Research Article

Security-Reliability Tradeoff Analysis of Untrusted Full-Duplex Relay Networks

Xingang Zhang,1 Dechuan Chen,2,3,4 Jin Li,2 Zhipeng Wang,2 and Xiaotan Li5

1The College of Computer Science and Technology, Nanyang Normal University, Nanyang 473061, China
2The College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang 473061, China
3The Key Lab of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), Ministry of Education, Nanjing 210003, China
4The Henan Engineering Research Center for Radio Frequency Front End and Antenna of Millimeter Wave Wireless Communication System, Nanyang 473061, China
5The College of Mechanical and Electrical Engineering, Sichuan Agricultural University, Yaan 625014, China

Correspondence should be addressed to Dechuan Chen; chenchuan927@163.com

Received 24 May 2022; Revised 19 June 2022; Accepted 29 June 2022; Published 11 July 2022

Academic Editor: Xingwang Li

Copyright © 2022 Xingang Zhang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In this work, we investigate the physical layer security problem of wireless cooperative network, where the communication from a source to a destination is assisted by an untrusted full-duplex amplify-and-forward (AF) relay. In order to realize a positive secrecy rate, cooperative jamming is exploited at the destination. The secrecy outage probability (SOP), connection outage probability (COP), and effective secrecy throughput (EST) are, respectively, derived in closed-form expressions for the fixed gain relaying (FGR) scheme and the variable gain relaying (VGR) scheme. Subsequently, we conduct an asymptotic analysis for both the relaying schemes in the high signal-to-noise ratio (SNR) region to offer valuable insights into practical design. Theory and simulation results demonstrate that the self-interference caused by full-duplex transmission is harmful for the reliability performance, while it is beneficial to the security performance. Moreover, the EST of the considered system increases as the self-interference level decreases, which implies that the self-interference deteriorates an overall performance in terms of the security-reliability tradeoff.

1. Introduction

Due to the broadcast nature of wireless transmission, the communications between legitimate users are particularly vulnerable to be overheard by malicious users [1, 2]. Traditionally, cryptographic mechanism in the upper layers of the network based on computational complexity has been employed to guarantee secure communication in wireless networks [3]. However, as the computing power of malicious users is continuously enhancing (e.g., by adopting the quantum computing technology), cryptographic mechanism is being increasingly challenged. Unlike the cryptographic mechanism, physical layer security, which explores the time-varying properties of physical channels to achieve perfect security, has attracted considerable attention from academia and industry [4, 5].

In recent years, full-duplex relay techniques, which can transmit and receive simultaneously in the same frequency band, have been exploited to improve physical layer security performance of wireless networks. The authors in [6] proposed a newly full-duplex jamming relay scheme, which has better secrecy performance than the half duplex scheme. For full-duplex two-way relay networks, [7] exploited artificial noise to strengthen the sum secrecy rate. In [8], a power allocation strategy between data and jamming was developed to effectively improve the tradeoff between security and reliability, where both the relay and the destination operated in full-duplex mode. Subsequently, full-duplex
The main contributions of this paper are summarized as follows. COP is used to characterize the reliability performance. The security performance and the connection outage probability (SOP) is used to evaluate the performance of the untrusted full-duplex relay network, where Compared with [18–20], we consider the outage performance comprehensively 

(i) To gain further insights, we conduct an asymptotic analysis in the high signal-to-noise ratio (SNR) region for the SOP, COP, and EST. Based on the asymptotic analysis, we find that there exists a EST for both the relaying schemes, which provide an efficient means to evaluate the reliability and security performance comprehensively.

(ii) The results demonstrate the intuition that the self-interference caused by full-duplex transmission is harmful for the reliability performance, while it is beneficial to the security performance. In addition, the EST of the considered system increases as the self-interference level decreases, which implies that the self-interference deteriorates an overall performance in terms of the security-reliability tradeoff.

The remainder of this paper is organized as follows. Section 2 gives the system model and describes the key metric in evaluating the performance of physical layer security, including the SOP, COP, and EST. In Section 3, we present the closed form expressions of the SOP, COP, and EST for the VGR scheme and the FGR scheme and analyze the corresponding asymptotic behavior in the high SNR region. Numerical results and conclusions are, respectively, provided in Sections 4 and 5.

2. System Model

We consider an untrusted full-duplex relay network shown in Figure 1, where a source S communicates with a destination D via an untrusted relay R. The source has Ns antennas and operates in the half-duplex mode, while the destination and the relay are equipped with dual antennas and operate in the full-duplex mode. It means that the destination and the relay can receive and send data concurrently. The system considered in this work is applicable to numerous practical full-duplex relay scenarios, for instance, the wireless sensor networks and IoT. Moreover, the direct link between the source and the destination is unavailable, due to severe shadow fading or significant obstacle [21]. Thus, source-destination communication can be performed only through the relay. In addition, all channels are modeled as quasistatic block fading channels, following the Rayleigh distribution. As in [13, 15], we assume that the channel between the relay and the destination is reciprocal.

Because the relay is untrusted, the source wishes to keep the information secret from the relay while simultaneously making use of it to forward the information. To maintain the confidentiality of the source information, the destination sends a jamming signal to the relay when the source transmits information to the relay. Thus, the received signal at the relay can be expressed as

\[ y_r[i] = h_{sr}w_s[i] + h_{sr}x_s[i] + h_{dr}x_d[i] + n_r[i], \]  

(i) We first present exact expressions for the SOP and COP of the fixed gain relaying (FGR) scheme and the variable gain relaying (VGR) scheme and then derive closed-form expressions for the EST of both the relaying schemes, which provide an efficient means to evaluate the reliability and security performance comprehensively.

(ii) To gain further insights, we conduct an asymptotic analysis in the high signal-to-noise ratio (SNR) region for the SOP, COP, and EST. Based on the asymptotic analysis, we find that there exists a EST for both the relaying schemes, which provide an efficient means to evaluate the reliability and security performance comprehensively.

(iii) The results demonstrate the intuition that the self-interference caused by full-duplex transmission is harmful for the reliability performance, while it is beneficial to the security performance. In addition, the EST of the considered system increases as the self-interference level decreases, which implies that the self-interference deteriorates an overall performance in terms of the security-reliability tradeoff.
where $h_{sr}$ is the $1 \times N_r$ channel vector between the source and the relay and its entries follow independent and identically distributed (i.i.d.) complex Gaussian distribution with zero mean and variance $\gamma_{SR}: w_{sr} = h_{sr}^\dagger / \| h_{sr} \|$ is the transmit precoding vector at the source. $h_{dr}$ is the channel coefficient between the relay and the destination with parameter $\gamma_{RD}$. $h_{dr}$ is the loopback interference channel coefficient between transmitting and receiving antennas at the relay. $x_i[i]$ is the confidential signal transferred from the source at time slot $i$ and satisfies $E\{|x_i[i]|^2\} = \beta P$, where $E\{\cdot\}$ represents the expectation operation. $x_i[i]$ is the jamming signal transferred from the destination at time slot $i$ and satisfies $E\{|x_i[i]|^2\} = (1-\beta)P$. Here, $\beta \in (0,1)$ is the power allocation factor between the source and the destination. $x_i[i]$ is the loopback interference signal transferred from the relay at time slot $i$ and satisfies $E\{|x_i[i]|^2\} = P$. $n_i[i]$ is the additive white Gaussian noise (AWGN) at the relay with zero mean and variance $N_0$. Since $x_i[i]$ is known to the relay, it can apply multiple stage interference cancellation methods to alleviate the loopback interference. Thus, the received signal at the relay after compensation can be expressed as

$$y_i[i] = h_{sr}w_{sr}x_i[i] + h_{dr}x_d[i] + I_i[i] + n_i[i],$$

where $I_i[i]$ can be modeled as a Gaussian random variable with mean zero and variance $\frac{P}{\beta} \gamma_{SR}$ [18, 22]. $I_i$ corresponds to the self-interference cancellation capability at the relay.

Then, the relay amplifies the signal $y_i[i]$ with factor $G$ and forwards it to the destination. The two most common factors employed at the relay are so-called fixed gain factor and variable gain factor. In the FGR scheme, the factor is constant based on the statistical CSI, resulting in an output signal with variable power. In the VGR scheme, the factor is variable dependent on the instantaneous CSI, resulting in an output signal with fixed power. The factors of both FGR and VGR schemes can be given by

$$G = \begin{cases} \frac{P}{\beta P \| h_{sr} \|^2 + (1-\beta)P \| h_{dr} \|^2 + \frac{P}{\kappa} + N_0} & \text{with FGR}, \\ \frac{P}{\beta P \| h_{sr} \|^2 + (1-\beta)P \| h_{dr} \|^2 + \frac{P}{\kappa} + N_0} & \text{with VGR}. \end{cases}$$

Hence, the received signal at the destination is given by

$$y_d[i] = h_{rd}x_r[i] + h_{dd}x_d[i] + n_d[i] = h_{rd}Gy_i[i] + h_{dd}x_d[i] + n_d[i],$$

where $h_{dd}$ is the loopback interference channel coefficient between transmitting and receiving antennas at the destination and $n_d[i]$ is the AWGN at the destination with zero mean and variance $N_0$. Analogously, the received signal at the destination after self-interference cancellation can be written as

$$\tilde{y}_d[i] = h_{rd}Gh_{sr}w_{sr}x_i[i] + h_{rd}Gx_d[i] + h_{rd}Gn_i[i] + I_d[i] + n_d[i],$$

where $I_d[i]$ can be modeled as a Gaussian random variable with mean zero and variance $\frac{P}{\kappa}(1-\beta)P$. $I_d$ corresponds to the self-interference cancellation capability at the destination.

According to (2), the achievable eavesdropping rate with the FGR scheme and the VGR scheme can be obtained as

$$C_{RGR} = C_{RGR} = \log_2 \left( 1 + \frac{\beta \lambda \| h_{sr} \|^2}{(1-\beta)\lambda \| h_{rd} \|^2 + \frac{P}{\kappa} + 1} \right),$$

$$C_{DGR} = \log_2 \left( 1 + \frac{\beta \lambda^2 \| h_{sr} \|^2 \| h_{dr} \|^2}{(\lambda + \frac{P}{\kappa})^2 \| h_{rd} \|^2 + C} \right),$$

where $\lambda = P/N_0$ denotes the transmit SNR. According to (3) and (5), the achievable data rate with the FGR scheme and the VGR scheme can be, respectively, obtained as

$$C_{DGR} = \log_2 \left( 1 + \frac{\beta \lambda^2 \| h_{sr} \|^2 \| h_{dr} \|^2}{(\lambda + \frac{P}{\kappa})^2 \| h_{rd} \|^2 + C} \right),$$

$$C_{DGR} = \log_2 \left( 1 + \frac{\beta \lambda^2 \| h_{sr} \|^2 \| h_{dr} \|^2}{C_1 \| h_{rd} \|^2 + C_2 \| h_{rd} \|^2 + C_3} \right),$$

where

$$C_1 = (1 + \frac{P}{\kappa} + \beta \lambda N_0 \gamma_{SR} + (1 - \beta) \lambda \gamma_{RD})(1 + \frac{P}{\kappa} + \lambda(1 - \beta)), \quad C_2 = \lambda + \frac{P}{\kappa} + \lambda(1 - \beta)(1 + \frac{P}{\kappa} + \lambda(1 - \beta)),$$

As discussed in [23], when the achievable eavesdropping rate is larger than the positive rate difference between the codeword transmission rate $R_o$ and the confidential information rate $R_s$, there will be a secrecy outage event. When the achievable data rate is less than $R_o$, there will be a connection outage event. Thus, we can formulate the SOP and COP of our system as

$$P_{so} = \Pr(C_{GR} > R_o - R_s),$$

$$P_{co} = \Pr(C_{DGR} < R_s).$$

The SOP and COP give practical insights into security and reliability performance of the transmission system, respectively. To establish the direct relationship between security and reliability, we adopt effective secrecy throughput (EST)
to measure the overall efficiency of our system, which is given by

$$\zeta = R_y \cdot Pr(C_R < R_0 - R_y, C_D > R_0).$$

(11)

### 3. Secrecy Performance Analysis

In this section, we endeavor to analyze both the reliability and security performance comprehensively for the untrusted full-duplex relay network. Specifically, we first derive closed form expressions of the SOP, COP, and EST for the FGR scheme and the VGR scheme. Then, the asymptotic analysis of the SOP, COP, and EST is provided to reveal additional insights on the secrecy performance.

3.1. Fixed Gain Relaying

3.1.1. Secrecy Outage Probability. Combining (6) and (9), the SOP of the untrusted full-duplex relay network with the FGR scheme can be given by

$$p_{sop}^{FGR} = Pr(\beta\lambda \parallel h_{tr} \parallel^2 > t_1) = \Pr(\parallel h_{tr} \parallel^2 > \frac{(1 - \beta)^2 t_1^2 \lambda + t_1}{\beta\lambda}),$$

(12)

where $t_1 = 2^{k_1 - k_2} - 1$. Noting that $X = \parallel h_{tr} \parallel^2$ is a central chi-square distribution random variable with $2N_s$ degrees of freedom, its cumulative distribution function (CDF) is given by

$$F_X(x) = 1 - e^{-x/\gamma_{ya}} \sum_{m=0}^{N_s-1} \frac{x^m}{m! \gamma_{ya}^m}.$$

(13)

On the other hand, $Y = \parallel h_{rd} \parallel^2$ is an exponential variable with probability density function (PDF) given by

$$f_Y(y) = \frac{1}{\gamma_{rd}} e^{-y/\gamma_{rd}}.$$  

(14)

Based on (13) and (14), we can rewrite (12) as

$$p_{sop}^{FGR} = \int_0^{\infty} \left(1 - F_X \left(\frac{(1 - \beta) t_1 y + \frac{t_1^2 t_1 \lambda + t_1}{\beta\lambda} \right) \right) f_Y(y) dy$$

$$= \sum_{m=0}^{N_s-1} \frac{e^{-t_1 \beta t_1 \lambda + t_1/\lambda_{ya}}}{m! \gamma_{rd}^m \beta^{m+1} \lambda^{m+1}} \int_0^{\infty} e^{-((1 - \beta) t_1 y_1/\lambda_{ya} + (1/\gamma_{rd})) y}$$

$$\times (t_1 + t_1^2 \lambda + (1 - \beta) t_1 \lambda y)^m dy.$$

(15)

Then, using $(t_1 + t_1^2 \lambda + (1 - \beta) t_1 \lambda y)^m = \sum_{n=0}^{m} \binom{m}{n} t_1^n t_1 \lambda y^n$, we can calculate $p_{sop}^{FGR}$ as

$$p_{sop}^{FGR} = \sum_{m=0}^{N_s-1} \binom{m}{n} (t_1^n t_1 \lambda + t_1)^{m-n} (1 - \beta)^n t_1 \lambda^n y^n,

(16)

From (16), we find that the SOP increases as the power allocation factor $\beta$ increases from 0 to 1. This is because that increasing $\beta$ results in decreasing transmission power of the jamming signal. Moreover, the SOP decreases as $l_1$ increases, which means that the self-interference caused by full-duplex transmission is harmful to the security performance.

3.1.2. Connection Outage Probability. Combining (7) and (10), the COP of the untrusted full-duplex relay network with the FGR scheme can be given by

$$p_{cop}^{FGR} = \Pr\left(\frac{\beta\lambda \parallel h_{tr} \parallel^2}{y_{rd}} < t_2\right) = \Pr\left(\parallel h_{tr} \parallel^2 < \frac{t_2 (1 + \lambda t_1^2)}{\beta\lambda} + \frac{t_2 C}{\beta^2 \lambda^2} \right).$$

(17)

where $t_2 = 2^{k_2} - 1$. Based on (13) and (14), we can rewrite (17) as

$$p_{cop}^{FGR} = \int_0^{\infty} F_Y \left(\frac{t_2 (1 + \lambda t_1^2)}{\beta\lambda} + \frac{t_2 C}{\beta^2 \lambda^2} \right) f_Y(y) dy$$

$$= 1 - \sum_{m=0}^{N_s-1} \frac{e^{-t_2 \lambda t_1^2 \lambda + t_2 /\lambda_{ya}}}{m! \gamma_{rd}^m \beta^{m+1} \lambda^{m+1}} \int_0^{\infty} \left(\frac{t_2 + t_2 \lambda t_1^2}{\beta\lambda^2 y} \right)^m$$

$$\times e^{-\left(t_2 C /\beta^2 \lambda_{ya}^2\right)} dy.$$  

(18)

Then, with the help of the binomial theorem and ([24], 3.471.9), the exact COP of the untrusted full-duplex relay network with the FGR scheme can be derived as

$$p_{cop}^{FGR} = 1 - \sum_{m=0}^{N_s-1} \sum_{n=0}^{m} \frac{m! t_2 C^m (1 + \lambda t_1^2)^{m-n} \lambda^{m-n} \beta^{m-n} \gamma_{rd}^m}{m! \beta^{m-n} \lambda^{m-n} \gamma_{rd}^m \gamma_{ya}^n} e^{-t_2 \lambda t_1^2 \lambda + t_2 /\lambda_{ya}}$$

$$\times \left(\frac{t_2 C \gamma_{ya}}{\beta^2 \lambda_{ya}^2}\right)^{1-n/2} K_{1-n} \left(\frac{4t_2 C}{\beta^2 \lambda_{ya}^2 \gamma_{rd}}\right).$$

(19)

where $K_{1-n}(\cdot)$ is the Bessel functions of imaginary argument. From (19), we find that the COP decreases as the power allocation factor $\beta$ increases from 0 to 1. The main reason is that when $\beta$ increases, the achievable data rate is larger which makes reliability better. In addition, the COP increases as $l_1$ or $l_2$ increases, which means that the self-interference caused by full-duplex transmission is harmful for the reliability performance.
3.1.3. Effective Secrecy Throughput. Combining (6), (7), and (11), the EST of the untrusted full-duplex relay network with the FGR scheme can be given by

$$\zeta_{GR} = R_{sr} \Pr \left[ |h_{sr}|^2 < \left( \frac{1 - \beta}{\beta} |t_2 h_{sr1}|^2 + \frac{t_2 t_1 + t_2}{\beta^2} |h_s|^2 \right) \frac{t_1 (1 + \lambda^2)}{\beta^2} + \frac{t_2 C}{\beta^2 |h_{sr}|^2} \right].$$

(20)

Since $((1 - \beta) t_1 h_{sr1}^2) / (\beta + t_2 t_1 + t_2 / (\beta^2))$ and $(t_2 (1 + \lambda t_2^2) / (\beta^2))$ have only one point of intersection when $|h_{sr1}|^2 > 0$, and the intersection is $u_1$. Thus, expression (20) can be expressed as

$$\zeta_{GR} = R_{sr} \int_{u_1}^{\alpha} F_X \left( \frac{(1 - \beta) t_1 y_{1} + t_2 t_1 + t_2}{\beta^2} \right) f_c(y) dy \cdot F_X \left( t_2 (1 + \lambda^2) y_{1} + t_2 C / \beta^2 y_{1} \right) f_c(y) dy \cdot \sum_{m=0}^{N-1} \sum_{n=0}^{m} \left( \frac{R_{sr} t_1 C (1 + \lambda^2) y_{1}}{m t_2 C / \beta^2 y_{1}} \right)^{m-n} \prod_{k=0}^{m-n} \frac{1}{\lambda} \int_{u_1}^{\alpha} e^{-((1 - \beta) \frac{1}{\beta^2} + \lambda^2) y_{1}} y_{1} dy. \quad \text{(21)}$$

where $u_1 = (-b_1 + \sqrt{b_1^2 - 4a_1c_1})/2a_1$, $a_1 = t_1 (1 - \beta)$, $b_1 = -t_2 C$, and $c_1 = -t_2 C$. Then, using [24, 1.211.1], [24, 3.51.2], and [24, 3.81.3], the exact EST of the untrusted full-duplex relay network with the FGR scheme can be derived as

$$\zeta_{GR} = \sum_{m=0}^{N-1} \sum_{n=0}^{m} \left( \frac{R_{sr} t_1 C (1 + \lambda^2) y_{1}}{m t_2 C / \beta^2 y_{1}} \right)^{m-n} \prod_{k=0}^{m-n} \frac{1}{\lambda} \int_{u_1}^{\alpha} e^{-((1 - \beta) \frac{1}{\beta^2} + \lambda^2) y_{1}} y_{1} dy.$$

(22)

From (22), we find that the EST of the considered system is small when the confidential information rate $R_s$ is small. At the other extreme, when the confidential information rate $R_s$ is too large, the secrecy performance of the considered system is poor which also results in small EST. Hence, there exists an optimal $R_s$ to maximize the EST of the considered system. Furthermore, the EST increases as the self-interference level decreases, which means that the self-interference deteriorates an overall performance in terms of the security-reliability tradeoff.

3.1.4. Asymptotic Behavior. To extract additional insights on the FGR scheme, we now investigate the high SNR asymptotic behavior of the SOP, COP, and EST of the considered system. According to (16), we have

$$\lim_{\lambda \to \infty} P_{GR}^{\infty} = \sum_{m=0}^{N-1} \sum_{n=0}^{m} \left( \frac{t_1 t_2}{R_{sr} C (1 + \lambda^2)} \right)^{m-n} \prod_{k=0}^{m-n} \frac{1}{\lambda} \int_{u_1}^{\alpha} e^{-((1 - \beta) \frac{1}{\beta^2} + \lambda^2) y_{1}} y_{1} dy.$$

(23)

From (19), we have

$$\lim_{\lambda \to \infty} P_{co}^{gr} = 1 - \sum_{m=0}^{N-1} \sum_{n=0}^{m} \left( \frac{m}{n} \right) \frac{2 t_1 t_2 C^{m-n-2} e^{-\frac{t_1 t_2}{R_{sr} C (1 + \lambda^2)}}}{m t_2 Y_{RD} Y_{SR}^{m-n-1}} \Gamma \left( 1 + \frac{4 t_2 C}{\beta Y_{SR} Y_{RD}} \right).$$

(24)

where $C = t_1 (1 - \beta) + \beta N_1 Y_{SR} + \beta Y_{RD} (1 - \beta)$. According to (22), we have

$$\lim_{\lambda \to \infty} \zeta_{GR} = \sum_{m=0}^{N-1} \sum_{n=0}^{m} \left( \frac{m}{n} \right) \frac{(-1)^k R_{sr} t_1 C (1 + \lambda^2) y_{1}^{m-n-k}}{m t_2 C / \beta^2 y_{1}^{m-n-k}} \prod_{k=0}^{m-n-k} \frac{1}{\lambda} \int_{u_1}^{\alpha} e^{-((1 - \beta) \frac{1}{\beta^2} + \lambda^2) y_{1}} y_{1} dy.$$

(25)

where $u_2 = (-t_2 t_1 + t_2 + \sqrt{t_2 (t_1 - t_2)^2 + 4 t_1 t_2 C (1 - \beta)/2t_1 \beta} - 1)$. It is interesting to note that when transmit power is sufficiently large, the security and reliability of the untrusted full-duplex relay network are still depend on the power allocation factor. Thus, the power allocation factor enables a tradeoff between reliability and security for the untrusted full-duplex relay network. From the numerical results, we find that there exists an optimal power allocation factor maximizing the EST.

3.2. Variable Gain Relaying

3.2.1. Secrecy Outage Probability. The gain factor employed at the relay determines the quality of signal reception at the destination and has no influence on the eavesdropping ability at the relay. Therefore, the SOP of the VGR scheme is the same as the FGR scheme and it is omitted here.

3.2.2. Connection Outage Probability. Combining (8) and (10), the COP of the untrusted full-duplex relay network
with the VGR scheme can be derived as

\[ p_{\text{VGR}}^{c_{o}} = \Pr \left( \frac{\beta \lambda^2 \| h_r \|^2 \| h_{rd} \|^2}{C_1 \| h_r \|^2 + C_2 \| h_{rd} \|^2 + C_3} < t_2 \right) = \Pr \left( \frac{(\beta \lambda^3 \| h_{rd} \|^2 - t_2 C_1) \| h_r \|^2}{t_2 C_2 \| h_{rd} \|^2 + t_2 C_1} \right) \]

The VGR scheme can be given by

\[ p_{\text{VGR}}^{c_{o}} = \int_{0}^{C_1} f_Y(y)dy + \int_{C_1}^{\infty} f_X \left( \frac{t_2 C_2 y + t_2 C_3}{\beta \lambda^2 y - t_2 C_1} \right) f_Y(y)dy \]

\[ = 1 - \sum_{m=0}^{N-1} \sum_{n=0}^{m} \left( \frac{m}{n} \right) 2^{C_1} e^{-(t_2 C_2 \gamma \gamma_{\text{yr}}} / (C_1 \gamma_{\text{yr}})} m \frac{(t_2 C_2)}{\beta \lambda^2} m \frac{1 + \frac{C_2}{\gamma - C_5}}{C_5} \times e^{-\left(\frac{t_2 C_2 \gamma \gamma_{\text{yr}}} {\beta \lambda^2 (\gamma - C_5)}\right) (\gamma_{\text{yr}})}dy, \]

where \( C_1 = (C_3 + C_2) + (t_2 C_1 / \beta \lambda^2) \), and \( C_5 = t_2 C_1 / \beta \lambda^2 \). Then, let \( \gamma = \gamma - C_5 \), and use [24, 1.211.1] and [24, 3.471.9], the exact COP of the untrusted full-duplex relay network with the VGR scheme can be derived as

\[ p_{\text{VGR}}^{c_{o}} = 1 - \sum_{n=0}^{N-1} \sum_{m=0}^{\infty} \frac{2^{C_1} e^{-(t_2 C_2 \gamma \gamma_{\text{yr}}}/(C_1 \gamma_{\text{yr}})} m \frac{(t_2 C_2)}{\beta \lambda^2} m \frac{1 + \frac{C_2}{\gamma - C_5}}{C_5} \times e^{-\left(\frac{t_2 C_2 \gamma \gamma_{\text{yr}}} {\beta \lambda^2 (\gamma - C_5)}\right) (\gamma_{\text{yr}})}dy, \]

When \( N_{s} \to \infty \), we have \( \| h_r \|^2 \approx \alpha \), \( N_{r} Y_{SR} \), where \( \alpha \) follows the law of large numbers. Thus, from (26), we clarify that increasing the number of antennas at the source unboundedly is not helpful because the channel between the relay and the destination will finally become the bottleneck and dominate the achievable data rate.

3.2.3. Effective Secrecy Throughput. Combining (6), (8), and (11), the EST of the untrusted full-duplex relay network with the VGR scheme can be given by

\[ \zeta_{VGR} = R_{u_4} \left( 1 - \frac{(\beta \lambda^2 \| h_{rd} \|^2)}{\beta} \frac{t_1 t_2}{\beta} + \frac{t_1 t_2}{\beta} \right) \]

\[ + \frac{t_1 t_2}{\beta} \left( \frac{t_1 t_2}{\beta \lambda^3} \| h_{rd} \|^2 + t_1 t_2 \right) \frac{t_2 C_1 \| h_{rd} \|^2}{\beta \lambda^2} \frac{t_2 C_1 \| h_{rd} \|^2 - t_2 C_1}{\beta \lambda^2} \]

where \( N_{s} \to \infty \), we have \( \| h_r \|^2 \approx \alpha \), \( N_{r} Y_{SR} \), where \( \alpha \) follows the law of large numbers. Thus, from (26), we clarify that increasing the number of antennas at the source unboundedly is not helpful because the channel between the relay and the destination will finally become the bottleneck and dominate the achievable data rate.

The derived exact results in (31) provide an efficient way to holistically examine the security and reliability performance with arbitrary system parameters, i.e., the number of antennas at the source and the self-interference cancellation capability at the relay and destination. Additionally, it is worth noting that the EST of the considered system will tend toward zero when \( N_{s} \to \infty \). An intuitive explanation to this phenomenon is that, more antennas at the source would bring us better reliability performance, but at the same time, the grade of the security is severely degraded. Thus, the designers have to carefully take into account the number of antennas at the source.
Figure 2: The outage probability of the FGR scheme and the VGR scheme versus the transmit SNR.

Figure 3: The outage probability of the FGR scheme and the VGR scheme versus the self-interference cancellation capability.
\[ \gamma_{RD} = 10 \text{ dB} \]
\[ \gamma_{RD} = 0 \text{ dB} \]

**Figure 4:** The EST of the FGR scheme and the VGR scheme versus the transmit SNR.

**Figure 5:** The EST of the FGR scheme and the VGR scheme versus the power allocation factor.
Figure 6: The EST of the FGR scheme and the VGR scheme versus the number of antennas at the source.

Figure 7: The EST of the FGR scheme and the VGR scheme versus the self-interference cancellation capability.
3.2.4. Asymptotic Behavior. To get more insight, we further study the asymptotic behavior of the COP and EST for the VGR scheme under high SNR case. According to (28), we have

\[
\lim_{\lambda \to \infty} \mu_{VGR}^{\lambda} = 1 - \sum_{m=0}^{N_s-1} \sum_{n=0}^{\infty} \left( \frac{m}{n} \right) \frac{2^{t_2(C_n^m C_n^m) e^{-(t_2 C_n^m)/(2 \gamma_{SR})} - (C_m^m)/(2 \gamma_{RD})} \times \left( \frac{t_2 C_n^m C_n^m}{\beta_{SR}^m} \right)^{(1-n)/2} K_{1-n} \left( \sqrt{4t_2 C_n^m \gamma_{SR}^m} \right)}{m! \beta_{SR}^m \gamma_{RD}^m} \right)
\]

(32)

where \( C_0 = \beta_2^2 (1 - \beta), \ C_7 = t_2^2 + t_2^2 (1 - \beta)^2, \ C_8 = t_2^3 t_2^2 (1 - \beta), \ C_9 = (C_0^2 C_7^2) + (t_2 C_6^2)/(2 \gamma_{SR}), \) and \( C_{10} = t_2 C_6^2/(2 \gamma_{SR}). \) From (31), we have

\[
\lim_{\lambda \to \infty} \omega_{VGR}^{\lambda} = \sum_{m=0}^{N_s-1} \sum_{n=0}^{\infty} \left( \frac{m}{n} \right) \frac{(-1)^{m+1} \omega_{C_m^m}^{C_m^m} e^{-(t_2 C_n^m)/(2 \gamma_{SR})} - (C_m^m)/(2 \gamma_{RD})} {m! \beta_{SR}^m \gamma_{RD}^m} \times \left( \frac{t_2 C_n^m}{\beta_{SR}^m} \right)^{m} \Gamma(1 - n - k, \frac{u_6 - C_{10}}{\gamma_{RD}}) \right)
\]

\[
\times \sum_{n=0}^{\infty} \left( \frac{n}{m} \right) \frac{R_{t_2 C_n^m}^{m} (1 - \beta)^{n} u_6}{m! \beta_{SR}^m \gamma_{RD}^m} \times \frac{e^{t_2^2 t_2^2 (1 - \beta)^2}}{\beta_{SR}^m} \left( \frac{1}{\beta_{RD}^m} \right)^{m} \left( \frac{1}{\beta_{RD}^m} \right)^{n-1} \Gamma(n + 1, (1 - \beta)^{t_2 C_6^2} + \frac{1}{\gamma_{RD}}) \right)
\]

(33)

where \( u_6 = \max \{u_5, t_2 C_6^2/(2 \gamma_{SR})\}, \ u_5 = (-b_3 + \sqrt{(b_3^2 - 4 a_5 c_3)})/2 a_3, \ a_3 = t_2 (1 - \beta), \ b_1 = t_2^2 (1 - \beta)^2 - \beta_2 C_7 t_2 - t_2 t_2 C_6 (1 - \beta), \) and \( c_5 = -\beta_2 C_9 t_2 - t_2 t_2 C_9^2 t_2^2. \)

From the asymptotic behaviour of the SOP, COP, and EST, we find that the continued boosting of the transmit power will not always improve the security and reliability performance of the considered system. This is due to the fact that the self-interference caused by full-duplex transmission becomes a bottleneck of improving the security and reliability performance at the high SNR region.

4. Numerical Results

In this section, we present simulation and numerical results to illustrate tendencies of the performance of the untrusted full-duplex relay network. Unless otherwise stated, we set the codeword transmission rate, \( R_0 = 2 \text{bits/sec/Hz}, \) and the confidential information rate, \( R_c = 1 \text{bits/sec/Hz}. \) Also, we set \( l_f = l_d = l_{ave}. \) It is evident from Figures 2-7 that the derived closed form expressions of SOP, COP, and EST agree well with their Monte Carlo simulation points, which indicates the accuracy of our theoretical analysis stated above.

Figure 2 shows the SOP and COP versus the transmit SNR of the FGR scheme as well as the VGR scheme, where \( N_s = 2, \ \beta = 0.5, \ l_{ave} = -15 \text{dB}, \ \gamma_{SR} = 0 \text{dB}, \) and \( \gamma_{RD} = 5 \text{dB}. \) We first observe that the SOP of the FGR and VGR schemes increases as the transmit SNR increases, whereas the COP of the FGR and VGR schemes decrease as the transmit SNR increases. This is due to the fact that an increasing transmit SNR will lead to a higher achievable eavesdropping rate and achievable data rate. Second, we observe that the SOP and COP of the FGR and VGR schemes converge to a constant when the transmit SNR is sufficiently large. Thus, we can conclude that the transmit SNR is not the larger the better. Moreover, we observe that the COP of the VGR scheme outperforms the FGR scheme at the high SNR region.

Figure 3 shows the SOP and COP versus the self-interference cancellation capability of the FGR scheme as well as the VGR scheme, where \( N_s = 2, \ \beta = 0.5, \lambda = 30, \ \gamma_{SR} = 0 \text{dB}, \) and \( \gamma_{RD} = 0 \text{dB}. \) We observe that the SOP and COP of the FGR and VGR schemes decreases as the self-interference cancellation capability decreases, whereas the COP of the FGR and VGR schemes increase as the self-interference cancellation capability decreases. The reason is that as the self-interference cancellation capability decreases, the loopback interference at the destination and the relay will be stronger. Thus, the self-interference cancellation capability enables a tradeoff between security and reliability of the untrusted full-duplex relay network.

Figure 4 depicts the EST as a function of the transmit SNR, where \( N_s = 2, \ \beta = 0.5, l_{ave} = -10 \text{dB}, \) and \( \gamma_{SR} = 0 \text{dB}. \) We first observe that the EST of the FGR scheme and the VGR scheme converge to a constant when the transmit SNR tends to infinity. This phenomenon is due to the fact that the EST is constrained by the self-interference caused by full-duplex transmission in the high SNR regime. Second, we observe that the EST of the VGR scheme is better than the FGR scheme in the high SNR region. Moreover, we observe that for a given transmit SNR, the EST of both the FGR scheme and the VGR scheme with \( \gamma_{RD} = 10 \text{dB} \) outperform the EST with \( \gamma_{RD} = 0 \text{dB}. \) This is because that the improved quality of the second hop channel is beneficial for secure transmission.

Figure 5 examines the impact of power allocation factor on the EST performance, where \( N_s = 2, \lambda = 20 \text{dB}, l_{ave} = -15 \text{dB}, \) and \( \gamma_{SR} = 0 \text{dB}. \) We observe that when the power allocation factor is either extremely small or large, the EST of the FGR scheme and the VGR scheme approach zero. This is because when the power allocation factor is small, it is hard to establish a reliable link from the source to the destination. On the other hand, when the power allocation factor is large, the power of the jamming signal at the destination is poor and secure transmission is impossible. Thus, there exists an optimal power allocation factor maximizing the EST. Moreover, the optimal power allocation factor gradually increases as \( \gamma_{RD} \) increases. It indicates that the destination does not need more power to transmit jamming when the channel between the relay and the destination is better.

Figure 6 illustrates the EST of the FGR scheme and the VGR scheme as a function of the number of antennas at the source, with \( \lambda = 20 \text{dB}, \beta = 0.5, l_{ave} = -15 \text{dB}, \) and \( \gamma_{SR} = 0 \text{dB}. \) We observe that the EST of the FGR scheme and the VGR
scheme first increase to a peak value and then decrease as a function of the number of antennas at the source. This phenomenon is due to the fact that increasing the number of antennas at the source leads to the enhancement of the reliability performance, but the degradation of the security performance. Second, we observe that the performance gain of the VGR scheme is much more pronounced for small $N_s$, and gradually diminishes when $N_s$ becomes large.

Figure 7 plots the EST of the FGR scheme and the VGR scheme as a function of the self-interference cancellation capability, with $N_s = 2$, $\beta = 0.5$, $\lambda = 20$, and $\gamma_{GR} = 0$ dB. It can be seen from the figure that the EST of the FGR and VGR schemes decrease as the self-interference cancellation capability decreases. From Figure 3, we know that the self-interference cancellation capability has a positive effect on the secure transmission but incurs a negative effect on the reliable transmission. Thus, we can conclude that the self-interference caused by full-duplex transmission does more harm than good for the untrusted full-duplex relay network. When the the level of self-interference is strong, the EST is close to zero, which suggests that both reliable and secure transmission cannot be achieved.

### 5. Conclusion

In this paper, we investigated the security-reliability tradeoff of an untrusted full-duplex relay network over the Rayleigh fading channels. Based on the availability of the CSI, we considered two types of relaying scheme, namely, the FGR scheme and the VGR scheme. The closed form expressions of the SOP, COP, and EST were, respectively, derived, which quantitatively reveal the relationship between the system performances and the number of antennas at the source, power allocation factor, and self-interference cancellation capability, as well as other various parameters. In addition, simple asymptotic results for the high SNR region, i.e., $\lambda \rightarrow \infty$, were also provided to offer valuable insights into practical design. Analytical and numerical results demonstrated that the self-interference caused by full-duplex transmission is harmful for the reliability performance, while it is beneficial to the security performance. Moreover, the EST of the considered system increases as the self-interference level decreases, which implies that the self-interference deteriorates an overall performance in terms of the security-reliability tradeoff.

### Data Availability

The simulation data used to support the findings of this study are included within the article.

### Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

### Acknowledgments

This work was supported in part by the Doctoral Research Start-up Funding of Nanyang Normal University under Grant 2022ZX017, in part by the Cultivating Fund Project for the National Natural Science Foundation of China of Nanyang Normal University under Grant 2022PY024, in part by the open research fund of Key Lab of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), Ministry of Education under Grant JZNY202107, in part by the Key Scientific Research Projects of Colleges and Universities in Henan Province of China under Grant 21A520033, and in part by the Key Scientific and Technological Research Projects in Henan Province under Grant 222102320369.

### References


