PERFORMANCE EVALUATION OF SECURITY WHEN USING ARTIFICIAL NOISE FOR ONE-WAY FULL-DUPLEX RELAY NETWORKS

Ho Quoc Bao*

Faculty of Engineering and Technology,

Van Hien University, 665-667-669 Dien Bien Phu St., Ward 1, District 3, Ho Chi Minh City

*Email: *baohq@vhu.edu.vn*

Received: 6 March 2025; Revised: 24 March 2025; Accepted: 16 April 2025

ABSTRACT

In this paper, we are presenting a method to improve physical layer security (PLS) in wireless communication networks. Specifically, we would like to propose a one-way full-duplex (OWFD) relay network model with artificial noise (AN). The model consists of five nodes (source node, destination node, relay node, eavesdropping node, jamming node). To evaluate the security performance of the model, we analyzed key performance metrics such as the secrecy outage probability (SOP) and the system's secrecy throughput (STP) through deriving closed-form expressions for SOP and STP. Simulation results verify the proposed expressions using the Monte-Carlo method. The findings of this study demonstrated a significant improvement in security performance compared to previous researches. Additionally, the proposed model has highlighted the feasibility of implementing PLS techniques in OWFD relay networks.

Keywords: Physical layer security, Secrecy outage probability, Secure throughput, Artificial noise, One-way full-duplex.

1. INTRODUCTION

Wireless networks, with their widespread applications, have become an indispensable part of our daily lives. These networks have been increasingly demanding more spectral resources to accommodate the growing number of users [1]. Full-duplex (FD) technology allows simultaneous transmission and reception on a single time-frequency channel, promising nearly to double the spectral efficiency compared to half-duplex (HD) systems [2-5]. In FD techniques, signals are transmitted and received on the same frequency and at the same time [6]. One of the growing concerns in wireless communication is the security of transmitted signals. Due to the open nature of wireless networks, they are inherently insecure [7]. The simplicity of accessing the wireless medium made communications easier to be eavesdropped on over this medium [8]. The artificial noise (AN) approach - proposed by Goel and Negi [9, 10] is a technique to ensure absolute secure communication between legitimate nodes. The authors demonstrated that perfect security could be achieved when the channel of the eavesdropper was noisier than the channel of the legitimate receiver. AN is added to the null space of the legitimate receiver's channel so that it deteriorates the signal reception of the eavesdroppers without harming the communications of the legitimate receiver [11].

1.1. Related works

In [12], the author analyzed and evaluated the trade-off between system reliability and security, using a Rayleigh fading channel, FD communication, and the DF protocol at the relay node, PLS is achieved by introducing AN to the eavesdropping node. In [13], the author evaluated the SOP and STP of the system, considering a Rayleigh fading channel, the DF protocol, and FD at the relay node, PLS is implemented by harvesting energy at the system's relay node. The research group also investigated, analyzed, and evaluated the SOP and interception probability (IP) of the system, where a Rayleigh fading channel was used in the model with the amplify-and-forward (AF) protocol and HD operation at the relay node [14]. A system consisting of five nodes, including one node acting as a signal reflector for the source node's transmission, was studied using a Rayleigh fading channel, HD operation, and the DF protocol at the relay node, the model examines the OP and secure energy efficiency performance, enhancing system security through an intelligent reflecting surface (IRS) [15]. In [16], the research group analyzed and evaluated the OP and IP of the system, using a Nakagami-m fading channel, the system does not employ FD devices, and PLS is achieved by utilizing an IRS for signal forwarding, since the signal is directly transmitted, neither the AF nor DF protocol is used. Notably, in [17], the author investigated the hardware of reconfigurable intelligent surfaces (RIS) to optimize PLS, introduced corresponding scenarios, and studied system models that do not include FD or relay devices. The author also discussed potential future research directions and challenges in RIS-assisted PLS communication.

From the above studies, we have also identified open issues for future research, such as introducing additional jamming devices into the system, enabling full-duplex operation at the source, relay, and legitimate receiver, adding a direct link from the source to both the legitimate receiver and the eavesdropper in the research model, modifying the channel model, and changing the relay node protocol.

1.2. Motivation

Although studies [12-17] analyzed and evaluated the trade-off between reliability and security, SOP, and STP for half-duplex and full-duplex models with relay nodes, jamming from the source node, and Rayleigh fading and Nakagami-m channels, they have not yet addressed the destination node in the system or artificial jamming from external nodes. Additionally, the direct signal transmission path from the source node to the destination node has not been investigated for this system.

This paper minimizes the signal-to-noise ratio (SNR) at the eavesdropping node by introducing interference from an external node and the destination node to enhance security and significantly improve the secrecy performance of the OWFD relay network. On the other hand, FD at the legitimate receiving node helps save bandwidth and protect useful information during signal transmission.

The main contributions of this paper include the following:

- Generate AN to enhance information security and apply FD to save bandwidth for the OWFD relay network.
- Propose closed-form and accurate expressions for SOP and STP for analyzing the performance of the OWFD relay network.
- Effectively demonstrate the role of AN generators and their significant impact on system performance in preventing eavesdropping.
- Conduct Monte Carlo simulations to validate the accuracy of the SOP and STP expressions.

1.3. Organization

This paper is structured into six sections as follows. The next section presents the system model under consideration. Section 3 analyzes and provides details on the expressions for secrecy outage probability (SOP) and secure throughput (STP). Section 4 presents the results and discussions. Section 5 provides the conclusion. Finally, there is an appendix.

2. SYSTEM MODEL

Consider a communication system consisting of a source node S, a full-duplex relay node R, a full-duplex destination node D, a passive eavesdropper node E, and a jammer node J, as shown in Figure 1 of this paper. Assume that S, E, and J each has a single antenna, while R and D are equipped with two antennas for transmission and reception. The relay R operates using the decode-and-forward (DF) protocol, D receives signals simultaneously from S and R, while node E only eavesdrops on the signal from R. Assume that node E cannot eavesdrop on the signal from node S due to terrain features such as trees, hills, high-rise buildings, etc., which obstruct the signal transmission path to node E. Given $p \in \{S-R,\ S-E,\ R-D,\ R-E,\ D-R,\ D-E, J-E\}$, the coefficient for the Rayleigh fading channel is h_p which is distributed according to $h_p \sim CN\left(0, \lambda_p\right)$, with $\lambda_p = E\left\{\left|h_p^2\right|\right\}$ being the average channel gain. By denoting $q \in \{S, R, D, J\}$, the transmit power at node q is P_q. The Gaussian noise at node k is $n_k(t)$, which follows the distribution $n_k(t) \sim CN(0, \sigma_k)$, with the normalized noise variance being $\sigma_k = N_0$, $k \in \{R, D, E\}$. The SNR at node k is denoted as γ_k. Since the channels in the system model follow the Rayleigh fading model, the probability density function (PDF) and the cumulative distribution function (CDF) of each channel gain are given by $f_{|h_p|^2}(x) = \frac{1}{\lambda_p} e^{-\frac{x}{\lambda_p}}$ and $F_{|h_p|^2}(x) = 1 - e^{-\frac{x}{\lambda_p}}$, respectively, with $x > 0$.

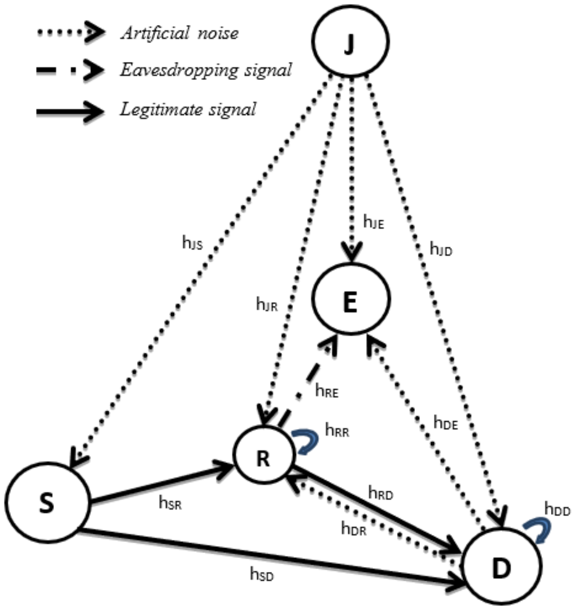

Figure 1. One-way full-duplex relay network model with the presence of an eavesdropping device.

Assume that at time t, S transmits signal $x_S(t)$ to R and D. Meanwhile, D and J transmit a jamming signal $w_D(t), w_J(t)$ to R and E, and E eavesdrops on the signal from R. The purpose of the jamming signals is to reduce the SNR at E, thereby enhancing the security performance. $w_D(t), w_J(t)$ and $x_S(t)$ are normalized such that $E\{|w_D(t)|^2\} = E\{|w_J(t)|^2\} = E\{|x_S(t)|^2\} = 1$, where $E\{.\}$ is the expectation operator. If R decodes $x_S(t)$ successfully, it decodes and re-encodes before broadcasting. Otherwise, it keeps idle.

$$E\{|\mathrm{w}_D(t)|^2\} = E\{|\mathrm{w}_J(t)|^2\} = E\{|x_S(t)|^2\} = 1.$$

where $E\{.\}$ is the expectation operator.
At time t, the received signal at R is given as follows

$$y_R(t) = h_{SR}\sqrt{P_S}x_S(t) + h_{RR}\sqrt{P_R}x_R(t) + h_{DR}\sqrt{P_D}w_D(t) + h_{JR}\sqrt{P_J}w_J(t) + n_R(t) \tag{1}$$

Since the artificial noise can be known in advance at R [2-3], and R can cancel the interference $h_{JR}w_J(t)$ and $h_{DR}w_D(t)$, the received signal after AN cancellation at R is given by

$$\tilde{y}_R(t) = h_{SR}\sqrt{P_S}x_S(t) + h_{RR}\sqrt{P_R}x_R(t) + n_R(t) \tag{2}$$

At time *t*, the received signals at E and D are given as follows

$$y_E(t) = h_{RE}\sqrt{P_R}x_R(t) + h_{DE}\sqrt{P_D}w_D(t) + h_{JE}\sqrt{P_J}w_J(t) + n_E(t) \tag{3}$$

$$y_D(t) = h_{SD}\sqrt{P_S}x_S(t) + h_{RD}\sqrt{P_R}x_R(t) + h_{DD}\sqrt{P_D}w_D(t) + h_{JD}\sqrt{P_J}w_J(t) + n_D(t) \tag{4}$$

Since the artificial noise can be known in advance at D, and D can cancel the interference $h_{JD}\mathrm{w}_J(t)$, the received signal after AN cancellation at D is given by

$$\tilde{y}_D(t) = h_{SD}\sqrt{P_S}x_S(t) + h_{RD}\sqrt{P_R}x_R(t) + h_{DD}\sqrt{P_D}w_D(t) + n_D(t) \tag{5}$$

From (1), (3), and (4), the SNRs at the nodes R, E, and D at time *t* are respectively given as follows. The SNR at node R is

$$\gamma_R = \frac{|h_{SR}|^2 P_S}{|h_{RR}|^2 P_R + N_0} \tag{6}$$

The SNR at node E when R decodes $x_S(t)$ successfully, which means $x_R(t) = x_S(t)$, is

$$\gamma_E = \frac{|h_{RE}|^2 P_R}{|h_{DE}|^2 P_D + |h_{JE}|^2 P_J + N_0} \tag{7}$$

The SNR at node E when R fails to decode $x_S(t)$, meaning $x_R(t) \neq x_S(t)$, is

$$\gamma_E^* = 0 \tag{8}$$

Then, the SNR at node D when R decodes $x_S(t)$ successfully is

$$\tilde{\gamma}_D = \frac{|h_{SD}P_S + h_{RD}P_R|^2}{|h_{DD}|^2 P_D + N_0} \leq \gamma_D = \frac{|h_{SD}|^2 P_S + |h_{RD}|^2 P_R}{|h_{DD}|^2 P_D + N_0} \tag{9}$$

The SNR at node D when decoding $x_S(t)$ fails:

The SNR at node D when R fails to decode $x_S(t)$ is

$$\gamma_D^* = \frac{|h_{SD}|^2 P_S}{|h_{RD}|^2 P_R + |h_{DD}|^2 P_D + N_0} \tag{10}$$

3. SECURITY PERFORMANCE ANALYSIS

In this section, the SOP is derived. The secrecy capacity is defined as the difference between the legitimate channel capacity C_D and the eavesdropping channel capacity C_E:

$$C_S = [C_D - C_E]^+ = \frac{1}{2}\left[\log_2 \frac{1+\gamma_D}{1+\gamma_E}\right]^+ \tag{11}$$

where C_T and C_E are the transmission signal capacity and the eavesdropping signal capacity, respectively, $[x]^+ = max(x,0)$.

Theorem 1: The CDF and PDF of γ_R are respectively given by

$$F_{\gamma_R}(x) = 1 - a_0 \frac{e^{-b_0 x}}{a_0 + x} \tag{12}$$

$$f_{\gamma_R}(x) = \frac{a_0 b_0 e^{-b_0 x}}{a_0 + x} + \frac{a_0 e^{-b_0 x}}{(a_0 + x)^2} \tag{13}$$

where $a_0 = \frac{\lambda_{SR} P_S}{\lambda_{RR} P_R}$ and $b_0 = \frac{N_0}{\lambda_{SR} P_S}$.

Proof of Theorem 1

From (6), the CDF of γ_R is calculated as follows

$$\begin{aligned} F_{\gamma_R}(x) &= \Pr\left(\frac{|h_{SR}|^2 P_S}{|h_{RR}|^2 P_R + N_0} < x \right) \\ &= \Pr\left(x_0 < x \frac{(x_1 P_R + N_0)}{P_S} \right) \\ &= \int_0^\infty \left(1 - e^{-\frac{1}{\lambda_{SR}} x \frac{(x_1 P_R + N_0)}{P_S}} \right) \frac{1}{\lambda_{RR}} e^{-\frac{1}{\lambda_{RR}} x_1} dx_1 \\ &= 1 - a_0 \frac{e^{-b_0 x}}{a_0 + x} \end{aligned} \tag{14}$$

where $x_0 = |h_{SR}|^2$ and $x_1 = |h_{RR}|^2$.

From (14), the PDF of γ_R is the first derivative of $F_{\gamma_R}(x)$, calculated as follows

$$f_{\gamma_R}(x) = -a_0 \frac{-b_0 e^{-b_0 x}(a_0 + x) - e^{-b_0 x}}{(a_0 + x)^2} = \frac{a_0 b_0 e^{-b_0 x}}{a_0 + x} + \frac{a_0 e^{-b_0 x}}{(a_0 + x)^2} \tag{15}$$

Theorem 2: The CDF of γ_D is given by

$$F_{\gamma_D}(y) = 1 - \frac{e^{-a_1 y}}{b_1 (y + c_1)} \left(1 + \frac{1}{d_1} \right) + \frac{e^{-f_1 y}}{e_1 d_1 (y + g_1)} \tag{16}$$

where $a_1 = \frac{N_0}{\lambda_{RD} P_R}$, $b_1 = \frac{\lambda_{DD} P_D}{\lambda_{RD} P_R}$, $c_1 = \frac{\lambda_{RD} P_R}{\lambda_{DD} P_D}$, $d_1 = \lambda_{RD} \left(\frac{P_R}{P_S \lambda_{SD}} - \frac{1}{\lambda_{RD}} \right)$, $e_1 = \frac{\lambda_{DD} P_D}{P_S \lambda_{SD}}$, $f_1 = \frac{N_0}{P_S \lambda_{SD}}$, and $g_1 = \frac{P_S \lambda_{SD}}{\lambda_{DD} P_D}$.

Proof of Theorem 2

When R does successful decoding, one has

$$\begin{aligned} F_{\gamma_D}(y) &= \Pr\left(\frac{|h_{SD}|^2 P_S + |h_{RD}|^2 P_R}{|h_{DD}|^2 P_D + N_0} < y \right) \\ &= \Pr\left(\frac{Q}{|h_{DD}|^2 P_D + N_0} < y \right) \end{aligned} \tag{17}$$

where

$$\begin{aligned}
F_Q(q) &= \Pr(Q<q) \\
&= \Pr\left(|h_{SD}|^2 P_S + |h_{RD}|^2 P_R < q\right) \\
&= \int_0^{\frac{q}{P_R}} \left(1-e^{-\frac{\frac{q}{P_S}-q_1\frac{P_R}{P_S}}{\lambda_{SD}}}\right)\frac{1}{\lambda_{RD}}e^{-\frac{q_1}{\lambda_{RD}}}dq_1 \\
&= 1-e^{-\frac{q}{\lambda_{RD}P_R}} - \frac{e^{-\frac{q}{\lambda_{RD}P_R}}}{\lambda_{RD}\left(\frac{P_R}{P_S\lambda_{SD}}-\frac{1}{\lambda_{RD}}\right)} + \frac{e^{-\frac{q}{P_S\lambda_{SD}}}}{\lambda_{RD}\left(\frac{P_R}{P_S\lambda_{SD}}-\frac{1}{\lambda_{RD}}\right)}
\end{aligned} \quad (18)$$

Therefore

$$\begin{aligned}
F_{\gamma_D}(y) &= \Pr\left(Q<y\left(|h_{DD}|^2 P_D + N_0\right)\right) \\
&= \int_0^{\infty} F_Q\left(y\left(y_0P_D+N_0\right)\right) f_{|h_{DD}|^2}(y_0)\,dy_0 \\
&= 1-\frac{e^{-a_1y}}{b_1(y+c_1)}\left(1+\frac{1}{d_1}\right)+\frac{e^{-f_1y}}{e_1d_1(y+g_1)}
\end{aligned} \quad (19)$$

where $y_0 = |h_{DD}|^2$.

When R suffers unsuccessful decoding, one has

$$\begin{aligned}
F_{\gamma_D^*}(z) &= \Pr\left(\frac{|h_{SD}|^2 P_S}{|h_{RD}|^2 P_R + |h_{DD}|^2 P_D + N_0} < z\right) \\
&= \Pr\left(z_0 < \frac{z}{P_S}\left(z_1P_R+z_2P_D+N_0\right)\right) \\
&= \int_0^{\infty}\int_0^{\infty}\left(1-e^{-\frac{z}{\lambda_{SD}P_S}\left(z_1P_R+z_2P_D+N_0\right)}\right) f(z_1)\,f(z_2)\,dz_1dz_2 \\
&= 1-\frac{1}{a_3}\left(\frac{e^{-b_3z}}{z+c_3}-\frac{e^{-b_3z}}{z+d_3}\right)
\end{aligned} \quad (20)$$

where $z_0 = |h_{SD}|^2$, $z_1 = |h_{RD}|^2$ and $z_2 = |h_{DD}|^2$.

Theorem 3: The CDF and PDF of γ_E are respectively given by

$$F_{\gamma_E}(t) = 1-\frac{1}{b_2}\left(\frac{e^{-a_2t}}{(t+c_2)}-\frac{e^{-a_2t}}{(t+d_2)}\right) \quad (21)$$

and

$$f_{\gamma_E}(t)=\frac{1}{b_2}\left(\frac{a_2e^{-a_2t}}{(t+c_2)}+\frac{e^{-a_2t}}{(t+c_2)^2}-\frac{a_2e^{-a_2t}}{(t+d_2)}-\frac{e^{-a_2t}}{(t+d_2)^2}\right) \tag{22}$$

where $a_2=\frac{N_0}{\lambda_{RE}P_R}$, $b_2=\frac{\lambda_{DE}P_D}{\lambda_{RE}P_R}-\frac{\lambda_{JE}P_J}{\lambda_{RE}P_R}$, $c_2=\frac{\lambda_{RE}P_R}{\lambda_{DE}P_D}$, and $d_2=\frac{\lambda_{RE}P_R}{\lambda_{JE}P_J}$.

Proof of Theorem 3

Analyzing (7), we have the CDF of γ_E by applying [18, eq. (3.352.4) and eq. (3.353.3)]

$$\begin{aligned}F_{\gamma_E}(t)&=\Pr\left(\frac{|h_{RE}|^2P_R}{|h_{DE}|^2P_D+|h_{JE}|^2P_J+N_0}<t\right)\\&=\int_0^\infty\int_0^\infty\left(1-e^{-\frac{t}{\lambda_{RE}P_R}(t_1P_D+t_2P_J+N_0)}\right)f(t_1)f(t_2)\,dt_1dt_2\\&=1-\frac{1}{b_2}\left(\frac{e^{-a_2t}}{t+c_2}-\frac{e^{-a_2t}}{t+d_2}\right)\end{aligned} \tag{23}$$

where $t_1=|h_{DE}|^2$ and $t_2=|h_{JE}|^2$.

From (23), the PDF of γ_E is the first derivative of $F_{\gamma_E}(t)$, calculated as follows

$$f_{\gamma_E}(t)=\frac{1}{b_2}\left(\frac{a_2e^{-a_2t}}{t+c_2}+\frac{e^{-a_2t}}{(t+c_2)^2}-\frac{a_2e^{-a_2t}}{t+d_2}-\frac{e^{-a_2t}}{(t+d_2)^2}\right) \tag{24}$$

3.1. System secrecy outage probability

The SOP is the probability that occurs if the secrecy capacity is lower than a given threshold C_{th}, hence given by

$$SOP=\Pr(C_S<C_{th}) \tag{25}$$

where C_S is the secure capacity of the system, and C_{th} is the predefined threshold of the capacity at the legitimate eavesdropper node.

When the node R does successful decoding, the SOP is calculated as follows

$$\begin{aligned}SOP_{Nerror}&=\Pr\left(C_s^{Nerror}<C_{th}\right)\\&=\Pr\left(\log_2\frac{1+\gamma_D}{1+\gamma_E}<C_{th}\right)\\&=\Pr\left(\gamma_D<2^{C_{th}}\gamma_E+2^{C_{th}}-1\right)\\&=F_{\gamma_D}\left(2^{C_{th}}\gamma_E+2^{C_{th}}-1\right)\end{aligned} \tag{26}$$

When the node R suffers unsuccessful decoding, the SOP is calculated as follows

$$\begin{aligned} SOP_{Error} &= \Pr\left(C_S^{Error} < C_{th}\right) \\ &= \Pr\left(\log_2 \frac{1+\gamma_D^*}{1+\gamma_E^*} < C_{th}\right) \\ &= \Pr\left(\gamma_D^* < 2^{C_{th}}\gamma_E^* + 2^{C_{th}} - 1\right) \\ &= \Pr\left(\gamma_D^* < 2^{C_{th}} - 1\right) \\ &= F_{\gamma_D^*}\left(2^{C_{th}} - 1\right) \end{aligned} \tag{27}$$

Therefore, the SOP of the system is provided by

$$\begin{aligned} SOP &= SOP_{Nerror} \Pr\left(\gamma_R \geq 2^{C_{th}} - 1\right) + SOP_{Error} \Pr\left(\gamma_R < 2^{C_{th}} - 1\right) \\ &= SOP_{Nerror}\left(1 - \Pr\left(\gamma_R < 2^{C_{th}} - 1\right)\right) + SOP_{Error} \Pr\left(\gamma_R < 2^{C_{th}} - 1\right) \\ &= SOP_{Nerror}\left(1 - F_{\gamma_R}\left(2^{C_{th}} - 1\right)\right) + SOP_{Error} F_{\gamma_R}\left(2^{C_{th}} - 1\right) \end{aligned} \tag{28}$$

3.2. Secrecy throughput

The secrecy throughput is the product of the secrecy rate and the secrecy outage probability, defined as follows

$$STP = R_s(1 - SOP) \ \ (\text{bit/ s/ Hz}) \tag{29}$$

where STP is the secrecy throughput of the system, R_S is the secrecy rate of the system, and SOP is the secrecy outage probability of the system.

4. RESULTS AND DISCUSSION

This section presents numerical results and simulations to verify the proposed SOP and STP expressions, and evaluate the security performance of the OWFD relay network. The SOP and STP are evaluated based on key operating parameters, such as the position of R, the position of E, the path loss exponent β, the given threshold of the capacity $C_{th} = \{0.01,\ 0.05,\ 0.1\}$ (bits/s/Hz).

To illustrate the performance, the coordinates of the users are chosen as S at $(0.0, 0.0)$, D at $(8.0, 8.0)$, R at $(5.0, 4.0)$, E at $(10.0, 14.0)$, J at $(8.0, 20.0)$. In the following, x_S, x_D, x_E, x_J and y_S, y_D, y_E, y_J represent the x-coordinate and y-coordinate of S, D, E, J, respectively. Additionally, $P_S = 20$ dB, $P_R = 1$ dB, $P_D = -25$ dB and $P_J = 25$ dB are considered. The path loss and fading power are modeled as $d^{-\beta}$, with d representing the distance from the transmitter to the receiver. Among all the results, one result considers different transmission environments, so the value of β is selected to run from 1 to 6, while the remaining results are chosen with $\beta = 3$.

Figure 2 describes the effect of SNR on SOP at three different positions of node J with $y_D = \{20, 25, 30\}$ meters and $C_{th} = 0.01$ (bits/s/Hz). This figure shows the match between the simulation and analysis, validating the proposed SOP expressions. It can be observed that as P_S/σ^2 increases, SOP decreases. This can be explained as follows: Node E eavesdrops on the signal from nodes S, R, D while being affected by AN from node J, whereas node D only receives the signal from node R and cancels out the AN from node J. Therefore, as P_S/σ^2 increases, the SNR at E

increases, but at a slower rate than the SNR at D, because node E receives three channels. There are two channels with noise, so these noise components reduce the increase of SNR at E, which causes C_S to increase, and thus SOP decreases. Additionally, as node J moves further away from the four nodes S,R,D,E, the SNR at E increases, leading to a decrease in C_S, while the SNR at D remains constant, causing SOP to increase.

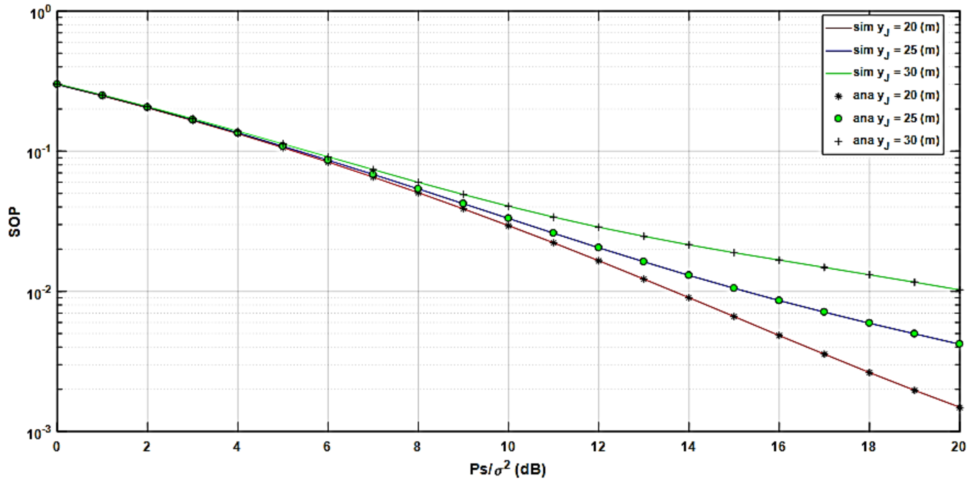

Figure 2. The effect of SNR on SOP at three different positions of node J.

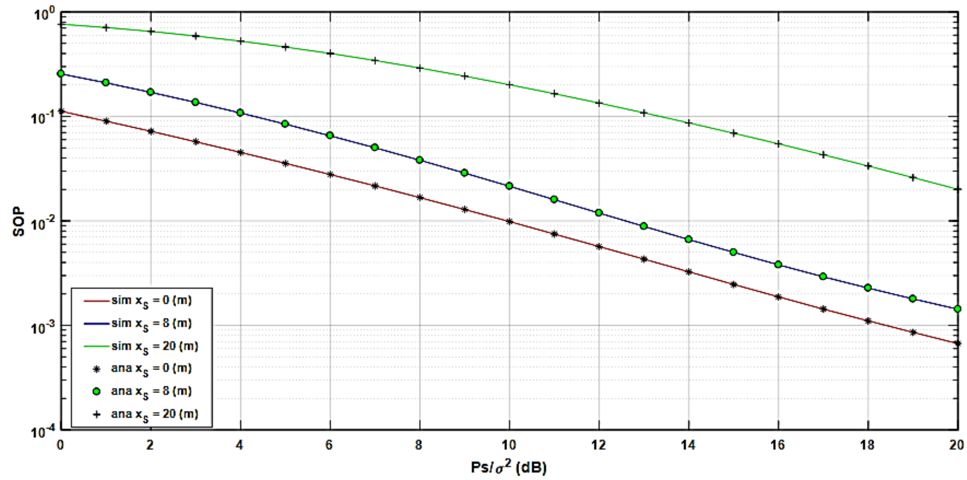

Figure 3. The impact of value P_S/σ^2 when changing the position of node S.

Figure 3 illustrates the effect of the distance of node S on SOP as different values of P_S/σ^2 are varied. The graph shows the match between simulation and analysis. As the transmission power of node S, P_S/σ^2 increases, the SNR at node R and D increases, leading to an increase in the system's security, or in other words, SOP decreases. Since the SNR at node D increases, the system's secrecy capacity increases, causing SOP to decrease. On the other hand, as the x-coordinate of node S increases, the SNR at D decreases, causing SOP to increase.

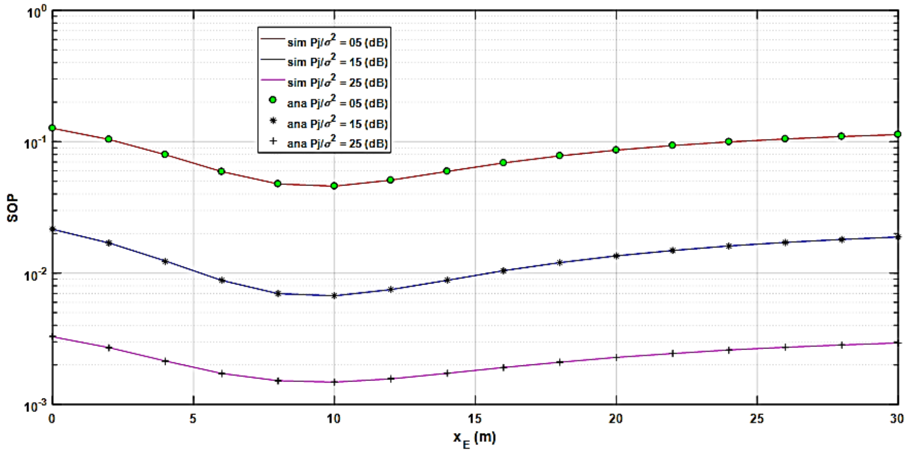

Figure 4. The effect of the position of node E on SOP as the value of P_S/σ^2 changes.

Figure 4 illustrates the effect of the distance of node E on SOP at three different values of P_S/σ^2. The graph shows the match between simulation and analysis. As the value of x_E gets closer to node J, SOP decreases, and as it moves further away from node J, SOP increases. This can be explained as follows: The node E is closer to node J, the higher the noise power at node E, and vice versa. Therefore, the SNR at node E increases, leading to a decrease in SOP, and vice versa. Furthermore, the adjacent position $x_E = 8\ (\text{m})$ of node E results in a minimum SOP, as it is closest to nodes D and J, causing the SNR at node E to be the lowest. On the other hand, as the transmission power of node J increases, SOP decreases because the SNR at node D increases, which in turn leads to an increase in the system's secrecy capacity.

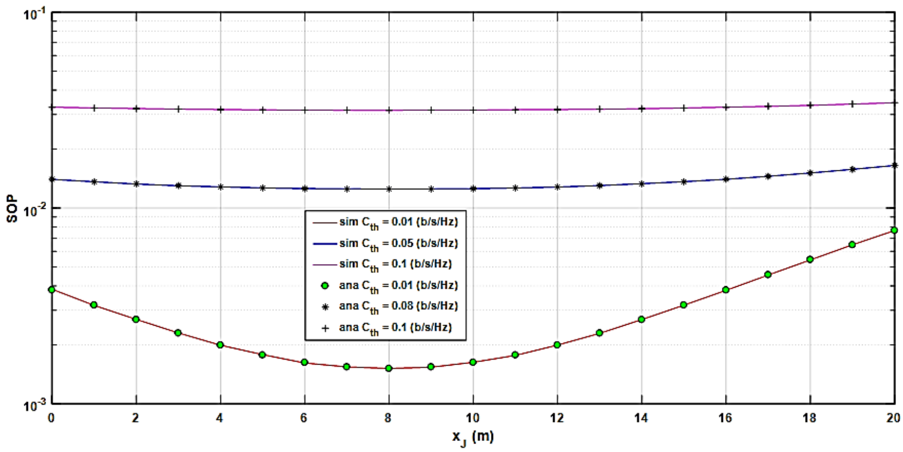

Figure 5. The effect of x_J on SOP at three different values of C_{th}.

Figure 5 shows the match between simulation and analysis. This figure illustrates that as the length x_J increases up to 8 (m), SOP gradually decreases. Beyond 8 (m), SOP starts to increase because, at $x_J = 8\ (\text{m})$, node J is closest to node E, while the distance from node E to node D remains fixed. As a result, the SNR at E is the lowest, meaning it reaches a minimum at point $J = (8.0, 20.0)$, leading to a minimum SOP. At the same time, the higher the predefined threshold C_{th}, the greater the SOP of the system.

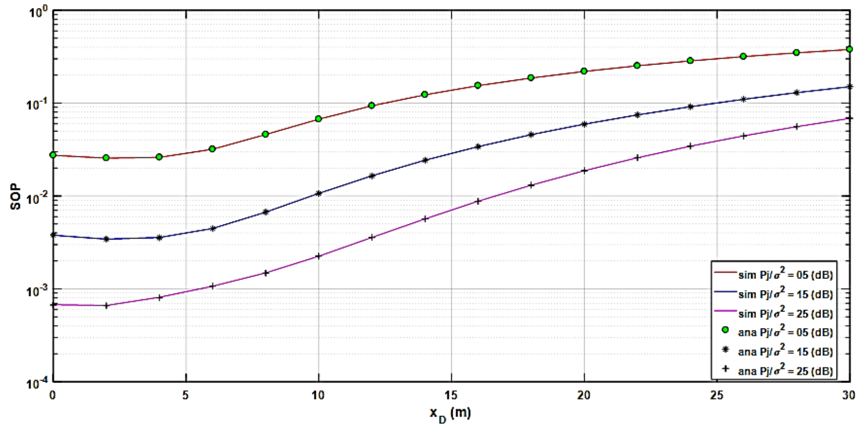

Figure 6. The impact of x_D on SOP at three values of P_J/σ^2 .

Figure 6 illustrates the impact of the distance of node D on SOP when varying the values of P_J/σ^2 . The graph shows a match between simulation and analysis. As the transmit power of node D, denoted as P_D/σ^2 , increases, the SNR at node E decreases, leading to a reduction in system security; in other words, SOP increases. On the other hand, as the abscissa of node x_D increases, meaning the distance from node D to node E increases, the SNR at E decreases, causing SOP to increase. Furthermore, when the distance between nodes is fix and the transmit power P_J/σ^2 increases, the SNR at node E decreases, resulting in a decrease in SOP.

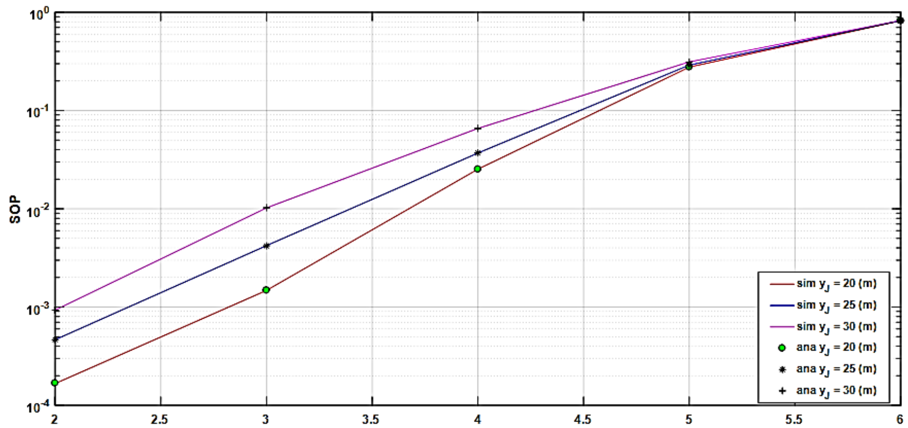

Figure 7. The effect of β on SOP at three values of $y_J = \{20,\ 25,\ 30\}$ (m).

Figure 7 illustrates the effect of β on SOP and also shows the match between simulation and analysis. It is clearly observed that as β increases, the received noise power at node E increases, leading to a decrease in SNR at node E. As a result, C_S increases, causing SOP to decrease. The simulation results clearly show that at $\beta = 2$, SOP reaches its minimum. On the other hand, as node J moves further away from node E, the SNR at node E decreases, leading to an increase in SOP of the system.

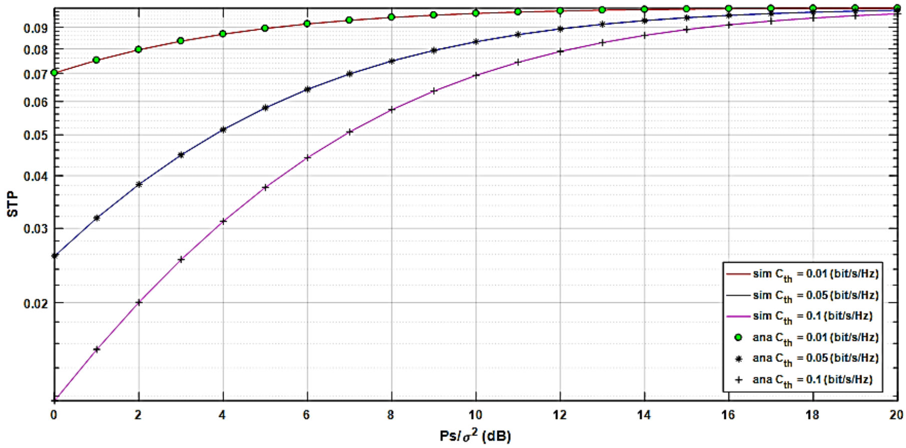

Figure 8. The influence of P_S/σ^2 on STP at three Values of C_{th}.

Figure 8 illustrates the impact of P_S/σ^2 on STP, also showing the consistency between simulation and analysis. It can be observed that as P_S/σ^2 increases, C_S also increases because the throughput is inversely proportional to the system's secure stopping probability. As a result, SOP decreases, leading to an increase in STP. On the other hand, as node E moves closer to node J while node D remains fixed, C_S increases because the SNR at node E decreases. As a result, SOP decreases, leading to an increase in STP. Therefore, P_S/σ^2 is always directly proportional to STP and inversely proportional to SOP.

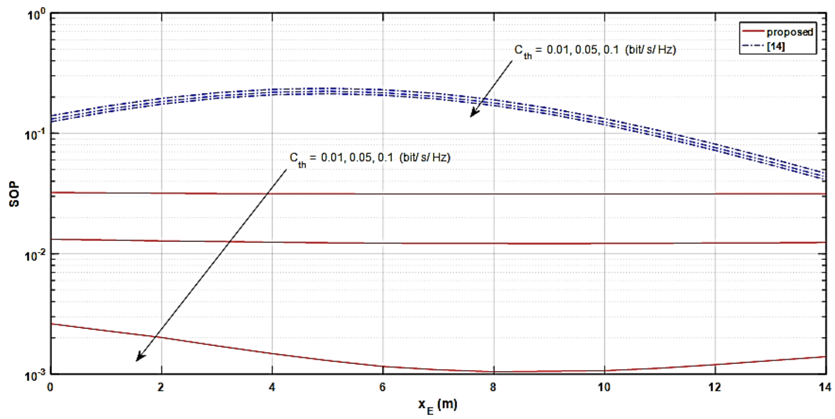

Figure 9. Comparison of SOP between the proposed model and [14] when varying C_{th}.

Figure 9 illustrates the simulation curves comparing the proposed model with the reference model in [14]. For a fair comparison, the total transmission power in both models is set to be equal. The results show that the SOP of the proposed model is significantly lower than that of the reference model. In other words, the security performance of the proposed model is much better than that of the reference model [14].

5. CONCLUSION

The problem model has proposed a jamming protocol to generate AN for the OWFD system. The AN is transmitted from J and D to reduce the signal capacity received by E, thereby increasing reliability R and improving C_S of the system. The analysis clearly showed that jamming is significantly more effective than non-jamming for the system. The results also indicated that the higher the SNR, the lower the SOP of the system, which leads to a higher STP of the system. By using MATLAB software and the Monte Carlo simulation method, the accuracy of analyzing the problems in the system is demonstrated through the alignment between the simulation curve and the analytical curve. Additionally, the results have assessed the impact of parameter β on the SOP of the system.

The paper has proposed the OWFD relay networks with AN. The analysis clearly showed that introducing AN is always much more effective than not introducing it into the system model. The results also indicated that as the SNR increases, the SOP decreases, leading to a higher STP. By using the MATLAB software and the Monte Carlo simulation method, the accuracy of the analysis has been demonstrated through the alignment between the simulation curve and the analytical curve. Furthermore, the results have provided the optimal selection of the power division coefficient and capacity threshold for maximum security performance. The results also evaluated how β influences security performance.

REFERENCES

1. He H., Lyu S., He Q., and Xu D. - Network coding assisted secure transmission in full-duplex relay networks, IEEE Transactions on Vehicular Technology **69** (8) (2020) 9196-9200. https://doi.org/10.1109/TVT.2020.3001871.
2. Park J., Yun S., Kim I., and Ha J. - Secure communications with a full-duplex relay network under residual self-interference, IEEE Communications Letters **24** (3) (2020) 496-500. https://doi.org/10.1109/LCOMM.2019.2958809.
3. Khoshafa M.H., Ngatched T.M.N., Ahmed M.H., and Ibrahim A. - Secure transmission in wiretap channels using full-duplex relay-aided D2D communications with outdated CSI, IEEE Wireless Communications Letters **9** (8) (2020) 1216-1220. https://doi.org/10.1109/LWC.2020.2986404.
4. Zaghdoud N., Mnaouer A.B., Alouane WH., Boujemaa H., and Touati F. - Secure performance analysis for full-duplex cooperative NOMA system in the presence of multiple eavesdroppers, 2020 International Wireless Communications and Mobile Computing (IWCMC) (2020) 1719-1725. https://doi.org/10.1109/IWCMC48107.2020.9148456.
5. Guo., Weidong., and Yuxi Liu. - On the performance of physical layer security in virtual full-duplex non-orthogonal multiple access system, EURASIP Journal on Wireless Communications and Networking (2021) 1-14. https://doi.org/10.21203/rs.3.rs-257146/v1.
6. Lim J.T., Kim T., and Bang I. - Impact of outdated csi on the secure communication in untrusted in-band full-duplex relay networks, IEEE Access **10** (2022) 19825-19835. https://doi.org/10.1109/ACCESS.2022.3151792.
7. Zabir I., Maksud A., Chen G., Sadler B.M., and Hua Y. - Secrecy of multi-antenna transmission with full-duplex user in the presence of randomly located eavesdroppers, IEEE Transactions on Information Forensics and Security **16** (2021) 2060-2075. https://doi.org/10.1109/TIFS.2020.3047763.
8. Din F.U., and Labeau F. - Artificial noise assisted in-band full-duplex secure channel estimation, IEEE Transactions on Vehicular Technology **70** (7) (2021) 6800-6813. https://doi.org/10.1109/TVT.2021.3082810.
9. Goel S., and Negi R. - Secret communication in presence of colluding eavesdroppers, MILCOM 2005 - 2005 IEEE Military Communications Conference **3** (2005) 1501–1506. https://doi.org/10.1109/MILCOM.2005.1605889.
10. Goel S., and Negi R. - Guaranteeing secrecy using artificial noise, IEEE Communications Letters **7** (6) (2008) 2180-2189. https://doi.org/10.1109/twc.2008.060848.
11. Zhang X., Chen D., Li J., Wang Z., Li X. - Security-Reliability tradeoff analysis of untrusted full-duplex relay networks, Wireless Communications & Mobile Computing (2022) 2419430. https://doi.org/10.1155/2022/2419430
12. Cao Z., Ji X., Wang J., Zhang S., Ji Y., Li Y., Wang J. - Security-reliability trade-off analysis of an-aided relay selection for full-duplex relay networks, IEEE Transactions on Vehicular Technology **70** (3) (2021) 2362-2377. https://doi.org/10.1109/TVT.2021.3057830

13. Silva I.W.G.D., Sánchez J.D.V., Olivo E.E.B., and Moya Osorio D.P. - Impact of self-energy recycling and cooperative jamming on SWIPT-based FD relay networks with secrecy constraints, IEEE Access **10** (2022) 24132-24148. https://doi.org/ 10.1109/ACCESS.2022.3155498

14. Venugopalachary K., Mishra D., and Saini R. - Exact outage analysis for non-regenerative secure cooperation against double-tap eavesdropping, Infocommunications Journal **14** (4) (2022) 42-48. https://doi.org/10.36244/ICJ.2022.4.6

15. Li X., Jiang J., Wang H., Han C., Chen G., Du J., Hu C., Mumtaz S. - Physical layer security for wireless-powered ambient backscatter cooperative communication networks, IEEE Transactions on Cognitive Communications and Networking **9** (4) (2023) 927-939. https://doi.org/10.1109/TCCN.2023.3270425

16. Jiangfeng Sun., Xingchang Chuai., Yanyang Zeng., and Xingwang Li. - Secrecy Analysis and prediction of ambient backscatter NOMA systems with I/Q imbalance, IEEE Open Journal of the Communications Society **5** (2024) 2980-2990, https://doi.org/ 10.1109/OJCOMS.2024.3395702

17. Mengzhao Guo., Zhi Lin., Ruiqian Ma., Kang An., Dong Li., Naofal Al-Dhahir., and Jiangzhou Wang. - Inspiring physical layer security with RIS: Principles, applications, and challenges, IEEE Open Journal of the Communications Society **5** (2024) 2903-2925. https://doi.org/10.1109/OJCOMS.2024.3392359

18. Gradshteyn I.S., Ryzhik I.M. - Table of Integrals, Series, and Products. Academic Press, 8th edition (2014) 1-1220. https://doi.org/10.1016/C2010-0-64839-5.

TÓM TẮT

ĐÁNH GIÁ HIỆU NĂNG BẢO MẬT CHO MẠNG CHUYỂN TIẾP SONG CÔNG MỘT CHIỀU SỬ DỤNG NHIỄU NHÂN TẠO

Hồ Quốc Bảo

Khoa Kỹ thuật Công nghệ,

Trường Đại học Văn Hiến, 665-667-669 Điện Biên Phủ, phường 1, quận 3, Tp.HCM

*Email: *baohq@vhu.edu.vn*

Bài báo này trình bày phương pháp để cải thiện các vấn đề bảo mật lớp vật lý (PLS) trong mạng truyền thông không dây. Cụ thể, chúng tôi xem xét mô hình mạng chuyển tiếp song công một chiều (OWFD) có gây nhiễu nhân tạo (AN) và sử dụng kênh truyền Rayleigh fading. Mô hình bao gồm năm nút: nút nguồn, nút chuyển tiếp, nút nghe lén, nút đích và nút gây nhiễu. Để đánh giá hiệu năng bảo mật của mô hình, chúng tôi tiến hành phân tích các thông số của các yếu tố như: xác suất dừng bảo mật (SOP), thông lượng bảo mật (STP) của hệ thống. Chúng tôi cũng đã đưa ra được các công thức dạng đóng cho các thông số SOP, STP trong mô hình. Kiểm chứng cho kết quả mô phỏng với kết quả tính toán bằng phương pháp Monte-Carlo. Kết quả nghiên cứu của bài báo cho thấy hiệu năng bảo mật được cải thiện đáng kể so với những nghiên cứu trước đây, đồng thời, mô hình đề xuất cũng cho thấy tính khả thi của việc triển khai các vấn đề PLS trong mạng OWFD.

Từ khóa: Bảo mật lớp vật lý, Xác suất dừng bảo mật, Thông lượng bảo mật, Nhiễu nhân tạo, Song công một chiều.