ĐẠI HỌC QUỐC GIA HA NỘI
**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ**

**QUÁCH XUÂN TRƯỞNG**

# ĐÁNH GIÁ HIỆU NĂNG BẢO MẬT TẦNG VẬT LÝ TRONG MẠNG KHÔNG DÂY

CHUYÊN NGÀNH: TRUYỀN DỮ LIỆU VÀ MẠNG MÁY TÍNH
MÃ SỐ: 9480102.01

TÓM TẮT LUẬN ÁN TIẾN SĨ CÔNG NGHỆ THÔNG TIN

**Hà Nội - 2020**

Công trình được hoàn thành tại: Trường đại học Công Nghệ, Đại học Quốc Gia Hà Nội

Người hướng dẫn khoa học: **TS. Trần Hùng**
**TS. Trần Trúc Mai**

Phản biện :.....
.....
Phản biện :.....
.....
Phản biện :.....
.....

Luận án sẽ được bảo vệ trước Hội đồng cấp Đại học Quốc Gia chấm luận án tiến sĩ họp tại .....
vào hồi.....giờ..... ngày..... tháng.....năm 2020

Có thể tìm hiểu luận án tại:

- Thư viện Quốc gia, Việt Nam
- Trung tâm Thông tin - Thư viện, Đại học Quốc Gia Hà Nội

# MỤC LỤC

# CÁC TỪ VIẾT TẮT

| Từ viết tắt | Từ gốc |
|---|---|
| APD | Average packet delay |
| CDF | Cumulative distribution function |
| CRN | Cognitive radio network |
| CCRN | Cognitive cooperative radio network |
| CSI | Channel state information |
| DF | Decode-and-forward |
| EAV | Eavesdropper |
| P-Rx | Primary receiver |
| P-Tx | Primary transmitter |
| PDF | Probability density function |
| PEP | Packet error probability |
| PU | Primary user |
| QoS | Quality of Service |
| RF | Radio Frequency |
| RFEH | Radio Frequency Energy Harvesting |
| SC | Selection combining |
| S-Rx | Secondary receiver |
| S-Tx | Secondary transmitter |
| SINR | Signal-to-interference-plus-noise ratio |
| SNR | Signal-to-noise radio |
| SRCP | Secure and reliable communication probability |
| SU | Secondary user |

**Chương 1**

# Kiến thức cơ sở và tổng quan

## 1.1 Mô hình kênh truyền

### 1.1.1 Tính chất của kênh truyền không dây

Các mô hình thống kê được sử dụng để mô tả cho các kênh truyền fading. Việc áp dụng mô hình thông kê nào phụ thuộc vào từng loại môi trường truyền sóng vô tuyến cụ thể. Trong luận án này, tác giả nghiên cứu và áp dụng phân bố Rayleigh trong kênh truyền cho các mô hình mạng.

### 1.1.2 Truyền thông hợp tác

Hợp tác trong truyền thông là một kỹ thuật có nhiều ưu điểm để nâng cao QoS của các hệ thống truyền thông không dây, kỹ thuật này được thực hiện với nhiều nút mạng cùng tham gia trong việc truyền và giải mã các bản tin .

### 1.1.3 Mạng vô tuyến nhận thức (CRN)

CRN gồm ba loại mô hình chính phụ thuộc vào kỹ thuật được sử dụng để cho phép SU sử dụng các dải tần số đã được cấp phép cho PU. Bao gồm mô hình đan xen, mô hình dạng chồng và mô hình dạng dưới ngưỡng nhiễu. Trong đó, mô hình dạng dưới ngưỡng nhiễu được xem là mô hình có tính khả thi cao, ít phức tạp hơn và đang nhận được nhiều sự quan tâm nghiên cứu.

## 1.2 Bảo mật lớp vật lý cho mạng không dây

Khái niệm kênh wiretap được giới thiệu bởi Wyner [7] 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 các kênh wiretap Gaussian, và kênh fading wiretap [2,5].

### 1.2.1 Độ đo đánh gía hiệu năng bảo mật hệ thống

Hiệu năng bảo mật của các hệ thống mạng không dây trong các kênh truyền fading được đánh giá chủ yếu thông qua ba tham số chính: Dung lượng bảo mật kênh, Xác suất dừng bảo mật và Xác suất khác 0 của dung lượng bảo mật [1,3,6].

### 1.2.2 Tổng quan tình hình nghiên cứu

Từ nghiên cứu về bảo mật dựa trên lý thuyết thông tin của Shannon và kênh wiretap của Wyner, Các nỗ lực nghiên cứu đã tập chung phát triển các kỹ thuật bảo mật lớp vật lý khác nhau với các hướng chính sau: Mã hóa và xử lý tín hiệu, tạo khóa bảo mật mức vật lý, đa ăng-ten, can nhiễu và chuyển tiếp. CRN là một mô

hình mạng nhiều tiềm năng để khắc phục được các hạn chế của các mạng không dây thế hệ mới. Tuy nhiên, với đặc điểm của CRN dẫn đến xuất hiện nhiều điểm yếu từ khía cạnh an toàn và bảo mật thông tin. Trong các nghiên cứu được công bố, mặc dù vấn đề phân tích hiệu suất cho bảo mật lớp vật lý cho mạng không dây, cụ thể là mô hình CRN đã có nhiều thành tựu. Tuy nhiên, việc xem xét tác động của kênh P-Tx→P-Rx đến hiệu suất bảo mật còn để ngỏ. Mặt khác, cũng chưa có nhiều tài liệu nghiên cứu phân tích hiệu suất về truyền thông tin cậy và bảo mật với nhiều tiếp cận điều kiện phụ thuộc khác nhau của hệ thống. Trong chương 2, nhóm nghiên cứu thực hiện đánh giá hiệu suất truyền thông tin cậy và bảo mật cho CRN. Hơn nữa, mặc dù đã cũng có khá nhiều kết quả thú vị đã được công bố phân tích hiệu suất trong CRN kết hợp kỹ thuật RFEH. Tuy nhiên, việc sử dụng tín hiệu can nhiễu từ nhiều PU để thu năng lượng, ngăn chặn EAV nghe trộm thông tin và đồng thời tăng cường độ tin cậy của truyền thông đối với CRN còn chưa được đề cập đến. Do đó, luận án tiếp tục nghiên cứu mô hình mạng CRN với kỹ thuật RFEH, xây dựng giải pháp truyền thông để không chỉ tăng cường hiệu quả sử dụng phổ tần và sử dụng năng lượng xanh, mà còn đảm bảo bảo mật thông tin cho SU trong điều kiện nhất định.

Tiếp theo, luận án đã khảo sát hai mô hình truyền thông nhằm khai thác các kỹ thuật truyền thông hợp tác để cải thiện hiệu suất bảo mật cho mạng CCRN trong Chương 3. Mặt khác, Qua quá trình khảo sát, tác giả nhận thấy ảnh hưởng quan trọng của các tham số hệ thống đối với hiệu suất và an toàn truyền thông. Do đó, luận án đã phân tích nghiên cứu giải pháp tối ưu giá trị giới hạn bảo mật nhằm nâng cao hiệu quả truyền thông an toàn.

**Chương 2**

# Đánh giá hiệu năng của truyền thông tin cậy và bảo mật thông tin trong mạng vô tuyến nhận thức

## 2.1 Mô hình #2.1

### 2.1.1 Mô hình hệ thống

Theo Hình 2.1, S-Tx và P-Tx có một ăng-ten đơn trong khi S-Rx, P-Rx và EAV có $N_s$, $N_p$ và $N_e$ ăng-ten. Độ lợi của S-Tx→S-Rx, P-Tx→P-Rx, S-Tx→P-Rx, P-Tx→S-Rx, P-Tx→EAV, và S-Tx→EAV được ký hiệu là $g_t, h_m, \varphi_m, \beta_n, \rho_t$ và $\alpha_t$, với $m \in \{1, \ldots, N_p\}, n \in \{1, \ldots, N_e\}$, và $t \in \{1, \ldots, N_s\}$. Dung lượng kênh của PU được biểu diễn là

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

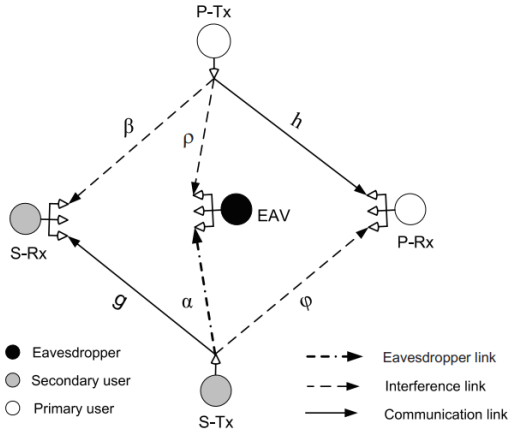
trong đó $\gamma_p = \max_{m \in \{1,2,\ldots,N_p\}} \left\{ \frac{P_p h_m}{P_s \varphi_m + N_0} \right\}$ là SINR của PU. $P_p$, $P_s$ là công suất của P-Tx và S-Tx. $N_0$ là công suất nhiễu AWGN.

Dung lượng kênh của SU và EAV là

$$C_s = B \log_2(1 + \gamma_s) \tag{2.2}$$

$$C_e = B \log_2(1 + \gamma_e) \tag{2.3}$$

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




Hình 2.1: *Mô hình CRN và EAV*

#### 2.1.1.1 Độ đo hiệu suất truyền thông tin cậy và bảo mật

Giả sử $R_0 > 0$ là tốc độ truyền từ mã có thể cung cấp truyền thông bảo mật cho các SU. Xác suất truyền thông tin cậy và bảo mật của SU được biểu diễn như sau

$$\mathcal{O}_{ss} = \Pr\left\{C_s > R_s, C_e \leq R_0\right\}, \tag{2.4}$$

trong đó $C_s$ và $C_e$ được trình bày trong (2.2) và (2.3), tương ứng.

#### 2.1.1.2 Các điều kiện cho công suất truyền tin của SU

• ***Kịch bản 1 ($S_1$)*:** S-Tx không có CSI của P-Tx→P-Rx, và S-Tx→EAV. Đặt $\xi$ là ngưỡng dừng truyền thông của PU, và $P_s^{max}$ là

công suất phát tối đa của S-Tx. Ta có

$$\mathcal{O}_I = \Pr\left\{\max_{m\in\{1,2,\ldots,N_p\}}\left\{\frac{P_s\varphi_m}{N_0}\right\} \geq Q_{pk}\right\} \leq \xi \tag{2.5}$$

$$0 \leq P_s \leq P_s^{max} \tag{2.6}$$

• ***Kịch bản 2 ($S_2$)*:** S-Tx có CSI của S-Tx→EAV nhưng không có CSI của P-Tx→P-Rx. Đặt $\epsilon$ là ngưỡng dừng bảo mật của SU. Ta có

$$\mathcal{O}_I \leq \xi \tag{2.7}$$

$$\mathcal{O}_{sec} \leq \epsilon \tag{2.8}$$

$$0 \leq P_s \leq P_s^{max} \tag{2.9}$$

• ***Kịch bản 3 ($S_3$)*:** S-Tx có CSI của P-Tx→P-Rx nhưng không có CSI của S-Tx→EAV. Đặt $\theta$ là ngưỡng dừng truyền thông của PU. Ta có

$$\mathcal{O}_p = \Pr\left\{C_p < R_p\right\} \leq \theta \tag{2.10}$$

$$0 \leq P_s \leq P_s^{max} \tag{2.11}$$

• ***Kịch bản 4 ($S_4$)*:** S-Tx có CSI của cả P-Tx→P-Rx và S-Tx→EAV. Công suất truyền tin của S-Tx chịu ba điều kiện như sau:

$$\mathcal{O}_p \leq \theta \tag{2.12}$$

$$\mathcal{O}_{sec} \leq \epsilon \tag{2.13}$$

$$0 \leq P_s \leq P_s^{max} \tag{2.14}$$

### 2.1.2 Phân tích hiệu suất của hệ thống

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

$$\mathcal{P}_{S_1} = \min\left\{\frac{Q_{pk}N_0}{\Omega_\varphi}\Psi, P_s^{max}\right\} \tag{2.15}$$

$$\mathcal{P}_{S_2} = \min\left\{\frac{Q_{pk}N_0}{\Omega_\varphi}\Psi, \frac{P_p\Omega_\rho\gamma_{th}^e}{\Omega_\alpha}\left(\frac{1}{\sqrt[N_e]{1-\epsilon}}-1\right), P_s^{max}\right\} \quad (2.16)$$

$$\mathcal{P}_{S_3} = \min\left\{\frac{P_p\Omega_h}{\gamma_{th}^p\Omega_\varphi}\Xi, P_s^{max}\right\} \quad (2.17)$$

$$\mathcal{P}_{S_4} = \min\left\{\frac{P_p\Omega_\rho\gamma_{th}^e}{\Omega_\alpha}\left(\frac{1}{\sqrt[N_e]{1-\epsilon}}-1\right), \frac{P_p\Omega_h}{\gamma_{th}^p\Omega_\varphi}\Xi, P_s^{max}\right\} \quad (2.18)$$

với $\Psi = \left(\log_e \frac{1}{1-\sqrt[N_p]{1-\xi}}\right)^{-1}$, và $\Xi = \max\left\{0, \frac{1}{1-\sqrt[N_p]{\theta}}\exp\left[-\frac{\gamma_{th}^p N_0}{P_p\Omega_h}\right]-1\right\}$.

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

Xác suất trong (2.4) có thể viết lại như sau

$$\mathcal{O}_{ss} = \Pr\{C_s > R_s\}\Pr\{C_e \le R_0\} \quad (2.19)$$

$$= (1-\mathcal{O}_s)(1-\mathcal{O}_{sec}) \quad (2.20)$$

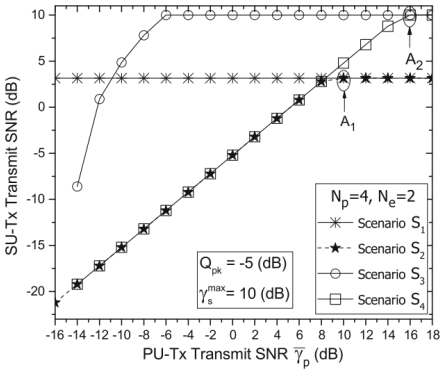
trong đó $\mathcal{O}_s$ và $\mathcal{O}_{sec}$ tính được như sau

$$\mathcal{O}_s = \sum_{i=0}^{N_s}\binom{N_s}{i}\frac{(-1)^i}{(A_s\gamma_{th}^s+1)^i}\exp\left(-\frac{i\gamma_{th}^s}{D_s}\right) \quad (2.21)$$

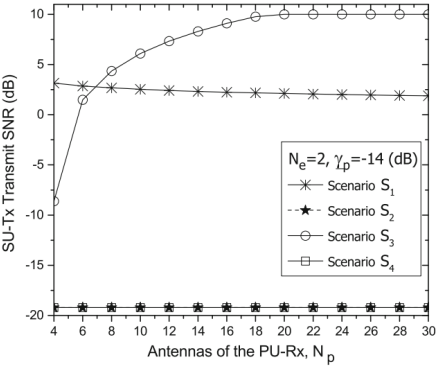
$$\mathcal{O}_{sec} = 1-\sum_{j=0}^{N_e}\binom{N_e}{j}\frac{(-1)^j}{(A_e\gamma_{th}^e+1)^j} \quad (2.22)$$

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 $\frac{1}{D_s} = \frac{N_0}{\mathcal{P}\Omega_g}$. $\mathcal{P} \in \{\mathcal{P}_{S_1}, \mathcal{P}_{S_2}, \mathcal{P}_{S_3}, \mathcal{P}_{S_4}\}$.

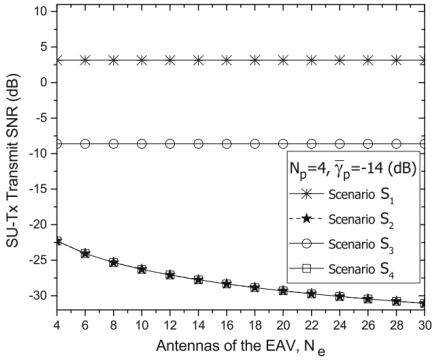
### 2.1.3 Mô phỏng và đánh giá kết quả



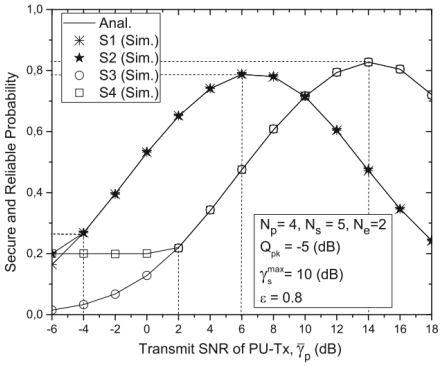

Hình 2.2: *SNR truyền tin của S-Tx cho bốn kịch bản theo SNR của P-Tx.*



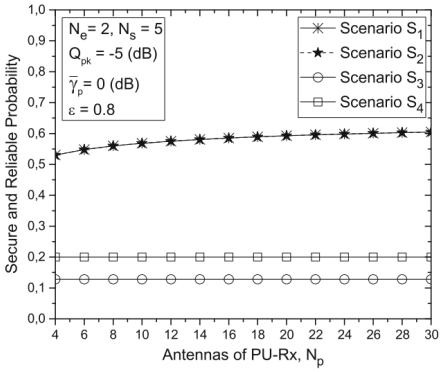

Hình 2.3: *Ảnh hưởng của số lượng ăng-ten của P-Tx lên SNR của S-Tx.*



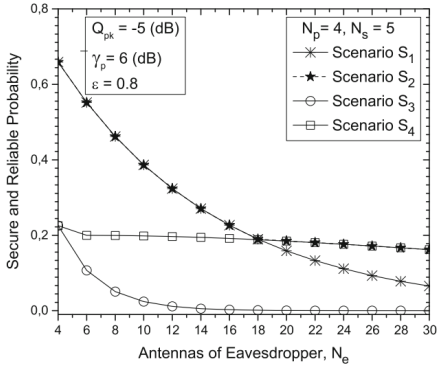

Hình 2.4: *Ảnh hưởng của số lượng ăng-ten của EAV lên SNR của S-Tx.*




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.*




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

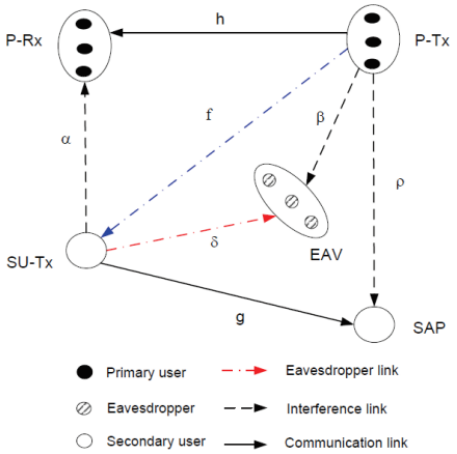
## 2.2 Mô hình #2.2

### 2.2.1 Mô hình hệ thống

#### 2.2.1.1 Mô hình hệ thống và các giả thuyết về kênh truyền

Xét mô hình hệ thống như Hình 2.8, SAP được giả định được trang bị $M$ ăng-ten trong khi P-Tx, P-Rx, EAV, và S-Tx có một ăng-

ten đơn. Độ lợi của các kênh P-Tx$_n$→P-Rx$_n$ và S-Tx→SAP được kí



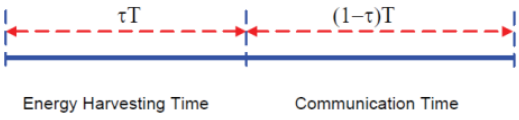

Hình 2.8: *Mô hình mạng CRN, trong đó S-Tx sử dụng năng lượng thu được từ các P-Tx để truyền thông trong khu vực có nhiều EAV.*

hiệu là $h_n$, và $g_m$, với $n = 1, \ldots, N$, $m = 1, \ldots, M$. Độ lợi $g_m$ biểu diễn cho kênh từ S-Tx đến nhánh $m$-ăngten của SAP. Độ lợi của các P-Tx$_n$→EAV$_k$, S-Tx→P-Rx$_n$, P-Tx$_n$→SAP được kí hiệu bởi $\beta_{nk}$, $\alpha_n$, và $\rho_{nm}$. Độ lợi của kênh wiretap S-Tx→EAV và kênh thu hoạch năng lượng P-Tx$_n$→S-Tx được biểu diễn tương ứng là $\delta_k$ và $f_n$, $k \in \{1, \ldots, K\}$.

#### 2.2.1.2 Giao thức truyền thông

- Bước 1: S-Tx thu hoạch năng lượng của $N$ thiết bị P-Tx thông qua $N$ kênh $f_n$, $n \in \{1, 2, \ldots, N\}$.

$$E_s = \mathbf{E}\left[\sum_{n=1}^{N} \theta\tau T P_p f_n\right] = \theta\tau T P_p \, \mathbf{E}\left[\sum_{n=1}^{N} f_n\right] \tag{2.23}$$




Hình 2.9: *Khung thời gian T để thu năng lượng và truyền thông.*

trong đó $\mathbf{E}[\cdot]$, $T$, và $\tau$ lần lượt là kỳ vọng, khung thời gian, và một phần của khung thời gian để thu hoạch năng lượng, $0 < \tau < 1$. Kí hiệu $P_p$ và $\theta$ là 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: Công suất phát của S-Tx trong $(1-\tau)T$ và tại kênh $n$-th là $P_{S-Tx}^{(n)}(1-\tau)T \leq E_s$. Do đó, chúng ta có

$$P_{S-Tx}^{(n)} \leq P_{avg} = \frac{E_s}{(1-\tau)T} = \frac{\tau\theta P_p}{1-\tau}\sum_{n=1}^{N}\Omega_{f_n} \tag{2.24}$$

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

### 2.2.2 Phân bổ công suất và chọn kênh của SU

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

Chính sách điều khiển công suất của SU chịu ràng buộc điều kiện của PU như sau

$$P_{S-Tx}^{(n)} \leq \min\left\{P_{PU}^{(n)}, P_{avg}\right\} \tag{2.25}$$

Với $P_{PU}^{(n)} = \frac{1}{A_n}\left[\frac{\exp(-B_n)}{1-\eta_p} - 1\right]$, $A_n = \frac{\gamma_{th}^p \Omega_{\alpha_n}}{P_p \Omega_{h_n}}$, $B_n = \frac{\gamma_{th}^p N_0}{P_p \Omega_{h_n}}$, $\gamma_{th}^p = 2^{\frac{R_p}{B}} - 1$. Trong đó $R_p$, $\eta_p$, và $B$ lần lượt là tốc độ xác định, điều kiện dừng, và băng thông của PU.

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

công suất truyền tin của S-Tx trong kênh $n$-th với điều kiện bảo mật thông tin có được như sau

$$P_{S-Tx}^{(n)} = \min\left\{\min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}, P_{avg}\right\}. \tag{2.26}$$

Với $P_{Eav}^{(n)} = \frac{\gamma_{th}^{e} P_p \Omega_{\beta_n} (1 - \sqrt[K]{1-\xi})}{\Omega_{\delta} \sqrt[K]{1-\xi}}$, $\gamma_{th}^{e} = 2^{\frac{R_e}{B}} - 1$ . Trong đó $R_e$ và $\xi$ lần lượt là tốc độ bảo mật xác định và điều kiện dừng bảo mật, $n$ là chỉ số băng tần được S-Tx chọn để truyền tin.

#### 2.2.2.3 Tối ưu hóa thời gian thu hoạch năng lượng và chọn kênh truyền thông

Từ (2.26), chúng ta xem xét hai trường hợp như sau:

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

$$P_{S-Tx}^{(n)} = \min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}, \tag{2.27}$$

- *Trường hợp 2:* $P_{avg} \leq \min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}$, công suất của S-Tx phụ thuộc vào năng lượng thu được, nghĩa là, $P_{S-Tx}^{(n)} = P_{avg}$. Hơn nữa, S-Tx luôn mong muốn giá trị của $P_{avg}$ đạt mức cao nhất, tức là, $P_{avg} = \min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}$. Do đó giá trị $\tau$ thu được như sau

$$\tau^* = \frac{\min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}}{\theta P_p \sum_{n=1}^{N} \Omega_{f_n} + \min\{P_{PU}^{(n)}, P_{Eav}^{(n)}\}}. \tag{2.28}$$

Ngoài ra, S-Tx lựa chọn kênh tốt nhất để có thể tối đa công suất truyền tin, kênh được chọn như sau

$$n^* = \arg \max_{n \in \{1,2,\ldots,N_e\}} \left\{ P_{S-Tx}^{(n)} \right\}, \tag{2.29}$$

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

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

### 2.2.3 Phân tích hiệu suất hệ thống

#### 2.2.3.1 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

$$\mathcal{O} = \Pr\{\gamma_s \leq \gamma_{th}\} \tag{2.30}$$

trong đó $\gamma_{th}$ là ngưỡng giá trị SINR xác định của SU và $\gamma_s = \max_{m \in \{1,2,\ldots,N_p\}} \left\{ \frac{P_{S-Tx}^{(n^*)} g_m}{P_p \rho_{n^* m} + N_0} \right\}$. Từ đó, PEP có thể thu được như sau

$$\mathcal{O} = \left( 1 - \frac{\exp\left( -\frac{\gamma_{th} N_0}{P_{S-Tx}^{(n^*)} \Omega_g} \right)}{\frac{\gamma_{th} P_p \Omega_{\rho_{n^*}}}{P_{S-Tx}^{(n^*)} \Omega_g} + 1} \right)^M \tag{2.31}$$

#### 2.2.3.2 Độ trễ gói tin với việc truyền sửa lỗi

Xác suất mà một gói tin được truyền đi thành công sau $\ell$ lần truyền được mô tả là

$$\Pr\{L = \ell\} = \mathcal{O}^{\ell-1}(1 - \mathcal{O}) \tag{2.32}$$

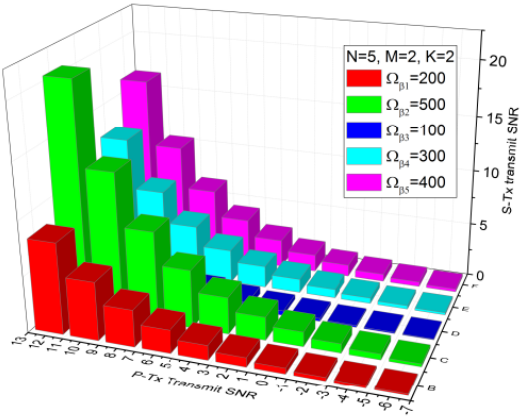
trong đó $L$ là số lần truyền một gói tin. Do đó, số lần truyền trung bình trên gói tin có thể được tính toán như sau

$$\mathbf{E}[L] = \sum_{\ell=1}^{\infty} \ell \mathcal{O}^{\ell-1}(1-\mathcal{O}) = \frac{1}{1-\mathcal{O}} \tag{2.33}$$

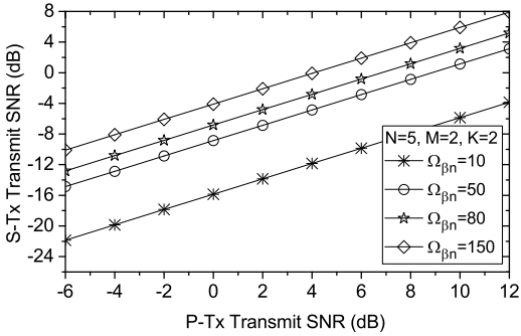
Cuối cùng, độ trễ trung bình để truyền thành công một gói tin có thể được tính như dưới đây

$$D = T\,\mathbf{E}[L] = \frac{T}{1-\mathcal{O}} \tag{2.34}$$

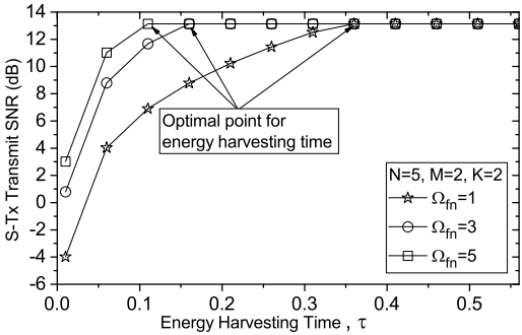
### 2.2.4 Mô phỏng và đánh giá kết quả



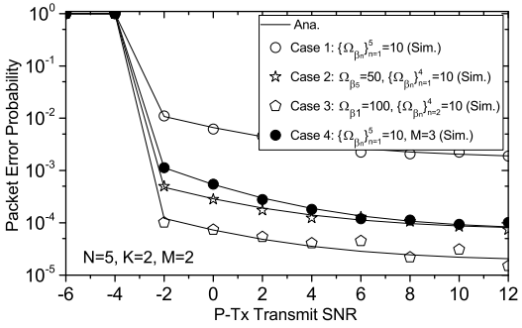

Hình 2.10: *Ảnh hưởng của độ lợi trung bình ($\Omega_{\beta_n}$) của P-Tx→EAV lên SNR của S-Tx.*



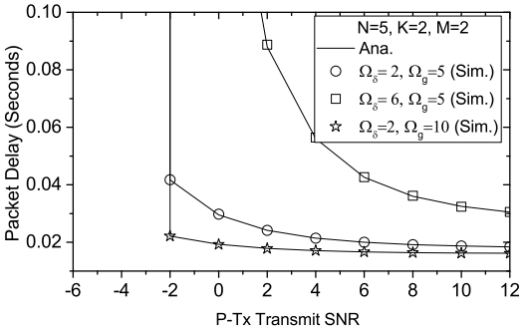

Hình 2.11: *SNR của S-Tx theo SNR của P-Tx với độ lợi trung bình khác nhau của S-Tx→EAV* ($\{\Omega_{\beta_n}\}_{n=1}^{5} = 10, 50, 80, 150$).




Hình 2.12: *SNR của S-Tx theo thời gian* $\tau$ *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 2.13: *Ảnh hưởng của các kênh can nhiễu P-Tx→EAV lên PEP.*




Hình 2.14: *Độ trễ của gói tin theo SNR của P-Tx.*

Chương 3

# Đánh giá hiệu năng bảo mật sử dụng kỹ thuật hợp tác chuyển tiếp trong mạng vô tuyến nhận thức

## 3.1 Mô hình #3.1:Hiệu năng bảo mật của mạng CCRN trong giới hạn dừng truyền thông và công suất phát mức đỉnh

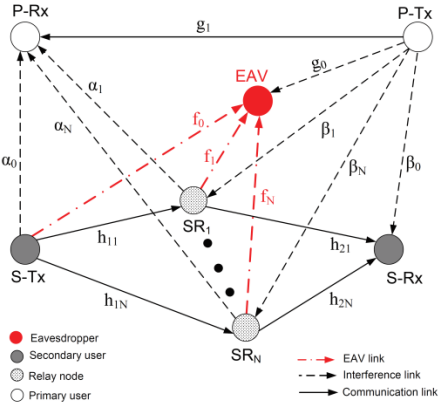
### 3.1.1 Mô hình của hệ thống

Xét một CCRN như hình 3.1. Độ lợi của S-Tx$\rightarrow SR_i$, $SR_i \rightarrow$ S-Rx, và P-Tx$\rightarrow$P-Rx được ký hiệu là $h_{1i}$, $h_{2i}$, $(i = 1, \ldots, N)$, và $g_1$. Độ lợi của S-Tx$\rightarrow$EAV, $SR_i \rightarrow$EAV, S-Tx$\rightarrow$P-Rx, $SR_i \rightarrow$P-Rx, P-Tx$\rightarrow SR_i$, P-Tx$\rightarrow$S-Rx, và P-Tx$\rightarrow$EAV được ký hiệu là $f_0$, $f_i$, $\alpha_0$, $\alpha_i$, $\beta_i$, $\beta_0$, và $g_0$, $i = 1, \ldots, N$, tương ứng. Độ lợi trung bình các kênh tương ứng là $\Omega_{\alpha_0}$, $\Omega_{\alpha}$, $\Omega_{\beta_0}$, $\Omega_{\beta}$, $\Omega_{h_1}$, $\Omega_{h_2}$, $\Omega_{f_0}$, $\Omega_{f}$, $\Omega_{g_0}$, và $\Omega_{g_1}$.

Trong pha đầu tiên, dung lượng của kênh S-Tx$\rightarrow SR_i$ như sau

$$C_{SR_i} = \frac{1}{2} B \log_2(1 + \gamma_{SR_i}) \tag{3.1}$$

trong đó $\gamma_{SR_i} = \frac{P_S h_{1i}}{P_P \beta_i + N_0}$ là SINR tại mỗi nút $SR_i$, với $P_P$, $P_S$ và $N_0$ lần lượt là công suất phát của PU, S-Tx và công suất nhiễu AWGN.




Hình 3.1: *Mô hình mạng CCRN với đa nút chuyển tiếp và một EAV*

Điều kiện truyền thông của hệ thống trong pha thứ nhất như sau:

$$\Pr\left\{C_P^{(S-Tx)} < R_p\right\} \leq \xi_p \tag{3.2}$$

$$P_S \leq P_{pk}^s \tag{3.3}$$

trong đó $C_P^{(S-Tx)} = B\log_2\left(1+\frac{P_P g_1}{P_S \alpha_0 + N_0}\right)$. Và dung lượng kênh của EAV được biểu diễn là

$$C_{SE} = \frac{1}{2}B\log_2\left(1+\gamma_{SE}\right) \tag{3.4}$$

trong đó $\gamma_{SE} = \frac{P_S f_0}{P_P g_0 + N_0} \approx \frac{P_S f_0}{P_P g_0}$ là SINR tại EAV.

Trong pha thứ hai, SINR tại S-Rx và EAV lần lượt là

$$\gamma_{RiD} = \frac{P_R h_{2i}}{P_P \beta_0 + N_0};\ \gamma_{RiE} = \frac{P_R f_i}{P_P g_0 + N_0} \approx \frac{P_R f_i}{P_P g_0} \tag{3.5}$$

trong đó $P_R$ là công suất phát của $SR_i$. Công suất phát của $SR_i$ phải đáp ứng điều kiện truyền thông như sau

$$\Pr\left\{C_P^{(SR_i)} < R_p\right\} \leq \xi_p \tag{3.6}$$

$$P_R \leq P_{pk}^r \tag{3.7}$$

trong đó $C_P^{(SR_i)} = B\log_2\left(1 + \frac{P_P g_1}{P_R \alpha_i + N_0}\right)$. Trong pha này, dung lượng kênh của EAV thu được là

$$C_{RiE} = \frac{1}{2} B \log_2 (1 + \gamma_{RiE}) \tag{3.8}$$

Dung lượng kênh từ nguồn đến đích của SU là

$$C_M = \max_{i=1,\ldots,N} \{\min \{C_{SR_i}, C_{RiD}\}\} \tag{3.9}$$

trong đó $C_{RiD} = \frac{1}{2} B \log_2(1 + \gamma_{RiD})$. và dung lượng kênh của EAV như sau

$$C_E = \max \left\{C_{SE}, C_{R_{i^*}E}\right\} \tag{3.10}$$

trong đó $i^*$ là chỉ số của nút chuyển tiếp được lựa chọn, nghĩa là,

$$i^* = \arg \max_{i=\{1,\ldots,N\}} \{\min \{C_{SR_i}, C_{RiD}\}\} \tag{3.11}$$

### 3.1.2 Độ đo đánh giá hiệu suất bảo mật của hệ thống

Dung lượng bảo mật của CCRN như sau

$$C_S = C_M - C_E \tag{3.12}$$

trong đó $C_M$ và $C_E$ được cho bởi công thức (3.9) và (3.10).

Xác suất dừng của dung lượng bảo mật kênh

$$\mathcal{O}_{sec} = \Pr \{C_S < R\} \tag{3.13}$$

Xác suất khác 0 của dung lượng bảo mật

$$\mathcal{O}_{nonZero} = \Pr \{C_S > 0\} \tag{3.14}$$

### 3.1.3 Phân tích hiệu suất hệ thống

#### 3.1.3.1 Chính sách phân bổ công suất truyền tin của SU

Công suất truyền tin của S-Tx và $SR$ được điều chỉnh theo công thức sau

$$P_S = \min\left\{P_{pk}^s, \frac{P_P\Omega_{g_1}}{\gamma_{th}^p\Omega_{\alpha_0}}\chi\right\};\ P_R = \min\left\{P_{pk}^r, \frac{P_P\Omega_{g_1}}{\gamma_{th}^p\Omega_{\alpha}}\chi\right\} \tag{3.15}$$

#### 3.1.3.2 Xác suất dừng bảo mật

Xác suất dừng bảo mật thu được như sau

$$\mathcal{O}_{sec} = I_1(n) + I_2(n) - I_3(n) \tag{3.16}$$

trong đó $I_1(n)$, $I_2(n)$, và $I_3(n)$ lần lượt là biểu thức như sau

$$I_1(n) = \sum_{n=0}^{N}\binom{N}{n}\frac{(-1)^n(\delta+1)}{A_2}\int_{\delta}^{\infty}\frac{\exp(-\frac{t}{D_1(n)})}{(B_1t+1)^n(t+C_1)^2(A_1(n)t+1)}dt \tag{3.17}$$

$$I_2(n) = \sum_{n=0}^{N}\binom{N}{n}\frac{(-1)^n(\delta+1)}{A_3}\int_{\delta}^{\infty}\frac{\exp(-\frac{t}{D_1(n)})}{(B_1t+1)^n(t+C_2)^2(A_1(n)t+1)}dt \tag{3.18}$$

$$I_3(n) = \sum_{n=0}^{N}\binom{N}{n}\frac{(-1)^n(\delta+1)}{A_2+A_3}\int_{\delta}^{\infty}\frac{\exp(-\frac{t}{D_1(n)})}{(B_1t+1)^n(t+C_3)^2(A_1(n)t+1)}dt \tag{3.19}$$

- Trường hợp 1: $n = 0$

$$I_1(0) = \frac{\delta+1}{A_2}\int_{\delta}^{\infty}\frac{dt}{(t+C_1)^2} = \frac{\delta+1}{A_2(\delta+C_1)} \tag{3.20}$$

$$I_2(0) = \frac{\delta+1}{A_3}\int_{\delta}^{\infty}\frac{dt}{(t+C_2)^2} = \frac{\delta+1}{A_3(\delta+C_2)} \tag{3.21}$$

$$I_3(0) = \frac{\delta+1}{A_2+A_3}\int_{\delta}^{\infty}\frac{dt}{(t+C_3)^2} = \frac{\delta+1}{(A_2+A_3)(\delta+C_3)} \tag{3.22}$$

- Trường hợp 2: $1 \leq n \leq N$. Để tính toán các tích phân bên trên, chúng ta hãy xem xét một bổ đề như sau:

  **Bổ đề 3.1.** *Giả sử $A$, $B$, $C$, $D$, và $\delta$ là các hằng số dương, chúng ta có*

$$\begin{aligned} K(A,B,C,D) &= \int_{\delta}^{\infty}\frac{\exp\left(-\frac{x}{D}\right)dx}{(Bx+1)^n(x+C)^2(Ax+1)} \\ &\approx K_{21}+K_{22}+K_{23}+K_{24} \end{aligned}$$

  *trong đó $K_{21}$, $K_{22}$, $K_{23}$, và $K_{24}$ lần lượt được biểu diễn như sau:*

$$K_{21} = \frac{\mathcal{B}\left[\frac{D_3}{D}, 1-n, n\right] - \pi\csc(\pi n)}{(D-D_1)(D-D_2)^2(D-D_3)^n}$$

$$K_{22} = \frac{\pi\csc(\pi n) - \mathcal{B}\left[\frac{D_3}{D_1}, 1-n, n\right]}{(D-D_1)(D-D_2)^2(D_1-D_3)^n}$$

$$K_{23} = \frac{n-1-n\,{}_2F_1\left(1,1;2-n;\frac{D_3}{D_2}\right)}{(n-1)D_2(D-D_2)(D_2-D_1)^2(D_2-D_3)D_3^{n-1}} - \frac{\pi n\csc(\pi n)}{(D-D_2)(D_2-D_1)^2(D_2-D_3)^{n+1}}$$

$$K_{24} = \frac{(2D_2-D-D_1)\left(\pi\csc(\pi n) - \mathcal{B}\left[\frac{D_3}{D}, 1-n, n\right]\right)}{(D-D_2)^2(D_2-D_1)^2(D_2-D_3)^n}$$

  *trong đó $D_1 = \frac{1+A\delta}{A}$, $D_2 = \delta + C$, và $D_3 = \frac{B\delta+1}{B}$. các hàm $\csc(x)$, $\mathcal{B}[\cdot,\cdot,\cdot]$, và ${}_2F_1(\cdot,\cdot;\cdot;\cdot)$ theo thứ tự là hàm lượng giác cosecant, hàm beta khuyết, và hàm siêu bội.*

*Chứng minh.* Chứng minh được trình bày trong phần phụ lục. □

Sử dụng kết quả của bổ đề 3.1, một biểu thức xấp xỉ cho $\mathcal{O}_{sec}$ của SU thu được như sau

$$\mathcal{O}_{sec} \approx I_0 + I_1(n) + I_2(n) - I_3(n) \tag{3.23}$$

trong đó

$$\begin{aligned}
I_0 &= I_1(0) + I_2(0) - I_3(0) \\
I_1(n) &= \sum_{n=1}^{N} \binom{N}{n} \frac{(-1)^n(\delta+1)K(A_1(n), B_1, C_1, D_1(n))}{A_2} \\
I_2(n) &= \sum_{n=1}^{N} \binom{N}{n} \frac{(-1)^n(\delta+1)K(A_1(n), B_1, C_2, D_1(n))}{A_3} \\
I_3(n) &= \sum_{n=1}^{N} \binom{N}{n} \frac{(-1)^n(\delta+1)K(A_1(n), B_1, C_3, D_1(n))}{A_2 + A_3}
\end{aligned}$$

trong đó $A_1(n)$, $B_1$, $D_1(n)$, $A_2(v)A_3$ lần lượt được định nghĩa là

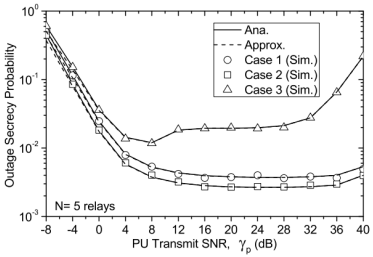
$$A_1(n) = \frac{nP_P\Omega_{\beta_0}}{P_R\Omega_{h_2}};\ B_1 = \frac{P_P\Omega_{\beta}}{P_S\Omega_{\beta_{h_1}}};\ \frac{1}{D_1(n)} = \left(\frac{1}{P_S\Omega_{h_1}} + \frac{1}{P_R\Omega_{h_2}}\right) nN_0$$

$$A_2 = \frac{P_P\Omega_{g_0}}{P_R\Omega_f};\ A_3 = \frac{P_P\Omega_{g_0}}{P_S\Omega_{f_0}}$$

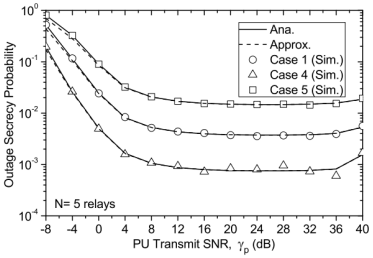
#### 3.1.3.3 Xác suất khác 0 của dung lượng bảo mật kênh

Xác suất khác 0 của dung lượng bảo mật được phân tích như sau

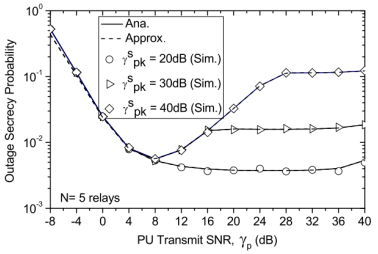
$$\mathcal{O}_{nonZero} = \Pr\{C_{sec} > 0\} \approx 1 - \mathcal{O}_{sec}\ ;\ \text{với}\ \delta = 0 \tag{3.24}$$



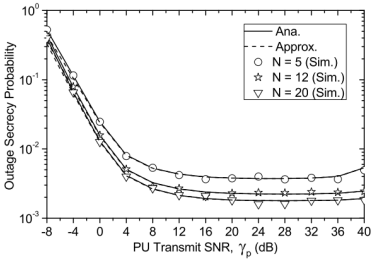

Hình 3.2: *$\mathcal{O}_{sec}$ của hệ thống với ba trường hợp độ lợi kênh trung bình khác nhau*



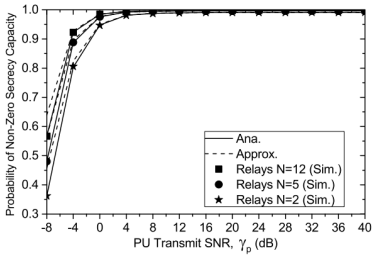

Hình 3.3: *$\mathcal{O}_{sec}$ của hệ thống với các trường hợp độ lợi trung bình khác nhau của các kênh wiretap.*




Hình 3.4: *$\mathcal{O}_{sec}$ của hệ thống với các SNR khác nhau của S-Tx*




Hình 3.5: $\mathcal{O}_{sec}$ *của hệ thống với số lượng nút SR khác nhau*




Hình 3.6: $P^{sec}_{non-zero}$ *với số lượng nút SR khác nhau*

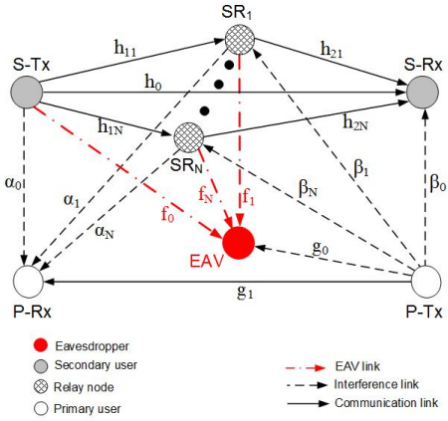
### 3.1.4 Mô phỏng và đánh giá kết quả

## 3.2 Mô hình #3.2:Hiệu năng bảo mật của mạng CCRN dưới dưới điều kiện dừng bảo mật và giới hạn can nhiễu

### 3.2.1 Mô hình hệ thống

Cho mô hình hệ thống như trong Hình 3.7.

Độ lợi của P-Tx→P-Rx, S-Tx→$SR_i$, $SR_i$→S-Rx, S-Tx→S-Rx, S-Tx→P-Rx, $SR_i$→P-Rx, P-Tx→$SR_i$, P-Tx→S-Rx, P-Tx→EAV, S-Tx→EAV




Hình 3.7: *Mô hình CCRN trong đó tồn tại kênh trực tiếp và EAV.*

và SR$_i$→EAV được kí hiệu bởi $g_1, h_{1i}, h_{2i}$, $h_0$, $\alpha_0, \alpha_i, \beta_i, \beta_0$, $g_0$, $f_0$ và $f_i$, $i \in \{1, \ldots, N\}$. Độ lợi trung bình của các kênh được kí hiệu là $\Omega_{g_1}, \Omega_{h_1}, \Omega_{h_2}, \Omega_{h_0}, \Omega_{\alpha_0}, \Omega_{\alpha_i}, \Omega_{\beta_0}, \Omega_{\beta_i}, \Omega_{g_0}, \Omega_{f_0}$, and $\Omega_f$.

Trong pha thứ nhất, dung lượng của S-Tx→SR$_i$ là

$$C_{SR_i} = \frac{1}{2} B \log_2(1 + \gamma_{SR_i}) \tag{3.25}$$

trong đó $\gamma_{SR_i} = \frac{P_S h_{1i}}{P_P \beta_i + N_0}$ là SINR tại SR$_i$, và $P_P$, $P_S$ là công suất phát của PU và SU, $N_0$ là công suất nhiễu AWGN. Và dung lượng kênh của kênh S-Tx→S-Rx được cho là

$$C_{SD} = B \log_2(1 + \gamma_{SD}) \tag{3.26}$$

trong đó $\gamma_{SD} = \frac{P_S h_0}{P_P \beta_0 + N_0}$ là SINR của kênh S-Tx→S-Rx. Dung lượng kênh tại EAV khi S-Tx truyền tin được mô tả là

$$C_{SE} = \frac{1}{2} B \log_2(1 + \gamma_{SE}) \tag{3.27}$$

trong đó $\gamma_{SE} = \frac{P_S f_0}{P_P g_0 + N_0} \approx \frac{P_S f_0}{P_P g_0}$ là SINR của kênh S-Tx→EAV.

Trong pha thứ hai, dung lượng của $SR_i$→S-Rx như sau

$$C_{R_iD} = \frac{1}{2} B \log_2(1 + \gamma_{R_iD}) \tag{3.28}$$

trong đó $\gamma_{R_iD} = \frac{P_R h_{2i}}{P_P \beta_0 + N_0}$ là SINR của kênh $SR_i$→S-Rx, và $P_R$ là công suất phát của SR. Dung lượng kênh của EAV là

$$C_{R_iE} = \frac{1}{2} B \log_2(1 + \gamma_{R_iE}) \tag{3.29}$$

trong đó $\gamma_{R_iE} = \frac{P_R f_i}{P_P g_0 + N_0} \approx \frac{P_R f_i}{P_P g_0}$ là SINR của kênh $SR_i$→EAV.

Cuối cùng, dung lượng kênh của mạng SU được biểu diễn là

$$C_{E2E} = \max_{i \in \{1,2,\ldots,N\}} \{C_{SD}, \min\{C_{SR_i}, C_{R_iD}\}\} \tag{3.30}$$

Mặt khác, dung lượng kênh thực tế thu được tại EAV sẽ là

$$C_E = \max\left\{C_{SE}, C_{R_{i^*}E}\right\} \tag{3.31}$$

trong đó $i^*$ là chỉ số của nút SR được lựa chọn, có nghĩa là

$$i^* = \arg \max_{i \in \{1,\ldots,N\}} \{\min\{C_{SR_i}, C_{RiD}\}\} \tag{3.32}$$

#### 3.2.1.1 Độ đo đánh giá hiệu suất bảo mật cho truyền thông của SU

Dung lượng bảo mật kênh của mạng SU được mô tả như sau

$$C_S = [C_{E2E} - C_E]^+ \tag{3.33}$$

Hiệu suất bảo mật của hệ thống được đánh giá thông qua các xác suất dừng bảo mật và xác suất khác 0 của dung lượng bảo mật sau:

$$\mathcal{O}_{SEC} = \Pr\{C_S < R\} \tag{3.34}$$

$$\mathcal{O}_{nonZero} = \Pr\{C_S > 0\} \tag{3.35}$$

#### 3.2.1.2 Điều kiện công suất cho SU và SR

- Điều kiện công suất của P-Tx→P-Rx khi S-Tx truyền tin

$$\mathcal{O}_{I_1} = \Pr\left\{\frac{P_S \alpha_0}{N_0} \geq I_{th}\right\} \leq \xi_P \tag{3.36}$$

$$0 \leq P_S \leq P_{pk}^S \tag{3.37}$$

- Điều kiện công suất của P-Tx→P-Rx khi $\text{SR}_{i^*}$ truyền tin

$$\mathcal{O}_{I_2} = \Pr\left\{\frac{P_R \alpha_{i^*}}{N_0} \geq I_{th}\right\} \leq \xi_P \tag{3.38}$$

$$0 \leq P_R \leq P_{pk}^R \tag{3.39}$$

trong đó $I_{th}$ là ngưỡng công suất can nhiễu của PU. $P_{pk}^S$ và $P_{pk}^R$ là công suất phát tối đa của S-Tx và $SR$. Mặt khác, dựa trên thông tin có được về CSI của EAV, công suất phát của S-Tx và $\text{SR}_i$ phải đáp ứng thêm hai điều kiện khác sau

$$\mathcal{O}_{SE} = \Pr\left\{C_{SE} > R\right\} \leq \epsilon \tag{3.40}$$

$$\mathcal{O}_{R_{i^*}E} = \Pr\left\{C_{R_{i^*}E} > R\right\} \leq \epsilon \tag{3.41}$$

trong đó $\epsilon$ là giới hạn dừng bảo mật được đưa ra bởi mạng SU.

### 3.2.2 Phân tích hiệu suất hệ thống

#### 3.2.2.1 Các chính sách phân bổ công suất

Chúng ta thu được chính sách công suất cho S-Tx như sau

$$P_S = \min\left\{P_{pk}^S, \frac{I_{th} N_0}{\Omega_{\alpha_0} \ln(\frac{1}{\xi_P})}, \frac{P_P \gamma_{th}^e \Omega_{g_0}}{\Omega_{f_0}\left(\frac{1}{\epsilon} - 1\right)}\right\} \tag{3.42}$$

và chính sách phân bổ công suất cho $SR_i$ là

$$P_R = \min\left\{P_{pk}^R, \frac{I_{th}N_0}{\Omega_{\alpha_{i^*}}\ln(\frac{1}{\xi_P})}, \frac{P_P\gamma_{th}^e\Omega_{g_0}}{\Omega_{f_{i^*}}\left(\frac{1}{\epsilon}-1\right)}\right\} \tag{3.43}$$

Giá trị tối ưu của $\epsilon$ có thể được tính toán bởi các thông số CSI thu được như sau

$$\epsilon_{\max} = \min\left\{\frac{\Omega_{f_0}P_I^S}{P_P\gamma_{th}^e\Omega_{g_0}+\Omega_{f_0}P_I^S}, \frac{\Omega_{f_{i^*}}P_I^R}{P_P\gamma_{th}^e\Omega_{g_0}+\Omega_{f_{i^*}}P_I^R}\right\} \tag{3.44}$$

#### 3.2.2.2 Xác suất truyền thông bảo mật của mạng CCRN

Để đánh giá hiệu năng bảo mật của hệ thống, chúng ta cần phân tích hai chỉ số đánh giá hiệu suất trong (3.34) và (**??**) dựa trên các chính sách phân bổ công suất của S-Tx và SR.

*a) Xác suất dừng bảo mật:*

$$\mathcal{O}_{SEC} \approx [I_1(n) + I_2(n) - I_3(n)] - [J_1(n) + J_2(n) - J_3(n)] \tag{3.45}$$

trong đó

$$I_1(n) = \sum_{n=0}^{N}\binom{N}{n}\frac{(-1)^n(\delta+1)K(B_n, B_0, C_1, C_n)}{A_2}$$
$$I_2(n) = \sum_{n=0}^{N}\binom{N}{n}\frac{(-1)^n(\delta+1)K(B_n, B_0, C_2, C_n)}{A_3}$$
$$I_3(n) = \sum_{n=0}^{N}\binom{N}{n}\frac{(-1)^n(\delta+1)K(B_n, B_0, C_3, C_n)}{A_2+A_3}$$
$$J_1(n) = \sum_{n=0}^{N}\binom{N}{n}\frac{(-1)^n(\delta+1)K(E_n, B_0, C_1, D_n)}{A_2}$$

$$J_2(n) = \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta+1) K(E_n, B_0, C_2, D_n)}{A_3}$$

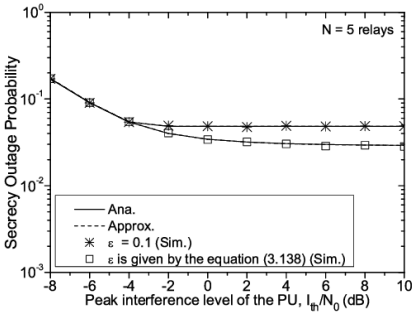
$$J_3(n) = \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta+1) K(E_n, B_0, C_3, D_n)}{A_2 + A_3}$$

với $B_0 = \frac{P_P \Omega_\beta}{P_S \Omega_{h_1}}$, $B_n = \frac{P_P \Omega_{\beta_0} n}{P_R \Omega_{h_2}}$, $A_2 = \frac{P_P \Omega_{g_0}}{P_R \Omega_f}$, $A_3 = \frac{P_P \Omega_{g_0}}{P_S \Omega_{f_0}}$,
và $E_n = \left(\frac{1}{P_S \Omega_{h_0}} + \frac{n}{P_R \Omega_{h_2}}\right) P_P \Omega_{\beta_0}$, $\frac{1}{C_n} = \left(\frac{1}{P_P \Omega_{h_1}} + \frac{1}{P_R \Omega_{h_2}}\right) N_0 n$,
$\frac{1}{D_n} = \left(\frac{1}{P_S \Omega_{h_0}} + \frac{n}{P_S \Omega_{h_1}} + \frac{n}{P_R \Omega_{h_2}}\right) N_0$, $E_n = \left(\frac{1}{P_S \Omega_{h_0}} + \frac{n}{P_R \Omega_{h_2}}\right) P_P \Omega_{\beta_0}$, và
$C_1 = \frac{1+\delta-A_2\delta}{A_2}$, $C_2 = \frac{1+\delta-A_3\delta}{A_3}$, $C_3 = \frac{1+\delta-(A_2+A_3)\delta}{A_2+A_3}$.

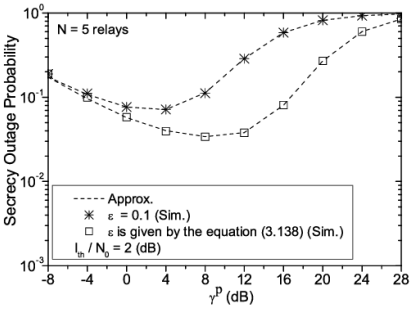
*b) Xác suất khác 0 của dung lượng bảo mật*

$$\mathcal{O}_{nonZero} = \Pr\{C_S > 0\} = \approx 1 - \mathcal{O}_{SEC}\ ;\ \text{với } \delta = 0 \tag{3.46}$$

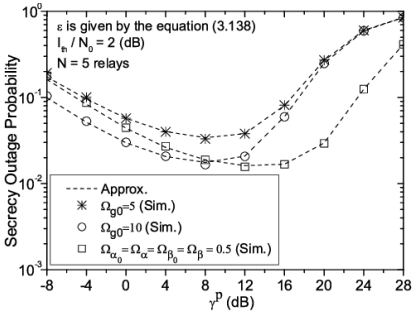
### 3.2.3 Mô phỏng và đánh giá kết quả



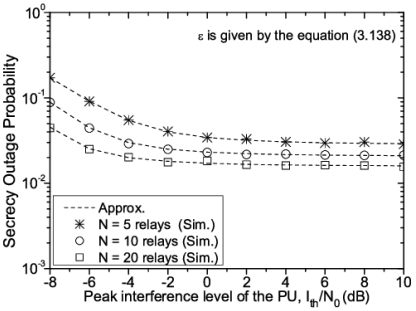

Hình 3.8: *Tác động của $\epsilon$ lên $\mathcal{O}_{SEC}$ của hệ thống theo tập giá trị $\frac{I_{th}}{N_0}$.*



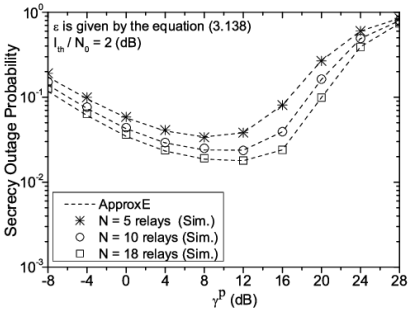

Hình 3.9: *Tác động của $\epsilon$ lên $\mathcal{O}_{SEC}$ của hệ thống theo tập giá trị $\gamma^p$.*



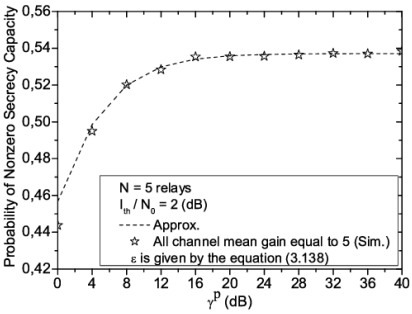

Hình 3.10: *Ảnh hưởng của các kênh can nhiễu lên $\mathcal{O}_{SEC}$ của hệ thống.*




Hình 3.11: *Tác động của số lượng nút SR đối với $\mathcal{O}_{SEC}$ theo tập giá trị của $I_{th}$.*




Hình 3.12: *Tác động của số lượng nút SR đối với $\mathcal{O}_{SEC}$ theo tập giá trị của $\gamma_p$.*




Hình 3.13: *$\mathcal{O}_{nonZero}$ với độ lợi trung bình của các kênh đồng nhất bằng* 5.

# KẾT LUẬN

Các kết quả chính của luận án bao gồm:

1. Nghiên cứu truyền thông tin cậy và bảo mật thông tin cho mô hình mạng CRN. Từ đó, xây dựng các chính sách phân bổ công suất với bốn kịch bản khác nhau. Đề xuất một độ đo hiệu suất mới (SRCP) và sử dụng để phân tích hiệu năng bảo mật hệ thống tương ứng với bốn kịch bản.

2. Nghiên cứu, xây dựng cơ chế truyền thông và thu hoạch năng lượng cùng với chính sách công suất và chiến lược chọn kênh cho mô hình mạng CRN dưới các điều kiện bảo mật thông tin chống lại tấn công nghe trộm thông tin. Ngoài ra, Luận án đánh giá hiệu suất hệ thống dựa trên các độ đo PEP và APD để đánh giá hiệu suất của hệ thống theo các chiến lược được áp dụng.

3. Nghiên cứu áp dụng kỹ thuật hợp tác chuyển tiếp để cải thiện hiệu suất bảo mật cho mạng CCRN. Khảo sát đánh giá hiệu năng bảo mật hệ thống dựa trên các biểu thức xấp xỉ của các độ đo với cách tiếp cận nhóm các điều kiện ràng buộc khác nhau. Đặc biệt, luận án nghiên cứu đưa ra biểu thức tính toán giá trị tối ưu cho ngưỡng giới hạn bảo mật theo trạng thái kênh truyền. Điều này giúp hệ thống điều chỉnh chính sách công suất, chiến lược truyền thông để cải thiện hiệu năng bảo mật.

# DANH MỤC CÔNG TRÌNH KHOA HỌC CỦA TÁC GIẢ LIÊN QUAN ĐẾN LUẬN ÁN


1. **Truong Xuan Quach**, Hung Tran, Elisabeth Uhlemann, G.Kaddoum, and T.Q. Anh (2017), "Power allocation policy and performance analysis of secure and reliable communication in cognitive radio networks", *Wireless Networks*, 25(4), pp. 1477-1489.

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

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

4. **Truong Xuan Quach**, Hung Tran, Elisabeth Uleman, Mai Tran Truc (2020), "Secrecy performance of cooperative cognitive radio networks under joint secrecy outage and primary user interference constraint", *IEEE Access*, 8, pp. 18442-18455.

# Tài liệu tham khảo


[1] 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.

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

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

[4] Gradshteyn I.S. and Ryzhik I.M. (2007), *Table of Integrals, Series, and Products* , Elsevier.

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

[6] 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.

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