BỘ GIÁO DỤC VÀ ĐÀO TẠO

ĐẠI HỌC THÁI NGUYÊN

BÁO CÁO TỔNG KẾT

ĐỀ TÀI KHOA HỌC VÀ CÔNG NGHỆ CẤP BỘ

NGHIÊN CỨU KHẢ NĂNG BẢO MẬT THÔNG TIN TẠI TẦNG VẬT LÝ VÀ ĐÁNH GIÁ HIỆU QUẢ HOẠT ĐỘNG CỦA MẠNG KHÔNG DÂY DỰA TRÊN CÁC RÀNG BUỘC NHIỄU VÀ KHẢ NĂNG TRUYỀN/NHẬN NĂNG LƯỢNG KHÔNG DÂY

Mã số: B2017-TNA-50

Xác nhận của tổ chức chủ trì **Chủ nhiệm đề tài**

THÁI NGUYÊN, 07/2019

MỤC LỤC

Danh sách hình vẽ

CÁC TỪ VIẾT TẮT

Từ viết tắt	Từ gốc	Dịch nghĩa
P-Tx	Primary transmitter	Máy phát sơ cấp
P-Rx	Primary receiver	Máy thu sơ cấp
S-Tx	Secondary transmitter	Máy phát thứ cấp
S-Rx	Secondary receiver	Máy thu thứ cấp
AF	Amplify-and-forward	Khuếch đại và chuyển tiếp
APD	Average packet delay	Độ trễ gói tin trung bình
CDF	Cumulative distribution function	Hàm phân bố xác suất tích lũy
CRN	Cognitive radio network	Mạng vô tuyến nhận thức
CCRN	Cognitive cooperative radio network	Mạng vô tuyến nhận thức hợp tác
CSI	Channel state information	Thông tin trạng thái kênh
DC	Direct Current	Một chiều
DF	Decode-and-forward	Giải mã và chuyển tiếp
DMC	Discrete memoryless channel	Kênh rời rạc không nhớ
EAV	Eaversdropper	Người nghe trộm
IoT	Internet of things	Internet vạn vật
LDPC	Low-density parity check	
MIMO	Multi-input Multi-output	Đa đầu vào - Đa đầu ra
MISO	Multi-input Single-output	Đa đầu vào - Đơn đầu ra
PDF	Probability density function	Hàm mật độ sác suất
PEP	Packet error probability	Xác suất lỗi gói tin
PU	Primary user	Người dùng sơ cấp
RF	Radio Frequency	Tần số vô tuyến
RFEH	Radio Frequency Energy Harvesting	Thu hoạch năng lượng vô tuyến
RV	Random variable	Biến ngẫu nhiên

Từ viết tắt	Từ gốc	Dịch nghĩa
RSS	Received signal strength	Cường độ tín hiệu thu được
SC	Selection combining	Lựa chọn kết hợp
SU	Secondary user	Người dùng thứ cấp
SIMO	Single-input multiple-output	Đơn đầu vào - Đa đầu ra
SRCP	Secure and reliable communication probability	Truyền thông tin cậy và bảo mật
SNR	Signal-to-noise radio	Tỉ lệ tín hiệu trên nhiễu
SINR	Signal-to-interference-plus-noise ratio	Tỉ lệ tín hiệu trên nhiễu cộng
SIMOME	Single-input multiple-output multiple-eavesdropper	Đơn đầu vào, đa đầu ra, đa nghe trộm
MISOME	Multiple-input single-output multiple-eavesdropper	Đa đầu vào, đơn đầu ra, đa nghe trộm
SISOSE	Single-input single-output single-eavesdropper	Đơn đầu vào, đơn đầu ra, đơn nghe trộm

THÔNG TIN KẾT QUẢ NGHIÊN CỨU

1. Thông tin chung

- Tên đề tài: Nghiên cứu khả năng bảo mật thông tin tại tầng vật lý và đánh giá hiệu quả của hoạt động của mạng không dây dựa trên các ràng buộc nhiễu và khả năng truyền/nhận năng lượng không dây.
- Mã số: B2017-TNA-50
- Chủ nhiệm đề tài: ThS. Quách Xuân Trưởng
- Tổ chức chủ trì: Đại học Thái Nguyên
- Thời gian thực hiện: 24 tháng

2. Mục tiêu

Nghiên cứu hiệu năng bảo mật mô hình mạng vô tuyến nhận thức tại tầng vật lý. Trên cơ sở các mô hình mạng được khảo sát, chúng tôi sẽ nghiên cứu đánh giá hiệu năng hoạt động và khả năng bảo mật thông tin tại tầng vật lí dưới sự tác động của các điều kiện ràng buộc cho trước. Đề tài giải quyết hai vấn đề chính sau đây: Một là đề xuất các chính sách điều khiển công suất cho thiết bị không dây nhằm hạn chế khả năng bị nghe trộm hoặc rỏ rỉ thông tin. Hai là đánh giá thời gian truyền các gói tin và xác suất gói tin truyền bị lỗi của thiết bị không dây sử dụng kỹ thuật thu hoạch năng lượng vô tuyến trong môi trường bị gây nhiễu hoặc bị ràng buộc bởi các chính sách an toàn thông tin.

3. Tính mới và sáng tạo

Trong những năm gần đây, sự phát triển nhanh chóng của lĩnh vực công nghệ mạng không dây dẫn đến công nghệ ngày càng phổ biến. Tuy nhiên, bên cạnh tiềm năng phát triển thì mạng không dây mang lại những thách thức lớn

cho việc đảm bảo truyền thông tin cậy và bảo mật thông tin. Hiện nay, bảo mật lớp vật lý trong mạng không dây đang là lĩnh vực thu hút được sự quan tâm nghiên cứu của các nhà nghiên cứu trên khắp thế giới. Do có độ phức tạp và độ trễ thấp, cũng như tính khả thi ở lớp vật lý và khả năng cùng tồn tại song song với các cơ chế bảo mật mã hóa hiện có ở các lớp trên, bảo mật lớp vật lý có khả năng cho phép truyền thông an toàn và giảm thiểu sự phức tạp tính toán, đặc biệt có hiệu quả đối với thiết bị mạng không dây có tài nguyên hạn chế như trong IoT. Vì vậy, nó có thể nâng cao mức độ tổng thể về sự tin cậy và an toàn thông tin cho hệ thống.

Mặc dù đã có khá nhiều các công trình nghiên cứu với cách tiếp cận khác nhau, song truyền thông bảo mật và tin cậy vẫn đang là một vấn đề mở. Với sự phổ biến và phát triển không ngừng của công nghệ mạng không dây, vấn đề bảo mật trong truyền thông sẽ có nhiều thách thức hơn nữa trong tương lai, làm cho chủ đề này trở thành một trong những lĩnh vực nghiên cứu quan trọng và liên tục. Bảo mật lớp vật lý có thể đóng góp cho truyền thông an toàn tổng thể bằng nhiều cách. Ý tưởng cơ bản của đề tài nghiên cứu này là khai thác các đặc tính của kênh không dây và tính chất ngẫu nhiên của tín hiệu trong môi trường fading để hạn chế lượng thông tin mà các phần tử nghe trộm có thể thu thập và giải mã được.

4. Kết quả nghiên cứu.

- Nghiên cứu khảo sát khả năng bảo mật thông tin ở tầng vật lý trong mạng không dây.
- Nghiên cứu tổng quát về đánh giá hiệu năng mạng cho mạng không dây trong môi trường kênh truyền fading.
- Nghiên cứu về mô hình mạng vô tuyến nhận thức và lợi ích của nó trong mạng không dây thế hệ mới.
- Nghiên cứu các kỹ thuật truyền thông hợp tác và ứng dụng trong mô hình mạng vô tuyến nhận thức.
- Nghiên cứu kỹ thuật thu hoạch năng lượng vô tuyến và ứng dụng trong mô hình mạng vô tuyến nhận thức.

- Nghiên cứu các phương pháp nhằm cải thiện khả năng bảo mật thông tin ở tầng vật lý đối với mô hình mạng vô tuyến nhận thức.
- Nghiên cứu, xây dựng phương pháp đánh giá độ tin cậy và bảo mật thông tin cho mạng vô tuyến nhận thức trong môi trường kênh truyền fading.
- Nghiên cứu đánh giá hiệu suất bảo mật trong mạng vô tuyến nhận thức khi áp dụng kỹ thuật truyền thông hợp tác để tăng cường QoS và bảo mật thông tin.
- Nghiên cứu phương pháp tối ưu hóa thời gian thu hoạch năng lượng và lựa chọn kênh cho mô hình mạng vô tuyến nhận thức thu hoạch năng lượng vô tuyến đảm bảo hiệu năng hoạt động và bảo mật thông tin.
- Nghiên cứu mô hình hóa toán học, xây dựng các chính sách điều khiển công suất cho các mô hình mạng được đề xuất dưới các điều kiện ràng buộc về can nhiễu và bảo mật thông tin.
- Thực hiện mô phỏng kiểm nghiệm tính chính xác của các công thức tìm được trong các chính sách điều khiển công suất cho các mô hình hệ thống nghiên cứu.
- Đánh giá và rút ra được các kết luận về mối liên hệ giữa những ràng buộc về can nhiễu, bảo mật thông tin, thu hoạch năng lượng không dây, tác động qua lại của các tham số hệ thống lên hiệu năng hoạt động của hệ thống và đề xuất các giải pháp nhằm cải thiện hiệu năng và an toàn cho hệ thống.
- Tổng hợp kết quả nghiên cứu để công bố công trình nghiên cứu trên các tạp chí và hội thảo quốc tế chuyên ngành.
- Nâng cao chất lượng trong hỗ trợ và đào tạo thạc sĩ, tiến sĩ ngành CNTT với các công trình nghiên cứu có chất lượng.

5. Sản phẩm.

Bài báo công bố tên tạp chí khoa học quốc tế thuộc danh mục ISI : 01 bài báo.

- Truong Xuan Quach, Hung Tran, Elisabeth Uleman, G.Kaddoum, and T.Q.Anh (2017), "Power allocation policy and performance analysis of secure and reliable communication in cognitive radio networks", Wireless Networks, https://doi.org/10.1007/s11276-017-1605-z.

Bài báo trên kỷ yếu hội thảo quốc tế: 02 bài báo.

- Truong Xuan Quach, Hung Tran, Elisabeth Uleman, Mai Tran Truc (2017), "Secrecy performance of cognitive cooperative industrial radio networks", 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1-8.

- Hung Tran, Truong Xuan Quach, Elisabeth Uleman, Ha-Vu Tran (2017), "Optimal energy harvesting time and power allocation policy in CRN under security constraints from eavesdroppers", 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1-8.

Thạc sĩ bảo vệ thành công luận văn tốt nghiệp: 01 thạc sĩ.

- Phạm lê Tiệp, Đề tài luận văn "Đánh giá khả năng bảo mật ở tầng vật lý trong mạng không dây", Thạc sĩ chuyên ngành Khoa học máy tính, Khoá 2015-2017, Trường Đại học Công nghệ Thông tin và Truyền thông. Đại học Thái Nguyên.

Hỗ trợ nghiên cứu sinh công bố công trình khoa học: 01 NCS

- NCS Quách Xuân Trưởng, Đề tài luận án "đánh giá hiệu năng bảo mật tầng vật lý trong mạng không dây". Ngành Công nghệ thông tin, trường đại học Công nghệ, đại học quốc gia Hà Nội.

6. Phương thức chuyển giao, địa chỉ ứng dụng, tác động và lợi ích mang lại của kết quả nghiên cứu.

6.1. Phương thức chuyển giao.

Sau khi đề tài được nghiên cứu thành công sẽ được chuyển giao cho đại học Thái Nguyên, góp phần bổ sung kết quả/tài liệu nghiên cứu khoa học trong các hướng tiếp cận mới trên thế giới trong lĩnh vực mạng truyền thông không dây. Kết quả nghiên cứu có thể được sử dụng tham khảo trong học tập, nghiên cứu và giảng dạy trong lĩnh vực mạng máy tính và truyền thông và đào tạo cán bộ chuyên ngành mạng và truyền thông, an toàn thông tin.

6.2. Địa chỉ ứng dụng.

Kết quả của đề tài được sử dụng/tham khảo tại Đại học Thái Nguyên.

6.3. Tác động và lợi ích mang lại đối với lĩnh vực giáo dục và đào tạo.

Nội dung nghiên cứu góp phần bổ sung kết quả/tài liệu nghiên cứu khoa học trong các hướng tiếp cận mới trên thế giới trong lĩnh vực mạng truyền thông không dây. Kết quả nghiên cứu có thể được sử dụng tham khảo trong học tập, nghiên cứu và giảng dạy trong lĩnh vực mạng máy tính và truyền thông.

Góp phần nâng cao chất lượng đào tạo trình độ cao chuyên ngành mạng máy tính và truyền thông

6.4. Tác động và lợi ích mang lại đối với lĩnh vực khoa học và công nghệ có liên quan.

Đề tài đóng góp giải quyết một số thách thức và khó khăn trong việc hiện thực hóa hệ thống mạng vô tuyến nhận thức cùng khả năng truyền/nhận năng lượng không dây vào ứng dụng trong đời sống thực tiễn.

Góp phần nâng cao khả năng giải quyết những vấn đề khoa học công nghệ trong lĩnh vực mạng máy tính và truyền thông, an toàn và bảo mật thông tin.

6.5. Tác động và lợi ích mang lại đối với phát triển kinh tế-xã hội.

Vài thập niên trở lại đây, mạng truyền thông không dây phát triển nhan chóng đã gây ra nhiều ảnh hưởng to lớn đến mọi lĩnh vực trong đời sống xã hội (như công nghiệp, y tế, giáo dục, an ninh quốc phòng, kinh tế, tài nguyên môi trường ...). Điều này dẫn đến nhu cầu cần thiết phải tối ưu hóa các dải tần số vô tuyến và khắc phục hạn chế về khả năng sử dụng năng lượng. Bên cạnh đó việc bảo mật thông tin trong mạng không dây trở thành một vấn đề

nóng cần được quan tâm, đặc biệt trong các lĩnh vực tài chính, ngân hàng, an ninh quốc phòng. Kết quả đóng góp của đề tài sẽ góp phần vào giải quyết các thách thức và khó khăn trong việc hiện thực hóa hệ thống mạng vô tuyến nhận thức cùng kỹ thuật thu hoạch năng lượng vô tuyến vào ứng dụng trong đời sống xã hội, làm cho cuộc sống chúng ta có thể trở nên thoái mái, tiện nghi, và an toàn trong liên lạc không dây.

6.6. Tác động và lợi ích mang lại đối với tổ chức chủ trì và các cơ sở ứng dụng kết quả nghiên cứu.

Đào tạo đội ngũ cán bộ khoa học cho trường đại học Công nghệ thông tin và Truyền thông, Đại học Thái Nguyên trong lĩnh vực công nghệ thông tin và an toàn bảo mật thông tin, góp phần nâng cao năng lực của trường đại học Công nghệ thông tin và truyền thông nói riêng và Đại học Thái nguyên nói chung.

Đối với cá nhân, cơ sở ứng dụng: Các kết quả tính toán và mô hình đề xuất mang tính khoa học làm căn cứ trong quá trình nghiên cứu, phát triển, thử nghiệm trong nghiên cứu khoa học và ứng dụng trong lĩnh vực công nghệ thông tin và an toàn bảo mật thông tin.

Ngày ..... tháng ..... năm 2019

Tổ chức chủ trì **Chủ nhiệm đề tài**

Quách Xuân Trưởng

INFORMATION ON RESEARCH RESULTS

1. General information

- Project title: Performance Evaluation of Physical Layer Security of Wireless Network based on Interference and Energy Harvesting Constraints.
- Code number: B2017-TNA-50
- Coordinator: MSc Quach Xuan Truong
- Implementing institution: Thai Nguyen University
- Duration: from 01/03/2017 to 01/03/2019 (24 month)

In this project, we study the security performance of cognitive radio network models at the physical layer. Given interference and energy harvesting constraints, we focus on two major issues: Firstly, propose power control policies to reduce the risk of overhearing by eavesdroppers. Secondly, evaluate the transmission time of packets and the symbol error probability of wireless devices using the RF energy harvesting technology under joined constraints of interference and security policies.

In recent years, wireless networking becomes the vital part of daily life. However, the new generation wireless networks are facing many challenges such as security and reliability in communication. Recently, physical layer security in wireless networks has been emerged as a hot research topic and attract a lot of attention of researchers around the world. Because it is considered powerful solution with a low complexity and latency, feasibility, and the ability to coexist with traditional encryption security mechanisms in the upper layers. Obtained research results have proved that physical layer security

can minimize computational complexity, especially effective for wireless network devices that have limited resources like in IoT. Therefore, it can enhance the overall level of reliability and information security for the system.

Although there have been many research with different approaches to physical layer security, secure and reliable communication is still an open problem. With the popularity and continued development of wireless networking technology, the security issue in wireless communication will be more challenging in the future, making this topic one of the continuous and important research areas. The basic idea of this project is to exploit the characteristics of the wireless channel and the random nature of the signal in the fading channel to limit the amount of information that eavesdroppers can collect and decode.

2. Research results

- An overview of physical layer security in wireless communication.
- An overview of evaluation performance network for wireless networks in fading channel environment.
- Research on the concept of the cognitive radio network and its benefits in the new generation wireless network.
- Research cooperative communication techniques and applications in cognitive radio network models.
- Research radio frequency energy harvesting techniques and applications in cognitive radio network models.
- Research methods to improve physical layer security for cognitive radio network models.
- Research methods to analyze the secure and reliable communication for cognitive radio networks in fading channels.

- Research on evaluating security performance in CCRN when applying collaborative communication techniques to enhance QoS and information security.
- Researching methods to optimize energy harvesting time and selecting channels for the energy harvesting cognitive radio network to ensure performance system and information security.
- Math modeling, proposed power allocation policies for proposed network models under the interference and security constraints.
- Simulation examines the accuracy of formulas obtained in power allocation policies for research system models.
- Evaluation and conclusions about the relationship between interference, security, and RF energy harvesting constraints. Consider the interactions of system parameters on the performance system and propose solutions to improve the security and performance system.
- Summary of research results to publish research works in international journals and conferences.
- Improving the quality of support and training of masters and Ph.D. in IT with quality research works.

5. Products.

Scientific products : 03 papers.

- Truong Xuan Quach, Hung Tran, Elisabeth Uleman, G.Kaddoum, and T.Q.Anh (2017), "Power allocation policy and performance analysis of secure and reliable communication in cognitive radio networks", Wireless Networks, https://doi.org/10.1007/s11276-017-1605-z.
- Truong Xuan Quach, Hung Tran, Elisabeth Uleman, Mai Tran Truc (2017), "Secrecy performance of cognitive cooperative industrial radio networks", 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1-8.

- Hung Tran, Truong Xuan Quach, Elisabeth Uleman, Ha-Vu Tran (2017), "Optimal energy harvesting time and power allocation policy in CRN under security constraints from eavesdroppers", 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1-8.

Training products: 01.

- Phạm Lê Tiệp (2017), "Evaluate physical layer security in wireless networks", Master thesis in computer science, University of Information And Communication Technology, Thai Nguyen University.

PhD co-adviser : 01 PhD

- PhD candidate Quach Xuan Truong, "Secrecy performance of wireless communications at the physical layer", PhD thesis in Information Technology, VNU University of Engineering and Technology.

6. Transfer alternatives, application institutions, impacts and benefits of research results.

Regarding transfer method and application address: After successfully research, the project will be transferred to Thai Nguyen university to supplement scientific research documents in new approaches in the field of wireless communication networks in the world. Research results can be used for reference in learning, research, and teaching in the field of computer networks and communication.

Regarding the impact and benefits of research: The project contributes to solving some challenges and difficulties in the field of computer networks and communication, information security. Research results can be used for reference in learning, research and teaching in universities and research institutes.

Chương 1

CÁC VẤN ĐỀ TỔNG QUAN

1.1 Tổng quan về bảo mật thông tin tại lớp vật lý trong mạng không dây

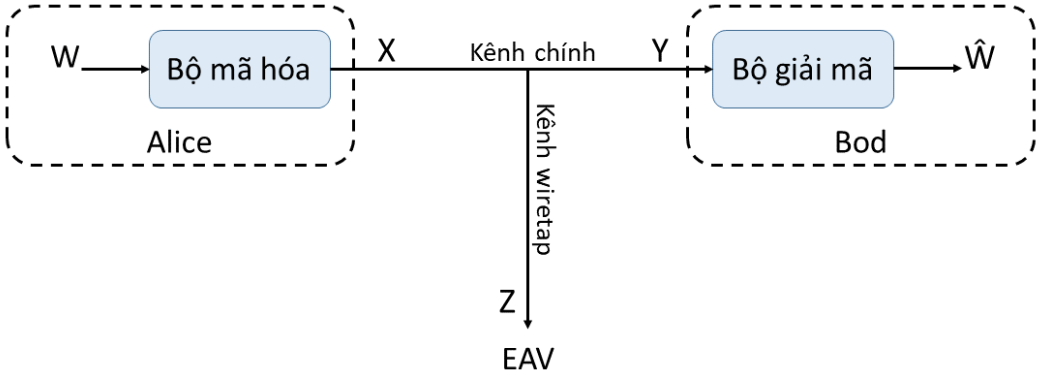
Mạng không dây luôn phải đối mặt với nhiều thách thức do đặc điểm vật lý tự nhiên của kênh truyền. Với bản chất quảng bá tự nhiên của kênh truyền vô tuyến, truyền thông không dây dễ dàng bị tấn công nghe trộm do người dùng bất kỳ trong vùng phủ sóng của máy phát đều có khả năng thu và giải mã thông tin. Ngoài ra, các vấn đề bảo mật khác phát sinh từ những khiếm khuyết của môi trường truyền dẫn tín hiệu như fading đa đường, path-loss, nhiễu. Kết quả là người dùng bất hợp pháp có thể có thể trích xuất thông tin truyền thông hoặc có thể gây suy giảm hoặc gián đoạn hoạt động truyền thông của hệ thống [58]. Các giải pháp giải quyết vấn đề an ninh trong mạng không dây theo cách tiếp cận truyền thống là sử dụng các kỹ thuật mã hóa để ngăn chặn kẻ truy cập bất hợp pháp thông tin [27, 35]. Phương thức mã hóa này dựa trên độ phức tạp tính toán cao, được sử dụng ở các lớp trên độc lập với lớp vật lý và luôn mặc định kết nối vật lý là hoàn hảo và không lỗi. Gần đây, bảo mật lớp vật lý đã được bổ sung để nâng cao tính bảo mật thông tin và chống lại các cuộc tấn công nghe trộm trong các mạng không dây. Ý tưởng của cách tiếp cận bảo mật trong lớp vật lý cho mạng không dây là dựa vào nguyên lý cơ bản của bảo mật dựa trên lý thuyết thông tin được giới thiệu bởi Shannon [76], người đã đề xuất ra khái niệm bảo mật tuyệt đối. Tiếp theo đó, Wyner đã đưa ra mô hình kênh wiretap và chứng minh được rằng việc truyền tải thông tin có thể đạt được bảo mật hoàn hảo nếu dung lượng kênh hợp pháp lớn hơn dung lượng kênh nghe trộm, mà không cần phải mã hóa

dữ liệu. Mô hình kênh wiretap rời rạc không nhớ của Wyner được xem là nền tảng cho các nghiên cứu bảo mật thông tin tại lớp vật lý [90].

Với tính chất quảng bá mở cùng với các đặc tính vật lý tự nhiên trong kênh truyền không dây như fading đa đường, nhiễu và path-loss đã đặt ra nhiều thách thức, nhưng cũng cho phép khả năng khai thác tính chất này trong vấn đề truyền thông bảo mật trong mạng không dây, Các nhà nghiên cứu đã phát triển, mở rộng nghiên cứu do Wyner khởi xướng cho kênh Gaussian [42] và một số kênh fading trong thực tế [8,43,73,74].

1.1.1 Giới thiệu về kênh wiretap

Như đã trình bày ở trên, khái niệm kênh wiretap được giới thiệu bởi Wyner [90] với giả thiết rằng kênh EAV là một phiên bản tín hiệu suy thoái của kênh chính. Wyner đã chứng minh được rằng tồn tại một tốc độ truyền tin lớn hơn không với khả năng bí mật hoàn hảo nếu kênh EAV bị nhiễu hơn kênh chính. Ý tưởng này của Wyner là có thể khai thác nhiễu trong kênh truyền thông cùng với mã hóa mức tín hiệu thích hợp để đảm bảo truyền thông an toàn.



Hình 1.1: *Mô hình kênh wiretap tổng quát*

Hình 1.1 mô tả mô hình kênh wiretap tổng quát trong đó Alice gửi bản tin bí mật tới Bob thông qua một kênh không nhớ rời rạc (DMC). Trong khi đó, EAV cố gắng nghe trộm bản tin này thông qua một phiên bản suy thoái khác của kênh DMC. Alice mã hóa thông tin W thành từ mã X có độ dài n và truyền qua kênh truyền, Bob nhận được tín hiệu Y và giải mã là $\hat{W}$. Tín hiệu

EAV thu được qua kênh wiretap được biểu diễn là Z. Mục tiêu là thiết kế một lược đồ mã hóa/giải mã để có thể truyền thông tin cậy và an toàn. Hiệu suất của lược đồ mã hóa/giải mã được đo bằng xác suất lỗi trung bình và tỉ lệ mập mờ (equivocation rate) [4, 68]. Trong đó, xác xuất lỗi trung bình cho biết mức độ truyền thông tin cậy giữa Alice và Bob, và tỉ lệ mập mờ tại EAV đánh giá mức độ bảo mật của bản tin được truyền đi.

Xác suất lỗi trung bình tại Bob được cho bởi

$$P_e = \Pr\{\hat{W} \neq W\} \tag{1.1}$$

Sự không chắc chắn về bản tin mà EAV giải mã được có thể đo bằng tỉ lệ mập mờ Δ hay có thể nói là độ khó của việc xác định bản tin đã được truyền đi tương ứng với dữ liệu nhận được tại EAV, và được định nghĩa như sau

$$\Delta = \frac{1}{n} H(W|Z) \tag{1.2}$$

trong đó $H(W|Z)$ là lượng entropy còn lại của W từ thông tin đầu ra Z tại EAV. Tỉ lệ mập mờ Δ càng cao thì lượng thông tin về bản tin W mà EAV biết được càng ít. Theo [4, 6, 44, 68], bảo mật hoàn hảo theo lý thuyết thông tin khi tỉ lệ mập mờ bằng với tốc độ của bản tin truyền đi. Bảo mật truyền tin hoàn hảo tại tốc độ R_s được cho là có thể đạt được, nếu với một $\varepsilon > 0$ nhỏ tùy ý, tồn tại một chuỗi mã $(2^{nR_s}, n)$ có độ dài từ mã 2^{nR_s} và độ dài bản tin n với n đủ lớn (tức là, $n \to \infty$), như sau

$$P_e \leq \varepsilon \tag{1.3}$$

$$\Delta \geq R_s - \varepsilon \tag{1.4}$$

Dung lượng bảo mật được định nghĩa là tốc độ bảo mật hoàn hảo tối đa có thể đạt được mà thỏa mãn (1.3) và (1.4). Nghĩa là, dung lượng bảo mật là tốc độ bảo mật lớn nhất trong tất cả các tốc độ bảo mật đạt được [68]. Tức là

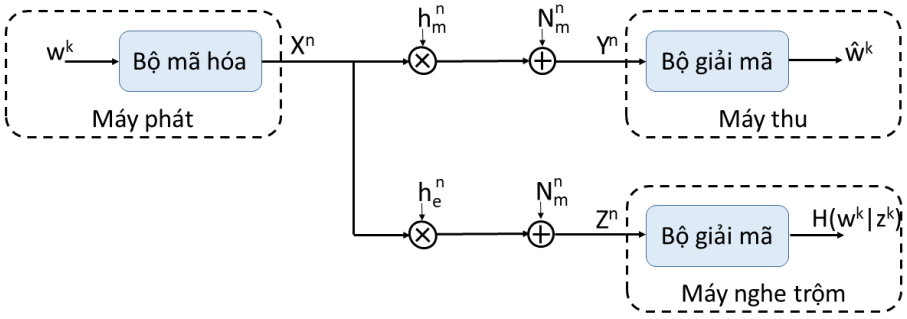
$$C_s \triangleq \sup R_s \text{ với } P_e \leq \varepsilon \tag{1.5}$$

Tiếp theo sau, các phát triển mở rộng cho kênh wiretap đến kênh truyền quảng bá với bản tin bí mật và kênh wiretap Gaussian [8, 42]. Các nghiên cứu

nghiên cứu trên đều được phát triển dựa trên nội dung tối ưu trong lý thuyết thông tin và đã chỉ ra rằng dung lượng bảo mật khác không có thể đạt được ngay cả khi kênh EAV không bị suy thoái [8]. Trong [42], dung lượng bảo mật của kênh wiretap Gausian có được từ sự khác biệt giữa dung lượng kênh của kênh chính và kênh wiretap.

1.1.2 Kênh fading wiretap

Các công trình nghiên cứu trước đây như [8,42,90] đã cho thấy dung lượng bảo mật khác không có thể có được khi kênh EAV có chất lượng thấp hơn kênh chính. Tuy nhiên, trong các công trình nghiên cứu mở rộng khác của kênh wiretap cho các kênh fading cho thấy bảo mật dựa trên lý thuyết thông tin là hoàn toàn có thể đạt được ngay cả khi EAV có SNR trung bình tốt hơn so với người dùng hợp pháp [4, 68]. Bên cạnh đó, các kỹ thuật như đa ăng-ten [2, 58, 75, 110], hợp tác chuyển tiếp [11, 109], can nhiễu [18, 101, 104], phân tập lựa chọn [2,6], đã được kết hợp sử dụng nhằm cải thiện hơn nữa khả năng bảo mật ở lớp vật lý chống lại các tấn công nghe trộm.



Hình 1.2: *Mô hình kênh fading wiretap*

Chúng ta xem xét mô hình kênh fading wire-tap như hình 1.2. Máy phát muốn gửi bản tin w đến máy thu, khối bản tin w^k được mã hóa vào từ mã $x^n = [x(1), ..., x(2)..., x(n)]$ để truyền tải qua kênh chính. Tín hiệu nhận được ở máy thu có dạng như sau

$$y_m(i) = h_m(i)x(i) + n_m(i) \tag{1.6}$$

trong đó $h_m(i)$ là hệ số kênh fading phức biến đổi theo thời gian và $n_m(i)$ là nhiễu Gausian phức đối xứng vòng với kỳ vọng bằng không của kênh chính. Hệ số $h_m(i)$ được tham khảo là trạng thái kênh (CSI) độc lập với đầu ra kênh và thu được theo một phân bố xác xuất $p(h_m)$. Chúng ta giả sử môi trường truyền tin là quasi-static, nghĩa là hệ số kênh là hằng số trong thời gian của một từ mã, tức là $h_m(i) = h_m, \forall i$. Cùng thời gian, thiết bị nghe trộm cũng có thể thu nhận được tín hiệu do máy phát truyền đi như sau

$$z(i) = h_e(i)x(i) + n_e(i) \tag{1.7}$$

Do trong cùng một môi trường fading, tương tự như kênh chính ta có $h_e(i) = h_e, \forall i$ là hệ số kênh của kênh wiretap và $n_e(i)$ là nhiễu Gausian phức đối xứng vòng với kỳ vọng bằng không tại kênh wiretap.

Kênh truyền bị giới hạn về mặt công suất bởi

$$\frac{1}{n}\sum_{i=1}^{n} E[|X(i)|^2] \leq P \tag{1.8}$$

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

$$\gamma_m(i) = \frac{P|h_m(i)|^2}{N_m} \tag{1.9}$$

$$\gamma_e(i) = \frac{P|h_e(i)|^2}{N_e} \tag{1.10}$$

Dung lượng bảo mật kênh trong (**??**) có thể được viết lại như sau [87, Appendix B]

$$C_s = \log_2(1 + \frac{P}{N_m}) - \log_2(1 + \frac{P}{N_e}) \tag{1.11}$$

Mặt khác với kênh fading, vì là môi trường quasi-static nên có thể xem kênh chính như là kênh AWGN phức và hệ số kênh là hằng số trong thời gian của một từ mã, [87, Chapter 5], với SNR $\gamma_m = \frac{P|h_m|^2}{N_m}$ và dung lượng kênh là

$$C_m = \log(1 + \gamma_m) \tag{1.12}$$

Tương tự, dung lượng kênh của kênh wiretap được cho bởi

$$C_m = \log_2(1 + \gamma_e) \tag{1.13}$$

với SNR $\gamma_e = \frac{P|h_e|^2}{N_e}$. Từ (1.12) và (1.13), chúng ta có thể mô tả dung lượng bảo mật kênh của hệ thống trong môi trường kênh fading như sau

$$C_s = \log_2(1 + \gamma_m) - \log_2(1 + \gamma_e) \tag{1.14}$$

1.1.3 Phương pháp đánh gía hiệu suất hoạt động và bảo mật thông tin của hệ thống

Hiệu suất hoạt động và bảo mật thông tin ở tầng vật lý của hệ thống mạng không dây trên các kênh fading được đánh giá chủ yếu thông qua ba tham số: *Dung lượng bảo mật hệ thống*, *Xác suất dung lượng bảo mật khác không* và *Xác suất dừng bảo mật*. Trong phần này báo cáo trình bày tóm lược lại một số độ đo hiệu suất được sử dụng trong nghiên cứu để đánh giá các mô hình hệ thống.

1.1.3.1 Dung lượng kênh

Dung lượng kênh là khái niệm cơ bản của lý thuyết thông tin trong kênh truyền thông không dây. Nó xác định tốc độ truyền tin tối đa của mỗi kênh truyền có thể đáp ứng được. Dung lượng kênh tức thời của một kênh fading được biểu diễn bởi công thức Shannon [19], như sau

$$C = B \log_2(1 + \gamma) \tag{1.15}$$

trong đó B là băng thông của kênh truyền và γ là SNR thu được.

1.1.3.2 Dung lượng bảo mật kênh

Như đã đề cập ở phần trên, các nghiên cứu về bảo mật lớp vật lý trong mạng không dây xác định dung lượng bảo mật kênh là sự khác biệt giữa dung lượng kênh của kênh hợp pháp và dung lượng kênh của kênh wiretap [4, 68]. Do tính chất không âm của dung lượng kênh, chúng ta có thể biểu diễn lại

như sau

$$C_s = \begin{cases} \log_2(1+\gamma_m) - \log_2(1+\gamma_e), & \text{nếu } \gamma_m > \gamma_e \\ 0, & \text{nếu } \gamma_m \leq \gamma_e \end{cases} \tag{1.16}$$

trong đó γ_m, γ_e lần lượt là SNR của kênh hợp pháp và kênh wiretap, tương ứng. Theo (1.16), có thể thấy rằng dung lượng bảo mật kênh lớn hơn 0 khi $\gamma_m > \gamma_e$. Vì vậy, một trong những nội dung quan trọng trong đánh giá khả năng bảo mật của hệ thống là tính toán xác suất tồn tại một dung lượng bảo mật kênh lớn hơn 0.

1.1.3.3 Dung lượng bảo mật khác 0

Giả định rằng kênh hợp pháp và kênh wiretap là độc lập nhau, Từ (1.16), chúng ta thấy rằng xác suất dung lượng bảo mật khác không chính là xác suất khi dung lượng kênh của kênh chính lớn hơn dung lượng kênh của kênh wiretap, điều đó có nghĩa là tỉ số tín hiệu trên nhiễu (SNR) của kênh chính lớn hơn tỉ số tín hiệu trên nhiễu (SNR) của kênh wiretap, Tức là

$$Pr(C_s > 0) = Pr(\gamma_m > \gamma_e) \tag{1.17}$$

1.1.3.4 Xác suất dừng bảo mật

Cuối cùng, chúng ta xem xét khái niệm xác suất dừng bảo mật. Gọi $R_s > 0$ là tốc độ bảo mật mong muốn của hệ thống, Xác suất dừng bảo mật của hệ thống là xác suất mà dung lượng bảo mật kênh tức thời C_s nhỏ hơn giá trị của R_s. Nghĩa là

$$SOP = Pr(C_s < R_s) \tag{1.18}$$

Ý nghĩa của khái niệm xác suất dừng bảo mật là khi thiết lập một tốc độ bảo mật R_s, máy phát giả định rằng dung lượng kênh wire-tap được cho bởi $C'_e = C_m - R_s$. Miễn là $R_s < C_s$, thì dung lượng kênh của kênh wiretap sẽ yếu hơn so với mức ước lượng của máy phát, tức là $C_e < C'_e$, và do đó mã code wiretap được sử dụng bởi máy phát sẽ đảm bảo bảo mật thông tin hoàn hảo cho truyền thông. Ngược lại, nếu $R_s > C_s$ thì $C_e > C'_e$ và như vậy theo nguyên

lý bảo mật dựa trên lý thuyết thông tin thì tính bảo mật thông tin sẽ bị phá vỡ và thiết bị nghe trộm có thể thu và giải mã thành công các bản tin được truyền đi từ nguồn.

1.2 Tổng quan về mạng vô tuyến nhận thức

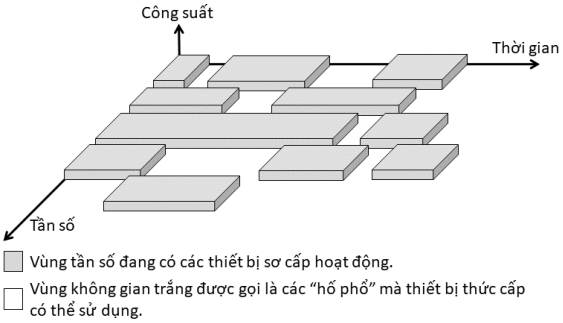
Với sự phát triển mạnh mẽ của mạng truyền thông không dây dẫn đến sự tăng trưởng với số lượng lớn của các thiết bị thông minh và các yêu cầu ngày càng cao của các dịch vụ mạng trong những thập kỷ qua và trong thời gian tiếp theo. Tuy nhiên, cùng với sự phát triển của công nghệ và dịch vụ mạng không dây là nhu cầu ngày càng cao về khai thác và sử dụng phổ tần số, một tài nguyên quốc gia hữu hạn. Hiện nay, với chính sách quản lý và phân bổ tần số, các mạng không dây chỉ được hoạt động trên dải tần số cố định được cấp phép. Bên cạnh đó, qua quá trình khảo sát về mức độ sử dụng tối ưu các dải tần số đã cấp phép chỉ ra rằng phần lớn các dải tần số đang được sử dụng một cách thiếu hiệu quả do chính sách quản lý phân bổ kém linh hoạt và khai thác thiếu hiệu quả [9,32]. Vì vậy, đây là một thách thức lớn đòi hỏi các nhà khoa học phải tìm kiếm các giải pháp tối ưu để giải quyết vấn đề này. Trong các giải pháp tiềm năng được đề xuất, J Mitola đề xuất một phương pháp sử dụng và quản lý các dải tần số mới có tên gọi là mạng vô tuyến nhận thức (Cognitive radio networks), Công nghệ này nổi lên là phương pháp hiệu quả và được xem là tiền đề cho các thế hệ tiếp theo của mạng không dây [26,55,56].

Mạng vô tuyến nhận thức được phân lớp thành hai thành phần mạng chính là thiết bị sơ cấp (PU) và thiết bị thứ cấp (SU). thiết bị PU được cấp phát và sở hữu một giải tần số nhất định, và nó có quyền ưu tiên cao nhất khi truy cập và thực hiện truyền thông mà không phải chịu tác động nhiễu tiêu cực của các thiết bị khác trong dải tần mà nó được cấp phép. Ngược lại, thiết bị SU được áp dụng các kỹ thuật xử lý tín hiệu tiên tiến và phương pháp truy cập thông minh nhằm tận dụng lại các dải tần số đã cấp phát cho PU mà không làm ảnh hưởng đến chất lượng dịch vụ của PU [20]. Tư tưởng của giải pháp này là các thiết bị di động thông minh có thể sử dụng chung các dải tần số đã được cấp phát cho đối tượng khác với một số điều kiện nhất định, với cách

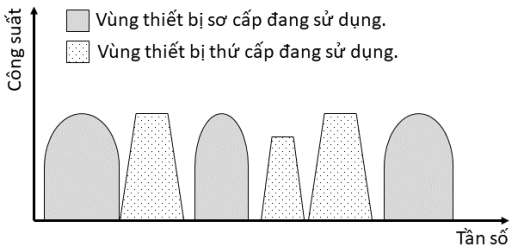
tiếp cận này mạng vô tuyến nhận thức có thể khai thác tối ưu các dải tần số và khắc phục được vấn đề cạn kiệt tài nguyên tần số trong mạng không dây.

1.2.1 Các mô hình của mạng vô tuyến nhận thức

Mạng vô tuyến nhận thức thường được phân lớp thành ba loại mô hình chính phụ thuộc vào các tiêu chí được sử dụng để cho phép SU sử dụng các dải tần số đã được cấp phép cho hoạt động truyền thông.



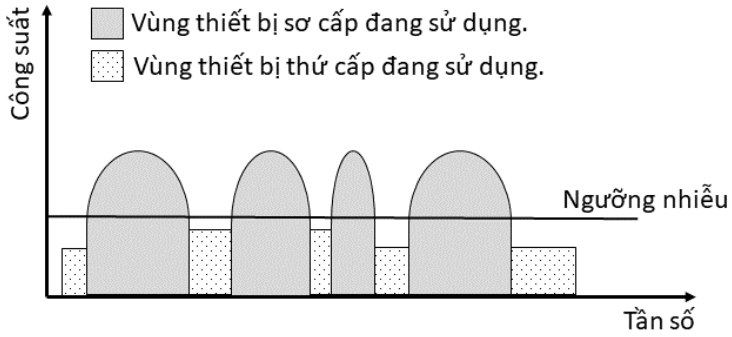
Hình 1.3: *Ví dụ về các "hố phổ"*



Hình 1.4: *mô hình truy cập đan xen*

Mô hình truy cập đan xen (Interweave Paradigm): Mô hình truy cập đan xen là mô hình hoạt động dựa trên khái niệm hố phổ như hình 1.3 Các thiết bị SU có khả năng tìm kiếm các "hố phổ" để sử dụng cho mục đích liên lạc mà không có tác động ảnh hưởng đến hoạt động của PU. Để truyền thông hiệu quả trong mô hình này, một trong những yếu tố có tính quyết định là các SU cần phải có các kỹ thuật thông minh để tìm kiếm các "hố phổ". Trong quá trình truyền thông của SU, nếu PU trở lại sử dụng dải phổ mà SU đang liên lạc, buộc SU phải nhảy ra khỏi dải phổ này để nhường chỗ cho PU và chuyển sang các "hố phổ" khác để tiếp tục liên lạc và không gây can nhiễu lên chất lượng dịch vụ của các PU, nếu không tìm ra "hố phổ" nào thì liên lạc của các SU buộc phải dừng. Theo hình 1.4, mô hình này có ưu điểm là SU có thể sử dụng tối đa công suất tại các "hố phổ" tìm được. Tuy nhiên, nhược điểm lớn của nó là khả năng thời gian thực của truyền thông khi hoàn toàn phụ thuộc vào tần suất hoạt động của hệ thống mạng sơ cấp. Bên cạnh đó, việc tìm kiếm chính xác các "hố phổ" là một thách thức đối với hệ thống mạng thứ cấp khi mà môi trường truyền thông là ngẫu nhiên và thường xuyên thay đổi.

Mô hình truy cập dạng chồng (Overlay Paradigm): Trong mô hình này, các thiết bị SU và PU hoạt động đồng thời trên cùng dải tần với giả định rằng hai hệ thống này có thể trao đổi thông tin và kết hợp lẫn nhau để loại bỏ hoặc tránh can nhiễu giữa hai hệ thống bằng những kỹ thuật xử lý tín hiệu phức tạp. Bên cạnh đó, các thiết bị SU còn có thể tham gia hỗ trợ các thiết bị PU trong quá trình truyền các bản tin. Như trong các tài liệu [20,78] đã giới thiệu các giải pháp kỹ thuật trong đó các thiết bị SU khi hoạt động có thể giúp PU cải thiện hiệu năng truyền thông dưới dạng chuyển tiếp. Hiện tại, mô hình này đang được nghiên cứu do tính phức tạp trong việc xử lý tín hiệu và hợp tác truyền thông giữa hai loại mạng sơ cấp và thứ cấp.

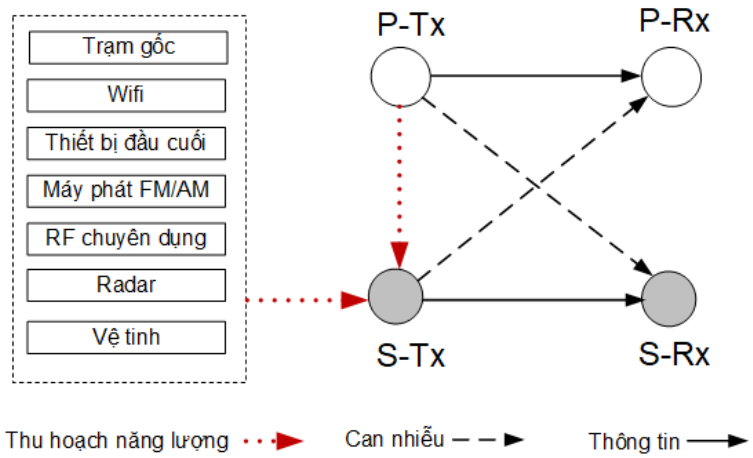


Hình 1.5: *Ví dụ về mô hình truy cập dạng nền*

Mô hình truy cập dạng nền (Underlay Paradigm): Ở mô hình truy cập dạng nền hay còn được gọi là truy cập dưới ngưỡng nhiễu, các PU và SU hoạt động đồng thời trên cùng một dải tần số với điều kiện là can nhiễu từ SU không được vi phạm các điều kiện đặt ra từ PU [17,98,99]. Hay nói cách khác, quá trình truyền thông của SU hoạt động đồng thời cùng với PU trên cùng một dải tần số nhưng phải đảm bảo các điều kiện nhất định để không làm ảnh hưởng đến chất lượng dịch vụ của các PU. Hình 1.5 minh họa mô hình truy cập dưới ngưỡng nhiễu, trong đó ta có thể thấy công suất truyền của mạng thứ cấp phải giữ dưới một ngưỡng nhiễu cho trước được đưa ra bởi mạng sơ cấp. Với các ràng buộc như trên, nhược điểm của mô hình này là tốc độ và phạm vi truyền thông của mạng thứ cấp bị giới hạn. Mặt khác, các thiết bị SU cần phải phân tích được thông tin trạng thái kênh truyền của kênh truyền can nhiễu từ mạng thứ cấp đến sơ cấp. Tuy nhiên trong thực tế, thông

tin trạng thái kênh nhận được có thể không hoàn hảo dẫn đến các thiết bị SU có thể không đảm bảo các mức can nhiễu theo quy định tại PU. Để cải thiện hiệu năng hoạt động của mạng, các thiết bị SU có thể sử dụng nhiều các giải pháp như kỹ thuật trải phổ tiên tiến, MIMO, truyền thông hợp tác, .v.v.

1.2.2 Mạng vô tuyến nhận thức kết hợp kỹ thuật thu hoạch năng lượng vô tuyến



Hình 1.6: *Mô hình tổng quát mạng CRN với kỹ thuật thu hoạch năng lượng vô tuyến*

Trong một số mô hình mạng không dây, chẳng hạn như mạng cảm biến. Năng lượng là một yếu tố quan trọng giới hạn hiệu suất hoạt động của mạng. Việc kéo dài thời gian hoạt động của các mạng này là một vấn đề thách thức lớn ở nhiều trường hợp triển khai trong thực tế do việc thay thế hoặc nạp năng lượng cho các nút mạng này là khó khăn hoặc vô cùng tốn kém. Gần đây, thu hoạch năng lượng từ các nguồn xung quanh, ví dụ như năng lượng mặt trời và gió, đã được coi là một công nghệ đầy hứa hẹn có thể giúp khắc phục những hạn chế về năng lượng của mạng không dây. Trong đó, thu hoạch năng lượng tần số vô tuyến (RFEH) là một giải pháp đặc biệt thú vị do các đặc tính linh hoạt và bền vững của nó trong các khu vực nơi các máy phát không dây được triển khai dày đặc và tín hiệu RF của chúng luôn có sẵn [52]. Với những tiến bộ phát triển của công nghệ vi điện tử, vật liệu và các kỹ thuật truyền thông không dây hiện nay đã làm cho kỹ thuật RFEH trở thành một

giải pháp kỹ thuật khả thi và thu hút được rất nhiều sự chú ý trong thời gian gần đây [23, 62]. Những nguồn này có thể cung cấp đủ năng lượng cho các mạng cảm biến không dây có nhu cầu năng lượng cho các nút cảm biến ở mức thấp [81]. Đối với các mạng đòi hỏi nhiều năng lượng hơn, các kỹ thuật truyền năng lượng không dây phức tạp cũng đã được nghiên cứu thiết kế [22, 100, 103].

Sự kết hợp của mô hình mạng CRN và kỹ thuật RFEH có thể mang lại lợi thế lớn cho các mạng truyền thông không dây và đã nhận được nhất nhiều sự quan tâm nghiên cứu trong thời gian gần đây [66, 67, 93]. Khi thu hoạch năng lượng được nghiên cứu trong các mạng CRN. Ngoài các tín hiệu RF từ các nguồn phát khác, các tín hiệu RF được tạo bởi máy phát P-Tx của mạng sơ cấp, theo truyền thống được coi là có hại đối với người dùng SU, thay vào đó có thể được chuyển đổi thành năng lượng hữu ích cho truyền thông của mạng thứ cấp. Theo đó, SU có thể sử dụng cả phổ tần số được cấp phép và năng lượng của PU [7, 28, 40, 57, 71, 92].

1.3 Tổng quan tình hình nghiên cứu

Đặc điểm chung trong truyền thông bảo mật thông qua hệ thống mạng không dây là do tính chất quảng bá mở tự nhiên cùng với các hiệu ứng fading trong môi trường kênh truyền không dây, đã làm phát sinh nhiều thách thức và yêu cầu nghiên cứu nhằm cải thiện an ninh cho truyền thông. Từ công trình nhiên cứu về bảo mật dựa trên lý thuyết thông tin của Shannon và kênh wiretap của Wyner, Các nỗ lực nghiên cứu đáng kể đã tập chung cho việc phát triển các kỹ thuật bảo mật lớp vật lý khác nhau và có thể phân loại thành một số hướng nghiên cứu chính sau: Kỹ thuật mã hóa và xử lý tín hiệu; Kỹ thuật tạo khóa bảo mật mức vật lý, kỹ thuật đa ăng-ten và kỹ thuật hợp tác chuyển tiếp.

Kỹ thuật mã hóa và xử ký tín hiệu thường được thiết kế để thực hiện liên lạc bảo mật và tin cậy bằng cách thêm dự phòng vào dữ liệu được truyền đi để cho phép thiết bị thu có thể phát hiện và sửa lỗi, đồng thời thêm tính ngẫu nhiên để ngăn cản EAV [49]. Một số phương pháp mã hóa như mã Polar hoặc

mã LDPC đã được đề xuất để đạt được khả năng bảo mật [38, 54, 85]. Các kỹ thuật mã hóa này thường yêu cầu CSI từ các kênh truyền. Với CSI hoàn hảo, mã hóa kênh có thể có được đầu vào tối ưu để tính toán khả năng bảo mật. Tuy nhiên, điều này là thách thức lớn trong môi trường kênh truyền fading và làm cho việc tối ưu và tính toán khả năng bảo mật là rất khó khăn.

Một kỹ thuật phổ biến được khai thác sử dụng để tăng cường khả năng bảo mật truyền thông trong mạng không dây là kỹ thuật đa ăng-ten [36,37,43, 107]. Tư tưởng chính trong nghiên cứu bảo mật với đa ăng-ten là làm tăng sự chênh lệnh cường độ tín hiệu giữa máy thu hợp pháp và thiết bị nghe trộm. Một lược đồ đơn giản trong đó các user (máy phát, máy thu và thiết bị nghe trộm) đều được trang bị một ăng-ten đơn, sơ đồ truyền thông này được gọi là SISOSE được giới thiệu trong [21]. Kịch bản thứ hai được khảo sát là khi máy phát được trang bị một ăng-ten đơn trong khi máy thu được trang bị đa ăng-ten. Kịch bản này được gọi là SIMOME [65]. Trường hợp thứ ba liên quan đến việc sử dụng đa ăng-ten tại máy phát và một ăng-ten đơn tại máy thu. Trường hợp này được gọi là MISOME [59, 89]. Và một kịnh bản cuối cùng trong kỹ thuật đa ăng-ten là MIMO được sử dụng rộng rãi trong nhiều mạng không dây [106]. Như chúng ta biết, bảo mật lớp vật lý được đặc trưng bởi tốc độ bảo mật đạt được, dung lượng bảo mật kênh được định nghĩa là tốc độ truyền tin tối đa giữa các người dùng hợp pháp mà kẻ nghe trộm không thể thu nhận được bất kỳ thông tin gì. Một số công trình nghiên cứu đã tập chung vào đặc trưng này bằng cách sử dụng một số độ đo hiệu suất như xác suất dừng bảo mật, dung lượng bảo mật kênh, xác suất dung lượng bảo mật khác không, dung lượng bảo mật Ergodic khảo sát cho các dạng phân bố fading phổ biến như Rayleigh, Rice, Nakagami-m, log-normal [45,47,72,83,105]. Hơn nữa, một số nhà nghiên cứu đã chỉ ra rằng sử dụng kỹ thuật lựa chọn ăng-ten có thể nâng cao hiệu suất bảo mật của truyền thông không dây [2]. Trong một hệ thống mà máy phát có đa ăng-ten, kỹ thuật lựa chọn ăng-ten có thể được sử dụng để khai thác sự biến đổi bất thường của kênh fading quanh các ăng-ten. Hiệu quả của kỹ thuật lựa chọn ăng-ten phát đến khả năng bảo mật của hệ thống MISO được xem xét trong [24, 37, 106], trong đó xác suất dừng bảo mật được sử dụng để đánh giá hiệu suất bảo mật và nó cho thấy rằng kỹ thuật

lựa chọn ăng-ten có thể cải thiện đáng kể khả năng bảo mật lớp vật lý của hệ thống.

Bên cạnh đó, một giải pháp khác cũng được sử dụng rộng rãi trong lĩnh vực bảo mật lớp vật lý để nâng cao hiệu suất bảo mật cho truyền thông không dây là kỹ thuật hợp tác chuyển tiếp [14, 69, 109]. Trong [109], các tác giả đã nghiên cứu hiệu suất bảo mật của hệ thống hợp tác sử dụng hai giao thức chuyển tiếp AF và DF và đã cho thấy rằng việc sử dụng các kỹ thuật chuyển tiếp hợp tác có khả năng cải thiện an ninh hệ thống chống lại tấn công nghe trộm. Ngoài ra, các tác giả trong [14] đã nghiên cứu bảo mật lớp vật lý trong các mạng chuyển tiếp MIMO và cho thấy khả năng bảo mật cải thiện đáng kể bằng cách sử dụng chuyển tiếp MIMO. Một cách tiếp cận khác trong sử dụng kỹ thuật hợp tác chuyển tiếp nhằm cải thiện bảo mật mức vật lý là tạo nhiễu nhân tạo để chủ động tấn công và làm giảm dung lượng kênh của kênh wiretap. Đã có nhiều công trình nghiên cứu trong đó thiết bị thu phát hợp pháp chủ động tạo ra can nhiễu nhân tạo để bảo vệ thông tin [10,11,39,46,88, 102]. Cụ thể, trong [11] và [102] đề xuất giải pháp tối ưu cho nút chuyển tiếp hợp tác gây can nhiễu để tối đa tốc độ bảo mật dữ liệu. Trong [39], Krikidis *et. al.* đề xuất việc lựa chọn khả năng cho hai nút chuyển tiếp trong đó một nút chuyển tiếp được sử dụng để chuyển tiếp tín hiệu từ nguồn, và nút còn lại được sử dụng cho chiến lược hợp tác gây can nhiễu. Hoặc trong [88], các tác giả đã xem xét các mức độ CSI của kênh truyền để khảo sát xác suất dừng bảo mật của hệ thống bằng cách sử dụng kỹ thuật hợp tác gây can nhiễu.

Như đã trình bày ở phần trước, mạng CRN là một mô hình mạng nhiều tiềm năng để khắc phục được các thách thức và hạn chế của các mạng không dây thế hệ mới. Tuy nhiên, với đặc điểm của mạng CRN dẫn đến khả năng các PU và SU có thể sẽ bị đặt vào rủi ro khi gặp phải các kẻ tấn công từ bên trong hoặc ngoài mạng khi chúng giả mạo thiết bị cảm biến [15, 82, 111]. Hơn nữa, kẻ tấn công có thể lạm dụng khả năng thích nghi của CRN để gây ra các tác động tiêu cực tới môi trường vô tuyến, ví dụ như bằng cách tạo can nhiễu, có thể làm giảm hiệu suất hoặc tiết lộ bí mật của thông tin liên lạc, thậm chí có thể gây ra các sự cố cho các hoạt động của người dùng hợp pháp. Do đó, việc giải quyết các vấn đề an toàn từ mọi khía cạnh của kiến trúc mạng trở thành

một trong những vấn đề khó khăn nhất với mạng CRN [1, 111]. Các nghiên cứu tổng quát nhất về hiệu năng bảo mật cho mạng CRN đã được công bố trong nhiều tài liệu như [1, 13, 31, 41, 50, 61, 84, 94, 97]. Cụ thể hơn, hình thức tấn công giả lập người dùng chính (PUE) đã được khảo sát trong [1] và các tác giả đã đề xuất một giải pháp để giảm tấn công PUE trong mạng CRN hoạt động trong băng tần TV kỹ thuật số (DTV). Cách tiếp cận này có hiệu quả có thể giảm thiểu các cuộc tấn công PUE với việc bổ sung một chip AES plugin vào phần cứng hệ thống. Khái niệm xác suất dừng bảo mật đã được khảo sát cho các SU trong tác động ảnh hưởng của kênh fading có phân bố Nakagami-m trong các tài liệu [41, 61, 84]. Trong [84], ngoài khái niệm xác suất dừng bảo mật, các tác giả khảo sát khái niệm xác suất dung lượng bảo mật khác 0 cho hệ thống với các SU, EAV sử dụng ăng-ten đơn. Các khảo sát hiệu suất bảo mật hệ thống cho các trường hợp khác nhau của SU, EAV sử dụng đa ăng-ten được đề cập trong [41, 61]. Mặt khác, các nghiên cứu hiệu suất bảo mật hệ thống mạng CRN trong ảnh hưởng kênh truyền Rayleigh fading cũng đã được đề cập trong [31, 50]. Trong công trình nghiên cứu [63], khái niệm dung lượng bảo mật ergodic trong mạng CRN dưới tác động của các kênh fading nhanh đã được sử dụng phân tích hiệu suất bảo mật hệ thống. Gần đây, các giao thức truyền thông và kỹ thuật xử lý tín hiệu đã được nghiên cứu và ứng dụng để nâng cao hiệu suất bảo mật của mạng CRN, được trình bày trong các tài liệu [5, 64, 73, 96, 111]. Trong [73], một lược đồ lựa chọn nút chuyển tiếp tối ưu để giảm thiểu xác suất dừng bảo mật của mạng vô tuyến hợp tác nhận thức (CCRN) đã được nghiên cứu để hỗ trợ SU và tối đa hóa tốc độ bảo mật có thể đạt được mà không làm gián đoạn PU. Các chiến lược lựa chọn chuyển tiếp khác nhau để tăng cường truyền thông bảo mật trong các mạng DF CRN đã được khảo sát. Các tác giả đã đề xuất một cặp nút chuyển tiếp để bảo vệ thông tin chống nghe trộm, trong đó một nút chuyển tiếp được chọn trước tiên để truyền thông tin bảo mật đến đích, trong khi nút còn lại được sử dụng như một thiết bị gây nhiễu hợp tác để phát tín hiệu nhiễu nhân tạo đến EAV [48]. Ở tài liệu [25], một phân tích hiệu suất về dung lượng bảo mật kênh trung bình với mạng CCRN có nhiều nút chuyển tiếp sử dụng kỹ thuật Reactive-DF đã được nghiên cứu và kết quả thu được cho thấy rằng việc sử

dụng các nút chuyển tiếp có thể nâng cao hiệu suất bảo mật. Ngoài ra, các kỹ thuật như đa ăng-ten, bemforming và gây can nhiễu hợp tác cho mạng CRN đã được tận dụng cho lĩnh vực nghiên cứu này đã được trình bày trong các tài liệu [5,60,64,77]. Trong các thảo luận về bảo mật cho nhiều người dùng trong mạng CRN, một chiến lược lập kế hoạch để tăng cường bảo mật cho truyền thông đã được đề xuất trong [96]. Ở các công trình nghiên cứu [95] và [80], các chiến lược kết hợp lý thuyết trò chơi đã được áp dụng để khảo sát bảo mật cho một kịch bản trong mạng CRN. Chiến lược phân bổ băng thông và các chính sách phân bổ công suất đã được đề xuất để tăng cường khả năng bảo mật truyền thông của PU. Trong [51], các tác giả đã nghiên cứu tác động truyền thông của mạng thứ cấp đến tính bảo mật của mạng sơ cấp. Kết quả cho thấy sự an toàn của mạng sơ cấp còn phụ thuộc rất nhiều vào điều kiện kênh truyền của máy phát SU đến thiết bị EAV và chính sách về công suất truyền tin của S-Tx. Mặt khác, việc áp dụng công nghệ thu hoạch năng lượng vô tuyến trong mạng CRN để tận dụng các đặc điểm thuận lợi của mô hình mạng này cũng dẫn đến tăng khả năng bị tấn công bởi các lỗ hổng an ninh tiềm ẩn, việc sử dụng nguồn cung cấp từ nguồn năng lượng có thông tin cao dẫn đến khả năng rò rỉ thông tin nghiêm trọng. Để khắc phục các vấn đề bảo mật trong chủ đề này, một số các công trình nghiên cứu như [29,34,70,79] đã tập trung vào các giải pháp ở lớp vật lý để giảm nguy cơ bị nghe trộm hoặc gây nhiễu. Trong [70], các tác giả xem xét một mô hình hệ thống trong đó một thiết bị gây nhiễu hợp tác thu năng lượng từ RF của máy phát thứ cấp (S-Tx) và sau đó tạo ra các tín hiệu gây nhiễu để bảo vệ chống lại EAV. Các biểu thức xấp xỉ của xác suất dừng và xác suất chặn cho các kênh fading có phân bố Nakagami-m đã được tính toán để phân tích hiệu suất hệ thống. Trong [79], mạng CRN trong đó nhiều thiết bị thu năng lượng có thể đóng vai trò là EAV tiềm ẩn đã được nghiên cứu trong môi trường fading tầm hẹp và pathloss, biểu thức tường minh cho xác suất dừng bảo mật được tính toán để phân tích hệ thống. Ngoài ra, [29] khảo sát một mạng CRN trong đó SU thu năng lượng từ nguồn năng lượng không dây và sau đó sử dụng nó để truyền dữ liệu trên kênh nhàn rỗi được cấp phép cho PU. Tuy nhiên, hiệu suất của SU trong CRN này có thể bị suy giảm rất nhanh do các cuộc tấn công gây nhiễu bởi người

dùng bất hợp pháp cũng sử dụng nguồn năng lượng này để thực hiện tấn công. Để khắc phục những vấn đề này, các thuật toán học đã được đề xuất để giảm các tác động tiêu cực từ những kẻ gây nhiễu không mong muốn.

Trong các công trình nghiên cứu được đề cập ở trên, mặc dù vấn đề phân tích hiệu suất cho bảo mật lớp vật lý cho mạng không dây, đặc biệt là mô hình mạng CRN đã có nhiều thành tựu [5,25,48,60,97,112]. Tuy nhiên,việc xem xét ảnh tác động của kênh P-Tx$\rightarrow$P-Rx đến hiệu suất bảo mật còn chưa được xem xét. Mặt khác, cũng chưa có nhiều tài liệu nghiên cứu phân tích hiệu suất về truyền thông tin cậy và bảo mật. Do đó, trong chương 2, nhóm nghiên cứu thực hiện đánh giá hiệu suất truyền thông tin cậy và bảo mật cho mô hình mạng SIMO CRN với sự hiện diện của EAV nghe trộm thông tin từ các truyền thông của SU.

Tiếp theo, mặc dù đã có khá nhiều kết quả thú vị đã được công bố cho vấn đề an toàn truyền thông trong CRN kết hợp kỹ thuật thu hoạch năng lượng vô tuyến. Tuy nhiên, việc sử dụng tín hiệu can nhiễu từ nhiều PU để thu năng lượng, giảm ảnh hưởng của EAV và đồng thời tăng cường độ tin cậy của truyền thông đối với CRN còn chưa được đề cập đến. Do đó, trong chương 3, nhóm nghiên cứu thực hiện nghiên cứu mô hình mạng CRN kết hợp kỹ thuật thu hoạch năng lượng để không chỉ tăng cường hiệu quả phổ tần số và sử dụng năng lượng xanh, mà còn đảm bảo một ràng buộc bảo mật nhất định cho SU.

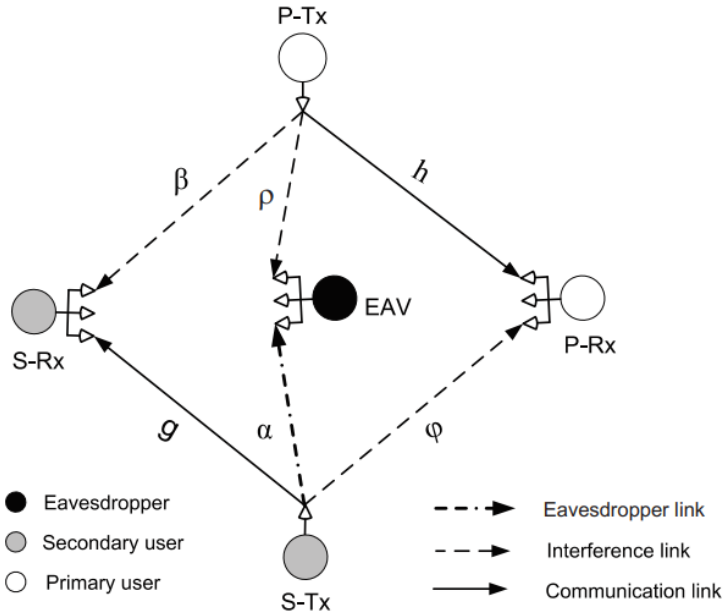
Chương 2

ĐÁNH GIÁ HIỆU SUẤT HOẠT ĐỘNG CỦA TRUYỀN THÔNG BẢO MẬT VÀ TIN CẬY TRONG MẠNG VÔ TUYẾN NHẬN THỨC

2.1 Mô hình hệ thống

Trong nội dung này, nhóm nghiên cứu sẽ xem xét một mô hình hệ thống mạng như trong hình 2.1, trong đó có ba loại người dùng trong cùng một không gian hoạt động của hệ thống, được gọi là SU, PU và EAV. PU cho phép SU tái sử dụng phổ tần số được cấp phép của nó với điều kiện SU không gây can nhiễu có hại cho PU. Mặt khác, một thiết bị EAV muốn nghe trộm thông tin liên lạc trong truyền thông của SU trên kênh wiretap. Trên thực tế, EAV có thể nghe trộm thông tin liên lạc của cả S-Tx và P-Tx, nhưng trong mô hình hệ thống này, thiết bị EAV muốn lợi dụng ảnh hưởng của can nhiễu từ P-Tx để khai thác sự trao đổi thông tin từ SU. Ở đây, chúng tôi giả định rằng S-Tx và P-Tx được trang bị một ăng-ten đơn trong khi S-Rx, P-Rx và EAV có N_s, N_p và N_e ăng-ten. Mô hình hệ thống này được coi là một thể hiện của một kịch bản trong thực tế trong đó P-Tx và S-Tx có thể là người dùng di động và P-Rx và S-Rx là các trạm gốc hoặc các điểm truy cập. Lưu ý rằng PU có thể truyền tin với mức công suất tùy chọn để đảm bảo liên lạc mà không cần quan tâm đến sự tồn tại của SU. Mặt khác, SU cần phải giữ mức ảnh hưởng can nhiễu đến PU dưới một ngưỡng xác định trước. Do đó, SU cần biết được độ lợi trung bình của kênh truyền thông P-Rx $\rightarrow$ P-Rx (không phải là độ lợi kênh tức thời) để điều chỉnh công suất phát của nó. Trên thực tế, để thu nhận các giá trị của các tham số kênh truyền, SU và PU có thể cộng tác bằng cách sử dụng một

dịch vụ cục bộ mà PU và SU có thể trao đổi với nhau về các tham số kênh truyền như khoảng cách truyền, độ lợi ăng-ten, v.v., [3, 108]. Hơn nữa, S-Tx và P-Tx được giả định là có đầy đủ thông tin CSI của các kênh truyền thông S-Tx→S-Rx và P-Tx→PRx. Điều này là hợp lý do trong thực tế cả SU và PU đều nằm trong cùng một hệ thống và nên thường có các kênh hồi đáp chuyên dụng riêng. Ngoài ra, độ lợi kênh của kênh nghe trộm S-Tx→EAV có thể có được theo [12, 53, 105].



Hình 2.1: *Mô hình CRN trong đó tồn tại EAV nghe trộm thông tin của S-Tx.*

Thêm nữa, tất cả các kênh trong hệ thống phụ thuộc vào kênh truyền fading có phân bố Rayleigh và độ lợi của các kênh là các biến ngẫu nhiên độc lập được phân phối theo hàm phân bố mũ. Theo đó, hàm mật độ xác suất (PDF) và hàm phân bố xác suất tích lũy (CDF) của các biến ngẫu nhiên (RV) có hàm phân bố mũ được biểu diễn, tương ứng như sau

$$f_X(x) = \frac{1}{\Omega_X} \exp\left(-\frac{x}{\Omega_X}\right) \tag{2.1}$$

$$F_X(x) = 1 - \exp\left(-\frac{x}{\Omega_X}\right) \tag{2.2}$$

trong đó biến RV X tham chiếu đến độ lợi kênh, và $\Omega_X = \mathbf{E}[X]$ là độ lợi kênh trung bình. Cụ thể hơn, các độ lợi kênh truyền thông S-Tx→S-Rx, và

P-Tx→P-Rx lần lượt được ký hiệu là g_m, h_n. Độ lợi của các kênh can nhiễu, S-Tx→P-Rx, P-Tx→S-Rx, và P-Tx→EAV được ký hiệu tương ứng là φ_m, β_n, và ρ_t. Độ lợi kênh của kênh nghe trộm được biểu diễn là α_t. Ở đây, m, n, và t ($m \in \{1, \ldots, N_p\}$, $n \in \{1, \ldots, N_e\}$, và $t \in \{1, \ldots, N_s\}$) biểu diễn chỉ số các ăng-ten của S-Rx, EAV, và P-Rx. Trong phần tiếp theo, P-Rx, S-Rx và EAV được giả sử sử dụng kỹ thuật SC để xử lý tín hiệu nhận được, tức là ăng-ten có tỷ số SINR cao nhất sẽ được sử dụng để xử lý các thông điệp nhận được. Trong thực tế là SU và PU cùng chia sẻ chung một dải phổ và do đó chúng có thể gây nhiễu lẫn nhau trong quá trình phát tín hiệu truyền. Theo định lý Shannon, dung lượng kênh của PU chịu ảnh hưởng can nhiễu từ SU có thể được biểu diễn như sau

$$C_p = B \log_2(1 + \gamma_p) \tag{2.3}$$

trong đó γ_p là SINR của PU được định nghĩa là

$$\gamma_p = \max_{m \in \{1,2,\ldots,N_p\}} \left\{ \frac{P_p h_m}{P_s \varphi_m + N_0} \right\} \tag{2.4}$$

trong đó P_p và P_s là công suất truyền của P-Tx và S-Tx. kí hiệu N_0 là công suất nhiễu nền được định nghĩa bởi $N_0 = B\mathcal{N}_0$; B và $\mathcal{N}_0$ là băng thông của hệ thống và hàm mật độ phổ công suất của nhiễu nhiệt. Vì các SU truyền thông với nhau bằng cách tái sử dụng lại băng tần của PU, bởi vậy S-Rx chịu tác động can nhiễu từ P-Tx, và do đó dung lượng kênh của SU phụ thuộc vào ảnh hưởng can nhiễu từ P-Tx và được trình bày bởi công thức sau

$$C_s = B \log_2(1 + \gamma_s) \tag{2.5}$$

trong đó

$$\gamma_s = \max_{t \in \{1,2,\ldots,N_s\}} \left\{ \frac{P_s g_t}{P_p \beta_t + N_0} \right\} \tag{2.6}$$

Cần lưu ý rằng theo giả thuyết của mô hình, thiết bị EAV nghe được thông tin SU, nhưng nó cũng bị tác động can nhiễu do P-Tx gây ra. Theo đó, dung lượng kênh của EAV được đưa ra là

$$C_e = B \log_2(1 + \gamma_e) \tag{2.7}$$

trong đó SINR tại EAV được biểu diễn như sau

$$\gamma_e = \max_{n\in\{1,2,\ldots,N_e\}} \left\{ \frac{P_s \alpha_n}{P_p \rho_n + N_0} \right\} \tag{2.8}$$

2.1.1 Độ đo hiệu suất cho truyền thông của mạng thứ cấp

Trong hệ thống đang khảo sát, công suất truyền tin của SU phải chịu các điều kiện rành buộc về an toàn và can nhiễu từ PU. Do đó, SU cần có một chính sách phân bổ công suất hợp lý không chỉ đáp ứng được các điều kiện trên mà còn có thể đạt được hiệu suất hoạt động phù hợp để đảm bảo truyền thông của nó. Chúng ta giả thuyết rằng mã code Wyner wiretap [90] được sử dụng trong truyền thông của SU. Và do đó tồn tại một tốc độ dương, $R_0 > 0$ được duy trì để cung cấp truyền thông bảo mật cho các SU, nghiên cứu này được trình bày trong các công trình khoa học [91, 105] như sau

$$R_0 = R_s - R_e \tag{2.9}$$

trong đó R_s là tốc độ truyền từ mã, và R_e tốc độ của thông tin bảo mật của SU tại EAV.

Theo đó, truyền thông của SU hoàn toàn bảo mật là có thể đạt được nếu dung lượng kênh tại EAV nhỏ hơn R_0, tức là $C_e < R_0$. Nói theo cách khác, sự kiện mất khả năng bảo mật của SU có thể sảy ra khi $C_e > R_0$, và vì vậy xác suất dừng bảo mật của SU được hình thành từ điều kiện sau

$$\mathcal{O}_{sec} = \Pr\{C_e > R_0\} \tag{2.10}$$

Hơn nữa, do tính chất ngẫu nhiên của các kênh truyền không dây và can nhiễu được gây ra bởi SU, truyền thông tin cậy của PU có thể không đạt được nếu tốc độ truyền từ mã của PU lớn hơn dung lượng kênh truyền, tức là $R_p > C_p$. Có nghĩa rằng sự kiện dừng truyền thông của PU được thể hiện như sau

$$\mathcal{O}_p = \Pr\{C_p < R_p\} \tag{2.11}$$

trong đó C_p được định nghĩa bởi (2.3).

Như vậy rõ ràng rằng, truyền thông tin cậy và bảo mật của SU có thể thu được nếu và chỉ khi cả hai sự kiện dừng bảo mật của SU và dừng truyền thông

của SU trên đều không xảy ra. Điều này có thể được diễn giải thành xác suất truyền thông tin cậy và bảo mật như sau

$$\mathcal{O}_{ss} = \Pr\left\{C_s > R_s, C_e \leq R_0\right\}, \tag{2.12}$$

trong đó C_s và C_e được trình bày trong (2.5) và (2.7), tương ứng.

2.1.2 Các điều kiện rành buộc cho công suất truyền tin của mạng thứ cấp

Trong phần này, chúng tôi áp dụng một giả định thường được sử dụng chung và phổ biến trong các công trình nghiên cứu về bảo mật mức vật lý rằng CSI của các kênh truyền là có thể thu được, bao gồm cả với kênh wiretap S-Tx→EAV [113]. Điều này hoàn toàn khả thi khi thiết bị EAV hoạt động trong vùng mạng và hành vi của nó có thể được theo dõi bởi hệ thống [4]. Trong phần tiếp theo, chúng tôi nghiên cứu các chính sách phân bổ công suất cho SU tương ứng với bốn đề xuất kịch bản truyền thông khác nhau.

2.1.2.1 Kịch bản 1 (S_1): S-Tx không có CSI của PU-Tx→PU-Rx và SU-Tx→EAV

Trong kịnh bản này, S-Tx truyền các thông tin bảo mật của nó mà không biết có sự tồn tại của thiết bị nghe trộm. Ngoài ra, SU-Tx cũng không thu nhận được thông tin về CSI của kênh truyền thông P-Tx→P-Rx. Do vậy, S-Tx chỉ điều chỉnh công suất phát tín hiệu của nó dựa trên điều kiện ràng buộc can nhiễu của PU là

$$\mathcal{O}_I = \Pr\left\{\max_{m\in\{1,2,\ldots,N_p\}}\left\{\frac{P_s\varphi_m}{N_0}\right\} \geq Q_{pk}\right\} \leq \xi \tag{2.13}$$

Trong đó Q_{pk} là mức can nhiễu tối đa mà PU có thể chấp nhận được. Như vậy có thể thấy rằng trong quá trình truyền thông, S-Tx được phép có thể gây can nhiễu tới P-Rx với một mức giới hạn cho phép. Tuy nhiên, xác suất của ảnh hưởng can nhiễu do S-Tx gây ra đối với P-Rx phải được giữ dưới ngưỡng (ξ) được xác định trước để không làm gián đoạn truyền thông của PU. Kết quả là, các điều kiện ràng buộc thiết lập cho công suất phát tín hiệu của S-Tx cần

phải thỏa mãn hai điều kiện như sau

$$\mathcal{O}_I \leq \xi \tag{2.14}$$

$$0 \leq P_s \leq P_s^{max} \tag{2.15}$$

trong đó ξ là ngưỡng dừng truyền thông được đưa ra bởi PU và P_s^{max} công suất phát tín hiệu đối đa của S-Tx.

2.1.2.2 Kịnh bản 2 (S_2): S-Tx có CSI của S-Tx→EAV nhưng không có CSI của P-Tx→P-Rx

Trong kịch bản thứ 2, S-Tx phát hiện được sự tồn tại của thiết bị nghe trộm trong khu vực hoạt động của nó. Tuy nhiên, S-Tx không có thông tin về CSI của kênh truyền thông P-Tx→P-Rx. Do đó, công suất phát tín hiệu của S-Tx cần phải thỏa mãn ba điều kiện ràng buộc như sau

$$\mathcal{O}_I \leq \xi \tag{2.16}$$

$$\mathcal{O}_{sec} \leq \epsilon \tag{2.17}$$

$$0 \leq P_s \leq P_s^{max}, \tag{2.18}$$

trong đó ϵ là ngưỡng ràng buộc dừng bảo mật đối với SU, còn $\mathcal{O}_{sec}$ và $\mathcal{O}_I$ đã được định nghĩa trong (2.10) và (2.13), tương ứng.

2.1.2.3 Kịnh bản 3 (S_3): S-Tx có CSI của P-Tx→P-Rx nhưng không có CSI của S-Tx→EAV

Trong kịnh bản thứ 3, S-Tx có CSI của kênh truyền thông P-Tx→P-Rx. Tuy nhiên, nó không phát hiện được sự tồn tại của EAV. Do đó, các điều kiện ràng buộc cho S-Tx bao gồm:

$$\mathcal{O}_p \leq \theta \tag{2.19}$$

$$0 \leq P_s \leq P_s^{max} \tag{2.20}$$

trong đó $\mathcal{O}_p$ được định nghĩa trong (2.11), và θ điều kiện ràng buộc dừng truyền thông của PU. Nói cách khác, công suất truyền tin của S-Tx cần giữ cho xác suất dừng của PU bên dưới một mức ràng buộc cho trước.

Trong kịch bản cuối, S-Tx điều chỉnh công suất truyền tín hiệu của nó để không bị tiết lộ thông tin cho EAV và đồng thời không gây can nhiễu ảnh hưởng đến hoạt động của P-Rx. Vì vậy, công suất truyền của S-Tx chịu ba điều kiện ràng buộc như sau:

$$\mathcal{O}_p \leq \theta \tag{2.21}$$

$$\mathcal{O}_{sec} \leq \epsilon \tag{2.22}$$

$$0 \leq P_s \leq P_s^{max} \tag{2.23}$$

trong đó $\mathcal{O}_p$ và $\mathcal{O}_{sec}$ đã được định nghĩa trong (2.11) và (2.10).

2.2 Phân tích hiệu suất của hệ thống

Trong phần này, đầu tiên tác giả nghiên cứu tìm được chính sách phân bổ công suất truyền tín hiệu của S-Tx, và sau đó sử dụng nó để tính toán trong môi trường fading, và hiệu suất dừng của S-Tx. Trước hết, chúng ta sẽ xem xét một tính chất như sau.

Tính chất 1. *Cho a, b, và c là các hằng số dương. Các biến ngẫu nhiên X_i and Y_i là độc lập và phân bố theo hàm mũ với các giá trị trung bình lần lượt Ω_X và Ω_Y. Một biến ngẫu nghiên U được xác định bởi*

$$U = \max_{i \in \{1,2,\ldots,N\}} \left(\frac{aX_i}{bY_i + c} \right), \tag{2.24}$$

và có CDF và PDF, tương ứng được cho bởi

$$\begin{aligned} F_U(u) &= \left[1 - \frac{1}{\frac{b\Omega_Y}{a\Omega_X}u + 1} \exp\left(-\frac{uc}{a\Omega_X} \right) \right]^N \\ &= \sum_{q=0}^{N} \binom{N}{q} \frac{(-1)^q}{(Au+1)^q} \exp\left(-\frac{qu}{D} \right) \end{aligned} \tag{2.25}$$

$$f_U(u) = N \sum_{q=0}^{N-1} \binom{N-1}{q} (-1)^q \left[\frac{A \exp\left(-\frac{(1+q)u}{D} \right)}{(1+Au)^{q+2}} + \frac{\exp\left(-\frac{(1+q)u}{D} \right)}{D(1+Au)^{q+1}} \right] \tag{2.26}$$

trong đó $A = \frac{b\Omega_Y}{a\Omega_X}$ và $\frac{1}{D} = \frac{c}{a\Omega_X}$.

Chứng minh. Chứng minh chi tiết được trình bày trong tài liệu [30, *Lemma 1*]. □

2.2.1 Chính sách phân bổ công suất truyền tin

Để đưa ra được chính sách phân bổ công suất cho S-Tx, chúng ta cần tính toán xác suất dừng bảo mật của SU được đưa ra trong (2.10), xác suất dừng của PU trong công thức (2.11), và xác suất dừng trong (2.13).

2.2.1.1 Công suất truyền tin của S-Tx dưới ngưỡng can nhiễu của PU

Từ (2.14), chúng ta có thể tính toán $\mathcal{O}_I$ như sau

$$\begin{aligned}\mathcal{O}_I &= \Pr\left\{\max_{m\in\{1,2,\ldots,N_p\}}\left\{\frac{P_s\varphi_m}{N_0}\right\} \geq Q_{pk}\right\} \leq \xi \\ &= 1 - \Pr\left\{\max_{m\in\{1,2,\ldots,N_p\}}\{\varphi_m\} < \frac{Q_{pk}N_0}{P_s}\right\} \leq \xi \\ &= 1 - \left\{1 - \exp\left(-\frac{Q_{pk}N_0}{\Omega_\varphi P_s}\right)\right\}^{N_p} \leq \xi \end{aligned} \tag{2.27}$$

Sau một số bước tính toán toán học, ta có thể kết luận rằng công suất truyền tin của S-Tx cần phải thỏa mãn điều kiện ràng buộc dưới đây

$$P_s \leq \frac{Q_{pk}N_0}{\Omega_\varphi}\left(\log_e \frac{1}{1 - \sqrt[N_p]{1-\xi}}\right)^{-1} \tag{2.28}$$

2.2.1.2 Công suất truyền tin của S-Tx dưới điều kiện ràng buộc dừng bảo mật

Ở đây, chúng tôi giả sử rằng thiết bị EAV có thể có bộ lọc nhiễu môi trường tiên tiến và EAV chỉ bị ảnh hưởng bởi can nhiễu từ công suất phát tín hiệu của P-Tx. Nói một cách khác, chúng ta xem xét trường hợp xấu nhất khi nhiễu môi trường được loại bỏ một cách đáng kể và ảnh hưởng can nhiễu từ công suất truyền tin của PU cao hơn rất nhiều lần so với nhiễu môi trường. Do đó, SINR của EAV được trình bày trong (2.8) có thể được viết lại là

$$\gamma_e = \max_{n\in\{1,2,\ldots,N_e\}}\left\{\frac{P_s\alpha_n}{P_p\rho_n + N_0}\right\} \approx \max_{n\in\{1,2,\ldots,N_e\}}\left\{\frac{P_s\alpha_n}{P_p\rho_n}\right\} \tag{2.29}$$

Theo đó, chúng ta có thể thu được xác suất dừng bảo mật của SU như sau

$$\mathcal{O}_{sec} = 1 - \Pr\left\{\max_{n\in\{1,2,\ldots,N_e\}}\left\{\frac{\alpha_n}{\rho_n}\right\} \leq \frac{P_p}{P_s}\gamma_{th}^e\right\} \leq \epsilon \tag{2.30}$$

trong đó $\gamma_{th}^e = 2^{\frac{R_0}{B}} - 1$. Theo lý thuyết thông kê, chúng ta có được xác suất dừng bảo mật như sau

$$\begin{aligned}\mathcal{O}_{sec} &= 1 - \prod_{n=1}^{N_e}\int_0^\infty \Pr\left\{\alpha_n \leq \frac{P_p}{P_s}\gamma_{th}^E x\right\} f_{\rho_n}(x)dx \\ &= 1 - \left(1 - \frac{1}{\frac{P_p\Omega_\rho}{P_s\Omega_\alpha}\gamma_{th}^e + 1}\right)^{N_e} \leq \epsilon\end{aligned} \tag{2.31}$$

Sau một số tính toán toán học, chúng ta thu được công suất truyền tin tối đa của S-Tx dưới điều kiện ràng buộc về dung lượng bảo mật kênh của nó như sau

$$P_s \leq \frac{P_p\Omega_\rho\gamma_{th}^E}{\Omega_\alpha}\left(\frac{1}{\sqrt[N_e]{1-\epsilon}} - 1\right) \tag{2.32}$$

2.2.1.3 Công suất truyền tin của S-Tx dưới điều kiện xác suất dừng của PU

Từ (2.11), chúng ta có thể tính toán xác suất dừng của PU như sau

$$\mathcal{O}_p = \Pr\left\{\max_{m\in\{1,2,\ldots,N_p\}}\left\{\frac{P_p h_m}{P_s\varphi_m + N_0}\right\} \leq \gamma_{th}^p\right\} \leq \theta \tag{2.33}$$

trong đó $\gamma_{th}^p = 2^{\frac{R_p}{B}} - 1$. Sử dụng sự hỗ trợ từ (2.25) trong tính chất 1 cho (2.33) bằng cách thiết lập các giá trị $a = P_p$, $b = P_s$, $c = N_0$, $\Omega_X = \Omega_h$, $\Omega_Y = \Omega_\varphi$, và $u = \gamma_{th}^p$, chúng ta thu được một biểu thức tường minh cho xác suất dừng của PU là

$$\mathcal{O}_p = \left[1 - \frac{1}{\frac{P_s\Omega_\varphi}{P_p\Omega_h}\gamma_{th}^p + 1}\exp\left(-\frac{\gamma_{th}^p N_0}{P_p\Omega_h}\right)\right]^{N_p} \leq \theta \tag{2.34}$$

Sau một số phép biến đổi toán học, chúng ta có được công suất truyền tin tối đa của SU-Tx như sau

$$P_s \leq \frac{P_p\Omega_h}{\gamma_{th}^p\Omega_\varphi}\Xi \tag{2.35}$$

trong đó Ξ được định nghĩa là

$$\Xi = \max\left\{0, \frac{1}{1-\sqrt[N_p]{\theta}} \exp\left[-\frac{\gamma_{th}^{p} N_0}{P_p \Omega_h}\right] - 1\right\} \tag{2.36}$$

2.2.1.4 Chính sách phân bổ công suất cho các kịch bản

Như vậy, chúng ta đã có thể thu được các chính sách phân bổ công suất truyền tin cho bốn kịch bản như sau:

- Đầu tiên, chính sách phân bổ công suất cho kịch bản S_1 nhận được bằng cách kết hợp (2.15) với (2.28) là

$$\mathcal{P}_{S_1} = \min\left\{\frac{Q_{pk} N_0}{\Omega_\varphi}\left(\log_e \frac{1}{1-\sqrt[N_p]{1-\xi}}\right)^{-1}, P_s^{max}\right\} \tag{2.37}$$

- Thứ hai, chúng ta thu được chính sách phân bổ công suất cho kịch bản S_2 bằng cách kết hợp (2.18), (2.28), với (2.32) như sau

$$\mathcal{P}_{S_2} = \min\left\{\frac{Q_{pk} N_0}{\Omega_\varphi}\left(\log_e \frac{1}{1-\sqrt[N_p]{1-\xi}}\right)^{-1}, \frac{P_p \Omega_\rho \gamma_{th}^{e}}{\Omega_\alpha}\left(\frac{1}{\sqrt[N_e]{1-\epsilon}} - 1\right), P_s^{max}\right\} \tag{2.38}$$

- Thứ ba, công suất truyền tin của S-Tx cho kịnh bản S_3 đạt được bằng việc kết hợp (2.20) với (2.35). Ta có

$$\mathcal{P}_{S_3} = \min\left\{\frac{P_p \Omega_h}{\gamma_{th}^{p} \Omega_\varphi} \Xi, P_s^{max}\right\} \tag{2.39}$$

  trong đó Ξ được định nghĩa trong (2.36) là

$$\Xi = \max\left\{0, \frac{1}{1-\sqrt[N_p]{\theta}} \exp\left[-\frac{\gamma_{th}^{p} N_0}{P_p \Omega_h}\right] - 1\right\} \tag{2.40}$$

- Cuối cùng, công suất truyền của S-Tx cho kịnh bản S_4 được thành lập bằng việc kết hợp các công thức (2.20), (2.35) với (2.32) như sau

$$\mathcal{P}_{S_4} = \min\left\{\frac{P_p \Omega_\rho \gamma_{th}^{e}}{\Omega_\alpha}\left(\frac{1}{\sqrt[N_e]{1-\epsilon}} - 1\right), \frac{P_p \Omega_h}{\gamma_{th}^{p} \Omega_\varphi} \Xi, P_s^{max}\right\} \tag{2.41}$$

Theo đó, thuật toán phân bổ công suất tương ứng với bốn kich bản nói trên được trình bày trong **Algorithm 1** dưới đây.

Algorithm 1 Thuật toán cho chính sách phân bổ công suất.

function PAP()
  INITIALIZE(); ▷ Khởi tạo các tham số hệ thống
  $\Xi = \max\left\{0, \frac{1}{1-\sqrt[N_p]{\theta}} \exp\left[-\frac{\gamma_{th}^{p} N_0}{P_p \Omega_h}\right] - 1\right\}$;
  /* Scenario S_4 */
  if S-Tx có CSI của cả P-Tx→P-Rx và S-Tx→EAV **then**
    $\mathcal{P}_S = \min\left\{\frac{P_p \Omega_\rho \gamma_{th}^{e}}{\Omega_\alpha}\left(\frac{1}{\sqrt[N_e]{1-\epsilon}} - 1\right), \frac{P_p \Omega_h}{\gamma_{th}^{p} \Omega_\varphi}\Xi, P_s^{max}\right\}$;
    return $\mathcal{P}_S$;
  end if
  /* Scenario S_3 */
  if S-Tx có CSI của P-Tx→P-Rx nhưng không có CSI của S-Tx→EAV **then**
    $\mathcal{P}_S = \min\left\{\frac{P_p \Omega_h}{\gamma_{th}^{p} \Omega_\varphi}\Xi, P_s^{max}\right\}$;
    return $\mathcal{P}_S$;
  end if
  /* Scenario S_2 */
  if S-Tx có CSI của S-Tx→EAV nhưng không có CSI của P-Tx→P-Rx **then**
    $\mathcal{P}_S = \min\left\{\frac{Q_{pk} N_0}{\Omega_\varphi}\left(\log_e \frac{1}{1-\sqrt[N_p]{1-\xi}}\right)^{-1}, \frac{P_p \Omega_\rho \gamma_{th}^{e}}{\Omega_\alpha}\left(\frac{1}{\sqrt[N_e]{1-\epsilon}} - 1\right), P_s^{max}\right\}$;
    return $\mathcal{P}_S$;
  end if
  /* Scenario S_1 */
  if S-Tx không có CSI của cả P-Tx→P-Rx và S-Tx→EAV **then**
    $\mathcal{P}_S = \min\left\{\frac{Q_{pk} N_0}{\Omega_\varphi}\left(\log_e \frac{1}{1-\sqrt[N_p]{1-\xi}}\right)^{-1}, P_s^{max}\right\}$;
    return $\mathcal{P}_S$;
  end if
end function

2.2.2 Xác suất truyền thông tin cậy và bảo mật

Như đã trình bày ở trên, xác suất truyền thông tin cậy và bảo mật được định nghĩa là xác suất mà SU-Tx có thể truyền thông hiệu quả với SU-Rx mà không bị lộ thông tin đối với EAV đồng thời không làm ảnh hưởng đến hiệu suất hoạt động của PU. Với các chính sách phân bổ công suất thu được và các kênh truyền là độc lập với nhau, chúng ta có thể viết lại xác suất truyền thông tin cậy và bảo mật trong (2.12) bằng

$$\begin{aligned}\mathcal{O}_{ss} &= \Pr\{C_s > R_s\}\Pr\{C_e \leq R_0\} \\ &= (1-\mathcal{O}_s)(1-\mathcal{O}_{sec})\end{aligned} \tag{2.42}$$

trong đó $\mathcal{O}_s$ và $\mathcal{O}_{sec}$ có được bằng cách sử dụng hỗ trợ của tính chất 1, do đó

$$\mathcal{O}_s = \sum_{i=0}^{N_s} \binom{N_s}{i} \frac{(-1)^i}{(A_s\gamma_{th}^s+1)^i} \exp\left(-\frac{i\gamma_{th}^s}{D_s}\right) \tag{2.43}$$

$$\mathcal{O}_{sec} = 1 - \sum_{j=0}^{N_e} \binom{N_e}{j} \frac{(-1)^j}{(A_e\gamma_{th}^e+1)^j} \tag{2.44}$$

trong đó $\gamma_{th}^s = 2^{\frac{R_s}{B}} - 1$, $A_s = \frac{P_p\Omega_\beta}{\mathcal{P}\Omega_g}$, $A_e = \frac{P_p\Omega_\rho}{\mathcal{P}\Omega_\alpha}$,and $\frac{1}{D_s} = \frac{N_0}{\mathcal{P}\Omega_g}$.

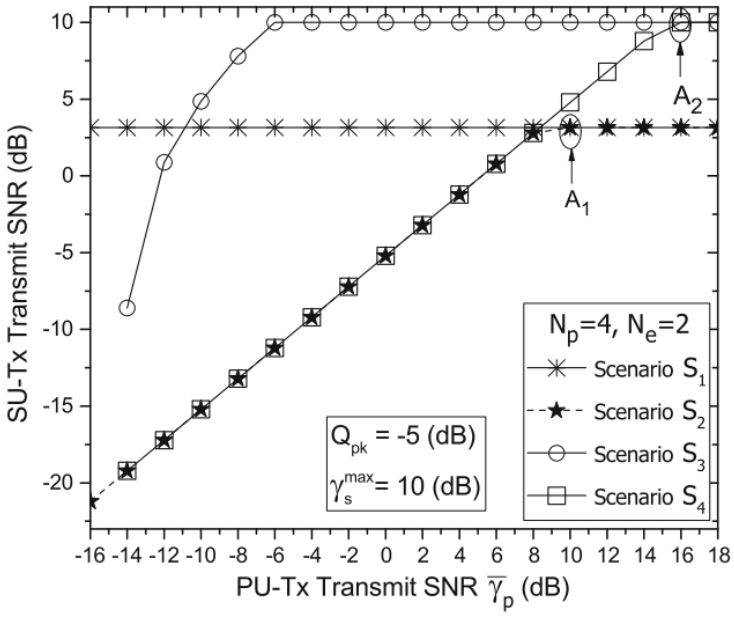
Cuối cùng, một biểu thức tường minh của một xác suất truyền thông tin cậy và bảo mật đạt được bằng cách thay thế (2.43) và (2.44) vào trong (2.42), trong đó $\mathcal{P} \in \{\mathcal{P}_{S_1}, \mathcal{P}_{S_2}, \mathcal{P}_{S_3}, \mathcal{P}_{S_4}\}$ là tập các chính sách phân bổ công suất truyền tin của SU.

2.3 Mô phỏng hệ thống

Trong phần này, tác giả trình bày các số liệu thử nghiệm mô phỏng để đánh giá các chính sách phân bổ công suất và SRCP cho mô hình đang khảo sát. Để hiểu rõ hơn, chúng tôi thực hiện so sánh giữa kịch bản S1 và kịch bản S2, kịch bản S3 và kịch bản S4. Trong kết quả mô phỏng này, chúng tôi giả định rằng S-Tx, S-Rx, P-Rx, EAV, and P-Tx được lần lượt đặt tại các vị trí $(0,0)$, $(-1,2)$, $(0.5,1)$, $(0,2.5)$, và $(0,2)$ trên mặt phẳng 2D. Các tham số cài đặt dưới đây trong các số liệu thử nghiệm đã được dùng tương tự và phổ biến trong rất nhiều các nghiên cứu ở lĩnh vực này như [16,33]:

- Băng thông hệ thống: B= 5 MHz;
- Tốc độ xác định của SU: R_s=128 Kbps;
- Tốc độ xác định của PU: R_p=64 Kbps;
- Tốc độ của thông tin bảo mật của SU tại EAV: R_e=64 Kbps;
- hệ số mũ suy hao đường truyền (Pathloss exponent) $\nu = 4$;
- Điều kiện xác suất dừng của PU và SU: $\theta = \xi = 0.01$;
- Điều kiện xác suất dừng của EAV: $\epsilon = 0.1$;
- SNR tối đa của S-Tx: $\gamma_s^{\max} = 10$ (dB);
- Mức can nhiễu tối đa của PU: $Q_{pk} = -5$ (dB)

Không mất tính tổng quát, chúng ta biểu diễn $\bar{\gamma}_s = \frac{\mathcal{P}}{N_0}$ và $\bar{\gamma}_p = \frac{P_p}{N_0}$ lần lượt là SNR của S-Tx và P-Tx khi thực hiện truyền tín hiệu. Hình 2.2 cho thấy SNR

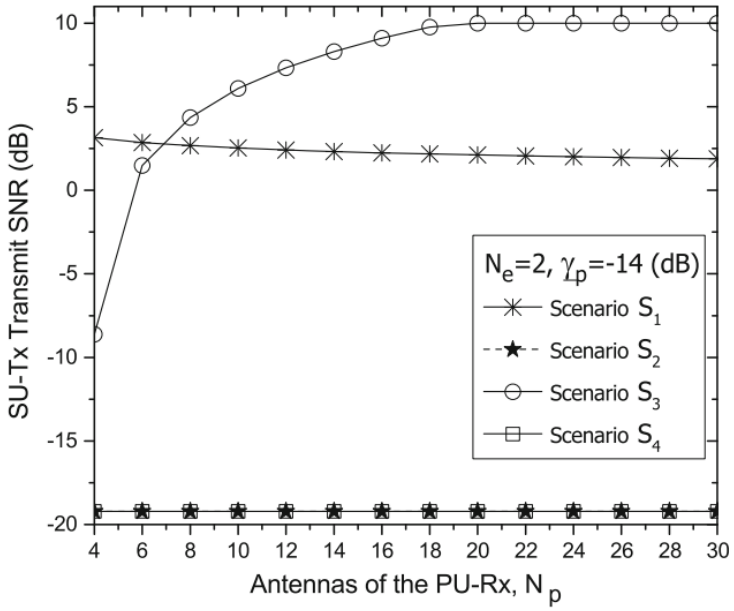


Hình 2.2: *SNR của S-Tx cho bốn kịch bản so với SNR của P-Tx*

của S-Tx là một hàm của SNR của P-Tx. Đầu tiên, chúng ta quan sát trạng thái SNR của S-Tx trong hai kịch bản S_1 và S_2, và có thể thấy rằng SNR của S-Tx trong kịnh bản S_1 là hằng số trong toàn bộ miền giá trị của SNR của P-Tx. Kết

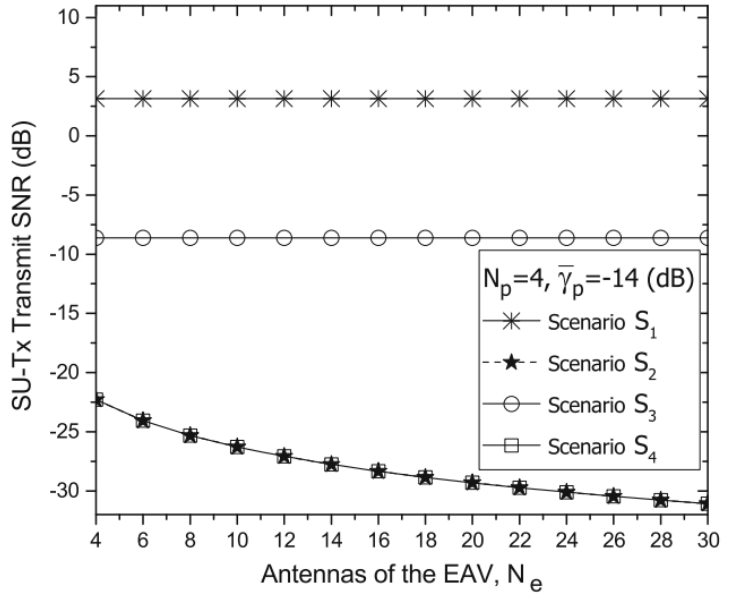
quả này phù hợp với công thức (2.37)khi mà SNR của S-Tx không phụ thuộc vào SNR của P-Tx. Ngược lại với kịch bản S_1, S-Tx tăng tuyến tính với sự gia tăng của SNR của S-Tx trong kịch bản S2. Tuy nhiên, khi SNR của P-Tx tăng vượt quá 10 dB (A_1), SNR của S-Tx bão hòa. Hiện tượng này có thể được giải thích là do SNR của S-Tx được phân bổ bằng công thức (2.38). Vì vậy, trong đoạn giá trị $[-16, 10]$ dB, SNR của S-Tx được điều khiển bởi điều kiện ràng buộc của EAV. Tuy nhiên, nếu mức SNR của P-Tx tăng thêm, SNR của S-Tx phải chịu phụ thuộc vào giá trị nhỏ nhất của giới hạn đầu tiên và giới hạn thứ ba trong công thức (2.38), tức là, trong phạm vi mức SNR cao của P-Tx, SNR của S-Tx tương tự như trong kịch bản S_1. Một vấn đề dễ hiểu nữa là SNR của S-Tx trong kịch bản S_2 luôn nhỏ hơn hoặc bằng với kịch bản S_1 do SNR của S-Tx trong S_2 phải chịu thêm điều kiện ràng buộc, đó là ràng buộc dừng của EAV. Tiếp theo, chúng ta quan sát tiếp trạng thái SNR của S-Tx trong kịch bản S_3 và S_4. Có thể thấy rằng SNR của S-Tx trong kịch bản S_4 luôn nhỏ hơn so với kịch bản S_3. Tuy nhiên, ở vùng giá trị mức SNR cao của P-Tx, ví dụ: $\bar{\gamma}_p \geq 16$ dB, chúng bằng nhau và bão hòa tại A_2. Hiện tượng này là do SNR của S-Tx trong kịch bản S_4 chịu nhiều điều kiện ràng buộc hơn so với kịch bản S_3, ở đây là điều kiện ràng buộc bởi EAV. Cuối cùng, chúng ta có thể kết luận rằng sự xuất hiện của EAV dẫn đến chính sách phân bổ công suất của S-Tx phức tạp hơn và có thể làm giảm hiệu suất hoạt động của SU.

Hình 2.3 biểu diễn SNR của S-Tx như là một hàm các ăng-ten của P-Tx, N_p. Chúng ta có thể thấy rằng SNR của S-Tx trong các kịch bản S_1 và S_3 cao hơn nhiều so với ở trong kịch bản S_2 và S_4. Điều này xảy ra với nguyên nhân tương tự như trong Fig. 2.2, cụ thể là, khi S-Tx chịu thêm điều kiện ràng buộc bổ sung của EAV dẫn đến SNR của S-Tx bị suy giảm. Ngoài ra, khi số lượng ăng-ten của P-Rx tăng lên, SNR của S-Tx trong kịch bản S_1 giảm nhẹ. Đó là do thực tế khi tăng số lượng ăng-ten của P-Rx dẫn đến giới hạn trong các ràng buộc cho S-Tx cũng tăng theo. Do đó, S-Tx phải giảm mức SNR của nó để không gây can nhiễu có hại cho P-Rx (xem công thức (2.13)). Một điều thú vị ở đây là SNR của các kịch bản S_2 và S_4 giống nhau cho toàn bộ miền giá trị của N_p. Điều này là do trong các điều kiện ràng buộc thì điều kiện của EAV là mạnh nhất (xem công thức (2.32)). Do đó, SNR của S-Tx dưới điều kiện ràng buộc



Hình 2.3: *Ảnh hưởng của số lượng ăng-ten của P-Tx lên SNR của S-Tx*

của EAV trở thành giá trị nhỏ nhất trong cả hai công thức (2.38) và (2.41) trong miền giá trị được khảo sát của N_p, tức là, $\mathcal{P}_{S_2} = \mathcal{P}_{S_4} = \frac{P_p \Omega_\rho \gamma_{th}^E}{\Omega_\alpha} \left(\frac{1}{\sqrt[N_e]{1-\epsilon}} - 1 \right)$.

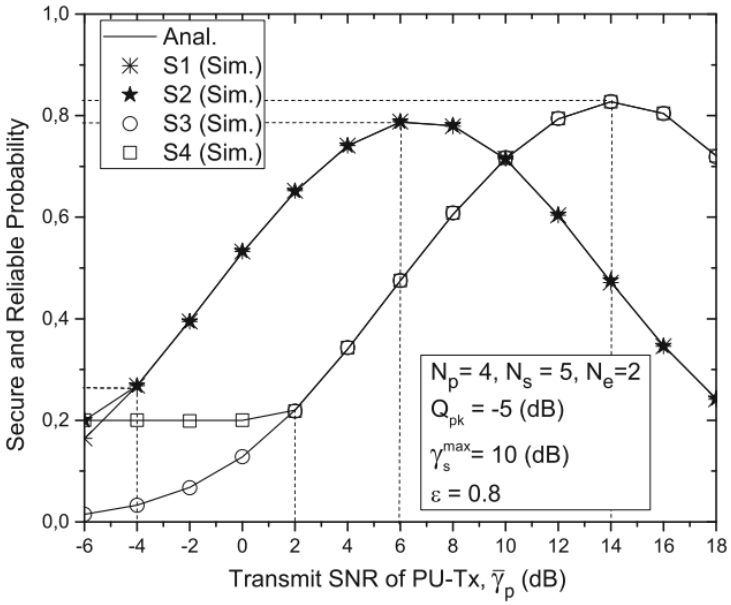


Hình 2.4: *Ảnh hưởng của số lượng ăng-ten của EAV lên SNR của S-Tx*

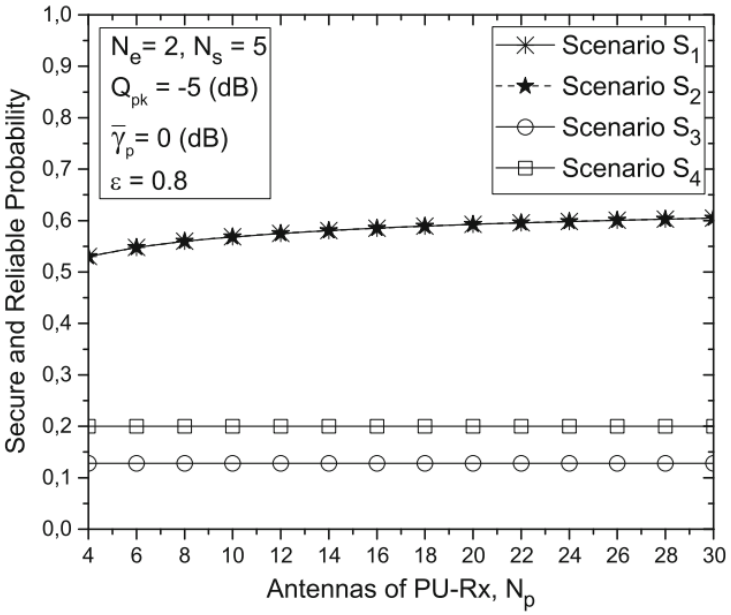
Hình 2.4 cho ta thấy tác động của số lượng ăng-ten của EAV lên SNR của S-Tx. Thứ nhất, chúng ta quan sát trạng thái SNR của S-Tx trong các kịch bản

S_1 và S_3 và thấy rằng SNR của S-Tx không thay đổi theo sự thay đổi của N_e. Điều này là do S-Tx không biết đến sự tồn tại của EAV. Tuy nhiên, khi S-Tx biết sự tồn tại của EAV như trong các kịch bản S_2 và S_4, SNR của S-Tx giảm đáng kể khi số lượng ăng-ten của EAV tăng lên. Điều này là do thực tế việc tăng số lượng ăng-ten của EAV dẫn đến làm tăng khả năng nghe trộm của EAV. Kết quả là, S-Tx trong các kịch bản S_2 và S_4 phải giảm mức SNR của nó để đảm bảo an toàn cho truyền thông.

Trong hình 2.5, chúng ta thấy ảnh hưởng của SNR lên CRCP của SU. Chúng ta có thể quan sát được rằng SRCP của kịch bản S_2 (kịch bản S_4) luôn luôn tốt hơn trong kịnh bản S_1 (kịch bản S_3) trong miền giá trị thấp của SNR của P-Tx, $\bar{\gamma}_p \leq -4$ dB ($\bar{\gamma}_p \leq 2$ dB). Tuy nhiên, khi SNR của P-Tx tăng thêm, SRCP của kịch bản S_1 và S_2 (kịnh bản S_3 và S_4) là giống nhau từng đôi một. Điều này là do khi P-Tx truyền tín hiệu với SNR ở mức thấp, SNR của S-Tx trong kịch bản S_1 (kịch bản S_3) lớn hơn so với kịch bản S_2 (kịch bản S_4). Do đó, xác suất bảo mật của SU giảm đáng kể, trong khi xác suất truyền thông an toàn không khác nhiều. Kết quả là, SRCP của kịch bản S_1 (kịch bản S_3) nhỏ hơn so với kịch bản S_2 (kịch bản S_4) (xem công thức (2.42)). Khi SNR của P-Tx tăng thêm, ví dụ 2 (dB) $\leq \bar{\gamma}_p \leq 14$ (dB), S-Tx có thể điều chỉnh công suất phát của nó đến giá trị cực đại trong mọi kịnh bản. Điều này dẫn đến SRCP trong các kịch bản S_1 và S_2 (kịch bản S_3 và S_4) là như nhau. Điều thú vị nhất ở đây là ở miền giá trị cao của SNR của P-Tx, SRCP cho các kịch bản S_1 và S_2 (kịch bản S_3 và S_4), ví dụ $\bar{\gamma}_p \geq 6$ (dB) or $\bar{\gamma}_p \geq 14$ (dB) bị suy giảm. Điều này là do thực tế ở miền giá trị thấp của SNR của P-Tx, S-Tx có thể điều chỉnh SNR của nó để đáp ứng các điều kiện ràng buộc đã cho. Tuy nhiên, khi mức SNR của P-Tx tăng thêm, nó sẽ trở thành nguồn gây can nhiễu mạnh cho S-Rx, dẫn đến làm suy giảm SRCP của SU. Trong hình 2.6, chúng tôi đã chỉ ra được tác động của số lượng ăng-ten của P-Rx lên SRCP của SU. Các SRCP giống nhau và tăng nhẹ đối với các kịnh bản S_1 và S_2. Điều này có thể được giải thích là do P-Rx có thể chịu được nhiều can nhiễu hơn từ S-Tx vì số lượng ăng-ten của nó tăng lên nên khả năng thu nhận tín hiệu được tăng cường. Vì vậy cho nên, S-Tx có thể tăng công suất phát của nó để nâng cao SRCP. Tuy nhiên, dưới điều kiện ràng buộc của mức can nhiễu tối đa Q_{pk}, điều kiện xác suất dừng

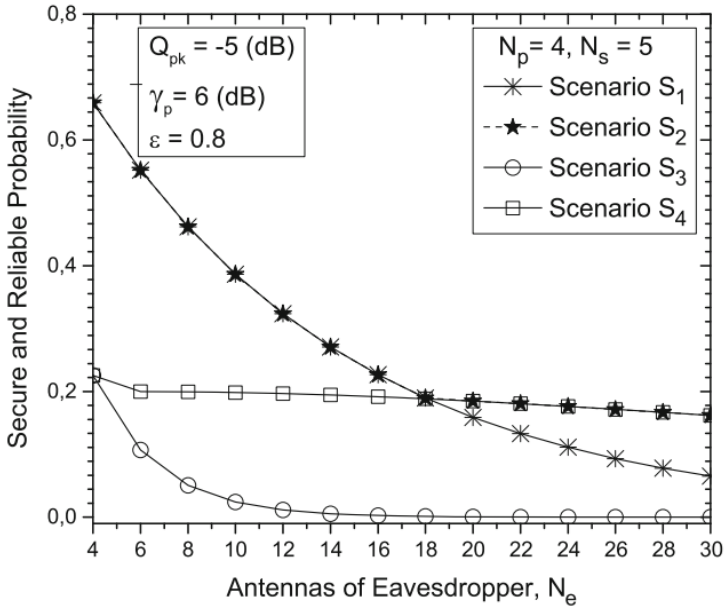


Hình 2.5: *SRCP theo SNR của P-Tx với* $\epsilon = 0.8$.



Hình 2.6: *Ảnh hưởng của số lượng ăng-ten của P-Tx lên SRCP của S-Tx.*

ξ, cũng như điều kiện dừng bảo mật ϵ, công suất phát của S-Tx là giống nhau cho cả hai kịnh bản S_1 và S_2. Do đó, SRCP cũng giống nhau với hai kịnh bản này. Ngược lại với kịch bản S_1 và S_2, SRCP trong kịch bản S_4 vượt trội so với kịch bản S_3. Điều này có được là do S-Tx trong kịch bản S_3 không biết đến sự tồn tại của EAV, do đó nó có thể truyền với công suất phát tối đa và thông tin



Hình 2.7: *Ảnh hưởng của số lượng ăng-ten của EAV lên lên SRCP của S-Tx.*

liên lạc của nó có thể bị khai thác bởi EAV. Trong trường hợp của kịch bản S_4, S-Tx biết sự tồn tại của EAV, do đó nó điều chỉnh công suất phát của nó để không tiết lộ thông tin cho EAV. Theo đó, SRCP trong kịch bản S_4 tốt hơn so với kịch bản S_3.

Cuối cùng, chúng ta xem xét tác động của số lượng ăng-ten của EAV lên SRCP của SU như trong hình 2.7. Có thể thấy rằng SRCP cho các kịch bản S_1 và S_3, nơi mà các điều kiện ràng buộc bảo mật không được xem xét, bị suy giảm nhanh chóng. Trong trường hợp khác, SRCP trong các kịnh bản S_2 và S_4, nơi mà điều kiện bảo mật được tích hợp, giảm dần. Rõ ràng, trong các kịch bản mà hệ thống SU có thông tin CSI của EAV, có thể làm cho việc truyền thông của SU bảo mật và đáng tin cậy hơn.

2.4 Kết luận

Trong chương này, nhóm nghiên cứu đã nghiên cứu giải pháp làm thế nào để có được truyền thông tin cậy và bảo mật cho mạng CRN mà trong đó truyền thông của mạng thứ cấp (SU) có thể bị nghe trộm bởi EAV. Với các điều kiện ràng buộc của PU, EAV và SU, chúng ta thu được bốn chính sách

phân bổ công suất truyền tin tương ứng với bốn kịch bản khác nhau tùy thuộc vào từng trường hợp hệ thống thu nhận được thông tin CSI khác nhau trong mạng. Từ đó, một chỉ số đo hiệu suất về xác suất truyền thông tin cậy và bảo mật được tác giả để xuất để đánh giá hiệu suất hệ thống. Các số liệu của kết quả phân tích và mô phỏng đã thể hiện được tính đúng đắn của độ đo hiệu suất bảo mật hệ thống và chứng minh tính chính xác của các kết quả phân tích của hệ thống.

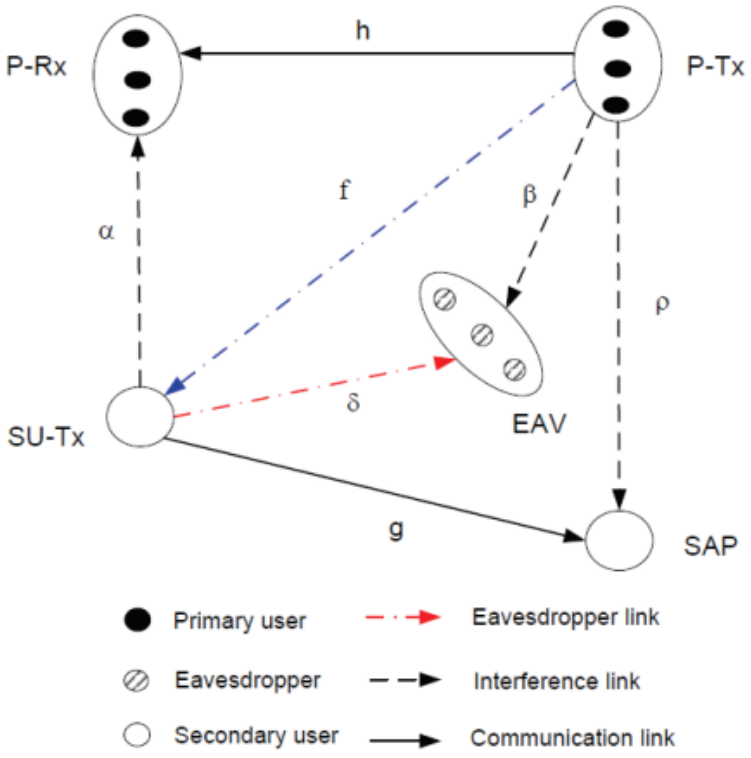
Chương 3

ĐÁNH GIÁ HIỆU SUẤT HOẠT ĐỘNG DỰA TRÊN THỜI GIAN THU HOẠCH NĂNG LƯỢNG VÀ CHÍNH SÁCH CÔNG SUẤT CHO MẠNG CRN DƯỚI ĐIỀU KIỆN BẢO MẬT THÔNG TIN

3.1 Mô hình hệ thống

3.1.1 Mô hình hệ thống mạng

Chúng ta xem xét một mạng CRN dạng dưới ngưỡng nhiễu như hình 3.1, trong đó có N thiết bị PU đang hoạt động trên các dải tần số trực giao. Thiết bị S-Tx thu hoạch năng lượng từ N thiết bị phát P-Tx và sau đó sử dụng năng lượng thu hoạch này để truyền các gói tin tới điểm truy cập (SAP). Bên cạnh đó, tồn tại K thiết bị EAV nghe trộm các thông tin được truyền từ S-Tx đến SAP. Trong mô hình này, SAP được giả định được trang bị M ăng-ten trong khi các thiết bị khác (P-Tx, P-Rx, EAV, và S-Tx) có một ăng-ten đơn. Độ lợi của các kênh truyền thông P-Tx$_n$→P-Rx$_n$ và S-Tx→SAP được kí hiệu là h_n, và g_m, $n = 1, \ldots, N$, $m = 1, \ldots, M$. Độ lợi kênh g_m biểu diễn cho kênh từ S-Tx đến nhánh m-ăngten của SAP. Độ lợi kênh của các kênh can nhiễu P-Tx$_n$→EAV$_k$, S-Tx→P-Rx$_n$, P-Tx$_n$→SAP được kí hiệu lần lượt bởi β_{nk}, α_n, và ρ_{nm}. Độ lợi kênh của kênh wiretap S-Tx→EAV và kênh thu hoạch năng lượng P-Tx$_n$→S-Tx được biểu diễn tương ứng là δ_k và f_n, $k \in \{1, \ldots, K\}$. Với giả định rằng tất cả các kênh được mô hình hóa dưới dạng kênh fading phẳng có phân bố Rayleigh, và các độ lợi kênh là các biến ngẫu nhiên độc lập và phân bố theo hàm mũ. Do đó, chúng có hàm mật độ xác suất (PDF) và hàm phân bố tích



Hình 3.1: *Mô hình mạng CRN dạng nền, trong đó S-Tx sử dụng năng lượng thu được từ các P-Tx để truyền thông trong môi trường nhiều EAV.*

lũy (CDF) được biểu diễn dưới dạng sau

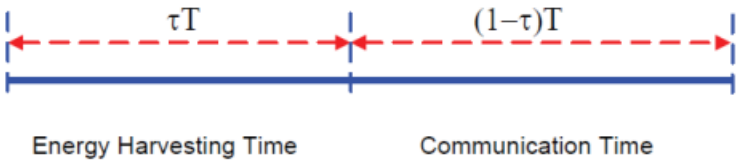
$$f_X(x) = \frac{1}{\Omega_X} \exp\left(-\frac{x}{\Omega_X}\right) \tag{3.1}$$

$$F_X(x) = 1 - \exp\left(-\frac{x}{\Omega_X}\right) \tag{3.2}$$

trong đó các biến ngẫu nhiên $X \in \{g_m, h_n, f_n, \alpha_n, \delta_k, \beta_{nk}, \rho_{nm}\}$, tham chiếu đến độ lợi kênh, và $\Omega_X = \mathbf{E}[X]$ là độ lợi kênh trung bình, tức là, $\Omega_g = \mathbf{E}[g_m]$, $\Omega_{h_n} = \mathbf{E}[h_n]$, $\Omega_{\alpha_n} = \mathbf{E}[\alpha_n]$, $\Omega_\delta = \mathbf{E}[\delta_k]$, $\Omega_{\beta_n} = \mathbf{E}[\beta_{nk}]$, $\Omega_{\rho_n} = \mathbf{E}[\rho_{nm}]$.

3.1.2 Cơ chế truyền thông và thu hoạch năng lượng

Ý tưởng cơ bản của thu hoạch năng lượng sóng vô tuyến trong mạng vô tuyến nhận thức là các thiết bị phát thứ cấp (S-Tx) có thể chuyển đổi công suất phát tín hiệu của các thiết bị phát sơ cấp (P-Tx) vốn được coi là can nhiễu gây hại cho các thiết bị mạng thứ cấp, thành năng lượng hữu ích cho truyền thông của mạng thứ cấp.



Hình 3.2: *Một khung thời gian T được sử dụng để thu hoạch năng lượng và truyền thông.*

Tổng thời gian được sử dụng cho thu hoạch năng lượng và truyền thông được mô tả như trong hình 3.2. Khung thời gian, kí hiệu là T, được sử dụng để SU thu hoạch năng lượng và truyền thông tin. τT là thời gian sử dụng để thu hoạch năng lượng từ các P-Tx, trong khi thời gian còn lại $(1-\tau)T$ là truyền các gói tin đến SAP. Theo đó, giao thức truyền thông được thực hiện theo 2 bước như sau:

- Bước 1: S-Tx thu hoạch năng lượng của N thiết bị P-Tx thông qua N kênh không dây f_n, $n \in \{1, 2, \ldots, N_e\}$. Năng lượng thu hoạch trung bình tại S-Tx có thể được biểu diễn như sau:

$$E_s = \mathbf{E}\left[\sum_{n=1}^{N} \theta\tau T P_p f_n\right] = \theta\tau T P_p \,\mathbf{E}\left[\sum_{n=1}^{N} f_n\right] \tag{3.3}$$

  trong đó $\mathbf{E}[\cdot]$, T, và τ lần lượt là kỳ vọng, tổng khung thời gian, và một phần của khung thời gian được sử dụng để thu hoạch năng lượng sóng vô tuyến, $0 < \tau < 1$. Kí hiệu P_p và θ đại diện cho công suất phát tín hiệu của P-Tx và hệ số hiệu suất thu hoạch năng lượng của S-Tx, $0 \leq \theta \leq 1$.

- Bước 2: Sau quá trình thu hoạch năng lượng, S-Tx cũng hoàn thành nhiệm vụ ước tính các thông số của trạng thái kênh truyền (CSI), và nó có thể biết băng tần nào tốt nhất cho truyền thông của SU. Ở đây, kênh tốt nhất là kênh mà cho phép S-Tx sử dụng tối đa công suất phát tín hiệu để nâng cao hiệu suất. Chú ý rằng công suất phát tín hiệu của S-Tx trong khoảng thời gian còn lại $(1-\tau)T$ và tại kênh n-th cụ thể bị hạn chế bởi năng lượng thu hoạch được E_s, nghĩa là, $P_{S-Tx}^{(n)}(1-\tau)T \leq E_s$. Do đó, chúng ta có

$$P_{S-Tx}^{(n)} \leq P_{avg} = \frac{E_s}{(1-\tau)T} = \frac{\tau\theta P_p}{1-\tau}\sum_{n=1}^{N}\Omega_{f_n} \tag{3.4}$$

trong đó P_{avg} được gọi là ngưỡng công suất trung bình được đưa ra bởi S-Tx. Dựa trên cơ sở này, chính sách phân bổ công suất và quá trình lựa chọn kênh cho SU có thể được tìm thấy.

3.2 Phân bổ công suất và lựa chọn kênh của SU

Để truyền các gói tin cho SAP. Đầu tiên, S-Tx tính toán chiến lược phân bổ công suất trong mỗi kênh để đảm bảo điều kiện ràng buộc về chất lượng dịch vụ (QoS) của PU và không để lộ thông tin bí mật của nó cho các EAV.

3.2.1 Giới hạn công suất của S-Tx dưới điều kiện ràng buộc của PU

Vì SU sử dụng một trong N kênh được cấp phép cho mạng sơ cấp, nên chính sách điều khiển công suất của nó phải được thiết kế để không can nhiễu có hại cho PU trong khi có thể đạt được mức công suất phát tối đa để nâng cao hiệu suất. Điều này có thể được diễn giải trong điều kiện xác suất dừng η_p được đưa ra bởi PU và ngưỡng công suất trung bình của S-Tx như sau:

$$\Pr\left\{C_p^{(n)} \leq R_p\right\} \leq \eta_p \tag{3.5}$$

$$P_{S-Tx}^{(n)} \leq P_{avg} \tag{3.6}$$

trong đó R_p, η_p, và P_{avg} lần lượt là tốc độ xác định, điều kiện dừng của PU, và điều kiện công suất trung bình của S-Tx. Kí hiệu $C_p^{(n)}$ là dung lượng kênh của SU tại băng tần n-th, và được định nghĩa là

$$C_p^{(n)} = B\log_2\left(1+\gamma_p^{(n)}\right) \tag{3.7}$$

trong đó B là băng thông và $\gamma_p^{(n)}$ là SINR của PU được cho bởi

$$\gamma_p^{(n)} = \frac{P_p h_n}{P_{S-Tx}^{(n)}\alpha_n + N_0} \tag{3.8}$$

trong đó kí hiệu N_0 là công suất nhiễu nền.

Bằng cách thay thế (3.8) và (3.7) vào (3.5), chúng ta có thể viết lại (3.5) như sau

$$\Pr\left\{\frac{P_p h_n}{P_{S-Tx}^{(n)}\alpha_n + N_0} \leq \gamma_{th}^p\right\} \leq \eta_p \tag{3.9}$$

trong đó $\gamma_{th}^p = 2^{\frac{R_p}{B}} - 1$. Tiếp theo, sử dụng [86, Property 1], biểu thức (3.9) được tính toán ra như sau

$$1 - \frac{P_p \Omega_{h_n}}{P_{S-Tx}^{(n)}\Omega_{\alpha_n}\gamma_{th}^p + P_p\Omega_{h_n}} \exp\left(-\frac{\gamma_{th}^p N_0}{P_p\Omega_{h_n}}\right) \leq \eta_p \tag{3.10}$$

Bằng cách đặt $A_n = \frac{\gamma_{th}^p \Omega_{\alpha_n}}{P_p\Omega_{h_n}}$, $B_n = \frac{\gamma_{th}^p N_0}{P_p\Omega_{h_n}}$, chúng ta có thể viết lại (3.10) là

$$P_{S-Tx}^{(n)} \leq \frac{1}{A_n}\left[\frac{\exp(-B_n)}{1-\eta_p} - 1\right] \tag{3.11}$$

Kết hợp (3.11) với (3.6), công suất phát tín hiệu của S-Tx cần thỏa mãn cả hai điều kiện là điều kiện dừng của PU và năng lượng thu được của nó như sau

$$P_{S-Tx}^{(n)} \leq \min\left\{P_{PU}^{(n)}, P_{avg}\right\} \tag{3.12}$$

trong đó $P_{PU}^{(n)}$ có được từ

$$P_{PU}^{(n)} = \frac{1}{A_n}\left[\frac{\exp(-B_n)}{1-\eta_p} - 1\right] \tag{3.13}$$

3.2.2 Giới hạn công suất của S-Tx dưới các yêu cầu bảo mật thông tin đối với nhiều EAV

Sự bảo mật thông tin trong truyền thông của SU trong mô hình bị đe dọa bởi K thiết bị EAV. Do đó, S-Tx cần điều chỉnh công suất của nó để tránh bị EAV giải mã được thông tin. Các yêu cầu này có thể được diễn giải bằng điều kiện dừng bảo mật và điều kiện công suất phát tín hiệu của S-Tx như sau

$$\Pr\left\{\max_{k\in\{1,\ldots,K\}}\left\{C_e^{(n,k)}\right\} \geq R_e\right\} \leq \xi \tag{3.14}$$

$$P_{S-Tx}^{(n)} \leq P_{avg} \tag{3.15}$$

trong đó R_e và ξ lần lượt là tốc độ bảo mật xác định và điều kiện dừng bảo mật. Kí hiệu $C_e^{(n,k)}$ biểu diễn dung lượng của EAV_k trên kênh S-Tx$\rightarrow\text{EAV}_k$ khi S-Tx lựa chọn băng tần n để truyền tin, được định nghĩa là

$$C_e^{(n,k)} = B\log_2\left(1+\gamma_e^{(n,k)}\right) \tag{3.16}$$

trong đó $\gamma_e^{(n,k)}$ là SINR của EAV_k tại băng tần n-th, và nó có thể xấp xỉ bằng

$$\gamma_e^{(n,k)} = \frac{P_{S-Tx}^{(n)}\delta_k}{P_p\beta_{nk}+N_e} \approx \frac{P_{S-Tx}^{(n)}\delta_k}{P_p\beta_{nk}}, \tag{3.17}$$

trong đó N_e là công suất của nhiễu nền tại EAV. Công thức xấp xỉ (3.17) có thể được hiểu rằng can nhiễu từ P-Tx đến EAV lớn hơn rất nhiều lần công suất của nhiễu nền, tức là, $P_p\beta_{nk} >> N_e$, và như vậy ở đây ta có thể xem xét EAV chỉ bị ảnh hưởng bởi can nhiễu từ P-Tx.

Thay thế (3.16) vào (3.14), ta có

$$\Pr\left\{\max_{k\in\{1,2,\ldots,K\}}\{B\log_2(1+\gamma_e^{(n,k)})\} \geq R_e\right\} \leq \xi \tag{3.18}$$

Vì tất cả các kênh truyền là biến ngẫu nhiên độc lập, biểu thức (3.18) có thể được viết lại như sau

$$1-\prod_{k=1}^{K}\underbrace{\Pr\left\{\frac{\delta_k}{\beta_{nk}} \leq \frac{\gamma_{th}^e P_p}{P_{S-Tx}^{(n)}}\right\}}_{I} \leq \xi \tag{3.19}$$

trong đó $\gamma_{th}^e = 2^{\frac{R_e}{B}}-1$. Hơn nữa, xác suất trong (3.19) có thể thu được từ tính phân sau

$$I = \int_0^\infty \Pr\left\{\delta_k \leq \frac{x\gamma_{th}^e P_p}{P_{S-Tx}^{(n)}}\right\} f_{\beta_{nk}}(x)dx \tag{3.20}$$

trong đó $f_{\beta_{nk}}(x) = \frac{1}{\Omega_{\beta_n}}\exp\left(-\frac{x}{\Omega_{\beta_n}}\right)$. Theo đó, tích phân I được tính là

$$\begin{aligned} I &= 1-\int_0^\infty \frac{1}{\Omega_{\beta_n}}\exp\left[-\left(\frac{\gamma_{th}^e P_p}{P_{S-Tx}^{(n)}\Omega_\delta}+\frac{1}{\Omega_{\beta_n}}\right)x\right]dx \\ &= 1-\frac{1}{\frac{\gamma_{th}^e P_p\Omega_{\beta_n}}{P_{S-Tx}^{(n)}\Omega_\delta}+1} \end{aligned} \tag{3.21}$$

Thay thế (3.21) vào (3.19) và sau một số tính toán toán học, chúng ta thu được điều kiện cho công suất của S-Tx để đối phó với các thiết bị nghe trộm như sau

$$P_{S-Tx}^{(n)} \leq \frac{\gamma_{th}^{e} P_p \Omega_{\beta_n} (1 - \sqrt[K]{1-\xi})}{\Omega_\delta \sqrt[K]{1-\xi}} \tag{3.22}$$

Kết hợp (3.22) với điều kiện thu hoạch năng lượng (3.15), ta có

$$P_{S-Tx}^{(n)} \leq \min \left\{ P_{Eav}^{(n)}, P_{avg} \right\} \tag{3.23}$$

trong đó $P_{Eav}^{(n)}$ được biểu diễn là

$$P_{Eav}^{(n)} = \frac{\gamma_{th}^{e} P_p \Omega_{\beta_n} (1 - \sqrt[K]{1-\xi})}{\Omega_\delta \sqrt[K]{1-\xi}} \tag{3.24}$$

Kết quả là, công suất truyền tin của S-Tx trong kênh n-th có được bằng cách kết hợp (3.12) với (3.23)

$$P_{S-Tx}^{(n)} = \min \left\{ \min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}, P_{avg} \right\} \tag{3.25}$$

Từ (3.25), chúng ta xem xét hai trường hợp như sau:

- *Trường hợp 1:* $P_{avg} > \min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}$, công suất truyền tin của S-Tx phụ thuộc vào điều kiện kết hợp của PU và EAV là

  $$P_{S-Tx}^{(n)} = \min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}, \tag{3.26}$$

  trong đó $P_{PU}^{(n)}$ và $P_{Eav}^{(n)}$ được định nghĩa trong (3.13) và (3.24). Lưu ý rằng nếu thời gian thu hoạch năng lượng τ trong trường hợp này tăng thêm, công suất truyền tin của S-Tx cũng không thể tăng thêm do chịu ràng buộc bởi các điều kiện kết hợp của PU và EAV.

- *Trường hợp 2:* $P_{avg} \leq \min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}$, công suất truyền tin tối đa của S-Tx phụ thuộc vào năng lượng thu hoạch được từ PU, nghĩa là, $P_{S-Tx}^{(n)} = P_{avg}$. Hơn nữa, S-Tx luôn mong muốn giá trị của P_{avg} đạt mức cao nhất có thể để đạt được hiệu suất cao cho hệ thống, điều này có nghĩa rằng giá trị tối đa của P_{avg} bằng $\min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}$, tức là, $P_{avg} = \min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}$.

Sau một số tính toán toán học, chúng ta thu được khoảng thời gian thu hoạch năng lượng tối ưu τ để có thể tối đa hóa giá trị của P_{avg} là

$$\tau^* = \frac{\min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}}{\theta P_p \sum_{n=1}^{N} \Omega_{f_n} + \min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}} \tag{3.27}$$

Ngoài ra, S-Tx mong muốn chọn kênh tốt nhất nhằm tối đa hóa công suất truyền tin của nó để cải thiện hiệu suất của hệ thống, việc lựa chọn kênh như sau

$$n^* = \arg \max_{n \in \{1,2,\ldots,N_e\}} \left\{ P_{S-Tx}^{(n)} \right\} \tag{3.28}$$

trong đó n^* là kênh được chọn sao cho công suất truyền tin của S-Tx là tối ưu, nghĩa là

$$P_{S-Tx}^{(n^*)} = \max_{n \in \{1,2,\ldots,N_e\}} \left\{ \min \left\{ \min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}, P_{avg} \right\} \right\}$$

Cuối cùng, chúng ta có một thuật toán cho phân bổ công suất và chọn kênh được mô tả như sau.

3.3 Phân tích hiệu suất hệ thống

Khi S-Tx gửi các gói tin, chúng có thể bị lỗi do chất lượng kênh truyền và do các tác nhân khác. Do đó, S-Tx cần nạp lại năng lượng để truyền lại gói tin bị lỗi. Để đánh giá quá trình này, chúng ta sẽ xem xét hai chỉ số hiệu suất, gọi là xác suất lỗi gói tin (PEP) và độ trễ gói tin trung bình (APD) như sau

3.3.1 Xác suất lỗi gói tin

PEP được định nghĩa là xác suất mà SINR của SU bị sụt giảm xuống dưới một ngưỡng xác định trước, nghĩa là

$$\mathcal{O} = \Pr\{\gamma_s \leq \gamma_{th}\} \tag{3.29}$$

trong đó γ_{th} là ngưỡng giá trị SINR xác định của SU và γ_s được định nghĩa là

$$\gamma_s = \max_{m \in \{1,2,\ldots,N_p\}} \left\{ \frac{P_{S-Tx}^{(n^*)} g_m}{P_p \rho_{n^* m} + N_0} \right\} \tag{3.30}$$

Algorithm 2 Phân bổ công suất và chọn kênh

procedure PASA
  $P_{S-Tx}^{(n^*)} := 0$;
  for $\{n = 1; n \leq N; n++\}$ **do**
    $P_{PU}^{(n)} = \frac{1}{A_n}\left[\frac{\exp(-B_n)}{1-\eta_p} - 1\right]$;
    $P_{Eav}^{(n)} = \frac{\gamma_{th}^e P_p \Omega_{\beta_n}(1-\sqrt[K]{1-\xi})}{\Omega_\delta \sqrt[K]{1-\xi}}$;
    $\tau = \frac{\min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}}{\theta P_p \sum_{n=1}^{N} \Omega_{f_n} + \min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}}$;
    $P_{avg} = \frac{\tau\theta P_p}{1-\tau} \sum_{n=1}^{N} \Omega_{f_n}$;
    $P_{S-Tx}^{(n)} = \min\left\{\min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}, P_{avg}\right\}$;
    if $P_{S-Tx}^{(n)} \geq P_{S-Tx}^{(n^*)}$ **then**
      $n^* = n$;
      $P_{S-Tx}^{(n^*)} = P_{S-Tx}^{(n)}$
    end if
  end forreturn n^* and $P_{S-Tx}^{(n^*)}$;
end procedure

Từ đó, PEP có thể được tính toán bằng cách sử dụng tính chất trong [86, Property 1] như sau

$$\begin{aligned}\mathcal{O} &= \Pr\left\{\max_{m\in\{1,2,\ldots,N_p\}}\left\{\frac{P_{S-Tx}^{(n^*)} g_m}{P_p \rho_{n^* m} + N_0}\right\} < \gamma_{th}\right\} \\ &= \prod_{m=1}^{M} \Pr\left\{\frac{P_{S-Tx}^{(n^*)} g_m}{P_p \rho_{n^* m} + N_0} < \gamma_{th}\right\} \\ &= \left(1 - \frac{\exp\left(-\frac{\gamma_{th} N_0}{P_{S-Tx}^{(n^*)} \Omega_g}\right)}{\frac{\gamma_{th} P_p \Omega_{\rho_{n^*}}}{P_{S-Tx}^{(n^*)} \Omega_g} + 1}\right)^M \end{aligned} \tag{3.31}$$

3.3.2 Độ trễ gói tin với việc truyền sửa lỗi

Khi một gói tin được truyền không thành công, S-Tx cần nạp lại năng lượng và truyền lại gói tin đó. Xác suất mà một gói tin được truyền đi thành

công sau ℓ lần truyền được mô tả là

$$\Pr\{L = \ell\} = \mathcal{O}^{\ell-1}(1 - \mathcal{O}) \tag{3.32}$$

trong đó L là số lần truyền một gói tin. Do đó, số lần truyền trung bình trên gói tin có thể được tính toán như sau

$$\mathbf{E}[L] = \sum_{\ell=1}^{\infty} \ell \mathcal{O}^{\ell-1}(1 - \mathcal{O}) = \frac{1}{1 - \mathcal{O}} \tag{3.33}$$

Cuối cùng, độ trễ trung bình để truyền thành công một gói tin có thể được tính như dưới đây

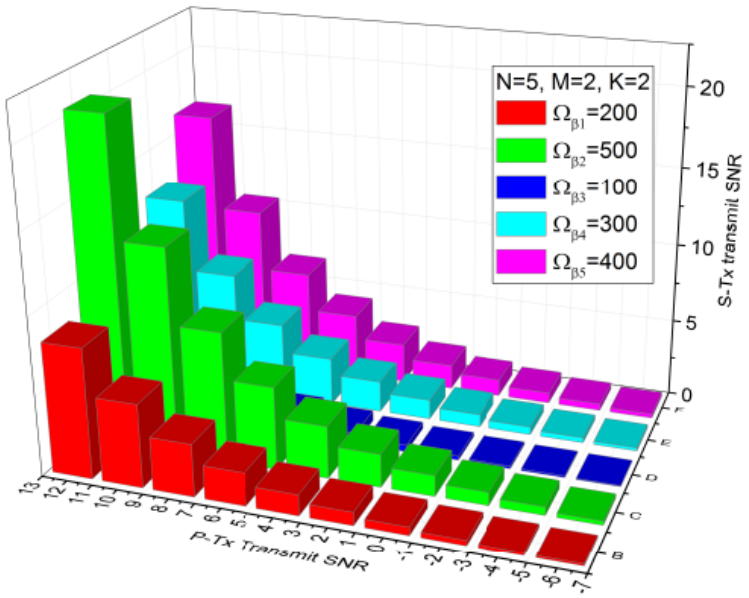
$$D = T\,\mathbf{E}[L] = \frac{T}{1 - \mathcal{O}} \tag{3.34}$$

trong đó T là tổng khung thời gian và $\mathcal{O}$ là PEP được định nghĩa trong (3.29).

3.4 Mô phỏng hệ thống

Trong chương này, nhóm nghiên cứu trình bày các kết quả phân tích và mô phỏng cho mô hình hệ thống. Cụ thể là chúng ta khảo sát ảnh hưởng từ SNR của P-Tx, thời gian thu hoạch năng lượng, và độ lợi kênh trung bình lên hai chỉ số PEP và APD. Theo các phương pháp phổ biến trong các tài liệu nghiên cứu hiện nay, các thông số hệ thống được sử dụng trong phân tích và mô phỏng được thiết lập ban đầu như sau:

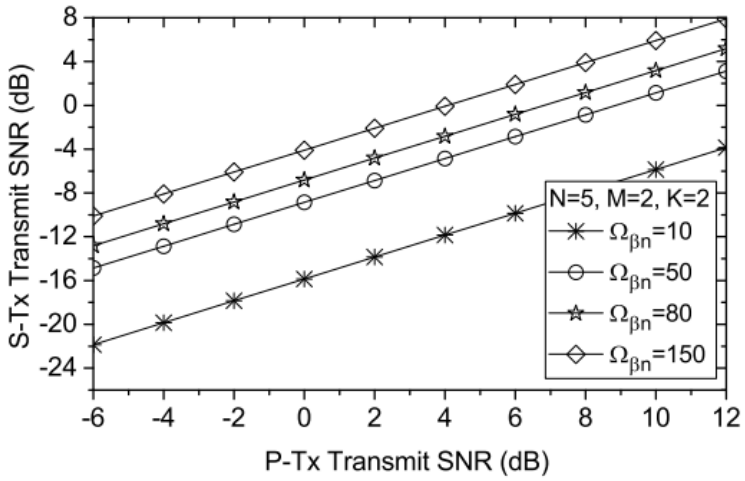
- Băng thông hệ thống: $B = 2$ MHz;
- Điều kiện dừng của PU: $\eta_p = 0.001$;
- Điều kiện bảo mật: $\xi = 0.001$;
- Hệ số hiệu suất thu hoạch năng lượng: $\theta = 0.5$;
- Tốc độ xác định của $R_s = 64$ Kbps;
- Tốc độ xác định của $R_p = 64$ Kbps;
- Tốc độ xác định của $R_e = 3$ Mbps;



Hình 3.3: *Ảnh hưởng của độ lợi trung bình (Ω_{β_n}) của P-Tx→EAV lên SNR của S-Tx.*

Hình 3.3 minh họa ảnh hưởng của độ lợi kênh trung bình (Ω_{β_n}) của kênh P-Tx→EAV lên SNR của S-Tx. Chúng ta có thể thấy rằng ở kênh chỉ số C, tương ứng với kênh số 2 có $\Omega_{\beta_2} = 500$ cung cấp cho hệ thống mức SNR của S-Tx là cao nhất. Mặt khác, tại kênh có chỉ số là D, tương ứng với kênh số 3 có $\Omega_{\beta_3} = 100$, cung cấp cho hệ thống mức SNR của S-Tx là thấp nhất. Nguyên nhân là do với một giá trị cao của độ lợi trung bình kênh của kênh P-Tx→EAV dẫn đến sự can nhiễu mạnh vào các EAV, tức là làm cho các EAV gặp khó khăn hơn trong quá trình thu và giải mã các gói tin truyền đi từ S-Tx. Kết quả là S-Tx có thể tăng công suất truyền tin của nó để nâng cao hiệu suất của hệ thống mà không bị tiết lộ bí mật truyền thông của SU cho các EAV. Nói cách khác, kênh số 2 sẽ được chọn cho truyền thông của SU. Quan sát hình 3.4 bổ sung cho chúng ta thấy hiện tượng nói trên, tức là khi tăng độ lợi kênh trung bình (Ω_{β_n}) của kênh P-Tx→EAV dẫn đến giá trị của SNR của S-Tx tăng theo, hoặc có thể nói rằng can nhiễu từ P-Tx đến EAV mang đến lợi ích cho SNR của S-Tx.

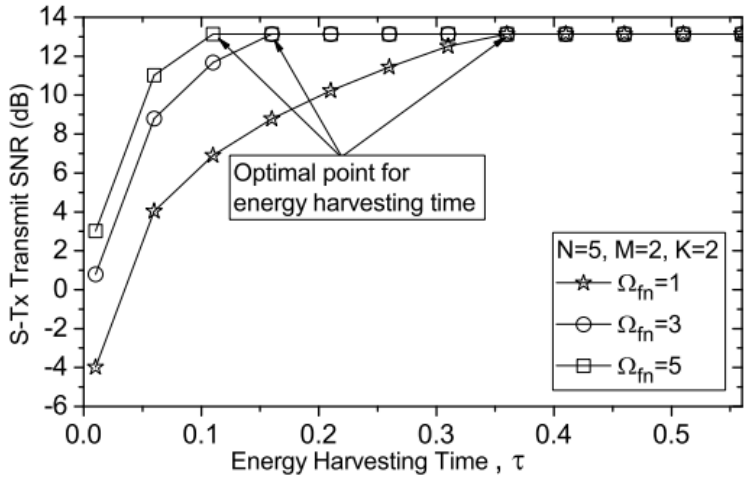
Hình 3.5 cho thấy tác động của phần thời gian thu hoạch năng lượng τ và độ lợi kênh trung bình ($\{\Omega_{f_n}\}_{n=1}^{5} = 1, 3, 5$) của kênh thu hoạch năng lượng P-Tx→S-Tx lên SNR của S-Tx. Có thể thấy rằng khi độ lợi kênh trung bình



Hình 3.4: *SNR của S-Tx theo SNR của P-Tx với độ lợi kênh trung bình khác nhau của S-Tx→EAV* ($\{\Omega_{\beta_n}\}_{n=1}^{5} = 10, 50, 80, 150$).

của kênh thu năng lượng P-Tx→S-Tx là cao nhất, ví dụ, $\{\Omega_{f_n}\}_{n=1}^{5} = 5$, SNR của S-Tx tăng rất nhanh trong khoảng đầu miền giá trị của τ và bão hòa tại $\tau = 0.1$. Hơn nữa, tất cả SNR của S-Tx tại các giá trị độ lợi kênh trung bình khác nhau đều bão hòa tại giá trị 13 dB khi $\tau > 0.4$, tức là giá trị lớn hơn 0.4 của phần thời gian thu hoạch năng lượng không còn ảnh hưởng đến kết quả của SNR của S-Tx. Hiện tượng này có thể hiểu rằng: Độ lợi kênh trung bình của kênh P-Tx→S-Tx càng cao thì dẫn đến mức năng lượng thu được từ P-Tx càng lớn, do đó phần thời gian sử dụng để thu năng lượng đủ cho hoạt động của SU sẽ nhỏ hơn. Tuy nhiên, khi phần thời gian thu hoạch năng lượng tiếp tục tăng thêm $\tau > 0.4$ thì SNR của S-Tx bão hòa, do nó không thể thu được lượng năng lượng lớn hơn bởi vì giá trị SNR của các P-Tx trong trường hợp này là cố định ($\gamma_{P-Tx} = 12$ dB).

Để thực hiện phân tích, mô phỏng đánh giá kết quả của PEP và độ trễ gói tin trong hoạt động của hệ thống, tác giả đã thiết lập các giá trị ban đầu của độ lợi kênh trung bình của kênh trong hệ thống như sau: Độ lợi kênh trung bình của kênh P-Tx→P-Rx: $\{\Omega_{h_n}\}_{n=1}^{5} = 2$; Độ lợi kênh trung bình của kênh S-Tx→P-Rx: $\{\Omega_{\alpha_n}\}_{n=1}^{5} = 2$; Độ lợi kênh trung bình của kênh P-Tx→S-Tx: $\{\Omega_{f_n}\}_{n=1}^{5} = 5$; Độ lợi kênh trung bình của kênh S-Tx→EAV: $\{\Omega_{\delta_k}\}_{k=1}^{2} = 1$; Độ lợi kênh trung bình của kênh P-Tx→SAP: $\{\Omega_{\rho_{nm}}\} = 1$ cho mọi n và m; Độ lợi kênh trung bình của kênh S-Tx→SAP: $\Omega_g = 8$;.



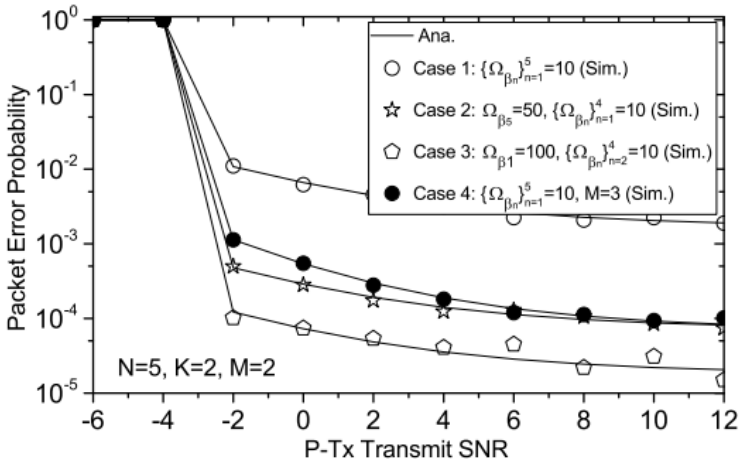
Hình 3.5: *SNR của S-Tx theo τ và độ lợi trung bình khác nhau của P-Tx→S-Tx ($\{\Omega_{f_n}\}_{n=1}^{5} = 1, 3, 5$, và $\gamma_{P-Tx} = 12$ dB).*

Hình 3.6 cho thấy tác động của các kênh can nhiễu P-Tx→EAV lên PEP với các trường hợp được xem xét dưới đây:

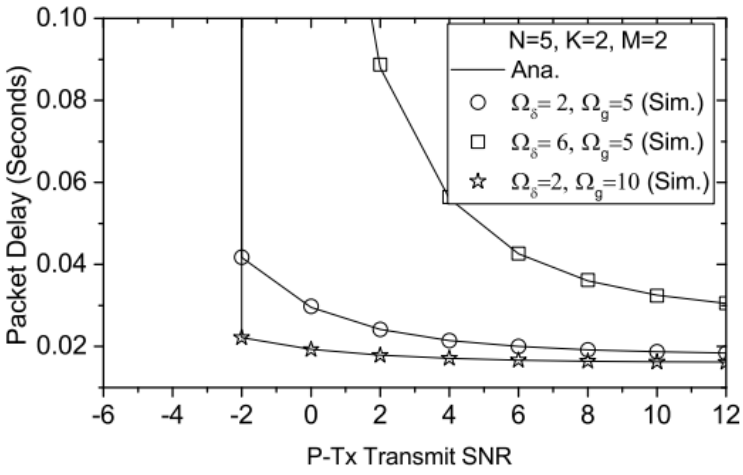
- Trường hợp 1: Các độ lợi kênh trung bình của các kênh can nhiễu P-Tx→EAV là đồng nhất: $\{\Omega_{\beta_n}\}_{n=1}^{5} = 10$;
- Trường hợp 2: Độ lợi kênh trung bình từ kênh can nhiễu P-Tx$_5$→EAV có giá trị lớn nhất: $\Omega_{\beta_5} = 50$, các kênh khác là đồng nhất: $\{\Omega_{\beta_n}\}_{n=1}^{4} = 10$;
- Trường hợp 3: Độ lợi kênh trung bình từ kênh can nhiễu P-Tx$_1$→EAV có giá trị lớn nhất: $\Omega_{\beta_1} = 100$, các kênh khác là đồng nhất: $\{\Omega_{\beta_n}\}_{n=2}^{4} = 10$;
- Trường hợp 4: Độ lợi kênh trung bình từ các kênh can nhiễu P-Tx→EAV là đồng nhất như trong trường hợp 1. Nhưng số ăng-ten của SAP thì lớn hơn trong trường hợp 1, ($M = 3$).

Từ trường hợp 1 đến trường hợp 3 cho ta thấy rằng nếu một trong số các kênh có mức can nhiễu P-Tx→EAV mạnh nhất, nó sẽ được lựa chọn để truyền thông và PEP được giảm xuống đáng kể. Cụ thể, PEP trong trường hợp 3 là tốt hơn PEP trong các trường hợp 1 và 2. Điều này có thể giải thích được bởi thực tế rằng do can nhiễu mạnh từ P-Tx đến EAV làm giảm chất lượng các gói tin được giải mã tại EAV. Do đó, S-Tx có thể tăng SNR để nâng cao hiệu suất của hệ thống mà không bị tiết lộ thông tin cho các EAV. Ngoài ra, chúng ta

có thể thấy PEP trong trường hợp 4 là tốt hơn PEP trong trường hợp 1. Điều này là do số ăng-ten của SAP trong trường hợp 4 nhiều hơn trong trường hợp 1, và do vậy tín hiệu thu được của nó tót hơn trường hợp 1, kết quả là PEP trong trường hợp 4 thấp hơn. Hình 3.7 cho thấy tác động của kênh S-



Hình 3.6: *Ảnh hưởng của các kênh can nhiễu P-Tx→EAV lên PEP.*



Hình 3.7: *Độ trễ của gói tin theo SNR của P-Tx.*

Tx→EAV và kênh S-Tx→SAP lên độ trễ gói tin. Chúng ta có thể thấy rằng ở phạm vi mức SNR thấp của P-Tx, ví dụ $\gamma_{P-Tx} < -2$ dB, độ trễ gói tin là vô cùng. Tuy nhiên, khi mức SNR của P-Tx tăng lên, độ trễ gói tin của SU giảm đáng kể. Hiện tượng này là do với mức SNR thấp của P-Tx, S-Tx chỉ thu được một lượng nhỏ năng lượng, do đó công suất cần thiết để phân phối các gói tin

là rất nhỏ, làm tăng mức độ lỗi gói tin. Vì vậy, S-Tx sẽ phải yêu cầu nhiều lần truyền lại các gói tin bị lỗi để đảm bảo gói tin được truyền thành công, tức là độ trễ của gói tin tăng lên. Hơn nữa, khi độ lợi kênh trung bình của các kênh S-Tx→EAV tăng từ $\Omega_\delta = 2$ lên $\Omega_\delta = 6$, độ trễ gói tin cũng tăng lên. Thực tế này là do các EAV có thể thu và giải mã các gói tin dễ dàng hơn khi độ lợi trung bình của các kênh wiretap tăng lên. Để đảm bảo truyền thông bảo mật, S-Tx phải giảm SNR để thỏa mãn các điều kiện ràng buộc về yêu cầu bảo mật. Do đó, tỉ lệ lỗi gói tin sẽ tăng lên, nghĩa là S-Tx sẽ phải yêu cầu truyền lại các gói tin nhiều lần hơn. Như vậy, độ trễ gói tin tăng lên. Cuối cùng, chúng ta cũng thấy rằng khi độ lợi kênh trung bình của S-Tx→SAP tăng từ $\Omega_g = 5$ lên $\Omega_g = 10$ thì độ trễ gói tin được cải thiện đáng kể. Điều này là dễ hiểu khi mọi điều kiện ràng buộc được thỏa mãn, một độ lợi kênh tốt giữa nguồn với đích thì tỉ lệ lỗi gói tin ở mức thấp, nghĩa là S-Tx không phải truyền lại các gói tin.

3.5 Kết luận

Trong nội dung tiếp theo này, nhóm nghiên cứu đã đề xuất một giao thức truyền thông và thu hoạch năng lượng cho mạng CRN có sử dụng công nghệ thu hoạch năng lượng vô tuyến. Trong đó S-Tx vừa phải tuân thủ các yêu cầu về thu hoạch năng lượng, vừa phải thỏa mãn các điều kiện ràng buộc về bảo mật đối với các EAV và điều kiện xác suất dừng của mạng sơ cấp. Trong mô hình nghiên cứu, chúng tôi đã tìm ra một giải pháp tối ưu thời gian thu hoạch năng lượng, một chính sách phân bổ công suất và một chiến lược lựa chọn kênh. Ngoài ra, hiệu suất hệ thống sẽ được phân tích dựa trên hai độ đo được tính toán là xác suất lỗi gói tin (PEP) và độ trễ gói tin trung bình (APD). Các số liệu từ kết quả phân tích và mô phỏng cho thấy chính sách phân bổ công suất và chiến lược chọn kênh có thể cung cấp truyền thông tin cậy và an toàn cho SU mà không vi phạm các điều kiện ràng buộc về bảo mật và giới hạn can nhiễu từ nhiều PU.

KẾT LUẬN CHUNG

Các kết quả chính của đề tài bao gồm:

1. Khảo sát truyền thông bảo mật cho mạng thứ cấp trong mô hình mạng CRN trên kênh fading có phân bố Rayleigh. Qua đó, xây dựng các chính sách phân bổ công suất cho mạng SU với bốn kịch bản CSI của hệ thống khác nhau. Đề xuất một độ đo hiệu suất truyền thông tin cậy và bảo mật mới (SRCP) để đánh giá hiệu suất hệ thống. Từ đó phân tích và đánh giá hiệu năng của mô hình mạng được khảo sát tương ứng với bốn kịch bản khác nhau.

2. Nghiên cứu về truyền thông tin cậy và bảo mật trong mạng CRN có sử dụng công nghệ thu hoạch năng lượng vô tuyến. Đề xuất một giao thức truyền thông và thu hoạch năng lượng cùng với một chính sách phân bổ công suất và chiến lược chọn kênh cho mô hình hệ thống. Từ đó, tính toán các độ đo xác suất lỗi gói tin (PEP) và đỗ trễ gói tin trung bình (APD) để đánh giá hiệu suất hoạt động của hệ thống trong các điều kiện ràng buộc về bảo mật thông tin.

Khả năng phát triển tiếp theo các kết quả của đề tài nghiên cứu như sau:

1. Trên cơ sở công trình "Đánh giá hiệu suất hoạt động của truyền thông bảo mật và tin cậy trong mạng vô tuyến nhận thức", có thể phát triển bài toán đánh giá hiệu năng bảo mật với các trường hợp CSI của kênh truyền là không hoàn hảo hoặc một phần, hoặc với nhiều EAV có khả năng hợp tác nghe trộm. Đồng thời tiếp tục nghiên cứu truyền thông tin cậy và bảo mật hệ thống CRN trong môi trường kênh truyền fading khác như Nakagami-m, $\alpha - \mu$.

2. Dựa trên các kết quả nghiên cứu của chương 3, có thể phát triển các bài toán đánh giá chất lượng hiệu suất của mô hình mạng này trên kênh truyền fading khác như kênh $\alpha - \mu$ fading. Đồng thời tiếp tục phát triển mô hình này kết hợp với các kỹ thuật nút hợp tác chuyển tiếp, đa ăng-ten.

3. Tiếp tục khảo sát các công trình nghiên cứu trong lĩnh vực bảo mật lớp vật lý trong mạng không dây để nghiên cứu phát triển các giải pháp bảo mật tầng vật lý trong truyền thông không dây của các mạng thế hệ 5G như Massive MIMO, NOMA,...

Tài liệu tham khảo

[1] Alahmadi A. and Abdelhakim M. and Jian Ren and Tongtong Li (2013), "Mitigating primary user emulation attacks in cognitive radio networks using advanced encryption standard", *Proc. IEEE Global Communications Conference*, pp. 3229-3234.

[2] Alves H. and Souza R. D. and Debbah M. and Bennis M. (2012), "Performance of Transmit Antenna Selection Physical Layer Security Schemes", *IEEE Signal Processing Letters*, 19(6), pp. 372-375.

[3] Bahrak B. and Bhattarai S. and Ullah A. and Park J. M. J. and Reed J. and Gurney D. (2014), "Protecting the primary users' operational privacy in spectrum sharing ", *Proc. IEEE International Symposium on Dynamic Spectrum Access Networks*, pp. 236-247.

[4] Bloch M. and Barros J. and Rodrigues M.R.D. and McLaughlin S.W. (2008), "Wireless Information-Theoretic Security", *IEEE Transactions on Information Theory*, 54(6), pp. 2515-2534.

[5] Chao Wang and Hui-Ming Wang (2014), "On the Secrecy Throughput Maximization for MISO Cognitive Radio Network in Slow Fading Channels", *IEEE Transactions on Information Forensics and Security*, 9(11), pp. 1814-1827.

[6] Chorti A. and Perlaza S. M. and Han Z. and Poor H. V. (2013), "On the Resilience of Wireless Multiuser Networks to Passive and Active Eavesdroppers", *IEEE Journal on Selected Areas in Communications*, 31(9), pp. 1850-1863.

[7] Chung W. and Park S. and Lim S. and Hong D. (2014), "Spectrum Sensing Optimization for Energy-Harvesting Cognitive Radio Systems", *IEEE Transactions on Wireless Communications*, 13(5), pp. 2601-2613.

[8] Csiszar I. and Korner J. (1978), "Broadcast channels with confidential messages", *IEEE Transactions on Information Theory*, 24(3), pp. 339-348.

[9] Datla D. and Wyglinski A. M. and Minden G. J. (2009), "A Spectrum Surveying Framework for Dynamic Spectrum Access Networks", *IEEE Transactions on Vehicular Technology*, 58(8), pp. 4158-4168.

[10] Ding Z. and Peng M. and Chen H. H. (2011), "A General Relaying Transmission Protocol for MIMO Secrecy Communications", *IEEE Transactions on Communications*, 60(11), pp. 3461-3471.

[11] Dong L. and Han Z. and Petropulu A. P. and Poor H. V. (2010), "Improving Wireless Physical Layer Security via Cooperating Relays", *IEEE Transactions on Signal Processing*, 58(3), pp. 1875-1888.

[12] Duy T. T. and Duong T. Q. and Thanh T. L. and Bao V. N. Q. (2015),"Secrecy performance analysis with relay selection methods under impact of co-channel interference", *IET Communications*, 9(11), pp. 1427-1435.

[13] Esch J. (2012), "A survey of security challenges in cognitive radio networks: Solutions and future research directions", *Proceedings of the IEEE*, 100(12), pp. 3170-3171.

[14] Fan L. and Lei X. and Duong T. Q. and Elkashlan M. and Karagiannidis G. K. (2014), "Secure Multiuser Communications in Multiple Amplify-and-Forward Relay Networks", *IEEE Transactions on Communications*, 62(9), pp. 3299-3310.

[15] Fragkiadakis A. G. and Tragos E. Z. and Askoxylakis I. G. (2013), "A survey on security threats and detection techniques in cognitive radio networks", *IEEE Commun. Surv. Tut.*, 15(1), pp. 428-445.

[16] Garg V. K. (2011), *LTE-The UMTS Long Term Evolution: From theory to practice*, Wiley.

[17] Ghasemi A. and Sousa E. S. (2007), "Fundamental limits of spectrum-sharing in fading environments", *IEEE Transactions on Wireless Communications*, 6(2), pp. 649-658.

[18] Goel S. and Negi R. (2008), "Guaranteeing Secrecy using Artificial Noise", *IEEE Transactions on Wireless Communications*, 7(6), pp. 2180-2189.

[19] Goldsmith A. J. (2005), *Wireless Communications*, Cambridge University Press.

[20] Goldsmith A. and Jafar S. A. and Maric I. and Srinivasa S. (2009), "Breaking Spectrum Gridlock With Cognitive Radios: An Information Theoretic Perspective", *Proceedings of the IEEE*, 97(5), pp. 894-914.

[21] Gungor O. and Koksal C. E. and Gamal H. E. (2013), "On secrecy outage capacity of fading channels under relaxed delay constraints", *2013 IEEE International Symposium on Information Theory*, pp. 2024-2028.

[22] Guo J. and Durrani S. and Zhou X. and Yanikomeroglu H. (2015), "Outage Probability of Ad Hoc Networks With Wireless Information and Power Transfer", *IEEE Wireless Communications Letters*, 4(4), pp. 409-412.

[23] Hadzi-Velkov Z. and Nikoloska I. and Karagiannidis G. K. and Duong T. Q. (2016), "Wireless Networks with Energy Harvesting and Power Transfer: Joint Power and Time Allocation", *IEEE Signal Processing Letters*, 23(1), pp. 50-54.

[24] Ha D. and Yo N. (2014), "Physical layer secrecy performance with transmitter antenna selection over dissimilar fading channels", *2014 International Conference on Computer, Communications, and Control Technology (I4CT)*, pp. 140-144.

[25] Ha D. B. and Tung T. Vu and Duy T. T. and Vo Nguyen Quoc Bao (2015), "Secure cognitive reactive Decode-and-Forward Relay networks

with and without eavesdroppers", *Springer Wireless Pers. Comm.*, 85(4), pp. 2619-2641.

[26] Haykin S. (2005), "Cognitive radio: brain-empowered wireless communications", *IEEE Journal on Selected Areas in Communications*, 23(2), pp. 201-220.

[27] Hellman M. E. (2002), "An overview of public key cryptography", *IEEE Communications Magazine*, 40(5), pp. 42-49.

[28] Hoang D. T. and Niyato D. and Wang P. and Kim D. I. (2014), "Opportunistic Channel Access and RF Energy Harvesting in Cognitive Radio Networks", *IEEE Journal on Selected Areas in Communications*, 32(11), pp. 2039-2052.

[29] Hoang D. T. and Niyato D. and Wang P. and Kim D. I. (2015), "Performance Analysis of Wireless Energy Harvesting Cognitive Radio Networks Under Smart Jamming Attacks", *IEEE Transactions on Cognitive Communications and Networking*, 1(2), pp. 200-216.

[30] Hung Tran and Maarig Aregawi Hagos and Marshed Mohamed and Hans-Jurgen Zepernick (2013), "Impact of primary networks on the performance of secondary networks ", *Proc. International Conference on Computing, Management and Telecommunications*, pp. 43-48.

[31] Hung Tran and Georges Kaddoum and Fran$\mathcal{C}$cois Gagnon and Louis Sibomana (2017), "Cognitive radio network with secrecy and interference constraints", *Physical Communication*, 22, pp. 32 - 41.

[32] Islam M. H. and Koh C. L. and Oh S. W. and Qing X. and Lai Y. Y. and Wang C. and Liang Y. C. and TohB. E. and Chin F. and Tan G. L. and Toh W. (2008), "Spectrum Survey in Singapore: Occupancy Measurements and Analyses", *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, pp. 1-7.

[33] ITU-R (2008), "Requirements related to technical performance for IMT-Advanced radio interface(s) ", *REPORT ITU-R M.2134*, (ITU-R M.2134).

[34] Jiang L. and Tian H. and Qin C. and Gjessing S. and Zhang Y. (2016), "Secure Beamforming in Wireless-Powered Cooperative Cognitive Radio Networks", *IEEE Communications Letters*, 20(3), pp. 522-525.

[35] Kartalopoulos S. V. (2006), "A primer on cryptography in communications", *IEEE Communications Magazine*, 44(4), pp. 146-151.

[36] Khisti A. and Wornell G. W. (2010), "Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel", *IEEE Transactions on Information Theory*, 56(7), pp. 3088-3104.

[37] Khisti A. and Wornell G. W. (2010), "Secure Transmission With Multiple Antennas—Part II: The MIMOME Wiretap Channel", *IEEE Transactions on Information Theory*, 56(11), pp. 5515-5532.

[38] D. Klinc and J. Ha and S. W. McLaughlin and J. Barros and B. Kwak (2011), "LDPC Codes for the Gaussian Wiretap Channel", *IEEE Transactions on Information Forensics and Security*, 6(3), pp. 532-540.

[39] Krikidis I. and Thompson J. S. and Mclaughlin S. (2009), "Relay selection for secure cooperative networks with jamming", *IEEE Transactions on Wireless Communications*, 8(10), pp. 5003-5011.

[40] Lee S. and Zhang R. and Huang K. (2013), "Opportunistic Wireless Energy Harvesting in Cognitive Radio Networks", *IEEE Transactions on Wireless Communications*, 12(9), pp. 4788-4799.

[41] Lei H., Gao C., Ansari I. S., Guo Y., Zou Y., Pan G. and Qaraqe K. A. (2017), "Secrecy Outage Performance of Transmit Antenna Selection for MIMO Underlay Cognitive Radio Systems Over Nakagami- *m* Channels", *IEEE Transactions on Vehicular Technology*, 66(3), pp. 2237-2250.

[42] Leung-Yan-Cheong S. and Hellman M. (1978), "The Gaussian wire-tap channel", *IEEE Transactions on Information Theory*, 24(4), pp. 451-456.

[43] Li J. and Petropulu A. P. (2011), "Ergodic Secrecy Rate for Multiple-Antenna Wiretap Channels With Rician Fading", *IEEE Transactions on Information Forensics and Security*, 6(3), pp. 861-867.

[44] Liang Y. and Poor H. V. and Ying L. (2011), "Secure Communications Over Wireless Broadcast Networks: Stability and Utility Maximization", *IEEE Transactions on Information Forensics and Security*, 6(3), pp. 682-692.

[45] Liu X. (2013), "Probability of Strictly Positive Secrecy Capacity of the Rician-Rician Fading Channel", *IEEE Wireless Communications Letters*, 2(1), pp. 50-53.

[46] Liu Y. and Li J. and Petropulu A. P. (2013), "Destination Assisted Cooperative Jamming for Wireless Physical-Layer Security", *IEEE Transactions on Information Forensics and Security*, 8(4), pp. 682-694.

[47] Liu X. (2014), "Strictly positive secrecy capacity of log-normal fading channel with multiple eavesdroppers", *2014 IEEE International Conference on Communications (ICC)*, pp. 775-779.

[48] Liu Y. and Wang L. and Duy T. T. and Elkashlan M. and Duong T. Q. (2015), "Relay Selection for Security Enhancement in Cognitive Relay Networks", *IEEE Wireless Communications Letters*, 4(1), pp. 46-49.

[49] Liu Y. and Chen H. and Wang L. (2017), "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges", *IEEE Communications Surveys Tutorials*, 19(1), pp. 347-376.

[50] Liu, Hequn and Zhao, Hui and Jiang, Hong and Tang, Chaoqing and Pan, Gaofeng and Li, Tingting and Chen, Yunfei (2016), "Physical-layer secrecy outage of spectrum sharing CR systems over fading channels", *Science China Information Sciences*, 59(10), pp. 102-308.

[51] Louis Sibomana and Hung Tran and Quang Anh Tran (2015), "Impact of secondary user communication on security communication of primary

user", *Security and Communication Networks, Journal of Wiley*, 8(18), pp. 4177-4190.

[52] Lu X. and Wang P. and Niyato D. and Kim D. I. and Han Z. (2015), "Wireless Networks With RF Energy Harvesting: A Contemporary Survey", *IEEE Communications Surveys Tutorials*, 17(2), pp. 757-789.

[53] Liu W. and Zhou X. and Durrani S. and Popovski P. (2016), "Secure Communication With a Wireless-Powered Friendly Jammer", *IEEE Transactions on Wireless Communications*, 15(1), pp. 401-415.

[54] Mahdavifar H. and Vardy A. (2011), "Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes", *IEEE Transactions on Information Theory*, 67(10), pp. 6428-6443.

[55] Mitola J. and Maguire G. Q. (1999), "Cognitive radio: making software radios more personal", *IEEE Personal Communications*, 6(4), pp. 13-18.

[56] Mitola J. (2009), "Cognitive Radio Architecture Evolution", *Proceedings of the IEEE*, 97(4), pp. 626-641.

[57] S. A. Mousavifar and Y. Liu and C. Leung and M. Elkashlan and T. Q. Duong (2014), "Wireless Energy Harvesting and Spectrum Sharing in Cognitive Radio", *IEEE Vehicular Technology Conference*, pp. 1-5.

[58] Mukherjee A. and Fakoorian S. A. A. and Huang J. and Swindlehurst A. L. (2014), "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey", *IEEE Communications Surveys Tutorials*, 16(3), pp. 1550-1573.

[59] Nguyen T. V. and Shin H. (2011), "Power Allocation and Achievable Secrecy Rates in MISOME Wiretap Channels", *IEEE Communications Letters*, 15(11), pp. 1196-1198.

[60] Nguyen V. D. and Duong T. Q. and Dobre O. and Shin O. S. (2016), "Joint Information and Jamming Beamforming for Secrecy Rate Maximization

in Cognitive Radio Networks", *IEEE Transactions on Information Forensics and Security*, 11(11), pp. 2609-2623.

[61] Nguyen Nam-Phong, Tu Lam Thanh, Trung Q. Duong and A. Nallanathan (2017), "Secure communications in cognitive underlay networks over Nakagami-m channel", *Physical Communication*, 25, pp. 610 - 618.

[62] Ni W. and Dong X. (2015), "Energy Harvesting Wireless Communications With Energy Cooperation Between Transmitter and Receiver", *IEEE Transactions on Communications*, 63(4), pp. 1457-1469.

[63] Pei Y. and Liang Y.-C. and Zhang L. and Teh K. C. and Li K. H. (2009), Achieving cognitive and secure transmissions using multiple antennas, *Proc. IEEE Personal Indoor Mobile Radio Communication*, pp. 1-5.

[64] Pei Y. and Liang Y.-C. and Zhang L. and Teh K. C. and Li K. H. (2011), "Increasing secrecy capacity via joint design of cooperative beamforming and jamming", *Proc. IEEE Personal Indoor Mobile Radio Communication*, pp. 1274–1278.

[65] Prabhu V. U. and RodriguesM. R. D. (2011), "On Wireless Channels With$M$-Antenna Eavesdroppers: Characterization of the Outage Probability and ε-Outage Secrecy Capacity", *IEEE Transactions on Information Forensics and Security*, 6(3), pp. 853-860.

[66] Pratibha M. and Li K. H. and Teh K. C. (2016), "Channel Selection in Multichannel Cognitive Radio Systems Employing RF Energy Harvesting", *IEEE Transactions on Vehicular Technology*, 65(1), pp. 457-462.

[67] Pratibha and Li K. H. and Teh K. C. (2016), "Dynamic Cooperative Sensing–Access Policy for Energy-Harvesting Cognitive Radio Systems", *IEEE Transactions on Vehicular Technology*, 65(12), pp. 10137-10141.

[68] Praveen Kumar Gopala and Lifeng Lai and El Gamal H. (2008), "On the Secrecy Capacity of Fading Channels", *IEEE Transactions on Information Theory*, 54(10), pp. 4687-4698.

[69] Poursajadi S. and Madani M. H. (2018), "Analysis and Enhancement of Joint Security and Reliability in Cooperative Networks", *IEEE Transactions on Vehicular Technology*, 67(12), pp. 12003-12012.

[70] Quang P. M. and Duy T. T. and Bao V. N. Q. (2016), "Performance evaluation of underlay cognitive radio networks over Nakagami-*m* fading channels with energy harvesting", *International Conference on Advanced Technologies for Communications (ATC)*, pp. 108-113.

[71] Rakovic V. and Denkovski D. and Hadzi-Velkov Z. and Gavrilovska L. (2015), "Optimal time sharing in underlay cognitive radio systems with RF energy harvesting", *IEEE International Conference on Communications (ICC)*, pp. 7689-7694.

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

[73] Sakran H. and Shokair M. and Nasr O. and El-Rabaie S. and El-Azm A.A. (2012), "Proposed relay selection scheme for physical layer security in cognitive radio networks", *IET Communications*, 6(16), pp. 2676-2687.

[74] Sarkar M. Z. I. and Ratnarajah T., (2011), "Secure Communication through Nakagami-m Fading MISO Channel", *2011 IEEE International Conference on Communications (ICC)*, pp. 1-5.

[75] Schaefer R. F. and Boche H. (2014), "Physical Layer Service Integration in Wireless Networks : Signal processing challenges", *IEEE Signal Processing Magazine*, 31(3), pp. 147-156.

[76] Shannon C. E. (1949), "Communication theory of secrecy systems", *The Bell System Technical Journal*, 28(4), pp. 656-715.

[77] Sibomana L. and Zepernick H. J. and Tran H. (2014), "On physical layer security for reactive DF cognitive relay networks", *Proc. IEEE GLOBECOM*, pp. 1290-1295.

[78] Simeone O. and Stanojev I. and Savazzi S. and Bar-Ness Y. and Spagnolini U. and Pickholtz R. (2008), "Spectrum Leasing to Cooperating Secondary Ad Hoc Networks", *IEEE Journal on Selected Areas in Communications*, 26(1), pp. 203-213.

[79] Singh A. and Bhatnagar M. R. and Mallik R. K. (2016), "Secrecy Outage of a Simultaneous Wireless Information and Power Transfer Cognitive Radio System", *IEEE Wireless Communications Letters*, 5(3), pp. 288-291.

[80] Stanojev I. and Yener A. (2013), "Improving Secrecy Rate via Spectrum Leasing for Friendly Jamming", *IEEE Transactions on Wireless Communications*, 12(1), pp. 134-145.

[81] Sudevalayam S. and Kulkarni P. (2011), "Energy Harvesting Sensor Nodes: Survey and Implications", *IEEE Communications Surveys Tutorials*, 13(3), pp. 443-461.

[82] Sugata Sanyal and Rohit Bhadauria and Ghosh C. (2009), "Secure communication in cognitive radio networks", *Proc. International Conference on Computers and Devices for Communication*, pp. 1-4.

[83] Sun X. and Wang J. and Xu W. and Zhao C. (2012), "Performance of Secure Communications Over Correlated Fading Channels", *IEEE Signal Processing Letters*, 19(8), pp. 479-482.

[84] Tang C. and Pan G. and Li T. (2014), "Secrecy Outage Analysis of Underlay Cognitive Radio Unit Over Nakagami-mFading Channels", *IEEE Wireless Communications Letters*, 3(6), pp. 609-612.

[85] Thangaraj A. and Dihidar S. and Calderbank A. R. and McLaughlin S. W. and Merolla J. (2007), "Applications of LDPC Codes to the Wiretap Channel", *IEEE Transactions on Information Theory*, 53(8), pp. 2933-2945.

[86] Tran H., Zepernick H. J., Phan H. (2013), "Cognitive Proactive and Reactive DF Relaying Schemes under Joint Outage and Peak Transmit Power Constraints ", *IEEE Communications Letters*, 17(8), pp. 1548-1551.

[87] Tse, David and Viswanath, Pramod (2005), *Fundamentals of Wireless Communication,* Cambridge University Press.

[88] Vilela J. P. and Bloch M. and Barros J. and McLaughlin S. W. (2011), "Wireless Secrecy Regions With Friendly Jamming", *IEEE Transactions on Information Forensics and Security*, 6(2), pp. 256-266.

[89] Wu H. and Tao X. and Han Z. and Li N. and Xu J. (2017), "Secure Transmission in MISOME Wiretap Channel With Multiple Assisting Jammers: Maximum Secrecy Rate and Optimal Power Allocation", *IEEE Transactions on Communications*, 65(2), pp. 775-789.

[90] Wyner A. D. (1975), "The wire-tap channel", *The Bell System Technical Journal*, 54(8), pp. 1355-1387.

[91] Xu X. and He B. and Yang W. and Zhou X. and Cai Y. (2016), "Secure Transmission Design for Cognitive Radio Networks With Poisson Distributed Eavesdroppers ", *IEEE Transactions on Information Forensics and Security*, 11(2), pp. 373-387.

[92] Yang Z. and Ding Z. and Fan P. and Karagiannidis G. K. (2016), "Outage Performance of Cognitive Relay Networks With Wireless Information and Power Transfer", *IEEE Transactions on Vehicular Technology*, 65(5), pp. 3828-3833.

[93] Yin S. and Zhang E. and Qu Z. and Yin L. and Li S. (2014), "Optimal Cooperation Strategy in Cognitive Radio Systems with Energy Harvesting", *IEEE Transactions on Wireless Communications*, 13(9), pp. 4693-4707.

[94] Yiyang Pei and Ying-Chang Liang and Lan Zhang and Teh K.C. and Kwok Hung Li (2010), "Secure communication over MISO cognitive radio channels", *IEEE Transactions on Wireless Communications*, 9(4), pp. 1494-1502.

[95] Yongle Wu and Liu K.J.R. (2011), "An Information Secrecy Game in Cognitive Radio Networks", *IEEE Wireless Communications Letters*, 6(3), pp. 831-842.

[96] Yulong Zou and Xianbin Wang and Weiming Shen (2013), "Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks", *IEEE Transactions on Communications*, 61(12), pp. 5103-5113.

[97] Yulong Zou and Xuelong Li and Ying-Chang Liang (2014), "Secrecy Outage and Diversity Analysis of Cognitive Radio Systems", *IEEE Journal on Selected Areas in Communications*, 32(11), pp. 2222-2236.

[98] Zhang R. (2009), "On peak versus average interference power constraints for protecting primary users in cognitive radio networks", *IEEE Transactions on Wireless Communications*, 8(4), pp. 2112-2120.

[99] Zhang R., Kang X. and Liang Y. C. (2009), "Protecting Primary Users in Cognitive Radio Networks: Peak or Average Interference Power Constraint", *2009 IEEE International Conference on Communications*, pp. 1-5.

[100] Zhang R. and Ho C. K. (2013), "MIMO Broadcasting for Simultaneous Wireless Information and Power Transfer", *IEEE Transactions on Wireless Communications*, 12(5), pp. 1989-2001.

[101] Zheng G., Krikidis I., Masouros C., Timotheou S., Toumpakaris D. and Ding Z. (2014), "Rethinking the role of interference in wireless networks", *IEEE Communications Magazine*, 52(11), pp. 152-158.

[102] Zheng G. and Choo L. C. and Wong K. K. (2011), "Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relays", *IEEE Transactions on Signal Processing*, 59(3), pp. 1317-1322.

[103] Zhong C. and Chen X. and Zhang Z. and Karagiannidis G. K. (2015), "Wireless-Powered Communications: Performance Analysis and Optimization", *IEEE Transactions on Communications*, 63(12), pp. 5178-5190.

[104] Zhou X. and McKay M. R. (2010), "Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation", *IEEE Transactions on Vehicular Technology*, 59(8), pp. 3831-3842.

[105] Zhou X. and McKay M. R. and Maham B. and Hjorungnes A. (2011), "Rethinking the Secrecy Outage Formulation: A Secure Transmission Design Perspective", *IEEE Communications Letters*, 15(3), pp. 302-304.

[106] Zhu J. and Zou Y. and Wang G. and Yao Y. and Karagiannidis G. K. (2016), "On Secrecy Performance of Antenna-Selection-Aided MIMO Systems Against Eavesdropping", *IEEE Transactions on Vehicular Technology*, 65(1), pp. 214-225.

[107] Zou Y. and Yao Y. D. and Zheng B. (2012), "Opportunistic Distributed Space-Time Coding for Decode-and-Forward Cooperation Systems", *IEEE Transactions on Signal Processing*, 60(4), pp. 1766-1781.

[108] Zou Y. and Zhu J. and Zheng B. and Yao Y. D. (2010), "An Adaptive Cooperation Diversity Scheme With Best-Relay Selection in Cognitive Radio Networks", *IEEE Transactions on Signal Processing*, 58(10), pp. 5438-5445.

[109] Zou Y. and Wang X. and Shen W. (2013), "Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks", *IEEE Journal on Selected Areas in Communications*, 31(10), pp. 2099-2111.

[110] Zou Y. and Zhu J. and Wang X. and Leung V. C. M. (2015), "Improving physical-layer security in wireless communications using diversity techniques", *IEEE Network*, 29(1), pp. 42-48.

[111] Zou Y. and Zhu J. and Yang L. and Liang Y. C. and Yao Y. D. (2015), "Securing physical-layer communications for cognitive radio networks", *IEEE Communications Magazine*, 53(9), pp. 48-54.

[112] Zou Y. and Wang G. (2016), "Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack", *IEEE Transactions on Industrial Informatics*, 12(2), pp. 780-787.

[113] Zou Y. and Zhu, J. (2016), *Physical-layer security for cooperative relay networks*, Berlin: Springer.