ĐẠI HỌC BÁCH KHOA HÀ NỘI

ĐỒ ÁN TỐT NGHIỆP

Cấp phát công suất phát cho các bên của mạng vô tuyến nhận thức trong điều kiện có kẻ nghe lén

VŨ XUÂN BẮC
bac.vx194230@sis.hust.edu.vn

Ngành: Kỹ thuật máy tính

Giảng viên hướng dẫn: TS. Trịnh Văn Chiến _____

Chữ kí GVHD

Khoa: Kỹ thuật máy tính

Trường: Công nghệ Thông tin và Truyền thông

HÀ NỘI, 06/2024

LỜI CẢM ƠN

Đồ án này không thể hoàn thành nếu không có những chia sẻ sâu sắc và quý báu từ thầy Trịnh Văn Chiến. Sự nhiệt tình, tận tâm và nghiêm túc của thầy đã truyền cảm hứng rất lớn để tôi theo đuổi đề tài này, một lĩnh vực rất mới, nhưng cũng rất thú vị với tôi. Thầy đã giúp tôi nhận ra những sai lầm trong tư duy và giúp tôi sửa cả những lỗi trình bày nhỏ nhất trong đồ án này. Thực sự, tôi rất khâm phục tài năng và sự tinh tế, cẩn thận của thầy.

Bên cạnh đó, tôi muốn gửi lời cảm ơn tới cô Ninh Thị Thanh Tâm, giảng viên Học viện Quản lý giáo dục, vì những gợi ý và hướng dẫn tôi làm quen với đề tài này. Cảm ơn Ngô Nam Khánh, sinh viên K65 khoa Kỹ thuật máy tính, vì những góp ý chân thành giúp tôi hoàn thiện đồ án.

Đặc biệt, tôi muốn bày tỏ tình yêu và sự biết ơn tới bố mẹ tôi vì vẫn luôn ở đó, cổ vũ, động viên tôi, là động lực, là chỗ dựa tinh thần và là mục tiêu cố gắng của tôi. Những lúc mệt mỏi và nản chí nhất, hình ảnh của bố mẹ luôn là động lực thôi thúc tôi phải cố gắng và sáng tạo.

Cuối cùng, tôi muốn cảm ơn Đại học Bách Khoa Hà Nội, cảm ơn Trường Công nghệ Thông tin và Truyền thông, cảm ơn thầy cô và bạn bè vì những bài học, những kỷ niệm quý báu thời sinh viên của tôi.

LỜI CAM KẾT

Họ và tên sinh viên: . . . . . .
MSSV: . . . . . .
Điện thoại liên lạc: . . . . . .
Email: . . . . . .
Lớp: . . . . . .
Chương trình đào tạo: . . . . . .

Tôi – Vũ Xuân Bắc – cam kết Đồ án Tốt nghiệp (ĐATN) là công trình nghiên cứu của bản thân tôi dưới sự hướng dẫn của TS. Trịnh Văn Chiến. Các kết quả nêu trong ĐATN là trung thực, là thành quả của riêng tôi, không sao chép theo bất kỳ công trình nào khác. Tất cả những tham khảo trong ĐATN – bao gồm hình ảnh, bảng biểu, số liệu, và các câu từ trích dẫn – đều được ghi rõ ràng và đầy đủ nguồn gốc trong danh mục tài liệu tham khảo. Tôi xin hoàn toàn chịu trách nhiệm với dù chỉ một sao chép vi phạm quy chế của nhà trường.

Hà Nội, ngày tháng năm

Tác giả ĐATN

Vũ Xuân Bắc

TÓM TẮT NỘI DUNG ĐỒ ÁN

Bảo mật lớp vật lý là một giải pháp tiềm năng giúp tăng cường an toàn thông tin trong truyền thông không dây. Cùng với các kỹ thuật mã hóa và xử lý tín hiệu, hợp tác cũng là một hướng tiếp cận giúp cải thiện mức độ an toàn. Một trong những mô hình mạng hợp tác tiềm năng cho công nghệ mạng di động thế hệ thứ năm (fifth generation - 5G) là mạng vô tuyến nhận thức, được giới thiệu với mục đích nâng cao hiệu quả sử dụng phổ. Trong mạng, bên sơ cấp có quyền sử dụng một phần tài nguyên tần số và sẵn sàng chia sẻ để các bên thứ cấp có thể khai thác sử dụng. Để truyền tin trên phần tài nguyên tần số của bên sơ cấp, bên thứ cấp có thể triển khai chiến lược truy cập phổ đồng thời, ở đó hai bên đồng thời truyền tin trong cùng khoảng thời gian và trên cùng dải tần số. Chiến lược này mặc dù giúp tận dụng hiệu quả tài nguyên tần số, song can nhiễu do tín hiệu từ bên thứ cấp lại làm giảm chất lượng tín hiệu nhận tại bên sơ cấp. Thế nhưng, khi xem xét thêm yêu cầu truyền tin an toàn, can nhiễu này có thể được tận dụng hiệu quả giúp bên sơ cấp cải thiện chất lượng truyền tin an toàn. Do đó, đồ án này đề xuất một giải pháp giúp lựa chọn công suất phát cho bên sơ cấp và thứ cấp của mạng vô tuyến nhận thức trong điều kiện có kẻ nghe lén ở cả hai bên, đảm bảo chất lượng truyền tin tin cậy và an toàn, ngay cả khi tốc độ truyền là cố định và các bên phát chỉ có thông tin thống kê về kênh truyền. Đồng thời, bằng việc mở rộng mô hình với nhiều bên thứ cấp, kết quả cho thấy bên sơ cấp có thể được lợi trong chiến lược hợp tác này. Với mô hình mở rộng, các bên thứ cấp cạnh tranh với nhau để được bên sơ cấp lựa chọn cùng hợp tác. Lúc này, khi là bên đề xuất chiến lược truyền, các bên thứ cấp phải cân nhắc lợi ích của cả hai bên để cân bằng giữa hai mục tiêu, đó là được truyền tin và chất lượng truyền tin an toàn.

MỤC LỤC

CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI 1

1.1 Đặt vấn đề 1

1.2 Các giải pháp hiện tại và hạn chế 1

1.3 Mục tiêu và định hướng giải pháp 3

1.4 Đóng góp của đồ án 4

1.5 Bố cục đồ án 4

CHƯƠNG 2. NỀN TẢNG LÝ THUYẾT 6

2.1 An toàn bảo mật lớp vật lý 6

2.2 Mạng vô tuyến nhận thức và an toàn bảo mật 7

2.3 Thông tin kênh truyền trong an toàn bảo mật 8

2.4 Các độ đo hiệu năng an toàn 9

2.4.1 Dung lượng an toàn và tốc độ an toàn 9

2.4.2 Xác suất mất an toàn 10

2.4.3 Công thức khác cho xác suất mất an toàn 10

2.4.4 Các độ đo dựa trên mức độ không rõ ràng 10

2.5 Tối ưu trong bài toán thiết kế 11

2.5.1 Bài toán tối ưu 12

2.5.2 Các phương pháp giải quyết bài toán tối ưu một mục tiêu 12

2.5.3 Tối ưu đa mục tiêu 15

2.5.4 Các phương pháp giải quyết bài toán tối ưu đa mục tiêu 17

2.6 Kết chương 19

CHƯƠNG 3. MÔ HÌNH HỆ THỐNG 21

3.1 Mô hình hệ thống 21

3.2 Mô hình tín hiệu 22

3.3 Lựa chọn hiệu năng cho bài toán 24
3.4 Phát biểu bài toán 25
3.5 Kết chương..... 26
CHƯƠNG 4. PHƯƠNG PHÁP ĐỀ XUẤT..... 27
4.1 Phân tích bài toán 27
4.1.1 Phân tích các đại lượng trong mô hình..... 27
4.1.2 Phân tích hàm mục tiêu..... 28
4.1.3 Phân tích điều kiện khả thi cho các ràng buộc 31
4.1.4 Phân tích trường hợp không hợp tác 33
4.2 Phát triển và giải quyết bài toán 34
4.2.1 Tối ưu cho người dùng thứ cấp 34
4.2.2 Mở rộng mô hình 35
4.3 Phương pháp giải quyết bài toán..... 36
4.4 Kết chương..... 36
CHƯƠNG 5. ĐÁNH GIÁ THỰC NGHIỆM..... 38
5.1 Các tham số thí nghiệm..... 38
5.2 Phương pháp thí nghiệm..... 39
5.3 Điều kiện ràng buộc về xác suất truyền tin trong trường hợp hợp tác..... 39
5.4 So sánh giữa các bài toán đề xuất 40
5.4.1 Trong điều kiện xác suất truyền tin tương đồng 41
5.4.2 Trong điều kiện kênh truyền nghe lén khác nhau..... 42
5.5 Hệ thống với nhiều người dùng thứ cấp..... 44
5.6 Kết chương..... 47
CHƯƠNG 6. KẾT LUẬN 50
6.1 Kết luận..... 50
6.2 Hướng phát triển trong tương lai 50

PHỤ LỤC **52**

A. Phân tích kênh truyền **52**

B. Phân tích mức độ không rõ ràng của kẻ nghe lén **54**

B.1 Hàm phân phối tích lũy 54

B.2 Giá trị kỳ vọng 55

B.2.1 Phụ thuộc vào biến ngẫu nhiên có phân phối mũ 55

B.2.2 Phụ thuộc vào hai biến ngẫu nhiên độc lập có phân phối mũ 55

C. Phân tích xác suất truyền tin **57**

C.1 Giá trị lớn nhất của xác suất truyền tin 57

C.2 Điều kiện để các bên đạt được xác suất truyền tin mong muốn 58

TÀI LIỆU THAM KHẢO **66**

DANH MỤC HÌNH VẼ

Hình 2.1 Biên Pareto 17

Hình 3.1 Mô hình hệ thống 22

Hình 5.1 Ảnh hưởng của xác suất truyền tin tối thiểu tới điều kiện khả thi của các bài toán tối ưu. $N = 50000$ 40

Hình 5.2 So sánh tốc độ lộ tin trung bình tại PU giữa các chiến lược tối ưu khác nhau. $N = 200000$ 41

Hình 5.3 So sánh xác suất truyền tin tại PU giữa các chiến lược tối ưu khác nhau. $N = 200000$ 42

Hình 5.4 So sánh tốc độ lộ thông tin giữa các chiến lược trong các trường hợp xác suất truyền tin tại PU tương đồng nhau. $N = 50000$. 43

Hình 5.5 So sánh tốc độ lộ thông tin giữa các chiến lược trong trường hợp điều kiện kênh truyền nghe lén khác nhau. $N = 100000$ 45

Hình 5.6 So sánh tốc độ lộ tin trung bình của PU và SU trong bài toán cạnh tranh với các giá trị $\theta^{(S)}$ khác nhau. $N = 50000$ 46

Hình 5.7 Đánh giá tốc độ lộ tin trong mô hình nhiều SU cạnh tranh. $N = 25000$ 48

Hình 5.8 Đánh giá xác suất truyền tin trong mô hình nhiều SU cạnh tranh. $N = 25000$ 49

Hình C.1 Tập G (phần bôi đậm) biểu diễn theo p_P và p_S với $p_P^{max} = 20$, $p_S^{max} = 20$ 60

DANH MỤC THUẬT NGỮ VÀ TỪ VIẾT TẮT

Thuật ngữ	Ý nghĩa
5G	Mạng di động thế hệ thứ năm (Fifth Generation)
AILR	Tốc độ lộ tin trung bình (Average Information Leakage Rate)
AN	Nhiễu nhân tạo (Artificial Noise)
ASOP	Xác suất mất an toàn thay thế (Alternative Secrecy Outage Probability)
CDF	Hàm phân phối tích lũy (Cumulative Distribution Function)
CRN	Mạng vô tuyến nhận thức (Cognitive Radio Network)
CSA	Truy cập phổ đồng thời (Concurrent Spectrum Access)
CSI	Thông tin kênh truyền (Channel State Information)
CSIR	Thông tin kênh truyền tại bên nhận (Channel State Information at the Receiver)
CSIT	Thông tin kênh truyền tại bên phát (Channel State Information at the Transmitter)
DSA	Truy cập phổ động (Dynamic Spectrum Access)
EAVP	Kẻ nghe lén bên sơ cấp
EAVS	Kẻ nghe lén bên thứ cấp
FSA	Truy cập phổ cố định (Fixed Spectrum Access)
GSOP	Xác suất mất an toàn tổng quát (Generalized Secrecy Outage Probability)

Thuật ngữ	Ý nghĩa
MOOP	Bài toán tối ưu đa mục tiêu (Multiobjective Optimization Problem)
OSA	Truy cập phổ cơ hội (Opportunistic Spectrum Access)
PLS	Bảo mật lớp vật lý (Physical Layer Security)
PRx	Bên nhận sơ cấp
PSD	Mật độ phổ công suất (Power Spectral Density)
PTx	Bên phát sơ cấp
PU	Bên sơ cấp (Primary User)
RIS	Bề mặt phản xạ thông minh (Reconfigurable Intelligent Surface)
SC	Dung lượng an toàn (Secrecy Capacity)
SEE	Hiệu quả năng lượng an toàn (Secrecy Energy Efficiency)
SINR	Tỷ số tín hiệu trên nhiễu và can nhiễu (Signal to Interference-plus-Noise Ratio)
SNR	Tỷ số tín hiệu trên nhiễu (Signal-to-Noise Ratio)
SOP	Xác suất mất an toàn (Secrecy Outage Probability)
SR	Tốc độ an toàn (Secrecy Rate)
SRx	Bên nhận thứ cấp
STx	Bên phát thứ cấp
SU	Bên thứ cấp (Secondary User)
TAS	Lựa chọn ăng-ten phát (Transmit Antenna Selection)

CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI

Chương đầu tiên của đồ án bắt đầu với việc nêu lên vấn đề cần giải quyết, đó là bài toán thiết kế an toàn bảo mật trong mạng vô tuyến nhận thức. Vấn đề nêu lên không phải là mới và thực tế có rất nhiều tác giả quan tâm nghiên cứu. Một số nghiên cứu cũng được giới thiệu trong chương này và được trình bày theo các hướng tiếp cận khác nhau. Trên cơ sở xác định những hạn chế của các nghiên cứu trước đây, đồ án lựa chọn mô hình cho vấn đề và nêu lên mục tiêu của nghiên cứu. Kết quả nghiên cứu được tóm tắt và tổng kết thành những đóng góp chính. Cuối chương là bố cục của đồ án, trình bày tổng quan nội dung của các chương tiếp theo.

1.1 Đặt vấn đề

Mạng vô tuyến nhận thức (cognitive radio network - CRN) là một công nghệ hứa hẹn giúp tăng hiệu quả sử dụng phổ tần số [1], ở đó, bên thứ cấp (secondary user - SU) vẫn có cơ hội được truyền tin trên dải tần số vốn chỉ dành cho bên sơ cấp (primary user - PU) sử dụng. Cũng giống như các mạng truyền thông khác, CRN cũng là mục tiêu tấn công an toàn bảo mật, đặc biệt là tấn công nghe lén, vì trong hệ thống có nhiều người dùng truyền tin. Một hướng tiếp cận an toàn bảo mật, mặc dù đã có nền tảng lý thuyết từ rất sớm, nhưng mới được quan tâm nghiên cứu gần đây là bảo mật lớp vật lý (physical layer security - PLS). Với các kết quả nghiên cứu sâu rộng, PLS cho thấy một giải pháp giúp tăng cường an toàn bảo mật trong truyền thông không dây, bao gồm cả CRN. Tuy nhiên, thiết kế an toàn bảo mật trong CRN có phần thách thức hơn, đặc biệt khi xem xét bên thứ cấp đồng thời truyền tin với bên sơ cấp, vì khi đó yêu cầu an toàn cần được đảm bảo ở cả hai bên. Ngoài ra, trong quá trình truyền tin, tín hiệu từ cả hai bên có thể tác động lẫn nhau, từ đó cũng đặt ra thêm yêu cầu về chất lượng truyền tin tin cậy và truyền tin an toàn cho bài toán thiết kế.

1.2 Các giải pháp hiện tại và hạn chế

Từ góc nhìn thiết kế hệ thống, các nghiên cứu về đảm bảo an toàn bảo mật trong mạng vô tuyến nhận thức thường tập trung vào các chủ đề (i) xử lý tín hiệu, (ii) lựa chọn hợp tác và (iii) cấp phát tài nguyên [2]. Các kỹ thuật liên quan đến xử lý tín hiệu như định hướng chùm tia (beamforming) hay sử dụng nhiễu nhân tạo (artificial noise - AN) thường được quan tâm nghiên cứu. Dựa trên kỹ thuật định hướng chùm tia, tác giả Kwon [3] đề xuất chiến lược cực đại hóa tốc độ truyền tin an toàn cho PU trong mạng CRN nhiều ăng-ten phát một ăng-ten thu (multiple input single output - MISO) với các mức độ khác nhau về thông tin mà bên phát có về kênh truyền nghe lén. Với mục tiêu thiết kế là cực đại hiệu quả năng lượng

an toàn (secrecy energy efficiency - SEE) của hệ thống, tác giả Ouyang [4] đề xuất chiến lược định hướng chùm tia tối ưu (optimal beamforming) và định hướng chùm tia dựa trên kỹ thuật ép không (zero-forcing based beamforming) để giải quyết bài toán tối ưu. Tác giả He [5] đã đề xuất chiến lược truy cập phổ cho các bên của CRN theo hai pha. Ở đó, trong pha truyền tin của mình, SU cần dành một phần năng lượng để phát lại tín hiệu tới bên nhận PU, đồng thời sinh nhiễu nhân tạo để cản trở kẻ nghe lén giải mã các thông điệp từ cả hai bên. Nhìn chung, kỹ thuật định hướng chùm tia được sử dụng nhằm khai thác khả năng tập trung năng lượng, từ đó giúp gia tăng chất lượng tín hiệu tại bên nhận hợp pháp. Nhiễu nhân tạo lại được thiết kế nhằm làm suy giảm chất lượng tín hiệu nhận tại bên nghe lén.

Hợp tác và xếp lịch cho các bên cũng là một hướng tiếp cận hiệu quả cho bài toán an toàn bảo mật. Với mô hình nhiều PU, nhiều SU và nhiều kẻ nghe lén, tác giả Houjeij và cộng sự [6] đã phân tích tương tác giữa các SU và kẻ nghe lén theo lý thuyết trò chơi (game theory). Trong mô hình đó, mỗi SU cần chọn kênh truyền của một trong các PU để truyền tin an toàn và hạn chế ảnh hưởng can nhiễu từ các SU khác; đồng thời, mỗi kẻ tấn công cần chọn một số kênh truyền của PU để nghe lén, đảm bảo tốc độ truyền tin an toàn của các SU là nhỏ nhất. Ở hướng tiếp cận khác, khi xem xét mô hình có nhiều SU cùng truyền tin tới một trạm gốc (base station) và nhiều kẻ nghe lén hợp tác với nhau, tác giả Zou [7] đề xuất một chiến lược lập lịch theo giải thuật định thời luân phiên (round-robin) cho các SU, đảm bảo hiệu năng an toàn của hệ thống là cao nhất. Tác giả Quach và các cộng sự [8] đề xuất một chiến lược tự điều chỉnh công suất phát cho các bên kết hợp với việc lựa chọn bộ phát lại (relay). Kết quả cho thấy tính hiệu quả của chiến lược hợp tác trong việc đảm bảo an toàn cho SU. Cũng dựa trên sự hỗ trợ của các bộ phát lại, tác giả Bouabdellah [9] xem xét trường hợp sử dụng bộ phát lại với nhiều ăng-ten thu và một ăng-ten phát, nhằm tăng cường tín hiệu cho SU. Kết quả cho thấy việc gia tăng số lượng ăng-ten thu cho bộ phát lại giúp tăng cường hiệu năng an toàn cho hệ thống. Có thể thấy, khi mở rộng mô hình với nhiều người dùng, ở đó có sự đa dạng về vị trí của các đối tượng, một chiến lược lựa chọn hợp tác phù hợp cũng giúp tăng cường hiệu năng an toàn cho toàn hệ thống.

Hướng tiếp cận an toàn bảo mật theo cấp phát tài nguyên thường liên quan đến việc sử dụng hiệu quả các tài nguyên như tần số, khe thời gian và năng lượng. Tác giả Wu [10] đã mô hình hóa bài toán xác định công suất phát cho các bên nhằm tối ưu tốc độ truyền an toàn ở PU và tốc độ truyền tin tin cậy ở SU theo lý thuyết trò chơi. Trong đó, tác giả đã xem xét lợi ích của PU trong vấn đề thiết kế khi PU có quyền ưu tiên chọn trước công suất phát và có thể quyết định không cùng truyền với SU nếu hiệu quả an toàn không cải thiện hơn khi truyền đơn lẻ. Khi nghiên cứu

hiệu năng của CRN với một ăng-ten phát nhiều ăng-ten thu (single input multiple output - SIMO), tác giả Hung [11] đề xuất chiến lược lựa chọn công suất phát cho SU đảm bảo truyền tin tin cậy và an toàn cho PU, đồng thời xem xét ảnh hưởng công suất phát từ PU lên chất lượng truyền tin an toàn của SU.

Như vậy, các nghiên cứu an toàn bảo mật trong mạng vô tuyến nhận thức được quan tâm nghiên cứu và khai thác ở nhiều khía cạnh khác nhau, cho thấy nhiều hướng tiếp cận tiềm năng giúp giải quyết vấn đề này. Tuy nhiên, các nghiên cứu này có một số giới hạn. Thứ nhất, bài toán thiết kế chỉ xem xét tính an toàn cho PU hoặc cho SU [3], [4], [6]–[10]. Với nghiên cứu [11], tác giả xem xét tính an toàn cho cả hai bên nhưng thiết kế công suất phát chỉ được đề cập cho bên SU. Thứ hai, để có được các chiến lược thiết kế có hiệu năng tốt, các nghiên cứu cũng giả thiết về thông tin kênh nghe lén mà bên phát có được là hoàn hảo hoặc chính xác một phần [3], [5], [10]. Giả thiết này thường khó đạt được trong thực tế, vì kẻ tấn công thường chỉ nghe lén và không có phản hồi tín hiệu tới bên phát. Thứ ba, mặc dù việc sử dụng các bộ phát lại giúp cải thiện chất lượng truyền tin và đảm bảo an toàn [8], [9], tính tin cậy và đồng bộ với bên thứ ba này cũng là một vấn đề cần quan tâm. Do đó, bài toán thiết kế an toàn bảo mật trong mạng vô tuyến nhận thức cần một mô hình gần với thực tế, giảm thiểu những hạn chế nêu trên.

1.3 Mục tiêu và định hướng giải pháp

Với mục tiêu phát triển một giải pháp truyền tin an toàn cho mạng vô tuyến nhận thức, mô hình truyền tin và bài toán thiết kế trong đồ án này được xem xét trong các điều kiện gần với thực tế khi: (i) tính an toàn của PU và SU đều được cân nhắc khi thiết kế chiến lược truyền tin, (ii) trong điều kiện thông tin kênh truyền về kẻ nghe lén là hạn chế và các bên chỉ ước lượng được khoảng cách từ kẻ nghe lén tới các bên phát, (iii) chỉ sử dụng tính chất hợp tác giữa PU và SU có sẵn trong mạng để đảm bảo an toàn cho cả hai bên, thay vì phụ thuộc vào một bên thứ ba như các bộ phát lại. Mô hình đề xuất này giúp tránh được một số hạn chế trong các nghiên cứu trước đây, đồng thời cũng khai thác sự hợp tác để giải quyết bài toán thiết kế ban đầu.

Ngoài ra, vấn đề lợi ích của PU trong việc chia sẻ tài nguyên tần số cho SU cũng được xem xét, khi mà PU có thể lựa chọn một trong nhiều SU đem lại hiệu quả an toàn cao nhất cho mình. Khi đó, bài toán truyền tin an toàn ban đầu trở thành bài toán cạnh tranh giữa các SU, ở đó, các SU cần cân nhắc giữa cơ hội được truyền tin và chất lượng truyền tin an toàn trong việc thiết kế chiến lược truyền khi đề xuất hợp tác tới PU.

1.4 Đóng góp của đồ án

Đồ án này có các đóng góp chính như sau:

- Đề xuất chiến lược xác định công suất phát cho bên sơ cấp và thứ cấp của mạng vô tuyến nhận thức, đảm bảo truyền tin tin cậy và an toàn cho hai bên.
- Khi xem xét tính cạnh tranh giữa các bên thứ cấp, khái niệm về "an toàn một phần" (partial secrecy) cũng được ứng dụng để các bên thứ cấp cân nhắc giữa mức độ an toàn và cơ hội được truyền tin cùng với bên sơ cấp.
- Các độ đo hiệu năng như lượng tin bị nghe lén và xác suất truyền tin tin cậy được biểu diễn cụ thể cho mô hình hệ thống đã nêu.
- Đồ án cũng cho thấy một hướng khai thác sự đa dạng về vị trí của các bên thứ cấp trong mạng để giúp cải thiện mức độ an toàn cho bên sơ cấp.

1.5 Bố cục đồ án

Phần còn lại của báo cáo đồ án tốt nghiệp này được tổ chức như sau:

Nội dung Chương 2 tập trung trình bày nền tảng lý thuyết và các kết quả nghiên cứu liên quan tới các công nghệ mà đồ án sử dụng. Mục tiêu của chương này là làm rõ ý tưởng cốt lõi của công nghệ bảo mật lớp vật lý và giới thiệu một số kỹ thuật giúp cải thiện mức độ an toàn. Trên cơ sở đó, chương này cho thấy một hướng tiếp cận giúp giải quyết vấn đề an toàn bảo mật trong mạng vô tuyến nhận thức. Để lượng hóa mức độ hiệu quả của giải pháp, chương này cũng giới thiệu một số độ đo đánh giá mức độ an toàn thường được sử dụng trong các nghiên cứu về bảo mật lớp vật lý. Cuối chương trình bày về lý thuyết tối ưu, một công cụ quan trọng giúp giải quyết các bài toán thiết kế.

Chương 3 trình bày kỹ hơn về mô hình hệ thống và mô hình truyền tin cho bài toán cần giải quyết. Với việc xác định rõ các đối tượng trong hệ thống cũng như đặc điểm kênh truyền, chương này lựa chọn các độ đo hiệu năng cho bài toán thiết kế. Cuối chương là phát biểu về bài toán tối ưu, mô hình cho bài toán thiết kế mà đồ án hướng tới giải quyết.

Với mô hình và bài toán xây dựng trong Chương 3, Chương 4 sẽ trình bày các phân tích và hướng giải quyết bài toán. Quá trình phân tích giúp làm rõ mối quan hệ giữa các đại lượng trong bài toán, tương ứng với các lợi ích khác nhau của các đối tượng trong hệ thống. Trên cơ sở phân tích đó, chương này trình bày các hướng giải quyết bài toán ban đầu. Một mô hình mở rộng cho bài toán cũng được đề xuất trong chương này.

Từ kết quả thu được trong Chương 4, phương pháp thử nghiệm và kết quả triển

khai với số liệu sẽ được thể hiện trong Chương 5. Các kết quả thử nghiệm góp phần chứng minh tính hiệu quả và nêu lên những hạn chế của giải pháp đề xuất.

Chương 6 là phần tổng kết các kết quả đạt được của đồ án này. Trên cơ sở các kết quả phân tích và thử nghiệm, chương này cũng nêu ra một số hướng phát triển trong tương lai, một phần giúp vượt qua các hạn chế của giải pháp đề xuất, một phần giúp mô hình hệ thống gần với thực tế.

CHƯƠNG 2. NỀN TẢNG LÝ THUYẾT

Chương 1 đã đề cập đến hai công nghệ trong truyền thông không dây là bảo mật lớp vật lý và mạng vô tuyến nhận thức. Các công nghệ này sẽ được trình bày kỹ hơn trong chương này. Mở đầu chương là giới thiệu tổng quan về bảo mật lớp vật lý và các kỹ thuật giúp tăng cường sự an toàn. Sau đó, mạng vô tuyến nhận thức được đề cập cùng với các vấn đề liên quan, đặc biệt là vấn đề an toàn bảo mật. Hai nền tảng để mô hình hóa bài toán thiết kế nêu lên trong chương trước được trình bày ở phần cuối chương, đó là các độ đo hiệu năng an toàn sử dụng để đánh giá và mô hình toán học của lý thuyết tối ưu.

2.1 An toàn bảo mật lớp vật lý

An toàn bảo mật thường được tiếp cận từ khái niệm an toàn tuyệt đối (perfect secrecy) của Shannon [12], theo đó, hệ thống sử dụng một chiến lược mã hóa với khóa chia sẻ bí mật và đảm bảo bản mã không mang bất kỳ thông tin nào của thông điệp cần gửi. Mức độ an toàn này yêu cầu độ dài của khóa không ít hơn độ dài của thông điệp cần gửi, trong khi khóa là không dùng lại và cần được chia sẻ bí mật. Bài toán truyền tin bảo mật chuyển thành bài toán trao đổi khóa với độ phức tạp tương đương. Mặt khác, phạm vi của hướng tiếp cận trên giới hạn bởi giả thiết kênh truyền không nhiễu, xem xét trường hợp tệ nhất khi mà kẻ tấn công có thể thu được chính xác bản mã. Song trong thực tế, nhiễu là một thành phần không thể thiếu trong hầu hết các kênh truyền vật lý.

Ở hướng khác, Wyner [13] giới thiệu mô hình kênh nghe lén (wiretap channel model), đánh giá ảnh hưởng của nhiễu trong truyền tin an toàn. Mô hình này đã đặt nền móng cho một hướng nghiên cứu gọi là bảo mật lớp vật lý. Mô hình của Wyner coi nhiễu như một đại lượng ngẫu nhiên giúp tăng khác biệt lợi thế giữa kênh truyền tới người dùng hợp pháp (gọi là kênh truyền chính - main channel) và kênh truyền tới kẻ tấn công (gọi là kênh truyền nghe lén - wiretap channel), cũng giống như lý thuyết của Shannon sử dụng khóa bí mật như một lợi thế về tính toán. Trong truyền thông không dây, cùng với nhiễu kênh truyền, các nghiên cứu sau này [14]–[20] cũng cho thấy các đặc tính kênh truyền suy hao như đa đường (multipath) hay hiệu ứng bóng râm (shadow), mặc dù vốn có nhiều ảnh hưởng tiêu cực đến truyền tin tin cậy (chất lượng khôi phục tín hiệu tại người dùng hợp pháp), lại đóng góp rất nhiều trong việc tăng lợi thế này.

Khi các đặc tính kênh truyền không đủ để gia tăng đáng kể lợi thế giữa kênh truyền chính và kênh truyền nghe lén, một giải pháp được sử dụng là chèn nhiễu nhân tạo (artificial noise - AN) nhằm làm suy giảm chất lượng giải mã tín hiệu

nhận tại bên nghe lén [21]. Nhiễu nhân tạo thường được triển khai trên các bộ hỗ trợ (helpers) hoặc sử dụng thêm các ăng-ten với kỹ thuật định hướng chùm tia [22]–[24]. Ngoài ra, định hướng chùm tia hay hợp tác với các bộ hỗ trợ cũng có thể nhằm mục đích tăng cường chất lượng tín hiệu tại người dùng hợp pháp [8], [24]. Tuy nhiên các hướng tiếp cận này có một số hạn chế. Dưới góc nhìn thiết kế hệ thống, sinh nhiễu không mang thông tin như nhiễu nhân tạo là một giải pháp sử dụng năng lượng không hiệu quả, đồng thời làm giảm thông lượng mạng. Cùng với đó, kỹ thuật định hướng chùm tia cũng làm tăng độ phức tạp triển khai cho hệ thống [25] và việc sử dụng các bộ hỗ trợ cũng yêu cầu sự đồng bộ và tin tưởng [26].

Mặt khác, kết quả từ [27] cho thấy can nhiễu từ một nguồn phát độc lập cũng giúp tăng hiệu quả an toàn ngay cả khi chất lượng của kênh truyền chính tệ hơn chất lượng trên kênh truyền nghe lén. Các kết quả nghiên cứu trong [28]–[30] với các mô hình mạng đa người dùng đồng thời truyền tin cũng củng cố cho kết quả trên. Như vậy, so với kỹ thuật định hướng chùm kia và sự giúp đỡ từ các bộ hỗ trợ, hợp tác với các người dùng khác là một giải pháp đơn giản, tiết kiệm mà hiệu quả cho việc cải thiện mức độ an toàn.

2.2 Mạng vô tuyến nhận thức và an toàn bảo mật

Những năm gần đây, nhu cầu sử dụng phổ tần số ngày càng gia tăng với sự phát triển của các ứng dụng và dịch vụ trên nền tảng mạng không dây. Để tránh vấn đề can nhiễu, mỗi phần trong tài nguyên tần số chỉ cấp cho một hoặc một số người dùng, và chỉ những người dùng này có quyền khai thác phổ được cấp phát. Chính sách cấp phát tần số này được gọi là chính sách truy cập phổ cố định (fixed spectrum access - FSA). Thế nhưng, phần lớn dải tần số được cấp phát này lại chưa được khai thác hiệu quả [1]. Mạng vô tuyến nhận thức với chính sách truy cập phổ động (dynamic spectrum access - DSA) được đề xuất như một giải pháp cho vấn đề chưa tận dụng hiệu quả tài nguyên tần số. Mô hình này có hai kiểu người dùng chia sẻ truyền tin trên cùng một dải tần số là bên sơ cấp (primary user - PU) và bên thứ cấp (secondary user - SU). PU là những bên được cấp phép và có quyền ưu tiên hơn khi sử dụng dải tần số, còn SU là những bên mong muốn được sử dụng phần tài nguyên tần số được cấp phép đó.

Có hai chiến lược mà SU có thể triển khai để sử dụng dải tần số được cấp phép là truy cập phổ cơ hội (opportunistic spectrum access - OSA) và truy cập phổ đồng thời (concurrent spectrum access - CSA). Trong OSA, SU thực hiện cảm nhận phổ (spectrum sensing) để phát hiện phần phổ chưa được sử dụng (spectrum hole) và tự điều chỉnh các tham số truyền để tham gia. Tuy nhiên, khi chất lượng của pha cảm nhận phổ không tốt, SU vẫn có thể gây nhiễu lên bên nhận của PU [25]. Ở chiến

lược CSA, SU có thể truyền đồng thời cùng với PU miễn là SU điều chỉnh công suất phát để can nhiễu gây cho bên nhận của PU nằm dưới một ngưỡng cho trước. Với chiến lược này, bằng việc thiết kế công suất phát hợp lý, hiệu quả sử dụng phổ có thể gia tăng đáng kể.

Khi xem xét vấn đề an toàn bảo mật, các nghiên cứu [31], [32] đã khảo sát chi tiết các kỹ thuật tấn công và phòng vệ trong CRN. Các tấn công vào CRN bao gồm các tấn công truyền thống như chèn nhiễu (jamming) hay nghe lén (eavesdropping) và các tấn công nhằm vào CRN như cạnh tranh người dùng sơ cấp (PU emulation - PUE) hay giả mạo dữ liệu cảm biến phổ (spectrum sensing data falsification - SSDF). Đồ án này tập trung nghiên cứu về tấn công nghe lén trong CRN, ở đó kẻ tấn công đe dọa đến tính riêng tư của dữ liệu được truyền trong mạng bằng việc lợi dụng tính mở của môi trường truyền dẫn không dây.

2.3 Thông tin kênh truyền trong an toàn bảo mật

Trong truyền thông không dây, thông tin kênh truyền (channel state information - CSI) phản ánh tri thức mà các bên thu nhận có được về các đặc tính của kênh truyền như cách thức lan truyền tín hiệu hay các hiệu ứng suy hao. CSI tại các bên có thể đạt được thông qua quá trình ước lượng kênh với hai pha: (i) bên phát gửi tín hiệu huấn luyện và (ii) bên nhận phản hồi lại CSI, thường trên một liên kết riêng. Trong đó, CSI tại bên nhận (CSIR), hỗ trợ trong việc giải mã thông điệp, thường được giả thiết là hoàn hảo, chính xác (mặc dù thực tế vẫn có sai số ước lượng), trong khi CSI tại bên phát (CSIT) có thể giả thiết ở nhiều mức độ khác nhau, thông qua chất lượng của pha phản hồi [33].

CSIT đóng vai trò rất quan trọng, tri thức về kênh truyền càng chính xác, bên phát có thể lựa chọn chiến lược mã hóa và xử lý tín hiệu càng tối ưu cho các độ đo hiệu năng. Với truyền tin an toàn, chiến lược truyền phụ thuộc cả vào chất lượng CSIT trên kênh truyền chính và CSIT trên kênh truyền nghe lén. Tuy nhiên, CSIT đầy đủ thường không đạt được trong thực tế, đặc biệt là CSIT về kênh truyền nghe lén vì kẻ nghe lén có thể không tương tác với bên ngoài (nghe lén thụ động), và như vậy bên phát không có phản hồi CSI về kênh truyền này [34].

Các nghiên cứu sâu rộng về ảnh hưởng của các mức CSIT khác nhau cũng cho thấy một số kỹ thuật giúp tăng cường mức độ an toàn ngay cả khi thông tin về kênh truyền tại bên phát không đầy đủ. Trong trường hợp bên phát chỉ có một ăng-ten, các nghiên cứu [22], [35]–[38] đề xuất chiến lược truyền "on-off": bên phát quyết định truyền hoặc hoãn truyền tin dựa trên tri thức có từ bên nhận. Phản hồi từ bên nhận có thể là kết quả ước lượng CSI [22], [35]–[37] hoặc có thể chỉ cần một bit [22], [38]. Trong trường hợp bên phát có nhiều ăng-ten, kỹ thuật định hướng chùm

tia kết hợp với nhiễu nhân tạo được sử dụng rộng rãi [21], [39], ngoài ra, có thể triển khai "on-off" mức ăng-ten trong chiến lược lựa chọn ăng-ten phát (transmit antenna selection - TAS) [40]. Như vậy, ngay cả khi chỉ có được thông tin kênh truyền rất ít, bên phát vẫn có cơ hội lựa chọn chiến lược truyền tin an toàn.

2.4 Các độ đo hiệu năng an toàn

Các độ đo đánh giá mức độ an toàn trong PLS được phát triển từ lý thuyết thông tin với mô hình truyền tin đơn giản gồm ba đối tượng. Bên phát (Alice) cần truyền một thông điệp M tới người dùng hợp pháp (Bob). Để giữ bí mật M với kẻ nghe lén (Eve), Alice sử dụng một bộ mã hóa ngẫu nhiên (stochastic encoder [13]) mã hóa M thành X^n với n là số lượt truy cập kênh (channel uses). Dưới tác động của các kênh truyền, Bob và Eve tương ứng thu được phiên bản Y^n và Z^n của X^n. Một bộ mã hóa xác định có hai tham số quan trọng là tốc độ truyền từ mã (codewords transmission rate) $R_b = \frac{H(X^n)}{n}$ và tốc độ truyền tin (transmission rate/confidential information rate) $R_s = \frac{H(M)}{n}$, trong đó ký hiệu $H(X)$ là lượng tin riêng (entropy) của X. Ngoài ra, một đại lượng cũng thường sử dụng trong lý thuyết thông tin là tốc độ không rõ ràng của kẻ nghe lén (eavesdropper's equivocation rate) $R_e = \frac{H(M|Z^n)}{n}$, với ký hiệu $H(X|Y)$ là lượng tin riêng của X với điều kiện Y. Đại lượng này phản ánh tốc độ tin trung bình mà kẻ nghe lén không biết về thông điệp truyền. Các độ đo mức độ an toàn dưới đây có liên quan mật thiết tới các đại lượng này.

2.4.1 Dung lượng an toàn và tốc độ an toàn

Trong việc lựa chọn độ đo đánh giá mức độ an toàn, chất lượng CSIT cũng đóng vai trò quan trọng. Với CSIT hoàn hảo cho cả kênh truyền chính và kênh truyền nghe lén, dung lượng an toàn (secrecy capacity - SC) C_s [15] thường được sử dụng để phân tích hiệu quả an toàn của hệ thống:

$$C_s = \max\left(C_B - C_E, 0\right), \tag{2.1}$$

trong đó C_B và C_E tương ứng là dung lượng (tức thời) của kênh truyền chính và kênh truyền nghe lén, được tính dựa trên chất lượng tín hiệu nhận, phản ánh thông qua tỷ số tín hiệu trên nhiễu (signal-to-noise ratio - SNR). Dung lượng an toàn xác định giới hạn trên cho tốc độ truyền tin an toàn R_s (secrecy rate) của hệ thống, là tốc độ truyền tin lớn nhất đạt được vẫn đảm bảo kẻ nghe lén không thể giải mã thông điệp.

Với CSIT không hoàn hảo, dung lượng an toàn ergodic [36], [37] và xác suất mất an toàn [15], [41] thường được sử dụng. Song, dung lượng an toàn ergodic chỉ phù hợp với các hệ thống chấp nhận độ trễ cao do tín hiệu truyền cần khoảng thời gian để trải nghiệm đủ thể hiện của kênh [34]. Do đó, đồ án chỉ giới thiệu các độ

đo dựa trên xác suất mất an toàn.

2.4.2 Xác suất mất an toàn

Xác suất mất an toàn (secrecy outage probability - SOP) xác định xác suất hệ thống không đạt được một tốc độ truyền tin an toàn R_s cho trước:

$$\text{SOP} = \mathbb{P}\left(C_s < R_s\right). \tag{2.2}$$

Tham số R_s được lựa chọn dựa trên ước lượng của Alice về khả năng giải mã tin của Eve: khi $C_s < R_s$ hay $C_E > C_B - R_s$ thì Eve có thể giải mã tin với tốc độ cao hơn mong đợi, tức là thông tin bị rò rỉ [15].

2.4.3 Công thức khác cho xác suất mất an toàn

Dựa trên công thức (2.2), có thể thấy SOP đánh giá hai sự kiện gây mất an toàn là (i) thông tin bị rò rỉ tới Eve hoặc (ii) Bob không thể giải mã chính xác thông điệp. Tức là, SOP đánh giá hệ thống ở cả tính tin cậy và an toàn. Nhằm tách biệt hai mục tiêu này, tác giả Zhou và cộng sự [22] đề xuất một công thức khác cho SOP (gọi là ASOP - alternative secrecy outage probability):

$$\text{ASOP} = \mathbb{P}\left(C_E > R_b - R_s \mid \text{message transmission}\right). \tag{2.3}$$

Khi thêm điều kiện cho công thức, việc xác định chiến lược truyền phù hợp có thể giúp gia tăng hiệu quả an toàn (giảm SOP) do chỉ đánh giá hiệu năng tại những phiên truyền thực tế giữa Alice và Bob. Ví dụ nếu Alice có thể xác định khả năng giải mã của Bob thì Alice có thể tạm dừng truyền tin trong một khoảng thời gian.

2.4.4 Các độ đo dựa trên mức độ không rõ ràng

Bằng việc chỉ ra các hạn chế của SOP như (i) không cho thấy khả năng giải mã của kẻ nghe lén và (ii) không cho thấy lượng tin bị lộ, tác giả He và cộng sự [38] đề xuất ba độ đo hiệu năng cho phép đánh giá *mức độ an toàn một phần* (partial secrecy), dựa trên mức độ không rõ ràng của kẻ nghe lén $\Delta = H(M \mid Z^n)/H(M)$. Đối với kênh truyền suy hao, mức độ không rõ ràng tối đa có thể đạt được là:

$$\Delta = \begin{cases} 1, & \text{nếu} \quad C_E \leq C_B - R_s \\ \left(C_B - C_E\right)/R_s, & \text{nếu} \quad C_B - R_s < C_E < C_B \\ 0, & \text{nếu} \quad C_B \leq C_E. \end{cases} \tag{2.4}$$

Từ đây, ba độ đo mới được đề xuất, dựa trên đánh giá phân bố của Δ.

1. Xác suất mất an toàn tổng quát (generalized SOP - GSOP)

Xác suất mất an toàn tổng quát được biểu diễn theo phân phối tích lũy của Δ:

$$\text{GSOP} = \mathbb{P}(\Delta < \theta), \tag{2.5}$$

trong đó $\theta \in (0, 1]$ là hằng số chọn trước, phản ánh tỷ lệ lượng tin yêu cầu tối thiểu mà Eve không biết về thông điệp truyền M, nói cách khác, $(1 - \theta)$ phản ánh tỷ lệ lượng tin bị tiết lộ tối đa chấp nhận được của hệ thống [38]. Khi $\theta = 1$, hệ thống yêu cầu mức an toàn cao nhất, tức là không để lộ bất kỳ lượng tin nào tới Eve, tương đương với SOP.

2. Tỷ lệ không rõ ràng trung bình (average fractional equivocation)

Giá trị trung bình của Δ có thể dùng làm tiệm cận dưới cho xác suất giải mã sai tại bên nghe lén [38]:

$$\bar{\Delta} = \mathbb{E}\{\Delta\}. \tag{2.6}$$

3. Tốc độ lộ thông tin trung bình (average information leakage rate - AILR)

Khác với xác suất mất an toàn, tốc độ lộ thông tin giúp phân tích định lượng hiệu năng an toàn của hệ thống. Các thiết kế truyền tin an toàn có thể đạt được xác suất mất an toàn như nhau nhưng lại khác nhau về tốc độ lộ thông tin [38]. Tốc độ lộ thông tin trung bình có thể được xác định dựa trên mức độ không rõ ràng của kẻ nghe lén Δ, vì $(1 - \Delta)$ phản ánh lượng thông tin mà Eve có được về thông điệp truyền. Tóm lại, tốc độ thông tin bị lộ trung bình có công thức:

$$R_L = \mathbb{E}\left\{\frac{I(M, Z^n)}{n}\right\} = \mathbb{E}\{(1 - \Delta)R_s\}. \tag{2.7}$$

Khi tốc độ truyền tin R_s không đổi, công thức này có thể đưa về dạng đơn giản:

$$R_L = \left(1 - \bar{\Delta}\right) R_s. \tag{2.8}$$

2.5 Tối ưu trong bài toán thiết kế

Các nghiên cứu về an toàn bảo mật lớp vật lý thường tập trung vào hai khía cạnh: (i) phân tích hệ thống theo lý thuyết thông tin, với các nghiên cứu liên quan đến dung lượng an toàn và tốc độ an toàn, (ii) thiết kế hệ thống, với các nghiên cứu về xử lý tín hiệu, cấp phát tài nguyên và hợp tác. Với ý nghĩa thực tiễn, vấn đề thiết kế hệ thống an toàn bảo mật ngày càng được quan tâm nghiên cứu, trong đó lý thuyết tối ưu thường được sử dụng vì ý tưởng tìm kiếm trạng thái tốt nhất giúp hệ thống đạt được hiệu năng cao nhất.

2.5.1 Bài toán tối ưu

Bài toán tối ưu được mô tả dưới dạng tổng quát sau:

$$\begin{aligned} \underset{\mathbf{x}}{\text{minimize}} \quad & f(\mathbf{x}) \\ \text{s.t} \quad & h_i(\mathbf{x}) \geq b_i, \quad i = 1, 2, \ldots, p \\ & g_j(\mathbf{x}) = c_j, \quad j = 1, 2, \ldots, q, \end{aligned} \tag{2.9}$$

trong đó $\mathbf{x}$ là một véc-tơ n-chiều, được gọi là biến quyết định hay biến tối ưu và $f : \mathbb{R}^n \to \mathbb{R}$ được gọi là hàm mục tiêu, hay hàm chi phí, mục tiêu của bài toán là giảm giá trị hàm mục tiêu này. Các điều kiện $h_i(x) \leq b_i$ và $g_j(x) = c_j$ tương ứng là các ràng buộc bất đẳng thức và ràng buộc đẳng thức của bài toán. Các ràng buộc này giới hạn một tập giá trị hợp lệ (feasible set) mà các biến quyết định có thể nhận, đồng thời cũng giới hạn tập giá trị mà hàm mục tiêu có thể đạt được (feasible objective set).

Giải quyết bài toán này là quá trình đi tìm một điểm thỏa mãn các điều kiện ràng buộc trong không gian các biến quyết định (decision space) mà giá trị của hàm mục tiêu ứng với điểm đó là nhỏ nhất trong tập các điểm hợp lệ. Điểm như vậy được gọi là nghiệm tối ưu toàn cục. Việc tìm kiếm nghiệm tối ưu toàn cục thường không dễ dàng với hầu hết các bài toán tối ưu, do việc này đòi hỏi việc kiểm tra trên toàn bộ tập các giá trị hợp lệ, ngoại trừ một số ít lớp bài toán có thể kiểm tra tính toàn cục của một nghiệm tìm được. Mặt khác, trong nhiều bài toán, việc tìm kiếm một giá trị tối ưu toàn cục là không cần thiết. Do đó, trong các vấn đề thiết kế thực tế, bài toán tối ưu thường hướng đến tìm kiếm lời giải nhanh và dễ dàng hơn khi chỉ tìm kiếm các nghiệm tối ưu cục bộ: trong số các điểm hợp lệ lân cận thì giá trị hàm mục tiêu tại nghiệm tối ưu cục bộ là nhỏ nhất.

2.5.2 Các phương pháp giải quyết bài toán tối ưu một mục tiêu

Với lịch sử phát triển lâu dài, các nghiên cứu về lý thuyết tối ưu đã giới thiệu rất đa dạng các phương pháp giải quyết cho nhiều lớp bài toán tối ưu [42]. Tuy nhiên, không có phương pháp nào hiệu quả với mọi bài toán. Các phương pháp thường đặt ra một số yêu cầu về bài toán cần giải quyết như tính chất lồi của hàm mục tiêu và tập giá trị hợp lệ [43] hay chỉ phù hợp với bài toán có số lượng nhỏ các biến quyết định và các điều kiện ràng buộc. Do đó, quá trình lựa chọn phương pháp giải bài toán tối ưu không chỉ dựa trên mức độ hiệu quả và tốc độ thực thi của phương pháp mà cần cân nhắc cả về đặc điểm của bài toán cần giải quyết.

Các phương pháp giải quyết bài toán tối ưu thường triển khai theo các bước lặp: với một ước lượng ban đầu về nghiệm của bài toán tối ưu, trong hữu hạn các lần lặp,

các phương pháp tìm cách sinh các giá trị cho biến quyết định nhằm làm cho hàm mục tiêu hội tụ về giá trị nhỏ nhất của nó. Các phương pháp khác nhau có chiến lược lựa chọn giá trị biến quyết định cho các vòng lặp khác nhau. Có rất nhiều phương pháp có tính ứng dụng cao đã khai thác hiệu quả tính khả vi của hàm mục tiêu trong việc tìm kiếm nghiệm tối ưu của bài toán. Cơ sở lý thuyết của ý tưởng này nằm ở tính chất: đạo hàm cấp một (đối với hàm một biến) hay gradient (đối với hàm nhiều biến) thể hiện tốc độ thay đổi giá trị của hàm số tại một điểm, đồng thời cũng xác định hướng biến thiên của hàm số tại điểm đó. Điều đó cho thấy, tại mỗi vòng lặp, thông tin về gradient (hay đạo hàm) có thể được dùng để định hướng tới nghiệm tối ưu của bài toán, giá trị của biến quyết định trong vòng lặp tiếp theo chỉ cần cập nhật dựa trên giá trị hiện tại cùng với hướng giảm xác định được của hàm mục tiêu. Các nghiên cứu sâu rộng dựa trên ý tưởng sử dụng gradient đã giới thiệu những kỹ thuật xử lý đặc biệt giúp cải thiện đáng kể tốc độ hội tụ của bài toán. Tuy nhiên, các phương pháp này đều có chung một hạn chế, nằm ở ý tưởng của phương pháp, đó là lời giải của bài toán phụ thuộc vào giá trị khởi tạo của biến quyết định. Với một thủ tục và một giá trị khởi tạo xác định, các phương pháp này thường chỉ lựa chọn các giá trị cho biến quyết định nằm trên một hoặc một số hướng tìm kiếm. Như vậy, rất khó để đảm bảo nghiệm tìm được là tối ưu toàn cục.

Một hướng tiếp cận giúp vượt qua hạn chế của các phương pháp đề cập ở trên là sinh một tập hợp các giá trị các biến quyết định (thay vì chỉ một) trong mỗi vòng lặp. Các phương pháp này được gọi là các phương pháp dựa trên quần thể (population based methods), mỗi giá trị của biến quyết định được gọi là một cá thể (individual). Hầu hết ý tưởng của các phương pháp dựa trên quần thể đều lấy cảm hứng từ tự nhiên với hai nhóm giải thuật là giải thuật tiến hóa (evolution algorithms) và giải thuật dựa trên trí tuệ bầy đàn (swarm intelligence-based algorithms). Các giải thuật tiến hóa lấy cảm hứng từ quá trình chọn lọc tự nhiên và cơ chế lai tạo giữa các cá thể trong một quần thể sinh học. Cụ thể, trong mỗi thế hệ (mỗi vòng lặp), các bộ hai cá thể được lựa chọn để lai tạo ra các cá thể mới (crossover), cá thể mới này mang những đặc điểm của hai cá thể cha mẹ, ngoài ra có cả những đặc điểm đột biến (mutation). Thông qua quá trình chọn lọc tự nhiên, những cá thể mang đặc điểm có lợi (ứng với các biến quyết định làm cho hàm mục tiêu nhỏ) có khả năng sống sót cao hơn (được giữ lại trong các vòng lặp tiếp theo). Qua mỗi thế hệ, chất lượng của cả quần thể được cải thiện, tương ứng với đó là tập các biến quyết định có xu hướng hội tụ về nghiệm tối ưu của bài toán. Đối với các giải thuật dựa trên trí tuệ bầy đàn, ý tưởng được lấy cảm hứng từ hành vi và cách thức liên lạc giữa các cá thể trong quần thể động vật. Với trí tuệ bầy đàn, các cá thể có thể hành động độc lập và không cần kiểm soát tập trung, song với chung một mục tiêu, sự tương tác

(cục bộ) giữa các cá thể có thể giúp cho cả quần thể hành động như một thể thống nhất, từ đó có thể giải quyết những bài toán phức tạp. Có thể thấy, các phương pháp dựa trên quần thể không chỉ giúp khám phá không gian biến quyết định để tăng khả năng tìm kiếm nghiệm toàn cục, mà còn khai thác thông tin từ các cá thể để giúp bài toán hội tụ tại nghiệm tốt nhất trong không gian tìm kiếm xác định được.

Các phương pháp dựa trên quần thể cho thấy tiềm năng trong việc giải quyết các bài toán tối ưu khó vì không đặt ra các giả thiết về bài toán cần giải quyết và cũng không dựa trên gradient, vốn không phải dễ dàng có được đối với nhiều hàm mục tiêu. Mặc dù nghiệm giải được của bài toán theo các phương pháp này không đảm bảo là tối ưu toàn cục nhưng trong hầu hết trường hợp, kết quả thu được là thỏa mãn mong muốn về nghiệm của người dùng. Đồ án này giới thiệu một giải thuật trong nhóm phương pháp này, giải thuật tiến hóa vi phân (differential evolution - DE), vì tính hiệu quả cũng như sự phù hợp đối với lớp bài toán tối ưu liên tục (không gian biến quyết định là liên tục).

Tiến hóa vi phân DE là một giải thuật tiến hóa được giới thiệu lần đầu bởi Storn và Price [44]. Cũng giống như các giải thuật tiến hóa khác, DE duy trì một tập NP cá thể, mỗi cá thể có D thuộc tính (tương ứng với số chiều của không gian biến quyết định) và biến đổi chúng qua các thế hệ $G = 0, 1, \ldots, G_{max}$ với ba thao tác: lai tạo (crossover), đột biến (mutation) và chọn lọc (selection). Ký hiệu cá thể thứ i trong thế hệ G là $X_{i,G} = \left[x_{1,i,G}, x_{2,i,G}, \ldots, x_{D,i,G}\right], i = 1, 2, \ldots, NP$. Thế hệ 0 là thế hệ khởi tạo của quần thể, các cá thể thường được sinh ngẫu nhiên với mục tiêu chúng có thể phân bố rộng khắp phạm vi tìm kiếm. Tại các thế hệ sau, các cá thể mới được tạo ra bằng cách lai giữa các cặp cá thể mục tiêu và cá thể đột biến. Điểm khác biệt quan trọng trong ý tưởng của DE so với các giải thuật tiến hóa khác là cách tạo ra cá thể đột biến: cá thể này được tạo dựa trên chính các cá thể trong quần thể hiện tại. Cụ thể, DE lựa chọn ngẫu nhiên ba cá thể khác nhau $X_{r_1^i}$, $X_{r_2^i}$ và $X_{r_3^i}$, trong đó hai cá thể bất kỳ dùng làm đại lượng đột biến cho cá thể còn lại:

$$V_{i,G} = X_{r_1^i,G} + F.\left(X_{r_2^i,G} - X_{r_3^i,G}\right), \tag{2.10}$$

trong đó $V_{i,G}$ là cá thể đột biến và F là biên độ đột biến (scaling factor/mutation constant), là tham số chọn trước trong thuật toán. Có thể thấy, DE khai thác thông tin từ chính phân bố của quần thể để quyết định mức độ đột biến: nếu các cá thể phân bố xa nhau thì lượng đột biến cũng lớn và khi chúng ở gần nhau (tức là bài toán dần hội tụ) thì chỉ cần ít sự đột biến. Điều này giúp các thế hệ đầu có thể khám phá không gian tìm kiếm mà vẫn đảm bảo lựa chọn nghiệm tốt nhất ở các thế hệ sau. Cá thể đột biến $V_{i,G}$ sau đó được lai tạo với cá thể mục tiêu $X_{i,G}$ bằng cách

chọn ngẫu nhiên mỗi thuộc tính từ một trong hai cá thể này làm thuộc tính cho cá thể mới. Mức độ ngẫu nhiên này được phản ánh thông qua một tham số gọi là tốc độ lai tạo CR (crossover rate), phản ánh xác suất một thuộc tính có thể bị đột biến trong cá thể lai tạo. Một trong những chiến lược lai tạo thường dùng trong DE là lai tạo đồng bộ (uniform crossover/binomial):

$$u_{j,i,G} = \begin{cases} v_{j,i,G}, & \text{nếu} \quad rand \leq CR \text{ hoặc } j = j_{rand} \\ x_{j,i,G}, & \text{trong trường hợp còn lại,} \end{cases} \tag{2.11}$$

với $rand$ là một giá trị ngẫu nhiên (với phân bố đều) trên đoạn $[0; 1]$ và j_{rand} là một chỉ số chọn ngẫu nhiên trên đoạn $[1; D]$, giá trị này được thêm vào với mục đích đảm bảo luôn có ít nhất một thuộc tính của cá thể đột biến được kế thừa. Để đảm bảo chất lượng quần thể không tệ hơn qua các thế hệ, cá thể mới $U_{i,G}$ cần được so sánh với cá thể mục tiêu $X_{i,G}$, cá thể nào trội hơn (với nghĩa là giá trị tương ứng của hàm mục tiêu nhỏ hơn) sẽ được giữ lại cho thế hệ tiếp theo:

$$X_{i,G+1} = \begin{cases} U_{i,G}, & \text{nếu} \quad f(U_{i,G}) \leq f(X_{i,G}) \\ X_{i,G}, & \text{trong trường hợp còn lại.} \end{cases} \tag{2.12}$$

Các quá trình đột biến, lai tạo và chọn lọc trên được lặp lại qua các thế hệ cho đến khi quần thể đạt đến trạng thái dừng. Trạng thái dừng có thể được xác định theo một số cách sau: (i) sau một số thế hệ xác định G_{max}, (ii) cá thể trội nhất của quần thể không đổi sau một chuỗi liên tiếp các thế hệ, hoặc (iii) đạt được một giá trị hàm mục tiêu mong muốn. Như vậy, có thể thấy, DE là một thuật giải không chỉ đơn giản, dễ triển khai, ít tham số cấu hình, phù hợp với nhiều bài toán, mà còn hiệu quả trong việc tìm kiếm nghiệm tối ưu toàn cục qua việc khám phá và khai thác không gian biến quyết định.

2.5.3 Tối ưu đa mục tiêu

Mô hình hóa bài toán thiết kế an toàn bảo mật với chỉ một hàm mục tiêu không phải lúc nào cũng dễ dàng, bởi cần cân nhắc giữa các độ đo hiệu năng (như tính tin cậy và tính an toàn) hoặc giữa lợi ích của các bên (trong hệ thống đa người dùng). Lúc này, xây dựng bài toán với chỉ một hàm mục tiêu cho thấy sự thiên vị ngay từ bước mô hình hóa bài toán. Với những vấn đề thiết kế này, lựa chọn phù hợp là mô hình hóa bài toán tối ưu với nhiều hàm mục tiêu, hay gọi là bài toán tối ưu đa mục

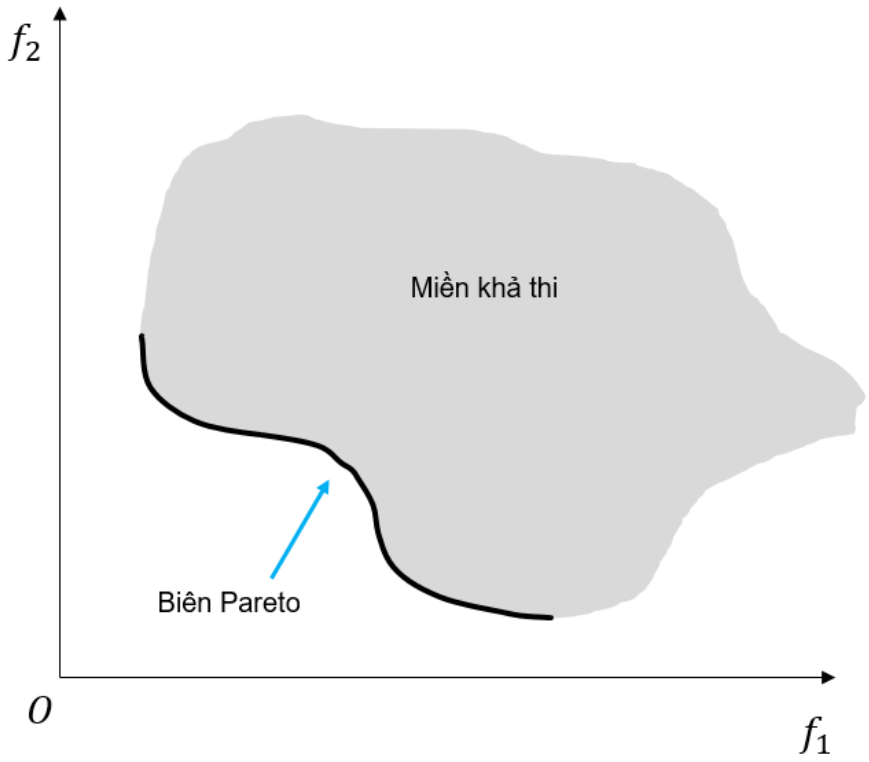
tiêu (multiobjective optimization problem - MOOP):

$$\begin{aligned} \underset{\mathbf{x}}{\text{minimize}} \quad & f_k(\mathbf{x}), \quad k = 1, 2, \ldots, m \\ \text{s.t} \quad & h_i(\mathbf{x}) \geq b_i, \quad i = 1, 2, \ldots, p \\ & g_j(\mathbf{x}) = c_j, \quad j = 1, 2, \ldots, q. \end{aligned} \tag{2.13}$$

Điểm khác biệt duy nhất của bài toán này so với bài toán tối ưu (2.9) là số lượng các hàm mục tiêu, $m > 1$, tức là không gian giá trị các hàm mục tiêu (không gian mục tiêu - objective space) trở thành không gian đa chiều $\mathbb{R}^m$.

Khi chỉ có một hàm mục tiêu, các giá trị khác nhau của biến quyết định có thể dễ dàng được xếp hạng dựa trên giá trị của hàm mục tiêu tương ứng (lúc này chỉ là các số thực), từ đó có thể đánh giá một điểm hợp lệ có là "tối ưu" hay không. Tuy nhiên, khái niệm "tối ưu" này không thể áp dụng trực tiếp vào bài toán tối ưu đa mục tiêu, vì không gian mục tiêu là nhiều chiều, không phải lúc nào cũng so sánh được hai véc-tơ giá trị với nhau. Vì thế, khái niệm "tối ưu Pareto" thường được sử dụng để định nghĩa nghiệm của bài toán tối ưu đa mục tiêu: một biến quyết định hợp lệ được gọi là tối ưu Pareto nếu như tất cả các biến quyết định hợp lệ khác nếu giúp cải thiện giá trị một hàm mục tiêu thì phải làm ít nhất một hàm mục tiêu khác tệ hơn. Về mặt toán học, biến quyết định hợp lệ $\mathbf{x}^*$ được gọi là tối ưu Pareto nếu không tồn tại một biến quyết định hợp lệ $\mathbf{x}$ nào khác thỏa mãn đồng thời $f_k(\mathbf{x}) \leq f_k(\mathbf{x}^*), \forall\, k = 1, 2, \ldots, m$ và $\exists\, l : f_l(\mathbf{x}) < f_l(\mathbf{x}^*)$. Việc tìm kiếm nghiệm tối ưu Pareto thường thu được một tập kết quả, ảnh của tập nghiệm đó được gọi là biên Pareto (Pareto front). Hình 2.1 biểu diễn biên Pareto trong không gian mục tiêu với hai hàm mục tiêu f_1 và f_2, trong đó đường cong kín mô tả tập giá trị có thể nhận của các hàm mục tiêu và phần biên được bôi đậm là biên Pareto. Có thể thấy, tập giá trị có thể nhận của các hàm mục tiêu có thể lồi (convex, tất cả các điểm nằm trên đoạn nối hai điểm bất kỳ trong tập hợp đều là phần tử của tập đó) hoặc không lồi (non-convex). Trong hình này, tập giá trị có thể nhận của các hàm mục tiêu là không lồi tại biên Pareto.

Định nghĩa bài toán thiết kế theo một mô hình khác cũng dẫn đến lời giải cho bài toán tối ưu cũng được xác định theo hướng khác. Khi có nhiều mục tiêu để tối ưu, các mục tiêu này có thể xung đột với nhau: giảm giá trị hàm mục tiêu này dẫn đến tăng giá trị cho hàm mục tiêu khác, và như vậy không có giá trị nào của biến quyết định làm cho mọi hàm mục tiêu cùng đạt đến giá trị nhỏ nhất có thể của nó. Lúc này, sự cân nhắc về mức độ ưu tiên giữa các mục tiêu trong quá trình thiết kế mô hình chuyển thành việc lựa chọn một nghiệm tối ưu phù hợp với mong muốn của người dùng. Việc lựa chọn này có thể được giải quyết với các bộ quyết định



Hình 2.1: Biên Pareto

(decision makers). Các bộ quyết định, với khả năng so sánh giữa các lời giải khác nhau theo sự ưu tiên của người dùng, có thể lựa chọn một lời giải phù hợp nhất trong tập các lời giải tìm được.

2.5.4 Các phương pháp giải quyết bài toán tối ưu đa mục tiêu

Về mặt toán học, việc tìm kiếm toàn bộ nghiệm tối ưu Pareto có thể coi như giải quyết xong bài toán tối ưu đa mục tiêu. Tuy nhiên, trong thực tế, số lượng các nghiệm này là rất lớn, trong khi, mục tiêu của việc giải bài toán này là lựa chọn một lời giải phù hợp nhất với mong muốn của người dùng. Như vậy, thay vì tìm kiếm toàn bộ nghiệm, các phương pháp giải chỉ cần đề xuất tới các bộ quyết định một hoặc một tập hữu hạn các lời giải tối ưu Pareto.

Các phương pháp giải bài toán tối ưu đa mục tiêu có thể nhóm thành ba nhóm [45]. Thứ nhất là nhóm các phương pháp tiên nghiệm (priori methods), ở đó mong muốn của người dùng về kết quả được xác định trước khi tiến hành tìm kiếm lời giải. Như vậy, việc tìm kiếm chỉ cần trả về một nghiệm phản ánh tốt nhất mong muốn đã đặt ra. Tuy nhiên, không phải lúc nào cũng có thể biểu diễn chính xác mong muốn về kết quả, tức là rất khó xác định hướng tìm kiếm nghiệm ngay từ đầu. Nhóm thứ hai là các phương pháp lũy tiến (progressive methods). Các phương pháp này đòi hỏi các bộ quyết định tham gia trong suốt quá trình tìm kiếm lời giải, với vai trò đánh giá kết quả, giúp điều chỉnh hướng tìm kiếm nhằm đi đến nghiệm

phù hợp nhất với mong muốn người dùng. Hạn chế lớn nhất của nhóm phương pháp này là việc đòi hỏi sự tham gia và phản hồi liên tục từ các bộ quyết định, cùng với đó, tốc độ phản hồi cũng ảnh hưởng đến thời gian thực thi của phương pháp. Thứ ba là nhóm các phương pháp hậu nghiệm (posteriori methods). Khác với các nhóm phương pháp trước, các phương pháp trong nhóm này thực hiện tìm kiếm và đề xuất một tập hữu hạn các lời giải để các bộ quyết định lựa chọn. Mặc dù không đòi hỏi phải biểu diễn mong muốn về kết quả hay sự phản hồi liên tục từ các bộ quyết định, ý tưởng sinh nhiều lời giải ở các phương pháp thuộc nhóm này lại khiến thời gian thực thi tăng lên đáng kể so với việc chỉ tìm kiếm một nghiệm. Bên cạnh đó, các nghiệm đề xuất cần đảm bảo ảnh của chúng đủ đại diện (thường với nghĩa phân bố đều) cho biên Pareto, trái lại, có thể không có nghiệm đề xuất nào đáp ứng được yêu cầu của các bộ quyết định. Có thể thấy, nếu như bài toán tối ưu đa mục tiêu có thể biểu diễn cụ thể mong muốn kết quả của người dùng ngay từ đầu thì các phương pháp trong nhóm tiên nghiệm giúp giảm đáng kể thời gian tìm kiếm lời giải. Các phương pháp này tránh lãng phí thời gian thực thi cho quá trình trao đổi thông tin với các bộ quyết định trong nhóm phương pháp lũy tiến và thời gian để sinh rất nhiều lời giải không cần thiết trong nhóm phương pháp hậu nghiệm.

Một ý tưởng tự nhiên giúp giải quyết các bài toán tối ưu đa mục tiêu là tìm cách đơn giản hóa về bài toán tối ưu với chỉ một hàm mục tiêu, từ đó có thể sử dụng các phương pháp giải hiệu quả của lớp bài toán tối ưu này. Với các phương pháp tiên nghiệm, tri thức có được từ các bộ quyết định về lời giải mong muốn có thể được khai thác để triển khai ý tưởng này. Một hướng tiếp cận truyền thống là tổng hợp các hàm mục tiêu thành một hàm duy nhất. Một ví dụ đơn giản là phương pháp tổng có trọng số các hàm mục tiêu (weighted-sum-of-objective-functions method), trong đó mỗi hàm mục tiêu được gán một trọng số ω_k dương xác định và hàm tổng hợp là tổng có trọng số các hàm mục tiêu đó:

$$\begin{aligned} \underset{\mathbf{x}}{\text{minimize}} \quad & f_{ws}(\mathbf{x}) = \sum_{k=1}^{m} \omega_k f_k(\mathbf{x}) \\ \text{s.t} \quad & h_i(\mathbf{x}) \geq b_i, \quad i = 1, 2, \ldots, p \\ & g_j(\mathbf{x}) = c_j, \quad j = 1, 2, \ldots, q. \end{aligned} \tag{2.14}$$

Bằng việc lựa chọn một bộ trọng số $\omega = (\omega_1, \omega_2, \ldots, \omega_m)$, ở đó các phần tử đều dương (và thường được chuẩn hóa $\sum_{k=1}^{m} \omega_k = 1$), nghiệm của bài toán (2.14) luôn là nghiệm tối ưu Pareto của bài toán (2.13) [46, Định lý 3.1.2 trang 78]. Tuy nhiên, rất khó để biểu diễn mong muốn của người dùng về kết quả thông qua các trọng số: một mặt, sự thay đổi nhỏ trên giá trị trọng số có thể gây ra sự thay đổi lớn trên

giá trị các hàm mục tiêu [46], mặt khác, tổ hợp tuyến tính của các hàm mục tiêu không thể đạt đến các phần không lồi trong biên Pareto [45]. Hướng tiếp cận thứ hai cho ý tưởng chuyển bài toán tối ưu đa mục tiêu về bài toán tối ưu một mục tiêu là lựa chọn tối ưu một hàm mục tiêu duy nhất và chuyển các hàm mục tiêu còn lại thành các ràng buộc bất đẳng thức với các giới hạn trên chọn trước. Phương pháp biến đổi này được gọi là ràng buộc ϵ (ϵ-constraint method). Không mất tổng quát, giả sử hàm mục tiêu f_1 được ưu tiên hơn các hàm mục tiêu còn lại, phương pháp ràng buộc ϵ biến đổi bài toán (2.13) về dạng:

$$\begin{aligned} \underset{\mathbf{x}}{\text{minimize}} \quad & f_1(\mathbf{x}) \\ \text{s.t} \quad & f_k(\mathbf{x}) \leq \epsilon_k, \quad k = 2, 3, \ldots, m \\ & h_i(\mathbf{x}) \geq b_i, \quad i = 1, 2, \ldots, p \\ & g_j(\mathbf{x}) = c_j, \quad j = 1, 2, \ldots, q. \end{aligned} \tag{2.15}$$

Chuyển các hàm mục tiêu thành các ràng buộc với giới hạn trên ϵ_k giúp cắt giảm tập các giá trị có thể đạt được của các hàm mục tiêu, cũng như giúp giới hạn quá trình tìm kiếm lời giải trong một phần nhỏ của biên Pareto. Với việc lựa chọn các giá trị ϵ_k hợp lý, bài toán (2.15) có thể tìm được lời giải trong phần không lồi của biên Pareto. Tuy nhiên, vì nằm trong các điều kiện ràng buộc mà các giá trị ϵ_k ảnh hưởng lớn tới kết quả của bài toán (2.15) cũng như bài toán ban đầu (2.13). Do đó, bên cạnh việc cân nhắc lựa chọn hàm mục tiêu được ưu tiên, phương pháp ràng buộc ϵ cũng đòi hỏi các giới hạn trên ϵ_k được lựa chọn cẩn thận, đảm bảo không nhỏ hơn giá trị nhỏ nhất có thể đạt được của từng hàm mục tiêu f_k. Ngoài hai hướng tiếp cận này, ý tưởng chuyển về bài toán tối ưu một mục tiêu có thể triển khai theo nhiều hướng khác. Các phương pháp triển khai ý tưởng này được đề cập trong [45] là các phương pháp vô hướng (scalar methods). Mỗi phương pháp có những ưu điểm và nhược điểm riêng, đồ án chỉ giới thiệu hai phương pháp trên vì sự đơn giản và dễ triển khai của chúng.

2.6 Kết chương

Chương này đã giới thiệu tổng quan về an toàn bảo mật lớp vật lý, cho thấy tư tưởng chính của các nghiên cứu về lĩnh vực này là: khai thác sự ngẫu nhiên (từ nhiễu kênh truyền, hiệu ứng suy hao hay can nhiễu, nhiễu nhân tạo) để tạo khác biệt lợi thế giữa kênh truyền chính và kênh truyền nghe lén, từ đó tăng cường mức độ an toàn cho hệ thống. Mạng vô tuyến nhận thức với chiến lược truy cập phổ đồng thời cho thấy một mô hình hợp tác, không chỉ giúp tận dụng hiệu quả tài nguyên tần số mà còn có thể giúp cải thiện mức độ an toàn cho các bên. Chương này cũng trình bày về các độ đo hiệu năng an toàn và giới thiệu về lý thuyết tối ưu, là nền

tảng trong quá trình mô hình hóa bài toán thiết kế. Trên cơ sở này, vấn đề nghiên cứu của đồ án được xây dựng, phát triển và giải quyết trong các chương tiếp theo.

CHƯƠNG 3. MÔ HÌNH HỆ THỐNG

Với kiến thức tổng quan về PLS và CRN trình bày trong Chương 2, đặc biệt là các độ đo hiệu năng an toàn, trong chương này, bài toán cần giải quyết sẽ được mô tả cụ thể. Trước đó, mô hình hệ thống và mô hình tín hiệu sẽ được trình bày nhằm xác định cụ thể bối cảnh của bài toán, bao gồm các đối tượng trong hệ thống, thông tin mà các bên có và đặc điểm kênh truyền. Trên cơ sở đó, đồ án đề xuất hiệu năng đánh giá phù hợp và xây dựng bài toán tối ưu cho vấn đề thiết kế hệ thống.

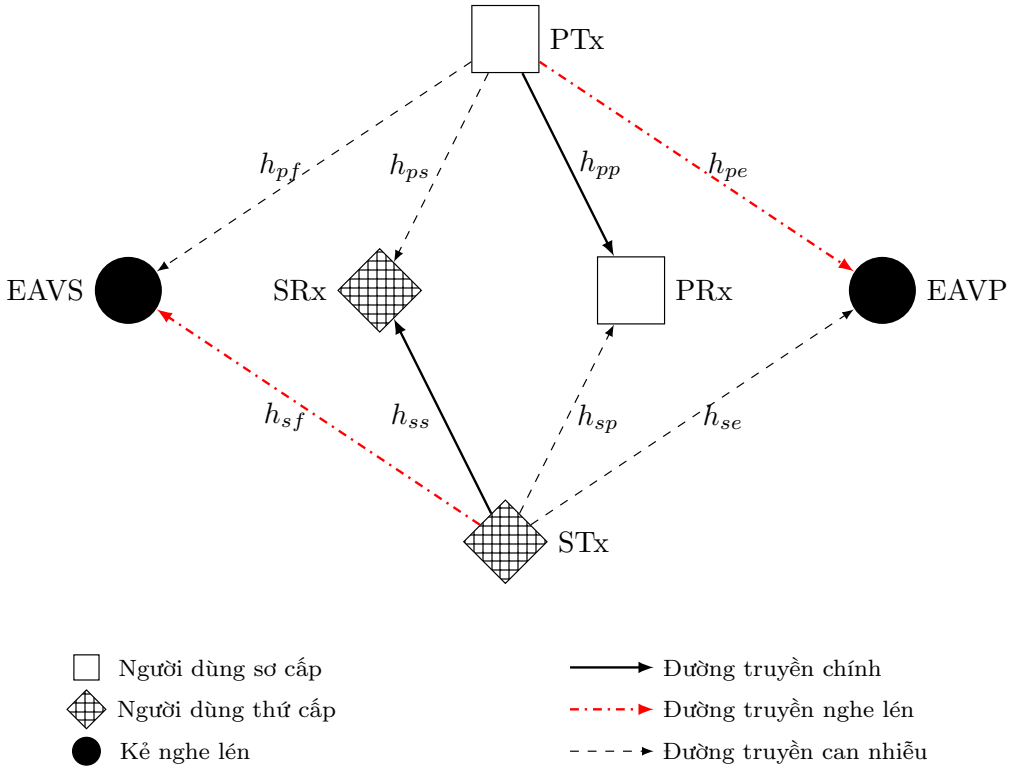
3.1 Mô hình hệ thống

Đồ án này xem xét mô hình mạng vô tuyến nhận thức truy cập phổ đồng thời. Trong đó, tại bên sơ cấp, bên phát PTx mong muốn truyền tin tới bên nhận PRx đảm bảo an toàn bí mật trước một kẻ nghe lén thụ động EAVP. Tương tự, tại bên thứ cấp, bên phát STx cũng cần truyền tin an toàn tới bên nhận SRx trước nguy cơ nghe lén thụ động của EAVS, xem Hình 3.1. Đồ án này tập trung vào phân tích lợi ích của truyền tin hợp tác nên chỉ xem xét trường hợp các bên phát và thu tín hiệu đều chỉ trang bị một ăng-ten.

Trong mô hình này, PTx và STx có thể truyền tin đồng thời, trên cùng dải tần số được cấp quyền cho PU. Khi đó, tín hiệu nhận tại các bên thu có thể bao gồm can nhiễu từ các bên phát không mong muốn. Giả thiết rằng chiến lược giải mã của các bên thu sẽ coi tín hiệu không mong muốn là nhiễu và loại bỏ mà không giải mã.

Ngoài ra, như đã nói trong phần trước, có thể coi như các bên nhận và các bên nghe lén có đầy đủ CSI trên tất cả các kênh truyền từ các bên phát tới. Đối với CSIT, giả thiết rằng bên nhận không thực hiện phản hồi CSI về bên phát và kẻ nghe lén là thụ động nên CSI tại các bên phát là không hoàn hảo. Song, CSIT đóng vai trò quan trọng trong việc xác định chiến lược truyền an toàn nên coi các bên phát có được thông tin thống kê về các kênh truyền. Cụ thể, các bên phát có thể ước lượng được độ lợi kênh (channel gain) trung bình thông qua khoảng cách từ bên phát tới bên thu [47].

Để đảm bảo an toàn bảo mật, các bên phát thực hiện chiến lược mã hóa ngẫu nhiên, trong đó mỗi thông điệp có thể được mã hóa thành nhiều từ mã [13]. Tốc độ truyền từ mã R_b và tốc độ truyền tin R_s là hai tham số quan trọng phản ánh đặc điểm bộ mã hóa. Với mô hình đề xuất, các tham số này là cố định, điều này giúp giảm độ phức tạp của hệ thống, đồng thời phù hợp với một số ứng dụng đòi hỏi truyền tin với tốc độ cố định như truyền phát video [38].



Hình 3.1: Mô hình hệ thống

3.2 Mô hình tín hiệu

Trong mô hình mạng vô truyến nhận thức truy cập phổ đồng thời, PTx với tín hiệu $x_P^n = [x_P(1), x_P(2), ..., x_P(n)]$ và STx với tín hiệu $x_S^n = [x_S(1), x_S(2), ..., x_S(n)]$ đồng thời truyền trên cùng một dải tần số, với n là độ dài từ mã. Tốc độ truyền từ mã và tốc độ truyền tin đối với tín hiệu từ PU là $R_b^{(P)}$ và $R_s^{(P)}$, đối với SU là $R_b^{(S)}$ và $R_s^{(S)}$. Khi đó, tín hiệu nhận tại PRx và SRx tại thời điểm i là:

$$y_P(i) = h_{pp}(i)x_P(i) + h_{sp}(i)x_S(i) + n_P(i),$$
$$y_S(i) = h_{ss}(i)x_S(i) + h_{ps}(i)x_P(i) + n_S(i),$$

trong đó, $h_{pp}(i), h_{ps}(i), h_{ss}(i), h_{sp}(i)$ tương ứng là hệ số các kênh truyền PTx $\rightarrow$ PRx, PTx $\rightarrow$ SRx, STx $\rightarrow$ SRx và STx $\rightarrow$ PRx; $n_P(i)$, $n_S(i)$ tương ứng là nhiễu Gauss trắng có tính cộng (additive white Gaussian noise - AWGN) tại PRx và SRx, với trung bình là không và mật độ phổ công suất (power spectral density - PSD) tương ứng là N_P và N_S.

Tương tự, tín hiệu nhận được tại EAVP y_E và tại EAVS y_F tương ứng là:

$$y_E(i) = h_{pe}(i)x_P(i) + h_{se}(i)x_S(i) + n_E(i),$$
$$y_F(i) = h_{sf}(i)x_S(i) + h_{pf}(i)x_P(i) + n_F(i),$$

với $h_{pe}(i), h_{pf}(i), h_{se}(i), h_{sf}(i)$ tương ứng là hệ số các kênh truyền PTx $\rightarrow$ EAVP, PTx $\rightarrow$ EAVS, STx $\rightarrow$ EAVP và STx $\rightarrow$ EAVS; $n_E(i)$, $n_F(i)$ tương ứng là nhiễu Gauss phức trắng có tính cộng tại EAVP và EAVS, với trung bình không và mật độ phổ công suất tương ứng là N_E và N_F.

Gọi các độ lợi kênh truyền trên là $g(i) = |h(i)|^2$, với $h(i)$ là hệ số kênh và bỏ qua việc thể hiện các chỉ số dưới nhằm chỉ chung cho tất cả các kênh truyền đã đề cập. Coi như tất cả các kênh truyền trong mô hình là kênh truyền suy hao Rayleigh bán tĩnh (quasi-static Rayleigh fading), tức là các độ lợi kênh truyền là không đổi trong suốt quá trình truyền từ mã và chúng là các biến ngẫu nhiên có phân phối mũ, với hàm mật độ xác suất (PDF) và hàm phân phối tích lũy (CDF) tương ứng là:

$$f_X(x) = \frac{1}{\Omega_X} \exp\left(-\frac{x}{\Omega_X}\right), \tag{3.1a}$$

$$F_X(x) = 1 - \exp\left(-\frac{x}{\Omega_X}\right), \tag{3.1b}$$

trong đó, biến ngẫu nhiên X đại diện cho độ lợi kênh truyền và $\Omega_X = \mathbb{E}\{X\}$ là trung bình độ lợi kênh tương ứng.

Ngoài ra các bên phát cũng bị giới hạn về năng lượng công suất phát, tức là:

$$p_P = \frac{1}{n}\sum_{i=1}^{n} |x_P(i)|^2 \leq p_P^{\max}, \tag{3.2a}$$

$$p_S = \frac{1}{n}\sum_{i=1}^{n} |x_S(i)|^2 \leq p_S^{\max}. \tag{3.2b}$$

Thông qua tín hiệu mà các bên thu được, có thể xác định tỷ số tín hiệu trên nhiễu và can nhiễu (signal-to-interference-plus-noise ratio - SINR), từ đó xác định dung lượng kênh tức thời tại các bên nhận như sau:

$$C^{(P)} = \log_2\left(1 + \text{SINR}^{(P)}\right) = \log_2\left(1 + \frac{p_P g_{pp}}{p_S g_{sp} + N_P}\right), \tag{3.3a}$$

$$C^{(E)} = \log_2\left(1 + \text{SINR}^{(E)}\right) = \log_2\left(1 + \frac{p_P g_{pe}}{p_S g_{se} + N_E}\right), \tag{3.3b}$$

$$C^{(S)} = \log_2\left(1 + \text{SINR}^{(S)}\right) = \log_2\left(1 + \frac{p_S g_{ss}}{p_P g_{ps} + N_S}\right), \tag{3.3c}$$

$$C^{(F)} = \log_2\left(1 + \text{SINR}^{(F)}\right) = \log_2\left(1 + \frac{p_S g_{sf}}{p_P g_{pf} + N_F}\right), \tag{3.3d}$$

trong đó các chỉ số trên P, E, S, F lần lượt đại diện cho các bên nhận PRx, EAVP, SRx và EAVS.

3.3 Lựa chọn hiệu năng cho bài toán

Mục tiêu của đồ án là thiết kế chiến lược truyền đảm bảo an toàn cho cả PU và SU. Do đó, một độ đo đánh giá mức độ an toàn là cần thiết cho bài toán thiết kế. Trong điều kiện chỉ có được các thông tin thống kê về kênh truyền, khi mà các bên phát không có đủ thông tin để lựa chọn chiến lược truyền luôn đảm bảo an toàn, các độ đo dựa trên xác suất mất an toàn thường được sử dụng để đánh giá hiệu năng. Song các độ đo này không phản ánh định lượng lượng thông tin bị nghe lén khi sự kiện mất an toàn xảy ra. Do đó, trong đồ án này, tốc độ lộ tin trung bình (AILR) sẽ được sử dụng là mục tiêu cho bài toán thiết kế.

Như đã đề cập, tốc độ truyền từ mã $R_b^{(P)}$ và $R_b^{(S)}$ trong mô hình là không đổi, trong khi, dưới ảnh hưởng của suy hao, dung lượng tức thời trên các kênh truyền chính $C^{(P)}, C^{(S)}$ có thể thấp hơn tốc độ này, dẫn đến giải mã sai ở các bên nhận mong muốn. Do đó, để đảm bảo truyền tin tin cậy, giả thiết rằng các bên nhận PRx và SRx đều có một kênh phản hồi tới bên phát tương ứng. Tương tự trong [22], [38], các bên nhận, với kết quả ước lượng dung lượng kênh của mình, có thể phản hồi một bit tới bên phát để đảm bảo bên phát chỉ truyền thông điệp khi $R_b^{(P)} \leq C^{(P)}$ và $R_b^{(S)} \leq C^{(S)}$. Với chiến lược này, xác suất truyền tương ứng là:

$$p_{tx}^{(P)} = \mathbb{P}\left(R_b^{(P)} \leq C^{(P)}\right), \tag{3.4a}$$

$$p_{tx}^{(S)} = \mathbb{P}\left(R_b^{(S)} \leq C^{(S)}\right). \tag{3.4b}$$

Tác giả trong [38] đã chứng minh rằng: với điều kiện $R_b^{(P)} \leq C^{(P)}$ và $R_s^{(P)} \leq R_b^{(P)}$, mức độ không rõ ràng Δ (2.4) tại kẻ nghe lén EAVP với dung lượng kênh $C^{(E)}$ có thể viết lại thành:

$$\Delta^{(P)} = \begin{cases} 1, & \text{nếu } C^{(E)} \leq R_b^{(P)} - R_s^{(P)} \\ \left(R_b^{(P)} - C^{(E)}\right)/R_s^{(P)}, & \text{nếu } R_b^{(P)} - R_s^{(P)} < C^{(E)} < R_b^{(P)} \\ 0, & \text{nếu } R_b^{(P)} \leq C^{(E)}, \end{cases} \tag{3.5}$$

Từ đó, tốc độ lộ tin trung bình tại PU với tốc độ truyền tin $R_s^{(P)}$ cố định là:

$$R_L^{(P)} = \left(1 - \bar{\Delta}^{(P)}\right) R_s^{(P)}, \tag{3.6}$$

và độ đo hiệu năng GSOP là:

$$p_{out}^{(P)}\left(\delta^{(P)}\right) = \mathbb{P}\left(\Delta^{(P)} < \delta^{(P)}\right). \tag{3.7}$$

Các công thức $\Delta^{(S)}$, $R_L^{(S)}$, $p_{out}^{(S)}$ ứng với SU và kẻ nghe lén EAVS được phát biểu tương tự.

$$\Delta^{(S)} = \begin{cases} 1, & \text{nếu } C^{(F)} \leq R_b^{(S)} - R_s^{(S)} \\ \left(R_b^{(S)} - C^{(F)}\right)/R_s^{(S)}, & \text{nếu } R_b^{(S)} - R_s^{(S)} < C^{(F)} < R_b^{(S)} \\ 0, & \text{nếu } R_b^{(S)} \leq C^{(F)}, \end{cases} \tag{3.8}$$

$$R_L^{(S)} = \left(1 - \bar{\Delta}^{(S)}\right) R_s^{(S)}, \tag{3.9}$$

$$p_{out}^{(S)}\left(\delta^{(S)}\right) = \mathbb{P}\left(\Delta^{(S)} < \delta^{(S)}\right). \tag{3.10}$$

3.4 Phát biểu bài toán

Đồ án này thực hiện giải quyết bài toán an toàn bảo mật cho mô hình trên theo hướng tiếp cận cấp phát công suất truyền cho các bên PTx và STx, đảm bảo truyền thông tin cậy và an toàn cho cả hai bên. Cụ thể, dựa trên độ đo an toàn bảo mật AILR và độ đo về chất lượng truyền tin là xác suất truyền tin, bài toán thiết kế trên được mô hình qua một bài toán tối ưu đa mục tiêu:

$$\begin{aligned} \underset{p_P, p_S}{\text{minimize}} \quad & R_L^{(P)}, R_L^{(S)} \\ \text{s.t} \quad & p_{tx}^{(P)} \geq \sigma^{(P)}, && \text{(3.11a)} \\ & p_{tx}^{(S)} \geq \sigma^{(S)}, && \text{(3.11b)} \\ & 0 \leq p_P \leq p_P^{\max}, && \text{(3.11c)} \\ & 0 \leq p_S \leq p_S^{\max}, && \text{(3.11d)} \end{aligned}$$

trong đó $\sigma^{(P)}, \sigma^{(S)} \in [0, 1]$ là xác suất truyền tối thiểu mà các bên yêu cầu đạt được; $p_P^{\max}, p_S^{\max}$ là công suất phát tối đa mà các bên phát có thể dùng. Khi xem xét điều kiện ràng buộc về công suất phát tối đa tại SU (3.11d) và xác suất truyền của PU (3.11a), bài toán tối ưu này cũng phản ánh điều kiện cần để SU có thể sử dụng chiến lược truy cập phổ đồng thời để truyền tin cùng với PU, đó là yêu cầu công suất phát của SU không làm giảm chất lượng truyền tin của PU [8], [11].

Trong mô hình CRN truyền thống, việc chia sẻ tài nguyên tần số thường không mang lại lợi ích cho PU, thậm chí can nhiễu từ SU có thể gây suy giảm chất lượng

truyền tin tại PU. Tuy nhiên, khi xét thêm yếu tố an toàn, can nhiễu từ SU có thể làm suy giảm chất lượng tín hiệu nghe lén của EAVP nhiều hơn đáng kể so với suy giảm gây ra cho PRx. Song, kết quả này cũng phụ thuộc vào các điều kiện kênh truyền từ STx tới PRx và EAVP. Do đó, PU hoàn toàn có thể lựa chọn chia sẻ tài nguyên tần số và cùng truyền với SU chỉ khi việc hợp tác này giúp cải thiện chất lượng truyền tin an toàn tại PU. Như vậy, một cách tự nhiên, bài toán thiết kế chiến lược truyền này cần dành cho SU giải quyết. Khi đó, SU có thể tùy chỉnh các tham số của bài toán để cân bằng giữa lợi ích từ việc được truyền tin (bằng việc gia tăng hiệu năng an toàn cho PU) và chất lượng truyền tin an toàn của chính mình.

Trong mô hình này, SU sẽ thực hiện giải bài toán thiết kế (3.11) nên giả thiết rằng PU và SU có thể truyền thông với nhau, tức là có một kênh truyền kết nối PU và SU [48]. Qua đó các bên có thể thống nhất các tham số cần thiết, đồng thời SU sau khi giải quyết bài toán tối ưu, có thể đề xuất chiến lược truyền tới PU và PU cũng có thể thông báo về quyết định hợp tác của mình.

3.5 Kết chương

Qua việc xây dựng mô hình và đưa ra các giả thiết về kênh truyền, CSI tại các bên và chiến lược mã hóa, chương này đã cụ thể hóa bài toán thiết kế hệ thống dưới dạng một bài toán tối ưu đa mục tiêu. Cách thức giải quyết bài toán này sẽ được đề cập trong chương sau.

CHƯƠNG 4. PHƯƠNG PHÁP ĐỀ XUẤT

Chương 3 đã phát biểu cụ thể một bài toán tối ưu đa mục tiêu, mô hình cho bài toán thiết kế hệ thống mà đồ án này hướng tới giải quyết. Mục tiêu của chương này là đề xuất hướng giải quyết cho bài toán đó. Trước hết chương này thực hiện phân tích bài toán để thấy rõ sự phụ thuộc của các đại lượng đối với các biến quyết định. Từ đó chương này phát biểu điều kiện ràng buộc cho các tham số để đảm bảo bài toán có nghiệm. Với kết quả phân tích có được, chương này thực hiện phát triển bài toán ban đầu thành hai bài toán tối ưu một mục tiêu ứng với sự ưu tiên khác nhau của người thiết kế - SU. Phương pháp giải quyết các bài toán này được đề cập ở cuối chương.

4.1 Phân tích bài toán

4.1.1 Phân tích các đại lượng trong mô hình

Trong Chương 3, đồ án đề xuất mô hình với hai bên phát PTx, STx đồng thời truyền tin. Từ các công thức (3.3), thấy rằng dung lượng kênh được biểu diễn theo tỷ số tín hiệu trên nhiễu và can nhiễu SINR. Mỗi đại lượng SINR lại phụ thuộc vào hai độ lợi kênh truyền từ các bên phát tới bên thu tương ứng. Đồ án cũng giả thiết rằng độ lợi của tất cả các kênh truyền trong mô hình là các biến ngẫu nhiên độc lập có phân phối mũ. Do đó, để xác định phân phối của dung lượng kênh, bổ đề sau thực hiện khảo sát biến ngẫu nhiên đại diện cho SINR tại các bên thu.

Bổ đề 1. *Với X và Y là các biến ngẫu nhiên độc lập có phân phối mũ với kỳ vọng tương ứng là Ω_X và Ω_Y ($\Omega_X > 0, \Omega_Y > 0$). Biến ngẫu nhiên U được định nghĩa là:*

$$U = \frac{aX}{bY + c}, \tag{4.1}$$

trong đó a, b, c là các hằng số dương. Khi đó, U có hàm phân phối tích lũy (cumulative distribution function - CDF) sau:

$$F_U(u) = 1 - \frac{1}{\frac{b\Omega_Y}{a\Omega_X}u + 1} \exp\left(-\frac{uc}{a\Omega_X}\right). \tag{4.2}$$

Chứng minh. Bổ đề 1 được chứng minh trong phần phụ lục A. ■

Trong mô hình đề xuất, độ đo đánh giá hiệu năng an toàn cho hệ thống được lựa chọn là tốc độ lộ tin trung bình. Theo định nghĩa (2.7), đại lượng này phụ thuộc vào mức độ không rõ ràng tại kẻ nghe lén $\Delta^{(P)}$ và $\Delta^{(S)}$. Đối với kênh truyền suy hao, từ các công thức (3.5) và (3.8), thấy rằng $\Delta^{(P)}$ và $\Delta^{(S)}$ chỉ phụ thuộc vào một biến

ngẫu nhiên là tỷ số tín hiệu trên nhiễu và can nhiễu SINR tại kẻ nghe lén EAVP, EAVS tương ứng. Do đó, khi xác định được phân phối của SINR tại bên nghe lén, tốc độ lộ tin trung bình có thể được xác định dựa trên kỳ vọng của biến ngẫu nhiên đại diện cho mức độ không rõ ràng tại kẻ nghe lén. Biến ngẫu nhiên đó được khảo sát trong bổ đề sau.

Bổ đề 2. *Gọi U là biến ngẫu nhiên liên tục có hàm phân phối tích lũy $F_U(u)$ và U chỉ nhận giá trị không âm, tức là $\mathbb{P}(U < 0) = 0$. Xét hàm của biến ngẫu nhiên U:*

$$h_{m,n}(U) = \begin{cases} 1, & \textit{nếu} \quad U \leq 2^{m-n} - 1 \\ \frac{m - \log_2(1+U)}{n}, & \textit{nếu} \quad 2^{m-n} - 1 < U < 2^m - 1 \\ 0, & \textit{nếu} \quad 2^m - 1 \leq U, \end{cases} \tag{4.3}$$

trong đó m, n là các hằng số thực thỏa mãn $m \geq n > 0$. Khi đó, $Z = h_{m,n}(U)$ là biến ngẫu nhiên, có hàm phân phối tích lũy (CDF) là:

$$F_Z(z) = \begin{cases} 1, & \textit{nếu} \quad z > 1 \\ 1 - F_U\left(2^{m-nz} - 1\right), & \textit{nếu} \quad 0 < z \leq 1 \\ 0, & \textit{nếu} \quad z \leq 0, \end{cases} \tag{4.4}$$

Chứng minh. Bổ đề 2 được chứng minh trong phần phụ lục B. ■

Với Bổ đề 2, khi U đại diện cho SINR tại kẻ nghe lén thì Z đại diện cho mức độ không rõ ràng tại kẻ nghe lén đó. Bổ đề này xem xét trường hợp tổng quát với U là biến ngẫu nhiên không âm bất kỳ. Khi đề cập mô hình truyền tin cụ thể, phân phối $F_U(u)$ của SINR tại kẻ nghe lén là xác định, từ đó có thể đánh giá kỳ vọng của Z, và theo công thức (2.7), có thể xác định tốc độ lộ tin trung bình.

4.1.2 Phân tích hàm mục tiêu

Các hàm mục tiêu của bài toán (3.11) đều là tốc độ lộ tin trung bình, $R_L^{(P)}$ và $R_L^{(S)}$ khi PU và SU đồng thời truyền tin. Như đã phân tích, các đại lượng này được xác định dựa vào giá trị trung bình, hay kỳ vọng của mức độ không rõ ràng tại kẻ nghe lén EAVP, EAVS tương ứng. Khi xem xét trường hợp PU và SU cùng truyền tin, SINR tại các kẻ nghe lén có thể được đại diện bởi biến ngẫu nhiên U định nghĩa trong Bổ đề 1. Dựa trên kết quả của Bổ đề 2, kỳ vọng của mức độ không rõ ràng tại kẻ nghe lén trong trường hợp này được xác định trong bổ đề sau.

Bổ đề 3. *Khi U là biến ngẫu nhiên được định nghĩa trong* (4.1)*, biến ngẫu nhiên*

$Z = h_{m,n}(U)$, với $h_{m,n}$ được định nghĩa trong (4.3)*, có kỳ vọng là:*

$$\begin{aligned}\mathbb{E}\{Z\} = 1 - \frac{\exp(k/l)}{n(l-1)\ln 2}\left[\text{Ei}\left(-k2^m + k - \frac{k}{l}\right) - \text{Ei}\left(-k2^{m-n} + k - \frac{k}{l}\right)\right] \\ + \frac{\exp(k)}{n(l-1)\ln 2}\left[\text{Ei}\left(-k2^m\right) - \text{Ei}\left(-k2^{m-n}\right)\right],\end{aligned} \tag{4.5}$$

trong đó, $\text{Ei}(x)$ *là hàm tích phân mũ và* k*,* l *được xác định bằng:*

$$\begin{aligned}k &= \frac{c}{a\Omega_X}, \\ l &= \frac{b\Omega_Y}{a\Omega_X},\end{aligned} \tag{4.6}$$

với a*,* b*,* c*,* Ω_X*,* Ω_Y *được đề cập trong* (4.1)*. Trong trường hợp đặc biệt khi* $l = 1$*, công thức biểu diễn cho* $\mathbb{E}\{Z\}$ *là:*

$$\begin{aligned}\mathbb{E}\{Z\} = 1 + \frac{k\exp(k)}{n\ln 2}\left[\text{Ei}\left(-k2^m\right) - \text{Ei}\left(-k2^{m-n}\right)\right] + \\ + \frac{1}{n\ln 2}\left[\frac{\exp\left(-k2^m + k\right)}{2^m} - \frac{\exp\left(-k2^{m-n} + k\right)}{2^{m-n}}\right].\end{aligned} \tag{4.7}$$

Chứng minh. Bổ đề 3 được chứng minh trong phần phụ lục B. ■

Từ kết quả Bổ đề 3, tốc độ lộ tin trung bình tại PU $R_L^{(P)}$ trong (3.6) được viết lại bằng việc coi Z là $\Delta^{(P)}$ và các tham số $a, b, c, m, n, \Omega_X, \Omega_Y$ tương ứng bằng p_P, p_S, N_E, $R_b^{(P)}$, $R_s^{(P)}$, Ω_{pe}, Ω_{se}. Ta có:

$$\begin{aligned}R_L^{(P)} &= \left(1 - \mathbb{E}\left\{\Delta^{(P)}\right\}\right) R_s^{(P)} \\ &= \frac{\exp\left(k^{(P)}/l^{(P)}\right)}{\left(l^{(P)} - 1\right)\ln 2}\left[\text{Ei}\left(-k^{(P)}\gamma_b^{(P)} - \frac{k^{(P)}}{l^{(P)}}\right) - \text{Ei}\left(-k^{(P)}\gamma_s^{(P)} - \frac{k^{(P)}}{l^{(P)}}\right)\right] \\ &\quad - \frac{\exp\left(k^{(P)}\right)}{\left(l^{(P)} - 1\right)\ln 2}\left[\text{Ei}\left(-k^{(P)}\gamma_b^{(P)} - k^{(P)}\right) - \text{Ei}\left(-k^{(P)}\gamma_s^{(P)} - k^{(P)}\right)\right],\end{aligned} \tag{4.8}$$

với trường hợp $l^{(P)} = 1$ là:

$$R_L^{(P)} = \frac{k^{(P)}\exp\left(k^{(P)}\right)}{\ln 2}\left[\text{Ei}\left(-k^{(P)}\gamma_s^{(P)} - k^{(P)}\right) - \text{Ei}\left(-k^{(P)}\gamma_b^{(P)} - k^{(P)}\right)\right] +$$

$$+\frac{1}{\ln 2}\left[\frac{\exp\left(-k^{(P)}\gamma_s^{(P)}\right)}{\gamma_s^{(P)}+1}-\frac{\exp\left(-k^{(P)}\gamma_b^{(P)}\right)}{\gamma_b^{(P)}+1}\right]. \tag{4.9}$$

với

$$\begin{aligned}\gamma_b^{(P)} &= 2^{R_b^{(P)}}-1,\\ \gamma_s^{(P)} &= 2^{R_b^{(P)}-R_s^{(P)}}-1,\end{aligned} \tag{4.10}$$

và k, l trong (4.6) trở thành:

$$\begin{aligned}k^{(P)} &= \frac{N_E}{p_P\Omega_{pe}},\\ l^{(P)} &= \frac{p_S\Omega_{se}}{p_P\Omega_{pe}},\end{aligned} \tag{4.11}$$

Tương tự, tốc độ lộ tin trung bình tại SU $R_L^{(S)}$ được viết lại là:

$$\begin{aligned}R_L^{(S)} &= \left(1-\mathbb{E}\left\{\Delta^{(S)}\right\}\right)R_s^{(S)}\\ &= \frac{\exp\left(k^{(S)}/l^{(S)}\right)}{\left(l^{(S)}-1\right)\ln 2}\left[\text{Ei}\left(-k^{(S)}\gamma_b^{(S)}-\frac{k^{(S)}}{l^{(S)}}\right)-\text{Ei}\left(-k^{(S)}\gamma_s^{(S)}-\frac{k^{(S)}}{l^{(S)}}\right)\right]\\ &\quad-\frac{\exp\left(k^{(S)}\right)}{\left(l^{(S)}-1\right)\ln 2}\left[\text{Ei}\left(-k^{(S)}\gamma_b^{(S)}-k^{(S)}\right)-\text{Ei}\left(-k^{(S)}\gamma_s^{(S)}-k^{(S)}\right)\right],\end{aligned} \tag{4.12}$$

với trường hợp $l^{(S)}=1$ là:

$$\begin{aligned}R_L^{(S)} &= \frac{k^{(S)}\exp\left(k^{(S)}\right)}{\ln 2}\left[\text{Ei}\left(-k^{(S)}\gamma_s^{(S)}-k^{(S)}\right)-\text{Ei}\left(-k^{(S)}\gamma_b^{(S)}-k^{(S)}\right)\right]+\\ &\quad+\frac{1}{\ln 2}\left[\frac{\exp\left(-k^{(S)}\gamma_s^{(S)}\right)}{\gamma_s^{(S)}+1}-\frac{\exp\left(-k^{(S)}\gamma_b^{(S)}\right)}{\gamma_b^{(S)}+1}\right].\end{aligned} \tag{4.13}$$

với

$$\begin{aligned}\gamma_b^{(S)} &= 2^{R_b^{(S)}}-1,\\ \gamma_s^{(S)} &= 2^{R_b^{(S)}-R_s^{(S)}}-1,\end{aligned} \tag{4.14}$$

và

$$\begin{aligned}k^{(S)} &= \frac{N_F}{p_S\Omega_{sf}},\\ l^{(S)} &= \frac{p_P\Omega_{pf}}{p_S\Omega_{sf}}.\end{aligned} \tag{4.15}$$

4.1.3 Phân tích điều kiện khả thi cho các ràng buộc

Để bài toán tối ưu (3.11) có nghiệm thì tập các giá trị (p_P, p_S) thỏa mãn các điều kiện ràng buộc phải không rỗng. Gọi tập các giá trị (p_P, p_S) thỏa mãn các điều kiện ràng buộc trong bài toán (3.11) với hai tham số tùy chỉnh $\sigma^{(P)}$ và $\sigma^{(S)}$ là $G\left(\sigma^{(P)}, \sigma^{(S)}\right)$. Phần này xác định dải giá trị cho $\sigma^{(P)}$ và $\sigma^{(S)}$ để G khác rỗng.

Trước hết, ta biểu diễn $p_{tx}^{(P)}$ và $p_{tx}^{(S)}$ theo p_P và p_S. Bắt đầu từ xác suất truyền tin của PU trong công thức (3.4a), ta thấy $p_{tx}^{(P)}$ có thể được biểu diễn theo phân phối tích lũy của $\text{SINR}^{(P)}$. Khi coi độ lợi kênh truyền từ PTx đến PRx và độ lợi kênh truyền STx đến PRx là các biến ngẫu nhiên độc lập X, Y có phân phối mũ, thì $\text{SINR}^{(P)}$ được đại diện bởi biến ngẫu nhiên U định nghĩa trong (4.1), với a, b, c tương ứng là p_P, p_S, N_P. Như vậy, ta có:

$$\begin{aligned} p_{tx}^{(P)} &= \mathbb{P}\left(R_b^{(P)} \le C^{(P)}\right) \\ &= \mathbb{P}\left(2^{R_b^{(P)}} - 1 \le \frac{p_P g_{pp}}{p_S g_{sp} + N_P}\right) \\ &= 1 - \mathbb{P}\left(\frac{p_P g_{pp}}{p_S g_{sp} + N_P} < 2^{R_b^{(P)}} - 1\right) \\ &= \frac{p_P \Omega_{pp}}{p_S \Omega_{sp} \gamma_b^{(P)} + p_P \Omega_{pp}} \exp\left(-\frac{\gamma_b^{(P)} N_P}{p_P \Omega_{pp}}\right), \end{aligned} \tag{4.16}$$

với $\gamma_b^{(P)} = 2^{R_b^{(P)}} - 1$. Tương tự, ta có công thức cho $p_{tx}^{(S)}$:

$$\begin{aligned} p_{tx}^{(S)} &= \mathbb{P}\left(R_b^{(S)} \le C^{(S)}\right) \\ &= \mathbb{P}\left(2^{R_b^{(S)}} - 1 \le \frac{p_S g_{ss}}{p_P g_{ps} + N_S}\right) \\ &= 1 - \mathbb{P}\left(\frac{p_S g_{ss}}{p_P g_{ps} + N_S} < 2^{R_b^{(S)}} - 1\right) \\ &= \frac{p_S \Omega_{ss}}{p_P \Omega_{ps} \gamma_b^{(S)} + p_S \Omega_{ss}} \exp\left(-\frac{\gamma_b^{(S)} N_S}{p_S \Omega_{ss}}\right), \end{aligned} \tag{4.17}$$

với $\gamma_b^{(S)} = 2^{R_b^{(S)}} - 1$. Từ các công thức (4.16) và (4.17), ta có thể xác định được xác suất truyền tin cực đại cho PU và SU, kết quả được thể hiện trong bổ đề sau.

Bổ đề 4. *Dải giá trị cho $p_{tx}^{(P)}$ và $p_{tx}^{(S)}$ là:*

$$0 \le p_{tx}^{(P)} \le \exp\left(-\frac{\gamma_b^{(P)} N_P}{p_P^{max} \Omega_{pp}}\right), \tag{4.18a}$$

$$0 \leq p_{tx}^{(S)} \leq \exp\left(-\frac{\gamma_b^{(S)} N_S}{p_S^{max}\Omega_{ss}}\right). \tag{4.18b}$$

Chứng minh. Bổ đề 4 được chứng minh trong phần phụ lục C. ■

Từ kết quả của Bổ đề 4, ta thấy rằng một bên chỉ đạt được xác suất truyền cao nhất khi bên đó truyền với công suất phát cao nhất và bên còn lại không tham gia truyền. Điều đó có nghĩa là nếu muốn hợp tác với SU, PU cần chấp nhận giảm mức độ hiệu quả sử dụng kênh truyền của mình.

Bổ đề 4 cũng cho thấy giá trị lớn nhất mà các bên có thể thiết lập cho $\sigma^{(P)}$ và $\sigma^{(S)}$. Tuy nhiên, các giới hạn này chỉ xem xét độc lập từng đại lượng, vì giá trị lớn nhất của một bên chỉ đạt được khi bên còn lại không phát tín hiệu. Tức là, nếu cả hai bên cùng yêu cầu xác suất truyền tin tối thiểu $\sigma^{(P)}$ và $\sigma^{(S)}$ quá cao thì không thể tìm được bộ công suất phát (p_P, p_S) thỏa mãn yêu cầu đó, hay PU và SU không thể hợp tác. Do đó, ta cần lựa chọn $\sigma^{(P)}$ và $\sigma^{(S)}$ phù hợp để điều kiện hợp tác xảy ra, tức là tập $G\left(\sigma^{(P)}, \sigma^{(S)}\right)$ của các bộ (p_P, p_S) là khác rỗng. Do PU có quyền ưu tiên trong việc lựa chọn các tham số của bài toán, nên giá trị $\sigma^{(P)}$ là cố định. Giả sử PU lựa chọn $\sigma^{(P)}$ đảm bảo nhỏ hơn xác suất truyền cao nhất có thể đạt được xác định trong (4.18a). Khi đó, giá trị lớn nhất của $\sigma^{(S)}$ mà SU có thể lựa chọn để đảm bảo tập $G\left(\sigma^{(P)}, \sigma^{(S)}\right)$ khác rỗng được xác định qua Bổ đề 5.

Bổ đề 5. *Giá trị lớn nhất của* $\sigma^{(S)}$ *trong* (3.11b) *là nghiệm của bài toán tối ưu:*

$$\begin{aligned} \underset{\sigma^{(S)}}{\text{maximize}} \quad & \sigma^{(S)} \\ \text{s.t} \quad & \phi_s\left(\phi_p\left(p_P^{max}\right)\right) \geq p_P^{max}, && (4.19a) \\ & \phi_p\left(\phi_s\left(p_S^{max}\right)\right) \geq p_S^{max}, && (4.19b) \end{aligned}$$

trong đó

$$\begin{aligned} \phi_p(x) &= \frac{x\Omega_{pp}}{\sigma^{(P)}\gamma_b^{(P)}\Omega_{sp}}\left[\exp\left(-\frac{\gamma_b^{(P)} N_P}{x\Omega_{pp}}\right) - \sigma^{(P)}\right], \\ \phi_s(x) &= \frac{x\Omega_{ss}}{\sigma^{(S)}\gamma_b^{(S)}\Omega_{ps}}\left[\exp\left(-\frac{\gamma_b^{(P)} N_S}{x\Omega_{ss}}\right) - \sigma^{(S)}\right]. \end{aligned} \tag{4.20}$$

Chứng minh. Bổ đề 5 được chứng minh trong phần phụ lục C. ■

Tóm lại, điều kiện để tập $G\left(\sigma^{(P)}, \sigma^{(S)}\right)$ khác rỗng, tức bài toán tối ưu (3.11) có

nghiệm là:

$$\begin{aligned} \sigma^{(P)} &< \exp\left(-\frac{\gamma_b^{(P)} N_P}{p_P^{\max}\Omega_{pp}}\right), \\ \sigma^{(S)} &\leq \sigma^{(S)*}, \end{aligned} \tag{4.21}$$

với $\sigma^{(S)*}$ là nghiệm của bài toán tối ưu (4.19).

4.1.4 Phân tích trường hợp không hợp tác

Như đã đề cập trong Chương 3, PU chỉ lựa chọn hợp tác với SU khi việc hợp tác này giúp hiệu năng an toàn cho PU cao hơn so với khi chỉ có PU tham gia truyền. Do đó, trong bài toán thiết kế, SU cần xem xét các độ đo hiệu năng tại PU khi PU thực hiện truyền đơn lẻ.

Khi chỉ có PU truyền tin trong hệ thống, dung lượng kênh truyền chính $C^{(P-NC)}$ và dung lượng kênh truyền nghe lén $C^{(E-NC)}$, trong đó ký hiệu NC (non-cooperative) chỉ trường hợp không hợp tác, có công thức là:

$$C^{(P-NC)} = \log_2\left(1 + \text{SINR}^{(P-NC)}\right) = \log_2\left(1 + \frac{p_P g_{pp}}{N_P}\right), \tag{4.22a}$$

$$C^{(E-NC)} = \log_2\left(1 + \text{SINR}^{(E-NC)}\right) = \log_2\left(1 + \frac{p_P g_{pe}}{N_E}\right). \tag{4.22b}$$

Từ đó, xác suất truyền tin tại PU có công thức là:

$$\begin{aligned} p_{tx}^{(NC)} &= \mathbb{P}\left(R_b^{(P)} \leq C^{(P-NC)}\right) \\ &= \mathbb{P}\left(2^{R_b^{(P)}} - 1 \leq \frac{p_P g_{pp}}{N_P}\right) \\ &= 1 - \mathbb{P}\left(g_{pp} < \frac{N_P \gamma_b^{(P)}}{p_P}\right) \\ &= \exp\left(-\frac{\gamma_b^{(P)} N_P}{p_P \Omega_{pp}}\right), \end{aligned} \tag{4.23}$$

với $\gamma_b^{(P)} = 2^{R_b^{(P)}} - 1$.

Tốc độ lộ tin trung bình tại PU $R_L^{(P-NC)}$ trong trường hợp này được xác định qua $\text{SINR}^{(E-NC)}$, giá trị $\text{SINR}^{(E-NC)}$ chỉ phụ thuộc vào một biến ngẫu nhiên g_{pe} có phân phối mũ. Dựa trên kết quả của Bổ đề 2, kỳ vọng của mức độ không rõ ràng tại kẻ nghe lén trong trường hợp không hợp tác được xác định trong bổ đề sau.

Bổ đề 6. *Khi U là biến ngẫu nhiên có phân phối mũ với kỳ vọng Ω_U, biến ngẫu*

nhiên $Z = h_{m,n}(U)$*, với* $h_{m,n}$ *được định nghĩa trong* (4.3)*, có kỳ vọng là:*

$$\mathbb{E}\{Z\} = 1 - \frac{\exp(1/\Omega_U)}{n \ln 2}\left[\text{Ei}\left(-\frac{2^m}{\Omega_U}\right) - \text{Ei}\left(-\frac{2^{m-n}}{\Omega_U}\right)\right], \tag{4.24}$$

Chứng minh. Bổ đề 6 được chứng minh trong phần phụ lục B. ■

Áp dụng Bổ đề 6 với U là biến ngẫu nhiên $\frac{p_P}{N_E} g_{pe}$ có phân phối mũ với kỳ vọng $p_P \Omega_{pe}/N_E$, ta có công thức tỷ lệ lượng tin bị lộ trong trường hợp không hợp tác là:

$$R_L^{(NC)} = \frac{1}{\ln 2} \exp\left(\frac{N_E}{p_P \Omega_{pe}}\right)\left[\text{Ei}\left(-\frac{N_E 2^{R_b^{(P)}}}{p_P \Omega_{pe}}\right) - \text{Ei}\left(-\frac{N_E 2^{R_b^{(P)} - R_s^{(P)}}}{p_P \Omega_{pe}}\right)\right]. \tag{4.25}$$

4.2 Phát triển và giải quyết bài toán

Với mô hình là một bài toán tối ưu đa mục tiêu, việc giải quyết bài toán (3.11) theo một phương pháp hậu nghiệm chỉ xác định một tập các lời giải tối ưu Pareto. Tức là sau đó, ta vẫn cần sử dụng một bộ hỗ trợ quyết định để lựa chọn lời giải phù hợp với mục tiêu của người dùng, ở đây là SU. Do đó, đồ án thực hiện giải quyết bài toán tối ưu đa mục tiêu (3.11) bằng việc chuyển về bài toán tối ưu đơn mục tiêu theo phương pháp ràng buộc ϵ. Việc lựa chọn hàm mục tiêu ưu tiên và các ràng buộc phụ thuộc vào mong muốn thiết kế của SU. Như đã đề cập trong Chương 3, SU có hai mục tiêu là (i) được PU lựa chọn và chia sẻ tài nguyên tần số để có thể thực hiện truyền tin và (ii) mức độ an toàn khi truyền tin phải được đảm bảo.

4.2.1 Tối ưu cho người dùng thứ cấp

Với hai mục tiêu đã đề cập, bài toán (3.11) được chuyển thành:

$$\begin{aligned}
\underset{p_P, p_S}{\text{minimize}} \quad & R_L^{(S)} && \text{(4.26a)}\\
\text{s.t} \quad & R_L^{(P)} \le \theta^{(P)}, && \text{(4.26b)}\\
& p_{tx}^{(P)} \ge \sigma^{(P)}, && \text{(4.26c)}\\
& p_{tx}^{(S)} \ge \sigma^{(S)}, && \text{(4.26d)}\\
& 0 \le p_P \le p_P^{\max}, && \text{(4.26e)}\\
& 0 \le p_S \le p_S^{\max}, && \text{(4.26f)}
\end{aligned}$$

Bài toán này thực hiện chuyển hàm mục tiêu $R_L^{(P)}$ thành điều kiện ràng buộc (4.26b). Lúc này, ưu tiên của SU là thiết kế chiến lược tối ưu cho hiệu năng an toàn của mình, trong khi hiệu năng an toàn của PU chỉ cần đảm bảo ở mức "chấp nhận được" $\theta^{(P)}$. Như đã đề cập trong Chương 3, PU sẵn sàng hợp tác (chia sẻ tần số và

cùng truyền tin) nếu như hiệu năng an toàn của PU khi hợp tác tốt hơn khi không hợp tác. Như vậy, mức "chấp nhận được" ở đây, $\theta^{(P)}$, là tốc độ lộ tin trung bình của PU trong điều kiện chỉ có PU truyền tin (non-cooperation, NC), hay $\theta^{(P)} = R_L^{(NC)}$. Có thể thấy, nghiệm tối ưu giải được từ bài toán (4.26) đảm bảo được cả hai mục tiêu của bài toán ban đầu. Đồng thời, thiết kế này cũng phù hợp với thực tế khi mà các đối tượng trong hệ thống luôn ích kỷ, chỉ lựa chọn chiến lược tốt nhất cho mình khi đưa ra các quyết định. Trong đồ án này, bài toán (4.26) được gọi là "Bài toán tối ưu cá nhân".

4.2.2 Mở rộng mô hình

Bài toán tối ưu cá nhân hoàn toàn phù hợp trong thực tiễn khi mà PU và SU có lợi ích khác nhau và không có lý do gì để SU, bên đề xuất chiến lược, hạn chế hiệu năng của mình để gia tăng hiệu năng cho PU. Tuy nhiên, khi xem xét trường hợp hệ thống có nhiều SU cạnh tranh với nhau để được PU lựa chọn cùng truyền tin, các SU sẽ cần cân nhắc kỹ hơn giữa hai mục tiêu truyền tin đã đề cập.

Trong vấn đề mở rộng này, mô hình hệ thống vẫn bao gồm một PU, song sẽ có nhiều SU, mỗi bên đều có một kẻ nghe lén riêng và đều cần đảm bảo truyền tin mức độ an toàn xác định. Khi muốn truyền tin, PU sẽ lựa chọn một trong các SU để cùng truyền. SU được lựa chọn là SU đem lại hiệu năng an toàn cao nhất cho PU và đồng thời, mức độ an toàn phải cao hơn khi PU không cần hợp tác. Giả thiết rằng, mặc dù mô hình có nhiều SU nhưng các SU này không có bất kỳ thông tin gì về nhau, mỗi SU có cách thức riêng để liên lạc với PU. Như vậy, việc mở rộng mô hình không làm thay đổi bài toán thiết kế (3.11) đã đề cập trong Chương 3. Các SU cũng giải bài toán tối ưu của riêng mình, độc lập với nhau và không bị chi phối bởi các tham số khác.

Việc mở rộng mô hình với nhiều SU giúp PU cải thiện hiệu năng an toàn của mình theo hai phương diện. Thứ nhất, số lượng SU càng tăng càng làm đa dạng vị trí của các SU và đặc tính kênh truyền, từ đó càng tăng khả năng có một SU với vị trí và điều kiện truyền tin phù hợp giúp tăng khác biệt lợi thế giữa kênh truyền chính và kênh truyền nghe lén của PU. Thứ hai, khi có càng nhiều SU, mức độ cạnh tranh tài nguyên tần số (do PU chia sẻ) càng cao, từ đó, trong việc thiết kế chiến lược truyền, các SU sẽ không chỉ tập trung vào hiệu năng cho riêng mình, mà cần cân nhắc cả hiệu năng của PU. Hiệu năng của PU càng được cải thiện thì cơ hội SU được lựa chọn càng cao.

Với mô hình mở rộng này, bài toán tối ưu đa mục tiêu (3.11) được chuyển thành:

$$\underset{p_P, p_S}{\text{minimize}} \quad R_L^{(P)} \tag{4.27a}$$

$$\text{s.t} \quad R_L^{(S)} \leq \theta^{(S)}, \tag{4.27b}$$

$$p_{tx}^{(P)} \geq \sigma^{(P)}, \tag{4.27c}$$

$$p_{tx}^{(S)} \geq \sigma^{(S)}, \tag{4.27d}$$

$$0 \leq p_P \leq p_P^{\max}, \tag{4.27e}$$

$$0 \leq p_S \leq p_S^{\max}, \tag{4.27f}$$

lúc này, hàm mục tiêu là hiệu năng an toàn ứng với PU $R_L^{(P)}$ và hiệu năng cho SU được đảm bảo thông qua một ngưỡng $\theta^{(S)}$ do SU lựa chọn.

Có một hướng tiếp cận khác cho "Bài toán cạnh tranh" này là chỉnh sửa bài toán cá nhân (4.26) theo hướng giảm giá trị ngưỡng cho $\theta^{(P)}$ trong (4.26b), giá trị ngưỡng này càng giảm tức là hiệu năng của PU càng được cải thiện, không chỉ dừng lại ở mức "chấp nhận được" như trong (4.26). Tuy nhiên, hướng giải quyết này không giúp gia tăng đáng kể cơ hội được PU lựa chọn, bởi các SU không có thông tin về nhau nên không thể lựa chọn giá trị ngưỡng tốt nhất cho bài toán. Với bài toán đề xuất (4.27), SU có thể đưa ra chiến lược chỉ dựa trên các thông tin mình có với tham số tùy chỉnh duy nhất là $\theta^{(S)}$, phụ thuộc vào mức độ quan trọng của thông điệp cần gửi. Khi thông điệp cần gửi có yêu cầu an toàn thấp, SU có thể lựa chọn $\theta^{(S)}$ lớn, từ đó tăng phạm vi giá trị hợp lệ của p_P và p_S, giúp tăng khả năng tìm được $R_L^{(P)}$ với giá trị nhỏ hơn, và kết quả là cơ hội SU được truyền tin càng cao.

4.3 Phương pháp giải quyết bài toán

Cả hai bài toán đề xuất đều là các bài toán tối ưu đơn mục tiêu với hàm mục tiêu là tốc độ lộ thông tin trung bình. Như đã phân tích ở đầu chương, các công thức $R_L^{(P)}$ (4.8) và $R_L^{(S)}$ (4.12) liên quan đến tích phân hàm mũ Ei, điều đó làm bài toán tối ưu khó giải quyết bằng phương pháp phân tích. Tác giả Huang và các cộng sự [49] đã giải quyết vấn đề này bằng việc xấp xỉ Ei với giả thiết về chất lượng tín hiệu nhận tại PU, $\text{SINR}^{(P)}$ là lớn. Trong đồ án này, các bài toán tối ưu (4.26) và (4.27) sẽ được giải quyết bằng thuật toán tiến hóa vi phân (differential evolution). Mặc dù phương pháp này đòi hỏi thời gian thực thi lớn hơn, nhưng lời giải tối ưu tìm được là chính xác và có cơ hội tìm được nghiệm tối ưu toàn cục của các bài toán.

4.4 Kết chương

Chương này đã giải quyết bài toán tối ưu đề cập trong Chương 3 bằng việc phân tích các đại lượng và các điều kiện ràng buộc, sau đó đề xuất hướng phát triển bài toán ban đầu. Trong quá trình đánh giá các điều kiện ràng buộc, chương này cũng

đề xuất các công thức giúp xác định dải giá trị hợp lệ cho các tham số của bài toán, đảm bảo bài toán tối ưu có nghiệm. Hai đề xuất phát triển bài toán ban đầu là "Bài toán tối ưu cá nhân" và "Bài toán cạnh tranh" cho thấy sự phù hợp với thực tế khi đưa lợi ích của các bên vào quá trình mô hình hóa bài toán tối ưu. Việc lựa chọn bài toán phản ánh sự ưu tiên của người thiết kế - SU, đối với các mục tiêu truyền tin của mình. Với kết quả phân tích và phát triển bài toán, giải thuật tiến hóa vi phân được đề xuất sử dụng, không chỉ vì những ưu điểm của thuật toán mà còn vì sự phức tạp của các bài toán cần giải quyết. Dựa trên các đề xuất trong chương này, Chương 5 sẽ triển khai thử nghiệm các bài toán với số liệu mô phỏng.

CHƯƠNG 5. ĐÁNH GIÁ THỰC NGHIỆM

Chương này thực hiện đánh giá kết quả của hai bài toán tối ưu (4.26) và (4.27) đã đề cập trong Chương 4 thông qua quá trình mô phỏng với dữ liệu ngẫu nhiên. Đồng thời, hiệu năng hệ thống trong hai chiến lược này cũng được so sánh. Ngoài ra, chương này cũng đánh giá các hiệu năng của các bên trong mô hình hệ thống mở rộng, với nhiều SU cạnh tranh với nhau.

5.1 Các tham số thí nghiệm

Trong các thử nghiệm, giá trị của một số tham số sau là cố định cho tất cả các trường hợp. Mật độ phổ công suất nhiễu tại các bên nhận được cố định là $\mathcal{N}_0 = 4.0 \times 10^{-21}$ W/Hz, với công suất phát tối đa cho các bên $20\mathcal{N}_0$ W/Hz. Tốc độ mã hóa tại các bên được thiết lập là $R_b^{(P)} = 1.0$ bps/Hz, $R_b^{(S)} = 1.0$ bps/Hz và tốc độ truyền tin tương ứng $R_s^{(P)} = 0.8$ bps/Hz, $R_s^{(S)} = 0.8$ bps/Hz.

Nhằm đánh giá ảnh hưởng của hiệu ứng suy giảm theo khoảng cách (path loss) tới các hiệu năng của hệ thống, các thử nghiệm số liệu trong đồ án này được tiến hành với giả thiết trung bình các độ lợi kênh truyền chỉ phụ thuộc vào khoảng cách giữa bên phát và bên nhận, theo công thức:

$$\Omega_X = \Omega_0 d^{-\alpha}, \tag{5.1}$$

với d là khoảng cách giữa bên phát và bên nhận (đơn vị mét, m), Ω_0 là trung bình độ lợi kênh truyền tại khoảng cách 1m và α là hệ số suy giảm. Trong các thử nghiệm, $\alpha = 3.5$ và Ω_0 được chọn để đảm bảo tỷ số tín hiệu trên nhiễu SNR (không bao gồm can nhiễu) tại khoảng cách 20m là 5dB, khi bên phát truyền tin với công suất phát là $10\mathcal{N}_0$ W/Hz.

Dễ thấy rằng, theo công thức (4.18), điều kiện kênh truyền cũng ảnh hưởng đến xác suất truyền tin tối đa mà các bên có thể đạt được. Do đó, thay vì xác định giá trị tuyệt đối cho xác suất truyền tin tối thiểu $\sigma^{(P)}$ và $\sigma^{(S)}$, các bên sẽ lựa chọn hai giá trị $\rho^{(P)}$ và $\rho^{(S)}$, phản ánh tỷ lệ xác suất truyền tin cần đạt được so với xác suất truyền tin cực đại, cụ thể:

$$\begin{aligned} \sigma^{(P)} &= \rho^{(P)} \max\left\{p_{tx}^{(P)}\right\}, \\ \sigma^{(S)} &= \rho^{(S)} \max\left\{p_{tx}^{(S)}\right\}, \end{aligned} \tag{5.2}$$

với $\max\left\{p_{tx}^{(P)}\right\}, \max\left\{p_{tx}^{(S)}\right\}$ xác định trong (4.18). Nếu như không đề cập cụ thể, các giá trị này mặc định là $\rho^{(P)} = 0.5$ và $\rho^{(S)} = 0.5$.

Về phương pháp giải quyết bài toán tối ưu, đồ án sử dụng giải thuật tiến hóa vi phân DE, với chiến lược DE/rand/1/bin, tức là cá thể mục tiêu được lựa chọn ngẫu nhiên (rand) với một cặp cá thể dùng làm đại lượng đột biến và chiến lược lai tạo là lai tạo đồng bộ (uniform crossover). Trong các thử nghiệm, kích thước quần thể được thiết lập là $NP = 20$ với biên độ đột biến $F = 0.5$ và tốc độ lai tạo $CR = 0.9$. Điều kiện dừng cho thuật toán DE xác định dựa trên số lượng thế hệ tối đa, $G_{max} = 50$.

5.2 Phương pháp thí nghiệm

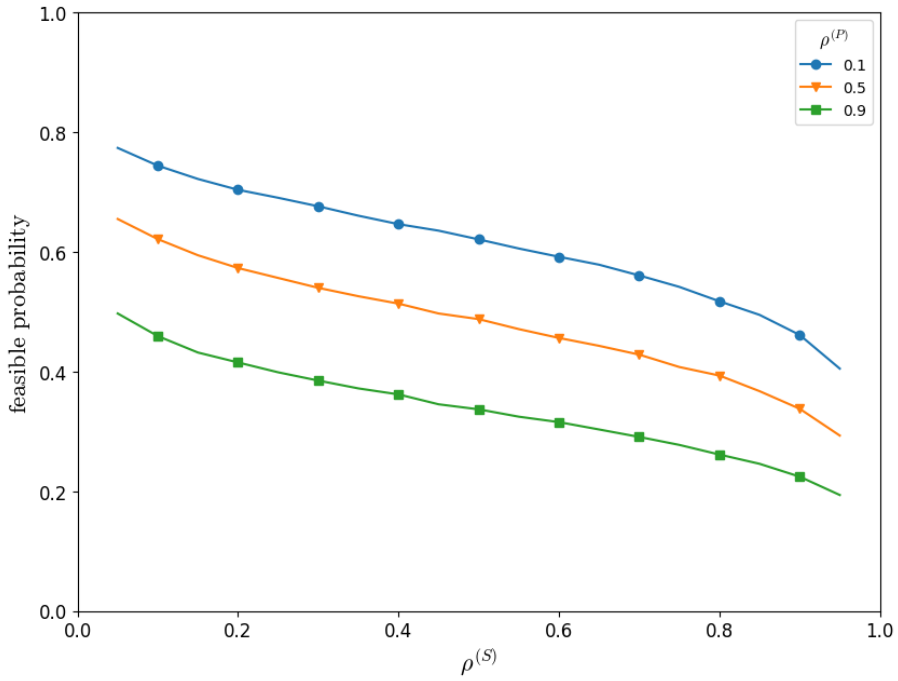
Phương pháp thí nghiệm được sử dụng trong đồ án là Monte Carlo với 200000 mẫu thử nghiệm. Trong các kết quả khác nhau, khi áp dụng các điều kiện lọc khác nhau, số lượng mẫu thử nghiệm có thể khác số lượng mẫu tổng cộng. Do đó, trong từng kết quả, số lượng mẫu thử nghiệm sẽ được thể hiện cụ thể theo tham số N.

Mỗi mẫu thử nghiệm tương ứng với một bộ các khoảng cách giữa từng cặp đối tượng thu-phát trong hệ thống. Các mẫu thử nghiệm được sinh ngẫu nhiên độc lập trong dải giá trị từ $[1, R_0]$. Giá trị R_0 được cố định là 30m trong tất cả thử nghiệm. Độ lợi kênh trung bình Ω_X tương ứng với từng khoảng cách sẽ được tính theo công thức (5.1). Các kết quả thử nghiệm hầu hết đều biểu diễn theo hàm phân phối tích lũy thực nghiệm (empirical CDF), biểu diễn phân bố các giá trị dưới một ngưỡng.

5.3 Điều kiện ràng buộc về xác suất truyền tin trong trường hợp hợp tác

Trước khi trình bày chi tiết các kết quả về hai bài toán chính của đồ án, phần này đánh giá các điều kiện ràng buộc về xác suất truyền tin trong các bài toán này. Các tham số $\sigma^{(P)}$ (hay $\rho^{(P)}$) và $\sigma^{(S)}$ (hay $\rho^{(S)}$) có tác động lớn tới điều kiện khả thi của các bài toán tối ưu. Hình 5.1 thể hiện tác động của ngưỡng xác suất truyền tin yêu cầu tại SU và PU ($\rho^{(S)}$ và $\rho^{(P)}$) tới xác suất có nghiệm của bài toán tối ưu (3.11). Kết quả chỉ ra rằng, khi PU và SU càng đặt ra yêu cầu cao về xác suất truyền tin của mình thì bài toán tối ưu này càng ít cơ hội có nghiệm, tức là SU càng ít khả năng được hợp tác. Điều này hoàn toàn dễ hiểu vì xác suất truyền tin phụ thuộc vào điều kiện kênh truyền từ bên phát tới bên thu, trong đó có cả đường truyền can nhiễu. Yêu cầu ngưỡng xác suất tối thiểu quá cao đồng nghĩa loại bỏ những điều kiện kênh truyền không tốt, từ đó mà giảm cơ hội một điều kiện truyền tin bất kỳ đạt được yêu cầu đó.

Dựa trên công thức về tốc độ lộ tin trung bình tại các bên (3.6) và (3.9), thấy rằng các giá trị này không phụ thuộc vào các kênh truyền h_{pp}, h_{ps}, h_{sp} và h_{ss}, tức là các tham số $\rho^{(P)}$ và $\rho^{(S)}$ chỉ ảnh hưởng đến xác suất truyền tin mà không ảnh hưởng đến các hiệu năng an toàn trong các bài toán (4.26) và (4.27). Do đó, trong các thử nghiệm ở phần sau, dữ liệu được sinh luôn thỏa mãn các điều kiện ràng buộc về xác



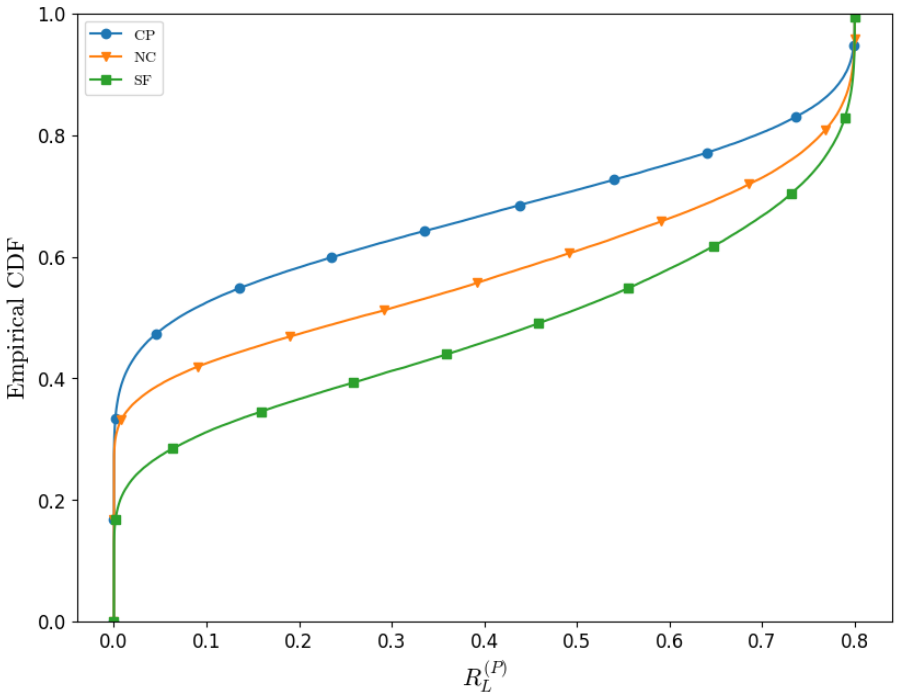
Hình 5.1: Ảnh hưởng của xác suất truyền tin tối thiểu tới điều kiện khả thi của các bài toán tối ưu. $N = 50000$

suất truyền tin. Cũng theo kết quả từ Hình 5.1, bộ tham số $\rho^{(P)} = 0.5, \rho^{(S)} = 0.5$ cho khoảng 50% trường hợp dữ liệu sinh là hợp lệ.

5.4 So sánh giữa các bài toán đề xuất

Để so sánh hiệu năng hệ thống giữa các bài toán đề xuất, phần này tạm thời bỏ qua các điều kiện ràng buộc (4.26b), (4.27b) liên quan đến tốc độ lộ tin trung bình trong "bài toán tối ưu cá nhân" (4.26) và "bài toán cạnh tranh" (4.27). Phần này thực hiện đánh giá hiệu năng tại PU trong ba trường hợp: (i) tối ưu tốc độ lộ tin trung bình $R_L^{(NC)}$ (4.24) khi chỉ có PU truyền tin (NC), (ii) ưu tiên tối ưu cho SU (SF), là bài toán (4.26) không bao gồm ràng buộc (4.26b) và (iii) ưu tiên tối ưu cho PU (CP), là bài toán (4.27) không bao gồm ràng buộc (4.27b). Có thể thấy rằng với ba chiến lược này, kết quả đánh giá hiệu năng an toàn của SU cũng có thể phát biểu tương tự vì tính đối xứng giữa hai chiến lược SF và CP. Cũng chú ý rằng, điều kiện ràng buộc (4.26b) của "bài toán tối ưu cá nhân" tương ứng với việc so sánh giữa hai chiến lược SF và NC. Như vậy, kết quả trong phần này cũng phản ánh điều kiện hợp tác giữa PU và SU.

Hình 5.2 so sánh tốc độ lộ tin trung bình tại PU trong ba trường hợp, NC, SF và CP, tương ứng với ba chiến lược tối ưu khác nhau. Khi so sánh giữa hai trường hợp ưu tiên tối ưu cho PU là NC (không hợp tác) và CP (hợp tác với SU), ta thấy rằng việc hợp tác với SU giúp PU đạt được trung bình tốc độ lộ tin nhỏ hơn nhiều so với trường hợp không hợp tác. Tuy nhiên, việc hợp tác này không đem lại hiệu



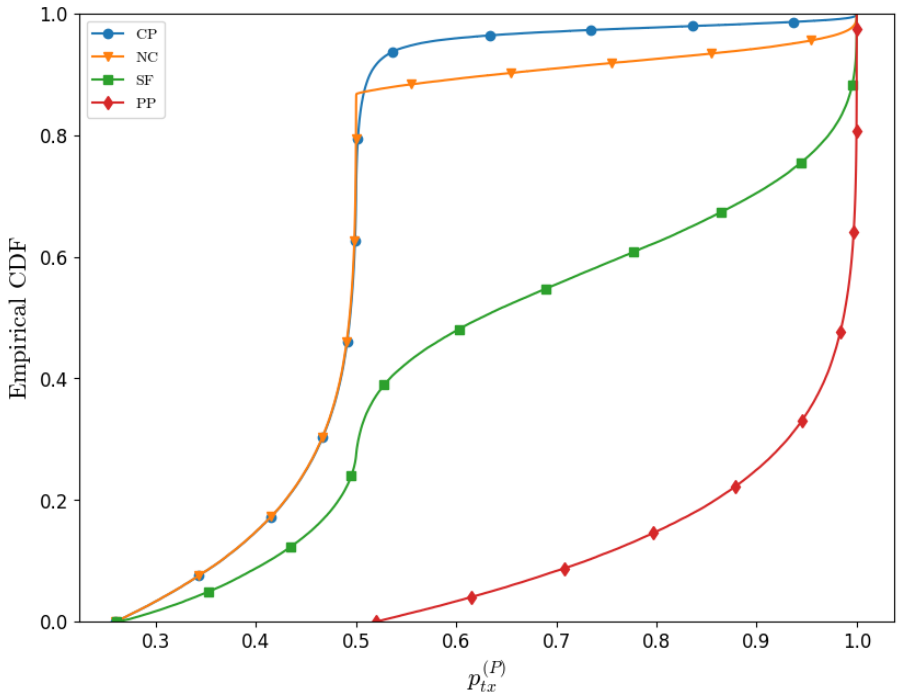
Hình 5.2: So sánh tốc độ lộ tin trung bình tại PU giữa các chiến lược tối ưu khác nhau. $N = 200000$

quả cho PU nếu như SU chỉ tập trung tối ưu cho lợi ích của mình, tương ứng với trường hợp SF.

Mặt khác, khi đánh giá hiệu năng của PU theo xác suất truyền tin $p_{tx}^{(P)}$, kết quả thu được trong Hình 5.3 cho thấy điều ngược lại. Lúc này xác suất truyền tin của PU trong chiến lược SF lại cao hơn nhiều so với hai chiến lược còn lại: có đến 60% các trường hợp trong NC và CP ở đó xác suất truyền tin dưới 50%, nhưng chỉ có khoảng 20% trường hợp xác suất truyền tin trong SF là dưới 50%. Do các kết quả thử nghiệm được đánh giá trên cùng tập mẫu, tức là cùng điều kiện kênh truyền, nên kết quả này phản ánh đặc điểm giá trị công suất phát tối ưu trong các trường hợp đó. Với cùng điều kiện kênh truyền và điều kiện hợp tác, công suất phát càng thấp thì xác suất truyền tin càng thấp. Trong Hình 5.3, ngoài ba chiến lược đã nêu, đường PP được thêm vào nhằm xác định giá trị xác suất truyền tin lớn nhất mà PU có thể đạt được, tương ứng với $\max\left\{p_{tx}^{(P)}\right\}$ và công suất phát tại PU là tối đa, p_P^{max}. Kết quả thể hiện trong Hình 5.2 và Hình 5.3 cho thấy rất khó để cùng tối ưu cho hiệu năng an toàn và hiệu quả truyền tin, các bên thường phải chịu đánh đổi một trong hai mục tiêu này.

5.4.1 Trong điều kiện xác suất truyền tin tương đồng

Để đánh giá khách quan hiệu quả an toàn của PU giữa các chiến lược, phần tiếp theo sẽ trình bày kết quả so sánh giữa các chiến lược khi xác suất truyền tin tại PU sai khác nhau dưới 1%. Hình 5.4a phản ánh mức độ chênh lệch về $R_L^{(P)}$ đạt được



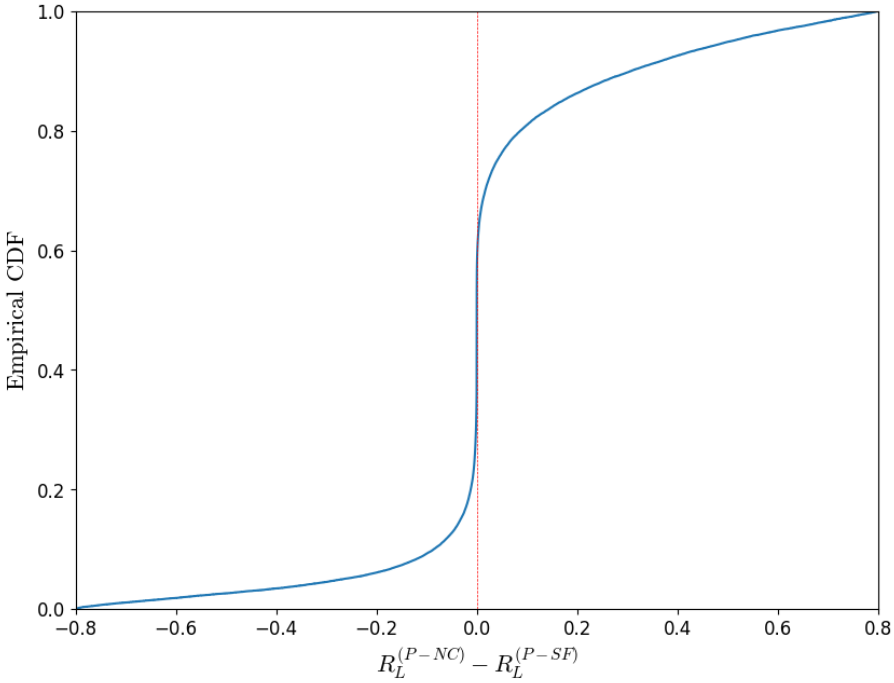
Hình 5.3: So sánh xác suất truyền tin tại PU giữa các chiến lược tối ưu khác nhau. $N = 200000$

tại hai chiến lược SF và NC. Trong hình, phần giá trị dương theo trục hoành tương ứng với các trường hợp $R_L^{(P)}$ trong chiến lược SF tốt hơn chiến lược NC. Có thể thấy trong hầu hết trường hợp, các giá trị chênh lệch đều rất gần 0. Khi so sánh phần giá trị dương với phần giá trị âm, ta thấy có đa số các trường hợp mà chiến lược SF (chiến lược hợp tác) giúp cải thiện hiệu năng an toàn so với NC (chỉ có PU truyền tin). Như vậy, với cùng xác suất truyền tin, ngay cả khi SU chỉ ưu tiên tối ưu cho hiệu năng của mình thì việc hợp tác với SU cũng giúp PU cải thiện hiệu năng an toàn. Hình 5.4b cũng cho thấy kết quả tương tự khi so sánh giữa hai chiến lược CP và NC. Song với trường hợp này, do chiến lược CP ưu tiên tối ưu $R_L^{(P)}$ nên chênh lệch về hiệu quả an toàn so với chiến lược NC là cao hơn rõ rệt.

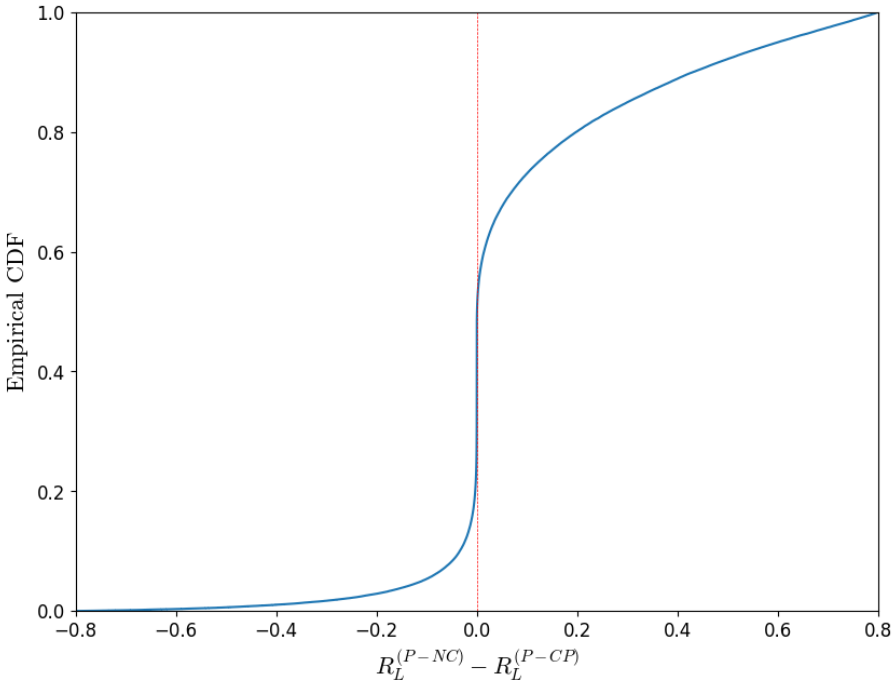
5.4.2 Trong điều kiện kênh truyền nghe lén khác nhau

Với mong muốn thấy rõ lợi ích của truyền tin hợp tác, phần này đánh giá các chiến lược trong trường hợp điều kiện kênh truyền nghe lén khác nhau. Cụ thể điều kiện này được đánh giá dựa trên so sánh khoảng cách từ PTx và STx tới kẻ nghe lén EAVP, tương ứng các đường truyền h_{pe} và h_{se}.

Hình 5.5a biểu diễn tốc độ lộ tin trung bình tại PU trong trường hợp bất lợi với kẻ nghe lén, vì lúc này can nhiễu từ STx gây ra lớn hơn. Do đó, trong trường hợp này, giá trị $R_L^{(P)}$ trong các chiến lược đều tập trung vào dải giá trị nhỏ. Khi so sánh giữa hai chiến lược SF và NC, ta thấy NC thể hiện tốt hơn khi mật độ dải giá trị nhỏ của $R_L^{(P)}$ ($[0, 0.4]$) cao hơn. Mặt khác, mật độ dải giá trị lớn của $R_L^{(P)}$ ($[0.4, 0.8]$)



(a) Giữa SF và NC



(b) Giữa CP và NC

Hình 5.4: So sánh tốc độ lộ thông tin giữa các chiến lược trong các trường hợp xác suất truyền tin tại PU tương đồng nhau. $N = 50000$

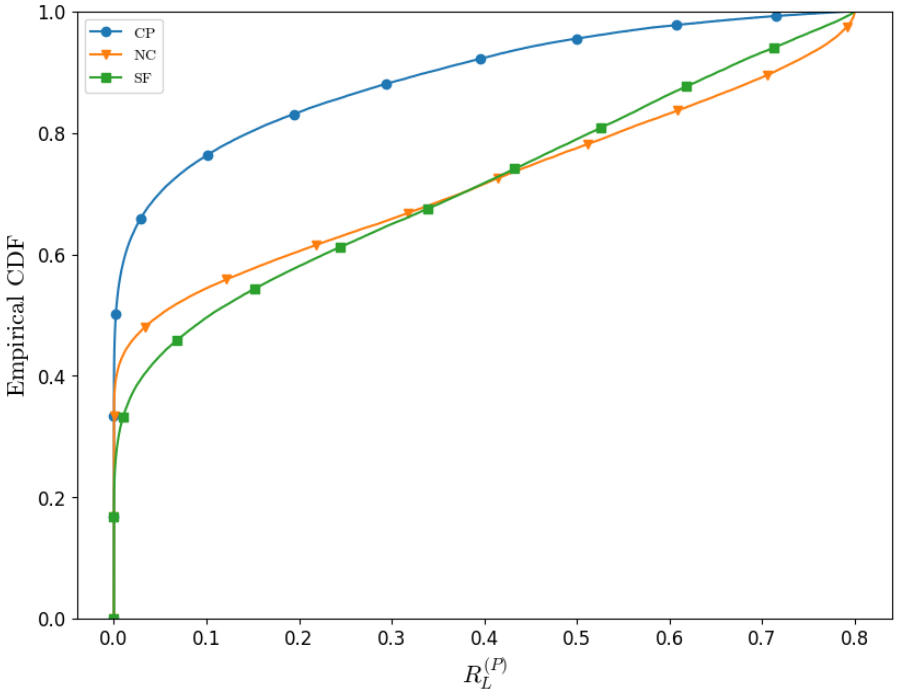
trong chiến lược NC lại cao hơn trong chiến lược SF. Điều này là do hiệu năng an toàn của NC chỉ phụ thuộc vào Ω_{pe}: dải giá trị nhỏ của $R_L^{(P)}$ tương ứng với Ω_{pe} nhỏ và dải giá trị lớn tương ứng với Ω_{pe} lớn. Trong khi đó, hiệu năng an toàn của SF được tác động bởi cả Ω_{pe} và Ω_{se}, nên kết quả ổn định hơn.

Khác với trường hợp trên, Hình 5.5b biểu diễn tốc độ lộ tin trung bình tại PU trong trường hợp có lợi với kẻ nghe lén. Vì thế, giá trị $R_L^{(P)}$ lúc này tập trung vào dải giá trị lớn. Trong trường hợp này, NC lại thể hiện là một chiến lược hiệu quả. Lý do là bởi hai chiến lược CP và SF không khai thác được nhiều lợi ích từ can nhiễu của SU. Tuy nhiên, tương tự như Hình 5.5a, khi so sánh giữa hai chiến lược CP và NC, ta thấy việc hợp tác với SU giúp chất lượng truyền tin an toàn của PU ổn định hơn. Có thể thấy, trong điều kiện kênh truyền này, cơ hội mà SU được hợp tác truyền tin với PU là rất thấp, hoặc nếu được lựa chọn thì hiệu năng an toàn tại SU cũng không cao.

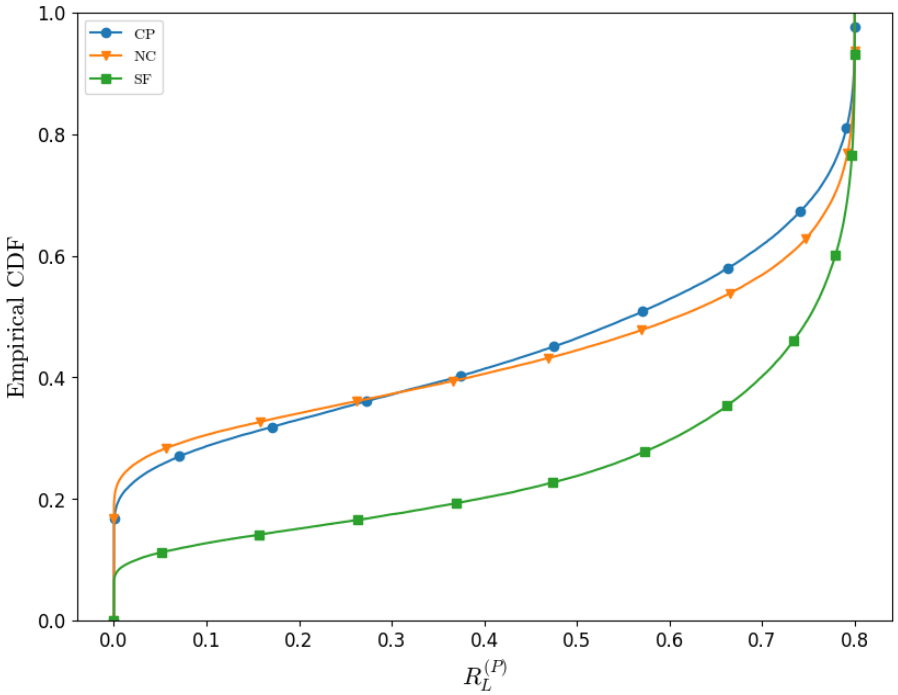
5.5 Hệ thống với nhiều người dùng thứ cấp

Phần này trình bày kết quả liên quan đến mô hình mở rộng, trong đó hệ thống có nhiều SU cạnh tranh với nhau để được PU lựa chọn cùng truyền tin. Trước hết, phần này thực hiện đánh giá hiệu năng hệ thống theo tham số $\theta^{(S)}$ trong "bài toán cạnh tranh". Hình 5.6a và Hình 5.6b biểu diễn tốc độ lộ tin trung bình tại PU và SU ứng với các giá trị $\theta^{(S)}$ khác nhau. Kết quả cho thấy, khi $\theta^{(S)}$ càng tăng, tức yêu cầu về an toàn của SU càng thấp, thì hiệu quả an toàn tại PU càng cao. Tuy nhiên, ngay cả khi các ngưỡng $\theta^{(S)}$ có sự thay đổi lớn (chênh lệch 0.3), giá trị $R_L^{(P)}$ không cho thấy sự thay đổi đáng kể. Điều đó cho thấy, điều kiện kênh truyền ảnh hưởng không nhỏ tới hiệu quả truyền tin của hệ thống. Ngay cả khi SU lựa chọn ưu tiên tối ưu cho hiệu năng an toàn của PU thì cũng không tăng đáng kể khả năng SU được PU lựa chọn hợp tác truyền tin.

Hình 5.7a và Hình 5.7b tương ứng biểu diễn tốc độ lộ tin trung bình tại PU và SU (SU được lựa chọn hợp tác) trong mô hình mở rộng với M SU. Như đã đề cập, SU được lựa chọn là SU đề xuất chiến lược mang lại hiệu quả an toàn cao nhất cho PU. Trong thử nghiệm này, tất cả SU đều lựa chọn chiến lược ưu tiên tối ưu $R_L^{(P)}$, ứng với bài toán (4.27), trong đó $\theta^{(S)} = 0.5$. Kết quả cho thấy, khi số lượng SU tăng lên thì hiệu quả an toàn tại PU được cải thiện rõ rệt. Đặc biệt, chỉ với hai SU, $M = 2$, có đến khoảng 50% cơ hội để tốc độ lộ tin trung bình của PU rất gần 0 (với sai số 10^{-3}), giá trị này lên tới 75% khi $M = 4$ và gần như chắc chắn khi $M = 8$. Như vậy, mặc dù PU khó cải thiện hiệu năng an toàn với các chiến lược thiết kế của SU, nhưng khi số lượng SU lớn, PU có thể tăng đáng kể hiệu quả truyền tin an toàn. Mặt khác, hiệu quả an toàn của SU lại không suy giảm nhiều, thậm chí còn

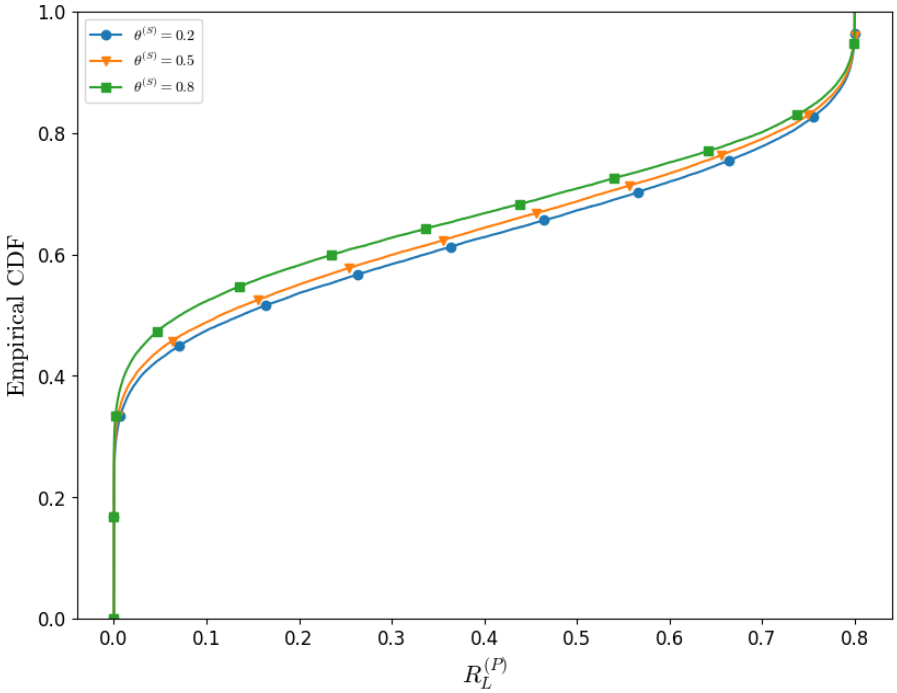


(a) $\Omega_{pe} < \Omega_{se}$

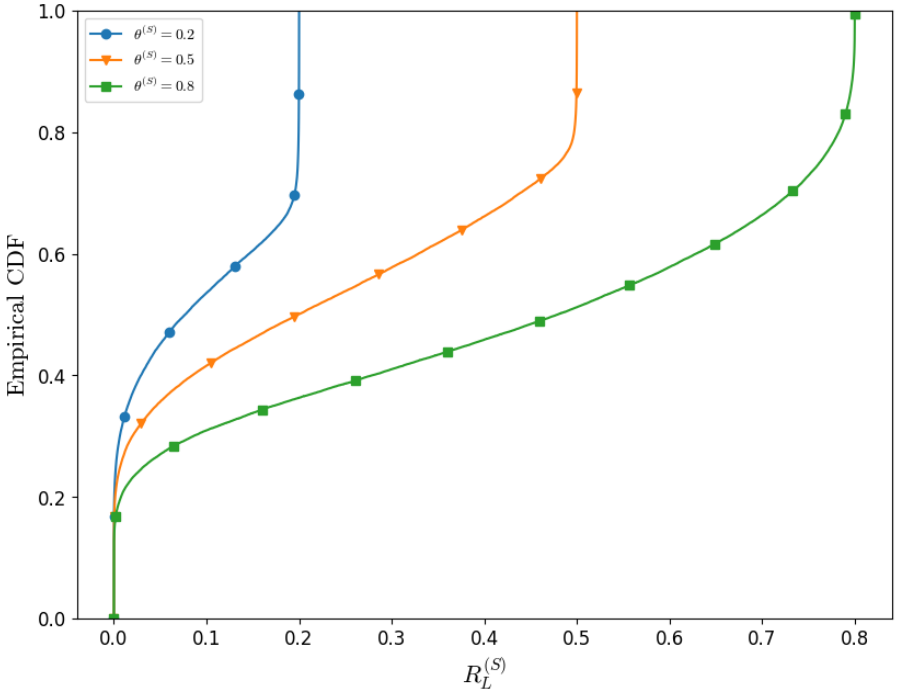


(b) $\Omega_{pe} > \Omega_{se}$

Hình 5.5: So sánh tốc độ lộ thông tin giữa các chiến lược trong trường hợp điều kiện kênh truyền nghe lén khác nhau. $N = 100000$



(a) PU



(b) SU

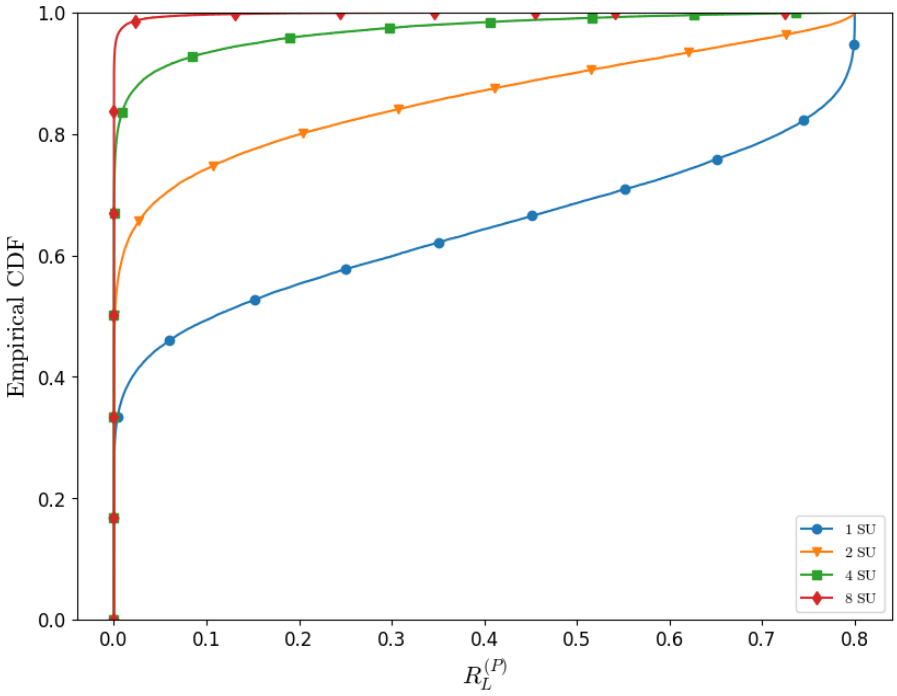
Hình 5.6: So sánh tốc độ lộ tin trung bình của PU và SU trong bài toán cạnh tranh với các giá trị $\theta^{(S)}$ khác nhau. $N = 50000$

có phần cải thiện khi mật độ của dải giá trị lớn giảm đi.

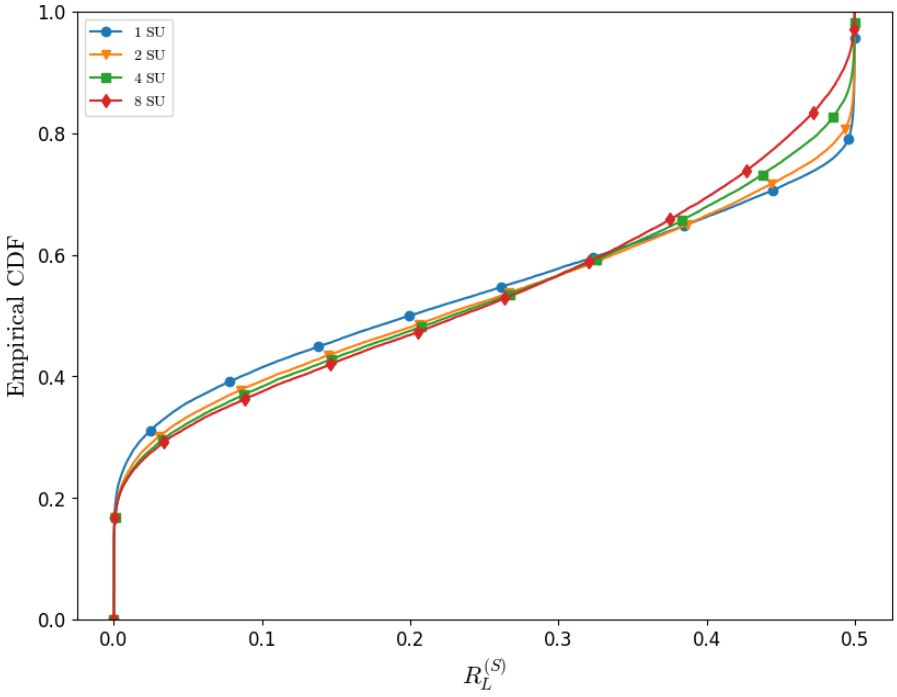
Với xác suất truyền tin của các bên trong mô hình mở rộng, kết quả thử nghiệm được thể hiện qua Hình 5.8a và Hình 5.8b. Kết quả cho thấy, khi số lượng SU tăng lên thì xác suất truyền tin tại PU cũng tăng lên đáng kể. Với $M = 8$, có tới 75% cơ hội để xác suất truyền tin của PU cao hơn 50%. Phía SU, xác suất truyền tin không cho thấy sự khác biệt rõ rệt. Như vậy, số lượng SU tăng lên không những giúp PU cải thiện hiệu quả truyền tin an toàn mà còn tăng xác suất truyền tin tại PU, trong khi đó, xác suất truyền tin tại SU không suy giảm. Từ các kết quả trên, có thể kết luận rằng, khi số lượng SU tăng lên, các hiệu năng an toàn của hệ thống ít chịu ảnh hưởng của điều kiện truyền tin.

5.6 Kết chương

Chương này đã thực hiện đánh giá tính hiệu quả của các bài toán đề xuất thông qua các thử nghiệm với dữ liệu sinh ngẫu nhiên, phản ánh các điều kiện đường truyền khác nhau. Thông qua các kết quả, chương này cũng cho thấy ưu điểm và hạn chế của các chiến lược đề xuất. Đặc biệt, kết quả thử nghiệm với nhiều người dùng cho thấy tiềm năng của đề xuất mở rộng hệ thống khi giúp tăng hiệu quả an toàn và xác suất truyền tin cho các bên, đặc biệt là bên sơ cấp.

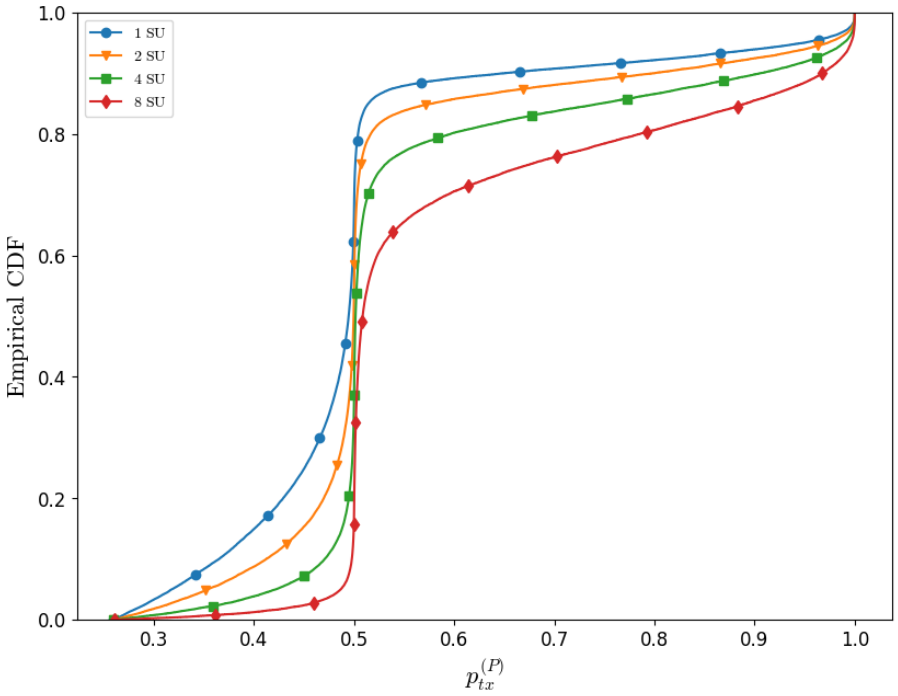


(a) PU

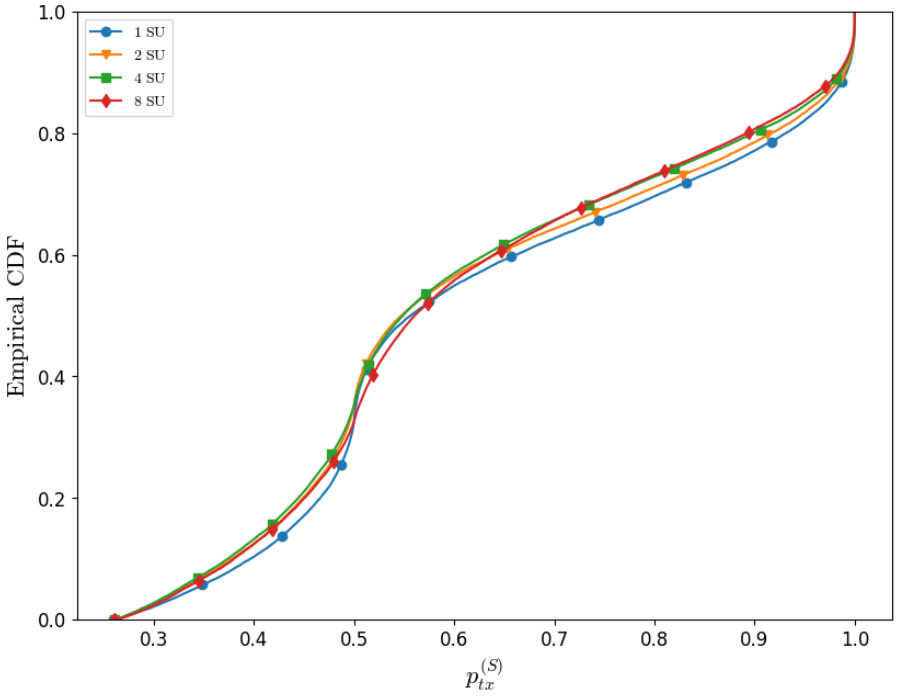


(b) SU được chọn

Hình 5.7: Đánh giá tốc độ lộ tin trong mô hình nhiều SU cạnh tranh. $N = 25000$



(a) PU



(b) SU được chọn

Hình 5.8: Đánh giá xác suất truyền tin trong mô hình nhiều SU cạnh tranh. $N = 25000$

CHƯƠNG 6. KẾT LUẬN

6.1 Kết luận

Trong quá trình hoàn thành đồ án tốt nghiệp, vấn đề an toàn bảo mật trong mạng vô tuyến nhận thức đã được đề cập, phân tích, đề xuất hướng giải quyết cũng như thử nghiệm đánh giá kết quả. Kết quả phân tích cho thấy vấn đề cần giải quyết là một vấn đề phức tạp khi hệ thống có nhiều người dùng khác nhau, với các lợi ích khác nhau, và thậm chí các lợi ích đó cũng xung đột với nhau. Để giúp giải quyết vấn đề này, đồ án đề xuất một chiến lược hợp tác giữa bên sơ cấp và bên thứ cấp thông qua một bài toán tối ưu đa mục tiêu. Trong đó, bên sơ cấp có quyền ưu tiên hơn trong vấn đề thiết kế, trong khi, bên thứ cấp có thể chủ động tùy chỉnh các mục tiêu và tham số thiết kế để cần cân bằng giữa hai lợi ích: được truyền tin và truyền tin an toàn. Trên cơ sở đó, bài toán ban đầu được phát triển và mở rộng, tương ứng phản ánh các lợi ích khác nhau của người dùng khác nhau. Kết quả thử nghiệm với các đề xuất đã chứng minh cho những phân tích trong đồ án. Tuy nhiên, do mô hình đề xuất còn đơn giản, các công nghệ và kỹ thuật xử lý tín hiệu chưa được khai thác sử dụng, nên kết quả thu được còn hạn chế và bị ảnh hưởng nhiều bởi điều kiện truyền tin. Song, với kết quả đạt được, đồ án cũng cho thấy tiềm năng của giải pháp đề xuất. Đồ án hy vọng rằng những đóng góp này sẽ được cộng đồng đón nhận, tiếp tục được khai thác và phát triển, góp phần hình thành một giải pháp cho vấn đề an toàn bảo mật trong mạng vô tuyến nhận thức.

6.2 Hướng phát triển trong tương lai

Kết quả của đồ án này còn nhiều hạn chế và bị chi phối nhiều bởi các điều kiện của môi trường truyền tin. Để vượt qua những hạn chế đó, hướng phát triển trong tương lai của đồ án tập trung vào việc khai thác những kỹ thuật xử lý tín hiệu cũng như các công nghệ hỗ trợ. Kỹ thuật định hướng búp sóng hay sinh nhiễu nhân tạo vốn là các kỹ thuật hiệu quả và được sử dụng nhiều trong các nghiên cứu về an toàn bảo mật lớp vật lý. Khi đó, mô hình hệ thống trong đồ án này có thể phát triển theo hướng sử dụng nhiều ăng-ten cho các bên nhằm định hướng tín hiệu tới người dùng hợp pháp hay gây nhiễu cho kẻ nghe lén. Bề mặt phản xạ thông minh (reconfigurable intelligent surfaces - RIS) cũng cho thấy là một công nghệ hiệu quả giúp hệ thống đạt được hiệu năng mong muốn ngay cả khi điều kiện kênh truyền không tốt. Cuối cùng, đồ án cũng mong muốn mở rộng mô hình hệ thống thành nhiều đối tượng cùng hợp tác, trong đó các bên thứ cấp có thể có cơ hội lựa chọn một trong nhiều bên sơ cấp để hợp tác truyền tin.

PHỤ LỤC

A. Phân tích kênh truyền

Trong Chương 3, đồ án đề xuất mô hình với hai bên phát PTx, STx đồng thời truyền tin. Cùng với đó, Chương 3 cũng xác định dung lượng kênh tại các bên nhận PRx, SRx, EAVP và EAVS. Dễ thấy rằng, khi độ lợi của tất cả các kênh truyền trong mô hình là các biến ngẫu nhiên độc lập có phân phối mũ với các kỳ vọng riêng, giá trị SINR tại các bên nhận có thể biểu diễn theo biến ngẫu nhiên U được định nghĩa trong (4.1), ứng với các bộ tham số a, b, c khác nhau. Do đó, phần này thực hiện khảo sát biến ngẫu nhiên U.

Biến ngẫu nhiên U được định nghĩa trong (4.1) phụ thuộc vào hai biến ngẫu nhiên độc lập X và Y có phân phối mũ với kỳ vọng tương ứng Ω_X và Ω_Y. Ta có hàm mật độ xác suất (PDF) và hàm phân phối tích lũy (CDF) của X, Y là:

$$
\begin{aligned}
f_X(x) &= \frac{1}{\Omega_X} \exp\left(-\frac{x}{\Omega_X}\right), \\
F_X(x) &= 1 - \exp\left(-\frac{x}{\Omega_X}\right), \\
f_Y(y) &= \frac{1}{\Omega_Y} \exp\left(-\frac{y}{\Omega_Y}\right), \\
F_Y(y) &= 1 - \exp\left(-\frac{y}{\Omega_Y}\right),
\end{aligned}
$$

và vì X, Y là độc lập thống kê nên có hàm mật độ xác suất đồng thời là:

$$
f_{XY}(x, y) = f_X(x) f_Y(y).
$$

Khi đó, hàm phân phối tích lũy $F_U(u)$ của biến ngẫu nhiên U định nghĩa trong (4.1) được tính như sau:

$$
\begin{aligned}
F_U(u) &= \mathbb{P}\left(\frac{aX}{bY + c} \leq u\right) \\
&= \mathbb{P}\left(X \leq \frac{u(bY + c)}{a}\right) \\
&= \int_0^{\infty} \int_0^{u(by+c)/a} f_{XY}(x, y)\, dxdy \\
&= \int_0^{\infty} \left(\int_0^{u(by+c)/a} f_X(x)\, dx\right) f_Y(y)\, dy \\
&= \int_0^{\infty} F_X\left(\frac{u(by + c)}{a}\right) f_Y(y)\, dy
\end{aligned}
$$

$$
\begin{aligned}
&= \int_0^\infty f_Y(y)\, dy - \int_0^\infty \exp\left(-\frac{u(by+c)}{a\Omega_X}\right) \frac{1}{\Omega_Y} \exp\left(-\frac{y}{\Omega_Y}\right) dy \\
&= 1 - \frac{1}{\Omega_Y} \exp\left(-\frac{uc}{a\Omega_X}\right) \int_0^\infty \exp\left(-y\left(\frac{ub}{a\Omega_X} + \frac{1}{\Omega_Y}\right)\right) dy \\
&= 1 - \frac{1}{\frac{b\Omega_Y}{a\Omega_X}u + 1} \exp\left(-\frac{uc}{a\Omega_X}\right).
\end{aligned}
$$

B. Phân tích mức độ không rõ ràng của kẻ nghe lén

Phụ lục A cho thấy các dung lượng kênh $C^{(E)}$, $C^{(F)}$ ứng với các bên nghe lén EAVP và EAVS có thể biểu diễn theo biến ngẫu nhiên U định nghĩa trong (4.1). Mặt khác, mức độ không rõ ràng của các kẻ nghe lén, $\Delta^{(P)}$ và $\Delta^{(S)}$ tương ứng, được biểu diễn theo các dung lượng kênh này. Từ công thức biểu diễn (3.5) và (3.8), thấy rằng biến ngẫu nhiên $Z = h_{m,n}(U)$ định nghĩa trong (4.3) có thể đại diện cho các đại lượng $\Delta^{(P)}$ và $\Delta^{(S)}$. Do đó, phần này thực hiện khảo sát biến ngẫu nhiên Z.

B.1 Hàm phân phối tích lũy

Dễ thấy $Z = h_{m,n}(U)$ định nghĩa trong (4.3) chỉ nhận giá trị trên đoạn $[0, 1]$, nên $F_Z(z) = 0$ với $z \leq 0$ và $F_Z(z) = 1$ với $z > 1$. Xét $z \in (0, 1]$, ta có:

$$\begin{aligned}
F_Z(z) &= \mathbb{P}(h(U) \leq z) \\
&= \mathbb{P}(2^m - 1 \leq U) + \mathbb{P}\left(2^{m-n} - 1 < U < 2^m - 1\right) \\
&\quad .\mathbb{P}\left(\frac{m - \log_2(1+U)}{n} \leq z \mid 2^{m-n} - 1 < U < 2^m - 1\right) \\
&= \mathbb{P}(2^m - 1 \leq U) + \mathbb{P}\left(2^{m-nz} - 1 \leq U < 2^m - 1\right) \\
&= 1 - F_U(2^m - 1) + F_U(2^m - 1) - F_U\left(2^{m-nz} - 1\right) \\
&= 1 - F_U\left(2^{m-nz} - 1\right),
\end{aligned}$$

với $F_U(u)$ là hàm phân phối tích lũy của U.

Tóm lại, hàm phân phối tích lũy của biến ngẫu nhiên $Z = h_{m,n}(U)$ có công thức:

$$F_Z(z) = \begin{cases} 1, & \text{nếu} \quad z > 1 \\ 1 - F_U\left(2^{m-nz} - 1\right), & \text{nếu} \quad 0 < z \leq 1 \\ 0, & \text{nếu} \quad z \leq 0. \end{cases} \tag{B.1}$$

B.2 Giá trị kỳ vọng

Do Z chỉ nhận giá trị trên đoạn $[0, 1]$, nên theo [50, định lý 5.3.8, trang 230], kỳ vọng của Z được xác định là:

$$\begin{aligned}\mathbb{E}\{Z\} &= \int_0^\infty \mathbb{P}(Z > z)\, dz \\ &= \int_0^1 \Big(1 - F_Z(z)\Big)\, dz \\ &= \int_0^1 F_U\left(2^{m-nz} - 1\right)\, dz. \end{aligned} \tag{B.2}$$

Đặt $u = 2^{m-nz} - 1$, ta có $du = -n \ln 2\,(u+1)\, dz$, khi đó (B.2) trở thành:

$$\mathbb{E}\{Z\} = \frac{1}{n \ln 2} \int_{2^{m-n}-1}^{2^m-1} \frac{F_U(u)}{u+1}\, du. \tag{B.3}$$

Các phần tiếp theo xác định kỳ vọng của Z ứng với biến ngẫu nhiên U có phân phối khác nhau.

B.2.1 Phụ thuộc vào biến ngẫu nhiên có phân phối mũ

Khi U là biến ngẫu nhiên có phân phối mũ với kỳ vọng Ω_U, ta có:

$$F_U(u) = 1 - \exp\left(-\frac{u}{\Omega_U}\right). \tag{B.4}$$

Thay (B.4) vào (B.3), ta được:

$$\begin{aligned}\mathbb{E}\{Z\} &= \frac{1}{n \ln 2} \int_{2^{m-n}-1}^{2^m-1} \frac{1 - \exp\left(-\frac{u}{\Omega_U}\right)}{u+1}\, du \\ &= \frac{1}{n \ln 2} \int_{2^{m-n}-1}^{2^m-1} \frac{1 - \exp\left(-\frac{u}{\Omega_U}\right)}{u+1}\, du \\ &= \frac{1}{n \ln 2} \left[\ln(u+1) - \exp\left(\frac{1}{\Omega_U}\right) \mathrm{Ei}\left(-\frac{u+1}{\Omega_U}\right)\right]_{u\,=\,2^{m-n}-1}^{u\,=\,2^m-1} \\ &= 1 - \frac{1}{n \ln 2} \exp\left(\frac{1}{\Omega_U}\right) \left[\mathrm{Ei}\left(-\frac{2^m}{\Omega_U}\right) - \mathrm{Ei}\left(-\frac{2^{m-n}}{\Omega_U}\right)\right]. \end{aligned} \tag{B.5}$$

B.2.2 Phụ thuộc vào hai biến ngẫu nhiên độc lập có phân phối mũ

Khi U là biến ngẫu nhiên được định nghĩa trong (4.1), ta có:

$$F_U(u) = 1 - \frac{1}{\frac{b\Omega_Y}{a\Omega_X} u + 1} \exp\left(-\frac{uc}{a\Omega_X}\right). \tag{B.6}$$

Để đơn giản, đặt $k = \frac{c}{a\Omega_X}$ và $l = \frac{b\Omega_Y}{a\Omega_X}$, khi đó, (B.6) thành:

$$F_U(u) = 1 - \frac{\exp(-ku)}{lu+1}. \tag{B.7}$$

Thay (B.7) vào (B.3), ta được:

$$\mathbb{E}\{Z\} = \frac{1}{n\ln 2}\int_{2^{m-n}-1}^{2^m-1}\left[\frac{1}{u+1} - \frac{\exp(-ku)}{(lu+1)(u+1)}\right]du. \tag{B.8}$$

Trong trường hợp $l \neq 1$, ta có thể biến đổi (B.8) thành:

$$\begin{aligned}
\mathbb{E}\{Z\} &= \frac{1}{n\ln 2}\int_{2^{m-n}-1}^{2^m-1}\left[\frac{1}{u+1} - \frac{1}{l-1}\left(\frac{\exp(-ku)}{u+1/l} - \frac{\exp(-ku)}{u+1}\right)\right]du \\
&= \frac{1}{n\ln 2}\left[\ln(u+1) - \frac{\exp(k/l)}{l-1}\mathrm{Ei}(-ku-k/l) + \frac{\exp(k)}{l-1}\mathrm{Ei}(-ku-k)\right]_{u=2^{m-n}-1}^{u=2^m-1} \\
&= 1 - \frac{\exp(k/l)}{n(l-1)\ln 2}\left[\mathrm{Ei}\left(-k2^m + k - \frac{k}{l}\right) - \mathrm{Ei}\left(-k2^{m-n} + k - \frac{k}{l}\right)\right] + \\
&\quad + \frac{\exp(k)}{n(l-1)\ln 2}\left[\mathrm{Ei}(-k2^m) - \mathrm{Ei}\left(-k2^{m-n}\right)\right].
\end{aligned} \tag{B.9}$$

Trong trường hợp $l = 1$, dễ dàng chứng minh kết quả sau:

$$\begin{aligned}
\mathbb{E}\{Z\} &= \frac{1}{n\ln 2}\int_{2^{m-n}-1}^{2^m-1}\left[\frac{1}{u+1} - \frac{\exp(-ku)}{(u+1)^2}\right]du \\
&= 1 + \frac{1}{n\ln 2}\left[\frac{\exp(-k2^m + k)}{2^m} - \frac{\exp\left(-k2^{m-n} + k\right)}{2^{m-n}}\right] + \\
&\quad + \frac{k\exp(k)}{n\ln 2}\left[\mathrm{Ei}(-k2^m) - \mathrm{Ei}\left(-k2^{m-n}\right)\right].
\end{aligned} \tag{B.10}$$

C. Phân tích xác suất truyền tin

Chương 4 đã phát biểu các công thức cho xác suất truyền tin tại PU và SU trong trường hợp hợp tác, cụ thể:

$$p_{tx}^{(P)} = \frac{p_P \Omega_{pp}}{p_S \Omega_{sp} \gamma_b^{(P)} + p_P \Omega_{pp}} \exp\left(-\frac{\gamma_b^{(P)} N_P}{p_P \Omega_{pp}}\right), \tag{C.1a}$$

$$p_{tx}^{(S)} = \frac{p_S \Omega_{ss}}{p_P \Omega_{ps} \gamma_b^{(S)} + p_S \Omega_{ss}} \exp\left(-\frac{\gamma_b^{(S)} N_S}{p_S \Omega_{ss}}\right). \tag{C.1b}$$

Phần này thực hiện khảo sát các công thức trên, từ đó xác định dải giá trị cho các tham số tùy chỉnh $\sigma^{(P)}$ và $\sigma^{(S)}$ trong bài toán tối ưu đề xuất trong Chương 3.

C.1 Giá trị lớn nhất của xác suất truyền tin

Trong các công thức xác suất truyền tin của PU và SU, các công suất phát p_P và p_S là các biến có thể thay đổi và các tham số còn lại là xác định trước đối với một điều kiện truyền tin cụ thể. Do đó, ta đi khảo sát hàm hai biến sau:

$$p\left(x, y; a, b\right) = \frac{x}{ay + x} \exp\left(-\frac{b}{x}\right), \tag{C.2}$$

với a, b là các hằng số dương, x, y là các biến thực, $x > 0, y \geq 0$. Khi đó, các đạo hàm riêng của p có công thức như sau:

$$\frac{\partial p}{\partial x} = \frac{\exp\left(-\frac{b}{x}\right)}{\left(ay + x\right)^2} \left(ay + b + ab\frac{y}{x}\right), \tag{C.3a}$$

$$\frac{\partial p}{\partial y} = \frac{\exp\left(-\frac{b}{x}\right)}{\left(ay + x\right)^2} \left(-a\right). \tag{C.3b}$$

Do a, b, x đều dương và $y \geq 0$ nên $\partial p/\partial x > 0$ và $\partial p/\partial y < 0$. Điều đó cho thấy p là hàm đồng biến theo x và nghịch biến theo y. Như vậy, giá trị lớn nhất của p đạt được khi $y = 0$ và x nhận giá trị lớn nhất, $x = x_{max}$, giá trị của p khi đó là:

$$\max_{x,y} \{p\} = \exp\left(-\frac{b}{x_{max}}\right).$$

Khi x không bị chặn trên, dễ thấy, $\max_{x,y} \{p\} = 1$.

Các công thức xác suất truyền tin (C.1a) và (C.1b) có thể được viết lại theo hàm

p định nghĩa trong (C.1) thành:

$$p_{tx}^{(P)} = p\left(p_P, p_S; \frac{\gamma_b^{(P)}\Omega_{sp}}{\Omega_{pp}}, \frac{\gamma_b^{(P)}N_P}{\Omega_{pp}}\right), \tag{C.4a}$$

$$p_{tx}^{(S)} = p\left(p_S, p_P; \frac{\gamma_b^{(S)}\Omega_{ps}}{\Omega_{ss}}, \frac{\gamma_b^{(S)}N_S}{\Omega_{ss}}\right). \tag{C.4b}$$

Như vậy, xác suất truyền tin cực đại tại các bên tương ứng là:

$$\max_{p_P,p_S}\left\{p_{tx}^{(P)}\right\} = \exp\left(-\frac{\gamma_b^{(P)}N_P}{p_P^{max}\Omega_{pp}}\right), \tag{C.5a}$$

$$\max_{p_P,p_S}\left\{p_{tx}^{(S)}\right\} = \exp\left(-\frac{\gamma_b^{(S)}N_S}{p_S^{max}\Omega_{ss}}\right). \tag{C.5b}$$

Ngoài ra, từ kết quả khảo sát hàm p, ta thấy $p_{tx}^{(P)}$ tỷ lệ thuận với p_P và tỷ lệ nghịch với p_S, ngược lại $p_{tx}^{(S)}$ tỷ lệ thuận với p_S và tỷ lệ nghịch với p_P. Tức là nếu thay đổi p_P và p_S để tăng giá trị $p_{tx}^{(P)}$ thì giá trị $p_{tx}^{(S)}$ sẽ giảm, cả hai bên không thể cùng đạt được xác suất truyền tin quá cao.

C.2 Điều kiện để các bên đạt được xác suất truyền tin mong muốn

Bài toán thiết kế (3.11), mặc dù do SU giải quyết, nhưng PU lại có quyền ưu tiên hơn trong việc xác định các tham số của mình, đó là $R_b^{(P)}$, $R_s^{(P)}$, p_P^{max} và đặc biệt là $\sigma^{(P)}$. Nếu đề xuất của SU không đảm bảo các yêu cầu đó thì SU không thể được chọn cùng truyền với PU. Do đó, trong bài toán thiết kế của mình, SU không thể tùy ý lựa chọn các tham số. Khi PU xác định trước yêu cầu về xác suất truyền tin tối thiểu $\sigma^{(P)}$, nếu muốn hợp tác cùng truyền với PU, SU chỉ có thể lựa chọn một giá trị $\sigma^{(S)}$ đảm bảo cho tập G khác rỗng, với G được định nghĩa bởi:

$$G = \left\{(p_P, p_S)\,\middle|\, p_{tx}^{(P)} \geq \sigma^{(P)}, p_{tx}^{(S)} \geq \sigma^{(S)}, 0 < p_P \leq p_P^{max}, 0 < p_S \leq p_S^{max}\right\}. \tag{C.6}$$

Tập G đại diện cho các lựa chọn công suất phát của PU và SU đảm bảo cả hai bên cùng đạt được xác suất truyền tin tối thiểu mong muốn, tương ứng là $\sigma^{(P)}$ và $\sigma^{(S)}$. Dễ thấy, tập G cũng chính là tập các giá trị hợp lệ của các biến quyết định trong bài toán tối ưu (3.11). Tập G rỗng đồng nghĩa SU không thể đề xuất bất kỳ chiến lược xác định công suất phát nào tới PU, và hai bên không thể hợp tác. Khi giá trị $p_{tx}^{(S)}$ càng tăng thì $p_{tx}^{(P)}$ càng giảm, từ đó điều kiện $p_{tx}^{(P)} \geq \sigma^{(P)}$ càng khó đạt được. Như vậy, khi SU càng yêu cầu cao về xác suất truyền tin tối thiểu thì lực lượng tập G càng giảm. Do đó, phần này thực hiện tìm giá trị lớn nhất của $\sigma^{(S)}$ đảm bảo tập G khác rỗng, khi $\sigma^{(P)}$ cố định.

Trước hết, từ (C.1), các điều kiện $p_{tx}^{(P)} \geq \sigma^{(P)}$ và $p_{tx}^{(S)} \geq \sigma^{(S)}$ biểu diễn lại theo p_P và p_S như sau:

$$p_S \leq \frac{p_P \Omega_{pp}}{\Omega_{sp} \gamma_b^{(P)}} \left(\frac{1}{\sigma^{(P)}} \exp\left(-\frac{\gamma_b^{(P)} N_P}{p_P \Omega_{pp}} \right) - 1 \right), \tag{C.7a}$$

$$p_P \leq \frac{p_S \Omega_{ss}}{\Omega_{ps} \gamma_b^{(S)}} \left(\frac{1}{\sigma^{(S)}} \exp\left(-\frac{\gamma_b^{(S)} N_S}{p_S \Omega_{ss}} \right) - 1 \right). \tag{C.7b}$$

Từ đó, ta khảo sát hàm $\phi\left(x; a, b, c\right)$ phụ thuộc vào biến x dương và các hằng số thực dương a, b, c và $b \geq 1$ được định nghĩa như sau:

$$\phi\left(x; a, b, c\right) = ax \left(b \exp\left(-\frac{c}{x} \right) - 1 \right). \tag{C.8}$$

Đạo hàm bậc một và bậc hai của ϕ theo biến x có công thức như sau:

$$\phi'\left(x\right) = ab \exp\left(-\frac{c}{x} \right) \left(1 + \frac{c}{x} \right) - a, \tag{C.9a}$$

$$\phi''\left(x\right) = ab \exp\left(-\frac{c}{x} \right) \frac{c^2}{x^3}. \tag{C.9b}$$

Do a, b, c dương nên $\phi''\left(x\right) > 0, \forall x > 0$. Ngoài ra, từ công thức định nghĩa, ta thấy phương trình $\phi\left(x; a, b, c\right) = 0$ có nghiệm dương duy nhất $x^* = c/\ln b$ và $\phi(x) < 0, \forall x < x^*$. Đồng thời, do $\phi''(x) > 0, \forall x > 0$ nên ta có $\phi'(x) \geq \phi'(x^*) > 0, \forall x \geq x^*$. Điều đó cho thấy, ϕ là hàm đồng biến trên khoảng $[x^*, \infty)$, nên ta có $\phi(x) \geq \phi(x^*) = 0, \forall x \geq x^*$. Tóm lại, $\phi(x)$ có ba tính chất quan trọng sau đây: (i) có nghiệm dương duy nhất x^*, (ii) đồng biến trên khoảng $[x^*, \infty)$ và (iii) $\phi(x) \geq 0$ khi và chỉ khi $x \geq x^*$.

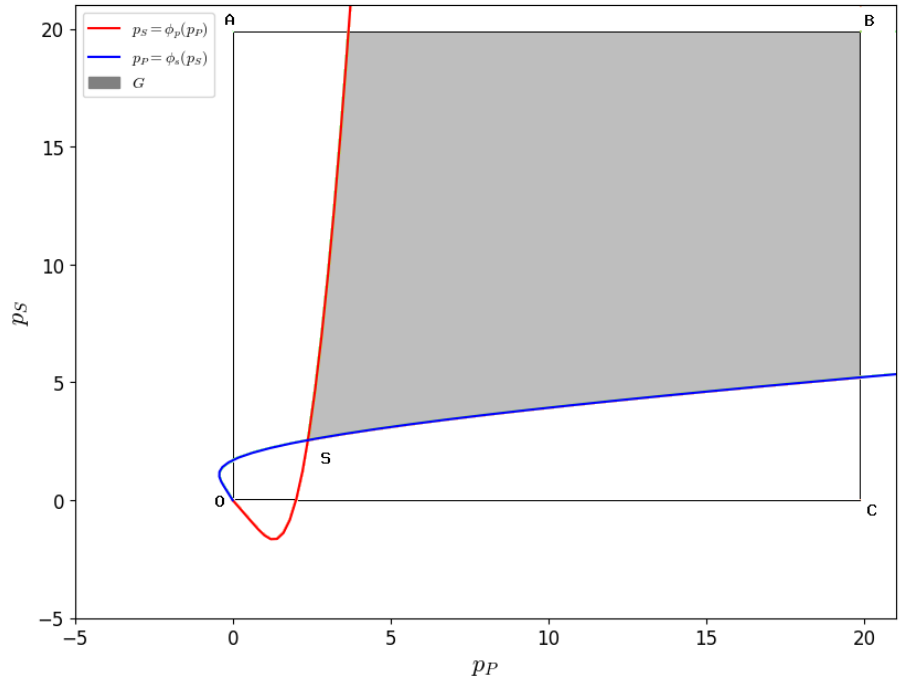
Dựa trên hàm ϕ trong (C.8), các công thức (C.7) trở thành:

$$p_S \leq \phi\left(p_P; \frac{\Omega_{pp}}{\Omega_{sp} \gamma_b^{(P)}}, \frac{1}{\sigma^{(P)}}, \frac{\gamma_b^{(P)} N_P}{\Omega_{pp}} \right) = \phi_p\left(p_P\right), \tag{C.10a}$$

$$p_P \leq \phi\left(p_S; \frac{\Omega_{ss}}{\Omega_{ps} \gamma_b^{(S)}}, \frac{1}{\sigma^{(S)}}, \frac{\gamma_b^{(S)} N_S}{\Omega_{ss}} \right) = \phi_s\left(p_S\right). \tag{C.10b}$$

Từ đó, ta có thể biểu diễn tập G trên hệ trục tọa độ như Hình C.1. Dễ thấy rằng, tập G khác rỗng khi và chỉ khi hai đường cong $p_S = \phi_p\left(p_P\right)$ và $p_P = \phi_s\left(p_S\right)$ cắt nhau tại một điểm S nằm trong hình chữ nhật $OABC$ với tọa độ 4 đỉnh lần lượt là $(0, 0)$, $\left(0, p_S^{max}\right)$, $\left(p_P^{max}, p_S^{max}\right)$ và $\left(p_P^{max}, 0\right)$.

Gọi tọa độ của điểm S là $\left(p_P^*, p_S^*\right)$, tức là ta có $p_S^* = \phi_p\left(p_P^*\right)$ và $p_P^* = \phi_s\left(p_S^*\right)$.



Hình C.1: Tập G (phần bôi đậm) biểu diễn theo p_P và p_S với $p_P^{max} = 20$, $p_S^{max} = 20$

Do $p_P^* > 0$ nên $\phi_s\left(p_S^*\right) > 0$, theo tính chất của hàm ϕ, điều kiện này chỉ xảy ra khi $p_S^* > p_S^z$ với p_S^z là nghiệm của $\phi_s(x) = 0$. Tương tự, ta có $p_P^* > p_P^z$, với p_P^z là nghiệm của $\phi_p(x) = 0$. Đây là các giới hạn dưới cho p_P^* và p_S^*. Đồng thời, ta có p_P^* là nghiệm của phương trình $\Phi_p\left(x\right) = 0$ với:

$$\Phi_p\left(x\right) = \phi_s\left(\phi_p\left(x\right)\right) - x, \tag{C.11}$$

và p_S^* là nghiệm của phương trình $\Phi_s\left(x\right) = 0$ với:

$$\Phi_s\left(x\right) = \phi_p\left(\phi_s\left(x\right)\right) - x. \tag{C.12}$$

Tiếp theo, ta đi khảo sát hàm Φ_p và Φ_s trên các khoảng $\left(p_P^z, p_P^{max}\right]$ và $\left(p_S^z, p_S^{max}\right]$ tương ứng.

Không mất tổng quát, ta đi khảo sát hàm $\Phi \equiv \Phi_p$ trên miền (x_p, ∞), với x_p là nghiệm dương của phương trình $\phi_p(x) = 0$. Đạo hàm cấp một và cấp hai của Φ có công thức sau:

$$\Phi'(x) = \phi_p'(x).\phi_s'(\phi_p(x)) - 1, \tag{C.13a}$$

$$\Phi''(x) = \phi_p''(x).\phi_s'(\phi_p(x)) + \phi_p'(x)^2.\phi_s''(\phi_p(x)). \tag{C.13b}$$

Gọi x_0 là nghiệm của phương trình $\phi_p(x) = x_s$ trên khoảng (x_p, ∞), với x_s là nghiệm dương duy nhất của phương trình $\phi_s(x) = 0$. Dễ thấy, x_0 luôn tồn tại vì

$\phi_p(x)$ nhận giá trị trên khoảng $(0, \infty)$ khi x biến thiên trên (x_p, ∞). Khi đó, ta có $\phi_s(\phi_p(x_0)) = \phi_s(x_p) = 0$. Từ đó, theo tính chất của hàm ϕ, ta dễ dàng chứng minh ba mệnh đề sau:

$$\phi_s(\phi_p(x)) \geq \phi_s(\phi_p(x_0)) = 0, \forall x \geq x_0, \tag{C.14a}$$

$$\phi_s'(\phi_p(x)) \geq 0, \forall x \geq x_0, \tag{C.14b}$$

$$\phi_s(\phi_p(x)) < \phi_s(\phi_p(x_0)) = 0, \forall\ x_p < x < x_0. \tag{C.14c}$$

Theo (C.14c), khi $x_p < x < x_0$, thì $\Phi(x) < 0$, phương trình $\Phi(x) = 0$ không thể có nghiệm trên khoảng (x_p, x_0). Khi $x \geq x_0$, theo (C.14b) và (C.13b), ta có $\Phi''(x) > 0$. Như vậy, Φ là hàm lồi trên khoảng $[x_0, \infty)$. Mà $\Phi(x_0) = -x_0 < 0$, từ đó dễ dàng chứng minh bằng phương pháp phản chứng: (i) phương trình $\Phi(x) = 0$ có nghiệm trên khoảng $(x_0, x_1]$, $x_1 > x_0$ khi và chỉ khi $\Phi(x_1) \geq 0$ và (ii) nghiệm trên miền xác định của phương trình $\Phi(x) = 0$ là duy nhất (nếu có).

Từ kết quả khảo sát hàm Φ, phương trình $\Phi_p(x) = 0$ có nghiệm p_P^* trên khoảng $\left(p_P^z, p_P^{max}\right]$ khi và chỉ khi $\phi_s(\phi_p(p_P^{max})) \geq p_P^{max}$. Tương tự, phương trình $\Phi_s(x) = 0$ có nghiệm p_S^* trên khoảng $\left(p_S^z, p_S^{max}\right]$ khi và chỉ khi $\phi_p(\phi_s(p_S^{max})) \geq p_S^{max}$. Đồng thời, các nghiệm này đều là duy nhất (nếu có). Như vậy, G khác rỗng khi và chỉ khi $\phi_s(\phi_p(p_P^{max})) \geq p_P^{max}$ và $\phi_p(\phi_s(p_S^{max})) \geq p_S^{max}$. Bài toán ban đầu được giải quyết.

TÀI LIỆU THAM KHẢO

[1] Y.-C. Liang, K.-C. Chen, G. Y. Li, and P. Mahonen, "Cognitive radio networking and communications: An overview," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 7, pp. 3386–3407, 2011. DOI: 10.1109/TVT.2011.2158673.

[2] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1878–1911, 2018.

[3] T. Kwon, V. W. Wong, and R. Schober, "Secure miso cognitive radio system with perfect and imperfect csi," in *2012 IEEE global communications conference (GLOBECOM)*, IEEE, 2012, pp. 1236–1241.

[4] J. Ouyang, M. Lin, Y. Zou, W.-P. Zhu, and D. Massicotte, "Secrecy energy efficiency maximization in cognitive radio networks," *IEEE Access*, vol. 5, pp. 2641–2650, 2017.

[5] Y. He, J. Evans, and S. Dey, "Secrecy rate maximization for cooperative overlay cognitive radio networks with artificial noise," in *2014 IEEE International Conference on Communications (ICC)*, IEEE, 2014, pp. 1663–1668.

[6] A. Houjeij, W. Saad, T. Bas, *et al.*, "A game-theoretic view on the physical layer security of cognitive radio networks," in *2013 IEEE International Conference on Communications (ICC)*, IEEE, 2013, pp. 2095–2099.

[7] Y. Zou, X. Li, and Y.-C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 11, pp. 2222–2236, 2014.

[8] T. X. Quach, H. Tran, E. Uhlemann, and M. T. Truc, "Secrecy performance of cognitive cooperative industrial radio networks," in *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, IEEE, 2017, pp. 1–8.

[9] M. Bouabdellah, F. El Bouanani, and H. Ben-Azza, "Secrecy outage probability in cognitive radio networks subject to rayleigh fading channels," in *2018 International Conference on Advanced Communication Technologies and Networking (CommNet)*, IEEE, 2018, pp. 1–5.

[10] Y. Wu and K. R. Liu, "An information secrecy game in cognitive radio networks," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 831–842, 2011.

[11] H. Tran, G. Kaddoum, F. Gagnon, and L. Sibomana, "Cognitive radio network with secrecy and interference constraints," *Physical Communication*, vol. 22, pp. 32–41, 2017.

[12] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[13] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[14] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[15] J. Barros and M. R. Rodrigues, "Secrecy capacity of wireless channels," in *2006 IEEE international symposium on information theory*, IEEE, 2006, pp. 356–360.

[16] P. Mukherjee and S. Ulukus, "Fading wiretap channel with no csi anywhere," in *2013 IEEE International Symposium on Information Theory*, IEEE, 2013, pp. 1347–1351.

[17] Y. Liang, L. Lai, H. V. Poor, and S. Shamai, "A broadcast approach for fading wiretap channels," *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 842–858, 2013.

[18] C. Tang, G. Pan, and T. Li, "Secrecy outage analysis of underlay cognitive radio unit over nakagami-m fading channels," *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 609–612, 2014.

[19] P.-H. Lin and E. Jorswieck, "On the fast fading gaussian wiretap channel with statistical channel state information at the transmitter," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 46–58, 2015.

[20] H. Lei, C. Gao, Y. Guo, and G. Pan, "On physical layer security over generalized gamma fading channels," *IEEE Communications Letters*, vol. 19, no. 7, pp. 1257–1260, 2015.

[21] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE transactions on wireless communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[22] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Communications Letters*, vol. 15, no. 3, pp. 302–304, 2011. DOI: 10.1109/LCOMM.2011.011811.102433.

[23] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7495–7505, 2017.

[24] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE transactions on signal processing*, vol. 58, no. 3, pp. 1875–1888, 2009.

[25] L. Sibomana, H. Tran, and Q. A. Tran, *Impact of secondary user communication on security communication of primary user*, 2014. arXiv: 1408.6986 [cs.CR].

[26] P. Yadav, S. Kumar, and R. Kumar, "A comprehensive survey of physical layer security over fading channels: Classifications, applications, and challenges," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 9, e4270, 2021.

[27] X. Tang, R. Liu, P. Spasojevi'c, and H. V. Poor, "Interference assisted secret communication," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 3153–3167, 2011.

[28] A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten, "Joint power control in wiretap interference channels," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 3810–3823, 2015.

[29] J. Xie and S. Ulukus, "Secure degrees of freedom of K-user gaussian interference channels: A unified view," *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2647–2661, 2015.

[30] L. Li, A. P. Petropulu, Z. Chen, and J. Fang, "Improving wireless physical layer security via exploiting co-channel interference," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1433–1448, 2016. DOI: 10.1109/JSTSP.2016.2600516.

[31] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. M. Leung, "A survey of security challenges in cognitive radio networks: Solutions and future research directions," *Proceedings of the IEEE*, vol. 100, no. 12, pp. 3172–3186, 2012. DOI: 10.1109/JPROC.2012.2208211.

[32] F. Salahdine and N. Kaabouch, "Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey," *Physical Communication*, vol. 39, p. 101 001, 2020.

[33] A. Hyadi, Z. Rezki, and M.-S. Alouini, "An overview of physical layer security in wireless communication systems with csit uncertainty," *IEEE Access*, vol. 4, pp. 6121–6132, 2016.

[34] B. He, X. Zhou, and T. D. Abhayapala, "Wireless physical layer security with imperfect channel state information: A survey," *arXiv preprint arXiv:1307.4146*, 2013.

[35] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1923–1936, 2013.

[36] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[37] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the ergodic secrecy capacity of the wiretap channel under imperfect main channel estimation," in *2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, IEEE, 2011, pp. 952–957.

[38] B. He, X. Zhou, and A. L. Swindlehurst, "On secrecy metrics for physical layer security over quasi-static fading channels," *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6913–6924, 2016.

[39] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2170–2181, 2013.

[40] H. Alves, M. D. C. Tomé, P. H. J. Nardelli, C. H. De Lima, and M. Latva-Aho, "Enhanced transmit antenna selection scheme for secure throughput maximization without csi at the transmitter," *IEEE Access*, vol. 4, pp. 4861–4873, 2016.

[41] P. Parada and R. Blahut, "Secrecy capacity of simo and slow fading channels," in *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, IEEE, 2005, pp. 2152–2155.

[42] M. J. Kochenderfer and T. A. Wheeler, *Algorithms for Optimization*. The MIT Press, 2019, ISBN: 0262039427.

[43] S. P. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[44] R. Storn and K. Price, "Differential evolution–a simple and efficient heuristic for global optimization over continuous spaces," *Journal of global optimization*, vol. 11, pp. 341–359, 1997.

[45] Y. Collette and P. Siarry, *Multiobjective Optimization: Principles and Case Studies* (Decision Engineering). Springer Berlin Heidelberg, 2004, ISBN: 9783540401827. [Online]. Available: `https://books.google.com.vn/books?id=XNYF4hltoF0C`.

[46] K. Miettinen, *Nonlinear multiobjective optimization*. Boston, USA: Kluwer, 1999.

[47] Y. Zou, J. Zhu, B. Zheng, and Y.-D. Yao, "An adaptive cooperation diversity scheme with best-relay selection in cognitive radio networks," *IEEE transactions on signal processing*, vol. 58, no. 10, pp. 5438–5445, 2010.

[48] W. Su, J. D. Matyjas, and S. Batalama, "Active cooperation between primary users and cognitive radio users in heterogeneous ad-hoc networks," *IEEE Transactions on Signal Processing*, vol. 60, no. 4, pp. 1796–1805, 2012.

[49] Y. Huang, W. Wang, B. He, L. Sun, and T. Jiang, "On secure transmission design: An information leakage perspective," in *2018 IEEE Global Communications Conference (GLOBECOM)*, IEEE, 2018, pp. 1–6.

[50] J. Blitzstein and J. Hwang, *Introduction to Probability* (Chapman and Hall/CRC Texts in Statistical Science Series). CRC Press, Taylor & Francis Group, 2019, ISBN: 9781138369917. [Online]. Available: `https://books.google.com.vn/books?id=pcPAuQEACAAJ`.