BỘ GIÁO DỤC VÀ ĐÀO TẠO BỘ QUỐC PHÒNG

HỌC VIỆN KỸ THUẬT QUÂN SỰ

ĐẶNG THẾ HÙNG

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

LUẬN ÁN TIẾN SĨ KỸ THUẬT

HÀ NỘI - 2021

BỘ GIÁO DỤC VÀ ĐÀO TẠO BỘ QUỐC PHÒNG

HỌC VIỆN KỸ THUẬT QUÂN SỰ

ĐẶNG THẾ HÙNG

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

LUẬN ÁN TIẾN SĨ KỸ THUẬT

Chuyên ngành: KỸ THUẬT ĐIỆN TỬ

Mã số: 9 52 02 03

NGƯỜI HƯỚNG DẪN KHOA HỌC:

1. TS TRẦN TRUNG DUY

2. PGS.TS ĐỖ QUỐC TRINH

HÀ NỘI - 2021

LỜI CAM ĐOAN

Tôi xin cam đoan các kết quả được trình bày trong Luận án là công trình nghiên cứu do tôi thực hiện dưới sự hướng dẫn khoa học của tập thể giáo viên hướng dẫn. Các số liệu, kết quả thể hiện trong Luận án là hoàn toàn trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác. Các kết quả sử dụng để tham khảo đã được trích dẫn đầy đủ, theo đúng quy định.

Hà Nội, ngày 06 tháng 01 năm 2021

Tác giả

Đặng Thế Hùng

LỜI CẢM ƠN

Luận án Tiến sĩ này được thực hiện tại Học viện Kỹ thuật Quân sự dưới sự hướng dẫn khoa học của TS Trần Trung Duy và PGS.TS Đỗ Quốc Trinh. Trong quá trình nghiên cứu và hoàn thành Luận án, tác giả đã nhận được nhiều sự quan tâm, giúp đỡ và đóng góp quý báu.

Trước tiên tác giả xin bày tỏ lòng biết ơn sâu sắc đến các Thầy giáo hướng dẫn đã luôn khuyến khích, động viên, tận tình giúp đỡ, thảo luận, rèn luyện tác phong kiên trì, nghiêm túc, chuyên nghiệp trong việc tiếp cận các vấn đề khoa học, tạo mọi điều kiện thuận lợi và tiếp thêm động lực, quyết tâm để vượt qua những thử thách, khó khăn trong suốt quá trình nghiên cứu.

Tác giả xin gửi lời cảm ơn đến Ban Giám đốc Học viện, Phòng Sau đại học, các Thầy giáo trong Ban chủ nhiệm Khoa Vô tuyến Điện tử, tập thể cán bộ, giáo viên Bộ môn Thông tin đã tạo điều kiện thuận lợi trong suốt quá trình tác giả học tập, sinh hoạt học thuật và hoàn thành công tác nghiên cứu.

Tiếp theo, tác giả xin chân thành cảm ơn Trường Đại học Thông tin liên lạc, Binh chủng Thông tin đã luôn tạo mọi điều kiện thuận lợi trong suốt quá trình học tập, nghiên cứu khoa học.

Tác giả cũng gửi lời cảm ơn chân thành đến Quỹ Phát triển Khoa học và Công nghệ Quốc gia (NAFOSTED) mã số 102.04-2017.317, Quỹ Nghiên cứu của Học viện Công nghệ Bưu chính Viễn thông mã số 09-HV-2018-RD_VT2, đã hỗ trợ một phần kinh phí trong công bố các công trình nghiên cứu.

Cuối cùng, tác giả xin gửi lời cảm ơn sâu sắc đến những người thân yêu trong gia đình, bạn bè và đồng nghiệp đã thường xuyên động viên, chia sẻ những khó khăn trong suốt khóa học để tác giả hoàn thành Luận án.

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Nghĩa Tiếng Anh	Nghĩa Tiếng Việt
5G	5th Generation	Mạng di động thế hệ thứ 5
ACK	Acknowledgement	Thông báo xác nhận
AF	Amplify-and-Forward	Khuếch đại và chuyển tiếp
AN	Artificial Noise	Nhiễu nhân tạo
ASC	Average Secrecy Capacity	Dung lượng bảo mật trung bình
AWGN	Additive White Gaussian Noise	Tạp âm Gauss trắng cộng
B	Beacon	Trạm phát sóng vô tuyến
BER	Bit Error Rate	Tốc độ lỗi bít
BS	Base Station	Trạm gốc
BP	Belief Propagation	Lan truyền niềm tin
CCI	Co-channel Interference	Nhiễu đồng kênh
CDF	Cumulative Distribution Function	Hàm phân bố tích lũy
CDM	Code Domain Multiplexing	Ghép kênh theo miền mã
CH	Cluster Head	Nút chủ cụm
CJ	Cooperative Jamming	Gây nhiễu cộng tác
CRN	Cognitive Radio Network	Mạng vô tuyến nhận thức
CSI	Channel State Information	Thông tin trạng thái kênh

D	Destination	Nút đích
DES	Data Encryption Standard	Tiêu chuẩn mã hóa bảo mật dữ liệu
DF	Decode-and-Forward	Giải mã và chuyển tiếp
E	Eavesdropper	Nút nghe lén
EGC	Equal-Gain Combining	Kết hợp cân bằng độ lợi
EH	Energy Harvesting	Thu thập năng lượng
FC	Fountain Code	Mã Fountain
FEC	Forward Error Correction	Sửa lỗi hướng đi
GE	Gaussian Elimination	Phép loại trừ Gauss
HJ	Harvest-to-Jam	Thu thập để gây nhiễu
HPA	High Power Amplifier	Khuếch đại công suất cao
HWI	Hardware Impairments	Suy giảm phần cứng
ID	Information Decoding	Giải mã thông tin
IoT	Internet of Things	Internet vạn vật
IP	Intercept Probability	Xác suất thu chặn
I/Q	In-phase and Quadrature-phase	Đồng pha và vuông pha
LEACH	Low Energy Adaptive Clustering Hierarchy	Phân cấp theo cụm thích ứng năng lượng thấp
LNA	Low Noise Amplifier	Khuếch đại tạp âm thấp
LOS	Line Of Sight	Tầm nhìn thẳng
LT	Luby Transform	Chuyển đổi Luby

MH	Multi-hop Communication	Truyền thông đa chặng
ML	Maximum Likelihood	Hợp lẽ cực đại
MIMO	Multi-Input Multi-Output	Đa đầu vào đa đầu ra
MISO	Multiple-Input Single-Output	Đa đầu vào đơn đầu ra
MRC	Maximal Ratio Combining	Kết hợp tỉ số tối đa
MRT	Maximal Ratio Transmission	Truyền tỉ số tối đa
MUST	Multiuser Superposition Transmission	Truyền dẫn xếp chồng đa người dùng
NOMA	Non-Orthogonal Multiple Access	Đa truy nhập không trực giao
NLOS	Non-Line-Of-Sight	Tầm nhìn không thẳng
OMA	Orthogonal Multiple Access	Đa truy nhập trực giao
OP	Outage Probability	Xác suất dừng
PDF	Probability Density Function	Hàm mật độ xác suất
PDM	Power Domain Multiplexing	Ghép kênh theo công suất
PU	Primary User	Người dùng sơ cấp
PT	Primary Transmitter	Máy phát sơ cấp
PR	Primary Receiver	Máy thu sơ cấp
PLS	Physical Layer Security	Bảo mật lớp vật lý
PN	Phase Noise	Nhiễu pha
PNSC	Probability of Non-zero Secrecy Capacity	Xác suất bảo mật khác không

PS	Power-splitting	Phân chia theo công suất
QoS	Quality of Sevice	Chất lượng dịch vụ
RC	Rateless Code	Mã Rateless
RF	Radio Frequency	Tần số vô tuyến
S	Source	Nút nguồn
SC	Selection Combining	Kết hợp có lựa chọn
SIC	Successive Interference Cancellation	Khử nhiễu nối tiếp
SINR	Signal-to-Interference-plus-Noise Ratio	Tỉ số tín hiệu trên nhiễu và tạp âm
SNR	Signal-to-Noise Ratio	Tỉ số tín hiệu trên tạp âm
SOP	Secrecy Outage Probability	Xác suất dừng bảo mật
SS	Successful and Secure Communication	Bảo mật thông tin thành công
SU	Secondary User	Người dùng thứ cấp
TAS	Transmit Antenna Selection	Lựa chọn ăng-ten phát
TDMA	Time Division Multiple Access	Đa truy nhập phân chia theo thời gian
TS	Average Number of Time Slots	Số khe thời gian trung bình
WSN	Wireless Sensor Network	Mạng cảm biến không dây
XOR	Exclusive-OR	Phép toán XOR

DANH MỤC HÌNH VẼ

DANH MỤC KÝ HIỆU TOÁN HỌC

Ký hiệu	Ý nghĩa
$a_1,\ a_2$	Hệ số phân bổ công suất của các tín hiệu NOMA, với $a_1 + a_2 = 1,\ a_1 > a_2 > 0$
C_{D}	Dung lượng từ đầu cuối đến đầu cuối của kênh dữ liệu
C_{E}	Dung lượng từ đầu cuối đến đầu cuối của kênh nghe lén
C_{th}	Tốc độ truyền mong muốn tại máy thu
$C_b^a \left(b \geq a\right)$	Hệ số nhị thức
$f_X\left(x\right)$	Hàm mật độ xác suất của biến ngẫu nhiên X
$F_X\left(x\right)$	Hàm phân bố tích lũy của biến ngẫu nhiên X
$I_0\left(.\right)$	Hàm Bessel sửa đổi loại 1
K_{D}	Hệ số K Rice của tất cả các kênh dữ liệu
K_{E}	Hệ số K Rice của liên kết $\mathrm{T}_{N-1} \rightarrow \mathrm{E}$
$K_{t+1}\left(.\right)$	Hàm Bessel sửa đổi loại 2
L	Số gói dữ liệu gốc tại nút nguồn
$N_{\mathrm{S}},\ N_{\mathrm{D}},\ N_{\mathrm{E}}$	Số ăng-ten tại nút nguồn (S), nút đích (D) và nghe lén (E)
N_{TS}	Số khe thời gian S sử dụng để phát các gói mã hóa đến D
$N_{\mathrm{req}}^{\mathrm{pkt}}$	Số gói mã hóa cần thiết để giải mã dữ liệu gốc
$N_{\mathrm{D}}^{\mathrm{pkt}},\ N_{\mathrm{E}}^{\mathrm{pkt}}$	Số gói mã hóa mà D và E có thể nhận thành công

$N_{\max}$	Số gói mã hóa tối đa mà nút nguồn có thể gửi đến nút đích
$Q_1(.)$	Hàm Marcum-Q
Q_n	Năng lượng được thu thập bởi nút T_n, với $n=0,1,...,N-1$
$\lfloor x \rfloor$	Số nguyên lớn nhất nhỏ hơn hoặc bằng x
$\lceil x \rceil$	Số nguyên nhỏ nhất bằng hoặc lớn hơn x
x^+	Phần dương của x, có nghĩa $x^+ = \max(0, x)$
$x_i[u]$	Tín hiệu phát thứ i trong NOMA, với $i=1,2,...$
$x_+[u]$	Tín hiệu xếp chồng tại nút nguồn trong NOMA
$y_{D,n}[u]$	Tín hiệu thu tại nút đích
$\exp(x)$	e^x
log	Lôgarit cơ số 2
τ	Tổng thời gian truyền mỗi gói mã hóa từ nguồn đến đích
$\alpha\tau(0 \le \alpha \le 1)$	Khoảng thời gian thu thập năng lượng từ trạm Beacon
$(1-\alpha)\tau$	Khoảng thời gian truyền dữ liệu
P	Công suất phát các CH trong giao thức LEACH không sử dụng gây nhiễu
P_X	Công suất phát của nút X
αP	Công suất phát các CH trong giao thức LEACH đề xuất $(0.5 \le \alpha \le 1)$
$(1-\alpha)P$	Công suất phát các nút gây nhiễu được lựa chọn

β	Hệ số suy hao hàm mũ
η	Hiệu suất chuyển đổi năng lượng $(0 \le \eta \le 1)$
$\eta_{t,X}$, $\eta_{r,Y}$	Nhiễu do phần cứng không lý tưởng tại nút X và Y
n_Y	Tạp âm Gauss tại nút Y
γ_{th}	Ngưỡng dừng tại máy thu
$\lambda_{X,Y}$	Tham số độ lợi kênh truyền giữa 2 nút X và Y
δ^2	Phương sai của tạp âm Gauss tại máy thu
ε	Phần thông tin bổ sung
$1+\varepsilon$	Giải mã không hiệu quả
ε_P	Ngưỡng dừng mong muốn của mạng sơ cấp
$\varepsilon\{.\}$	Toán tử kỳ vọng
$\kappa^2_{X,Y}$	Tổng mức suy giảm phần cứng giữa 2 nút X và Y
$d_{X,Y}$	Khoảng cách Euclid giữa 2 nút X và Y
$h_{X,Y}$	Hệ số pha đinh của kênh truyền từ X đến Y
$\gamma_{X,Y}$	Độ lợi kênh truyền giữa 2 nút X và Y, với $\gamma_{X,Y} = \lvert h_{X,Y} \rvert^2$
γ_P	Giá trị ngưỡng mà PR không thể giải mã dữ liệu từ PT
$\psi_{X,Y}$	SINR tức thời giữa 2 nút X và Y
$\chi_{D,0}$, $\chi_{D,1}$, $\chi_{D,2}$	Xác suất trong 1 khe thời gian D không nhận được gói nào, chỉ nhận 1 gói và nhận được cả 2 gói mã hóa
$\chi_{E,0}$, $\chi_{E,1}$, $\chi_{E,2}$	Xác suất trong 1 khe thời gian E không nhận được gói nào, chỉ nhận 1 gói và nhận được cả 2 gói mã hóa

MỞ ĐẦU

Trong những năm gần đây, với sự bùng nổ thông tin nói chung và truyền thông không dây nói riêng đã mang lại cho con người nhiều tiện ích, cơ hội tiếp cận các loại hình dịch vụ khác nhau. Để đáp ứng nhu cầu trên thì các hệ thống thông tin vô tuyến đã không ngừng cải tiến và phát triển cả về phần cứng cũng như phần mềm, với yêu cầu chất lượng dịch vụ ngày càng cao và dung lượng lớn [1]. Các hệ thống vô tuyến thế hệ sau luôn kế thừa những ưu điểm dựa trên nền tảng trước đó và tích hợp công nghệ tiên tiến để tạo ra các hệ thống mới có tính năng vượt trội nhằm đáp ứng nhu cầu ngày càng cao của người dùng. Tuy nhiên, cùng với sự phát triển đó, đã làm gia tăng các hành vi về ứng xử, đánh cắp thông tin, cản trở sự hoạt động của những người dùng hợp pháp trong mạng, do đó bảo đảm an toàn thông tin là một trong những yêu cầu cơ bản, cấp thiết, là mối quan tâm hàng đầu trong quá trình thiết kế các hệ thống thông tin hiện đại, đặc biệt trong các lĩnh vực hoạt động như chính phủ, quân đội, tài chính - ngân hàng và thông tin cá nhân [2].

Trong các hệ thống truyền thông không dây, do đặc tính quảng bá của kênh truyền vô tuyến, dẫn đến những nút nghe lén (eavesdroppers) có thể dễ dàng thu thập hoặc tấn công hay sửa đổi thông tin, do đó việc bảo đảm an toàn thông tin càng trở nên hết sức quan trọng. Trước tiên, kênh truyền vô tuyến rất dễ bị gây nhiễu (jamming), những người dùng hợp pháp không thể truy nhập vào mạng, loại tấn công này rất khó ngăn chặn vì mục tiêu của nút nghe lén nhắm tới là phá vỡ lưu lượng thông tin hơn là đánh cắp thông tin. Thứ hai, với một cơ chế nhận thực không tốt, kẻ tấn công có thể truy xuất tài nguyên mạng và vượt qua cơ sở hạ tầng bảo mật để đánh cắp thông tin. Cuối cùng, do đặc tính mở của kênh truyền vô tuyến, nút nghe lén có thể dễ dàng thu được tín hiệu mà không cần phải sử dụng các thiết bị phức tạp. Giải pháp

cho những vấn đề trên được đưa ra là dựa vào cách tiếp cận dạng lớp và với phương pháp truyền thống, đã thực hiện ở các lớp trên tầng vật lý, với việc sử dụng các thuật toán mã hóa và giải mã dữ liệu, như DES, RSA được phát triển rộng rãi để tăng cường mức độ bảo mật thông tin. Ưu điểm của các phương pháp này là thực hiện bảo mật trực tiếp và đang được sử dụng rộng rãi trong các hệ thống thông tin thực tế hiện nay. Tuy nhiên, nhược điểm là các thuật toán được thiết kế, cài đặt ở lớp ứng dụng, đòi hỏi yêu cầu về độ phức tạp cao, gây khó khăn cho việc triển khai mạng và thiết kế phần cứng, tiêu tốn năng lượng, khả năng xử lý của thiết bị phần cứng mạnh, thực hiện với giả sử rằng liên kết vật lý giữa máy phát và máy thu được thiết lập sẵn và không lỗi [2]. Ngoài ra, sử dụng các kỹ thuật mã hóa bảo mật cho hệ thống vô tuyến gây khó khăn trong việc phân bổ, chi phí quản lý khóa đối với các mạng phân tán, khóa hoặc bản tin có thể bị thu chặn. Hơn nữa, với sự phát triển mạnh mẽ của các hệ thống máy tính thì bảo mật dựa vào thời gian tính toán và bộ nhớ cần thiết để phá mã hiện tại, có thể không còn phù hợp trong tương lai. Khi thời gian và năng lực tính toán của hệ thống bẻ khóa ngày càng cao và có khả năng không còn bị giới hạn, ví dụ như máy tính lượng tử (quantum computer), dẫn đến các hệ thống vô tuyến có thể dễ dàng bị phá vỡ hàng rào bảo mật, đặc biệt là đối với các ứng dụng có yêu cầu bảo mật mạnh mẽ (như mạng quân sự), nên sẽ rất khó hiệu quả để bảo đảm an toàn thông tin. Ví dụ, phương thức mã hóa bảo mật dữ liệu tiêu chuẩn (Data Encryption Standard: DES), sử dụng khóa 56 bít, được thừa nhận bởi Cục Tiêu chuẩn Quốc gia Hoa Kỳ năm 1976. Tuy nhiên, mật mã DES công khai đã bị phá vỡ lần đầu tiên vào năm 1997 và hơn nữa, khóa DES bị phá vỡ bởi phần cứng Deep Crack chỉ trong 56 giờ vào năm 1998 [3]. Vậy nên, các thuật toán mật mã phải thường xuyên cập nhật nhằm đối mặt với khả năng tính toán ngày càng cao của hệ thống máy tính.

Để giải quyết vấn đề này, gần đây đã có nhiều nghiên cứu cả trong và ngoài nước [4-14], tập trung các vấn đề bảo mật lớp vật lý (Physical Layer

Security: PLS) và chỉ ra rằng lớp vật lý có thể nâng cao mức độ bảo mật cho hệ thống vô tuyến. Ý tưởng của PLS là khai thác các đặc tính vật lý của kênh truyền vô tuyến, như nhiễu và pha đinh đa đường, khoảng cách, tính linh động các nút trong mạng, nhằm tăng cường khả năng bảo mật hệ thống. Các đặc điểm trên, theo quan điểm truyền thống là các yếu tố gây ảnh hưởng và làm giảm chất lượng của mạng, nhưng ngược lại theo quan điểm PLS thì giúp tăng cường độ tin cậy, nâng cao hiệu năng bảo mật, chống lại việc nghe lén của hệ thống. PLS không phụ thuộc vào độ phức tạp tính toán, có nghĩa mức độ bảo mật đạt được sẽ không bị thỏa hiệp ngay cả khi các thiết bị thông minh không được phép có khả năng tính toán mạnh mẽ. Điều này trái ngược với mã hóa bảo mật dựa trên giả thiết các thiết bị bất hợp pháp có khả năng hạn chế với các vấn đề tính toán phức tạp. Hơn nữa, trong tương lai các thiết bị sẽ luôn kết nối đến các nút với công suất, khả năng tính toán và cấu trúc phân cấp khác nhau. Cũng vậy, do tính chất phân tán nên các thiết bị luôn tham gia hoặc rời khỏi mạng với thời gian ngẫu nhiên. Do đó, việc phân bổ và quản lý khóa mật càng trở nên thách thức, vì thế PLS có thể được sử dụng để cung cấp truyền dữ liệu bảo mật trực tiếp hoặc thuận tiện cho phân bổ khóa mật. Vậy nên, PLS đã thu hút được nhiều sự quan tâm và hứa hẹn là giải pháp đầy tiềm năng để ứng dụng rộng rãi vào các hệ thống thông tin vô tuyến thế hệ sau.

Hệ thống đa đầu vào đa đầu ra (Multiple-Input Multiple-Output: MIMO) là hệ thống truyền dẫn vô tuyến sử dụng đồng thời nhiều ăng-ten ở máy phát và máy thu để truyền nhiều dữ liệu theo không gian tại một thời điểm trên mỗi ăng-ten, nên có thể làm tăng đáng kể dung lượng và độ tin cậy hệ thống [15, 16]. Tuy nhiên, sử dụng nhiều ăng-ten yêu cầu triển khai nhiều chuỗi tần số vô tuyến (Radio Frequency: RF), làm tăng độ phức tạp phần cứng, kích thước, công suất tiêu thụ lớn và triển khai tốn kém. Để giải quyết vấn đề này, các hệ thống lựa chọn ăng-ten với chi phí và độ phức tạp thấp, nhưng vẫn bảo đảm được các ưu điểm của hệ thống MIMO, trong đó chỉ một tập con các

ăng-ten trong tổng số các ăng-ten sẵn có được hoạt động trong cùng thời điểm. Hơn nữa, lựa chọn ăng-ten cho hệ thống MIMO là yếu tố đầy tiềm năng để nâng cao dung lượng mà không cần sử dụng thêm công suất, băng thông và được xem là phương pháp thay thế với chi phí thấp để tối đa độ phức tạp của hệ thống MIMO [17]. Ngoài ra, tín hiệu MIMO có thể cải thiện truyền thông vô tuyến bằng hai cách khác nhau, đó là các phương pháp phân tập và ghép kênh không gian. Để nâng cao hiệu năng, các kỹ thuật phân tập như kết hợp lựa chọn (Selection Combining: SC), kết hợp cân bằng độ lợi (Equal Gain Combining: EGC) hay kết hợp tỉ số tối đa (Maximal Ratio Combining: MRC) có thể được sử dụng tại nút đích để kết hợp các tín hiệu nhận được từ nút nguồn, giúp cải thiện mạnh mẽ hệ thống về mặt tốc độ lỗi bít (Bit Error Rate: BER). Việc kết hợp các tín hiệu khác nhau giữa máy phát và máy thu một cách thích hợp, sẽ làm giảm ảnh hưởng của pha đinh và tăng độ tin cậy của tín hiệu phát mà không yêu cầu tăng công suất phát hoặc mở rộng băng thông [18]. Động lực quan trọng bởi các ứng dụng với các thiết bị đầu cuối đa ăng-ten, PLS trong các kênh MIMO gần đây đã được giải quyết từ góc độ của lý thuyết thông tin [19]. Hơn nữa, lựa chọn ăng-ten phát (Transmit Antenna Selection: TAS) để nâng cao hiệu quả bảo mật trong kênh MIMO với chi phí xử lý tín hiệu thấp và giảm độ phức tạp phần cứng đã được khảo sát [20].

Đa truy nhập không trực giao (Non-Orthogonal Multiple Access: NOMA) là kỹ thuật đa truy nhập hứa hẹn cho các mạng vô tuyến thế hệ tiếp theo, do hiệu quả sử dụng phổ cao, tăng thông lượng, mật độ kết nối lớn, độ trễ thấp và tính công bằng của các người dùng cao [21, 22]. Trái ngược với các hệ thống đa truy nhập trực giao (Orthogonal Multiple Access: OMA) thường dựa trên chia sẻ tài nguyên trực giao, NOMA có tiềm năng hỗ trợ số lượng người dùng cao hơn bằng cách ghép kênh các người dùng khác nhau trong cùng một tài nguyên không trực giao, do đó có thể hỗ trợ truyền dẫn lớn và cải thiện dung lượng hệ thống với nguồn tài nguyên hạn chế (phổ tần hoặc

ăng-ten). Gần đây, công nghệ đa ăng-ten đã được sử dụng trong các hệ thống NOMA và đã chứng minh rằng tốc độ tổng thể của hệ thống MIMO-NOMA hoàn toàn vượt trội so với MIMO-OMA [23]. Mặt khác, để giảm độ phức tạp phần cứng mà vẫn bảo tồn sự phân tập và lợi ích thông lượng, kỹ thuật TAS được công nhận là giải pháp đầy hiệu quả [24]. Hơn nữa, PLS thực hiện truyền bảo mật bằng cách sử dụng các đặc tính ngẫu nhiên và thay đổi theo thời gian của kênh truyền vô tuyến mà không có bất kỳ thuật toán mã hóa [5-14]. Hiệu năng bảo mật của NOMA đa ăng-ten với nhiễu nhân tạo (Artificial Noise: AN) được khảo sát, với các biểu thức chính xác và tiệm cận cho xác suất dừng bảo mật (Secrecy Outage Probability: SOP) đã được đưa ra [25]. Trong [26], đã khảo sát hiệu năng dừng bảo mật của hệ thống đa đầu vào đơn đầu ra (Multiple-Input Single-Output: MISO) NOMA với các phương thức TAS khác nhau, gồm một trạm gốc (Base Station: BS) đa ăng-ten, hai người dùng đường xuống và một nút nghe lén đơn ăng-ten. Các kết quả thể hiện, hiệu năng SOP của người dùng xa (far user) với phân bổ công suất cố định xấu hơn do công suất vượt quá ngưỡng cho phép và nhiễu nền từ người dùng gần (near user) tăng khi tăng công suất phát. Hơn nữa, phương pháp phân bổ năng lượng hiệu quả được đề xuất để đạt được bậc phân tập khác không trong tất cả các phương thức TAS, nên có thể nâng cao hiệu năng bảo mật hệ thống.

Truyền thông đa chặng là cách thức hiệu quả trong việc mở rộng vùng phủ sóng, cải thiện chất lượng tín hiệu, chống lại các ảnh hưởng của nhiễu và pha đinh mà không cần thêm tài nguyên mạng [27]. Trong khi truyền thông trực tiếp dẫn đến kết quả là hiệu năng bảo mật trong một số trường hợp bị suy giảm nghiêm trọng, thì việc thêm vào một số nút chuyển tiếp, giúp nâng cao độ tin cậy và tăng cường khả năng bảo mật hệ thống [28, 29].

Không giống với mã hóa tốc độ cố định, mã Fountain (Fountain Code: FC) [30-39] hay mã Rateless là mã không đưa ra tốc độ cố định, với số lượng các gói mã hóa được tạo ra từ dữ liệu nguồn có khả năng không giới hạn. Do

đó, FC có ưu điểm là không yêu cầu biết trước các điều kiện kênh truyền cụ thể và được áp dụng trong các hệ thống mã hóa có tốc độ không xác định trước. Việc khai thác các đặc tính FC dựa vào cơ chế hồi tiếp nhằm điều chỉnh linh hoạt bộ mã hóa Fountain để phù hợp với các điều kiện kênh thay đổi theo thời gian. Để đảm bảo truyền bảo mật, máy thu hợp pháp nhận đủ số gói mã hóa cần thiết nhằm phục hồi bản tin gốc và tốc độ giải mã đạt được cao hơn nút nghe lén [40-46]. Ngoài ra, phương pháp này không cần yêu cầu bổ sung thêm năng lượng và triển khai với độ phức tạp thấp. Tuy nhiên, theo khảo sát của tác giả, hiện nay chưa có nhiều công trình nghiên cứu, phân tích các giao thức sử dụng FC từ quan điểm bảo mật, do đó Luận án đề xuất các mô hình PLS trong hệ thống sử dụng FC với các giao thức MISO TAS, MIMO TAS/SC, MIMO-NOMA TAS SC/MRC, mạng đa chặng thu thập năng lượng và giao thức LEACH với gây nhiễu cộng tác. Phân tích hiệu năng hệ thống đề xuất nhằm bổ sung những khoảng trống bảo mật là vấn đề rất quan trọng, cần thiết và chính là mục tiêu nghiên cứu của Luận án.

Xuất phát từ thực tiễn, ý nghĩa khoa học, tác giả đã lựa chọn và thực hiện đề tài: *"Nghiên cứu hiệu năng bảo mật lớp vật lý của một số hệ thống thông tin vô tuyến sử dụng mã Fountain*". Các kết quả của đề tài sẽ góp phần quan trọng trong việc hoàn thiện xây dựng cơ sở lý thuyết, giải quyết bài toán phân tích hiệu năng bảo mật hệ thống với các mô hình được đề xuất, làm tiền đề áp dụng trong thực tiễn cho các mạng thông tin vô tuyến thế hệ tiếp theo.

1. MỤC TIÊU NGHIÊN CỨU

Trong Luận án này, tác giả giải quyết những vấn đề chính nhằm nâng cao hiệu năng bảo mật trong các mạng vô tuyến, cụ thể là:

• Nghiên cứu khả năng bảo đảm an toàn thông tin ở lớp vật lý, phân tích hiệu quả bảo mật của giao thức đề xuất trong các hệ thống vô tuyến sử dụng FC, như MISO TAS trong môi trường vô tuyến nhận thức dạng nền, MIMO TAS/SC, MIMO-NOMA TAS/SC/MRC, mạng chuyển tiếp đa chặng dựa vào

thu thập năng lượng sóng vô tuyến và giao thức LEACH đa chặng với gây nhiễu cộng tác;

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

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

2. PHẠM VI NGHIÊN CỨU

• Nghiên cứu lý thuyết an toàn thông tin, các giao thức PLS sử dụng FC, đặc tính và mô hình tính toán các loại kênh truyền;

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

• Các kỹ thuật lựa chọn ăng-ten phát, phân tập thu, thu thập năng lượng, gây nhiễu cộng tác và chuyển tiếp tín hiệu trong các mạng đa chặng để cải thiện hiệu quả bảo mật hệ thống ở lớp vật lý.

3. ĐỐI TƯỢNG NGHIÊN CỨU

• Kỹ thuật lựa chọn ăng-ten phát và các kỹ thuật kết hợp tại máy thu như SC hoặc MRC trong hệ thống MISO, MIMO, MIMO-NOMA với FC;

• Mạng đa chặng với thu thập năng lượng (Energy Harvesting: EH), giao thức LEACH với gây nhiễu cộng tác, các kỹ thuật xử lý tín hiệu tại nút chuyển tiếp như khuếch đại và chuyển tiếp (Amplify-and-Forward: AF) và giải mã và chuyển tiếp (Decode-and-Forward: DF) trong hệ thống FC;

• Các kênh truyền vô tuyến như pha đinh Rayleigh và pha đinh Rice.

4. PHƯƠNG PHÁP NGHIÊN CỨU

• Dựa trên cơ sở kết hợp phân tích lý thuyết và sử dụng các công cụ phần mềm toán học để kiểm chứng, mô phỏng;

• Xây dựng các mô hình toán học nhằm phân tích và đánh giá hiệu năng bảo mật của hệ thống thông qua các tham số đánh giá là xác suất giải mã và bảo mật thông tin thành công (Successful and Secure Communication: SS), xác

suất thu chặn (Intercept Probability: IP), số khe thời gian trung bình (Average Number of Time Slots: TS) và xác suất dừng (Outage Probability: OP);

• Dựa trên các mô hình đề xuất, sử dụng phần mềm Matlab để mô phỏng nhằm kiểm chứng các kết quả phân tích lý thuyết, khảo sát đặc tính thống kê trên kênh pha đinh Rayleigh phẳng, biến đổi chậm và kênh pha đinh Rice.

5. ĐÓNG GÓP CỦA LUẬN ÁN

Trong Luận án này, một số đóng góp chính được tóm tắt như sau:

• Đề xuất và phân tích hiệu năng bảo mật sử dụng FC như MISO TAS trong mạng vô tuyến nhận thức dạng nền, MIMO TAS/SC, dựa vào các biểu thức chính xác của SS và IP được đưa ra trên kênh truyền pha đinh Rayleigh. Các kết quả thể hiện, giao thoa đồng kênh, suy giảm phần cứng và các tham số đặc trưng của kênh truyền có tác động lớn đến hiệu năng bảo mật hệ thống;

• Đề xuất và đánh giá hiệu năng của FC với giao thức truyền bảo mật trong hệ thống MIMO-NOMA TAS/SC/MRC, dựa vào các biểu thức dạng tường minh TS và IP được đưa ra trên kênh truyền pha đinh Rayleigh. Các kết quả thể hiện giao thức sử dụng NOMA không chỉ giảm TS mà còn đạt được IP thấp hơn tại các tỉ số tín hiệu trên tạp âm (Signal-to-Noise Ratio: SNR) phát trung bình và cao so với giao thức tương ứng không sử dụng NOMA;

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

6. BỐ CỤC LUẬN ÁN

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

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

• **Chương 1:** NHỮNG VẤN ĐỀ CHUNG

Nội dung Chương này, trình bày các khái niệm cơ bản có liên quan trực tiếp đến Luận án, dựa vào những vấn đề được đề cập, làm cơ sở đề xuất các giao thức, trình bày cụ thể trong nội dung các Chương tiếp theo.

• **Chương 2:** HIỆU NĂNG BẢO MẬT TRONG CÁC MẠNG MISO TAS VÀ MIMO TAS/SC SỬ DỤNG MÃ FOUNTAIN

Trong Chương này, tác giả đưa ra hai mô hình, bao gồm mạng MISO TAS trong môi trường vô tuyến nhận thức dạng nền và mạng MIMO TAS/SC, đánh giá hiệu năng bảo mật dựa vào biểu thức SS và IP được đưa ra.

• **Chương 3:** HIỆU NĂNG BẢO MẬT TRONG MẠNG MIMO-NOMA TAS/SC/MRC SỬ DỤNG MÃ FOUNTAIN

Chương này, đánh giá hiệu năng của FC dựa vào các giao thức truyền bảo mật trong hệ thống MIMO-NOMA với TAS/SC/MRC, tác giả đưa ra các biểu thức chính xác của TS và IP trên kênh truyền pha đinh Rayleigh để phân tích mức độ bảo mật đạt được của giao thức đề xuất.

• **Chương 4:** HIỆU NĂNG BẢO MẬT TRONG CÁC MẠNG CHUYỂN TIẾP ĐA CHẶNG SỬ DỤNG MÃ FOUNTAIN

Nội dung Chương này trình bày hai giao thức của mạng chuyển tiếp đa chặng sử dụng FC, cụ thể: phân tích hiệu năng bảo mật trong mạng đa chặng với thu thập năng lượng sóng vô tuyến từ trạm Beacon; tiếp theo, khảo sát sự đánh đổi giữa bảo mật và độ tin cậy của giao thức LEACH đa chặng trong WSN với nút tạo nhiễu cộng tác. Đánh giá hiệu năng dựa vào các biểu thức chính xác OP và IP trên kênh truyền pha đinh Rayleigh được đưa ra.

Cuối cùng, tác giả thực hiện các mô phỏng máy tính để kiểm chứng các kết quả phân tích lý thuyết.

Chương 1
NHỮNG VẤN ĐỀ CHUNG

1.1. MỘT SỐ KHÁI NIỆM CƠ BẢN VỀ BẢO MẬT THÔNG TIN

1.1.1. Một số khái niệm và giới hạn của mã hóa bảo mật hiện đại

Cùng với sự phát triển nhanh chóng của lưu lượng truy cập di động và ứng dụng mới của các thiết bị, do đặc tính quảng bá tự nhiên của kênh truyền vô tuyến, dẫn đến nhiều nguy cơ bảo mật khác nhau. Vậy nên, cần phải tăng cường bảo mật hệ thống do kênh truyền vô tuyến rất dễ bị nghe lén và thu chặn tín hiệu [47]. Các liên kết truyền thông bảo mật trong mạng vô tuyến truyền thống được thiết lập thông qua các phương pháp mã hóa bảo mật thông thường. Tuy nhiên, các phương pháp này đặt ra những thách thức khác nhau trong việc trao đổi và phân bổ khóa mật [48], đặc biệt là các cấu hình mạng trong tương lai. Để bảo đảm an toàn thông tin, bản tin trước khi truyền sẽ thực hiện mã hóa bảo mật dựa trên các thuật toán mật mã với các chuỗi bít bí mật chỉ được biết bởi máy phát và máy thu hợp pháp, gọi là khóa mật (secret key) [49]. Nút nghe lén với mục tiêu thu thập thông tin để phá được khóa mã nhằm giải mã bản tin gốc, nhưng không biết khóa mật được sử dụng bởi máy phát và máy thu hợp pháp. Do vậy, mức độ bảo mật của các hệ thống mã hóa bảo mật thường được đo bởi số phép tính và thời gian để phá được mã mật. Hơn nữa, các thuật toán này cần phải thường xuyên được cập nhật để chống lại khả năng tính toán ngày càng cao của các hệ thống máy tính hiện đại.

Đối với các hệ thống thông tin thực tế hiện nay, có hai giao thức mã hóa bảo mật đang được sử dụng rộng rãi là mã hóa đối xứng và mã hóa công khai. Trong khi mã hóa đối xứng có ưu điểm là sử dụng các khóa mật tương đối ngắn để mật mã bản tin, nên có thể hoạt động ở tốc độ cao. Tuy nhiên, mức độ bảo mật không chỉ phụ thuộc vào các thuật toán khó để thực hiện phá mã

mà còn phụ thuộc vào hiệu quả của việc phân bổ và quản lý khóa mật. Để giải quyết vấn đề này thì giao thức mã hóa công khai (public key) hay mã hóa bất đối xứng đã được đưa ra, trong đó máy phát và máy thu hợp pháp sử dụng các khóa mật riêng biệt và khóa công khai luôn có sẵn để máy phát mã hóa bảo mật bản tin. Có nghĩa rằng, khóa công khai có chức năng như một ổ khóa mà bất cứ ai cũng có thể đóng (mã hóa bảo mật bản tin), nhưng chỉ có máy thu hợp pháp mới mở được vì có khóa mật cá nhân (private key), do đó khóa mật mã cá nhân được sử dụng cho việc giải mã thông tin và được giữ bí mật tại người dùng hợp pháp. Tuy nhiên, cùng với sự phát triển mạnh mẽ của công nghệ tính toán, thì phép đo mức độ bảo mật dựa trên thời gian và bộ nhớ lưu trữ cần thiết để phá mã mật là rất khó khả thi. Mặc dù phép đo bảo mật đang được sử dụng trong hầu hết các hệ thống thông tin hiện nay, nhưng khi khả năng tính toán của máy tính ngày càng mạnh mẽ, ví dụ máy tính lượng tử (quantum computer), mức độ tính toán của những giải thuật dựa trên mã hóa bảo mật có thể tồn tại trong một khoảng thời gian hạn chế nhất định, khiến nhiều hệ thống mật mã hiện tại có thể bị phá vỡ [48].

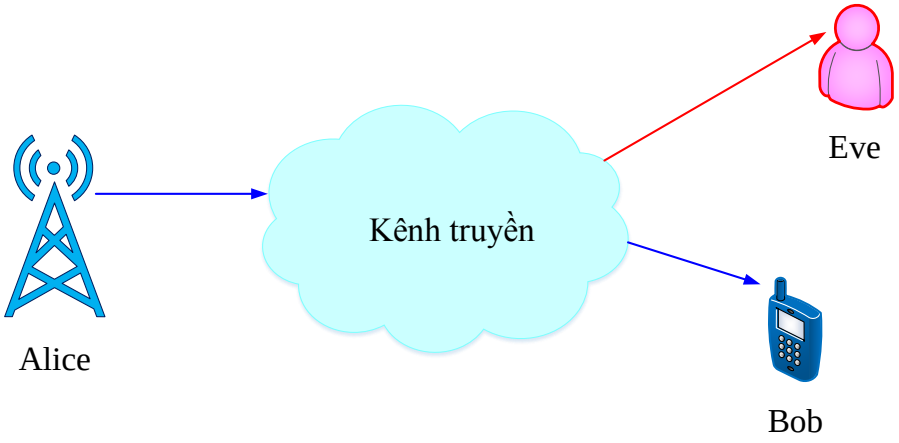
1.1.2. Các nghiên cứu tiên phong của PLS

Cơ sở lý thuyết của PLS bắt đầu từ khái niệm bảo mật hoàn hảo (perfect secrecy) của Shannon vào năm 1949 [4], đã chứng minh tồn tại phương pháp mã hóa để đạt được bảo mật hoàn hảo, nếu độ bất định của bản tin sau khi quan sát từ mã bằng độ bất định của thông tin bản tin trước đó hoặc thông tin lẫn nhau giữa bản tin và từ mã bằng không, dựa trên khái niệm bảo mật hoàn hảo thì nút nghe lén không có cách nào suy luận được bản tin mà không có khóa mã. Khái niệm này được chấp nhận rộng rãi là thước đo bảo mật chặt chẽ nhất, nhưng lại không đặt ra bất kỳ giới hạn nào về khả năng tính toán của nút nghe lén. Do không có sự tương quan giữa bản tin và từ mã nên bảo mật hoàn hảo có thể miễn dịch với tất cả các thuật toán phân tích mã, Shannon đã chứng minh rằng dạng mật mã nhằm thỏa mãn điều kiện này là sử dụng khóa

mã một lần (one-time pad) và điều kiện duy nhất để áp dụng khóa mã một lần là độ dài của khóa lớn hơn hoặc bằng chiều dài bản tin, sử dụng thuật toán Modulo 2 để mật mã và giải mã bản tin. Tuy nhiên, có nhiều hạn chế đối với bảo mật hoàn hảo, vì mỗi khóa bít chỉ sử dụng một lần, cho nên không thể đạt được bảo mật hoàn hảo bằng việc sử dụng các kỹ thuật mật mã hóa hiện đại, do cơ chế phân bổ khóa mật chủ yếu dựa vào việc sử dụng lại một số ít lần trong các hệ thống thông tin thực tế. Do vậy, việc thực hiện bảo mật hoàn hảo là không khả thi, trừ khi có một phương pháp phân bổ khóa mật hiệu quả giữa máy phát và máy thu hợp pháp. Ngoài ra, việc khởi tạo và lưu trữ các khóa mật có chiều dài bằng với độ dài bản tin là không thực tế, do chi phí tính toán và yêu cầu lưu trữ cần thiết cho các khóa. Hơn nữa, các khóa mới phải được tạo ra theo chu kỳ, điều kiện bảo mật hoàn hảo sẽ bị thỏa hiệp nếu cùng một khóa được sử dụng để mã hóa hai bản tin khác nhau. Trong mật mã hiện đại, các hệ thống mật mã thực tế đều dựa trên giả định bi quan của Shannnon. Do những ràng buộc thực tế, các khóa bí mật ngắn hơn nhiều so với bản tin và do đó, các hệ thống mật mã thực tế này về mặt lý thuyết dễ bị phá vỡ bởi những kẻ tấn công. Tuy nhiên, mục tiêu của việc thiết kế các mật mã thực tế như vậy là để đảm bảo rằng không tồn tại thuật toán hiệu quả để phá vỡ chúng.

Dựa trên khái niệm này, Wyner [5] đã khởi đầu trong công trình nghiên cứu tiên phong về PLS từ kênh nghe lén cơ bản, như miêu tả trong Hình 1.1. Đây là mô hình đơn giản nhất để nghiên cứu bảo mật thông tin và gọi là mô hình kênh nghe lén bị suy giảm (degraded wiretap channel), khai thác đặc tính ngẫu nhiên của các kênh truyền vô tuyến để bảo đảm bí mật của bản tin phát. Wyner đã chỉ ra rằng kết quả tiêu cực ở trên là hệ quả của giả định giới hạn Shannon, rằng nút nghe lén có quyền truy nhập chính xác thông tin tương tự như máy thu hợp pháp. Wyner đã xem xét kịch bản, trong đó một nút nghe lén nhận được tín hiệu phát trên kênh bị suy giảm liên quan đến kênh máy thu hợp pháp, giả sử rằng nút nghe lén không có giới hạn tính toán và biết được từ

mã sử dụng bởi máy phát. Các kết quả thể hiện, sự mù mờ bản tin tại nút nghe lén có thể đạt được dung lượng bảo mật hoàn hảo không âm cho kịch bản này.



Hình 1.1: Mô hình kênh nghe lén.

Trong mô hình xem xét như Hình 1.1, máy phát (Alice) phát bản tin đến máy thu hợp pháp (Bob), trong khi giữ bản tin bí mật đối với nút nghe lén (Eve). Lý thuyết bảo mật thông tin cho phép xác định phép đo bảo mật trong mô hình này dựa vào dung lượng bảo mật (secrecy capacity), là tốc độ bảo mật lớn nhất mà tại đó bản tin có thể được phát một cách tin cậy và bảo mật.

$$C_s = \left[C_M - C_E\right]^+, \tag{1.1}$$

trong đó, $\left[x\right]^+ = \max\left(x, 0\right)$ và dung lượng của kênh chính và kênh nghe lén lần lượt là C_M và C_E.

Hơn nữa, từ (1.1), ta thấy rằng nếu $C_s > 0,$ truyền thông bảo mật không cần khóa có thể được thực hiện miễn là chất lượng kênh hợp pháp lớn hơn kênh nghe lén và ngược lại $C_s = 0,$ có nghĩa là không có truyền thông bảo mật giữa Alice và Bob. Lưu ý rằng mô hình kênh nghe lén được giới thiệu bởi Wyner khác với hệ thống mật mã Shannon, bao gồm có nhiễu trên kênh truyền và không có bất kỳ khóa mật chung nào giữa Alice và Bob, nên cho phép thiết kế từ mã độc lập.

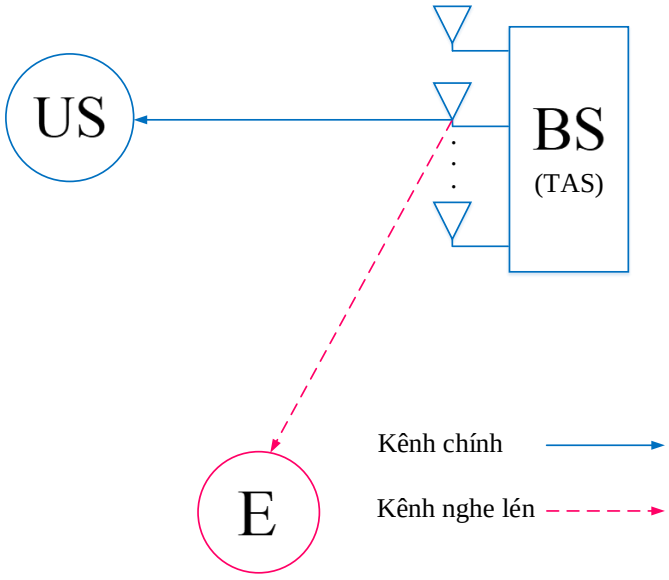
Sau đó, công trình của Wyner đã được khái quát cho một số kịch bản quan trọng khác. Năm 1978, Csiszár và Körner đã nghiên cứu các kênh không bị suy giảm và thể hiện rằng có khả năng đạt được dung lượng bảo mật khác không (non-zero secrecy capacity) nếu chất lượng kênh chính lớn hơn kênh nghe lén [6]. Trong cùng năm đó, kết quả của Wyner cho các kênh không nhớ rời rạc cũng được mở rộng cho kênh Gauss [7]. Tuy nhiên, trong suốt thời gian dài kể từ khi công trình của Wyner công bố, kỹ thuật PLS đã không thu hút được nhiều sự quan tâm. Điều này được giải thích vì các lý do sau: trước tiên, dung lượng bảo mật có thể đạt được phụ thuộc vào sử dụng mã hóa ngẫu nhiên, nhưng cực kỳ khó khăn để xây dựng mã ngẫu nhiên thực tế với độ phức tạp có thể chấp nhận được; thứ hai, để đạt được dung lượng bảo mật dương, SNR của kênh chính phải lớn hơn kênh nghe lén, điều này khó được đảm bảo trong môi trường vô tuyến. Mặt khác, ngay sau khi khái niệm dung lượng bảo mật được đề xuất, Diffie và Hellman đã phát minh ra mật mã khóa công khai dựa trên các hàm toán học được cho là khó tính toán và đã chi phối nghiên cứu bảo mật kể từ khi xuất hiện và do đó, lý thuyết bảo mật thông tin chạm đến một điểm thấp trong những năm 1970 và thập niên 1980.

Gần đây, nhiều ứng dụng dịch vụ vô tuyến ngày càng phổ biến, vấn đề bảo mật trở nên quan trọng hơn, do đó nhiều công trình nghiên cứu để khảo sát PLS từ cả hai khía cạnh lý thuyết và thực tế. Các kỹ thuật mã hóa kênh nâng cao [8-10], được đề xuất nhằm đạt được dung lượng bảo mật. Tuy nhiên, tương tự các mạng truyền thông mà không có ràng buộc bảo mật, hiệu năng tổng thể bị giới hạn bởi các điều kiện kênh truyền. Đặc biệt, để truyền bảo mật, Alice và Bob cần có một số lợi thế so với Eve, ví dụ chất lượng kênh tốt hơn hoặc truy nhập đến một kênh hồi tiếp. Nhiều kỹ thuật được đề xuất để vượt qua các giới hạn này, như sử dụng các hệ thống đa ăng-ten MIMO, bảo mật của các hệ thống đa người dùng, đặc biệt nhấn mạnh khả năng cộng tác giữa các người dùng để nâng cao hiệu quả bảo mật.

1.2. BẢO MẬT LỚP VẬT LÝ TRONG HỆ THỐNG MIMO

1.2.1. Bảo mật lớp vật lý trong các hệ thống MIMO lựa chọn ăng-ten

Hệ thống MIMO với nhiều ăng-ten tại cả máy phát và máy thu có thể làm tăng đáng kể dung lượng và độ tin cậy hệ thống, bằng việc sử dụng nhiều đường giữa máy phát và máy thu. Tuy nhiên, sử dụng đa ăng-ten yêu cầu triển khai nhiều chuỗi RF, dẫn đến độ phức tạp phần cứng, kích thước, công suất tiêu thụ lớn và chi phí triển khai tốn kém. Để giải quyết vấn đề này, kỹ thuật TAS với chi phí, độ phức tạp thấp, đã được đề xuất [50] để khai thác các ưu điểm của hệ thống MIMO, nhưng sử dụng ít chuỗi RF hơn. Phương pháp này là yếu tố đầy tiềm năng để nâng cao dung lượng hệ thống mà không cần sử dụng thêm công suất và băng thông, chỉ một tập con các ăng-ten trong tổng số các ăng-ten sẵn có được hoạt động trong cùng thời điểm. Các kỹ thuật lựa chọn ăng-ten độ phức tạp thấp đã được đề nghị và chuẩn hóa trong IEEE 802.11n cho WLAN [51], IEEE 802.16 cho WiMAX [52], Long Term Evolution (LTE) và LTE-Advanced [53].



Hình 1.2: Mô hình cơ bản hệ thống với kỹ thuật TAS ở máy phát.

Trường hợp TAS dựa vào SNR nhận được, trong đó một ăng-ten được lựa chọn tại máy phát để tối đa SNR tức thời sẽ được ước lượng tại máy thu

và thông tin sẵn có tại máy phát thông qua kênh hồi tiếp tốc độ thấp, để máy thu có thể gửi thông tin về chỉ số ăng-ten tối đa SNR tức thời nhận được. Dựa vào thông tin phản hồi, bộ lựa chọn ăng-ten thực hiện kết nối đến ăng-ten tương ứng để gửi dữ liệu điều chế thích hợp. Trong đó, khối lựa chọn ăng-ten có thể chỉ yêu cầu một bộ chuyển mạch RF, mà không cần đầy đủ tập RF tại mỗi ăng-ten của máy phát và để lựa chọn một ăng-ten phát, tập chuỗi tín hiệu hoa tiêu (pilot) được phát lần lượt từ các ăng-ten phát cho mỗi lần truyền.

PLS sử dụng lựa chọn ăng-ten phát để nâng cao hiệu năng bảo mật đã được khảo sát [19, 20]. Như thể hiện trong Hình 1.2, giả sử hệ thống gồm một BS trang bị M ăng-ten sử dụng TAS và máy thu hợp pháp (User: US), trong sự xuất hiện của nút nghe lén (Eavesdropper: E), các thiết bị đầu cuối là đơn ăng-ten. Máy phát sử dụng TAS trên kênh chính để khai thác những ưu điểm của phương pháp này như chi phí và độ phức tạp thấp. Trong hệ thống xem xét, US thông báo cho máy phát chỉ số ăng-ten tốt nhất thông qua kênh hồi tiếp (không đảm bảo an toàn) với tốc độ truyền thấp và tín hiệu hồi tiếp này cung cấp CSI đến máy phát. Sau đó, máy phát sử dụng chỉ số ăng-ten này để kết nối đến ăng-ten phát tương ứng và truyền tín hiệu phù hợp đến máy thu, mặc dù máy nghe lén có thể truy nhập được các kênh truyền mở nhưng chỉ biết được chỉ số ăng-ten, mà không thể khai thác bất kỳ sự phân tập nào từ máy phát. Do vậy, hệ thống sử dụng TAS sẽ tăng dung lượng kênh hợp pháp càng lớn hơn kênh nghe lén khi tăng số ăng-ten phát.

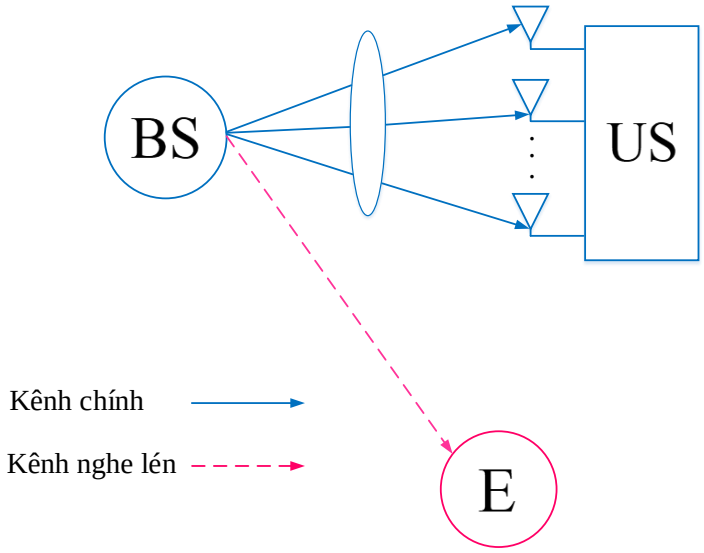
Biểu thức lựa chọn ăng-ten phát tốt nhất (ký hiệu ăntен b) là:

$$b : \gamma_{b\mathrm{U}} = \max_{i=1,2,\ldots,M} \left(\gamma_{i\mathrm{U}}\right), \tag{1.2}$$

1.2.2. Bảo mật lớp vật lý với kỹ thuật phân tập thu

Trong thông tin vô tuyến, các kỹ thuật phân tập được sử dụng rộng rãi để giảm ảnh hưởng của pha đinh đa đường, cải thiện độ tin cậy truyền dẫn mà không phải tăng công suất phát hoặc mở rộng băng thông. Ý tưởng cơ bản của

phân tập là nếu hai hoặc nhiều mẫu tín hiệu độc lập được đưa tới và bị ảnh hưởng của pha đinh độc lập, có nghĩa các tín hiệu chịu tác động của pha đinh khác nhau. Do đó, bằng cách kết hợp một cách thích hợp các mẫu khác nhau sẽ giảm ảnh hưởng của pha đinh và tăng độ tin cậy của tín hiệu phát.



Hình 1.3: Mô hình cơ bản hệ thống phân tập sử dụng đa ăng-ten ở máy thu.

Trên cơ sở toán học thực hiện phân tích các tham số hiệu năng bảo mật thể hiện rằng, khả năng bảo mật được cải thiện khi SNR của kênh chính lớn hơn nhiều so với kênh nghe lén. Giải pháp để cải thiện vấn đề này là dùng các kỹ thuật phân tập thu ở kênh chính với việc sử dụng nhiều ăng-ten. Với giả sử máy nghe lén chiếm giữ một lượng thông tin cố định, để tăng dung lượng cho người dùng hợp pháp ta có thể tăng công suất phát hoặc máy phát sử dụng nhiều ăng-ten, như vậy cũng làm tăng hiệu suất thu của máy nghe lén, nên giải pháp này có thể sẽ không hiệu quả. Như thể hiện trong Hình 1.3, gồm BS đơn ăng-ten, giả sử rằng cài đặt nhiều ăng-ten ở máy thu hợp pháp và sử dụng kỹ thuật phân tập thu để nâng cao dung lượng bảo mật trên kênh chính, trong khi dung lượng kênh truyền của máy nghe lén đơn ăng-ten không thay đổi. Phương pháp này cho phép nâng cao dung lượng kênh thông tin, do đó dung lượng bảo mật hệ thống được cải thiện đáng kể.

Trong các kỹ thuật phân tập thu, MRC cho hiệu năng và các thông số bảo mật tối ưu nhất, nhưng độ phức tạp phần cứng tăng tuyến tính theo số ăng-ten thu. Do đó, trong một số hệ thống xem xét sự ràng buộc về phần cứng và mức năng lượng thì việc sử dụng các kỹ thuật phân tập khác có độ phức tạp thấp hơn như SC hoặc EGC trong thiết kế hệ thống là rất quan trọng. Các kỹ thuật phân tập được xem xét như sau:

• Kỹ thuật phân tập MRC với M ăng-ten ở máy thu:

$$\gamma_{\mathrm{MRC}} = \sum_{i=1}^{M} \gamma_{i\mathrm{U}}, \tag{1.3}$$

trong đó, γ ký hiệu là SNR tương đương của nhánh thứ *i*.

• Kỹ thuật phân tập SC với M ăng-ten ở máy thu:

$$\gamma_{\mathrm{SC}} = \max_{i=1,2,\ldots,M} \left(\gamma_{i\mathrm{U}}\right). \tag{1.4}$$

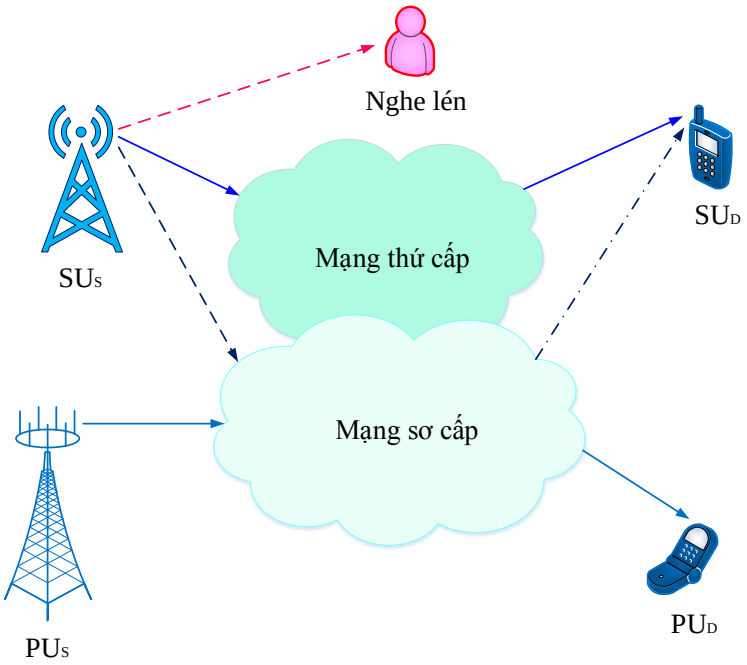
• Kỹ thuật phân tập EGC với M ăng-ten ở máy thu:

$$\gamma_{\mathrm{EGC}} = \left(\sum_{i=1}^{M} \sqrt{\gamma_{i\mathrm{U}}} \right)^2 \Big/ M. \tag{1.5}$$

1.3. BẢO MẬT TRONG MẠNG VÔ TUYẾN NHẬN THỨC

Vấn đề khan hiếm phổ ngày càng trở nên là mối quan tâm lớn đối với thiết kế hệ thống và hoạch định chính sách viễn thông. Trong khung điều chỉnh phổ hiện tại, tất cả các dải tần số được phân bổ độc quyền cho các dịch vụ cụ thể và không cho phép vi phạm từ những người dùng không được cấp phép. Để giải quyết sự xung đột giữa khan hiếm phổ tần và phổ tần dưới mức sử dụng, mạng vô tuyến nhận thức [54] (Cognitive Radio Network: CRN) lần đầu tiên được đề xuất bởi Mitola vào năm 1999, nhằm giải quyết vấn đề khan hiếm phổ tần và sử dụng phổ tần hiệu quả hơn. Trong CRN, mạng sơ cấp hay các người dùng được cấp phép sử dụng tần số (Primary User: PU) có thể chia sẻ phổ tần với những người dùng không được phép sử dụng tần số (unlicensed) hay người dùng thứ cấp (Secondary User: SU), theo các kịch bản

như dạng nền (underlay), chồng (overlay) hoặc xen kẻ (interweave), để tận dụng các khoảng phổ tần nhàn rỗi.



Hình 1.4: Minh họa mô hình bảo mật mạng vô tuyến nhận thức dạng nền.

Theo phương pháp dạng chồng hay xen kẻ, SU phải thăm dò hoạt động của PU để có thể truy nhập vào những phổ tần trống. Nhưng các phương pháp này không hiệu quả bởi hoạt động của SU phụ thuộc quá nhiều vào sự xuất hiện của PU. Hơn thế nữa, khi quá trình thăm dò xảy ra sai sót, chất lượng dịch vụ của mạng sơ cấp có thể bị ảnh hưởng nghiêm trọng bởi giao thoa gây ra từ mạng thứ cấp. Do đó, phương pháp chia sẻ phổ tần dạng nền [97], cho phép SU hoạt động song song với PU, trở nên hiệu quả nhằm bảo đảm truyền dữ liệu liên tục cho mạng thứ cấp. Tuy nhiên, điều kiện ràng buộc là SU phải hiệu chỉnh công suất phát để thỏa mãn ràng buộc ngưỡng nhiễu và không làm ảnh hưởng đến chất lượng dịch vụ của PU. Vậy nên, hiệu năng mạng thứ cấp trong CRN dạng nền bị suy giảm nghiêm trọng do công suất truyền dẫn bị giới hạn. Vì thế, vấn đề bảo mật thông tin trong mạng vô tuyến nhận thức dạng nền [55-64] hiện đang trở thành một chủ đề thu hút nhiều sự quan tâm của các nhà nghiên cứu trong và ngoài nước.

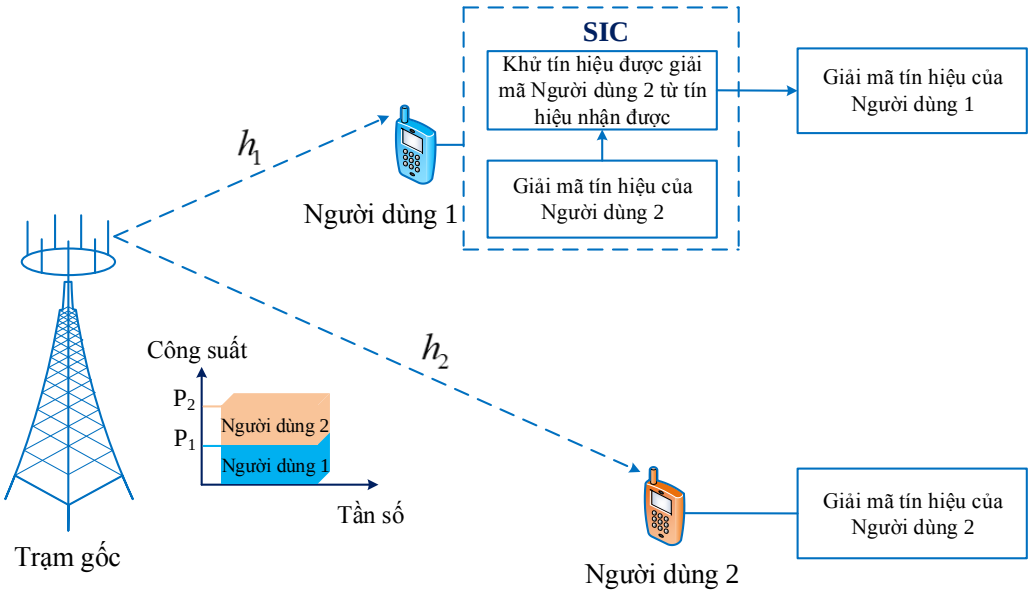
1.4. KỸ THUẬT ĐA TRUY NHẬP KHÔNG TRỰC GIAO

Gần đây, NOMA đã được chấp nhận như là một công nghệ tiềm năng cho các mạng di động thế hệ thứ 5 (The Fifth Generation: 5G) trước sự bùng nổ của nhu cầu lưu lượng dữ liệu [21, 22]. Hơn nữa, NOMA còn có khả năng tương thích với các công nghệ khác, nên dễ dàng tích hợp với các hệ thống không dây hiện tại và tương lai. Trái ngược với OMA thông thường, (ví dụ: đa truy nhập phân chia thời gian/ tần số/ mã), NOMA có thể cải thiện đáng kể hiệu quả phổ tần bằng cách cung cấp nhiều người dùng đồng thời thông qua ghép kênh theo miền công suất. Nhìn chung, các phương pháp NOMA hiện tại được phân thành hai loại: NOMA ghép kênh theo miền công suất (Power Domain Multiplexing: PDM-NOMA) và NOMA ghép kênh theo miền mã (Code Domain Multiplexing: CDM-NOMA).

Trong mục này chỉ tập trung thảo luận PDM-NOMA và ý tưởng chính của PDM-NOMA là sử dụng hiệu quả miền công suất cho đa truy nhập để đồng thời phục vụ nhiều người dùng trong cùng một khe thời gian, dải tần và mã, bằng phương pháp mã hóa xếp chồng (Superposition Coding: SC) tại máy phát. Trong đó, mức công suất cho một người dùng được quyết định dựa trên độ lợi kênh, với người dùng có độ lợi kênh cao hơn thường được gán mức công suất thấp hơn. Tại máy thu, các tín hiệu người dùng khác nhau được phân tách bằng cách khai thác sự khác biệt về công suất người dùng dựa trên SIC [22]. Những thách thức PDM-NOMA là khả năng phân bổ hệ số công suất phù hợp theo điều kiện kênh của mỗi người dùng cũng như cơ hội hợp nhất NOMA với các phương pháp điều chế và mã hóa thích ứng để nâng cao dung lượng hệ thống và tốc độ tổng người dùng. Để giải quyết vấn đề này, BS cần phải biết CSI của mỗi người dùng.

Xem xét hệ thống NOMA đường xuống miền công suất như Hình 1.5, theo nguyên tắc NOMA, tại BS thực hiện phân bổ công suất lớn hơn cho các người dùng có điều kiện kênh kém và ngược lại [22]. Giả sử người dùng 1 có

độ lợi kênh truyền lớn hơn người dùng 2, do đó thực hiện phân bổ mức công suất cao hơn để tăng tỉ số tín hiệu trên nhiễu và tạp âm (Signal-to-Interference-plus-Noise Ratio: SINR) tại người dùng 2, cụ thể $|h_1|^2 > |h_2|^2$ và các hệ số phân bổ công suất được đặt là $0 < a_1 < a_2$.



Hình 1.5: NOMA đường xuống miền công suất hai người dùng.

Sử dụng mã hóa xếp chồng, BS tạo tín hiệu xếp chồng và truyền đồng thời đến người dùng 1 và 2. Tín hiệu xếp chồng s tại BS được viết là

$$s = \sqrt{a_1 P_S} x_1 + \sqrt{a_2 P_S} x_2, \tag{1.6}$$

trong đó, P_S là công suất phát của BS, a_1 và a_2 là các hệ số phân bổ công suất, với $a_1 + a_2 = 1$, và tín hiệu bản tin x_m, $\{m = 1, 2\}$.

Tín hiệu nhận được tại người dùng m, $\{m = 1, 2\}$, được biểu diễn là

$$y_m = h_m s + n_m, \tag{1.7}$$

với h_m là hệ số kênh truyền giữa BS và người dùng m và n_m là tạp âm Gauss trắng cộng (Additive White Gaussian Noise: AWGN) tại máy thu người dùng m, có trung bình bằng 0 và phương sai σ^2, ta giả sử $\sigma_1^2 = \sigma_2^2 = \sigma^2$.

Để giải mã bản tin của người dùng m, $\{m=1,\ 2\}$, từ tín hiệu xếp chồng s, phương pháp SIC được thực hiện dựa vào sử dụng mức phân bổ công suất khác nhau giữa các người dùng trong mã hóa xếp chồng [21, 22]. Ý tưởng cơ bản của SIC là tín hiệu người dùng được giải mã liên tiếp, trong đó người dùng có cường độ tín hiệu lớn nhất được giải mã trước, bằng cách xem tín hiệu của các người dùng khác là nhiễu. Sau khi tín hiệu của một người dùng được giải mã, tín hiệu này sẽ được loại bỏ khỏi tín hiệu kết hợp trước khi tín hiệu của người dùng tiếp theo được giải mã. Quá trình tương tự được thực hiện lặp lại cho đến khi tín hiệu mong muốn được giải mã. Với thứ tự này, mỗi người dùng có thể loại bỏ đáng kể can nhiễu từ tín hiệu của các người dùng khác có thứ tự giải mã xuất hiện sau người dùng đó. Lưu ý rằng BS định kỳ thực hiện thứ tự SIC dựa vào CSI hồi tiếp nhận được từ các người dùng và người dùng nhận thông tin được cập nhật thứ tự SIC từ BS. Trong Hình 1.5, đối với người dùng 1, trước tiên giải mã tín hiệu x_2 của người dùng 2 và loại bỏ tín hiệu này từ tín hiệu nhận được y_1, sau đó giải mã tín hiệu của chính mình. Đối với người dùng 2, xem tín hiệu x_1 của người dùng 1 là tạp âm và do đó giải mã trực tiếp tín hiệu của chính mình từ y_2 mà không thực hiện SIC. Nếu SIC hoàn hảo, tốc độ dữ liệu có thể đạt được của người dùng NOMA thứ m, $\{m=1,\ 2\}$, R_m^{NOMA} truyền dẫn băng thông 1 Hz được viết là

$$R_1^{\mathrm{NOMA}}=\log_2\left(1+a_1\rho\left|h_1\right|^2\right),\ \ R_2^{\mathrm{NOMA}}=\log_2\left(1+\frac{a_2\left|h_2\right|^2}{a_1\left|h_2\right|^2+1/\rho}\right), \qquad (1.8)$$

với $\rho=P_{\mathrm{S}}/\sigma^2$ là SNR phát.

Dung lượng tổng có thể đạt được $R^{\mathrm{NOMA}}=R_1^{\mathrm{NOMA}}+R_2^{\mathrm{NOMA}}$. Trong công thức (1.8) có thể thấy rằng BS có thể điều khiển tốc độ dữ liệu cho mỗi người dùng bằng cách điều chỉnh các hệ số phân bổ công suất a_1 và a_2.

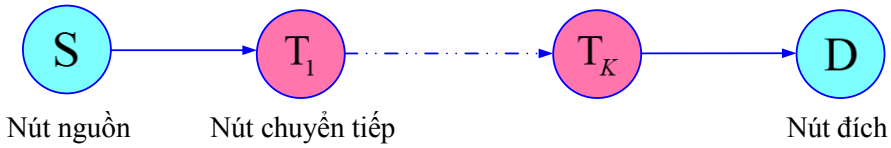
Mặc dù về mặt lý thuyết không có giới hạn về số lượng người dùng NOMA, nhưng thực tế, NOMA đường xuống được áp dụng cho số lượng nhỏ người dùng (thường là hai hoặc ba) trong một cụm (cluster), đối với số lượng lớn người dùng, có sự suy giảm về BER do lỗi truyền lan hoặc SIC không hoàn hảo. Ngoài ra, khi số lượng người dùng trong một cụm tăng, các thiết bị người dùng cuối yêu cầu công suất tính toán và năng lượng cao hơn, có thể không khả thi trong thực tế, đặc biệt đối với các thiết bị hạn chế tài nguyên. Lưu ý rằng NOMA miền công suất đường xuống đã được chuẩn hóa trong 3GPP (3rd Generation Partnership Project), gọi là truyền dẫn xếp chồng đa người dùng (Multiuser Superposition Transmission: MUST) [65]. So với OMA, một số ưu điểm chính của NOMA như hiệu suất phổ tần cao, hỗ trợ kết nối lớn, cải thiện tính công bằng của người dùng và độ trễ thấp. Tuy nhiên, nhược điểm của NOMA là: CSI hoàn hảo cần được biết tại BS để sắp xếp thứ tự SIC, làm tăng chi phí hồi tiếp; quá trình SIC đưa ra độ phức tạp tính toán và độ trễ lớn hơn tại phía thu; các người dùng mạnh hơn phải biết được phân bổ công suất của người dùng yếu để thực hiện SIC, sẽ làm tăng chi phí tín hiệu; phân bổ công suất lớn hơn đến các người dùng yếu (thường ở biên của tế bào), tạo ra sự can nhiễu giữa các tế bào trong hệ thống. Gần đây, cả NOMA và PLS được xem là công nghệ đầy hứa hẹn cho các hệ thống vô tuyến trong tương lai và sự tồn tại đồng thời hai kỹ thuật quan trọng này đã được nghiên cứu để đảm bảo truyền dẫn hiệu quả và an toàn [25, 26].

1.5. MẠNG ĐA CHẶNG THU THẬP NĂNG LƯỢNG VÔ TUYẾN

1.5.1. Hệ thống chuyển tiếp đa chặng và tác động của HWI

Các mạng chuyển tiếp được sử dụng rộng rãi trong thông tin vô tuyến hiện đại, do có thể mở rộng vùng phủ sóng, giảm giá thành triển khai, giảm can nhiễu, nâng cao độ tin cậy, cải thiện chất lượng dịch vụ cho các kênh vô tuyến bằng cách nhận các tín hiệu phát từ nguồn và sau đó chuyển tiếp đến đích mà có hoặc không có thêm quá trình xử lý, nên chịu ảnh hưởng suy hao

ít hơn [27]. Tuy nhiên, kỹ thuật này lại đối mặt với nhiều hạn chế, đặc biệt là khoảng cách truyền dẫn, nếu khoảng cách xa thì cần công suất phát cao, gặp khó khăn về nguồn cung cấp và dễ gây nhiễu cho các thiết bị khác. Hơn nữa, độ trễ xử lý tín hiệu giữa các nút chuyển tiếp cao, hiệu quả sử dụng phổ tần hạn chế so với truyền trực tiếp. Hệ thống truyền đa chặng thông thường, bao gồm một nút nguồn (Source: S), một nút đích (Destination: D) và số lượng giới hạn nút chuyển tiếp. Mô hình có thể được mô tả như Hình 1.6.



Hình 1.6: Mô hình hệ thống truyền thông đa chặng.

Trong hệ thống truyền đa chặng, để truyền một đơn vị dữ liệu từ nút nguồn đến nút đích qua T nút chuyển tiếp thì cần T+1 khung thời gian. Có hai kỹ thuật xử lý tín hiệu cơ bản tại nút chuyển tiếp, đó là khuếch đại và chuyển tiếp (Amplify-and-Forward: AF) và giải mã và chuyển tiếp (Decode-and-Forward: DF). Kỹ thuật AF là phương thức chuyển tiếp tín hiệu đơn giản, nút chuyển tiếp chỉ khuếch đại tín hiệu nhận được và sau đó chuyển tiếp từ nút nguồn đến nút đích. Đối với DF, nút chuyển tiếp giải điều chế, điều chế lại và chuyển tiếp tín hiệu từ nguồn đến đích. Về mặt kỹ thuật, kiểu AF đơn giản hơn nhưng nút chuyển tiếp phải có nhiều bộ nhớ để lưu trữ các mẫu tín hiệu thu, trước khi khuếch đại và chuyển tiếp. Trong khi đó, DF có ưu điểm thích hợp cho các hệ thống số sử dụng mã hóa. Tuy nhiên, tại mức công suất phát cao, chất lượng hệ thống của hai kiểu xử lý tín hiệu này là như nhau. Hiện nay, truyền đa chặng đã được xem xét để tích hợp trong các mạng vô tuyến thế hệ sau như WIMAX, 802.16e, …

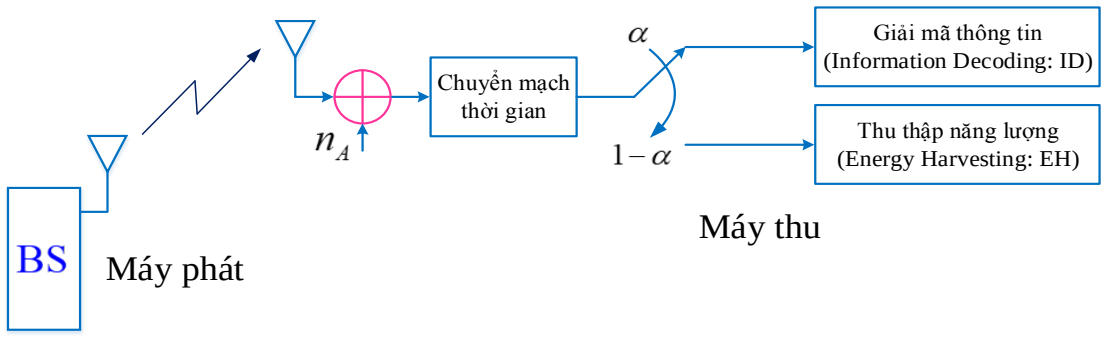
Hiện nay, hầu hết các đóng góp kỹ thuật trong lĩnh vực vô tuyến đều bỏ qua sự suy giảm phần cứng (Hardware Impairments: HWI) với giả sử phần cứng thiết bị thu/phát là lý tưởng (ideal hardware). Tuy nhiên, hiệu năng có

thể bị ảnh hưởng bởi HWI, nên việc xấp xỉ như vậy chỉ có ý nghĩa trong các hệ thống truyền tốc độ thấp và có thể dẫn đến kết quả sai lệch khi phân tích các hệ thống tốc độ cao trong tương lai [66-68]. HWI có thể làm biến dạng tín hiệu mong muốn, dẫn đến giới hạn hiệu suất tổng thể của hệ thống [66]. HWI tạo ra một giới hạn dung lượng không thể vượt qua bằng tăng công suất phát và có tác động đáng kể, đặc biệt các hệ thống tốc độ cao [67], gây méo tín hiệu ở cả máy thu/phát, giảm SINR và tăng sự phát xạ ngoài dải tần mong muốn. HWI phát sinh do sự phi tuyến trong bộ khuếch đại công suất cao (High Power Amplifier: HPA)/ khuếch đại tạp âm thấp (Low Noise Amplifier: LNA) hoặc không cân bằng I/Q (I/Q Imbalance) trước RF và nhiễu pha (Phase Noise: PN) [66]. HWI được giảm nhẹ bằng các thuật toán bù, nhưng luôn tồn tại nhiễu gây méo tín hiệu (distortion noises), làm ảnh hưởng nghiêm trọng đến hiệu năng hệ thống, đặc biệt những ứng dụng với phần cứng rẻ tiền [66]. Mặt khác, việc sử dụng các nút chuyển tiếp khác với trạm gốc có kích thước lớn, các nút chuyển tiếp thường có giá thành thấp, nên có thể chịu tác động rất lớn bởi HWI. Ngoài ra, mặc dù mạng chuyển tiếp có thể khắc phục pha đinh để tăng hiệu quả truyền dẫn, nhưng các nút mạng thường bị hạn chế về nguồn pin, nên nguồn cung cấp là một thách thức lớn và do đó mạng này rất phù hợp với thu thập năng lượng sóng vô tuyến (Radio Frequency Energy Harvesting: RF-EH), nhằm cải thiện hiệu năng hệ thống, nâng cao độ tin cậy truyền dẫn.

1.5.2. Kỹ thuật thu thập năng lượng sóng vô tuyến

Để giải quyết bài toán về nguồn năng lượng cho thiết bị di động, các nghiên cứu gần đây đã đề xuất kỹ thuật RF-EH, với ý tưởng sử dụng năng lượng tín hiệu vô tuyến ở máy thu, chuyển đổi thành nguồn điện một chiều để cung cấp cho các thiết bị [69]. RF-EH là phương thức truyền năng lượng vô tuyến trường vùng xa và là phương pháp duy nhất phù hợp truyền năng lượng khoảng cách xa của các thiết bị di động. Sử dụng RF-EH sẽ giúp hệ thống duy

trì hoạt động bình thường, mà không hoặc giảm sự phụ thuộc việc cấp nguồn dựa vào năng lượng lưu trữ (pin) hoặc nguồn điện mạng như hiện nay. Điều này giúp cải thiện hiệu suất hệ thống, tạo ra công suất ổn định và là giải pháp khả thi nhằm kéo dài thời gian sống cho các thiết bị có năng lượng hữu hạn, hoạt động trong những môi trường khắc nghiệt mà việc thay thế hoặc nạp lại pin là rất khó khăn. Trong kỹ thuật này, thông tin cũng được mang bởi tín hiệu tần số vô tuyến và năng lượng, nên có thể được lấy tại máy thu cùng thời điểm, phương pháp này được gọi là truyền năng lượng và thông tin vô tuyến đồng thời (Simultaneous Wireless Information and Power Transfer: SWIPT). Có hai cấu trúc đề xuất cho SWIPT là chuyển mạch theo thời gian (Time Switching: TS) và phân chia theo công suất (Power Splitting: PS) [69].



Hình 1.7: Cấu trúc máy thu cho SWIPT với một ăng-ten cho chế độ TS.

Cấu trúc của TS như trong Hình 1.7, tín hiệu thu được bởi ăng-ten chịu tác động của tạp âm tại máy thu n_A. Mỗi khung dữ liệu (frame) truyền τ được chia thành hai khe thời gian, một để truyền thông tin và khe thời gian còn lại để thu thập năng lượng. Do đó, tín hiệu nhận được đưa trở lại các thiết bị đầu cuối giải mã thông tin (Information Decoding: ID) và thu thập năng lượng (Energy Harvesting: EH) định kỳ thông qua bộ chuyển mạch thời gian tại máy thu, với $\alpha\tau$ là khoảng thời gian để thu thập năng lượng từ pha nguồn vô tuyến và thời gian còn lại $(1-\alpha)\tau$ được sử dụng cho truyền dữ liệu. Theo nguyên tắc TS, nút thu thập năng lượng chuyển đổi giữa năng lượng thu thập

và thông tin nhận được theo sự phân bổ thời gian khác nhau. Năng lượng thu thập tại máy thu được biểu diễn là

$$E_{\mathrm{EH}} = \eta\alpha\tau P_{\mathrm{S}}|h|^2, \tag{1.9}$$

với $\eta\left(0 \le \eta \le 1\right)$ là hiệu suất chuyển đổi năng lượng, phụ thuộc vào quá trình chỉnh lưu và mạch thu thập năng lượng [69], P_{S} là công suất tại máy phát, h là độ lợi kênh truyền giữa máy phát và máy thu. Phương thức TS yêu cầu lập lịch chính xác cho thông tin và năng lượng. Có hai loại nguồn được sử dụng trong RF-EH là nguồn chuyên dụng và nguồn xung quanh. Nguồn chuyên dụng sử dụng ăng-ten định hướng để đáp ứng yêu cầu về chất lượng dịch vụ (Quality of Sevice: QoS) trong mạng với công suất phát không đổi, ví dụ trạm phát sóng vô tuyến (Beacon). Nguồn xung quanh là tín hiệu RF được phát trên kênh vô tuyến. Để đáp ứng QoS của các ứng dụng di động, nguồn chuyên dụng là phương pháp phù hợp bởi vì nó có thể được cấu hình đầy đủ.

Nhìn chung, thường sử dụng tốc độ để đánh giá độ tin cậy truyền dẫn trong mạng RF-EH, nên năng lượng được thu thập và tốc độ thông tin trở thành một tham số hết sức quan trọng. Để đáp ứng các yêu cầu về QoS, nhiều sự đánh đổi khác nhau đã được phân tích tại lớp vật lý có liên quan đến RF-EH. PLS khai thác các đặc tính của kênh truyền vô tuyến để bảo đảm an toàn thông tin, là giải pháp đầy hứa hẹn để giải quyết vấn đề bảo mật hệ thống, sử dụng các giao thức chuyển tiếp đa chặng/cộng tác [28, 29], gây nhiễu cộng tác (Cooperative Jamming: CJ) [70], thu thập để gây nhiễu (Harvest-to-Jam).

1.6. MẠNG CẢM BIẾN KHÔNG DÂY VÀ GÂY NHIỄU CỘNG TÁC

1.6.1. Mạng cảm biến không dây

Các mạng cảm biến không dây (Wireless Sensor Network: WSN) bao gồm một số lượng lớn các nút cảm biến rẻ tiền, trong đó mỗi nút có các thành phần cảm biến, xử lý dữ liệu, giao tiếp với khả năng tính toán và năng lượng bị giới hạn [71]. Các nút cảm biến đa chức năng với ràng buộc mức năng

lượng, giá thành thấp đã được triển khai rộng rãi trong nhiều môi trường rộng lớn phục vụ cho các ứng dụng trong thương mại, dân sự và quân sự như giám sát, theo dõi xe cộ, khí hậu, … [72]. Khi các nút cảm biến được triển khai trên một khu vực địa lý xác định, chúng thực hiện thu thập dữ liệu từ môi trường và tự động thiết lập các mạng riêng để phát dữ liệu đến trạm gốc. Các nút cộng tác để thu thập dữ liệu và kéo dài thời gian hoạt động của hệ thống. Nhưng do bị hạn chế về công suất, bộ nhớ và khả năng tính toán, nên hiệu quả năng lượng được xem là mục tiêu chủ yếu, do mỗi nút cảm biến có thể chỉ được cung cấp nguồn năng lượng nhất định.

Là một trong những cơ chế điều khiển cấu trúc liên kết được nghiên cứu rộng rãi nhất cho WSN, thuật toán phân cụm (clustering algorithm) cung cấp khả năng mở rộng mạng và hiệu quả năng lượng bằng cách giảm chi phí truyền dẫn và nâng cao độ tin cậy [73]. Phân cụm là một trong những phương pháp thiết kế được sử dụng để quản lý hiệu quả tiêu thụ năng lượng, bằng cách tối thiểu số nút tham gia trao đổi ở khoảng cách xa so với trạm gốc và phân phối nguồn năng lượng tiêu thụ đồng đều giữa các nút trong mạng. Trong phương pháp này, mỗi nhóm cảm biến có một nút chủ cụm (Cluster Head: CH) để tập hợp dữ liệu tương ứng của cụm và gửi đến trạm gốc. Do đó, ứng dụng phương pháp phân cụm làm giảm lượng thông tin cần truyền, cũng như tăng cường việc phân bổ nguồn tài nguyên và tái sử dụng băng thông. Giao thức phân cụm LEACH [74, 75] là giao thức phân cấp theo cụm thích ứng năng lượng thấp, trong đó các nút tự tổ chức thành các cụm và một nút đóng vai trò là nút chủ cụm (CH) và các CH được chọn để quản lý các cụm riêng, tức là thu thập dữ liệu từ tất cả các nút cụm, thực hiện xử lý dữ liệu cục bộ rồi truyền đến các bộ thu phát (Sink) hoặc đến các CH lân cận. Hoạt động của LEACH được chia thành các vòng và mỗi vòng bắt đầu cùng với pha cài đặt khi các cụm được hình thành, sau đó đến pha ổn định khi các khung dữ liệu được gửi tới các CH và trạm gốc. LEACH là cấu trúc giao thức cho các

mạng cảm biến kết hợp định tuyến dựa vào cụm để đạt được hiệu năng tốt hơn về hiệu quả sử dụng năng lượng, độ trễ và chất lượng của hệ thống.

Bảo mật là vấn đề quan trọng trong WSN do khả năng tính toán, bộ nhớ và lưu trữ bị giới hạn, các nút cảm biến được phân bố mật độ ngẫu nhiên và dày đặc, dẫn đến khó khăn trong vấn đề bảo mật. Gần đây, PLS được đề xuất để cung cấp bảo mật cho WSN [76], do PSL không dựa vào các phương pháp mã hóa phức tạp, độ phức tạp thấp, triển khai đơn giản, nên phù hợp với các mạng bị hạn chế năng lượng so với các phương pháp thông thường.

1.6.2. Gây nhiễu cộng tác

CJ là kỹ thuật đặc biệt, với việc sử dụng nhiễu nhân tạo như một nguồn nhiễu hữu ích để làm mù mờ hoặc gây nhầm lẫn thông tin tại nút nghe lén và tín hiệu gây nhiễu có chủ ý này được tạo ra bởi các nút trợ giúp hợp pháp (legitimate helpers) trong mạng. Để cải thiện dung lượng bảo mật, cần tăng SNR tại máy thu hợp pháp hoặc giảm SNR của máy nghe lén. Phương pháp tự nhiên để đạt được trong cách thức thứ hai là giảm SNR tại nút nghe lén, thực hiện can nhiễu vào hệ thống và được đề xuất trong [70], nhằm cải thiện bảo mật của hệ thống, thông qua sử dụng gây nhiễu cộng tác.

Như miêu tả trong Hình 1.8, nút nguồn giao tiếp với nút đích trong sự xuất hiện của một nút nghe lén. Do đặc tính quảng bá của kênh truyền vô tuyến, nút nghe lén có thể thu chặn thông tin trên kênh chính, do đó tín hiệu nhận được tại nút bất hợp pháp (illegitimate node) được cho bởi

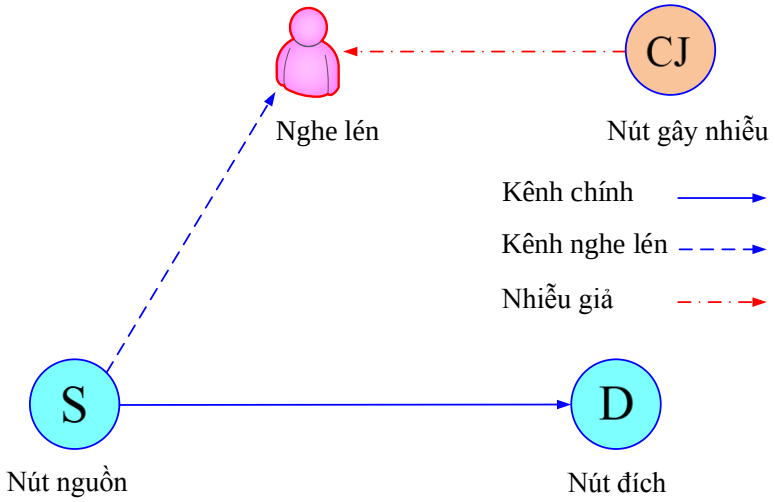
$$\gamma_{\mathrm{SE}} = P_{\mathrm{S}} \left| h_{\mathrm{SE}} \right|^2 \Big/ \sigma^2 , \tag{1.10}$$

trong đó, P_{S} là công suất phát của nút nguồn, h_{SE} là hệ số kênh truyền từ nút nguồn đến nút nghe lén và σ^2 là phương sai của nhiễu cộng tại máy nghe lén.

Tiếp theo, nhiễu được tạo ra bởi nút gây nhiễu (jammer) để gây nhầm lẫn nút nghe lén, trong khi máy thu mong muốn không bị ảnh hưởng do nhiễu được biết trước tại máy thu và SNR nhận được tại nút nghe lén bị suy giảm là

$$\gamma_{\mathrm{SE,CJ}} = \frac{P_{\mathrm{S}} \left| h_{\mathrm{SE}} \right|^2}{\sigma^2 + P_{\mathrm{J}} \left| h_{\mathrm{JE}} \right|^2}, \tag{1.11}$$

với P_{J} là công suất của nút gây nhiễu và h_{JE} là hệ số kênh truyền giữa nút gây nhiễu đến nút nghe lén.



Hình 1.8: Minh họa mô hình gây nhiễu cộng tác thông thường.

So sánh các biểu thức (1.10) và (1.11) thể hiện rằng SNR nhận được tại nút nghe lén bị suy giảm, do đó dung lượng bảo mật hệ thống cải thiện rõ rệt.

1.7. KHÁI NIỆM CƠ BẢN VỀ MÃ FOUNTAIN

1.7.1. Mã hóa tốc độ cố định

Trong các hệ thống thông tin, lỗi hay hiện tượng mất gói tin có thể xảy ra tại bất kỳ lớp nào trong hệ thống như lớp vật lý, liên kết, mạng, vận chuyển hoặc lớp ứng dụng. Việc phân bổ tài nguyên sẵn có cho việc sửa lỗi giữa các lớp khác nhau là vấn đề quan trọng cho quá trình hoạt động tối ưu của hệ thống. Lỗi có thể được phát hiện và sửa bởi các kỹ thuật khác nhau, ví dụ sửa lỗi hướng đi (Forward Error Correction: FEC) tại lớp ứng dụng/vận chuyển để sửa lỗi gói tin. FEC là kỹ thuật mã hóa kênh (channel coding), với nguyên tắc là thêm vào gói tin được phát những phần dư (redundancy), phần dư này được tính toán dựa trên thông tin được gửi và kiểu của FEC. Trong đó, tổng số luồng dữ liệu phát lớn hơn luồng dữ liệu gốc và dữ liệu gốc có thể được khôi

phục từ tập con đủ lớn bất kỳ của dữ liệu phát. Ví dụ, cho bản tin gốc k symbol (symbol là một chuỗi bít), mã tốc độ cố định tạo ra n symbol mã hóa, với $n > k$. Sau đó, bản tin gốc có thể được khôi phục lại từ tập k bất kỳ ra khỏi n symbol mã hóa và $n-k$ gọi là các symbol được bổ sung (overhead). Khi số symbol mã hóa được tạo ra, n phải được xác định trước (mã hóa tốc độ cố định). Nhìn chung, hệ thống mã hóa sử dụng các symbol bản tin gốc như một phần symbol mã hóa, trong đó tỉ số $r = k/n$ gọi là tốc độ mã và để đo lượng thông tin trên mỗi bít đầu ra. Mã sửa lỗi sao cho $r < 1$ và nếu $r \to 1$ thì mã đạt hiệu quả về tốc độ, nhưng nếu r thấp hơn thì mã có khả năng sửa nhiều lỗi hơn. Đối với mã hóa tốc độ cố định, tốc độ phải được chọn theo các điều kiện kênh xấu nhất, các máy thu có điều kiện kênh tốt phải chịu trễ thông tin và giảm tốc độ. Do vậy, tồn tại sự đánh đổi không thể tránh khỏi giữa độ tin cậy (tốc độ mã hóa thấp) và hiệu quả truyền dẫn (tốc độ mã hóa cao).

1.7.2. Mã hóa Fountain

Để giải quyết sự không linh hoạt của mã tốc độ cố định, yêu cầu phải biết trước điều kiện kênh sao cho máy phát tạo ra đủ số symbol mã hóa tới máy thu. Byers và cộng sự [30] đề xuất ý tưởng mã Fountain hay mã Rateless, với khả năng số lượng không giới hạn các symbol mã hóa được tạo ra từ một bản tin gốc k symbol. Sau đó, máy thu có thể khôi phục bản tin gốc từ tập bất kỳ n symbol mã hóa có xác suất thành công cao, với:

$$n = k(1+\varepsilon), \tag{1.12}$$

trong đó, ε $(\varepsilon \geq 0)$ là phần thông tin được bổ sung.

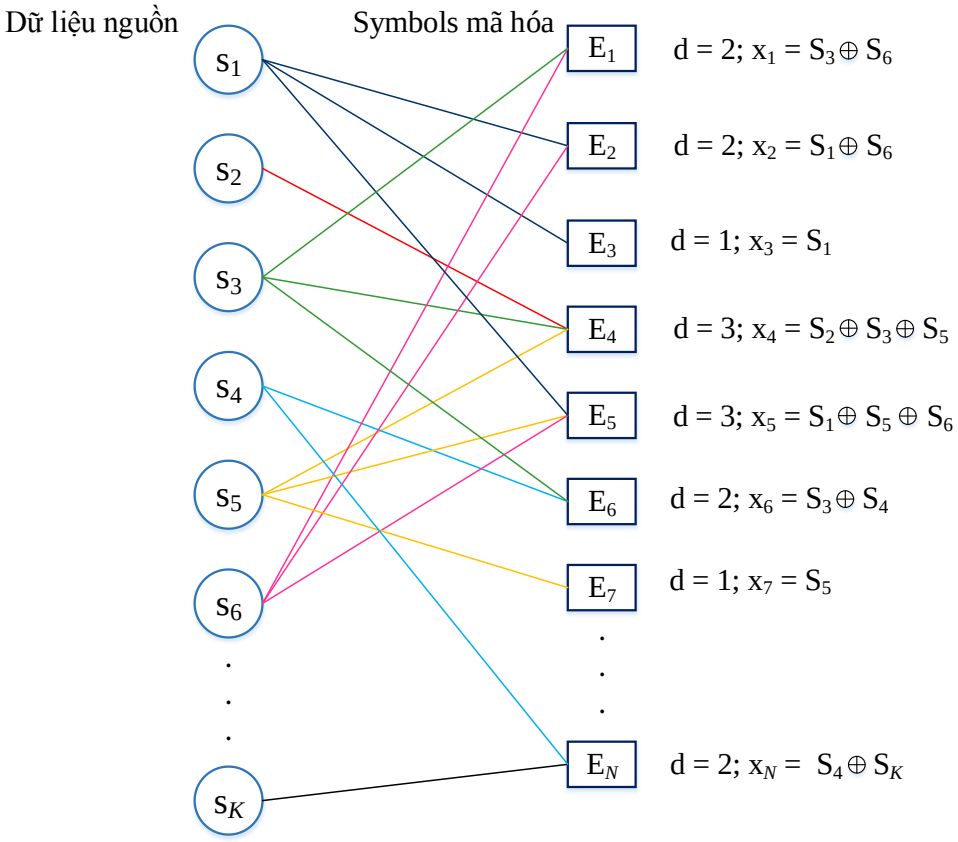
Hệ thống sử dụng FC, máy phát có thể tạo ra số lượng không giới hạn các gói mã hóa độc lập, máy thu cố gắng nhận các gói mã hóa này và khi nhận đủ số gói mã hóa cần thiết để khôi phục bản tin gốc, thì máy thu có thể ngắt kết nối, do đó tiết kiệm thời gian và năng lượng truyền dẫn. Số gói mã hóa thường lớn hơn một ít so với thông tin gốc ban đầu do bổ sung phần dư.

Hơn nữa, FC có thể thích ứng với chất lượng các điều kiện kênh cụ thể, mà không cần ước lượng kênh tại máy phát. Nếu kênh truyền có chất lượng tốt, bộ giải mã có thể giải mã với phần thông tin bổ sung nhỏ, nếu kênh truyền chất lượng xấu thì bộ giải mã sẽ cần một số lượng lớn các symbol đầu ra. Máy phát thực hiện cho đến khi nhận được thông báo xác nhận (acknowledgement) từ bộ giải mã, thông qua kênh hồi tiếp. Vậy nên, mã Fountain có ưu điểm là không yêu cầu biết trước các điều kiện kênh truyền cụ thể, nên được áp dụng trong các hệ thống có bộ mã hóa không yêu cầu tốc độ xác định. Thuật toán giải mã có thể thực hiện trên bất kỳ tập con của các symbol đầu ra và xác suất giải mã thông tin thành công sẽ tăng tuyến tính với số symbol đầu ra. Các thuật toán giải mã điển hình đối với FC gồm thuật toán lan truyền niềm tin (Belief Propagation: BP) và phép loại trừ Gauss (Gaussian Elimination: GE) và tương tự như LDPC, FC được minh họa dạng biểu đồ. Có nhiều phương pháp mã hóa Fountain số đã được đề xuất như mã chuyển đổi Luby (Luby Transform: LT) [31] và mã Raptor (Raptor code) [33]. Trong đó, LT là mã Fountain sửa lỗi tuyến tính hiệu quả đầu tiên, được công bố bởi Michael Luby năm 2002 [31], thiết kế phân bố bậc để tối ưu sự phức tạp của mã hóa và giải mã, nhưng bảo đảm phần thông tin bổ sung nhỏ, quá trình mã hóa và giải mã được thực hiện:

• Phương pháp mã hóa (Encoding)

Khi thông tin được gửi từ máy phát đến máy thu, trước tiên dữ liệu gốc chia thành K phần bằng nhau và được mã hóa với nhau một cách thích hợp với phép XOR, để tạo ra chuỗi các gói mã hóa. Số lượng các phần chứa trong mỗi gói được mã hóa được gọi là bậc (degree) của gói. Luby miêu tả bậc là một tham số quan trọng để xác định hiệu suất mã hóa. Phân bố bậc tốt không chỉ đưa vào phần dư phù hợp trong luồng thông tin, mà còn làm đơn giản thủ tục giải mã. Do đó, Luby đã đề xuất phân bố Robust Soliton (Robust Soliton Distribution: RSD) như là phân bố bậc tối ưu [8]. Phân bố bậc này được thiết

kế sao cho thuật toán giải mã có thể thực hiện hiệu quả và được gọi là thuật toán lan truyền niềm tin.



Hình 1.9: Minh họa đồ thị phân tán dạng thưa của mã Fountain.

Hình 1.9 minh họa mã Fountain giữa k nút đầu vào bên trái và n nút mã hóa bên phải, các nút mã hóa gọi là các nút đầu ra. Mặc dù chiều dài khối của FC có khả năng vô hạn, nhưng thực tế chỉ một phần được bổ sung vào đầu từ mã. Độ dài của phần bổ sung thêm dựa vào tốc độ xóa trung bình của kênh và thuật toán sử dụng trong bộ giải mã. Các thuật toán giải mã có vai trò rất quan trọng trong hiệu suất mã hóa tổng thể, với mong muốn phần bổ sung nhỏ.

Số lượng bất kỳ các symbol mã hóa có thể được tạo ra độc lập từ k symbol nguồn bởi quá trình mã hóa sau đây:

Bước 1: Mã LT tạo ra các symbol mã hóa bằng cách chọn ngẫu nhiên bậc d từ phân bố bậc (degree distribution) cho trước.

Bước 2: Lựa chọn ngẫu nhiên đồng nhất các symbol bản tin bậc d khác nhau và những symbol mã hóa này sẽ là các lân cận (neighbour) của nhau.

Bước 3: Các symbol mã hóa bậc d được tạo ra bằng cách gán phép XOR (Exclusive-OR) của các symbol thông tin.

Ví dụ, cho bản tin gốc gồm có $k = 10$ symbol, cụ thể $\mathrm{s} = (\mathrm{s}_1, \mathrm{s}_2, ..., \mathrm{s}_{10})$ và bậc $d = 3$ được lựa chọn từ phân bố bậc cho trước. Tiếp theo, 3 symbol bản tin duy nhất được chọn ngẫu nhiên từ tập s để tạo ra một symbol mã hóa x_1, với $x_1 = \mathrm{s}_i \oplus \mathrm{s}_j \oplus \mathrm{s}_k$ và $i \neq j \neq k$.

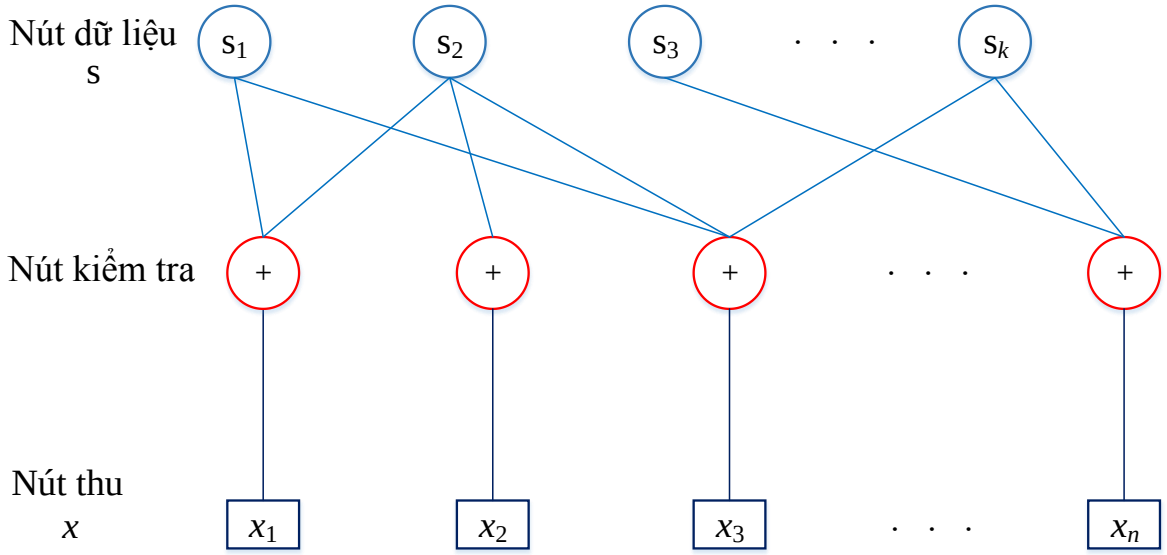
Phân bố bậc xác định hiệu suất của mã LT trong [31], bao gồm phân bố Ideal Soliton và Robust Soliton, để thỏa mãn các yêu cầu như số symbol mã hóa và xác suất giải mã thành công bản tin.

• Phương pháp giải mã (Decoding)

Quá trình giải mã được kích hoạt ngay khi nút đích nhận đủ gói mã hóa để giải mã dữ liệu gốc. Thuật toán giải mã hiệu quả nhất cho bất kỳ mã ngẫu nhiên nào trên kênh xóa là giải mã hợp lẽ cực đại (Maximum Likelihood: ML). Giải mã ML tương đương với việc giải hệ phương trình tuyến tính và có thể được thực hiện bằng cách sử dụng phép loại trừ Gauss. Mặc dù giải mã ML có xác suất lỗi thấp, nhưng độ phức tạp có thể tăng nhanh với cả hai N (số lượng gói tin nhận được) và K (độ dài từ mã), theo bậc $\mathcal{O}(NK)$.

Một phương pháp giải mã thay thế đòi hỏi ít phức tạp hơn về tính toán là sử dụng kỹ thuật giải mã dựa trên đồ thị, gọi là thuật toán lan truyền niềm tin [31]. Giải mã BP giải các phương trình tuyến tính dựa trên đồ thị hai phía. Tại mỗi bước, bộ giải mã xác định một gói mã hóa có bậc bằng 1 và nếu không tồn tại symbol mã hóa bậc 1 thì giải mã không thành công. Ngược lại, giá trị của phân đoạn gốc chứa trong gói mã hóa xác định được khôi phục và sự kết hợp của phân đoạn này sẽ bị loại bỏ khỏi phần còn lại của các gói mã hóa đang chờ giải mã. Các bước này được lặp lại cho đến khi phân đoạn cuối cùng

được khôi phục thành công và thuật toán BP có độ phức tạp $\mathcal{O}(Kln(K))$. Vậy nên, để giải mã LT, bộ giải mã cần biết các symbol lân cận của mỗi symbol mã hóa, ví dụ máy phát có thể chuyển một gói tin gồm một symbol mã hóa và danh sách các lân cận, hoặc bộ mã hóa và giải mã chia sẻ một bộ khởi tạo số ngẫu nhiên, bộ giải mã tìm ra các lân cận của mỗi symbol mã hóa bằng cách tạo ra các kết hợp tuyến tính ngẫu nhiên được đồng bộ với bộ mã hóa. Sử dụng thuật toán giải mã BP tiến hành lặp và khôi phục symbol nguồn tại mỗi bước. Khi nhận được n gói mã hóa, thực hiện giải mã bản tin nguồn có độ dài k. Thuật toán BP là phương pháp giải mã đơn giản, chi phí tính toán thấp hơn so với các thuật toán khác để khôi phục dữ liệu gốc.



Hình 1.10: Minh họa đồ thị giải mã LT.

Như được thể hiện trong Hình 1.10, giả sử mỗi nút dữ liệu thể hiện một bít trong bản tin gốc s và mỗi nút thu gồm một bít trong symbol thu x. Đối với mỗi nút thu $x_i (i = 1, 2, ..., n)$, tạo một nút kiểm tra tương ứng và kết nối các nút thu với nút kiểm tra. Nút kiểm tra này cũng kết nối với tất cả các nút dữ liệu mà xuất hiện trong phương trình x_i. Vì thế, mỗi nút kiểm tra thể hiện một phép tính XOR của tất cả các nút dữ liệu mà nút này kết nối đến, cụ thể đồ thị trên được thể hiện tập các phương trình tuyến tính

$$\begin{cases} x_1 = \mathrm{s}_1 \oplus \mathrm{s}_2 \\ x_2 = \mathrm{s}_2 \\ x_3 = \mathrm{s}_1 \oplus \mathrm{s}_2 \oplus \mathrm{s}_k . \\ ..... \\ x_n = \mathrm{s}_3 \oplus \mathrm{s}_k \end{cases} \quad (1.13)$$

Miêu tả các symbol mã hóa và symbol bản tin trong đồ thị hai phía, bản tin gốc có thể được khôi phục trong các bước sau:

Bước 1: Tất cả các symbol mã hóa bậc một (degree one) lan truyền các giá trị của chúng đến các symbol bản tin được kết nối tương ứng. Nếu không có symbol mã hóa bậc 1 thì việc giải mã sẽ sớm thất bại.

Bước 2: Sự kết nối giữa những symbol mã hóa bậc một này và những symbol bản tin tương ứng được loại bỏ.

Bước 3: Các symbol bản tin có liên quan trong cả Bước 1 và Bước 2 sẽ ghi lại các giá trị mới nhất và sau đó lan truyền những giá trị mới nhất này đến tất cả các symbol mã hóa được kết nối tương ứng.

Bước 4: Các symbol mã hóa có liên quan trong Bước 3 sẽ cập nhật các giá trị riêng của chúng với các giá trị nhận được (bằng phép XOR) tương ứng.

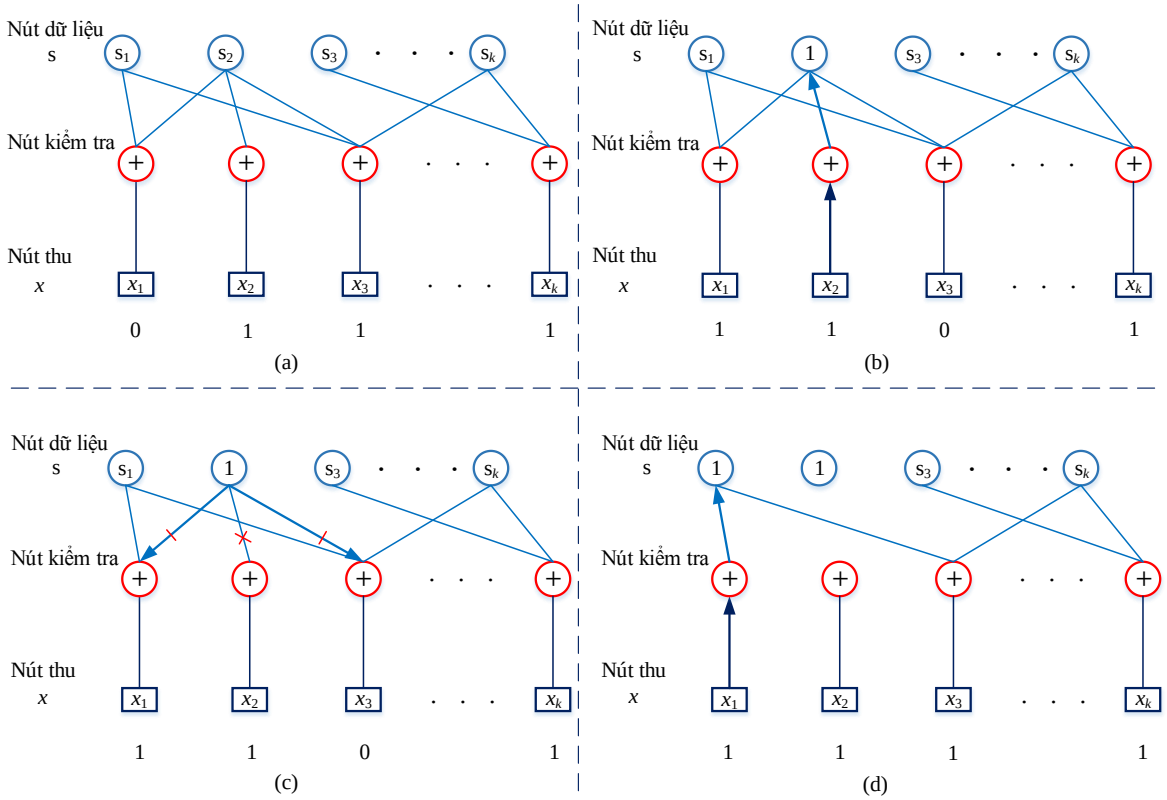
Bước 5: Các kết nối có liên quan trong Bước 3 và Bước 4 được loại bỏ.

Bước 6: Lặp lại từ Bước 1 cho đến khi tất cả các symbol bản tin được khôi phục.

Để thể hiện rõ hơn phương pháp giải mã, tác giả xem xét bản tin gồm có $\mathrm{s}_1, \mathrm{s}_2, \mathrm{s}_3, ..., \mathrm{s}_k$ symbol mã hóa, trên đồ thị hai phía như thể hiện trong Hình 1.11. Giả sử rằng, các vòng tròn phía trên đồ thị là các giá trị chưa biết và các hình vuông $(x_1, x_2, x_3, ..., x_k)$ ở phía dưới là các symbol mã hóa nhận được với các giá trị 0, 1, 1…1, tương ứng. Cụ thể, x_1 là symbol mã hóa bậc 2 liên kết với s_1 và s_2, x_2 là symbol mã hóa bậc 1 liên kết với s_2, x_3 là symbol mã

hóa bậc 3 liên kết với s_1, s_2, s_k và x_k là symbol mã hóa bậc 2 liên kết với s_3 và s_k của đồ thị hai phía.

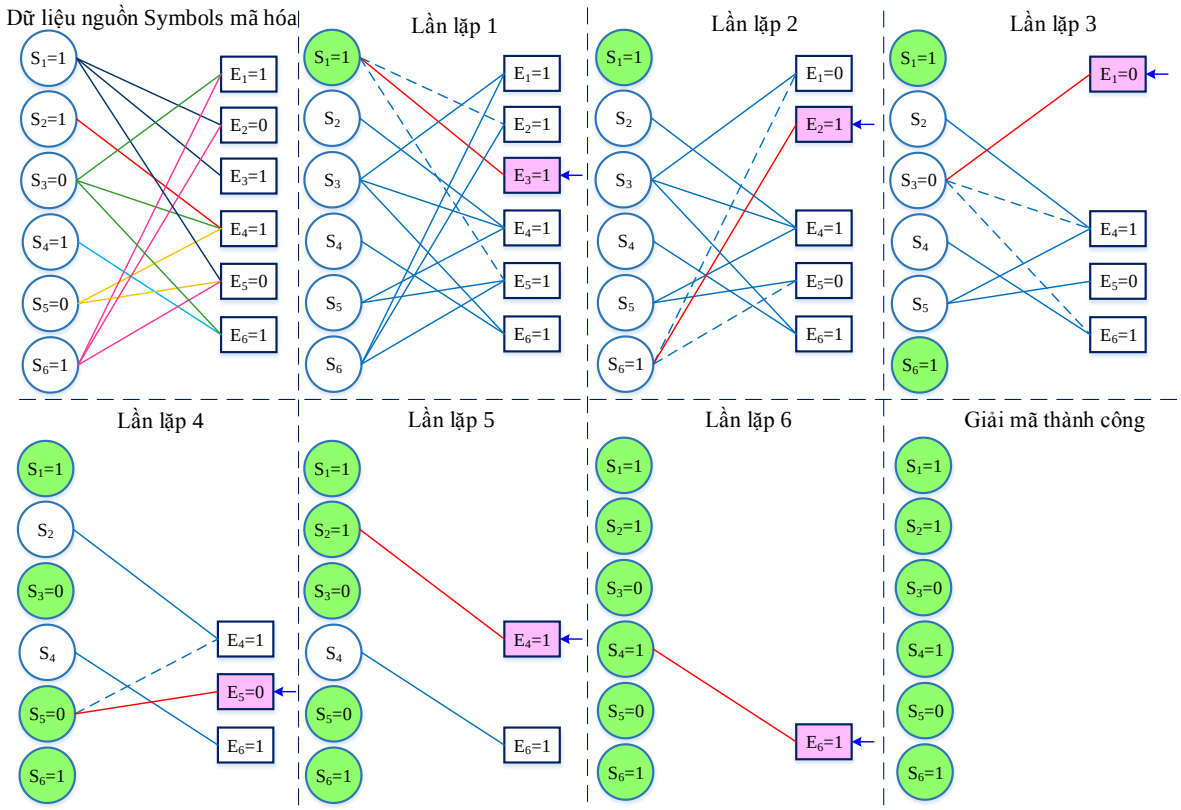
Ta có symbol mã hóa bậc 1 (x_2) liên kết với s_2 (Bước 1, Hình 1.11 a). Sau đó, x_2 lan truyền trực tiếp giá trị đến lân cận của symbol này và kết nối tương ứng được loại bỏ (Bước 2). Tiếp theo, s_2 lan truyền giá trị mới đến x_1 và x_3 (Bước 3), với $x_1 \leftarrow x_1 \oplus s_2$ và $x_3 \leftarrow x_3 \oplus s_2$ (Bước 4, Hình 1.11 b).



Hình 1.11: Minh họa quá trình giải mã LT.

Kế tiếp, các kết nối tương ứng trong Bước 3 và Bước 4 được loại bỏ (Bước 5, Hình 1.11 c). Kết quả, symbol mới bậc 1 (cụ thể x_1) liên kết với s_1. Lặp lại từ Bước 1, x_1 lan truyền giá trị tới lân cận của symbol này, cập nhật giá trị mới và loại bỏ kết nối tương ứng (Bước 6, Hình 1.11 d). Quá trình xử lý này tiếp tục đến khi tất cả các giá trị của symbol bản tin được khôi phục.

Minh họa các bước giải mã BP cho một đầu vào nhị phân $s = [1\ 1\ 0\ 1\ 0\ 1]$, được thể hiện trong Hình 1.12. Trong ví dụ này, trình bày bởi đồ thị hai phía giữa $k = 6$ các symbol nguồn ở bên trái và $n = 6$ các symbol mã hóa thu được ở bên phải. Symbol mã hóa E_i được kết nối đến symbol nguồn S_j. Bộ giải mã BP lặp lại các bước cho đến khi lỗi xảy ra trong Bước 1, hoặc bộ giải mã dừng lại sau khi giải mã thành công trong Bước 6.



Hình 1.12: Minh họa bộ giải mã BP cho LT với $k = 6$ và $n = 6$.

Nếu quá trình xử lý này được lặp lại đến k lần mà không thất bại thì giải mã hoàn thành với tất cả k symbol nguồn được khôi phục và độ phức tạp của thuật toán mã hóa và giải mã BP là giống nhau.

1.7.3. Một số ứng dụng của mã Fountain

FC có thể được sử dụng trong các hệ thống vô tuyến gói để cung cấp việc sửa lỗi hiệu quả bằng cách tạo ra số lượng các gói dư (redundant packets) không giới hạn. Mã kênh được sử dụng để bảo vệ các gói Fountain là yếu tố

then chốt để nâng cao hiệu năng thông lượng của hệ thống. FC có thể được ứng dụng trong các mạng đơn hướng (unicast) và đa hướng (multicast) cho các giao thức truyền tin cậy trong thông tin vô tuyến với đặc tính kênh truyền thay đổi theo thời gian. Ứng dụng khác của FC là lưu trữ dữ liệu, xóa gói, ví dụ các bộ định tuyến có thể mất gói do tắc nghẽn, một tập tin trong hệ thống lưu trữ dữ liệu có thể bị xóa do xảy ra lỗi. Ngoài ra, trong các mạng vô tuyến, truyền khung ACK chiếm khoảng dung lượng trung bình kênh và do đó ảnh hưởng xấu đến băng thông kênh truyền. Theo phương pháp truyền thống, sử dụng các kỹ thuật truyền và tái tạo lại, do đó bị giới hạn về độ tin cậy và ảnh hưởng xấu đến hiệu suất thông lượng của hệ thống. Vậy nên, các mã của FC như LT và Raptor được đề xuất đã giải quyết độ phức tạp của quá trình giải mã. Hơn nữa, FC là một lớp mã mới được thiết kế hiệu quả, đồng bộ và truyền thông tin từ máy phát đến máy thu một cách tin cậy trên kênh vô tuyến. Vì vậy, bảo mật trong các hệ thống sử dụng FC là một trong những vấn đề rất quan trọng và PLS trong thiết kế các giao thức truyền bảo mật sử dụng FC là một khái niệm mới cần được khảo sát [40-46] và cũng chính là nội dung nghiên cứu xuyên suốt của Luận án.

1.8. CÁC CÔNG TRÌNH NGHIÊN CỨU LIÊN QUAN

1.8.1. Bảo mật với kênh nghe lén MIMO

Bảo mật là một trong những vấn đề quan trọng trong thông tin vô tuyến do đặc tính quảng bá tự nhiên của kênh truyền vô tuyến. Thông thường, các phương pháp mã hóa tại các lớp trên được sử dụng để đạt được bảo mật dựa vào các khóa mật được tạo ra. Tuy nhiên, các nút nghe lén có thể giải mã được tín hiệu mã hóa nếu chúng được trang bị ăng-ten thông minh và có đủ thời gian cho hoạt động giải mã. Trong [4-14], các tác giả đã giới thiệu phương pháp PLS, với các đặc tính của kênh truyền vô tuyến như khoảng cách và CSI, có thể khai thác để bảo đảm bí mật truyền dữ liệu. Để đạt được bảo mật trong PLS, dung lượng bảo mật phải dương hoặc dung lượng kênh

của kênh dữ liệu lớn hơn kênh nghe lén. Ví dụ, các phương pháp phân tập cho cả thu và phát [20], [77, 78] được đề xuất để nâng cao hiệu năng bảo mật cho các giao thức MIMO với SOP và xác suất bảo mật khác không (Probability of Non-zero Secrecy Capacity: PNSC). Trong các nghiên cứu này, máy phát lựa chọn ăng-ten phát tốt nhất để tối đa SNR đạt được tại máy thu định trước sử dụng MRC hoặc SC và do các nút nghe lén chỉ đạt được phân tập thu với các bộ kết hợp MRC hoặc SC, cho nên bậc phân tập của các kênh dữ liệu có thể lớn hơn các kênh nghe lén. Mặt khác, để nâng cao hiệu năng bảo mật, gây nhiễu cộng tác có thể được sử dụng, trong đó nút gây nhiễu được dùng để tạo nhiễu nhân tạo (artificial noises) lên nút nghe lén nhằm làm giảm chất lượng các kênh nghe lén [70]. Tuy nhiên, việc triển khai các phương pháp gây nhiễu cộng tác yêu cầu tính đồng bộ cao giữa các nút, có thể là vấn đề khó khăn.

Hơn nữa, gần đây các giao thức PLS trong CRN đã thu hút nhiều sự quan tâm nghiên cứu [55-64], [79]. Trong [55], Duy và cộng sự đã đánh giá hiệu năng bảo mật của phương pháp lựa chọn nút chuyển tiếp đơn phần (Partial Relay Selection: PRS) dựa vào các biểu thức dung lượng bảo mật trung bình (Average Secrecy Capacity: ASC), SOP và PNSC. Ngoài ra, cả phương pháp DF truyền thống và phương pháp ngẫu nhiên và chuyển tiếp (Randomize-and-Forward: RF) tạo bảng mã ngẫu nhiên, để nút nghe lén không thể kết hợp dữ liệu phát khi sử dụng kỹ thuật MRC, cũng đã được xem xét [56]. Trong [57] đã đề xuất khung truyền bảo mật trong CRN ngẫu nhiên dạng nền để tối đa hiệu quả phổ tần và hiệu suất năng lượng. Trong [58], các phương pháp lập lịch SU đường xuống và đường lên đã được nghiên cứu để tối đa tốc độ bảo mật. Các tác giả trong [59] đề xuất giao thức cộng tác mạng thứ cấp để tối đa tốc độ bảo mật của mạng sơ cấp trong khi vẫn thỏa mãn yêu cầu của mạng thứ cấp. Trong [60], hiệu năng bảo mật của mạng hai chặng CRN cộng tác dạng nền đã được khảo sát, trong đó cả nút đích và nút nghe lén có thể kết hợp dữ liệu nhận được từ các liên kết trực tiếp và chuyển tiếp.

Trong [61], đề xuất phương pháp lựa chọn nút chuyển tiếp cơ hội để cải thiện sự đánh đổi giữa bảo mật và tin cậy cho CRN hai chặng ngẫu nhiên. Trong [62], khảo sát sự đánh đổi giữa bảo mật và độ tin cậy cho CRN dạng nền, trong đó các trạm gốc vô tuyến nhận thức có thể thu thập năng lượng sóng vô tuyến từ môi trường xung quanh để truyền dữ liệu. Nghiên cứu [63] đã đề xuất giao thức PRS tổng quát để nâng cao hiệu năng bảo mật cho CRN cộng tác dựa vào các biểu thức chính xác của SOP và PNSC được đưa ra. Trong [64] đề xuất giao thức truyền bảo mật trong CRN dạng nền với thu thập năng lượng từ PU, hiệu năng bảo mật được đánh giá dựa vào xác suất dừng tại nút đích thứ cấp dưới điều kiện ràng buộc mức can nhiễu từ PU, công suất phát tối đa của máy phát thứ cấp. Trong [79], hiệu năng dừng bảo mật của phương pháp TAS/MRC trong các CRN đã được phân tích. Trái ngược với [79], trong [80] đề xuất giao thức truyền bảo mật trong CRN dạng chồng, máy phát thứ cấp song công (full-duplex) sử dụng TAS/MRC để phát dữ liệu thứ cấp và thu dữ liệu sơ cấp tại cùng thời điểm. Ngoài ra, có thể sử dụng phương pháp tạo búp sóng tương tác cưỡng bức về không (interactive zero forcing beam-forming) để phát quảng bá đồng thời cả dữ liệu sơ cấp và thứ cấp. Giao thức đề xuất trong [80] không chỉ nâng cao hiệu năng SOP cho mạng sơ cấp mà còn cải thiện thông lượng truyền mạng thứ cấp. Các nghiên cứu [81, 82] giới thiệu các phương pháp PLS trong môi trường RF-EH. Cụ thể, trong [81], một trạm gốc đa ăng-ten sử dụng TAS để gửi thông tin và năng lượng đến một máy thu mong muốn và các máy thu EH, tương ứng. Vì các máy thu EH có thể giải mã thông tin của máy thu dự định một cách bất hợp pháp, nên tồn tại sự đánh đổi giữa năng lượng thu thập và bảo mật truyền dữ liệu. Trong [82], một nguồn năng lượng bị giới hạn thu thập năng lượng RF từ trạm phát sóng vô tuyến chuyên dụng để phát dữ liệu trong sự xuất hiện của nhiều máy nghe lén. Thêm vào đó, nút nguồn có thể sử dụng TAS hoặc truyền tỉ số tối đa (Maximal Ratio Transmission: MRT) để nâng cao bậc phân tập bảo mật.

Trong [83], giao thức truyền bảo mật trong hệ thống chuyển tiếp MIMO hai chặng sử dụng TAS/MRC trên kênh pha đinh Nakagami-*m* đã được phân tích. Các tác giả trong [84] đã xem xét hệ thống cộng tác MIMO được hỗ trợ bộ đệm trong sự xuất hiện của một nút nghe lén thụ động (passive eavesdropper). Đặc biệt, do thiếu CSI của kênh nghe lén, cả phương pháp lựa chọn ăng-ten phát và nút chuyển tiếp được đề xuất để nâng cao chất lượng của kênh chính.

Gần đây, các phương pháp truyền bảo mật cho hệ thống NOMA cũng đã nhận được nhiều sự quan tâm. Trái ngược với các kỹ thuật truyền dẫn phụ thuộc vào điều kiện, nút nguồn sử dụng NOMA có thể gửi nhiều tín hiệu đến nút đích tại cùng thời gian, tần số và mã. Thật vậy, các tín hiệu được kết hợp tuyến tính với các mức công suất phát khác nhau, sau đó truyền đến nút đích sử dụng kỹ thuật SIC để trích xuất các tín hiệu mong muốn. Tài liệu [85] đã khảo sát hiệu năng SOP của hệ thống bảo mật NOMA sử dụng phương pháp TAS max-min, với sự kết hợp và không kết hợp các nút nghe lén. Trong [86] đã khảo sát hiệu năng bảo mật của hệ thống NOMA cộng tác với các phương pháp lựa chọn nút chuyển tiếp khác nhau. Trong [87], nút nguồn thực hiện hoạt động gây nhiễu để nâng cao bảo mật cho các mạng chuyển tiếp hai chặng sử dụng NOMA. Trong [88], các phương thức truyền NOMA bảo mật trong CRN đã được đề xuất và phân tích. Trong [89], sự đánh đổi giữa bảo mật và độ tin cậy của CRN cộng tác NOMA đã được khảo sát dựa vào SOP và xác suất dừng kết nối (Connection Outage Probability: COP).

1.8.2. Bảo mật trong mạng chuyển tiếp đa chặng dựa vào trạm Beacon

Gần đây, thu thập năng lượng dựa vào trạm phát sóng vô tuyến (Power Beacon) [90-94] đã thu hút nhiều sự quan tâm như là phương pháp hiệu quả để giải quyết vấn đề ràng buộc mức năng lượng trong các mạng vô tuyến như WSN, mạng ad-hoc,… trong đó, các trạm phát sóng vô tuyến được triển khai trong mạng để hỗ trợ nguồn cho các thiết bị vô tuyến. Các phương pháp EH-Beacon trong CRN đa chặng dạng nền đã được đề xuất [90]. Để cải thiện OP

từ đầu cuối đến đầu cuối cho các giao thức chuyển tiếp đa chặng EH-Beacon trong mạng cluster, trong [91] đưa ra nhiều phương pháp chọn lựa nút chuyển tiếp khác nhau. Trong [92] xem xét EH-Beacon của các giao thức chuyển tiếp hai chiều, trong đó hai nút nguồn bị ràng buộc mức năng lượng thực hiện thu thập năng lượng RF từ một trạm Beacon đa ăng-ten để liên lạc với nhau với sự hỗ trợ của một nút chuyển tiếp. Trong [93], xác suất dừng và thông lượng hệ thống của các phương thức lựa chọn nút chuyển tiếp từng phần và cơ hội trong EH-Beacon với hỗ trợ mạng hai chặng CRN WSN dưới tác động của phần cứng không hoàn hảo đã được khảo sát. Trong [94], xem xét giao thức truyền bảo mật EH-Beacon đa chặng đa đường, các máy phát tự điều chỉnh công suất, do đó các nút nghe lén không thể giải mã dữ liệu nhận được.

1.8.3. Bảo mật trong giao thức chuyển tiếp đa chặng LEACH

Do năng lượng pin thấp, hạn chế bộ nhớ, khả năng xử lý thông tin của WSN bị giới hạn, nên giao thức LEACH [74, 75] được sử dụng để kéo dài thời gian sống của mạng. Trong WSN dữ liệu được cảm biến thường rất nhạy cảm, do đó truyền bảo mật là vấn đề quan trọng và PLS gần đây được giới thiệu trong WSN nhằm chống lại việc nghe lén [76]. Để nâng cao hiệu năng bảo mật, trong [95] đề xuất giao thức chuyển tiếp phân tập để nâng cao dung lượng bảo mật thông qua tăng chất lượng kênh dữ liệu. Trong [96], cả phương pháp chuyển tiếp và gây nhiễu cộng tác được đề xuất để giảm dung lượng của kênh nghe lén và cải thiện hơn nữa hiệu năng bảo mật, nhưng việc triển khai kỹ thuật CJ là rất phức tạp và có thể gây nhiễu đồng kênh đến các thiết bị khác trong mạng. Khác với các nghiên cứu trong [95, 96], công trình [97] đã khảo sát sự đánh đổi giữa bảo mật và độ tin cậy bằng việc tính toán xác suất thu chặn và xác suất dừng của kênh nghe lén và dữ liệu, tương ứng.

1.8.4. Bảo mật trong các hệ thống sử dụng mã Fountain

Mã Fountain hay mã Rateless thu hút nhiều sự quan tâm do độ phức tạp giải mã thấp. Trái ngược với các loại mã tốc độ cố định điển hình, máy phát

FC có thể tạo ra một chuỗi không giới hạn các gói mã hóa từ số lượng hữu hạn các gói tin nguồn. Các gói mã hóa sau đó được phát liên tục đến các máy thu mong muốn cho đến khi mỗi máy thu có thể nhận số lượng hiệu quả các gói mã hóa để khôi phục dữ liệu gốc (bất kể các gói mã hóa nhận được). Do đó, FC không yêu cầu biết CSI, tự động thích ứng các điều kiện kênh truyền và tránh kênh hồi tiếp. Trong [36], các tác giả đã đề xuất mạng chuyển tiếp cộng tác dựa vào FC, với tiêu thụ năng lượng và thời gian truyền giảm đáng kể do sự tích lũy thông tin lẫn nhau. Nghiên cứu trong [37] đã trình bày ưu điểm của việc ứng dụng FC vào các hệ thống thông tin quảng bá với hiệu quả truyền dẫn. Trong [38], mô hình truy cập phổ tần dựa vào mã Rateless trong CRN dạng chồng đã được đề xuất. Phương pháp đề xuất trong [38], các máy phát thứ cấp trợ giúp một máy phát sơ cấp chuyển tiếp các gói Fountain đến một máy thu sơ cấp và sau đó tìm kiếm cơ hội để truy nhập các băng tần được cấp phép. Trong [39], đã xem xét mạng chuyển tiếp cộng tác sử dụng FC và RF-EH, trong đó nút nguồn và nút chuyển tiếp sử dụng FC, do đó nút đích có thể tích lũy năng lượng và thông tin lẫn nhau. Tuy nhiên, các nút nghe lén cũng có thể nhận đủ số gói mã hóa cho việc thu chặn dữ liệu gốc. Vì vậy, bảo mật trong các hệ thống PLS dựa vào FC trở thành vấn đề quan trọng. Ý tưởng cơ bản của các giao thức PLS dựa vào FC là khi nút đích dự định có thể nhận đủ số gói mã hóa trước nút nghe lén, truyền dữ liệu là thành công và bảo mật [40]. Trong [41], đã đánh giá xác suất thu chặn, định nghĩa là xác suất mà nút nghe lén có thể nhận đủ các gói mã hóa để khôi phục dữ liệu gốc. Nghiên cứu trong [42], đã đề xuất mô hình đa hướng để đạt được bảo mật cho mạng Internet vạn vật (Internet of Things: IoT) sử dụng FC nhằm làm giảm xác suất thu chặn tại máy nghe lén. Tài liệu [43] đã xem xét kịch bản cộng tác bảo mật sử dụng FC tại lớp ứng dụng và gây nhiễu cộng tác tại lớp vật lý để nâng cao bảo mật và độ tin cậy của truyền dữ liệu cho mạng WSN công nghiệp. Trong [44], các tác giả đề xuất các phương pháp lựa chọn nút chuyển tiếp và nút gây

nhiễu khác nhau nhằm nâng cao cả hiệu năng dừng và hiệu năng IP cho các mạng hai chặng nhiều nút chuyển tiếp sử dụng kỹ thuật DF. Các tác giả [45] đã đề xuất giao thức truyền dẫn dựa vào FC để bảo mật thông tin từ nút nguồn đến nút đích. Hơn nữa, phương pháp tái cấu trúc FC mới, thích ứng cơ hội giải mã theo phương thức dự báo xác suất dừng (outage prediction) đã được khảo sát trong [45]. Giao thức truyền dựa vào mã Rateless để cung cấp bảo mật cho các hệ thống vô tuyến cũng được đề cập trong [46], với nút nguồn sử dụng kỹ thuật TAS để phát các gói mã hóa đến nút đích và nút gây nhiễu cộng tác (cooperative jammer) thu thập năng lượng từ các tín hiệu RF của nút nguồn và các nguồn nhiễu xung quanh để tạo nhiễu nhân tạo đến nút nghe lén.

Tuy nhiên, qua khảo sát các công trình có liên quan, theo sự hiểu biết tốt nhất của tác giả, hiện nay có rất ít nghiên cứu về PLS trong các hệ thống sử dụng FC và đây là hướng nghiên cứu mới đầy tiềm năng để có thể phát triển trong tương lai. Trong luận án này, tác giả nghiên cứu hiệu năng bảo mật các giao thức sử dụng FC. Thông thường, các công trình liên quan đánh giá OP và IP dựa vào dung lượng của kênh dữ liệu và kênh nghe lén. Tuy nhiên, luận án nghiên cứu về FC nên sự đánh giá bảo mật khác hơn, nhưng về mặt kỹ thuật sử dụng cho PLS như hệ thống MISO, MIMO, truyền đa chặng và tạo nhiễu nhân tạo đã được áp dụng. Chính vì vậy, tác giả đề xuất các giao thức như MISO TAS trong môi trường vô tuyến nhận thức dạng nền, MIMO TAS/SC, MIMO-NOMA TAS/SC/MRC và các hệ thống đa chặng, nhằm cải thiện hiệu năng bảo mật mạng, làm cơ sở áp dụng vào trong thực tiễn.

1.9. KẾT LUẬN CHƯƠNG

Chương 1 đã trình bày những vấn đề cơ bản về khái niệm lý thuyết bảo mật thông tin, PLS trong một số mạng vô tuyến thông thường, vô tuyến nhận thức có liên quan trực tiếp đến hướng nghiên cứu và các hệ thống bảo mật sử dụng mã Fountain. Trên cơ sở những vấn đề được đề cập, làm cơ sở để NCS giải quyết các nội dung đặt ra trong các Chương kế tiếp của Luận án.

Chương 2
HIỆU NĂNG BẢO MẬT TRONG CÁC MẠNG MISO TAS VÀ MIMO TAS/SC SỬ DỤNG MÃ FOUNTAIN

2.1. GIỚI THIỆU

Phổ tần số vô tuyến là tài nguyên hữu hạn rất quan trọng, được chia thành các băng tần không chồng lên nhau và được gán đến các tế bào khác nhau trong hệ thống thông tin di động tế bào (GSM và LTE) [95, 98]. Các hệ thống vô tuyến di động tế bào dựa trên sự phân bổ thông minh và tái sử dụng các kênh trên toàn bộ một vùng phủ sóng, trong vùng phủ sóng nhất định có một số tế bào (cell) khác nhau được sử dụng lặp lại cùng một tập các tần số, gọi là các tế bào đồng kênh và nhiễu giữa các tín hiệu này gọi là nhiễu đồng kênh. Không giống như nhiễu nhiệt (thermal noise) có thể được khắc phục bằng cách tăng SNR, nhiễu đồng kênh không thể chống lại bằng phương pháp đơn giản là tăng công suất sóng mang của máy phát. Bởi vì khi tăng công suất phát thì sẽ tăng nhiễu đến các tế bào đồng kênh lân cận. Để làm giảm CCI, các tế bào đồng kênh phải được phân tách vật lý bởi một khoảng cách tối thiểu nhằm cung cấp sự cách ly hiệu quả do quá trình truyền lan sóng vô tuyến. Do vậy, CCI thường được xác nhận là một trong những yếu tố làm hạn chế dung lượng và chất lượng truyền dẫn trong thông tin vô tuyến. Vậy nên, việc khảo sát đặc tính thống kê của CCI là vấn đề cực kỳ quan trọng khi phân tích và thiết kế các hệ thống vô tuyến đa người dùng hoặc khai thác các kỹ thuật để giảm thiểu ảnh hưởng không mong muốn của CCI [95, 98]. Mặt khác, các thiết bị vô tuyến nhỏ gọn, rẻ tiền như các nút cảm biến, phần cứng bị suy giảm do không cân bằng I/Q, nhiễu pha và không tuyến tính trong bộ khuếch đại [66-68]. Do đó, đánh giá sự tác động của giao thoa đồng kênh và HWI lên hiệu năng bảo mật hệ thống cần được khảo sát.

Xuất phát từ những vấn đề trên, trong Chương 2, Luận án đề xuất hai mô hình để phân tích hiệu năng bảo mật của các mạng MISO TAS và MIMO TAS/SC sử dụng FC dưới tác động của CCI, gồm có: Phần 2.2 phân tích mô hình truyền dữ liệu của mạng MISO sử dụng mã Fountain, với kỹ thuật lựa chọn ăng-ten phát trong môi trường vô tuyến nhận thức dạng nền, dưới sự tác động của chung giao thoa đồng kênh từ mạng sơ cấp và suy giảm phần cứng. Phần 2.3 đánh giá mô hình MIMO TAS/SC nhằm nâng cao độ tin cậy của truyền các gói mã hóa trên kênh chính sử dụng FC dưới tác động của CCI.

Trong mô hình đề xuất ở Phần 2.2, nút nguồn thứ cấp mã hóa dữ liệu gốc với FC và sử dụng TAS để gửi các gói mã hóa đến một nút đích thứ cấp. Theo nguyên lý hoạt động của kỹ thuật chia sẻ phổ tần dạng nền (underlay), công suất phát của nút nguồn thứ cấp phải được hiệu chỉnh để không làm ảnh hưởng đến chất lượng dịch vụ của mạng sơ cấp. Dưới tác động chung của giao thoa đồng kênh từ mạng sơ cấp và suy giảm phần cứng, nút đích thứ cấp phải cố gắng đạt được đủ số gói mã hóa trước nút nghe lén thứ cấp để bảo mật thông tin nguồn. Trong Chương này, luận án đưa ra các biểu thức đánh giá bảo mật dựa vào hai thông số hiệu năng chính là xác suất giải mã và bảo mật thông tin thành công (SS) và xác suất thu chặn (IP) trên kênh truyền pha đinh Rayleigh. Hơn nữa, tác giả cũng thực hiện mô phỏng Monte Carlo để kiểm chứng các biểu thức toán học được đưa ra.

Mô hình đề xuất trong Phần 2.3, khác với mô hình đã xét trong Phần 2.2, tác giả xem xét mô hình tổng quát hơn, với cả nút đích và nút nghe lén đều chịu ảnh hưởng của giao thoa đồng kênh gây ra từ nhiều nguồn giao thoa, trong môi trường vô tuyến thông thường. Mặc dù mô hình đề xuất trong Phần 2.2 đã xem xét sự tác động của giao thoa đồng kênh và suy giảm phần cứng lên hiệu năng bảo mật trong môi trường vô tuyến nhận thức, tuy nhiên chỉ khảo sát hệ thống với 01 nguồn giao thoa và các thiết bị thu chỉ được trang bị đơn ăng-ten. Do đó, trong Phần 2.3, một nút nguồn lựa chọn ăng-ten phát tốt

nhất để gửi từng gói mã hóa đến một nút đích. Cùng lúc đó, một nút nghe lén cố gắng nhận những gói mã hóa này để giải mã dữ liệu gốc của nút nguồn. Cả nút đích và nút nghe lén đều sử dụng kỹ thuật SC để giải mã những gói mã hóa nhận được. Hơn nữa, cả hai nút này đều chịu ảnh hưởng từ nhiều nguồn giao thoa trong mạng. Trong đó, tác giả xem xét với hai trường hợp: 1) Nút đích và nút nghe lén không có CSI đến các nguồn giao thoa; 2) Nút đích và nút nghe lén có thể ước lượng chính xác CSI đến các nguồn giao thoa. Tiếp theo, nội dung Phần này đã đưa ra biểu thức tính xác suất giải mã và bảo mật thông tin thành công trên kênh truyền pha đinh Rayleigh trong cả hai trường hợp. Cuối cùng, mô phỏng máy tính để kiểm chứng các biểu thức toán học.

Phần còn lại của Chương này được tổ chức như sau: Phần 2.2 miêu tả mô hình đề xuất 1 và mô hình đề xuất 2 được trình bày trong Phần 2.3, trong đó các biểu thức của SS, IP được đưa ra và các kết quả mô phỏng được thể hiện. Cuối cùng, nội dung của Chương được kết luận trong Phần 2.4.

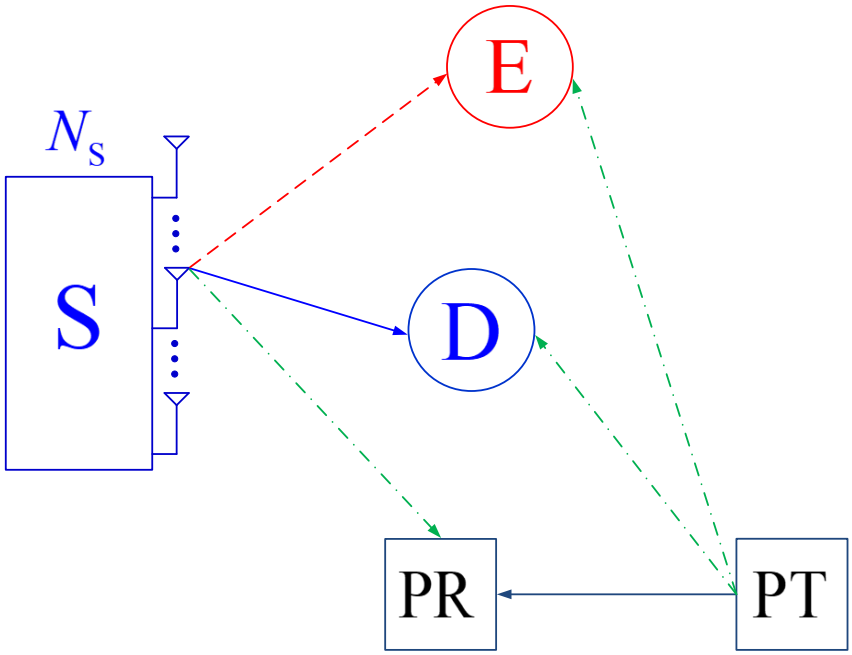
Đóng góp của Chương 2 được trình bày trong các công trình A1 và A2.

2.2. MÔ HÌNH 1: MẠNG MISO TAS SỬ DỤNG MÃ FOUNTAIN TRONG MÔI TRƯỜNG VÔ TUYẾN NHẬN THỨC DẠNG NỀN

2.2.1. Mô hình hệ thống

Như được miêu tả trong Hình 2.1, hai mạng sơ cấp và thứ cấp cùng sử dụng chung một băng tần. Đối với mạng sơ cấp, máy phát sơ cấp PT (Primary Transmitter) muốn gửi dữ liệu đến một máy thu sơ cấp PR (Primary Receiver). Cùng lúc đó, trong mạng thứ cấp, một nút nguồn thứ cấp S (Secondary Source) cũng truyền dữ liệu đến nút đích thứ cấp D (Secondary Destination). Cũng trong mạng thứ cấp, nút nghe lén thứ cấp E (Secondary Eavesdropper) đang cố gắng nghe lén dữ liệu mà S muốn gửi đến D. Do hai mạng sơ cấp và thứ cấp cùng hoạt động trên một dải tần, các máy phát sơ cấp và thứ cấp sẽ gây nhiễu đồng kênh lên các thiết bị thu thứ cấp và sơ cấp. Tuy

nhiên, để đảm bảo chất lượng dịch vụ cho mạng sơ cấp (mạng được cấp phép sử dụng băng tần), S phải hiệu chỉnh công suất phát một cách thích hợp.



Hình 2.1: Mô hình hệ thống đề xuất.

Giả sử rằng PT, PR, D và E chỉ có 01 ăng-ten, trong khi S được trang bị với N_S ăng-ten phát và sử dụng kỹ thuật TAS để gửi các gói dữ liệu đến D sử dụng FC. Đầu tiên, S chia dữ liệu gốc của mình thành L gói nhỏ có độ dài bằng nhau. Từ đó, một số lượng các gói nhỏ này sẽ được chọn một cách ngẫu nhiên và XOR lại với nhau để tạo thành những gói mới (ta gọi các gói mới này là các gói tin được mã hóa hay gói mã hóa). Kích thước của những gói mã hóa có thể lớn hơn kích thước của những gói nhỏ đã chọn ra do chúng được thêm vào một số thông tin trong phần mào đầu để phục vụ cho việc giải mã sau này. Sau đó, S sẽ lần lượt gửi các gói mã hóa đến D sử dụng những khe thời gian trực giao theo phương thức đa truy nhập phân chia theo thời gian (Time Division Multiple Access: TDMA). Bởi tính chất quảng bá của kênh thông tin vô tuyến, E cũng nhận được các gói mã hóa của S. Tác giả xem xét hệ thống giới hạn về thời gian trễ, trong đó số lượng gói mã hóa tối đa mà S có thể gửi đến D được cố định bởi $N_{\max}$. Theo nguyên lý giải mã FC, D và E

sẽ cố gắng giải mã các gói mã hóa và lưu trữ dữ liệu vào bộ đệm của mình. Để có thể khôi phục lại dữ liệu gốc của S, thì D và E phải nhận thành công ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa, với $N_{\text{req}}^{\text{pkt}} = (1+\varepsilon)L$ và $\varepsilon(\varepsilon > 0)$ là phần thông tin được bổ sung, phụ thuộc vào việc thiết kế mã [34, 35], [38], [40-46], trong đó $N_{\text{req}}^{\text{pkt}} \le N_{\max}$. Hơn thế nữa, nếu D có thể nhận đủ $N_{\text{req}}^{\text{pkt}}$ gói mã hóa trước khi S phát đủ $N_{\max}$ gói, D sẽ ngay lập tức gửi thông điệp ACK đến S để S dừng truyền dữ liệu. Trong trường hợp này, nếu E không thể nhận đủ $N_{\text{req}}^{\text{pkt}}$ gói mã hóa từ S thì E sẽ không thể giải mã được dữ liệu gốc của S, quá trình truyền dữ liệu giữa S và D là thành công và bảo mật (SS). Ngược lại, nếu E có thể nhận được ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa, dữ liệu gốc sẽ mất bảo mật hay bị thu chặn (IP). Sau khi D nhận thành công dữ liệu, S sẽ bắt đầu gửi dữ liệu mới đến D sử dụng phương pháp như đã trình bày ở trên. Cũng vậy, E sẽ cố gắng nhận những gói mã hóa mới để đạt được dữ liệu gốc của S.

2.2.1.1. Mô hình kênh truyền và suy giảm phần cứng

Giả sử tất cả các kênh truyền đều là kênh pha đinh Rayleigh. Tác giả ký hiệu $\gamma_{\text{X,Y}}$ là độ lợi kênh giữa hai nút X và Y. Hơn nữa, $\gamma_{\text{X,Y}}$ sẽ có phân phối mũ với hàm phân bố tích lũy (Cumulative Distribution Functions: CDF) là:

$$F_{\gamma_{\text{X,Y}}}(x) = 1 - \exp(-\lambda_{\text{X,Y}} x), \tag{2.1}$$

trong đó, $\lambda_{\text{X,Y}}$ là tham số đặc trưng của biến ngẫu nhiên $\gamma_{\text{X,Y}}$, được cho là $\lambda_{\text{X,Y}} = 1/\varepsilon\{\gamma_{\text{X,Y}}\}$, với $\varepsilon\{.\}$ là toán tử kỳ vọng và tham số $\lambda_{\text{X,Y}}$ có thể được biểu diễn bằng công thức sau (xem tài liệu [108]):

$$\lambda_{\text{X,Y}} = d_{\text{X,Y}}^{\beta}, \tag{2.2}$$

với $d_{\text{X,Y}}$ là khoảng cách giữa 2 nút $\text{X}-\text{Y}$ và β là hệ số suy hao đường truyền có giá trị từ 2 đến 6. Do đó, hàm mật độ xác suất (Probability Density Function: PDF) của $\gamma_{\text{X,Y}}$ sẽ là:

$$f_{\gamma_{\mathrm{X,Y}}}(x)=\lambda_{\mathrm{X,Y}}\exp\left(-\lambda_{\mathrm{X,Y}}x\right). \tag{2.3}$$

Ta cũng ký hiệu $\gamma_{\mathrm{S}_m,\mathrm{Y}}$ là độ lợi kênh pha đinh Rayleigh giữa ăng-ten phát thứ m của S và nút Y, với $m=1,2,...,N_{\mathrm{S}}$. Giả sử rằng các độ lợi kênh truyền $\gamma_{\mathrm{S}_m,\mathrm{Y}}$ là độc lập và đồng nhất (independent and identically distributed: i.i.d.) với nhau, cụ thể là $\lambda_{\mathrm{S}_m,\mathrm{Y}}=\lambda_{\mathrm{S,Y}}$ với mọi m.

Xem xét quá trình truyền dữ liệu giữa máy phát X và máy thu Y, với sự xuất hiện của suy giảm phần cứng, tín hiệu nhận được tại Y được cho như trong [67, 68] là:

$$y=\sqrt{P_{\mathrm{X}}}h_{\mathrm{X,Y}}\left(x_0+\eta_{\mathrm{t,X}}\right)+\eta_{\mathrm{r,Y}}+n_{\mathrm{Y}}, \tag{2.4}$$

với x_0 là dữ liệu nguồn, P_{X} là công suất phát của X, $h_{\mathrm{X,Y}}$ là hệ số kênh truyền của liên kết $\mathrm{X}-\mathrm{Y}$, $\eta_{\mathrm{t,X}}$ và $\eta_{\mathrm{r,Y}}$ là nhiễu sinh ra do phần cứng không lý tưởng tại X và Y, tương ứng và n_{Y} là nhiễu Gauss tại Y.

Tương tự, các kết quả đo lường và khảo sát lý thuyết như trong [67, 68], đã thể hiện $\eta_{\mathrm{t,X}}$, $\eta_{\mathrm{r,Y}}$ và n_{Y} được mô hình là các biến ngẫu nhiên Gauss với trung bình bằng 0 và phương sai được cho, tương ứng là

$$\mathrm{var}\left\{\eta_{\mathrm{t,X}}\right\}=\kappa_{\mathrm{t}}^2,\ \mathrm{var}\left\{\eta_{\mathrm{r,Y}}\right\}=\kappa_{\mathrm{r}}^2P_{\mathrm{X}}\left|h_{\mathrm{X,Y}}\right|^2,\ \mathrm{var}\left\{n_{\mathrm{Y}}\right\}=\sigma^2, \tag{2.5}$$

trong đó, κ_{t}^2 và κ_{r}^2 là các mức suy giảm phần cứng tại X và Y, tương ứng.

Do đó, HWI được sử dụng để định lượng sự sai lệch giữa dữ liệu nguồn xác định trước x_0 và tín hiệu thực tế trong các máy thu/phát RF. Lưu ý rằng, khi $\kappa_{\mathrm{t}}=\kappa_{\mathrm{r}}=0$, có nghĩa là phần cứng lý tưởng tại máy phát và máy thu.

Hơn nữa, nhiễu gây ra do suy giảm phần cứng của máy thu/phát được xem như nguồn nhiễu bổ sung của phương sai $\left(\kappa_{\mathrm{t}}^2+\kappa_{\mathrm{r}}^2\right)P_{\mathrm{X}}\left|h_{\mathrm{X,Y}}\right|^2$, nên ta xác định mức độ suy giảm phần cứng tại cả máy phát và máy thu là $\kappa=\sqrt{\kappa_{\mathrm{t}}^2+\kappa_{\mathrm{r}}^2}$.

Từ các công thức (2.4) và (2.5), SINR tức thời được tính bởi

$$\psi_{\mathrm{X,Y}} = \frac{P_{\mathrm{X}} \left| h_{\mathrm{X,Y}} \right|^2}{\left(\kappa_{\mathrm{t}}^2 + \kappa_{\mathrm{r}}^2 \right) P_{\mathrm{X}} \left| h_{\mathrm{X,Y}} \right|^2 + \sigma^2}$$

$$= \frac{P_{\mathrm{X}} \left| h_{\mathrm{X,Y}} \right|^2}{\kappa^2 P_{\mathrm{X}} \left| h_{\mathrm{X,Y}} \right|^2 + \sigma^2}, \tag{2.6}$$

với $\kappa^2 = \kappa_{\mathrm{t}}^2 + \kappa_{\mathrm{r}}^2$ là tổng mức suy giảm phần cứng.

2.2.1.2. Điều kiện đối với công suất phát của nút nguồn thứ cấp

Giả sử S sử dụng ăng-ten phát thứ m để gửi gói mã hóa đến D với công suất phát P_{S}. Như vậy, SINR nhận được tại PR được viết như sau (xem [98]):

$$\psi_{\mathrm{PT,PR}} = \frac{P_{\mathrm{PT}} \gamma_{\mathrm{PT,PR}}}{\kappa_{\mathrm{P}}^2 P_{\mathrm{PT}} \gamma_{\mathrm{PT,PR}} + P_{\mathrm{S}} \gamma_{\mathrm{S}_m,\mathrm{PR}} + \sigma^2}, \tag{2.7}$$

với P_{PT} là công suất phát của PT, σ^2 là phương sai của nhiễu cộng tại PR và κ_{P}^2 là mức suy giảm phần cứng tổng cộng tại PT và PR. Để đơn giản cho việc trình bày và tính toán, ta giả sử phương sai của nhiễu cộng tại tất cả các thiết bị thu đều có phân bố Gauss với giá trị trung bình bằng 0 và phương sai bằng σ^2.

Đặt γ_{P} là giá trị ngưỡng dương xác định trước mà ở đó PR không thể giải mã thành công dữ liệu nhận được từ PT, nếu SINR thu được $\psi_{\mathrm{PT,PR}}$ nhỏ hơn γ_{P}. Thật vậy, xác suất của sự kiện này xảy ra được tính như sau:

$$\rho_{\mathrm{P}} = \Pr\left(\psi_{\mathrm{PT,PR}} < \gamma_{\mathrm{P}} \right). \tag{2.8}$$

Bổ đề 1: Nếu $1 - \kappa_{\mathrm{P}}^2 \gamma_{\mathrm{P}} \le 0,$ thì $\rho_{\mathrm{P}} = 1$ và ngược lại nếu $1 - \kappa_{\mathrm{P}}^2 \gamma_{\mathrm{P}} > 0,$ biểu thức xác suất của ρ_{P} được viết dưới dạng chính xác là

$$\rho_{\mathrm{P}} = 1 - \frac{\lambda_{\mathrm{S,PR}} \left(1 - \kappa_{\mathrm{P}}^2 \gamma_{\mathrm{P}} \right) P_{\mathrm{PT}}}{\lambda_{\mathrm{S,PR}} \left(1 - \kappa_{\mathrm{P}}^2 \gamma_{\mathrm{P}} \right) P_{\mathrm{PT}} + \lambda_{\mathrm{PT,PR}} \gamma_{\mathrm{P}} P_{\mathrm{S}}} \exp\left(- \frac{\sigma^2 \lambda_{\mathrm{PT,PR}} \gamma_{\mathrm{P}}}{\left(1 - \kappa_{\mathrm{P}}^2 \gamma_{\mathrm{P}} \right) P_{\mathrm{PT}}} \right). \tag{2.9}$$

Chứng minh: Xem chứng minh và các ký hiệu trong mục A1, Phụ lục A.

Để mạng sơ cấp đảm bảo chất lượng dịch vụ: $\rho_{\mathrm{P}} \le \varepsilon_{\mathrm{P}}$, công suất phát tối đa mà S có thể sử dụng được tính như sau:

$$P_{\mathrm{S}} = \left[0, \frac{\lambda_{\mathrm{S,PR}} \left(1-\kappa_{\mathrm{P}}^2 \gamma_{\mathrm{P}}\right) P_{\mathrm{PT}}}{\lambda_{\mathrm{PT,PR}} \gamma_{\mathrm{P}}} \left(\frac{1}{\left(1-\varepsilon_{\mathrm{P}}\right)} \exp\left(-\frac{\sigma^2 \lambda_{\mathrm{PT,PR}} \gamma_{\mathrm{P}}}{\left(1-\kappa_{\mathrm{P}}^2 \gamma_{\mathrm{P}}\right) P_{\mathrm{PT}}} \right) - 1 \right) \right]^+, \quad (2.10)$$

với $\left[x,0\right]^+ = \max\left(x,0\right)$ và ε_{P} là ngưỡng dừng mong muốn của mạng sơ cấp (mạng sơ cấp mong muốn ngưỡng dừng phải nhỏ hơn hoặc bằng giá trị này). Công thức (2.10) có ý nghĩa rằng nếu có sự giao thoa từ mạng thứ cấp làm cho $\rho_{\mathrm{P}} \ge \varepsilon_{\mathrm{P}}$ thì mạng sơ cấp sẽ không cho phép mạng thứ cấp hoạt động nữa, tức là mạng thứ cấp phải im lặng và công suất phát của nút nguồn thứ cấp phải thiết lập về 0 $\left(P_{\mathrm{S}} = 0\right)$, đồng nghĩa PR không cho phép S sử dụng chung phổ tần với mình. Ta cũng quan sát từ công thức (2.10) rằng công suất phát tối đa của tất cả các ăng-ten phát tại S đều như nhau $\left(P_{\mathrm{S}_m} = P_{\mathrm{S}} \forall m\right)$ và cũng là một hàm của P_{PT}. Hơn nữa, khi P_{PT} đủ lớn $\left(P_{\mathrm{PT}} \to +\infty\right)$, ta có xấp xỉ sau:

$$P_{\mathrm{S}} \overset{P_{\mathrm{PT}} \to +\infty}{\approx} P_{\mathrm{S}}^* = \frac{\lambda_{\mathrm{S,PR}} \left(1-\kappa_{\mathrm{P}}^2 \gamma_{\mathrm{P}}\right) \varepsilon_{\mathrm{P}}}{\lambda_{\mathrm{PT,PR}} \left(1-\varepsilon_{\mathrm{P}}\right) \gamma_{\mathrm{P}}} P_{\mathrm{PT}}. \quad (2.11)$$

Từ (2.11), khi P_{PT} đủ lớn, công suất phát của S tăng tuyến tính theo P_{PT}.

2.2.1.3. Lựa chọn ăng-ten phát tại nút nguồn thứ cấp

Trước khi gửi một gói mã hóa đến D, S lựa chọn ăng-ten phát tốt nhất của mình theo tiêu chí sau:

$$\gamma_{\mathrm{S}_{a^*},\mathrm{D}} = \max_{m=1,2,...,N_{\mathrm{S}}} \left(\gamma_{\mathrm{S}_m,\mathrm{D}}\right), \quad (2.12)$$

trong đó, a^* là ăng-ten được chọn để phát dữ liệu tại S, với $a^* \in \left\{1,2,...,N_{\mathrm{S}}\right\}$. Công thức (2.12) có nghĩa rằng S sẽ lựa chọn ăng-ten đạt được độ lợi kênh đến D lớn nhất để gửi dữ liệu. Hơn nữa, khi $\gamma_{\mathrm{S}_m,\mathrm{D}}$ là độc lập và đồng nhất với nhau thì hàm phân bố tích lũy của $\gamma_{\mathrm{S}_{a^*},\mathrm{D}}$ sẽ là

$$F_{\gamma_{S_{a^*},D}}(x) = \left(1-\exp\left(-\lambda_{S,D}x\right)\right)^{N_S}$$

$$= 1+\sum_{m=1}^{N_S}(-1)^m C_{N_S}^m \exp\left(-m\lambda_{S,D}x\right). \quad (2.13)$$

Do đó, SINR nhận được tại D và E để giải mã mỗi gói mã hóa của S trong một khe thời gian sẽ lần lượt đạt được như sau:

$$\psi_D = \frac{P_S\gamma_{S_{a^*},D}}{\kappa_D^2 P_S\gamma_{S_{a^*},D} + P_{PT}\gamma_{PT,D} + \sigma^2}, \quad (2.14)$$

$$\psi_E = \frac{P_S\gamma_{S_{a^*},E}}{\kappa_E^2 P_S\gamma_{S_{a^*},E} + P_{PT}\gamma_{PT,E} + \sigma^2}, \quad (2.15)$$

trong đó, κ_D^2 và κ_E^2 lần lượt là tổng mức suy giảm phần cứng trên các kênh liên kết $S \to D$ và $S \to E$.

Tiếp theo, giả sử rằng một gói mã hóa có thể được giải mã thành công nếu SINR nhận được tại D và E lớn hơn một ngưỡng γ_{th} xác định trước. Ngược lại, gói mã hóa đó sẽ không được giải mã thành công. Vì vậy, xác suất mà D và E không thể nhận thành công một gói dữ liệu sẽ được viết như sau:

$$\rho_D = \Pr\left(\psi_D \le \gamma_{th}\right), \quad (2.16)$$

$$\rho_E = \Pr\left(\psi_E \le \gamma_{th}\right). \quad (2.17)$$

Tiếp theo, lưu ý rằng xác suất mà D và E có thể nhận được một gói mã hóa thành công sẽ lần lượt là: $1-\rho_D$ và $1-\rho_E$. Hơn nữa, giả sử rằng các xác suất ρ_D và ρ_E không thay đổi trong mỗi khe thời gian và do đó, ta có thể bỏ qua chỉ số thời gian trong các ký hiệu này.

Do hệ thống bị ràng buộc độ trễ, số khe thời gian được sử dụng để phát các gói mã hóa bị giới hạn bởi N_{max}. Tác giả ký hiệu $N\left(N_{req}^{pkt} \le N \le N_{max}\right)$ là số khe thời gian được sử dụng bởi nút nguồn (hoặc số gói mã hóa được phát bởi nút nguồn), N_D^{pkt} và N_E^{pkt} là số gói mã hóa nhận được bởi nút D và nút E

sau khi nút nguồn dừng truyền, tương ứng. Bây giờ, tác giả đưa ra biểu thức tính xác suất giải mã và bảo mật thông tin thành công (SS) của quá trình truyền từ S đến D như sau:

$$\mathrm{SS} = \Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}},\ N_{\mathrm{E}}^{\mathrm{pkt}} < N_{\mathrm{req}}^{\mathrm{pkt}} \mid N \le N_{\max}\right). \tag{2.18}$$

Biểu thức (2.18) ngụ ý rằng nút đích có thể nhận đủ số gói mã hóa $\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}}\right)$ trước nút nghe lén $\left(N_{\mathrm{E}}^{\mathrm{pkt}} < N_{\mathrm{req}}^{\mathrm{pkt}}\right)$ khi số khe thời gian được sử dụng $\left(N \le N_{\max}\right)$.

Kế tiếp, tác giả đưa ra biểu thức xác suất thu chặn (IP), được định nghĩa là xác suất mà nút nghe lén có thể đạt được thành công $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa trước hoặc cùng lúc với nút đích.

$$\mathrm{IP} = \Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}},\ N_{\mathrm{D}}^{\mathrm{pkt}} \le N_{\mathrm{req}}^{\mathrm{pkt}} \mid N \le N_{\max}\right). \tag{2.19}$$

Lưu ý từ biểu thức (2.19) rằng khi nút nghe lén đạt được $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa, nút này không cần nhận thêm số gói mã hóa nữa. Thay vào đó, E sẽ bắt đầu giải mã dữ liệu gốc của nút nguồn.

2.2.2. Phân tích hiệu năng

2.2.2.1. Xác suất của ρ_{D} và ρ_{E}

Bổ đề 2: Nếu $1-\kappa_{\mathrm{D}}^2\gamma_{\mathrm{th}} \le 0,$ thì $\rho_{\mathrm{D}} = 1$ và nếu $1-\kappa_{\mathrm{D}}^2\gamma_{\mathrm{th}} > 0,$ ρ_{D} có thể được biểu diễn dưới dạng chính xác là

$$\rho_{\mathrm{D}} = 1 + \sum_{m=1}^{N_{\mathrm{S}}} \frac{(-1)^m C_{N_{\mathrm{S}}}^m \lambda_{\mathrm{PT,D}}}{\lambda_{\mathrm{PT,D}} + m\lambda_{\mathrm{S,D}}\mu_{\mathrm{D}}} \exp\left(-m\lambda_{\mathrm{S,D}}\omega_{\mathrm{D}}\right). \tag{2.20}$$

Chứng minh: Xem chứng minh và các ký hiệu trong mục A2, Phụ lục A.

Tiếp đến, khi công suất phát của PT đủ lớn, biểu thức xấp xỉ của ρ_{D} đạt được như sau:

$$\rho_{\mathrm{D}} \overset{P_{\mathrm{PT}} \to +\infty}{\approx} 1 + \sum_{m=1}^{N_{\mathrm{S}}} (-1)^m C_{N_{\mathrm{S}}}^m \frac{\lambda_{\mathrm{PT,D}}}{\lambda_{\mathrm{PT,D}} + m\lambda_{\mathrm{S,D}}\mu_{\mathrm{D}}^*}, \tag{2.21}$$

với

$$\mu_{\mathrm{D}}^{*}=\frac{\lambda_{\mathrm{PT,PR}}\left(1-\varepsilon_{\mathrm{P}}\right)\gamma_{\mathrm{P}}\gamma_{\mathrm{th}}}{\lambda_{\mathrm{S,PR}}\left(1-\kappa_{\mathrm{D}}^{2}\gamma_{\mathrm{th}}\right)\left(1-\kappa_{\mathrm{P}}^{2}\gamma_{\mathrm{P}}\right)\varepsilon_{\mathrm{P}}}. \tag{2.22}$$

Quan sát từ các công thức (2.21) và (2.22), ta thấy rằng khi P_{PT} đủ lớn thì ρ_{D} không phụ thuộc vào P_{PT} nữa. Điều này có nghĩa rằng do ảnh hưởng của nhiễu đồng kênh và khi công suất phát của PT tăng, công suất phát của mạng thứ cấp cũng tăng, dẫn đến SNR ở các giá trị công suất phát sơ cấp cao và sẽ không phụ thuộc vào công suất phát của mạng sơ cấp nữa.

Bổ đề 3: Nếu $1-\kappa_{\mathrm{E}}^{2}\gamma_{\mathrm{th}}\le 0,$ thì $\rho_{\mathrm{E}}=1$ và nếu $1-\kappa_{\mathrm{E}}^{2}\gamma_{\mathrm{th}}>0,$ ρ_{E} được tính chính xác là

$$\rho_{\mathrm{E}}=1-\frac{\lambda_{\mathrm{PT,E}}}{\lambda_{\mathrm{PT,E}}+\lambda_{\mathrm{S,E}}\mu_{\mathrm{E}}}\exp\left(-\lambda_{\mathrm{S,E}}\omega_{\mathrm{E}}\right), \tag{2.23}$$

với

$$\mu_{\mathrm{E}}=\frac{P_{\mathrm{PT}}\gamma_{\mathrm{th}}}{\left(1-\kappa_{\mathrm{E}}^{2}\gamma_{\mathrm{th}}\right)P_{\mathrm{S}}},\ \omega_{\mathrm{E}}=\frac{\sigma^{2}\gamma_{\mathrm{th}}}{\left(1-\kappa_{\mathrm{E}}^{2}\gamma_{\mathrm{th}}\right)P_{\mathrm{S}}}. \tag{2.24}$$

Hơn nữa, khi $P_{\mathrm{PT}}\to+\infty,$ ρ_{E} cũng không phụ thuộc vào $P_{\mathrm{PT}},$ cụ thể:

$$\rho_{\mathrm{E}}\overset{P_{\mathrm{PT}}\to+\infty}{\approx}1-\frac{\lambda_{\mathrm{PT,E}}}{\lambda_{\mathrm{PT,E}}+\lambda_{\mathrm{S,E}}\mu_{\mathrm{E}}^{*}}, \tag{2.25}$$

với

$$\mu_{\mathrm{E}}^{*}=\frac{\lambda_{\mathrm{PT,PR}}\left(1-\varepsilon_{\mathrm{P}}\right)\gamma_{\mathrm{P}}\gamma_{\mathrm{th}}}{\lambda_{\mathrm{S,PR}}\left(1-\kappa_{\mathrm{E}}^{2}\gamma_{\mathrm{th}}\right)\left(1-\kappa_{\mathrm{P}}^{2}\gamma_{\mathrm{P}}\right)\varepsilon_{\mathrm{P}}}. \tag{2.26}$$

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

Tổng xác suất của SS trong (2.18) có thể được viết lại là

$$\mathrm{SS}=\sum_{w=N_{\mathrm{req}}^{\mathrm{pkt}}}^{N_{\max}}\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}\mid N=w\right)\times\sum_{q=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1}\Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}}=q\mid N=w\right). \tag{2.27}$$

Trong (2.27), $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \mid N = w\right)$ là xác suất mà D có thể nhận thành công $N_{\mathrm{D}}^{\mathrm{pkt}}$ gói mã hóa khi số khe thời gian được sử dụng bởi S là *w*. Khi quá trình truyền dữ liệu giữa S và D kết thúc tại khe thời gian thứ *w*, với $w\left(N_{\mathrm{req}}^{\mathrm{pkt}} \le w \le N_{\max}\right)$, thì $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \mid N = w\right)$ được tính tương tự như [38, công thức (8)]:

$$\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \mid N = w\right) = C_{w-1}^{w-N_{\mathrm{req}}^{\mathrm{pkt}}} \left(1-\rho_{\mathrm{D}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}} \left(\rho_{\mathrm{D}}\right)^{w-N_{\mathrm{req}}^{\mathrm{pkt}}}. \tag{2.28}$$

Hơn nữa, $\Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}} = q \mid N = w\right)$ trong (2.28) thể hiện là xác suất mà E chỉ có thể nhận thành công q gói mã hóa, với $0 \le q < N_{\mathrm{req}}^{\mathrm{pkt}}$, khi S kết thúc quá trình truyền sau khi đã gửi w gói mã hóa và được tính như sau:

$$\Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}} = q \mid N = w\right) = C_w^q \left(1-\rho_{\mathrm{E}}\right)^q \left(\rho_{\mathrm{E}}\right)^{w-q}. \tag{2.29}$$

Thay thế (2.28) và (2.29) vào (2.27), biểu thức chính xác dạng tường minh của SS được cho là

$$\mathrm{SS} = \sum_{w=N_{\mathrm{req}}^{\mathrm{pkt}}}^{N_{\max}} \left[C_{w-1}^{w-N_{\mathrm{req}}^{\mathrm{pkt}}} \left(1-\rho_{\mathrm{D}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}} \left(\rho_{\mathrm{D}}\right)^{w-N_{\mathrm{req}}^{\mathrm{pkt}}} \times \sum_{q=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} C_w^q \left(1-\rho_{\mathrm{E}}\right)^q \left(\rho_{\mathrm{E}}\right)^{w-q} \right]. \tag{2.30}$$

2.2.2.3. Xác suất thu chặn (IP)

Xác suất thu chặn trong (2.19) có thể được viết lại bởi

$$\mathrm{IP} = \sum_{w=N_{\mathrm{req}}^{\mathrm{pkt}}}^{N_{\max}} \Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \mid N = w\right)$$

$$\times \left[\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \mid N = w\right) + \sum_{r=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} \Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = r \mid N = w\right) \right]. \tag{2.31}$$

Trong (2.31), $\Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \mid N = w\right)$ là xác suất mà E có thể nhận đủ số gói mã hóa trong w khe thời gian, có thể được tính tương tự như (2.28) là

$$\Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \mid N = w\right) = C_{w-1}^{w-N_{\mathrm{req}}^{\mathrm{pkt}}} \left(1-\rho_{\mathrm{E}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}} \left(\rho_{\mathrm{E}}\right)^{w-N_{\mathrm{req}}^{\mathrm{pkt}}}. \tag{2.32}$$

Tiếp theo, $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \mid N = w\right)$ trong (2.31) được tính bởi (2.28) và $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = r \mid N = w\right)$ trong (2.31) có thể đạt được bởi

$$\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = r \mid N = w\right) = C_w^r \left(1-\rho_{\mathrm{D}}\right)^r \left(\rho_{\mathrm{D}}\right)^{w-r}. \tag{2.33}$$

Thay thế (2.28), (2.32) và (2.33) vào (2.31), biểu thức dạng tường minh của IP được đưa ra như sau:

$$\mathrm{IP} = \sum_{w=N_{\mathrm{req}}^{\mathrm{pkt}}}^{N_{\max}} C_{w-1}^{w-N_{\mathrm{req}}^{\mathrm{pkt}}} \left(1-\rho_{\mathrm{E}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}} \left(\rho_{\mathrm{E}}\right)^{w-N_{\mathrm{req}}^{\mathrm{pkt}}} \times \left[C_{w-1}^{w-N_{\mathrm{req}}^{\mathrm{pkt}}} \left(1-\rho_{\mathrm{D}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}} \left(\rho_{\mathrm{D}}\right)^{w-N_{\mathrm{req}}^{\mathrm{pkt}}} + \sum_{r=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} C_w^r \left(1-\rho_{\mathrm{D}}\right)^r \left(\rho_{\mathrm{D}}\right)^{w-r} \right]. \tag{2.34}$$

Để tính xác suất IP, ta xét hai trường hợp: Trường hợp 1: D có thể đạt được $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa từ S, tuy nhiên E cũng đạt được ít nhất $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa trong trường hợp này. Trường hợp 2: D không thể nhận đủ $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa sau khi S đã gửi hết $N_{\max}$ gói mã hóa, tuy nhiên E lại có thể đạt được ít nhất $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa. Trong công thức (2.34), số hạng đầu tiên là xác suất của trường hợp 1 và số hạng thứ hai là xác suất của trường hợp 2.

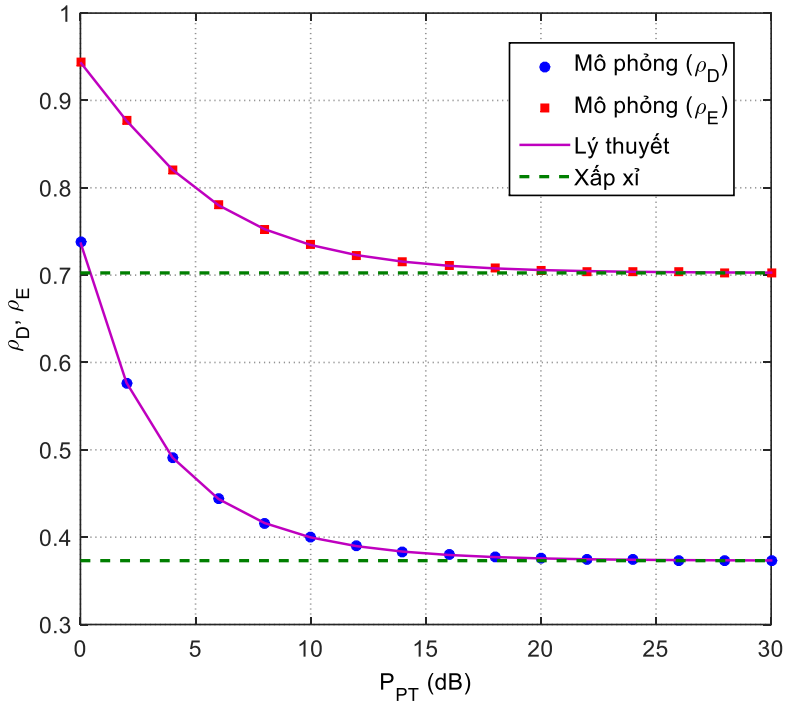
Lưu ý rằng, xác suất giải mã và bảo mật thông tin thành công có thể đạt được khi nút đích có thể nhận đủ số gói mã hóa từ nút nguồn trước nút nghe lén khi số khe thời gian được sử dụng nhỏ hơn hoặc bằng $N_{\max}$. Mặt khác, dữ liệu gốc của S bị thu chặn khi nút E đạt được $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa, bất kể nút nguồn sẽ phát các gói mã hóa trong những khe thời gian tiếp theo, thay vào đó E sẽ bắt đầu giải mã dữ liệu gốc của S.

Cuối cùng, thay các biểu thức của ρ_{D} và ρ_{E} đã đạt được trong Mục 2.2.2.1 vào (2.30) và (2.34), ta đạt được các biểu thức dạng tường minh (closed-form) chính xác cho SS và IP.

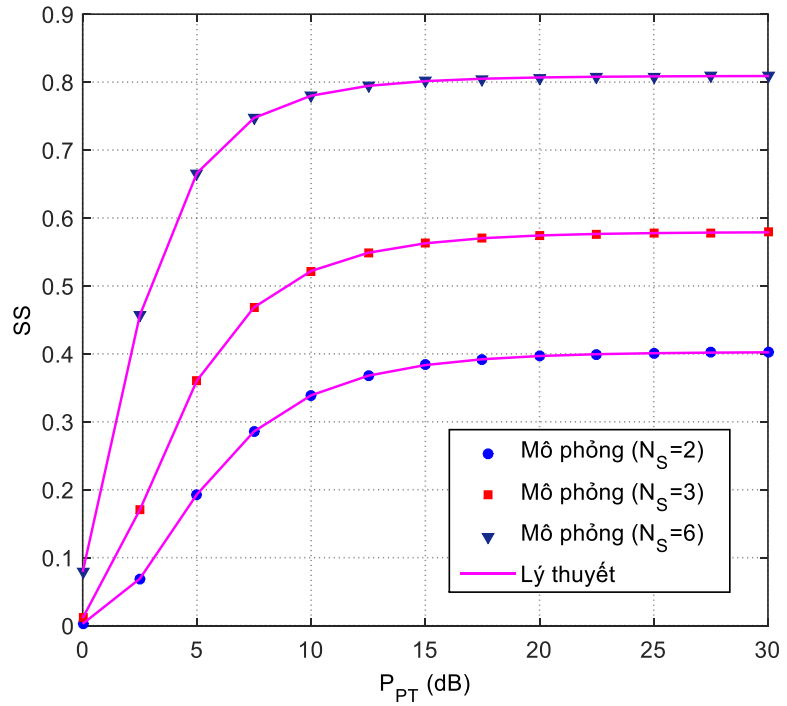
2.2.3. Các kết quả mô phỏng

Trong phần này, tác giả thực hiện các mô phỏng Monte Carlo để kiểm chứng các công thức đã được trình bày ở Phần 2.2.2. Trong môi trường mô phỏng, các nút mạng trong hệ trục tọa độ Đề-các (Descartes), với nút S được đặt tại gốc tọa độ (0,0), trong khi tọa độ của D là (1,0). Ta cũng đặt PT và PR cố định tại các vị trí PT(0.5,0.5) và PR(0.5,0), tương ứng. Để sự ảnh hưởng của giao thoa đồng kênh từ PT tác động đến D và E là đồng đều, cũng như khoảng cách từ S đến D và E là như nhau, ta cũng đặt E ở vị trí (1,0) (xem như E ở rất gần D). Do đó, ta dễ dàng tính được khoảng cách giữa các nút như sau: $d_{\mathrm{S,D}} = d_{\mathrm{S,E}} = 1,\ d_{\mathrm{PT,PR}} = 0.5,\ d_{\mathrm{S,PR}} = 0.5$ và $d_{\mathrm{PT,D}} = d_{\mathrm{PT,E}} = 1/\sqrt{2}.$ Giả sử hệ số suy hao đường truyền được cố định bằng 3 $(\beta = 3),$ tham số đặc trưng các kênh truyền là $\lambda_{\mathrm{S,D}} = \lambda_{\mathrm{S,E}} = 1,\ \lambda_{\mathrm{PT,PR}} = \lambda_{\mathrm{S,PR}} = 1/8$ và $\lambda_{\mathrm{PT,D}} = \lambda_{\mathrm{PT,E}} = 1/\left(\sqrt{2}\right)^3.$ Trong tất cả các mô phỏng, tác giả cũng cố định các tham số hệ thống khác như sau: $\sigma^2 = 1,\ N_{\mathrm{req}}^{\mathrm{pkt}} = 5,\ \gamma_{\mathrm{th}} = 0.3$ và $\varepsilon_{\mathrm{P}} = 0.1.$ Đối với tham số suy giảm phần cứng, ta giả sử: $\kappa_{\mathrm{P}}^2 = 0$ và $\kappa_{\mathrm{D}}^2 = \kappa_{\mathrm{E}}^2.$

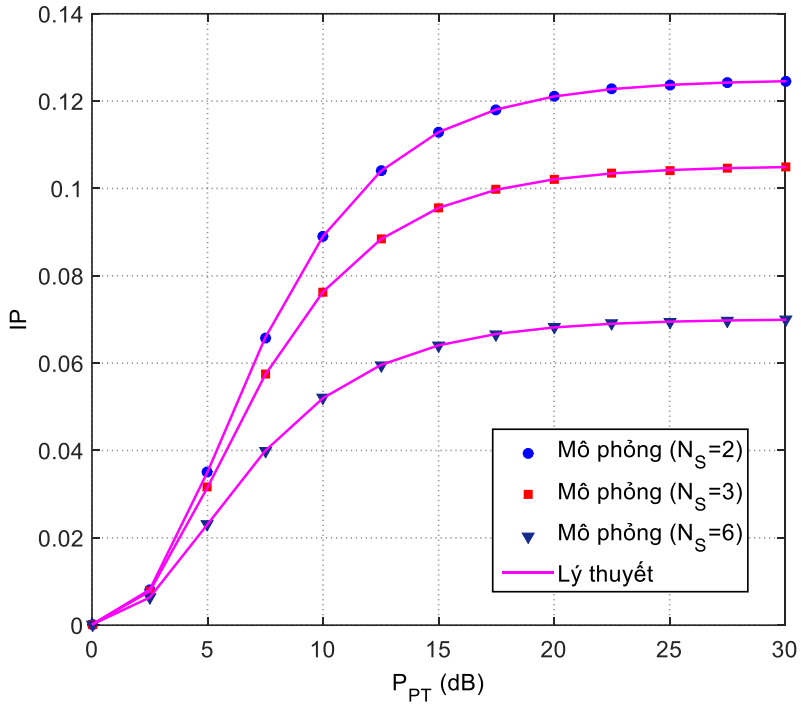
Hình 2.2 nhằm mục đích để kiểm chứng các công thức tính xác suất $\rho_{\mathrm{D}},$ ρ_{E} và ta nhận thấy P_{S} (dB) được tìm ra theo công thức (2.10) là một hàm phụ thuộc P_{PT} (dB), nên vẽ theo P_{S} (dB) thì cũng chính là vẽ theo P_{PT} (dB). Do đó, tác giả biểu diễn các biểu thức xác suất ρ_{D} và ρ_{E} theo giá trị khác nhau của P_{PT} (dB), với số ăng-ten tại S bằng 7, số gói mã hóa tối đa mà S có thể gửi D là 10 gói và các mức suy giảm phần cứng trên các kênh dữ liệu và kênh nghe lén đều bằng 0.1. Ta thấy ρ_{D} và ρ_{E} giảm khi P_{PT} tăng nhưng các giá trị này sẽ hội tụ về các giá trị tiệm cận khi P_{PT} đủ lớn. Ta cũng thấy rằng ρ_{D} thấp hơn rất nhiều so với ρ_{E} bởi S sử dụng TAS để gửi dữ liệu đến D.



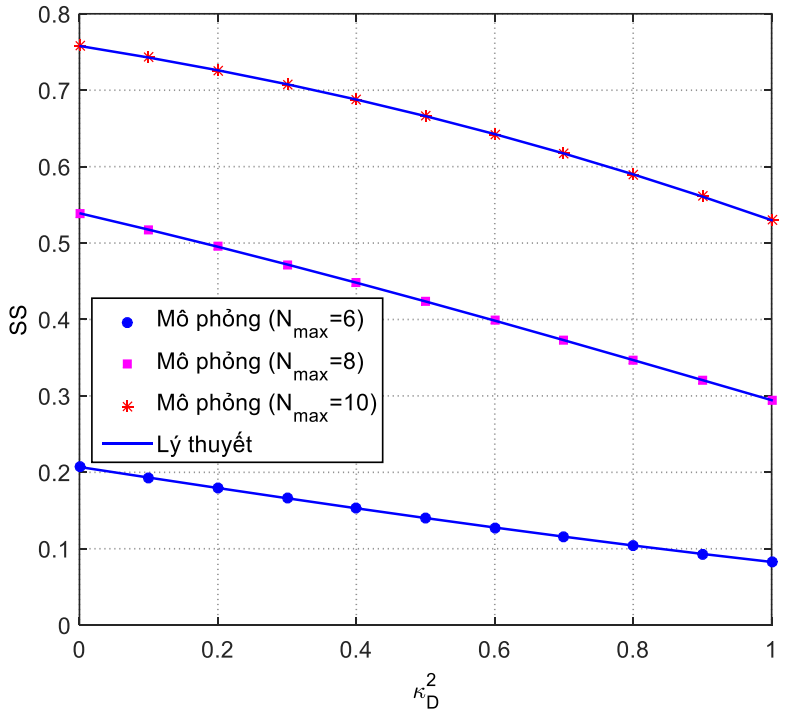
Hình 2.2: Xác suất của ρ_D và ρ_E vẽ theo P_{PT} (dB) khi $N_S = 7,\ N_{max} = 10$ và $\kappa_D^2 = \kappa_E^2 = 0.1$.



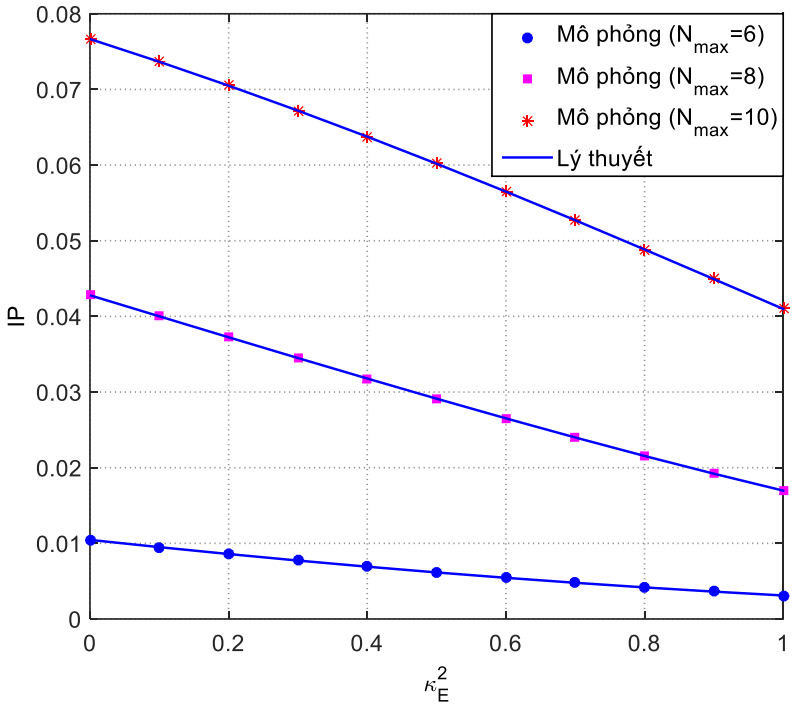
Hình 2.3: Xác suất SS vẽ theo P_{PT} (dB) khi $N_{max} = 10$ và $\kappa_D^2 = \kappa_E^2 = 0$.



Hình 2.4: Xác suất IP vẽ theo P_{PT} (dB) khi $N_{\max}=10$ và $\kappa_{\mathrm{D}}^2=\kappa_{\mathrm{E}}^2=0$.



Hình 2.5: Xác suất SS vẽ theo κ_{D}^2 khi $N_{\mathrm{S}}=5$ và $\kappa_{\mathrm{D}}^2=\kappa_{\mathrm{E}}^2$.



Hình 2.6: Xác suất IP vẽ theo κ_E^2 khi $N_S = 5$ và $\kappa_D^2 = \kappa_E^2$.

Hình 2.3 và 2.4 vẽ các xác suất SS và IP theo công suất phát của PT. Trong cả hai hình vẽ, các tham số hệ thống được cố định bởi $N_{max} = 10$ và $\kappa_D^2 = \kappa_E^2 = 0$. Trong Hình 2.3, giá trị của SS tăng khi P_{PT} tăng nhưng giá trị của SS sẽ tiến về hằng số khi P_{PT} đủ lớn. Điều này có thể được giải thích dựa vào kết quả đạt được trong Hình 2.2, đó là khi P_{PT} tăng thì xác suất ρ_D giảm, nhưng khi P_{PT} đủ lớn thì ρ_D sẽ không đổi nữa. Hình 2.3 cũng cho thấy rằng khi tăng số lượng ăng-ten phát N_S, xác suất dữ liệu nguồn có thể nhận được thành công và bảo mật tại D cũng tăng lên đáng kể.

Ngược lại với SS, Hình 2.4 cho thấy rằng xác suất mất bảo mật của hệ thống sẽ giảm khi nút nguồn được trang bị nhiều ăng-ten hơn. Tương tự như giá trị của SS, giá trị của IP cũng tăng khi P_{PT} tăng và đạt đến giá trị bão hòa khi P_{PT} đủ lớn.

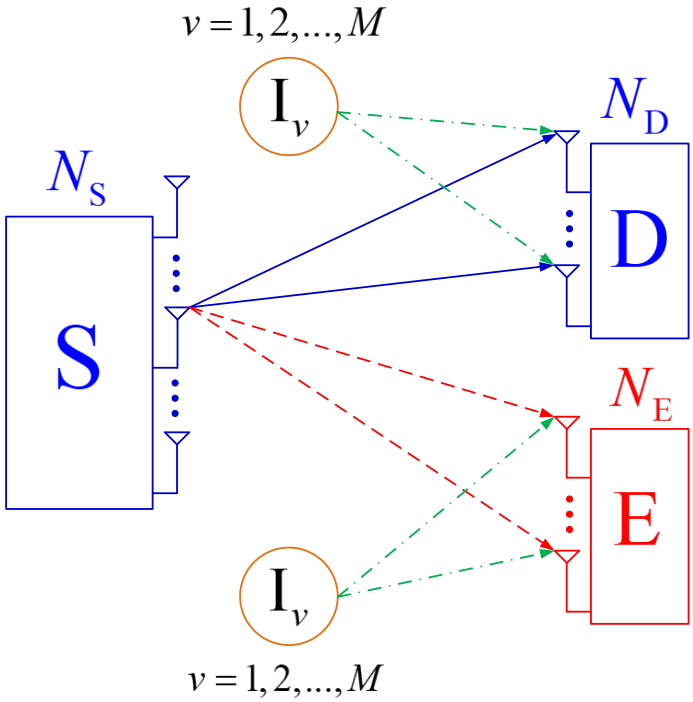
Hình 2.5 và 2.6 cho thấy sự ảnh hưởng của suy giảm phần cứng lên xác suất SS và IP của hệ thống. Như ta có thể thấy, giá trị của SS và IP giảm

nhanh khi giá trị κ_D^2 tăng từ 0 lên 1. Ta thấy trong Hình 2.5 rằng SS tăng khi giá trị N_{max} tăng. Tuy nhiên, khi N_{max} tăng thì giá trị IP cũng tăng do nút nghe lén có nhiều cơ hội nhận đủ N_{req}^{pkt} gói mã hóa.

Cuối cùng, từ các Hình 2.2 đến 2.6, các kết quả mô phỏng đã kiểm chứng sự chính xác của các kết quả phân tích lý thuyết.

2.3. MÔ HÌNH 2: MẠNG MIMO TAS/SC SỬ DỤNG MÃ FOUNTAIN

2.3.1. Mô hình hệ thống



Hình 2.7: Mô hình nghiên cứu đề xuất.

Hình 2.7 miêu tả mô hình hệ thống của giao thức đề xuất, trong đó một nút nguồn S (Source) muốn gửi dữ liệu đến một nút đích D (Destination), trong sự xuất hiện của một nút nghe lén E (Eavesdropper) cố gắng nghe lén dữ liệu của S. Giả sử, S được trang bị với N_S ăng-ten phát, D và E lần lượt có N_D và N_E ăng-ten thu, sử dụng kỹ thuật SC để kết hợp các tín hiệu thu. Trong thực tế, việc thực hiện kỹ thuật SC đơn giản hơn các kỹ thuật kết hợp khác như kỹ thuật EGC hay MRC bởi vì bộ thu SC chỉ cần chọn liên kết có

SNR lớn nhất để giải mã dữ liệu. Việc lựa chọn SC tại máy thu chủ yếu được áp dụng trong điều kiện máy thu bị ràng buộc hạn chế về tài nguyên, ví dụ như máy thu chỉ có một bộ khuếch đại hoặc chỉ cho phép thực hiện với một chíp đơn để giảm giá thành và công suất tiêu thụ. Ngoài ra, việc áp dụng SC tại máy nghe lén đa ăng-ten tương đương với trường hợp nhiều máy nghe lén đơn ăng-ten độc lập với nhau. Ta cũng quan sát tại Hình 2.7 rằng hai nút D và E đều chịu ảnh hưởng bởi nhiễu gây ra từ M nguồn giao thoa đơn ăng-ten được ký hiệu là $\mathrm{I}_1, \mathrm{I}_2, ..., \mathrm{I}_{M-1}$ và I_M.

Tương tự như phần trình bày trong mô hình đề xuất 1, hệ thống sử dụng mã Fountain, nút S sẽ chia dữ liệu gốc của mình thành L gói nhỏ có độ dài bằng nhau và thực hiện phép XOR với nhau để tạo ra các gói mã hóa. Tiếp theo, S gửi các gói mã hóa đến D trong những khe thời gian trực giao theo phương pháp TDMA và do tính chất mở của kênh truyền vô tuyến, nút E cũng có thể nhận được những gói mã hóa này. Dữ liệu gốc có thể được khôi phục nếu D (E) nhận thành công ít nhất $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa, khi D nhận đủ số gói mã hóa cần thiết cho giải mã dữ liệu gốc thì nút D ngay lập tức gửi thông điệp ACK để nút S dừng truyền. Trong trường hợp này, nếu E không thể nhận đủ $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa thì E sẽ không thể giải mã được dữ liệu nguồn, do đó quá trình truyền dữ liệu là thành công và bảo mật.

2.3.1.1. Mô hình kênh truyền

Giả sử, kênh truyền giữa các thiết bị là kênh pha đinh Rayleigh và để thuận tiện cho việc thể hiện, ta sẽ bỏ qua việc ký hiệu chỉ số thời gian trên các hệ số và độ lợi kênh truyền. Thật vậy, tác giả ký hiệu $h_{\mathrm{S}_m\mathrm{D}_n}$ và $h_{\mathrm{S}_m\mathrm{E}_t}$ là các hệ số kênh truyền giữa ăng-ten phát thứ m của S với ăng-ten thu thứ n của D và ăng-ten phát thứ m của S với ăng-ten thu thứ t của E trong một khe thời gian truyền dữ liệu bất kỳ, tương ứng, trong đó $m = 1, 2, ..., N_{\mathrm{S}}$, $n = 1, 2, ..., N_{\mathrm{D}}$,

$t = 1,2,...,N_{\mathrm{E}}$. Đối với các kênh giao thoa, tác giả sẽ ký hiệu $h_{\mathrm{I}_v\mathrm{D}_n}$ và $h_{\mathrm{I}_v\mathrm{E}_t}$ lần lượt là hệ số kênh truyền giữa nguồn giao thoa thứ v đến ăng-ten thu thứ n và t của D và E, với $v = 1,2,...,M$. Giả sử rằng tất cả các kênh là độc lập và đồng nhất, pha đinh khối và phẳng, được giữ không đổi trong một khe thời gian nhưng thay đổi độc lập tại các khe thời gian khác nhau. Do đó, các độ lợi kênh truyền $\gamma_{\mathrm{S}_m\mathrm{D}_n} = \left|h_{\mathrm{S}_m\mathrm{D}_n}\right|^2$, $\gamma_{\mathrm{S}_m\mathrm{E}_t} = \left|h_{\mathrm{S}_m\mathrm{E}_t}\right|^2$, $\gamma_{\mathrm{I}_v\mathrm{D}_n} = \left|h_{\mathrm{I}_v\mathrm{D}_n}\right|^2$ và $\gamma_{\mathrm{I}_v\mathrm{E}_t} = \left|h_{\mathrm{I}_v\mathrm{E}_t}\right|^2$ là các biến ngẫu nhiên phân bố hàm mũ (Exponential Random Variables: RVs), các hàm CDF của chúng được biểu diễn là [99]:

$$F_{\gamma_{\mathrm{S}_m\mathrm{D}_n}}(x) = 1 - \exp(-\lambda_{\mathrm{SD}} x),\ F_{\mathrm{S}_m\mathrm{E}_t}(x) = 1 - \exp(-\lambda_{\mathrm{SE}} x),$$
$$F_{\gamma_{\mathrm{I}_v\mathrm{D}_n}}(x) = 1 - \exp(-\lambda_{\mathrm{ID}} x),\ F_{\gamma_{\mathrm{I}_v\mathrm{E}_t}}(x) = 1 - \exp(-\lambda_{\mathrm{IE}} x), \quad (2.35)$$

với $\lambda_{\mathrm{SD}} = 1/\varepsilon\{\gamma_{\mathrm{S}_m\mathrm{D}_n}\}$, $\lambda_{\mathrm{SE}} = 1/\varepsilon\{\gamma_{\mathrm{S}_m\mathrm{E}_t}\}$, $\lambda_{\mathrm{ID}} = 1/\varepsilon\{\gamma_{\mathrm{I}_v\mathrm{D}_n}\}$ và $\lambda_{\mathrm{IE}} = 1/\varepsilon\{\gamma_{\mathrm{I}_v\mathrm{E}_t}\}$, trong đó $\varepsilon\{.\}$ là toán tử kỳ vọng.

2.3.1.2. Lựa chọn ăng-ten phát tại S và phân tập thu SC tại D

Giả sử, S sử dụng ăng-ten phát thứ m để gửi gói mã hóa đến D, SINR nhận được tại ăng-ten thu thứ n của D sẽ được đưa ra như sau:

$$\psi_{\mathrm{S}_m\mathrm{D}_n} = \frac{P_{\mathrm{S}}\gamma_{\mathrm{S}_m\mathrm{D}_n}}{\sum_{v=1}^{M} P_{\mathrm{I}}\gamma_{\mathrm{I}_v\mathrm{D}_n} + \sigma^2}, \quad (2.36)$$

với P_{S} là công suất phát của các ăng-ten tại S, P_{I} là công suất phát của các nguồn giao thoa (giả sử là như nhau tại các nguồn) và σ^2 là phương sai của tạp âm Gauss trắng cộng tại D (giả sử tất cả nhiễu cộng đều có phân bố Gauss có trung bình bằng 0 và phương sai bằng σ^2).

Từ (2.36), với $Q_{\mathrm{S}} = P_{\mathrm{S}}/\sigma^2$, $Q_{\mathrm{I}} = P_{\mathrm{I}}/\sigma^2$ và $X_n^{\mathrm{sum}} = \sum_{v=1}^{M} \gamma_{\mathrm{I}_v\mathrm{D}_n}$, ta có:

$$\psi_{\mathrm{S}_m\mathrm{D}_n} = \frac{Q_{\mathrm{S}}\gamma_{\mathrm{S}_m\mathrm{D}_n}}{Q_{\mathrm{I}}X_n^{\mathrm{sum}} + 1}, \quad (2.37)$$

Tương tự, SINR nhận được tại ăng-ten thu thứ t của E sẽ là:

$$\psi_{\mathrm{S}_m\mathrm{E}_t} = \frac{P_\mathrm{S}\gamma_{\mathrm{S}_m\mathrm{E}_t}}{\sum_{v=1}^{M} P_\mathrm{I}\gamma_{\mathrm{I}_v\mathrm{E}_t} + \sigma^2} = \frac{Q_\mathrm{S}\gamma_{\mathrm{S}_m\mathrm{E}_t}}{Q_\mathrm{I}Y_t^{\mathrm{sum}} + 1}, \tag{2.38}$$

với $Y_t^{\mathrm{sum}} = \sum_{v=1}^{M} \gamma_{\mathrm{I}_v\mathrm{E}_t}$.

Tiếp đến, xem xét hai mô hình TAS/SC như sau:

• Mô hình TAS/SC số 1 (MH1)

Trong mô hình này, giả sử rằng D và E không biết được CSI giữa các ăng-ten của chúng và các nguồn giao thoa. Đây là mô hình TAS/SC truyền thống [100], khi chỉ dựa vào CSI trên các kênh chính. Kỹ thuật TAS/SC này được miêu tả bằng công thức (2.39) bên dưới:

$$a^*, b^* : \gamma_{\mathrm{S}_{a^*}\mathrm{D}_{b^*}} = \max_{m=1,2,\ldots,N_\mathrm{S}} \max_{n=1,2,\ldots,N_\mathrm{D}} \left(\gamma_{\mathrm{S}_m\mathrm{D}_n}\right), \tag{2.39}$$

trong đó, a^* và b^* lần lượt là ăng-ten được chọn để phát và giải mã dữ liệu tại S và D, với $a^* \in \{1,2,\ldots,N_\mathrm{S}\}$ và $b^* \in \{1,2,\ldots,N_\mathrm{D}\}$. Do đó, SINR nhận được tại D trong một khe thời gian được tính bởi

$$\psi_\mathrm{D}^{\mathrm{TAS/SC/MH1}} = \frac{Q_\mathrm{S}\gamma_{\mathrm{S}_{a^*}\mathrm{D}_{b^*}}}{Q_\mathrm{I}X_{b^*}^{\mathrm{sum}} + 1}. \tag{2.40}$$

Tương tự như D, E cũng sử dụng SC để giải mã gói dữ liệu. Để công bằng với D, giả sử rằng E cũng không biết được CSI đến các nguồn giao thoa, mà chỉ biết CSI đến các ăng-ten phát của S. Thông thường, CSI của kênh truyền giữa S và D sẽ được ước lượng tại máy thu D thông qua tín hiệu hoa tiêu (pilot) hoặc symbol huấn luyện được gửi từ S. Tuy nhiên, do đặc tính quảng bá tự nhiên của kênh thông tin vô tuyến, E cũng có thể dễ dàng nhận được các tín hiệu huấn luyện này để ước lượng các hệ số kênh truyền giữa S và E. Trong thực tế, việc ước lượng hệ số kênh truyền thường xảy ra sai số do giới hạn về thời gian, tài nguyên và số mẫu huấn luyện. Tuy nhiên, để tập

trung vào việc phân tích các hiệu năng của hệ thống, trong phần này giả sử rằng các nút D và E có thể ước lượng chính xác các hệ số kênh truyền. Do đó, ăng-ten tốt nhất được sử dụng để giải mã dữ liệu tại E sẽ được đưa ra như sau:

$$t^* : \gamma_{\mathrm{S}_{a^*}\mathrm{E}_{t^*}} = \max_{t=1,2,...,N_{\mathrm{E}}} \left(\gamma_{\mathrm{S}_{a^*}\mathrm{E}_t} \right), \tag{2.41}$$

trong đó, t^* là ăng-ten được chọn để giải mã tại E.

Cũng vậy, SINR nhận được tại E trong một khe thời gian được viết là

$$\psi_{\mathrm{E}}^{\mathrm{SC/MH1}} = \frac{Q_{\mathrm{S}} \gamma_{\mathrm{S}_{a^*}\mathrm{E}_{t^*}}}{Q_{\mathrm{I}} Y_{t^*}^{\mathrm{sum}} + 1}. \tag{2.42}$$

Ta có nhận xét từ công thức (2.40): MH1 không đạt được SINR tối đa cho kênh truyền giữa S và D do thiếu thông tin về CSI từ các kênh giao thoa.

• Mô hình TAS/SC số 2 (MH2)

Trong mô hình này, giả sử rằng D và E có thể ước lượng chính xác CSI giữa các ăng-ten của chúng và các nguồn giao thoa. Do đó, tác giả đã đề xuất phương pháp TAS/SC mới để đạt được SINR tối đa cho D, cụ thể:

$$a,b : \psi_{\mathrm{D}}^{\mathrm{TAS/SC/MH2}} = \max_{m=1,2,...,N_{\mathrm{S}}} \max_{n=1,2,...,N_{\mathrm{D}}} \left(\psi_{\mathrm{S}_m\mathrm{D}_n} \right), \tag{2.43}$$

trong đó, a và b lần lượt là ăng-ten được chọn để phát và giải mã dữ liệu tại S và D, với $a \in \{1,2,...,N_{\mathrm{S}}\}$ và $b \in \{1,2,...,N_{\mathrm{D}}\}$.

Tương tự, E cũng sẽ chọn ăng-ten thu tốt nhất để giải mã gói dữ liệu theo tiêu chí sau:

$$t : \psi_{\mathrm{E}}^{\mathrm{SC/MH2}} = \max_{t=1,2,...,N_{\mathrm{E}}} \left(\psi_{\mathrm{S}_a\mathrm{E}_t} \right), \tag{2.44}$$

Giả sử rằng một gói mã hóa có thể được giải mã thành công nếu SINR nhận được tại thiết bị thu lớn hơn một ngưỡng γ_{th}, cho trước. Ngược lại, gói mã hóa đó sẽ không được nhận thành công. Vì vậy, xác suất mà D và E không thể nhận đúng một gói dữ liệu trong MH1 và MH2 sẽ lần lượt được đưa ra trong (2.45) và (2.46) như sau:

$$\rho_{1,\mathrm{D}} = \Pr\left(\psi_{\mathrm{D}}^{\mathrm{TAS/SC/MH1}} \le \gamma_{\mathrm{th}}\right),\ \rho_{1,\mathrm{E}} = \Pr\left(\psi_{\mathrm{E}}^{\mathrm{SC/MH1}} \le \gamma_{\mathrm{th}}\right), \tag{2.45}$$

$$\rho_{2,\mathrm{D}} = \Pr\left(\psi_{\mathrm{D}}^{\mathrm{TAS/SC/MH2}} \le \gamma_{\mathrm{th}}\right),\ \rho_{2,\mathrm{E}} = \Pr\left(\psi_{\mathrm{E}}^{\mathrm{SC/MH2}} \le \gamma_{\mathrm{th}}\right), \tag{2.46}$$

Do đó, xác suất mà B và E có thể nhận được một gói mã hóa thành công lần lượt được xác định như sau: $1-\rho_{1,\mathrm{D}}$, $1-\rho_{1,\mathrm{E}}$, $1-\rho_{2,\mathrm{D}}$ và $1-\rho_{2,\mathrm{E}}$.

Trong hệ thống được xem xét, như đã thảo luận trong Mục 2.3.1, quá trình truyền các gói mã hóa giữa S và D kết thúc, nếu như E không nhận đủ số gói để phục hồi thông tin gốc thì sự truyền dữ liệu là thành công và bảo mật (SS). Tác giả ký hiệu N_{TS} là tổng số gói mã hóa mà S phải gửi đến D để D có thể nhận đủ $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa cho việc khôi phục thông tin gốc. Ta cũng ký hiệu $N_{\mathrm{D}}^{\mathrm{pkt}}$ và $N_{\mathrm{E}}^{\mathrm{pkt}}$ là số gói mã hóa mà D và E đã nhận thành công trong N_{TS} khe thời gian truyền, tương ứng. Như đã đề cập ở trên, xác suất giải mã và bảo mật thông tin thành công (SS) có thể được định nghĩa bởi

$$\mathrm{SS} = \Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}},\ N_{\mathrm{E}}^{\mathrm{pkt}} < N_{\mathrm{req}}^{\mathrm{pkt}}\right). \tag{2.47}$$

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

2.3.2. Phân tích hiệu năng

2.3.2.1. Xác suất của $\rho_{1,\mathrm{D}}$, $\rho_{1,\mathrm{E}}$, $\rho_{2,\mathrm{D}}$ và $\rho_{2,\mathrm{E}}$

Các biểu thức xác suất này có thể được biểu diễn dưới dạng chính xác là

$$\rho_{1,\mathrm{D}} = 1 + \sum_{k=1}^{N_{\mathrm{S}}N_{\mathrm{D}}} (-1)^k \frac{C_{N_{\mathrm{S}}N_{\mathrm{D}}}^{k} \lambda_{\mathrm{ID}}^{M}}{\left(k\lambda_{\mathrm{SD}}\theta_2 + \lambda_{\mathrm{ID}}\right)^{M}} \exp\left(-k\lambda_{\mathrm{SD}}\theta_1\right). \tag{2.48}$$

$$\rho_{1,\mathrm{E}} = 1 + \sum_{t=1}^{N_{\mathrm{E}}} (-1)^t \frac{C_{N_{\mathrm{E}}}^{t} \lambda_{\mathrm{IE}}^{M}}{\left(t\lambda_{\mathrm{SE}}\theta_2 + \lambda_{\mathrm{IE}}\right)^{M}} \exp\left(-t\lambda_{\mathrm{SE}}\theta_1\right). \tag{2.49}$$

$$\rho_{2,\mathrm{D}} = \left[1 - \frac{\lambda_{\mathrm{ID}}^{M}}{\left(\lambda_{\mathrm{SD}}\theta_2 + \lambda_{\mathrm{ID}}\right)^{M}} \exp\left(-\lambda_{\mathrm{SD}}\theta_1\right)\right]^{N_{\mathrm{S}}N_{\mathrm{D}}}. \tag{2.50}$$

$$\rho_{2,\mathrm{E}} = \left[1 - \frac{\lambda_{\mathrm{IE}}^{M}}{\left(\lambda_{\mathrm{SE}}\theta_2 + \lambda_{\mathrm{IE}}\right)^{M}} \exp\left(-\lambda_{\mathrm{SE}}\theta_1\right)\right]^{N_{\mathrm{E}}}. \tag{2.51}$$

Chứng minh: Xem chứng minh, các ký hiệu trong Mục A3, 4, Phụ lục A.

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

Tổng xác suất của SS trong (2.47) có thể được viết lại là

$$\mathrm{SS} = \sum_{N_{\mathrm{TS}}=N_{\mathrm{req}}^{\mathrm{pkt}}}^{+\infty} \Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \mid N_{\mathrm{TS}}\right) \times \sum_{q=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} \Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}} = q \mid N_{\mathrm{TS}}\right), \tag{2.52}$$

trong đó, $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \mid N_{\mathrm{TS}}\right) \times \Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}} = q \mid N_{\mathrm{TS}}\right)$ là xác suất mà D (E) có thể nhận chính xác $N_{\mathrm{D}}^{\mathrm{pkt}}(q)$ gói mã hóa dưới điều kiện số gói mã hóa được phát bởi S là N_{TS}. Mặt khác, $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \mid N_{\mathrm{TS}}\right)$ và $\Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}} = q \mid N_{\mathrm{TS}}\right)$ được tính tương tự như các công thức (2.28) và (2.29). Do đó, tác giả đưa ra công thức tính SS trong mô hình MH1 bằng biểu thức sau:

$$\mathrm{SS}_{\mathrm{MH1}} = \sum_{N_{\mathrm{TS}}=N_{\mathrm{req}}^{\mathrm{pkt}}}^{+\infty} \left[C_{N_{\mathrm{TS}}-1}^{N_{\mathrm{TS}}-N_{\mathrm{req}}^{\mathrm{pkt}}} \left(1-\rho_{1,\mathrm{D}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}} \left(\rho_{1,\mathrm{D}}\right)^{N_{\mathrm{TS}}-N_{\mathrm{req}}^{\mathrm{pkt}}}\right] \times \left[\sum_{q=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} C_{N_{\mathrm{TS}}}^{q} \left(1-\rho_{1,\mathrm{E}}\right)^{q} \left(\rho_{1,\mathrm{E}}\right)^{N_{\mathrm{TS}}-q}\right], \tag{2.53}$$

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

Để thể hiện kết quả lý thuyết, tác giả cắt chuỗi vô cùng trong (2.53) bằng một giá trị hữu hạn N_{T}, ta có:

$$\mathrm{SS}_{\mathrm{MH1}} \approx \sum_{N_{\mathrm{TS}}=N_{\mathrm{req}}^{\mathrm{pkt}}}^{N_{\mathrm{T}}} \left[C_{N_{\mathrm{TS}}-1}^{N_{\mathrm{TS}}-N_{\mathrm{req}}^{\mathrm{pkt}}} \left(1-\rho_{1,\mathrm{D}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}} \left(\rho_{1,\mathrm{D}}\right)^{N_{\mathrm{TS}}-N_{\mathrm{req}}^{\mathrm{pkt}}}\right] \times \left[\sum_{q=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} C_{N_{\mathrm{TS}}}^{q} \left(1-\rho_{1,\mathrm{E}}\right)^{q} \left(\rho_{1,\mathrm{E}}\right)^{N_{\mathrm{TS}}-q}\right]. \tag{2.54}$$

Tiếp theo, SS của mô hình MH2 sẽ được tính chính xác như sau:

$$\mathrm{SS}_{\mathrm{MH2}} = \sum_{N_{\mathrm{TS}}=N_{\mathrm{req}}^{\mathrm{pkt}}}^{+\infty} \left[C_{N_{\mathrm{TS}}-1}^{N_{\mathrm{TS}}-N_{\mathrm{req}}^{\mathrm{pkt}}} \left(1-\rho_{2,\mathrm{D}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}} \left(\rho_{2,\mathrm{D}}\right)^{N_{\mathrm{TS}}-N_{\mathrm{req}}^{\mathrm{pkt}}} \right] \times \left[\sum_{q=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} C_{N_{\mathrm{TS}}}^{q} \left(1-\rho_{2,\mathrm{E}}\right)^{q} \left(\rho_{2,\mathrm{E}}\right)^{N_{\mathrm{TS}}-q} \right]. \quad (2.55)$$

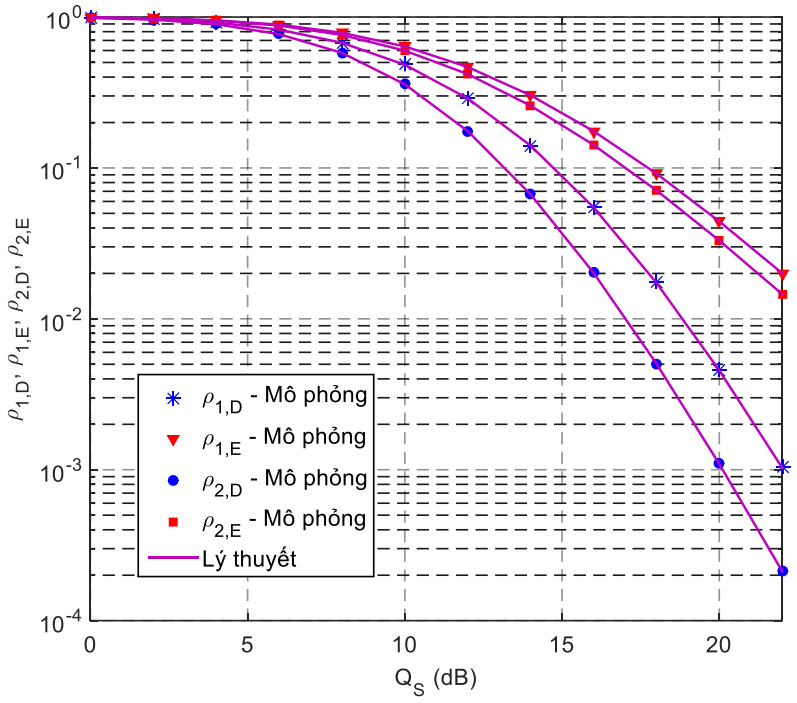
Tương tự, ta có thể biểu diễn $\mathrm{SS}_{\mathrm{MH2}}$ bằng một biểu thức dạng tiệm cận:

$$\mathrm{SS}_{\mathrm{MH2}} \approx \sum_{N_{\mathrm{TS}}=N_{\mathrm{req}}^{\mathrm{pkt}}}^{N_{\mathrm{T}}} \left[C_{N_{\mathrm{TS}}-1}^{N_{\mathrm{TS}}-N_{\mathrm{req}}^{\mathrm{pkt}}} \left(1-\rho_{2,\mathrm{D}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}} \left(\rho_{2,\mathrm{D}}\right)^{N_{\mathrm{TS}}-N_{\mathrm{req}}^{\mathrm{pkt}}} \right] \times \left[\sum_{q=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} C_{N_{\mathrm{TS}}}^{q} \left(1-\rho_{2,\mathrm{E}}\right)^{q} \left(\rho_{2,\mathrm{E}}\right)^{N_{\mathrm{TS}}-q} \right]. \quad (2.56)$$

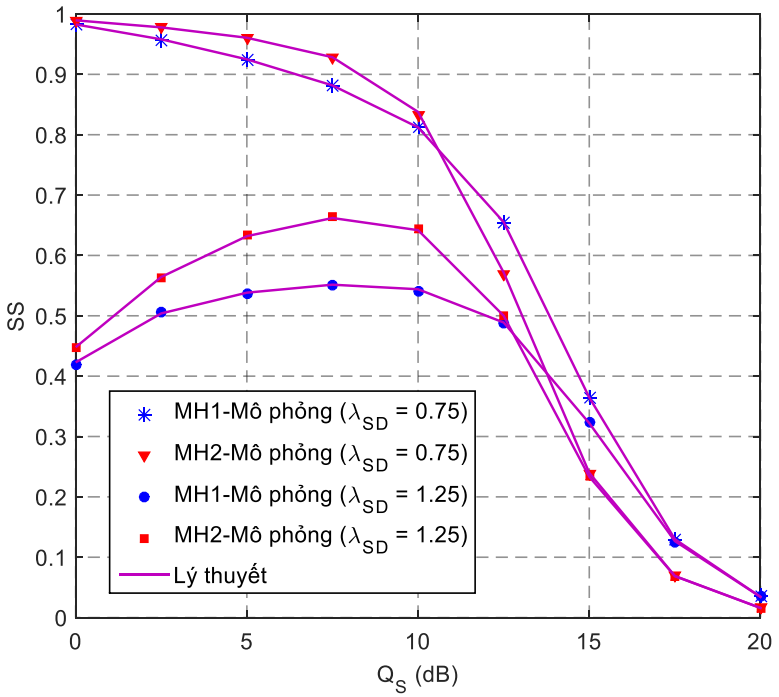
2.3.3. Các kết quả mô phỏng

Trong phần này, Luận án thực hiện các mô phỏng Monte Carlo để kiểm chứng các công thức đã được trình bày ở Phần 2.3.2. Trong tất cả các mô phỏng, tác giả sử dụng giá trị của N_{T} bằng 1000.

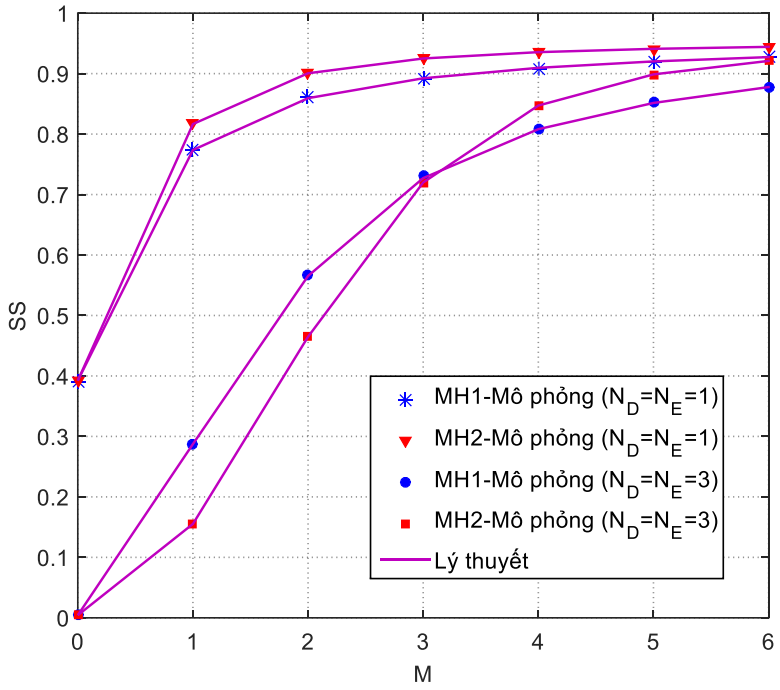
Trong Hình 2.8, Luận án sử dụng mô phỏng Monte Carlo để kiểm chứng các biểu thức của $\rho_{1,\mathrm{D}}$, $\rho_{1,\mathrm{E}}$, $\rho_{2,\mathrm{D}}$ và $\rho_{2,\mathrm{E}}$. Trong mô phỏng này, các tham số hệ thống được thiết lập như sau: $N_{\mathrm{S}} = N_{\mathrm{D}} = N_{\mathrm{E}} = 2$, $M = 2$, $\lambda_{\mathrm{SD}} = \lambda_{\mathrm{SE}} = 1$, $\lambda_{\mathrm{ID}} = \lambda_{\mathrm{IE}} = 1$ và $\gamma_{\mathrm{th}} = 1$. Nhìn vào Hình vẽ, ta thấy giá trị của các xác suất $\rho_{1,\mathrm{D}}$, $\rho_{1,\mathrm{E}}$, $\rho_{2,\mathrm{D}}$ và $\rho_{2,\mathrm{E}}$ giảm nhanh khi tăng giá trị của Q_{S}. Các giá trị của $\rho_{1,\mathrm{D}}$ và $\rho_{2,\mathrm{D}}$ nhỏ hơn giá trị $\rho_{1,\mathrm{E}}$ và $\rho_{2,\mathrm{E}}$ do sự kết hợp đồng thời hai kỹ thuật TAS tại S và SC tại D. Hơn nữa, bởi vì MH2 quan tâm đến khả năng ước lượng kênh giao thoa tại D và E nên ta có thể thấy rằng giá trị của $\rho_{2,\mathrm{D}}$ luôn nhỏ hơn giá trị của $\rho_{1,\mathrm{D}}$ và $\rho_{2,\mathrm{E}}$ luôn nhỏ hơn $\rho_{1,\mathrm{E}}$ trong tất cả trường hợp. Cũng được quan sát trên hình vẽ này, giá trị $\rho_{2,\mathrm{D}}$ là nhỏ nhất bởi kỹ thuật TAS/SC trong mô hình 2 (MH2) đạt được giá trị SINR tức thời lớn nhất.



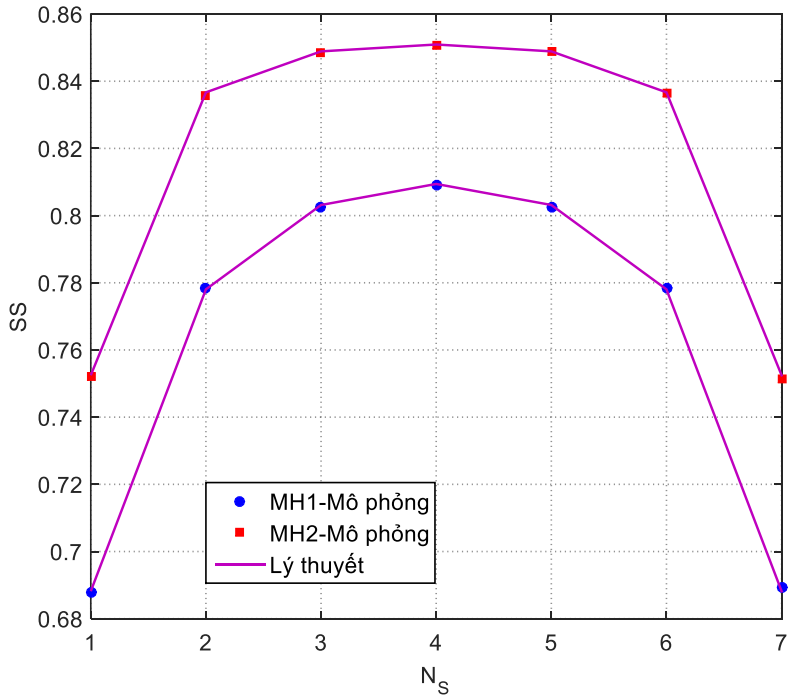
Hình 2.8: $\rho_{1,D}$, $\rho_{1,E}$, $\rho_{2,D}$ và $\rho_{2,E}$ vẽ theo Q_S (dB) khi $N_S = N_D = N_E = 2$, $M = 2$, $\lambda_{SD} = \lambda_{SE} = \lambda_{ID} = \lambda_{IE} = 1$, $Q_I = 10$ (dB) và $\gamma_{th} = 1$.



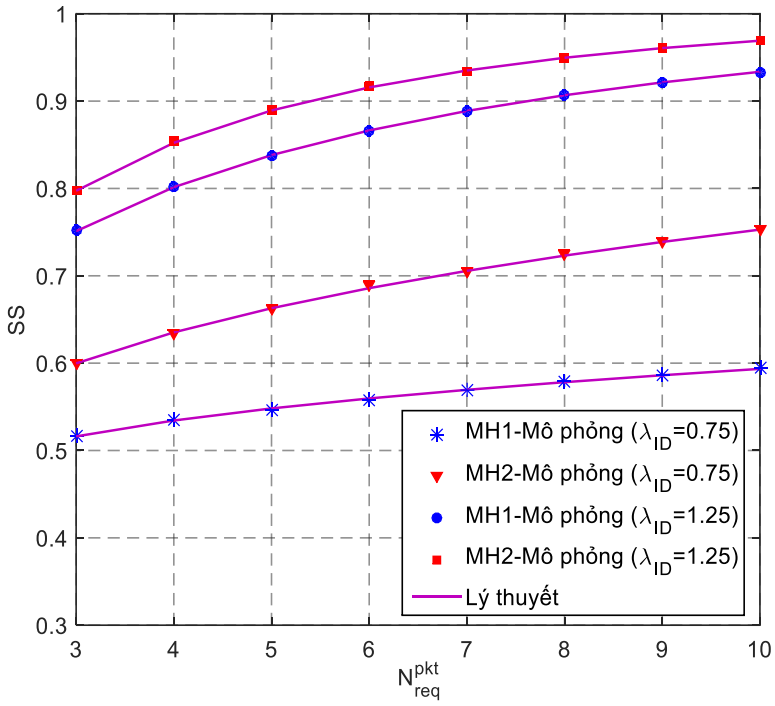
Hình 2.9: SS vẽ theo Q_S (dB) khi $Q_I = 10$ (dB), $N_S = 2$, $N_D = N_E = 3$, $M = 2$, $\lambda_{SE} = 1$, $\lambda_{ID} = \lambda_{IE} = 2$, $\gamma_{th} = 1.5$ và $N_{req}^{pkt} = 5$.



Hình 2.10: SS vẽ theo M khi $Q_S = Q_I = 10$ (dB), $N_S = 3$, $\lambda_{SD} = \lambda_{SE} = 1$, $\lambda_{ID} = \lambda_{IE} = 3$, $\gamma_{th} = 1$ và $N_{req}^{pkt} = 5$.



Hình 2.11: SS vẽ theo N_S khi $Q_S = 5$ (dB), $Q_I = 10$ (dB), $N_E = 3$, $M = 1$, $\lambda_{SD} = \lambda_{SE} = 1$, $\lambda_{ID} = \lambda_{IE} = 5$, $\gamma_{th} = 1.75$ và $N_{req}^{pkt} = 4$.



Hình 2.12: SS vẽ theo $N_{\text{req}}^{\text{pkt}}$ khi $Q_{\text{S}} = Q_{\text{I}} = 10\,(\text{dB}),\ N_{\text{S}} = 2,\ N_{\text{D}} = N_{\text{E}} = 2,$ $M = 2,\ \lambda_{\text{SD}} = \lambda_{\text{SE}} = 1,\ \lambda_{\text{IE}} = 1$ và $\gamma_{\text{th}} = 1.$

Hình 2.9 vẽ giá trị SS của MH1 và MH2 theo Q_{S} (dB). Ta thấy rằng khi $\lambda_{\text{SD}} = 0.75$ thì giá trị SS trong MH1 và MH2 lớn ở các giá trị Q_{S} thấp. Tuy nhiên khi $\lambda_{\text{SD}} = 1.25,$ giá trị SS của MH1 và MH2 lại thấp ở các giá trị Q_{S} thấp. Ta cũng thấy rằng khi công suất phát của S lớn (Q_{S} lớn) sẽ làm tăng khả năng đạt được dữ liệu gốc của E, điều này kéo theo sự giảm của giá trị SS. Ta cũng quan sát được rằng MH2 đạt được giá trị SS lớn hơn MH1 khi giá trị Q_{S} nhỏ và trung bình. Mặt khác, khi Q_{S} đủ lớn thì MH1 lại đạt được giá trị SS cao hơn. Điều này có thể được giải thích như sau: MH2 đạt được hiệu quả truyền dữ liệu cao hơn MH1 cho nên MH2 sẽ đạt được hiệu năng tốt hơn MH1 ở các giá trị Q_{S} thấp. Tuy nhiên, do nút E trong MH2 đạt được CSI đến các nguồn giao thoa nên khả năng nghe lén của E trong MH2 cao hơn trong MH1, và đây là lý do giá trị SS của MH2 lại thấp hơn MH1 khi Q_{S} lớn.

Trong Hình 2.10, SS được biểu diễn theo số nguồn giao thoa M. Nhìn vào hình vẽ, ta thấy giá trị SS của cả hai mô hình đề xuất đều tăng khi tăng số nguồn giao thoa M. Hơn nữa, trong khi D và E là các thiết bị đơn ăng-ten $\left(N_{\mathrm{D}} = N_{\mathrm{E}} = 1\right)$ thì SS của MH2 luôn lớn hơn MH1. Điểm đáng chú ý thứ hai trong Hình 2.10, đó là khi tăng số ăng-ten thu tại D và E $\left(N_{\mathrm{D}} = N_{\mathrm{E}} = 3\right)$ thì SS trong MH1 tại giá trị $\left(M > 3\right)$ lại lớn hơn MH2 và ngược lại. Mặt khác, SS sẽ giảm mạnh khi tăng số ăng-ten tại nút nghe lén E, do E có thể khai thác được độ lợi phân tập thu nhờ sử dụng kỹ thuật SC.

Trong Hình 2.11, ta giả sử rằng tổng số lượng ăng-ten được trang bị tại S và D là không đổi và bằng 8 $\left(N_{\mathrm{S}} + N_{\mathrm{D}} = 8\right)$, vẽ giá trị của SS khi tăng N_{S} từ 01 đến 07. Quan sát từ hình vẽ, ta thấy rằng giá trị của SS biến thiên theo N_{S} và SS đạt giá trị lớn nhất khi $\left(N_{\mathrm{S}} = N_{\mathrm{D}} = 4\right)$. Như vậy, để đạt được hiệu năng truyền thông và bảo mật tốt nhất, ta cần thiết kế (phân phối) phù hợp số ăng-ten tại nút nguồn (S) và nút đích (D).

Trong Hình 2.12, khảo sát sự ảnh hưởng của số gói mã hóa $N_{\mathrm{req}}^{\mathrm{pkt}}$ lên giá trị của SS. Ta nhận thấy rằng, SS sẽ tăng khi tăng số gói mã hóa để khôi phục thông tin gốc và giá trị của SS trong MH2 lớn hơn MH1. Thật vậy, khi số lượng gói $N_{\mathrm{req}}^{\mathrm{pkt}}$ càng lớn thì xác suất mà D có thể nhận đủ $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa trước E càng lớn. Ta cũng thấy rằng khi tăng giá trị tham số đặc trưng kênh truyền giữa các nguồn giao thoa đến D (tăng λ_{ID}), giá trị SS cũng tăng. Bởi vì λ_{ID} càng lớn thì chất lượng kênh giữa D và các nguồn giao thoa giảm, do đó nâng cao khả năng giải mã thành công những gói mã hóa nhận được tại D.

Quan sát từ Hình 2.8 đến Hình 2.12, ta có thể thấy rằng các kết quả mô phỏng phù hợp với các kết quả phân tích lý thuyết, điều này đã chứng minh tính đúng đắn của các kết quả phân tích trong Mục 2.3.2.

2.4. KẾT LUẬN CHƯƠNG

Chương 2 của Luận án đề xuất hai mô hình để phân tích hiệu năng bảo mật trong mạng MISO TAS và MIMO TAS/SC, bao gồm: i) phân tích hiệu năng truyền bảo mật trong CRN dạng nền sử dụng FC dưới tác động chung của giao thoa đồng kênh từ mạng sơ cấp và suy giảm phần cứng; ii) phân tích khả năng giải mã và bảo mật dữ liệu thành công trong mạng vô tuyến thông thường sử dụng FC dưới tác động của giao thoa đồng kênh. Các mô phỏng Monte Carlo được thực hiện để kiểm chứng biểu thức toán học được đưa ra.

Đề xuất trong mô hình 1, hiệu năng truyền bảo mật của mạng thứ cấp sử dụng FC đã được đánh giá và phân tích. Dưới sự giới hạn của giao thoa định mức, tác động chung của giao thoa đồng kênh và suy giảm phần cứng, sử dụng kỹ thuật TAS để nâng cao độ tin cậy truyền dẫn và bảo mật dữ liệu. Các kết quả thể hiện mô hình đề xuất đạt được hiệu năng tốt hơn khi nút nguồn thứ cấp được trang bị nhiều ăng-ten phát và phần cứng của thiết bị thứ cấp tốt hơn. Hơn nữa, để nâng cao hiệu năng bảo mật của hệ thống thì cần phải giảm số lần truyền các gói mã hóa và tăng số ăng-ten tại nút nguồn thứ cấp một cách thích hợp để nâng cao chất lượng của kênh hợp pháp.

Các kết quả trong mô hình đề xuất 2 đã phân tích khả năng giải mã và bảo mật thông tin thành công của hệ thống sử dụng FC, dưới tác động từ nhiều nguồn giao thoa đồng kênh. Các kết quả cho thấy rằng hiệu năng của mô hình đề xuất chịu ảnh hưởng lớn bởi các tham số đặc trưng kênh truyền và số nguồn giao thoa đồng kênh. Để nâng cao hiệu năng bảo mật một cách chủ động, cần tăng chất lượng kênh dữ liệu bằng cách giảm giá trị tham số đặc trưng của kênh chính, tăng hoặc phân phối số ăng-ten tại các nút phát và thu phù hợp, tăng số gói mã hóa được yêu cầu để khôi phục dữ liệu gốc. Tùy thuộc vào các điều kiện và tham số hệ thống cụ thể, có thể chọn lựa mô hình thích hợp (MH1 hoặc MH2) để đạt được hiệu năng hệ thống tốt hơn.

Chương 3
HIỆU NĂNG BẢO MẬT TRONG MẠNG MIMO-NOMA TAS/SC/MRC SỬ DỤNG MÃ FOUNTAIN

3.1. GIỚI THIỆU

Trong Chương 2, Luận án đã đề xuất, nghiên cứu hai mô hình hệ thống sử dụng FC trên kênh truyền pha đinh Rayleigh, bao gồm: i) hiệu năng bảo mật thông tin cho hệ thống MISO TAS trong môi trường vô tuyến nhận thức dạng nền dưới tác động chung của giao thoa đồng kênh từ máy phát sơ cấp và suy giảm phần cứng; ii) hiệu năng bảo mật của hệ thống vô tuyến MIMO TAS/SC thông thường dưới tác động của giao thoa đồng kênh. Các kết quả cho thấy rằng, để đạt được bảo mật thông tin thì nút đích phải cố gắng nhận được đủ số gói mã hóa cần thiết nhằm khôi phục dữ liệu gốc trước nút nghe lén. Hơn nữa, các mô hình đề xuất đạt được hiệu năng tốt hơn khi nút nguồn trang bị nhiều ăng-ten phát với kỹ thuật TAS và phần cứng của các thiết bị người dùng hợp pháp tốt hơn hoặc kỹ thuật phân tập thu SC tại nút đích được sử dụng để nâng cao độ tin cậy truyền dẫn và bảo mật dữ liệu. Mặt khác, một trong những vấn đề cơ bản trong thông tin vô tuyến là tăng thông lượng một cách hiệu quả trên các kênh truyền biến đổi theo thời gian. Nhìn chung, việc truyền tín hiệu trên các kênh vô tuyến phải đối mặt với rất nhiều thách thức đó là sự suy giảm nghiêm trọng về chất lượng kênh truyền, bao gồm nhiễu, pha đinh, suy hao đường truyền, hiện tượng bóng mờ,… thay đổi trong suốt quá trình truyền và để đạt được thông lượng cao, các hệ thống vô tuyến cần phải thích ứng với tất cả các điều kiện kênh truyền khác nhau. Trong bảo mật lớp vật lý, thông tin có thể được bảo mật khi chất lượng kênh dữ liệu tốt hơn kênh nghe lén, do vậy các kỹ thuật truyền phân tập thường được sử dụng để nâng cao chất lượng của kênh dữ liệu.

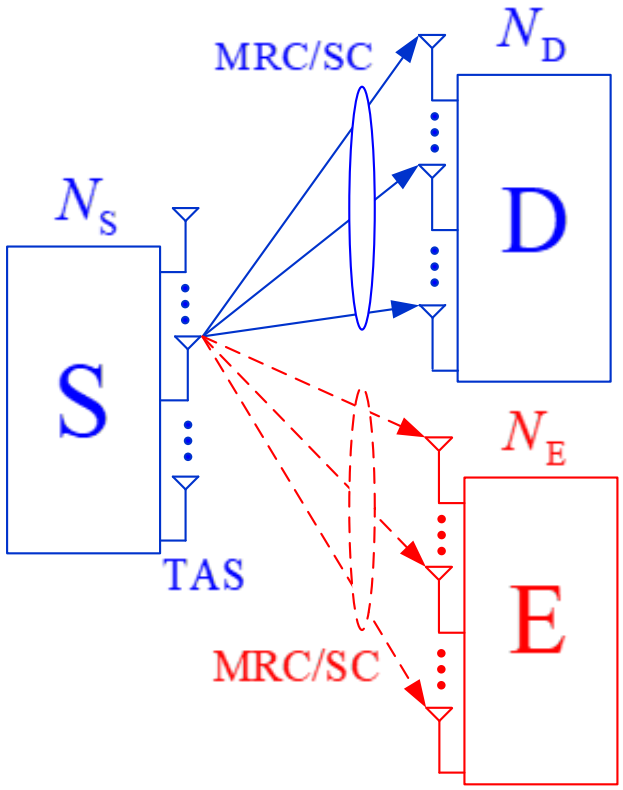
Trong Chương này, Luận án đề xuất hệ thống truyền bảo mật MIMO-NOMA sử dụng FC. Trong giao thức đề xuất, một nút nguồn (S) đa ăng-ten sử dụng TAS để phát các gói mã hóa đến một nút đích (D) đa ăng-ten trong sự xuất hiện của nút nghe lén (E) đa ăng-ten. Các máy thu bao gồm nút D và nút E có thể sử dụng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

Luận án so sánh hiệu năng của các giao thức đề xuất trong hai trường hợp với nút S sử dụng NOMA (gọi là NOMA) và không sử dụng NOMA (gọi là Wo-NOMA), dựa vào số khe thời gian trung bình (TS) và xác suất thu chặn (IP). Các kết quả đã thể hiện rằng giao thức truyền bảo mật dựa vào FC sử dụng NOMA có thể giảm cả TS và IP, khi so sánh với giao thức tương ứng mà không sử dụng NOMA. Luận án đưa ra các biểu thức chính xác của TS, IP cho các giao thức NOMA và Wo-NOMA trên kênh truyền pha đinh Rayleigh và thực hiện mô phỏng máy tính để kiểm chứng kết quả phân tích lý thuyết.

Phần còn lại của Chương này được tổ chức như sau: Mô hình hệ thống của NOMA và Wo-NOMA được miêu tả trong Phần 3.2. Trong Phần 3.3, các hiệu năng TS và IP của NOMA và Wo-NOMA được phân tích. Các kết quả mô phỏng và lý thuyết được thể hiện trong Phần 3.4. Cuối cùng, kết luận Chương trong Phần 3.5.

Đóng góp của Chương 3 được trình bày trong công trình A3.

3.2. MÔ HÌNH HỆ THỐNG



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

Hình 3.1 trình bày mô hình hệ thống của giao thức đề xuất, với một nút nguồn S (Source) được trang bị N_S ăng-ten sử dụng FC để phát dữ liệu đến một nút đích D (Destination) có N_D ăng-ten, trong sự xuất hiện của nút nghe lén thụ động E (Eavesdropper) với N_E ăng-ten. Tương tự như phần trình bày trong Chương 2, đối với hệ thống sử dụng mã Fountain, dữ liệu gốc của nút nguồn được chia thành L gói, sau đó được mã hóa một cách thích hợp bởi bộ mã hóa FC để tạo ra các gói mã hóa. Tại mỗi khe thời gian, nút nguồn lựa chọn ăng-ten tốt nhất của mình để phát hai (hoặc một) gói mã hóa đến nút đích, những gói mã hóa này cũng được nhận bởi nút nghe lén. Tiếp theo, các nút D và E cố gắng giải mã các gói mã hóa. Để giải mã được dữ liệu gốc, D và E phải nhận chính xác ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa, với $N_{\text{req}}^{\text{pkt}} = (1+\varepsilon)L$. Sau khi nhận đủ số gói mã hóa hiệu quả cho việc khôi phục dữ liệu gốc, D gửi một

bản tin ACK để thông báo đến S và sau đó nút nguồn dừng truyền dữ liệu. Tương tự như các nội dung đã được trình bày trước đó, nếu E nhận thành công ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa, E cũng có thể phục hồi dữ liệu gốc và do đó dữ liệu nguồn bị thu chặn.

3.2.1. Mô hình kênh truyền

Tác giả ký hiệu $h_{\text{S}_m\text{D}_n}$ và $h_{\text{S}_m\text{E}_t}$ là các hệ số kênh truyền giữa ăng-ten thứ m của S và ăng-ten thứ n của D và giữa ăng-ten thứ m của S và ăng-ten thứ t của E, trong đó $m=1,2,...,N_{\text{S}}$, $n=1,2,...,N_{\text{D}}$, $t=1,2,...,N_{\text{E}}$. Giả sử rằng tất cả các kênh truyền là pha đinh Rayleigh khối phẳng, độc lập và đồng nhất (i.i.d.) và do vậy, độ lợi kênh truyền $\gamma_{\text{S}_m\text{D}_n}=\left|h_{\text{S}_m\text{D}_n}\right|^2$ và $\gamma_{\text{S}_m\text{E}_t}=\left|h_{\text{S}_m\text{E}_t}\right|^2$ là các biến ngẫu nhiên phân bố hàm mũ. Vậy nên, hàm PDF của $\gamma_{\text{S}_m\text{D}_n}$ và $\gamma_{\text{S}_m\text{E}_t}$ có thể được cho tương ứng là

$$f_{\gamma_{\text{S}_m\text{D}_n}}(x)=\lambda_{\text{SD}}\exp(-\lambda_{\text{SD}}x),$$

$$f_{\text{S}_m\text{E}_t}(x)=\lambda_{\text{SE}}\exp(-\lambda_{\text{SE}}x). \quad (3.1)$$

Tương tự, tác giả đặt N_{TS} là số khe thời gian được sử dụng bởi nút nguồn để phát các gói mã hóa đến nút đích. Ta đặt $N_{\text{D}}^{\text{pkt}}$ và $N_{\text{E}}^{\text{pkt}}$ là số gói mã hóa mà nút đích và nút nghe lén có thể nhận thành công trong N_{TS} khe thời gian truyền, tương ứng.

Hàm $\lfloor x \rfloor$ biểu thị là số nguyên lớn nhất nhỏ hơn hoặc bằng x, và hàm $\lceil x \rceil$ là số nguyên nhỏ nhất bằng hoặc lớn hơn x.

3.2.2. Không sử dụng NOMA (Wo-NOMA)

Nếu nút nguồn không sử dụng NOMA, tại mỗi khe thời gian, S phát một gói mã hóa đến D. Giả sử mỗi gói mã hóa, cụ thể p, bao gồm U symbol, có nghĩa là $p=\{x_1[1],x_1[2],...,x_1[U]\}$, trong đó $x[u]$ là một symbol của p, và

$u = 1,2,...,U$. Khi S sử dụng ăng-ten thứ m để phát $x[u]$ đến D, tín hiệu nhận được tại ăng-ten thứ n của D được thể hiện là

$$y_{\mathrm{D},n}[u] = \sqrt{P_{\mathrm{S}}} h_{\mathrm{S}_m\mathrm{D}_n} x[u] + n_{\mathrm{D}}[u], \tag{3.2}$$

trong đó P_{S} là công suất phát tất cả các ăng-ten của S, $n_{\mathrm{D}}[u]$ là nhiễu Gauss trắng cộng tại D. Để dễ phân tích và trình bày, giả sử rằng tất cả nhiễu cộng được mô hình hóa là các biến ngẫu nhiên Gauss với trung bình bằng 0 và phương sai σ^2.

Từ (3.2), SNR tức thời của liên kết $\mathrm{S}_m \to \mathrm{D}_n$ được cho là

$$\psi_{\mathrm{S}_m\mathrm{D}_n} = \frac{P_{\mathrm{S}} \gamma_{\mathrm{S}_m\mathrm{D}_n}}{\sigma^2} = \Delta \gamma_{\mathrm{S}_m\mathrm{D}_n}, \tag{3.3}$$

với $\Delta = P_{\mathrm{S}} / \sigma^2$ là SNR phát.

Khi nút đích sử dụng kỹ thuật SC, SNR đạt được tại đầu ra của bộ kết hợp có thể được tính tương tự như công thức (3) của [102] là

$$\psi_{\mathrm{S}_m\mathrm{D}_b} = \max_{n=1,2,...,N_{\mathrm{D}}} \left(\psi_{\mathrm{S}_m\mathrm{D}_n} \right), \tag{3.4}$$

với b biểu thị là chỉ số ăng-ten thu tại D được sử dụng để giải mã $x[u]$, $b \in \{1,2,...,N_{\mathrm{D}}\}$.

Tiếp theo, nút nguồn lựa chọn ăng-ten tốt nhất của mình để tối đa SNR tức thời của liên kết dữ liệu là

$$\psi_{\mathrm{S}_a\mathrm{D}_b} = \max_{m=1,2,...,N_{\mathrm{S}}} \left(\psi_{\mathrm{S}_m\mathrm{D}_b} \right), \tag{3.5}$$

với a biểu thị là chỉ số ăng-ten phát được lựa chọn tại nút nguồn.

Kết hợp (3.4) và (3.5), ta có thể viết lại SNR của liên kết dữ liệu là

$$\psi_{\mathrm{D}}^{\mathrm{TAS/SC}} = \max_{m=1,2,...,N_{\mathrm{S}}} \left(\max_{n=1,2,...,N_{\mathrm{D}}} \left(\psi_{\mathrm{S}_m\mathrm{D}_n} \right) \right), \tag{3.6}$$

Để so sánh công bằng, nút nghe lén cũng sử dụng bộ kết hợp SC cho giải mã p. Tương tự (3.4), SNR đạt được của liên kết nghe lén được tính là

$$\psi_{\mathrm{E}}^{\mathrm{SC}} = \max_{t=1,2,\ldots,N_{\mathrm{E}}} \left(\psi_{\mathrm{S}_a\mathrm{E}_t} \right), \tag{3.7}$$

với $\psi_{\mathrm{S}_a\mathrm{E}_t} = \Delta\gamma_{\mathrm{S}_a\mathrm{E}_t}$.

Nếu nút đích sử dụng MRC, tín hiệu kết hợp tại D có thể được cho là

$$\begin{aligned} y_{\mathrm{D},n}^{\mathrm{MRC}}[u] &= \sum_{n=1}^{N_{\mathrm{D}}} \frac{\sqrt{P_{\mathrm{S}}} h_{\mathrm{S}_m\mathrm{D}_n}^*}{\sum_{n=1}^{N_{\mathrm{D}}} P_{\mathrm{S}} \left| h_{\mathrm{S}_m\mathrm{D}_n} \right|^2} y_{\mathrm{D},n}[u] \\ &= x[u] + \sum_{n=1}^{N_{\mathrm{D}}} \frac{\sqrt{P_{\mathrm{S}}} h_{\mathrm{S}_m\mathrm{D}_n}^* n_{\mathrm{D}}[u]}{\sum_{n=1}^{N_{\mathrm{D}}} P_{\mathrm{S}} \left| h_{\mathrm{S}_m\mathrm{D}_n} \right|^2}, \end{aligned} \tag{3.8}$$

với $h_{\mathrm{S}_m\mathrm{D}_n}^*$ là liên hợp số phức $h_{\mathrm{S}_m\mathrm{D}_n}$.

Từ (3.8), SNR đạt được tại D được tính là

$$\psi_{\mathrm{S}_m\mathrm{D}}^{\mathrm{MRC}} = \sum_{n=1}^{N_{\mathrm{D}}} \Delta \left| h_{\mathrm{S}_m\mathrm{D}_n} \right|^2 = \sum_{n=1}^{N_{\mathrm{D}}} \psi_{\mathrm{S}_m\mathrm{D}_n}. \tag{3.9}$$

Kế tiếp, kỹ thuật TAS được sử dụng để cung cấp SNR lớn nhất cho liên kết dữ liệu, tức là

$$\psi_{\mathrm{D}}^{\mathrm{TAS/MRC}} = \max_{m=1,2,\ldots,N_{\mathrm{S}}} \left(\sum_{n=1}^{N_{\mathrm{D}}} \psi_{\mathrm{S}_m\mathrm{D}_n} \right). \tag{3.10}$$

Tương tự (3.9), SNR tức thời của liên kết nghe lén được tính là

$$\psi_{\mathrm{E}}^{\mathrm{MRC}} = \sum_{t=1}^{N_{\mathrm{E}}} \psi_{\mathrm{S}_a\mathrm{E}_t}, \tag{3.11}$$

với a biểu thị là chỉ số ăng-ten được lựa chọn tại nút nguồn.

Nhận xét 1. *Do kênh pha đinh khối, SNR tức thời của các symbol* $x[u]$ *không đổi với mọi* u *trong khoảng thời gian mà kênh truyền chưa thay đổi. Do đó, trong (3.6), (3.7), (3.10) và (3.11), Luận án bỏ qua chỉ số* u *khi trình bày SNR của các kênh dữ liệu và nghe lén. Kế tiếp, giả sử rằng gói mã hóa* p *có thể được giải mã thành công nếu SNR tức thời nhận được tại nút đích và*

nút nghe lén lớn hơn một ngưỡng xác định trước, được định nghĩa bởi γ_{th}, *có thể được tính tương ứng là*

$$\rho_{\text{D}} = \Pr\left(\psi_{\text{D}}^{\text{Y}} \geq \gamma_{\text{th}}\right),$$
$$\rho_{\text{E}} = \Pr\left(\psi_{\text{E}}^{\text{Z}} \geq \gamma_{\text{th}}\right), \tag{3.12}$$

với $\text{Y} \in \{\text{TAS/SC, TAS/MRC}\}$ *và* $\text{Z} \in \{\text{SC, MRC}\}$.

Tiếp theo, xác suất mà các nút D và E không thể giải mã chính xác gói mã hóa p được cho là $1-\rho_{\text{D}}$ và $1-\rho_{\text{E}}$, tương ứng.

3.2.3. Sử dụng NOMA

Để giảm số khe thời gian được sử dụng để phát các gói mã hóa, nút nguồn có thể sử dụng NOMA để phát hai gói mã hóa, cụ thể p_1 và p_2, đến nút đích trong một khe thời gian. Giả sử rằng $p_1 = \{x_1[1], x_1[2], ..., x_1[U]\}$ và $p_2 = \{x_2[1], x_2[2], ..., x_2[U]\}$, với $x_1[u]$ và $x_2[u]$ là các symbol của p_1 và p_2, tương ứng, và $u = 1, 2, ..., U$. Thật vậy, nút nguồn kết hợp tuyến tính hai tín hiệu $x_1[u]$ và $x_2[u]$ [93], có nghĩa là, $x_+[u] = \sqrt{a_1 P_{\text{S}}}\, x_1[u] + \sqrt{a_2 P_{\text{S}}}\, x_2[u]$, và sau đó gửi $x_+[u]$ đến nút đích, trong đó a_1 và a_2 là các hệ số phân bổ công suất, với $a_1 + a_2 = 1$, $a_1 > a_2 > 0$. Tương tự như (3.2), tín hiệu nhận được tại D có thể được biểu diễn là

$$\begin{aligned} y_{\text{D},n}[u] &= h_{\text{S}_m\text{D}_n} x_+[u] + n_{\text{D}}[u] \\ &= h_{\text{S}_m\text{D}_n}\left(\sqrt{a_1 P_{\text{S}}}\, x_1[u] + \sqrt{a_2 P_{\text{S}}}\, x_2[u]\right) + n_{\text{D}}[u]. \end{aligned} \tag{3.13}$$

Theo nguyên tắc SIC, nút đích giải mã $x_1[u]$ trước bằng cách xem $x_2[u]$ là nhiễu. Sau khi giải mã thành công $x_1[u]$, D loại bỏ thành phần bao gồm $x_1[u]$, tức là, $\sqrt{a_1 P_{\text{S}}}\, h_{\text{S}_m\text{D}_n} x_1[u]$, từ $y_{\text{D},n}[u]$. Sau đó, tín hiệu được sử dụng để giải mã $x_2[u]$ có thể được biểu diễn là (xem [103])

$$z_{\mathrm{D}}[u]=\sqrt{a_2P_{\mathrm{S}}}h_{\mathrm{S}_m\mathrm{D}_n}x_2[u]+n_{\mathrm{D}}[u]. \tag{3.14}$$

Từ (3.13) và (3.14), SNR tức thời, với khía cạnh $x_1[u]$ và $x_2[u]$ được cho tương ứng là

$$\psi_{\mathrm{S}_m\mathrm{D}_n}^{x_1[u]}=\frac{a_1\Delta\gamma_{\mathrm{S}_m\mathrm{D}_n}}{a_2\Delta\gamma_{\mathrm{S}_m\mathrm{D}_n}+1},\ \psi_{\mathrm{S}_m\mathrm{D}_n}^{x_2[u]}=a_2\Delta\gamma_{\mathrm{S}_m\mathrm{D}_n}. \tag{3.15}$$

Khi kỹ thuật TAS/SC được sử dụng, tương tự (3.6), SNR đạt được của liên kết dữ liệu cho giải mã $x_1[u]$ và $x_2[u]$ có thể biểu diễn tương ứng là

$$\psi_{\mathrm{D},1}^{\mathrm{TAS/SC}}=\frac{a_1\max\limits_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\max\limits_{n=1,2,\ldots,N_{\mathrm{D}}}\left(\psi_{\mathrm{S}_m\mathrm{D}_n}\right)\right)}{a_2\max\limits_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\max\limits_{n=1,2,\ldots,N_{\mathrm{D}}}\left(\psi_{\mathrm{S}_m\mathrm{D}_n}\right)\right)+1},$$

$$\psi_{\mathrm{D},2}^{\mathrm{TAS/SC}}=a_2\max_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\max_{n=1,2,\ldots,N_{\mathrm{D}}}\left(\psi_{\mathrm{S}_m\mathrm{D}_n}\right)\right). \tag{3.16}$$

Tương tự, nút nghe lén E giải mã $x_1[u]$ trước, và sau đó thực hiện SIC trước khi giải mã $x_2[u]$. Cùng với bộ kết hợp SC, SNR tức thời của kênh nghe lén được sử dụng để giải mã $x_1[u]$ và $x_2[u]$ được cho tương ứng là

$$\psi_{\mathrm{E},1}^{\mathrm{SC}}=\frac{a_1\max\limits_{t=1,2,\ldots,N_{\mathrm{E}}}\left(\psi_{\mathrm{S}_a\mathrm{E}_t}\right)}{a_2\max\limits_{t=1,2,\ldots,N_{\mathrm{E}}}\left(\psi_{\mathrm{S}_a\mathrm{E}_t}\right)+1},\ \psi_{\mathrm{E},2}^{\mathrm{SC}}=a_2\max_{t=1,2,\ldots,N_{\mathrm{E}}}\left(\psi_{\mathrm{S}_a\mathrm{E}_t}\right). \tag{3.17}$$

Trong trường hợp kỹ thuật MRC được sử dụng, tín hiệu kết hợp tại D có thể được cho là

$$y_{\mathrm{D},x_1}^{\mathrm{MRC}}[u]=\sum_{n=1}^{N_{\mathrm{D}}}\frac{\sqrt{a_1P_{\mathrm{S}}}h_{\mathrm{S}_m\mathrm{D}_n}^{*}}{a_1P_{\mathrm{S}}\sum\limits_{n=1}^{N_{\mathrm{D}}}\left|h_{\mathrm{S}_m\mathrm{D}_n}\right|^2}\left(\sqrt{a_1P_{\mathrm{S}}}h_{\mathrm{S}_m\mathrm{D}_n}x_1[u]+\sqrt{a_2P_{\mathrm{S}}}h_{\mathrm{S}_m\mathrm{D}_n}x_2[u]+n_{\mathrm{D}}[u]\right)$$

$$=x_1[u]+\frac{\sqrt{a_2}}{\sqrt{a_1}}x_2[u]+\sum_{n=1}^{N_{\mathrm{D}}}\frac{\sqrt{a_1P_{\mathrm{S}}}h_{\mathrm{S}_m\mathrm{D}_n}^{*}n_{\mathrm{D}}[u]}{a_1P_{\mathrm{S}}\sum\limits_{n=1}^{N_{\mathrm{D}}}\left|h_{\mathrm{S}_m\mathrm{D}_n}\right|^2}. \tag{3.18}$$

Sau khi loại bỏ các thành phần bao gồm $x_1[u]$ từ các tín hiệu nhận được tại tất cả các ăng-ten, nút đích dùng MRC để giải mã $x_2[u]$ sử dụng tín hiệu kết hợp dưới đây:

$$y_{\mathrm{D},x_2}^{\mathrm{MRC}}[u]=\sum_{n=1}^{N_{\mathrm{D}}}\frac{\sqrt{a_2P_{\mathrm{S}}}h_{\mathrm{S}_m\mathrm{D}_n}^{*}}{a_2P_{\mathrm{S}}\sum_{n=1}^{N_{\mathrm{D}}}\left|h_{\mathrm{S}_m\mathrm{D}_n}\right|^2}\left(\sqrt{a_2P_{\mathrm{S}}}h_{\mathrm{S}_m\mathrm{D}_n}x_2[u]+n_{\mathrm{D}}[u]\right)$$

$$=x_2[u]+\sum_{n=1}^{N_{\mathrm{D}}}\frac{\sqrt{a_2P_{\mathrm{S}}}h_{\mathrm{S}_m\mathrm{D}_n}^{*}n_{\mathrm{D}}[u]}{a_2P_{\mathrm{S}}\sum_{n=1}^{N_{\mathrm{D}}}\left|h_{\mathrm{S}_m\mathrm{D}_n}\right|^2}. \tag{3.19}$$

Từ (3.18) và (3.19), SNR đạt được đối với $x_1[u]$ và $x_2[u]$, được thể hiện tương ứng là

$$\psi_{\mathrm{S}_m\mathrm{D}}^{x_1[u]}=\frac{a_1\sum_{n=1}^{N_{\mathrm{D}}}\psi_{\mathrm{S}_m\mathrm{D}_n}}{a_2\sum_{n=1}^{N_{\mathrm{D}}}\psi_{\mathrm{S}_m\mathrm{D}_n}+1},\ \psi_{\mathrm{S}_m\mathrm{D}}^{x_2[u]}=a_2\sum_{n=1}^{N_{\mathrm{D}}}\psi_{\mathrm{S}_m\mathrm{D}_n}. \tag{3.20}$$

Khi nút nguồn sử dụng TAS để tối ưu chất lượng liên kết dữ liệu, SNR đạt được sử dụng để giải mã $x_1[u]$ và $x_2[u]$ có thể được tính tương ứng là

$$\psi_{\mathrm{D},1}^{\mathrm{TAS/MRC}}=\max_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\frac{a_1\sum_{n=1}^{N_{\mathrm{D}}}\psi_{\mathrm{S}_m\mathrm{D}_n}}{a_2\sum_{n=1}^{N_{\mathrm{D}}}\psi_{\mathrm{S}_m\mathrm{D}_n}+1}\right),$$

$$\psi_{\mathrm{D},2}^{\mathrm{TAS/MRC}}=\max_{m=1,2,\ldots,N_{\mathrm{S}}}\left(a_2\sum_{n=1}^{N_{\mathrm{D}}}\psi_{\mathrm{S}_m\mathrm{D}_n}\right). \tag{3.21}$$

Tương tự, đối với kênh nghe lén, SNR tức thời, đối với $x_1[u]$ và $x_2[u]$, có thể được tính tương ứng là

$$\psi_{\mathrm{E},1}^{\mathrm{MRC}}=\frac{a_1\sum_{t=1}^{N_{\mathrm{E}}}\psi_{\mathrm{S}_a\mathrm{E}_t}}{a_2\sum_{t=1}^{N_{\mathrm{E}}}\psi_{\mathrm{S}_a\mathrm{E}_t}+1},\ \psi_{\mathrm{E},2}^{\mathrm{MRC}}=a_2\sum_{t=1}^{N_{\mathrm{E}}}\psi_{\mathrm{S}_a\mathrm{E}_t}, \tag{3.22}$$

trong đó nút nguồn lựa chọn ăntен thứ a để phát dữ liệu đến nút đích.

Nhận xét 2. *Để giảm hơn nữa số khe thời gian được sử dụng cho truyền dẫn, nút nguồn có thể gửi nhiều hơn hai gói mã hóa đến nút đích tại mỗi khe thời gian. Tuy nhiên, khi nhiều tín hiệu hơn được kết hợp bởi nút nguồn, việc triển khai là phức tạp hơn. Ngoài ra, phần công suất phát được phân bổ đến mỗi tín hiệu là thấp hơn, có thể làm suy giảm hiệu năng hệ thống. Ví dụ, xem xét* $\psi_{\mathrm{D},1}^{\mathrm{TAS/SC}}$ *trong (3.16) có thể được xấp xỉ là*

$$\psi_{\mathrm{D},1}^{\mathrm{TAS/SC}}\approx\frac{a_1\max\limits_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\max\limits_{n=1,2,\ldots,N_{\mathrm{D}}}\left(\psi_{\mathrm{S}_m\mathrm{D}_n}\right)\right)}{a_2\max\limits_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\max\limits_{n=1,2,\ldots,N_{\mathrm{D}}}\left(\psi_{\mathrm{S}_m\mathrm{D}_n}\right)\right)}=\frac{a_1}{a_2}. \tag{3.23}$$

Rõ ràng từ (3.23) ta thấy rằng để giá trị SNR tức thời $\psi_{\mathrm{D},1}^{\mathrm{TAS/SC}}$ cao, a_1 nên lớn hơn nhiều so với a_2 (hoặc a_2 rất nhỏ). Cho ví dụ khác, nếu nút nguồn kết hợp 3 tín hiệu sử dụng các hệ số $a_1,\ a_2, a_3,$ với $a_1>a_2>a_3$ và $a_1+a_2+a_3=1,$ tương tự, chúng ta có $a_1\gg a_2\gg a_3,$ và do đó công suất phát được phân bổ đến tín hiệu thứ 3 là rất nhỏ.

Nhận xét 3. *Lưu ý rằng để giải mã được gói tin* $p_2,$ *nút đích phải giải mã chính xác gói tin* p_1 *trước. Nếu trạng thái giải mã của* p_1 *là không thành công,* p_2 *cũng không thể giải mã thành công. Do đó, xác suất mà trong một khe thời gian nút đích không thể thu được bất kỳ gói nào, chỉ thu được* $p_1,$ *và thu được cả* p_1 *và* p_2 *được tính tương ứng là*

$$\chi_{\mathrm{D},0}=\Pr\left(\psi_{\mathrm{D},1}^{\mathrm{Y}}<\gamma_{\mathrm{th}}\right),$$

$$\chi_{\mathrm{D},1}=\Pr\left(\psi_{\mathrm{D},1}^{\mathrm{Y}}\geq\gamma_{\mathrm{th}},\psi_{\mathrm{D},2}^{\mathrm{Y}}<\gamma_{\mathrm{th}}\right),$$

$$\chi_{\mathrm{D},2} = \Pr\left(\psi_{\mathrm{D},1}^{\mathrm{Y}} \geq \gamma_{\mathrm{th}}, \psi_{\mathrm{D},2}^{\mathrm{Y}} \geq \gamma_{\mathrm{th}}\right), \tag{3.24}$$

với $\mathrm{Y} \in \{\text{TAS/SC, TAS/MRC}\}$.

Tương tự, xác suất mà nút nghe lén không thể thu được bất kỳ gói mã hóa nào, chỉ thu được p_1, và thu được cả p_1 và p_2 được tính tương ứng là

$$\begin{aligned}
\chi_{\mathrm{E},0} &= \Pr\left(\psi_{\mathrm{E},1}^{\mathrm{Z}} < \gamma_{\mathrm{th}}\right), \\
\chi_{\mathrm{E},1} &= \Pr\left(\psi_{\mathrm{E},1}^{\mathrm{Z}} \geq \gamma_{\mathrm{th}}, \psi_{\mathrm{E},2}^{\mathrm{Z}} < \gamma_{\mathrm{th}}\right), \\
\chi_{\mathrm{E},2} &= \Pr\left(\psi_{\mathrm{E},1}^{\mathrm{Z}} \geq \gamma_{\mathrm{th}}, \psi_{\mathrm{E},2}^{\mathrm{Z}} \geq \gamma_{\mathrm{th}}\right),
\end{aligned} \tag{3.25}$$

với $\mathrm{Z} \in \{\text{SC, MRC}\}$.

3.3. PHÂN TÍCH HIỆU NĂNG

Trong phần này, Luận án đưa ra các biểu thức chính xác số khe thời gian trung bình (TS) và xác suất thu chặn (IP) của giao thức đề xuất. Đầu tiên, các xác suất ρ_{D}, ρ_{E}, $\chi_{\mathrm{D},i}$ và $\chi_{\mathrm{E},i}\left(i = 0,1,2\right)$ được tính toán.

3.3.1. Xác suất của ρ_{D} và ρ_{E}

- Trường hợp 1: Bộ kết hợp SC được sử dụng bởi D và E

$$\rho_{\mathrm{D}} = 1 - \left[1 - \exp\left(-\frac{\lambda_{\mathrm{SD}}\gamma_{\mathrm{th}}}{\Delta}\right)\right]^{N_{\mathrm{S}}N_{\mathrm{D}}}. \tag{3.26}$$

$$\rho_{\mathrm{E}} = 1 - \left[1 - \exp\left(-\frac{\lambda_{\mathrm{SE}}\gamma_{\mathrm{th}}}{\Delta}\right)\right]^{N_{\mathrm{E}}}. \tag{3.27}$$

- Trường hợp 2: Bộ kết hợp MRC được sử dụng bởi D và E

$$\rho_{\mathrm{D}} = 1 - \left[1 - \sum_{m=0}^{N_{\mathrm{D}}-1} \frac{1}{m!}\left(\frac{\lambda_{\mathrm{SD}}\gamma_{\mathrm{th}}}{\Delta}\right)^{m} \exp\left(-\frac{\lambda_{\mathrm{SD}}\gamma_{\mathrm{th}}}{\Delta}\right)\right]^{N_{\mathrm{S}}}. \tag{3.28}$$

$$\rho_{\mathrm{E}} = \sum_{t=0}^{N_{\mathrm{E}}-1} \frac{1}{t!}\left(\frac{\lambda_{\mathrm{SE}}\gamma_{\mathrm{th}}}{\Delta}\right)^{t} \exp\left(-\frac{\lambda_{\mathrm{SE}}\gamma_{\mathrm{th}}}{\Delta}\right). \tag{3.29}$$

Chứng minh: Xem chứng minh và các ký hiệu trong mục B.1, Phụ lục B.

3.3.2. Xác suất của $\chi_{\mathrm{D},i}$ *và* $\chi_{\mathrm{E},i}$

• Trường hợp 1: Bộ kết hợp SC được sử dụng bởi D và E

$$\chi_{\mathrm{D},2} = 1-\left[1-\exp\left(-\lambda_{\mathrm{SD}}\mu_2\right)\right]^{N_{\mathrm{S}}N_{\mathrm{D}}},$$

$$\chi_{\mathrm{D},0} = \left(1-\exp\left(-\lambda_{\mathrm{SD}}\mu_1\right)\right)^{N_{\mathrm{S}}N_{\mathrm{D}}},$$

$$\chi_{\mathrm{D},1} = \left(1-\exp\left(-\lambda_{\mathrm{SD}}\mu_2\right)\right)^{N_{\mathrm{S}}N_{\mathrm{D}}} - \left(1-\exp\left(-\lambda_{\mathrm{SD}}\mu_1\right)\right)^{N_{\mathrm{S}}N_{\mathrm{D}}}. \quad (3.30)$$

Mặt khác, $\chi_{\mathrm{E},0}, \chi_{\mathrm{E},1},$ và $\chi_{\mathrm{E},2}$ được tính tương ứng là

$$\chi_{\mathrm{E},0} = \left(1-\exp\left(-\lambda_{\mathrm{SE}}\mu_1\right)\right)^{N_{\mathrm{E}}},$$

$$\chi_{\mathrm{E},1} = \left(1-\exp\left(-\lambda_{\mathrm{SE}}\mu_2\right)\right)^{N_{\mathrm{E}}} - \left(1-\exp\left(-\lambda_{\mathrm{SE}}\mu_1\right)\right)^{N_{\mathrm{E}}},$$

$$\chi_{\mathrm{E},2} = 1-\left(1-\exp\left(-\lambda_{\mathrm{SE}}\mu_2\right)\right)^{N_{\mathrm{E}}}. \quad (3.31)$$

• Trường hợp 2: Bộ kết hợp MRC được sử dụng bởi D và E

$$\chi_{\mathrm{D},0} = \left[1-\sum_{m=0}^{N_{\mathrm{D}}-1}\frac{\left(\lambda_{\mathrm{SD}}\mu_1\right)^m}{m!}\exp\left(-\lambda_{\mathrm{SD}}\mu_1\right)\right]^{N_{\mathrm{S}}},$$

$$\chi_{\mathrm{D},1} = \left[1-\sum_{m=0}^{N_{\mathrm{D}}-1}\frac{\left(\lambda_{\mathrm{SD}}\mu_2\right)^m}{m!}\exp\left(-\lambda_{\mathrm{SD}}\mu_2\right)\right]^{N_{\mathrm{S}}} - \left[1-\sum_{m=0}^{N_{\mathrm{D}}-1}\frac{\left(\lambda_{\mathrm{SD}}\mu_1\right)^m}{m!}\exp\left(-\lambda_{\mathrm{SD}}\mu_1\right)\right]^{N_{\mathrm{S}}},$$

$$\chi_{\mathrm{D},2} = 1-\left[1-\sum_{m=0}^{N_{\mathrm{D}}-1}\frac{\left(\lambda_{\mathrm{SD}}\mu_2\right)^m}{m!}\exp\left(-\lambda_{\mathrm{SD}}\mu_2\right)\right]^{N_{\mathrm{S}}},$$

$$\chi_{\mathrm{E},0} = 1-\sum_{t=0}^{N_{\mathrm{E}}-1}\frac{\left(\lambda_{\mathrm{SE}}\mu_1\right)^t}{t!}\exp\left(-\lambda_{\mathrm{SE}}\mu_1\right),$$

$$\chi_{\mathrm{E},1} = \sum_{t=0}^{N_{\mathrm{E}}-1}\frac{\left(\lambda_{\mathrm{SE}}\mu_1\right)^t}{t!}\exp\left(-\lambda_{\mathrm{SE}}\mu_1\right) - \sum_{t=0}^{N_{\mathrm{E}}-1}\frac{\left(\lambda_{\mathrm{SE}}\mu_2\right)^t}{t!}\exp\left(-\lambda_{\mathrm{SE}}\mu_2\right),$$

$$\chi_{\mathrm{E},2} = \sum_{t=0}^{N_{\mathrm{E}}-1}\frac{\left(\lambda_{\mathrm{SE}}\mu_2\right)^t}{t!}\exp\left(-\lambda_{\mathrm{SE}}\mu_2\right). \quad (3.32)$$

Chứng minh: Xem chứng minh và các ký hiệu trong mục B.2, Phụ lục B.

3.3.3. Số khe thời gian trung bình (TS)

TS thể hiện số khe thời gian trung bình được sử dụng hay là số lần truyền cần thiết và là thông số quan trọng. Rõ ràng truyền càng nhiều khe thời gian thì càng tiêu tốn nhiều năng lượng, thời gian trễ và do đó hệ thống sử dụng càng ít TS thì phẩm chất đạt được càng tốt.

3.3.3.1. Không sử dụng NOMA (Wo-NOMA)

Số khe thời gian trung bình của giao thức Wo-NOMA có thể được tính là

$$\text{TS}= \sum_{N_{\text{TS}}=N_{\text{req}}^{\text{pkt}}}^{+\infty} N_{\text{TS}} \times \Pr\left(N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}} \mid N_{\text{TS}}\right), \tag{3.33}$$

với $\Pr\left(N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}} \mid N_{\text{TS}}\right)$ là xác suất mà D đạt được $N_{\text{req}}^{\text{pkt}}$ gói mã hóa sau N_{TS} khe thời gian, theo phân bố nhị thức âm (negative binomial distribution) (xem công thức (9), tài liệu [105]):

$$\Pr\left(N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}} \mid N_{\text{TS}}\right) = C_{N_{\text{TS}}-1}^{N_{\text{req}}^{\text{pkt}}-1} \left(\rho_{\text{D}}\right)^{N_{\text{req}}^{\text{pkt}}} \left(1-\rho_{\text{D}}\right)^{N_{\text{TS}}-N_{\text{req}}^{\text{pkt}}}, \tag{3.34}$$

và $C_b^a \left(b \geq a\right)$ định nghĩa là hệ số nhị thức:

$$C_b^a = \frac{b!}{a!\left(b-a\right)!}.$$

Biểu thức (3.34) có thể được giải thích như sau. Sau $\left(N_{\text{TS}}-1\right)$ khe thời gian, nút đích đạt được $N_{\text{req}}^{\text{pkt}}-1$ gói mã hóa và D nhận chính xác một gói mã hóa nữa tại khe thời gian thứ N_{TS}. Trong (3.34), $C_{N_{\text{TS}}-1}^{N_{\text{req}}^{\text{pkt}}-1}$ là số trường hợp có thể xảy ra khi D có $N_{\text{req}}^{\text{pkt}}-1$ gói mã hóa trước khe thời gian cuối cùng.

Thay thế (3.34) vào (3.33) và sử dụng công thức (8) của [95], ta có

$$\text{TS}= \frac{N_{\text{req}}^{\text{pkt}}}{\rho_{\text{D}}}. \tag{3.35}$$

Thay thế (3.26) và (3.28) vào (3.35), ta đạt được các biểu thức chính xác tương ứng của TS khi các bộ kết hợp SC và MRC được sử dụng.

3.3.3.1. Sử dụng NOMA

Trong giao thức này, tác giả tính toán số khe thời gian trung bình được sử dụng bởi nút nguồn là

$$\text{TS}= \sum_{N_{\text{TS}}=\left\lceil N_{\text{req}}^{\text{pkt}}/2 \right\rceil}^{+\infty} N_{\text{TS}} \times \Pr\left(N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}} \cup N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}} + 1 | \, N_{\text{TS}} \right), \qquad (3.36)$$

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

Trong phần này, định nghĩa T_1 và T_2 là số khe thời gian mà nút đích có thể nhận chính xác một và hai gói mã hóa, tương ứng. Để tính toán $\Pr\left(N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}} \cup N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}} + 1 | \, N_{\text{TS}} \right),$ ta xem xét ba trường hợp như sau:

• Trường hợp 1: Sau $N_{\text{TS}} - 1$ khe thời gian, nút đích đạt được $N_{\text{req}}^{\text{pkt}} - 2$ gói mã hóa và tại khe thời gian cuối cùng, D đạt được cả hai gói mã hóa.

Trong trường hợp này, sau khi quá trình truyền kết thúc, nút đích có $N_{\text{req}}^{\text{pkt}}$ gói mã hóa, tức là $N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}}$ và $\text{T}_1 + 2\text{T}_2 = N_{\text{req}}^{\text{pkt}}$. Hơn nữa, xác suất của Trường hợp 1 có thể được tính toán như sau:

$$\theta_{\text{D},1} = \sum_{\text{T}_2=1}^{\left\lfloor N_{\text{req}}^{\text{pkt}}/2 \right\rfloor} C_{N_{\text{TS}}-1}^{\text{T}_1} C_{N_{\text{TS}}-\text{T}_1-1}^{\text{T}_2-1} \left(\chi_{\text{D},2} \right)^{\text{T}_2} \left(\chi_{\text{D},1} \right)^{\text{T}_1} \left(\chi_{\text{D},0} \right)^{N_{\text{TS}}-\text{T}_2-\text{T}_1}, \qquad (3.37)$$

với $\text{T}_1 \le N_{\text{TS}} - 1,\ \text{T}_2 \le N_{\text{TS}} - \text{T}_1.$

• Trường hợp 2: Sau $N_{\text{TS}} - 1$ khe thời gian, nút đích đạt được $N_{\text{req}}^{\text{pkt}} - 1$ gói mã hóa và tại khe thời gian cuối cùng, D chỉ đạt được một gói mã hóa.

Trong Trường hợp 2, ta cũng có $N_{\text{D}}^{\text{pkt}} = N_{\text{req}}^{\text{pkt}}$ và $\text{T}_1 + 2\text{T}_2 = N_{\text{req}}^{\text{pkt}}$. Tiếp theo, xác suất của sự kiện này được tính là

$$\theta_{\text{D},2} = \sum_{\text{T}_2=0}^{\left\lfloor N_{\text{req}}^{\text{pkt}}/2 \right\rfloor} C_{N_{\text{TS}}-1}^{\text{T}_2} C_{N_{\text{TS}}-\text{T}_2-1}^{\text{T}_1-1} \left(\chi_{\text{D},2} \right)^{\text{T}_2} \left(\chi_{\text{D},1} \right)^{\text{T}_1} \left(\chi_{\text{D},0} \right)^{N_{\text{TS}}-\text{T}_2-\text{T}_1}, \qquad (3.38)$$

với $1 \le \mathrm{T}_1 \le N_{\mathrm{TS}} - \mathrm{T}_2,\ \mathrm{T}_2 \le N_{\mathrm{TS}} - 1.$

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

Trong Trường hợp này, nút đích có thể nhận thành công $N_{\mathrm{req}}^{\mathrm{pkt}} + 1$ gói mã hóa sau N_{TS} khe thời gian: $\mathrm{T}_1 + 2\mathrm{T}_2 = N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} + 1.$ Do đó, xác suất mà sự kiện này xảy ra có thể được tính toán chính xác là

$$\theta_{\mathrm{D},3} = \sum_{\mathrm{T}_2=1}^{\left\lceil N_{\mathrm{req}}^{\mathrm{pkt}}/2 \right\rceil} C_{N_{\mathrm{TS}}-1}^{\mathrm{T}_1} C_{N_{\mathrm{TS}}-\mathrm{T}_1-1}^{\mathrm{T}_2-1} \left(\chi_{\mathrm{D},2}\right)^{\mathrm{T}_2} \left(\chi_{\mathrm{D},1}\right)^{\mathrm{T}_1} \left(\chi_{\mathrm{D},0}\right)^{N_{\mathrm{TS}}-\mathrm{T}_2-\mathrm{T}_1}, \qquad (3.39)$$

trong đó $\mathrm{T}_1 \le N_{\mathrm{TS}} - 1,\ \mathrm{T}_2 \le N_{\mathrm{TS}} - \mathrm{T}_1.$

Từ (3.37)-(3.39), ta có thể đạt được biểu thức chính xác của $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \cup N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} + 1 | N_{\mathrm{TS}}\right)$ bằng cách sử dụng công thức tính toán dưới đây:

$$\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \cup N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} + 1 | N_{\mathrm{TS}}\right) = \theta_{\mathrm{D},1} + \theta_{\mathrm{D},2} + \theta_{\mathrm{D},3}.$$

Sau đó, từ (3.36), chúng ta có thể viết số các khe thời gian trung bình được sử dụng trong giao thức NOMA như sau:

$$\mathrm{TS} = \sum_{N_{\mathrm{TS}}=\left\lceil N_{\mathrm{req}}^{\mathrm{pkt}}/2 \right\rceil}^{+\infty} N_{\mathrm{TS}} \times \left(\theta_{\mathrm{D},1} + \theta_{\mathrm{D},2} + \theta_{\mathrm{D},3}\right). \qquad (3.40)$$

Nhận xét 4. *Từ (3.35) và (3.40), chúng ta có thể quan sát rằng khi SNR phát đủ lớn, cụ thể* $\Delta \to +\infty$*, tất cả sự truyền tại các khe thời gian đều thành công, giá trị của TS trong các giao thức Wo-NOMA và NOMA hội tụ đến* $N_{\mathrm{req}}^{\mathrm{pkt}}$ *và* $\left\lceil N_{\mathrm{req}}^{\mathrm{pkt}}/2 \right\rceil$*, tương ứng. Thực tế rằng, tại các mức* Δ *lớn, tất cả các gói mã hóa có thể được nhận chính xác bởi nút đích. Do đó, bằng cách sử dụng NOMA, giao thức đề xuất có thể giảm một nữa số khe thời gian được sử dụng cho truyền các gói mã hóa.*

3.3.4. Xác suất thu chặn (IP)

Trong Phần này, tác giả tính toán xác suất thu chặn của các giao thức đề xuất cùng với sử dụng và không sử dụng NOMA.

3.3.4.1. Không sử dụng NOMA (Wo-NOMA)

Trước tiên, chúng ta thấy rằng dữ liệu nguồn bị thu chặn nếu nút nghe lén có thể đạt được đủ số gói mã hóa cho khôi phục dữ liệu gốc trước hoặc cùng thời điểm với nút đích. Diễn giải về mặt toán học, chúng ta có thể viết

$$\mathrm{IP}=\sum_{N_{\mathrm{TS}}^{\mathrm{E}}=N_{\mathrm{req}}^{\mathrm{pkt}}}^{+\infty}\left[\begin{array}{l}\left(\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}\mid N_{\mathrm{TS}}^{\mathrm{E}}\right)+\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}}<N_{\mathrm{req}}^{\mathrm{pkt}}\mid N_{\mathrm{TS}}^{\mathrm{E}}\right)\right)\\ \times\Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}\mid N_{\mathrm{TS}}^{\mathrm{E}}\right)\end{array}\right]. \quad (3.41)$$

Công thức (3.41) ngụ ý rằng nút nghe lén có thể đạt được $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa sau $N_{\mathrm{TS}}^{\mathrm{E}}$ khe thời gian, trong khi nút đích có thể nhận đủ hoặc không. Trong (3.41), $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}\mid N_{\mathrm{TS}}^{\mathrm{E}}\right)$ được tính như trong (3.34) và tương tự, $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}}<N_{\mathrm{req}}^{\mathrm{pkt}}\mid N_{\mathrm{TS}}^{\mathrm{E}}\right)$ cũng được cho là

$$\Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}\mid N_{\mathrm{TS}}^{\mathrm{E}}\right)=C_{N_{\mathrm{TS}}^{\mathrm{E}}-1}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1}\left(\rho_{\mathrm{E}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}}\left(1-\rho_{\mathrm{E}}\right)^{N_{\mathrm{TS}}^{\mathrm{E}}-N_{\mathrm{req}}^{\mathrm{pkt}}}. \quad (3.42)$$

Xem xét $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}}<N_{\mathrm{req}}^{\mathrm{pkt}}\mid N_{\mathrm{TS}}^{\mathrm{E}}\right)$ trong (3.41), là xác suất mà nút đích không thể nhận đủ số gói mã hóa cho việc khôi phục dữ liệu sau $N_{\mathrm{TS}}^{\mathrm{E}}$ khe thời gian và được tính là

$$\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}}<N_{\mathrm{req}}^{\mathrm{pkt}}\mid N_{\mathrm{TS}}^{\mathrm{E}}\right)=\sum_{N_{\mathrm{D}}^{\mathrm{pkt}}=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1}C_{N_{\mathrm{TS}}^{\mathrm{E}}}^{N_{\mathrm{D}}^{\mathrm{pkt}}}\left(\rho_{\mathrm{D}}\right)^{N_{\mathrm{D}}^{\mathrm{pkt}}}\left(1-\rho_{\mathrm{D}}\right)^{N_{\mathrm{TS}}^{\mathrm{E}}-N_{\mathrm{D}}^{\mathrm{pkt}}}. \quad (3.43)$$

Nhận xét 5. *Khi E đạt được $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa, nút nghe lén không giải mã các gói mã hóa thêm nữa, bất kể nút nguồn vẫn phát các gói mã hóa đến nút đích. Điều này có nghĩa rằng sau khi nhận được $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa, E dừng nghe lén việc dữ liệu truyền và bắt đầu khôi phục dữ liệu.*

Kết hợp (3.41)-(3.43), IP có thể được tính chính xác là

$$\mathrm{IP}=\sum_{N_{\mathrm{TS}}^{\mathrm{E}}=N_{\mathrm{req}}^{\mathrm{pkt}}}^{+\infty}\left[\begin{array}{l}\left(\begin{array}{l}C_{N_{\mathrm{TS}}^{\mathrm{E}}-1}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1}\left(\rho_{\mathrm{D}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}}\left(1-\rho_{\mathrm{D}}\right)^{N_{\mathrm{TS}}^{\mathrm{E}}-N_{\mathrm{req}}^{\mathrm{pkt}}}\\+\sum_{N_{\mathrm{D}}^{\mathrm{pkt}}=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1}C_{N_{\mathrm{TS}}^{\mathrm{E}}}^{N_{\mathrm{D}}^{\mathrm{pkt}}}\left(\rho_{\mathrm{D}}\right)^{N_{\mathrm{D}}^{\mathrm{pkt}}}\left(1-\rho_{\mathrm{D}}\right)^{N_{\mathrm{TS}}^{\mathrm{E}}-N_{\mathrm{D}}^{\mathrm{pkt}}}\end{array}\right)\\\times C_{N_{\mathrm{TS}}^{\mathrm{E}}-1}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1}\left(\rho_{\mathrm{E}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}}\left(1-\rho_{\mathrm{E}}\right)^{N_{\mathrm{TS}}^{\mathrm{E}}-N_{\mathrm{req}}^{\mathrm{pkt}}}\end{array}\right]. \tag{3.44}$$

3.3.4.2. Sử dụng NOMA

Trong giao thức này, IP có thể được tính là

$$\mathrm{IP}=\sum_{N_{\mathrm{TS}}^{\mathrm{E}}=\left\lceil N_{\mathrm{req}}^{\mathrm{pkt}}/2\right\rceil}^{+\infty}\left[\begin{array}{l}\left(\begin{array}{l}\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}\cup N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}+1|\,N_{\mathrm{TS}}^{\mathrm{E}}\right)\right)\\+\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}}<N_{\mathrm{req}}^{\mathrm{pkt}}\,|\,N_{\mathrm{TS}}^{\mathrm{E}}\right)\end{array}\right)\\\times\Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}\cup N_{\mathrm{E}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}+1|\,N_{\mathrm{TS}}^{\mathrm{E}}\right)\end{array}\right]. \tag{3.45}$$

$\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}\cup N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}+1|\,N_{\mathrm{TS}}^{\mathrm{E}}\right)$, $\Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}\cup N_{\mathrm{E}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}+1|\,N_{\mathrm{TS}}^{\mathrm{E}}\right)$ được tính tương tự như (3.37)-(3.39) là

$$\begin{aligned}\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}\cup N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}+1|\,N_{\mathrm{TS}}^{\mathrm{E}}\right)&=\theta_{\mathrm{D},1}+\theta_{\mathrm{D},2}+\theta_{\mathrm{D},3},\\\Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}\cup N_{\mathrm{E}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}+1|\,N_{\mathrm{TS}}^{\mathrm{E}}\right)&=\theta_{\mathrm{E},1}+\theta_{\mathrm{E},2}+\theta_{\mathrm{E},3}.\end{aligned} \tag{3.46}$$

Trong (3.46), lưu ý rằng $\theta_{\mathrm{D},1}$, $\theta_{\mathrm{D},2}$ và $\theta_{\mathrm{D},3}$ đạt được bằng cách thay thế N_{TS} trong (3.37)-(3.39) bởi $N_{\mathrm{TS}}^{\mathrm{E}}$. Đối với $\theta_{\mathrm{E},1}$, $\theta_{\mathrm{E},2}$ và $\theta_{\mathrm{E},3}$, phương pháp tương tự như được đưa ra trong $\theta_{\mathrm{D},1}$, $\theta_{\mathrm{D},2}$, $\theta_{\mathrm{D},3}$, chúng ta có thể đạt được

$$\begin{aligned}\theta_{\mathrm{E},1}&=\sum_{\mathrm{V}_2=1}^{\left\lfloor N_{\mathrm{req}}^{\mathrm{pkt}}/2\right\rfloor}C_{N_{\mathrm{TS}}^{\mathrm{E}}-1}^{\mathrm{V}_1}C_{N_{\mathrm{TS}}^{\mathrm{E}}-\mathrm{V}_1-1}^{\mathrm{V}_2-1}\left(\chi_{\mathrm{E},2}\right)^{\mathrm{V}_2}\left(\chi_{\mathrm{E},1}\right)^{\mathrm{V}_1}\left(\chi_{\mathrm{E},0}\right)^{N_{\mathrm{TS}}^{\mathrm{E}}-\mathrm{V}_2-\mathrm{V}_1},\\\theta_{\mathrm{E},2}&=\sum_{\mathrm{V}_2=0}^{\left\lfloor N_{\mathrm{req}}^{\mathrm{pkt}}/2\right\rfloor}C_{N_{\mathrm{TS}}^{\mathrm{E}}-1}^{\mathrm{V}_2}C_{N_{\mathrm{TS}}^{\mathrm{E}}-\mathrm{V}_2-1}^{\mathrm{V}_1-1}\left(\chi_{\mathrm{E},2}\right)^{\mathrm{V}_2}\left(\chi_{\mathrm{E},1}\right)^{\mathrm{V}_1}\left(\chi_{\mathrm{E},0}\right)^{N_{\mathrm{TS}}^{\mathrm{E}}-\mathrm{V}_2-\mathrm{V}_1},\\\theta_{\mathrm{E},3}&=\sum_{\mathrm{V}_2=1}^{\left\lceil N_{\mathrm{req}}^{\mathrm{pkt}}/2\right\rceil}C_{N_{\mathrm{TS}}^{\mathrm{E}}-1}^{\mathrm{V}_1}C_{N_{\mathrm{TS}}^{\mathrm{E}}-\mathrm{V}_1-1}^{\mathrm{V}_2-1}\left(\chi_{\mathrm{E},2}\right)^{\mathrm{V}_2}\left(\chi_{\mathrm{E},1}\right)^{\mathrm{V}_1}\left(\chi_{\mathrm{E},0}\right)^{N_{\mathrm{TS}}^{\mathrm{E}}-\mathrm{V}_2-\mathrm{V}_1},\end{aligned} \tag{3.47}$$

trong đó V_1 và V_2 là số khe thời gian mà nút nghe lén nhận chính xác một và hai gói mã hóa, tương ứng.

Xem xét $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} < N_{\mathrm{req}}^{\mathrm{pkt}} \mid N_{\mathrm{TS}}^{\mathrm{E}}\right)$, là xác suất mà nút đích không thể đạt được $N_{\mathrm{req}}^{\mathrm{pkt}}$ gói mã hóa sau $N_{\mathrm{TS}}^{\mathrm{E}}$ khe thời gian và được tính là

$$\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} < N_{\mathrm{req}}^{\mathrm{pkt}} \mid N_{\mathrm{TS}}^{\mathrm{E}}\right) \triangleq \theta_{\mathrm{D},4}$$

$$= \sum_{N_{\mathrm{D}}^{\mathrm{pkt}}=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} \sum_{\mathrm{T}_2=0}^{\left\lfloor N_{\mathrm{D}}^{\mathrm{pkt}}/2 \right\rfloor} C_{N_{\mathrm{TS}}^{\mathrm{E}}}^{\mathrm{T}_2} C_{N_{\mathrm{TS}}^{\mathrm{E}}-\mathrm{T}_2}^{\mathrm{T}_1} \left(\chi_{\mathrm{D},2}\right)^{\mathrm{T}_2} \left(\chi_{\mathrm{D},1}\right)^{\mathrm{T}_1} \left(\chi_{\mathrm{D},0}\right)^{N_{\mathrm{TS}}^{\mathrm{E}}-\mathrm{T}_2-\mathrm{T}_1}. \quad (3.48)$$

Từ (3.45)-(3.48), IP trong giao thức NOMA được viết lại như sau:

$$\mathrm{IP}= \sum_{N_{\mathrm{TS}}^{\mathrm{E}}=\left\lceil N_{\mathrm{req}}^{\mathrm{pkt}}/2 \right\rceil}^{+\infty} \left[\left(\theta_{\mathrm{D},1}+\theta_{\mathrm{D},2}+\theta_{\mathrm{D},3}+\theta_{\mathrm{D},4}\right)\times\left(\theta_{\mathrm{E},1}+\theta_{\mathrm{E},2}+\theta_{\mathrm{E},3}\right)\right]. \quad (3.49)$$

Nhận xét 6. *Các biểu thức (3.44) và (3.49) biểu diễn chính xác hiệu năng IP của các giao thức Wo-NOMA và NOMA. Để đạt được các giá trị của IP, tác giả cắt các chuỗi vô hạn bởi 500 số hạng đầu tiên. Hơn nữa, bởi vì (3.44) và (3.49) là các biểu thức dạng chính xác, có thể được sử dụng hiệu quả trong việc thiết kế và tối ưu mạng.*

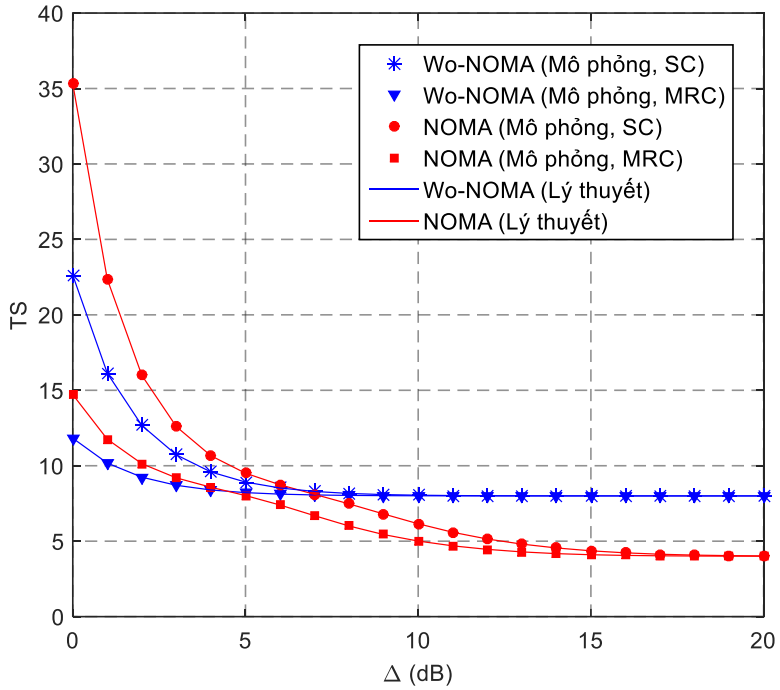
3.4. CÁC KẾT QUẢ MÔ PHỎNG

Trong phần này, Luận án trình bày các kết quả mô phỏng sử dụng phương pháp Monte Carlo để kiểm chứng kết quả lý thuyết đã đạt được trong Phần 3.3, so sánh hiệu năng của các giao thức đề xuất sử dụng và không sử dụng NOMA dưới góc độ TS và IP. Tất cả các kết quả mô phỏng và lý thuyết, tác giả thực hiện $10^5 - 5\times10^6$ phép thử, hệ số kênh truyền Rayleigh của liên kết X-Y được tạo bởi $h_{\mathrm{XY}} = 1/sqrt\left(2\times L_{\mathrm{XY}}\right)\times\left(randn(1,1)+j\times randn(1,1)\right)$, với $\left(\mathrm{X},\mathrm{Y}\right)\in\left\{\mathrm{S}_m,\mathrm{D}_n,\mathrm{E}_t\right\}$, L_{XY} (hoặc λ_{XY}) là tham số kênh X-Y, $randn(1,1)$ là hàm MATLAB tạo ra số chuỗi giả ngẫu nhiên phân bố Gauss có trung bình bằng 0 và phương sai bằng 1. Đối với kết quả lý thuyết, biểu thức TS và IP

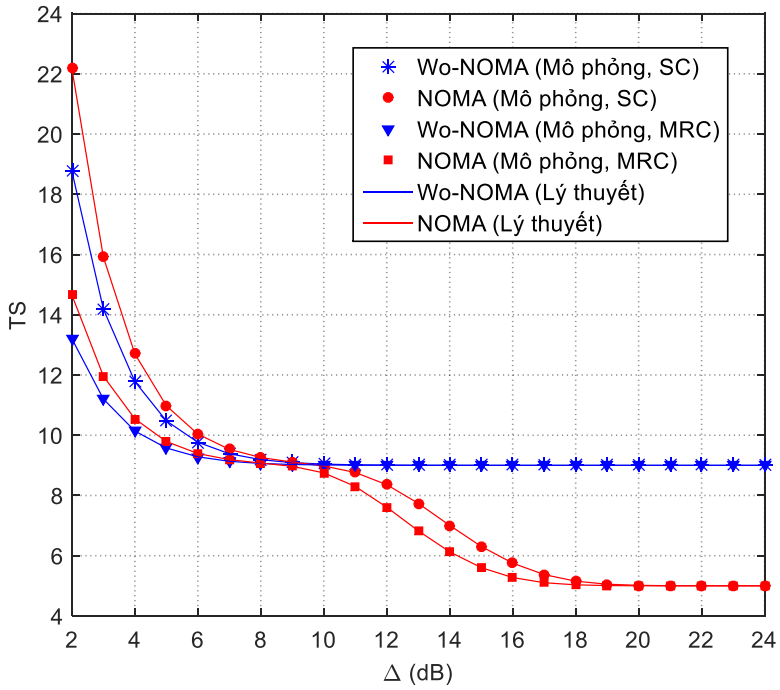
đưa ra trong phần trước được sử dụng trình bày. Như đề cập trong *Nhận xét 6*, chuỗi vô hạn trong công thức tính toán được cắt bởi 500 số hạng đầu tiên.

3.4.1. Số khe thời gian trung bình (TS)

Trong Hình 3.2, Luận án trình bày số khe thời gian trung bình mà nút nguồn sử dụng để phát các gói mã hóa đến nút đích như là hàm của SNR phát $\Delta(\mathrm{dB})$. Trong Hình vẽ này, số ăng-ten tại nút nguồn (N_{S}) và nút đích (N_{D}) là 1 và 3, tương ứng, tham số của liên kết dữ liệu (λ_{SD}) được cố định bằng 2, số gói mã hóa yêu cầu cho khôi phục thành công dữ liệu gốc $\left(N_{\mathrm{req}}^{\mathrm{pkt}}\right)$ được đặt bằng 8, và ngưỡng γ_{th} được đặt bằng 1. Như đã được đề cập trong *Nhận xét* của công thức B.8, mục B.2, phần Phụ lục, giá trị của a_1 phải thỏa mãn điều kiện: $a_1 > (1+\gamma_{\mathrm{th}})a_2$ hoặc $a_1 > (1+\gamma_{\mathrm{th}})/(2+\gamma_{\mathrm{th}}) = 2/3$, do đó tác giả có thể lựa chọn $a_1 = 0.9$ $(a_2 = 0.1)$. Như có thể thấy từ Hình 3.2 rằng các giá trị TS của giao thức Wo-NOMA và NOMA giảm khi tăng Δ và thấp hơn khi nút đích được trang bị bộ kết hợp MRC. Tuy nhiên, tại miền Δ cao, các giá trị TS của giao thức Wo-NOMA hội tụ đến $N_{\mathrm{req}}^{\mathrm{pkt}}$, trong khi giao thức NOMA đạt đến $N_{\mathrm{req}}^{\mathrm{pkt}}/2$. Thực tế rằng tại SNR phát cao, nút đích trong giao thức NOMA có thể đạt được hai gói mã hóa tại mỗi khe thời gian, và do đó nút nguồn chỉ sử dụng $N_{\mathrm{req}}^{\mathrm{pkt}}/2$ khe thời gian cho truyền dữ liệu. Tuy nhiên, chúng ta có thể quan sát rằng giao thức NOMA không thực hiện tốt tại các giá trị Δ thấp khi NOMA sử dụng nhiều khe thời gian hơn giao thức Wo-NOMA. Lưu ý rằng các kết quả mô phỏng hoàn toàn phù hợp với các kết quả lý thuyết để kiểm chứng việc phân tích.

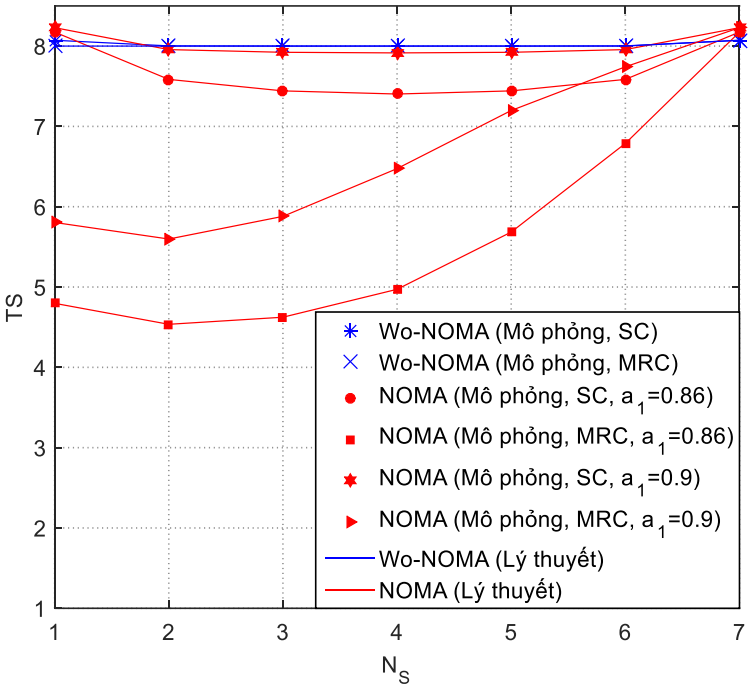


Hình 3.2: Số khe thời gian trung bình như một hàm của $\Delta\ (\mathrm{dB})$ khi $N_S = 1,\ N_D = 3,\ \lambda_{SD} = 2,\ N_{req}^{pkt} = 8,\ a_1 = 0.9,\ \gamma_{th} = 1.$



Hình 3.3: Số khe thời gian trung bình như là một hàm của $\Delta\ (\mathrm{dB})$ khi $N_S = N_D = 2,\ \lambda_{SD} = 3,\ N_{req}^{pkt} = 9,\ a_1 = 0.95,\ \gamma_{th} = 1.$

Hình 3.3 thể hiện các kết quả tương tự như Hình 3.2, cụ thể hiệu năng của giao thức NOMA tốt hơn Wo-NOMA tại các giá trị SNR phát trung bình và cao. Chúng ta cũng thấy từ Hình 3.3 rằng các giá trị TS của Wo-NOMA và NOMA tại các mức Δ cao hội tụ đến $N_{\text{req}}^{\text{pkt}}$ và $\lceil N_{\text{req}}^{\text{pkt}}/2 \rceil$, tương ứng. Thêm vào đó, như thể hiện trong Hình 3.2 và Hình 3.3, hiệu năng TS của Wo-NOMA hội tụ nhanh hơn NOMA.



Hình 3.4: Số khe thời gian trung bình như là hàm của N_{S} khi $\Delta = 8\ (\text{dB})$, $N_{\text{D}} + N_{\text{S}} = 8,\ \lambda_{\text{SD}} = 3,\ N_{\text{req}}^{\text{pkt}} = 8,\ \gamma_{\text{th}} = 1.5.$

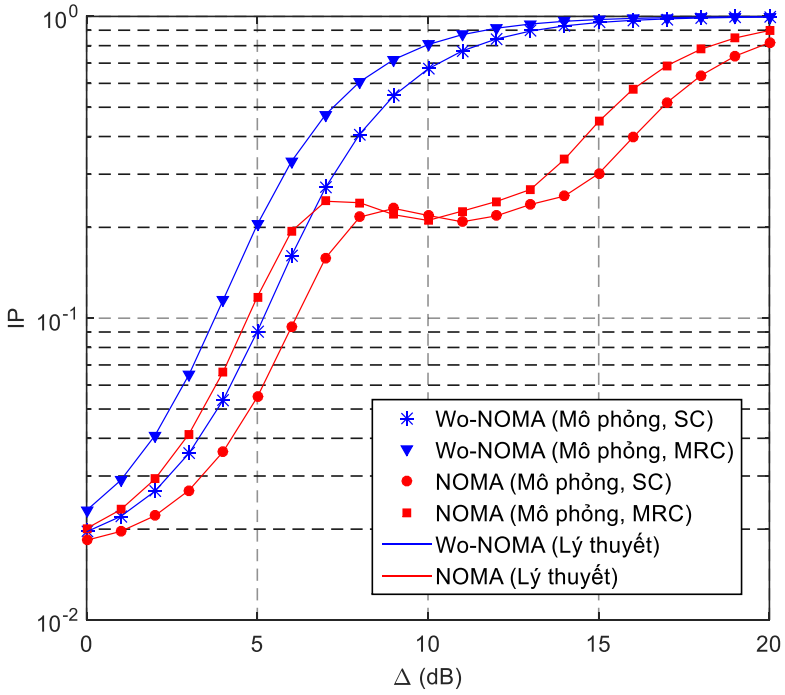
Trong Hình 3.4, tác giả cố định tổng số ăng-ten tại nút nguồn và nút đích, cụ thể $N_{\text{D}} + N_{\text{S}} = 8,$ và thể hiện TS như một hàm của N_{S}. Trong Hình vẽ này, giao thức Wo-NOMA gần như sử dụng 8 khe thời gian cho truyền các gói mã hóa, với tất cả N_{S}. Trong giao thức NOMA, số khe thời gian trung bình biến đổi đáng kể khi thay đổi số ăng-ten N_{S} từ 1 đến 7. Chúng ta có thể thấy rằng với kỹ thuật SC, hiệu năng TS của giao thức NOMA là giống nhau khi số ăng-ten tại nút nguồn là N_{S} và $8 - N_{\text{S}}$. Hơn nữa, trong trường hợp này,

giá trị của TS là thấp nhất khi $N_S = N_D = 4$. Tuy nhiên, trong trường hợp khi nút đích được trang bị với kỹ thuật MRC, giá trị tối ưu của N_S là 2 $(N_D = 6)$, và hiệu năng TS kém nhất khi $N_S = 7$. Do thực tế rằng bộ kết hợp MRC là tốt hơn SC, và do đó nên phân bổ nhiều ăng-ten hơn tại nút đích để tối ưu hiệu năng TS. Cuối cùng, có thể thấy rằng các giá trị TS của giao thức NOMA với $a_1 = 0.86$ $(a_2 = 0.14)$ thấp hơn giá trị $a_1 = 0.9$ $(a_2 = 0.1)$. Điều này được giải thích như sau: Giảm a_2 có nghĩa rằng công suất phát của tín hiệu thứ hai thấp hơn, do vậy giảm xác suất mà nút đích có thể đạt được hai gói mã hóa trong mỗi khe thời gian (xem $\chi_{D,2}$ trong (3.24) và (3.32)), cũng như tăng số khe thời gian trung bình được sử dụng.

3.4.2. Xác suất thu chặn (IP)

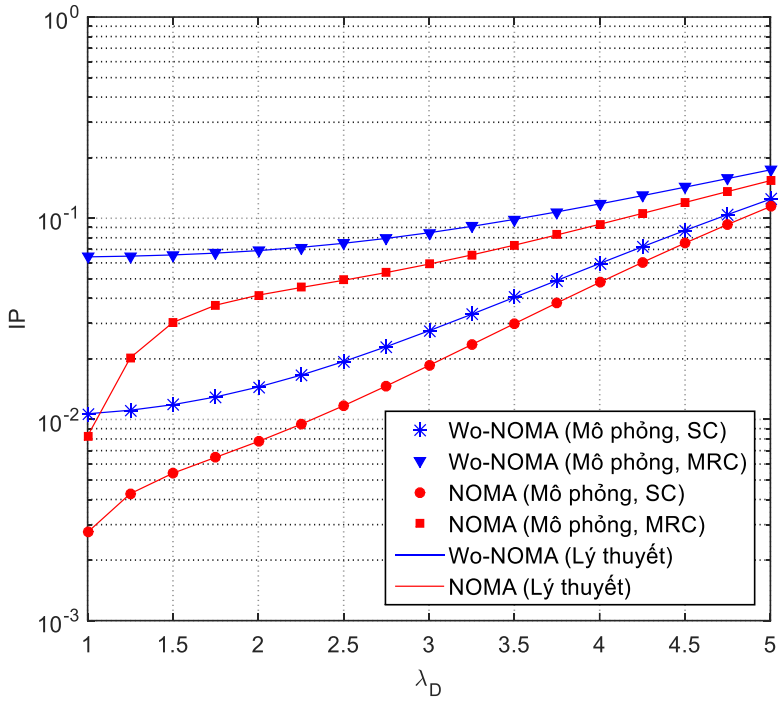
Trong Hình 3.5, Luận án trình bày IP của các giao thức đề xuất là hàm của Δ (dB). Có thể thấy IP của các giao thức Wo-NOMA và NOMA hầu hết tăng khi tăng SNR phát. Do thực tế rằng khi công suất phát của nút nguồn cao, SNR của liên kết nghe lén cũng tăng, điều này làm nâng cao xác suất thu chặn. Tuy nhiên, trong giao thức NOMA thuộc khoảng (8 dB, 10 dB), IP giảm nhẹ khi tăng Δ, và do đó, tồn tại một khoảng hiệu năng cao giữa Wo-NOMA và NOMA trong đoạn này. Bởi vì xác suất thu chặn tại nút nghe lén phụ thuộc vào trạng thái giải mã tại nút đích và nhiễu giữa các tín hiệu, do đó việc thay đổi IP trong giao thức NOMA sẽ phức tạp hơn Wo-NOMA, xét trên khía cạnh Δ SNR phát. Thật vậy, từ (3.16), (3.17), (3.21) và (3.22), có thể quan sát rằng khi Δ tăng, nhiễu từ $x_2[u]$ đến $x_1[u]$ cũng tăng, dẫn đến SNR của $x_1[u]$ đạt được tại các nút D và E tăng chậm. Bởi vì D và E phải giải mã $x_1[u]$ trước, SNR tăng chậm có thể làm IP tăng nhẹ. Tuy nhiên, khi Δ đủ lớn, tất cả các gói mã hóa có thể nhận được chính xác bởi D và E. Trong trường

hợp này, D và E có thể đạt được $N_{\text{req}}^{\text{pkt}}$ gói mã hóa tại cùng thời điểm, và do vậy giá trị IP hội tụ tới 1, như được thể hiện trong Hình 3.5. Tiếp theo, chúng ta có thể quan sát rằng khi nút đích và nút nghe lén sử dụng MRC, các giá trị IP của giao thức đề xuất cao hơn. Bởi vì, khả năng thu chặn của nút nghe lén tốt hơn khi được trang bị MRC. Cuối cùng, có thể nhận thấy rằng giao thức NOMA đạt được hiệu năng IP tốt hơn so với giao thức Wo-NOMA.

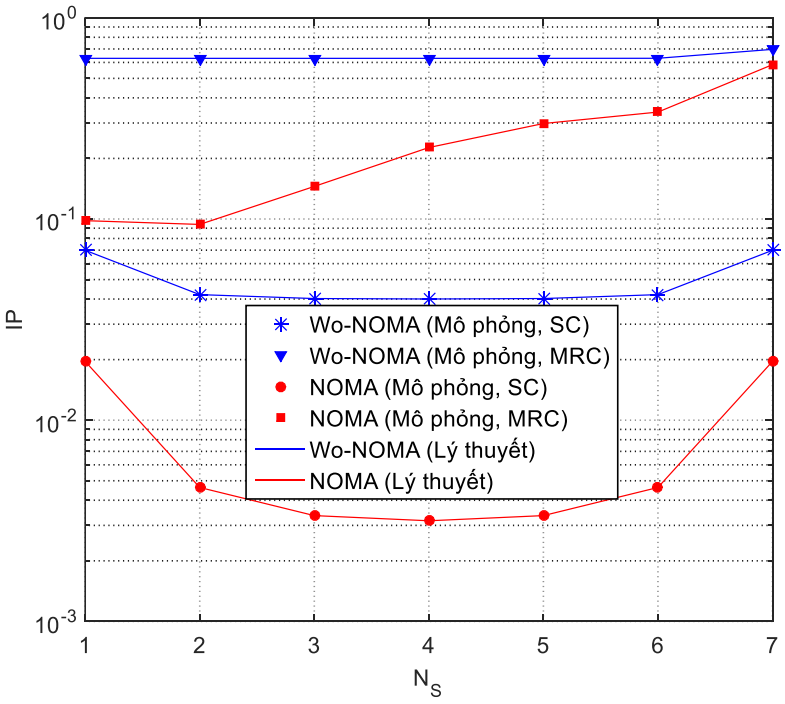


Hình 3.5: Xác suất thu chặn như là một hàm của Δ (dB) khi $N_{\text{S}} = 3$, $N_{\text{D}} = N_{\text{E}} = 2,\ \lambda_{\text{SD}} = \lambda_{\text{SE}} = 2.5,\ N_{\text{req}}^{\text{pkt}} = 8,\ a_1 = 0.9,\ \gamma_{\text{th}} = 1.$

Trong Hình 3.6, tác giả khảo sát ảnh hưởng của tham số liên kết dữ liệu (λ_{SD}) lên hiệu năng IP. Như chúng ta có thể thấy, IP của các giao thức đề xuất tăng khi λ_{SD} tăng. Do thực tế rằng khi chất lượng của kênh dữ liệu xấu hơn (λ_{SD} cao), nút nghe lén có nhiều cơ hội hơn để đạt được đủ số gói mã hóa cho việc khôi phục dữ liệu gốc. Chúng ta cũng có thể thấy rằng hiệu năng IP của giao thức Wo-NOMA là kém hơn giao thức NOMA. Tương tự Hình 3.5, xác suất thu chặn của nút nghe lén tăng khi E sử dụng MRC.

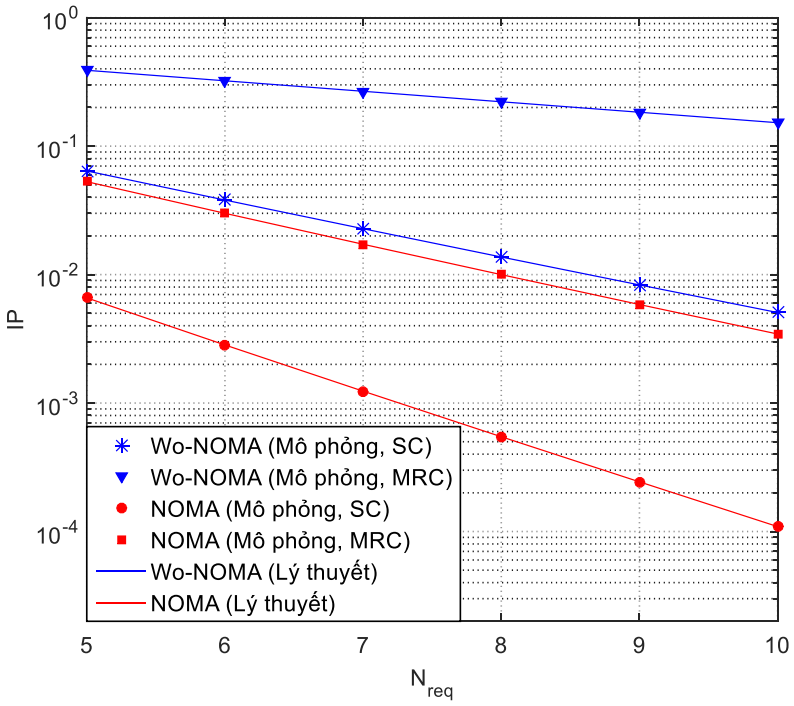


Hình 3.6: Xác suất thu chặn là một hàm của λ_{SD} khi $\Delta = 7$ (dB), $N_S = N_D = N_E = 2,\ \lambda_{SE} = 5,\ N_{req}^{pkt} = 9,\ a_1 = 0.95,\ \gamma_{th} = 1.$

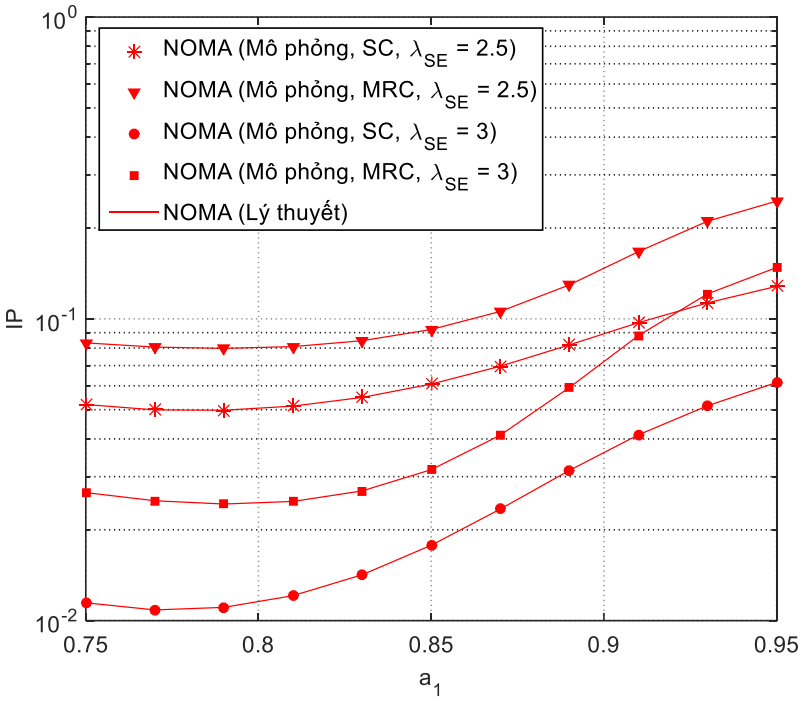


Hình 3.7: Xác suất thu chặn như là một hàm của N_S khi $\Delta = 5$ (dB), $N_S + N_D = 8,\ N_E = 4,\ \lambda_{SD} = 2,\ \lambda_{SE} = 3,\ N_{req}^{pkt} = 8,\ a_1 = 0.9,\ \gamma_{th} = 1.5.$

Hình 3.7 thể hiện IP như một hàm của N_S khi $N_S + N_D = 8$. Tương tự như Hình 3.4, trong trường hợp các nút D và E sử dụng SC, giá trị IP thấp nhất khi $N_S = N_D = 4$, và khi MRC được sử dụng, giá trị tối ưu của N_S là 2. Ta cũng nhận thấy rằng hiệu năng IP của giao thức Wo-NOMA biến đổi nhẹ khi thay đổi N_S, nhưng với giao thức NOMA thì biến đổi đáng kể. Một lần nữa, giao thức NOMA đạt được hiệu năng tốt hơn so với Wo-NOMA. Ngoài ra, chúng ta có thể thấy từ Hình vẽ này rằng khi kỹ thuật MRC được sử dụng bởi nút nghe lén, hiệu năng IP không tốt. Thật vậy, nếu giá trị mong muốn của IP là (dưới) 0.1, có thể thấy thực tế rằng cả Wo-NOMA và NOMA không thể triển khai được. Trong trường hợp này, để giảm IP, nút nguồn có thể giảm công suất phát hoặc thiết kế các tham số hệ thống $N_{\text{req}}^{\text{pkt}}$ và a_1 phù hợp (xem Hình 3.8 và Hình 3.9 phía dưới).



Hình 3.8: Xác suất thu chặn như là một hàm của $N_{\text{req}}^{\text{pkt}}$ khi $\Delta = 5\ (\text{dB})$, $N_S = N_D = N_E = 3,\ \lambda_{SD} = 2,\ \lambda_{SE} = 3,\ a_1 = 0.85,\ \gamma_{\text{th}} = 1.5.$



Hình 3.9: Xác suất thu chặn là một hàm của a_1 khi $\Delta = 7.5\ (\text{dB})$, $N_S = N_D = N_E = 2,\ \lambda_{SD} = 2,\ N_{req}^{pkt} = 8,\ \gamma_{th} = 1.5.$

Trong Hình 3.8, Luận án trình bày IP của các giao thức đề xuất như là một hàm của N_{req}^{pkt}. Để dễ quan sát, tác giả chỉ thay đổi N_{req}^{pkt} từ 5 đến 10. Chúng ta có thể thấy rằng các giá trị của IP giảm khi N_{req}^{pkt} tăng. Do thực tế rằng khi N_{req}^{pkt} cao hơn, xác suất mà nút đích có thể đạt được N_{req}^{pkt} gói mã hóa trước nút nghe lén tăng, do đó có thể giảm xác suất thu chặn tại nút nghe lén. Các kết quả đạt được trong Hình vẽ này có thể được sử dụng để thiết kế mạng xem xét. Ví dụ, giả sử rằng các nút D và E được trang bị bộ kết hợp MRC, và do đó Wo-NOMA không thể sử dụng do giá trị IP cao (lớn hơn 0.1). Thay vì Wo-NOMA, giao thức NOMA có thể được sử dụng để đạt được bảo mật cao hơn cho dữ liệu nguồn. Với ví dụ khác, giả sử rằng hệ thống không thể sử dụng NOMA do giới hạn phần cứng và khả năng xử lý. Trong trường hợp này, nút nguồn trong giao thức Wo-NOMA có thể tăng số gói N_{req}^{pkt} để giảm

IP. Tuy nhiên, lưu ý rằng việc tăng $N_{\text{req}}^{\text{pkt}}$ cũng làm tăng số khe thời gian và thời gian trễ của hệ thống.

Hình 3.9 khảo sát ảnh hưởng các phần của công suất phát (a_1, a_2) lên hiệu năng IP của giao thức NOMA bằng cách thay đổi a_1, và thể hiện IP như một hàm của a_1. Một lần nữa, từ *Nhận xét* của B.8, mục B.2, phần Phụ lục, giá trị a_1 phải được thiết kế sao cho $a_1 > (1+\gamma_{\text{th}})/(2+\gamma_{\text{th}}) = 0.7143$. Do vậy, trong Hình này, tác giả có thể lựa chọn khoảng a_1 là $(0.75, 0.95)$. Như chúng ta có thể thấy, tồn tại các giá trị tối ưu của a_1 tại đó giá trị IP thấp nhất. Ta cũng có thể quan sát rằng các giá trị IP cao hơn khi λ_{SE} giảm, bởi vì độ lợi kênh truyền trung bình của kênh nghe lén lớn hơn.

Lưu ý rằng từ các Hình 3.3-3.9, các kết quả mô phỏng và lý thuyết hoàn toàn trùng khớp nhau, xác nhận tính chính xác của biểu thức IP được đưa ra.

3.5. KẾT LUẬN CHƯƠNG

Chương 3 của Luận án đã thể hiện rằng, áp dụng kỹ thuật NOMA vào các giao thức truyền bảo mật FC không chỉ giảm số khe thời gian được sử dụng mà còn nâng cao bảo mật. Cụ thể, giao thức NOMA có thể giảm một nữa số khe thời gian so với Wo-NOMA. Đối với truyền bảo mật, IP của nút nghe lén giảm đáng kể khi nút nguồn sử dụng NOMA để phát hai gói mã hóa đến nút đích tại mỗi khe thời gian. Để minh họa hiệu năng, Luận án đưa ra các biểu thức chính xác của TS và IP, được xác nhận bằng mô phỏng máy tính. Các kết quả thể hiện rằng hiệu năng của giao thức Wo-NOMA và NOMA có thể được nâng cao đáng kể bằng cách tăng hoặc thiết kế số ăng-ten một cách tối ưu tại nút nguồn và nút đích, lựa chọn thích hợp khoảng công suất phát được phân bổ đến các tín hiệu NOMA và tăng số gói mã hóa được yêu cầu cho việc khôi phục dữ liệu.

Chương 4
HIỆU NĂNG BẢO MẬT TRONG CÁC MẠNG CHUYỂN TIẾP ĐA CHẶNG SỬ DỤNG MÃ FOUNTAIN

4.1. GIỚI THIỆU

Trong Chương 3, Luận án đề xuất và đánh giá hiệu năng của mã Fountain dựa vào các giao thức truyền bảo mật trong các hệ thống vô tuyến MIMO sử dụng và không sử dụng NOMA, trong sự xuất hiện của một nút nghe lén thụ động (passive eavesdropper) trên kênh truyền pha đinh Rayleigh. Trong các giao thức được đề xuất, một nút nguồn chọn lựa ăng-ten tốt nhất của mình để phát các gói mã hóa Fountain đến một nút đích sử dụng kỹ thuật SC hoặc MRC để nâng cao độ tin cậy của việc giải mã. Các kết quả đạt được đã thể hiện rằng giao thức truyền sử dụng FC dựa vào NOMA cho hiệu năng bảo mật tốt hơn so với giao thức không sử dụng NOMA. Hơn nữa, các giao thức chuyển tiếp hai chặng/đa chặng [27], [93, 94], [98] thường được sử dụng để nâng cao tốc độ dữ liệu, mở rộng vùng phủ sóng của mạng, làm giảm thiểu ảnh hưởng của môi trường pha đinh và bù lại tổn thất hiệu năng do công suất phát thấp và phần cứng không hoàn hảo.

Trong Chương này, Luận án đề xuất hai mô hình để phân tích sự đánh đổi giữa hiệu quả bảo mật và độ tin cậy trong các mạng chuyển tiếp đa chặng sử dụng FC, bao gồm: Phần 4.2 trình bày mô hình đề xuất mạng chuyển tiếp đa chặng sử dụng mã Fountain với kỹ thuật thu thập năng lượng sóng vô tuyến từ trạm Beacon (EH-Beacon) dưới tác động của suy giảm phần cứng và Phần 4.3 đánh giá mô hình đề xuất của giao thức đa chặng LEACH sử dụng mã Fountain và gây nhiễu cộng tác.

Trong mô hình đề xuất ở Phần 4.2, một nút nguồn mã hóa dữ liệu của mình bởi mã Fountain và gửi những gói mã hóa tới một nút đích dựa vào các

nút chuyển tiếp trung gian, một nút nghe lén xuất hiện xung quanh nút đích cố gắng nhận các gói mã hóa nhằm khôi phục dữ liệu gốc. Đóng góp chính của mô hình đề xuất trong Phần 4.2, có thể được tóm tắt như sau:

• Luận án xem xét một mô hình thực tế với phần cứng máy thu/phát của tất cả các nút là không hoàn hảo do nhiễu pha, không cân bằng I/Q và bộ khuếch đại không tuyến tính [67, 68], [93, 94]. Do đó, tác giả đã khảo sát ảnh hưởng của suy giảm phần cứng lên hiệu năng hệ thống;

• Nghiên cứu mô hình kênh pha đinh không đối xứng, cụ thể các kênh dữ liệu và kênh nghe lén là pha đinh Rice, trong khi các kênh thu thập năng lượng sóng vô tuyến là kênh pha đinh Rayleigh. Thực tế là các nút trên đường truyền giữa nút nguồn và nút đích có thể được đặt tại các vị trí theo kế hoạch bởi nhà khai thác mạng, do đó các liên kết giữa chúng thực tế trong tầm nhìn thẳng (Line of Sight: LOS) [106, 107];

• Luận án đưa ra các biểu thức dạng chính xác của xác suất dừng (OP) và xác suất thu chặn (IP) dựa vào EH-Beacon trên kênh truyền pha đinh Rayleigh dưới tác động của suy giảm phần cứng, để đánh giá sự đánh đổi giữa bảo mật và độ tin cậy cho phương pháp đề xuất. Các mô phỏng Monte Carlo được trình bày để kiểm chứng các kết quả phân tích.

Mô hình đề xuất trong Phần 4.3, Luận án khảo sát sự đánh đổi giữa bảo mật và độ tin cậy của mạng phân cấp theo cụm thích ứng năng lượng thấp (LEACH) dựa trên mã Fountain, trong đó các gói mã hóa được gửi đến nút đích sử dụng truyền đa chặng thông qua các cụm trung gian, với sự hỗ trợ của các nút chủ cụm (CH). Để bảo đảm an toàn truyền dữ liệu dưới sự tấn công của nút nghe lén, mỗi cụm (cluster) lựa chọn ngẫu nhiên một nút cụm để thực hiện hoạt động gây nhiễu cộng tác. Để đánh giá hiệu năng, Luận án đưa ra các biểu thức chính xác dạng tường minh của xác suất dừng (OP) và xác suất thu chặn (IP) trên kênh truyền pha đinh Rayleigh. Sau đó, thực hiện mô phỏng

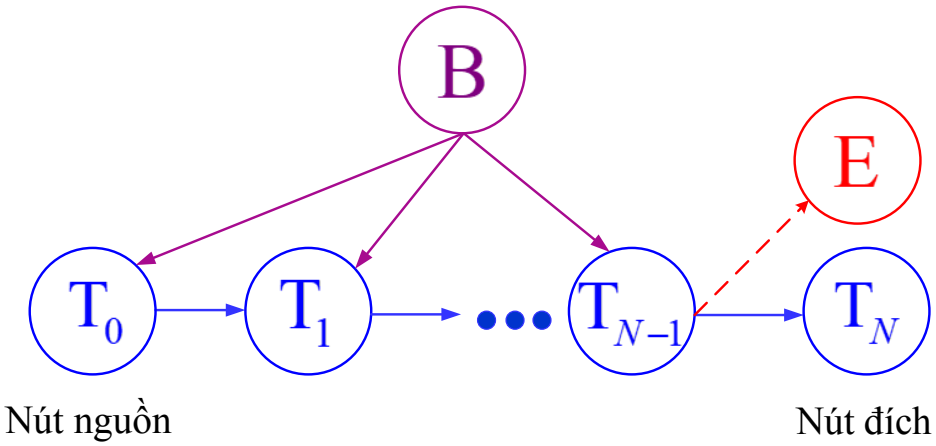
máy tính để kiểm chứng các kết quả lý thuyết và so sánh hiệu năng của giao thức đề xuất với LEACH truyền thống mà không sử dụng gây nhiễu.

Phần còn lại của Chương này được tổ chức như sau: Mô hình đề xuất 1 được miêu tả trong Phần 4.2 và mô hình đề xuất 2 được trình bày ở Phần 4.3, trong đó đưa ra các biểu thức của IP, OP và các kết quả mô phỏng được thể hiện. Cuối cùng, nội dung của Chương được kết luận trong Phần 4.4.

Đóng góp của Chương 4 được trình bày trong các công trình A4 và A5.

4.2. MÔ HÌNH 1: MẠNG CHUYỂN TIẾP ĐA CHẶNG SỬ DỤNG MÃ FOUNTAIN VỚI THU THẬP NĂNG LƯỢNG SÓNG VÔ TUYẾN

4.2.1. Mô hình hệ thống



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

Như thể hiện trong Hình 4.1, nút nguồn (T_0) muốn gửi dữ liệu của mình tới nút đích (T_N) dựa vào $N-1$ nút chuyển tiếp, biểu thị bởi $T_1, T_2, ..., T_{N-1}$. Giả sử rằng các máy phát như nút nguồn và nút chuyển tiếp là các thiết bị vô tuyến bị ràng buộc mức năng lượng, nên phải thu thập năng lượng từ trạm phát sóng vô tuyến (Beacon: B) được triển khai trong mạng nhằm giúp các nút có thể thu thập năng lượng. Trong mạng này, nút nghe lén (Eavesdropper: E) xuất hiện xung quanh nút đích, do đó E có thể nghe lén dữ liệu được phát đến nút này. Bởi vì nút nghe lén gần với nút đích, Luận án giả sử rằng nút E

chỉ nhận được dữ liệu phát từ nút chuyển tiếp T_{N-1}. Giả sử rằng tất cả các thiết bị đầu cuối chỉ có đơn ăng-ten và hoạt động ở chế độ bán song công (half-duplex). Do đó, phương pháp TDMA có thể được sử dụng để gửi các gói mã hóa từ nút nguồn đến nút đích dựa vào *N* khe thời gian trực giao.

Tương tự như phần trình bày ở Chương 2 và Chương 3, trong hệ thống sử dụng FC, nút nguồn chia dữ liệu gốc thành *L* gói có độ dài bằng nhau và thực hiện phép XOR với nhau để tạo ra các gói Fountain. Tiếp theo, nút nguồn gửi mỗi gói mã hóa đến nút đích với sự trợ giúp của các nút chuyển tiếp trung gian. Xem xét hệ thống ràng buộc thời gian trễ với số khe thời gian tối đa có thể được sử dụng để phát các gói mã hóa bị giới hạn bởi $N_{\max}$, có nghĩa rằng nút nguồn sẽ dừng truyền sau khi gửi $N_{\max}$ gói Fountain tới nút đích. Để khôi phục dữ liệu nguồn, nút đích và nút nghe lén phải nhận thành công ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa trong $N_{\max}$ khe thời gian, với $N_{\text{req}}^{\text{pkt}} = (1+\varepsilon)L$ và $N_{\text{req}}^{\text{pkt}} \le N_{\max}$. Ta có $N_{\text{D}}^{\text{pkt}}$ và $N_{\text{E}}^{\text{pkt}}$ là số gói mã hóa mà nút đích và nút nghe lén có thể đạt được sau $N_{\max}$ khe thời gian, tương ứng. Nếu $N_{\text{D}}^{\text{pkt}} \ge N_{\text{req}}^{\text{pkt}}$, nút đích có thể khôi phục hoàn toàn dữ liệu gốc. Ngược lại, nếu $N_{\text{D}}^{\text{pkt}} < N_{\text{req}}^{\text{pkt}}$, sự kiện dừng có thể xảy ra. Đối với trạng thái giải mã tại nút E, nếu $N_{\text{E}}^{\text{pkt}} \ge N_{\text{req}}^{\text{pkt}}$, dữ liệu nguồn bị thu chặn và nếu $N_{\text{E}}^{\text{pkt}} < N_{\text{req}}^{\text{pkt}}$, truyền dữ liệu được bảo mật.

4.2.1.1. Mô hình kênh truyền

Giả sử các kênh EH thực nghiệm là kênh truyền pha đinh Rayleigh, bởi vì không có LOS (Non-Line-of-Sight) giữa trạm Beacon và các máy phát. Độ lợi kênh truyền $\gamma_{\text{B},n}$ là biến ngẫu nhiên có hàm CDF và PDF tương ứng là

$$F_{\gamma_{\text{B},n}}(x) = 1 - \exp\left(-\lambda_{\text{B},n} x\right),\ f_{\gamma_{\text{B},n}}(x) = \lambda_{\text{B},n} \exp\left(-\lambda_{\text{B},n} x\right), \tag{4.1}$$

trong đó $\lambda_{\text{B},n}$ là tham số được cho như trong [108]:

$$\lambda_{\text{B},n} = l_n^{\beta}, \tag{4.2}$$

với β là hệ số suy hao hàm mũ và l_n là khoảng cách giữa B và T_n.

Bởi vì kênh truyền giữa T_n và T_{n+1} là kênh pha đinh Rice, hàm CDF và PDF của $\gamma_{\mathrm{D},n}$ được cho, tương ứng như trong [106]:

$$F_{\gamma_{\mathrm{D},n}}(x) = 1 - Q_1\left(\sqrt{2K_{\mathrm{D}}}, \sqrt{2(1+K_{\mathrm{D}})\lambda_{\mathrm{D},n}x}\right),$$

$$f_{\gamma_{\mathrm{D},n}}(x) = (1+K_{\mathrm{D}})\lambda_{\mathrm{D},n}\exp(-K_{\mathrm{D}}) \times \exp\left(-(1+K_{\mathrm{D}})\lambda_{\mathrm{D},n}x\right) I_0\left(2\sqrt{K_{\mathrm{D}}(1+K_{\mathrm{D}})\lambda_{\mathrm{D},n}x}\right), \quad (4.3)$$

với $Q_1(.)$ là hàm Marcum-Q [109], $I_0(.)$ là hàm Bessel sửa đổi loại 1 [110], K_{D} là hệ số K Rice của tất cả các liên kết dữ liệu và tham số $\lambda_{\mathrm{D},n}$ được mô hình hóa như trong (4.2): $\lambda_{\mathrm{D},n} = d_n^{\beta}$, với d_n là khoảng cách giữa T_n và T_{n+1}.

Tương tự, hàm CDF và PDF của γ_{E} được viết, tương ứng là

$$F_{\gamma_{\mathrm{D},n}}(x) = 1 - Q_1\left(\sqrt{2K_{\mathrm{E}}}, \sqrt{2(1+K_{\mathrm{E}})\lambda_{\mathrm{E}}x}\right),$$

$$f_{\gamma_{\mathrm{D},n}}(x) = (1+K_{\mathrm{E}})\lambda_{\mathrm{E}}\exp(-K_{\mathrm{E}}) \times \exp\left(-(1+K_{\mathrm{E}})\lambda_{\mathrm{E}}x\right) I_0\left(2\sqrt{K_{\mathrm{E}}(1+K_{\mathrm{E}})\lambda_{\mathrm{E}}x}\right), \quad (4.4)$$

với K_{E} là hệ số K Rice của liên kết $\mathrm{T}_{N-1} \to \mathrm{E}$, $\lambda_{\mathrm{E}} = d_{\mathrm{E}}^{\beta}$ và d_{E} là khoảng cách giữa T_{N-1} và E.

Ngoài ra, với sự trợ giúp của [110, công thức (8.445)], ta có thể biểu diễn $f_{\gamma_{\mathrm{D},n}}(x)$ trong (4.3) bởi một chuỗi vô hạn là

$$f_{\gamma_{\mathrm{D},n}}(x) = \exp(-K_{\mathrm{D}})\sum_{k=0}^{+\infty}\frac{1}{(k!)^2}(K_{\mathrm{D}})^k \times \left((1+K_{\mathrm{D}})\lambda_{\mathrm{D},n}\right)^{k+1} x^k \exp\left(-(1+K_{\mathrm{D}})\lambda_{\mathrm{D},n}x\right). \quad (4.5)$$

4.2.1.2. Dung lượng kênh truyền từ đầu cuối đến đầu cuối

Đặt τ là tổng thời gian truyền của mỗi gói Fountain từ nút nguồn đến nút đích. Bằng cách sử dụng giao thức chuyển mạch thời gian, tương tự [90-

94], khoảng thời gian $\alpha\tau\left(0\le\alpha\le1\right)$ được sử dụng cho nút nguồn và các nút chuyển tiếp thu thập năng lượng từ trạm Beacon và khoảng thời gian còn lại $\left(1-\alpha\right)\tau$ được sử dụng cho truyền dữ liệu. Bởi vì quá trình truyền dữ liệu được chia thành *N* khe thời gian trực giao, mỗi khe thời gian truyền gói mã hóa có thể được phân bổ giống nhau bởi $\left(1-\alpha\right)\tau$ / *N*.

Tiếp theo, năng lượng được thu thập bởi nút T_n được xác định là

$$Q_n=\eta\alpha\tau P_{\mathrm{B}}\gamma_{\mathrm{B},n}, \tag{4.6}$$

với $n=0,1,...,N-1,\ \eta\left(0\le\eta\le1\right)$ là hiệu suất chuyển đổi năng lượng, P_{B} là công suất phát của B và $\gamma_{\mathrm{B},n}$ là độ lợi kênh truyền của liên kết của $\mathrm{B}\to\mathrm{T}_n$.

Từ (4.6), công suất phát trung bình của T_n được tính bởi

$$P_n=\frac{Q_n}{\left(1-\alpha\right)\tau/N}=\omega P_{\mathrm{B}}\gamma_{\mathrm{B},n}, \tag{4.7}$$

với

$$\omega=\frac{N\eta\alpha}{1-\alpha}. \tag{4.8}$$

Tiếp theo, dưới ảnh hưởng của suy giảm phần cứng, tốc độ dữ liệu tức thời của liên kết $\mathrm{T}_n\to\mathrm{T}_{n+1}$ có thể được cho là

$$\begin{aligned}C_n&=\frac{\left(1-\alpha\right)\tau}{N}\log_2\left(1+\frac{P_n\gamma_{\mathrm{D},n}}{\kappa_{\mathrm{D}}^2P_n\gamma_{\mathrm{D},n}+\sigma^2}\right)\\&=\frac{\left(1-\alpha\right)\tau}{N}\log_2\left(1+\frac{\omega\Delta\gamma_{\mathrm{B},n}\gamma_{\mathrm{D},n}}{\kappa_{\mathrm{D}}^2\omega\Delta\gamma_{\mathrm{B},n}\gamma_{\mathrm{D},n}+1}\right),\end{aligned} \tag{4.9}$$

với $\gamma_{\mathrm{D},n}$ là độ lợi kênh truyền của liên kết $\mathrm{T}_n\to\mathrm{T}_{n+1}$, κ_{D}^2 là tổng mức suy giảm phần cứng lên tất cả các kênh dữ liệu [93, 94], [98], σ^2 là phương sai của nhiễu Gauss tại tất cả các máy thu và $\Delta=P_{\mathrm{B}}/\sigma^2$ là SNR phát.

Sử dụng kỹ thuật DF [91], [108], thì chặng yếu nhất quyết định hiệu năng toàn trình, do đó dung lượng kênh truyền đầu cuối đến đầu cuối của liên kết dữ liệu được tính là

$$C_{\mathrm{D}} = \min_{n=1,2,\ldots,N} \left(C_n\right). \tag{4.10}$$

Tương tự (4.9), tốc độ dữ liệu tức thời của liên kết $\mathrm{T}_{N-1} \to \mathrm{E}$ được cho là

$$C_{\mathrm{Eav}} = \frac{(1-\alpha)\tau}{N} \log_2 \left(1 + \frac{\omega \Delta \gamma_{\mathrm{B},n} \gamma_{\mathrm{E}}}{\kappa_{\mathrm{E}}^2 \omega \Delta \gamma_{\mathrm{B},n} \gamma_{\mathrm{E}} + 1}\right), \tag{4.11}$$

với γ_{E} là độ lợi kênh truyền của liên kết $\mathrm{T}_{N-1} \to \mathrm{E}$ và κ_{E}^2 là tổng mức suy giảm phần cứng của liên kết kênh nghe lén.

Cũng vậy, ta có thể tính toán dung lượng kênh truyền đầu cuối đến đầu cuối của liên kết kênh nghe lén là

$$C_{\mathrm{E}} = \min_{n=1,2,\ldots,N-1} \left(C_n, C_{\mathrm{Eav}}\right). \tag{4.12}$$

Mỗi gói Fountain có thể được giải mã thành công nếu tốc độ dữ liệu đầu cuối đến đầu cuối cao hơn một tốc độ mong muốn được xác định trước, C_{th}. Ngược lại, gói Fountain không thể được nhận chính xác. Do đó, xác suất mà nút đích không thể nhận chính xác một gói mã hóa được cho là

$$\rho_{\mathrm{D}} = \Pr\left(C_{\mathrm{D}} < C_{\mathrm{th}}\right). \tag{4.13}$$

Lưu ý rằng xác suất giải mã thành công mỗi gói Fountain là $\Pr\left(C_{\mathrm{D}} \geq C_{\mathrm{th}}\right) = 1 - \rho_{\mathrm{D}}$. Tương tự, xác suất một gói Fountain có thể được nhận không chính xác và chính xác bởi nút nghe lén có thể được cho, tương ứng là

$$\rho_{\mathrm{E}} = \Pr\left(C_{\mathrm{E}} < C_{\mathrm{th}}\right),$$

$$\Pr\left(C_{\mathrm{E}} \geq C_{\mathrm{th}}\right) = 1 - \rho_{\mathrm{E}}. \tag{4.14}$$

Xác suất dừng (OP) tại nút đích và xác suất thu chặn (IP) tại nút nghe lén được tính bởi

$$\mathrm{OP} = \Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} < N_{\mathrm{req}}^{\mathrm{pkt}} \mid N_{\max}\right), \quad \mathrm{IP} = \Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}} \geq N_{\mathrm{req}}^{\mathrm{pkt}} \mid N_{\max}\right). \tag{4.15}$$

4.2.2. Phân tích hiệu năng

4.2.2.1. Xác suất của ρ_{D} và ρ_{E}

Bổ đề 1: Nếu $1-\kappa_{\mathrm{D}}^2\chi \le 0,$ thì $\rho_{\mathrm{D}}=1$ và nếu $1-\kappa_{\mathrm{D}}^2\chi > 0,$ ρ_{D} có thể được biểu diễn dưới dạng chính xác là

$$\rho_{\mathrm{D}} = 1-\prod_{n=1}^{N}\left[\sum_{k=0}^{+\infty}\frac{2}{\left(k!\right)^2}\left(K_{\mathrm{D}}\right)^k \exp\left(-K_{\mathrm{D}}\right)\left(\psi_n\right)^{\frac{k+1}{2}} K_{t+1}\left(2\sqrt{\psi_n}\right)\right]. \qquad (4.16)$$

Chứng minh: Xem chứng minh và các ký hiệu trong mục C1, Phụ lục C.

Bổ đề 2: Nếu $1-\kappa_{\mathrm{E}}^2\chi \le 0,$ thì $\rho_{\mathrm{E}}=1$ và nếu $1-\kappa_{\mathrm{E}}^2\chi > 0,$ ρ_{E} được biểu diễn dưới dạng chính xác là

$$\rho_{\mathrm{E}} = 1-\left[\prod_{n=1}^{N-1}\left(\begin{array}{l}\displaystyle\sum_{k=0}^{+\infty}\frac{2}{\left(k!\right)^2}\left(K_{\mathrm{D}}\right)^k \exp\left(-K_{\mathrm{D}}\right)\times\left(\left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{B},n}\lambda_{\mathrm{D},n}\theta_{\mathrm{D}}\right)^{\frac{k+1}{2}} \\ \times K_{t+1}\left(2\sqrt{\left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{B},n}\lambda_{\mathrm{D},n}\theta_{\mathrm{D}}}\right)\end{array}\right)\right]$$
$$\times\left(\sum_{k=0}^{+\infty}\frac{2}{\left(k!\right)^2}\left(K_{\mathrm{E}}\right)^k \exp\left(-K_{\mathrm{E}}\right)\left(\psi_{\mathrm{E}}\right)^{\frac{k+1}{2}} K_{t+1}\left(2\sqrt{\psi_{\mathrm{E}}}\right)\right). \qquad (4.17)$$

Chứng minh: Xem chứng minh và các ký hiệu trong mục C1, Phụ lục C.

4.2.2.2. Xác suất dừng và xác suất thu chặn

Từ (4.15), biểu thức chính xác của OP có thể được cung cấp như sau:

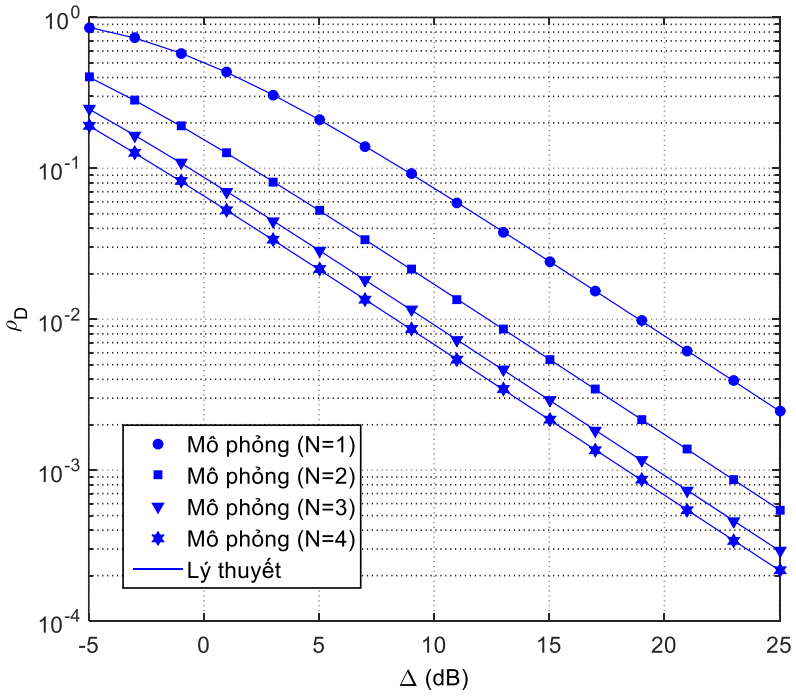
$$\mathrm{OP} = \sum_{N_{\mathrm{D}}^{\mathrm{pkt}}=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} C_{N_{\max}}^{N_{\mathrm{D}}^{\mathrm{pkt}}} \rho_{\mathrm{D}}^{N_{\mathrm{D}}^{\mathrm{pkt}}} \left(1-\rho_{\mathrm{D}}\right)^{N_{\max}-N_{\mathrm{D}}^{\mathrm{pkt}}}. \qquad (4.18)$$

Biểu thức (4.18) ngụ ý rằng nút đích không thể khôi phục dữ liệu gốc của nút nguồn bởi vì số gói Fountain nhận được ít hơn $N_{\mathrm{req}}^{\mathrm{pkt}},$ các giá trị có khả năng của $N_{\mathrm{D}}^{\mathrm{pkt}}$ là từ 0 đến $N_{\mathrm{req}}^{\mathrm{pkt}}-1$ và có $C_{N_{\max}}^{N_{\mathrm{D}}^{\mathrm{pkt}}}$ trường hợp cho mỗi giá trị của $N_{\mathrm{D}}^{\mathrm{pkt}}.$ Cũng vậy, xác suất thu chặn (IP) có thể được tính là

$$\mathrm{IP} = \sum_{N_{\mathrm{E}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}}^{N_{\max}} C_{N_{\max}}^{N_{\mathrm{E}}^{\mathrm{pkt}}} \rho_{\mathrm{E}}^{N_{\mathrm{E}}^{\mathrm{pkt}}} \left(1-\rho_{\mathrm{E}}\right)^{N_{\max}-N_{\mathrm{E}}^{\mathrm{pkt}}}. \qquad (4.19)$$

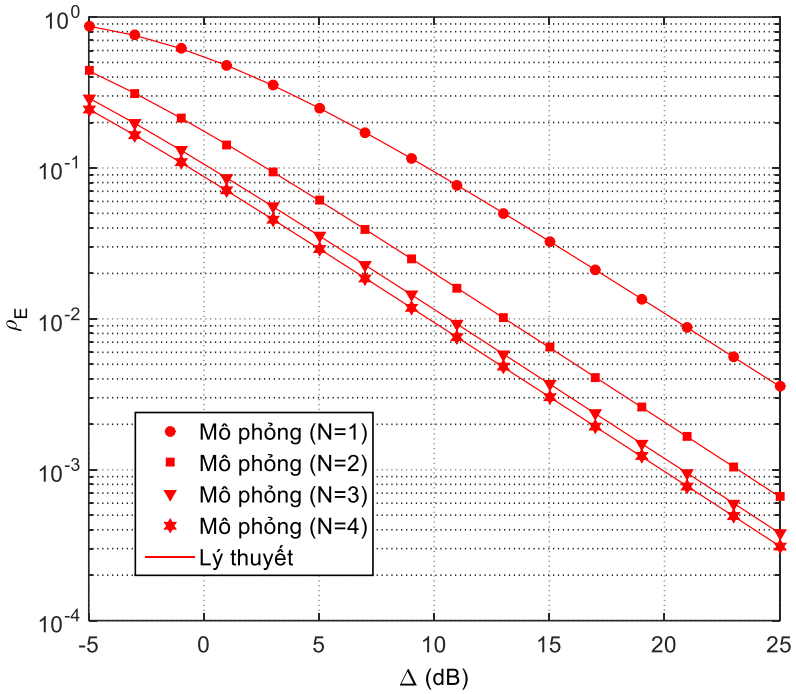
4.2.3. Các kết quả mô phỏng

Trong phần này, tác giả thực hiện các mô phỏng Monte Carlo để kiểm chứng kết quả phân tích lý thuyết được đưa ra trong phần trước.



Hình 4.2: ρ_{D} là hàm của $\Delta\,(\mathrm{dB})$ khi $K_{\mathrm{D}}=10,\ K_{\mathrm{E}}=5,\ \kappa_{\mathrm{D}}^2=\kappa_{\mathrm{E}}^2=0.01,$ $\alpha=0.25$ và $C_{\mathrm{th}}=0.5.$

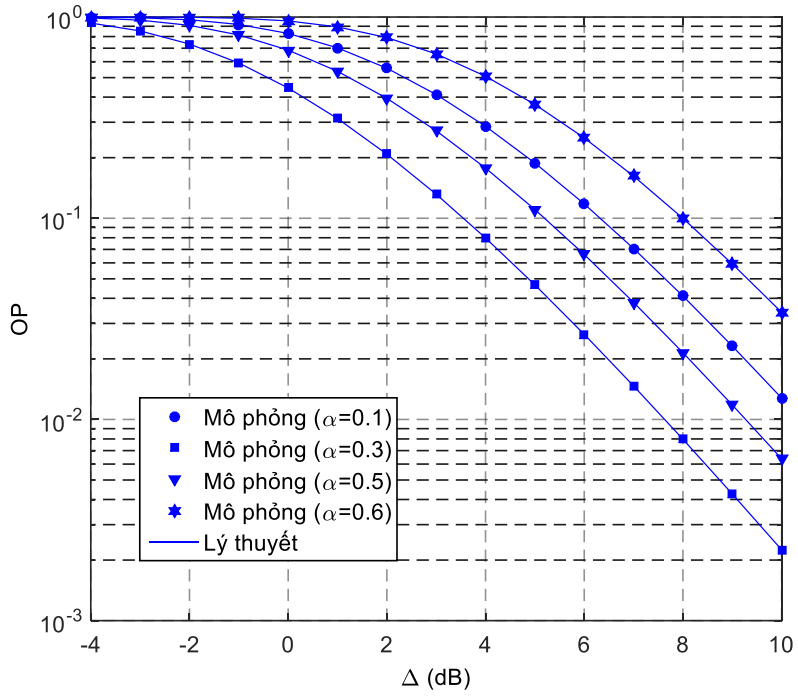
Luận án xem xét một hệ trục tọa độ hai chiều Oxy trong đó tọa độ của nút T_n và B là $(n/N,0)$ và $(0.5,\ 0.5)$, tương ứng, với $n=0,1,...,N$. Do đó, nút nguồn được đặt tại gốc tọa độ $(0,0)$, trong khi nút đích được đặt tại $(1,0)$. Bởi vì nút nghe lén ở gần nút đích, vị trí của nút này được giả sử là $(1,\ 0.2)$. Trong tất cả các mô phỏng, tác giả cố định các giá trị của hệ số suy hao hàm mũ (β), số gói Fountain được yêu cầu để khôi phục dữ liệu gốc $\left(N_{\mathrm{req}}^{\mathrm{pkt}}\right)$, tổng thời gian truyền của mỗi khe thời gian (τ) và hiệu suất chuyển đổi năng lượng (η) bằng 3, 5, 1 và 1, tương ứng. Ngoài ra, để thể hiện các kết quả lý thuyết, chuỗi vô cùng được cắt bởi 50 giá trị đầu tiên.



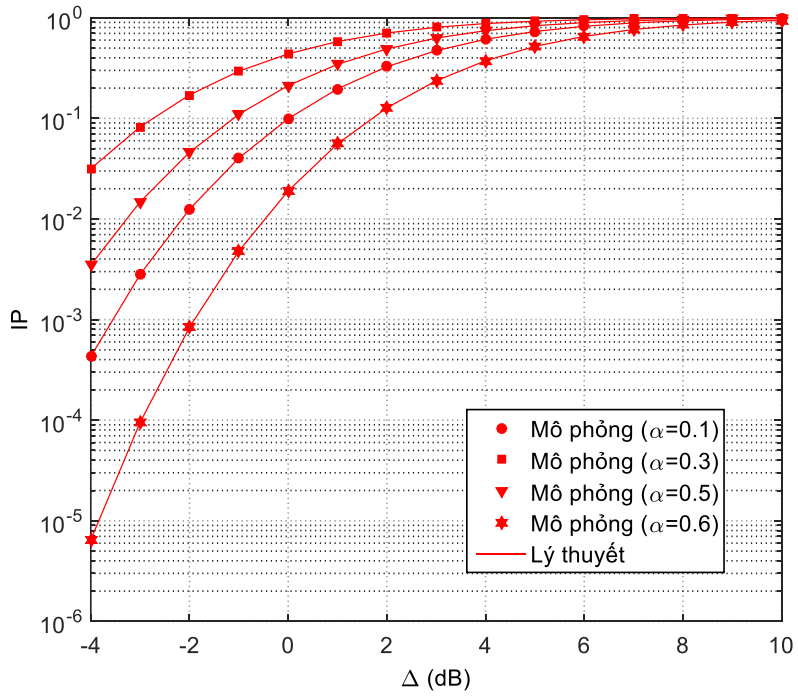
Hình 4.3: ρ_E là hàm của Δ (dB) khi $K_D = 10,\ K_E = 5,\ \kappa_D^2 = \kappa_E^2 = 0.01,$ $\alpha = 0.25$ và $C_{th} = 0.5.$

Các Hình 4.2 và Hình 4.3 thể hiện ρ_D và ρ_E như là hàm của SNR phát Δ (dB) với số chặng (N). Các kết quả thể hiện rằng ρ_D và ρ_E giảm khi tăng Δ và N. Các kết quả mô phỏng và lý thuyết là hoàn toàn trùng khít nhau, thể hiện tính đúng đắn của các kết quả phân tích trong Phần 4.2.2.

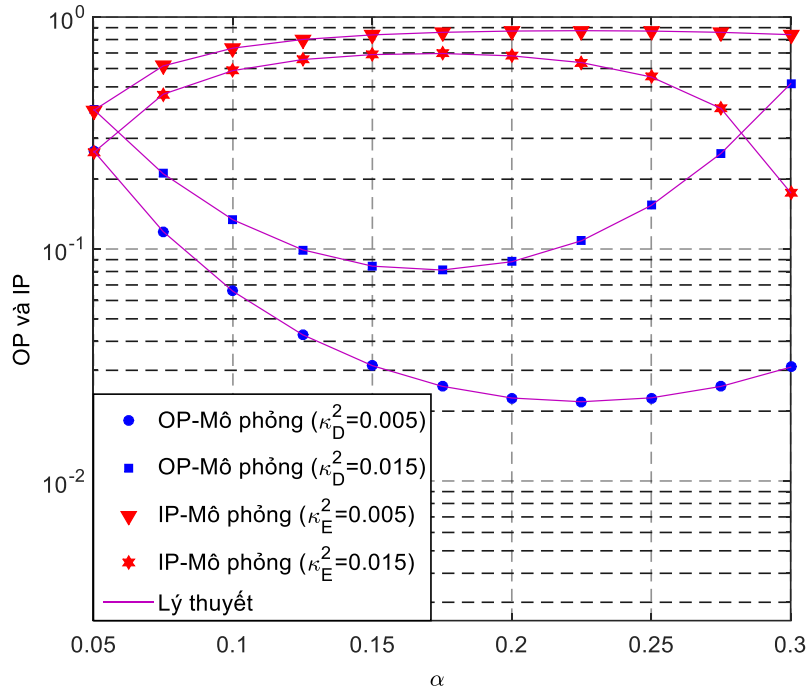
Trong các Hình 4.4-4.5, tác giả khảo sát sự đánh đổi giữa bảo mật và độ tin cậy. Như có thể quan sát, OP trong Hình 4.4 giảm khi tăng SNR phát (Δ). Tuy nhiên, như thể hiện trong Hình 4.5, IP tăng nhanh với các giá trị Δ cao. Có thể thấy trong Hình 4.5 rằng khi Δ cao hơn 6 dB, thông tin gốc gần như bị thu chặn, tức là $\text{IP} \approx 1$. Các Hình 4.4 và 4.5 cũng thể hiện ảnh hưởng của khoảng thời gian được phân bổ đến pha thu thập năng lượng lên các giá trị của OP và IP. Cụ thể, OP là thấp nhất và cao nhất với giá trị $\alpha = 0.3$ và $\alpha = 0.6,$ trong khi khả năng thu chặn của nút nghe lén là tốt nhất và xấu nhất tại $\alpha = 0.3$ và $\alpha = 0.6,$ tương ứng.



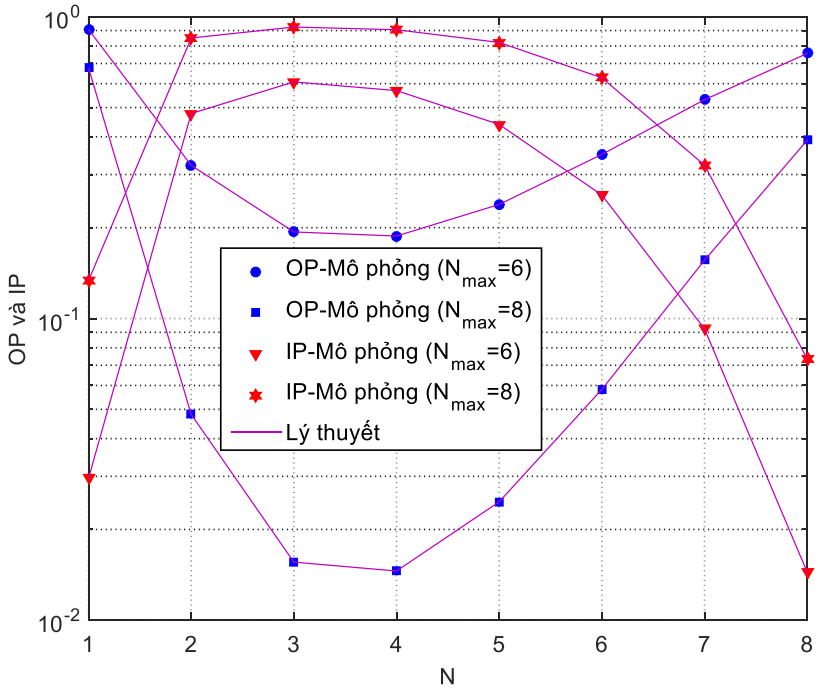
Hình 4.4: OP là hàm của Δ (dB) khi $N=3,\ K_{\mathrm{D}}=10,\ K_{\mathrm{E}}=5,\ \kappa_{\mathrm{D}}^2=\kappa_{\mathrm{E}}^2=0,$ $C_{\mathrm{th}}=1,\ N_{\max}=7$ và $N_{\mathrm{req}}^{\mathrm{pkt}}=5.$



Hình 4.5: IP là hàm của Δ (dB) khi $N=3,\ K_{\mathrm{D}}=10,\ K_{\mathrm{E}}=5,\ \kappa_{\mathrm{D}}^2=\kappa_{\mathrm{E}}^2=0,$ $C_{\mathrm{th}}=1,\ N_{\max}=7$ và $N_{\mathrm{req}}^{\mathrm{pkt}}=5.$



Hình 4.6: OP và IP như là hàm của α khi $\Delta = 5\,\text{dB}$, $N = 4$, $K_D = 20$, $K_E = 1$, $C_{th} = 1$, $N_{max} = 8$ và $N_{req}^{pkt} = 5$.



Hình 4.7: OP và IP là hàm của N khi $\Delta = 3\,\text{dB}$, $K_D = 20$, $K_E = 1$, $\kappa_D^2 = \kappa_E^2 = 0$, $C_{th} = 0.9$ và $N_{req}^{pkt} = 5$.

Hình 4.6 thể hiện OP và IP là hàm của α với các mức suy giảm phần cứng khác nhau. Như quan sát, tồn tại các giá trị của α để OP là nhỏ nhất và IP là lớn nhất. Ví dụ, khi $\kappa_D^2 = \kappa_E^2 = 0.015,$ hiệu năng dừng tốt nhất và khả năng thu chặn cao nhất có thể đạt được tại $\alpha = 0.175.$ Cũng thấy trong các hình vẽ này rằng OP cao hơn và IP thấp hơn khi các mức suy giảm phần cứng κ_D^2 và κ_E^2 tăng.

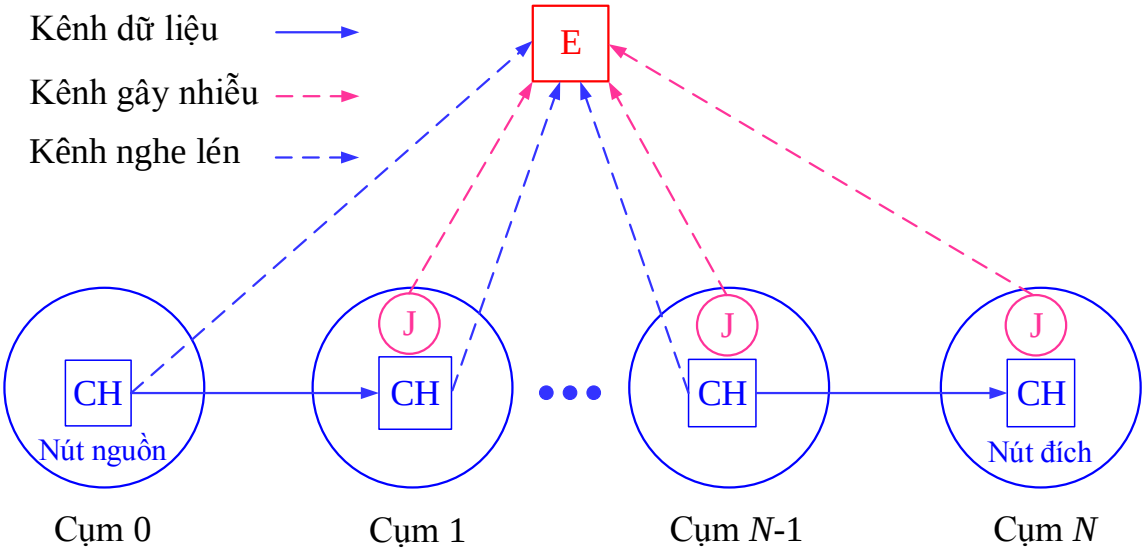
Trong Hình 4.7, Luận án khảo sát ảnh hưởng của số lượng các chặng đến giá trị của OP và IP. Trong hình này, giá trị tối ưu của OP đạt được tại $N = 4.$ Chúng ta cũng thấy rằng khi tăng giá trị của $N_{\max}$ từ 6 đến 8, OP giảm đáng kể. Tuy nhiên, tăng số khe thời gian được sử dụng cho việc truyền các gói Fountain $\left(N_{\max}\right)$ cũng làm tăng xác suất thu chặn, bởi vì nút nghe lén có nhiều cơ hội hơn để nhận đủ số gói mã hóa.

Từ các Hình 4.4-4.7, chúng ta có thể thấy rằng các kết quả mô phỏng là hoàn toàn phù hợp với kết quả lý thuyết, một lần nữa chứng minh tính đúng đắn kết quả phân tích.

4.3. MÔ HÌNH 2: GIAO THỨC CHUYỂN TIẾP ĐA CHẶNG LEACH SỬ DỤNG MÃ FOUNTAIN VÀ NÚT GÂY NHIỄU CỘNG TÁC

4.3.1. Mô hình hệ thống

Hình 4.8 thể hiện mô hình hệ thống của giao thức đề xuất, với một nút nguồn (CH của cụm 0) muốn truyền dữ liệu của mình đến một nút đích (CH của cụm *N*) dựa vào giao thức chuyển tiếp đa chặng LEACH với sự hỗ trợ của nhiều nút chuyển tiếp (CH của các cụm trung gian). Sử dụng FC, dữ liệu nút nguồn được chia thành *L* gói rồi sau đó được mã hóa một cách thích hợp để tạo ra các gói mã hóa [34]-[46]. Tiếp theo, nút nguồn phát các gói mã hóa đến nút đích. Giả sử rằng tất cả các CH trang bị đơn ăng-ten và do đó truyền dữ liệu của mỗi gói mã hóa được thực hiện thông qua *N* khe thời gian trực giao, theo phương pháp TDMA.



Hình 4.8: Mô hình hệ thống của giao thức đề xuất.

Trong giao thức được xem xét, nút nghe lén (E) cố gắng thu được dữ liệu nguồn một cách bất hợp pháp. Tương tự như nội dung trình bày ở trong các phần trước đó, thật vậy, E cố gắng nhận được các gói mã hóa để khôi phục dữ liệu gốc. Theo phương pháp giải mã FC, nút đích và nút nghe lén phải nhận thành công ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa để khôi phục được dữ liệu gốc. Tác giả cũng định nghĩa $N_{\max}$ là số gói mã hóa tối đa mà nút nguồn có thể gửi đến nút đích, với $N_{\max} \geq N_{\text{req}}^{\text{pkt}}$, có nghĩa rằng sau khi gửi $N_{\max}$ gói mã hóa, nút nguồn sẽ dừng truyền. Nếu nút đích không thể nhận thành công ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa thì không thể khôi phục dữ liệu gốc, đề cập như sự kiện dừng. Ngược lại, truyền dữ liệu giữa nút nguồn và nút đích là thành công. Đối với nút nghe lén, nếu E có thể nhận ít nhất $N_{\text{req}}^{\text{pkt}}$ gói mã hóa, dữ liệu nguồn bị thu chặn.

4.3.1.1. Mô hình kênh truyền

Giả sử rằng tất cả các kênh liên kết là pha đinh Rayleigh và đặt $\gamma_{\text{D},n}$ là độ lợi kênh truyền giữa CH của cụm thứ $(n-1)$ và CH của cụm thứ n, với $n=1,2,...,N$. Tác giả cũng định nghĩa $\gamma_{\text{E},n-1}$ là độ lợi kênh truyền giữa CH của cụm thứ $(n-1)$ với nút nghe lén và $\gamma_{\text{J},n}$ là độ lợi kênh truyền giữa nút gây

nhiễu được lựa chọn của cụm thứ n với nút nghe lén. Do đó các độ lợi kênh truyền $\gamma_{\mathrm{D},n}$, $\gamma_{\mathrm{E},n-1}$ và $\gamma_{\mathrm{J},n}$ là các biến ngẫu nhiên phân bố mũ với các hàm CDF được cho, tương ứng là

$$F_{\gamma_{\mathrm{D},n}}(x)=1-\exp\left(-\lambda_{\mathrm{D},n}x\right),$$
$$F_{\gamma_{\mathrm{E},n}}(x)=1-\exp\left(-\lambda_{\mathrm{E},n}x\right),$$
$$F_{\gamma_{\mathrm{J},n}}(x)=1-\exp\left(-\lambda_{\mathrm{J},n}x\right), \tag{4.20}$$

với $\lambda_{\mathrm{D},n}$, $\lambda_{\mathrm{E},n}$ và $\lambda_{\mathrm{J},n}$ là các tham số của $\gamma_{\mathrm{D},n}$, $\gamma_{\mathrm{E},n}$ và $\gamma_{\mathrm{J},n}$, tương ứng, có thể được mô hình như trong [108]:

$$\lambda_{\mathrm{D},n}=d_{\mathrm{D},n}^{\beta},\ \lambda_{\mathrm{E},n}=d_{\mathrm{E},n}^{\beta},\ \lambda_{\mathrm{J},n}=d_{\mathrm{J},n}^{\beta}, \tag{4.21}$$

với $d_{\mathrm{D},n}$, $d_{\mathrm{E},n}$ và $d_{\mathrm{J},n}$ là các khoảng cách liên kết giữa CH của cụm thứ $(n-1)$ và CH của cụm thứ n, giữa CH của cụm thứ $(n-1)$ với nút nghe lén và giữa nút gây nhiễu được lựa chọn của cụm thứ n với nút nghe lén, tương ứng.

Từ (4.20), các hàm PDF tương ứng được viết lại bởi

$$f_{\gamma_{\mathrm{D},n}}(x)=\lambda_{\mathrm{D},n}\exp\left(-\lambda_{\mathrm{D},n}x\right),$$
$$f_{\gamma_{\mathrm{E},n-1}}(x)=\lambda_{\mathrm{E},n-1}\exp\left(-\lambda_{\mathrm{E},n-1}x\right),$$
$$f_{\gamma_{\mathrm{J},n}}(x)=\lambda_{\mathrm{J},n}\exp\left(-\lambda_{\mathrm{J},n}x\right). \tag{4.22}$$

4.3.1.2. Dung lượng kênh truyền từ đầu cuối đến đầu cuối

Xem xét quá trình truyền dữ liệu tại chặng thứ n, ta có SNR tức thời nhận được tại CH của cụm thứ n được cho bởi

$$\psi_{\mathrm{D},n}=\frac{\alpha P\gamma_{\mathrm{D},n}}{\sigma^2}=\alpha\Delta\gamma_{\mathrm{D},n}, \tag{4.23}$$

với σ^2 là phương sai của tạp âm Gauss trắng cộng (AWGN) tại CH của cụm thứ n, P là công suất phát tối đa của tất cả các CH, αP là công suất phát của các CH trong giao thức được đề xuất $(0.5\le\alpha\le1)$ và $\Delta=P/\sigma^2$ là SNR phát.

Lưu ý rằng để so sánh công bằng, công suất phát của các CH và các nút gây nhiễu được lựa chọn trong giao thức đề xuất là αP và $(1-\alpha)P$, tương ứng, trong khi đó các CH trong giao thức LEACH truyền thống mà không sử dụng kỹ thuật gây nhiễu cộng tác là P. Hơn nữa, để đạt được (4.23), giả sử rằng CH của cụm thứ n có thể loại bỏ hoàn toàn nhiễu được tạo ra bởi các nút gây nhiễu được lựa chọn [43], [46].

Khi nút nghe lén không thể loại bỏ được nhiễu, SINR tức thời nhận được bởi nút E tại chặng này được thể hiện như sau

$$\psi_{\mathrm{E},n} = \frac{\alpha P \gamma_{\mathrm{E},n}}{(1-\alpha) P \gamma_{\mathrm{J},n} + \sigma^2} = \frac{\alpha \Delta \gamma_{\mathrm{E},n}}{(1-\alpha)\Delta \gamma_{\mathrm{J},n} + 1}. \tag{4.24}$$

Từ (4.23) và (4.24), dung lượng tức thời của kênh dữ liệu và kênh nghe lén có thể được tính, tương ứng bởi

$$C_{\mathrm{D},n} = \frac{1}{N}\log_2\left(1+\psi_{\mathrm{D},n}\right) = \frac{1}{N}\log_2\left(1+\alpha\Delta\gamma_{\mathrm{D},n}\right), \tag{4.25}$$

$$C_{\mathrm{E},n} = \frac{1}{N}\log_2\left(1+\psi_{\mathrm{E},n}\right) = \frac{1}{N}\log_2\left(1+\frac{\alpha\Delta\gamma_{\mathrm{E},n}}{(1-\alpha)\Delta\gamma_{\mathrm{J},n}+1}\right). \tag{4.26}$$

Tiếp theo, nếu kỹ thuật gây nhiễu cộng tác không được sử dụng, công thức (4.25) và (4.26) có thể được viết lại, tương ứng bởi

$$C_{\mathrm{D},n} = \frac{1}{N}\log_2\left(1+\Delta\gamma_{\mathrm{D},n}\right), \tag{4.27}$$

$$C_{\mathrm{E},n} = \frac{1}{N}\log_2\left(1+\Delta\gamma_{\mathrm{E},n}\right). \tag{4.28}$$

Lưu ý rằng các công thức (4.27) và (4.28) đạt được từ các biểu thức (4.25) và (4.26) bằng cách thay thế α bằng 1. Giả sử rằng mỗi gói mã hóa có thể được giải mã thành công bởi các CH và nút nghe lén nếu dung lượng kênh tức thời đạt được lớn hơn một ngưỡng xác định trước, được biểu thị bởi C_{th}. Ngược lại, gói mã hóa không thể nhận thành công. Do sử dụng phương pháp chuyển tiếp DF, xác suất mà một gói mã hóa nhận được thành công bởi nút đích có thể được xác định bởi

$$\rho_{\text{D}} = \prod_{n=1}^{N} \Pr\left(C_{\text{D},n} \geq C_{\text{th}}\right). \tag{4.29}$$

Tiếp theo, xác suất mà nút nghe lén có thể nhận chính xác một gói mã hóa được xác định là

$$\rho_{\text{E}} = \sum_{n=1}^{N} \Pr\left(C_{\text{E},n} \geq C_{\text{th}}\right) \times \prod_{q=1}^{n-1} \Pr\left(C_{\text{D},q} \geq C_{\text{th}}\right) \Pr\left(C_{\text{E},q} < C_{\text{th}}\right). \tag{4.30}$$

Trong (4.30), $\Pr\left(C_{\text{E},n} \geq C_{\text{th}}\right)$ là xác suất mà nút nghe lén có thể nhận thành công gói mã hóa tại chặng thứ n và sự kiện này xảy ra khi: i) quá trình truyền dữ liệu tại các chặng trước đó phải thành công ($\Pr\left(C_{\text{D},q} \geq C_{\text{th}}\right)$, $1 \leq q \leq n-1$); ii) nút nghe lén không thể đạt được gói mã hóa tại các chặng trước đó $\left(\Pr\left(C_{\text{E},q} < C_{\text{th}}\right),\ 1 \leq q \leq n-1\right)$.

Lưu ý rằng xác suất mà nút đích và nút nghe lén không thể nhận thành công một gói mã hóa được cho bởi $1-\rho_{\text{D}}$ và $1-\rho_{\text{E}}$, tương ứng.

4.3.2. Phân tích hiệu năng

4.3.2.1. Xác suất của ρ_{D} và ρ_{E}

• Trường hợp: Kỹ thuật gây nhiễu cộng tác được sử dụng, các biểu thức xác suất này có thể được biểu diễn dưới dạng chính xác là

$$\rho_{\mathrm{D}} = \exp\left(-\sum_{n=1}^{N} \frac{\lambda_{\mathrm{D},n}\theta}{\alpha\Delta} \right). \tag{4.31}$$

$$\rho_{\mathrm{E}} = \sum_{n=1}^{N} \left(\frac{\lambda_{\mathrm{J},n}}{\lambda_{\mathrm{J},n} + \lambda_{\mathrm{E},n}\omega_2} \exp\left(-\lambda_{\mathrm{E},n}\omega_1\right) \right) \times \prod_{q=1}^{n-1} \left[\exp\left(-\frac{\lambda_{\mathrm{D},q}\theta}{\alpha\Delta} \right) \left(1 - \frac{\lambda_{\mathrm{J},q}}{\lambda_{\mathrm{J},q} + \lambda_{\mathrm{E},q}\omega_2} \exp\left(-\lambda_{\mathrm{E},q}\omega_1\right) \right) \right]. \tag{4.32}$$

Chứng minh: Xem chứng minh và các ký hiệu trong mục C2, Phụ lục C.

• Trường hợp: Kỹ thuật gây nhiễu cộng tác không được sử dụng, các biểu thức xác suất này có thể được viết lại, tương ứng là

$$\rho_{\mathrm{D}} = \exp\left(-\sum_{n=1}^{N} \lambda_{\mathrm{D},n} \frac{\theta}{\Delta} \right), \tag{4.33}$$

$$\rho_{\mathrm{E}} = \sum_{n=1}^{N} \exp\left(-\lambda_{\mathrm{E},n} \frac{\theta}{\Delta} \right) \times \prod_{q=1}^{n-1} \left[\exp\left(-\lambda_{\mathrm{D},q} \frac{\theta}{\Delta} \right) \left(1 - \exp\left(-\lambda_{\mathrm{E},q} \frac{\theta}{\Delta} \right) \right) \right]. \tag{4.34}$$

4.3.2.2. Xác suất dừng và xác suất thu chặn

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

$$\mathrm{OP} = \sum_{r=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} C_{N_{\max}}^{r} \left(\rho_{\mathrm{D}}\right)^{r} \left(1-\rho_{\mathrm{D}}\right)^{N_{\max}-r}. \tag{4.35}$$

Biểu thức (4.35) ngụ ý rằng sau khi nút nguồn dừng truyền, nút đích chỉ nhận được r gói mã hóa, với $0 \le r \le N_{\mathrm{req}}^{\mathrm{pkt}} - 1$.

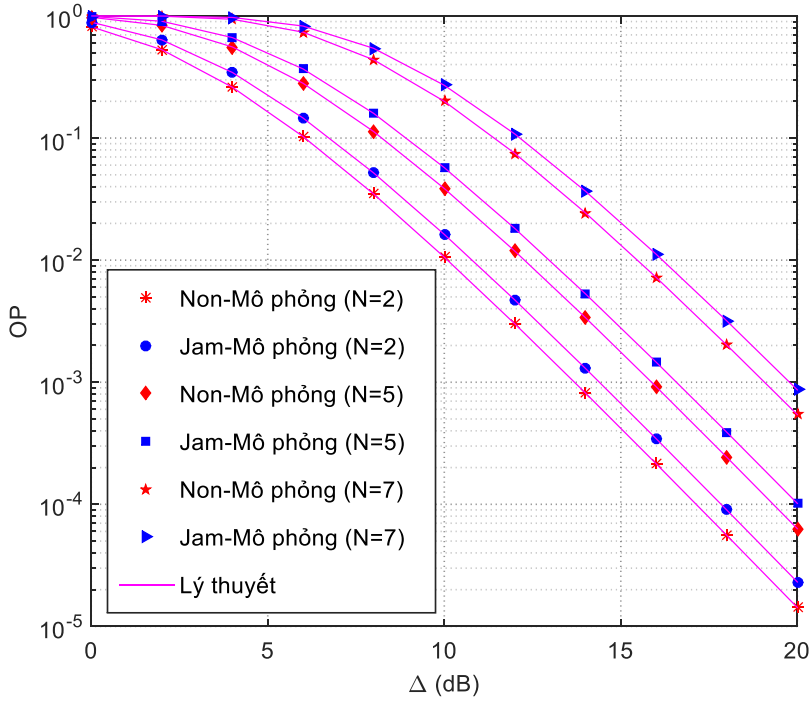
Chúng ta xem xét xác suất thu chặn (IP), có thể được tính toán là

$$\mathrm{IP} = \sum_{w=N_{\mathrm{req}}^{\mathrm{pkt}}}^{N_{\max}} C_{N_{\max}}^{w} \left(\rho_{\mathrm{E}}\right)^{w} \left(1-\rho_{\mathrm{E}}\right)^{N_{\max}-w}. \tag{4.36}$$

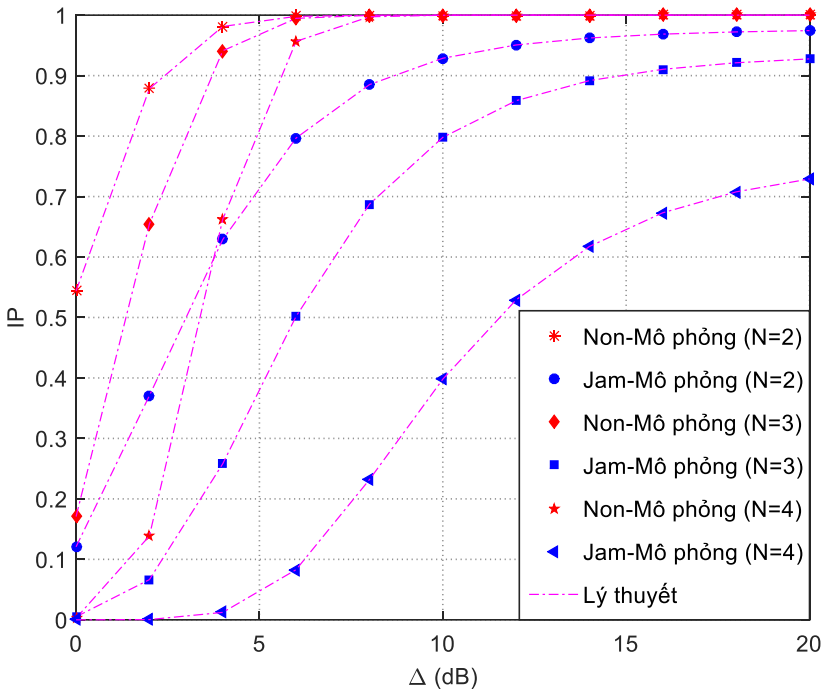
Trong (4.36), khi nút nghe lén có thể đạt được w gói mã hóa, với $N_{\mathrm{req}}^{\mathrm{pkt}} \le w \le N_{\max}$, E có thể khôi phục dữ liệu gốc của nút nguồn và do đó dữ liệu nguồn bị thu chặn.

4.3.3. Các kết quả mô phỏng

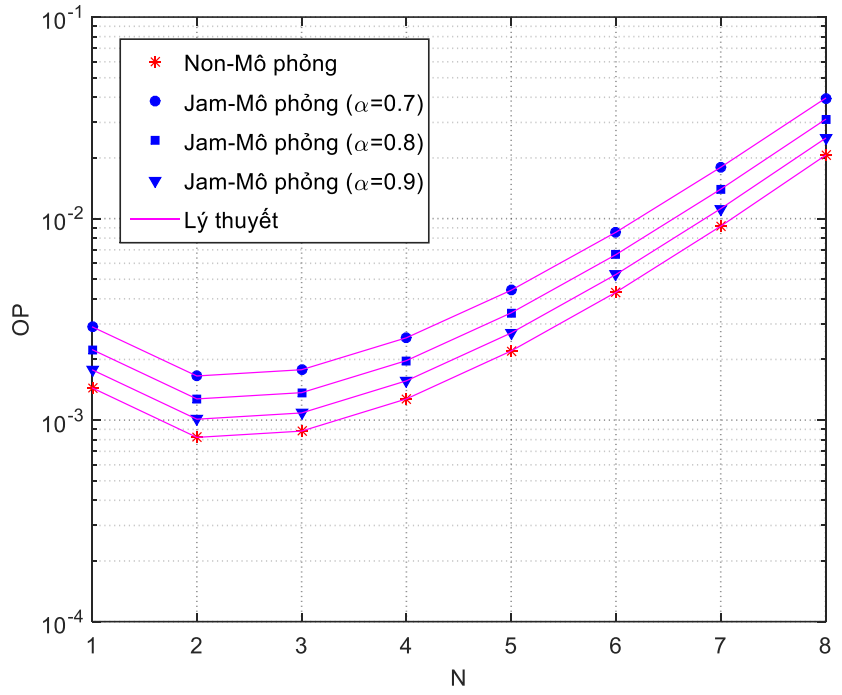
Trong phần này, Luận án thực hiện mô phỏng Monte Carlo để kiểm chứng các kết quả lý thuyết được thể hiện trong Phần 4.3.2, cũng như so sánh hiệu năng của giao thức được đề xuất (Jam) và giao thức LEACH truyền thống (Non). Trong môi trường mô phỏng, không gian hai chiều Oxy được xem xét, với tất cả các nút trong cụm thứ m được đặt tại $(n/N, 0)$ và nút nghe lén được đặt tại $(0.5,\ 0.5)$ với $n = 0,1,...,N$. Trong tất cả các mô phỏng, tác giả cố định hệ số suy hao (β) bằng 3 và tốc độ mong muốn (C_{th}) bằng 1.



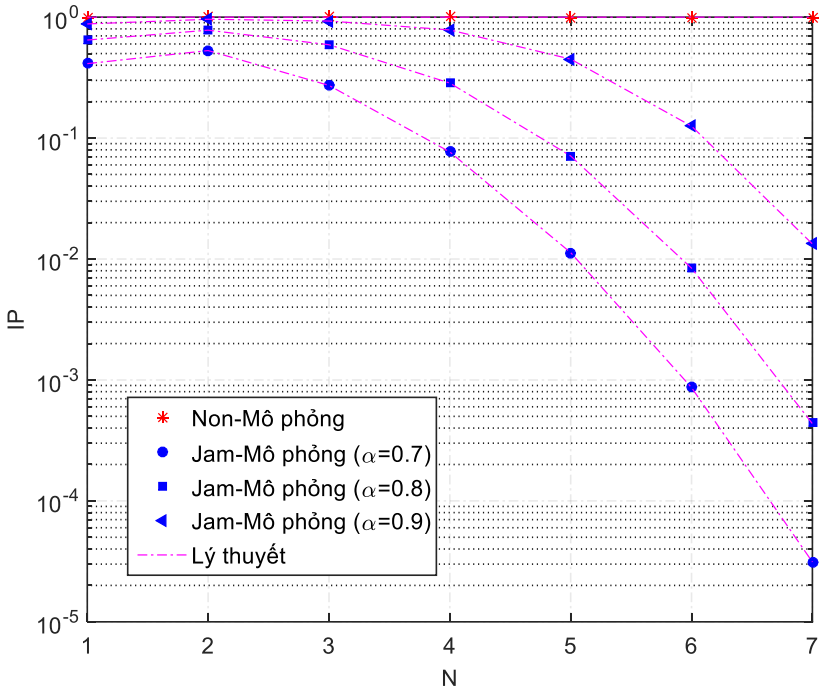
Hình 4.9: OP là hàm của Δ(dB) khi $\alpha = 0.85$, $N_{\mathrm{req}}^{\mathrm{pkt}} = 5$ và $N_{\max} = 7$.



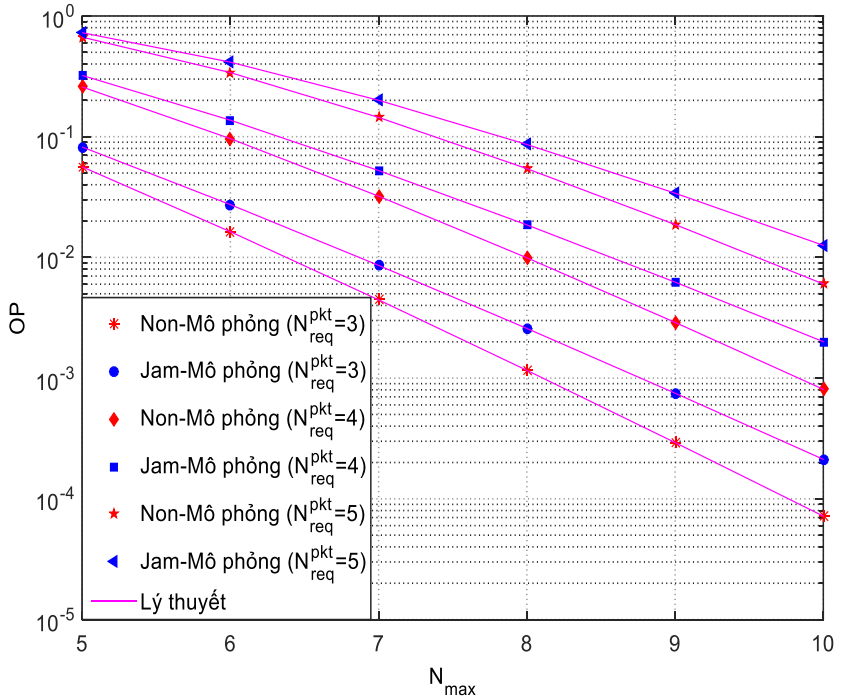
Hình 4.10: IP là hàm của Δ (dB) khi $\alpha = 0.85$, $N_{\text{req}}^{\text{pkt}} = 5$ và $N_{\max} = 7$.



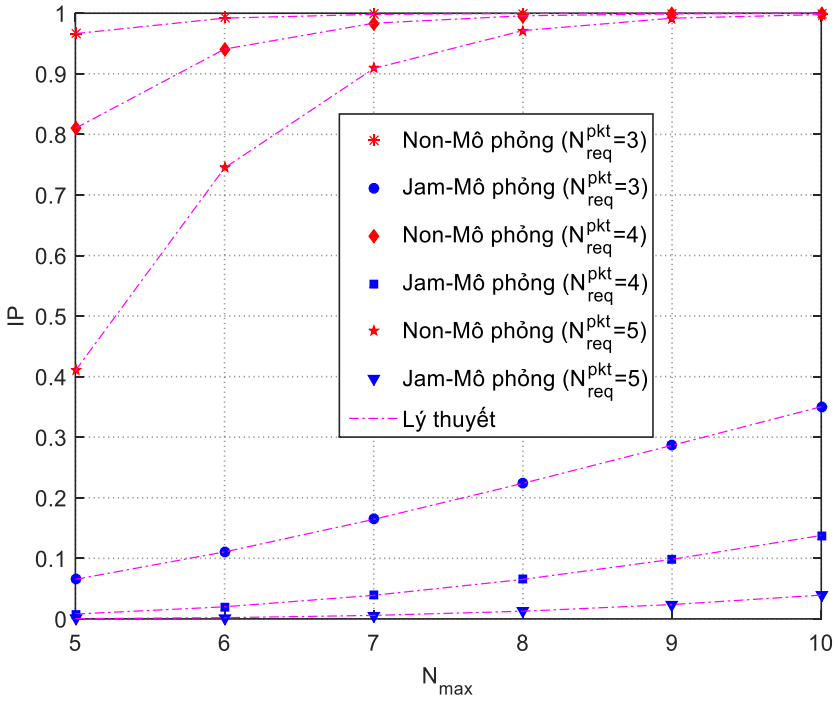
Hình 4.11: OP là hàm của N khi $\Delta = 20\,\text{dB}$, $N_{\text{req}}^{\text{pkt}} = 5$ và $N_{\max} = 6$.



Hình 4.12: IP là hàm của N khi $\Delta = 20\text{dB}$, $N_{\text{req}}^{\text{pkt}} = 5$ và $N_{\max} = 6$.



Hình 4.13: OP là hàm của $N_{\max}$ khi $\Delta = 7.5\text{dB}$, $\alpha = 0.85$ và $N = 5$.



Hình 4.14: IP là hàm của $N_{\max}$ khi $\Delta = 7.5\text{dB}$, $\alpha = 0.85$ và $N = 5$.

Trong các Hình 4.9 đến 4.10, Luận án thể hiện OP và IP như là hàm của SNR phát Δ(dB). Trong những vẽ hình này, khoảng α được cố định bằng 0.85 và các giá trị của $N_{\text{req}}^{\text{pkt}}$ và $N_{\max}$ được gán bởi 5 và 7, tương ứng. Trong Hình 4.9, chúng ta thấy rằng các giá trị của OP giảm khi tăng Δ. Hơn nữa, OP của giao thức được đề xuất (Jam) cao hơn so với giao thức không gây nhiễu (Non), bởi vì công suất phát của các CH trong giao thức không gây nhiễu lớn hơn. Như có thể quan sát, hiệu năng bị suy giảm khoảng 1dB. Ta cũng nhận thấy từ Hình 4.9 rằng hiệu năng OP của các giao thức đề xuất kém hơn khi tăng số chặng. Trong Hình 4.10, các giá trị của IP tăng nhanh khi tăng Δ và IP của giao thức đề xuất (Jam) thấp hơn nhiều so với giao thức không gây nhiễu (Non). Thêm vào đó, các giá trị IP giảm khi tăng số chặng giữa nút nguồn và nút đích (N).

Các Hình 4.11 và 4.12 trình bày OP và IP như là hàm của N với các giá trị khác nhau của α. Một lần nữa, hiệu năng OP của giao thức (Non) tốt hơn

giao thức đề xuất (Jam), nhưng hiệu năng IP của giao thức (Non) kém hơn nhiều. Như quan sát trong Hình 4.12, dữ liệu nguồn trong giao thức (Non) gần như bị thu chặn bởi nút nghe lén. Đối với giao thức đề xuất, các giá trị IP giảm khi giảm α bởi vì công suất phát của các nút gây nhiễu được lựa chọn tăng. Tuy nhiên, giảm giá trị của α sẽ giảm công suất phát của các CH, dẫn đến sự suy giảm hiệu năng OP. Trong các Hình 4.11 đến 4.12, ta có thể nhận thấy rằng khi $N = 2,$ giá trị của OP (IP) là nhỏ nhất (lớn nhất).

Các Hình 4.13 và Hình 4.14 khảo sát sự đánh đổi giữa IP và OP cùng với các giá trị khác nhau của $N_{\text{req}}^{\text{pkt}}$ và $N_{\max}$. Như chúng ta có thể thấy trong Hình 4.13, hiệu năng OP của các giao thức được xem xét tốt hơn khi $N_{\text{req}}^{\text{pkt}}$ giảm và $N_{\max}$ tăng. Thật vậy, với giá trị thấp hơn của $N_{\text{req}}^{\text{pkt}}$ và giá trị cao hơn của $N_{\max},$ xác suất mà nút đích có thể nhận đủ số gói mã hóa tăng, điều này làm giảm xác suất dừng. Tuy nhiên, như được minh họa trong Hình 4.14, các giá trị IP cũng tăng khi $N_{\text{req}}^{\text{pkt}}$ giảm và $N_{\max}$ tăng. Do đó, các giá trị của $N_{\text{req}}^{\text{pkt}}$ và $N_{\max}$ nên được thiết kế phù hợp để bảo đảm chất lượng dịch vụ (Quality of Sevice: QoS) (OP) và bảo mật (IP). Ví dụ, trong giao thức đề xuất, để thỏa mãn yêu cầu QoS của $\text{OP} \le 0.01$ và mức độ bảo mật $\text{IP} \le 0.1,$ ta phải thiết lập các giá trị của $N_{\text{req}}^{\text{pkt}}$ và $N_{\max}$ bằng 4 và 9, tương ứng.

Cuối cùng, một lần nữa chúng ta thấy rằng các kết quả mô phỏng và lý thuyết là hoàn toàn phù hợp với nhau, điều này thể hiện tính đúng đắn của các kết quả lý thuyết được đưa ra trong Mục 4.3.2.

4.4. KẾT LUẬN CHƯƠNG

Chương 4 đã đề xuất hai mô hình để phân tích hiệu năng bảo mật cho mạng chuyển tiếp đa chặng sử dụng mã Fountain, bao gồm: i) mô hình mạng đa chặng thu thập năng lượng sóng vô tuyến và ii) mô hình đa chặng LEACH với gây nhiễu cộng tác trong các mạng WSN. Các kết quả phân tích lý thuyết

được kiểm chứng bởi mô phỏng Monte Carlo dựa vào phần mềm Matlab để phân tích và chứng minh ưu điểm của các phương pháp đề xuất.

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

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

KẾT LUẬN VÀ HƯỚNG NGHIÊN CỨU TIẾP THEO

Nội dung của Luận án đã giới thiệu khái quát những vấn đề cơ bản về bảo mật lớp vật lý trong các hệ thống MIMO, mã Fountain, kỹ thuật lựa chọn ăng-ten tại máy phát (TAS), các kỹ thuật phân tập thu (SC/MRC), NOMA, vô tuyến nhận thức, giao thoa đồng kênh, suy giảm phần cứng. Hơn nữa, Luận án cũng đã nghiên cứu những nội dung liên quan đến các mạng chuyển tiếp đa chặng, thu thập năng lượng sóng vô tuyến. Mặt khác, các công trình nghiên cứu liên quan trực tiếp đến nội dung Luận án cũng đã được khảo sát. Trên cơ sở đó, Luận án đã đề xuất một số mô hình hệ thống để phân tích, đánh giá nhằm cải thiện hiệu năng bảo mật trong các mạng vô tuyến. Một số đóng góp chính của Luận án có thể được liệt kê như sau:

A. MỘT SỐ KẾT QUẢ ĐẠT ĐƯỢC CỦA LUẬN ÁN

• Trước tiên, Luận án đã nghiên cứu hiệu năng bảo mật lớp vật lý của các giao thức truyền bảo mật sử dụng FC, bao gồm: i) giao thức MISO TAS trong mạng vô tuyến nhận thức dạng nền dưới tác động chung của giao thoa đồng kênh từ mạng sơ cấp và suy giảm phần cứng; ii) giao thức MIMO TAS/SC dưới tác động của nhiều nguồn giao thoa đồng kênh, với kịch bản có và không có CSI đến các nguồn giao thoa. Để cải thiện hiệu quả bảo mật, cần tăng số ăng-ten được trang bị tại nút nguồn phù hợp, giảm số lần truyền các gói mã hóa, giảm thiểu tác động của suy giảm phần cứng tại các thiết bị của mạng thứ cấp. Tiếp theo, cần thiết lập các tham số như số ăng-ten tại nút nguồn/đích, tăng số gói mã hóa cần thiết để khôi phục dữ liệu gốc, phân bổ mức công suất phát của nút nguồn phù hợp và có thể lựa chọn mô hình thích hợp (MH1 hoặc MH2) để đạt hiệu năng bảo mật cao hơn.

• Thứ hai, Luận án đề xuất và phân tích hiệu năng của mã Fountain dựa vào các giao thức truyền bảo mật trong hệ thống MIMO-NOMA với các kỹ

thuật TAS/SC/MRC và thể hiện rằng giao thức sử dụng NOMA đạt được hiệu năng bảo mật tốt hơn tại SNR trung bình và cao khi so sánh với Wo-NOMA. Mặt khác, hiệu năng bảo mật của cả Wo-NOMA và NOMA có thể được nâng cao bằng cách lựa chọn số ăng-ten tối ưu tại nút nguồn/đích, tăng số gói mã hóa yêu cầu và phân bổ khoảng công suất phát đến các tín hiệu NOMA.

• Thứ ba, Luận án phân tích độ tin cậy và bảo mật trong các mạng chuyển tiếp đa chặng sử dụng FC với các mô hình đề xuất. Các tham số hệ thống như số chặng, khoảng thời gian cho pha thu thập năng lượng hoặc công suất phân bổ cho phát nhiễu giả, số gói mã hóa yêu cầu, số lần truyền tối đa tại nút nguồn nên được thiết kế phù hợp để bảo đảm cả bảo mật và QoS.

• Hơn nữa, một trong những đóng góp quan trọng nhất của Luận án này là tác giả đã phân tích, đánh giá hiệu năng bảo mật của các giao thức được đề xuất bằng cách đưa ra các biểu thức dạng chính xác trên kênh truyền pha đinh Rayleigh. Những đóng góp này là cực kỳ quan trọng bởi vì các biểu thức tính toán có thể dễ dàng để phân tích và đánh giá hiệu năng hệ thống nhằm giúp các nhà nghiên cứu hoặc thiết kế hệ thống thực hiện so sánh giữa các giao thức mạng, các kỹ thuật phân tập, mã hóa,… xác định các lựa chọn tối ưu dưới những điều kiện ràng buộc được đưa ra trong mạng.

• Cuối cùng, các kết quả phân tích lý thuyết được kiểm chứng bằng mô phỏng Monte Carlo.

B. CÁC ĐỊNH HƯỚNG NGHIÊN CỨU TƯƠNG LAI

Mặc dù Luận án đã nghiên cứu một số mô hình đề xuất để đánh giá, phân tích hiệu năng bảo mật của hệ thống. Tuy nhiên, theo nhận định của tác giả, vẫn còn một số vấn đề cần được tiếp tục mở rộng để thực hiện khảo sát trong tương lai.

• Trong Luận án này, tác giả đã phân tích hiệu năng bảo mật của các giao thức mạng sử dụng FC như MISO TAS, MIMO TAS/SC hoặc MIMO-NOMA TAS/SC/MRC. Do đó, việc mở rộng các giao thức này trong những

kịch bản khác nhau với tham số như xác suất dừng, mối quan hệ giữa IP (OP) hoặc trong môi trường vô tuyến nhận thức sẽ là chủ đề thu hút được nhiều sự quan tâm. Ngoài ra, có thể đánh giá hiệu năng mạng dưới tác động đồng thời của giao thoa đồng kênh và suy giảm phần cứng hoặc thu thập năng lượng sóng vô tuyến của một nút trong mạng để tạo nhiễu giả đến nút nghe lén, cũng là nội dung nghiên cứu quan trọng trong tương lai.

• Trong Luận án này, tác giả đã nghiên cứu bảo mật trong các mạng đa chặng sử dụng FC. Hơn nữa, các nút có thể di chuyển linh hoạt trong mạng, nên hiệu năng có thể phụ thuộc vào sự định tuyến và tính linh động của các nút mạng, do đó truyền thông cộng tác (cooperative communication) trong các mạng vô tuyến di động và mạng vô tuyến nhận thức với các phương pháp lựa chọn nút chuyển tiếp sẽ là một chủ đề nghiên cứu tiếp theo.

• Ngoài ra, phân tích hiệu năng bảo mật trong các mạng vô tuyến thông thường và vô tuyến nhận thức sử dụng FC trên các loại kênh truyền khác nhau như Nakagami-*m* cũng sẽ là chủ đề được quan tâm.

PHỤ LỤC

Phụ lục A: Các chứng minh trong Chương 2

A.1. Dẫn xuất xác suất ρ_{P} của mô hình đề xuất 1 trong Phần 2.2

Từ công thức (2.8), ta có thể viết lại như sau:

$$\rho_{\mathrm{P}} = \Pr\left(\left(1-\kappa_{\mathrm{P}}^2\gamma_{\mathrm{P}}\right)P_{\mathrm{PT}}\gamma_{\mathrm{PT,PR}} < P_S\gamma_{\mathrm{P}}\gamma_{\mathrm{S}_m,\mathrm{PR}} + \sigma^2\gamma_{\mathrm{P}}\right). \tag{A.1}$$

Ta tính xác suất ρ_{P} trong trường hợp $1-\kappa_{\mathrm{P}}^2\gamma_{\mathrm{P}} > 0,$ trong (A.1) như sau:

$$\rho_{\mathrm{P}} = \int_0^{+\infty} F_{\gamma_{\mathrm{PT,PR}}}\left(\frac{P_S\gamma_{\mathrm{P}}}{\left(1-\kappa_{\mathrm{P}}^2\gamma_{\mathrm{P}}\right)P_{\mathrm{PT}}}x + \frac{\sigma^2\gamma_{\mathrm{P}}}{\left(1-\kappa_{\mathrm{P}}^2\gamma_{\mathrm{P}}\right)P_{\mathrm{PT}}}\right) f_{\gamma_{\mathrm{S}_m,\mathrm{PR}}}(x)dx. \tag{A.2}$$

Thay các hàm phân bố xác suất đã đưa ra trong (2.1) và (2.3) vào trong (A.2), sau một số tính toán tích phân, ta có biểu thức dạng chính xác cho ρ_{P} như trong (2.9).

A.2. Dẫn xuất các xác suất ρ_{D} của mô hình đề xuất 1 trong Phần 2.2

Thay công thức (2.14) vào trong (2.16), ta có:

$$\rho_{\mathrm{D}} = \Pr\left(\left(1-\kappa_{\mathrm{D}}^2\gamma_{\mathrm{th}}\right)P_{\mathrm{S}}\gamma_{\mathrm{S}_{a^*},\mathrm{D}} < P_{\mathrm{PT}}\gamma_{\mathrm{th}}\gamma_{\mathrm{PT,D}} + \sigma^2\gamma_{\mathrm{th}}\right). \tag{A.3}$$

Từ (A.3), dễ thấy rằng nếu $1-\kappa_{\mathrm{D}}^2\gamma_{\mathrm{th}} \le 0$ thì $\rho_{\mathrm{D}} = 1$ và ngược lại, ta viết

$$\begin{aligned}\rho_{\mathrm{D}} &= \Pr\left(\gamma_{\mathrm{S}_{a^*},\mathrm{D}} < \mu_{\mathrm{D}}\gamma_{\mathrm{PT,D}} + \omega_{\mathrm{D}}\right)\\ &= \int_0^{+\infty} F_{\gamma_{\mathrm{S}_{a^*},\mathrm{D}}}\left(\mu_{\mathrm{D}}x + \omega_{\mathrm{D}}\right) f_{\gamma_{\mathrm{PT,D}}}(x)dx,\end{aligned} \tag{A.4}$$

với

$$\mu_{\mathrm{D}} = \frac{P_{\mathrm{PT}}\gamma_{\mathrm{th}}}{\left(1-\kappa_{\mathrm{D}}^2\gamma_{\mathrm{th}}\right)P_{\mathrm{S}}},\ \omega_{\mathrm{D}} = \frac{\sigma^2\gamma_{\mathrm{th}}}{\left(1-\kappa_{\mathrm{D}}^2\gamma_{\mathrm{th}}\right)P_{\mathrm{S}}}. \tag{A.5}$$

Thay các công thức (2.3) và (2.13) vào (A.4), sau một số bước tính toán, biểu thức chính xác của ρ_{D} đạt được trong (2.20).

Khi công suất phát của PT đủ lớn, ta có thể xấp xỉ ψ_{D} bởi:

$$\psi_{\mathrm{D}} \overset{P_{\mathrm{PT}}\to+\infty}{\approx} \frac{P_{\mathrm{S}}^{*}\gamma_{\mathrm{S}_{a^{*}},\mathrm{D}}}{\kappa_{\mathrm{D}}^{2}P_{\mathrm{S}}^{*}\gamma_{\mathrm{S}_{a^{*}},\mathrm{D}}+P_{\mathrm{PT}}\gamma_{\mathrm{PT,D}}}. \tag{A.6}$$

Kết hợp (2.11), (2.16) và (A.6), với cùng phương pháp tính toán như trên, ta có thể đạt được biểu thức xấp xỉ cho ρ_{D} như trong (2.21).

A.3. Dẫn xuất của $F_{\gamma_{\mathrm{S}_{a^{*}}\mathrm{D}_{b^{*}}}}(x)$ và $F_{\gamma_{\mathrm{S}_{a^{*}}\mathrm{E}_{t^{*}}}}(x)$ của mô hình đề xuất 2 trong Phần 2.3

Trước tiên, hàm CDF của $\gamma_{\mathrm{S}_{a^{*}}\mathrm{D}_{b^{*}}}$ trong (2.39) được xác định bởi:

$$F_{\gamma_{\mathrm{S}_{a^{*}}\mathrm{D}_{b^{*}}}}(x)=\Pr\left(\max_{m=1,2,\ldots,N_{\mathrm{S}}}\max_{n=1,2,\ldots,N_{\mathrm{D}}}\left(\gamma_{\mathrm{S}_m\mathrm{D}_n}\right)<x\right)=\left(F_{\gamma_{\mathrm{S}_m\mathrm{D}_n}}(x)\right)^{N_{\mathrm{S}}N_{\mathrm{D}}}. \tag{A.7}$$

Sử dụng hàm CDF đưa ra trong (2.35), ta viết lại (A.7) như sau:

$$F_{\gamma_{\mathrm{S}_{a^{*}}\mathrm{D}_{b^{*}}}}(x)=\left(1-\exp\left(-\lambda_{\mathrm{SD}}x\right)\right)^{N_{\mathrm{S}}N_{\mathrm{D}}}. \tag{A.8}$$

Hơn nữa, thực hiện khai triển nhị thức Newton, ta có:

$$F_{\gamma_{\mathrm{S}_{a^{*}}\mathrm{D}_{b^{*}}}}(x)=1+\sum_{k=1}^{N_{\mathrm{S}}N_{\mathrm{D}}}(-1)^{k}C_{N_{\mathrm{S}}N_{\mathrm{D}}}^{k}\exp\left(-k\lambda_{\mathrm{SD}}x\right). \tag{A.9}$$

Tương tự, hàm CDF của $\gamma_{\mathrm{S}_{a^{*}}\mathrm{E}_{t^{*}}}$ trong (2.41) cũng có dạng như sau:

$$\begin{aligned}F_{\gamma_{\mathrm{S}_{a^{*}}\mathrm{E}_{t^{*}}}}(x)&=\left(1-\exp\left(-\lambda_{\mathrm{SE}}x\right)\right)^{N_{\mathrm{E}}}\\&=1+\sum_{t=1}^{N_{\mathrm{E}}}(-1)^{t}C_{N_{\mathrm{E}}}^{t}\exp\left(-t\lambda_{\mathrm{SE}}x\right).\end{aligned} \tag{A.10}$$

Tiếp đến, sử dụng [101, phương trình (7)], hàm PDF của X_n^{sum} và Y_t^{sum} sẽ lần lượt được biểu diễn như bên dưới:

$$\begin{aligned}f_{X_n^{\mathrm{sum}}}(y)&=\frac{\lambda_{\mathrm{ID}}^{M}}{(M-1)!}y^{M-1}\exp\left(-\lambda_{\mathrm{ID}}y\right),\\f_{Y_t^{\mathrm{sum}}}(y)&=\frac{\lambda_{\mathrm{IE}}^{M}}{(M-1)!}y^{M-1}\exp\left(-\lambda_{\mathrm{IE}}y\right).\end{aligned} \tag{A.11}$$

A.4. Dẫn xuất của các xác suất $\rho_{1,\mathrm{D}}$, $\rho_{1,\mathrm{E}}$, $\rho_{2,\mathrm{D}}$ *và* $\rho_{2,\mathrm{E}}$

Để tính xác suất $\rho_{1,\mathrm{D}}$, ta cần biểu diễn xác suất này dưới dạng sau:

$$\rho_{1,\mathrm{D}} = \Pr\left(\frac{Q_{\mathrm{S}} \gamma_{\mathrm{S}_{a^*}\mathrm{D}_{b^*}}}{Q_{\mathrm{I}} X_{b^*}^{\mathrm{sum}} + 1} \le \gamma_{\mathrm{th}} \right)$$

$$= \Pr\left(\gamma_{\mathrm{S}_{a^*}\mathrm{D}_{b^*}} < \frac{Q_{\mathrm{I}}}{Q_{\mathrm{S}}} \gamma_{\mathrm{th}} X_{b^*}^{\mathrm{sum}} + \frac{\gamma_{\mathrm{th}}}{Q_{\mathrm{S}}} \right). \quad \text{(A.12)}$$

Để thuận tiện cho việc trình bày, ta ký hiệu:

$$\theta_1 = \gamma_{\mathrm{th}} / Q_{\mathrm{S}},\ \theta_2 = Q_{\mathrm{I}} \gamma_{\mathrm{th}} / Q_{\mathrm{S}}. \quad \text{(A.13)}$$

Từ (A.13), công thức (A.12) sẽ được biểu diễn như sau:

$$\rho_{1,\mathrm{D}} = \Pr\left(\gamma_{\mathrm{S}_{a^*}\mathrm{D}_{b^*}} < \theta_1 + \theta_2 X_{b^*}^{\mathrm{sum}} \right)$$

$$= \int_0^{+\infty} F_{\gamma_{\mathrm{S}_{a^*}\mathrm{D}_{b^*}}} \left(\theta_1 + \theta_2 y \right) f_{X_{b^*}^{\mathrm{sum}}} \left(y \right) dy. \quad \text{(A.14)}$$

Thay (A.9) và (A.11) vào trong (A.14), ta có:

$$\rho_{1,\mathrm{D}} = 1 + \sum_{k=1}^{N_{\mathrm{S}} N_{\mathrm{D}}} \left(-1 \right)^k C_{N_{\mathrm{S}} N_{\mathrm{D}}}^k \frac{\lambda_{\mathrm{ID}}^M}{\left(M - 1 \right)!} \exp\left(-k \lambda_{\mathrm{SD}} \theta_1 \right)$$

$$\times \int_0^{+\infty} y^{M-1} \exp\left(-\left(k \lambda_{\mathrm{SD}} \theta_2 + \lambda_{\mathrm{ID}} \right) y \right) dy. \quad \text{(A.15)}$$

Sau khi tính tích phân trong (A.15), ta có biểu thức dạng tường minh (closed-form) cho $\rho_{1,\mathrm{D}}$ như trong (2.48).

Đối với xác suất $\rho_{1,\mathrm{E}}$, tương tự, ta có:

$$\rho_{1,\mathrm{E}} = \Pr\left(\gamma_{\mathrm{S}_{a^*}\mathrm{E}_{t^*}} < \theta_1 + \theta_2 Y_{t^*}^{\mathrm{sum}} \right)$$

$$= \int_0^{+\infty} F_{\gamma_{\mathrm{S}_{a^*}\mathrm{E}_{t^*}}} \left(\theta_1 + \theta_2 y \right) f_{Y_{t^*}^{\mathrm{sum}}} \left(y \right) dy. \quad \text{(A.16)}$$

Thay (A.10) và (A.11) vào (A.16) và sau khi tính tích phân, ta có (2.49).

Tiếp theo, kết hợp (2.37), (2.43) và (2.46), ta sẽ biểu diễn $\rho_{2,\mathrm{D}}$ như sau:

$$\rho_{2,\mathrm{D}} = \Pr\left(\max_{m=1,2,\ldots,N_\mathrm{S}} \max_{n=1,2,\ldots,N_\mathrm{D}} \left(\psi_{\mathrm{S}_m\mathrm{D}_n} \right) \le \gamma_{\mathrm{th}} \right)$$

$$= \left[\Pr\left(\frac{Q_\mathrm{S}\gamma_{\mathrm{S}_m\mathrm{D}_n}}{Q_\mathrm{I}X_n^{\mathrm{sum}}+1} \le \gamma_{\mathrm{th}} \right) \right]^{N_\mathrm{S}N_\mathrm{D}}$$

$$= \Pr\left(\gamma_{\mathrm{S}_m\mathrm{D}_n} < \frac{Q_\mathrm{I}}{Q_\mathrm{S}}\gamma_{\mathrm{th}}X_n^{\mathrm{sum}} + \frac{\gamma_{\mathrm{th}}}{Q_\mathrm{S}} \right)^{N_\mathrm{S}N_\mathrm{D}} . \qquad \text{(A.17)}$$

Tương tự như các bước tính toán ở trên, ta đạt được $\rho_{2,\mathrm{D}}$ trong (2.50).

Xác suất $\rho_{2,\mathrm{E}}$ sẽ được đưa ra bởi biểu thức như sau:

$$\rho_{2,\mathrm{E}} = \Pr\left(\max_{t=1,2,\ldots,N_\mathrm{E}} \left(\psi_{\mathrm{S}_a\mathrm{E}_t} \right) \le \gamma_{\mathrm{th}} \right)$$

$$= \left[\Pr\left(\frac{Q_\mathrm{S}\gamma_{\mathrm{S}_a\mathrm{E}_t}}{Q_\mathrm{I}Y_t^{\mathrm{sum}}+1} \le \gamma_{\mathrm{th}} \right) \right]^{N_\mathrm{E}}$$

$$= \Pr\left(\gamma_{\mathrm{S}_a\mathrm{E}_t} < \frac{Q_\mathrm{I}}{Q_\mathrm{S}}\gamma_{\mathrm{th}}Y_t^{\mathrm{sum}} + \frac{\gamma_{\mathrm{th}}}{Q_\mathrm{S}} \right)^{N_\mathrm{E}} . \qquad \text{(A.18)}$$

Tương tự như trên, sau một số bước tính toán ta đạt được biểu thức dạng tường minh cho $\rho_{2,\mathrm{E}}$ như trong (2.51).

Phụ lục B: Các chứng minh trong Chương 3

B.1. Dẫn xuất của ρ_D và ρ_E

• Trường hợp 1: D và E sử dụng bộ kết hợp SC

Kết hợp hàm CDF trong (2.1) với (3.6) và (3.12), ta có thể đạt được biểu thức (B.1) như trong (3.26).

$$\rho_\mathrm{D} = 1 - \Pr\left(\max_{m=1,2,\ldots,N_\mathrm{S}} \left(\max_{n=1,2,\ldots,N_\mathrm{D}} \left(\psi_{\mathrm{S}_m\mathrm{D}_n} \right) \right) < \gamma_{\mathrm{th}} \right)$$

$$= 1 - \prod_{m=1}^{N_\mathrm{S}} \prod_{n=1}^{N_\mathrm{D}} F_{\gamma_{\mathrm{S}_m\mathrm{D}_n}} \left(\frac{\gamma_{\mathrm{th}}}{\Delta} \right)$$

$$=1-\left[1-\exp\left(-\frac{\lambda_{\mathrm{SD}}\gamma_{\mathrm{th}}}{\Delta}\right)\right]^{N_{\mathrm{S}}N_{\mathrm{D}}}. \qquad \text{(B.1)}$$

Tương tự, kết hợp hàm CDF trong (2.1) với (3.7) và (3.12), xác suất ρ_{E} đạt được trong (B.2) như (3.27).

$$\rho_{\mathrm{E}}=1-\Pr\left(\max_{t=1,2,\ldots,N_{\mathrm{E}}}\left(\psi_{\mathrm{S}_a\mathrm{E}_t}\right)<\gamma_{\mathrm{th}}\right)$$

$$=1-\left[1-\exp\left(-\frac{\lambda_{\mathrm{SE}}\gamma_{\mathrm{th}}}{\Delta}\right)\right]^{N_{\mathrm{E}}}. \qquad \text{(B.2)}$$

• Trường hợp 2: D và E sử dụng bộ kết hợp MRC

Từ (2.1), (3.10) và (3.12), xác suất ρ_{D} có thể được tính là

$$\rho_{\mathrm{D}}=1-\Pr\left(\max_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\sum_{n=1}^{N_{\mathrm{D}}}\psi_{\mathrm{S}_m\mathrm{D}_n}\right)<\gamma_{\mathrm{th}}\right)$$

$$=1-\Pr\left[\left(\sum_{n=1}^{N_{\mathrm{D}}}\psi_{\mathrm{S}_m\mathrm{D}_n}\right)<\gamma_{\mathrm{th}}\right]^{N_{\mathrm{S}}}. \qquad \text{(B.3)}$$

Sử dụng hàm CDF của tổng các biến ngẫu nhiên độc lập và đồng nhất hàm mũ [104], chúng ta có thể đạt được (B.4) như (3.28).

$$\rho_{\mathrm{D}}=1-\left[1-\sum_{m=0}^{N_{\mathrm{D}}-1}\frac{1}{m!}\left(\frac{\lambda_{\mathrm{SD}}\gamma_{\mathrm{th}}}{\Delta}\right)^{m}\exp\left(-\frac{\lambda_{\mathrm{SD}}\gamma_{\mathrm{th}}}{\Delta}\right)\right]^{N_{\mathrm{S}}}. \qquad \text{(B.4)}$$

Tương tự, chúng ta có thể tính xác suất ρ_{E} trong trường hợp này (B.5) như (3.29).

$$\rho_{\mathrm{E}}=\sum_{t=0}^{N_{\mathrm{E}}-1}\frac{1}{t!}\left(\frac{\lambda_{\mathrm{SE}}\gamma_{\mathrm{th}}}{\Delta}\right)^{t}\exp\left(-\frac{\lambda_{\mathrm{SE}}\gamma_{\mathrm{th}}}{\Delta}\right). \qquad \text{(B.5)}$$

B.2. Dẫn xuất của $\chi_{\mathrm{D},i}$ và $\chi_{\mathrm{E},i}$

• Trường hợp 1: Nút đích và nút nghe lén sử dụng kỹ thuật SC

Trước tiên, xem xét $\chi_{\mathrm{D},2}$ kết hợp (3.16) và (3.24), chúng ta có

$$\chi_{\mathrm{D},2}=\Pr\left[\begin{array}{l}\left(a_1-a_2\gamma_{\mathrm{th}}\right)\max\limits_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\max\limits_{n=1,2,\ldots,N_{\mathrm{D}}}\left(\psi_{\mathrm{S}_m\mathrm{D}_n}\right)\right)\geq\gamma_{\mathrm{th}},\\ a_2\max\limits_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\max\limits_{n=1,2,\ldots,N_{\mathrm{D}}}\left(\psi_{\mathrm{S}_m\mathrm{D}_n}\right)\right)\geq\gamma_{\mathrm{th}}\end{array}\right]. \quad \text{(B.6)}$$

Chúng ta quan sát từ (B.6) rằng, nếu $a_1-a_2\gamma_{\mathrm{th}}\leq 0$, thì $\chi_{\mathrm{D},2}=0$. Ngược lại, (B.6) có thể được viết lại là

$$\chi_{\mathrm{D},2}=\Pr\left(\max_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\max_{n=1,2,\ldots,N_{\mathrm{D}}}\left(\gamma_{\mathrm{S}_m\mathrm{D}_n}\right)\right)\geq\mu_1,\ \max_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\max_{n=1,2,\ldots,N_{\mathrm{D}}}\left(\gamma_{\mathrm{S}_m\mathrm{D}_n}\right)\right)\geq\mu_2\right), \quad \text{(B.7)}$$

với

$$\mu_1=\frac{\gamma_{\mathrm{th}}}{\left(a_1-a_2\gamma_{\mathrm{th}}\right)\Delta},\ \mu_2=\frac{\gamma_{\mathrm{th}}}{a_2\Delta}. \quad \text{(B.8)}$$

Nhận xét: *Như đã đề cập trong Nhận xét 2, a_1 nên lớn hơn nhiều so với a_2 do vậy SNR đạt được, $\psi_{\mathrm{D},1}^{\mathrm{TAS/SC}}$, là đủ lớn. Vì vậy, có thể giả sử rằng $a_1>\left(1+\gamma_{\mathrm{th}}\right)a_2$, dẫn đến kết quả như sau: $0<\mu_1<\mu_2$. Tiếp theo, xác suất $\chi_{\mathrm{D},2}$ được tính trong (B.9) như (3.30).*

$$\begin{aligned}\chi_{\mathrm{D},2}&=\Pr\left(\max_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\max_{n=1,2,\ldots,N_{\mathrm{D}}}\left(\gamma_{\mathrm{S}_m\mathrm{D}_n}\right)\right)\geq\mu_2\right)\\&=1-\Pr\left(\max_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\max_{n=1,2,\ldots,N_{\mathrm{D}}}\left(\gamma_{\mathrm{S}_m\mathrm{D}_n}\right)\right)<\mu_2\right)\\&=1-\left[1-\exp\left(-\lambda_{\mathrm{SD}}\mu_2\right)\right]^{N_{\mathrm{S}}N_{\mathrm{D}}}.\end{aligned} \quad \text{(B.9)}$$

Tiếp theo, chúng ta có thể tính $\chi_{\mathrm{D},0}$ và $\chi_{\mathrm{D},1}$ tương ứng (B.10) như (3.30)

$$\begin{aligned}\chi_{\mathrm{D},0}&=\Pr\left(\max_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\max_{n=1,2,\ldots,N_{\mathrm{D}}}\left(\gamma_{\mathrm{S}_m\mathrm{D}_n}\right)\right)<\mu_1\right)\\&=\left(1-\exp\left(-\lambda_{\mathrm{SD}}\mu_1\right)\right)^{N_{\mathrm{S}}N_{\mathrm{D}}},\\\chi_{\mathrm{D},1}&=\Pr\left(\mu_1\leq\max_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\max_{n=1,2,\ldots,N_{\mathrm{D}}}\left(\gamma_{\mathrm{S}_m\mathrm{D}_n}\right)\right)<\mu_2\right)\\&=\left(1-\exp\left(-\lambda_{\mathrm{SD}}\mu_2\right)\right)^{N_{\mathrm{S}}N_{\mathrm{D}}}-\left(1-\exp\left(-\lambda_{\mathrm{SD}}\mu_1\right)\right)^{N_{\mathrm{S}}N_{\mathrm{D}}}.\end{aligned} \quad \text{(B.10)}$$

Tương tự, chúng ta có thể tính $\chi_{\mathrm{E},0}$, $\chi_{\mathrm{E},1}$ và $\chi_{\mathrm{E},2}$, tương ứng như (3.31).

• Trường hợp 2: Nút đích và nút nghe lén sử dụng kỹ thuật MRC, được tính trong (3.32).

Phụ lục C: Các chứng minh trong Chương 4

C.1. Dẫn xuất ρ_{D} và ρ_{E} của mô hình đề xuất 1 trong Phần 4.2

Để tính xác suất ρ_{D}, kết hợp (4.10) và (4.13), ta có:

$$\rho_{\mathrm{D}} = \Pr\left(\min_{n=1,2,\ldots,N}\left(C_n\right) < C_{\mathrm{th}}\right)$$

$$= 1 - \prod_{n=1}^{N}\left(1-\rho_{\mathrm{D},n}\right), \tag{C.1}$$

với $\rho_{\mathrm{D},n} = \Pr\left(C_n < C_{\mathrm{th}}\right)$. Sử dụng (4.9), ta có

$$\rho_{\mathrm{D},n} = \Pr\left(\frac{\omega\Delta\gamma_{\mathrm{B},n}\gamma_{\mathrm{D},n}}{\kappa_{\mathrm{D}}^2\omega\Delta\gamma_{\mathrm{B},n}\gamma_{\mathrm{D},n}+1} < \chi\right)$$

$$= \Pr\left(\left(1-\kappa_{\mathrm{D}}^2\chi\right)\omega\Delta\gamma_{\mathrm{B},n}\gamma_{\mathrm{D},n} < \chi\right), \tag{C.2}$$

với

$$\chi = 2^{\frac{NC_{\mathrm{th}}}{(1-\alpha)\tau}} - 1. \tag{C.3}$$

Ngoài ra, từ (C.2), nếu $1-\kappa_{\mathrm{D}}^2\chi \le 0$, thì $\rho_{\mathrm{D},n} = 1$ và nếu $1-\kappa_{\mathrm{D}}^2\chi > 0$, ta có:

$$\rho_{\mathrm{D},n} = \Pr\left(\gamma_{\mathrm{B},n}\gamma_{\mathrm{D},n} < \theta_{\mathrm{D}}\right)$$

$$= \int_0^{+\infty} F_{\gamma_{\mathrm{B},n}}\left(\frac{\theta_{\mathrm{D}}}{x}\right) f_{\gamma_{\mathrm{D},n}}\left(x\right)dx, \tag{C.4}$$

trong đó

$$\theta_{\mathrm{D}} = \frac{\chi}{\left(1-\kappa_{\mathrm{D}}^2\chi\right)\omega\Delta}. \tag{C.5}$$

Thay thế (4.1) và (4.5) vào (C.4), ta có

$$\rho_{\mathrm{D},n} = 1 - \exp\left(-K_{\mathrm{D}}\right) \sum_{k=0}^{+\infty} \frac{1}{\left(k!\right)^2} \left(K_{\mathrm{D}}\right)^k \left(\left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{D},n}\right)^{k+1}$$

$$\times \int_0^{+\infty} x^k \exp\left(-\frac{\lambda_{\mathrm{B},n}\theta_{\mathrm{D}}}{x}\right) \exp\left(-\left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{D},n} x\right) dx. \qquad \text{(C.6)}$$

Tiếp theo, áp dụng [110, công thức (3.471.9)] cho tích phân tương ứng trong (C.6), chúng ta đạt được

$$\rho_{\mathrm{D},n} = 1 - \sum_{k=0}^{+\infty} \frac{2}{\left(k!\right)^2} \left(K_{\mathrm{D}}\right)^k \exp\left(-K_{\mathrm{D}}\right) \times \left(\left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{B},n}\lambda_{\mathrm{D},n}\theta_{\mathrm{D}}\right)^{\frac{k+1}{2}}$$

$$\times K_{t+1}\left(2\sqrt{\left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{B},n}\lambda_{\mathrm{D},n}\theta_{\mathrm{D}}}\right), \qquad \text{(C.7)}$$

với $K_{t+1}(.)$ là hàm Bessel sửa đổi loại 2 [110].

Kết hợp (C.1) và (C.7) với nhau, chúng ta có thể biểu diễn ρ_{D} như trong (4.16), với $\psi_n = \left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{B},n}\lambda_{\mathrm{D},n}\theta_{\mathrm{D}}$. Tiếp theo, từ (4.11), ta có:

$$\rho_{\mathrm{E},N} = \Pr\left(C_{\mathrm{Eav}} < C_{\mathrm{th}}\right). \qquad \text{(C.8)}$$

Từ (C.8), với cùng phương pháp phân tích như trên, nếu $1-\kappa_{\mathrm{E}}^2\chi \le 0,$ thì $\rho_{\mathrm{E},N} = 1$ và nếu $1-\kappa_{\mathrm{E}}^2\chi > 0,$ chúng ta có thể đạt được:

$$\rho_{\mathrm{E},N} = 1 - \sum_{k=0}^{+\infty} \frac{2}{\left(k!\right)^2} \left(K_{\mathrm{E}}\right)^k \exp\left(-K_{\mathrm{E}}\right) \left(\psi_{\mathrm{E}}\right)^{\frac{k+1}{2}} K_{t+1}\left(2\sqrt{\psi_{\mathrm{E}}}\right), \qquad \text{(C.9)}$$

với

$$\theta_{\mathrm{E}} = \frac{\chi}{\left(1-\kappa_{\mathrm{E}}^2\chi\right)\omega\Delta},$$

$$\psi_{\mathrm{E}} = \left(1+K_{\mathrm{E}}\right)\lambda_{\mathrm{B},N-1}\lambda_{\mathrm{E}}\theta_{\mathrm{E}}. \qquad \text{(C.10)}$$

Tương tự như (C.1), xác suất của ρ_{E} có thể được biểu diễn là

$$\rho_{\mathrm{E}} = \Pr\left(C_{\mathrm{E}} < C_{\mathrm{th}}\right)$$

$$= 1 - \left[\prod_{n=1}^{N-1}\left(1-\rho_{\mathrm{D},n}\right)\right] \times \left(1-\rho_{\mathrm{E},N}\right). \qquad \text{(C.11)}$$

Thay (C.7) và (C.9) vào (C.11), biểu thức chính xác của ρ_{E} có thể đạt được như trong (4.17). Lưu ý rằng ρ_{E} phụ thuộc vào trạng thái giải mã tại chặng thứ n $\left(\rho_{\mathrm{D},n}\right)$, với $n=1,2,...,N-1$.

C.2. Dẫn xuất ρ_{D} và ρ_{E} của mô hình đề xuất 2 trong Phần 4.3

Đối với ρ_{D}, kết hợp (4.25) và (4.29), chúng ta có

$$\begin{aligned}\rho_{\mathrm{D}} &= \prod_{n=1}^{N} \Pr\left(\gamma_{\mathrm{D},n} \geq \frac{\theta}{\alpha\Delta}\right) \\ &= \prod_{n=1}^{N}\left[1-F_{\gamma_{\mathrm{D},n}}\left(\frac{\theta}{\alpha\Delta}\right)\right], \end{aligned} \tag{C.12}$$

với

$$\theta = 2^{NC_{\mathrm{th}}}-1.$$

Thay thế (4.20) vào (C.12), ta có thể đạt được ρ_{D} như trong (4.31).

Đối với ρ_{E}, kết hợp (4.25), (4.26) và (4.30), chúng ta đạt được

$$\begin{aligned}\rho_{\mathrm{E}} = &\sum_{n=1}^{N} \Pr\left(\frac{\alpha\Delta\gamma_{\mathrm{E},n}}{(1-\alpha)\Delta\gamma_{\mathrm{J},n}+1} \geq \theta\right) \\ &\times \prod_{q=1}^{n-1}\left[1-F_{\gamma_{\mathrm{D},q}}\left(\frac{\theta}{\alpha\Delta}\right)\right] \Pr\left(\frac{\alpha\Delta\gamma_{\mathrm{E},q}}{(1-\alpha)\Delta\gamma_{\mathrm{J},q}+1} < \theta\right). \end{aligned} \tag{C.13}$$

Xem xét xác suất $\Pr\left(\frac{\alpha\Delta\gamma_{\mathrm{E},q}}{(1-\alpha)\Delta\gamma_{\mathrm{J},q}+1} < \theta\right)$ trong (C.13), được tính là

$$\begin{aligned}\Pr\left(\frac{\alpha\Delta\gamma_{\mathrm{E},q}}{(1-\alpha)\Delta\gamma_{\mathrm{J},q}+1} < \theta\right) &= \Pr\left(\gamma_{\mathrm{E},q} < \omega_1 + \omega_2\gamma_{\mathrm{J},q}\right) \\ &= \int_0^{+\infty} F_{\gamma_{\mathrm{E},q}}\left(\omega_1+\omega_2 x\right) f_{\gamma_{\mathrm{J},q}}\left(x\right) dx, \end{aligned} \tag{C.14}$$

với

$$\omega_1 = \frac{\theta}{\alpha\Delta},\ \omega_2 = \frac{(1-\alpha)\theta}{\alpha}.$$

Kết hợp (4.20), (4.22) và (C.14) với nhau, sau một số phép tính toán, ta có

$$\Pr\left(\frac{\alpha\Delta\gamma_{\mathrm{E},q}}{(1-\alpha)\Delta\gamma_{\mathrm{J},q}+1}<\theta\right)=1-\frac{\lambda_{\mathrm{J},q}}{\lambda_{\mathrm{J},q}+\lambda_{\mathrm{E},q}\omega_2}\exp\left(-\lambda_{\mathrm{E},q}\omega_1\right). \qquad \text{(C.15)}$$

Cùng với cách thức tương tự như dẫn xuất (C.15), chúng ta có thể viết xác suất $\Pr\left(\frac{\alpha\Delta\gamma_{\mathrm{E},n}}{(1-\alpha)\Delta\gamma_{\mathrm{J},n}+1}\geq\theta\right)$ trong (C.13) là

$$\Pr\left(\frac{\alpha\Delta\gamma_{\mathrm{E},n}}{(1-\alpha)\Delta\gamma_{\mathrm{J},n}+1}\geq\theta\right)=\frac{\lambda_{\mathrm{J},n}}{\lambda_{\mathrm{J},n}+\lambda_{\mathrm{E},n}\omega_2}\exp\left(-\lambda_{\mathrm{E},n}\omega_1\right). \qquad \text{(C.16)}$$

Thay thế (4.20), (C.15) và (C.16) vào (C.13), ta có biểu thức xác suất dạng chính xác của ρ_{E} như trong (4.32).

DANH MỤC CÁC CÔNG TRÌNH ĐÃ CÔNG BỐ

A. CÁC CÔNG TRÌNH SỬ DỤNG KẾT QUẢ TRONG LUẬN ÁN

[*A1*] **Đặng Thế Hùng**, Trần Trung Duy và Đỗ Quốc Trinh, "Nghiên Cứu Hiệu Năng Truyền Bảo Mật Sử Dụng Mã Fountain Trong Mạng Vô Tuyến Nhận Thức Dưới Sự Tác Động Của Khiếm Khuyết Phần Cứng," *Tạp Chí Nghiên Cứu Khoa Học và Công Nghệ Quân Sự*, số 59, trang 58-69, 02/2019, ISSN: 1859-1043.

[*A2*] **Đặng Thế Hùng**, Trần Trung Duy và Đỗ Quốc Trinh, "Đánh Giá Khả Năng Giải Mã và Bảo Mật Dữ Liệu Thành Công Trong Mạng MIMO TAS/SC Sử Dụng Mã Fountain Dưới Tác Động Của Giao Thoa Đồng Kênh," *Tạp Chí Khoa Học và Kỹ Thuật, Học Viện Kỹ Thuật Quân Sự*, số 192, trang 89-102, 08/2018, ISSN: 1859-0209.

[*A3*] **D. T. Hung**, T. T. Duy, T. T. Phuong, D. Q. Trinh, and T. Hanh, "Performance Comparison between Fountain Codes-Based Secure MIMO Protocols With and Without Using Non-Orthogonal Multiple Access," *Entropy*, vol. 21, no. 10, (928), Oct. 2019, SCIE/Q2, IF: 2.494, DOI: https://doi:10.3390/e21100982, ISSN: 1099-4300.

[*A4*] **D. T. Hung**, T. T. Duy, D. Q. Trinh, V. N. Q. Bao, and T. Hanh, "Security-Reliability Analysis of Power Beacon-Assisted Multi-hop Relaying Networks Exploiting Fountain Codes with Hardware Imperfection," in *The International Conference on Advanced Technologies for Communications (ATC)*, 2018, Ho Chi Minh city, Vietnam, pp. 354-359, Oct. 2018, DOI: 10.1109/ATC.2018.8587493.

[*A5*] **D. T. Hung**, T. T. Duy, and D. Q. Trinh, "Security-Reliability Analysis of Multi-hop LEACH Protocol with Fountain Codes and Cooperative Jamming," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems,* vol. 6, no. 18, pp. 1-7, March 2019, DOI: http://dx.doi.org/10.4108/eai.28-3-2019.157120, ISSN: 2410-0218.

B. CÁC CÔNG BỐ KHÁC TRONG THỜI GIAN THỰC HIỆN LUẬN ÁN

[*B1*] **Đặng Thế Hùng**, T. T. Duy, V. N. Q. Bảo, Đ. Q. Trinh và T. Hạnh, "Phân Tích Hiệu Năng Mô Hình Truyền Đường Xuống Sử Dụng Kỹ Thuật Chọn Lựa Ăng-ten Phát và Mã Fountain Dưới Sự Ảnh Hưởng Của Nhiễu Đồng Kênh," *REV-ECIT 2017*, trang 270-274, TP. HCM, Việt Nam, 12/2017.

[*B2*] P. T. Tin, **D. T. Hung**, T. T. Duy, and M. Voznak, "Security-Reliability Analysis of NOMA-based Multi-Hop Relay Networks in Presence of an Active Eavesdropper with Imperfect Eavesdropping CSI," *Advances in Electrical and Electronic Engineering (AEEE),* vol. 15, no. 4, pp. 591-597, Nov. 2017, (Scopus).

[*B3*] **D. T. Hung**, T. T. Duy, D. Q. Trinh, and V. N. Q. Bao, "Secrecy Performance Evaluation of TAS Protocol Exploiting Fountain Codes and Cooperative Jamming under Impact of Hardware Impairments," in *SigTelCom 2018,* HCM city, Vietnam, pp. 164-169, Jan. 2018.

[*B4*] **Đặng Thế Hùng**, T. T. Duy, L. C. Khẩn và Đ. Q. Trinh, "Đánh Giá Hiệu Năng Xác Suất Dừng Mạng Thông Tin Vệ Tinh Chuyển Tiếp Hai Chiều Sử Dụng Mã Fountain," *REV-ECIT 2019,* trang 152-156, Hà Nội, Việt Nam, 12/2019.

[*B5*] B. Q. Đức, **Đặng Thế Hùng**, T. T. Duy và N. T. Bình, "Phân Tích Hiệu Năng Mạng Khuếch Đại Chuyển Tiếp Đa Chặng Dưới Sự Ảnh Hưởng Chung Của Nhiễu Đồng Kênh Và Nhiễu Phần Cứng," *REV-ECIT 2019*, trang 247-252, Hà Nội, Việt Nam, 12/2019.

[*B6*] Đ. V. Phương, N. T. Đông, **Đặng Thế Hùng** và H. V. Toàn, "Xác Suất Dừng Hệ Thống FD-NOMA Với Nút Chuyển Tiếp Sử Dụng Công Nghệ Thu Thập Năng Lượng," *REV-ECIT 2019*, trang 283-288, Hà Nội, Việt Nam, 12/2019.

[*B7*] P. T. Tin, **D. T. Hung**, N. N. Tan, T. T. Duy, and M. Voznak, "Secrecy Performance Enhancement for Underlay Cognitive Radio Networks Employing Cooperative Multi-hop Transmission With and Without Presence of Hardware Impairments," *Entropy*, vol. 21, no. 2, (217), Feb. 2019, SCIE/Q2, IF: 2.494.

[*B8*] **Đặng Thế Hùng** và N. T. Dũng, "Phân Tích Hiệu Năng Truyền Bảo Mật Sử Dụng Mã Fountain Với Kỹ Thuật Lựa Chọn Ăng-ten Phát," *REV-ECIT 2020*, trang 108-113, Hà Nội, Việt Nam, 12/2020.

[*B9*] **Đặng Thế Hùng**, L. C. Khẩn, N. V. Toàn và Đ. Q. Trinh, "Nghiên Cứu Hiệu Năng Bảo Mật Lớp Vật Lý Cho Mạng Chuyển Tiếp Lai Ghép Vệ Tinh-Mặt Đất Dưới Sự Tác Động Của Nhiễu Đồng Kênh Và Nhiễu Phần Cứng," *Tạp Chí Khoa Học Công Nghệ Thông Tin và Truyền Thông, Học Viện Công Nghệ Bưu Chính Viễn Thông*, số …, trang …, 12/2020, ISSN: 2525-2224, (Đã được chấp nhận đăng).

TÀI LIỆU THAM KHẢO

[1] A. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe, and T. Thomas, "LTE Advanced: Next-Generation Wireless Broadband Technology," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 10-22, June 2010.

[2] S. Singh, *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography,* 1st ed. New York, NY, USA: Doubleday, 1999.

[3] M. Loukides and J. Gilmore. *Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design,* 1998.

[4] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Techn. J.*, vol. 28, no. 4, pp. 656-715, Oct. 1949.

[5] A. Wyner, "The Wire-tap Channel," *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[6] I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Trans. Inf. Theory,* vol. 24, no. 3, pp. 339-348, May 1978.

[7] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian Wire-tap Channel," *IEEE Trans. on Inf. Theory,* vol. 24, no. 4, pp. 451-456, Jul. 1978.

[8] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Trans. Inf. Theory,* vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[9] S. Goel and R. Negi, "Guaranteeing Secrecy Using Artificial Noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, June 2008.

[10] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[11] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure Transmission with Optimal Power Allocation in Untrusted Relay Networks," *IEEE Wirel. Commun. Lett.*, vol. 3, no. 3, pp. 289-292, June 2014.

[12] J. Zhang, T. Q. Duong, R. Woods, and A. Marshall, "Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview," *Entropy*, vol. 19, no. 8, pp. 420, 2017.

[13] G. Li, C. Sun, J. Zhang, E. Jorswieck, B. Xiao, and A. Hu, "Physical Layer Key Generation in 5G and Beyond Wireless Communications: Challenges and Opportunities," *Entropy*, vol. 21, no. 5, pp. 497, 2019.

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

[15] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-Time Codes for High Data Rate Wireless Communication: Performance Criteria and Code Construction," *IEEE Trans. Inform. Theory*, vol. 44, no. 2, pp. 744-765, Mar. 1998.

[16] G. J. Foschini and M.J. Gans, "On Limits of Wireless Communications in a Fading Environment when Using Multiple Antennas," *Wireless Pers. Commun.*, vol. 6, no. 3, pp. 311-335, 1998.

[17] S. Sanayei and A. Nosratinia, "Antenna Selection in MIMO Systems," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 68-73, Oct. 2004.

[18] T. S. Rappaport, *Wireless Communications Principles and Practice.* Upper Saddle River, NJ, Prentice Hall PTR, 1996.

[19] T. Liu and S. Shamai (Shitz), "A Note on the Secrecy Capacity of the Multiple-Antenna Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547-2553, June 2009.

[20] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144-154, Jan. 2013.

[21] S. M. R. Islam, N. Avazov, O. A. Dobre, and K. Kwak, "Power-Domain Non-Orthogonal Multiple Access (NOMA) in 5G Systems: Potentials and Challenges," *IEEE Commun. Surv. Tutor.*, vol. 19, no. 2, pp. 721-742, 2017.

[22] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, "A Survey of Non-Orthogonal Multiple Access for 5G," *IEEE Commun. Surv. Tutor*, vol. 20, no. 3, pp. 2294-2323, 2018.

[23] Y. Liu, G. Pan, H. Zhang, and M. Song, "On the Capacity Comparison Between MIMO-NOMA and MIMO-OMA," *IEEE Access*, vol. 4, pp. 2123-2129, May 2016.

[24] Y. Yu, H. Chen, Y. Li, Z. Ding, L. Song, and B. Vucetic, "Antenna Selection for MIMO Non-Orthogonal Multiple Access Systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3158-3171, Apr. 2018.

[25] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and F. Lajos Hanzo, "Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access in Large Scale Networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656-1672, Mar. 2017.

[26] H. Lei, J. Zhang, K. H. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M. S. Alouini, "On Secure NOMA Systems With Transmit Antenna Selection Schemes," *IEEE Access*, vol. 5, pp. 17450-17464, 2017.

[27] M. O. Hasna and M. S. Alouini, "End-to-End Performance of Transmission System with Relays over Rayleigh Fading Channels," *IEEE Trans. Wireless Commun.*, vol. 2, no. 6, pp. 1126-1131, Nov. 2003.

[28] V. N. Q. Bao and N. Linh-Trung, "Multihop Decode-and-Forward Relay Networks: Secrecy Analysis and Relay Position Optimization," *REV Journal on Electronics and Communications*, vol. 2, no. 1-2, pp. 33-42, June 2012.

[29] T. T. Duy and H. Y. Kong, "Secrecy Performance Analysis of Multihop Transmission Protocols in Cluster Networks," *Wireless Pers. Commun.*, vol. 82, no. 4, pp. 2505-2518, 2015.

[30] J. Byers, M. Luby, M. Mitzenmacher, and A. Rege, "A Digital Fountain Approach to Reliable Distribution of Bulk Data", in *Proc. of ACM SIGCOMM*, pp. 56-67, Sept. 1998.

[31] M. Luby, "LT Codes," in *The 43rd Annual IEEE Symposium on Foundations of Computer Science*, pp. 271-280, 2002.

[32] D. J. C. Mackay, "Fountain Codes," *IEE Proc. Commun.*, vol. 152, pp. 1062-1068, Dec. 2005.

[33] A. Shokrollahi, "Raptor Codes," *IEEE Trans. Inform. Theory*, vol. 52, pp. 2551-2567, Jun. 2006.

[34] J. Castura and Y. Mao, "Rateless Coding over Fading Channels," *IEEE Commun. Lett.*, vol. 10, no. 1, pp. 46-48, Jan. 2006.

[35] J. Castura and Y. Mao, "Rateless Coding for Wireless Relay Channels," *IEEE Trans. Wireless Commun.*, vol. 6, no. 5, pp. 1638-1642, May 2007.

[36] A. F. Molisch, N. B. Mehta, J. S. Yedidia, and J. Zhang, "Performance of Fountain Codes in Collaborative Relay Networks," *IEEE Trans. Wirel. Commun.*, vol. 6, no. 11, pp. 4108-4119, Nov. 2007.

[37] H. D. T. Nguyen, L. N. Tran, and E. K. Hong, "On Transmission Efficiency for Wireless Broadcast Using Network Coding and Fountain Codes," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 569-571, May 2011.

[38] T. T. Duy and H.Y. Kong, "Secondary Spectrum Access in Cognitive Radio Networks Using Rateless Codes over Rayleigh Fading Channels," *Wireless Pers. Commun.*, vol. 77, no. 2, pp. 963-978, Jul. 2014.

[39] X. Di, K. Xiong, P. Fan, and H. C. Yang, "Simultaneous Wireless Information and Power Transfer in Cooperative Relay Networks with Rateless Codes," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 2981-2996, Apr. 2017.

[40] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, “Exploiting Fountain Codes for Secure Wireless Delivery,” *IEEE Commun. Lett.,* vol. 18, no. 5, pp. 777-780, May 2014.

[41] A. S. Khan, A. Tassi, and I. Chatzigeorgiou, “Rethinking the Intercept Probability of Random Linear Network Coding,” *IEEE Commun. Lett.,* vol. 19, no. 10, pp. 1762-1765, Oct. 2015.

[42] Q. Du, Y. Xu, W. Li, and H. Song, “Security Enhancement for Multicast over Internet of Things by Dynamically Constructed Fountain Codes,” *Wirel. Commun. Mob. Comput.,* vol. 2018, Article ID 8404219, pp. 1-11, 2018.

[43] L. Sun, P. Ren, Q. Du, and Y. Wang, “Fountain-Coding Aided Strategy for Secure Cooperative Transmission in Industrial Wireless Sensor Networks,” *IEEE Trans. Industrial Inform.,* vol. 12, no. 1, pp. 291-300, Feb. 2016.

[44] A. S. Khan and I. Chatzigeorgiou, “Opportunistic Relaying and Random Linear Network Coding for Secure and Reliable Communication,” *IEEE Trans. Wirel. Commun.,* vol. 17, no. 1, pp. 223-234, Jan. 2018.

[45] L. Sun and H. Xu, “Fountain-Coding-Based Secure Communications Exploiting Outage Prediction and Limited Feedback,” *IEEE Trans. Veh. Technol.,* vol. 68, no. 1, pp. 740-753, Jan. 2019.

[46] P. T. Tin, N. N. Tan, N. Q. Sang, T. T. Duy, T. T. Phuong, and M. Voznak, “Rateless Codes based Secure Communication Employing Transmit Antenna Selection and Harvest-To-Jam under Joint Effect of Interference and Hardware Impairments,” *Entropy*, vol. 21, no. 7, pp. 700, Jul. 2019.

[47] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems*. Springer Publishing Company, Incorporated, 2013.

[48] B. Schneier, “Cryptographic Design Vulnerabilities,” *IEEE Comput.,* vol. 31, no. 9, pp. 29-33, sept. 1998.

[49] D. Stinson, *Cryptography: Theory and Practice.* Chapman & Hall/CRC, 2005.

[50] S. Sanayei and A. Nosratinia, "Antenna Selection in MIMO Systems," *IEEE Commun. Mag.*, vol. 42, pp. 68-73, Oct 2004.

[51] H. Zhang, A. F. Molisch, and J. Zhang, "Applying Antenna Selection in WLANs for Achieving Broadband Multimedia Communications," *IEEE Trans. Broadcasting,* vol. 52, no 4, pp. 475-482, Dec. 2006.

[52] Q. Li, X. E. Lin, J. Zhang, and W. Rho, "Advancement of MIMO Technology in WiMAX: from IEEE 802.16d/e/j to 802.16m," *IEEE Commun. Mag.*, vol. 47, no. 6, pp. 100-107, Jun 2009.

[53] N. B. Mehta, S. Kashyap, and A. F. Molisch, "Antenna Selection in LTE: from Movitation to Specification," *IEEE Commun. Mag.,* vol. 50, no. 10, pp. 144-150, 2012.

[54] J. Mitola and G. Q. Maguire, "Cognitive Radio: Making Software Radios more Personal," *IEEE Personal Commun.,* vol. 6, no. 4, pp. 13-18, Aug. 1999.

[55] T. T. Duy and P. N. Son, "Secrecy Performances of Multicast Underlay Cognitive Protocols with Partial Relay Selection and without Eavesdroppers Information," *KSII Trans. Internet and Inform. Syst.,* vol. 9, no. 11, pp. 4623-4643, Nov. 2015.

[56] J. Mo, M. Tao, and Y. Liu, "Relay Placement for Physical Layer Security: A Secure Connection Perspective," *IEEE Commun. Lett.,* vol. 16, no. 6, pp. 878-881, June 2012.

[57] X. Xu, W. Yang, Y. Cai, and S. Jin, "On the Secure Spectral-Energy Efficiency Tradeoff in Random Cognitive Radio Networks," *IEEE J. Sel. Areas Commun.,* vol. 34, no. 10, pp. 2706-2722, Oct. 2016.

[58] L. Yang, H. Jiang, S. A. Vorobyov, J. Chen, and H. Zhang, "Secure Communications in Underlay Cognitive Radio Networks: User Scheduling and

Performance Analysis," *IEEE Commun. Lett.,* vol. 20, no. 6, pp. 1191-1194, June 2016.

[59] K. Lee, C. Chae, and J. Kang, "Spectrum Leasing via Cooperation for Enhanced Physical-Layer Secrecy," *IEEE Trans. Veh. Technol.,* vol. 62, no. 9, Nov. 2013.

[60] P. Chakraborty and S. Prakriya, "Secrecy Outage Performance of a Cooperative Cognitive Relay Network," *IEEE Commun. Lett.,* vol. 21, no. 2, pp. 326-329, Feb. 2017.

[61] X. Xu, W. Yang, and Y. Cai, "Opportunistic Relay Selection Improves Reliability-Reliability Tradeoff and Security-Reliability Tradeoff in Random Cognitive Radio Networks," *IET Commun.,* vol. 11, no. 3, pp. 335-343, Feb. 2017.

[62] P. Yan, Y. Zou, and J. Zhu, "Energy-Aware Multiuser Scheduling for Physical-Layer Security in Energy-Harvesting Underlay Cognitive Radio Systems," *IEEE Trans. Veh. Technol.,* vol. 67, no. 3, pp. 2084-2096, Mar. 2018.

[63] T. D. Hieu, T. T. Duy, and S. G. Choi, "Secrecy Performance of a Generalized Partial Relay Selection Protocol in Underlay Cognitive Networks," *Int. J. of Commun. Syst.,* vol. 31, no. 17, pp. 1-17, Nov. 2018.

[64] K. Ho-Van and T. Do-Dac, "Performance Analysis of Jamming Technique in Energy Harvesting Cognitive Radio Networks," *Telecomm. Sys.,* vol. 70, no. 3, pp. 321-336, Mar. 2019.

[65] J. M. Meredith, "Study on Downlink Multiuser Superposition Transmission for LTE", in *TSG RAN Meeting,* vol. 67, 2015.

[66] T. Schenk, *RF Imperfections in High-Rate Wireless Systems: Impact and Digital Compensation,* Springer, 2008.

[67] E. Björnson, P. Zetterberg, M. Bengtsson, and B. Ottersten, "Capacity Limits and Multiplexing Gains of MIMO Channels with Transceiver Impairments," *IEEE Commun. Lett.*, vol. 17, no. 1, pp. 91-94, Jan. 2013.

[68] E. Björnson, M. Matthaiou, and M. Debbah, "A New Look at Dual-hop Relaying: Performance Limits with Hardware Impairments," *IEEE Trans. Commun.*, vol. 61, pp. 4512-4525, 2013.

[69] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying Protocols for Wireless Energy Harvesting and Information Processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622-3636, July 2013.

[70] S. Goel and R. Negi, "Guaranteeing Secrecy Using Artificial Noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, June 2008.

[71] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[72] G. R. Sakthidharan and S. Chitra, "A Survey on Wireless Sensor Network: An Application Perspective," *2012 International Conference on Computer Communication and Informatics,* Coimbatore, 2012, pp. 1-5.

[73] Z. Zhou, S. Zhou, S. Cui, and J. Cui, "Energy-Efficient Cooperative Communication in a Clustered Wireless Sensor Network," *IEEE Trans. Veh. Technol.*, vol. 57, no. 6, pp. 3618-3628, Nov. 2008.

[74] Asaduzzaman and H. Y. Kong, "Energy Efficient Cooperative LEACH Protocol for Wireless Sensor Networks," *J. Commun. Networks,* vol. 12, no. 4, pp. 358-365, 2010.

[75] S. K. Singh, P. Kumar, and J. P. Singh, "A Survey on Successors of LEACH Protocol," *IEEE Access*, vol. 5, pp. 4298-4328, 2017.

[76] S. Marano, V. Matta, and P. K. Witlett, "Distributed Detection with Censoring Sensors under Physical Layer Secrecy," *IEEE Trans. Signal Process.*, vol. 57, no. 5, pp. 1976-1986, May 2009.

[77] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical Layer Security of TAS/MRC with Antenna Correlation," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 1, pp. 254-259, Jan. 2013.

[78] J. Xiong, Y. Tang, D. Ma, P. Xiao, and K. -K. Wong, "Secrecy Performance Analysis for TAS-MRC System with Imperfect Feedback," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 8, pp. 1617-1629, Aug. 2015.

[79] H. Zhao, Y. Tan, G. Pan, Y. Chen, and N. Yang, "Secrecy Outage on Transmit Antenna Selection/Maximal Ratio Combining in MIMO Cognitive Radio Networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10236-10242, Dec. 2016.

[80] M. Li, Y. Huang, H. Yin, Y. Wang, and C. Cai, "Improving the Security and Spectrum Efficiency in Overlay Cognitive Full-Duplex Wireless Networks," *IEEE Access*, vol. 7, pp. 68359-68372, 2019.

[81] G. Pan, H. Lei, Y. Deng, L. Fan, J. Yang, Y. Chen, and Z. Ding, "On Secrecy Performance of MISO SWIPT Systems with TAS and Imperfect CSI," *IEEE Commun.*, vol. 64, no. 9, pp. 3831-3843, Sep. 2016.

[82] Y. Huang, P. Zhang, Q. Wu, and J. Wang, "Secrecy Performance of Wireless Powered Communication Networks With Multiple Eavesdroppers and Outdated CSI," *IEEE Access*, vol. 6, pp. 33774-33788, 2018.

[83] R. Zhao, H. Lin, Y. C. He, D. H. Chen, Y. Huang, and L. Yang, "Secrecy Performance of Transmit Antenna Selection for MIMO Relay Systems with Outdated CSI," *IEEE Trans. Commun.*, vol. 66, no. 2, pp. 546-559, Feb. 2018.

[84] X. Tang, Y. Cai, Y. Huang, T. Q. Duong, W. Yang, and W. Yang, "Secrecy Outage Analysis of Buffer-Aided Cooperative MIMO Relaying Systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2035-2048, Mar. 2018.

[85] H. Lei, J. Zhang, K. H. Park, P. Xu, Z. Zhang, G. Pan, and M. S. Alouini, "Secrecy Outage of Max-Min TAS Scheme in MIMO-NOMA Systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 6981-6990, Aug. 2018.

[86] Z. Wang and Z. Peng, "Secrecy Performance Analysis of Relay Selection in Cooperative NOMA Systems," *IEEE Access*, vol. 7, pp. 86274-86287, 2019.

[87] 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," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2682-2696, Mar. 2019.

[88] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical Layer Security in Cognitive Radio Inspired NOMA Network," *IEEE J. Sel. Top. Sig. Process.*, vol. 13, no. 3, pp. 700-714, June 2019.

[89] 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," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 83-96, Jan. 2019.

[90] C. Xu, M. Zheng, W. Liang, H. Yu, and Y. C. Liang, "End-to-End Throughput Maximization for Underlay Multi-hop Cognitive Radio Networks with RF Energy Harvesting," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3561-3572, Jun. 2017.

[91] V. N. Q. Bao, N. T. Van, and T. T. Duy, "Exact Outage Analysis of Energy-Harvesting Multihop Cluster-Based Networks with Multiple Power Beacons over Nakagami-*m* Fading Channels," in *SigTelCom*, HCM city, Vietnam, 2018, pp. 1-6.

[92] C. Zhong, H. Liang, H. Lin, H. A. Suraweera, F. Qu, and Z. Zhang, "Energy Beamformer and Time Split Design for Wireless Powered Two-Way Relaying Systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 1-14, Jun. 2018.

[93] T. D. Hieu, T. T. Duy, L. T. Dung, and S. G. Choi, "Performance Evaluation of Relay Selection Schemes in Beacon-Assisted Dual-hop Cognitive Radio Wireless Sensor Networks under Impact of Hardware Noises," *Sensors*, vol. 18, no. 6, pp. 1-24, Jun. 2018.

[94] T. D. Hieu, T. T. Duy, and B.-S. Kim, "Performance Enhancement for Multi-hop Harvest-to-Transmit WSNs with Path-Selection Methods in

Presence of Eavesdroppers and Hardware Noises," *IEEE Sensors J.*, vol. 18, no. 12, pp. 5173-5186, Jun. 2018.

[95] T. T. Duy, T. Q. Duong, T. L. Thanh, and V. N. Q. Bao, "Secrecy Performance Analysis with Relay Selection Methods under Impact of Co-channel Interference," *IET Commun.*, vol. 9, no. 11, pp. 1427-1435, Jul. 2015.

[96] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay Selection for Security Enhancement in Cognitive Relay Networks," *IEEE Commun. Lett.*, vol. 4, no. 1, pp. 46-49, Feb. 2015.

[97] Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo, "Relay-Selection Improves the Security-Reliability Trade-off in Cognitive Radio Systems," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215-228, Jan. 2015.

[98] T. T. Duy, Trung Q. Duong, D. B. da Costa, V. N. Q. Bao, and M. Elkashlan, "Proactive Relay Selection with Joint Impact of Hardware Impairment and Co-channel Interference," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1594-1606, May 2015.

[99] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Processes*, 4th ed., McGraw-Hill Europe: London, UK, 2002.

[100] V. N. Q. Bao, B. P. L. Phuong, and T. T. Thanh, "Performance Analysis of TAS/SC-Based MIMO Decode-and-Forward Relaying for Multi-hop Transmission over Rayleigh Fading Channels," in *ICCE 2012*, Hue, Vietnam, 2012, pp. 150-155.

[101] V. A. Aalo and C. Chayawan, "Outage Probability of Cellular Radio Systems Using Maximal Ratio Combining in Rayleigh Fading Channel with Multiple Interferers," *Electronics Letters*, vol. 36, no. 15, pp. 1314-1315, 2000.

[102] D. Qin, Y. Wang, F. Zhou, and K. K. Wong, "Performance Analysis of AF Relaying With Selection Combining in Nakagami-*m* Fading," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2375-2385, Sep. 2019.

[103] C. Yu, H. L. Ko, X. Peng, and W. Xie, "Secrecy Outage Performance Analysis for Cooperative NOMA Over Nakagami-*m* Channel," *IEEE Access*, vol. 7, pp. 79866-79876, 2019.

[104] S. V. Amari and R. B. Misra, "Closed-form Expressions for Distribution of Sum of Exponential Random Variables," *IEEE Trans. Reliab.*, vol. 46, no. 4, pp. 519-522, Dec. 1997.

[105] X. Wang, W. Chen, and Z. Cao, "A Rateless Coding Based Multi-relay Cooperative Transmission Scheme for Cognitive Radio Networks," in *IEEE Globecom*, Honolulu, HI, USA, 30 Nov. 2009, pp. 164-169.

[106] H. A. Suraweera, R. H. Y. Louie, Y. Li, G. K. Karagiannidis, and B. Vucetic, "Two Hop Amplify-and-Forward Transmission in Mixed Rayleigh and Rician Fading Channels," *IEEE Commun. Lett.*, vol. 13, no. 4, pp. 227-229, Apr. 2009.

[107] T. Q. Duong, T. T. Duy, M. Matthaiou, T. Tsiftsis, and G. K. Karagiannidis, "Cognitive Cooperative Networks in Dual-Hop Asymmetric Fading Channels," in *IEEE Globecom*, Atlanta, GA, 2013, pp. 977-983.

[108] J. N. Laneman, D. Tse, and G. Wornell, "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062-3080, Dec. 2004.

[109] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels: A Unified Approach to Performance Analysis.* Wiley, 2000.

[110] D. Zwillinger, *Table of integrals, series, and products.* Elsevier, 2014.