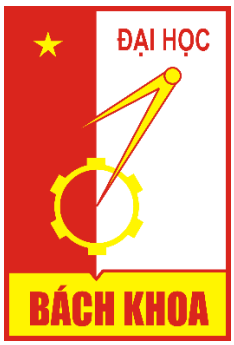
ĐẠI HỌC BÁCH KHOA HÀ NỘI

TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

----- ☙ 🕮 ❧ -----



BÀI TẬP LỚN

MÔN: PROJECT II

(Mã học phần: IT3931)

Đề tài:

SO SÁNH CONVERT COMMUNICATION VÀ PHYSICAL LAYER SECURITY

Giảng viên hướng dẫn: **TS. Trịnh Văn Chiến**

Sinh viên thực hiện: **Đào Văn Nguyên Huy**

Mã số sinh viên: **20215589**

Lớp: **IT2 - 03**

Hà Nội, năm 2024

MỤC LỤC

MỞ ĐẦU

Trong kỷ nguyên số hóa hiện nay, bảo mật thông tin là một yếu tố thiết yếu cho sự phát triển của các hệ thống mạng. Trong truyền thông, tại tầng vật lý có 2 phương pháp chủ yếu để bảo mật thông tin bao gồm: Physical Layer Security và Convert Communication. Mỗi phương pháp đều có ưu và nhược điểm riêng khi áp dụng trong các môi trường truyền khác nhau. Trong bài tập lớn này, em sẽ so sánh Physical Layer Security (PLS) với Convert Communication dựa trên các điều kiện khác nhau liên quan đến khoảng cách đến trạm thu bất hợp pháp, độ lớn của nhiễu. Qua đó, em hy vọng sẽ cung cấp một cái nhìn toàn diện về hiệu quả của từng phương pháp trong việc bảo mật thông tin.

I. MÔ HÌNH HỆ THỐNG

Hệ thống bao gồm 1 trạm truyền (Alice), 1 trạm nhận hợp pháp (Bob), và 1 trạm nghe lén (Eve). Alice muốn truyền tin mật đến Bob bằng cách truyền tín hiệu Jam để che dấu tín hiệu đến Bob. Ta xem xét 2 cách tiếp cận bao gồm Physical Layer Security và Convert Communication. Khoảng cách từ Alice đến Bob và từ Alice đến Eve lần lượt là d_{ab} và d_{ae}. Hệ số kênh truyền giữa Alice và Bob và giữa Alice và Eve lần lượt là h_{ab}, h_{ae}. Hệ số kênh tuân theo phân phối Gauss phức với giá trị trung bình bằng 0 và phương sai bằng 1.

II. PHYSICAL LAYER SECURITY

Trong [1], Wyner đã chứng minh nếu kênh nghe lén kém hơn kênh hợp pháp (tức là tỷ số tín hiệu trên nhiễu của kênh hợp pháp lớn hơn của kênh nghe lén) thì trạm truyền có thể truyền 1 lượng dữ liệu mật lớn hơn 0 trên kênh truyền đến trạm thu.

Tín hiệu nhận được tại trạm thu m (Bob hoặc Eve) là $y_m = \frac{\sqrt{P_j}h_{am}x_j}{d_{am}^{a/2}} + \frac{\sqrt{p_{ab}}h_{am}x_b}{d_{am}^{a/2}} + \eta_m$, với p_j và p_{ab} là năng lượng của tín hiệu Jam và năng lượng Alice truyền đến Bob, α là số mũ suy hao đường truyền, $\eta_m \sim \mathcal{CN}(0, \sigma_m^2 I_n)$ là nhiễu tại trạm thu m (Bob hoặc Eve). Tỷ số tín hiệu trên nhiệu tại Bob và Eve lần lượt là $SINR_b = \frac{p_{ab}|h_{ab}|^2}{d_{ab}^a \sigma_b^2 + p_j|h_{ab}|^2}$, $SINR_e = \frac{p_{ab}|h_{ae}|^2}{d_{ae}^a \sigma_e^2 + p_j|h_{ae}|^2}$

Do vậy nếu $\text{SINR}_b > \text{SINR}_e$ thì tốc độ truyền tin mật

$$R_{\text{sec}} = \log(1 + \text{SINR}_b) - \log(1 + \text{SINR}_e)$$

III. CONVERT COMMUNICATION

Khác với PLS, với cách tiếp cận sử dụng Convert Communication, Alice sẽ truyền theo từng khung thời gian. Alice và Bob trao đổi trước khung thời gian truyền, khung thời gian này không được tiết lộ với Eve. Eve phải xác định xem Alice có truyền trong khung thời gian đó không dựa vào 1 giá trị ngưỡng công suất. Xác suất để Eve quyết định sai phụ thuộc vào công suất của tín hiệu truyền và tín hiệu Jam được truyền từ Alice đến Bob, do đó ta có thể điều chỉnh công suất tín hiệu này để xác suất Eve quyết định sai lớn từ đó Alice có thể truyền 1 cách bí mật đến Bob.

Tín hiệu nhận được tại trạm thu m (Bob hoặc Eve) được tính theo công thức :

$$y_m = \begin{cases} \frac{\sqrt{P_j}h_{am}x_j}{d_d^{a/2}} + \eta_m, & \text{với trường hợp } \Psi_0 \\ \frac{\sqrt{P_j}h_{am}x_j}{d_{am}^{a/2}} + \frac{\sqrt{p_{ab}}h_{am}x_b}{d_{am}^{a/2}} + \eta_m, & \text{với trường hợp } \Psi_1 \end{cases}$$

Trong đó ψ_0 là trường hợp Alice không truyền tín hiệu đến Bob, ψ_1 là trường hợp Alice có truyền tín hiệu đến Bob.

Eve quyết định sai trong 2 trường hợp. Trường hợp 1, Alice truyền nhưng Eve quyết định là không truyền, gọi là bỏ qua phát hiện và xác suất tương ứng là P_{MD}. Trường hợp 2, Alice không truyền nhưng Eve quyết định là truyền, gọi là cảnh báo sai và xác suất tương ứng là P_{FA}.

Để xác định Alice có truyền tin đến Bob trong 1 khung thời gian không, Eve tính năng lượng trung bình trong khung thời gian đó và so sánh với giá trị ngưỡng ϑ. Nếu năng lượng trung bình lớn hơn ϑ, Eve cho rằng Alice có truyền tin trong khung thời gian và ngược lại.

Với $\varphi_0 = \frac{p_j}{d_{ae}^{\alpha}}$ và $\varphi_1 = \frac{p_j + p_{ab}}{d_{ae}^{\alpha}}$, theo [2] :

$$P_{FA} = \begin{cases} e^{-\frac{(\vartheta - {\sigma_e}^2)}{\varphi_0}} & với\ \vartheta - \sigma_e^2 \geq 0 \\ 1 & với\ \vartheta - \sigma_e^2 < 0 \end{cases}$$

$$P_{MD} = \begin{cases} 1 - e^{-\frac{(\vartheta - {\sigma_e}^2)}{\varphi_1}} & với\ \vartheta - \sigma_e^2 \geq 0 \\ 0 & với\ \vartheta - \sigma_e^2 < 0 \end{cases}$$

Trong góc nhìn của Eve, Eve cần xác định giá trị ngưỡng ϑ để xác suất lỗi là nhỏ nhất.

Theo [2], giá trị ngưỡng ϑ đó là $\vartheta^* = \left(\ln\left(\frac{\varphi_0}{\varphi_1}\right) + \sigma_e^2\left(\frac{\varphi_0 - \varphi_1}{\varphi_0 \varphi_1}\right)\right)\left(\frac{\varphi_0 \varphi_1}{\varphi_0 - \varphi_1}\right)$

Từ đó ta tính được $P_{FA} + P_{MD} = 1 - e^{-\frac{(\vartheta^* - \sigma_e^2)}{\varphi_1}} + e^{-\frac{(\vartheta^* - \sigma_e^2)}{\varphi_0}}$

Do đó, tốc độ truyền tin mật $R_{sec} = P_{\varphi_1} \log\left(1 + \frac{p_{ab}|h_{ab}|^2}{d_{ab}^{\alpha}\sigma_b^2 + p_j|h_{ab}|^2}\right)$ với P_{φ_1} là xác suất mà Alice truyền tin cho Bob trong 1 khung thời gian

IV. MÔ TẢ BÀI TOÁN TỐI ƯU

IV.1. Physical Layer Security

Dựa vào phần II, tốc độ truyền tin mật tối đa: $Max(R_{\text{sec}}) = Max(\log(1 + \text{SINR}_b) - \log(1 + \text{SINR}_e))$ với $P_{ab} + P_j \leq P_{max}$.

IV.2. Convert Communication

Dựa vào phần III, tốc độ truyền tin mật tối đa: $Max(R_{sec}) = Max(P_{\varphi_1} \log\left(1 + \frac{p_{ab}|h_{ab}|^2}{d_{ab}^{\alpha}\sigma_b^2 + p_j|h_{ab}|^2}\right))$ với $P_{ab} + P_j \leq P_{max}$ và $P_{FA} + P_{MD} = 1 - e^{-\frac{(\vartheta^* - \sigma_e^2)}{\varphi_1}} + e^{-\frac{(\vartheta^* - \sigma_e^2)}{\varphi_0}} \geq 1 - \varepsilon$ trong đó ε là 1 số rất nhỏ.

V. GIẢI BÀI TOÁN TỐI ƯU

V.1. Physical Layer Security

Để giải bài toán trong phần IV.1, em đã thực hiện 2 phương pháp. Phương pháp thứ 1, em duyệt các giá trị có thể có của P_{ab} và P_j thỏa mãn điều kiện, các giá trị cách nhau 0.01 sau đó lấy giá trị lớn nhất. Từ kết quả của phần 1, nhận thấy R_{sec} lớn nhất khi $P_{ab}+P_j = P_{max}$. Do đó ở phương pháp thứ 2, em tìm Max(R_{sec}) với $P_{ab} + P_j = P_{max}$.

Để giải bài toán này, em đặt $\gamma_b = \frac{p_{\max}|h_{ab}|^2}{d_{ab}^{\alpha}\sigma_b^2}$, $\gamma_e = \frac{p_{max}|h_{ae}|^2}{d_{ae}^{\alpha}\sigma_e^2}$,

$p_j = (1-\lambda)p_{max}$ từ đó ta tính được $R_{\text{sec}}(\lambda) = \log\left(\frac{1+\gamma_b}{1+(1-\lambda)\gamma_b}\right) - \log\left(\frac{1+\gamma_e}{1+(1-\lambda)\gamma_e}\right)$

Với $\lambda \in (0,1)$.

Bài toán trở thành: $\max_{\lambda} \frac{(1+\gamma_b)(1+(1-\lambda)\gamma_e)}{(1+\gamma_e)(1+(1-\lambda)\gamma_b)}$ với $\lambda \in (0,1)$. Do hàm tối ưu là một hàm lồi nên có thể giải sử dụng công cụ CVX [3].

V.2. Convert Communication

Tương tự như PLS, em cũng áp dụng 2 phương pháp. Phương pháp thứ nhất vẫn là duyệt các giá trị có thể có của P_{ab}, P_j thỏa mãn các điều kiện của hàm tối ưu và lấy giá trị lớn nhất. Phương pháp thứ 2 em cũng lấy $P_{ab} + P_j = P_{max}$ từ đó chuyển bài toán thành: $\max_{\lambda} \log\left(1 + \frac{\lambda\gamma_b}{1+(1-\lambda)\gamma_b}\right)$ với $\lambda p_{max} \ln(\lambda p_{\max}) + (1-\lambda)p_{max} \ln\big((1-\lambda)p_{\max}\big) - p_{\max} \ln p_{\max} - \lambda p_{\max} \ln \varepsilon \leq 0$ (1) . Ta thấy $\max_{\lambda} \log\left(1 + \frac{\lambda\gamma_b}{1+(1-\lambda)\gamma_b}\right)$ đạt giá trị lớn nhất khi λ lớn nhất. Vậy bài toán trở thành tìm max λ với $\lambda \in (0,1)$ và (1). Do hàm tối ưu là hàm lồi nên có thể sử dụng công cụ CVX [3] để giải quyết.

VI. THỬ NGHIỆM VÀ ĐÁNH GIÁ.

VI.1. Môi trường thử nghiệm

Trong báo cáo này, em sẽ tìm và so sánh tốc độ truyền tin mật theo cách tiếp cận PLS với Convert Communication bằng Matlab và công cụ CVX với các tham số:

$p_{max} = 5Watts, d_{ab} = 5\text{m}, \sigma_b^2 = -10\text{dB}, \alpha = 4, \varepsilon = 0.1,\ P_{\varphi_1} = 0.7$

VI.2. Tốc độ truyền bí mật (Secrecy rate) theo khoảng cách d_{ae} theo cách tiếp cận PLS

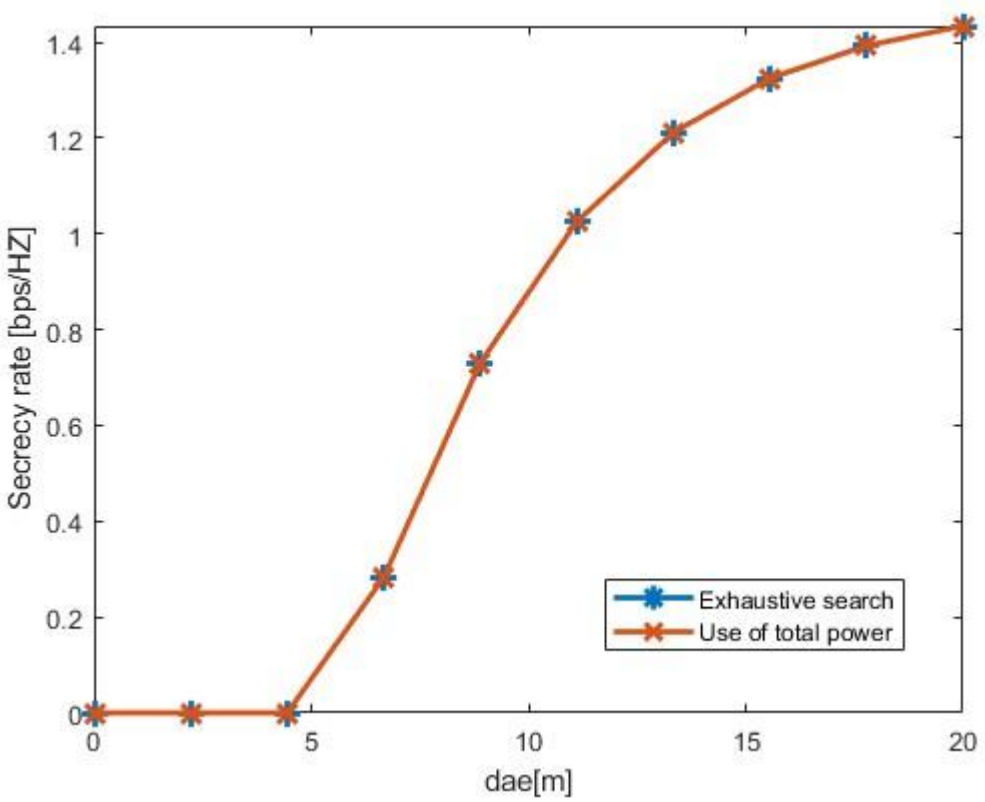


Figure 1: Physical Layer Security

Nhìn vào đồ thị có thể thấy 2 phương pháp (duyệt toàn bộ giá trị và sử dụng $P_{ab} + P_j = P_{max}$) cho kết quả tương đồng nhau.

VI.3. Tốc độ truyền bí mật (Convert rate) theo khoảng cách d_{ae} theo cách tiếp cận Convert Communication

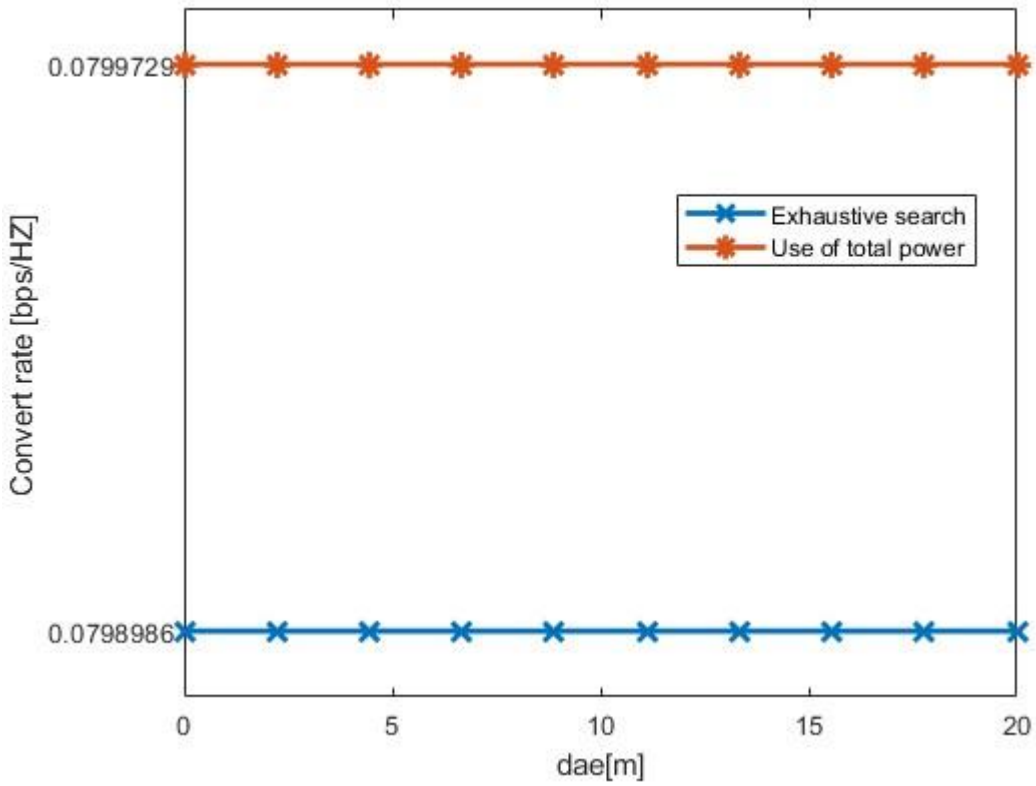


Figure 2: Convert Communication

Nhìn vào đồ thị có thể thấy 2 phương pháp (duyệt toàn bộ giá trị và sử dụng $P_{ab} + P_j = P_{max}$) cho kết quả tương đồng nhau.

VI.4. So sánh PLS với Convert Communication khi thay đổi giá trị nhiễu

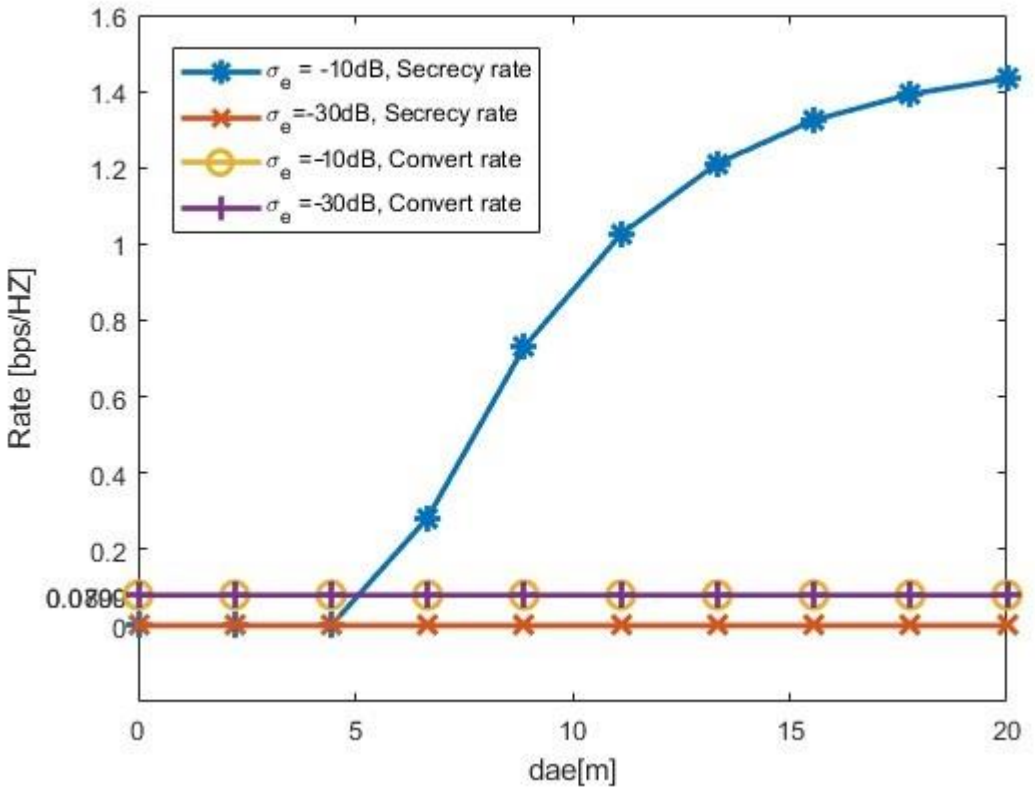


Figure 3: So sánh Convert Communication và PLS

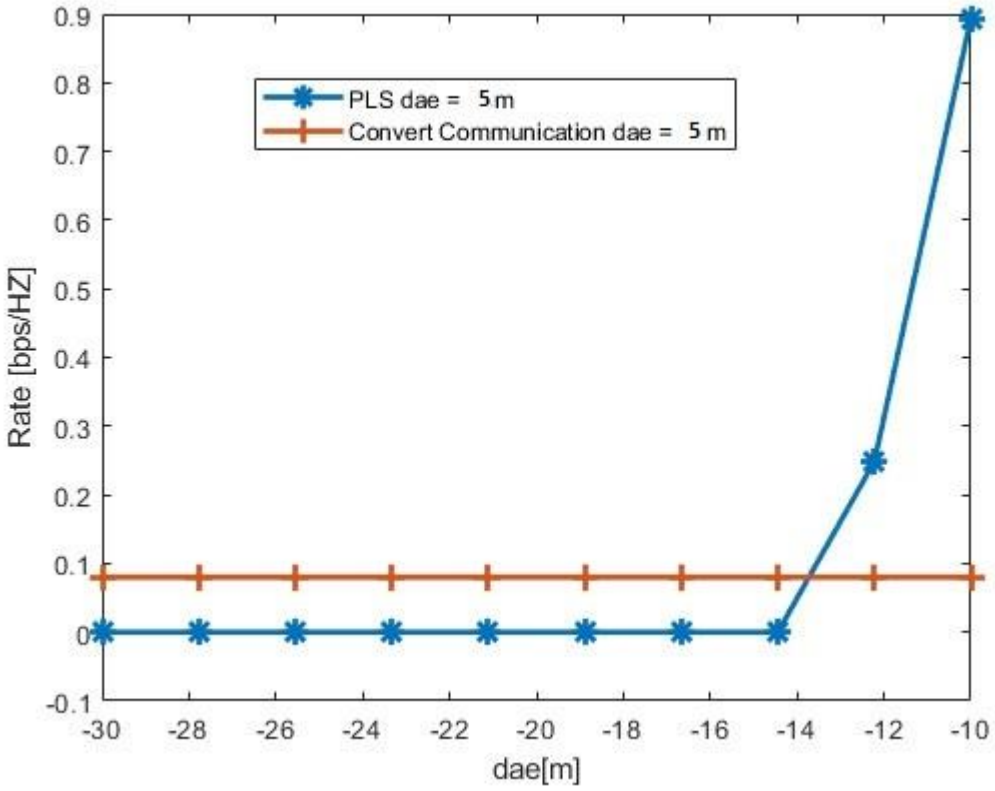


Figure 4: So sánh Convert Comunication và PLS phụ thuộc vào nhiễu thay đổi

Nhìn vào hình 3 ta thấy với trường hợp nhiễu tại Eve nhỏ, Tốc độ truyền tin mật theo cách tiếp cận PLS bằng 0 trong khi đối với cách tiếp cận Convert Communication bằng 0.08. Trong trường hợp nhiễu tại Eve lớn, khi khoảng cách d_{ae} nhỏ, tương tự như trường hợp nhiễu tại Eve nhỏ, tốc độ truyền tin mật theo cách tiếp cận PLS bằng 0, trong khi đối với cách tiếp cận Convert Communication bằng 0.08. Nhưng khi nhiễu tại Eve lớn và khoảng cách d_{ae} lớn, tốc độ truyền tin mật với cách tiếp cận PLS vượt trội hơn so với Convert Communication.

Theo hình 4 ta thấy khi nhiễu tăng thì tốc độ truyền tin mật theo PLS tăng, còn theo cách tiếp cận Convert Communication không đổi.

VII. KẾT LUẬN

Dựa vào phần thực nghiệm (VI) có thể thấy các ưu và nhược điểm khi áp dụng các cách tiếp cận PLS và Convert Communication:

	PLS	Convert Communication
Ưu điểm	Khi khoảng cách giữa trạm phát và trạm nghe lén xa nhau hoặc nhiễu tại trạm nghe lén lớn thì tốc độ truyền tin mật lớn	Không cần thông tin kênh truyền, tốc độ truyền tin mật ổn định không phụ thuộc vào vị trí của trạm nghe lén hay nhiễu tại trạm nghe lén
Nhược điểm	Cần thông tin kênh truyền, khi vị trí của trạm nghe lén ở gần trạm phát thì tốc độ truyền tin mật bằng 0	Tốc độ truyền tin mật nhỏ

VIII. ĐÓNG GÓP CỦA BẢN THÂN

Trong bài tập lớn này, em đã khái quát lại tổng quan về Physical Layer Security (PLS) và Convert Communication. Em đã tìm hiểu và tổng hợp các khái niệm cơ bản, nguyên lý hoạt động của hai phương pháp này trong lĩnh vực bảo mật thông tin. Ngoài ra, em đã sử dụng Matlab và công cụ CVX để triển khai mã và so sánh, đánh giá ưu điểm và nhược điểm của hai cách tiếp cận PLS và Convert Communication. Qua việc lập trình và phân tích kết quả, em đã rút ra được những nhận định quan trọng về hiệu quả và hạn chế của mỗi phương pháp.

Source Code: https://github.com/HuyHKr/Convert-communication-versus-PLS-using-CVX

IX. TÀI LIỆU THAM KHẢO

[1] A. D. Wyner, *The wire-tap channel*, Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355-1387, Oct. 1975

[2] *Covert Communications Versus Physical Layer Security* Moslem Forouzesh, Paeiz Azmi, Senior Member, IEEE, Nader Mokari, Member, IEEE, and Kai Kit Wong, Fellow, IEEE

[3] I. CVX Research, CVX: Matlab software for disciplined convex programming, version 2.0, http://cvxr.com/cvx, Aug. 2012.