiệu theo thứ tự tăng dần của độ lợi kênh truyền, dung lượng của U_i được tính tương ứng như sau

$$R_1 = \log_2\left(1 + \frac{P_1|h_1|^2}{N_0}\right), R_2 = \log_2\left(1 + \frac{P_2|h_2|^2}{P_1|h_1|^2 + N_0}\right). \tag{1.26}$$

Tổng dung lượng của hệ thống như sau

$$R_1 + R_2 = \log_2\left(1 + \frac{P_1|h_1|^2 + P_2|h_2|^2}{N_0}\right). \tag{1.27}$$

Chúng ta thấy rằng, tổng dung lượng của U_i không phụ thuộc vào thứ tự tăng hay giảm của độ lợi kênh truyền khi thực hiện quá trình SIC để bóc tách tín hiệu. Tuy nhiên, kết luận tổng dung lượng của U_i là giống nhau với thứ tự SIC khác nhau chỉ đúng khi quá trình truyền tín hiệu không có lỗi xảy ra. Trong các hệ thống thực tế, quá trình truyền tín hiệu thường có lỗi xả ra thì thứ tự tối ưu là thứ tự giảm dần của độ lợi kênh truyền khi thực hiện quá trình SIC.



Hình 1.6: *Minh họa đường truyền lên trong mạng NOMA sử dụng SIC tại máy phát*

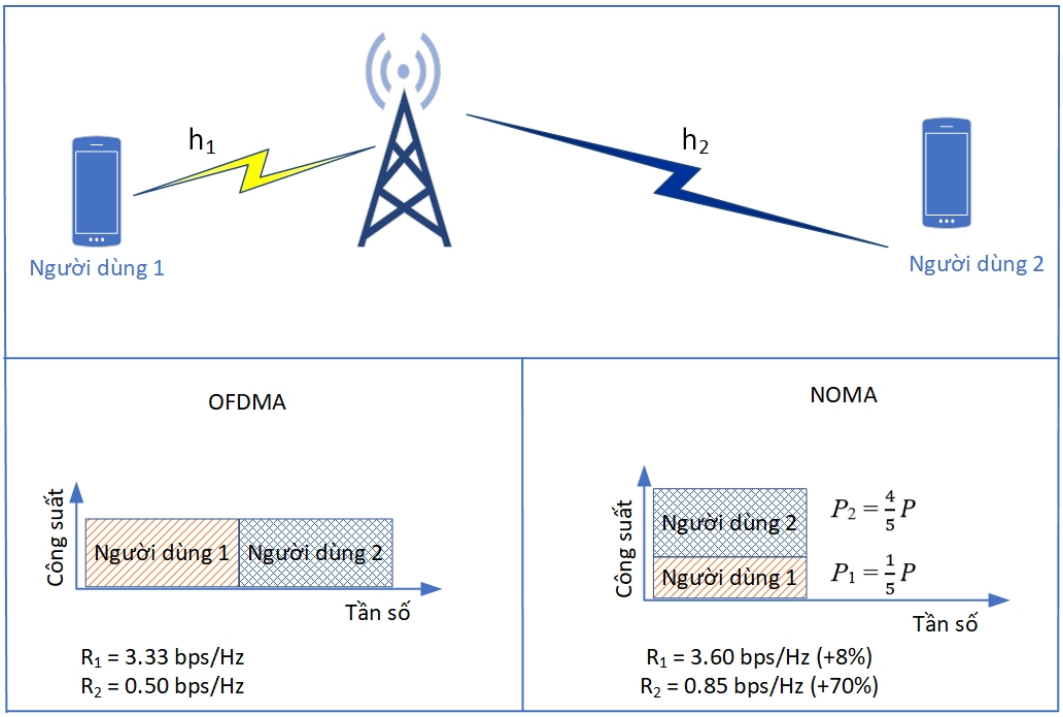
1.5.3.2 So sánh dung lượng kênh truyền lên giữa NOMA và OMA

Giả thiết lượng băng thông giành cho U_1 là α ($0 \leq \alpha \leq 1$) và lượng băng thông còn lại (1-α) Hz giành cho U_2. Dung lượng kênh của U_i được tính như sau

$$R_1 = \alpha \log_2\left(1 + \frac{P_1|h_1|^2}{\alpha N_0}\right), R_2 = (1-\alpha)\log_2\left(1 + \frac{P_2|h_2|^2}{(1-\alpha)N_0}\right). \tag{1.28}$$

Hình 1.7 so sánh dung lượng người dùng giữa mạng NOMA và OMA. U_1 là người dùng trung tâm và U_2 là người dùng ở biên xa máy phát BS hơn so với U_1, trong đó $\frac{|h_1|^2}{N_{0,1}}$ và $\frac{|h_2|^2}{N_{0,1}}$ có giá trị lần lượt là 20 dB và 0 dB tương ứng. Trong mạng OMA, băng thông được chia đều cho mỗi người dùng (α = 0.5), và tốc độ truyền tin được tính theo công thức (1.28), R_1 = 3.33 bps và R_2 = 0.50 bps. Mặt

khác, trong NOMA, giả thiết tổng công suất truyền của hai người dùng giống như trong OMA, tốc độ truyền tin được tính theo công thức (1.25), R_1 = 3.60 bps và R_2 = 0.85 bps. Tổng dung lượng của hai người dùng trong mạng NOMA so với OMA tăng lên 16%. Do đó, đối với NOMA đường lên, chúng ta có thể đạt được hiệu suất tương tự như đối với NOMA đường xuống [29].



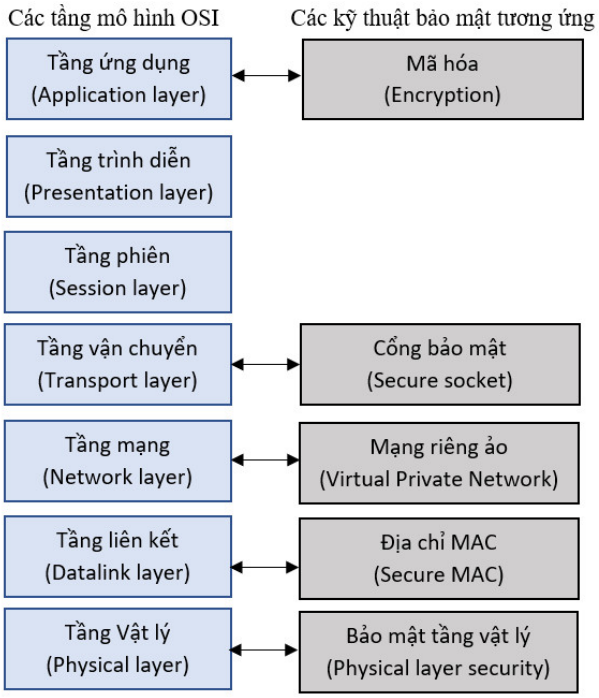
Hình 1.7: *So sánh dung lượng đường truyền lên trong mạng NOMA và OMA*

1.6 Bảo mật tầng vật lý trong mạng NOMA

1.6.1 Cơ sở lý thuyết bảo mật tầng vật lý

OSI là một mô hình tham chiếu được phát triển bởi tổ chức tiêu chuẩn quốc tế, đóng vai trò chuẩn hóa các chức năng bên trong của một hệ thống thông tin bằng cách chia nó thành các tầng. Mô hình OSI được biểu diễn như hình 1.8 và gồm có 7 tầng: Tầng vật lý (Physical Layer), tầng liên kết dữ liệu (Data link layer), tầng mạng (Network layer), tầng vận chuyển (Transport layer), tầng phiên (Session layer), tầng biểu diễn (Presentation layer) và tầng ứng dụng (Application layer). Các tầng trong mô hình OSI có quan hệ chặt chẽ với nhau, mỗi tầng nhằm định nghĩa một phân đoạn trong quá trình di chuyển thông tin qua mạng. Mô

hình OSI ra đời để giải quyết vấn đề kết nối, trao đổi thông tin giữa các hệ thống thông tin với nhau. Tầng vật lý là tầng thấp nhất trong mô hình OSI, xử lý các



Hình 1.8: *Mô hình tham chiếu OSI*

vấn đề liên quan đến việc truyền các dòng bít nhị phân phi cấu trúc từ máy này sang máy khác, thiết lập duy trì và hủy kết nối vật lý. Ngoài ra nó chỉ định các thông số kỹ thuật về cơ, điện, các thủ tục để truy cập vào đường truyền vật lý.

Để đảm bảo bảo mật thông tin trao đổi giữa các hệ thống thông tin, các giải pháp bảo mật khác nhau đã được nghiên cứu, triển khai áp dụng ở các tầng khác nhau. Đặc biệt, đối với các hệ thống truyền tin không dây, do đặc tính quảng bá tự nhiên của kênh truyền nên rất dễ bị tấn công dạng nghe lén hoặc làm suy giảm chất lượng kênh truyền hoặc làm gián đoạn hoạt động truyền tin của hệ thống [16]. Giải pháp cho các vấn đề trên theo cách tiếp cận truyền thống là sử dụng phương pháp mã hóa để ngăn chặn người dùng bất hợp pháp thu thập thông tin. Bản tin trước khi được truyền đi được mã hóa và chỉ có người nhận hợp pháp có khóa bí mật mới có thể giải mã bản tin. Do vậy mức độ bảo mật của phương pháp mã hóa được đo bằng độ phức tạp của thuật toán mã hóa. Tuy nhiên với sự phát triển mạnh mẽ của công nghệ tính toán thì mức độ bảo mật đo bằng thời gian tính toán và bộ nhớ lưu trữ cần thiết để phá mã mật thì rất khó

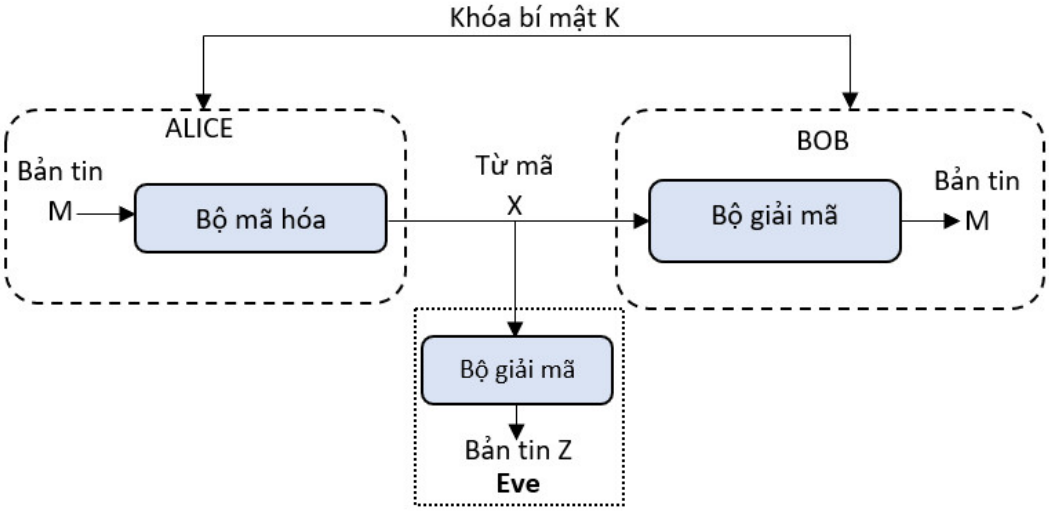
được đảm bảo trong tương lai, thực tế nhiều thuật toán mã hóa hiện tại đã bị phá vỡ [91]. Ngoài ra một thách thức nữa mà phương pháp mã hóa gặp phải là vấn đề chi phí, khó khăn trong việc quản lý và phân phối khóa trong các hệ thống phân tán, các hệ thống thông tin trong tương lai ở đó các nút mạng kết nối và rời đi một cách ngẫu nhiên, liên tục [98].

Phương pháp bảo mật tầng vật lý được khởi xướng bởi Wyner từ năm 1975 [30]. Cơ sở lý thuyết của PLS xuất phát từ khái niệm bảo mật hoàn hảo (perfect secrecy) và lý thuyết thông tin đưa ra bởi Shannon vào năm 1949 [23]. Xét mô hình hệ thống bảo mật của Shannon mô tả như trong hình 1.9, giả thiết cả kênh hợp pháp và kênh nghe lén đều không có nhiễu. Khóa bí mật K được biết bởi cả máy phát và máy thu hợp pháp. Máy phát hợp pháp gọi là ALICE mã hóa bản tin M thành từ mã X và truyền cho máy thu hợp pháp BOB, trong quá trình truyền bản tin M, thiết bị nghe lén bất hợp pháp Eve cũng thu được từ mã X qua kênh nghe lén. Shannon gọi quá trình truyền tin trên kênh hợp pháp đạt bảo mật hoàn hảo nếu và chỉ nếu độ bất định còn lại của bản tin M từ thông tin đầu ra Z tại Eve bằng với độ bất định của bản tin M, có nghĩa là [159]

$$H(M|Z) = H(M). \tag{1.29}$$

Điều này có nghĩa rằng từ mã X độc lập hoàn toàn với M hay nói cách khác Z không chứa bất kỳ thông tin nào về bản tin M. Khi đó thông tin tương hỗ $I(M;Z) = H(X) - H(M|Z)$ sẽ bằng 0 trong trường hợp kênh truyền tin đạt bảo mật hoàn hảo. $H(M|Z)$ còn gọi là entropy có điều kiện của bản tin M khi biết bản tin Z hay còn gọi là độ mập mờ (equivocation) của Eve về bản tin M. Do không có mối tương quan giữa bản tin và từ mã nên không tồn tại thuật toán để Eve có thể trích xuất thông tin về bản tin M.

Với mô hình mã mật đề ra, Shannon đã chứng minh rằng bảo mật hoàn hảo chỉ có thể đạt được nếu độ bất định của khóa bí mật K tối thiểu bằng độ bất định của bản tin, có nghĩa rằng $H(K) \geq H(M)$. Điều này có nghĩa rằng cần sử dụng ít nhất một bít khóa bí mật cho mỗi một bít của bản tin và Shannon cũng chỉ ra rằng chỉ có khóa mã một lần (one-time pad) là có thể đáp ứng được yêu cầu về khóa bí mật như vậy. Khái niệm bảo mật hoàn hảo của Shannon được chấp nhận như là phép đo bảo mật chặt chẽ nhất nhưng không đặt ra bất kỳ giới hạn nào về khả năng tính toán của thiết bị nghe lén.



Hình 1.9: *Mô hình hệ thống bảo mật của Shannon*

1.6.2 Kênh nghe lén

Xuất phát từ khái niệm bảo mật hoàn hảo và lý thuyết thông tin, Wyner đã khởi xướng nghiên cứu về bảo mật tầng vật lý trên kênh nghe lén [30]. Hình 1.10 mô tả mô hình kênh nghe lén tổng quát, trong đó bản tin M được chọn ngẫu nhiên từ tập các bản tin $\mathcal{M}$. Bộ mã hóa chuyển bản tin M thành từ mã X^n có độ dài n. X^n được truyền từ ALICE đến BOB qua một kênh rời rạc không nhớ, tại đầu ra của kênh chính thu được từ mã Y^n và là đầu vào của kênh nghe lén. BOB sẽ giải mã và thu được bản tin $\hat{M}$ và Eve giải mã được bản tin Z^n. Kênh nghe lén được giả thiết rằng là một phiên bản tín hiệu suy thoái của kênh chính. Độ tin cậy của quá trình truyền tin được đo bằng xác suất lỗi trung bình, được định nghĩa như sau [30]:

$$P_e^{(n)} = P\{\hat{M} \neq M\} = \frac{1}{|\mathcal{M}|} \sum_{M \in \mathcal{M}} P\{\hat{M} \neq M\} \tag{1.30}$$

Độ mập mờ (equivocation) về nguồn tin của Eve sau khi giải mã và nhận được bản tin Z^n, hay còn gọi là độ khó của việc xác định nguồn tin đã gửi tương ứng với dữ liệu đã nhận, được định nghĩa như sau [30]:

$$R_e^{(n)} = \frac{1}{n} H(M|Z^n) \tag{1.31}$$

Mục tiêu là thiết kế hệ thống truyền tin sao cho $P_e^{(n)}$ tiến về 0 trong khi tốc độ truyền tin và độ mập mờ càng lớn càng tốt. Wyner đã chỉ ra rằng khi $n \to \infty$ thì

sự mập mờ tại kênh nghe lén sẽ tiệm cận độ bất định của nguồn tin vô điều kiện, có nghĩa là quá trình truyền tin đạt được bảo mật gần như hoàn hảo. Tuy nhiên tốc độ truyền tin $R = \frac{H(M)}{n} \to 0$. Vậy vấn đề đặt ra là có thể truyền tin ở một tốc độ lớn hơn 0 một lượng đáng kể mà vẫn đạt được độ an toàn gần như tuyệt đối ($R_e^{(n)} \approx H(M)$).

Wyner đã phát biểu rằng một cặp tốc độ truyền tin - độ mập mờ (R_s, R_e) có thể đạt được nếu tồn tại một bộ mã hóa - giải mã thỏa mãn [4, 12, 19]:

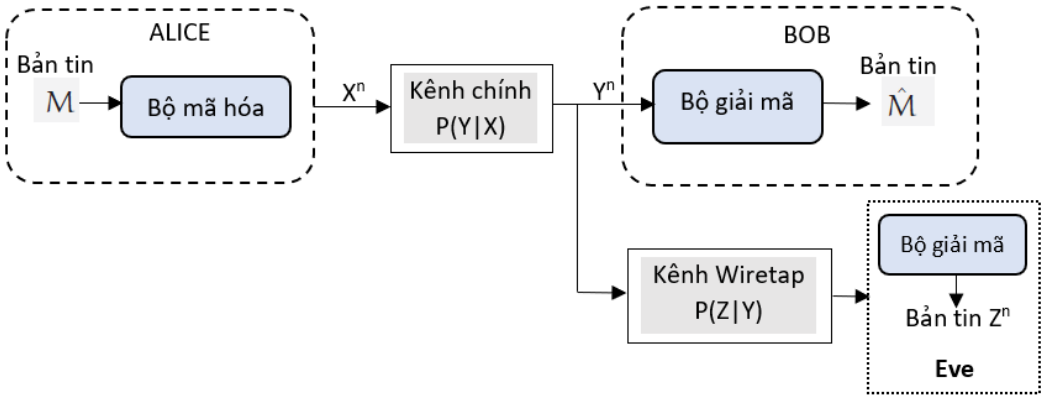
$$\lim_{n\to\infty} P_e^{(n)} \to 0 \tag{1.32}$$

$$\lim_{n\to\infty} \inf \frac{1}{n} R_e^{(n)} \geq R_e \tag{1.33}$$

(R_s, R_e) cho biết tốc độ truyền tin an toàn bảo mật đạt được với một mức độ bảo mật là R_e. Khi $R_e < R_s$ thì thông tin bị rò rỉ cho đối tượng nghe lén Eve. Khi $R_s = R_e$ thì quá trình truyền tin đạt bảo mật hoàn hảo, R_s gọi là tốc độ bảo mật hoàn hảo. Tốc độ truyền tin bảo mật lớn nhất gọi là dung lượng bảo mật [30].

$$C_s = \max_{(R_s,R_e)\in\bar{\mathcal{R}}} R_s, \tag{1.34}$$

trong đó $\bar{\mathcal{R}}$ là tập bao đóng tất cả các cặp (R_s, R_e) có thể đạt được.



Hình 1.10: *Mô hình kênh nghe lén tổng quát*

Wyner đã tiên phong nghiên cứu bảo mật tầng vật lý, tuy nhiên kể từ khi công trình của ông được công bố thì PLS đã không nhận được nhiều sự quan tâm của các nhà nghiên cứu, vấn đề này có thể do những nguyên nhân sau: Nguyên nhân thứ nhất, kỹ thuật mã hóa cho kênh nghe lén thực tế chưa sẵn sàng; mô hình kênh nghe lén đưa ra giả thiết rằng kênh nghe lén là kênh suy thoái hơn

kênh hợp pháp, tức tỷ số công suất tín hiệu trên nhiễu của kênh hợp pháp luôn lớn hơn kênh nghe lén, giả thiết này khó được đảm bảo trong môi trường truyền thông không dây. Nguyên nhân thứ hai, ngay sau khi khái niệm dung lượng bảo mật được đề xuất, Diffe và Hellman đã phát minh ra mật mã khóa công khai với thuật toán mã hóa có độ phức tạp được cho là rất khó phá mã và đã thống trị nghiên cứu bảo mật kể từ khi xuất hiện vì vậy bảo mật tầng vật lý không được quan tâm trong những năm thập niên 1970 và thập niên 1980.

Mở rộng các kết quả của Wyner, hai nhà khoa học Imre Csiszár và János Körner đã nghiên cứu trên kênh quảng bá và đã chứng minh rằng có thể truyền các bản tin bí mật với tốc độ R_s $(R_s > 0)$ với mức bảo mật hoàn hảo cùng với các bản tin chung không cần giữ bí mật cho tất cả mọi người trong hệ thống [7].

1.6.3 Kênh nghe lén Gaussian

Kênh truyền nghe lén có nhiễu AWGN được nghiên cứu và công bố trong công trình [14], nhóm tác giả trong công trình này đã chỉ ra rằng dung lượng bảo mật của kênh nghe lén Gaussian có được từ sự khác biệt giữa dung lượng kênh chính và kênh nghe lén.

Mô hình kênh nghe lén Gaussian được mô tả trong Hình 1.11. Trong đó, máy phát sẽ mã hóa bản tin M thành từ mã X^n, sau đó truyền qua kênh có nhiễu Gaussian, phía máy thu sẽ giải mã tín hiệu thu được Y^n thành bản tin $\hat{M}$, bên cạnh đó máy nghe lén Eve cũng thu nhận được tín hiệu Z^n truyền đi từ máy phát và giải mã thành bản tin $\bar{M}$. Mối quan hệ giữa đầu vào/ra của kênh truyền được mô tả như sau

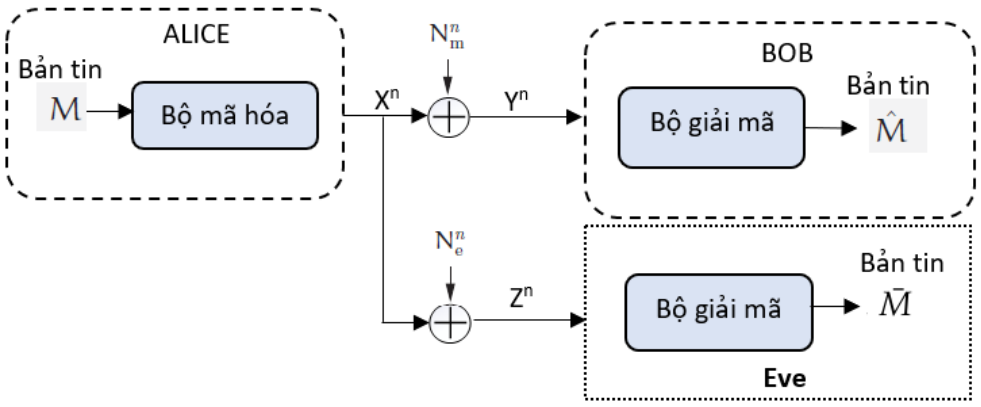
$$y_i = x_i + n_{m,i}, \tag{1.35}$$

$$z_i = x_i + n_{e,i}, \tag{1.36}$$

trong đó $n_{m,i}$ và $n_{e,i}$ là nhiễu AWGN thực (real-valued Gaussian) độc lập và có cùng phân bố, có giá trị trung bình bằng 0 và có phương sai tương ứng là σ_m^2 và σ_e^2, tức là $n_{m,i} \sim \mathcal{N}(0, \sigma_m^2)$ và $n_{e,i} \sim \mathcal{N}(0, \sigma_e^2)$.

Theo [14], tốc độ truyền tin bảo mật tối đa có thể đạt được hay còn gọi là dung lượng bảo mật cho kênh nghe lén Gaussian là [14]

$$C_s = \{C_m - Ce\}^+. \tag{1.37}$$



Hình 1.11: *Mô hình kênh nghe lén Gaussian*

trong đó $\{x\}^+ = max\{x, 0\}$ và C_m là dung lượng kênh chính, C_e là dung lượng kênh nghe lén, áp dụng công thức dung lượng kênh Gaussian [12], ta có

$$C_m = \frac{1}{2}\log_2\left(1 + \frac{P}{\sigma_m^2}\right). \tag{1.38}$$

$$C_e = \frac{1}{2}\log_2\left(1 + \frac{P}{\sigma_e^2}\right). \tag{1.39}$$

Như vậy dung lượng bảo mật của kênh nghe lén Gaussian được tính bằng hiệu dung lượng giữa kênh chính và dung lượng kênh nghe lén. Từ (1.37) chúng ta có thể thấy dung lượng bảo mật khác không khi tỉ số tín hiệu trên nhiễu của kênh hợp pháp tốt hơn kênh nghe lén, ngược lại dung lượng bảo mật bằng không. Trong thực tế, điều này có thể được hiểu là thiết bị nghe lén đang ở vị trí xa hơn thiết bị thu hợp pháp và nhận một phiên bản tín hiệu suy thoái.

Thay công thức (1.38) và (1.39) vào (1.37), dung lượng bảo mật kênh khi công suất truyền rất lớn có dạng như sau

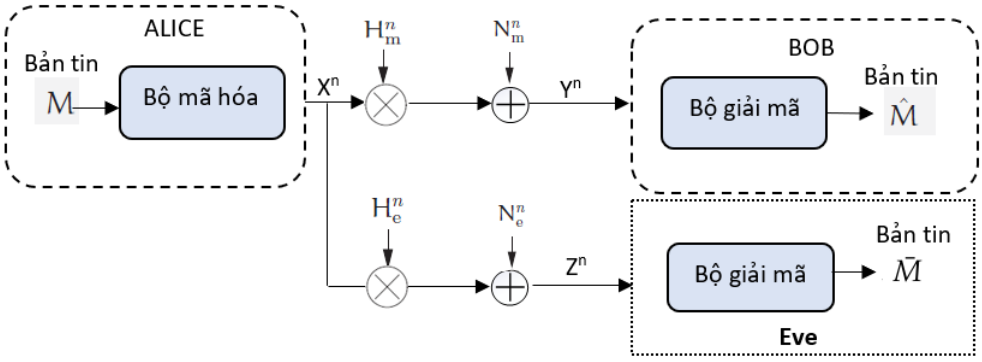
$$\lim_{P\to\infty} C_s(P) = \left(\frac{1}{2}\log\left(\frac{\sigma_e^2}{\sigma_m^2}\right)\right)^+. \tag{1.40}$$

Chúng ta thấy rằng khi tăng công suất truyền, dung lượng bảo mật kênh không tăng một cách không giới hạn. Điều này trái ngược với dung lượng kênh, khi tăng công suất truyền tin thì dung lượng kênh cũng tăng.

1.6.4 Kênh nghe lén fading

Chúng ta xem xét mô hình kênh fading có nghe lén như Hình 1.12. Trong luận án này tác giả giới hạn trên mô hình kênh truyền quasi-static fading, tức là hệ số

kênh truyền mặc dù là ngẫu nhiên nhưng không thay đổi trong toàn bộ quá trình truyền một từ mã [4].



Hình 1.12: *Mô hình kênh nghe lén fading*

Máy phát gửi bản tin M đến máy thu, bản tin M được mã hóa vào từ mã X^n với độ dài n để truyền tải qua kênh chính. Tín hiệu nhận được ở máy thu có dạng như sau

$$y_i = h_{m,i}x_i + n_{m,i}. \tag{1.41}$$

trong đó $h_{m,i}$ là hệ số kênh fading phức biến đổi theo thời gian và $n_{m,i}$ là nhiễu Gaussian phức đối xứng vòng với kỳ vọng bằng không của kênh chính, $n_{m,i} \sim \mathcal{CN}(0, \sigma_m^2)$. Hệ số $h_{m,i}$ là trạng thái kênh truyền độc lập với đầu ra kênh và thu được theo một phân bố xác suất $P(h_m)$. Do môi trường truyền tin là môi trường kênh truyền quasi-static fading nên hệ số kênh là hằng số trong thời gian truyền một từ mã, tức là $h_{m,i} = h_m$ với $\forall i$. Cùng thời gian, thiết bị nghe lén cũng có thể thu nhận được tín hiệu do máy phát truyền đi như sau

$$z_i = h_{e,i}x_i + n_{e,i}. \tag{1.42}$$

Do trong cùng một môi trường fading, tương tự như kênh chính ta có $h_{e,i} = h_e$ với $\forall i$ là hệ số kênh của kênh nghe lén và $n_{e,i}$ là nhiễu Gaussian phức đối xứng vòng với kỳ vọng bằng không tại kênh nghe lén, $n_{e,i} \sim \mathcal{CN}(0, \sigma_e^2)$.

Kênh truyền bị giới hạn về mặt công suất bởi [3]

$$\frac{1}{n}\sum_{i=1}^{n} E[|X(i)|^2] \leq P. \tag{1.43}$$

trong đó P là công suất phát trung bình, ngoài ra ta kí hiệu N_m và N_e lần lượt là công suất nhiễu trên kênh chính và kênh nghe lén. Khi đó tỉ số tín hiệu trên nhiễu tức thời tại máy thu hợp pháp và thiết bị nghe lén là

$$\gamma_{m,i} = \frac{P|h_m(i)|^2}{N_m}. \tag{1.44}$$

$$\gamma_{e,i} = \frac{P|h_e(i)|^2}{N_e}. \tag{1.45}$$

Trong mô hình nghe lén trên kênh Gaussian, nhiễu Gaussian được giả thiết là nhiễu thực. Trong mô hình nghe lén trên kênh fading, kênh chính và kênh nghe lén đều là kênh AWGN phức, tức là nhiễu trên hai kênh đều là biến ngẫu nhiên phức đối xứng vòng và có kỳ vọng bằng không. Do mỗi kênh AWGN phức có thể xem là hai kênh AWGN thực [27, Phụ lục B], vì vậy dung lượng bảo mật kênh trong (1.37) có thể được viết lại như sau

$$C_s = \log_2(1 + \frac{P}{N_m}) - \log_2(1 + \frac{P}{N_e}). \tag{1.46}$$

Kênh truyền là kênh quasi-static fading nên có thể xem kênh chính như là kênh AWGN phức và hệ số kênh là hằng số trong thời gian truyền một từ mã, [27, Chương 5], với SNR $\gamma_m = \frac{P|h_m|^2}{N_m}$ và dung lượng kênh là

$$C_m = \log_2(1 + \gamma_m). \tag{1.47}$$

Tương tự, dung lượng kênh của kênh nghe lén được cho bởi

$$C_e = \log_2(1 + \gamma_e) \tag{1.48}$$

với SNR $\gamma_e = \frac{P|h_e|^2}{N_e}$. Từ (1.47) và (1.48), chúng ta có thể mô tả dung lượng bảo mật của hệ thống trong môi trường kênh fading như sau [3]

$$C_s = \begin{cases} \log_2(1 + \gamma_m) - \log_2(1 + \gamma_e), & \text{nếu } \gamma_m > \gamma_e \\ 0, & \text{nếu } \gamma_m \leq \gamma_e \end{cases} \tag{1.49}$$

Các công trình nghiên cứu đầu tiên về bảo mật tầng vật lý [7, 14, 30] đã chỉ ra rằng dung lượng bảo mật khác không đạt được khi kênh nghe lén có chất lượng thấp hơn kênh chính, yêu cầu này nhiều khi rất khó khả thi trong thực tế. Tuy

nhiên, trong các công trình nghiên cứu mở rộng sau đó cho các kênh fading có sự xuất hiện của thiết bị nghe lén đã chứng minh được rằng bảo mật dựa trên lý thuyết thông tin là hoàn toàn có thể đạt được ngay cả khi kênh nghe lén có SNR trung bình tốt hơn so với kênh hợp pháp [3,4,19].

Trong những năm gần đây, kỹ thuật truyền tin vô tuyến đã phát triển nhanh, các kỹ thuật như truyền theo búp sóng [68, 120, 121], đa ăng-ten [2, 16, 22, 38], truyền thông cộng tác [8,37], nhiễu nhân tạo [9,34,35], phân tập lựa chọn [2,125], đã được kết hợp sử dụng nhằm nâng cao khả năng bảo mật ở tầng vật lý để chống lại kiểu tấn công nghe lén.

1.6.5 Mã wiretap

Mục tiêu khi truyền tin trên kênh nghe lén là đảm bảo tính bí mật của thông tin được truyền đi, có nghĩa rằng đối tượng nghe lén Eve càng mập mờ về bản tin truyền đi thì tính an toàn, bảo mật càng cao. Mô hình kênh nghe lén như đã mô trong hình 1.10, một thông điệp M được mã hóa thành một từ mã $X^n = (X_1, ..., X_n)$ và truyền qua kênh nghe lén, Eve thu được bản tin Z^n, khi đó thông tin tương hỗ giữa bản tin M và Z^n được mô tả như sau [139].

$$\begin{aligned} I(M;Z^n) &= I(X^n;Z^n) - I(X^n;Z^n|M) \\ &= I(X^n;Z^n) + H(X^n|Z^n,M) - H(X^n|M). \end{aligned} \tag{1.50}$$

Từ đây có thể thấy rằng nếu $H(X^n|M)$ bằng không, tức là có một ánh xạ một-một giữa các thông điệp và các từ mã, chúng ta có $I(M|Z^n) = I(X^n;Z^n)$ tăng tuyến tính với n. Do đó nếu làm cho $H(X^n|M)$ khác không, chúng ta có thể kiểm soát được quá trình tăng của $I(M;Z^n) = H(X^n|M)$, điều này có thể đạt được bằng cách ánh xạ một thông điệp vào một trong các từ mã hợp lệ một cách ngẫu nhiên. Như vậy bản mã thu được phải có tính ngẫu nhiên để đảm bảo việc mã hóa gây ra khó khăn cho Eve khi thu thập thông tin. Trong những năm gần đây, các nhà nghiên cứu đã nỗ lực để phát triển các bộ mã tường minh cho kênh nghe lén. Một số loại mã theo cấu trúc tập từ mã (Coset) đã được xây dựng thành công như mã LDPC, [26], mã polar [15], và mã lattice [140, 141].

1.6.6 Phép đo hiệu năng bảo mật hệ thống

Hiệu năng bảo mật của hệ thống mạng không dây trên các kênh fading được đánh giá chủ yếu thông qua các phép đo [160]: *Dung lượng bảo mật*, *xác suất dừng bảo mật*, *xác suất nghe lén hợp pháp thành công*, *xác suất bị nghe lén* và *thông lượng bảo mật*. Trong phần này tác giả tóm lược một số phép đo hiệu năng bảo mật dùng để đánh giá hiệu năng bảo mật các mô hình mạng NOMA được đề xuất trong luận án.

1.6.6.1 Dung lượng bảo mật

Trước tiên cần nhắc lại khái niệm dung lượng kênh truyền không dây. Nó là tốc độ truyền tin cực đại mà tại tốc độ này truyền thông tin trên kênh đó đảm bảo được độ tin cậy. Theo Shannon, dung lượng tức thời của kênh fading được biểu diễn bởi công thức sau [27]

$$C = W \log_2(1+\gamma). \tag{1.51}$$

trong đó W là băng thông của kênh truyền và γ là tỷ số công suất tín hiệu trên nhiễu tại máy thu.

Như đã đề cập ở phần trên, các nghiên cứu về bảo mật tầng vật lý trong mạng không dây định nghĩa dung lượng bảo mật C_s là sự khác biệt giữa dung lượng kênh hợp pháp và dung lượng kênh nghe lén [4, 19]. Nói cách khác, dung lượng bảo mật là hiệu dung lượng kênh hợp pháp và kênh nghe lén. Do tính chất không âm của dung lượng kênh, dung lượng bảo mật được biểu diễn như sau [3]

$$C_s = \begin{cases} \log_2(1+\gamma_m) - \log_2(1+\gamma_e), & \text{nếu } \gamma_m > \gamma_e \\ 0, & \text{nếu } \gamma_m \leq \gamma_e \end{cases} \tag{1.52}$$

trong đó γ_m, và γ_e lần lượt là SNR của kênh hợp pháp và kênh nghe lén, tương ứng. Từ (1.52), có thể thấy rằng dung lượng bảo mật kênh lớn hơn 0 khi $\gamma_m > \gamma_e$. Từ công thức định nghĩa dung lượng bảo mật của kênh truyền ở trên, có thể thấy rằng để tăng dung lượng bảo mật của hệ thống ta có thể tăng dung lượng kênh của kênh chính. Điều này có thể thực hiện một cách đơn giản là tăng công suất của máy phát. Tuy nhiên, việc này cũng đồng nghĩa với việc làm tăng hiệu suất chặn thu tín hiệu của thiết bị nghe lén. Do đó, để có thể đảm bảo tính bảo mật

khi truyền tin, hệ thống cần có những giải pháp tăng dung lượng kênh hợp pháp và làm suy hao tối đa dung lượng kênh nghe lén. Đây là một trong những vấn đề mà các nghiên cứu về bảo mật thông tin tầng vật lý trong mạng không dây cần giải quyết.

1.6.6.2 Xác suất dừng bảo mật

Khái niệm xác suất dừng bảo mật (SOP) được giới thiệu lần đầu tiên trong công trình [4]. Gọi $R_s > 0$ là tốc độ truyền tin bảo mật của hệ thống. Xác suất dừng bảo mật xảy ra khi dung lượng bảo mật tức thời C_s nhỏ hơn giá trị của R_s, nghĩa là

$$\mathcal{O}_{sec} = Pr\{C_s < R_s\}. \tag{1.53}$$

Để tính toán được xác suất dừng bảo mật, trạng thái kênh truyền của thiết bị nghe lén phải được xác định. Tuy nhiên trong trường hợp thiết bị nghe lén hoạt động theo chế độ thụ động thì việc xác định được trạng thái kênh truyền có thể không khả thi trừ trường hợp trong một số mạng mà thiết bị nghe lén là một phần của hệ thống, tức là thiết bị nhận là hợp pháp với một số bản tin nhất định nhưng đồng thời là thiết bị nghe lén đối với các bản tin của người dùng khác trong hệ thống [5,6]. Trường hợp không xác định được trạng thái kênh nghe lén, chúng ta buộc phải chọn một tốc độ bảo mật R_s, trong trường hợp này máy phát giả thiết rằng dung lượng kênh nghe lén sẽ là $C'_e = C_s - R_s$. Khi tốc độ bảo mật $R_s < C_s$, tức là tốc độ bảo mật được chọn nhỏ hơn dung lượng bảo mật thức thời, hay nói cách khác kênh nghe lén có chất lượng kém hơn so với kênh hợp pháp thì quá trình truyền tin được bảo mật. Ngược lại, nếu $R_s > C_s$ thì $C_e > C'_e$ và theo nguyên lý bảo mật dựa trên lý thuyết thông tin thì tính bảo mật thông tin sẽ bị phá vỡ, thiết bị nghe lén có thể thu và giải mã thành công các tín hiệu được truyền đi từ máy phát. Từ những phân tích ở trên chúng ta thấy xác suất dừng bảo mật thích ứng cả trường hợp máy phát không có đầy đủ thông tin về trạng thái của kênh nghe lén và phải chọn một tốc độ bảo mật, do đó xác suất dừng bảo mật của hệ thống là phép đo quan trọng và được sử dụng phổ biến nhất để đánh giá hiệu năng bảo mật.

1.6.6.3 Xác suất nghe lén hợp pháp thành công

Đối với các hệ thống vô tuyến, bên cạnh mục đích truyền tin thì trong rất nhiều ngữ cảnh, hệ thống được thiết kế với mục đích thu thập tín hiệu từ các thiết bị bất hợp pháp với mục đích giám sát để đảm bảo an ninh, an toàn cho hệ thống. Khi đó hiệu suất bảo mật của hệ thống được đánh giá thông qua xác suất nghe lén hợp pháp thành công (SLEP) tức là xác suất mà máy thu hợp pháp thu thập và giải mã thành công tín hiệu từ máy phát tín hiệu bất hợp pháp [119]. Gọi R_m là tốc độ thu thập dữ liệu đạt được trên thiết bị nghe lén hợp pháp và R là ngưỡng tốc độ truyền dữ liệu tối thiểu để máy thu hợp pháp có thể giải mã tín hiệu. Xác suất nghe lén hợp pháp thành công xảy ra khi tốc độ truyền dữ liệu đạt được trên kênh nghe lén hợp pháp lớn hơn ngưỡng tốc độ truyền dữ liệu tối thiểu quy định trước, khi đó xác suất nghe lén hợp pháp thành công được mô tả như sau

$$\mathcal{O}_{suc} = Pr\{R_m \geq R\}. \tag{1.54}$$

Xác suất nghe lén hợp pháp thành công phụ thuộc vào chất lượng kênh nghe lén hợp pháp, công suất tín hiệu thu được. Vì vậy các nghiên cứu hiện nay tập trung vào các kỹ thuật như gây nhiễu chủ động kết hợp với kỹ thuật đa ăng-ten, truyền thông cộng tác để chủ động cải thiện chất lượng tín hiệu nghe lén.

1.6.6.4 Xác suất bị nghe lén

Xác suất bị nghe lén (IP) thường được sử dụng như một phép đo hiệu suất khác trong việc đánh giá bảo mật tầng vật lý. Nó được định nghĩa là xác suất mà dung lượng bảo mật nhỏ hơn không, nói cách khác kênh nghe lén tốt hơn kênh hợp pháp [142]. Trên mô hình kênh nghe lén như mô tả trong Hình 1.10, khi máy phát truyền tín hiệu đến máy thu, thiết bị nghe lén Eve cũng thu và giải mã được tín hiệu từ máy phát, nói cách khác hệ thống bị nghe lén. Xác suất bị nghe lén xảy ra khi tốc độ thu thập dữ liệu đạt được trên kênh nghe lén lớn hơn ngưỡng tốc độ dữ liệu tối thiểu mà Eve có thể giải mã tín hiệu. Ký hiệu R_e là tốc độ thu thập dữ liệu đạt được kênh nghe lén và R ngưỡng tốc độ dữ liệu tối thiểu để Eve có thể giải mã, xác suất bị nghe lén được mô tả như sau

$$\mathcal{O}_{int} = Pr\{R_e > R\}. \tag{1.55}$$

1.6.6.5 Xác suất rớt gói tin

Trong quá trình truyền các gói tin từ máy phát tới máy thu, do tác động vật lý của môi trường truyền nên thời gian truyền các gói tin có thể bị kéo dài vượt ngưỡng thời gian chờ cho phép tức gói tin truyền không thành công. Xác suất rớt gói tin (PTP) xảy ra khi thời gian truyền gói tin lớn hơn ngưỡng thời gian chờ gói tin t_{out} [143], được mô tả bằng công thức toán học như sau

$$\mathcal{O}_{otm} = Pr\{T \geq t_{out}\}, \tag{1.56}$$

trong đó T là thời gian truyền gói tin và t_{out} là ngưỡng thời gian chờ gói tin.

1.6.6.6 Tính công bằng thời gian truyền tin

Trong mạng NOMA, người dùng được nhóm thành từng nhóm, mỗi người dùng trong nhóm được phân bổ công suất theo nguyên tắc người dùng có độ lợi kênh truyền mạnh hơn sẽ được phân bổ công suất nhỏ hơn. Trong thực tế, nhiều ứng dụng đòi hỏi thời gian truyền tin từ máy phát đến những người dùng trong cùng một nhóm (cặp) phải bằng nhau để đảm bảo chất lượng dịch vụ giữa những người dùng là như nhau. Do đó máy phát cần điều chỉnh mức phân bổ công suất cho từng người dùng để đảm bảo thời gian truyền gói tin trung bình từ máy phát đến những người dùng trong cùng một nhóm là xấp xỉ bằng nhau, điều này được mô tả bằng công thức toán học như sau

$$\alpha^* = \arg \min_{0<\alpha<0.5} |\, \mathbf{E}[T_1] - \mathbf{E}[T_2]|, \tag{1.57}$$

trong đó $\mathbf{E}[T_i]$ (i = 1,2) là thời gian kỳ vọng để truyền gói tin từ máy phát tới hai người dùng cuối và α là hệ số phân bổ công suất.

1.6.7 So sánh bảo mật dùng mật mã và bảo mật tầng vật lý

Bảo mật tầng vật lý chưa được hoàn thiện và chưa được ứng dụng nhiều trong thực tế, tuy nhiên các đặc điểm của bảo mật tầng vật lý so với bảo mật dùng mật mã được so sánh như trong Bảng 1.2 dưới đây đã thu hút sự quan tâm của các nhà nghiên cứu trên khắp thế giới [97].

Tiêu chí so sánh	Bảo mật dùng mật mã	Bảo mật tầng vật lý
Cơ sở lý thuyết	Dựa trên độ phức tạp tính toán như phân tích các số nguyên lớn, tính logarit rời rạc,...của các thuật toán mã hóa	Dựa trên lý thuyết thông tin
Mức độ bảo mật	Có thể bị phá mã bởi tính toán vét cạn	Đạt độ bảo mật hoàn hảo, không có giới hạn tính toán đối với thiết bị nghe lén
Các yêu cầu về khả năng tính toán	Phụ thuộc nhiều vào khả năng tính toán	Độc lập với khả năng tính toán
Vấn đề quản lý khóa	Chi phí lớn cho việc tạo, quản lý và phân phối khóa	Không cần khóa nên không cần bất kỳ chi phí gì về khóa
Tiêu chí đánh giá	Không thể đánh giá chính xác lượng thông tin bí mật bị rò rỉ	Đánh giá chính xác mức độ bảo mật bằng tỷ lệ mập mờ về nguồn tin
Khả năng thích ứng với những thay đổi của kênh truyền	Ít có khả năng thích ứng với thay đổi của kênh truyền	Điều chỉnh tham số và chiến lược truyền tin để thích ứng tốt với các thay đổi của kênh truyền
Thực tế triển khai	Đang được triển khai rộng rãi, công nghệ đã hoàn chỉnh và không quá tốn kém	Đã xuất hiện giải pháp cho mạng không dây như phân phối khóa lượng tử và đã được triển khai trên một vài hệ thống tuy nhiên công nghệ chưa thực sự sẵn sàng và có khả năng tốn kém để triển khai

Bảng 1.2: *So sánh bảo mật dùng mã mật với bảo mật tầng vật lý* [97].

1.7 Các công trình nghiên cứu liên quan đến luận án

1.7.1 Các nghiên cứu về bảo mật mạng NOMA cộng tác

Một kỹ thuật phổ biến được khai thác sử dụng để cải thiện hiệu năng bảo mật trong mạng NOMA là kỹ thuật truyền thông cộng tác hay còn gọi là kỹ thuật truyền thông đa chặng. Kỹ thuật này vừa nâng cao tính an toàn bảo mật vừa tăng độ tin cậy của hệ thống. Cho đến nay đã có một số nghiên cứu về chủ đề này [36, 57, 78, 79, 123, 132]. Trong [57], các tác giả đã khảo sát hiệu năng bảo mật thông qua xác suất dừng bảo mật và dung lượng bảo mật dương của hệ thống NOMA cộng tác trong trường hợp sử dụng giao thức khuếch đại và chuyển tiếp, giải mã và chuyển tiếp, các tác giả đã chỉ ra rằng xác suất dừng bảo mật là hằng số trên miền SNR cao và hiệu năng bảo mật của hệ thống không phụ thuộc vào điều kiện kênh truyền giữa thiết bị chuyển tiếp và người dùng yếu. Trong [36, 78], các tác giả khảo sát hiệu năng bảo mật của hệ thống NOMA với nút chuyển tiếp hoạt động theo chế độ song công (full-duplex) với hai kịch bản là các đối tượng nghe lén cộng tác (colluding) và không cộng tác với nhau (non-colluding), các kết quả nghiên cứu đã chỉ ra rằng sử dụng nút chuyển tiếp song công sẽ cải thiện đáng kể mức độ bảo mật của hệ thống so với nút chuyển tiếp bán song công (half-duplex) với cả hai kịch bản hoạt động của thiết bị nghe lén. Trong [79, 81, 123], các tác giả đã đánh giá SOP của một hệ thống NOMA được trang bị nhiều nút chuyển tiếp sử dụng giao thức DF và AF và đề xuất ra các phương thức lựa chọn nút chuyển tiếp khác nhau, các kết quả phân tích và mô phỏng đã cho thấy hiệu năng bảo mật của hệ thống được cải thiện đáng kể. Một cách tiếp cận khác nhận được nhiều quan tâm trong kỹ thuật hợp tác chuyển tiếp là tạo nhiễu nhân tạo để làm suy giảm dung lượng kênh nghe lén từ đó cải thiện hiệu năng bảo mật mạng NOMA. Các công trình [50–52, 80, 124, 129] đã khảo sát mô hình mạng NOMA sử dụng máy phát hoặc nút chuyển tiếp gây nhiễu nhân tạo lên thiết bị nghe lén. Cụ thể, trong [124] đề xuất giải pháp nút nguồn gây nhiễu lên thiết bị nghe lén trong khi nút chuyển tiếp truyền tín hiệu đến thiết bị đích. Trong tài liệu [80], các tác giả đề xuất mô hình mạng NOMA cộng tác sử dụng thiết bị chuyển tiếp song công với nhiều ăng-ten, thiết bị chuyển tiếp truyền tín hiệu từ nguồn tới đích đồng thời sinh nhiễu nhân tạo để gây nhiễu lên thiết bị nghe lén. Hoặc trong công trình

nghiên cứu [50] đã đề xuất sử dụng cả thiết bị chuyển tiếp song công và máy phát để gây nhiễu lên thiết bị nghe lén theo từng giai đoạn truyền tín hiệu từ nút nguồn tới đích dựa trên nút chuyển tiếp. Ngoài ra, sử dụng thiết bị chuyển tiếp song công để tạo nhiễu nhân tạo trên mạng NOMA chuyển tiếp hai chiều cũng đã được xem xét trong [51].

1.7.2 Các nghiên cứu về chủ động nghe lén trong mạng NOMA

Theo cách tiếp cận truyền thống, nghe lén được coi là hoạt động bất hợp pháp. Do đó, phần lớn các nghiên cứu tập trung theo hướng tìm các giải pháp để ngăn chặn việc bị lộ hoặc bị thu thập một cách bất hợp pháp, ví dụ [51,53,63,68,81,149]. Tuy nhiên có rất nhiều ngữ cảnh trong thực tế như trong lĩnh vực quân sự, phòng chống tội phạm..., chúng ta cần thu thập thông tin để thực hiện việc giám sát, theo dõi các hoạt động bất hợp pháp trên mạng, khi đó quá trình nghe lén để thu thập thông tin được trao đổi giữa máy phát và máy thu bất hợp pháp được coi là hợp pháp [102, 119, 150]. Mô hình tổng quát cho hệ thống chủ động nghe lén hợp pháp gồm có máy phát và máy thu bất hợp pháp, một thiết bị giám sát có khả năng nghe lén, thu thập thông tin trao đổi giữa máy phát và máy thu bất hợp pháp [102]. Để thực hiện mục đích nghe lén hợp pháp thì dung lượng kênh nghe lén hợp pháp phải lớn hơn dung lượng kênh bất hợp pháp nên các công trình nghiên cứu đều tập trung làm giảm chất lượng kênh truyền tin bất hợp pháp, tăng chất lượng kênh nghe lén hợp pháp. Các nghiên cứu sử dụng các phép đo như tốc độ nghe lén đạt được, tốc độ nghe lén trung bình, xác suất nghe lén hợp pháp thành công, xác suất giám sát thành công [54,106,108,112,119] để đánh giá hiệu suất quá trình nghe lén hợp pháp.

Cho đến nay, đã có một số nghiên cứu về các kỹ thuật chủ động nghe lén hợp pháp để xây dựng các hệ thống giám sát nhằm mục đích ngăn chặn các hoạt động bất hợp pháp trên mạng không dây. Cụ thể, nghiên cứu [102], các tác giả đề xuất một hệ thống nghe lén hợp pháp thông qua phương pháp gây nhiễu để tối đa hóa tốc độ nghe lén trung bình, trong đó thiết bị giám sát phát tín hiệu làm nhiễu và điều chỉnh tối ưu công suất để điều chỉnh tốc độ nghe lén. Trong công trình [150], J. Xu và cộng sự nghiên cứu một mô hình chủ động nghe lén bằng cách sử dụng kỹ thuật gây nhiễu có khả năng nhận thức và đề xuất chính sách

phân phối công suất tối ưu để tối đa hóa xác suất nghe lén thành công và tốc độ nghe lén trong cả trường hợp kênh nghe lén nhạy cảm và không nhạy cảm với độ trễ. Mở rộng từ các công trình nghiên cứu [102,150], các tác giả trong [111] nghiên cứu mô hình trong đó thiết bị giám sát hoạt động ở chế độ song công và sử dụng đa ăng-ten. Các tác giả đã tối ưu hóa xác suất nghe lén thành công bằng cách tối ưu công suất làm nhiễu và sử dụng các véc tơ chùm tín hiệu (beamforming) khi truyền và nhận tín hiệu.

Bên cạnh đó, một số nghiên cứu tập trung theo hướng chủ động nghe lén trên các hệ thống truyền tin bất hợp pháp sử dụng kỹ thuật truyền thông cộng tác [103,109,110]. Cụ thể, G. Ma và cộng sự nghiên cứu nghe lén trên kênh truyền bất hợp pháp truyền tin qua hai chặng và sử dụng một thiết bị giám sát hợp pháp hoạt động chế độ bán song công. Họ kết luận rằng tốc độ nghe lén tại thiết bị giám sát hợp pháp có thể được cải thiện đáng kể bằng cách tối ưu hóa lựa chọn chế độ nghe lén cũng như công suất gây nhiễu [110]. X. Jiang và cộng sự nghiên cứu một hệ thống hoạt động bất hợp pháp sử dụng thiết bị chuyển tiếp bằng giao thức DF. Trong nghiên cứu này, các tác giả đề xuất hai chiến lược để tối đa hóa tốc độ nghe lén và chiến lược phân phối công suất tối ưu. Kết quả nghiên cứu chỉ ra rằng hiệu suất nghe lén của hệ thống tốt hơn so với các mô hình tham chiếu chuẩn [109]. Trong khi đó, các tác giả trong [103] đề xuất một kịch bản làm nhiễu tối ưu rút gọn cho việc chủ động nghe lén trên mạng chuyển tiếp bằng giao thức AF. Kết quả chỉ ra rằng kịch bản làm nhiễu tối ưu vượt trội so với giám sát chủ động và giám sát chủ động thông qua làm nhiễu với mức công suất cố định. Trong bài báo [151], H. Wu và đồng nghiệp nghiên cứu một kịch bản chủ động nghe lén với một thiết bị giám sát hoạt động như một thiết bị chuyển tiếp theo giao thức DF. Các tác giả đã tối ưu hóa công suất gây nhiễu của thiết bị giám sát và vị trí triển khai thiết bị chuyển tiếp để tối đa hóa tốc độ nghe lén trung bình.

Ngược lại với các nghiên cứu chủ động nghe lén trên các mô hình mạng sử dụng kỹ thuật truyền thông cộng tác, một số công trình lại sử dụng kỹ thuật truyền thông cộng tác để thực hiện chủ động nghe lén. Trong nghiên cứu [106], J. Moon và đồng nghiệp xem xét một hệ thống chủ động nghe lén trong đó một thiết bị giám sát thực hiện nghe lén thông tin trao đổi giữa một cặp thiết bị phát và thu tín hiệu bất hợp pháp với sự hỗ trợ của các thiết bị chuyển tiếp sử dụng

giao thức AF, FD và một thiết bị gây nhiễu. Các tác giả trong nghiên cứu này đề xuất một phương pháp tối ưu hai lớp để phân phối công suất cho cả thiết bị chuyển tiếp và thiết bị gây nhiễu nhằm tối đa hóa tốc độ nghe lén. Ngoài ra, J. Moon và đồng nghiệp còn đề xuất một phương pháp chủ động nghe lén mới thông qua phương pháp giả mạo cộng tác để cải thiện khả năng nghe lén thông tin của thiết bị giám sát hợp pháp, và ba chiến lược làm giả mạo cộng tác khả dụng được đề xuất để tối đa hóa hiệu suất nghe lén [105].

Tất cả các nghiên cứu trên đều giả thiết giữa máy phát và máy thu bất hợp pháp chỉ có một kênh truyền, B. Li và đồng nghiệp đã mở rộng, nghiên cứu mô hình chủ động nghe lén trên hệ thống truyền tin bất hợp pháp có nhiều kênh truyền [39, 104]. Trong [104], B. Li đưa ra phép đo có tên là hiệu quả năng lượng nghe lén để đánh giá hiệu quả của quá trình nghe lén và đề xuất giải pháp trong đó thiết bị giám sát hợp pháp có khả năng vừa nghe lén vừa gây nhiễu lên máy thu bất hợp pháp để tối đa hóa hiệu quả năng lượng nghe lén trên nhiều kênh truyền bất hợp pháp. Mở rộng từ công trình [104], B. Li và đồng nghiệp trong nghiên cứu [39] đã đề xuất một chiến lược lựa chọn chiến thuật can thiệp mới và giải pháp phân bổ công suất dựa trên kỹ thuật gây nhiễu hoặc chuyển tiếp cho thiết bị giám sát dưới ràng buộc công suất phát tối đa của thiết bị giám sát để cải thiện hiệu suất nghe lén.

Trong các nghiên cứu kể trên đều xem xét các mô hình mạng không dây truyền tin bất hợp pháp nói chung, chỉ có D. Xu và cộng sự đã xem xét một hệ thống mà ở đó máy phát bất hợp pháp sử dụng NOMA để truyền dữ liệu tới nhiều nhóm người dùng hoạt động bất hợp pháp, các tác giả đã đề xuất một thuật toán lặp theo kinh nghiệm (heuristics) để thu thập được thông tin từ nhiều người dùng bất hợp pháp nhất [55].

1.7.3 Các nghiên cứu về bảo mật mạng SISO NOMA

Dựa vào số lượng ăng-ten của máy phát, máy thu và thiết bị nghe lén, có thể chia thành các mô hình mạng NOMA thành bốn nhóm sau: Nhóm thứ nhất, tất cả các nút trong mạng được trang bị một ăng-ten, mô hình này gọi là SISO NOMA [53, 63, 70, 77, 85]; Nhóm thứ 2 là mô hình mạng trong đó máy phát được trang bị nhiều ăng-ten và máy thu được trang bị một ăng-ten, còn gọi là SIMO

NOMA [52, 83, 84, 120]; Nhóm thứ ba cả máy phát và máy thu đều được trang bị nhiều ăng-ten, nhóm này được gọi là MIMO NOMA [76, 101, 121]; Nhóm cuối cùng cả máy phát, máy thu đều được trang bị với số lượng ăng-ten rất lớn, gọi là massive MIMO NOMA [72–75].

Các công trình nghiên cứu áp dụng PLS vào NOMA ban đầu chủ yếu tập trung vào các hệ thống SISO. Cụ thể, trong [70], các tác giả đã đề xuất giải pháp phân bổ công suất một cách tối ưu để tổng dung lượng bảo mật đạt tối đa và thỏa mãn ràng buộc giới hạn công suất phát và chất lượng dịch vụ của tất cả người dùng. Các kết quả thu được cho thấy rằng tổng dung lượng bảo mật được tối đa hóa khi công suất phụ được sử dụng và chỉ tăng dung lượng bảo mật cho người dùng mạnh nhất, điều này dẫn đến tình trạng không công bằng trong hệ thống. Để giải quyết tình trạng này, vấn đề tối đa dung lượng bảo mật tối thiểu thỏa mãn ràng buộc về ngưỡng dừng bảo mật và công suất truyền tin đã được xem xét trong [63]. Các tác giả trong [77] đã khảo sát hệ thống NOMA với trạm cơ sở có khả năng truyền cả tín hiệu và năng lượng cho máy thu, tính toán tối ưu phân bổ công suất và lựa chọn tỷ lệ phân chia năng lượng để tổng dung lượng bảo mật của hệ thống là lớn nhất. Mở rộng cách tiếp cận từ các công trình đã trình bày ở trên, các tác giả trong [85] đã khảo sát tính bảo mật của một mô hình mạng NOMA thỏa mãn ràng buộc đảm bảo độ tin cậy với hai kịch bản khác nhau về khả năng giải mã tín hiệu của thiết bị nghe lén. Khác với kịch bản thiết bị nghe lén hoạt động thụ động trong đa số các nghiên cứu, trong [53], một cơ chế phân bổ công suất để vừa đảm bảo tính bảo mật vừa tối ưu về xác suất dừng hệ thống đã được đề xuất để chống lại thiết bị nghe lén vừa có khả năng thu tín hiệu đồng thời gây nhiễu lên máy phát.

1.7.4 Các nghiên cứu về bảo mật mạng NOMA nhận thức

Mạng vô tuyến nhận thức (CRN) là công nghệ tiềm năng để giải quyết vấn đề khan hiếm tần số. Người dùng trong CRN được chia thành hai loại, gọi là người dùng sơ cấp (PU) và người dùng thứ cấp (SU). PU có ưu tiên cao nhất để truy cập tần số được cấp phép trong khi SU được phép truy cập tần số được cấp phép nếu nó không làm giảm hiệu suất của PU [144]. Mạng vô tuyến nhận thức được chia thành ba loại, đó là: dạng nền, dạng đan xen và dạng chồng chập trong đó mạng

vô tuyến nhận thức dạng nền nhận được sự quan tâm của các nhà nghiên cứu do mạng thứ cấp không bị giới hạn bởi hoạt động của mạng sơ cấp [153]. Tuy nhiên, để tránh gây can nhiễu cho mạng sơ cấp, máy phát thứ cấp của mạng vô tuyến nhận thức dạng nền phải điều chỉnh công suất phát để công suất can nhiễu nhận tại máy thu sơ cấp phải nhỏ hơn một giá trị quy định trước, thường được gọi là công suất can nhiễu tối đa cho phép [152].

Trong khi đó công nghệ NOMA được đề xuất như một ứng viên tiềm năng cho mạng 5G do khả năng đạt được mức hiệu suất phổ tần số cao, tăng dung lượng kênh truyền, hỗ trợ nhiều kết nối [154]. Công nghệ này có thể tích hợp với các công nghệ khác như massive MIMO, milimeter-Wave, thu hoạch năng lượng qua sóng vô tuyến...

Các nghiên cứu đã chỉ ra rằng, tích hợp công nghệ NOMA với CRN, hiệu quả sử dụng phổ tần số được cải thiện đáng kể [145]. Ví dụ, mô hình mạng NOMA nhận thức được đề xuất trong [144] bao gồm mạng sơ cấp (PN) gồm có một máy phát (P-Tx) và một máy thu (P-Rx), mạng thứ cấp (SN) gồm có một máy phát (S-Tx) và hai máy thu (SDs), mạng thứ cấp sử dụng công nghệ NOMA để truyền tin. Trong nghiên cứu này, các tác giả đề xuất giải pháp tối ưu phân bổ công suất phát để có thể giảm đáng kể xác suất dừng hoạt động của mạng thứ cấp và cải thiện thông lượng hệ thống so với các kịch bản phân phối công suất bằng nhau hoặc ngẫu nhiên. Trong [146], các tác giả nghiên cứu mạng NOMA nhận thức với sự hỗ trợ của các thiết bị chuyển tiếp. Các tác giả đã đề xuất một kịch bản S-Tx lựa chọn từng phần thiết bị chuyển tiếp để truyền dữ liệu đến người dùng thứ cấp. Các kết quả phân tích cho thấy hiệu suất của mạng NOMA nhận thức tốt hơn đáng kể so với kịch bản sử dụng phương pháp đa truy cập trực giao nhận thức (cognitive OMA).

Cho đến nay, bên cạnh những nghiên cứu đánh giá về hiệu suất, đã có một số nghiên cứu về bảo mật thông tin trong mạng NOMA nhận thức. Trong [147], các tác giả đã đề xuất một phương pháp cộng tác kết hợp kênh nghe lén và kênh hợp pháp. Các tác giả đã xây dựng các biểu thức dạng đóng xác suất dừng hoạt động của người dùng PU, SUs và xác suất nghe lén của Eve để đánh giá hiệu suất bảo mật mạng NOMA nhận thức. Các kết quả cho thấy rằng phương án chọn SU khi kết hợp với kênh nghe lén có khả năng cải thiện một phần về hiệu suất bảo mật

so với kênh hợp pháp. Nghiên cứu [148] đã đề xuất chiến lược mới để đảm bảo bí mật khi truyền tin trên môi trường kênh truyền Nakagami-m fading bằng cách nhóm người dùng PU và SU thành cặp dựa trên độ lợi kênh truyền của chúng với giả định coi người dùng SU như là đối tượng nghe lén. Nghiên cứu [157] đề xuất hai lược đồ lựa chọn người dùng thứ cấp là gây nhiễu tối thiểu và gây nhiễu tối đã để cải thiện tính bảo mật của người dùng sơ cấp trong mạng NOMA nhận thức. Mở rộng hơn so với [157], trong [158] các tác giả đã xem xét mô hình mạng NOMA nhận thức có nhiều thiết bị nghe lén có khả năng thu thập năng lượng qua sóng vô tuyến và sử dụng cơ chế sử dụng mạng sơ cấp để cộng tác gây nhiễu nhân tạo lên thiết bị nghe lén nhằm nâng cao tính bảo mật cho người dùng mạng sơ cấp.

Khác với các bài báo ở trên tập trung vào việc cải thiện hiệu năng bảo mật, trong công trình [156], các tác giả ngoài việc đề xuất giải pháp nâng cao khả năng bảo mật mà còn khảo sát sự đánh đổi giữa bảo mật và độ tin cậy của mô hình mạng NOMA nhận thức dạng nền.

1.7.5 Nhận xét về các công trình nghiên cứu

Qua khảo sát và phân tích các kết quả nghiên cứu về bảo mật tầng vật lý trong mạng NOMA trên đây, nghiên cứu sinh nhận thấy còn một số vấn đề tồn tại cần được xem xét, cụ thể như sau:

Các công trình nghiên cứu đánh giá hiệu năng bảo mật tầng vật lý mạng NOMA cộng tác được đề cập ở trên [54, 106, 108, 112, 119], mặc dù đã có nhiều thành tựu, tuy nhiên các nghiên cứu này mới chỉ xem xét trường hợp mô hình hệ thống có một thiết bị nghe lén độc lập hoặc có nhiều thiết bị nghe lén kết hợp với nhau hoặc không kết hợp với nhau để thu thập thông tin. Hơn nữa, cho đến nay cũng chưa có bài báo nào xem xét mô hình mạng NOMA cộng tác trên kênh truyền tổng quát $\alpha - \mu$ fading.

Mặt khác, các nghiên cứu đánh giá hiệu năng bảo mật mô hình mạng có chiến lược chủ động nghe lén cho đến nay đều xem xét trên mô hình mạng không dây nói chung [39,102–106,109–111,150,151], chỉ có bài báo [55] là công trình duy nhất xem xét vấn đề này trên mạng NOMA. Trong nghiên cứu này, các tác giả đã xem xét vấn đề chủ động nghe lén thông tin trên hệ thống truyền tin bất hợp pháp sử

dụng NOMA cho đường truyền xuống từ trạm cơ sở đến các nhóm người dùng cuối. Tuy nhiên, trong nghiên cứu [55] chưa xem xét đến trường hợp trạng thái kênh truyền gây nhiễu từ thiết bị giám sát đến máy phát bất hợp pháp là xác định và cũng chưa xem xét trường hợp NOMA đường truyền lên.

Trong khi đó, các nghiên cứu về bảo mật tầng vật lý trong mạng SISO NOMA [53, 63, 70, 77, 85], đều xem xét trường hợp thiết bị nghe lén có khả năng giải mã bằng SIC mà chưa có nghiên cứu nào xem xét trường hợp thiết bị nghe lén sử dụng PIC để giải mã và so sánh hiệu năng bảo mật của hệ thống trong hai kịch bản này. Một hạn chế nữa là các nghiên cứu này chỉ phân tích, đánh giá hiệu năng bảo mật hệ thống và bỏ qua hiệu năng bảo mật của từng người dùng trong hệ thống.

Đối với các nghiên cứu về hiệu năng bảo mật mạng SISO NOMA nhận thức hầu hết tập trung theo hướng đề xuất giải pháp nâng cao hiệu năng bảo mật [147, 148, 157, 158], vấn đề đánh giá mối tương quan giữa bảo mật và độ tin cậy của hệ thống chưa được xem xét. Cho đến nay, có duy nhất bài báo [156] khảo sát mối quan hệ giữa bảo mật và độ tin cậy mạng NOMA cộng tác trong môi trường vô tuyến nhận thức dạng nền, tuy nhiên nghiên cứu này còn vấn đề tồn tại đó là bỏ qua điều kiện ràng buộc về mức can nhiễu và công suất phát mức đỉnh của mạng thứ cấp, làm cho bài toán cải thiện hiệu năng chỉ phù hợp với vùng tỷ lệ tín hiệu trên nhiễu nhỏ và do đó có phần khó khả thi khi áp dụng thực tế.

1.8 Đề xuất hướng nghiên cứu của luận án

Xuất phát từ việc khảo sát và phân tích những tồn tại trong nghiên cứu liên quan, nghiên cứu sinh đề xuất hướng nghiên cứu của luận án là đề xuất mô hình mạng NOMA, đánh giá hiệu năng bảo mật tầng vật lý, phân tích các yếu tố ảnh hưởng đến hiệu năng bảo mật hệ thống từ đó làm cơ sở đề xuất giải pháp cải thiện hiệu năng bảo mật tầng vật lý trong mạng NOMA, cụ thể như sau:

- Làm rõ các khái niệm liên quan đến luận án như: cơ sở lý thuyết bảo mật tầng vật lý, mạng NOMA, mạng NOMA nhận thức, truyền thông cộng tác, các phép đo hiệu năng bảo mật.

- Nghiên cứu, đánh giá và đề xuất cơ chế đối phó chủ động với hình thức tấn

công hợp tác để cải thiện hiệu năng bảo mật mô hình mạng NOMA cộng tác trên kênh $\alpha - \mu$ fading, phân tích các yếu tố ảnh hưởng đến hiệu năng bảo mật hệ thống như công suất gây nhiễu, độ lợi kênh truyền, số lượng ăng ten của thiết bị chuyển tiếp.

- Đề xuất mô hình, nghiên cứu, đánh giá hiệu năng bảo mật mạng NOMA có chiến lược chủ động nghe lén, đề xuất chính sách điều khiển công suất phát gây nhiễu dưới ràng buộc công suất phát mức đỉnh và hiệu suất hoạt động của hệ thống để nâng cao hiệu năng bảo mật hệ thống các kịch bản khác nhau về trạng thái kênh truyền.

- Nghiên cứu, so sánh và phân tích hiệu năng bảo mật mạng SISO NOMA trong các trường hợp thiết bị nghe lén sử dụng kỹ thuật loại bỏ nhiễu SIC, PIC, thiết bị nghe lén được trang bị một và nhiều ăng-ten. Đánh giá hiệu suất hệ thống dựa trên phép đo thời gian truyền tin trung bình, chính sách phân bổ công suất.

- Nghiên cứu, khảo sát sự đánh đổi giữa bảo mật và độ tin cậy, xây dựng chính sách điều khiển công suất phát gây nhiễu mô hình mạng NOMA trong môi trường vô tuyến nhận thức dạng nền dưới ràng buộc mức can nhiễu của mạng sơ cấp và công suất phát mức đỉnh của mạng thứ cấp.

1.9 Kết luận

Chương 1 đã trình bày những vấn đề cơ bản về kênh truyền không dây, mạng NOMA, bảo mật thông tin tầng vật lý trong mạng NOMA và khảo sát các công trình đã được công bố liên quan trực tiếp đến hướng nghiên cứu của luận án, phân tích những tồn tại và đề xuất hướng nghiên cứu của luận án. Những vấn đề, nội dung đã được trình bày trong chương này sẽ làm cơ sở để nghiên cứu sinh giải quyết các nội dung đặt ra trong các chương kế tiếp của luận án.

Chương 2

ĐÁNH GIÁ HIỆU NĂNG BẢO MẬT MẠNG NOMA CỘNG TÁC CÓ CHIẾN LƯỢC ĐỐI PHÓ CHỦ ĐỘNG VỚI HÌNH THỨC TẤN CÔNG HỢP TÁC

2.1 Giới thiệu

Truyền thông cộng tác được sử dụng như là một giải pháp hiệu quả trong mạng NOMA để cải thiện độ tin cậy trong truyền tin và mở rộng phạm vi phủ sóng, ví dụ [36, 50, 124]. Mặc dù mạng NOMA cộng tác có thể cải thiện độ tin cậy trong truyền thông nhưng vấn đề an toàn, bảo mật thông tin lại là một trong những thách thức lớn do thông tin truyền đi được lặp lại qua nhiều chặng nên dễ bị tấn công nghe lén. Cho đến nay, để giải quyết vấn đề này, một số nghiên cứu đã tập trung vào chiến lược thiết kế các mạng NOMA cộng tác sử dụng kỹ thuật gây nhiễu như đã trình bày tại mục 1.7.1. Tuy nhiên, các nghiên cứu này mới chỉ xem xét trường hợp mô hình hệ thống có một thiết bị nghe lén độc lập hoặc có nhiều thiết bị nghe lén kết hợp với nhau để thu thập thông tin, chưa có nghiên cứu nào xem xét trường hợp Eve cộng tác với thiết bị gây nhiễu lên máy thu buộc máy phát phải tăng công suất phát từ đó làm tăng khả năng thu thập thông tin của thiết bị nghe lén. Ngoài ra, trong trường hợp hệ thống bị hợp tác tấn công nghe lén như vậy, về mặt thiết kế hệ thống cần phải có chiến lược để chủ động đối phó. Hơn nữa, chưa có tài liệu nào xem xét mô hình mạng NOMA cộng tác trên kênh truyền $\alpha - \mu$, đây là một mô hình kênh truyền fading tổng quát, các phân bố mũ, Rayleigh...chỉ là những trường hợp cụ thể.

Xuất phát từ những vấn đề trên, trong chương này, luận án đề xuất mô hình mạng NOMA cộng tác có chiến lược đối phó chủ động với hình thức tấn công hợp tác trên kênh fading theo phân bố $\alpha - \mu$. Luận án đánh giá hiệu năng bảo

mật trong kịch bản hệ thống không có chiến lược đối phó chủ động với hình thức tấn công hợp tác. Tiếp theo, luận án đề xuất cơ chế đối phó chủ động trên hệ thống để chống lại hình thức tấn công cộng tác và so sánh khả năng bảo mật của hệ thống trong trường hợp có chiến lược đối phó chủ động với trường hợp không có chiến lược đối phó chủ động. Cuối cùng, luận án phân tích tác động của các yếu tố như số lượng ăng-ten của thiết bị chuyển tiếp, công suất gây nhiễu, độ lợi kênh tryền lên hiệu năng bảo mật của hệ thống.

Phần còn lại của chương này được tổ chức như sau: Phần 2.2 mô tả mô hình đề xuất, trong đó mô tả kịch bản hệ thống không có chiến lược đối phó chủ động và kịch bản hệ thống có chiếu lược đối phó chủ động; Phần 2.3 phân tích hiệu suất bảo mật thông qua phép đo xác suất dừng bảo mật; Phần 2.4 mô phỏng bằng phương pháp Monte Carlo và đánh giá kết quả; Phần 2.5 kết luận nội dung của chương.

Nội dung của chương này được trình bày trên cơ sở các kết quả công trình $A1$ đã được công bố tại hội thảo khoa học *2019 International Conference On Advanced Technologies For Communications (ATC 2019)*.

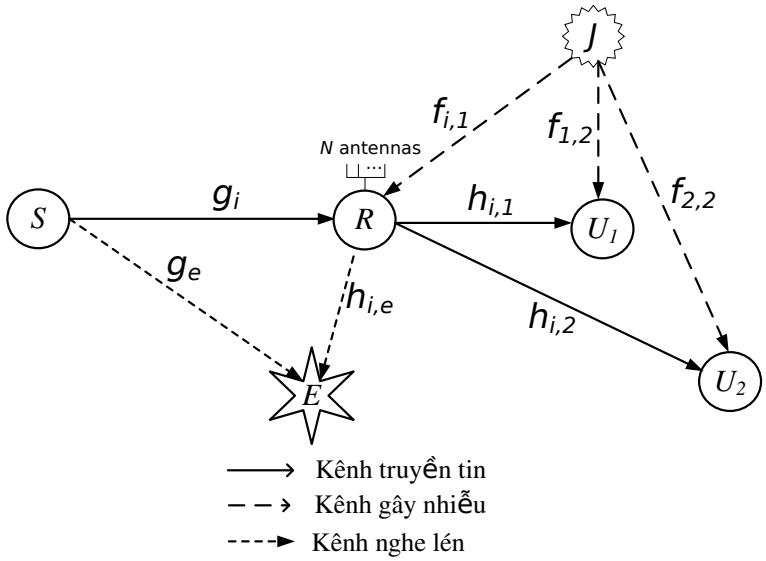
2.2 Mô hình hệ thống

Luận án khảo sát một mô hình mạng NOMA cộng tác, bao gồm một máy phát tin S, một thiết bị chuyển tiếp R, và hai người dùng cuối U_1 và U_2. U_1 được giả thiết gần R hơn U_2. Nguồn S truyền tín hiệu đồng thời đến cả U_1 và U_2 với sự hỗ trợ của thiết bị chuyển tiếp R sử dụng giao thức giải mã và chuyển tiếp, có hai thiết bị hoạt động bất hợp pháp (một thiết bị gây nhiễu J và một thiết bị nghe lén E). Giải thiết rằng S, U_1, U_2, và E được trang bị đơn ăng-ten, thiết bị chuyển tiếp R được trang bị N ăng-ten.

Ở đây, thiết bị nghe lén E hợp tác với thiết bị gây nhiễu J nhằm thu thập thông tin mật truyền từ nguồn tới đích. Cụ thể, E hoạt động ở chế độ thụ động để nghe lén, trong khi đó thiết bị gây nhiễu J phát ra các tín hiệu nhiễu lên máy phát S và thiết bị chuyển tiếp R. Kết quả là máy phát và thiết bị chuyển tiếp buộc phải tăng công suất truyền tin để đảm bảo hiệu suất truyền tin, tận dụng cơ hội này E dễ dàng cải thiện chất lượng tín hiệu mà nó nghe lén được.

Trong mô hình này giả định rằng do các hiệu ứng fading nên không tồn tại

kênh truyền trực tiếp giữa máy phát và đích. Thiết bị chuyển tiếp đóng vai trò mở rộng phạm vi truyền tín hiệu. Giả thiết rằng tất cả các kênh truyền fading phân bổ theo phân phối $\alpha - \mu$.



Hình 2.1: *Mô hình mạng NOMA cộng tác không sử dụng chiến lược đối phó chủ động với hình thức tấn công hợp tác.*

Tiếp theo, tác giả mô tả giao thức hoạt động của mô hình hệ thống trong hai trường hợp: Trường hợp thứ nhất, hệ thống không có cơ chế đối phó chủ động (Non Protection Scheme); Trường hợp thứ hai hệ thống có cơ chế đối phó chủ động (Active Protection Scheme). Hiệu năng bảo mật của hệ thống sẽ được đánh giá và so sánh giữa hai trường hợp nêu trên.

2.2.1 Kịch bản hệ thống không có chiến lược đối phó chủ động

Trong phần này, tác giả xem xét hệ thống trong kịch bản hệ thống không có cơ chế đối phó chủ động NPS như minh họa trong hình 2.1, trong đó cả máy phát S và thiết bị chuyển tiếp R không có bất kỳ chiến lược nào để bảo mật kênh truyền. Do đó, nếu J phát tín hiệu gây giảm hiệu suất của hệ thống thì S và R sẽ tăng công suất truyền ngay lập tức để duy trì chất lượng dịch vụ mà không hề biết có sự tồn tại của nút nghe lén E.

Quá trình truyền tin trên hệ thống được chia thành hai pha: Pha thứ nhất máy phát S truyền tin cho thiết bị chuyển tiếp R, pha thứ hai thiết bị chuyển tiếp giải mã và chuyển tiếp bản tin cho người dùng U_1 và U_2. Tại pha thứ nhất, S gửi

tín hiệu kết hợp $\sqrt{\alpha_1 P_s}s_1 + \sqrt{\alpha_2 P_s}s_2$ tới R, trong đó α_1, α_2 là hệ số phân bổ công suất, s_1 và s_2 là tín hiệu của U_1 và U_2 tương ứng. Lưu ý rằng hệ số phân bổ công suất thỏa mãn điều kiện $\alpha_2 \geq \alpha_1$ và $\alpha_1 + \alpha_2 = 1$ [47]. Tín hiệu thu được ở nhánh ăng-ten thứ i của R, $1 \leq i \leq N$ được biểu diễn bởi công thức sau

$$y_i^r = \sqrt{\alpha_1 P_s}s_1 g_i + \sqrt{\alpha_2 P_s}s_2 g_i + \omega_i^r, \tag{2.1}$$

trong đó P_s là công suất truyền tin của S, g_i là hệ số kênh truyền giữa R và nhánh ăng-ten thứ i của R và ω_i^r là công suất nhiễu AWGN với giá trị trung bình bằng không và phương sai bằng σ_i^2, nghĩa là $\omega_i^r \sim \mathcal{CN}(0, \sigma_i^2)$. Do nút nghe lén E giả thiết nằm trong vùng bao phủ của máy phát nên E có thể nghe lén được tín hiệu kết hợp truyền từ S với giá trị như sau

$$y_e^{(1)} = \sqrt{\alpha_1 P_s}s_1 g_e + \sqrt{\alpha_2 P_s}s_2 g_e + \omega_e, \tag{2.2}$$

trong đó g_e hệ số kênh truyền từ S tới E và ω_e công suất nhiễu AWGN tại E, ω_e có giá trị trung bình và phương sai như sau $\omega_e \sim \mathcal{CN}(0, \sigma_e^2)$. S phân bổ mức công suất cho U_2 lớn hơn so với U_1 do đó tại nhánh ăng-ten thứ i, R giải mã s_2 trước và coi s_1 là tín hiệu nhiễu, và sau đó giải mã tín hiệu s_1 bằng kỹ thuật SIC [48]. Kết quả chúng ta có biểu thức tỉ số tín hiệu trên nhiễu và tạp âm để giải mã tín hiệu s_1 và s_2 trên nhánh ăng-ten thứ i tại R dưới tác động của tín hiệu nhiễu gây ra bởi J như sau

$$\gamma_{i,r}^{s_1} = \frac{\alpha_1 P_s |g_i|^2}{P_j |f_{i,1}|^2 + \sigma_r^2}, \tag{2.3}$$

$$\gamma_{i,r}^{s_2} = \frac{\alpha_2 P_s |g_i|^2}{P_j |f_{i,1}|^2 + \alpha_1 P_s |g_i|^2 + \sigma_r^2}, \tag{2.4}$$

trong đó P_j là công suất gây nhiễu của J và $f_{i,1}$ hệ số kênh truyền giữa J và ăng-ten thứ i của R.

R sử dụng kỹ thuật kết hợp lựa chọn để xử lý tín hiệu nhận được. Hơn nữa để nâng cao hiệu năng bảo mật khi truyền tin, thiết bị chuyển tiếp R sẽ chọn ăng-ten có tỉ số SINR của s_2 là lớn nhất, tức ăng-ten có chỉ số như sau

$$i^* = \arg \max_{i \in \{1,2,\ldots,N_p\}} \{\gamma_{i,r}^{s_2}\}. \tag{2.5}$$

Do đó, tỉ số SINR để giải mã tín hiệu s_1 và s_2 tại R được tính toán theo biểu thức sau

$$\gamma_r^{s_1} = \frac{\alpha_1 P_s |g_{i^*}|^2}{P_j |f_{i^*,1}|^2 + \sigma_r^2}, \tag{2.6}$$

$$\gamma_r^{s_2} = \frac{\alpha_2 P_s |g_{i^*}|^2}{P_j |f_{i^*,1}|^2 + \alpha_1 P_s |g_{i^*}|^2 + \sigma_r^2}. \tag{2.7}$$

Lưu ý rằng J cộng tác với E để nghe lén tín hiệu vì vậy tại E sẽ sử dụng kỹ thuật để loại bỏ tín hiệu gây nhiễu từ J một cách hiệu quả [45]. Chính vì vậy, biểu thức tỉ số SNR và SINR để giải mã s_1 và s_2 tại E có dạng như sau

$$\gamma_{s_1,e}^{(1)} = \frac{\alpha_1 P_s |g_e|^2}{\sigma_e^2}, \tag{2.8}$$

$$\gamma_{s_2,e}^{(1)} = \frac{\alpha_2 P_s |g_e|^2}{\alpha_1 P_s |g_e|^2 + \sigma_e^2}. \tag{2.9}$$

Tại pha thứ hai: Thiết bị chuyển tiếp R giải mã và chuyển tiếp tín hiệu kết hợp tới U_1 và U_2. Do vậy tín hiệu nhận được tại U_k được biểu diễn như sau

$$y_k^d = \sqrt{\beta_1 P_r} s_1 h_{i,k} + \sqrt{\beta_2 P_r} s_2 h_{i,k} + \omega_k^d, \tag{2.10}$$

trong đó $k \in \{1, 2\}$, $h_{i,k}$ là hệ số kênh truyền từ ăng-ten thứ i của R tới U_k, P_r là công suất truyền tin của R, và ω_k^d là công suất nhiễu AWGN tại U_k, tức là $\omega_k^d \sim \mathcal{CN}(0, \sigma_d^2)$.

Ngoài ra, U_2 có vị trí xa R hơn so với U_1 nên độ lợi kênh truyền sẽ kém hơn. Vì vậy, để cải thiện hiệu suất bảo mật, ăng-ten nào có độ lợi kênh truyền đối với U_2 là tốt nhất sẽ được chọn trong số N ăng-ten của R, cụ thể ăng-ten có chỉ số thỏa mãn biểu thức sau

$$m^* = \arg \max_{i \in \{1,2,\ldots,N_p\}} \{h_{i,2}\}. \tag{2.11}$$

Do đó, biểu thức tỉ số SINR tại U_1 và U_2 như sau

$$\gamma_d^{s_1} = \frac{\beta_1 P_r |h_{m^*,1}|^2}{P_j |f_{1,2}|^2 + \sigma_d^2}, \tag{2.12}$$

$$\gamma_d^{s_2} = \frac{\beta_2 P_r |h_{m^*,2}|^2}{\beta_1 P_r |h_{m^*,2}|^2 + P_j |f_{2,2}|^2 + \sigma_d^2}. \tag{2.13}$$

Do đặc tính quảng bá của mạng không dây, E cũng nhận được tín hiệu kết hợp từ thiết bị chuyển tiếp và được tính theo công thức sau

$$y_e^{(2)} = \sqrt{\beta_1 P_r} s_1 h_{i,e} + \sqrt{\beta_2 P_r} s_2 h_{i,e} + \omega_e, \tag{2.14}$$

trong đó $h_{i,e}$ là hệ số kênh truyền từ ăng-ten i của R tới E. Vì vậy biểu thức tỉ số SNR và SINR để giải mã tín hiệu s_1 và s_2 tại E trong pha thứ hai được biểu diễn bởi công thức sau

$$\gamma_{s_1,e}^{(2)} = \frac{\beta_1 P_r |h_{m^*,e}|^2}{\sigma_e^2}, \tag{2.15}$$

$$\gamma_{s_2,e}^{(2)} = \frac{\beta_2 P_r |h_{m^*,e}|^2}{\beta_1 P_r |h_{m^*,e}|^2 + \sigma_e^2}. \tag{2.16}$$

Để nâng cao hiệu quả quá trình nghe lén, E được giả định sử dụng kỹ thuật SC để cải thiện chất lượng tín hiệu nhận được, điều này cũng giúp cho việc giải mã tín hiệu nghe lén được dễ dàng hơn. Vì vậy biểu thức tỉ số SNR và SINR tại E như sau

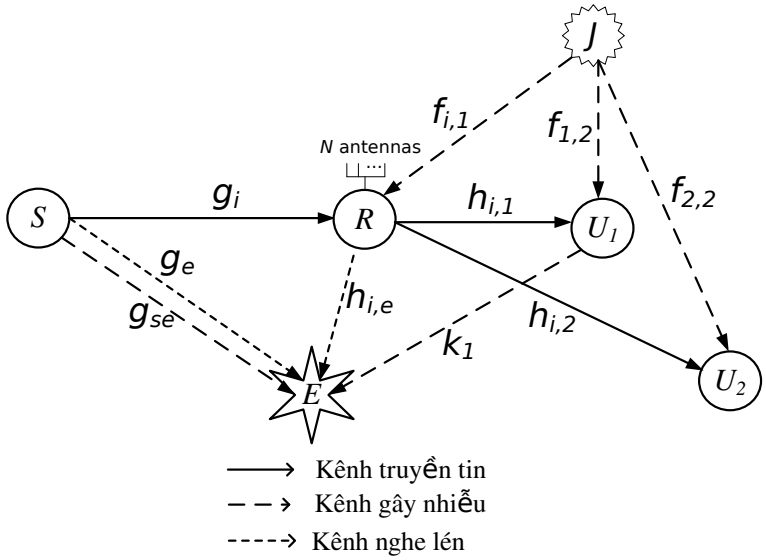
$$\gamma_e^{s_1} = \max\left\{\gamma_{s_1,e}^{(1)}, \gamma_{s_1,e}^{(2)}\right\}, \tag{2.17}$$

$$\gamma_e^{s_2} = \max\left\{\gamma_{s_2,e}^{(1)}, \gamma_{s_2,e}^{(2)}\right\}. \tag{2.18}$$

2.2.2 Kịch bản hệ thống có chiến lược đối phó chủ động

Trong phần này, để bảo mật kênh truyền từ máy phát S tới U_1 và U_2, tác giả đề xuất chiến lược đối phó chủ động được minh họa như trên hình 2.2, trong đó người dùng U_1 và S sẽ phát ra tín hiệu gây nhiễu tới E để làm giảm khả năng nghe lén tín hiệu. Quá trình truyền tin của hệ thống diễn ra trong hai pha như sau:

Pha thứ nhất, máy phát S truyền tin đến thiết bị chuyển tiếp R, trong lúc S truyền tin đến R thì U_1 hoạt động như là thiết bị gây nhiễu thân thiện bằng cách chủ động phát tín hiệu gây nhiễu tới E với công suất P_1. Do R cộng tác với U_1 vì vậy R có khả năng loại bỏ tín hiệu nhiễu phát ra từ U_1 [45]. R sử dụng kỹ thuật SC lựa chọn ăng-ten có tỉ số SINR tốt nhất trong số N ăng-ten của R và giải mã tín hiệu. Trong đó, SINR tại ăng-ten thứ i của R để giải mã tín hiệu s_1 và s_2 được mô tả trong công thức (2.6) và (2.7).



Hình 2.2: *Mô hình mạng NOMA cộng tác có sử dụng chiến lược đối phó chủ động với hình thức tấn công hợp tác.*

Mặt khác, E bị tác động bởi tín hiệu gây nhiễu từ U_1 nên tỉ số SINR của E để giải mã s_1 và s_2 dưới tác động của tín hiệu nhiễu được biểu diễn như sau

$$\gamma_{s_1,ej}^{(1)} = \frac{\alpha_1 P_s |g_e|^2}{P_1 |k_1|^2 + \sigma_e^2}, \tag{2.19}$$

$$\gamma_{s_2,ej}^{(1)} = \frac{\alpha_2 P_s |g_e|^2}{\alpha_1 P_s |g_e|^2 + P_1 |k_1|^2 + \sigma_e^2}, \tag{2.20}$$

trong đó k_1 là hệ số kênh truyền của kênh $U_1 \rightarrow E$.

Tại pha thứ hai, thiết bị chuyển tiếp truyền tín hiệu tới U_1 và U_2, trong lúc R giải mã và chuyển tiếp tín hiệu đến U_1 và U_2, S hoạt động như một thiết bị gây nhiễu thân thiện thứ hai bằng cách phát tín hiệu gây nhiễu với công suất P_{se} để làm giảm hiệu suất nghe lén của E. Tương tự như trong pha thứ nhất, U_1 và U_2 hợp tác với S nên chúng có khả năng loại bỏ tín hiệu gây nhiễu từ S. Hơn nữa, R chọn ăng-ten có tỉ số SINR tốt nhất trong số N ăng-ten để nâng cao hiệu năng bảo mật, trong đó biểu thức tỉ số SINR để giải mã tín hiệu s_1 và s_2 tại U_1 và U_2 được mô tả trong công thức (2.12) và (2.13). Tại E do chịu tác động bởi tín hiệu gây nhiễu phát ra từ S nên tỉ số SINR để giải mã tín hiệu s_1 và s_2 tại E trong pha thứ hai được biểu diễn bởi công thức sau

$$\gamma_{s_1,ej}^{(2)} = \frac{\beta_1 P_r |h_{m^*,e}|^2}{P_{se} |g_{se}|^2 + \sigma_e^2}, \tag{2.21}$$

$$\gamma_{s_2,ej}^{(2)} = \frac{\beta_2 P_r |h_{m^*,e}|^2}{\beta_1 P_r |h_{m^*,e}|^2 + P_{se}|g_{se}|^2 + \sigma_e^2}, \tag{2.22}$$

trong đó P_{se} và g_{se} lần lượt là công suất tín hiệu gây nhiễu của S tới E và hệ số kênh truyền của kênh gây nhiễu $S \to E$ trong pha truyền tin thứ hai.

Cuối cùng, chúng ta có biểu thức tỉ số SINR của tín hiệu s_1 và s_2 mà E nghe lén được như sau

$$\gamma_{ej}^{s_1} = \max\left\{\gamma_{s_1,ej}^{(1)}, \gamma_{s_1,ej}^{(2)}\right\}, \tag{2.23}$$

$$\gamma_{ej}^{s_2} = \max\left\{\gamma_{s_2,ej}^{(1)}, \gamma_{s_2,ej}^{(2)}\right\}. \tag{2.24}$$

2.3 Phân tích xác suất dừng bảo mật

Trong phần này, tác giả phân tích xác suất dừng bảo mật của hệ thống trong cả hai kịch bản. Kịch bản thứ nhất là hệ thống không có chiến lược đối phó tấn công hợp tác và kịch bản thứ hai là hệ thống có chiến lược chủ động đối phó tấn công hợp tác. Để đánh giá hiệu quả của chiến lược đối phó chủ động so kịch bản không có chiến lược đối phó chủ động, luận án so sánh xác suất dừng bảo mật của hệ thống trong hai kịch bản.

Xác suất dừng bảo mật xảy ra khi dung lượng bảo mật của kênh truyền từ S tới U_1 và U_2 nhỏ hơn ngưỡng tốc độ bảo mật [45], được thể hiện như sau

$$\mathcal{O}_{sec} = \Pr\{C_s < R\}, \tag{2.25}$$

trong đó C_S là dung lượng bảo mật và được định nghĩa là hiệu dung lượng kênh truyền hợp pháp và dung lượng kênh nghe lén, R là ngưỡng tốc độ bảo mật.

2.3.1 Xác suất dừng bảo mật trong kịch bản hệ thống không có chiến lược đối phó chủ động

Theo lý thuyết Shannon, dung lượng kênh hợp pháp để giải mã s_1 tại U_1 và dung lượng kênh nghe lén để giải mã s_1 tại E trong kịch bản hệ thống không có chiến lược đối phó chủ động tương ứng như sau

$$C_{NPS}^{1} = \frac{B}{2}\log_2\left(1 + \gamma^{s_1}\right), \tag{2.26}$$

$$C_{NPS}^{1,e} = \frac{B}{2}\log_2\left(1 + \gamma_e^{s_1}\right), \tag{2.27}$$

trong đó B là băng thông của hệ thống, $\gamma^{s_1} = \min\{\gamma_r^{s_1}, \gamma_d^{s_1}\}$, $\gamma_r^{s_1}$ và $\gamma_d^{s_1}$ được định nghĩa trong công thức (2.6) và (2.12) tương ứng, $\gamma_e^{s_1}$ được định nghĩa trong công thức (2.17).

Tương tự, dung lượng kênh hợp pháp để giải mã s_2 tại U_2 và dung lượng kênh nghe lén để giải mã s_2 tại E được biểu diễn bởi công thức sau

$$C_{NPS}^{2} = \frac{B}{2}\log_2\left(1+\gamma^{s_2}\right), \tag{2.28}$$

$$C_{NPS}^{2,e} = \frac{B}{2}\log_2\left(1+\gamma_e^{s_2}\right). \tag{2.29}$$

trong đó $\gamma^{s_2} = \min\{\gamma_r^{s_2}, \gamma_d^{s_2}\}$, $\gamma_r^{s_2}$, $\gamma_d^{s_2}$ được định nghĩa trong công thức (2.7), (2.13) tương ứng. $\gamma_e^{s_2}$ được định nghĩa trong công thức (2.18).

Do đó, dung lượng bảo mật kênh truyền từ S tới U_1 và U_2 lần lượt được biểu diễn như sau

$$C_s^{1,NPS} = \left\{C_{NPS}^{1} - C_{NPS}^{1,e}\right\}^{+}, \tag{2.30}$$

$$C_s^{2,NPS} = \left\{C_{NPS}^{2} - C_{NPS}^{2,e}\right\}^{+}, \tag{2.31}$$

trong đó $\{x\}^+ = \max\{x, 0\}$.

Hơn thế nữa, tín hiệu trên kênh truyền sẽ bị nghe lén nếu dung lượng bảo mật tức thời $C_s^{1,NPS}$ hoặc $C_s^{2,NPS}$ nằm dưới ngưỡng tốc độ bảo mật R_1, R_2 tương ứng. Nói cách khác xác suất dừng bảo mật trong kịch bản này được diễn tả như sau

$$\begin{aligned}
\mathcal{O}_{sec}^{NPS} &= \Pr\left\{C_s^{1,NPS} < R_1 \ \ or \ \ C_s^{2,NPS} < R_2\right\} \\
&= \Pr\left\{\frac{1+\gamma^{s_1}}{1+\gamma_e^{s_1}} < 2^{\frac{2R_1}{B}} \ \ or \ \ \frac{1+\gamma^{s_2}}{1+\gamma_e^{s_2}} < 2^{\frac{2R_2}{B}}\right\} \\
&= \Pr\left\{\gamma^{s_1} < \delta_1 + (\delta_1+1)\gamma_e^{s_1}\right. \\
&\qquad \left. or \ \ \gamma^{s_2} < \delta_2 + (\delta_2+1)\gamma_e^{s_2}\right\},
\end{aligned} \tag{2.32}$$

trong đó $\delta_1 = 2^{\frac{2R_1}{B}} - 1$ và $\delta_2 = 2^{\frac{2R_2}{B}} - 1$.

2.3.2 Xác suất dừng bảo mật trong kịch bản hệ thống có chiến lược đối phó chủ động

Trong kịch bản này, dung lượng bảo mật kênh hợp pháp tại U_1 và dung lượng kênh nghe lén tại E để giải mã s_1 trong kịch bản có chiến lược đối phó chủ động

được biểu diễn như sau

$$C_{APS}^{1} = \frac{B}{2}\log_2\left(1+\gamma^{s_1}\right), \tag{2.33}$$

$$C_{APS}^{1,ej} = \frac{B}{2}\log_2\left(1+\gamma_{ej}^{s_1}\right). \tag{2.34}$$

Tương tự, dung lượng kênh hợp pháp tại U_2 và dung lượng kênh nghe lén tại E để giải mã s_2 trong kịch bản này được biểu diễn bởi công thức sau

$$C_{APS}^{2} = \frac{B}{2}(\log_2\left(1+\gamma^{s_2}\right), \tag{2.35}$$

$$C_{APS}^{2,ej} = \frac{B}{2}\log_2\left(1+\gamma_{ej}^{s_2}\right). \tag{2.36}$$

Do đó, dung lượng bảo mật kênh truyền S tới U_1 và U_2 trong kịch bản này được tính bởi công thức sau

$$C_s^{1,APS} = \left\{C_{APS}^{1} - C_{APS}^{1,ej}\right\}^+, \tag{2.37}$$

$$C_s^{2,APS} = \left\{C_{APS}^{2} - C_{APS}^{2,ej}\right\}^+. \tag{2.38}$$

Cuối cùng, xác suất dừng bảo mật của hệ thống trong kịch bản có chiến lược đối phó chủ động được thể hiện như sau

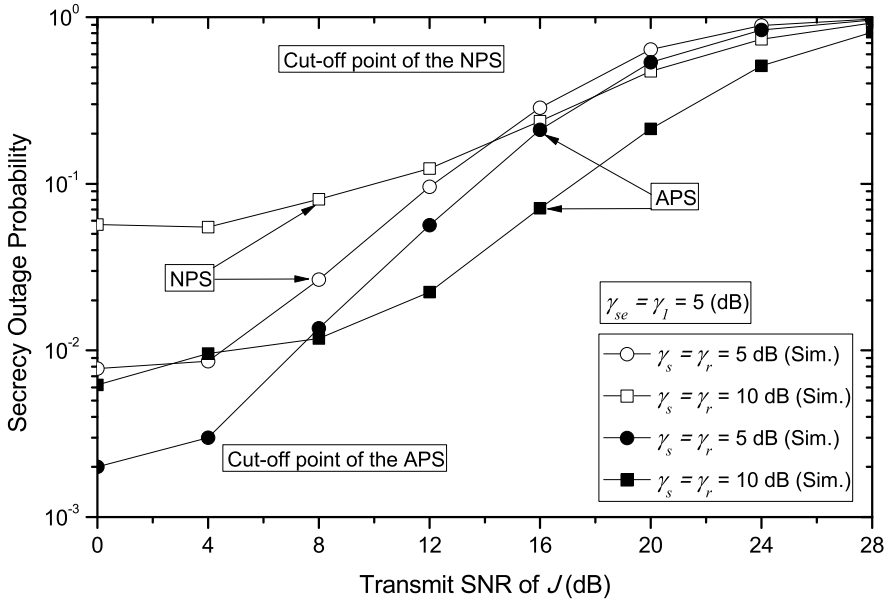
$$\begin{aligned}
\mathcal{O}_{sec}^{APS} &= \Pr\left\{C_s^{1,APS} < R_1 \ \ or \ \ C_s^{2,APS} < R_2\right\} \\
&= \Pr\left\{\frac{1+\gamma^{s_1}}{1+\gamma_{ej}^{s_1}} < 2^{\frac{2R_1}{B}} \ \ or \ \ \frac{1+\gamma^{s_2}}{1+\gamma_{ej}^{s_2}} < 2^{\frac{2R_2}{B}}\right\} \\
&= \Pr\left\{\gamma^{s_1} < \delta_1 + (\delta_1+1)\gamma_{ej}^{s_1}\right. \\
&\qquad \left. or \ \ \gamma^{s_2} < \delta_2 + (\delta_2+1)\gamma_{ej}^{s_2}\right\}.
\end{aligned} \tag{2.39}$$

Như chúng ta đã biết α-μ fading là một trong những kênh truyền phức tạp nhất, nó có thể mô tả các kênh truyền fading khác bằng cách thay đổi tham số α và μ. Do tính phức tạp của kênh truyền này nên việc tìm biểu thức dạng đóng cho công thức (2.32) và (2.39) là không khả thi cho hệ thống đang xem xét. Tuy nhiên, luận án sẽ thực hiện mô phỏng để đánh giá hiệu năng bảo mật của hệ thống trong kịch bản có chiến lược đối phó chủ động và so sánh với kịch bản không có chiến lược đối phó chủ động.

2.4 Mô phỏng và đánh giá kết quả

Trong phần này, luận án trình bày các số liệu thử nghiệm mô phỏng bằng phương pháp Monte Carlo để chỉ ra sự ảnh hưởng của các tham số lên xác suất dừng bảo mật của hệ thống. Ngoài ra, SOP trong kịch bản hệ thống không có chiến lược đối phó chủ động được so sánh với SOP trong kịch bản hệ thống có chiến lược đối phó chủ động. Trong kết quả mô phỏng này, luận án giả thiết rằng $\sigma_r^2 = \sigma_d^2 = \sigma_e^2 = N_0$ [124] và $\gamma_s = P_s/N_0, \gamma_{se} = P_{se}/N_0, \gamma_r = P_r/N_0, \gamma_j = P_j/N_0$, $\gamma_1 = P_1/N_0$ là tỉ số SNR của S, R, J, và U_1 tương ứng. Các tham số của hệ thống được thiết lập như sau

- Băng thông hệ thống $W = 5$ MHz
- Ngưỡng tốc độ bảo mật $R_1 = R_2 = 1$ kbps
- Số ăng-ten của thiết bị chuyển tiếp $N = 5$

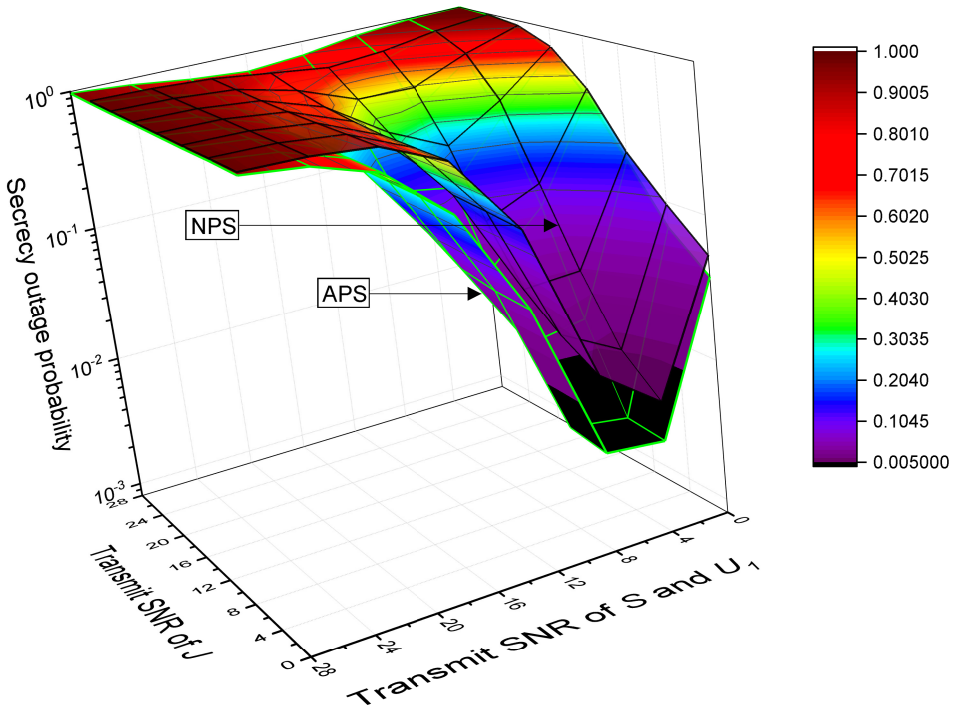


Hình 2.3: *Tác động của SNR tại J, S, và R lên SOP trong kịch bản NPS và APS với* $\alpha = 2$, $\mu = 1, \Omega_{g_i} = \Omega_{h_{i,1}} = \Omega_{h_{i,2}} = \Omega_{k_1} = 5$, *và* $\Omega_{g_e} = \Omega_{g_{s,e}} = \Omega_{h_{i,e}} = \Omega_{f_{i,1}} = \Omega_{f_{1,2}} = \Omega_{f_{2,2}} = 0.1$.

Hình 2.3 mô tả mức độ ảnh hưởng của công suất truyền SNR γ_j lên xác suất dừng bảo mật trong hai kịch bản hệ thống có chiến lược đối phó chủ động và kịch bản hệ thống không có chiến lược đối phó chủ động khi SNR γ_s và γ_r thay đổi. Chúng ta thấy rằng SOP trong kịch bản APS thấp hơn đáng kể so với kịch

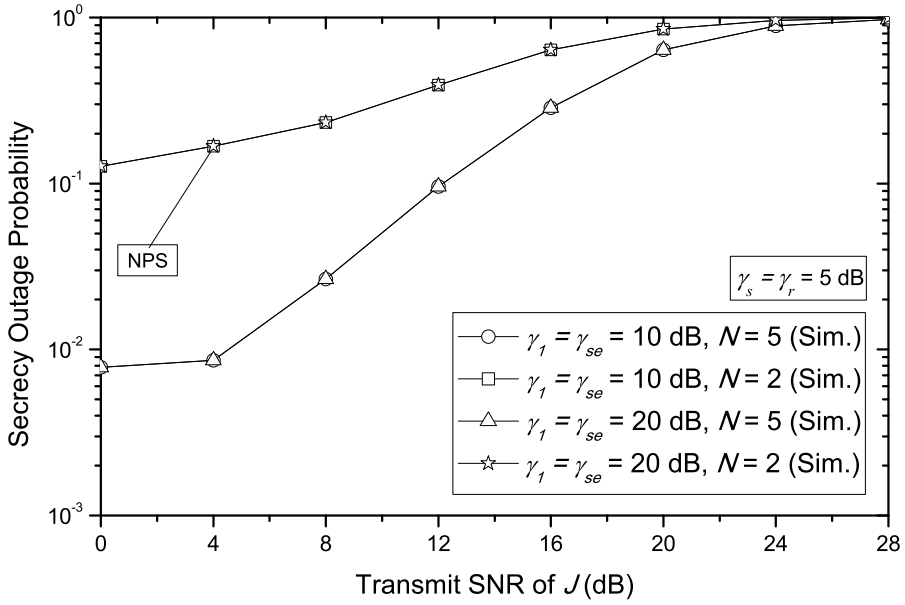
bản NPS trên toàn bộ miền giá trị SNR của thiết bị gây nhiễu. Điều này được giải thích như sau, S và U_1 được sử dụng như là thiết bị gây nhiễu thân thiện để làm suy giảm tín hiệu nghe lén tại E trong kịch bản APS. Hơn thế nữa, khi SNR của J giảm thì SOP của hệ thống trong cả hai kịch bản đều được cải thiện bởi vì SINR để giải mã các tín hiệu s_1 và s_2 tại R, U_1, U_2 chịu ảnh hưởng tiêu cực từ tín hiệu nhiễu gây ra bởi J.

Ngoài ra, SOP trong kịch bản APS với γ_s và γ_r ở mức cao, cụ thể $\gamma_s = \gamma_r = 10$ (dB) thì tốt hơn SOP so với γ_s và γ_r ở mức thấp hơn, cụ thể $\gamma_s = \gamma_r = 5$ (dB) khi γ_j lớn hơn điểm giao cắt (cut-off point) của APS và ngược lại. Trong kịch bản NPS cũng tương tự kịch bản APS, khi γ_j nằm trên điểm giao cắt của lược đồ NPS, tức là khi γ_s và γ_r ở mức cao thì SOP tốt hơn khi γ_s và γ_r ở mức thấp và ngược lại. Để quan sát được rõ hơn, tác giả vẽ thêm hình 2.4 để chỉ ra mức ảnh hưởng của γ_j, γ_s, và γ_r lên SOP.

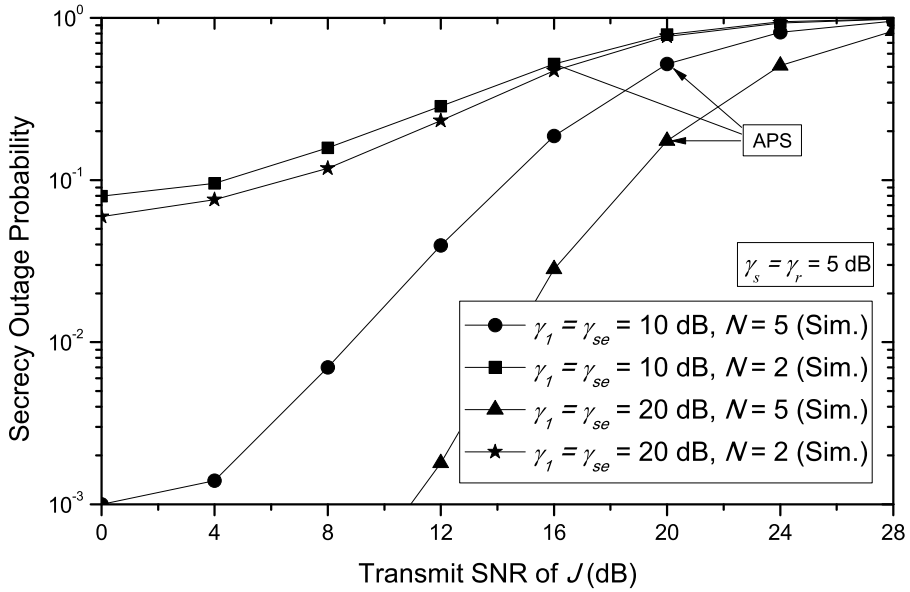


Hình 2.4: *Tác động của SNR tại J, S, và R lên SOP trong kịch bản NPS và APS với* $\alpha = 2$, $\mu = 1, \Omega_{g_i} = \Omega_{h_{i,1}} = \Omega_{h_{i,2}} = \Omega_{k_1} = 5$, *và* $\Omega_{g_e} = \Omega_{g_{s,e}} = \Omega_{h_{i,e}} = \Omega_{f_{i,1}} = \Omega_{f_{1,2}} = \Omega_{f_{2,2}} = 0.1$.

Hình 2.5 và 2.6 chỉ ra mức ảnh hưởng của số lượng ăng-ten của R và công suất truyền SNR tại J, S, và U_1 lên SOP hệ thống. Rõ ràng rằng công suất SNR của thiết bị gây nhiễu thân thiện S và U_1 khi tăng từ $\gamma_{se} = \gamma_1 = 10$ dB đến $\gamma_{se} = \gamma_1 = 20$



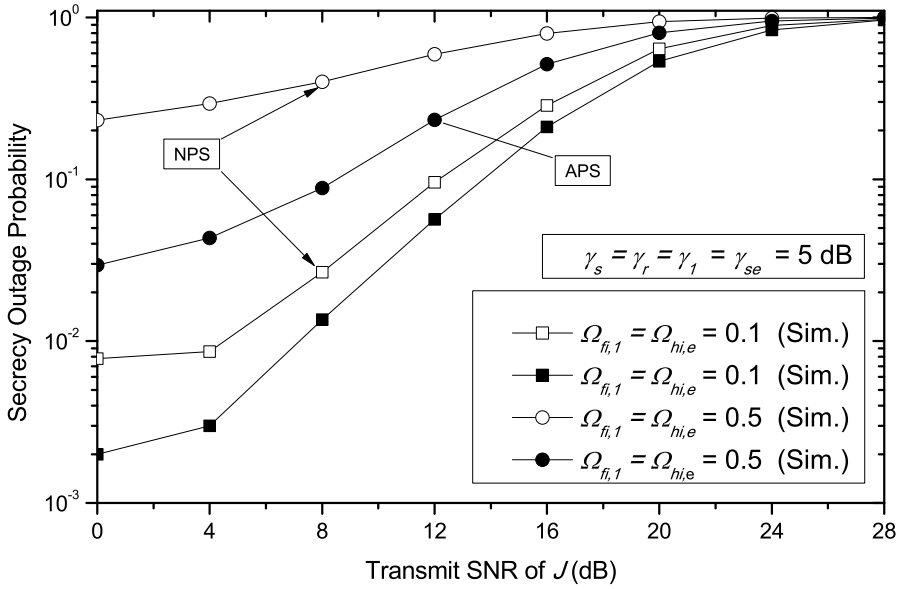
Hình 2.5: *Tác động của số lượng ăng-ten tại R và SNR tại J, S, và* U_1 *lên SOP trong kịch bản NPS với* $\alpha = 2$, $\mu = 1$, $\Omega_{g_i} = \Omega_{h_{i,1}} = \Omega_{h_{i,2}} = \Omega_{k_1} = 5$ *và* $\Omega_{g_e} = \Omega_{g_{se}} = \Omega_{h_{i,e}} = \Omega_{f_{1,2}} = \Omega_{f_{2,2}} = \Omega_{f_{i,1}} = 0.1$.



Hình 2.6: *Tác động của số lượng ăng-ten của R và SNR của J, S, và* U_1 *lên SOP trong kịch bản APS với* $\alpha = 2$, $\mu = 1$, $\Omega_{g_i} = \Omega_{h_{i,1}} = \Omega_{h_{i,2}} = \Omega_{k_1} = 5$ *và* $\Omega_{g_e} = \Omega_{g_{se}} = \Omega_{h_{i,e}} = \Omega_{f_{1,2}} = \Omega_{f_{2,2}} = \Omega_{f_{i,1}} = 0.1$.

dB, SOP trong kịch bản APS giảm đáng kể trong khi ở kịch bản NPS thì không thay đổi. Hiện tượng trên xảy ra bởi vì trong kịch bản NPS hệ thống không có bất kỳ chiến lược nào để bảo vệ hệ thống, ngược lại trong kịch bản APS hệ thống sử dụng S và U_1 như là hai thiết bị gây nhiễu thân thiện để làm suy yếu tín hiệu

nghe lén tại E. Hơn nữa, SOP của hệ thống trong cả hai kịch bản được cải thiện khi số lượng ăng-ten của thiết bị chuyển tiếp tăng lên. Nguyên nhân là do khi số lượng ăng-ten tăng lên thì độ lợi phân tập (diversity gain) tại R cũng tăng lên.



Hình 2.7: *Tác động của độ lợi kênh truyền $J \rightarrow R$ và $R \rightarrow E$ lên SOP trong kịch bản NPS và APS với $\alpha = 2, \mu = 1, \Omega_{g_i} = \Omega_{h_{i,1}} = \Omega_{h_{i,2}} = \Omega_{k_1} = 5$ và $\Omega_{g_e} = \Omega_{g_{s,e}} = \Omega_{f_{1,2}} = \Omega_{f_{2,2}} = 0.1$.*

Hình 2.7 phân tích ảnh hưởng của độ lợi kênh truyền trung bình $\Omega_{f_{i,1}}$ và $\Omega_{h_{i,e}}$ của kênh $J \rightarrow R$ và $R \rightarrow E$ lên hiệu năng bảo mật của hệ thống. Chúng ta quan sát thấy rằng SOP tăng nhanh khi kênh truyền bất hợp pháp từ J và E trở lên mạnh hơn. Điều này được giải thích như sau nếu kênh truyền $J \rightarrow R$ càng tốt thì tín hiệu gây nhiễu tại R càng mạnh, ngược lại, nếu điều kiện kênh truyền $R \rightarrow E$ càng tốt, thì E càng dễ thu thập thông tin. Từ phân tích trên, chúng ta đưa ra kết luận rằng hiệu năng bảo mật của hệ thống khi có chiến lược đối phó chủ động tốt hơn trong trường hợp hệ thống không có chiến lược đối phó chủ động.

2.5 Kết luận

Trong chương này, luận án đã nghiên cứu, đánh giá, đề xuất chiến lược nâng cao hiệu năng bảo mật mô hình mạng NOMA sử dụng kỹ thuật hợp tác truyền tin qua một thiết bị chuyển tiếp được trang bị nhiều ăng-ten và hoạt động theo cơ chế giải mã và chuyển tiếp tín hiệu dưới sự hiện diện của một thiết bị gây nhiễu hợp tác với một Eve để thực hiện tấn công hợp tác nhằm nghe lén thông tin. Luận

án đã xây dựng biểu thức tính xác suất dừng bảo mật trên kênh truyền fading tuân theo phân bố α-μ trong hai trường hợp. Trường hợp thứ nhất, hệ thống truyền thông tin nhưng không có chiến lược đối phó lại hình thức tấn công hợp tác của Eve. Trường hợp thứ hai, luận án đề xuất chiến lược đối phó chủ động để chống lại hình thức tấn công hợp tác của Eve. Sau đó thực hiện mô phỏng để so sánh xác suất dừng bảo mật của hệ thống trong kịch bản có chiến lược đối phó chủ động với kịch bản hệ thống không có chiến lược đối phó chủ động. Kết quả thu được cho thấy SOP trong kịch bản có chiến lược đối phó chủ động cải thiện đáng kể so với kịch bản hệ thống không có chiến lược đối phó chủ động. Ngoài ra, luận án đã đánh giá tác động của các tham số hệ thống như số lượng ăng-ten của thiết bị chuyển tiếp, độ lợi kênh truyền của kênh gẫy nhiễu và kênh nghe lén, công suất truyền SNR của máy phát, trạm chuyển tiếp, thiết bị gẫy nhiễu lên hiệu năng bảo mật của hệ thống.

Chương 3

ĐÁNH GIÁ HIỆU NĂNG BẢO MẬT MẠNG NOMA CÓ CHIẾN LƯỢC CHỦ ĐỘNG NGHE LÉN

3.1 Giới thiệu

Các hoạt động bất hợp pháp trên mạng ngày càng gia tăng và phức tạp, chủ động thu thập thông tin để kịp thời ngăn chặn các hoạt động bất hợp pháp đóng vai trò quan trọng để đảm bảo an toàn, an ninh cho hệ thống. Do tính quảng bá nên hệ thống mạng không dây rất dễ bị tấn công dưới hình thức nghe lén. Chính vì vậy, theo cách tiếp cận truyền thống, các nghiên cứu tập trung theo hướng đề xuất các giải pháp để chống lại kiểu tấn công bị nghe lén bất hợp pháp này [51,53,63,68,81,149]. Ngược lại, đối với các hệ thống theo dõi, giám sát lại cần thực hiện chiến lược chủ động nghe lén để thu thập, phân tích thông tin, đây là hoạt động nghe lén phục vụ cho mục đích hợp pháp. Trong số các bài báo nghiên cứu về vấn đề này như đã trình bày trong mục 1.7.2, ngoại trừ bài báo [55], đều xem xét vấn đề nghe lén trên hệ thống mạng không dây nói chung. Cho đến nay, bài báo [55] là bài công trình duy nhất nghiên cứu về vấn đề chủ động nghe lén trên mạng NOMA. Trong nghiên cứu này, các tác giả đã xem xét vấn đề chủ động nghe lén thông tin trên hệ thống truyền tin bất hợp pháp sử dụng NOMA cho đường truyền xuống từ trạm cơ sở đến các nhóm người dùng cuối. Sử dụng thuật toán lặp theo kinh nghiệm kết hợp với tối ưu công suất gây nhiễu và thứ tự giải mã tín hiệu tại thiết bị giám sát, bài báo đã chứng minh cải thiện được khả năng nghe lén thông tin với số lượng nhiều người dùng cuối bị nghe lén là nhiều nhất. Tuy nhiên, trong nghiên cứu [55] chưa xem xét đến trường hợp trạng thái kênh truyền gây nhiễu từ thiết bị giám sát đến máy phát bất hợp pháp là xác định và cũng chưa xem xét trường hợp NOMA đường truyền lên.

Xuất phát từ những hạn chế trên, trong chương này, luận án đề xuất mô hình mạng cộng tác có chiến lược chủ động nghe lén thông tin đường truyền lên trong mạng NOMA. Trong mô hình này, đối tượng bất hợp pháp sử dụng mạng NOMA để truyền tin từ các cặp người dùng cuối ($U_l^{(k)}$) về máy thu B, hệ thống giám sát hợp pháp sử dụng một thiết bị giám sát E vừa có khả năng sinh ra tín hiệu gây nhiễu tại máy thu bất hợp pháp B đồng thời giải mã và chuyển tiếp tín hiệu về thiết bị đích D, thiết bị đích D cũng có thể thu tín hiệu trực tiếp từ những người dùng cuối. Thiết bị giám sát E phát tín hiệu gây nhiễu phải điều chỉnh công suất gây nhiễu thỏa mãn ràng buộc không làm gián đoạn hoạt động của thiết bị bất hợp pháp. Chính sách điều khiển công suất của thiết bị giám sát E được nghiên cứu trong hai kịch bản. Kịch bản thứ nhất đó là trạng thái kênh truyền gây nhiễu từ E đến B là xác định và kịch bản thứ hai là CSI của kênh gây nhiễu từ E đến B không xác định. Tiếp theo, tác giả xây dựng biểu thức tính xác suất nghe lén hợp pháp thành công, đây là một phép đo để đánh giá khả năng thu thập thông tin của thiết bị hợp pháp từ các đối tượng bất hợp pháp, và sử dụng nó để đánh giá hiệu quả của hệ thống trong việc thu thập tín hiệu của người dùng cuối bất hợp pháp có tín hiệu mạnh nhất, yếu nhất. Cuối cùng, luận án cũng thực hiện mô phỏng Monte Carlo để kiểm chứng các biểu thức toán học được đưa ra.

Phần còn lại của chương này được tổ chức như sau: Phần 3.2 mô tả mô hình đề xuất; Phần 3.3 phân tích chính sách phân bổ công suất gây nhiễu trong hai trường hợp trạng thái kênh gây nhiễu là xác định và không xác định; Phần 3.4 phân tích hiệu suất bảo mật hệ thống dựa trên phép đo xác suất nghe lén hợp pháp thành công; Phần 3.5 mô phỏng bằng Monte Carlo và đánh giá kết quả; Phần 3.6 kết luận nội dung của chương.

Các nội dung trình bày ở chương này dựa trên các kết quả của công trình $A3$ đã được công bố trên tạp chí *IEEE Access*.

3.2 Mô hình hệ thống

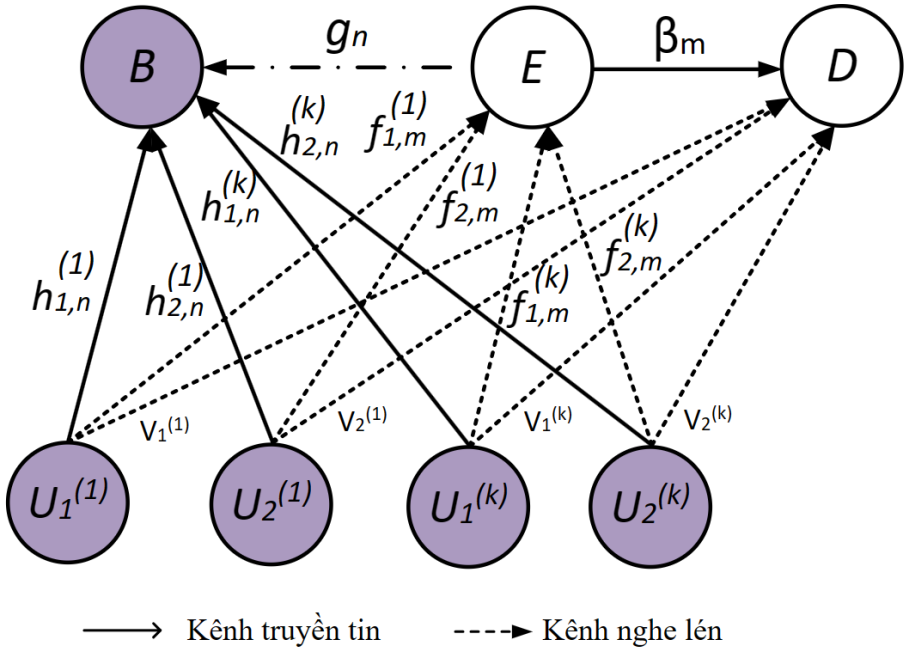
Luận án khảo sát một mô hình mạng NOMA như hình 3.1. Hệ thống bao gồm một máy thu sóng bất hợp pháp B được trang bị N ăng-ten, 2K thiết bị đầu cuối bất hợp pháp $U = \{U^{(1)}, ..., U^{(2K)}\}$. Các thiết bị đầu cuối được nghép lại thành từng đôi một ngẫu nhiên $U_l^{(k)}$, $l \in \{1, 2\}$ và $k \in \{1, 2, \ldots, K\}$, mỗi thiết bị được

trang bị một ăng-ten. Một thiết bị giám sát hợp pháp được trang bị $M+1$ ăng-ten và máy thu hợp pháp D được trang bị một ăng-ten. Mỗi cặp $U_l^{(k)}$ sử dụng kỹ thuật NOMA để truyền tín hiệu về máy thu sóng B và giả định $U_1^{(k)}$ gần B hơn so với $U_2^{(k)}$. Theo nguyên lý của mạng NOMA $U_2^{(k)}$ được cấp phát mức công suất lớn hơn $U_1^{(k)}$. Thiết bị giám sát E có khả năng sinh ra tín hiệu để gây nhiễu B trong lúc nghe lén tín hiệu từ các cặp $U_l^{(k)}$, đồng thời E nghe lén tín hiệu từ $U_l^{(k)}$ truyền đến B và thực hiện giải mã, sau đó chuyển tiếp tín hiệu về thiết bị nhận D. Ngoài ra, D có thể thu tín hiệu qua kênh truyền trực tiếp từ $U_l^{(k)}$ tới D. Trong trường hợp kênh truyền trực tiếp yếu thì D sẽ thu nhận tín hiệu từ E. Như vậy E hoạt động đồng thời vừa là thiết bị gây nhiễu vừa là thiết bị chuyển tiếp để cải thiện hiệu năng thu thập tín hiệu. Để mô hình hóa mô hình mạng này bằng toán học, độ lợi kênh truyền giữa $U_l^{(k)}$ và nhánh ăng-ten thứ n của B, giữa $U_l^{(k)}$ và nhánh ăng-ten thứ m của E và kênh truyền $U_l^{(k)} \rightarrow D$, $(n \in \{1,2,\ldots,N_e\}, m \in \{1,2,\ldots,N_p\})$ được ký hiệu lần lượt là $h_{l,n}^{(k)}$, $f_{l,m}^{(k)}$ và $v_l^{(k)}$. Ký hiệu g_n là độ lợi kênh truyền giữa nhánh ăng-ten thứ n của B và E, β_m là ký hiệu độ lợi kênh truyền giữa nhánh ăng-ten thứ m của E và D. Giả thiết mô hình mạng hoạt động trong môi trường có các vật cản dẫn đến tín hiệu gặp hiện tượng fading đang đường khi đến máy thu. Do đó tất cả các kênh truyền trong mô hình được giả thiết là kênh truyền fading có phân bố Rayleigh, khi đó độ lợi kênh truyền là các biến ngẫu nhiên độc lập được phân phối theo hàm mũ.

Trong mô hình hệ thống này, tác giả giả định rằng tất cả các ăng-ten của nút chuyển tiếp có thể giải mã được thông tin từ $U_l^{(k)}$ và một chiến lược chọn ăng-ten của nút chuyển tiếp được sử dụng để hỗ trợ truyền tin giữa nguồn và đích, nghĩa là kỹ thuật lựa chọn ăng-ten tốt nhất của nút chuyển tiếp được sử dụng cho việc giải mã và chuyển tiếp tín hiệu [1]. Ngoài ra, giả định rằng thông tin trạng thái của các kênh truyền đều được xác định tại E và D bằng những phương pháp đã có [39, 40].

Cặp người dùng cuối $U_l^{(k)}$ truyền tín hiệu về B, đây là tín hiệu kết hợp của $U_1^{(k)}$ và $U_2^{(k)}$. Đồng thời khi đó, thiết bị giám sát hợp pháp E sinh tín hiệu gây nhiễu s_J cho B với công suất P_J. Tín hiệu nhận được tại nhánh ăng-ten thứ n của B được thể hiện như sau

$$y_k^{(B)} = \sqrt{\alpha_1^{(k)} P_s} x_1^{(k)} h_{1,n}^{(k)} + \sqrt{(1-\alpha_1^{(k)}) P_s} x_2^{(k)} h_{2,n}^{(k)}$$



Hình 3.1: *Mô hình mạng NOMA có chiến lược chủ động nghe lén.*

$$+ \sqrt{P_J} s_J g_n + \sigma_B, \tag{3.1}$$

trong đó P_s là tổng công suất của cặp thiết bị $U_l^{(k)}$, $\alpha_1^{(k)}$ là hệ số phân bổ công suất cho thiết bị $U_1^{(k)}$ trong cặp thiết bị $U_l^{(k)}$ và $\sigma_B \sim \mathcal{CN}(0, N_0)$ là công suất nhiễu AWGN. Do thiết bị $U_1^{(k)}$ gần B hơn nên có chất lượng kênh truyền tốt hơn $U_2^{(k)}$. Tức là $U_2^{(k)}$ sẽ được phân bổ mức công suất lớn hơn $U_1^{(k)}$, nghĩa là $\alpha_1^{(k)} < 0.5$.

Theo nguyên lý đường truyền lên trong mạng NOMA, B đầu tiên giải mã tín hiệu của thiết bị có độ lợi kênh truyền lớn hơn là $U_1^{(k)}$ từ tín hiệu kết hợp nhận được và coi tín hiệu của thiết bị $U_2^{(k)}$ là nhiễu. Sau đó, B loại bỏ tín hiệu của $U_1^{(k)}$ bằng cách sử dụng kỹ thuật SIC và thực hiện giải mã tín hiệu của $U_2^{(k)}$ [41]. Kết quả là tỉ số SINR tức thời của $U_1^{(k)}$ và $U_2^{(k)}$ tại nhánh ăng-ten thứ n của B dưới tác động của tín hiệu gây nhiễu gây ra bởi E có công thức lần lượt là

$$\gamma_{1,n}^{(k,B)} = \frac{\alpha_1^{(k)} P_s h_{1,n}^{(k)}}{P_J g_n + (1 - \alpha_1^{(k)}) P_s h_{2,n}^{(k)} + N_0}, \tag{3.2}$$

$$\gamma_{2,n}^{(k,B)} = \frac{(1 - \alpha_1^{(k)}) P_s h_{2,n}^{(k)}}{P_J g_n + N_0}, \tag{3.3}$$

trong đó P_J là công suất gây nhiễu sinh ra bởi E.

B sử dụng kỹ thuật SC để lựa chọn ăng-ten có tín hiệu tốt nhất vì vậy SINR

của cặp $U_l^{(k)}$ tại B được tính như sau

$$\gamma_1^{(k,B)} = \max_{n\in\{1,2,\dots,N_e\}} \left\{\gamma_{1,n}^{(k,B)}\right\}, \tag{3.4}$$

$$\gamma_2^{(k,B)} = \max_{n\in\{1,2,\dots,N_e\}} \left\{\gamma_{2,n}^{(k,B)}\right\}. \tag{3.5}$$

Từ phương trình (3.4) và (3.5), tốc độ truyền tin từ $U_l^{(k)} \to B$ dưới tác động của tín hiệu gây nhiễu từ E có dạng sau

$$R_1^{(k,B)} = W \log_2\left(1+\gamma_1^{(k,B)}\right), \tag{3.6}$$

$$R_2^{(k,B)} = W \log_2\left(1+\gamma_2^{(k,B)}\right), \tag{3.7}$$

trong đó W là băng thông của hệ thống.

Mặt khác, do đặc tính quảng bá của kênh truyền không dây, E cũng thu nhận được tín hiệu mà cặp $U_l^{(k)}$ truyền tới E. Tín hiệu nhận được tại ăng-ten thứ m của E được biểu diễn là

$$y_k^{(E)} = \sqrt{\alpha_1^{(k)} P_s} x_1^{(k)} f_{1,m}^{(k)} + \sqrt{(1-\alpha_1^{(k)}) P_s} x_2^{(k)} f_{2,m}^{(k)} + \sigma_E, \tag{3.8}$$

$\sigma_E \sim \mathcal{CN}(0, N_0)$ là công suất nhiễu additive white Gaussian noise (AWGN) tại E.

Tương tự, giả thiết rằng kỹ thuật SIC cũng được áp dụng thành công tại E, tức là E sẽ giải mã tín hiệu $x_2^{(k)}$ của $U_2^{(k)}$ trước, sau đó nó tiếp tục dò tìm tín hiệu $x_1^{(k)}$ của $U_1^{(k)}$. Vì vậy, tỉ số SINR tức thời của cặp $U_l^{(k)}$ tại nhánh ăng-ten thứ m như sau

$$\gamma_{1,m}^{(k,E)} = \frac{\alpha_1^{(k)} P_s f_{1,m}^{(k)}}{(1-\alpha_1^{(k)}) P_s f_{2,m}^{(k)} + N_0}, \tag{3.9}$$

$$\gamma_{2,m}^{(k,E)} = \frac{(1-\alpha_1^{(k)}) P_s f_{2,m}^{(k)}}{N_0}. \tag{3.10}$$

E cũng sử dụng kỹ thuật SC để thu thập tín hiệu có chất lượng tốt nhất. Vì vậy, tỉ số SINR của cặp thiết bị $U_l^{(k)}$ tại E được tính như sau

$$\gamma_1^{(k,E)} = \max_{m\in\{1,2,\dots,N_p\}} \left\{\gamma_{1,m}^{(k,E)}\right\}, \tag{3.11}$$

$$\gamma_2^{(k,E)} = \max_{m\in\{1,2,\ldots,N_p\}} \left\{\gamma_{2,m}^{(k,E)}\right\}. \tag{3.12}$$

Trong pha thứ hai, E chuyển tiếp tín hiệu tới D qua ăng-ten có độ lợi kênh truyền tốt nhất. E hoạt động như một thiết bị để sinh tín hiệu gây nhiễu được nhận biết bởi D nhưng không bị phát hiện bởi các thiết bị bất hợp pháp. Vì vậy tín hiệu gây nhiễu được triệt tiêu tại D và chỉ gây hại cho các thiết bị bất hợp pháp. Tín hiệu thu thập được tại D như sau

$$\begin{aligned} y_k^{(D)} = &\sqrt{\delta_1^{(k)} P_e} x_1^{(k)} \beta_m^{(k)} + \sqrt{(1-\alpha_1^{(k)}) P_e} x_2^{(k)} \beta_m^{(k)} \\ &+ \sigma_D, \end{aligned} \tag{3.13}$$

trong đó $P_e \in [0, P_J^{max}]$ là công suất truyền mà E sử dụng để chuyển tiếp tín hiệu nghe lén được tới D, $\delta_1^{(k)}$ là hệ số phân bổ công suất và $\sigma_D \sim \mathcal{CN}(0, N_0)$ là công suất nhiễu AWGN.

D khi nhận được tín hiệu sẽ giải mã tín hiệu của $U_2^{(k)}$ trước tiên và coi tín hiêu của $U_1^{(k)}$ như là tín hiệu nhiễu. Kết quả ta có tỉ số SINR tức thời tại D được tính theo công thức sau

$$\gamma_{1,m}^{(k,D)} = \frac{\delta_1^{(k)} P_e \beta_m^{(k)}}{N_0}, \tag{3.14}$$

$$\gamma_{2,m}^{(k,D)} = \frac{(1-\delta_1^{(k)}) P_e \beta_m^{(k)}}{\delta_1^{(k)} P_e \beta_m^{(k)} + N_0}, \tag{3.15}$$

D cũng sử dụng kỹ thuật SC để cải thiện chất lượng tín hiệu thu được. Vì vậy, tỉ số SINR của cặp thiết bị $U_l^{(k)}$ tại D có dạng như sau

$$\gamma_1^{(k,D)} = \max_{m\in\{1,2,\ldots,N_p\}} \left\{\gamma_{1,m}^{(k,D)}\right\}, \tag{3.16}$$

$$\gamma_2^{(k,D)} = \max_{m\in\{1,2,\ldots,N_p\}} \left\{\gamma_{2,m}^{(k,D)}\right\}, \tag{3.17}$$

Dựa trên phương trình (3.11) và (3.16), tốc độ truyền dữ liệu thu được từ $U_1^{(k)}$ tại E và D như sau

$$R_1^{(k,E)} = \frac{1}{2} W \log_2\left(1+\gamma_1^{(k,E)}\right), \tag{3.18}$$

$$R_1^{(k,D)} = \frac{1}{2} W \log_2\left(1+\gamma_1^{(k,D)}\right). \tag{3.19}$$

Tiếp theo, kết hợp (3.12) và (3.17), tốc độ truyền dữ liệu thu được từ $U_2^{(k)}$ tại E và D như sau

$$R_2^{(k,E)} = \frac{1}{2} W \log_2 \left(1 + \gamma_2^{(k,E)}\right), \tag{3.20}$$

$$R_2^{(k,D)} = \frac{1}{2} W \log_2 \left(1 + \gamma_2^{(k,D)}\right). \tag{3.21}$$

Trên kênh truyền trực tiếp, D thu nhận tín hiệu trực tiếp từ $U_l^{(k)}$. Do đó, tỉ số SINR của kênh truyền $U_l^{(k)} \rightarrow D$ có dạng sau

$$\gamma_1^{(k,SD)} = \frac{\alpha_1^{(k)} P_s v_1^{(k)}}{(1-\alpha_1^{(k)}) P_s v_2^{(k)} + N_0}, \tag{3.22}$$

$$\gamma_2^{(k,SD)} = \frac{(1-\alpha_1^{(k)}) P_s v_2^{(k)}}{N_0}. \tag{3.23}$$

Từ (3.22) và (3.23), tốc độ truyền tin của kênh truyền $U_l^{(k)} \rightarrow D$ như sau

$$R_1^{(k,SD)} = W \log_2 \left(1 + \gamma_1^{(k,SD)}\right), \tag{3.24}$$

$$R_2^{(k,SD)} = W \log_2 \left(1 + \gamma_2^{(k,SD)}\right). \tag{3.25}$$

Kết hợp các phương trình (3.18), (3.19), (3.24), (3.25), (3.20) và (3.21), dung lượng kênh đầu cuối từ $U_l^{(k)}$ tới D thông qua kênh liên kết trực tiếp và gián tiếp như sau

$$R_{l,E2E}^{(k)} = \max \left\{ R_l^{(k,SD)}, \min \left\{ R_l^{(k,E)}, R_l^{(k,D)} \right\} \right\}. \tag{3.26}$$

3.3 Chính sách phân bổ công suất gây nhiễu

E phát tín hiệu gây nhiễu tại B với công suất P_J do đó sẽ làm suy giảm tốc độ giải mã tín hiệu từ $U_l^{(k)}$ truyền đến B, để đảm bảo chất lượng dịch vụ truyền tin, $U_l^{(k)}$ phản ứng lại ngay lập tức bằng cách tăng công suất truyền tin P_s mà không biết đến sự tồn tại của thiết bị gây nhiễu E . Trong trường hợp E gây nhiễu mạnh tại B có thể dẫn đến hệ quả $U_l^{(k)}$ không thể tăng thêm công suất truyền tin để duy trì hiệu suất hoạt động của hệ thống vì đã đạt đến công suất mức đỉnh, lúc đó $U_l^{(k)}$ sẽ dừng truyền tin và quá trình nghe lén hợp pháp sẽ bị thất bại.

Công suất truyền tin P_s của cặp thiết bị $U_l^{(k)}$ và công suất gây nhiễu P_J của E trong thực tế phải thỏa mãn ràng buộc nhỏ hơn hoặc bằng công suất tối đa hay còn gọi là công suất mức đỉnh được diễn tả như sau

$$0 \leq P_J \leq P_J^{max}, \tag{3.27}$$

$$0 \leq P_s \leq P_s^{max}. \tag{3.28}$$

Hơn nữa, E phải điều chỉnh công suất gây nhiễu để đảm bảo điều kiện xác suất dừng giải mã tín hiệu tại B không vượt quá ngưỡng xác suất dừng cho trước

$$\mathcal{O}_{out}^{(1)} = \Pr\left\{R_1^{(k,B)} \leq \gamma_{th}\right\} \leq \theta_{th}, \tag{3.29}$$

$$\mathcal{O}_{out}^{(2)} = \Pr\left\{R_2^{(k,B)} \leq \gamma_{th}\right\} \leq \theta_{th}, \tag{3.30}$$

trong đó $\mathcal{O}_{out}^{(1)}$, $\mathcal{O}_{out}^{(2)}$ là xác suất dừng của $U_1^{(k)}$ và $U_2^{(k)}$, γ_{th} và θ_{th} là ngưỡng tốc độ truyền tin và ngưỡng xác suất dừng hoạt động của B.

Từ phương trình (3.4) và (3.5), $\mathcal{O}_{out}^{(1)}$, $\mathcal{O}_{out}^{(2)}$ được viết lại như sau

$$\begin{aligned}\mathcal{O}_{out}^{(1)} &= \Pr\left\{\max_{n\in\{1,2,\ldots,N_e\}}\left\{\gamma_{1,n}^{(k,B)}\right\} \leq \phi_0\right\}, \\ &= \prod_{n=1}^{N}\Pr\left\{\frac{\alpha_1^{(k)}P_s h_{1,n}^{(k)}}{P_J g_n + (1-\alpha_1^{(k)})P_s h_{2,n}^{(k)} + N_0} \leq \phi_0\right\}.\end{aligned} \tag{3.31}$$

$$\begin{aligned}\mathcal{O}_{out}^{(2)} &= \Pr\left\{\max_{n\in\{1,2,\ldots,N_e\}}\left\{\frac{(1-\alpha_1^{(k)})P_s h_{2,n}^{(k)}}{P_J g_n + N_0}\right\} \leq \phi_0\right\}, \\ &= \prod_{n=1}^{N}\Pr\left\{\frac{(1-\alpha_1^{(k)})P_s h_{2,n}^{(k)}}{P_J g_n + N_0} < \phi_0\right\},\end{aligned} \tag{3.32}$$

với $\phi_0 = 2^{\frac{\gamma_{th}}{W}} - 1$.

Căn cứ vào thông tin trạng thái kênh truyền gây nhiễu từ E đến B, luận án xem xét chính sách phân bổ công suất gây nhiễu trong hai trường hợp sau:

3.3.1 Trạng thái kênh gây nhiễu là xác định

Trong trường hợp này, trạng thái kênh gây nhiễu là xác định tại E. Có nghĩa độ lợi kênh truyền g_n là xác định.

$$\mathcal{O}_{out}^{(1)} = \prod_{n=1}^{N} \int_{0}^{\infty} F_{h_{1,n}^{(k)}} \left(\frac{\phi_0(P_J g_n + N_0 + (1-\alpha_1^{(k)})P_s x)}{\alpha_1^{(k)} P_s} \right) \times f_{h_{2,n}^{(k)}}(x) dx. \tag{3.33}$$

Sử dụng phương trình (1.11) và (1.12), $f_{h_{2,n}^{(k)}}$ và $F_{h_{1,n}^{(k)}}$ được tính theo công thức sau

$$f_{h_{2,n}^{(k)}}(x) = \frac{1}{\Omega_{h_{2,n}^{(k)}}} \exp\left(-\frac{x}{\Omega_{h_{2,n}^{(k)}}} \right). \tag{3.34}$$

$$F_{h_{1,n}^{(k)}} = 1 - \exp\left\{ \frac{\phi_0(P_J g_n + N_0 + (1-\alpha_1^{(k)})P_s x)}{\alpha_1^{(k)} P_s \Omega_{h_{1,n}^{(k)}}} \right\}. \tag{3.35}$$

Thay thế (3.34) và (3.35) vào (3.33), chúng ta có kết quả sau

$$\mathcal{O}_{out}^{(1)} = \prod_{n=1}^{N} \left[1 - \frac{\alpha_1^{(k)} P_s \Omega_{h_{1,n}^{(k)}} \exp\left(-\frac{(N_0 + P_J g_n)\phi_0}{\alpha_1^{(k)} P_s \Omega_{h_{1,n}^{(k)}}} \right)}{(1-\alpha_1^{(k)}) P_s \phi_0 \Omega_{h_{2,n}^{(k)}} + \alpha_1^{(k)} P_s \Omega_{h_{1,n}^{(k)}}} \right]. \tag{3.36}$$

Giả thiết rằng tất cả các ăng-ten của trạm thu sóng B là gần nhau. Vì vậy, tất cả các nhánh ăng-ten có độ lợi kênh truyền là giống nhau, tức là $\Omega_{h_{1,n}^{(k)}} = \Omega_{h_1^{(k)}}$ và $\Omega_{h_{2,n}^{(k)}} = \Omega_{h_2^{(k)}}$ [42]. Cuối cùng, $\mathcal{O}_1$ được tính bởi công thức sau

$$\mathcal{O}_{out}^{(1)} = \left[1 - \frac{\alpha_1^{(k)} P_s \Omega_{h_1^{(k)}} \exp\left(-\frac{(N_0 + P_J g_n)\phi_0}{\alpha_1^{(k)} P_s \Omega_{h_1^{(k)}}} \right)}{(1-\alpha_1^{(k)}) P_s \phi_0 \Omega_{h_2^{(k)}} + \alpha_1^{(k)} P_s \Omega_{h_1^{(k)}}} \right]^N. \tag{3.37}$$

Thay thế công thức (3.37) vào (3.29) và thực hiện một số phép biến đổi toán học, chúng ta nhận được biểu thức công suất tín hiệu gây nhiễu như sau

$$P_J \leq P_{J_1}, \tag{3.38}$$

trong đó

$$P_{J_1} = \left\{ \frac{\ln(\tau)\alpha_1 P_s \Omega_{h_1^{(k)}} - N_0\phi_0}{\phi_0 g_n} \right\}^+, \tag{3.39}$$

$$\tau = \frac{\alpha_1^{(k)} P_s \Omega_{h_1^{(k)}}}{\left(1 - \sqrt[N]{\theta_{th}}\right)\left(\left(1-\alpha_1^{(k)}\right) P_s \phi_0 \Omega_{h_2^{(k)}} + \alpha_1 P_s \Omega_{h_1^{(k)}}\right)} \tag{3.40}$$

và $\{x\}^+ = \max\{x, 0\}$.

Trong khi $U_l^{(k)}$ có thể tăng công suất truyền tin của nó để đáp trả lại tín hiệu gây nhiễu và để đảm bảo hiệu suất hoạt động của B, E cũng đồng thời tăng công suất gây nhiễu P_J. Tuy nhiên, E phải dừng việc tăng công suất gây nhiễu khi $U_l^{(k)}$ đạt tới giá trị công suất mức đỉnh $P_s = P_s^{max}$. Do đó, công suất của tín hiệu gây nhiễu dưới ràng buộc xác suất dừng hoạt động của $U_1^{(k)}$ phải thỏa mãn điều kiện sau

$$P_J \leq \min\left\{P_{J_1}, P_J^{max}\right\}. \tag{3.41}$$

Tiếp theo, thực hiện tính toán biểu thức công suất gây nhiễu của E với điều kiện đảm bảo ràng buộc về xác suất dừng hoạt động của $U_2^{(k)}$. Áp dụng hàm phân bố mũ, công thức (3.32) được biến đổi về dạng sau

$$\begin{aligned}\mathcal{O}_{out}^{(2)} &= \prod_{n=1}^{N}\left[1 - \exp\left(-\frac{\phi_0(P_J g_n + N_0)}{(1-\alpha_1^{(k)})P_s\Omega_{h_{2,n}^{(k)}}}\right)\right], \\ &= \left[1 - \exp\left(-\frac{\phi_0(P_J g_n + N_0)}{(1-\alpha_1^{(k)})P_s\Omega_{h_2^{(k)}}}\right)\right]^N. \end{aligned} \tag{3.42}$$

Kết hợp công thức (3.30) và (3.42), chúng ta nhận được biểu thức về công suất gây nhiễu như sau

$$P_J \leq P_{J_2}, \tag{3.43}$$

với

$$P_{J_2} = \left\{ \frac{\ln\left(\frac{1}{1-\sqrt[N]{\theta_{th}}}\right)(1-\alpha_1^{(k)})P_s\Omega_{h_2^{(k)}} - \phi_0 N_0}{\phi_0 g_n} \right\}^+ \tag{3.44}$$

P_J là công suất gây nhiễu tương ứng với công suất truyền tin P_s. Mặc dù $U_l^{(k)}$ có thể tăng giảm công suất phát P_s tùy theo trạng thái kênh truyền và tín hiệu gây nhiễu tại B, nhưng nó không thể tăng công suất vượt quá giá trị công suất tối đa P_s^{max}. Ngoài ra, bên phải công thức (3.43) là một hàm tăng đơn điệu tương ứng với P_s. Vì vậy, miền giá trị công suất P_J dưới ràng buộc xác suất dừng hoạt động của $U_2^{(k)}$ và công suất gây nhiễu tối đa của E được xác định như sau

$$P_J \leq \min\left\{P_{J_2}, P_J^{max}\right\}. \tag{3.45}$$

Kết hợp công thức (3.27), (3.41) và (3.45), miền công suất của tín hiệu gây nhiễu trong trường hợp trạng thái kênh truyền gây nhiễu từ E tới B là xác định được mô tả bởi công thức sau

$$0 \leq P_J \leq \min\left\{\min\left\{P_{J_1}, P_{J_2}\right\}, P_J^{max}\right\}. \tag{3.46}$$

3.3.2 Trạng thái kênh gây nhiễu không xác định

Trong trường hợp này, độ lợi kênh truyền g_n là một biến ngẫu nhiên phân bố theo phân phối mũ với độ lợi kênh truyền trung bình là Ω_g. Để tìm biểu thức dạng đóng của $\mathcal{O}_{out}^{(1)}$ từ công thức (3.31), chúng ta có bổ đề sau.

Bổ đề 3.1. *Cho a,b, và c là các hằng số dương. Cho X, Y, và Z là các biến ngẫu nhiên độc lập và phân bố theo phấn phối mũ với giá trị trung bình Ω_X, Ω_Y, và Ω_Z tương ứng. Hàm phấn phối tích lũy của T được xác định bằng công thức* (3.48) *trong đó T được định nghĩa như trong công thức* (3.47)

$$T = \frac{aX}{bY + cZ + 1} \tag{3.47}$$

$$F_T(t) = 1 - \frac{\exp\left(\frac{-t}{a\Omega_X}\right)}{\Omega_X\Omega_Y\left(\frac{tb}{a\Omega_X + \frac{1}{\Omega_Y}}\right)\left(\frac{tc}{a\Omega_X + \frac{1}{\Omega_Z}}\right)}. \tag{3.48}$$

Chứng minh. Hàm CDF của T được định nghĩa như sau:

$$\begin{aligned} F_T(t) &= \Pr\left\{\frac{aX}{bY + cZ + 1} < t\right\} \\ &= \Pr\left\{X < \frac{t(bY + cZ + 1)}{a}\right\} \end{aligned}$$

$$= \int_0^\infty \int_0^\infty F_X\left(\frac{t(by+cz+1)}{a}\right) f_Y(y) f_Z(z) dydz, \tag{3.49}$$

trong đó $F_X(x)$ là hàm CDF và $f_Y(y), f_Z(z)$ là các hàm PDF theo phân bố mũ, do đó $F_T(t)$ được tính toán như sau

$$\begin{aligned} F_T(t) = \int_0^\infty \int_0^\infty & \left[1 - \exp\left(-\frac{t(by+cz+1)}{a\Omega_X}\right)\right] \\ & \times \frac{1}{\Omega_Y} \exp\left(\frac{-y}{\Omega_Y}\right) \frac{1}{\Omega_Z} \exp\left(-\frac{z}{\Omega_Z}\right) dydz, \end{aligned} \tag{3.50}$$

trong đó Ω_X,Ω_Y, Ω_Z là giá trị trung bình của các biến ngẫu nhiên X,Y,Z tương ứng. Thực hiện các phép tính, $F_T(t)$ có dạng như sau

$$\begin{aligned} F_T(t) &= \frac{1}{\Omega_Y}\frac{1}{\Omega_Z} \int_0^\infty \int_0^\infty \left(1 - \exp\left(-\frac{t(by+cz+1)}{a\Omega_X}\right)\right) \\ &\quad \times \exp\left(-\frac{y}{\Omega_Y}\right) \exp\left(-\frac{z}{\Omega_Z}\right) dy\, dz \\ &= \frac{1}{\Omega_Y\Omega_Z} \int_0^\infty \int_0^\infty \left[\exp\left(-\frac{y}{\Omega_Y}\right) - \exp\left(\left(-\frac{tb}{a\Omega_X} - \frac{1}{\Omega_Y}\right) y\right)\right] \\ &\quad \times \exp\left(-\frac{tc}{a\Omega_X} z\right) \exp\left(-\frac{z}{\Omega_Z}\right) dy\, dz \end{aligned} \tag{3.51}$$

Sau khi thực hiện các phép tính tích phân, ta nhận được công thức của $F_T(t)$ như sau

$$F_T(t) = 1 - \frac{\exp\left(\frac{-t}{a\Omega_X}\right)}{\Omega_Y\Omega_Z \left(\frac{tb}{a\Omega_X} + \frac{1}{\Omega_Y}\right)\left(\frac{tc}{a\Omega_X} + \frac{1}{\Omega_Z}\right)}. \tag{3.52}$$

□

Áp dụng công thức (3.48), xác suất dừng của $U_1^{(k)}$ được mô tả bởi công thức sau

$$\mathcal{O}_{out}^{(1)} = \prod_{n=1}^{N} \left(1 - \frac{\exp\left(\frac{-\phi_0 N_0}{\alpha_1^{(k)} P_s \Omega_{h_{1,n}^{(k)}}}\right)}{\Delta}\right),$$

$$= \left(1 - \frac{\exp\left(\frac{-\phi_0 N_0}{\alpha_1^{(k)} P_s \Omega_{h_1^{(k)}}} \right)}{\Delta} \right)^N . \tag{3.53}$$

với $\Delta = \frac{\Omega_{h_1^{(k)}} \Omega_{h_2^{(k)}} \Omega_g^2 \phi_0^2 P_J P_s (1-\alpha_1^{(k)})}{\left(\alpha_1^{(k)} P_s \Omega_{h_1^{(k)}} \Omega_g + N_0 \right) \left(\alpha_1^{(k)} P_s \Omega_{h_1^{(k)}} \Omega_{h_2^{(k)}} + N_0 \right)}$.

Thay công thức (3.53) vào (3.29) và thực hiện một số phép biến đổi toán học, chúng ta nhận được biểu thức cho công suất gây nhiễu của E dưới ràng buộc xác suất dừng hoạt động của $U_1^{(k)}$ như sau

$$P_J \leq \underbrace{\frac{\exp\left(-\frac{\phi_0 N_0}{\alpha_1^{(k)} P_s \Omega_{h_1^{(k)}}} \right)}{1 - \sqrt[N]{\theta_{th}}}}_{P_{J_1^*}} \pi_1, \tag{3.54}$$

với π_1 được định nghĩa như sau

$$\pi_1 = \frac{(\alpha_1^{(k)} P_s \Omega_{h_1^{(k)}} \Omega_g + N_0)(\alpha_1^{(k)} P_s \Omega_{h_1^{(k)}} \Omega_{h_2^{(k)}} + N_0)}{(1 - \alpha_1^{(k)}) P_s \Omega_{h_1^{(k)}} \Omega_{h_2^{(k)}} \Omega_g^2 \phi_0^2}, \tag{3.55}$$

Để duy trì hiệu suất hoạt động của $U_1^{(k)}$, E phải điều khiển công suất gây nhiễu thỏa mãn điều kiện sau

$$P_J \leq \min \left\{ P_{J_1^*}, P_J^{max} \right\}. \tag{3.56}$$

Tiếp theo, thực hiện tính toán xác suất dừng hoạt động của $U_2^{(k)}$, $\mathcal{O}_{out}^{(2)}$ được tính toán như sau

$$\mathcal{O}_{out}^{(2)} = \prod_{n=1}^{N} \left[1 - \frac{(1-\alpha_1^{(k)}) P_s \Omega_{h_{2,n}^{(k)}} \exp\left(\frac{-N_0 \phi_0}{(1-\alpha_1^{(k)}) P_s \Omega_{h_{2,n}^{(k)}}} \right)}{\phi_0 P_J \Omega_g + (1-\alpha_1^{(k)}) P_s \Omega_{h_{2,n}^{(k)}}} \right],$$

$$= \left[1 - \frac{(1-\alpha_1^{(k)}) P_s \Omega_{h_2^{(k)}} \exp\left(\frac{-N_0 \phi_0}{(1-\alpha_1^{(k)}) P_s \Omega_{h_2^{(k)}}} \right)}{\phi_0 P_J \Omega_{gn} + (1-\alpha_1^{(k)}) P_s \Omega_{h_2^{(k)}}} \right]^N . \tag{3.57}$$

Kết hợp công thức (3.27) và (3.57), chúng ta có biểu thức công suất gây nhiễu dưới điều kiện xác suất dừng hoạt động của $U_2^{(k)}$ là

$$P_J \leq \underbrace{\frac{(1-\alpha_k)P_s\Omega_{h_2^{(k)}}}{\phi_0\Omega_g}\pi_2}_{P_{J_2^*}}, \tag{3.58}$$

với π_2 được định nghĩa như sau

$$\pi_2 = \left\{ \frac{\exp\left(-\frac{N_0\phi_0}{(1-\alpha_1^{(k)})P_s\Omega_{h_2^{(k)}}}\right)}{1-\sqrt[N]{\theta_{th}}} - 1 \right\}^+. \tag{3.59}$$

Vế bên phải của công thức (3.58) là một hàm tăng đơn điệu theo P_s. Vì vậy, miền giá trị của công suất gây nhiễu P_J dưới ràng buộc xác suất dừng hoạt động của $U_2^{(k)}$ và công suất mức đỉnh của E được tính theo công thức sau

$$P_J \leq \min\left\{P_{J_2^*}, P_J^{max}\right\}. \tag{3.60}$$

Kết hợp công thức (3.27), (3.56) và (3.58), miền giá trị của công suất tín hiệu nhiễu của E trong trường hợp trạng thái kênh truyền không xác định như sau

$$0 \leq P_J \leq \min\left\{\min\left\{P_{J_1^*}, P_{J_2^*}\right\}, P_J^{max}\right\}. \tag{3.61}$$

3.4 Xác suất nghe lén hợp pháp thành công

Mục tiêu của các hệ thống giám sát là thu thập thông tin để phát hiện và ngăn chặn các hoạt động bất hợp pháp kịp thời. Trong phần này, luận án tính toán xác suất nghe lén hợp pháp thành công tại D. Quá trình nghe lén được gọi là thành công khi và chỉ khi tín hiệu nghe lén được giải mã thành công tại D với sự trợ giúp của E. E hoạt động như một thiết bị chuyển tiếp và đồng thời là thiết bị gây nhiễu để tăng hiệu suất quá trình nghe lén tại D.

Như đã giả thiết, $U_1^{(k)}$ gần B hơn nên có độ lợi kênh truyền tốt hơn $U_2^{(k)}$, do đó tỉ số SINR của $U_1^{(k)}$ tốt hơn $U_2^{(k)}$. Chính vì vậy luận án xem xét hai trường hợp là xác suất nghe lén thành công đối với người dùng cuối có tín hiệu mạnh nhất và người dùng cuối có tín hiệu yếu nhất.

3.4.1 Xác suất nghe lén hợp pháp thành công đối với thiết bị đầu cuối có tín hiệu mạnh nhất

Trong phần này luận án trình bày quá trình xây dựng biểu thức xác suất nghe lén hợp pháp thành công đối với $U_1^{(k)}$ có tín hiệu mạnh nhất trong số K cặp người dùng. Xác suất nghe lén hợp pháp thành công đối với người dùng có tín hiệu mạnh nhất được định nghĩa như sau

$$\mathcal{O}_{suc}^{(1)} = \Pr\left\{\max_{k\in\{1,2,\ldots,K\}}\left\{R_{1,E2E}^{(k)}\right\} \geq r_1\right\}, \tag{3.62}$$

với $R_{1,E2E}^{(k)}$ được định nghĩa tại công thức (3.26). Tiếp theo, $\mathcal{O}_{suc}^{(1)}$ được biến đổi như sau

$$\begin{aligned}\mathcal{O}_{suc}^{(1)} &= 1 - \prod_{k=1}^{K}\Pr\left\{\max\left\{R_1^{(k,SD)}, R_1^{min}\right\} \leq r_1\right\}, \\ &= 1 - \prod_{k=1}^{K} P_1 P_2,\end{aligned} \tag{3.63}$$

với $R_1^{min} = \min\left\{R_1^{(k,E)}, R_1^{(k,D)}\right\}$. P_1 và P_2 được diễn tả tương ứng như sau

$$P_1 = \Pr\left\{R_1^{(k,SD)} \leq r_1\right\}, \tag{3.64}$$

$$P_2 = \Pr\left\{R_1^{min} \leq r_1\right\}. \tag{3.65}$$

Tiếp tục, thực hiện phép đổi đối với P_1

$$\begin{aligned}P_1 &= \Pr\left\{\frac{\alpha_1^{(k)} P_s v_1^{(k)}}{(1-\alpha_1^{(k)})P_s v_2^{(k)} + N_0} \leq \phi_1\right\}, \\ &= \int_0^{\infty}\Pr\left\{\frac{\alpha_1^{(k)} P_s v_1^{(k)}}{(1-\alpha_1^{(k)})P_s x + N_0} \leq \phi_1\right\} f_{v_2^{(k)}}(x)dx.\end{aligned} \tag{3.66}$$

với $\phi_1 = 2^{\frac{r_1}{W}} - 1$ và $f_{v_2^{(k)}} = \frac{1}{\Omega_{v_2^{(k)}}}\exp\left(-\frac{x}{\Omega_{v_2^{(k)}}}\right)$. P_1 được biến đổi tiếp như sau

$$\begin{aligned}P_1 = \frac{1}{\Omega_{v_2^{(k)}}}\int_0^{\infty}&\left(1 - \exp\left(-\frac{\phi_1((1-\alpha_1^{(k)})P_s x + N_0)}{\alpha_1^{(k)} P_s \Omega_{v_1^{(k)}}}\right)\right) \\ &\times \exp\left(-\frac{x}{\Omega_{v_2^{(k)}}}\right)dx.\end{aligned} \tag{3.67}$$

Sau một số phép biến đổi toán học, chúng ta thu được công thức P_1 như sau

$$P_1 = 1 - \frac{\alpha_1^{(k)} \Omega_{v_1^{(k)}} \exp\left(-\frac{\phi_1 N_0}{\alpha_1^{(k)} P_s \Omega_{v_1^{(k)}}}\right)}{\phi_1 (1-\alpha_1^{(k)}) \Omega_{v_2^{(k)}} + \alpha_1^{(k)} \Omega_{v_1^{(k)}}}. \tag{3.68}$$

Tiếp theo, thực hiện việc tính toán P_2

$$\begin{aligned} P_2 &= \Pr\left\{\min\left\{R_1^{(k,E)}, R_1^{(k,D)}\right\} \leq r_1\right\}, \\ &= 1 - (1 - P_{21})(1 - P_{22}), \end{aligned} \tag{3.69}$$

trong đó

$$P_{21} = \Pr\left\{R_1^{(k,E)} \leq r_1\right\}, \tag{3.70}$$

$$P_{22} = \Pr\left\{R_1^{(k,D)} \leq r_1\right\}. \tag{3.71}$$

Tiếp theo, thực hiện tính toán P_{21}

$$P_{21} = \Pr\left\{\gamma_1^{(k,E)} \leq \phi_2\right\}, \tag{3.72}$$

với $\phi_2 = 2^{\frac{2r_1}{W}} - 1$. P_{21} biến đổi như sau

$$\begin{aligned} P_{21} &= \Pr\left\{\max_{m \in \{1,2,\ldots,N_p\}} \left\{\gamma_{1,m}^{(k,E)}\right\} \leq \phi_2\right\}, \\ &= \prod_{m=1}^{M} \int_0^{\infty} \Pr\left\{\frac{\alpha_1^{(k)} P_s f_{1,m}^{(k)}}{(1-\alpha_1^{(k)}) P_s x + N_0} \leq \phi_2\right\} f_{f_{2,m}^{(k)}}(x) dx, \end{aligned} \tag{3.73}$$

với $f_{f_{2,m}^{(k)}} = \frac{1}{\Omega_{f_{2,m}^{(k)}}} \exp\left(-\frac{x}{\Omega_{f_{2,m}^{(k)}}}\right)$.

Chúng ta cũng giả thiết rằng, tất cả các nhánh ăng-ten của E có độ lợi kênh truyền là giống nhau, có nghĩa là $\Omega_{f_{1,m}^{(k)}} = \Omega_{f_1^{(k)}}$, $\Omega_{f_{2,m}^{(k)}} = \Omega_{f_2^{(k)}}$, $\Omega_{\beta_m^{(k)}} = \Omega_\beta$.

Sau khi thực hiện một số phép biến đổi toán học, P_{21} được diễn tả như sau

$$P_{21} = \left[1 - \frac{\alpha_1^{(k)} \Omega_{f_1^{(k)}} \exp\left(-\frac{\phi_2 N_0}{\alpha_1^{(k)} P_s \Omega_{f_1^{(k)}}}\right)}{\phi_2 (1-\alpha_1^{(k)}) \Omega_{f_2^{(k)}} + \alpha_1^{(k)} \Omega_{f_1^{(k)}}}\right]^M. \tag{3.74}$$

Tiếp theo, để tính P_{22}, thực hiện phép thế công thức (3.19) vào (3.71), P_{22} được tính như sau

$$\begin{aligned} P_{22} &= \Pr\left\{\gamma_1^{(k,D)} \leq \phi_2\right\}, \\ &= \prod_{m=1}^{M} \Pr\left\{\frac{\delta_k P_e \beta_m^{(k)}}{N_0} \leq \phi_2\right\}. \end{aligned} \tag{3.75}$$

Áp dụng hàm phân bố mũ, chúng ta nhận được biểu thức của P_{22} như sau

$$\begin{aligned} P_{22} &= \prod_{m=1}^{M} \left[\left(1 - \exp\left\{-\frac{\phi_2 N_0}{\delta_1^{(k)} P_e \Omega_{\beta_m^{(k)}}}\right\}\right)\right], \\ &= \left[1 - \exp\left(-\frac{\phi_2 N_0}{\delta_1^{(k)} P_e \Omega_\beta}\right)\right]^M. \end{aligned} \tag{3.76}$$

Thay thế công thức (3.74) vào (3.76), chúng ta biểu thức của P_2 có dạng như sau

$$\begin{aligned} P_2 = 1 - &\left(1 - \left[1 - \exp\left(-\frac{\phi_2 N_0}{\delta_1^{(k)} P_e \Omega_\beta}\right)\right]^M\right) \\ \times &\left(1 - \left[1 - \frac{\alpha_1^{(k)} \Omega_{f_1^{(k)}} \exp\left(-\frac{\phi_2 N_0}{\alpha_1^{(k)} P_s \Omega_{f_1^{(k)}}}\right)}{\phi_2 (1 - \alpha_1^{(k)}) \Omega_{f_2^{(k)}} + \alpha_1^{(k)} \Omega_{f_1^{(k)}}}\right]^M\right) \end{aligned} \tag{3.77}$$

Và cuối cùng, $\mathcal{O}_{suc}^{(1)}$ được tính toán bởi công thức sau

$$\mathcal{O}_{suc}^{(1)} = 1 - \prod_{k=1}^{K} P_1 P_2, \tag{3.78}$$

với P_1 và P_2 được tính bởi công thức (3.68) và (3.77).

3.4.2 Xác suất nghe lén hợp pháp thành công đối với thiết bị đầu cuối có tín hiệu yếu nhất

Trong phần này luận án tính toán xác suất nghe lén hợp pháp thành công đối với người dùng $U_2^{(k)}$ có tín hiệu yếu nhất giữa K cặp người dùng. Xác suất nghe

lén hợp pháp thành công đối với người dùng có tín hiệu yếu nhất được mô tả bởi biểu thức sau

$$\mathcal{O}_{suc}^{(2)} = \Pr\left\{\min_{k\in\{1,2,\ldots,K\}}\left\{R_{2,E2E}^{(k)}\right\} \geq r_2\right\}, \tag{3.79}$$

với $R_{2,E2E}^{(k)}$ được định nghĩa trong công thức (3.26).

Tiếp theo, thực hiện phép biến đổi $\mathcal{O}_{suc}^{(2)}$

$$\begin{aligned}\mathcal{O}_{suc}^{(2)} &= \prod_{k=1}^{K}\left(1 - \Pr\left\{\max\left\{R_2^{(k,SD)}, R_2^{min}\right\} \leq r_2\right)\right\}, \\ &= \prod_{k=1}^{K}(1 - F_1F_2),\end{aligned} \tag{3.80}$$

với $R_2^{min} = \min\left\{R_2^{(k,E)}, R_2^{(k,D)}\right\}$. F_1 và F_2 được biển diễn là

$$F_1 = \Pr\left\{R_2^{(k,SD)} \leq r_2\right\}, \tag{3.81}$$

$$F_2 = \Pr\left\{R_2^{min} \leq r_2\right\}. \tag{3.82}$$

Tiếp tục, F_1 được biến đổi như sau

$$F_1 = \Pr\left\{\gamma_2^{(k,SD)} \leq \lambda_1\right\}, \tag{3.83}$$

trong đó $\lambda_1 = 2^{\frac{r_2}{W}} - 1$. Áp dụng hàm phân bố mũ, F_1 được tính như sau

$$F_1 = 1 - \exp\left(-\frac{\lambda_1 N_0}{(1-\alpha_1^{(k)})P_s\Omega_{v_2^{(k)}}}\right). \tag{3.84}$$

Tiếp theo, thực hiện tính toán F_2

$$\begin{aligned}F_2 &= 1 - \Pr\left\{\min\left\{R_2^{(k,E)}, R_2^{(k,D)}\right\} \geq r_2\right\}, \\ &= 1 - F_{21}F_{22},\end{aligned} \tag{3.85}$$

ở đây F_{21} và F_{21} được định nghĩa là

$$F_{21} = \Pr\left\{R_2^{(k,E)} \geq r_2\right\}, \tag{3.86}$$

$$F_{22} = \Pr\left\{R_2^{(k,D)} \geq r_2\right\}. \tag{3.87}$$

F_{21} được tính toán như sau

$$\begin{aligned} F_{21} &= 1 - \Pr\left\{\gamma_2^{(k,E)} \leq \lambda_2\right\}, \\ &= 1 - \prod_{m=1}^{M} \Pr\left\{f_{2,m}^{(k)} \leq \frac{\lambda_2 N_0}{(1-\alpha_1^{(k)})P_s}\right\}, \end{aligned} \tag{3.88}$$

trong đó $\lambda_2 = 2^{\frac{2r_2}{W}} - 1$.

Áp dụng hàm phân bố mũ, F_{21} được biến đổi như sau

$$\begin{aligned} F_{21} &= 1 - \prod_{m=1}^{M} \left[1 - \exp\left(\frac{-\lambda_2 N_0}{(1-\alpha_1^{(k)})P_s \Omega_{f_{2,m}^{(k)}}}\right)\right], \\ &= 1 - \left[1 - \exp\left(\frac{-\lambda_2 N_0}{(1-\alpha_1^{(k)})P_s \Omega_{f_2^{(k)}}}\right)\right]^M. \end{aligned} \tag{3.89}$$

Tiếp theo, thực hiện tính toán F_{22}

$$\begin{aligned} F_{22} &= 1 - \Pr\left\{\gamma_2^{(k,D)} \leq \lambda_2\right\}, \\ &= 1 - \prod_{m=1}^{M} \Pr\left\{\beta_m^{(k)} \leq \frac{\lambda_2 N_0}{\mu P_e}\right\}, \end{aligned}$$

với $\mu = 1 - (1+\lambda_2)\delta_1^{(k)}$. Áp dụng hàm phân bố mũ, F_{22} được biến đổi như sau

$$\begin{aligned} F_{22} &= 1 - \prod_{m=1}^{M} \left[\left(1 - \exp\left\{\frac{-\lambda_2 N_0}{\mu P_e \Omega_{\beta_m^{(k)}}}\right\}\right)\right], \\ &= 1 - \left[1 - \exp\left(\frac{-\lambda_2 N_0}{\mu P_e \Omega_\beta}\right)\right]^M. \end{aligned} \tag{3.90}$$

Thực hiện phép thế công thức (3.89) và (3.90) vào công thức (3.85), F_2 được tính như sau

$$\begin{aligned} F_2 = 1 - &\left(1 - \left[1 - \exp\left(\frac{-\lambda_2 N_0}{(1-\alpha_1^{(k)})P_s \Omega_{f_2^{(k)}}}\right)\right]^M\right) \\ &\times \left(1 - \left[1 - \exp\left(\frac{-\lambda_2 N_0}{\mu P_e \Omega_\beta}\right)\right]^M\right). \end{aligned} \tag{3.91}$$

Cuối cùng, $\mathcal{O}_{suc}^{(2)}$ được tính bởi biểu thức sau

$$\mathcal{O}_{suc}^{(2)} = \prod_{k=1}^{K}(1 - F_1 F_2), \tag{3.92}$$

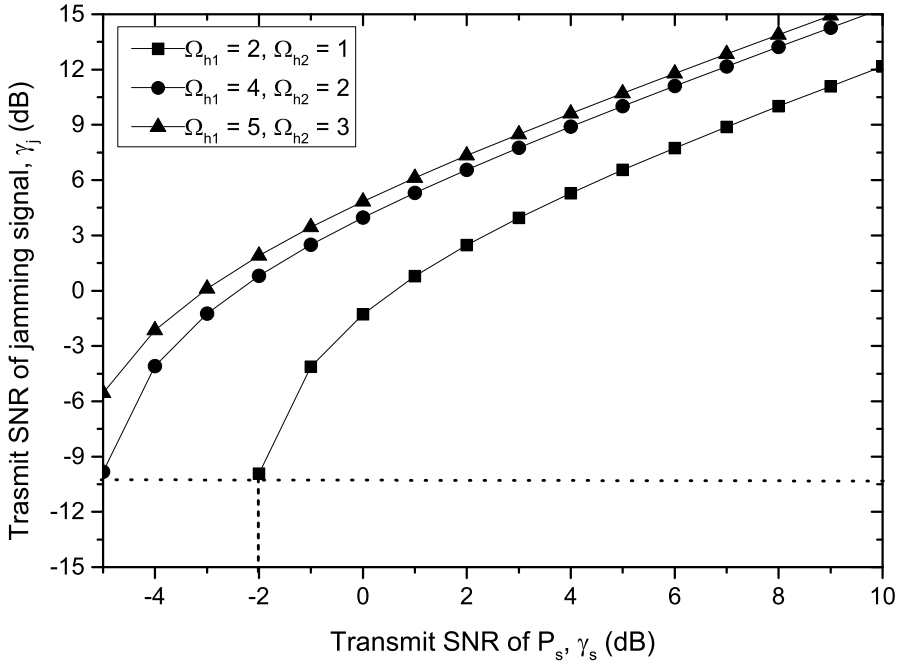
với F_1 và F_2 được định nghĩa tại công thức (3.84) và (3.91).

3.5 Mô phỏng và đánh giá kết quả

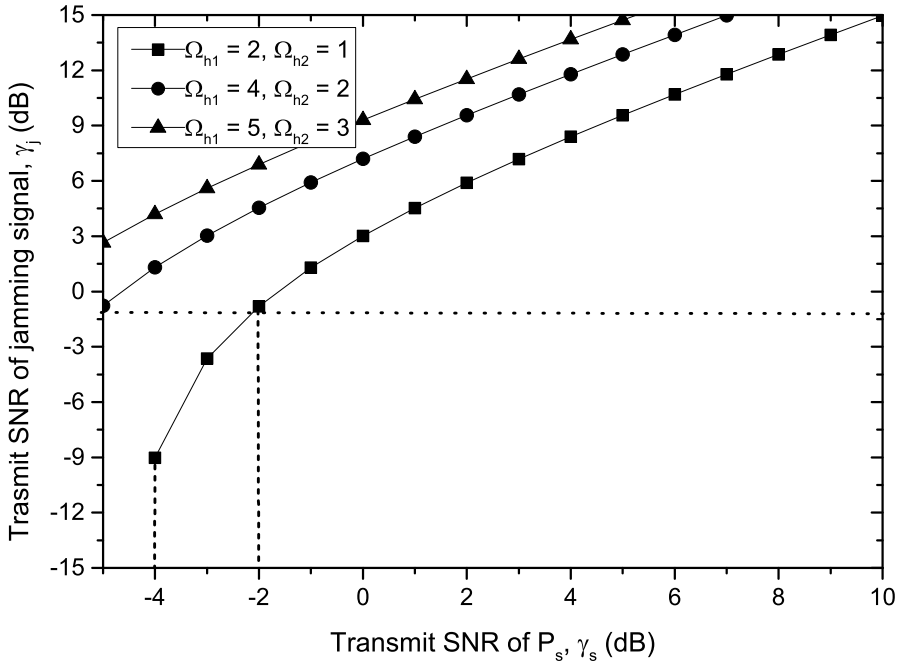
Trong phần này, luận án trình bày các kết quả phân tích và mô phỏng để đánh giá tác động của chính sách phân bổ công suất gây nhiễu và xác suất nghe lén hợp pháp thành công của hệ thống. Luận án sử dụng phương pháp Monte Carlo để mô phỏng bằng cách lấy giá trị trung bình các vòng lặp độc lập. Tác giả xem xét trường hợp hệ thống có 3 cặp người dùng (K = 3), độ lợi kênh truyền trung bình tương ứng là $\Omega_{h_1}^{(k)} = \{2, 4, 5\}$, $\Omega_{h_2}^{(k)} = \{1, 2, 3\}$, $\Omega_{f_1}^{(k)} = \{1, 0.5, 1.2\}$, $\Omega_{f_2}^{(k)} = \{0.3, 0.1, 0.01\}$, $\Omega_{v_1}^{(k)} = \{0.05, 0.02, 0.09\}$, $\Omega_{v_2}^{(k)} = \{0.002, 0.001, 0.005\}$, $\Omega_\beta = 1$. Các tham số khác của hệ thống được thiết lập như sau [43]:

- Băng thông của hệ thống: $W = 10^6$ Hz.
- Ngưỡng tốc độ truyền tin của E: $r_1 = r_2 = 10^5$ bps.
- Ngưỡng tốc độ truyền tin của B: $\gamma_{th} = 10^5$ bps.
- Xác suất dừng: $\theta_{th} = 0.01$.
- Số lượng ăng-ten của E: $M = 5$.
- Số lượng ăng-ten của B: $N = 5$.
- SNR của thiết bị giám sát E: $\gamma_e = \frac{P_e}{N_0} = 0$ dB.
- SNR cực đại của tín hiệu nhiễu: $\gamma_J^{max} = \frac{P_J^{max}}{N_0} = 20$ dB.
- SNR cực đại của $U_l^{(k)}$: $\gamma_s^{max} = \frac{P_s^{max}}{N_0} = 20$ dB.
- Hệ số phân bổ công suất: $\alpha_1^{(k)} = 0.3$, $\delta_1^{(k)} = 0.2$.

Hình 3.2 và 3.3 minh họa mối quan hệ giữa SNR tín hiệu gẫy nhiễu $\gamma_J = P_J/N_0$ của E và SNR $\gamma_s = P_s/N_0$ của $U_l^{(k)}$ đối với trường hợp kênh truyền gây



Hình 3.2: *SNR của tín hiệu nhiễu trong trường hợp kênh truyền gây nhiễu E→B xác định và* $\Omega_{g_n} = 1$.



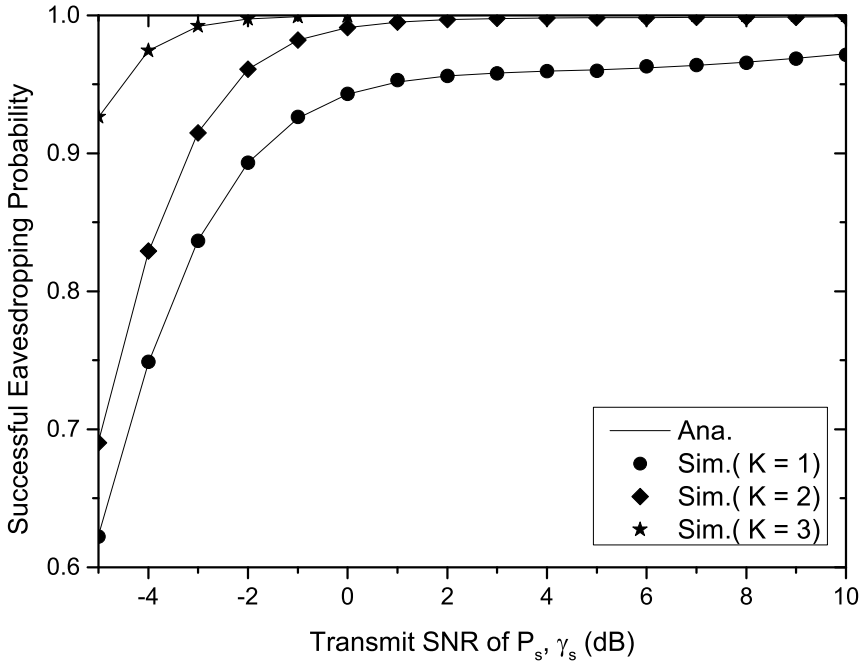
Hình 3.3: *SNR của tín hiệu nhiễu trong trường hợp kênh truyền gây nhiễu E→B không xác định và* $\Omega_{g_n} = 1$.

nhiễu xác định và không xác định. Chúng ta quan sát thấy rằng khi $U_l^{(k)}$ tăng công suất phát γ_s, E phải tăng công suất γ_e của tín hiệu gây nhiễu.

Tuy nhiên, trên cùng một miền giá trị SNR [-5, 10] dB của $U_l^{(k)}$ thì SNR của tín

hiệu gây nhiễu trong trường hợp kênh truyền không xác định thì luôn luôn cao hơn SNR so với trường hợp kênh truyền xác định. Để làm rõ kết luận này, chúng ta có thể thấy trường hợp $\Omega_{g_n} = 1$ ở Hình 3.2 và 3.3, rõ ràng rằng SNR của tín hiệu gây nhiễu chỉ tăng từ -10 dB lên 12 dB để giữ SNR của $U_1^{(k)}$ trong miền giá trị [-2, 10] dB (xem Hình 3.2). Tuy nhiên, SNR của tín hiệu gây nhiễu phải tăng từ 2 dB to 15 dB để giữ SNR của $U_1^{(k)}$ trong miền giá trị [-2, 10] dB (xem Hình 3.3). Nói cách khác, E chỉ cần mức công suất thấp để gây nhiễu khi E biết chính xác CSI của kênh truyền $E \rightarrow B$.

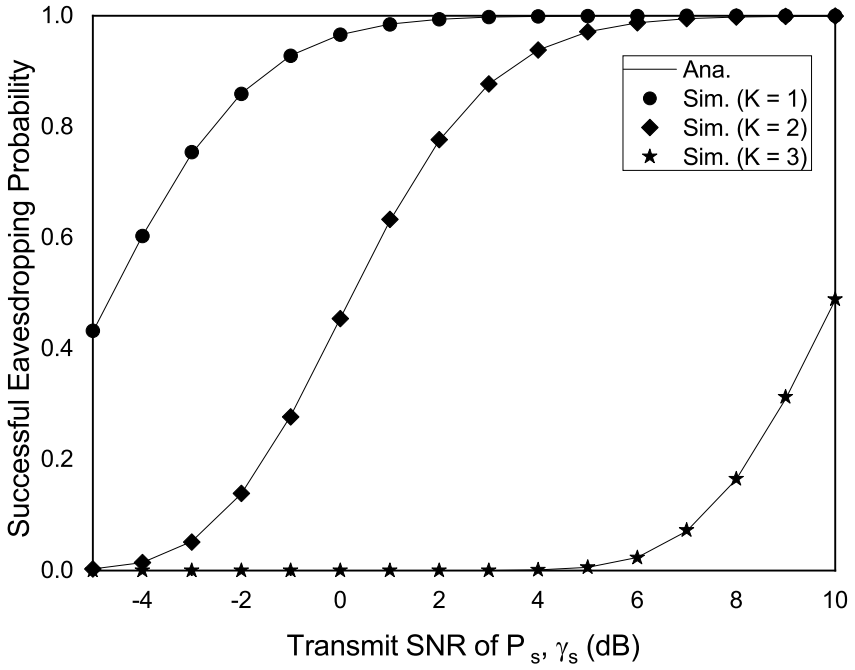
Hơn thế nữa, các kết quả trên hình chỉ ra rằng khi độ lợi kênh truyền $U_l^{(k)} \rightarrow B$ tăng tức $\Omega_{h_1} = \{2, 4, 5\}$ thì E cần mức SNR của tín hiệu gây nhiễu lớn hơn để giữ SNR của $U_l^{(k)}$ ở cùng mức, cụ thể γ_s = -2 dB. Điều này có thể được giải thích như sau: người dùng $U_l^{(k)}$ chỉ cần duy nhất mức công suất nhỏ để duy trì chất lượng dịch vụ khi kênh truyền $U_l^{(k)} \rightarrow B$ ở điều kiện tốt, do đó E cần phát mức công suất cao của tín hiệu gây nhiễu để tạo ra ảnh hưởng đủ lớn lên B.



Hình 3.4: *Tác động của số lượng cặp người dùng lên $\mathcal{O}_{suc}^{(1)}$ theo tập giá trị của γ_s.*

Hình 3.4 cho thấy mức ảnh hưởng của số lượng cặp người dùng lên xác suất nghe lén thành công của người dùng cuối có tín hiệu tốt nhất. Chúng ta dễ dàng nhận thấy rằng khi số lượng cặp người dùng tăng lên thì xác suất nghe lén thành công được cải thiện rõ rệt, nghĩa là hiệu suất của hệ thống được cải thiện. Như

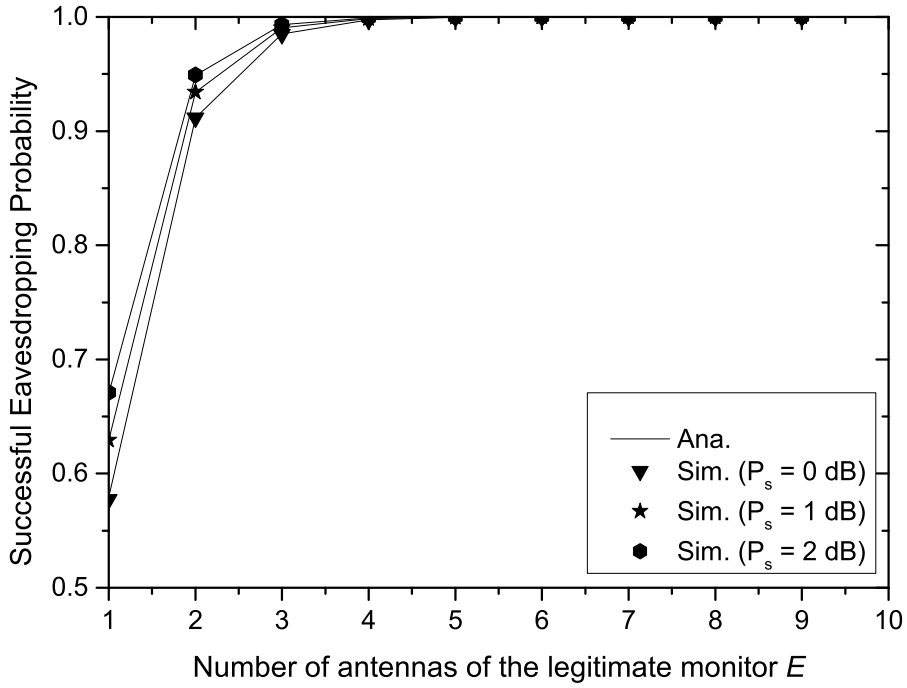
chúng ta thấy khi K tăng ($K = 1, 2, 3$) thì xác suất này tăng dần tới 1. Nguyên nhân là do khi số lượng cặp người dùng tăng, thì khả năng để chọn người dùng cuối có tín hiệu tốt nhất sẽ đa dạng và hiệu quả hơn. Kết quả là, xác suất nghe lén của hệ thống được cải thiện.



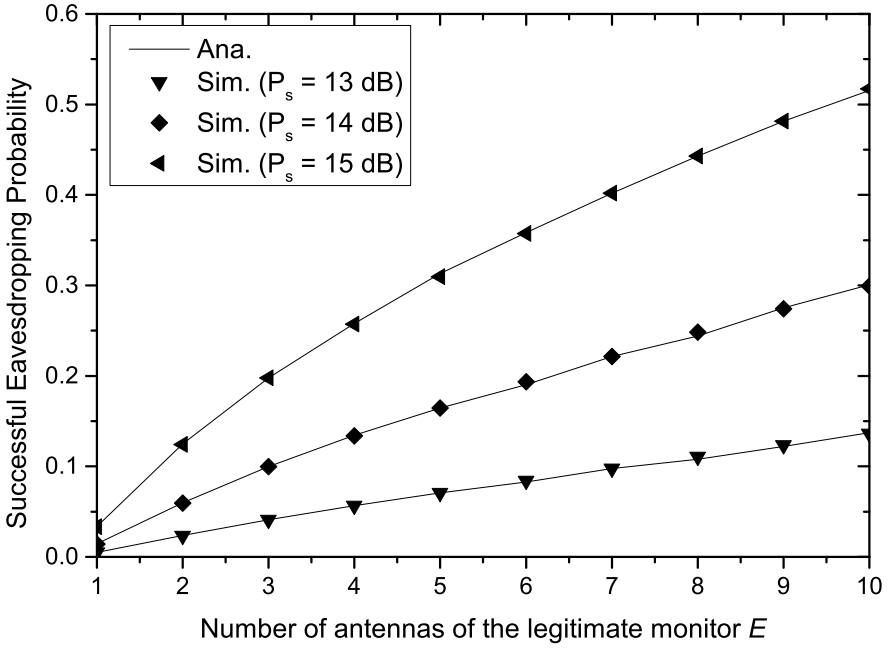
Hình 3.5: *Tác động của số lượng cặp người dùng lên $\mathcal{O}_{suc}^{(2)}$ theo tập giá trị của γ_s.*

Hình 3.5 minh họa ảnh hưởng của số lượng cặp người dùng lên xác suất nghe lén hợp pháp thành công của người dùng cuối có tín hiệu yếu nhất. Đối lập với trường hợp người dùng cuối có tín hiệu tốt nhất, xác suất nghe lén thành công sẽ giảm nhanh khi số lượng cặp người dùng tăng. Trong trường hợp K = 3, chúng ta thấy rằng xác suất nghe lén thành công bằng không khi SNR γ_s nhỏ hơn 5 dB. Nguyên nhân là do với số lượng cặp người dùng tăng lên thì khả năng để chọn người dùng có tín hiệu yếu nhất sẽ đa dạng và hiệu quả hơn. Chính vì vậy xác suất nghe lén thành công của hệ thống sẽ giảm.

Hình 3.6 và 3.7 chỉ ra tác động của số lượng ăng-ten của E lên xác suất nghe lén hợp pháp thành công đối với người dùng cuối có tín hiệu mạnh nhất và yếu nhất. Có thể thấy rằng xác suất nghe lén thành công cho cả người dùng có tín hiệu mạnh nhất và yếu nhất đều tăng khi số lượng ăng-ten của E tăng. Điều này xảy ra do khi số lượng ăng-ten của E tăng lên thì độ lợi phân tập tại E cũng tăng lên. Điều này cho thấy tăng số lượng ăng-ten tại E là cách đơn giản và hiệu quả



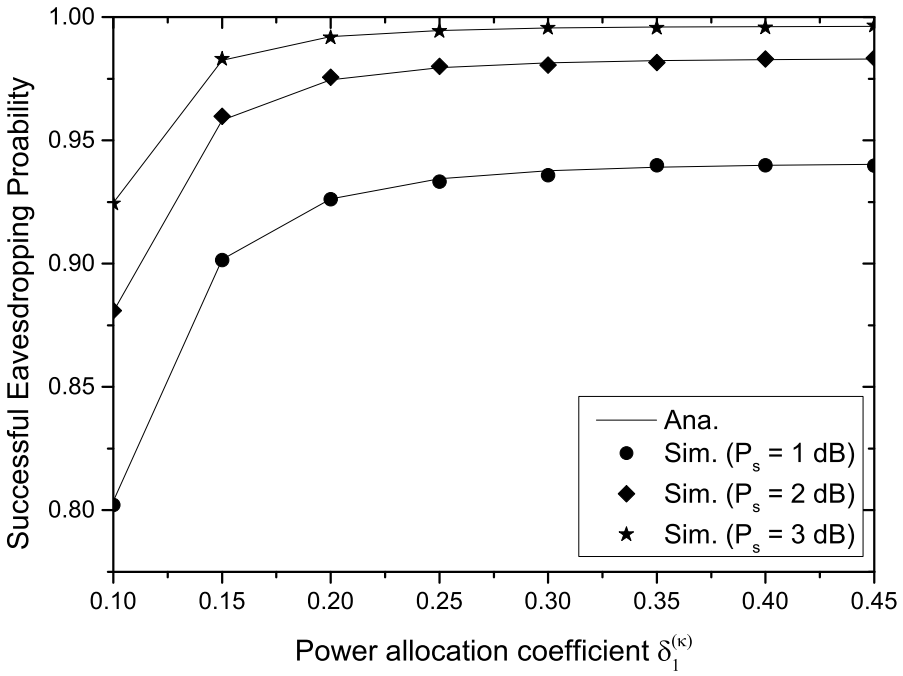
Hình 3.6: *Tác động của số lượng ăng-ten lên $\mathcal{O}_{suc}^{(1)}$ theo tập giá trị của γ_s.*



Hình 3.7: *Tác động của số lượng ăng-ten lên $\mathcal{O}_{suc}^{(2)}$ theo tập giá trị của γ_s.*

để cải thiện xác suất nghe lén hợp pháp, việc tăng số lượng ăng-ten dễ dàng thực hiện được trong mạng 5G vì công nghệ mạng 5G hỗ trợ các thiết bị đa ăng-ten.

Cuối cùng, Hình 3.8 cho thấy tác động của hệ số phân bổ công suất $\delta_1^{(k)}$ và SNR P_s của $U_l^{(k)}$ lên xác suất nghe lén thành công của người dùng có tín hiệu tốt



Hình 3.8: *Tác động của hệ số phân bổ công suất $\delta_1^{(k)}$ đối với $\mathcal{O}_{suc}^{(1)}$ theo tập giá trị của γ_s.*

nhất trong số K người dùng $U_1^{(k)}$. Hệ số $\delta_1^{(k)}$ phải nằm trong khoảng giá trị từ 0 tới 0.5. Có thể thấy rằng xác suất nghe lén thành công tăng lên đáng kể khi hệ số phân bổ công suất và công suất truyền tăng lên. Điều này có thể được giải thích như sau: D sẽ dễ dàng thu và giải mã tín hiệu được truyền từ những người dùng bất hợp pháp tới B khi chúng tăng công suất truyền tín hiệu.

3.6 Kết luận

Trong chương này, luận án nghiên cứu về mô hình mạng NOMA có chiến lược chủ động nghe lén. Trong đó thiết bị giám sát hợp pháp E chủ động gẫy nhiễu lên thiết bị thu tín hiệu bất hợp pháp B để cải thiện hiệu năng nghe lén. Thiết bị giám sát gây nhiễu E phải có chính sách điều chỉnh công suất phù hợp để đảm bảo hiệu suất hoạt động của người dùng bất hợp pháp. Luận án đã xây dựng biểu thức tính toán công suất tín hiệu gẫy nhiễu của thiết bị giám sát E trong trường hợp CSI của kênh truyền gây nhiễu $E \rightarrow B$ xác định và trường hợp CSI không xác định. Tiếp theo, luận án tính toán hiệu suất nghe lén thành công để đánh giá hiệu năng thu thập thông tin của hệ thống. Kết quả tính toán đã chỉ ra rằng khi CSI của kênh gây nhiễu xác định thì mức công suất để gây nhiễu nhỏ hơn mức công gây nhiễu khi CSI của kênh gây nhiễu không xác định. Ngoài ra,

các số liệu của kết quả phân tích và mô phỏng cũng chỉ ra rằng xác suất nghe lén hợp pháp thành công đối với người dùng có tín hiệu mạnh nhất tăng đáng kể khi số lượng cặp người dùng cuối, số lượng ăng-ten của thiết bị giám sát E tăng lên. Ngược lại, xác suất nghe lén hợp pháp thành công đối với người dùng có tín hiệu yếu nhất giảm khi số lượng cặp người dùng cuối, số lượng ăng-ten của thiết bị giám sát E tăng lên. Ngoài ra, hệ số phân bổ công suất giữa những người dùng của mỗi cặp người dùng trong mạng NOMA tăng thì xác suất nghe lén hợp pháp thành công của người dùng có tín hiệu mạnh nhất cũng tăng.

Chương 4

ĐÁNH GIÁ HIỆU NĂNG BẢO MẬT, ĐỘ TIN CẬY MẠNG SISO NOMA VÀ MẠNG NOMA NHẬN THỨC

4.1 Giới thiệu

Các nghiên cứu về bảo mật tầng vật lý trong mạng NOMA ban đầu chủ yếu tập trung vào các hệ thống SISO như đã trình bày trong mục 1.7.3. Các nghiên cứu đều xem xét trường hợp thiết bị nghe lén có khả năng giải mã bằng phương pháp loại bỏ nhiễu nối tiếp mà chưa có nghiên cứu nào xem xét trường hợp thiết bị nghe lén sử dụng phương pháp loại bỏ nhiễu song song và so sánh hiệu năng bảo mật của hệ thống trong hai trường hợp này. Ngoài ra, các nghiên cứu này chỉ phân tích, đánh giá hiệu năng bảo mật hệ thống và bỏ qua hiệu năng bảo mật của từng người dùng trong hệ thống. Hơn nữa, cũng chưa có nghiên cứu nào xem xét vấn đề hiệu suất mạng NOMA dựa trên phép đo xác suất dừng gói tin, điều chỉnh hệ số phân bổ công suất giữa hai người dùng trong một nhóm để đảm bảo thời gian truyền tin trung bình giữa hai người dùng là như nhau.

Bên cạnh đó, nghiên cứu vấn đề bảo mật mạng NOMA trong môi trường vô tuyến nhận thức nhận được sự quan tâm của nhiều nhà nghiên cứu. Trong số các bài báo nghiên cứu về vấn đề này như đã trình bày trong mục 1.7.4, ngoại trừ bài báo [156], đều xem xét bài toán cải thiện hiệu năng bảo mật. Trong nghiên cứu [156], các tác giả đã khảo sát sự đánh đổi giữa bảo mật và độ tin cậy mạng NOMA cộng tác trong môi trường vô tuyến nhận thức và sử dụng công nghệ đa ăng-ten và vùng loại trừ nghe lén để nâng cao bảo mật, tuy nhiên nghiên cứu này bỏ qua điều kiện ràng buộc về mức can nhiễu và công suất phát mức đỉnh của mạng thứ cấp, làm cho bài toán cải thiện hiệu năng chỉ phù hợp với vùng tỷ lệ tín hiệu trên nhiễu nhỏ và do đó có phần khó khả thi khi áp dụng thực tế.

Xuất phát từ những tồn tại trên, trong chương này, luận án đề xuất hai mô hình để đánh giá hiệu năng bảo mật mạng SISO NOMA và mạng SISO NOMA nhận thức dạng nền dưới ràng buộc mức can nhiễu của mạng sơ cấp trên kênh truyền Rayleigh fading.

Mô hình thứ nhất: Mô hình mạng SISO NOMA gồm có một thiết bị truyền tin và hai thiết bị thu nhận thông tin. Một thiết bị nghe lén thông tin hoạt động ở chế độ thụ động để thu thập thông tin. Luận án thực hiện tính toán biểu thức xác suất dừng bảo mật để đánh giá hiệu năng bảo mật của từng người dùng trong hệ thống và của toàn bộ hệ thống trong hai kịch bản, kịch bản thứ nhất thiết bị Eve sử dụng kỹ thuật SIC và kịch bản thứ hai thiết bị Eve sử dụng kỹ thuật PIC để bóc tách tín hiệu nghe lén. Hơn nữa, khả năng đảm bảo an toàn thông tin của hệ thống trong trường hợp thiết bị nghe lén Eve được trang bị một ăng-ten và trường hợp được trang bị nhiều ăng-ten cũng được xem xét. Ngoài ra, thời gian truyền tin trung bình từ máy phát đến người dùng cuối, xác suất rớt gói tin cũng được tính toán. Ngoài ra, luận án đề xuất thuật toán tìm hệ số phân bổ công suất để đảm bảo tính công bằng về thời gian truyền từ tin từ máy phát đến những người dùng cuối. Cuối cùng, luận án cũng thực hiện mô phỏng Monte Carlo để kiểm chứng các biểu thức toán học được đưa ra.

Mô hình thứ hai: Mở rộng từ mô hình thứ nhất, đó là mô hình mạng SISO NOMA trong môi trường vô tuyến nhận thức dạng nền dưới ràng buộc mức can nhiễu của mạng sơ cấp, gồm có mạng thứ cấp và mạng sơ cấp. Mạng thứ cấp SISO NOMA sử dụng băng tần của mạng sơ cấp và được phép gây nhiễu lên mạng sơ cấp nhưng phải điều khiển công suất để đảm bảo công suất gây nhiễu tại máy thu sơ cấp không vượt ngưỡng mức can nhiễu quy định. Thiết bị nghe lén Eve hoạt động ở chế độ thụ động để thu thập thông tin truyền trên mạng thứ cấp. Các thiết bị trong mô hình này đều được trang bị một ăng-ten. Trên cơ sở ràng buộc về giới hạn ngưỡng can nhiễu của mạng sơ cấp, luận án đã đưa ra biểu thức xác định công suất phát của mạng thứ cấp để đảm bảo không ảnh hưởng đến hiệu suất của mạng sơ cấp, đồng thời đưa ra biểu thức đánh giá bảo mật dựa trên phép đo xác suất bị nghe lén và biểu thức đánh giá độ tin cậy dựa trên phép đo xác suất dừng hoạt động của mạng thứ cấp. Hơn nữa, luận án thực hiện mô phỏng Monte Carlo để kiểm chứng các biểu thức toán học được đưa ra.

Phần còn lại của chương này được trình bày như sau: Phần 4.2 mô tả mô hình đề xuất 1, trong đó đưa ra các biểu thức SOP của hệ thống và của từng người dùng với các kịch bản về Eve khác nhau và các kết quả mô phỏng được thể hiện; Phần 4.3 mô tả đề xuất mô hình 2, trong đó đưa ra các biểu thức OP và IP và các kết quả mô phỏng được thể hiện; Phần 4.4 kết luận nội dung của chương.

Các nội dung được trình bày trong chương này dựa trên các kết quả nghiên cứu trong công trình *A*2 đã được công bố trên tạp chí *IEEE Access* và công trình *A*4 đã được báo cáo tại Hội thảo khoa học *12th International Symposium on Information and Communication Technology (SOICT 2023)*.

4.2 MÔ HÌNH 4.1: Đánh giá hiệu năng bảo mật và tính công bằng thời gian truyền tin mạng SISO NOMA

4.2.1 Mô hình hệ thống

Mô hình mạng NOMA được mô tả như trong hình 4.1, trong đó máy phát S đồng thời truyền tin đến hai người dùng cuối là U_1 và U_2, cùng thời điểm đó thiết bị nghe lén Eve thực hiện việc nghe lén thông tin. S có khả năng phân bổ công suất truyền tin dựa trên chất lượng kênh truyền của người dùng. Tức là S sẽ phân bổ mức công suất cao hơn cho người dùng U_2 do nằm ở vị trí xa BS hơn, và phân bố mức công suất nhỏ hơn cho người dùng U_1 vì gần S hơn.

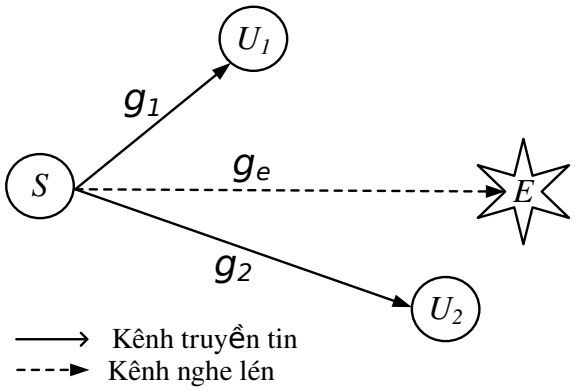
Ký hiệu g_1, g_2 và g_e lần lượt là hệ số kênh truyền từ $S \rightarrow U_1$, $S \rightarrow U_2$, và $S \rightarrow E$. Giả thiết rằng tất người dùng hoạt động trong môi trường văn phòng và không tồn tại đường truyền thẳng giữa thiết bị nguồn và đích. Vì vậy, tất cả các kênh truyền tuân theo phân bố Rayleigh fading, và có độ lợi kênh truyền $|g_i|^2$ $(i \in \{1, 2, e\})$ là biến ngẫu nhiên phân bố theo hàm mũ có độ lợi kênh truyền trung bình là Ω_i. Hàm PDF và hàm CDF của $X_i = |g_i|^2$ được tính theo công thức sau

$$f_{X_i}(x) = \frac{1}{\Omega_i} \exp(-\frac{x}{\Omega_i}), \tag{4.1}$$

$$F_{X_i}(x) = 1 - \exp(-\frac{x}{\Omega_i}). \tag{4.2}$$

Chúng ta biết rằng nút nghe lén Eve có khả năng sử dụng kỹ thuật SIC hoặc PIC để giải mã tín hiệu kết hợp được truyền từ S đến người dùng U_1, U_2. SIC là kỹ thuật giải mã tín hiệu được đề xuất từ năm 1990 [49], cho phép thiết bị nhận

phát hiện và loại bỏ tín hiệu khác cho tới khi nó nhận được tín hiệu của chính nó. Trong hệ thống này mỗi người dùng sẽ giải mã tín hiệu của chính nó bằng cách coi tín hiệu của người dùng còn lại với mức công suất truyền thấp hơn là tín hiệu nhiễu [57]. Để cải thiện hiệu suất của kỹ thuật SIC, kỹ thuật adaptive SIC và gần đây là kỹ thuật SIC nâng cao đã ra đời [60, 61]. Đối lập với kỹ thuật SIC, kỹ thuật PIC cho phép Eve loại bỏ tín hiệu nhiễu theo cơ chế song song [62]. Nói cách khác, nút nghe lén Eve với kỹ thuật PIC có khả năng bóc tách tín hiệu đồng thời của nhiều người dùng và thông minh hơn kỹ thuật SIC [57].



Hình 4.1: *Mô hình mạng NOMA có một máy phát S, hai người dùng cuối U_1, U_2, và một thiết bị nghe lén E.*

Đầu tiên S truyền tín hiệu x, đây là tín hiệu kết hợp giữa tín hiệu x_1 và x_2 tới U_1 và U_2

$$x = \sqrt{\alpha_1 P} x_1 + \sqrt{\alpha_2 P} x_2, \tag{4.3}$$

trong đó P là công suất truyền của S, α_j $(j \in \{1, 2\})$ hệ số kênh truyền tương ứng với người dùng U_j và thỏa mãn điều kiện $\alpha_1 + \alpha_2 = 1$. Do ở xa hơn S nên U_2 được phân bổ mức công suất lớn hơn có nghĩa là $\alpha_2 = 1 - \alpha_1 > 0.5$, trong khi đó U_1 gần S hơn nên được phân bổ mức công suất thấp hơn so với U_2, tức là $\alpha_1 < 0.5$. Tín hiệu nhận được tại U_1, U_2, và Eve là

$$y_i = \sqrt{\alpha_1 P} x_1 g_i + \sqrt{\alpha_2 P} x_2 g_i + n_i, \tag{4.4}$$

trong đó n_i là công suất nhiễu AWGN có giá trị trung bình bằng không và phương sai N_0. Vì S phân bổ công suất cao hơn cho tín hiệu của U_2 nên theo

nguyên lý của mạng NOMA, tín hiệu nhận được tại U_2 được giải mã và coi tín hiệu của U_1 như là tín hiệu nhiễu, trong khi đó người dùng U_1 trực tiếp giải mã tín hiệu của chính nó [68]. Kết quả là tỷ số SNR và SINR tại U_1 và U_2 được mô tả bởi công thức sau

$$\gamma_{U_1} = \frac{\alpha_1 P|g_1|^2}{N_0}, \tag{4.5}$$

$$\gamma_{U_2} = \frac{\alpha_2 P|g_2|^2}{\alpha_1 P|g_2|^2 + N_0}. \tag{4.6}$$

Hơn nữa, Eve nằm trong vùng phủ sóng của S nên nó cũng có thể nghe lén tín hiệu từ S, và sau đó nó có thể sử dụng kỹ thuật xử lý tín hiệu như SIC hoặc PIC để giải mã tín hiệu nghe lén. Trường hợp sử dụng kỹ thuật SIC, Eve có thể giải mã tín hiệu U_1 trực tiếp, trong khi giải mã tín hiệu của U_2, Eve sẽ coi tín hiệu người dùng U_1 là tín hiệu nhiễu. Do đó tỷ số SNR và SINR có dạng tương tự như trong công thức (4.5) và (4.6), có nghĩa là

$$\gamma_{E,1}^{SIC} = \frac{\alpha_1 P|g_e|^2}{N_0}, \tag{4.7}$$

$$\gamma_{E,2}^{SIC} = \frac{\alpha_2 P|g_e|^2}{\alpha_1 P|g_e|^2 + N_0}, \tag{4.8}$$

trong đó $\gamma_{E,1}^{SIC}$ là tỷ số SNR tại Eve khi thực hiện việc giải mã tính hiệu của U_1, và $\gamma_{E,2}^{SIC}$ là tỷ số SINR tại Eve khi nó giải mã tín hiệu của U_2.

Trường hợp Eve sử dụng kỹ thuật PIC, Eve sẽ hoạt động thông minh hơn U_1 và U_2, tức là nó có thể giải mã tín hiệu của nhiều người dùng tại cùng một thời điểm và nhiễu gây ra bởi các tín hiệu khác được loại bỏ một cách hiệu quả. Do đó, biểu thức tỷ số SNR tức thời của Eve khi nó giải mã tín hiệu của U_1 giống như biểu thức SNR của Eve ở chế độ SIC, có nghĩa là

$$\gamma_{E,1}^{PIC} = \frac{\alpha_1 P|g_e|^2}{N_0}, \tag{4.9}$$

trong đó khi đó tỷ số SNR tại Eve liên quan đến U_2 có dạng sau

$$\gamma_{E,2}^{PIC} = \frac{\alpha_2 P|g_e|^2}{N_0}. \tag{4.10}$$

Chúng ta thấy rằng SNR ở chế độ PIC luôn luôn lớn hơn hoặc bằng SNR ở chế độ SIC. Luận án sẽ phân tích mức độ ảnh hưởng của kỹ thuật SIC và PIC mà Eve sử dụng lên hiệu năng bảo mật của hệ thống đang xem xét.

4.2.2 Hiệu năng bảo mật trong kịch bản Eve có một ăng-ten

Trong phần này, luận án xây dựng biểu thức tính toán xác suất dừng bảo mật của từng người dùng và của hệ thống trong trường hợp Eve sử dụng kỹ thuật loại bỏ nhiễu SIC và PIC.

4.2.2.1 Xác suất dừng bảo mật trong kịch bản Eve sử dụng kỹ thuật loại bỏ nhiễu SIC

Trong kịch bản Eve sử dụng SIC để loại bỏ nhiễu, giả định rằng Eve, U_1, và U_2 có khả năng loại bỏ nhiễu là như nhau.

- Xác suất dừng bảo mật của người dùng

  Mục tiêu của Eve là nghe lén thành công tín hiệu của cả người dùng U_1 và U_2. Xuất phát từ công thức (1.52), chúng ta nhận được biểu thức dung lượng bảo mật tức thời của U_1 ($C_s^{U_1,SIC}$) và U_2 ($C_s^{U_2,SIC}$) tương ứng như sau

$$C_s^{U_1,SIC} = \{B\log_2(1+\gamma_{U_1}) - B\log_2(1+\gamma_{E,1}^{SIC})\}^+, \tag{4.11}$$
$$C_s^{U_2,SIC} = \{B\log_2(1+\gamma_{U_2}) - B\log_2(1+\gamma_{E,2}^{SIC})\}^+, \tag{4.12}$$

  trong đó $x^+ = \max\{x, 0\}$, B là băng thông hệ thống, ký hiệu γ_{U_1}, γ_{U_2}, $\gamma_{E,1}^{SIC}$ và $\gamma_{E,2}^{SIC}$ được tính theo công thức (4.5), (4.6), (4.7) và (4.8) tương ứng.

  Xác suất dừng bảo mật của U_1 xảy ra khi dung lượng bảo mật tức thời nhỏ hơn ngưỡng tốc độ bảo mật cho trước và được xác định như sau

$$\mathcal{O}_{sec}^{U_1,SIC} = \Pr\{C_s^{U_1,SIC} < R_1\} = \Pr\{\gamma_{U_1} \le \delta_1 + (\delta_1+1)\gamma_{E,1}^{SIC}\} \tag{4.13}$$

  Tiếp theo, áp dụng công thức [67, 3.5], chúng ta nhận được biểu thức SOP của U_1 như sau

$$\mathcal{O}_{sec}^{U_1,SIC} = \int_0^\infty F_{\gamma_{U_1}}(\delta_1 + (\delta_1+1)x) f_{\gamma_{E,1}^{SIC}}(x)dx, \tag{4.14}$$

  trong đó $\delta_1 = 2^{R_1/B} - 1$ và R_1 là ngưỡng tốc độ bảo mật của U_1.

  Để đơn giản hóa tích phân (4.14), chúng ta lần lượt tiến hành tìm hàm CDF và PDF của γ_{U_1} và $\gamma_{E,1}^{SIC}$.

Áp dụng phân bố mũ [66], hàm CDF của γ_{U_1} nhận được như sau

$$F_{\gamma_{U_1}}(t) = \Pr\{\gamma_{U_1} < t\} = 1 - \exp(-\lambda_1 t), \tag{4.15}$$

trong đó $\lambda_1 = \frac{N_0}{\alpha_1 P \Omega_1}$. Hơn nữa, hàm CDF của $\gamma_{E,1}^{SIC}$ được tính như sau

$$F_{\gamma_{E,1}^{SIC}}(x) = \Pr\{\gamma_{E,1}^{SIC} < x\} = 1 - \exp(-\lambda_{e_1} x), \tag{4.16}$$

trong đó $\lambda_{e_1} = \frac{N_0}{\alpha_1 P \Omega_e}$. Vì vậy, hàm PDF của $\gamma_{E,1}^{SIC}$ tính được bằng cách tính vi phân (4.16) theo x như sau

$$f_{\gamma_{E,1}^{SIC}}(x) = \lambda_{e_1} \exp(-\lambda_{e_1} x). \tag{4.17}$$

Thực hiện phép thế công thức (4.15) với $t = \delta_1 + (\delta_1 + 1)x$ và (4.17) vào (4.13), SOP của U_1 nhận được như sau

$$\mathcal{O}_{sec}^{U_1,SIC} = 1 - \frac{\lambda_{e_1} \exp(-\lambda_1 \delta_1)}{\lambda_1(\delta_1 + 1) + \lambda_{e_1}}. \tag{4.18}$$

Tương tự, xuất phát từ công thức (4.12), SOP của U_2 được viết lại như sau

$$\begin{aligned} \mathcal{O}_{sec}^{U_2,SIC} &= \Pr\{C_s^{U_2,SIC} < R_2\} = 1 - \Pr\left\{\gamma_{E,2}^{SIC} < \frac{\gamma_2 - \delta_2}{\delta_2 + 1}\right\} \\ &= 1 - \int_0^{\infty} F_{\gamma_{E,2}^{SIC}}\left(\frac{x - \delta_2}{\delta_2 + 1}\right) f_{\gamma_{U_2}}(x) dx, \end{aligned} \tag{4.19}$$

trong đó $\delta_2 = 2^{R_2/B} - 1$ và R_2 ngưỡng tốc độ bảo mật của U_2. Để tính công thức (4.19), chúng ta sẽ lần lượt tính CDF và DFP của $\gamma_{E,2}^{SIC}$ và γ_{U_2}

$$F_{\gamma_{E,2}^{SIC}}(x) = \Pr\{\gamma_{E,2}^{SIC} < x\} = \Pr\left\{|g_e|^2 < \frac{N_0 x}{(\alpha_2 - \alpha_1 x)P}\right\}.$$

Sử dụng hàm phân phối mũ, hàm CDF của $\gamma_{E,2}^{SIC}$ được tính như sau

$$F_{\gamma_{E,2}^{SIC}}(x) = \begin{cases} 1 - \exp\left(-\frac{\lambda_e x}{\alpha_2 - \alpha_1 x}\right) & \text{if } x < \alpha_2/\alpha_1, \\ 0 & \text{if } x \geq \alpha_2/\alpha_1\ , \end{cases} \tag{4.20}$$

trong đó $\lambda_e = \frac{N_0}{P \Omega_e}$. Ngoài ra, hàm PDF của γ_{U_2} được biến đổi như sau

$$F_{\gamma_{U_2}}(x) = \Pr\{\gamma_{U_2} < x\} = \Pr\left\{|g_2|^2 < \frac{N_0 x}{(\alpha_2 - \alpha_1 x)P}\right\}$$

$$= \begin{cases} 1 - \exp\left(-\frac{\lambda_2 x}{\alpha_2 - \alpha_1 x}\right) & \text{if } x < \alpha_2/\alpha_1 \\ 0 & \text{if } x \geq \alpha_2/\alpha_1, \end{cases} \tag{4.21}$$

trong đó $\lambda_2 = \frac{N_0}{P\Omega_2}$. Thực hiện phép vi phân phương trình (4.21) theo x, chúng ta nhận được hàm PDF của γ_{U_2} như sau

$$f_{\gamma_{U_2}}(x) = \begin{cases} \frac{\lambda_2 \alpha_2}{(\alpha_2 - \alpha_1 x)^2} \exp\left(-\frac{\lambda_2 x}{\alpha_2 - \alpha_1 x}\right) & \text{if } x < \alpha_2/\alpha_1 \\ 0 & \text{if } x \geq \alpha_2/\alpha_1, \end{cases} \tag{4.22}$$

Thế công thức (4.20) và (4.22) vào (4.19), SOP của U_2 được tính như sau

$$\mathcal{O}_{sec}^{U_2,SIC} = 1 - \lambda_2 \alpha_2 (I_1 - I_2), \tag{4.23}$$

trong đó I_1 và I_2 được định nghĩa như sau

$$I_1 = \int_0^{\alpha_2/\alpha_1} \frac{1}{(\alpha_2 - \alpha_1 x)^2} \exp\left(-\frac{\lambda_2 x}{\alpha_2 - \alpha_1 x}\right) dx, \tag{4.24}$$

và

$$I_2 = \int_0^{\alpha_2/\alpha_1} \frac{1}{(\alpha_2 - \alpha_1 x)^2} \exp \frac{A_1 x^2 - B_1 x + C_1}{(\delta_2 + \alpha_2 - \alpha_1 x)(\alpha_2 - \alpha_1 x)} dx, \tag{4.25}$$

Với A_1, B_1 và C_1 được định nghĩa như sau

$$A_1 = \lambda_e \alpha_1 + \lambda_2 \alpha_1, \tag{4.26}$$

$$B_1 = \lambda_e \alpha_2 + \lambda_e \alpha_1 \delta_2 + \lambda_2 \delta_2 + \lambda_2 \alpha_2, \tag{4.27}$$

$$C_1 = \lambda_e \alpha_2 \delta_2. \tag{4.28}$$

- Xác suất dừng bảo mật của hệ thống

U_1 và U_2 nhận tín hiệu từ S truyền tới, hệ thống sẽ không bảo mật khi hoặc dung lượng bảo mật của U_1 là $C_s^{U_1,SIC}$ hoặc dung lượng bảo mật của U_2 là $C_s^{U_2,SIC}$ nhỏ hơn ngưỡng tốc độ bảo mật của hệ thống. Theo đó, SOP của hệ thống được được định nghĩa như sau

$$\mathcal{O}_{sec}^{SIC} = \Pr\{C_s^{U_1,SIC} < R_1 \; or \; C_s^{U_2,SIC} < R_2\}$$

$$= 1 - \Pr\left\{ B\log_2\left(\frac{1+\gamma_{U_1}}{1+\gamma_{E,1}^{SIC}}\right) > R_1, \right.$$
$$\left. B\log_2\left(\frac{1+\gamma_{U_2}}{1+\gamma_{E,2}^{SIC}}\right) > R_2 \right\}$$
$$= 1 - \int_0^{\rho} \Pr\{|g_1|^2 > F_1(x)\} \Pr\{|g_2|^2 > F_2(x)\} f_{|g_e|^2}(x)dx, \tag{4.29}$$

trong đó $f_{|g_e|^2}(x)$ là hàm PDF của $|g_e|^2$, $\rho = \frac{\beta_2 - \beta_1\delta_2}{\delta_2\beta_1(\beta_1+\beta_2)}$, $\beta_1 = \frac{\alpha_1 P}{N_0}$, $\beta_2 = \frac{\alpha_2 P}{N_0}$, $F_1(x)$ và $F_2(x)$ được định nghĩa như sau

$$F_1(x) = \frac{\delta_1}{\beta_1} + (\delta_1 + 1)x, \tag{4.30}$$
$$F_2(x) = \frac{\delta_2 + [\delta_2(\beta_1+\beta_2) + \beta_2]x}{(\beta_2 - \delta_2\beta_1) - \delta_2\beta_1(\beta_1+\beta_2)x}. \tag{4.31}$$

Sau khi thực hiện một số phép biến đổi toán học, chúng ta nhận được biểu thức $\mathcal{O}_{sec}^{SIC}$ như sau

$$\mathcal{O}_{sec}^{SIC} = 1 - \frac{1}{\Omega_e}\int_0^{\rho} \exp\left(-\frac{F_1(x)}{\Omega_1} - \frac{F_2(x)}{\Omega_2} - \frac{x}{\Omega_e}\right)dx$$
$$= 1 - K\int_0^{\rho} \exp\left(-\frac{-A_2Hx^2 + (A_2G + A_3)x + B_2}{G - Hx}\right)dx, \tag{4.32}$$

trong đó K, A_2, A_3, B_2, G, H được định nghĩa như sau

$$K = \frac{\exp\left(\frac{-\delta_1}{\beta_1\Omega_1}\right)}{\Omega_e}, \tag{4.33}$$
$$A_2 = \frac{(\delta_1+1)\Omega_e + \Omega_1}{\Omega_1\Omega_e}, \tag{4.34}$$
$$A_3 = \frac{\delta_2(\beta_1+\beta_2) + \beta_2}{\Omega_2}, \tag{4.35}$$
$$B_2 = \frac{\delta_2}{\Omega_2}, \tag{4.36}$$
$$G = \beta_2 - \delta_2\beta_1, \tag{4.37}$$
$$H = \delta_2\beta_1(\beta_1+\beta_2). \tag{4.38}$$

4.2.2.2 Xác suất dừng bảo mật trong kịch bản Eve sử dụng kỹ thuật loại bỏ nhiễu PIC

- Xác suất dừng bảo mật của người dùng

Trong kịch bản Eve sử dụng kỹ thuật PIC để loại bỏ nhiễu, SOP của U_1 là $\mathcal{O}_{sec}^{U_1,PIC}$ giống như SOP của U_1 trong kịch bản Eve sử dụng kỹ thuật SIC và được mô tả trong công thức (4.18).

Tiếp theo, dung lượng bảo mật kênh truyền từ S tới U_2 được tính theo công thức sau

$$C_s^{U_2,PIC} = \left\{ B\log_2(1+\gamma_{U_2}) - B\log_2(1+\gamma_{E,2}^{PIC}) \right\}^+. \tag{4.39}$$

Do đó, SOP của U_2 trong kịch bản này được tính bởi công thức sau

$$\begin{aligned}\mathcal{O}_{sec}^{U_2,PIC} &= \Pr\{C_s^{U_2,PIC} < R_2\} = 1 - \Pr\{C_s^{U_2,PIC} > R_2\} \\ &= 1 - \int_0^{\infty} F_{\gamma_{E,2}^{PIC}}\left(\frac{x-\delta_2}{\delta_2+1}\right) f_{\gamma_2}(x).\end{aligned} \tag{4.40}$$

Tương tự như tính SOP của người dùng U_1 ở công thức (4.18), trước tiên chúng ta đi tìm hàm CDF và hàm PDF của $\gamma_{E,2}^{PIC}$ và γ_{U_2} như sau

$$\begin{aligned}F_{\gamma_{E,2}^{PIC}}(x) &= \Pr\{\gamma_{E,2}^{PIC} < x\} = \Pr\left\{ |g_e|^2 < \frac{N_0 x}{\alpha_2 P} \right\} \\ &= 1 - \exp(-\lambda_{e_2} x),\end{aligned} \tag{4.41}$$

trong đó $\lambda_{e_2} = \frac{N_0}{\alpha_2 P \Omega_e}$ và PDF của $f_{\gamma_2}(x)$ được diễn tả trong công thức (4.22). Thay thế công thức (4.22) và (4.41) vào công thức (4.40), biểu thức SOP của người dùng U_2 như sau

$$\mathcal{O}_{sec}^{U_2,PIC} = 1 - \lambda_2 \alpha_2 (I1 - I3), \tag{4.42}$$

trong đó I_1 được định nghĩa trong công thức (4.24) và I_3 được mô tả như sau

$$I_3 = \int_0^{\alpha_2/\alpha_1} \frac{1}{(\alpha_2 - \alpha_1 x)^2} \exp \frac{A_4 x^2 - B_3 x + C_2}{(\delta_2+1)(\alpha_2 - \alpha_1 x)} dx, \tag{4.43}$$

Với A_4, B_3, và C_2 được định nghĩa như sau

$$A_4 = \alpha_1 \lambda_{e_2}, \tag{4.44}$$

$$B_3 = \alpha_2 \lambda_{e_2} + \alpha_1 \delta_2 \lambda_{e_2} + \lambda_2(\delta_2+1), \tag{4.45}$$

$$C_2 = \alpha_2 \delta_2 \lambda_{e_2}. \tag{4.46}$$

- Xác suất dừng bảo mật của hệ thống

Từ công thức (4.11) và (4.39), SOP của hệ thống trong trường hợp Eve sử dụng kỹ thuật PIC được định nghĩa như sau

$$\begin{aligned}\mathcal{O}_{sec}^{PIC} &= \Pr\{C_s^{U_1,PIC} < R_1 \; or \; C_s^{U_2,PIC} < R_2\} \\ &= 1 - \Pr\left\{ B\log_2\left(\frac{1+\gamma_{U_1}}{1+\gamma_{E,1}^{PIC}}\right) > R_1, \right. \\ &\qquad \left. B\log_2\left(\frac{1+\gamma_{U_2}}{1+\gamma_{E,2}^{PIC}}\right) > R_2 \right\} \\ &= 1 - \int_0^{\epsilon} \Pr\{|g_1|^2 > F_1(x)\} \\ &\qquad \times \Pr\{|g_2|^2 > F_3(x)\} f_{|g_e|^2}(x)dx \\ &= 1 - \frac{1}{\Omega_e}\int_0^{\epsilon} \exp\left(-\frac{F_1(x)}{\Omega_1} - \frac{F_3(x)}{\Omega_2} - \frac{x}{\Omega_e}\right)dx, \end{aligned} \tag{4.47}$$

trong đó ϵ và $F_3(x)$ được xác định bởi công thức sau

$$F_3(x) = \frac{\delta_2 + (\delta_2+1)\beta_2 x}{\beta_2 - \beta_1\delta_2 - \beta_1\beta_2(\delta_2+1)x}, \tag{4.48}$$

$$\epsilon = \frac{\beta_2 - \beta_1\delta_2}{\beta_1\beta_2(\delta_2+1)}. \tag{4.49}$$

Sau một vài phép biến đổi toán học, $\mathcal{O}_{sec}^{PIC}$ có dạng như sau

$$\mathcal{O}_{sec}^{PIC} = 1 - K\int_0^{\epsilon} \exp(\psi)dx, \tag{4.50}$$

trong đó ψ, A_5, A_6, J được định nghĩa như sau

$$\psi = \frac{-A_5Hx^2 + (A_6 + A_2G)x + B_2}{Jx - G}, \tag{4.51}$$

$$A_5 = \frac{(\delta_2+1)\lambda_2}{\Omega_2}, \tag{4.52}$$

$$A_6 = \frac{(\delta_2+1)\beta_2}{\Omega_2}, \tag{4.53}$$

$$J = \beta_1\beta_2(\delta_2+1). \tag{4.54}$$

4.2.3 Hiệu năng bảo mật trong kịch bản Eve có nhiều ăng-ten

Trong phần này, luận án đánh giá hiệu năng bảo mật của hệ thống trong trường hợp Eve được trang bị nhiều ăng-ten và giả định kênh truyền trên các ăng-ten đều là các kênh fading có phân bố độc lập và giống nhau.

4.2.3.1 Xác suất dừng bảo mật hệ thống trong kịch bản Eve sử dụng kỹ thuật loại bỏ nhiễu SIC

Từ công thức (4.11) và (4.12), dung lượng bảo mật cho tín hiệu s_1 và s_2 tại ăng-ten thứ j của Eve được diễn tả như sau

$$C_s^{U_1(j),SIC} = \left\{ B\log_2\left(1+\gamma_{U_1}\right) - B\log_2\left(1+\gamma_{E,1(j)}^{SIC}\right)\right\}^+, \tag{4.55}$$

$$C_s^{U_2(j),SIC} = \left\{ B\log_2\left(1+\gamma_{U_2}\right) - B\log_2\left(1+\gamma_{E,2(j)}^{SIC}\right)\right\}^+, \tag{4.56}$$

trong đó $j \in \{1,2,..,N\}$. Do đó, xác suất dừng bảo mật xảy ra khi dung lượng bảo mật nhỏ nhất của U_1 hoặc của U_2 nhỏ hơn ngưỡng tốc độ bảo mật tương ứng. Xuất phát từ định nghĩa này, SOP diễn tả như sau

$$\mathcal{O}_{sec}^{(N,SIC)} = \Pr\left\{ \min_{j\in\{1,2,\ldots,N_p\}} \left\{ C_s^{U_1(j),SIC}\right\} < R_1 \right.$$
$$\left. \text{or} \min_{j\in\{1,2,\ldots,N_p\}} \left\{ C_s^{U_2(j),SIC}\right\} < R_2 \right\}. \tag{4.57}$$

$$= 1 - \Pr\left\{ Blog_2\left(\frac{1+\gamma_{U_1}}{1+\max\limits_{i\in\{1,2,\ldots,N_p\}}\gamma_{E,1(i)}^{SIC}}\right) > R_1 \right. \tag{4.58}$$
$$\left. \cap\ Blog_2\left(\frac{1+\gamma_{U_2}}{1+\max\limits_{i\in\{1,2,\ldots,N_p\}}\gamma_{E,2(i)}^{SIC}}\right) > R_2 \right\}$$

$$= 1 - \int_0^{\rho} \Pr\{|g_1|^2 > F_1(x)\Pr\{|g_2|^2 > F_2(x) f_{|g_{e,i^*}|^2}(x)dx \tag{4.59}$$

Sau một số phép biến đổi toán học, biểu thức $\mathcal{O}_{sec}^{(N,SIC)}$ có dạng như sau

$$\mathcal{O}_{sec}^{(N,SIC)} = 1 - \int_0^{\rho} \exp\left[-\frac{F_1(x)}{\Omega_1} - \frac{F_2(x)}{\Omega_2}\right] f_{|g_{e,i^*}|^2}(x)dx, \tag{4.60}$$

trong đó $|g_{e,i^*}|^2 = \max\limits_{j\in\{1,2,\ldots,N_p\}}\{|g_{e(j)}|^2\}$, $f_{|g_{e,i^*}|^2}$ là hàm PDF của $|g_{e,i^*}|^2$, $F_1(x)$ và $F_2(x)$ được định nghĩa trong công thức (4.30), (4.31) tương ứng. Để tính công thức (4.60), chúng ta cần tìm hàm CDF và hàm PDF của $|g_{e,i^*}|^2$. Trước tiên chúng ta tìm hàm CDF của $|g_{e,i^*}|^2$ theo công thưc sau

$$\begin{aligned} F_{|g_{e,i^*}|^2}(x) &= \Pr\left\{\max_{j\in\{1,2,\ldots,N_p\}}\left\{|g_{e(j)}|^2\right\} < x\right\} \\ &= \prod_{j=1}^{N}\Pr\left\{|g_{e(j)}|^2 < x\right\} \\ &= \prod_{j=1}^{N}\left[1-\exp\left(-\frac{x}{\Omega_{e(j)}}\right)\right]. \end{aligned} \tag{4.61}$$

Ở đây, chúng ta giả thiết rằng tất cả các ăng-ten có độ lợi kênh truyền là giống nhau, tức là $\Omega_{e(1)} = \Omega_{e(2)} = \cdots = \Omega_{e(N)} = \Omega_e$ [42]. Vì vậy công thức (4.61) được viết lại như sau

$$F_{|g_{e,i^*}|^2}(x) = \left[1-\exp\left(-\frac{x}{\Omega_e}\right)\right]^N. \tag{4.62}$$

Thực hiện phép toán vi phân (4.62) theo x, hàm PDF của $|g_{e,i^*}|^2$ như sau

$$\begin{aligned} f_{|g_{e,i^*}|^2}(x) &= \frac{N}{\Omega_e}\exp\left(-\frac{x}{\Omega_e}\right)\left[1-\exp\left(-\frac{x}{\Omega_e}\right)\right]^{(N-1)} \\ &= \frac{N}{\Omega_e}\exp\left(-\frac{x}{\Omega_e}\right)\sum_{k=0}^{N-1}C_k^{N-1}\left[-\exp\left(-\frac{x}{\Omega_e}\right)\right]^k. \end{aligned} \tag{4.63}$$

Thay thế công thức (4.63) vào công thức (4.60), SOP của hệ thống được viết lại như sau

$$\mathcal{O}_{sec}^{(N,SIC)} = 1 - N*K\int_0^{\rho}\exp(\chi)\nu dx, \tag{4.64}$$

trong đó χ và ν được tính bởi các công thức như sau

$$\chi = \left[-\frac{-A_2Hx^2+(A_2G+A_3)x+B_2}{G-Hx}\right], \tag{4.65}$$

$$\nu = \sum_{k=0}^{N-1}C_k^{N-1}\left[-\exp\left(-\frac{kx}{\Omega_e}\right)\right]. \tag{4.66}$$

4.2.3.2 Xác suất dừng bảo mật hệ thống trong kịch bản Eve sử dụng kỹ thuật loại bỏ nhiễu PIC

Giống như kịch bản Eve sử dụng kỹ thuật xử lý tín hiệu SIC, dung lượng bảo mật của tín hiệu s_1 và s_2 tại ăng-ten thứ i của Eve trong kịch bản này được diễn tả bởi công thức sau

$$C_s^{U_1(j),PIC} = \left\{ B\log_2(1+\gamma_{U_1}) - B\log_2\left(1+\gamma_{E,1(j)}^{PIC}\right)\right\}^+, \tag{4.67}$$

$$C_s^{U_2(j),PIC} = \left\{ B\log_2(1+\gamma_{U_2}) - B\log_2\left(1+\gamma_{E,2(j)}^{PIC}\right)\right\}^+. \tag{4.68}$$

Do đó, SOP của hệ thống được tính như sau

$$\mathcal{O}_{sec}^{(N,PIC)} = \Pr\left\{ \min_{j\in\{1,2,\ldots,N_p\}} \left\{ C_s^{U_1(j),PIC}\right\} < R_1 \right. \tag{4.69}$$

$$\left. \text{or} \min_{j\in\{1,2,\ldots,N_p\}} \left\{ C_s^{U_2(j),PIC}\right\} < R_2 \right\}.$$

$$= 1 - \Pr\left\{ Blog_2\left(\frac{1+\gamma_{U_1}}{1+\max\limits_{i\in\{1,2,\ldots,N_p\}}\gamma_{E,1(i)}^{PIC}}\right) > R_1 \right. \tag{4.70}$$

$$\left. \cap\ Blog_2\left(\frac{1+\gamma_{U_2}}{1+\max\limits_{i\in\{1,2,\ldots,N_p\}}\gamma_{E,2(i)}^{PIC}}\right) > R_2 \right\}$$

$$= 1 - \int_0^{\rho} \Pr\{|g_1|^2 > F_1(x)\}\Pr\{|g_2|^2 > F_3(x)\} f_{|g_{e,i^*}|^2}(x)dx \tag{4.71}$$

Sau một số thao tác biến đổi toán học, chúng ta nhận được biểu thức $\mathcal{O}_{sec}^{(N,PIC)}$ như sau

$$\mathcal{O}_{sec}^{(N,PIC)} = 1 - N * K \int_0^{\epsilon} \exp(\pi)\nu dx, \tag{4.72}$$

trong đó $F_3(x)$ được tính theo công thức (4.48) và

$$\pi = \frac{-A_5Hx^2 + (A_6 + A_2G)x + B_2}{Jx - G}.$$

4.2.4 Phân tích xác suất rớt gói tin

Trong các phần tiếp theo, luận án thực hiện tính xác suất rớt gói tin, thời gian truyền tin trung bình tới từng người dùng mà không phụ thuộc vào Eve sử dụng

kỹ thuật xử lý tín hiệu nào bởi vì Eve hoạt động ở chế độ thụ động và không ảnh hưởng tới đốc độ truyền gói tin. Lưu ý rằng S cần truyền mỗi gói tin tới U_1 và U_2 với lượng tin chuẩn hóa theo băng thông $\tilde{B}$ (nats/Hz) và trong khoảng thời gian quy định t_{out}. Ký hiệu T_j $(j \in \{1,2\})$ là thời gian để truyền một gói tin từ S tới U_j (bao gồm cả gói tin bị rớt). Theo [71], thời gian để truyền một gói tin tới U_j có biểu thức như sau

$$T_j = \frac{\tilde{B}}{\log_e(1+\gamma_j)}, \tag{4.73}$$

trong đó γ_j được định nghĩa trong công thức (4.5) và (4.6).

Với điều kiện kênh truyền cho trước, xác suất rớt gói tin $\mathcal{O}_{otm}$ là xác suất mà thời gian truyền gói tin T_j vượt quá khoảng thời gian quy định t_{out}, có nghĩa là

$$\mathcal{O}_{otm}^{(j)} = \Pr\{T_j \geq t_{out}\}. \tag{4.74}$$

Do đó, xác suất rớt gói tin tới $\mathcal{O}_{otm}^{(1)}$ được tính như sau

$$\mathcal{O}_{otm}^{(1)} = \Pr\{T_1 \geq t_{out}\} = 1 - F_{T_1}(t_{out}). \tag{4.75}$$

Để giải phương trình (4.75), chúng ta tính hàm CDF và PDF của T_1. Đầu tiên, chúng ta sử dụng phân bố mũ để tính CDF của T_1 như sau

$$F_{T_1}(t) = \Pr\{T_1 < t\} = \exp\left\{-\lambda_1\left[\exp\left(\frac{\tilde{B}}{t}\right) - 1\right]\right\}. \tag{4.76}$$

Hàm PDF của T_1 được tính bằng cách vi phân phương trình (4.76) theo t như sau

$$f_{T_1}(t) = \frac{\tilde{B}\lambda_1}{t^2}\exp\left\{\frac{\tilde{B}}{t} - \lambda_1\left[\exp\left(\frac{\tilde{B}}{t}\right) - 1\right]\right\}. \tag{4.77}$$

Thực hiện phép thế công thức (4.76) vào (4.75), xác suất rớt gói tin U_1 diễn tả là

$$\mathcal{O}_{otm}^{(1)} = 1 - \exp\left\{-\lambda_1\left[\exp\left(\frac{\tilde{B}}{t_{out}}\right) - 1\right]\right\}. \tag{4.78}$$

Mặt khác, ký hiệu $T_{suc}^{(1)}$ là thời gian truyền của một gói tin thành công [69], chúng ta có

$$T_{suc}^{(1)} = \{T_1 | T_1 < t_{out}\}. \tag{4.79}$$

Áp dụng công thức Bayes, xác suất xảy ra sự kiện $T_{suc}^{(1)}$ được mô tả bởi công thức sau

$$\Pr\{T_1|T_1 < t_{out}\} = \frac{\Pr\{T_1, T_1 < t_{out}\}}{\Pr\{T_1 < t_{out}\}}. \tag{4.80}$$

Vì vậy, hàm CDF của $T_{suc}^{(1)}$ sẽ như sau:

$$F_{T_{suc}^{(1)}}(x) = \begin{cases} \frac{1}{1-\mathcal{O}_{otm}^{(1)}} \int_0^{t_{out}} f_{T_1}(t)dt & \text{, if } 0 \leq t < t_{out} \\ 0 & \text{, if } t \geq t_{out}. \end{cases} \tag{4.81}$$

Thực hiện phép toán vi phân hai vế của công thức (4.81) theo x, hàm PDF của gói tin được truyền thành công sẽ như sau

$$f_{T_{suc}^{(1)}}(t) = \begin{cases} \frac{f_{T_1}(t)}{1-\mathcal{O}_{otm}^{(1)}} & \text{, if } 0 \leq t < t_{out} \\ 0 & \text{, if } t \geq t_{out}. \end{cases} \tag{4.82}$$

Thay thế công thức (4.77) vào công thức (4.82), hàm PDF $f_{T_{suc}^{(1)}}(t)$ được viết lại như sau

$$f_{T_{suc}^{(1)}}(t) = \begin{cases} \frac{\tilde{B}\lambda_1}{\left(1-P_{out}^{(1)}\right)t^2} \exp\left[\frac{\tilde{B}}{t} - \lambda_1(\exp\left(\frac{\tilde{B}}{t}\right) - 1)\right] & \\ & \text{, if } 0 \leq t < t_{out} \\ 0 & \text{, if } t \geq t_{out}. \end{cases} \tag{4.83}$$

Tương tự như $\mathcal{O}_{otm}^{(1)}$, xác suất rớt gói tin $\mathcal{O}_{otm}^{(2)}$ từ S tới người dùng U_2 được diễn tả là

$$\begin{aligned} \mathcal{O}_{otm}^{(2)} &= \Pr\{T_2 \geq t_{out}\} \\ &= 1 - F_{T2}(t_{out}). \end{aligned} \tag{4.84}$$

Để giải phương trình (4.84), chúng ta lần lượt tìm hàm CDF và PDF của T_2. Hàm CDF của T_2 được tính toán như sau

$$\begin{aligned} F_{T_2}(t) &= \Pr\{T_2 < t\} \\ &= 1 - F_{T_2}\left[\exp\left(\frac{\tilde{B}}{t}\right) - 1\right]. \end{aligned} \tag{4.85}$$

Tương tự cách tính hàm CDF của T_1, chúng ta có

$$F_{T_2}(t) = \begin{cases} \exp(M) & \text{, if } t > \frac{\tilde{B}}{\log_e\left(\frac{1}{\alpha_1}\right)} \\ 1 & \text{, if } t \leq \frac{\tilde{B}}{\log_e\left(\frac{1}{\alpha_1}\right)}, \end{cases} \tag{4.86}$$

trong đó $M = \frac{-\lambda_2\left[\exp\left(\frac{\tilde{B}}{t}\right)-1\right]}{\left(1-\alpha_1\exp\left(\frac{\tilde{B}}{t}\right)\right)}$. Hàm PDF của T_2 được tính bằng cách thực hiện phép tính vi phân phương trình (4.86) theo t như sau

$$f_{T_2}(t) = \begin{cases} \frac{\exp(M+\frac{B}{t})\lambda_2\alpha_2\tilde{B}}{t^2\left(1-\alpha_1\exp\left(\frac{\tilde{B}}{t}\right)\right)^2} & \text{, if } t > \frac{\tilde{B}}{\log_e\left(\frac{1}{\alpha_1}\right)} \\ 0 & \text{, if } t \leq \frac{\tilde{B}}{\log_e\left(\frac{1}{\alpha_1}\right)}. \end{cases} \tag{4.87}$$

Thay thế công thức (4.86) vào (4.84), chúng ta nhận được biểu thức xác suất rớt gói tin đến U_2 như sau

$$\mathcal{O}_{otm}^{(2)} = \begin{cases} 1 - \exp\left\{\frac{\lambda_2\left[\exp\left(\frac{\tilde{B}}{t_{out}}\right)-1\right]}{1-\alpha_1\exp\left(\frac{\tilde{B}}{t_{out}}\right)}\right\} \\ \qquad\qquad \text{, if } t_{out} > \frac{\tilde{B}}{\log_e\left(\frac{1}{\alpha_1}\right)} \\ 0 \qquad\qquad \text{, if } t_{out} \leq \frac{\tilde{B}}{\log_e\left(\frac{1}{\alpha_1}\right)}. \end{cases} \tag{4.88}$$

Mặt khác, ký hiệu $T_{suc}^{(2)}$ là thời gian truyền gói tin thành công, $T_{suc}^{(2)}$ được tính như sau

$$T_{suc}^{(2)} = \{T_2 | T_2 < t_{out}\}. \tag{4.89}$$

Thực hiện phép biến đổi tương tự từ công thức (4.81) và (4.82), hàm CDF và PDF của $T_{suc}^{(2)}$ được tính như sau

$$F_{T_{suc}^{(2)}}(x) = \begin{cases} \frac{1}{1-\mathcal{O}_{otm}^{(2)}} \int_0^{t_{out}} f_{T_2}(t)dt & \text{, if } 0 \leq t < t_{out} \\ 0 & \text{, if } t \geq t_{out}, \end{cases} \tag{4.90}$$

$$f_{T_{suc}^{(2)}}(t) = \begin{cases} \frac{f_{T_2}(t)}{1-\mathcal{O}_{otm}^{(2)}} & \text{, if } 0 \leq t < t_{out} \\ 0 & \text{, if } t \geq t_{out}. \end{cases} \tag{4.91}$$

Thay thế công thức (4.87) vào công thức (4.91), hàm PDF của thời gian truyền gói tin không bị dừng được viết lại như sau

$$f_{T_{suc}^{(2)}}(t) = \begin{cases} \frac{\lambda_2 \alpha_2 \tilde{B}}{1-\mathcal{O}_{otm}^{(2)}} \frac{I_4}{t^2\left[1-\alpha_1 \exp\left(\frac{\tilde{B}}{t}\right)\right]^2} \\ \qquad\qquad , \text{if } 0 \leq t < t_{out} \\ 0 \qquad\qquad , \text{if } t \geq t_{out} \end{cases}, \tag{4.92}$$

trong đó $I_4 = \exp\left\{\frac{\tilde{B}}{t} - \frac{\lambda_2\left[\exp\left(\frac{\tilde{B}}{t}\right)-1\right]}{1-\alpha_1 \exp\left(\frac{\tilde{B}}{t}\right)}\right\}$.

4.2.5 Thời gian truyền gói tin trung bình

Thời gian truyền gói tin trung bình là thời gian để truyền một gói tin từ nguồn S tới người dùng (bao gồm cả các gói tin rớt tức truyền không thành công).

- Thời gian truyền tin trung bình từ S tới U_1

Thời gian truyền gói tin trung bình không bị dừng là

$$E[T_{suc}^{(1)}] = \int_0^{t_{out}} t f_{T_{suc}^{(1)}}(t) dt. \tag{4.93}$$

Thay thế công thức (4.77) vào công thức (4.93), chúng ta có moment bậc nhất của thời gian truyền gói tin từ S tới U_1 không bị rớt như sau

$$E[T_{suc}^{(1)}] = \int_0^{t_{out}} \frac{\lambda_1 \tilde{B}}{1-P_{out}^{(1)}} \frac{1}{t} \times \exp\left\{\frac{\tilde{B}}{t} - \lambda_1\left[\exp\left(\frac{\tilde{B}}{t}\right) - 1\right]\right\} dt. \tag{4.94}$$

Cuối cùng, áp dụng luật tổng kỳ vọng, moment bậc nhất của T_1 (bao gồm cả gói tin bị rớt) được tính như sau

$$E[T_1] = (1-\mathcal{O}_{otm}^{(1)})E[T_{suc}^{(1)}] + t_{out}\mathcal{O}_{otm}^{(1)}, \tag{4.95}$$

trong đó $\mathcal{O}_{otm}^{(1)}$ và $E[T_{suc}^{(1)}]$ tính theo công thức (4.78) và (4.94) tương ứng.

- Thời gian truyền tin trung bình từ S tới U_2

Tương tự như cách tính $E[T_{suc}^{(1)}]$, moment bậc nhất của thời gian truyền gói tin từ S tới U_2 không bị rớt như sau:

$$E[T_{suc}^{(2)}] = \int_{\epsilon}^{t_{out}} t f_{T_{suc}^{(2)}}(t) dt$$
$$= \frac{\lambda_2 \alpha_2 \tilde{B}}{1 - \mathcal{O}_{otm}^{(2)}} \int_{\epsilon}^{t_{out}} \frac{1}{t} \frac{I_5}{\left[1 - \alpha_1 \exp\left(\frac{\tilde{B}}{t}\right)\right]^2} dt, \tag{4.96}$$

trong đó $\epsilon = \tilde{B} / \log_e\left(\frac{1}{\alpha_1}\right)$ và I_5 được định nghĩa như sau

$$I_5 = \exp\left[\frac{\tilde{B}}{t} - \frac{\lambda_2(\exp\left(\frac{\tilde{B}}{t}\right) - 1)}{1 - \alpha_1 \exp\left(\frac{\tilde{B}}{t}\right)}\right]. \tag{4.97}$$

Cuối cùng, chúng ta có mô men bậc nhất của thời gian truyền gói tin T_2 (bao gồm cả gói tin bị rớt) bằng cách sử dụng luật tổng kỳ vọng như sau:

$$E[T_2] = (1 - \mathcal{O}_{otm}^{(2)}) E[T_{suc}^{(2)}] + t_{out} \mathcal{O}_{otm}^{(2)}, \tag{4.98}$$

trong đó $\mathcal{O}_{otm}^{(2)}$ và $E[T_{suc}^{(2)}]$ được mô tả bởi công thức (4.88) và (4.96) tương ứng.

4.2.6 Tính công bằng về thời gian truyền tin

Trong phần này, luận án phân tích vấn đề tối ưu việc phân bổ công suất cho mỗi người dùng để đảm bảo thời gian truyền gói tin trung bình $E[T_1]$ từ S tới U_1 bằng với thời gian trung bình $E[T_2]$ từ S tới U_2. Vấn đề này được biểu diễn bằng công thức sau đây

$$\alpha_1^* = \arg \min_{0 < \alpha_1 < 0.5} |E[T_1] - E[T_2]|, \tag{4.99}$$

trong đó α_1^* hệ số phân bổ công suất thỏa mãn điều kiện sự chênh lệch giữa thời gian truyền gói tin trung bình từ S tới U_1 và U_2 là nhỏ nhất. Để giải quyết vấn đề này, luận án đề xuất thuật toán **Algorithm 1** để tìm hệ số phân bổ công suất α_1^* với độ chính xác cho trước như sau

4.2.7 Mô phỏng và phân tích kết quả

Trong phần này, luận án trình bày các kết quả phân tích và mô phỏng để đánh giá hiệu năng bảo mật, hiệu suất của hệ thống và tính công bằng trong truyền tin

Algorithm 1 Thuật toán tìm hệ số phân bổ công suất α_1^*

$\alpha_1 \leftarrow$giá trị tùy ý ($0 < \alpha_1 < 0.5$)
while $abs(E[T_1] - E[T_2]) > \nu$ **do**
    $\alpha_2 \leftarrow 1 - \alpha_1$
    Tính $E[T_1]$ sử dụng công thức (4.95)
    Tính $E[T_2]$ sử dụng công thức (4.98)
    $\alpha_1 \leftarrow \alpha_1 + \zeta$
end while
$\alpha_1^* \leftarrow \alpha_1 - \zeta$
return α_1^*

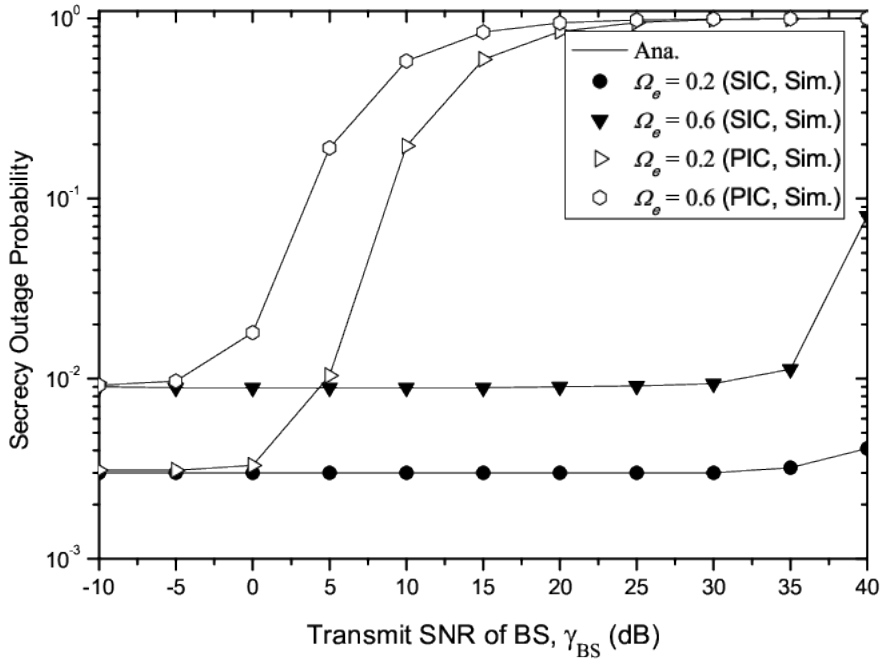
trong đó ν là độ chính xác mong muốn và ζ là bước tăng.

của từng cặp người dùng trong hệ thống. Các tham số dùng để thử nghiệm dưới đây đã được dùng phổ biến trong rất nhiều các nghiên cứu ở lĩnh vực này. Các tham số của hệ thống được thiết lập như sau

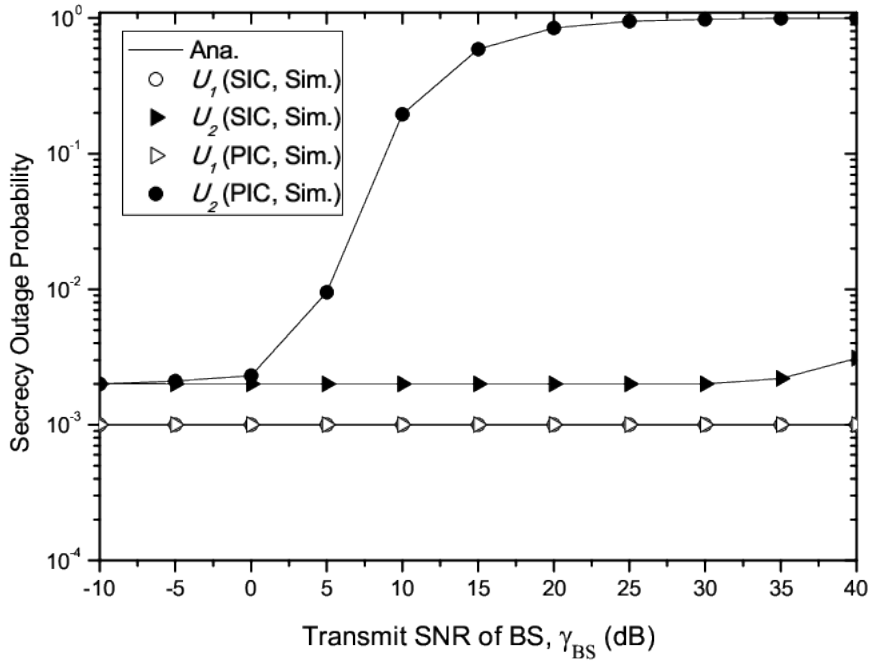
- SNR của S: $\gamma_{BS} = P/N_0$
- Băng thông hệ thống: W = 5 MHz
- Kích thước gói tin: L = 4096 bits (512 bytes)
- Thời gian truyền tin: $t_{out} = 10^{-3}s$
- Ngưỡng tốc độ bảo mật của U_1, U_2: $R_1 = R_2$ = 1000 Kbps

Hình 4.2 minh họa tác động của công suất truyền SNR của S lên SOP với cả trường hợp Eve sử dụng SIC và PIC. Chúng ta thấy rằng SOP trong kịch bản Eve sử dụng SIC thấp hơn so với kịch bản Eve sử dụng PIC trên toàn bộ miền công suất phát của S. Nguyên nhân là do Eve sử dụng kỹ thuật PIC thì có thể giải mã tín hiệu đồng thời của nhiều người dùng trong tín hiệu kết hợp từ S truyền tới. Hơn nữa, SOP tăng khi SNR của S tăng trong cả hai kịch bản SIC và PIC. Bởi vì thực tế dung lượng bảo mật giảm khi Eve nghe lén được tín hiệu có công suất lớn hơn từ S.

Hình 4.3 mô tả ảnh hưởng của công suất truyền tin SNR lên SOP cho cả kịch bản SIC và PIC. Chúng ta quan sát thấy rằng SOP của U_1 trong cả hai kịch bản



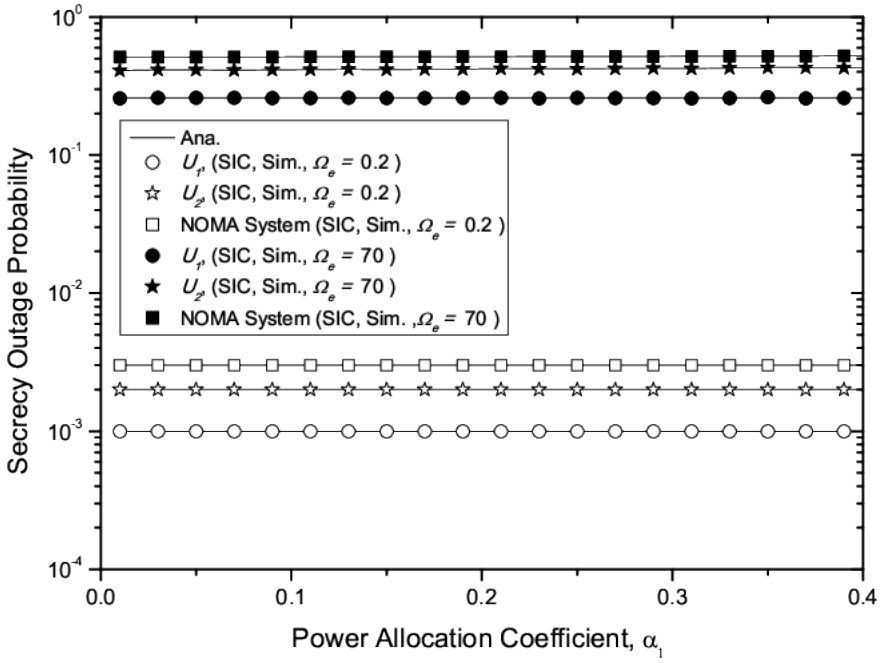
Hình 4.2: *SOP của hệ thống theo tập giá trị SNR trong kịch bản Eve sử dụng kỹ thuật loại bỏ nhiễu SIC và PIC với* $\Omega_1 = 200, \Omega_2 = 100$, *và* $\alpha_1 = 0.3$.



Hình 4.3: *SOP của* U_1 *và* U_2 *theo tập giá trị SNR trong kịch bản Eve sử dụng kỹ thuật loại bỏ nhiễu SIC và PIC với* $\Omega_1 = 200, \Omega_2 = 100, \Omega_e = 0.2$, *và* $\alpha_1 = 0.3$.

SIC và PIC là giống nhau và là hằng số khi SNR tăng. Điều này xảy ra bởi vì SNR tồn tại ở cả tử số và mẫu số trong công thức dung lượng bảo mật của U_1 (4.11) (công thức dung lượng bảo mật được viết lại như sau $B \log_2 \left(\frac{1+\alpha_1 \gamma_{BS} |g_1|^2}{1+\alpha_1 \gamma_{BS} |g_e|^2} \right)$ với

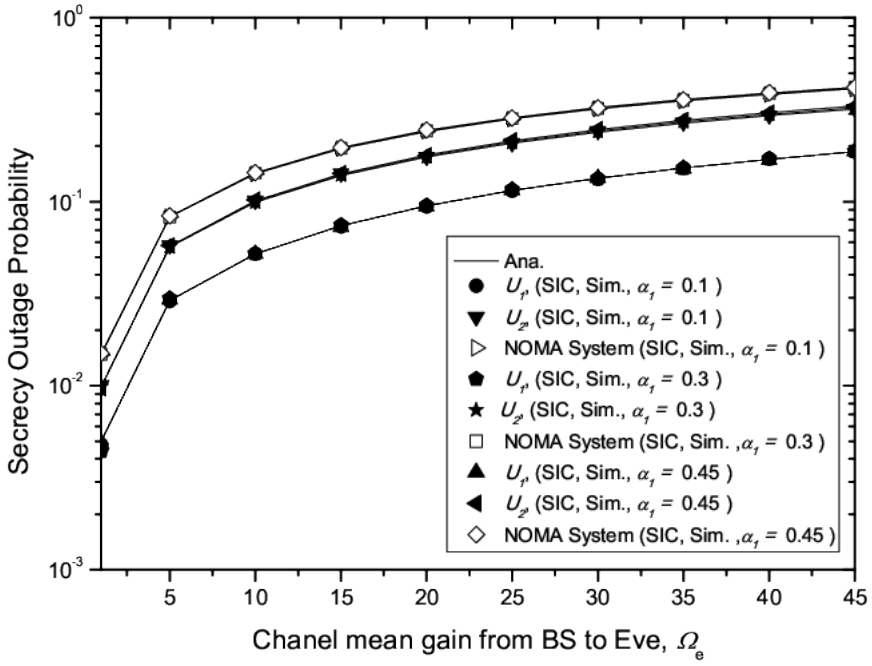
$\gamma_{BS} = P/N_0$). Vì vậy, khi công suất truyền SNR tăng, cả tử số và mẫu số đồng thời tăng. Điều đó có nghĩa rằng dung lượng bảo mật của U_1 không thay đổi, tức là U_1 có xác suất dừng bảo mật xấp xỉ là hằng số. Hơn nữa, SOP của U_2 đối với cả hai kịch bản SIC và PIC đều tăng khi công suất truyền SNR tăng. Nguyên nhân của hiện tượng này đã được thảo luận trong Hình 4.2, dung lượng bảo mật của kênh truyền sẽ giảm đi khi Eve nhận được tín hiệu có công suất mạnh hơn từ S. Ngoài ra, SOP của U_2 trong kịch bản PIC cao hơn so với SOP trong kịch bản SIC. Điều này là do Eve với kịch bản sử dụng PIC có khả năng giải mã tín hiệu đồng thời của nhiều người dùng một lúc trong tín hiệu hỗn hợp mà Eve nghe lén được.



Hình 4.4: *SOP của hệ thống theo miền giá trị của hệ số phân bổ công suất α_1 trong kịch bản Eve sử dụng kỹ thuật SIC với $\Omega_1 = 200, \Omega_2 = 100, \Omega_e = 0.2$, và SNR = 10 dB.*

Hình 4.4 mô tả SOP của U_1, U_2 và hệ thống như là hàm số của hệ số α_1 trong kịch bản Eve sử dụng kỹ thuật SIC. Chúng ta có thể thấy rằng, thay đổi giá trị của hệ số phân bổ công suất ít ảnh hưởng đến SOP của U_1, U_2, và toàn hệ thống. Hiện tượng này có thể giải thích như sau, trong trường hợp này U_1, U_2, và Eve sử dụng kỹ thuật SIC và khi α_1 tăng thì SINR của tín hiệu x_1 tại U_1 và Eve đồng thời tăng trong khi đó SINR của tín hiệu x_2 tại U_2 và Eve đồng thời giảm. Chính vì vậy, dung lượng bảo mật của tín hiệu x_1 và x_2 không thay đổi khi α_1 tăng. Kết luận cũng được kiểm chứng lại lần nữa trên Hình 4.5.

Hình 4.5 thể hiện SOP của U_1, U_2 và của hệ thống so với độ lợi kênh truyền

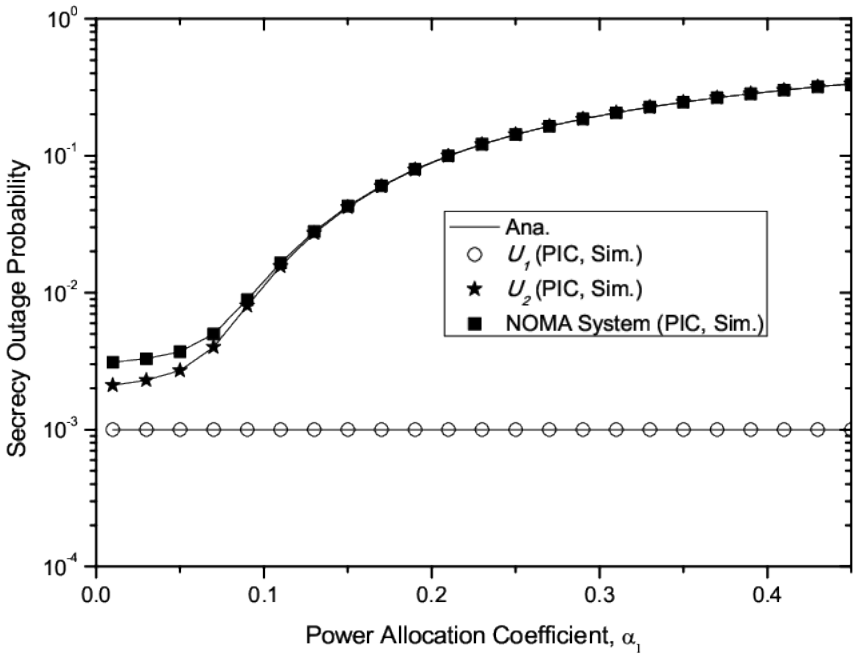


Hình 4.5: *SOP của hệ thống theo miền giá trị độ lợi kênh truyền trong kịch bản Eve sử dụng kỹ thuật SIC với* $\Omega_1 = 200, \Omega_2 = 100$, *và SNR = 10 dB.*

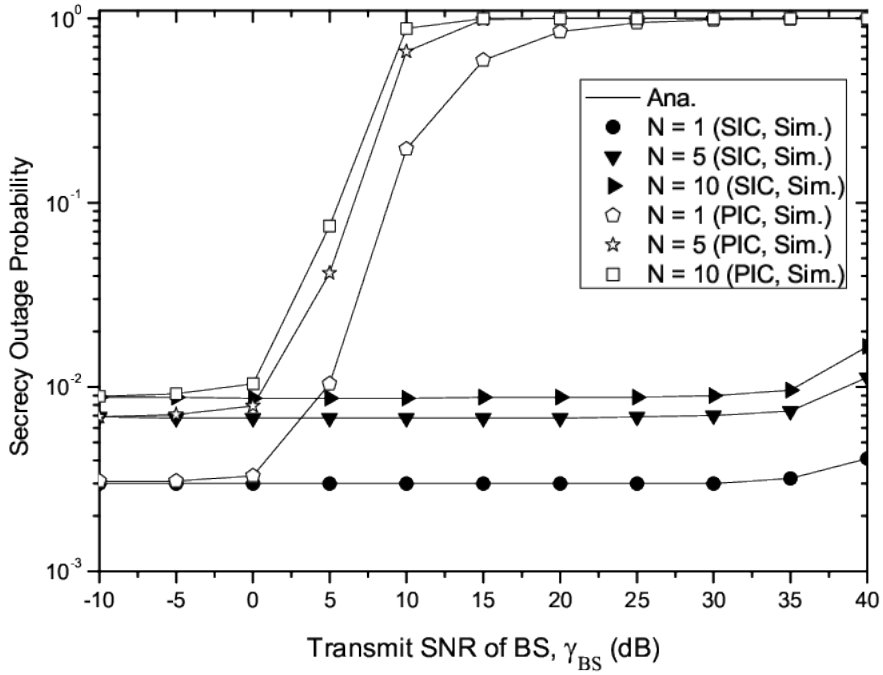
của Eve trong kịch bản Eve sử dụng kỹ thuật SIC. Chúng ta quan sát thấy rằng khi tăng độ lợi kênh truyền Ω_e thì SOP của cả U_1, U_2 và hệ thống tăng lên. Điều này do khi Ω_e tăng có nghĩa là Eve gần S hơn nên Eve có thể giải mã tín hiệu tốt hơn, vì vậy SOP của U_1, U_2 và hệ thống giảm. Một quan sát khác chúng ta thấy rằng với các hệ số phân bổ công suất α_1 khác nhau thì các đồ thị đều có hình dáng giống nhau. SOP của cả U_1, U_2 và hệ thống không chịu ảnh hưởng bởi việc thay đổi giá trị của α_1. Điều này được xác nhận trong kết luận trong Hình 4.4.

Hình 4.6 mô tả ảnh hưởng của hệ số phân bổ công suất α_1 lên SOP trong kịch bản Eve sử dụng kỹ thuật PIC. Lưu ý rằng hệ số phân bổ công suất này phải nằm trong miền giá trị từ 0 đến 0.5. Chúng ta thấy rằng SOP của U_2 và hệ thống tăng lên nhanh khi tăng hệ số phân bổ công suất α_1. Bởi vì khi hệ số phân bổ công suất α_1 tăng, SINR của U_2 giảm nhanh hơn SNR tại Eve (căn cứ vào công thức (4.8) và (4.10)) dẫn đến giảm dung lượng bảo mật của U_2. Có nghĩa rằng SOP của U_2 và hệ thống tăng.

Hình 4.7 chỉ ra ảnh hưởng của số lượng ăng-ten của Eve lên SOP hệ thống. Chúng ta thấy rằng SOP hệ thống trong cả hai kịch bản SIC và PIC đều tăng khi số lượng ăng-ten của Eve tăng. Nguyên nhân là do số lượng ăng-ten càng lớn thì độ lợi phân tập tại Eve càng cao.

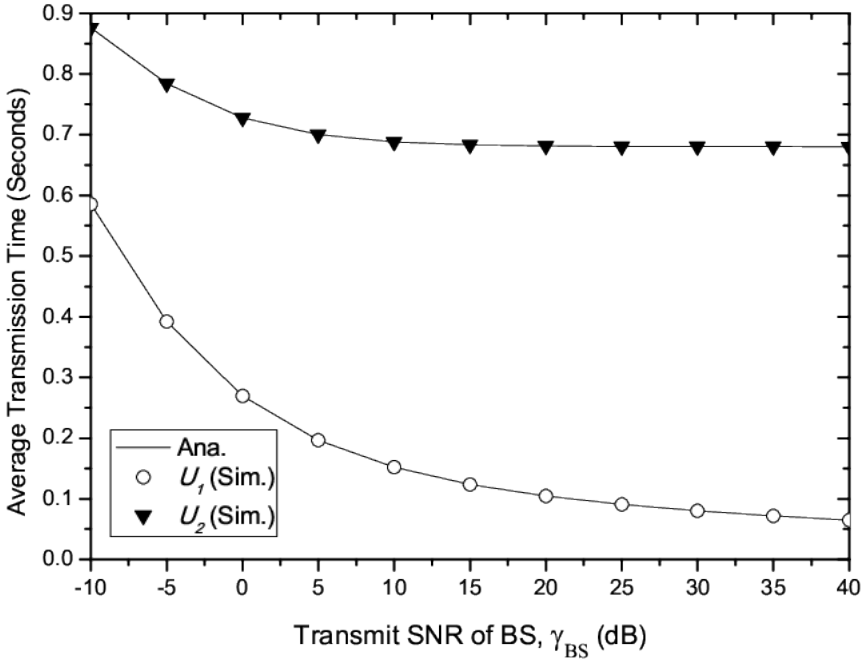


Hình 4.6: *SOP của hệ thống theo tập giá trị của hệ số phân bổ công suất α_1 trong kịch bản Eve sử dụng kỹ thuật PIC với $\Omega_1 = 200, \Omega_2 = 100, \Omega_e = 0.2$, và SNR = 10 dB.*



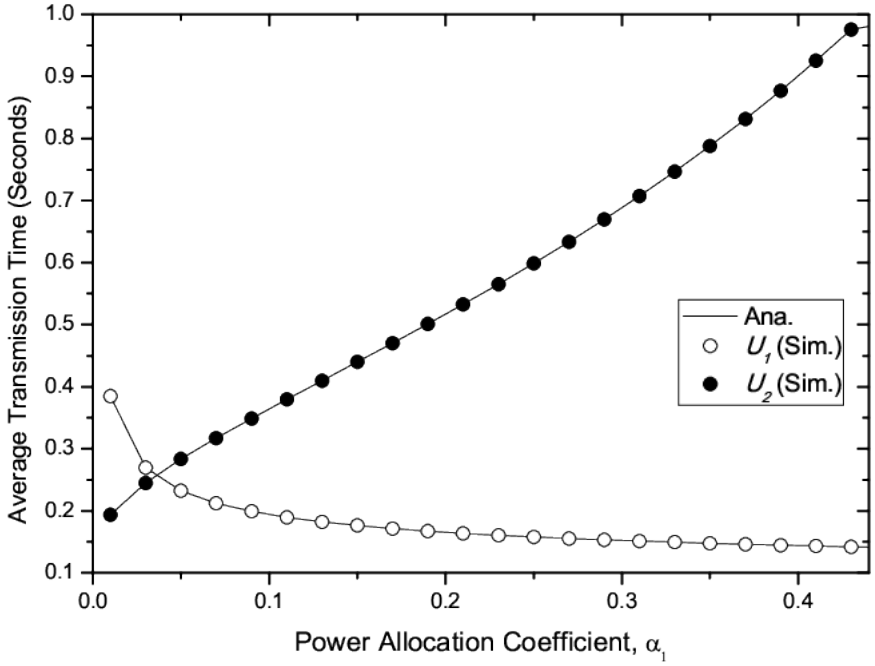
Hình 4.7: *Tác động của số lượng ăng-ten của Eve lên SOP của hệ thống với $\Omega_1 = 200, \Omega_2 = 100, \Omega_e = 2$.*

Hình 4.8 chỉ ra mối quan hệ giữa thời gian truyền gói tin trung bình với công suất truyền tin. Chúng ta thấy rằng thời gian truyền tin trung bình từ S tới U_1 nhỏ hơn thời gian truyền tin S tới U_2. Nguyên nhân là do độ lợi kênh truyền của



Hình 4.8: *Thời gian truyền tin trung bình theo tập giá trị của SNR với* $\Omega_1 = 200, \Omega_2 = 100$, *và* $\alpha_1 = 0.3$.

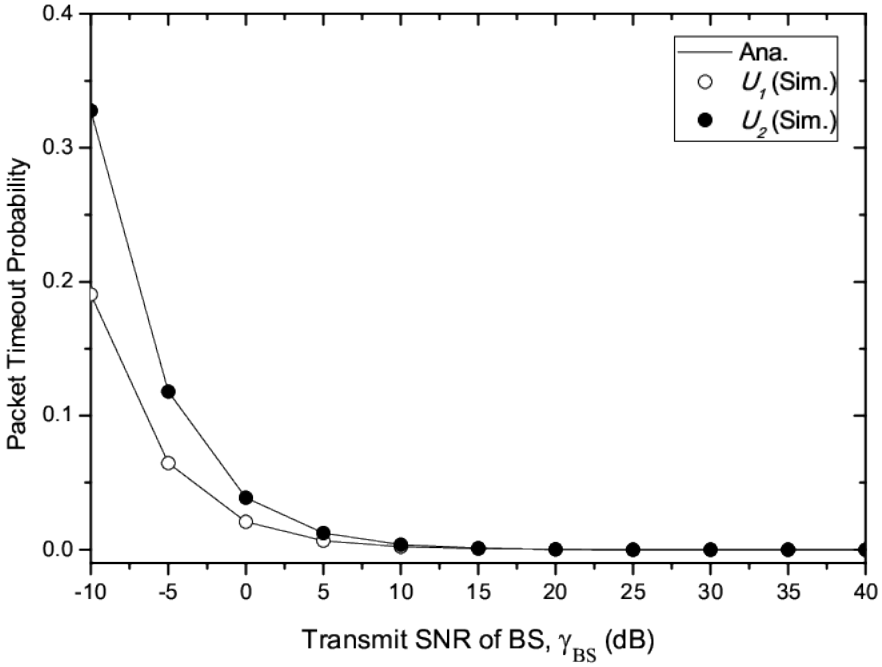
U_1 tốt hơn so với U_2.



Hình 4.9: *Thời gian truyền tin trung bình của* U_1 *và* U_2 *theo tập giá trị của hệ số phân bổ công suất* α_1 *với* $\Omega_1 = 200, \Omega_2 = 100$, *và SNR = 10 dB.*

Hình 4.9 mô tả tác động của hệ số phần bổ công suất α_1 lên thời gian truyền tin trung bình từ S tới U_1 và U_2. Chúng ta quan sát thấy α_1 có thể điều chỉnh để

thời gian truyền trung bình từ S tới U_1 và U_2 là bằng nhau, ký hiệu là α_1^*. Khởi tạo giá trị của α_1 là 10^{-3}, độ chính xác mong muốn $\sigma = 10^{-5}$, bước tăng $\zeta = 10^{-3}$, α_1^* có giá trị xấp xỉ bằng 0.035.



Hình 4.10: *Xác suất rớt gói tin theo tập giá trị của SNR với* $\Omega_1 = 200, \Omega_2 = 100$, *và* $\alpha_1 = 0.3$..

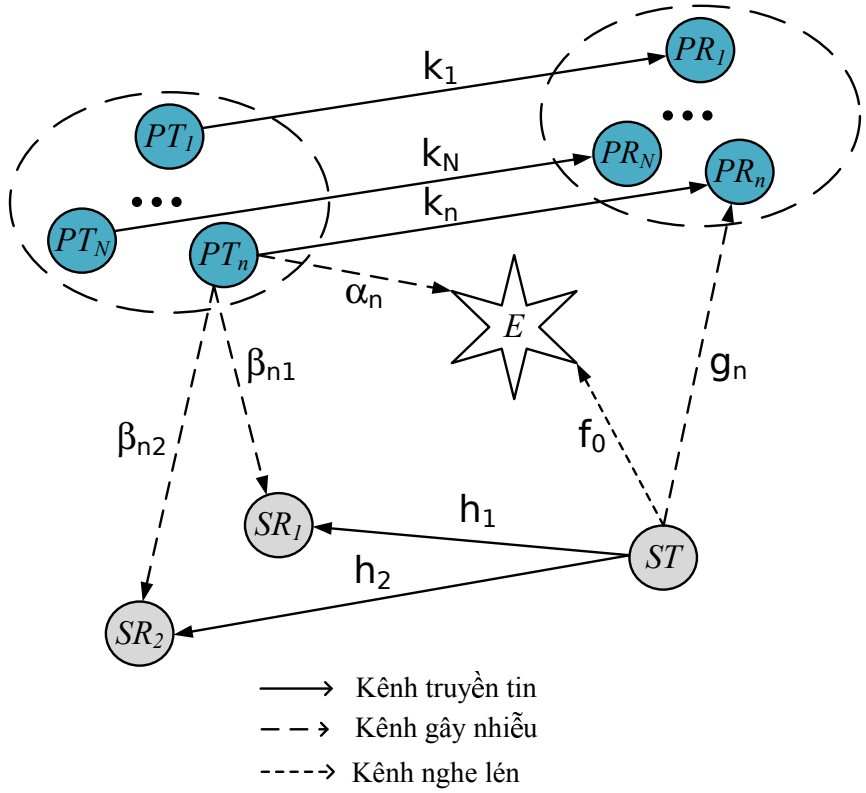
Hình 4.10 mô tả ảnh hưởng của SNR đến xác suất rớt gói tin truyền từ S đến U_1 và U_2. Chúng ta thấy rằng xác suất rớt gói tin cho cả hai người dùng đều giảm khi SNR của S tăng. Điều này được giải thích như sau: SNR tăng dẫn đến tốc độ truyền gói tin sẽ tăng và kết quả thời gian truyền gói tin sẽ giảm đi. Mặt khác, xác suất truyền gói tin giảm nhanh khi SNR có miền giá trị cao khoảng 14 dB trở lên. Nguyên nhân là do thời gian truyền sẽ giảm khi tăng công suất truyền SNR.

4.3 MÔ HÌNH 4.2: Đánh giá hiệu năng bảo mật và độ tin cậy mạng NOMA nhận thức dạng nền dưới ràng buộc mức can nhiễu của mạng sơ cấp

4.3.1 Mô hình hệ thống

Trong phần này, luận án xem xét mô hình mạng NOMA nhận thức dạng nền như mô tả trong hình 4.11. Trong đó mạng NOMA nhận thức gồm có mạng sơ cấp và mạng thứ cấp. Mạng sơ cấp gồm có N cặp nguồn-đích $PT_n \rightarrow PR_n$ $(1 \leq n \leq N)$.

Trong khi đó, mạng thứ cấp gồm một thiết bị phát ST sử dụng kỹ thuật NOMA để truyền tin đến hai thiết bị nhận SR_1 và SR_2 tương ứng. Ngoài ra, mạng thứ cấp có khả năng cảm nhận và sử dụng lại băng tần của mạng sơ cấp với điều kiện tác động nhiễu của mạng thứ cấp lên mạng sơ cấp nằm dưới ngưỡng cho trước. Mạng thứ cấp còn gọi là mạng NOMA nhận thức. Khi mạng thứ cấp truyền thông tin, một thiết bị nghe lén E hoạt động ở chế độ thụ động để thu thập thông tin phát đi từ ST. Giải thiết rằng các thiết bị ST, SR_1, SR_2, và E được trang bị một ăng-ten. Ký hiệu h_1, h_2, f_0 và g_n là độ lợi kênh truyền từ thiết bị ST tới SR_1, SR_2, E, và PR_n tương ứng. Đồng thời ký hiệu $\beta_{n_1}, \beta_{n_2}, \alpha_{n_1}, \alpha_n$ và k_n là độ lợi kênh truyền từ PT_n tới SR_1, SR_2, E, và PR_n. Giả thiết tất cả các kênh truyền tuân theo phân bố Rayleigh fading, và độ lợi kênh truyền X (X $\in \{h_1, h_2, f_0, g_n, \beta_{n_1}, \beta_{n_2}, \alpha_n, k_n\}$) là các giá trị ngẫu nhiên (RV) tuân theo phân bố mũ với giá trị trung bình Ω_X. Mạng thứ cấp sử dụng lại băng tần của mạng sơ cấp để thực hiện việc truyền tin,



Hình 4.11: *Mô hình mạng NOMA nhận thức dưới ràng buộc mức can nhiễu của mạng sơ cấp*

thiết bị nhận SR_i (i $\in \{1, 2\}$) sẽ bị tác động nhiễu từ PT_n. Vì vậy dung lượng kênh truyền của mạng thứ cấp dưới tác động nhiễu từ PT_n được biểu diễn như sau

$$C^{(1)} = B \log_2(1 + \gamma_{SR_1}), \tag{4.100}$$

$$C^{(2)} = B\log_2(1+\gamma_{SR_2}), \tag{4.101}$$

trong đó γ_{SR_1} và γ_{SR_2} là tỷ số công suất tín hiệu trên nhiễu tại SR_1, SR_2 và có giá trị như sau

$$\gamma_{SR_1} = \frac{P_s^{(1)}h_1}{P_p^{(n)}\beta_{n_1} + N_0}, \tag{4.102}$$

$$\gamma_{SR_2} = \frac{P_s^{(2)}h_2}{P_p^{(n)}\beta_{n_2} + P_s^{(1)}h_2 + N_0}, \tag{4.103}$$

trong đó $P_s^{(1)}$ và $P_s^{(2)}$ là công suất truyền của tín hiệu cho SR_1 và SR_2 tương ứng. N_0 là công suất nhiễu và $P_p^{(n)}$ là công suất của mạng sơ cấp. Giả thiết rằng SR_1 ở gần ST hơn so với SR_2. Điều đó có nghĩa rằng SR_2 được cấp mức công suất lớn hơn công suất cấp cho SR_1 [68].

Cần lưu ý rằng E nghe lén thông tin của người dùng SR_i trong SN, nhưng bị tác động bởi nhiễu từ PT_n. Do đó, dung lượng kênh truyền của E được biểu diễn như sau:

$$C_{Eve}^{(1)} = B\log_2(1+\gamma_{Eve}^{(1)}), \tag{4.104}$$

$$C_{Eve}^{(2)} = B\log_2(1+\gamma_{Eve}^{(2)}), \tag{4.105}$$

trong đó $\gamma_{Eve}^{(1)}$ và $\gamma_{Eve}^{(2)}$ là tỷ số công suất tín hiệu trên nhiễu tại E và được biểu diễn như sau

$$\gamma_{Eve}^{(1)} = \frac{P_s^{(1)}f_0}{P_p^{(n)}\alpha_n + N_0}, \tag{4.106}$$

$$\gamma_{Eve}^{(2)} = \frac{P_s^{(2)}f_0}{P_p^{(n)}\alpha_n + P_s^{(1)}f_0 + N_0}. \tag{4.107}$$

4.3.2 Phân tích hiệu suất hệ thống

Trong phần này, luận án thiết lập chính sách điều khiển công suất phát của ST dưới ràng buộc mức can nhiễu của mạng sơ cấp và công suất phát mức đỉnh của mạng thứ cấp, cũng như đánh giá độ tin cậy và hiệu suất bảo mật của mạng thứ cấp. Cụ thể, chúng ta sử dụng xác suất dừng hệ thống làm phép đo để đánh giá độ tin cậy và xác suất bị nghe lén để đánh giá về tính an toàn, bảo mật của hệ thống.

4.3.2.1 Ràng buộc về công suất của mạng thứ cấp

Trong mô hình này, ST truyền thông tin bí mật mà không hề biết đến sự tồn tại của đối tượng nghe lén E. Hơn nữa, ST thiếu thông tin về trạng thái kênh truyền (CSI) từ PT_n đến PR_n. Kết quả là, ST thiết lập công suất phát dựa hoàn toàn vào ràng buộc mức can nhiễu của mạng sơ cấp, nói cách khác ST được phép truyền tin nhưng không làm ảnh hưởng đến QoS được đặt ra bởi mạng sơ cấp, ràng buộc công suất phát của mạng thứ cấp được mô tả bằng biểu thức xác suất dừng hoạt động của mạng sơ cấp như sau:

$$\mathcal{O}_{out}^{P} = \Pr\left\{\max_{n\in\{1,\ldots,N\}}\left\{\frac{P_s g_n}{N_0}\right\} > Q_{pk}\right\} \leq \xi, \tag{4.108}$$

Trong đó, ξ và Q_{pk} lần lượt là giới hạn xác suất dừng hệ thống do mạng sơ cấp quy định và công suất nhiễu tối đa mà mạng sơ cấp có thể chịu được. Điều này có nghĩa là cho phép ST truyền tin với giới hạn mức độ gây nhiễu cho phép đối với PR_n. Nói cách khác, xác suất gây nhiễu do ST gây ra phải duy trì dưới một ngưỡng xác định trước ξ để tránh làm gián đoạn hoạt động của mạng sơ cấp. Do đó, ràng buộc đặt ra về công suất phát của ST phải thỏa mãn hai điều kiện sau đây:

$$\mathcal{O}_{out}^{P} \leq \xi, \tag{4.109}$$

$$0 \leq P_s \leq P_s^{max}, \tag{4.110}$$

trong đó P_s^{max} là công suất phát cực đại của ST.

Chúng ta thực hiện tính toán $\mathcal{O}_{out}^{P}$ như sau [20]:

$$\begin{aligned}\mathcal{O}_{out}^{P} &= \Pr\left\{\max_{n\in\{1,\ldots,N\}}\left\{\frac{P_s g_n}{N_0}\right\} \geq Q_{pk}\right\} \leq \xi \\ &= 1 - \Pr\left\{\max_{n\in\{1,..,N\}}\{g_n\} < \frac{Q_{pk}}{P_s}\right\} \leq \xi \\ &= 1 - \left(1 - \exp\left\{-\frac{Q_{pkN_0}}{\Omega_g P_s}\right\}\right)^{N} \leq \xi. \end{aligned} \tag{4.111}$$

Thực hiện thêm các bước tính toán, chúng ta nhận được biểu thức công suất phát P_s của mạng thứ cấp như sau:

$$P_s \leq \underbrace{\frac{Q_{pkN_0}}{\Omega_g}\left(\log_e \frac{1}{1 - \sqrt[N]{1-\xi}}\right)^{-1}}_{P_I}. \tag{4.112}$$

Kết hợp công thức (4.110) và (4.112), công suất phát của mạng thứ cấp dưới ràng buộc giới hạn can nhiễu của mạng sơ cấp phải thỏa mãn điều kiện sau:

$$0 \leq P_s \leq \min\left\{P_I, P_s^{max}\right\}. \tag{4.113}$$

4.3.2.2 Xác suất bị nghe lén

Thông tin truyền đi trên mạng thứ cấp sẽ bị E nghe lén và có thể giải mã thành công các tín hiệu x_1 hoặc x_2 từ ST. Do đó, xác suất bị nghe lén được định nghĩa là xác suất mà dung lượng kênh truyền $ST \to SR_1$ hoặc kênh truyền $ST \to SR_2$ lớn hơn các ngưỡng $\theta_{th}^{(1)}$ và $\theta_{th}^{(2)}$ tương ứng được xác định trước [138], xác suất thông tin mạng thứ cấp bị E nghe lén được biểu diễn như sau

$$\mathcal{O}_{int} = \Pr\left\{C_{Eve}^{(1)} > \theta_{th}^{(1)} \; or \; C_{Eve}^{(2)} > \theta_{th}^{(2)}\right\}, \tag{4.114}$$

trong đó $C_{Eve}^{(1)}$ và $C_{Eve}^{(2)}$ được định nghĩa trong công thức (4.104) và (4.105).

Thay công thức (4.104) và (4.105) vào (4.114), chúng ta có biểu thức xác suất bị nghe lén như sau

$$\begin{aligned}
\mathcal{O}_{int} &= 1 - \Pr\left\{B\log_2\left(1 + \frac{P_s^{(1)} f_0}{P_p^{(n)}\alpha_n + N_0}\right) < \theta_{th}^{(1)}, \right. \\
&\quad \left. B\log_2\left(1 + \frac{P_s^{(2)} f_0}{P_p^{(n)}\alpha_n + P_s^{(1)} f_0 + N_0}\right) < \theta_{th}^{(2)}\right\} \\
&= 1 - \int_0^{\infty} \Pr\left\{B\log_2\left(1 + \frac{P_s^{(1)} x}{P_p^{(n)}\alpha_n + N_0}\right) < \theta_{th}^{(1)}, \right. \\
&\quad \left. B\log_2\left(1 + \frac{P_s^{(2)} x}{P_p^{(n)}\alpha_n + P_s^{(1)} x + N_0}\right) < \theta_{th}^{(2)}\right\} f_{f_0}(x)dx,
\end{aligned}$$

trong đó $f_{f_0}(x)$ là hàm mật độ của biến ngẫu nhiên f_0. Đặt giá trị

$$I_1(x) = \frac{P_s^{(1)} x - \lambda_1 N_0}{\lambda_1 P_p^{(n)}}, \tag{4.115}$$

$$I_2(x) = \frac{P_s^{(2)} x - \lambda_2 P_s^{(1)} x - \lambda_2 N_0}{\lambda_2 P_p^{(n)}}, \tag{4.116}$$

chúng ta nhận được biểu thức của $\mathcal{O}_{int}$ như sau

$$\begin{aligned}\mathcal{O}_{int} &= 1 - \int_0^\infty \Pr\left\{\alpha_n < I_1(x), \alpha_n < I_2(x)\right\} f_{f_0}(x)dx \\ &= 1 - \int_0^\infty \Pr\left\{\alpha_n < \min\{I_1(x), I_2(x)\}\right\} f_{f_0}(x)dx.\end{aligned}$$

Thay thế hàm phân phối của biến ngẫu nhiêu α_n có giá trị trung bình Ω_{α_n}, ta có

$$\mathcal{O}_{int} = 1 - \int_0^\infty \left(1 - e^{-\frac{\min\{I_1(x), I_2(x)\}}{\Omega_{\alpha_n}}}\right) f_{f_0}(x)dx.$$

Tiếp tục, thực hiện phân phối tích phân qua phép trừ và chúng ta thu được

$$\mathcal{O}_{int} = 1 - \int_0^\infty f_{f_0}(x)dx - \int_0^\infty e^{-\frac{\min\{I_1(x), I_2(x)\}}{\Omega_{\alpha_n}}} f_{f_0}(x)dx. \tag{4.117}$$

trong công thức trên, tích phân đầu tiên là hàm mật độ của $f_{f_0}(x)$ và có giá trị bằng 1. Do đó, $\mathcal{O}_{int}$ được tính như sau:

$$\mathcal{O}_{int} = \int_0^\infty e^{-\frac{\min\{I_1(x), I_2(x)\}}{\Omega_{\alpha_n}}} f_{f_0}(x)dx. \tag{4.118}$$

Gọi x_0 là điểm mà $I_1(x_0) = I_2(x_0)$. Khi đó, $\mathcal{O}_{int}$ sẽ có dạng như sau

$$\mathcal{O}_{int} = \underbrace{\int_0^{x_0} e^{-\frac{I_1(x)}{\Omega_{\alpha_n}}} f_{f_0}(x)dx}_{P_1} + \underbrace{\int_{x_0}^\infty e^{-\frac{I_2(x)}{\Omega_{\alpha_n}}} f_{f_0}(x)dx}_{P_2}. \tag{4.119}$$

Thay hàm phân phối của biến ngẫu nhiên f_0 vào P_1, chúng ta nhận được biểu thức sau:

$$\begin{aligned}P_1 =& \frac{\lambda_1 P_p^{(n)} \Omega_{\alpha_n} \exp\left\{\frac{N_0}{P_p^{(n)}\Omega_{\alpha_n}}\right\}}{P_s^{(1)}\Omega_{f_0} + \lambda_1 P_p^{(n)}\Omega_{\alpha_n}} \\ &\times \left(1 - \exp\left\{-\frac{P_s^{(1)}\Omega_{f_0} + \lambda_1 P_p^{(n)}\Omega_{\alpha_n}}{\lambda_1 P_p^{(n)}\Omega_{\alpha_n}\Omega_{f_0}} x_0\right\}\right).\end{aligned} \tag{4.120}$$

Tương tự như cách tính biểu thức P_1, chúng ta có thể tính P_2 như sau:

$$P_2 = \frac{\lambda_2 P_p^{(n)} \Omega_{\alpha_n} \exp\left\{\frac{N_0}{P_p^{(n)}\Omega_{\alpha_n}}\right\}}{P_s^{(2)}\Omega_{f_0} - \lambda_2 P_s^{(1)}\Omega_{f_0} + \lambda_2 P_p^{(n)}\Omega_{\alpha_n}}$$

$$\times \exp\left\{-\frac{P_s^{(2)}\Omega_{f_0} - \lambda_2 P_s^{(1)}\Omega_{f_0} + \lambda_2 P_p^{(n)}\Omega_{\alpha_n}}{\lambda_2 P_p^{(n)}\Omega_{\alpha_n}\Omega_{f_0}} x_0\right\}. \tag{4.121}$$

Cuối cùng, thay thế công thức (4.120) và (4.121) vào (4.119), chúng ta nhận được biểu thức đóng của xác suất bị nghe lén như sau:

$$\begin{aligned}\mathcal{O}_{int} =& 1 - \frac{\lambda_1 P_p^{(n)}\Omega_{\alpha_n} \exp\left\{\frac{N_0}{P_p^{(n)}\Omega_{\alpha_n}}\right\}}{P_s^{(1)}\Omega_{f_0} + \lambda_1 P_p^{(n)}\Omega_{\alpha_n}} \\ &\times \left(1 - \exp\left\{-\frac{P_s^{(1)}\Omega_{f_0} + \lambda_1 P_p^{(n)}\Omega_{\alpha_n}}{\lambda_1 P_p^{(n)}\Omega_{\alpha_n}\Omega_{f_0}} x_0\right\}\right) \\ &- \frac{\lambda_2 P_p^{(n)}\Omega_{\alpha_n} \exp\left\{\frac{N_0}{P_p^{(n)}\Omega_{\alpha_n}}\right\}}{P_s^{(2)}\Omega_{f_0} - \lambda_2 P_s^{(1)}\Omega_{f_0} + \lambda_2 P_p^{(n)}\Omega_{\alpha_n}} \\ &\times \exp\left\{-\frac{P_s^{(2)}\Omega_{f_0} - \lambda_2 P_s^{(1)}\Omega_{f_0} + \lambda_2 P_p^{(n)}\Omega_{\alpha_n}}{\lambda_2 P_p^{(n)}\Omega_{\alpha_n}\Omega_{f_0}} x_0\right\},\end{aligned} \tag{4.122}$$

trong đó $\lambda_1 = 2^{(\theta_{th}^{(1)}/B)} - 1$, $\lambda_2 = 2^{(\theta_{th}^{(2)}/B)} - 1$, và $x_0 = \frac{P_s^{(1)}\lambda_1\lambda_2}{P_s^{(2)}\lambda_1 - P_s^{(1)}\lambda_2}$.

4.3.2.3 Xác suất dừng hệ thống

Xác suất dừng hệ thống là xác suất mà dung lượng kênh truyền nhỏ hơn ngưỡng được quy định trước [135]. Như đã đề cập trong phần giới thiệu, ý nghĩa của xác suất dừng hệ thống để đánh giá độ tin cậy của mạng thứ cấp dưới ràng buộc về giới hạn can nhiễu của mạng sơ cấp. Trong mô hình này, mạng thứ cấp dừng hệ thống khi dung lượng kênh truyền từ ST đến SR_1 và SR_2 nằm dưới ngưỡng được xác định cho trước tương ứng của R_1 và R_2. Cụ thể, chúng ta tính toán xác suất dừng hệ thống từ ST đến SR_1 và SR_2 được mô tả như sau [43]:

$$\mathcal{O}_{out} = \Pr\left\{C^{(1)} < R_1 \; or \; C^{(2)} < R_2\right\}, \tag{4.123}$$

trong đó $C^{(1)}$ và $C^{(2)}$ được định nghĩa trong công thức (4.100) và (4.101) tương ứng.

Thay thế công thức (4.100) và (4.101) vào (4.123), chúng ta nhận được biểu

thức xác suất dừng hệ thống như sau:

$$\begin{aligned}\mathcal{O}_{out} &= \Pr\left\{ B\log_2\left(1+\frac{P_s^{(1)}h_1}{P_p^{(n)}\beta_{n_1}+N_0}\right) < R_1 \right. \\ &\quad \left. or\ B\log_2\left(1+\frac{P_s^{(2)}h_2}{P_p^{(n)}\beta_{n_2}+P_s^{(1)}h_2+N_0}\right) < R_2 \right\} \\ &= \underbrace{\Pr\left\{ B\log_2\left(1+\frac{P_s^{(1)}h_1}{P_p^{(n)}\beta_{n_1}+N_0}\right) < R_1 \right\}}_{A_1} \\ &\quad \times \underbrace{\Pr\left\{ B\log_2\left(1+\frac{P_s^{(2)}h_2}{P_p^{(n)}\beta_{n_2}+P_s^{(1)}h_2+N_0}\right) < R_2 \right\}}_{A_2}. \end{aligned} \tag{4.124}$$

A_1 được tính toán như sau:

$$\begin{aligned} A_1 &= \int_0^{\infty} \Pr\left\{ \beta_{n_1} > \frac{P_s^{(1)}x - N_0\delta_1}{\delta_1 P_p^{(n)}} \right\} f_{h_1}(x)dx \\ &= \int_0^{\rho} \Pr\left\{ \beta_{n_1} > \frac{P_s^{(1)}x - N_0\delta_1}{\delta_1 P_p^{(n)}} \right\} f_{h_1}(x)dx \\ &\quad + \int_{\rho}^{\infty} \Pr\left\{ \beta_{n_1} > \frac{P_s^{(1)}x - N_0\delta_1}{\delta_1 P_p^{(n)}} \right\} f_{h_1}(x)dx, \end{aligned} \tag{4.125}$$

trong đó $\delta_1 = 2^{(R_1/B)} - 1, \rho = \frac{N_0\delta_1}{P_s^{(1)}}$, và $f_{h_1}(x)$ là hàm mật độ của biến ngẫu nhiên h_1. Do $(P_s^{(1)} - N_0\delta_1) < 0$ khi $x < \rho$, vì vậy A_1 được viết lại như sau

$$A_1 = \int_0^{\rho} f_{h_1}(x)dx + \int_{\rho}^{\infty} \Pr\left\{ \beta_{n_1} > \frac{P_s^{(1)}x - N_0\delta_1}{\delta_1 P_p^{(n)}} \right\} f_{h_1}(x)dx.$$

Thay thế hàm mật độ của phân phối mũ vào công thức (4.125) và thực hiện một số tính toán, biểu thức A_1 có dạng như sau:

$$A_1 = 1 - \exp\left\{ -\frac{\rho}{\Omega_{h_1}} \right\} + \frac{\delta_1 P_p^{(p)}\Omega_{\beta_1} \exp\left\{ \frac{N_0}{P_p^{(n)}\Omega_{\beta_{n_1}}} \right\}}{P_s^{(1)}\Omega_{h_1} + \delta_1 P_p^{(n)}\Omega_{\beta_{n_1}}}$$

$$\times \exp\left\{-\frac{P_s^{(1)}\Omega_{h_1}+\delta_1 P_p^{(n)}\Omega_{\beta_{n_1}}}{\delta_1 P_p^{(n)}\Omega_{\beta_{n_1}}\Omega_{h_1}}\right\}. \tag{4.126}$$

Tính toán tương tự như A_1, chúng ta nhận được biểu thức A_2 như sau:

$$\begin{aligned}A_2 &= \int_0^{\infty} \Pr\left\{\beta_2 > \frac{P_s^{(2)}x-\delta_2 P_s^{(1)}x-\delta_2 N_0}{P_p^{(p)}\delta_2}\right\} f_{h_2}(x)dx \\ &= \int_0^{\sigma} f_{h_2}(x)dx + \int_{\sigma}^{\infty} \exp\left\{-\frac{(P_s^{(2)}-\delta_2 P_s^{(1)})x-\delta_2 N_0}{\delta_2 P_p^{(n)}\Omega_{\beta_{n_2}}}\right\} \\ &\quad \times f_{h_2}(x)dx,\end{aligned} \tag{4.127}$$

trong đó $\sigma = \frac{\delta_2 N_0}{P_s^{(2)}-\delta_2 P_s^{(1)}}, \delta_2 = 2^{(R_2/B)}-1$. Do $\int_0^{\infty} f_{\beta_{n_2}}(y)dy = 1$, vì vậy A_2 có giá trị như sau:

$$\begin{aligned}A_2 =& 1-\exp\left\{-\frac{\sigma}{\Omega_{h_2}}\right\} + \frac{\delta_2 P_p^{(n)}\Omega_{\beta_{n_2}}\exp\left\{\frac{N_0}{\delta_2 P_p^{(n)}}\right\}}{(P_s^{(2)}-\delta_2 P_s^{(1)})\Omega_{h_2}+\delta_2 P_p^{(n)}\Omega_{\beta_{n_2}}} \\ &\times \exp\left\{-\frac{(P_s^{(2)}-\delta_2 P_s^{(1)})\Omega_{h_2}+\delta_2\Omega_{\beta_{n_2}}P_p^{(n)}}{\delta_2\Omega_{\beta_{n_2}}\Omega_{h_2}P_p^{(n)}}\right\}.\end{aligned} \tag{4.128}$$

Cuối cùng, thay thế công thức (4.126) và (4.128) vào (4.129), chúng ta nhận được biểu thức xác suất dừng hệ thống của mạng thứ cấp như sau:

$$\begin{aligned}\mathcal{O}_{out} =& 1-\exp\left\{-\frac{\rho}{\Omega_{h_1}}\right\} + 1-\exp\left\{-\frac{\sigma}{\Omega_{h_2}}\right\} \\ &+ \frac{\delta_1 P_p^{(p)}\Omega_{\beta_1}\exp\left\{\frac{N_0}{P_p^{(n)}\Omega_{\beta_{n_1}}}\right\}}{P_s^{(1)}\Omega_{h_1}+\delta_1 P_p^{(n)}\Omega_{\beta_{n_1}}} \\ &\times \exp\left\{-\frac{P_s^{(1)}\Omega_{h_1}+\delta_1 P_p^{(n)}\Omega_{\beta_{n_1}}}{\delta_1 P_p^{(n)}\Omega_{\beta_{n_1}}\Omega_{h_1}}\right\} \\ &+ \frac{\delta_2 P_p^{(n)}\Omega_{\beta_{n_2}}\exp\left\{\frac{N_0}{\delta_2 P_p^{(n)}}\right\}}{(P_s^{(2)}-\delta_2 P_s^{(1)})\Omega_{h_2}+\delta_2 P_p^{(n)}\Omega_{\beta_{n_2}}} \\ &\times \exp\left\{-\frac{(P_s^{(2)}-\delta_2 P_s^{(1)})\Omega_{h_2}+\delta_2\Omega_{\beta_{n_2}}P_p^{(n)}}{\delta_2\Omega_{\beta_{n_2}}\Omega_{h_2}P_p^{(n)}}\right\}.\end{aligned} \tag{4.129}$$

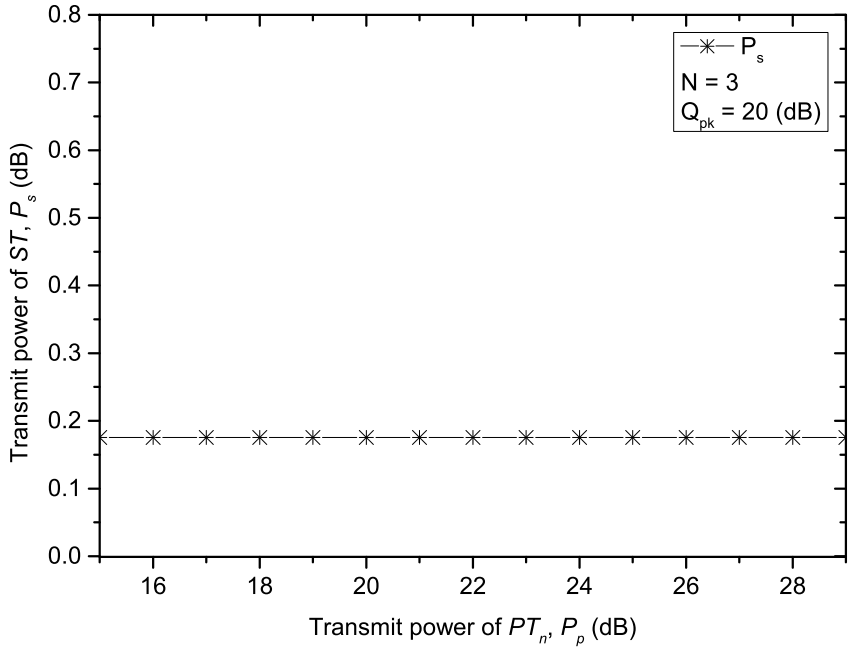
4.3.3 Mô phỏng và đánh giá kết quả

Trong phần này, luận án trình bày kết quả mô phỏng và phân tích của hệ thống. Mô phỏng được thực hiện bằng phương pháp Monte Carlo, với mục tiêu đối sánh với kết quả của phương pháp phân tích lý thuyết được trình bày trong phần 4.3.2. Các thông số hệ thống sau đây được áp dụng cho cả phương pháp mô phỏng và phân tích:

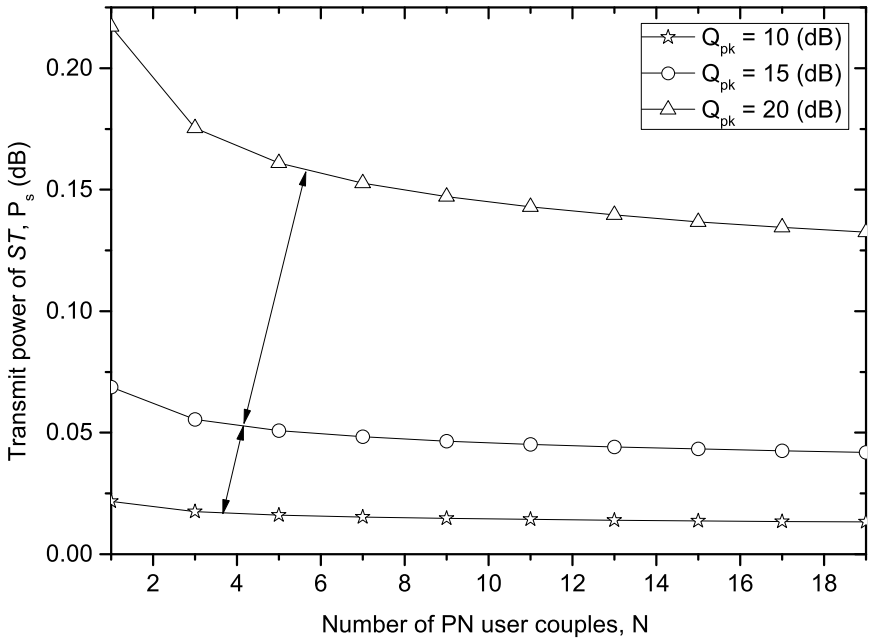
- Băng thông hệ thống: $W = 10^6$ Hz
- Ngưỡng giới hạn tốc độ bảo mật của mạng thứ cấp: $\theta_{th}^{(1)} = \theta_{th}^{(2)} = 10^3$ bps
- Ngưỡng giới hạn tốc độ truyền tin của mạng thứ cấp: $R_1 = R_2 = 10^3$ bps
- Hệ số phân bổ công suất cho SR_1 và SR_2: $P_s^{(1)} = 0.3P_s$, $P_s^{(2)} = 0.7P_s$
- Công suất phát của mạng sơ cấp, $P_p^{(n)} = 25$ dB
- Công suất nhiễu: $N_0 = 10^{-3}$ dB
- Công suất nhiễu mức đỉnh của mạng sơ cấp: Q_{pk} = {10, 15, 20} dB
- Giới hạn xác suất dừng hệ thống của mạng sơ cấp: $\xi = 0.01$
- $\Omega_{h_1} = 2, \Omega_{h_2} = 1, \Omega_{f_0} = \{0.1, 0.3, 0.5\}, \Omega_{\alpha_n} = 20, \Omega_{\beta_{n_1}} = \{1, 2, 3\}, \Omega_{\beta_{n_2}} = 2, \Omega_g = 0.1$

Hình 4.12 biểu thị công suất phát của mạng thứ cấp P_s như là một hàm số có đối số là công suất phát của mạng sơ cấp P_p. Chúng ta có thể thấy rằng công suất phát của mạng thứ cấp duy trì ổn định, không thay đổi trong toàn bộ khoảng công suất phát của mạng sơ cấp. Kết quả này khớp với công thức (4.113) trong đó công suất phát của mạng thứ cấp không phụ thuộc vào công suất phát của mạng sơ cấp.

Hình 4.13 cho thấy sự ảnh hưởng của số lượng cặp người dùng của mạng sơ cấp đối với công suất phát của mạng thứ cấp. Có thể thấy rằng khi số lượng cặp người dùng mạng sơ cấp tăng lên, công suất phát của mạng thứ cấp giảm đi. Điều này xảy ra vì khi số lượng cặp người dùng mạng sơ cấp tăng lên, việc điều chỉnh công suất phát của mạng thứ cấp để đáp ứng ràng buộc về giới hạn can nhiễu của mạng sơ cấp trở lên dễ dàng hơn.

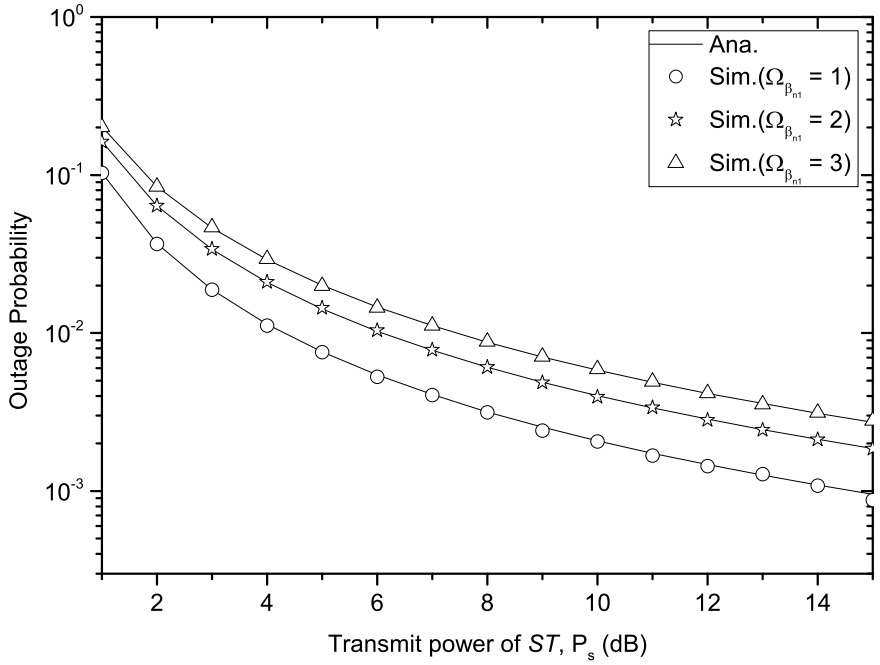


Hình 4.12: *Công suất phát của mạng thứ cấp P_s so với công suất phát của mạng sơ cấp P_p*



Hình 4.13: *Mối quan hệ giữa công suất phát của mạng thứ cấp và số cặp người dùng của mạng sơ cấp*

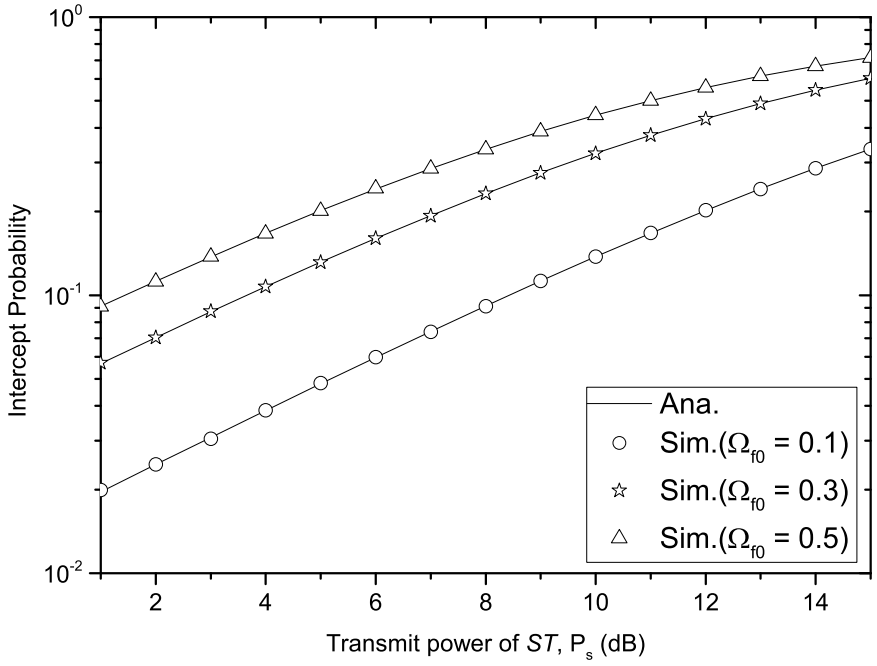
Hình 4.14 mô tả mối quan hệ giữa xác suất dừng hệ thống so với công suất phát P_s dưới các mức độ nhiễu khác nhau gây ra từ mạng sơ cấp tác động lên SR_i. Chúng ta thấy rằng kết quả của phương pháp phân tích toán học và kết quả mô



Hình 4.14: *Mối quan hệ giữa xác suất dừng hoạt động với công suất phát của của mạng thứ cấp*

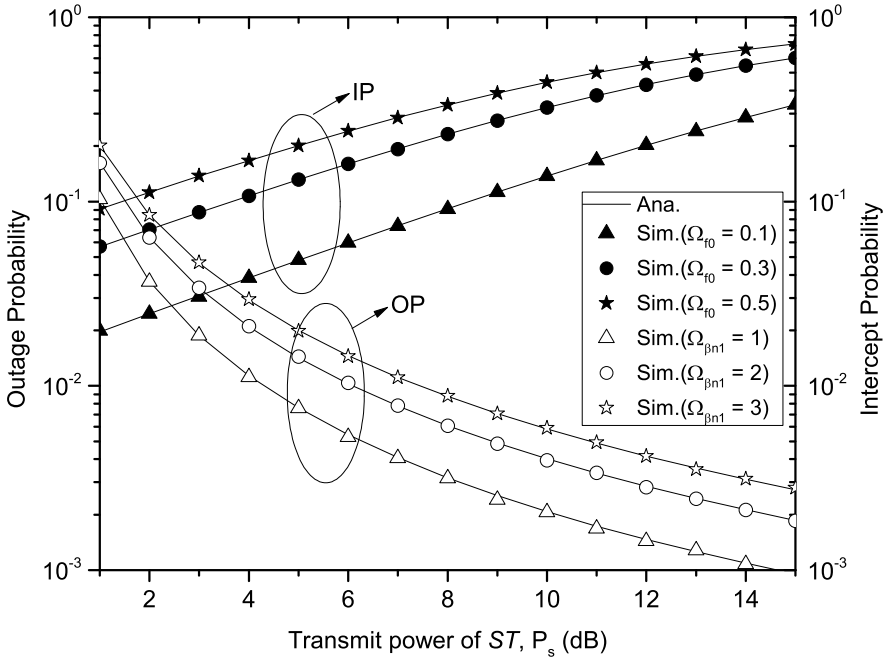
phỏng bằng phương pháp Monte-Carlo trùng khớp nhau trong hình này. Đáng chú ý, xác suất dừng hệ thống của mạng thứ cấp sẽ giảm đi khi công suất phát của ST tăng lên. Một kết quả quan trọng cần nhấn mạnh là chúng ta có thể tăng công suất phát P_s để nâng cao độ tin cậy của mạng thứ cấp nhưng chúng ta phải đảm bảo rằng điều này không làm gián đoạn hoạt động của mạng sơ cấp. Hơn nữa, cũng có thể thấy rằng xác suất dừng hệ thống của mạng thứ cấp giảm đi khi mức độ nhiễu từ mạng sơ cấp tăng lên. Điều này có nghĩa là tín hiệu nhiễu gây ra từ mạng sơ cấp có tác động tiêu cực đến hiệu suất của mạng thứ cấp.

Hình 4.15 mô tả mối quan hệ giữa xác suất nghe lén và công suất phát của mạng thứ cấp P_s với các giá trị trung bình của độ lợi kênh truyền (Ω_{f_0}) khác nhau. Chúng ta thấy rằng các kết quả phân tích toán học tương ứng với kết quả mô phỏng. Số liệu thể hiện trên đồ thị cho thấy rằng hiệu suất bảo mật của mạng thứ cấp bị giảm đi, tức xác suất nghe lén của E tăng lên khi công suất phát của nó tăng lên. Điều này có thể được giải thích như sau: Khi công suất phát P_s tăng lên, các tín hiệu bị nghe lén bởi E trở lên tốt hơn vì vậy E có thể giải mã tín hiệu dễ dàng hơn. Hơn nữa, cũng có thể thấy rằng xác suất nghe lén của E tăng lên khi độ lợi kênh truyền từ ST đến E tăng. Cuối cùng, từ Hình 4.14 và 4.15 cho thấy tối ưu hóa công suất phát của mạng thứ cấp là rất quan trọng vì độ tin cậy và



Hình 4.15: *Xác suất mạng thứ cấp bị nghe lén so với công suất phát của mạng thứ cấp*

hiệu năng bảo bảo mật của mạng thứ cấp có quan hệ đối nghịch nhau. Mặt khác, chúng ta thấy rằng khi giá trị trung bình độ lợi kênh truyền của thiết biệt nghe lén E tăng lên, tính bảo mật của mạng thứ cấp dần bị giảm đi.



Hình 4.16: *Mối quan hệ giữa xác suất dừng hoạt động, xác suất bị nghe lén của mạng thứ cấp so với công suất phát của mạng thứ cấp P_s*

Hình 4.16 chỉ ra mối tương quan giữa xác suất dừng hệ thống của mạng thứ cấp và xác suất nghe lén của E so với công suất phát của mạng thứ cấp. Chúng ta có thể quan sát thấy khi xác suất dừng hệ thống tăng lên thì xác suất bị nghe lén giảm xuống, và ngược lại. Do đó, việc tối ưu hóa một bộ tham số đảm bảo đồng thời khả năng bảo mật thông tin và độ tin cậy khi truyền tin của hệ thống trở lên rất quan trọng để đạt được sự cân bằng tối ưu hóa giữa khả năng bảo mật thông tin của hệ thống và độ tin cậy. Đối với cả xác suất dừng hệ thống và xác suất bị nghe lén khi độ lợi kênh truyền tăng lên, khoảng cách giữa các đường cong xác suất dừng hệ thống và xác suất bị nghe lén sẽ thu hẹp lại.

4.4 Kết luận

Trong chương này, với mô hình thứ nhất, luận án nghiên cứu, đánh giá hiệu năng bảo mật, hiệu suất truyền tin và tính công bằng thời gian truyền tin trong mạng SISO NOMA trên kênh truyền Rayleigh fading với sự hiện diện của một thiết bị nghe lén Eve. Trong đó xem xét hai kịch bản Eve có thể sử dụng kỹ thuật loại bỏ nhiễu SIC hoặc PIC để xử lý tín hiệu thu thập được. Luận án đã xây dựng biểu thức tính xác suất dừng bảo mật của từng người dùng và của toàn hệ thống cho cả kịch bản Eve sử dụng kỹ thuật SIC và kịch bản Eve sử dụng kỹ thuật PIC. Hơn nữa, luận án đã xây dựng biểu thức tính xác suất rớt gói tin và thời gian truyền tin trung bình, đề xuất thuật toán để tìm hệ số phân bố công suất để đảm bảo tính công bằng thời gian truyền tin giữa những người dùng trong cùng một nhóm. Tiếp theo, luận án phân tích, đánh giá tác động của các tham số hệ thống lên hiệu suất bảo mật của hệ thống. Các số liệu phân tích và mô phỏng đã chỉ ra rằng xác suất dừng bảo mật của từng người dùng cũng như của toàn bộ hệ thống khi Eve sử dụng kỹ thuật SIC tốt hơn khi Eve sử dụng kỹ thuật PIC. Mặt khác, xác suất dừng bảo mật của từng người dùng cũng như của toàn bộ hệ thống khi Eve được trang bị một ăng-ten tốt hơn khi Eve được trang bị nhiều ăng-ten. Ngoài ra, trong mạng NOMA chúng ta có thể điều chỉnh công suất truyền tin để đảm bảo tính công bằng trong thời gian truyền tin giữa những người dùng trong một nhóm.

Trong mô hình thứ hai, luận án phân tích sự đánh đổi giữa hiệu năng bảo mật và độ tin cậy của mạng NOMA nhận thức dưới ràng buộc mức can nhiễu và công

suất phát mức đỉnh của mạng sơ cấp. Dưới ràng buộc mức can nhiễu do mạng sơ cấp áp đặt, luận án đã trình bày quá trình xây dựng biểu thức xác định công suất phát của mạng thứ cấp, xác suất dừng hoạt động của mạng thứ cấp, xác suất nghe lén thông tin của thiết bị nghe lén. Các kết quả phân tích và mô phỏng đã chỉ ra rằng tính an toàn, bảo mật thông tin và độ tin cậy của hệ thống có mối quan hệ tỷ lệ nghịch. Khi tính an toàn, bảo mật thông tin của hệ thống được nâng cao thì độ tin cậy khi truyền tin giảm đi và ngược lại. Tiếp theo, tác giả đã phân tích, đánh giá tác động của các tham số hệ thống lên hiệu suất của hệ thống.

KẾT LUẬN VÀ ĐỊNH HƯỚNG NGHIÊN CỨU TIẾP THEO

Mạng NOMA là công nghệ tiềm năng cho mạng 5G để nâng cao hiệu quả sử dụng phổ tần số, hỗ trợ nhiều kết nối, tăng dung lượng kênh truyền. Đảm bảo an toàn thông tin của mạng NOMA là vấn đề cấp thiết, ưu tiên hàng đầu trong quá trình thiết kế hệ thống mạng không dây. Luận án đã nghiên cứu, đánh giá và đề xuất giải pháp nâng cao bảo mật tầng vật lý trong mạng NOMA. Các kết quả của luận án đã đạt được mục đích đề ra đó là: i) Đề xuất các mô hình mạng NOMA sử dụng các kỹ thuật truyền thông tiên tiến như truyền thông cộng tác, vô tuyến nhận thức, gây nhiễu cộng tác; ii) Phân tích, đánh giá khả năng đảm bảo an toàn thông tin tầng vật lý, đề xuất các chiến lược nhằm nâng cao khả năng bảo mật và phân tích hiệu quả bảo mật của chiến lược được đề xuất trên kênh truyền Rayleigh fading và $\alpha - \mu$ fading và iii) Xây dựng biểu thức toán học, chương trình mô phỏng để đánh giá tác động của các tham số hệ thống lên hiệu năng bảo mật của hệ thống. Các kết quả nghiên cứu đã được trình bày chi tiết trong các chương, cụ thể như sau: Chương 1 trình bày tổng quan về những vấn đề nghiên cứu; Chương 2 phân tích, đánh giá hiệu năng bảo mật mạng NOMA có chiến lược đối phó chủ động với hình thức tấn công hợp tác; Chương 3 đề xuất và đánh giá hiệu năng bảo mật mạng NOMA có chiến lược chủ động nghe lén dựa trên phép đo xác suất nghe lén hợp pháp thành công; Chương 4 phân tích hiệu năng bảo mật mô hình mạng SISO NOMA, khảo sát mối quan hệ giữa bảo mật và độ tin cậy của mạng NOMA nhận thức dạng nền dưới ràng buộc mức can nhiễu của mạng sơ cấp và công suất phát mức đỉnh.

Các kết quả đóng góp mới về khoa học của Luận án bao gồm:

1. Luận án đã phân tích làm rõ các khái niệm mạng NOMA, bảo mật tầng vật lý, cơ sở lý thuyết của kỹ thuật bảo mật tầng vật lý, so sánh ưu nhược điểm của kỹ thuật bảo mậng tầng vật lý với kỹ thuật mã hóa truyền thống, các phép đo để đánh giá hiệu năng bảo mật tầng vật lý trong mạng NOMA. Từ đó khẳng định bảo mật tầng vật lý là có cơ sở khoa học và có tính thực tiễn

cao, trên cơ sở đó đề xuất ra các mô hình mạng NOMA cơ bản để làm cở sở nghiên cứu, đánh giá các mô hình mạng NOMA phức tạp hơn trong thực tế.

2. Luận án đã đề xuất chiến lược bảo mật thông tin cho mạng NOMA cộng tác trên kênh truyền α-μ fading bị thiết bị gây nhiễu và nghe lén hợp tác tấn công dựa trên biểu thức dạng đóng của phép đo xác suất dừng bảo mật trong kịch bản hệ thống có chiến lược đối phó chủ động và không có chiến lược đối phó chủ động. Các kết quả mô phỏng đã chỉ ra rằng hiệu năng bảo mật của hệ thống được cải thiện đáng kể trong kịch bản có chiến lược đối phó chủ động.

3. Luận án đã đề xuất và đánh giá hiệu năng bảo mật mô hình mạng NOMA có chiến lược chủ động nghe lén. Tác giả đã xây dựng một chính sách điều khiển công suất phát trong kịch bản trạng thái kênh truyền xác định và không xác định vừa đảm bảo hiệu suất nghe lén vừa thỏa mãn ràng buộc về QoS của hệ thống truyền tin bất hợp pháp. Mặt khác, luận án sử dụng phép đo xác suất nghe lén hợp pháp thành công để đánh giá hiệu năng bảo mật của hệ thống và đánh giá hiệu suất nghe lén hợp pháp thành công đối với người dùng bất hợp pháp có tín hiệu mạnh nhất và người dùng bất hợp pháp có tín hiệu yếu nhất. Các kết quả phân tích lý thuyết và mô phỏng chỉ ra rằng hiệu năng bảo mật của hệ thống tăng đáng kể khi số lượng ăng-ten của thiết bị chuyển tiếp tăng lên.

4. Luận án đã nghiên cứu, đánh giá khả năng bảo mật thông tin mô hình mạng SISO NOMA với các kịch bản khác nhau về thiết bị nghe lén Eve. Hiệu năng bảo mật được phân tích, đánh giá thông qua các phép đo xác suất dừng bảo mật của từng người dùng, của toàn bộ hệ thống với kịch bản Eve sử dụng các kỹ thuật SIC, PIC để xử lý tín hiệu thu được, kịch bản Eve được trang bị một và nhiều ăng-ten. Các kết quả phân tích lý thuyết và mô phỏng đã chỉ ra rằng hiệu năng bảo mật của hệ thống giảm đi trong trường hợp Eve sử dụng PIC so với trường hợp Eve sử dụng kỹ thuật SIC. Hơn nữa, hệ thống sẽ bảo mật hơn khi Eve chỉ được trang bị một ăng-ten so với trường hợp thiết bị nghe lén được trang bị nhiều ăng-ten.

5. Luận án đã phân tích mối quan hệ giữa bảo mật và độ tin cậy trong mạng NOMA nhận thức dưới ràng buộc mức can nhiễu của mạng sơ cấp và công suất phát mức đỉnh của mạng thứ cấp, từ đó đưa ra chính sách điều chỉnh công suất phát của mạng thứ cấp để vừa đảm bảo khả năng bảo mật của mạng thứ cấp và QoS của mạng sơ cấp. Các kết quả đã chỉ ra rằng giữa tính bảo mật và độ tin cậy có mối quan hệ tỷ lệ nghịch. Hiệu năng bảo mật của mạng thứ cấp được cải thiện khi giảm công suất phát và khi số lượng cặp người dùng của mạng sơ cấp tăng thì có thể giảm công suất phát của mạng thứ cấp.

   Với những kết quả đạt được như đã trình bày trong luận án, chúng ta thấy rằng với mỗi mô hình mạng cụ thể, hiệu năng bảo mật tầng vật lý trong mạng NOMA có thể được cải thiện bằng các giải pháp khác nhau như cộng tác gây nhiễu, tăng số ăng-ten của thiết bị chuyển tiếp trong truyền thông đa chặng, tăng số lượng cặp người dùng mạng sơ cấp. Nghiên cứu sinh hy vọng những kết quả này góp phần nhỏ bé làm phong phú và sáng tỏ sự hiểu biết về bảo mật thông tin tầng vật lý trong mạng NOMA và triển khai ứng dụng trong các hệ thống thực tế.

Định hướng nghiên cứu, phát triển các kết quả của luận án như sau:

1. Dựa trên các kết quả nghiên cứu trên mô hình trong chương 2, trường hợp hệ thống có chiến lược đối phó chủ động có thể phát triển bài toán với mục tiêu tối ưu công suất gây nhiễu của thiết bị chuyển tiếp và của U_1, đồng thời đảm bảo xác suất dừng bảo mật không nhỏ hơn một ngưỡng cho trước, so sánh hiệu năng bảo mật hệ thống giữa kịch bản thiết bị chuyển tiếp hoạt động theo cơ chế song công và bán công, giữa kịch bản thiết bị chuyển tiếp hoạt động theo cơ chế giải mã - chuyển tiếp và cơ chế khuếch đại - chuyển tiếp, giữa kịch bản thiết bị chuyển tiếp sử dụng phương pháp kết hợp lựa chọn và kết hợp tỉ số cực đại để xử lý tín hiệu.

2. Từ các nghiên cứu trên mô hình mạng trong chương 3, nghiên cứu sinh đã đưa ra chính sách điều khiển công suất gây nhiễu để cải thiện hiệu năng nghe lén giám sát, mô hình bài toán này có thể nghiên cứu mở rộng cho trường hợp sau: Tối ưu công suất gây nhiễu để tối đa tốc độ nghe lén với

giả thiết là thiết bị giám sát E là một thiết bị UAV có khả năng linh hoạt thay đổi khoảng cách khi thực hiện chức năng thu thập tín hiệu và thiết bị đích D được trang bị nhiều ăng-ten.

3. Trên cơ sở từ các nghiên cứu các mô hình mạng trong chương 4, có thể mở rộng khảo sát trong trường hợp có nhiều Eve với hai kịch bản là: Các thiết bị nghe lén Eve cùng phối hợp thu thập tín hiệu và kịch bản mỗi Eve hoạt động độc lập. So sánh tổng thông lượng bảo mật của hệ thống trong hai kịch bản hoạt động của Eve. Phân tích xác suất dừng bảo mật với ràng buộc về xác suất dừng tin cậy. Khảo sát xác suất dừng bảo mật của hệ thống trên miền SNR cao.

4. Các nghiên cứu về bảo mật tầng vật lý trong mạng NOMA hiện nay đều dựa trên giả thiết về trạng thái kênh truyền của các thiết bị nghe lén là có thể xác định, tuy nhiên trong thực tế các thiết bị nghe lén hoạt động ở chế độ thụ động, việc xác định được chính xác trạng thái kênh truyền là một thách thức [63, 70, 155]. Theo hiểu biết của nghiên cứu sinh, hiện nay có rất ít công trình nghiên cứu về vấn đề này [24, 25, 64]. Do đó, làm phong phú thêm các phương pháp ước lượng CSI của kênh truyền nghe lén để áp dụng trong lớp các bài toán đánh giá, nâng cao hiệu năng bảo mật mạng NOMA nói riêng và mạng không dây nói chung là một bài toán thú vị.

5. Tiếp tục khảo sát các công trình nghiên cứu trong lĩnh vực bảo mật tầng vật lý trong mạng NOMA và đề xuất các giải pháp nâng cao bảo mật tầng vật lý trong mạng NOMA tích hợp với các công nghệ quan trọng trong mạng thế hệ thứ 5, 6 như Massive MIMO, mmWave,...

DANH MỤC CÔNG TRÌNH KHOA HỌC CỦA TÁC GIẢ LIÊN QUAN ĐẾN LUẬN ÁN

A. Các công trình khoa học được sử dụng trong luận án

[A1] **Tung Pham Huu**, Van Nhan Vo, Hung Tran and Truong Xuan Quach and Viet Nguyen Dinh, "Secrecy Performance Analysis of Cooperative NOMA Networks With Active Protection under α - μ Fading",*2019 International Conference on Advanced Technologies for Communications (ATC)*, Hanoi, Vietnam, 2019, pp. 215-22.

[A2] **Tung Pham Huu**, Tam Ninh Thi-Thanh, Chi Nguyen-Yen, Hung Tran, Viet Nguyen Dinh and Van Vo Nhan, "Secrecy Outage Probability and Fairness of Packet Transmission Time in a NOMA System",*IEEE Access*, vol. 8, pp.79637-79649, 2020.

[A3] **Tung Pham Huu**, Van Vo Nhan, Hung Tran, Truong Quach Xuan and Viet Nguyen Dinh, "Proactive Eavesdropping via Jamming in NOMA Network", *IEEE Access*, vol. 9, pp.168121-168133, 2021.

[A4] **Tung Pham Huu**, Hung Tran, Duc-Tan Tran, Viet-Hung Dang, Van Nhan Vo, and Viet Nguyen Dinh, "Security and Reliability Performance Analysis of Cognitive NOMA Network Under Outage Constraint of Multiple Primary Users", *12th International Symposium on Information and Communication Technology (SoICT 2023)*, Ho Chi Minh City, Vietnam, 2023.

B. Các công trình khoa học có liên quan đến luận án

[B1] **Tung Pham Huu**, Truong Xuan Quach, Hung Tran, Hans-Jurgen Zepernick, and Louis Sibomana (2017), "On proactive attacks for coping with cooperative attacks in relay networks", *23rd Asia-Pacific Conference on Communications (APCC)*, Perth, 2017, pp. 1-6.

[B2] Van Nhan Vo, Chakchai So-In, Hung Tran, Duc-Dung Tran and **Tung Pham Huu**, "Performance Analysis of an Energy-Harvesting IoT System Using a UAV Friendly Jammer and NOMA Under Cooperative Attack," in IEEE Access, vol. 8, pp. 221986-222000, 2020.

[B3] Hung Tran, Hung Pham Ngoc, Van Vo Nhan, Xuan Truong Quach, **Tung Pham Huu**, Long Nguyen Quoc, and Giang Quynh Le Vu "Secure Conversation: A View From Physical Layer", *The 12th International Conference on Computational Data and Social Networks*, Hanoi, Vietnam, 2023.

[B4] Hung Tran, **Tung Pham Huu**, Lam-Thanh Tu, Vu Le Quynh Giang, Trinh Van Chien, Viet-Hung Dang, and Vo Nhan Van, "Packet Timeout Probability of CRN under Security Constraints of Multiple Primary Users", *12th International Symposium on Information and Communication Technology (SoICT 2023)*, Ho Chi Minh City, Vietnam, 2023.

Tài liệu tham khảo

[1] Aggelos Bletsas and Hyundong Shin and Moe Z. Win (2007), "Cooperative Communications with Outage-Optimal Opportunistic Relaying", *IEEE Transactions on Wireless Communications*, 6(9), pp. 3450-3460.

[2] Alves H. and Souza R. D. and Debbah M. and Bennis M. (2012), "Performance of Transmit Antenna Selection Physical Layer Security Schemes", *IEEE Signal Processing Letters*, 19(6), pp. 372-375.

[3] Barros J. and Rodrigues M. R. D. (2006), "Secrecy Capacity of Wireless Channels ", *IEEE International Symposium on Information Theory*, pp. 356-360.

[4] Bloch M. and Barros J. and Rodrigues M.R.D. and McLaughlin S.W. (2008), "Wireless Information-Theoretic Security", *IEEE Transactions on Information Theory*, 54(6), pp. 2515-2534.

[5] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai and S. Verdu, "Capacity of Cognitive Interference Channels With and Without Secrecy," *IEEE Transactions on Information Theory*, vol. 55, no. 2, pp. 604-619, Feb. 2009.

[6] Y. Wu and K. J. R. Liu, "An Information Secrecy Game in Cognitive Radio Networks," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 831-842, Sept. 2011.

[7] Csiszar I. and Korner J. (1978), "Broadcast channels with confidential messages", *IEEE Transactions on Information Theory*, 24(3), pp. 339-348.

[8] Dong L. and Han Z. and Petropulu A. P. and Poor H. V. (2010), "Improving Wireless Physical Layer Security via Cooperating Relays", *IEEE Transactions on Signal Processing*, 58(3), pp. 1875-1888.

[9] Goel S. and Negi R. (2008), "Guaranteeing Secrecy using Artificial Noise", *IEEE Transactions on Wireless Communications*, 7(6), pp. 2180-2189.

[10] Goldsmith A. J. (2005), *Wireless Communications,* Cambridge University Press.

[11] Vijay Garg (2010), *Wireless Communications & Networking,* Morgan Kaufmann.

[12] Matthieu Bloch, João Barros (2011), *Physical-Layer Security From Information Theory to Security Engineering,* Cambridge University Press.

[13] Hassan Amer A. and Wayne E. Stark and John E. Hershey and Sandeep Chennakeshu (1996), "Cryptographic Key Agreement for Mobile Radio", *Digital Signal Processing*, 6(4), pp. 207 - 212.

[14] Leung-Yan-Cheong S. and Hellman M. (1978), "The Gaussian wire-tap channel", *IEEE Transactions on Information Theory*, 24(4), pp. 451-456.

[15] Mahdavifar H. and Vardy A. (2011), "Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes", *IEEE Transactions on Information Theory*, 67(10), pp. 6428-6443.

[16] Mukherjee A. and Fakoorian S. A. A. and Huang J. and Swindlehurst A. L. (2014), "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey", *IEEE Communications Surveys Tutorials*, 16(3), pp. 1550-1573.

[17] Patwari N. and Croft J. and Jana S. and Kasera S. K. (2010), "High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements", *IEEE Transactions on Mobile Computing*, 9(1), pp. 17-30.

[18] Peng Y. and Alexandropoulos G. C. and Wang P. and Li Y. and Ha D. (2014), "Poster: Secret key generation from CFR for OFDM TDD systems over fading channels", *9th International Conference on Communications and Networking in China*, pp. 660-661.

[19] Praveen Kumar Gopala and Lifeng Lai and El Gamal H. (2008), "On the Secrecy Capacity of Fading Channels", *IEEE Transactions on Information Theory*, 54(10), pp. 4687-4698.

[20] Quach T. X. and Tran H. and Uhlemann E. and Kaddoum G. and Tran Q. A. (2017), "Power allocation policy and performance analysis of secure and reliable communication in cognitive radio networks", *Wireless Networks*, 25(4), pp. 1477-1489.

[21] Ren K. and Su H. and Wang Q. (2011), "Secret key generation exploiting channel characteristics in wireless communications", *IEEE Wireless Communications*, 18(4), pp. 6-12.

[22] Schaefer R. F. and Boche H. (2014), "Physical Layer Service Integration in Wireless Networks : Signal processing challenges", *IEEE Signal Processing Magazine*, 31(3), pp. 147-156.

[23] Shannon C. E. (1949), "Communication theory of secrecy systems", *The Bell System Technical Journal*, 28(4), pp. 656-715.

[24] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2012, pp. 2809-2812.

[25] A. Chaman, J. Wang, J. Sun, H. Hassanieh, and R. R.Choudhury, "Ghostbuster: Detecting the presence of hidden eavesdroppers," in MobiCom, 2018.

[26] Thangaraj A. and Dihidar S. and Calderbank A. R. and McLaughlin S. W. and Merolla J., (2007), "Applications of LDPC Codes to the Wiretap Channel", *IEEE Transactions on Information Theory*, 53(8), pp. 2933-2945.

[27] Tse, David and Viswanath, Pramod (2005), *Fundamentals of Wireless Communication*, Cambridge University Press.

[28] Yulong Zou , Jia Zhu (2016) *Physical-Layer Security for Cooperative Relay Networks*, Springer Cham

[29] Fa-Long Luo, Charlie Jianzhong Zhang (2016), *Signal Processing for 5G: Algorithms and Implementations*, Wiley-IEEE Press.

[30] Wyner A. D. (1975), "The wire-tap channel", *The Bell System Technical Journal*, 54(8), pp. 1355-1387.

[31] Yacoub M. D. (2007), "The α-μ Distribution: A Physical Fading Model for the Stacy Distribution", *IEEE Transactions on Vehicular Technology*, 51(1), pp. 27-34.

[32] Ye C. and Reznik A. and Shah Y. (2006), "Extracting Secrecy from Jointly Gaussian Random Variables", *2006 IEEE International Symposium on Information Theory*, pp. 2593-2597.

[33] Zhang S. and Jin L. and Lou Y. and Zhong Z. (2018), "Secret key generation based on two-way randomness for TDD-SISO system", *China Communications*, 15(7), pp. 202-216.

[34] Zheng G. and Krikidis I. and Masouros C. and Timotheou S. and Toumpakaris D. and Ding Z. (2014), "Rethinking the role of interference in wireless networks", *IEEE Communications Magazine*, 52(11), pp. 152-158.

[35] Zhou X. and McKay M. R. (2010), "Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation", *IEEE Transactions on Vehicular Technology*, 59(8), pp. 3831-3842.

[36] C. Liu, L. Zhang, M. Xiao, Z. Chen and S. Li, "Secrecy Performance Analysis in Downlink NOMA Systems with Cooperative Full-Duplex Relaying," 2018 IEEE International Conference on Communications Workshops (ICC Workshops), 2018, pp. 1-6.

[37] Zou Y. and Wang X. and Shen W. (2013), "Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks", *IEEE Journal on Selected Areas in Communications*, 31(10), pp. 2099-2111.

[38] Zou Y. and Zhu J. and Wang X. and Leung V. C. M. (2015), "Improving physical-layer security in wireless communications using diversity techniques", *IEEE Network*, 29(1), pp. 42-48.

[39] B. Li, Y. Yao, H. Chen, Y. Li and S. Huang, "Wireless Information Surveillance and Intervention Over Multiple Suspicious Links," in IEEE Signal Processing Letters, vol. 25, no. 8, pp. 1131-1135, Aug. 2018.

[40] X. Wang, J. Wang, L. He and J. Song, "Outage Analysis for Downlink NOMA With Statistical Channel State Information," in IEEE Wireless Communications Letters, vol. 7, no. 2, pp. 142-145, April 2018.

[41] K. Cao, B. Wang, H. Ding, L. Lv, J. Tian and F. Gong, "On the Security Enhancement of Uplink NOMA Systems With Jammer Selection," in IEEE Transactions on Communications, vol. 68, no. 9, pp. 5747-5763, Sept. 2020.

[42] P. Wang, G. Yu and Z. Zhang, "On the Secrecy Capacity of Fading Wireless Channel with Multiple Eavesdroppers," 2007 IEEE International Symposium on Information Theory, 2007, pp. 1301-1305.

[43] T. X. Quach, H. Tran, E. Uhlemann and M. T. Truc, "Secrecy Performance of Cooperative Cognitive Radio Networks Under Joint Secrecy Outage and Primary User Interference Constraints," in IEEE Access, vol. 8, pp. 18442-18455, 2020.

[44] A. A. Nasir, H. D. Tuan, T. Q. Duong and H. V. Poor, "UAV-Enabled Communication Using NOMA," in IEEE Transactions on Communications, vol. 67, no. 7, pp. 5126-5138, July 2019.

[45] V. N. Vo, T. G. Nguyen, C. So-In and D. Ha, "Secrecy Performance Analysis of Energy Harvesting Wireless Sensor Networks With a Friendly Jammer," in IEEE Access, vol. 5, pp. 25196-25206, 2017.

[46] M. D. Yacoub, "The α-μ Distribution: A Physical Fading Model for the Stacy Distribution," in IEEE Transactions on Vehicular Technology, vol. 56, no. 1, pp. 27-34, Jan. 2007.

[47] Vo, V.N., Nguyen, T.G., So-In, C. et al. Outage Performance Analysis of Energy Harvesting Wireless Sensor Networks for NOMA Transmissions. Mobile Netw Appl 25, 23–41 (2020).

[48] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen and L. Hanzo, "A Survey of Non-Orthogonal Multiple Access for 5G," in IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2294-2323, thirdquarter 2018.

[49] P. R. Patel and J. M. Holtzman, "Analysis of a DS/CDMA successive interference cancellation scheme using correlations," Proceedings of GLOBECOM '93. IEEE Global Telecommunications Conference, 1993, pp. 76-80 vol.1.

[50] Y. Cao et al., "Secrecy Analysis for Cooperative NOMA Networks With Multi-Antenna Full-Duplex Relay," in IEEE Transactions on Communications, vol. 67, no. 8, pp. 5574-5587, Aug. 2019.

[51] B. Zheng et al., "Secure NOMA Based Two-Way Relay Networks Using Artificial Noise and Full Duplex," in IEEE Journal on Selected Areas in Communications, vol. 36, no. 7, pp. 1426-1440, July 2018.

[52] L. Lv, Z. Ding, Q. Ni and J. Chen, "Secure MISO-NOMA Transmission With Artificial Noise," in IEEE Transactions on Vehicular Technology, vol. 67, no. 7, pp. 6700-6705, July 2018.

[53] L. Lv, Z. Ding, J. Chen and N. Al-Dhahir, "Design of Secure NOMA Against Full-Duplex Proactive Eavesdropping," in IEEE Wireless Communications Letters, vol. 8, no. 4, pp. 1090-1094, Aug. 2019.

[54] H. Xu and L. Sun, "Wireless Surveillance via Proactive Eavesdropping and Rotated Jamming," in IEEE Transactions on Vehicular Technology, vol. 68, no. 11, pp. 10713-10727, Nov. 2019.

[55] D. Xu, "Proactive Eavesdropping of Suspicious Non-Orthogonal Multiple Access Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 11, pp. 13958-13963, Nov. 2020.

[56] I. Gradshteyn and I. Ryzhik, Table of Integrals, series and products, 7th ed. Elsevier, 2007.

[57] J. Chen, L. Yang and M. -S. Alouini, "Physical Layer Security for Cooperative NOMA Systems," in IEEE Transactions on Vehicular Technology, vol. 67, no. 5, pp. 4645-4649, May 2018.

[58] Y. Feng, Z. Yang and S. Yan, "Non-Orthogonal Multiple Access and Artificial-Noise Aided Secure Transmission in FD Relay Networks," 2017 IEEE Globecom Workshops (GC Wkshps), 2017, pp. 1-6.

[59] Z. Chang et al., "Energy-Efficient and Secure Resource Allocation for Multiple-Antenna NOMA With Wireless Power Transfer," in IEEE Transactions on Green Communications and Networking, vol. 2, no. 4, pp. 1059-1071, Dec. 2018.

[60] Youngkwon Cho and Jae Hong Lee, "Analysis of an adaptive SIC for near-far resistant DS-CDMA," in IEEE Transactions on Communications, vol. 46, no. 11, pp. 1429-1432, Nov. 1998

[61] B. Xia, J. Wang, K. Xiao, Y. Gao, Y. Yao and S. Ma, "Outage Performance Analysis for the Advanced SIC Receiver in Wireless NOMA Systems," in IEEE Transactions on Vehicular Technology, vol. 67, no. 7, pp. 6711-6715, July 2018.

[62] D. Divsalar, M. K. Simon and D. Raphaeli, "Improved parallel interference cancellation for CDMA," in IEEE Transactions on Communications, vol. 46, no. 2, pp. 258-268, Feb. 1998.

[63] B. He, A. Liu, N. Yang and V. K. N. Lau, "On the Design of Secure Non-Orthogonal Multiple Access Systems," in IEEE Journal on Selected Areas in Communications, vol. 35, no. 10, pp. 2196-2206, Oct. 2017.

[64] Zhang, Q.Y. and Liang, M.L. (2021), On non-destructive detection of hidden passive radio-frequency eavesdroppers. Electron. Lett., 57: 529-531.

[65] H. Zhang, N. Yang, K. Long, M. Pan, G. K. Karagiannidis and V. C. M. Leung, "Secure Communications in NOMA System: Subcarrier Assignment and Power Allocation," in IEEE Journal on Selected Areas in Communications, vol. 36, no. 7, pp. 1441-1452, July 2018.

[66] A. Goldsmith, Wireless Communnication, 1st ed. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[67] S. M. Ross, Introduction to Probability Models, 9th, Academic Publishers, 2007.

[68] Y. Feng, S. Yan, Z. Yang, N. Yang and J. Yuan, "Beamforming Design and Power Allocation for Secure Transmission With NOMA," in IEEE Transactions on Wireless Communications, vol. 18, no. 5, pp. 2639-2651, May 2019.

[69] H. Tran, T. Q. Duong, and H.-J. Zepernick, "Delay performance of cognitive radio networks for point-to-point and point-to-multipoint communication," in EURASIP J. Wireless Communication Networking, vol. 2012, no. 1, Dec. 2012, Art. no. 9.

[70] Y. Zhang, H. Wang, Q. Yang and Z. Ding, "Secrecy Sum Rate Maximization in Non-orthogonal Multiple Access," in IEEE Communications Letters, vol. 20, no. 5, pp. 930-933, May 2016.

[71] N. B. Mehta, V. Sharma and G. Bansal, "Performance Analysis of a Cooperative System with Rateless Codes and Buffered Relays," in IEEE Transactions on Wireless Communications, vol. 10, no. 4, pp. 1069-1081, April 2011

[72] X. Chen, Z. Zhang, C. Zhong, D. W. K. Ng and R. Jia, "Exploiting Inter-User Interference for Secure Massive Non-Orthogonal Multiple Access," in IEEE Journal on Selected Areas in Communications, vol. 36, no. 4, pp. 788-801, April 2018.

[73] M. Zeng, N. Nguyen, O. A. Dobre and H. V. Poor, "Securing Downlink Massive MIMO-NOMA Networks With Artificial Noise," in IEEE Journal of Selected Topics in Signal Processing, vol. 13, no. 3, pp. 685-699, June 2019.

[74] N. -P. Nguyen, O. A. Dobre, L. D. Nguyen, C. T. Nguyen and H. V. Poor, "Secure Downlink Massive MIMO NOMA Network in the Presence of a Multiple-Antenna Eavesdropper," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 2019, pp. 1-6.

[75] N. -P. Nguyen, M. Zeng, O. A. Dobre and H. V. Poor, "Securing Massive MIMO-NOMA Networks with ZF Beamforming and Artificial Noise," 2019 IEEE Global Communications Conference (GLOBECOM), 2019, pp. 1-6.

[76] M. Tian, Q. Zhang, S. Zhao, Q. Li and J. Qin, "Secrecy Sum Rate Optimization for Downlink MIMO Nonorthogonal Multiple Access Systems," in IEEE Signal Processing Letters, vol. 24, no. 8, pp. 1113-1117, Aug. 2017.

[77] G. He, L. Li, X. Li, W. Chen, L. -L. Yang and Z. Han, "Secrecy sum rate maximization in NOMA systems with wireless information and power transfer," 2017 9th International Conference on Wireless Communications and Signal Processing (WCSP), 2017.

[78] N. Zaghdoud, A. B. Mnaouer, W. H. Alouane, H. Boujemaa and F. Touati, "Secure Performance Analysis for Full-Duplex Cooperative NOMA System in the Presence of Multiple Eavesdroppers," 2020 International Wireless Communications and Mobile Computing (IWCMC), 2020, pp. 1719-1725.

[79] H. Lei et al., "Secrecy Outage Analysis for Cooperative NOMA Systems With Relay Selection Schemes," in IEEE Transactions on Communications, vol. 67, no. 9, pp. 6282-6298, Sept. 2019.

[80] D. Li et al., "Secrecy Analysis in NOMA Full-Duplex Relaying Networks With Artificial Jamming," in IEEE Transactions on Vehicular Technology, vol. 70, no. 9, pp. 8781-8794, Sept. 2021.

[81] Y. Feng, S. Yan, C. Liu, Z. Yang and N. Yang, "Two-Stage Relay Selection for Enhancing Physical Layer Security in Non-Orthogonal Multiple Access," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 6, pp. 1670-1683, June 2019.

[82] N. Rupasinghe, Y. Yapıcı, İsmail Guvenc, H. Dai and A. Bhuyan, "Enhancing Physical Layer Security for NOMA Transmission in mmWave Drone Networks," 2018 52nd Asilomar Conference on Signals, Systems, and Computers, 2018, pp. 729-733.

[83] H. Lei et al., "On Secure NOMA Systems With Transmit Antenna Selection Schemes," in IEEE Access, vol. 5, pp. 17450-17464, 2017.

[84] K. Shim, H. Oh, T. N. Do and B. An, "A Physical Layer Security-Based Transmit Antenna Selection Scheme for NOMA Systems," 2018 Tenth Interna-

tional Conference on Ubiquitous and Future Networks (ICUFN), 2018, pp. 597-602.

[85] H. Lei, R. Gao, K. -H. Park, I. S. Ansari, K. J. Kim and M. -S. Alouini, "On Secure Downlink NOMA Systems With Outage Constraint," in IEEE Transactions on Communications, vol. 68, no. 12, pp. 7824-7836, Dec. 2020.

[86] L. Dai, B. Wang, Y. Yuan, S. Han, I. Chih-lin and Z. Wang, "Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends," in IEEE Communications Magazine, vol. 53, no. 9, pp. 74-81, September 2015.

[87] Z. Ding, Z. Zhao, M. Peng and H. V. Poor, "On the Spectral Efficiency and Security Enhancements of NOMA Assisted Multicast-Unicast Streaming," in IEEE Transactions on Communications, vol. 65, no. 7, pp. 3151-3163, July 2017.

[88] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," in IEEE Transactions on Wireless Communications, vol. 7, no. 6, pp. 2180-2189, June 2008.

[89] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao and L. Hanzo, "Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access in Large-Scale Networks," in IEEE Transactions on Wireless Communications, vol. 16, no. 3, pp. 1656-1672, March 2017.

[90] Y. Yu, H. Chen, Y. Li, Z. Ding, L. Song and B. Vucetic, "Antenna Selection for MIMO Nonorthogonal Multiple Access Systems," in IEEE Transactions on Vehicular Technology, vol. 67, no. 4, pp. 3158-3171, April 2018.

[91] Electronic Foundation. Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design, 1998.

[92] Y. Wang, Z. Jin and X. Zhao, "Practical Defense against WEP and WPA-PSK Attack for WLAN," 2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), 2010, pp. 1-4.

[93] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," in IEEE Communications Magazine, vol. 53, no. 6, pp. 33-39, June 2015.

[94] Lin, R., Xu, L., Fang, H. et al. Efficient physical layer key generation technique in wireless communications. J Wireless Com Network 2020, 13 (2020).

[95] A. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe and T. Thomas, "LTE-advanced: next-generation wireless broadband technology [Invited Paper]," in IEEE Wireless Communications, vol. 17, no. 3, pp. 10-22, June 2010.

[96] D. Datla, A. M. Wyglinski and G. J. Minden, "A Spectrum Surveying Framework for Dynamic Spectrum Access Networks," in IEEE Transactions on Vehicular Technology, vol. 58, no. 8, pp. 4158-4168, Oct. 2009.

[97] D. Wang, B. Bai, W. Zhao and Z. Han, "A Survey of Optimization Approaches for Wireless Physical Layer Security," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1878-1911, Secondquarter 2019.

[98] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. -K. Wong and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," in IEEE Journal on Selected Areas in Communications, vol. 36, no. 4, pp. 679-695, April 2018.

[99] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao and K. Zeng, "Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8169-8181, Oct. 2019.

[100] Y. Liang, H. V. Poor and S. Shamai, "Secure Communication Over Fading Channels," in IEEE Transactions on Information Theory, vol. 54, no. 6, pp. 2470-2492, June 2008.

[101] H. Lei et al., "Secrecy Outage of Max–Min TAS Scheme in MIMO-NOMA Systems," in IEEE Transactions on Vehicular Technology, vol. 67, no. 8, pp. 6981-6990, Aug. 2018.

[102] J. Xu, L. Duan and R. Zhang, "Proactive Eavesdropping Via Jamming for Rate Maximization Over Rayleigh Fading Channels," in IEEE Wireless Communications Letters, vol. 5, no. 1, pp. 80-83, Feb. 2016.

[103] D. Hu, Q. Zhang, P. Yang and J. Qin, "Proactive Monitoring via Jamming in Amplify-and-Forward Relay Networks," in IEEE Signal Processing Letters, vol. 24, no. 11, pp. 1714-1718, Nov. 2017.

[104] B. Li, Y. Yao, H. Zhang, Y. Lv and W. Zhao, "Energy Efficiency of Proactive Eavesdropping for Multiple Links Wireless System," in IEEE Access, vol. 6, pp. 26081-26090, 2018.

[105] J. Moon, H. Lee, C. Song, S. Kang and I. Lee, "Relay-Assisted Proactive Eavesdropping With Cooperative Jamming and Spoofing," in IEEE Transactions on Wireless Communications, vol. 17, no. 10, pp. 6958-6971, Oct. 2018.

[106] J. Moon, H. Lee, C. Song, S. Lee and I. Lee, "Proactive Eavesdropping With Full-Duplex Relay and Cooperative Jamming," in IEEE Transactions on Wireless Communications, vol. 17, no. 10, pp. 6707-6719, Oct. 2018.

[107] Q. Li, H. Zhang, J. Qiao and D. Yuan, "Cooperative Relay-Assisted Proactive Eavesdropping for Wireless Information Surveillance Systems," 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 1-6.

[108] Y. Zeng and R. Zhang, "Wireless Information Surveillance via Proactive Eavesdropping with Spoofing Relay," in IEEE Journal of Selected Topics in Signal Processing, vol. 10, no. 8, pp. 1449-1461, Dec. 2016.

[109] X. Jiang, H. Lin, C. Zhong, X. Chen and Z. Zhang, "Proactive Eavesdropping in Relaying Systems," in IEEE Signal Processing Letters, vol. 24, no. 6, pp. 917-921, June 2017.

[110] G. Ma, J. Xu, L. Duan and R. Zhang, "Wireless surveillance of two-hop communications : (Invited paper)," 2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), 2017, pp. 1-5.

[111] C. Zhong, X. Jiang, F. Qu and Z. Zhang, "Multi-Antenna Wireless Legitimate Surveillance Systems: Design and Performance Analysis," in IEEE Transactions on Wireless Communications, vol. 16, no. 7, pp. 4585-4599, July 2017.

[112] J. Moon, S. H. Lee, H. Lee and I. Lee, "Proactive Eavesdropping With Jamming and Eavesdropping Mode Selection," in IEEE Transactions on Wireless Communications, vol. 18, no. 7, pp. 3726-3738, July 2019.

[113] G. Hu, Y. Cai and J. Ouyang, "Proactive Eavesdropping via Jamming for Multichannel Decode-and-Forward Relay System," in IEEE Communications Letters, vol. 24, no. 3, pp. 491-495, March 2020.

[114] M. Zhu, J. Mo, N. Xiong and J. Wang, "Legitimate Monitoring via Cooperative Relay and Proactive Jamming," in IEEE Access, vol. 7, pp. 40133-40143, 2019.

[115] Y. Zhang, X. Jiang, C. Zhong and Z. Zhang, "Performance of Proactive Eavesdropping in Dual-Hop Relaying Systems," 2017 IEEE Globecom Workshops (GC Wkshps), 2017, pp. 1-6.

[116] H. Cai, Q. Zhang, Q. Li and J. Qin, "Proactive Monitoring Via Jamming for Rate Maximization Over MIMO Rayleigh Fading Channels," in IEEE Communications Letters, vol. 21, no. 9, pp. 2021-2024, Sept. 2017.

[117] J. Moon, H. Lee, C. Song and I. Lee, "Multiple Amplify-and-Forward Full-Duplex Relays for Legitimate Eavesdropping," 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1-6.

[118] W. Huang, W. Chen, B. Bai and Z. Han, "Wiretap Channel With Full-Duplex Proactive Eavesdropper: A Game Theoretic Approach," in IEEE Transactions on Vehicular Technology, vol. 67, no. 8, pp. 7658-7663, Aug. 2018.

[119] H. Tran and H. -J. Zepernick, "Proactive attack: A strategy for legitimate eavesdropping," 2016 IEEE Sixth International Conference on Communications and Electronics (ICCE), 2016, pp. 457-461.

[120] Y. Li, M. Jiang, Q. Zhang, Q. Li and J. Qin, "Secure Beamforming in Downlink MISO Nonorthogonal Multiple Access Systems," in IEEE Transactions on Vehicular Technology, vol. 66, no. 8, pp. 7563-7567, Aug. 2017.

[121] M. Jiang, Y. Li, Q. Zhang, Q. Li and J. Qin, "Secure Beamforming in Downlink MIMO Nonorthogonal Multiple Access Networks," in IEEE Signal Processing Letters, vol. 24, no. 12, pp. 1852-1856, Dec. 2017

[122] N. Zaghdoud, A. B. Mnaouer, W. H. Alouane, H. Boujemaa and F. Touati, "Secrecy Performance Analysis of Multi-Antenna NOMA System with AF/DF relaying under External and Internal Eavesdropping Scenarios," 2020 International Wireless Communications and Mobile Computing (IWCMC), 2020, pp. 1726-1732.

[123] Z. Wang and Z. Peng, "Secrecy Performance Analysis of Relay Selection in Cooperative NOMA Systems," in IEEE Access, vol. 7, pp. 86274-86287, 2019.

[124] C. Yuan, X. Tao, N. Li, W. Ni, R. P. Liu and P. Zhang, "Analysis on Secrecy Capacity of Cooperative Non-Orthogonal Multiple Access With Proactive Jamming," in IEEE Transactions on Vehicular Technology, vol. 68, no. 3, pp. 2682-2696, March 2019.

[125] Chorti A. and Perlaza S. M. and Han Z. and Poor H. V.,(2013), On the Resilience of Wireless Multiuser Networks to Passive and Active Eavesdroppers, *IEEE Journal on Selected Areas in Communications*, 31(9), pp.

[126] J. M. Meredith, “Study on Downlink Multiuser Superposition Transmission for LTE”, in TSG RAN Meeting, vol. 67, 2015.

[127] Z. Ding, P. Fan and H. V. Poor, "Impact of User Pairing on 5G Nonorthogonal Multiple-Access Downlink Transmissions," in IEEE Transactions on Vehicular Technology, vol. 65, no. 8, pp. 6010-6023, Aug. 2016.

[128] W. Chen, S. Zhao, R. Zhang, H. Chen and L. Yang, "Generalized User Grouping in NOMA: An Overlapping Perspective," in IEEE Transactions on Wireless Communications, vol. 20, no. 5, pp. 2876-2887, May 2021.

[129] C. Gong, X. Yue, Z. Zhang, X. Wang and X. Dai, "Enhancing Physical Layer Security With Artificial Noise in Large-Scale NOMA Networks," in IEEE Transactions on Vehicular Technology, vol. 70, no. 3, pp. 2349-2361, March 2021.

[130] H. Li et al., "Secrecy Outage Probability of Relay Selection Based Cooperative NOMA for IoT Networks," in IEEE Access, vol. 9, pp. 1655-1665, 2021.

[131] W. Khalid and H. Yu, "Security Improvement With QoS Provisioning Using Service Priority and Power Allocation for NOMA-IoT Networks," in IEEE Access, vol. 9, pp. 9937-9948, 2021.

[132] S. Sharma, S. D. Roy and S. Kundu, "Secrecy Performance of Uplink-Downlink NOMA Network at Physical Layer," 2021 Sixth International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2021, pp. 57-61.

[133] V. P. Tuan and I. -P. Hong, "Enhancing Secrecy Performance for NOMA Systems With Intelligent Reflecting Surface: Analysis and Optimization," in IEEE Access, vol. 9, pp. 99060-99072, 2021.

[134] Z. Zhang, L. Lv, Q. Wu, H. Deng and J. Chen, "Robust and Secure Communications in Intelligent Reflecting Surface Assisted NOMA Networks," in IEEE Communications Letters, vol. 25, no. 3, pp. 739-743, March 2021.

[135] J. N. Laneman, D. N. C. Tse and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," in IEEE Transactions on Information Theory, vol. 50, no. 12, pp. 3062-3080, Dec. 2004.

[136] Y. Zou, J. Zhu, X. Wang and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," in Proceedings of the IEEE, vol. 104, no. 9, pp. 1727-1765, Sept. 2016.

[137] Y. -S. Shiu, S. Y. Chang, H. -C. Wu, S. C. . -H. Huang and H. -H. Chen, "Physical layer security in wireless networks: a tutorial," in IEEE Wireless Communications, vol. 18, no. 2, pp. 66-74, April 2011.

[138] X. Li et al., "Security and Reliability Performance Analysis of Cooperative Multi-Relay Systems With Nonlinear Energy Harvesters and Hardware Impairments," in IEEE Access, vol. 7, pp. 102644-102661, 2019.

[139] M. Bloch et al., "An Overview of Information-Theoretic Security and Privacy: Metrics, Limits and Applications," in IEEE Journal on Selected Areas in Information Theory, vol. 2, no. 1, pp. 5-22, March 2021.

[140] C. Ling, L. Luzzi, J. -C. Belfiore and D. Stehlé, "Semantically Secure Lattice Codes for the Gaussian Wiretap Channel," in IEEE Transactions on Information Theory, vol. 60, no. 10, pp. 6399-6416, Oct. 2014, doi: 10.1109/TIT.2014.2343226.

[141] J. -C. Belfiore and F. Oggier, "Secrecy gain: A wiretap lattice code design," 2010 International Symposium On Information Theory & Its Applications, Taichung, Taiwan, 2010, pp. 174-178.

[142] Y. Zou, X. Wang and W. Shen, "Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack," 2013 IEEE International Conference on Communications (ICC), Budapest, Hungary, 2013, pp. 2183-2187.

[143] L. Sibomana, H. Tran and H. -J. Zepernick, "Packet timeout probability for uplink spectrum sharing," 2013 International Conference on Advanced Technologies for Communications (ATC 2013), Ho Chi Minh City, Vietnam, 2013, pp. 496-500.

[144] S. Arzykulov, G. Nauryzbayev, T. A. Tsiftsis and B. Maham, "Performance Analysis of Underlay Cognitive Radio Nonorthogonal Multiple Access Networks," in IEEE Transactions on Vehicular Technology, vol. 68, no. 9, pp. 9318-9322, Sept. 2019.

[145] Y. Liu, Z. Ding, M. Elkashlan and J. Yuan, "Nonorthogonal Multiple Access in Large-Scale Underlay Cognitive Radio Networks," in IEEE Transactions on Vehicular Technology, vol. 65, no. 12, pp. 10152-10157, Dec. 2016.

[146] A. V. and B. A. V., "Performance Analysis of NOMA-Based Underlay Cognitive Radio Networks With Partial Relay Selection," in IEEE Transactions on Vehicular Technology, vol. 70, no. 5, pp. 4615-4630, May 2021.

[147] M. Li, H. Yuan, C. Maple, W. Cheng and G. Epiphaniou, "Physical Layer Security Analysis of Cognitive NOMA Internet of Things Networks," in IEEE Systems Journal, vol. 17, no. 1, pp. 1045-1055, March 2023.

[148] Z. Xiang, W. Yang, G. Pan, Y. Cai and Y. Song, "Physical Layer Security in Cognitive Radio Inspired NOMA Network," in IEEE Journal of Selected Topics in Signal Processing, vol. 13, no. 3, pp. 700-714, June 2019.

[149] K. Cao, B. Wang, H. Ding, T. Li, J. Tian and F. Gong, "Secure Transmission Designs for NOMA Systems Against Internal and External Eavesdropping," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2930-2943, 2020.

[150] J. Xu, L. Duan and R. Zhang, "Proactive Eavesdropping via Cognitive Jamming in Fading Channels," in IEEE Transactions on Wireless Communications, vol. 16, no. 5, pp. 2790-2806, May 2017.

[151] H. Wu, L. Yan, R. Ma, J. Ou and J. Cui, "A Decode-and-Forward Relay-Aided Proactive Eavesdropping Scheme for Wireless Surveillance," 2020 IEEE/CIC International Conference on Communications in China (ICCC), Chongqing, China, 2020, pp. 1104-1109.

[152] J. Lee, H. Wang, J. G. Andrews and D. Hong, "Outage Probability of Cognitive Relay Networks with Interference Constraints," in IEEE Transactions on Wireless Communications, vol. 10, no. 2, pp. 390-395, February 2011.

[153] Y. Noam and A. J. Goldsmith, "Blind Null-Space Learning for MIMO Underlay Cognitive Radio with Primary User Interference Adaptation," in IEEE Transactions on Wireless Communications, vol. 12, no. 4, pp. 1722-1734, April 2013.

[154] Y. Saito, A. Benjebbour, Y. Kishiyama and T. Nakamura, "System-Level Performance of Downlink Non-Orthogonal Multiple Access (NOMA) under

Various Environments," 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, UK, 2015, pp. 1-5.

[155] F. Jameel, S. Wyne, G. Kaddoum and T. Q. Duong, "A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security," in IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2734-2771, thirdquarter 2019.

[156] B. Li, X. Qi, K. Huang, Z. Fei, F. Zhou and R. Q. Hu, "Security-Reliability Tradeoff Analysis for Cooperative NOMA in Cognitive Radio Networks," in IEEE Transactions on Communications, vol. 67, no. 1, pp. 83-96, Jan. 2019.

[157] M. Qin, S. Yang, H. Deng and M. H. Lee, "Enhancing Security of Primary User in Underlay Cognitive Radio Networks With Secondary User Selection," in IEEE Access, vol. 6, pp. 32624-32636, 2018

[158] F. Zhou, Z. Chu, H. Sun, R. Q. Hu and L. Hanzo, "Artificial Noise Aided Secure Cognitive Beamforming for Cooperative MISO-NOMA Using SWIPT," in IEEE Journal on Selected Areas in Communications, vol. 36, no. 4, pp. 918-931, April 2018.

[159] M. Bloch and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering. Cambridge, UK: Cambridge University Press, 2011.

[160] J. M. Hamamreh, H. M. Furqan and H. Arslan, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1773-1828, Secondquarter 2019.