# 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 |
| 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, 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.
- 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.***

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, một số kỹ thuật truyền thông và thu hoạch năng lượng không dây vào ứng dụng trong đời sống thực tiễn. Bổ sung các phương pháp 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.

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

*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 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 Bảo mật lớp vật lý cho mạng không dây

### 1.1.1 Kênh wiretap

Khái niệm kênh wiretap được giới thiệu bởi Wyner [40] với giả thiết rằng kênh EAV là một phiên bản tín hiệu suy thoái của kênh chính. Tiếp theo sau, các phát triển mở rộng cho kênh wiretap đến kênh tryền quản bá với bản tin bí mật, kênh wiretap Gaussian, và kênh fading wiretap [6, 19].

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

#### 1.1.2.1 Dung lượng kênh

Dung lượng kênh tức thời của một kênh fading được biểu diễn bởi công thức Shannon [10], như sau

$$C = B\log_2(1+\gamma) \tag{1.1}$$

trong đó $B$ là băng thông của kênh truyền và $\gamma$ là $SNR$ thu được.

#### 1.1.2.2 Dung lượng bảo mật kênh

Do tính chất không âm của dung lượng kênh, chúng ta có thể biểu diễn như sau [2, 30].

$$C_s = \begin{cases} \log_2(1+\gamma_m) - \log_2(1+\gamma_e), & \text{nếu } \gamma_m > \gamma_e \\ 0, & \text{nếu } \gamma_m \leq \gamma_e \end{cases} \tag{1.2}$$

trong đó $\gamma_m$, $\gamma_e$ lần lượt là SNR của kênh hợp pháp và kênh wiretap, tương ứng.

#### 1.1.2.3 Dung lượng bảo mật khác 0

$$Pr(C_s > 0) = Pr(\gamma_m > \gamma_e) \tag{1.3}$$

#### 1.1.2.4 Xác suất dừng bảo mật

$$SOP = Pr(C_s < R_s) \tag{1.4}$$

Với $R_s > 0$ là tốc độ bảo mật mong muốn của hệ thống.

## 1.2 Mạng vô tuyến nhận thức

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 sử 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 [11].

### 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. Bao gồm mô hình đan xen, mô hình dạng chồng và mô hình dạng nền. Trong đó, mô hình dạng nền được xem là mô hình có tính khả thi cao, ít phức tạp hơn và có nhiều ưu điểm. Mô hình dạng nền đang nhận được nhiều sự quan tâm nghiên cứu từ các nhà khoa học.

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

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 [28, 29, 44]. 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 chính (P-Tx), 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 [4, 14, 18, 26, 32, 43].

## 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 [17, 24, 25, 37]; Kỹ thuật tạo khóa

bảo mật mức vật lý [1, 24, 33], kỹ thuật đa ăng-ten [12, 16, 20–22, 34, 36, 46–48], và kỹ thuật hợp tác chuyển tiếp [7, 31, 49].

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 [8, 35, 50].

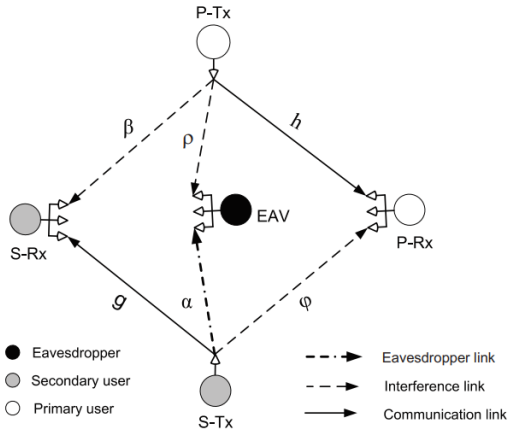
Trong các công trình nghiên cứu được công bố trước đây, mặc dù vấn đề phân tích hiệu suất cho bảo mật lớp vật lý cho mạng không dây, đặc biệt là mô hình mạng CRN đã có nhiều thành tựu [3, 13, 23, 27, 45, 51]. Tuy nhiên,việc xem xét ảnh tác động của kênh P-Tx→P-Rx đến hiệu suất bảo mật còn chưa được xem 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 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




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

Trong phần này, nhóm nghiên cứu sẽ xem xét một mô hình hệ thống như trong hình 2.1, 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. 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 $\varphi_m$, $\beta_n$, và $\rho_t$. Độ lợi kênh của kênh nghe trộm được biểu diễn là $\alpha_t$. 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, EVA, và P-Rx.

Theo định lý Shannon, dung lượng kênh của PU chịu ảnh hưởng can nhiễu từ SU có thể được biểu diễn như sau

$$C_p = B \log_2(1 + \gamma_p), \tag{2.1}$$

trong đó $\gamma_p$ là SINR của PU được định nghĩa là

$$\gamma_p = \max_{m \in \{1,2,\ldots,N_p\}} \left\{ \frac{P_p h_m}{P_s \varphi_m + N_0} \right\}, \tag{2.2}$$

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. Dung lượng kênh của SU và EAV được trình bày bởi công thức sau

$$C_s = B\log_2(1+\gamma_s), \tag{2.3}$$

$$C_e = B\log_2(1+\gamma_e). \tag{2.4}$$

trong đó $\gamma_s$ và $\gamma_e$ được tính bởi

$$\gamma_s = \max_{t\in\{1,2,\ldots,N_s\}}\left\{\frac{P_s g_t}{P_p\beta_t + N_0}\right\};\ \gamma_e = \max_{n\in\{1,2,\ldots,N_e\}}\left\{\frac{P_s\alpha_n}{P_p\rho_n + N_0}\right\}. \tag{2.5}$$

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

Theo [40, 41, 46], giả sử $R_0 > 0$ là tốc độ truyền từ mã có thể cung cấp truyền thông bảo mật cho các SU. Như vậy, 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

$$\mathcal{O}_{sec} = \Pr\{C_e > R_0\}. \tag{2.6}$$

Hơn nữa, 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

$$\mathcal{O}_p = \Pr\left\{C_p < R_p\right\}. \tag{2.7}$$

trong đó $C_p$ được định nghĩa bởi (2.1).

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 trong (2.6) và (2.7) đều không xảy ra. Điều này có thể được diễn giải thành xác suất truyền thông tin cậy và bảo mật như sau

$$\mathcal{O}_{ss} = \Pr\{C_s > R_s, C_e \le R_0\}, \tag{2.8}$$

trong đó $C_s$ và $C_e$ được trình bày trong (2.3) và (2.4), tương ứng.

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

#### 2.1.2.1 Kịch bản 1 ($S_1$): S-Tx không có CSI của các kênh 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 của nó dựa trên điều kiện ràng buộc can nhiễu của PU là

$$\mathcal{O}_I = \Pr\left\{\max_{m\in\{1,2,\ldots,N_p\}}\left\{\frac{P_s\varphi_m}{N_0}\right\} \ge Q_{pk}\right\} \le \xi, \tag{2.9}$$

Trong đó $Q_{pk}$ là mức can nhiễu tối đa mà PU có thể chấp nhận được. Kết quả là, các điều kiện thiết lập cho công suất phát của S-Tx cần phải thỏa mãn hai điều kiện như sau

$$\mathcal{O}_I \leq \xi, \tag{2.10}$$
$$0 \leq P_s \leq P_s^{max}, \tag{2.11}$$

trong đó $\xi$ là ngưỡng dừng truyền thông được đưa ra bởi PU và $P_s^{max}$ công suất phát 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 của S-Tx cần phải thỏa mãn ba điều kiện như sau

$$\mathcal{O}_I \leq \xi, \tag{2.12}$$
$$\mathcal{O}_{sec} \leq \epsilon, \tag{2.13}$$
$$0 \leq P_s \leq P_s^{max}, \tag{2.14}$$

trong đó $\epsilon$ là ngưỡng ràng buộc dừng bảo mật đối với SU, còn $\mathcal{O}_I$ và $\mathcal{O}_{sec}$ đã được định nghĩa trong (2.6) và (2.9), 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:

$$\mathcal{O}_p \leq \theta, \tag{2.15}$$
$$0 \leq P_s \leq P_s^{max}, \tag{2.16}$$

trong đó $\mathcal{O}_p$ được định nghĩa trong (2.7), và $\theta$ điều kiện dừng truyền thông của PU.

#### 2.1.2.4 Kịnh bản 4 ($S_4$): S-Tx có CSI của cả hai P-Tx→P-Rx và S-Tx→EAV

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:

$$\mathcal{O}_p \leq \theta, \tag{2.17}$$
$$\mathcal{O}_{sec} \leq \epsilon, \tag{2.18}$$
$$0 \leq P_s \leq P_s^{max}, \tag{2.19}$$

trong đó $\mathcal{O}_p$ và $\mathcal{O}_{sec}$ đã được định nghĩa trong (2.7) và (2.6).

## 2.2 Phân tích hiệu suất của hệ thống

### 2.2.1 Chính sách phân bổ công suất truyền tin

Sau một số bước tính toán, chúng ta 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 $S_1$

$$\mathcal{P}_{S_1} = \min\left\{\frac{Q_{pk}N_0}{\Omega_\varphi}\left(\log_e \frac{1}{1-\sqrt[N_p]{1-\xi}}\right)^{-1}, P_s^{max}\right\}. \tag{2.20}$$

- Thứ hai, chúng ta thu được chính sách phân bổ công suất cho kịch bản $S_2$

$$\mathcal{P}_{S_2} = \min\left\{\frac{Q_{pk}N_0}{\Omega_\varphi}\left(\log_e \frac{1}{1-\sqrt[N_p]{1-\xi}}\right)^{-1}, \frac{P_p\Omega_\rho\gamma_{th}^e}{\Omega_\alpha}\left(\frac{1}{\sqrt[N_e]{1-\epsilon}}-1\right), P_s^{max}\right\}. \tag{2.21}$$

- Thứ ba, công suất truyền tin của S-Tx cho kịnh bản $S_3$

$$\mathcal{P}_{S_3} = \min\left\{\frac{P_p\Omega_h}{\gamma_{th}^p\Omega_\varphi}\Xi, P_s^{max}\right\}, \tag{2.22}$$

trong đó $\Xi$ được định nghĩa là

$$\Xi = \max\left\{0, \frac{1}{1-\sqrt[N_p]{\theta}}\exp\left[-\frac{\gamma_{th}^p N_0}{P_p\Omega_h}\right]-1\right\}. \tag{2.23}$$

- Cuối cùng, công suất truyền của S-Tx cho kịnh bản $S_4$

$$\mathcal{P}_{S_4} = \min\left\{\frac{P_p\Omega_\rho\gamma_{th}^e}{\Omega_\alpha}\left(\frac{1}{\sqrt[N_e]{1-\epsilon}}-1\right), \frac{P_p\Omega_h}{\gamma_{th}^p\Omega_\varphi}\Xi, P_s^{max}\right\}. \tag{2.24}$$

### 2.2.2 Xác suất truyền thông tin cậy và bảo mật

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 (2.8) bằng

$$\mathcal{O}_{ss} = \Pr\{C_s > R_s\}\Pr\{C_e \le R_0\} = (1-\mathcal{O}_s)(1-\mathcal{O}_{sec}) \tag{2.25}$$

trong đó $\mathcal{O}_s$ và $\mathcal{O}_{sec}$ có được bằng cách sử dụng hỗ trợ của tính chất 1 trong tài liệu [**?**], theo đó

$$\mathcal{O}_s = \sum_{i=0}^{N_s}\binom{N_s}{i}\frac{(-1)^i}{(A_s\gamma_{th}^s+1)^i}\exp\left(-\frac{i\gamma_{th}^s}{D_s}\right) \tag{2.26}$$

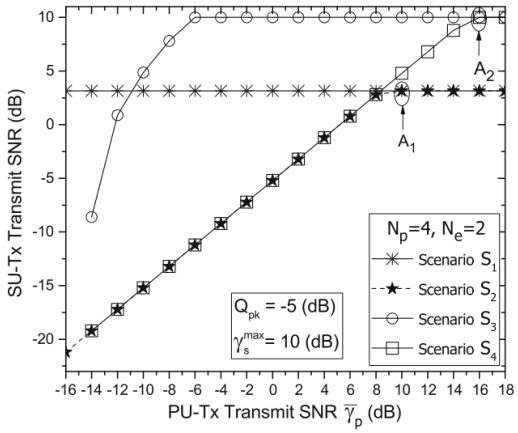
$$\mathcal{O}_{sec} = 1-\sum_{j=0}^{N_e}\binom{N_e}{j}\frac{(-1)^j}{(A_e\gamma_{th}^e+1)^j} \tag{2.27}$$

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 $\frac{1}{D_s} = \frac{N_0}{\mathcal{P}\Omega_g}$.

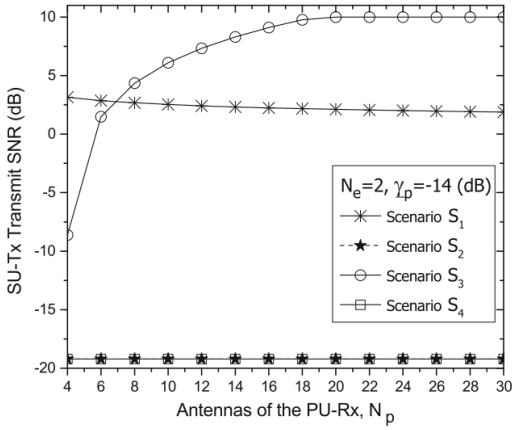
Cuối cùng, một biểu thức tường minh của một xác suất truyền thông tin cậy và bảo mật đạt được bằng cách thay thế (2.26) và (2.27) vào trong (2.25), trong đó $\mathcal{P} \in \{\mathcal{P}_{S_1}, \mathcal{P}_{S_2}, \mathcal{P}_{S_3}, \mathcal{P}_{S_4}\}$ là tập các chính sách phân bổ công suất truyền tin của SU.

## 2.3 Mô phỏng hệ thống

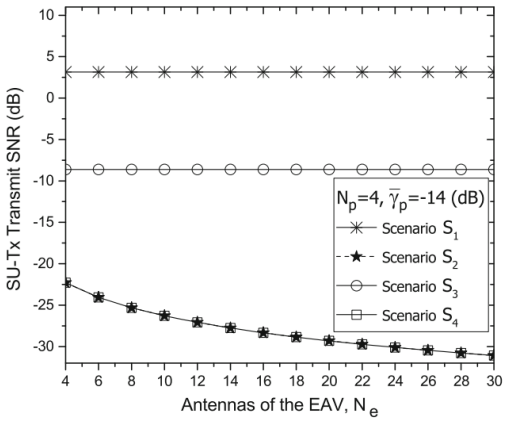
Các tham số cài đặt dưới đây trong các số liệu thử nghiệm đã được dùng tương tự và phổ biến trong rất nhiều các nghiên cứu ở lĩnh vực này như [9, 15]. Không mất tính tổng quát, chúng ta biểu diễn $\bar{\gamma}_s = \frac{\mathcal{P}}{N_0}$ và $\bar{\gamma}_p = \frac{P_p}{N_0}$ lần lượt là SNR của S-Tx và P-Tx khi thực hiện truyền tín hiệu.



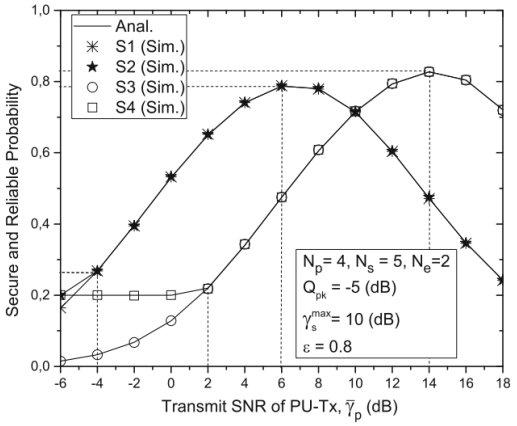

Hình 2.2: *SNR của S-Tx cho bốn kịch bản*



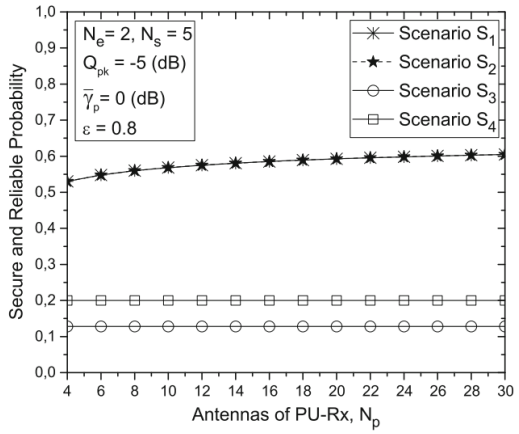

Hình 2.3: *Tác động của số ăng-ten P-Tx lên SNR của S-Tx*



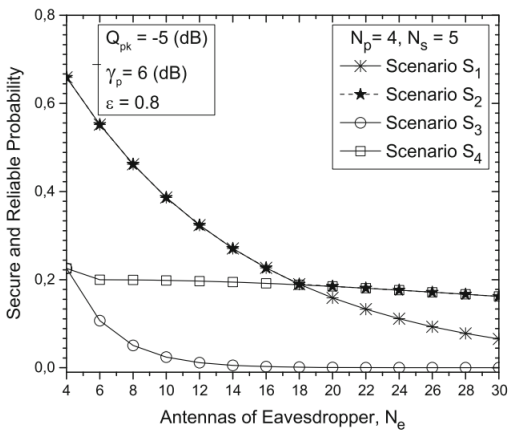

Hình 2.4: *Tác động của số ăng-ten EAV lên SNR của S-Tx*




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




Hình 2.6: *Tác động của số ăng-ten P-Tx lên SRCP*.




Hình 2.7: *Tác động của số ăng-ten EAV lên SRCP*.

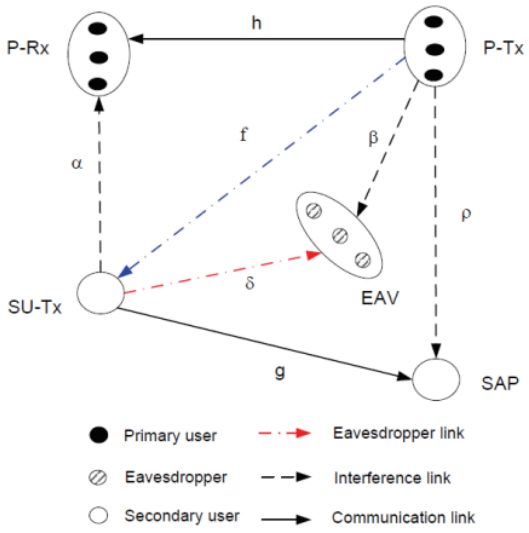
# Chương 3

# 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

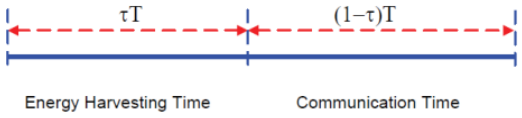
Chúng ta xem xét một mạng CRN như hình 3.1. Trong mô hình này, SAP được giả định được trang bị $M$ ăng-ten trong khi các thiết bị khác (P-Tx, P-Rx, EAV, và S-Tx) có một ăng-ten đơn. Độ lợi của các kênh truyền thông P-Tx$_n$→P-Rx$_n$ và S-Tx→SAP được kí hiệu là $h_n$, và $g_m$,




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.*

$n = 1, \ldots, N$, $m = 1, \ldots, M$. 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 $\beta_{nk}$, $\alpha_n$, và $\rho_{nm}$. Độ lợi kênh của kênh wire-tap S-Tx→EAV và kênh thu hoạch năng lượng P-Tx$_n$→S-Tx được biểu diễn tương ứng là $\delta_k$ và $f_n$, $k \in \{1, \ldots, K\}$.

### 3.1.2 Cơ chế truyền thông và thu hoạch năng lượng




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

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 $f_n$, $n \in \{1, 2, \ldots, N_e\}$.

$$E_s = \mathbf{E}\left[\sum_{n=1}^{N} \theta\tau T P_p f_n\right] = \theta\tau T P_p \, \mathbf{E}\left[\sum_{n=1}^{N} f_n\right], \tag{3.1}$$

  trong đó $\mathbf{E}[\cdot]$, $T$, và $\tau$ lần lượt là kỳ vọng, tổng thời gian, và một phần thời gian sử dụng để thu hoạch năng lượng, $0 < \tau < 1$. Kí hiệu $P_p$ và $\theta$ đại diện cho công suất phát 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. 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

$$P_{S-Tx}^{(n)} \leq P_{avg} = \frac{E_s}{(1-\tau)T} = \frac{\tau\theta P_p}{1-\tau} \sum_{n=1}^{N} \Omega_{f_n}, \tag{3.2}$$

  trong đó $P_{avg}$ được gọi là ngưỡng công suất trung bình được đưa ra bởi S-Tx.

## 3.2 Phân bổ công suất và lựa chọn kênh của SU

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

chính sách điều khiển công suất của SU chịu ràng buộc sau

$$\Pr\left\{C_p^{(n)} \leq R_p\right\} \leq \eta_p, \tag{3.3}$$

$$P_{S-Tx}^{(n)} \leq P_{avg}, \tag{3.4}$$

trong đó $R_p$, $\eta_p$, 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.

$$C_p^{(n)} = B \log_2\left(1 + \gamma_p^{(n)}\right), \tag{3.5}$$

trong đó $B$ là băng thông và $\gamma_p^{(n)}$ là SINR của PU được cho bởi $\gamma_p^{(n)} = \frac{P_p h_n}{P_{S-Tx}^{(n)} \alpha_n + N_0}$, với $N_0$ là công suất nhiễu nền. Phân tích biểu thức xác suất (3.3), chúng ta có

$$P_{S-Tx}^{(n)} \leq P_{PU}^{(n)} = \frac{1}{A_n}\left[\frac{\exp(-B_n)}{1-\eta_p} - 1\right]. \tag{3.6}$$

Với $A_n = \frac{\gamma_{th}^p \Omega_{\alpha_n}}{P_p \Omega_{h_n}}$, $B_n = \frac{\gamma_{th}^p N_0}{P_p \Omega_{h_n}}$, $\gamma_{th}^p = 2^{\frac{R_p}{B}} - 1$.

Kết hợp (3.6) với (3.4), 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

$$P_{S-Tx}^{(n)} \leq \min \left\{ P_{PU}^{(n)}, P_{avg} \right\}, \tag{3.7}$$

### 3.2.2 Giới hạn công suất của S-Tx dưới các yêu cầu bảo mật thông tin khi có nhiều EAV

Điều kiện dừng bảo mật và điều kiện công suất phát tín hiệu của S-Tx như sau

$$\Pr \left\{ \max_{k \in \{1,\dots,K\}} \left\{ C_e^{(n,k)} \right\} \geq R_e \right\} \leq \xi, \tag{3.8}$$

$$P_{S-Tx}^{(n)} \leq P_{avg}, \tag{3.9}$$

trong đó $R_e$ và $\xi$ 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 $\text{EAV}_k$ trên kênh S-Tx$\rightarrow\text{EAV}_k$ khi S-Tx lựa chọn băng tần $n$ để truyền tin, được định nghĩa là

$$C_e^{(n,k)} = B \log_2 \left( 1 + \gamma_e^{(n,k)} \right), \tag{3.10}$$

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

$$\gamma_e^{(n,k)} = \frac{P_{S-Tx}^{(n)} \delta_k}{P_p \beta_{nk} + N_e} \approx \frac{P_{S-Tx}^{(n)} \delta_k}{P_p \beta_{nk}}, \tag{3.11}$$

trong đó $N_e$ là công suất của nhiễu nền is tại EAV.

Phân tích biểu thức (3.8), chúng ta thu được điều kiện cho công suất của S-Tx để đối phó với các thiết bị nghe trộm như sau

$$P_{S-Tx}^{(n)} \leq P_{Eav}^{(n)} = \frac{\gamma_{th}^e P_p \Omega_{\beta_n} (1 - \sqrt[K]{1-\xi})}{\Omega_\delta \sqrt[K]{1-\xi}}. \tag{3.12}$$

Kết hợp (3.12) với điều kiện thu hoạch năng lượng (3.9), ta có

$$P_{S-Tx}^{(n)} \leq \min \left\{ P_{Eav}^{(n)}, P_{avg} \right\}, \tag{3.13}$$

Kết quả là, công suất truyền tin của S-Tx trong kênh $n$-th có được bằng cách kết hợp (3.7) với(3.13)

$$P_{S-Tx}^{(n)} = \min \left\{ \min\{ P_{PU}^{(n)}, P_{Eav}^{(n)} \}, P_{avg} \right\}. \tag{3.14}$$

Từ (3.14), 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

$$P_{S-Tx}^{(n)} = \min\{ P_{PU}^{(n)}, P_{Eav}^{(n)} \}, \tag{3.15}$$

- *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 $\tau$ để có thể tối đa hóa giá trị của $P_{avg}$ là

$$\tau^* = \frac{\min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}}{\theta P_p \sum_{n=1}^{N} \Omega_{f_n} + \min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}}. \tag{3.16}$$

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

$$n^* = \arg \max_{n \in \{1,2,\ldots,N_e\}} \left\{ P_{S-Tx}^{(n)} \right\}, \tag{3.17}$$

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

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

## 3.3 Phân tích hiệu suất hệ thống

### 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

$$\mathcal{O} = \Pr\{\gamma_s \leq \gamma_{th}\}, \tag{3.18}$$

trong đó $\gamma_{th}$ là ngưỡng giá trị SINR xác định của SU và $\gamma_s$ được định nghĩa là

$$\gamma_s = \max_{m \in \{1,2,\ldots,N_p\}} \left\{ \frac{P_{S-Tx}^{(n^*)} g_m}{P_p \rho_{n^* m} + N_0} \right\}. \tag{3.19}$$

Từ đó, PEP có thể được tính toán bằng cách sử dụng tính chất trong [38, Property 1] như sau

$$\mathcal{O} = \left( 1 - \frac{\exp\left( -\frac{\gamma_{th} N_0}{P_{S-Tx}^{(n^*)} \Omega_g} \right)}{\frac{\gamma_{th} P_p \Omega_{\rho_{n^*}}}{P_{S-Tx}^{(n^*)} \Omega_g} + 1} \right)^M. \tag{3.20}$$

### 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 $\ell$ lần truyền được mô tả là

$$\Pr\{L = \ell\} = \mathcal{O}^{\ell - 1}(1 - \mathcal{O}), \tag{3.21}$$

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

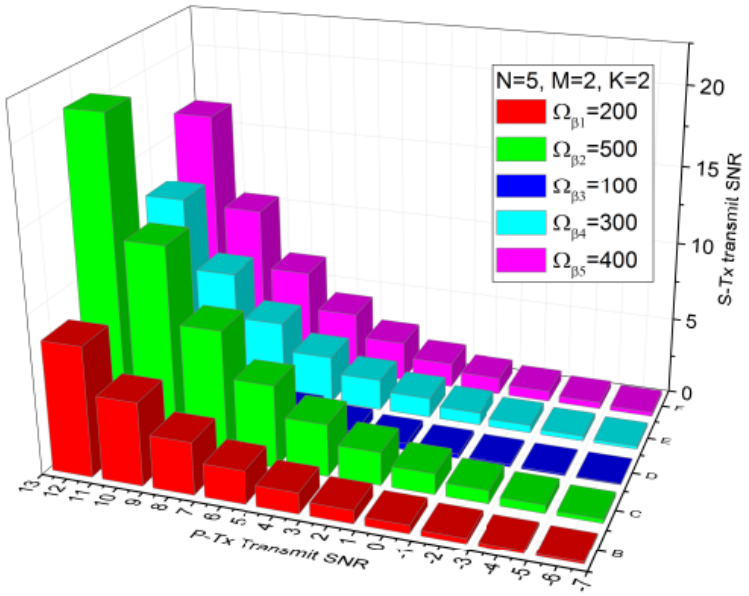
$$\mathbf{E}[L] = \sum_{\ell=1}^{\infty} \ell \mathcal{O}^{\ell-1}(1-\mathcal{O}) = \frac{1}{1-\mathcal{O}}. \tag{3.22}$$

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

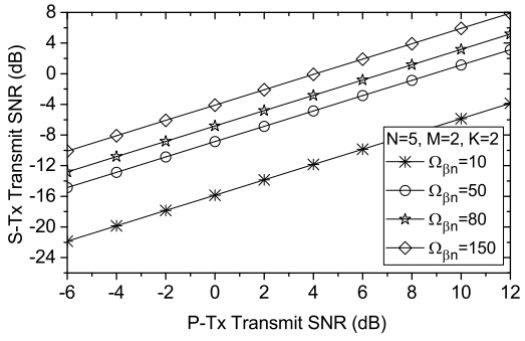
$$D = T\,\mathbf{E}[L] = \frac{T}{1-\mathcal{O}}, \tag{3.23}$$

trong đó $T$ là tổng khung thời gian và $\mathcal{O}$ là PEP được định nghĩa trong (3.18).

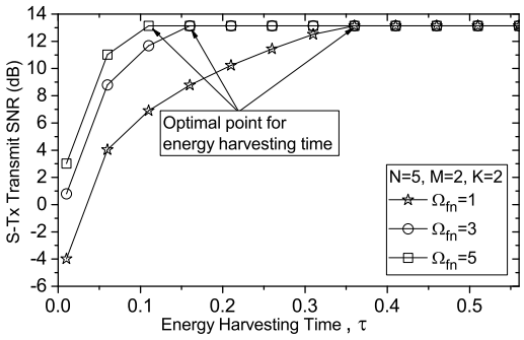
## 3.4 Mô phỏng hệ thống



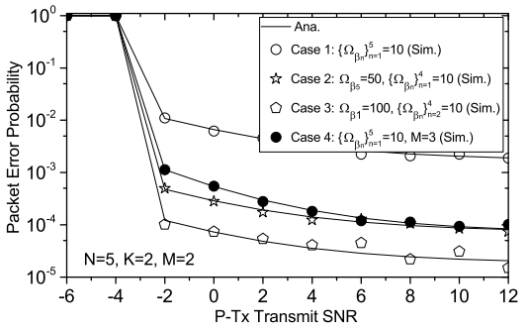

Hình 3.3: *Ảnh hưởng của $\Omega_{\beta_n}$ của P-Tx→EAV lên SNR của S-Tx.*



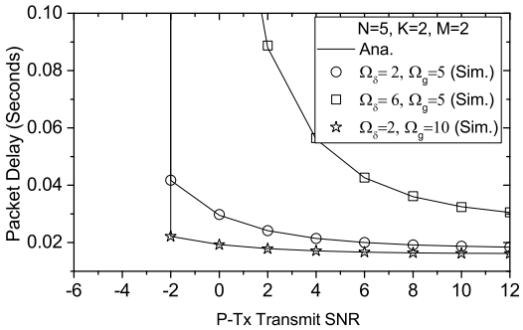

Hình 3.4: *SNR của S-Tx theo SNR của P-Tx với các* $\{\Omega_{\beta_n}\}_{n=1}^{5} = 10, 50, 80, 150$.




Hình 3.5: *SNR của S-Tx theo* $\tau$ *và* $\{\Omega_{f_n}\}_{n=1}^{5} = 1, 3, 5$, *và* $\gamma_{P-Tx} = 12\,dB$.




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




Hình 3.7: *Độ trễ của gói tin*.

# 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] Aono T. and Higuchi K. and Taromaru M. and Ohira T. and Sasaoka H. (2005), "Wireless secret key generation exploiting the reactance-domain scalar response of multipath fading channels : RSSI interleaving scheme", *The European Conference on Wireless Technology 2005*, pp. 173-176.

[2] 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.

[3] 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.

[4] 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.

[5] Clancy T. C. (2007), "Formalizing the interference temperature model", *Wireless Communications and Mobile Computing*, 7(9), pp. 1077–1086.

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

[7] 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.

[8] 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.

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

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

[16] 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.

[17] 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.

[18] 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.

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

[20] 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.

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

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] Ren K. and Su H. and Wang Q. (2011), "Secret key generation exploiting channel characteristics in wireless communications", *IEEE Wireless Communications*, 18(4), pp. 6-12.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] Tran H. and Zepernick H. J. and 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.

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

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

[41] 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.

[42] Yacoub M. D. (2007), "The $\alpha$-$\mu$ Distribution: A Physical Fading Model for the Stacy Distribution", *IEEE Transactions on Vehicular Technology*, 51(1), pp. 27-34.

[43] 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.

[44] 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.

[45] 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.

[46] 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.

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] 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.