Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 2419430, 12 pages
https://doi.org/10.1155/2022/2419430

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 Li[5]

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

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

techniques were extended to secure multirelay networks [9] and nonorthogonal multiple access (NOMA) networks [10].

The works in [6–10] were focused on the security of full-duplex relay networks, where the eavesdroppers are external nodes in addition to legitimate nodes. However, even in the absence of external eavesdroppers, the security caused by legitimate nodes in the network may still be a concern [11–13]. For example, the relay may be untrusted, which means that they can possibly try to eavesdrop the source's confidential information. The untrusted relay is also a potential eavesdropper, even though it complies with the communication protocols to assist the source forwarding information to the destination [14–16]. In practice, untrusted relay scenario may occur in Internet of Things (IoT), government intelligence networks, and device-to-device (D2D) communications, where not all users do have the same security clearance.

Recently, a few works about untrusted full-duplex relay networks have been considered in the context of physical layer security. Based on the source jamming scheme, [17] derived the secrecy outage probability for untrusted full-duplex relay networks. The impact of outdated channel state information (CSI) on the ergodic secrecy rate of untrusted full-duplex relay networks was investigated in [18]. The authors of [19] proposed an artificial noise-aided secure transmission scheme to confuse the untrusted full-duplex relay and external eavesdroppers. In [20], an optimal beamforming scheme was design to maximize the secrecy sum rate for full-duplex multiple-input multiple-output two-way untrusted relay networks. The aforementioned contributions are mainly concerned on enhancing the secrecy rate of untrusted full-duplex relay networks without paying much attention to the communication reliability. In particular, the impact of self-interference caused by full-duplex transmission on the security-reliability tradeoff is indeed worthy of our attention.

Motivated by the above considerations, we explore the physical layer security of untrusted full-duplex relay networks, where a source operates in half duplex mode and an untrusted relay and a destination operate in a full-duplex mode. In addition, the source equipped with multiple antennas uses a maximal ratio transmission (MRT) scheme to increase reliability. Depending on the availability of the CSI, the relay amplifies and forwards the source's signal with a fixed-gain or variable-gain factor. Different from the source-based jamming scheme in [17], we employ destination-assisted jamming for secrecy improvement. Compared with [18–20], we consider the outage performance of the untrusted full-duplex relay network, where the secrecy outage probability (SOP) is used to evaluate the security performance and the connection outage probability (COP) is used to characterize the reliability performance. The main contributions of this paper are summarized as follows:

(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 floor for both the relaying schemes in the high SNR region and the floor of the VGR scheme is higher than that of the FGR scheme

(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

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 N_s 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

$$y_r[i] = h_{sr} w_{sr} x_s[i] + h_{dr} x_d[i] + h_{rr} x_r[i] + n_r[i], \quad (1)$$

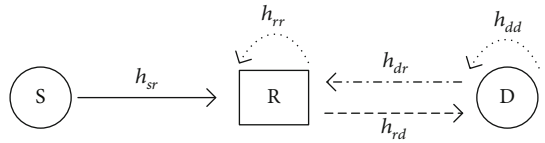

Figure 1: System model, where S, R, and D denote the source, untrusted relay, and destination, respectively.

where h_{sr} is the $1 \times N_s$ 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 $\bar{\gamma}_{SR}$. $w_{sr} = h_{sr}^{\dagger}/\|h_{sr}\|$ is the transmit precoding vector at the source. h_{dr} is the channel coefficient between the relay and the destination with parameter $\bar{\gamma}_{RD}$. h_{rr} is the loopback interference channel coefficient between transmitting and receiving antennas at the relay. $x_s[i]$ is the confidential signal transferred from the source at time slot i and satisfies $E\{|x_s[i]|^2\} = \beta P$, where $E\{\cdot\}$ represents the expectation operation. $x_d[i]$ is the jamming signal transferred from the destination at time slot i and satisfies $E\{|x_d[i]|^2\} = (1-\beta)P$. Here, $\beta \in (0,1)$ is the power allocation factor between the source and the destination. $x_r[i]$ is the loopback interference signal transferred from the relay at time slot i and satisfies $E\{|x_r[i]|^2\} = P$. $n_r[i]$ is the additive white Gaussian noises (AWGN) at the relay with zero mean and variance N_0. Since $x_r[i]$ 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

$$\widehat{y}_r[i] = h_{sr} w_{sr} x_s[i] + h_{dr} x_d[i] + I_r[i] + n_r[i], \tag{2}$$

where $I_r[i]$ can be modeled as a Gaussian random variable with mean zero and variance $l_r^2 P$ [18, 22]. l_r corresponds to the self-interference cancellation capability at the relay.

Then, the relay amplifies the signal $\widehat{y}_r[i]$ 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 depended on the instantaneous CSI, resulting in an output signal with fixed power. The factors of both FGR and VGR schemes can be given by

$$G = \begin{cases} E\left(\sqrt{\dfrac{P}{\beta P\|h_{sr}\|^2 + (1-\beta)P|h_{dr}|^2 + l_r^2 P + N_0}}\right), & \text{with FGR,} \\ \sqrt{\dfrac{P}{\beta P\|h_{sr}\|^2 + (1-\beta)P|h_{dr}|^2 + l_r^2 P + N_0}}, & \text{with VGR.} \end{cases} \tag{3}$$

Hence, the received signal at the destination is given by

$$y_d[i] = h_{rd} x_r[i] + h_{dd} x_d[i] + n_d[i] = h_{rd} G \widehat{y}_r[i] + h_{dd} x_d[i] + n_d[i], \tag{4}$$

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

$$\widehat{y}_d[i] = h_{rd} G h_{sr} w_{sr} x_s[i] + h_{rd} G I_r[i] + h_{rd} G n_r[i] + I_d[i] + n_d[i], \tag{5}$$

where $I_d[i]$ can be modeled as a Gaussian random variable with mean zero and variance $l_d^2(1-\beta)P$. l_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

$$C_R^{\mathrm{FGR}} = C_R^{\mathrm{VGR}} = \log_2\left(1 + \frac{\beta\lambda\|h_{sr}\|^2}{(1-\beta)\lambda|h_{rd}|^2 + l_r^2\lambda + 1}\right), \tag{6}$$

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

$$C_D^{\mathrm{FGR}} = \log_2\left(1 + \frac{\beta\lambda^2\|h_{sr}\|^2|h_{rd}|^2}{\left(\lambda + \lambda^2 l_r^2\right)|h_{rd}|^2 + C}\right), \tag{7}$$

$$C_D^{\mathrm{VGR}} = \log_2\left(1 + \frac{\beta\lambda^2\|h_{sr}\|^2|h_{rd}|^2}{C_1\|h_{sr}\|^2 + C_2|h_{rd}|^2 + C_3}\right), \tag{8}$$

where $C = (1 + l_r^2\lambda + \beta\lambda N_s\bar{\gamma}_{SR} + (1-\beta)\lambda\bar{\gamma}_{RD})(1 + l_d^2\lambda(1-\beta))$, $C_1 = \beta\lambda(1 + l_d^2\lambda(1-\beta))$, $C_2 = \lambda + \lambda^2 l_r^2 + \lambda(1-\beta)(1 + l_d^2\lambda(1-\beta))$, and $C_3 = (1 + l_r^2\lambda)(1 + l_d^2\lambda(1-\beta))$.

As discussed in [23], when the achievable eavesdropping rate is larger than the positive rate difference between the codeword transmission rate R_0 and the confidential information rate R_s, there will be a secrecy outage event. When the achievable data rate is less than R_0, there will be a connection outage event. Thus, we can formulate the SOP and COP of our system as

$$P_{so} = \Pr(C_R > R_0 - R_s), \tag{9}$$

$$P_{co} = \Pr(C_D < R_0). \tag{10}$$

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

$$\varsigma = R_s \cdot \Pr(C_R < R_0 - R_s, C_D > R_0). \tag{11}$$

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

$$\begin{aligned} P_{so}^{\mathrm{FGR}} &= \Pr\left(\frac{\beta\lambda\|h_{sr}\|^2}{(1-\beta)\lambda|h_{rd}|^2 + l_r^2\lambda + 1} > t_1\right) \\ &= \Pr\left(\|h_{sr}\|^2 > \frac{(1-\beta)t_1|h_{rd}|^2}{\beta} + \frac{l_r^2 t_1\lambda + t_1}{\beta\lambda}\right), \end{aligned} \tag{12}$$

where $t_1 = 2^{R_0 - R_s} - 1$. Noting that $X = \|h_{sr}\|^2$ is a central chi-square distribution random variable with $2N_s$ degrees of freedom, its cumulative distribution function (CDF) is given by

$$F_X(x) = 1 - e^{-x/\bar{\gamma}_{SR}} \sum_{m=0}^{N_s-1} \frac{x^m}{m!\bar{\gamma}_{SR}^m}. \tag{13}$$

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

$$f_Y(y) = \frac{1}{\bar{\gamma}_{RD}} e^{-y/\bar{\gamma}_{RD}}. \tag{14}$$

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

$$\begin{aligned} P_{so}^{\mathrm{FGR}} &= \int_0^\infty \left(1 - F_X\left(\frac{(1-\beta)t_1 y}{\beta} + \frac{l_r^2 t_1\lambda + t_1}{\beta\lambda}\right)\right) f_Y(y)dy \\ &= \sum_{m=0}^{N_s-1} \frac{e^{-t_1 l_r^2\lambda + t_1/\beta\lambda\bar{\gamma}_{SR}}}{m!\bar{\gamma}_{RD}\bar{\gamma}_{SR}^m\beta^m\lambda^m} \int_0^\infty e^{-(((1-\beta)t_1/\beta\bar{\gamma}_{SR}) + (1/\bar{\gamma}_{RD}))y} \\ &\quad \times \left(t_1 + t_1 l_r^2\lambda + (1-\beta)t_1\lambda y\right)^m dy. \end{aligned} \tag{15}$$

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

$$\begin{aligned} P_{so}^{\mathrm{FGR}} = &\sum_{m=0}^{N_s-1}\sum_{n=0}^{m} \frac{\left(t_1 l_r^2\lambda + t_1\right)^{m-n}(1-\beta)^n t_1^n\lambda^n}{(m-n)!\bar{\gamma}_{RD}\bar{\gamma}_{SR}^m\beta^m\lambda^m} \\ &\times \left(\frac{(1-\beta)t_1}{\beta\bar{\gamma}_{SR}} + \frac{1}{\bar{\gamma}_{RD}}\right)^{-n-1} e^{-t_1 l_r^2\lambda + t_1/\beta\lambda\bar{\gamma}_{SR}}. \end{aligned} \tag{16}$$

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

$$P_{co}^{\mathrm{FGR}} = \Pr\left(\frac{\beta\lambda^2\|h_{sr}\|^2|h_{rd}|^2}{(\lambda + \lambda^2 l_r^2)|h_{rd}|^2 + C} < t_2\right) = \Pr\left(\|h_{sr}\|^2 < \frac{t_2(1+\lambda l_r^2)}{\beta\lambda} + \frac{t_2 C}{\beta\lambda^2|h_{rd}|^2}\right), \tag{17}$$

where $t_2 = 2^{R_0} - 1$. Based on (13) and (14), we can rewrite (17) as

$$\begin{aligned} P_{co}^{\mathrm{FGR}} &= \int_0^\infty F_X\left(\frac{t_2(1+\lambda l_r^2)}{\beta\lambda} + \frac{t_2 C}{\beta\lambda^2 y}\right) f_Y(y)dy \\ &= 1 - \sum_{m=0}^{N_s-1} \frac{e^{-t_2\lambda l_r^2 + t_2/\beta\lambda\bar{\gamma}_{SR}}}{m!\bar{\gamma}_{RD}\bar{\gamma}_{SR}^m} \int_0^\infty \left(\frac{t_2 + t_2\lambda l_r^2}{\beta\lambda} + \frac{t_2 C}{\beta\lambda^2 y}\right)^m \\ &\quad \times e^{-\left(t_2 C/\beta\lambda^2\bar{\gamma}_{SR}y\right) - (y/\bar{\gamma}_{RD})} dy. \end{aligned} \tag{18}$$

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

$$\begin{aligned} P_{co}^{\mathrm{FGR}} = 1 - &\sum_{m=0}^{N_s-1}\sum_{n=0}^{m} \binom{m}{n} \frac{2t_2^m C^n\left(1+\lambda l_r^2\right)^{m-n}}{m!\beta^m\lambda^{m+n}\bar{\gamma}_{RD}\bar{\gamma}_{SR}^m} e^{-t_2\lambda l_r^2 + t_2/\beta\lambda\bar{\gamma}_{SR}} \\ &\times \left(\frac{t_2 C\bar{\gamma}_{RD}}{\beta\lambda^2\bar{\gamma}_{SR}}\right)^{1(-n)/2} K_{1-n}\left(\sqrt{\frac{4t_2 C}{\beta\lambda^2\bar{\gamma}_{SR}\bar{\gamma}_{RD}}}\right), \end{aligned} \tag{19}$$

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 β increases from 0 to 1. The main reason is that when β increases, the achievable data rate is larger which makes reliability better. In addition, the COP increases as l_r or l_d 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

$$\varsigma^{\mathrm{FGR}} = R_s \Pr\left(\|h_{sr}\|^2 < \frac{(1-\beta)t_1|h_{rd}|^2}{\beta} + \frac{l_r^2 t_1\lambda + t_1}{\beta\lambda}, \|h_{sr}\|^2 > \frac{t_2(1+\lambda l_r^2)}{\beta\lambda} + \frac{t_2 C}{\beta\lambda^2|h_{rd}|^2}\right). \tag{20}$$

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

$$\begin{aligned}
\varsigma^{\mathrm{FGR}} &= R_s \int_{u_1}^{\infty} F_X\left(\frac{(1-\beta)t_1 y}{\beta} + \frac{l_r^2 t_1\lambda + t_1}{\beta\lambda}\right) f_Y(y)dy \\
&\quad \cdot - R_s \int_{u_1}^{\infty} F_X\left(\frac{t_2(1+\lambda l_r^2)}{\beta\lambda} + \frac{t_2 C}{\beta\lambda^2 y}\right) f_Y(y)dy \\
&= \sum_{m=0}^{N_s-1}\sum_{n=0}^{m}\binom{m}{n} \frac{R_s t_2^m C^n (1+\lambda l_r^2)^{m-n} e^{-t_2+t_2\lambda l_r^2/\beta\lambda\bar{\gamma}_{SR}}}{m!\bar{\gamma}_{SR}^m \beta^m \bar{\gamma}_{RD}\lambda^{m+n}} \\
&\quad \times \int_{u_1}^{\infty} \frac{1}{y^n} e^{-\left(\left(t_2 C/\beta\lambda^2\bar{\gamma}_{SR}y\right) + \left(y/\bar{\gamma}_{RD}\right)\right)} dy - \sum_{m=0}^{N_s-1}\sum_{n=0}^{m}\binom{m}{n} \\
&\quad \times \frac{R_s t_1^m (1-\beta)^n e^{-t_1(1+\lambda l_r^2)/\beta\lambda\bar{\gamma}_{SR}}}{m!\bar{\gamma}_{SR}^m \beta^m \bar{\gamma}_{RD}} \left(\frac{1+\lambda l_r^2}{\lambda}\right)^{m-n} \\
&\quad \times \int_{u_1}^{\infty} y^n e^{-(((1-\beta)t_1/\beta\bar{\gamma}_{SR}) + (1/\bar{\gamma}_{RD}))y} dy,
\end{aligned} \tag{21}$$

where $u_1 = (-b_1 + \sqrt{b_1^2 - 4a_1c_1})/2a_1$, $a_1 = t_1\lambda^2(1-\beta)$, $c_1 = -t_2 C$, and $b_1 = \lambda(t_1 - t_2)(l_r^2\lambda + 1)$. Then, using [24, 1.211.1], [24, 3.351.2], and [24, 3.381.3], the exact EST of the untrusted full-duplex relay network with the FGR scheme can be derived as

$$\begin{aligned}
\varsigma^{\mathrm{FGR}} &= \sum_{m=0}^{N_s-1}\sum_{n=0}^{m}\sum_{k=0}^{\infty}\binom{m}{n} \frac{(-1)^k R_s C^{n+k}(1+\lambda l_r^2)^{m-n}}{m!k!\bar{\gamma}_{RD}^{n+k}\lambda^{m+n+2k}} \\
&\quad \times \left(\frac{t_2}{\beta\bar{\gamma}_{SR}}\right)^{m+k} e^{-t_2+t_2\lambda l_r^2/\beta\lambda\bar{\gamma}_{SR}} \Gamma\left(1-n-k, \frac{u_1}{\bar{\gamma}_{RD}}\right) \\
&\quad \cdot - \sum_{m=0}^{N_s-1}\sum_{n=0}^{m}\binom{m}{n} \frac{R_s t_1^m (1-\beta)^n e^{-t_1(1+\lambda l_r^2)/\beta\lambda\bar{\gamma}_{SR}}}{m!\bar{\gamma}_{SR}^m \beta^m \bar{\gamma}_{RD}} \\
&\quad \times \left(\frac{1+\lambda l_r^2}{\lambda}\right)^{m-n} \left(\frac{(1-\beta)t_1}{\beta\bar{\gamma}_{SR}} + \frac{1}{\bar{\gamma}_{RD}}\right)^{-n-1} \\
&\quad \times \Gamma\left(n+1, \frac{(1-\beta)t_1 u_1}{\beta\bar{\gamma}_{SR}} + \frac{u_1}{\bar{\gamma}_{RD}}\right).
\end{aligned} \tag{22}$$

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 (16), we have

$$\begin{aligned}
\lim_{\lambda\longrightarrow\infty} P_{so}^{\mathrm{FGR}} &= \sum_{m=0}^{N_s-1}\sum_{n=0}^{m} \frac{\left(t_1 l_r^2\right)^{m-n}(1-\beta)^n t_1^n e^{-t_1 l_r^2/\beta\bar{\gamma}_{SR}}}{(m-n)!\bar{\gamma}_{RD}\bar{\gamma}_{SR}^m \beta^m} \\
&\quad \times \left(\frac{t_1 - t_1\beta}{\beta\bar{\gamma}_{SR}} + \frac{1}{\bar{\gamma}_{RD}}\right)^{-n-1}.
\end{aligned} \tag{23}$$

From (19), we have

$$\begin{aligned}
\lim_{\lambda\longrightarrow\infty} P_{co}^{FGR} &= 1 - \sum_{m=0}^{N_s-1}\sum_{n=0}^{m}\binom{m}{n} \frac{2t_2^m \bar{C}^n l_r^{2m-2n} e^{-t_2 l_r^2/\beta\bar{\gamma}_{SR}}}{m!\bar{\gamma}_{RD}\bar{\gamma}_{SR}^m \beta^m} \\
&\quad \times \left(\frac{t_2\bar{C}\bar{\gamma}_{RD}}{\beta\bar{\gamma}_{SR}}\right)^{1-n/2} K_{1-n}\left(\sqrt{\frac{4t_2\bar{C}}{\beta\bar{\gamma}_{SR}\bar{\gamma}_{RD}}}\right),
\end{aligned} \tag{24}$$

where $\bar{C} = l_d^2(1-\beta)(l_r^2 + \beta N_s\bar{\gamma}_{SR} + \bar{\gamma}_{RD}(1-\beta))$. According to (22), we have

$$\begin{aligned}
\lim_{\lambda\longrightarrow\infty} \varsigma^{\mathrm{FGR}} &= \sum_{m=0}^{N_s-1}\sum_{n=0}^{m}\sum_{k=0}^{\infty}\binom{m}{n} \frac{(-1)^k R_s t_2^{m+k} l_r^{2m-2n} \bar{C}^{n+k}}{m!k!\bar{\gamma}_{SR}^{m+k}\bar{\gamma}_{RD}^{n+k}\beta^{m+k}} \\
&\quad \times e^{-t_2 l_r^2/\beta\bar{\gamma}_{SR}} \Gamma\left(1-n-k, \frac{u_2}{\bar{\gamma}_{RD}}\right) - \sum_{m=0}^{N_s-1}\sum_{n=0}^{m}\binom{m}{n} \\
&\quad \times \frac{R_s t_1^m (1-\beta)^n l_r^{2m-2n}}{m!\bar{\gamma}_{SR}^m \beta^m \bar{\gamma}_{RD}} e^{-t_1 l_r^2/\beta\bar{\gamma}_{SR}} \left(\frac{(1-\beta)t_1}{\beta\bar{\gamma}_{SR}} + \frac{1}{\bar{\gamma}_{RD}}\right)^{-n-1} \\
&\quad \Gamma\left(n+1, \frac{(1-\beta)t_1 u_2}{\beta\bar{\gamma}_{SR}} + \frac{u_2}{\bar{\gamma}_{RD}}\right),
\end{aligned} \tag{25}$$

where $u_2 = (-l_r^2(t_1 - t_2) + \sqrt{l_r^4(t_1 - t_2)^2 + 4t_1 t_2\bar{C}(1-\beta)})/2t_1(1-\beta)$. 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 given by

$$P_{co}^{\mathrm{VGR}} = \Pr\left(\frac{\beta\lambda^2\|h_{sr}\|^2|h_{rd}|^2}{C_1\|h_{sr}\|^2 + C_2|h_{rd}|^2 + C_3} < t_2\right) = \Pr\left(\left(\beta\lambda^2|h_{rd}|^2 - t_2C_1\right)\|h_{sr}\|^2 < t_2C_2|h_{rd}|^2 + t_2C_3\right). \tag{26}$$

Based on (13) and (14), we can rewrite (26) as

$$P_{co}^{\mathrm{VGR}} = \int_0^{C_5} f_Y(y)dy + \int_{C_5}^{\infty} F_X\left(\frac{t_2C_2y + t_2C_3}{\beta\lambda^2y - t_2C_1}\right)f_Y(y)dy = 1 - \sum_{m=0}^{N_s-1}\frac{e^{-t_2C_2/\beta\lambda^2\bar{\gamma}_{SR}}}{m!\bar{\gamma}_{RD}\bar{\gamma}_{SR}^m}\left(\frac{t_2C_2}{\beta\lambda^2}\right)^m\int_{C_5}^{\infty}\left(1 + \frac{C_4}{y - C_5}\right)^m \times e^{-\left(\left(t_2C_2C_4/\beta\lambda^2\bar{\gamma}_{SR}(y-C_5)\right) + (y/\bar{\gamma}_{RD})\right)}dy, \tag{27}$$

where $C_4 = (C_3/C_2) + (t_2C_1/\beta\lambda^2)$, and $C_5 = t_2C_1/\beta\lambda^2$. Then, let $\tilde{y} = y - C_5$, 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

$$P_{co}^{VGR} = 1 - \sum_{m=0}^{N_s-1}\sum_{n=0}^{m}\binom{m}{n}\frac{2C_4^ne^{-\left(t_2C_2/\beta\lambda^2\bar{\gamma}_{SR}\right) - (C_5/\bar{\gamma}_{RD})}}{m!\bar{\gamma}_{RD}\bar{\gamma}_{SR}^m}\left(\frac{t_2C_2}{\beta\lambda^2}\right)^m \times \left(\frac{t_2C_2C_4\bar{\gamma}_{RD}}{\beta\lambda^2\bar{\gamma}_{SR}}\right)^{(1-n)/2}K_{1-n}\left(\sqrt{\frac{4t_2C_2C_4}{\beta\lambda^2\bar{\gamma}_{SR}\bar{\gamma}_{RD}}}\right). \tag{28}$$

When $N_s \longrightarrow \infty$, we have $\|h_{sr}\|^2 \approx^{(a)} N_s\bar{\gamma}_{SR}$, where (a) 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

$$\varsigma^{\mathrm{VGR}} = R_s\Pr\left(\|h_{sr}\|^2 < \frac{(1-\beta)t_1|h_{rd}|^2}{\beta} + \frac{l_r^2t_1\lambda + t_1}{\beta\lambda}, \|h_{sr}\|^2 > \frac{t_2C_2|h_{rd}|^2 + t_2C_3}{\beta\lambda^2|h_{rd}|^2 - t_2C_1}, |h_{rd}|^2 > \frac{t_2C_1}{\beta\lambda^2}\right). \tag{29}$$

Since $((1-\beta)t_1|h_{rd}|^2/\beta) + (l_r^2t_1\lambda + t_1/\beta\lambda)$ and $(t_2C_2|h_{rd}|^2 + t_2C_3)/(\beta\lambda^2|h_{rd}|^2 - t_2C_1)$ have only one point of intersection when $|h_{rd}|^2 > 0$, and the intersection is u_3. Thus, the expression (29) can be expressed as

$$\begin{aligned}\varsigma^{\mathrm{VGR}} &= R_s\int_{u_4}^{\infty}F_X\left(\frac{(1-\beta)t_1y}{\beta} + \frac{l_r^2t_1\lambda + t_1}{\beta\lambda}\right)f_Y(y)dy - R_s\int_{u_4}^{\infty}F_X\left(\frac{t_2C_2y + t_2C_3}{\beta\lambda^2y - t_2C_1}\right)f_Y(y)dy \\ &= \sum_{m=0}^{N_s-1}\sum_{n=0}^{m}\binom{m}{n}\frac{R_sC_4^ne^{-t_2C_2/\beta\lambda^2\bar{\gamma}_{SR} - C_5/\bar{\gamma}_{RD}}}{m!\bar{\gamma}_{SR}^m\bar{\gamma}_{RD}}\left(\frac{t_2C_2}{\beta\lambda^2}\right)^m \times \int_{u_4-C_5}^{\infty}\frac{1}{y^n}e^{-\left(t_2C_2C_4/\beta\lambda^2\bar{\gamma}_{SR}y\right) - (y/\bar{\gamma}_{RD})}dy - \sum_{m=0}^{N_s-1}\sum_{n=0}^{m}\binom{m}{n} \\ &\times \frac{R_st_1^m(1-\beta)^ne^{-t_1\left(1+\lambda l_r^2\right)/\beta\lambda\bar{\gamma}_{SR}}}{m!\bar{\gamma}_{SR}^m\beta^m\bar{\gamma}_{RD}}\left(\frac{1+\lambda l_r^2}{\lambda}\right)^{m-n} \times \int_{u_4}^{\infty}y^ne^{-(((1-\beta)t_1/\beta\bar{\gamma}_{SR}) + (1/\bar{\gamma}_{RD}))y}dy,\end{aligned} \tag{30}$$

where $u_4 = \max(u_3, t_2C_1/\beta\lambda^2)$, $u_3 = (-b_2 + \sqrt{b_2^2 - 4a_2c_2})/2a_2$, $a_2 = t_1\beta\lambda^3(1-\beta)$, $b_2 = t_1\beta\lambda^2(1 + l_r^2\lambda) - t_1t_2\lambda C_1(1-\beta) - \beta\lambda t_2C_2$, and $c_2 = -\beta\lambda t_2C_3 - t_1t_2C_1(1 + l_r^2\lambda)$. Then, using [24, 1.211.1], [24, 3.351.2] and [24, 3.381.3], the exact EST of the untrusted full-duplex relay network with the VGR scheme can be derived as

$$\begin{aligned}\varsigma^{\mathrm{VGR}} &= \sum_{m=0}^{N_s-1}\sum_{n=0}^{m}\sum_{k=0}^{\infty}\binom{m}{n}\frac{(-1)^kR_sC_4^{n+k}e^{-\left(t_2C_2/\beta\lambda^2\bar{\gamma}_{SR}\right) - (C_5/\bar{\gamma}_{RD})}}{m!k!\bar{\gamma}_{SR}^{m+k}\bar{\gamma}_{RD}^{n+k}} \times \left(\frac{t_2C_2}{\beta\lambda^2}\right)^{m+k}\Gamma\left(1 - n - k, \frac{u_4 - C_5}{\bar{\gamma}_{RD}}\right) \\ &\cdot - \sum_{m=0}^{N_s-1}\sum_{n=0}^{m}\binom{m}{n}\frac{R_st_1^m(1-\beta)^ne^{-t_1\left(1+\lambda l_r^2\right)/\beta\lambda\bar{\gamma}_{SR}}}{m!\bar{\gamma}_{SR}^m\beta^m\bar{\gamma}_{RD}} \times \left(\frac{1+\lambda l_r^2}{\lambda}\right)^{m-n}\left(\frac{(1-\beta)t_1}{\beta\bar{\gamma}_{SR}} + \frac{1}{\bar{\gamma}_{RD}}\right)^{-n-1} \\ &\times \Gamma\left(n+1, \frac{(1-\beta)t_1u_4}{\beta\bar{\gamma}_{SR}} + \frac{u_4}{\bar{\gamma}_{RD}}\right).\end{aligned} \tag{31}$$

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 $N_s \longrightarrow \infty$. 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.

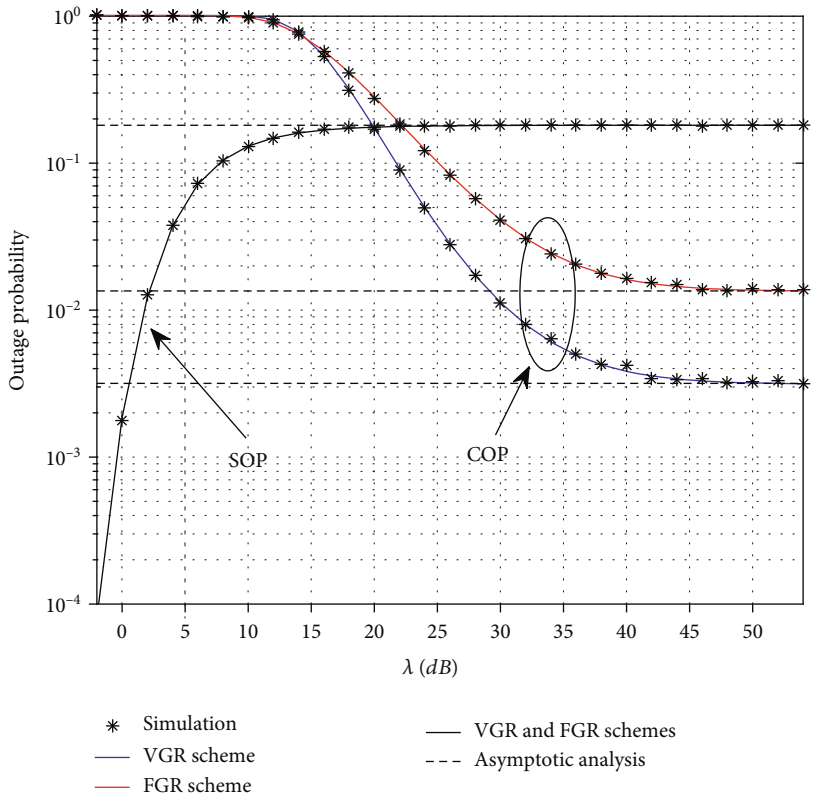

Figure 2: The outage probability of the FGR scheme and the VGR scheme versus the transmit SNR.

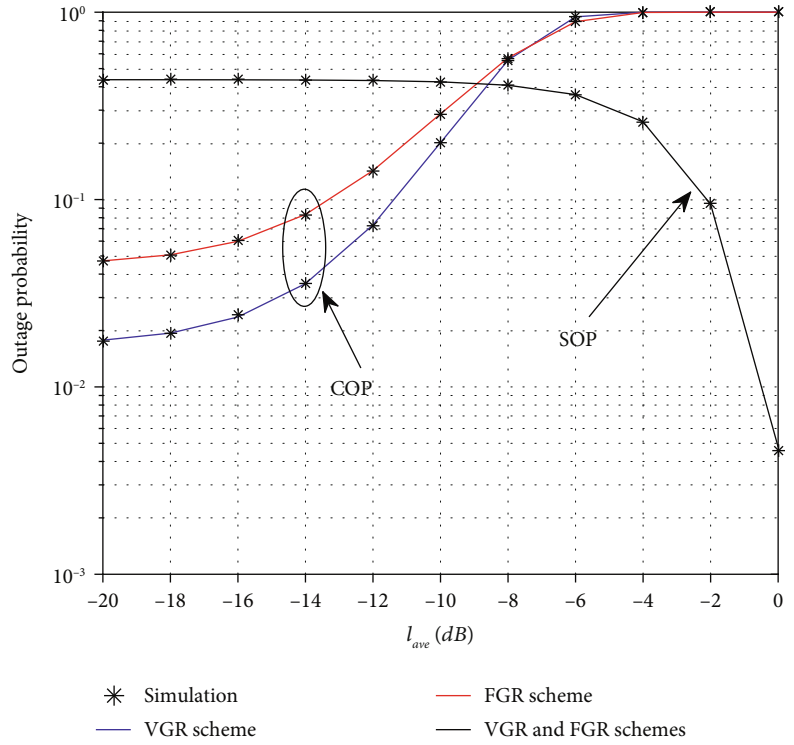

Figure 3: The outage probability of the FGR scheme and the VGR scheme versus the self-interference cancellation capability.

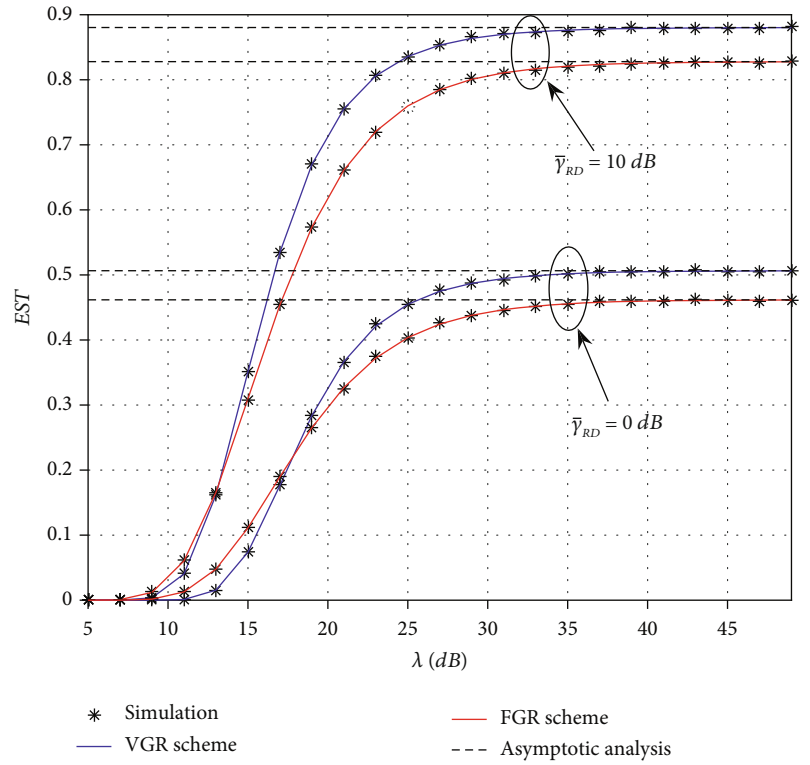

Figure 4: The EST of the FGR scheme and the VGR scheme versus the transmit SNR.

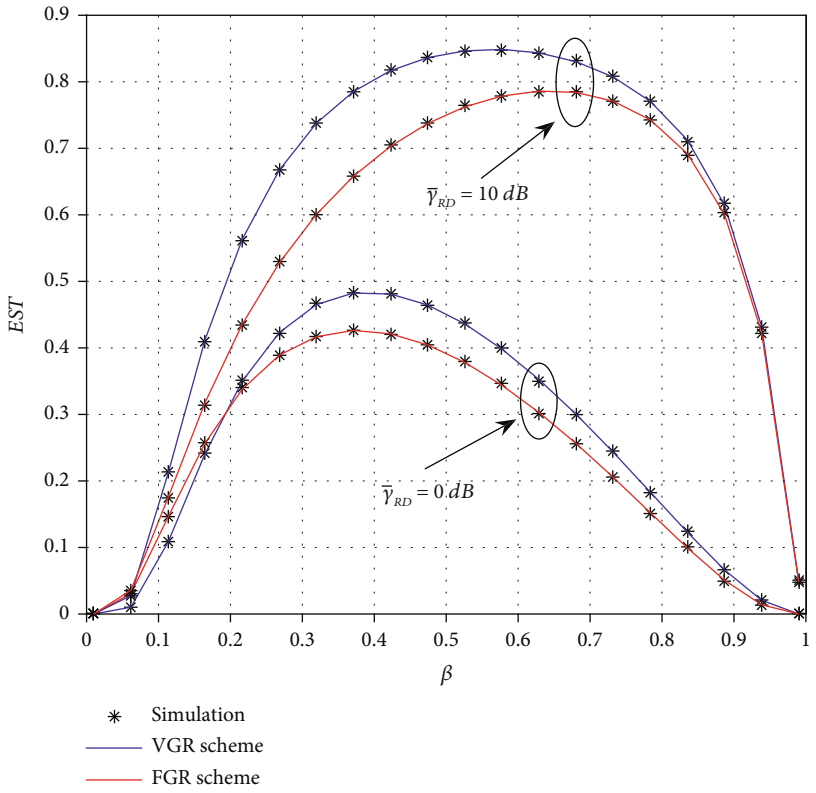

Figure 5: The EST of the FGR scheme and the VGR scheme versus the power allocation factor.

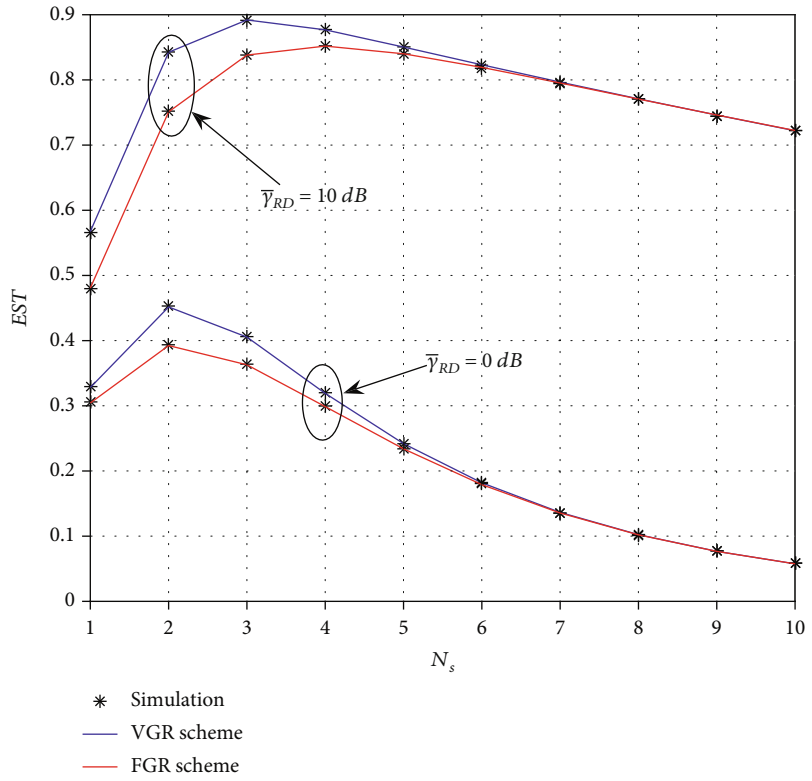

Figure 6: The EST of the FGR scheme and the VGR scheme versus the number of antennas at the source.

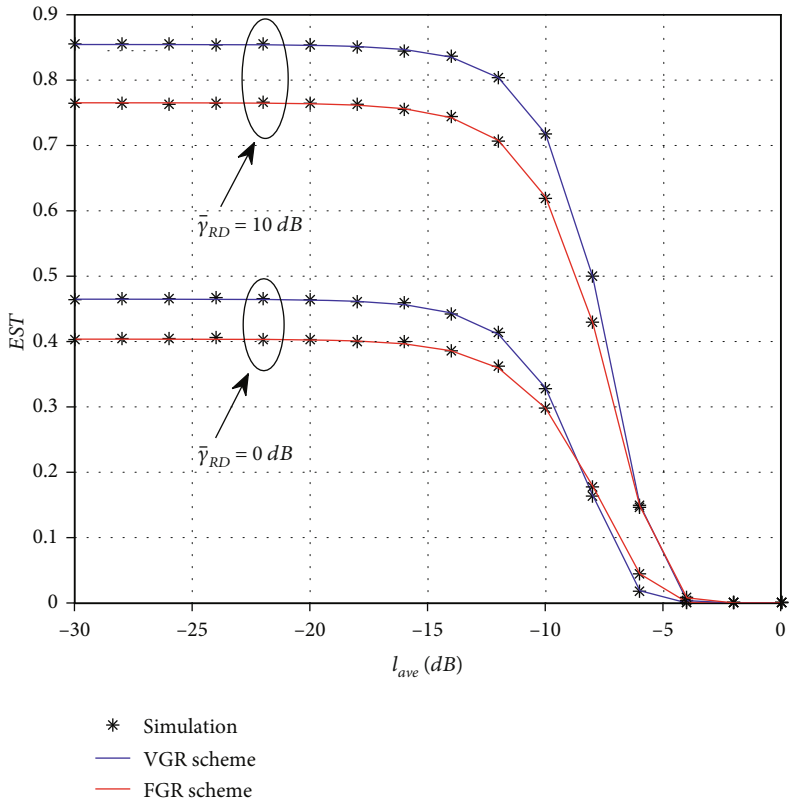

Figure 7: The EST of the FGR scheme and the VGR scheme versus the self-interference cancellation capability.

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

$$\lim_{\lambda\longrightarrow\infty} P_{co}^{\mathrm{VGR}} = 1 - \sum_{m=0}^{N_s-1}\sum_{n=0}^{m}\binom{m}{n}\frac{2t_2^m C_7^m C_9^n e^{-(t_2C_7/\beta\bar{\gamma}_{SR})-(C_{10}/\bar{\gamma}_{RD})}}{m!\beta^m\bar{\gamma}_{RD}\bar{\gamma}_{SR}^m} \times\left(\frac{t_2C_7C_9\bar{\gamma}_{RD}}{\beta\bar{\gamma}_{SR}}\right)^{(1-n)/2} K_{1-n}\left(\sqrt{\frac{4t_2C_7C_9}{\beta\bar{\gamma}_{SR}\bar{\gamma}_{RD}}}\right), \tag{32}$$

where $C_6 = \beta l_d^2(1-\beta)$, $C_7 = l_r^2 + l_d^2(1-\beta)^2$, $C_8 = l_r^2 l_d^2(1-\beta)$, $C_9 = (C_8/C_7) + (t_2C_6/\beta)$, and $C_{10} = t_2C_6/\beta$. From (31), we have

$$\begin{aligned}\lim_{\lambda\longrightarrow\infty}\varsigma^{\mathrm{VGR}} = {} & \sum_{m=0}^{N_s-1}\sum_{n=0}^{m}\sum_{k=0}^{\infty}\binom{m}{n}\frac{(-1)^k R_s C_9^{n+k} e^{-(t_2C_7/\beta\bar{\gamma}_{SR})-(C_{10}/\bar{\gamma}_{RD})}}{m!k!\bar{\gamma}_{SR}^{m+k}\bar{\gamma}_{RD}^{n+k}} \\ & \times\left(\frac{t_2C_7}{\beta}\right)^{m+k}\Gamma\left(1-n-k, \frac{u_6-C_{10}}{\bar{\gamma}_{RD}}\right) \\ & \cdot - \sum_{m=0}^{N_s-1}\sum_{n=0}^{m}\binom{m}{n}\frac{R_s t_1^m(1-\beta)^n l_r^{2m-2n}}{m!\bar{\gamma}_{SR}^m\beta^m\bar{\gamma}_{RD}} \\ & \times e^{-t_1l_r^2/\beta\bar{\gamma}_{SR}}\left(\frac{(1-\beta)t_1}{\beta\bar{\gamma}_{SR}}+\frac{1}{\bar{\gamma}_{RD}}\right)^{-n-1} \\ & \times\Gamma\left(n+1, \frac{(1-\beta)t_1u_6}{\beta\bar{\gamma}_{SR}}+\frac{u_6}{\bar{\gamma}_{RD}}\right),\end{aligned} \tag{33}$$

where $u_6 = \max(u_5, t_2C_6/\beta)$, $u_5 = (-b_3 + \sqrt{b_3^2 - 4a_3c_3})/2a_3$, $a_3 = t_1\beta(1-\beta)$, $b_3 = t_1\beta l_r^2 - \beta t_2C_7 - t_1t_2C_6(1-\beta)$, and $c_3 = -\beta t_2C_8 - t_2t_1C_6l_r^2$.

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, $R_0 = 2$ bits/sec/Hz, and the confidential information rate $R_s = 1$ bits/sec/Hz. Also, we set $l_r = l_d = l_{\mathrm{ave}}$. 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 $N_s = 2$, $\beta = 0.5$, $l_{\mathrm{ave}} = -15dB$, $\bar{\gamma}_{SR} = 0$ dB, and $\bar{\gamma}_{RD} = 5$ 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 $N_s = 2$, $\beta = 0.5$, $\lambda = 30$, $\bar{\gamma}_{SR} = 0$ dB, and $\bar{\gamma}_{RD} = 0$ dB. We observe that the SOP 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 $N_s = 2$, $\beta = 0.5$, $l_{\mathrm{ave}} = -10$ dB, and $\bar{\gamma}_{SR} = 0$ 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 $\bar{\gamma}_{RD} = 10$ dB outperform the EST with $\bar{\gamma}_{RD} = 0$ 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 $N_s = 2$, $\lambda = 20$ dB, $\l_{\mathrm{ave}} = -15$ dB, and $\bar{\gamma}_{SR} = 0$ 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 $\bar{\gamma}_{RD}$ 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 $\lambda = 20$ dB, $\beta = 0.5$, $l_{\mathrm{ave}} = -15$ dB, and $\bar{\gamma}_{SR} = 0$ 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 $\bar{\gamma}_{SR} = 0$ 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 can not 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., $\lambda \longrightarrow \infty$, 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

[1] W. Yang, X. Lu, S. Yan, F. Shu, and Z. Li, "Age of information for short-packet covert communication," *IEEE Wireless Communications Letters*, vol. 10, no. 9, pp. 1890–1894, 2021.

[2] X. Lu, W. Yang, S. Yan, Z. Li, and D. W. K. Ng, "Covertness and timeliness of data collection in UAV-aided wireless-powered IoT," *IEEE Internet of Things Journal*, vol. 9, no. 14, pp. 12573–12587, 2021.

[3] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[4] M. Li, X. Tao, N. Li, H. Wu, and J. Xu, "Secrecy energy efficiency maximization in UAV-enabled wireless sensor networks without eavesdropper's CSI," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3346–3358, 2022.

[5] P. Angueira, I. Val, J. Montalban et al., "A survey of physical layer techniques for secure wireless communications in industry," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 810–838, 2022.

[6] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 574–583, 2015.

[7] Q. Li, W. K. Ma, and D. Han, "Sum secrecy rate maximization for full-duplex two-way relay networks using Alamouti-based rank-two beamforming," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1359–1374, 2016.

[8] C. Zhang, F. Jia, J. Ge, and F. Gong, "Security-reliability tradeoff for secure relaying systems with full-duplex radio," *IEEE Access*, vol. 6, pp. 60862–60868, 2018.

[9] Z. Cao, X. Ji, J. Wang et al., "Security-reliability trade-off analysis of AN-aided relay selection for full-duplex relay networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 3, pp. 2362–2377, 2021.

[10] B. Chen, Y. Chen, Y. Chen et al., "Secure primary transmission assisted by a secondary full-duplex NOMA relay," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 7214–7219, 2019.

[11] X. He and A. Yener, "Cooperation with an untrusted relay: a secrecy perspective," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3807–3827, 2010.

[12] C. Jeong, I. M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Transactions on Signal Processing*, vol. 60, no. 1, pp. 310–325, 2012.

[13] J. Huang, A. Mukherjee, and A. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2536–2550, 2013.

[14] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Transactions on Signal Processing*, vol. 62, no. 9, pp. 2185–2199, 2014.

[15] L. Sun, P. Ren, Q. Du, Y. Wang, and Z. Gao, "Security-aware relaying scheme for cooperative networks with untrusted relay nodes," *IEEE Communications Letters*, vol. 19, no. 3, pp. 463–466, 2015.

[16] H. Xu, L. Sun, P. Ren, and Q. Du, "Securing two-way cooperative systems with an untrusted relay: a constellation-rotation aided approach," *IEEE Communications Letters*, vol. 19, no. 12, pp. 2270–2273, 2015.

[17] S. Atapattu, N. Ross, Y. Jing, and M. Premaratne, "Source-based jamming for physical-layer security on untrusted full-duplex relay," *IEEE Communications Letters*, vol. 23, no. 5, pp. 842–846, 2019.

[18] J. Lim, T. Kim, and I. Bang, "Impact of outdated CSI on the secure communication in untrusted in-band full-duplex relay networks," *IEEE Access*, vol. 10, pp. 19825–19835, 2022.

[19] A. Mabrouk, A. E. Shafie, K. Tourki, N. Al-Dhahir, and N. Hamdi, "Securing untrusted full-duplex relay channels in the presence of multiple external cluster-based eavesdroppers," *IEEE Systems Journal*, vol. 14, no. 1, pp. 665–668, 2020.

[20] S. Zhao, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Secure beamforming for full-duplex MIMO two-way untrusted relay systems," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3775–3790, 2020.

[21] C. Yang, W. Wang, S. Zhao, and M. Peng, "Performance of decode-and-forward opportunistic cooperation with channel estimation errors," in *21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1967–1971, Istanbul, Turkey, 2010.

[22] Z. Liu, Y. Ye, G. Lu, and R. Q. Hu, "System outage performance of SWIPT enabled full-duplex two-way relaying with residual hardware impairments and self-interference," *IEEE Systems Journal*, pp. 1–12, 2022.

[23] J. Hu, W. Yang, N. Yang, X. Zhou, and Y. Cai, "On–off-based secure transmission design with outdated channel state information," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6075–6088, 2016.

[24] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series, and Products*, Academic Press, Inc., 7th edition, 2007.