Joint Relay and Jammer Selection Improves the Physical Layer Security in the Face of CSI Feedback Delays

Lei Wang, *Student Member, IEEE*, Yueming Cai, *Senior Member, IEEE*, Yulong Zou, *Senior Member, IEEE*, Weiwei Yang, *Member, IEEE*, and Lajos Hanzo, *Fellow, IEEE*

***Abstract*—We enhance the physical layer security (PLS) of amplify-and-forward (AF) relaying networks with the aid of joint relay and jammer selection (JRJS), despite the deleterious effect of channel state information (CSI) feedback delays. Furthermore, we conceive a new outage-based characterization approach for the JRJS scheme. The traditional best relay selection (TBRS) is also considered as a benchmark. We first derive closed-form expressions of both the connection outage probability (COP) and the secrecy outage probability (SOP) for both the TBRS and JRJS schemes. Then, a reliable and secure connection probability (RSCP) is defined and analyzed for characterizing the effect of the correlation between the COP and the SOP introduced by the corporate source–relay link. The reliability–security ratio (RSR) is introduced for characterizing the relationship between the reliability and the security through asymptotic analysis. Moreover, the concept of effective secrecy throughput is defined as the product of the secrecy rate and of the RSCP for the sake of characterizing the overall efficiency of the system, as determined by the transmit SNR, the secrecy codeword rate, and the power sharing ratio between the relay and the jammer. The impact of the direct source–eavesdropper link and additional performance comparisons with respect to other related selection schemes are also included. Our numerical results show that the JRJS scheme outperforms the TBRS method both in terms of the RSCP and in terms of its effective secrecy throughput, but it is more sensitive to the feedback delays. Increasing the transmit signal-to-noise ratio (SNR) will not always improve the overall throughput. Moreover, the RSR results demonstrate that, upon reducing the CSI feedback delays, the reliability improves more substantially than the security degrades, implying an overall improvement in terms of the security–reliability tradeoff. Additionally, the secrecy throughput loss due to the second-hop feedback delay is more pronounced than that due to the first-hop one.**

Manuscript received October 2, 2014; revised February 25, 2015 and July 27, 2015; accepted September 8, 2015. This work was supported in part by the National Natural Science Foundation of China under Grant 61371122, Grant 61471393, and Grant 61501512 and in part by the Natural Science Foundation of Jiangsu Province under Grant BK20150718 and Grant BK20150040. The review of this paper was coordinated by Prof. M. C. Gursoy.

L. Wang, Y. Cai, and W. Yang are with the College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China (e-mail: csu-wl@163.com; caiym@vip.sina.com; yww_1010@aliyun.com).

Y. Zou is with the School of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: yulong.zou@njupt.edu.cn).

L. Hanzo is with the Department of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (e-mail: lh@ecs.soton.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2015.2478029

***Index Terms*—Effective secrecy throughput, feedback delay, physical layer security (PLS), relay and jammer selection, reliability and security.**

I. Introduction

WIRELESS communications systems are particularly vulnerable to security attacks because of the inherent openness of the transmission medium. Traditionally, the information privacy of wireless networks has been focused on the higher layers of the protocol stack employing cryptographically secure schemes. However, these methods typically assume a limited computing power for the eavesdroppers and exhibit inherent vulnerabilities in terms of the inevitable secret key distribution and management [1]. In recent years, physical layer security (PLS) has emerged as a promising technique of improving the confidentiality wireless communications, which exploits the time-varying properties of fading channels, instead of relying on conventional cryptosystems. The pivotal idea of PLS solutions is to exploit the dynamically fluctuating random nature of radio channels for maximizing the uncertainty concerning the source messages at the eavesdropper [2], [3].

To achieve this target, several PLS-enhancement approaches have been proposed in the literature, including secrecy-enhancing channel coding [4], secure on–off transmission designs [5], secrecy-improving beamforming (BF)/precoding, and artificial-noise-aided techniques relying on multiple antennas [6], as well as secure relay-assisted transmission techniques [7]. Specifically, apart from improving the reliability and coverage of wireless transmissions, user cooperation also has a great potential in terms of enhancing the wireless security against eavesdropping attacks. There has been a growing interest in improving the security of cooperative networks at the physical layer [8]–[14]. To explore the spatial diversity potential of the relaying networks and to boost the secrecy capacity (the difference between the channel capacity of the legitimate main link and that of the eavesdropping link), most of the existing work has been focused on secrecy-enhancing BF [8], [9], as well as on intelligent relay node/jammer node (RN/JN) selection, etc. Notably, given the availability of multiple relays, appropriately designed RN/JN selection is capable of achieving a significant security improvement for cooperative networks, which is emerging as a promising research topic. In particular, Zou *et al.* investigated both amplify-and-forward (AF)- and decode-and-forward (DF)-based optimal relay selection conceived for

enhancing the PLS in cooperative wireless networks [10], [11], where the global channel state information (CSI) of both the main link and the eavesdropping link was assumed to be available. Similarly, jamming techniques, which impose artificial interference on the eavesdropper, have also attracted substantial attention [12]–[14]. More specifically, several sophisticated joint relay and jammer selection (JRJS) schemes were proposed in [12], where the beneficially selected relay increases the reliability of the main link, whereas the carefully selected jammer imposes interference on the eavesdropper and simultaneously protects the legitimate destination from interference. In [13] and [14], cooperative jamming has been studied in the context of bidirectional scenarios, and efficient RN/JN selection criteria have been developed for achieving improved secrecy rates with the aid of multiple relays. Furthermore, more effective relaying and jamming schemes, when taking the information leakage of the source–eavesdropper link into consideration, have been presented lately in [15] and [16].

Nevertheless, an idealized assumption of the previously reported research on PLS is the availability of perfect channel state information (CSI), which is regarded as a stumbling block in the way of invoking practical secrecy-enhancing Wyner coding, on–off design, BF/precoding, and RN/JN selection. However, this idealized simplifying assumption is not realistic, since practical channel estimation imposes CSI imperfections, which are aggravated by the feedback delay, limited-rate feedback, and channel estimation errors (CEEs) [17]. Generally, the related research has been focused on the issues of robust secure BF design from an average secrecy-rate-based optimization perspective for point-to-point multiantenna aided channels and relay channels [18], [19] supporting delay-tolerant systems. For systems imposing stringent delay constraints, particularly in imperfect CSI scenarios, perfect secrecy cannot always be achieved. Hence, the secrecy-outage-based characterization of systems is more appropriate, which provides a probabilistic performance measure of secure communication. The concept of secrecy outage was adopted in [20] for characterizing the probability of having both reliable and secure transmission, which, however, is inapplicable for the imperfect CSI case and fails to distinguish a connection outage from the secrecy outage. In [21], an alternative secrecy outage formulation is proposed for characterizing the attainable security level and provided a general framework for designing transmission schemes that meet specific target security requirements. To quantify both the reliability and security performance at both the legitimate and eavesdropper nodes separately, two types of outages, namely, the connection outage probability (COP) and the secrecy outage probability (SOP) are introduced. Then, considering the impact of time delay caused by the antenna selection process at the legitimate receiver, Hu *et al.* [22] proposed a new secure transmission scheme in the multiinput multioutput multieavesdropper wiretap channel. Much recently, considering the outdated CSI from the legitimate receiver, a new secure on–off transmission scheme was proposed for enhancing the secrecy throughput in [23].

Moreover, prior studies of the outage-based secure transmission design are limited to single-antenna-assisted single-hop systems and have not been considered for cooperative relaying systems. Hence, the issues of secure transmissions over cooperative relaying channels expressed in terms of the SOP, COP, and secrecy throughput constitute an open problem. On the other hand, apart from CEE, the CSI feedback delay results in critical challenges for the PLS of cooperative relaying systems, particularly when considering the specifics of RN/JN selection. In [15], the effects of outdated CSI knowledge concerning the legitimate links on the ergodic secrecy rate achieved by the proposed secure transmission strategy in the context of DF relaying is investigated. The impact of CSI feedback delay on the secure relay and jammer selection conceived for DF relaying was investigated in [24], albeit only in terms of the SOP. In our previous study [25], we considered the secure transmission design and the secrecy performance of an opportunistic DF system relying on outdated CSI, where only a single relay is invoked. Additionally, during the revision of this work, we investigated the security performance for outdated AF relay selection in [26]. Therefore, in this treatise, we extend our investigations to the PLS of multiple AF relaying assisted networks relying on RN/JN selection.

Explicitly, we focus our attention on the outage-based characterization of secure transmissions in cooperative relay-aided networks relying on realistic CSI feedback delay. To exploit the multirelay induced diversity gain and the associated jamming capabilities, joint AF relay node and jammer node selection is employed by the relay–destination link. We assume that, in line with the practical reality, the instantaneous eavesdropper's CSI is unavailable at the legitimate transmitter and that the RN/JN selections are performed based on the outdated CSI of the main links. Two types of cooperative strategies are invoked by our cooperative network operating under secrecy constraints, namely, the traditional best relay selection (TBRS) strategy and the JRJS strategy. Specifically, the main contributions of this paper can be summarized as follows.

- We develop an outage-based characterization for quantifying both the reliability and security performance of a two-hop AF relaying system. Specifically, in contrast to [21] and [22], we propose the novel definition of the reliable and secure connection probability (RSCP). Explicitly, closed-form expressions of the COP, the SOP, and the RSCP are derived for both the TBRS and for our JRJS strategies. Numerical results demonstrate that the JRJS scheme outperforms the TBRS scheme in terms of its RSCP.
- We also introduce the reliability–security ratio (RSR) for characterizing their direct relationship by a single parameter through the asymptotic analysis of the COP and the SOP in the high-SNR regime. We derive the RSR for both the TBRS and JRJS strategies for investigating the effect of secrecy codeword rate setting, as well as that of the feedback delay and that of the power sharing ratio between the relay and the jammer on the RSR.
- We then modify the definition of effective secrecy throughput by multiplying the secrecy rate with the RSCP, which results in an optimization problem of the transmit signal-to-noise ratio (SNR), secrecy codeword rate, and power sharing between the relay and the jammer.

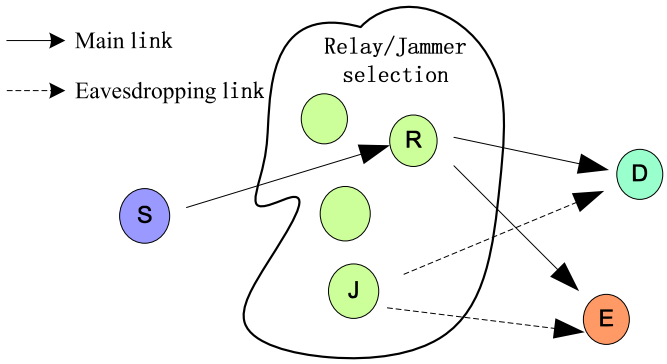

Fig. 1. Cooperative relaying network assisted by multiple relays in the presence of an eavesdropper.

It is shown that, compared with the TBRS strategy, JRJS achieves a significantly higher effective secrecy throughput, and the corresponding throughput loss is more sensitive to feedback delays. The impact of the direct source–eavesdropper link and additional throughput performance comparisons with respect to other related selection schemes are further discussed.

The remainder of this paper is organized as follows. Section II introduces our system model and describes both the TBRS and our JRJS strategies. In Sections III and IV, we present the mathematical framework of our performance analysis both for the TBRS strategy and for the JRJS strategy, respectively, including the COP, the SOP, the RSCP, the RSR, and the effective secrecy throughput. Our numerical results and discussions are provided in Section V. Finally, Section VI presents our concluding remarks.

II. System Model

A. System Description

Consider a cooperative relaying network consisting of a source S, a destination D, K_r relays R_k, $k = 1, \ldots, K_r$, and an eavesdropper E, as shown in Fig. 1, where all nodes are equipped with a single transmit antenna (TA), except for the source, which has N_t TAs. The cooperative relay architecture in Fig. 1 is generally applicable to diverse practical wireless systems in the presence of an eavesdropper, including the family of wireless sensor networks (WSNs), mobile ad hoc networks (MANETs), and the long-term evolution advanced cellular systems [11].

To exploit the diversity potential of multiple relay nodes over independently fading channels, AF relay/jammer selection is employed. All relays operate in the half-duplex AF mode, and data transmission is performed in two phases. More particularly, during the broadcast phase, the source node transmits its signal to a selected relay with the aid of BF, which is invoked for forwarding the signal received from S to D. An inherent assumption is that the transmit BF weights are based on the CSI estimates quantified and fed back by the selected relay. During the cooperative phase, a pair of appropriately selected relays transmit toward D and E, respectively. A conventional relay (denoted by R^*) forwards the source's message to the destination. Another relay (denoted by J^*) operates in the "jammer mode" and imposes intentional interference upon E in order confuse it. However, D is unable to mitigate the artificial interference emanating from the jammer node J^* due to its critical secrecy constraints [12]. It should be noted that both the process of RN/JN selection and the feedback of the transmit BF weights from R^* to S may impose a time lag between the data transmission and the channel estimation. These time delays are denoted by $T_{d_{SR}}$ and $T_{d_{RD}}$, respectively. Furthermore, we assume that the BF and RN/JN selection process is based on the perfectly estimated but outdated CSI. We employ the first-order autoregressive outdated CSI model of [20], while relying on the correlation coefficients of $\rho_{SR} = J_0(2\pi f_d T_{d_{SR}})$ and $\rho_{RD} = J_0(2\pi f_d T_{d_{RD}})$ for the two hops, where $J_0(\cdot)$ is the zero-order Bessel function of the first kind, and f_d is the Doppler frequency.

A slow flat block Rayleigh fading environment is assumed, where the channel remains static for the coherence interval (one slot) and changes independently in different coherence intervals, as denoted by $h_{i,j} \sim \mathcal{CN}(0, \sigma^2_{i,j})$, $i, j \in \{S, R, J, D, E\}$. The direct communication links are assumed to be unavailable due to the presence of obstructions between S and D, as well as the eavesdropper.[1] This assumption follows the rationale of [12] and has been routinely exploited in previous literature (see [27] and [28] and the references therein), where the source and relays belong to the same cluster, whereas the destination and the eavesdropper are located in another. More specifically, this assumption is particularly valid in networks with broadcast and unicast transmission, where each terminal is a legitimate receiver for one signal and acts as an eavesdropper for some other signal. Therefore, the security concerns are only related to the cooperative relay-aided channel. Furthermore, additive white Gaussian noise (AWGN) is assumed with zero mean and unit variance N_0. Let P_i be the transmit power of node i, and the instantaneous SNR of the $i \to j$ link is given by $\gamma_{i,j} = P_i |h_{i,j}|^2 / N_0$.

We employ the constant-rate Wyner coding scheme for constructing wiretap codes of [2] to meet the PLS requirements due to the fact that the accurate global CSI is not available. Let $\mathbb{C}(R_0, R_s, N)$ denote the set of all possible Wyner codes of length N, where R_0 is the codeword transmission rate, and R_s is the confidential information rate ($R_0 > R_s$). The positive rate difference $R_e = R_0 - R_s$ is the cost of providing secrecy against the eavesdropper. A confidential message is encoded into a codeword at S and then transmitted to D.

B. Secure Transmission

In the broadcast phase, S transmits its BF signal $s(t)$ to the selected relay R^*, where the relay selection is performed before data transmission commences, and the selection criterion will be detailed later in the context of the cooperative phase. The transmit BF vector $\mathbf{w}(t|T_d)$ is calculated using the perfectly estimated but outdated CSI given by

[1] The case when the $S \to E$ link is introduced will be investigated separately in Section VI.

$\mathbf{w}(t|T_{d_{SR}}) = \mathbf{h}^H_{SR^*}(t-T_d)/|\mathbf{h}_{SR^*}(t-T_{d_{SR}})|$ [29], where we have $\mathbf{h}_{SR^*}(t) = [h_{SR^*,1}(t), \ldots, h_{SR^*,N_t}(t)]^T$, and the signal received by the relay R^* can be written as

$$y_{R^*}(t) = \sqrt{P_s}\mathbf{w}(t|T_d)\mathbf{h}_{SR^*}(t)s(t) + n_{SR^*}(t) \tag{1}$$

where $n_{SR^*}(t)$ is the AWGN at the relay. Then, we can define the received SNR at the relay node as $\gamma_{SR} = P_S|\mathbf{w}(t|T_{d_{SR}})\mathbf{h}_{SR^*}(t)|^2/N_0$.

In the cooperative phase, we consider two RN/JN selection schemes performed by D: relay selection without jamming and JRJS.

1) Traditional Best Relay Selection: The first category of solutions does not involve a jamming process, and therefore, only a conventional relay accesses the channel during the second phase of the protocol. The relay selection process is performed based on the highest instantaneous SNR of the second hop, which is formulated as

$$R^* = \arg\max_{R_k \in \mathcal{R}} \left\{ \frac{\tilde{\gamma}_{R_k D}}{\mathbb{E}\left[\gamma_{R_k E}\right]} = \frac{P_R \left|\tilde{h}_{R_k D}(t-T_d)\right|^2}{N_0 \mathbb{E}\left[\gamma_{R_k E}\right]} \right\} \tag{2}$$

where $\tilde{\gamma}_{R_k D}$ is the instantaneous SNR in the relay selection process, and $\mathbb{E}[\gamma_{R_k E}]$ denotes the average SNR at E. We can model $\gamma_{R_k D}$ and $\tilde{\gamma}_{R_k D}$ as two gamma distributed random variables having the correlation factor of ρ^2_{RD}.

During the second phase, the received signal $y_{R^*}(t)$ is multiplied by a time-variant AF-relay gain G and retransmitted to D, where we have $G = \sqrt{P_R/(P_S|\mathbf{w}_{\text{opt}}(t|T_{d_{SR}})\mathbf{h}_{SR^*}(t)|^2 + N_0)}$. After further mathematical manipulations, the mutual information (MI) between S and D, as well as the eavesdropper, can be written as

$$I_D^{\text{TBRS}} = \frac{1}{2}\log\left(1+\gamma_D^{\text{TBRS}}\right) = \frac{1}{2}\log\left(1+\frac{\gamma_{SR}\gamma_{R^*D}}{\gamma_{SR}+\gamma_{R^*D}+1}\right) \tag{3}$$

$$I_E^{\text{TBRS}} = \frac{1}{2}\log\left(1+\gamma_E^{\text{TBRS}}\right) = \frac{1}{2}\log\left(1+\frac{\gamma_{SR}\gamma_{R^*E}}{\gamma_{SR}+\gamma_{R^*E}+1}\right). \tag{4}$$

2) Joint Relay and Jammer Selection: Similarly, considering the unavailability of the instantaneous CSI regarding the eavesdropper, we adopt a suboptimal RN/JN selection metric conditioned on the outdated CSI as

$$\begin{aligned} R^* &= \arg\max_{R_k \in \mathcal{R}} \left\{ \frac{\tilde{\gamma}_{R_k D}}{\mathbb{E}\left[\gamma_{R_k E}\right]} \right\} \\ J^* &= \arg\min_{R_k \in \mathcal{R}-R^*} \left\{ \frac{\tilde{\gamma}_{R_k D}}{\mathbb{E}\left[\gamma_{R_k E}\right]} \right\} \end{aligned} \tag{5}$$

where J^* is selected for minimizing the interference imposed on D.

It should be noted that, to have the same transmit power as that of the TBRS case, we assume that $P_{R*} + P_{J^*} = P_R$ for our JRJS strategy and introduce $\lambda = P_{R^*}/(P_{R^*} + P_{J^*})$ as the ratio of the relay's transmit power to the total power required by the active relay and jammer.

In the cooperative phase, R^* will also amplify the received signal $y_{R^*}(t)$ by G and forward it to D. At the same time, the jammer J^* will generate intentional interference to confuse E, which will also cause interference at D. Consequently, the MI between the terminals is given by

$$I_D^{\text{JRJS}} = \frac{1}{2}\log\left(1+\gamma_D^{\text{JRJS}}\right) = \frac{1}{2}\log\left(1+\frac{\gamma_{SR}\frac{\gamma_{R^*D}}{\gamma_{J^*D}+1}}{\gamma_{SR}+\frac{\gamma_{R^*D}}{\gamma_{J^*D}+1}+1}\right) \tag{6}$$

$$I_E^{\text{JRJS}} = \frac{1}{2}\log\left(1+\gamma_E^{\text{JRJS}}\right) = \frac{1}{2}\log\left(1+\frac{\gamma_{SR}\frac{\gamma_{RE}}{\gamma_{JE}+1}}{\gamma_{SR}+\frac{\gamma_{RE}}{\gamma_{JE}+1}+1}\right). \tag{7}$$

Remark 1: Generally, the optimal RN/JN selection scheme should take into account the global SNR knowledge set $\{\gamma_{SR}, \gamma_{RD}, \gamma_{RE}\}$. However, given the potentially excessive implementational complexity overhead of the optimal selection schemes and the unavailability of the global CSI, we employ suboptimal selection schemes as in [12].[2] Furthermore, it is commonly assumed that the average SNR of the eavesdropper is available at the transmitter, which seems, somehow, not reasonable. However, as stated in most of the literature, such as [12]–[22], [24]–[28], and [30], provided that the eavesdropper belongs to the network, which is also the case in our paper, the related assumption might still be deemed reasonably. Additionally, as in [8], [11], [12], and [24], for mathematical convenience, we assume that the relaying channels are independent and identically distributed and that we have $\mathbb{E}[\gamma_{SR_k}] = \bar{\gamma}_{SR}$, $\mathbb{E}[\gamma_{R_k D}] = \bar{\gamma}_{RD}$, and $\mathbb{E}[\gamma_{R_k E}] = \bar{\gamma}_{RE}$. The distances between the relays are assumed to be much smaller than the distances between relays and source/destination/eavesdropper; hence, the corresponding path losses among the different relays are approximately the same. This assumption is reasonable both for WSNs and for MANETs associated with a symmetric clustered relay configuration, and it may be also satisfied as valid by classic cellular systems in a statistical sense [11].

III. Secure Transmission Without Jamming

Here, we endeavor to characterize both the reliability and security performance comprehensively of the TBRS scheme. We first derive closed-form expressions for both the COP and the SOP. Then, the RSR is introduced through the asymptotic analysis of the COP and the SOP. Furthermore, we propose the novel definition of the RSCP and the effective secrecy throughput.

[2] To further alleviate the cooperation-related overhead, the selection criterion is based on the $R \to D$ link, since the second hop plays a dominant role in determining the received SNR, because the first hop corresponds to a multiple-input–single-output channel with the aid of multiple antennas, and hence, it is more likely to be better than the second hop. The optimal selection based on both hops is beyond the scope of this work.

A. COP and SOP

When the perfect instantaneous CSI of the eavesdropper's channel and even the legitimate users' channel is unavailable, alternative definitions of the outage probability may be adopted for the statistical characterization of the attainable secrecy performance, particularly for delay-limited applications. Based on [31, Def. 2], perfect secrecy cannot be achieved, when we have $R_e < I_E$, where I_E denotes the MI between the source and the eavesdropper. Encountering this event is termed as a secrecy outage. Furthermore, the destination is unable to flawlessly decode the received codewords when $R_0 > I_D$, which is termed as a connection outage. The grade of reliability and the grade of security maintained by a transmission scheme may be then quantified by the COP and the SOP, respectively.

We continue by presenting our preliminary results versus the point-to-point SNRs. Let us denote the cumulative distribution function (CDF) and the probability density function (PDF) of a random variable X by $F_X(x)$ and $f_X(x)$, respectively. On one hand, the PDF of γ_{SR} using [29, eq. (15)] is given by

$$f_{\gamma_{SR}}(x) = \sum_{n=0}^{N_t-1} \binom{N_t-1}{n} \frac{\rho_{SR}^{2(N_t-1-n)} \left(\bar{\gamma}_{SR}\left(1-\rho_{SR}^2\right)\right)^n}{\bar{\gamma}_{SR}^{N_t}(N_t-1-n)!} \times x^{N_t-1-n} e^{\frac{-x}{\bar{\gamma}_{SR}}} \quad (8)$$

whereas its CDF is given by

$$F_{\gamma_{SR}}(x) = 1 - \sum_{n=0}^{N_t-1} \sum_{m=0}^{N_t-1-n} \binom{N_t-1}{n} \times \frac{\rho_{SR}^{2(N_t-1-n)} \left(1-\rho_{SR}^2\right)^n}{m!\bar{\gamma}_{SR}^m} x^m e^{\frac{-x}{\bar{\gamma}_{SR}}}. \quad (9)$$

On the other hand, for the instantaneous SNR of the $R \to D$ hop, according to the principles of concomitants or induced order statistics, the CDF of γ_{R^*D} can be derived as in [32]

$$F_{\gamma_{R^*D}}(y) = K_r \sum_{k=0}^{K_r-1} (-1)^k \binom{K_r-1}{k} \frac{1-e^{\frac{-(k+1)y}{\left(k\left(1-\rho_{RD}^2\right)+1\right)\bar{\gamma}_{RD}}}}{k+1}. \quad (10)$$

Thus, the COP of the TBRS strategy is given by

$$P_{\rm co}^{\rm TBRS}(R_0) = \Pr\left[I_D^{\rm TBRS} < R_0\right] = F_{\gamma_D^{\rm TBRS}}\left(\gamma_{th}^D\right) \quad (11)$$

where we have $\gamma_{th}^D = 2^{2R_0} - 1$, and the CDF of $\gamma_D^{\rm TBRS}$ can be calculated as

$$F_{\gamma_D^{\rm TBRS}}(x) = 1 - \int_0^\infty \left[1 - F_{\gamma_{R^*D}}\left(\frac{xz + x(x+1)}{z}\right)\right] f_{\gamma_{SR^*}}(z+x)dz. \quad (12)$$

Consequently, by substituting (8) and (10) into (12) and using [33, eq. (3.471.9)], we arrive at a closed-form expression for $F_{\gamma_D^{\rm TBRS}}(x)$ as

$$F_{\gamma_D^{\rm TBRS}}(x) = 1 - 2\sum_{n=0}^{N_t-1}\sum_{k=0}^{K_r-1}\sum_{m=0}^{N_t-1-n} (-1)^k K_r \binom{N_t-1}{n} \times \binom{K_r-1}{k}\binom{N_t-1-n}{m} \times \frac{\rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n x^{N_t-1-n-m}}{(N_t-1-n)!(k+1)\bar{\gamma}_{SR}^{N_t-n}} \times \left[\frac{\bar{\gamma}_{SR}x(x+1)}{\omega_k\bar{\gamma}_{RD}}\right]^{\frac{m+1}{2}} \times e^{-\left(\frac{\bar{\gamma}_{SR}+\omega_k\bar{\gamma}_{RD}}{\omega_k\bar{\gamma}_{SR}\bar{\gamma}_{RD}}\right)x} K_{m+1}\left(2\sqrt{\frac{x(x+1)}{\omega_k\bar{\gamma}_{SR}\bar{\gamma}_{RD}}}\right) \quad (13)$$

where we have $\omega_k = (k(1-\rho_{RD}^2)+1)/(k+1)$. Then, by substituting $x = \gamma_{th}^D$ into (13), we obtain $P_{\rm co}^{\rm TBRS}$.

Furthermore, the SOP of the TBRS strategy may be expressed as

$$P_{\rm so}^{\rm TBRS}(R_0, R_s) = \Pr\left[I_E^{\rm TBRS} > R_0 - R_s\right] = 1 - F_{\gamma_E^{\rm TBRS}}\left(\gamma_{th}^E\right) \quad (14)$$

where we have $\gamma_{th}^E = 2^{2(R_0-R_s)} - 1$. Similarly, we may calculate the CDF of $\gamma_E^{\rm TBRS}$ in (14) as

$$F_{\gamma_E^{\rm TBRS}}(x) = 1 - 2\sum_{n=0}^{N_t-1}\sum_{m=0}^{N_t-1-n} \binom{N_t-1}{n}\binom{N_t-1-n}{m} \times \frac{\rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n x^{N_t-1-n-m}}{(N_t-1-n)!\bar{\gamma}_{SR}^{N_t-n}} \times \left[\frac{\bar{\gamma}_{SR}x(x+1)}{\bar{\gamma}_{RE}}\right]^{\frac{m+1}{2}} \times e^{-\left(\frac{\bar{\gamma}_{SR}+\bar{\gamma}_{RE}}{\bar{\gamma}_{SR}\bar{\gamma}_{RE}}\right)x} K_{m+1}\left(2\sqrt{\frac{x(x+1)}{\bar{\gamma}_{SR}\bar{\gamma}_{RE}}}\right). \quad (15)$$

Then, by substituting $x = \gamma_{th}^E$ into (15), we can derive $P_{\rm so}^{\rm TBRS}$.

The COP and the SOP in (11) and (14) characterize the attainable reliability and security performance, respectively, and can be regarded as the detailed requirements of accurate system design. From the definition of COP and SOP, it is clear that the reliability of the main link can be improved by increasing the transmit SNR (or decreasing its data rate) to reduce the COP, which unfortunately increases the risk of eavesdropping. Thus, a tradeoff between reliability and security may be struck, despite the fact that closed-from expressions cannot be obtained as in [11]. Furthermore, we denote the minimal reliability and security requirements by υ and δ, where the feasible range of the reliability constraint is $0 < \upsilon < 1$. Bearing in mind that the COP is a monotonously increasing function of R_0, the corresponding threshold of the codeword transmission rate is $R_0^{th} = \arg\{P_{\rm co}^{\rm TBRS}(R_0) = \upsilon\}$, which leads to a lower bound of the SOP, when we have $(R_0 - R_s) \to R_0^{th}$. Thus, the feasible range of δ is $P_{\rm so}^{\rm TBRS}(R_0^{th}, 0) < \delta < 1$. The preceding analysis indicates that, given a reliability constraint υ, the lower bound of the security constraint is determined.

B. Reliability–Security Ratio

Here, we will focus our attention on the asymptotic analysis of the COP and the SOP in the high-SNR regime. Then, inspired by [25], we introduce the concept of the RSR for characterizing the direct relationship between reliability and security.

Proposition 1: Based on the asymptotic probabilities of $P_{\rm co}$ and $P_{\rm so}$ at high SNRs,[3] the RSR is defined as

$$P_{\rm co}(R_0) = \Lambda\left[1 - P_{\rm so}(R_0, R_s)\right] \tag{16}$$

where $\Lambda = \lim_{\eta\to\infty} P_{\rm co}/(1 - P_{\rm so})$, which represents the improvement in COP upon decreasing the SOP. More specifically, since the reduction of the SOP/COP must be followed by an improvement of COP/SOP, a lower Λ implies that, when the security is reduced, the reliability is improved, and *vice versa*. Thus, for the TBRS scheme studied earlier, the RSR is derived as (17), shown at the bottom of the page.

Proof: The proof is given in Appendix B.

Remark 2: It can be seen from the preceding expression that the factor Λ is independent of the transmit SNR, but directly depends on the channel gains, the rate pair (R_0, R_s), and the number of TAs and relays. For a given R_s, reducing R_0 to enhance the reliability may erode the security, because $(R_0 - R_s)$ is also reduced. Conversely, increasing R_0 provides more redundancy for protecting the security of the information, but simultaneously, the reliability is reduced. Hence, the RSR analysis underlines an important point of view concerning how to balance the reliability versus security tradeoff by adjusting (R_0, R_s). Furthermore, as long as a CSI feedback delay exists, the RSR has an intimate relationship with ρ_{SR} and ρ_{RD}. It is clear that the value of $\Lambda^{\rm TBRS}$ decreases as ρ_{RD} increases, which is due to the fact that the relay selection process only improves the reliability of the legitimate user. On the other hand, since we always have the conclusion that $\sum_{k=0}^{K_r-1}(-1)^k\binom{K_r-1}{k}(K_r/(k(1-\rho_{RD}^2)+1)) < 1$, when σ_{RD}^2 and σ_{RE}^2 are comparable, $\Lambda^{\rm TBRS}$ will be reduced as ρ_{SR} increases. This observation implies that, although both $P_{\rm co}$ and $(1 - P_{\rm so})$ are reduced when the first-hop CSI becomes better, the improvement of the reliability is more substantial than the security loss, as ρ_{SR} increases.

[3]Assume equal power allocation between S and the relay, yielding $P_S = P_R = P$, and define $\eta = P/N_0$ as the transmit SNR [24].

C. Effective Secrecy Throughput

It should be noted that the COP and SOP metrics ignore the correlation between these two outage events. More specifically, in contrast to the point-to-point transmission case, since the $S \to R$ link's SNR included in the MI expressions of (3) and (4), the secrecy outage and the connection outage are definitely not independent of each other. Therefore, it might be of limited benefit in evaluating the reliability or the security separately. We note furthermore that, although another metric referred to as the secrecy throughput was introduced as the product of the successful decoding probability and of the secrecy rate [21], [22], this definition ignores the fact that a reliable transmission may be insecure, and the SOP is not taken into consideration. Hence, this metric is unable to holistically characterize the efficiency of our scheme, while capable of achieving both reliable and secure transmission. Therefore, here, we redefine the effective secrecy throughput as the probability of a successful transmission (reliable and secure) multiplied by the secrecy rate, namely, as $\varsigma = R_s P_{R\&S}$, where the RSCP is defined as

$$P_{R\&S} = \Pr\{I_D > R_0, I_E < R_0 - R_s\}. \tag{18}$$

Upon substituting the expressions of I_D and I_E in (3) and (4) into (18), we can rewrite $P_{R\&S}$ for the TBRS strategy in (19), shown at the bottom of the page.

Finally, using the corresponding CDFs and PDFs of (8)–(10) from our previous analysis, we can obtain $P_{R\&S}^{\rm TBRS}$ in (20), shown at the bottom of the next page, as well as the secrecy throughput.

Furthermore, considering the asymptotic result for RSCP at high SNRs in (20) by applying the approximation $K_v(x) \approx (v-1)!/2(x/2)^v$ and closing the highest terms of η after invoking the McLaurin series representation for the exponential function, the asymptotic effective secrecy throughput can be approximated as

Remark 3: Given the definition of COP, SOP, and the secrecy throughput result of (21), shown at the bottom of the next page, it can be shown that, for a fixed R_s, if R_0 is too small, although

$$\Lambda^{\rm TBRS} = \frac{\left[\left(1-\rho_{SR}^2\right)^{N_t-1} + \sum_{k=0}^{K_r-1}(-1)^k\binom{K_r-1}{k}\frac{K_r\sigma_{SR}^2}{\left[k\left(1-\rho_{RD}^2\right)+1\right]\sigma_{RD}^2}\right]\left(2^{2R_0}-1\right)}{\left[N_t\left(1-\rho_{SR}^2\right)^{N_t-1} + \sigma_{SR}^2/\sigma_{RE}^2\right]\left(2^{2(R_0-R_s)}-1\right)} \tag{17}$$

$$\begin{aligned} P_{R\&S}^{\rm TBRS} &= \Pr\left\{\left\{\gamma_{SR} > \gamma_{th}^D, \gamma_{R^*D} > \frac{\gamma_{th}^D\gamma_{SR} + \gamma_{SR}}{\gamma_{SR} - \gamma_{th}^D}\right\} \cap \left[\left\{\gamma_{SR} > \gamma_{th}^E, \gamma_{R^*E} < \frac{\gamma_{th}^E\gamma_{SR} + \gamma_{SR}}{\gamma_{SR} - \gamma_{th}^E}\right\} \cup \left\{\gamma_{SR} < \gamma_{th}^E\right\}\right]\right\} \\ &= \Pr\left\{\gamma_{SR} > \gamma_{th}^D, \gamma_{R^*D} > \gamma_{th}^D + \frac{\gamma_{th}^D\left(\gamma_{th}^D+1\right)}{\gamma_{SR} - \gamma_{th}^D}, \gamma_{R^*E} < \gamma_{th}^E + \frac{\gamma_{th}^E\left(\gamma_{th}^E+1\right)}{\gamma_{SR} - \gamma_{th}^E}\right\} \end{aligned} \tag{19}$$

P_{RS} may be high (i.e., close to 1), the value of ς remains small. By contrast, if R_0 is too large, the value of $P_{\rm co}$ is close to 1, and therefore, ς will also become small. This observation is also suitable for R_s. Thus, as pointed out in the RSR analysis, it is elusive to improve both the reliability and the security simultaneously, but both of them are equally crucial in terms of the effective secrecy throughput, which depends on the rate pair (R_0, R_s).

Additionally, (21) also reveals that increasing the SNR would drastically reduce the effective secrecy throughput. For high transmit SNRs, a high reliability can indeed be perfectly guaranteed, but at the same time, the grade of the security is severely degraded. However, the probability of a reliable and simultaneously secure transmission will tend toward zero. Hence, we may conclude that there exists an optimal SNR, which achieves the maximal secrecy throughput.

In conclusion, adopting the appropriate code rate pair and transmit SNR is crucial for achieving the maximum effective secrecy throughput, which can be formulated as

$$\begin{aligned} &\max_{R_0,R_s,\eta} \varsigma(R_0,R_s) = R_s P_{R\&S}^{\rm TBRS} \\ &\text{s.t. } P_{\rm co} \le \upsilon, P_{\rm so} \le \delta, 0 < R_s < R_0 \end{aligned} \tag{22}$$

where υ and δ denote the system's reliability and security requirements. Unfortunately, it is quite a challenge to find the closed-form optimal solution to this problem due to the complexity of the expressions. Although suboptimal solutions can be found numerically (with the aid of gradient-based search techniques), the secrecy throughput optimization problem and the corresponding complexity analysis and performance comparisons are beyond the scope of this work.

IV. Secure Transmission With Jamming

Here, we consider the extension of the aforementioned relay selection approaches to systems additionally invoking relay-aided jamming. JRJS is based on the outdated but perfectly estimated CSI, and the details have been presented in Section II. We would also like to investigate the security performance from an outage-based perspective. The COP, SOP, RSCP, and effective secrecy throughput will be included.

A. COP and SOP

It is plausible that the main differences between the JRJS and TBRS schemes are determined by the instantaneous SNR of the $R \to D$ hop, where, now, a jammer is included. Based on our preliminary results detailed for the point-to-point SNRs in (8) and (10), we now focus our attention on the statistical analysis of the SNR, including J^*. As stated for the JRJS scheme in Section II, J^* corresponds to the lowest $\tilde{\gamma}_{R_k D}$ and is selected from the set $\{\mathcal{R} - R^*\}$. Recalling that R^* is the best relay of the second hop, we have $\tilde{\gamma}_{J^*D} = \min_{R_k \in \mathcal{R}-R^*}\{\tilde{\gamma}_{R_k D}\} \triangleq \min_{R_k \in \mathcal{R}}\{\tilde{\gamma}_{R_k D}\}$ for $K_r > 1$. Using the induced order statistics, the corresponding CDF of γ_{R^*D} is presented in (10), whereas the PDF of γ_{J^*D} can be formulated as

$$f_{\gamma_{J^*D}}(x) = \frac{K_r \exp\left(\frac{-K_r x}{\left[(K_r-1)\left(1-\rho_{RD}^2\right)+1\right]\bar{\gamma}_{JD}}\right)}{\left[\left(K_r-1\right)\left(1-\rho_{RD}^2\right)+1\right]\bar{\gamma}_{JD}}. \tag{23}$$

Although the relay and jammer selection processes are not entirely disjoint, we may exploit the assumption that γ_{R^*D} and γ_{J^*D} are independent of each other, which is valid when the number of relays is sufficiently high, as justified in [24]. Let us define the signal-to-interference-plus-noise ratio of the second hop as $\xi_D = \gamma_{R^*D}/(\gamma_{J^*D}+1)$, using (10) and (23), whose CDF can be formulated as

$$F_{\xi_D}(x) = 1 - K_r \sum_{k=0}^{K_r-1} (-1)^k \binom{K_r-1}{k} \frac{\varphi_k e^{\frac{-x}{\bar{\gamma}_{RD}\omega_k}}}{(k+1)(x+\varphi_k)} \tag{24}$$

where we have $\varphi_k = \lambda K_r \omega_k / ([(K_r-1)(1-\rho_{RD}^2)+1](1-\lambda))$.

$$\begin{aligned} P_{R\&S}^{\rm TBRS} = &\int_{\gamma_{th}^D}^{\infty} \left[1 - F_{\gamma_{R^*D}}\left(\gamma_{th}^D + \frac{\gamma_{th}^D\left(\gamma_{th}^D+1\right)}{x-\gamma_{th}^D}\right)\right] F_{\gamma_{R^*E}}\left(\gamma_{th}^E + \frac{\gamma_{th}^E\left(\gamma_{th}^E+1\right)}{x-\gamma_{th}^E}\right) f_{\gamma_{SR^*}}(x)dx \\ \approx & 2\sum_{n=0}^{N_t-1}\sum_{k=0}^{K_r-1}\sum_{m=0}^{N_t-1-n} (-1)^k \binom{K_r-1}{k}\binom{N_t-1}{n}\binom{N_t-1-n}{m} \frac{K_r \rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n \left(\gamma_{th}^D\right)^{N_t-1-n-m}}{(N_t-1-n)!(k+1)\bar{\gamma}_{SR}^{N_t-n-(m+1)/2}} \\ & \times \exp\left[-\left(\frac{\gamma_{th}^D}{\bar{\gamma}_{SR}} + \frac{\gamma_{th}^D}{\omega_k\bar{\gamma}_{RD}}\right)\right]\left[\left(\frac{\gamma_{th}^D\left(\gamma_{th}^D+1\right)}{\omega_k\bar{\gamma}_{RD}}\right)^{\frac{m+1}{2}} K_{m+1}\left(2\sqrt{\frac{\gamma_{th}^D\left(\gamma_{th}^D+1\right)}{\omega_k\bar{\gamma}_{SR}\bar{\gamma}_{RD}}}\right)\right. \\ & \left. - \exp\left(\frac{-\gamma_{th}^E}{\bar{\gamma}_{RE}}\right)\left(\frac{\gamma_{th}^D\left(\gamma_{th}^D+1\right)}{\omega_k\bar{\gamma}_{RD}} + \frac{\gamma_{th}^E\left(\gamma_{th}^E+1\right)}{\bar{\gamma}_{RE}+\gamma_{th}^D-\gamma_{th}^E}\right)^{\frac{m+1}{2}} K_{m+1}\left(2\sqrt{\frac{\gamma_{th}^D\left(\gamma_{th}^D+1\right)}{\omega_k\bar{\gamma}_{SR}\bar{\gamma}_{RD}} + \frac{\gamma_{th}^E\left(\gamma_{th}^E+1\right)}{\bar{\gamma}_{SR}\left(\bar{\gamma}_{RE}+\gamma_{th}^D-\gamma_{th}^E\right)}}\right)\right] \end{aligned} \tag{20}$$

$$\varsigma^{\rm TBRS}(R_0,R_s,\eta) = R_s\left\{1 - \left[\frac{N_t\left(1-\rho_{SR}^2\right)^{N_t-1}}{\sigma_{SR}^2} + \sum_{k=0}^{K_r-1}\frac{K_r(-1)^k}{\left[k\left(1-\rho_{RD}^2\right)+1\right]\sigma_{RD}^2}\binom{K_r-1}{k}\right] \times \frac{2^{2R_0}-1}{\eta}\right\}\frac{2^{2(R_0-R_s)}-1}{\sigma_{RE}^2\eta} \tag{21}$$

As far as the eavesdropper is concerned, γ_{R^*E} and γ_{J^*E} are independent and exponentially distributed. Furthermore, for $\xi_E = \gamma_{R^*E}/(\gamma_{J^*E}+1)$, we have

$$F_{\xi_E}(x) = 1 - \frac{\phi}{x+\phi} e^{\frac{-x}{\bar{\gamma}_{RE}}} \tag{25}$$

where $\phi = \lambda/(1-\lambda)$. According to the definition of COP and SOP in Section III-A, we can obtain the following closed-form approximations of the COP and the SOP.[4]

Lemma 1: The COP and the SOP of the JRJS strategy associated with feedback delays are approximated by

$$\begin{aligned} P_{\rm co}^{\rm JRJS}(R_0) \approx 1 - &\sum_{n=0}^{N_t-1}\sum_{k=0}^{K_r-1}\sum_{m=0}^{N_t-1-n}\binom{N_t-1}{n} \\ &\times \binom{K_r-1}{k}\binom{N_t-1-n}{m} \\ &\times \frac{(-1)^k(K_r+1)\rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n}{(N_t-1-n)!(k+1)\bar{\gamma}_{SR}^{N_t-n}} \\ &\times \frac{\Gamma(m+2)\hat{\varphi}_k\left(\gamma_{th}^D\right)^{N_t-n}\left(\gamma_{th}^D+1\right)^{m+1}}{\left(\gamma_{th}^D+\hat{\varphi}_k\right)^{m+2}} \\ &\times \exp\left[-\frac{\gamma_{th}^D(\hat{\varphi}_k-1)}{\bar{\gamma}_{SR}\left(\gamma_{th}^D+\hat{\varphi}_k\right)}\right] \\ &\times \Gamma\left(-m-1, \frac{\gamma_{th}^D\left(\gamma_{th}^D+1\right)}{\bar{\gamma}_{SR}\left(\gamma_{th}^D+\hat{\varphi}_k\right)}\right) \end{aligned} \tag{26}$$

where $\hat{\varphi}_k = K_r\lambda\omega_k\eta\sigma_{RD}^2/([(K_r-1)(1-\rho_{RD}^2)+1](1-\lambda)\eta\sigma_{RD}^2+K_r)$, and

$$\begin{aligned} P_{\rm so}^{\rm JRJS}(R_0,R_s) \approx &\sum_{n=0}^{N_t-1}\sum_{m=0}^{N_t-1-n}\binom{N_t-1}{n} \\ &\times \frac{\rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n}{m!\bar{\gamma}_{SR}^m} \\ &\times \frac{\left(2\gamma_{th}^E\right)^m\phi}{\left(2\gamma_{th}^E+\phi\right)}\exp\left[-\left(\frac{2\gamma_{th}^E}{\bar{\gamma}_{SR}}+\frac{2\gamma_{th}^E}{\bar{\gamma}_{RE}}\right)\right]. \end{aligned} \tag{27}$$

Proof: The proof is given in Appendix B.

The feasible range of the reliability constraint is similar to that of the TBRS strategy, and hence, it is omitted here.

B. Reliability–Security Ratio

Lemma 2: Recalling the definition in Section III, the RSR for the JRJS strategy may be expressed in (28), shown at the bottom of the page.

[4]When we have $\lambda \to 1$, (24) will degenerate into the TBRS case seen in (10). The performance analysis of the JRJS will be presented separately in the following, since several approximations have to be included.

It can be seen from the previous expression that, in contrast to the analysis of the TBRS strategy operating without jamming, for a fixed SNR threshold, the CDF of the second-hop SNR will converge to a nonzero limit. We also find that this limit is determined by the power sharing ratio between the relay and the jammer. Furthermore, according to the analysis of the TBRS strategy, for $\eta \to \infty$, we have $F_{\gamma_{SR^*}}(x) \to 0$. Thus, by exploiting the tight upper bound that $\gamma_D^{\rm TBRS} \le \min\{\gamma_{SR}, \gamma_{R^*D}\}$ and $\gamma_E^{\rm TBRS} \le \min\{\gamma_{SR}, \gamma_{R^*E}\}$, we have $P_{\rm co}^{\rm JRJS,\infty} \to F_{\gamma_{\xi_D}}(\gamma_{th}^D)$ and $1 - P_{\rm so}^{\rm JRJS,\infty} \to F_{\gamma_{\xi_E}}(\gamma_{th}^E)$. Finally, substituting the corresponding results into (16), we arrive at the RSR of the JRJS strategy.

Remark 4: It can be seen from the RSR expression of (28) again that the rate-pair setting (R_0, R_s) has an inconsistent influence on the RSR, and hence, we have to carefully adjust R_0 and R_s to balance the reliability versus security performance. Let us now focus our attention on the differences between the JRJS scheme and the TBRS arrangement.

First, we may find that the power sharing ratio λ between the relay and the jammer plays a very important role. The optimization of λ will be investigated from an effective secrecy throughput optimization point of view in the following.

Second, it is plausible that, in contrast to the behavior of the TBRS strategy, $\Lambda^{\rm JRJS}$ of (28) is only related to the delay of the second hop, but it is still a monotonically decreasing function of ρ_{RD}. This implies that the improvement of the channel quality of the JRJS will achieve a more pronounced COP improvement than the associated SOP improvement. Furthermore, recalling that the RSR is considered in the high-SNR region, it has no dependence on the first hop quality. This is due to the fact that if the first-hop channel quality is sufficiently high for ensuring a successful transmission, the asymptotic CDFs of ξ_D and ξ_E in (29) and (30) associated with $\eta \to \infty$ will converge to a nonzero limit at high SNRs, which ultimately dominates the COP and the SOP. AQ2

C. Effective Secrecy Throughput

Before proceeding to the effective secrecy throughput analysis, we also have to investigate the RSCP.

Lemma 3: The RSCP of our JRJS strategy may be approximated as in (31), shown at the bottom of the next page, where we have $\theta_{1,k} = (\gamma_{th}^D(\gamma_{th}^D+1))/(\gamma_{th}^D+\hat{\varphi}_k)$, $\theta_2 = \gamma_{th}^D - \gamma_{th}^E + (\gamma_{th}^E(\gamma_{th}^E+1)/(\gamma_{th}^E+\hat{\phi}))$, and $\hat{\phi} = \lambda\eta\sigma_{RE}^2/((1-\lambda)\eta\sigma_{RE}^2+1)$.

Proof: The proof is given in Appendix C.

Apart from the rate pair (R_0, R_s), the aforementioned $P_{R\&S}^{\rm JRJS}$ of (31) is also a function of the power sharing ratio λ between the selected relay and the jammer.

Given the complexity of the RSCP expression, it is quite a challenge to find a closed-form result for maximizing the

$$\Lambda^{\rm JRJS} = \frac{(2^{2R_0}-1)}{\left(2^{2(R_0-R_s)}-1\right)}\sum_{k=0}^{K_r-1}\binom{K_r-1}{k}\frac{(-1)^k K_r\left[(K_r-1)\left(1-\rho_{RD}^2\right)+1\right]\left[(\lambda^{-1}-1)\left(2^{2(R_0-R_s)}-1\right)+1\right]}{\left[(K_r-1)\left(1-\rho_{RD}^2\right)+1\right](k+1)(\lambda^{-1}-1)(2^{2R_0}-1)+K_r\left[k\left(1-\rho_{RD}^2\right)+1\right]} \tag{28}$$

effective secrecy throughput that $\max_{0<\lambda<1}\varsigma = R_s P_{R\&S}^{\mathrm{JRJS}}$. Alternatively, we can focus on the asymptotic analysis in the high-SNR region and try to find a general closed-form solution for λ. Specifically, when we have $\eta \to \infty$, $P_{R\&S}^{\mathrm{JRJS}}$ will be dominated by the channel quality of the second hop; hence, we have

$$P_{R\&S}^{\mathrm{JRJS},\infty}(R_0, R_s, \lambda) \approx \Pr\left\{\xi_D > \gamma_{th}^D, \xi_E < \gamma_{th}^E\right\} = \left[1 - F_{\xi_D}\left(\gamma_{th}^D\right)\right] F_{\xi_E}\left(\gamma_{th}^E\right) \quad (32)$$

where the approximation is based on the fact that, in contrast to both $F_{\xi_D}(\gamma_{th}^D)$ and $F_{\xi_E}(\gamma_{th}^E)$, which converge to a nonzero limit regardless of η, the first hop's $F_{\gamma_{SR}}(x)$ will tend to zero, and hence, it can be neglected. Substituting the asymptotic results of (29) and (30) into (33), we can obtain $P_{R\&S}^{\mathrm{JRJS},\infty}$. In contrast to the TBRS case operating without jamming, as the SNR tends to ∞, the RSCP will tend to a nonzero value and, upon increasing the transmit SNR beyond a certain limit, will no longer increase the effective secrecy throughput.

Then, based on (32), we arrive at the approximated optimal value λ_{opt}, which is the solution of the following equation:

$$\frac{\partial P_{R\&S}^{\mathrm{JRJS},\infty}(R_0, R_s, \lambda)}{\partial \lambda} = 0. \quad (33)$$

Then, by exploiting the approximation of $[k(1-\rho_{RD}^2)+1]/(k+1) \approx 1-\rho_{RD}^2$ in (29) for a large ρ_{RD} (practically, the CSI delay is small, and $\rho_{RD} \to 1$), we have

$$\lambda_{\mathrm{subopt}} = \frac{\sqrt{\left[(K_r-1)\left(1-\rho_{RD}^2\right)+1\right]\gamma_{th}}}{\sqrt{\left[(K_r-1)\left(1-\rho_{RD}^2\right)+1\right]\gamma_{th}} + \sqrt{K_r\left(1-\rho_{RD}^2\right)}} \quad (34)$$

where $\gamma_{th} = (2^{2R_0}-1)(2^{2(R_0-R_s)}-1)$. It is clear that this value is determined by the number of relays and (R_0, R_s).

V. Numerical Results

Both our numerical and Monte Carlo simulation results are presented here for verifying the theoretical PLS performance analysis of the multiple-relay-aided network under CSI feedback delays. Explicitly, the COP, SOP, RSCP, and RSR are validated for both the TBRS and JRJS strategies. Furthermore, the effects of feedback delays and system parameters (including the transmission rate pair (R_0, R_s) and the power sharing ratio λ between the relay and the jammer) on the achievable effective secrecy throughput are evaluated. The Rayleigh fading model is employed for characterizing all communication links in our system. Additionally, we set the total power to $P = 1$ and $\sigma_{SR}^2 = \sigma_{RD}^2 = \sigma_{RE}^2 = 1$, and used $T_{d_{SR}} = T_{d_{RD}} = T_d$.

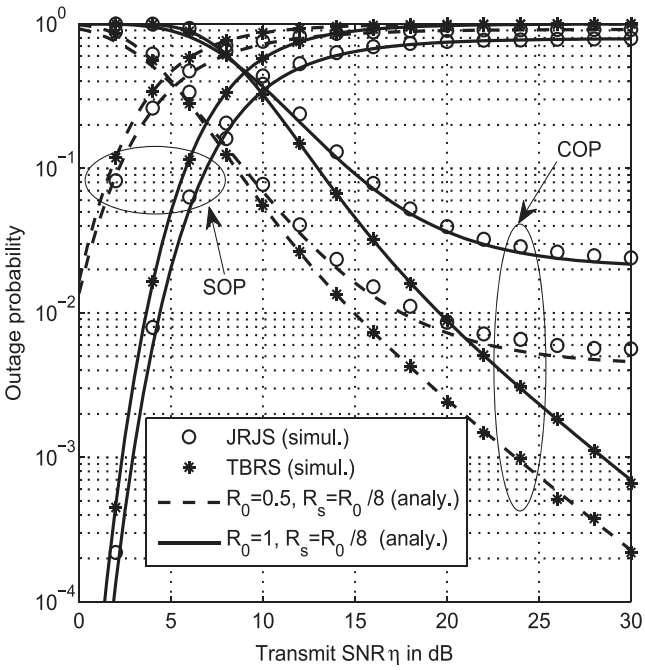

Fig. 2. COP and SOP versus transmit SNR for the TBRS and JRJS strategies in conjunction with different rate pairs, for $N_t = K_r = 3$, $f_d T_d = 0.1$, and $\lambda = 1/10$.

Fig. 2 plots the COP and the SOP versus the transmit SNR for both the TBRS and JRJS strategies in conjunction with different rate pairs. The analytical lines are plotted by using (11) and (14) for the TBRS strategy and by using (26) and (27) for the JRJS

$$P_{R\&S}^{\mathrm{JRJS}}(R_0, R_s, \lambda) \approx \sum_{n=0}^{N_t-1}\sum_{k=0}^{K_r-1}\sum_{m=0}^{N_t-1-n}(-1)^k \binom{N_t-1}{n}\binom{K_r-1}{k}\binom{N_t-1-n}{m} \times \frac{K_r \rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n \hat{\varphi}_k \left(\gamma_{th}^D\right)^{N_t-1-n-m}}{(N_t-1-n)!(k+1)\bar{\gamma}_{SR}^{N_t-n}\left(\gamma_{th}^D+\hat{\varphi}_k\right) e^{\frac{\gamma_{th}^D}{\bar{\gamma}_{SR}}+\frac{\gamma_{th}^D}{\bar{\gamma}_{RD}\omega_k}}} \times \left\{\theta_{1,k}^{m+1} e^{\frac{\theta_1}{\bar{\gamma}_{SR}}}\Gamma(m+2)\Gamma\left(-m-1, \frac{\theta_{1,k}}{\bar{\gamma}_{SR}}\right) - \frac{\hat{\phi}e^{-\gamma_{th}^E/\bar{\gamma}_{RE}}}{\left(\gamma_{th}^E+\phi\right)\left(\theta_{1,k}-\theta_2\right)}\Gamma(m+3) \times \left[\theta_2^{m+2} e^{\frac{\theta_2}{\bar{\gamma}_{SR}}}\Gamma\left(-m-2, \frac{\theta_2}{\bar{\gamma}_{SR}}\right) - \theta_{1,k}^{m+2} e^{\frac{\theta_1}{\bar{\gamma}_{SR}}}\Gamma\left(-m-2, \frac{\theta_{1,k}}{\bar{\gamma}_{SR}}\right)\right] + \Gamma(m+2)\left(\gamma_{th}^D-\gamma_{th}^E\right) \times \left[\theta_2^{m+1} e^{\frac{\theta_2}{\bar{\gamma}_{SR}}}\Gamma\left(-m-1, \frac{\theta_2}{\bar{\gamma}_{SR}}\right) - \theta_{1,k}^{m+1} e^{\frac{\theta_1}{\bar{\gamma}_{SR}}}\Gamma\left(-m-1, \frac{\theta_{1,k}}{\bar{\gamma}_{SR}}\right)\right]\right\} \quad (31)$$

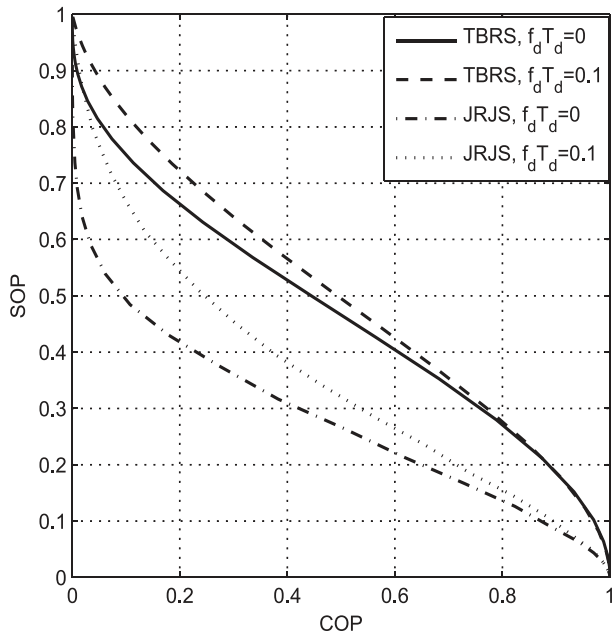

Fig. 3. SOP versus COP for the TBRS and JRJS strategies with different feedback delays for $N_t = K_r = 3$, $R_s = R_0/8$, and $\lambda = 1/10$.

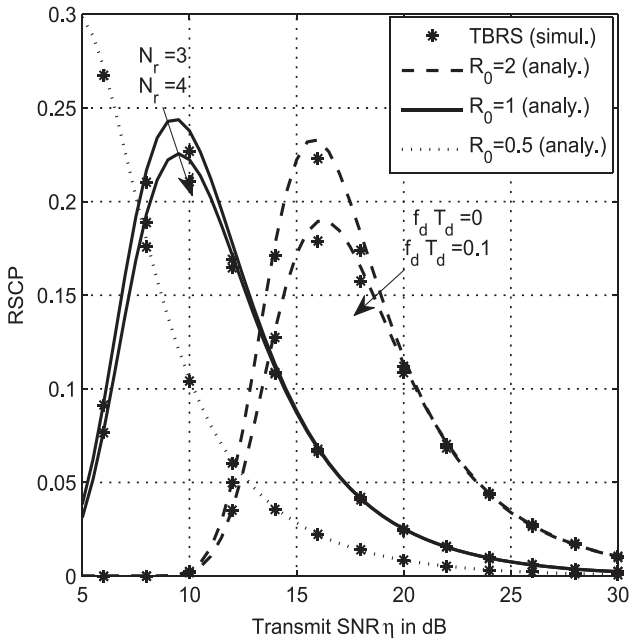

Fig. 4. RSCP versus transmit SNR for the TBRS strategy with different rate pairs for $N_t = K_r = 3$, $f_d T_d = 0.1$.

case, respectively. It can be clearly seen from the figure that the analytical and simulated outage probability curves match well, which confirms the accuracy of the mathematical analysis. As expected, compared with the TBRS strategy, the SOP of the JRJS strategy is much better, whereas the COP is worse. We can also find that both the COP and the SOP will converge to an outage floor at high SNRs for the JRJS strategy. The reason for this is that the jammer also imposes interference on the destination and the interference inflicted increases with the SNR. Thus, the designers have to take into account the tradeoff between the reliability and the security and the interference imposed on D, particularly when considering the JRJS strategy. Moreover, we can observe in Fig. 2 that increasing the transmission rate decreases the COP and increases the SOP.

Fig. 3 further characterizes the SOP versus COP for both the TBRS and JRJS strategies based on the numerical results in Fig. 2, which shows the tradeoff between the reliability and the security. It can be seen from the figure that the SOP decreases as the COP increases, and for a specific COP, the SOP of the JRJS scheme is strictly lower than that of TBRS. This confirms that the JRJS scheme performs better than the conventional TBRS scheme. Furthermore, the CSI feedback delay will also degrade the system tradeoff performance.

Fig. 4 illustrates the RSCP versus transmit SNR for the TBRS strategy in the context of different network configurations, including different rate pairs, different number of relays, and both perfect and outdated CSI feedback scenarios. The analytical lines are plotted by using the approximation in (20). We may conclude from the figure that the rate-pair setting (R_0, R_s) determines both the reliability and security transmission performance. These curves also show that the RSCP is a concave function of the transmit SNR, whereas the continued boosting of the SNR would only decrease the probability of a successful transmission. We can observe from Fig. 4 that,

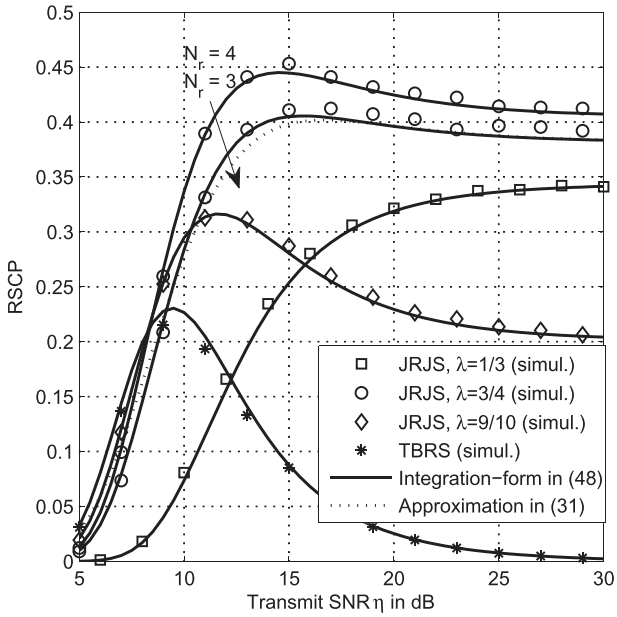

Fig. 5. RSCP versus transmit SNR for the JRJS strategy for different power sharing ratios λ and for $N_t = K_r = 3$, $f_d T_d = 0.1$, and $R_0 = 1$, $R_s = R_0/8$.

for a high transmit SNR, total reliability can be guaranteed, whereas the associated grade of security is severely eroded. Furthermore, increasing the number of relays and decreasing the feedback delay will improve both the reliability and security performance.

The RSCP of the JRJS strategy is presented in Fig. 5 for different power sharing ratios between relaying and jamming. Both the integration form (45) and the approximated closed form in (31) match well with the Monte Carlo simulations. The performance of the TBRS strategy is also included for comparison. The JRJS scheme outperforms the TBRS operating

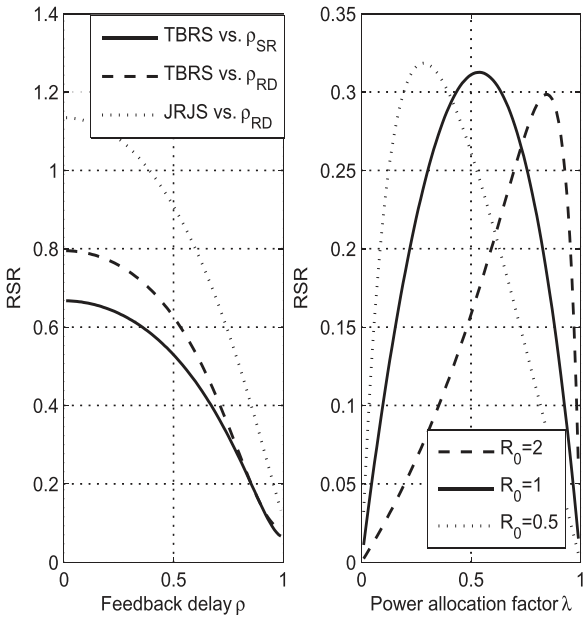

Fig. 6. RSR versus feedback delay coefficient ($R_0 = 1$, $R_s = R_0/8$, $\lambda = 3/4$) and power sharing ratio λ ($R_s = R_0/8$, $\rho_{SR} = \rho_{RD} = 0.9$) for the TBRS and JRJS strategies, with $N_t = K_r = 3$.

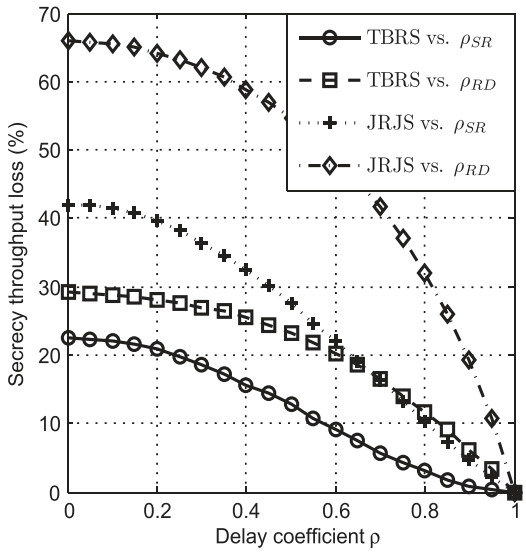

Fig. 7. Percentage secrecy throughput loss versus delay coefficients with $N_t = K_r = 3$, $R_0 = 1$, $R_s = R_0/8$, $\lambda = 3/4$, and $\eta = 10$ dB.

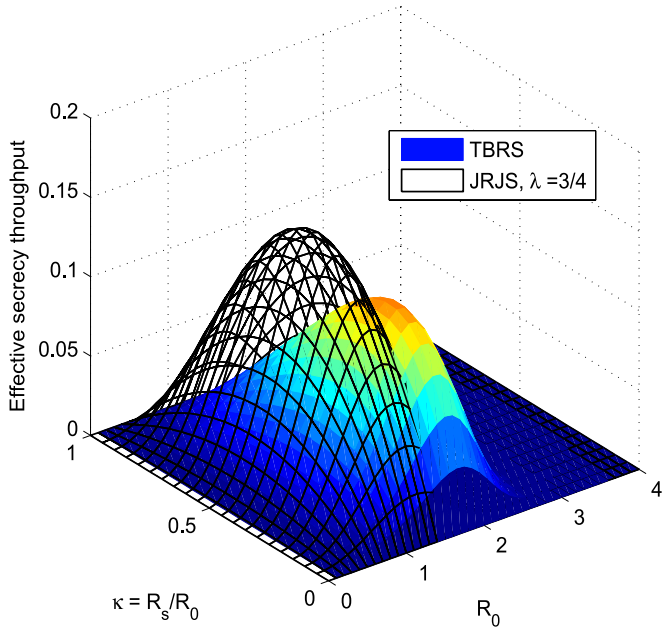

Fig. 8. Secrecy throughput versus R_0 and $\kappa = R_s/R_0$ for both the TBRS and JRJS strategies with $N_t = K_r = 3$, $f_d T_d = 0.1$, and $\eta = 15$ dB.

without jamming under the scenario considered when encountering comparable relay–destination and relay–eavesdropper channels. For some extreme configurations (when the relay–eavesdropper links are comparatively weak), this statement may not hold, but this scenario is beyond the scope of this paper. The maximum RSCP appears at about $\eta = 15$ dB for the JRJS strategy using $\lambda = 3/4$, whereas it is $\eta = 10$ dB for the TBRS strategy. Furthermore, as expected, increasing the number of available relays and jamming nodes will always be able to improve the reliability and security performance. However, the continued boosting of the jammer's power (decreasing λ) will not always improve the overall performance, because the interference improves initially the security, but then, it starts to reduce the reliability as λ decreases. This further motivates the designer to carefully take into account the power sharing between relaying and jamming. The effect of the rate-pair setting on the security and reliability of the JRJS strategy is neglected here, which follows a similar trend to that of the TBRS strategy.

Fig. 6 characterizes the RSR versus feedback delay and power sharing ratio for both TBRS and JRJS, in which the RSR curves are plotted by using (17) and (28), respectively. The first illustration shows that the RSR decreases as the delay coefficients (ρ_{SR} and ρ_{RD}), which confirms that the improvement of reliability becomes more pronounced than the reduction of the security as the feedback delay decreases. This observation implies an improvement in terms of the security–reliability tradeoff. In addition, the RSR versus ρ_{RD} is larger than that of ρ_{SR}, which indicates that the impact of the second-hop CSI feedback delay is more prominent. The other illustration in the right demonstrates that the RSR is a concave function of the power sharing ratio, which reflects the tradeoff between the reliability and the security struck by adjusting λ.

To further evaluate the effect of feedback delays on the secrecy performance, Fig. 7 plots the resultant percentage of secrecy throughput loss versus the delay, which is defined as

$$\varsigma_{\text{loss}} = \frac{\varsigma_{\text{no-delay}} - \varsigma_{\text{delay}}}{\varsigma_{\text{no-delay}}}. \tag{35}$$

It can be seen from the figure that, compared with the TBRS scheme, JRJS is more sensitive to the feedback delays. Furthermore, recalling that increasing the delay coefficient ρ_{SR} of the first hop improves the reliability, but at the same time also helps the eavesdropper, it is not surprising that the secrecy throughput loss due to the second-hop feedback delay is more pronounced.

Fig. 8 illustrates the achievable effective secrecy throughput for both the TBRS and JRJS strategies versus the codeword

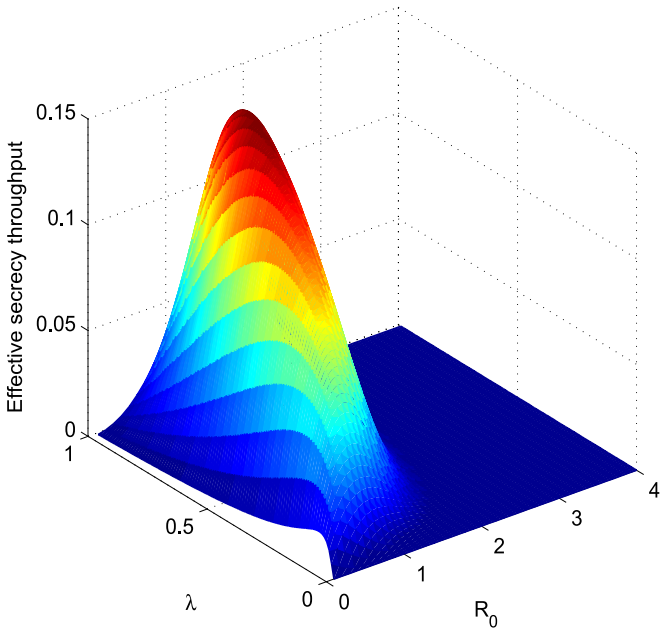

Fig. 9. Secrecy throughput versus R_0 and λ for the JRJS strategy with $N_t = K_r = 3$, $f_d T_d = 0.1$, $\eta = 15$ dB, and $R_s/R_0 = 1/8$.

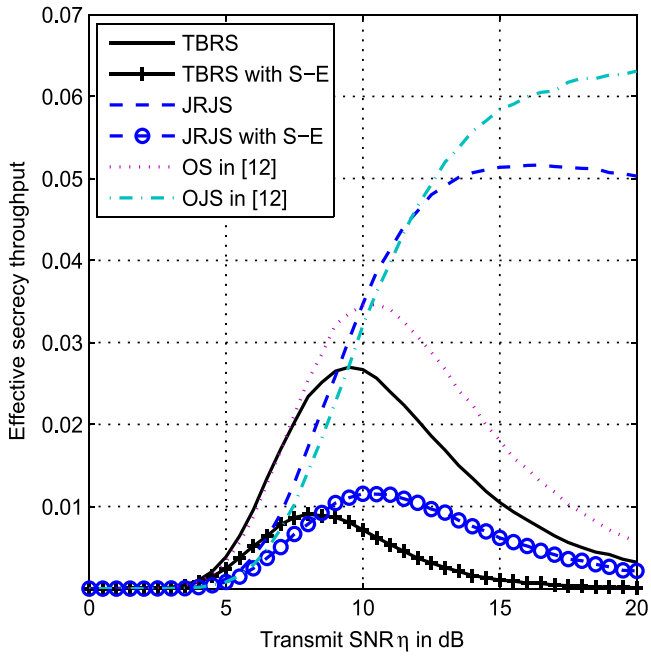

Fig. 10. Comparisons for different strategies with and without the S–E link, for $N_t = K_r = 3$, $R_0 = 1$, $R_s = R_0/8$, $f_d T_d = 0.1$, and $\lambda = 3/4$.

transmission rate R_0 and the secrecy code ratio $\kappa = R_s/R_0$ with no outage constraints ($\upsilon = \delta = 1$). The values of the effective secrecy throughput are plotted by using $\varsigma = R_s P_{R\&S}$. We can observe in Fig. 8 that, subject to a fixed code rate ratio κ, the effective secrecy throughput increases to a peak value as R_0 reaches its optimal value and then decreases. This phenomenon can be explained as follows. At a low transmission rate, although the COP increases with R_0, which has a negative effect on the effective secrecy throughput, both the secrecy rate and the SOP performance will benefit. However, after reaching the optimal R_0, the effective secrecy throughput drops since the main link cannot afford a reliable transmission, and the resultant COP increase becomes dominant. On the other hand, subject to a fixed R_0 (which results in a constant COP), the effective secrecy throughput is also a concave function of κ, and increasing the code rate ratio ultimately results in an increased secrecy information rate at the cost of an increased SOP.

The achievable effective secrecy throughput for the JRJS strategy is also presented in Fig. 8, and similar conclusions and trends can be observed to that of the TBRS case. Additionally, the comparison of the two strategies indicates that the JRJS scheme attains a higher effective secrecy throughput than the TBRS scheme operating without jamming, even if no power sharing optimization has been employed.

Fig. 9 further illustrates the impact of power sharing between the relay and the jammer on the achievable effective secrecy throughput of the JRJS strategy versus R_0 in the absence of outage constraints. Given a fixed code rate pair (R_0, R_s), the effective secrecy throughput follows the trend of the RSCP, which is a concave function of λ, as shown in Fig. 6. The interference introduced by the jammer initially improves both the reliability and the security as λ increases, but this trend is reversed beyond a certain point.

VI. Discussion

A. Impact of the S–E Link

We note that the introduction of the S–E link, i.e., the information leakage in the first phase, is very critical to the security. There are also some research studies focusing on the corresponding secure transmission design and performance evaluation for cooperative networks with the S–E link, such as [15] and [16]. Here, we assume that the eavesdropper can receive information directly from the source in the first phase. Thus, following the steps in the prior sections, for the TBRS and JRJS schemes, it is clear that the SNR experienced at the eavesdropper should be rewritten as

$$\tilde{\gamma}_E^{\tau} = \gamma_{SE} + \gamma_E^{\tau} \tag{36}$$

where $\gamma_{SE} = P_s |\mathbf{w}_{\text{opt}}(t|T_{d_{SR}}) \mathbf{h}_{SE}(t)|^2 / N_0$ follows the exponential distribution with the average value $\bar{\gamma}_{SE}$, $\tau = \{\text{TBRS}, \text{JRJS}\}$, and γ_E^{τ} has been defined in (4) and (7).

Then, the corresponding SOP, RSCP, and effective secrecy throughput have to be reconsidered. Unfortunately, to the best of our knowledge, it is a mathematically intractable problem to obtain closed-form results for the related performance evaluations. Therefore, we resorted to numerical simulations for further investigating the impact of the S–E link. Fig. 10 compares the effective secrecy throughput of the TBRS and JRJS schemes both with and without considering the direct S–E link. It becomes clear that the information leakage in the first phase will lead to a severe security performance degradation, particularly for the JRJS scheme, which will no longer be capable of maintaining a steady throughput at high SNRs. The reason for this trend is that increasing the transmit SNR will help the eavesdropper in the presence of the direct S–E link.

B. Comparisons

Here, based on the outdated CSI assumption, we provide performance comparisons with a range of other schemes advocated in [12] with the aid of the proposed outage-based characterization. Fig. 10 also incorporates our effective secrecy throughput performance comparison, where the optimal selection (OS) regime and the optimal selection combined with jamming (OSJ) were proposed in [12]. They are formulated as

$$\text{OS}: R^* = \arg\max_{R_k \in \mathcal{R}} \left\{ \frac{\tilde{\gamma}_{R_k D}}{\tilde{\gamma}_{R_k E}} \right\} \tag{37}$$

$$\text{OSJ}: \begin{cases} R^* = \arg\max_{R_k \in \mathcal{R}} \left\{ \frac{\tilde{\gamma}_{R_k D}}{\tilde{\gamma}_{R_k E}} \right\} \\ J^* = \arg\min_{R_k \in \mathcal{R}-R^*} \left\{ \frac{\tilde{\gamma}_{R_k D}}{\tilde{\gamma}_{R_k E}} \right\} \end{cases} \tag{38}$$

where $\tilde{\gamma}_{R_k E}$ is the delayed version of the instantaneous CSI of the R–E link. It should be noted that this constitutes an entirely new performance characterization of these schemes from the perspective of the effective secrecy throughput. It is shown in Fig. 1 that the selection combined with jamming outperforms the corresponding nonjamming techniques at high SNRs, albeit this trend may no longer prevail at low SNRs. In comparison, compared with those selections relying on the average SNRs of the R–E link, the optimal selections relying on the idealized simplifying assumptions of having global CSI (OS and OSJ schemes) knowledge can only achieve throughput gains at high SNRs due to the inevitable feedback delay.

VII. Conclusion

An outage-based characterization of cooperative relay networks has been provided in the face of CSI feedback delays. Two types of relaying strategies were considered, namely, the TBRS strategy and the JRJS strategy. Closed-form expressions of the COP, the SOP, and the RSCP, as well as of the RSR, were derived. The RSR results demonstrated that the reliability is improved more substantially than the security performance when the CSI feedback delays are reduced. Furthermore, we presented a modified effective secrecy throughput definition and demonstrated that the JRJS strategy achieves a significant effective secrecy throughput gain over the TBRS strategy. The transmit SNR, the secrecy codeword rate setting, and the power sharing ratio between the relay and jammer nodes play important roles in striking a balance between the reliability and the security in terms of the secrecy throughput. The impact of the direct S–E link and the performance comparisons with other selection schemes were also included. Additionally, our results demonstrate that JRJS is more sensitive to the feedback delays and that the secrecy throughput loss due to the second-hop feedback delay is more pronounced than that due to the first-hop one.

Appendix A
Proof of Proposition 1

To simplify the asymptotic performance analysis, (3) can be expressed in a more mathematically tractable form by the commonly used tight upper bound of $\gamma_D^{\text{TBRS}} \leq \min\{\gamma_{SR}, \gamma_{R^*D}\}$ and $\gamma_E^{\text{TBRS}} \leq \min\{\gamma_{SR}, \gamma_{R^*E}\}$. When we have $\eta \to \infty$, based on the CDFs in (9) and (10) and closing the smallest order terms of x/η, we have

$$\begin{aligned} F_{\gamma_{SR}}(x) \to & 1 - \left[\sum_{n=0}^{N_t-1} \binom{N_t-1}{n} \rho_{SR}^{2(N_t-1-n)} \left(1-\rho_{SR}^2\right)^n \right. \\ & + \sum_{n=0}^{N_t-2} \binom{N_t-1}{n} \times \rho_{SR}^{2(N_t-1-n)} \\ & \left. \times \left(1-\rho_{SR}^2\right)^n \frac{x}{\bar{\gamma}_{SR}} + \mathcal{O}\left(\frac{x}{\bar{\gamma}_{SR}}\right) \right] \\ & \times \left[1 - \frac{x}{\bar{\gamma}_{SR}} + \mathcal{O}\left(\frac{x}{\bar{\gamma}_{SR}}\right) \right] \\ = & 1 - \left[1 + \left(1 - \left(1-\rho_{SR}^2\right)^{N_t-1} \right) \frac{x}{\bar{\gamma}_{SR}} + \mathcal{O}\left(\frac{x}{\bar{\gamma}_{SR}}\right) \right] \\ & \times \left[1 - \frac{x}{\bar{\gamma}_{SR}} + \mathcal{O}\left(\frac{x}{\bar{\gamma}_{SR}}\right) \right] \\ = & \left(1-\rho_{SR}^2\right)^{N_t-1} \frac{x}{\bar{\gamma}_{SR}} + \mathcal{O}\left(\frac{x}{\bar{\gamma}_{SR}}\right) \end{aligned} \tag{39}$$

where $\mathcal{O}(x)$ denotes the high-order infinitely small contributions as a function of x, and

$$\begin{aligned} F_{\gamma_{R^*D}}(x) \to & 1 - \sum_{k=0}^{K_r-1} (-1)^k \frac{K_r}{k+1} \binom{K_r-1}{k} \\ & \times \left[1 - \frac{k+1}{k\left(1-\rho_{RD}^2\right)+1} \frac{x}{\bar{\gamma}_{RD}} + \mathcal{O}\left(\frac{x}{\bar{\gamma}_{RD}}\right) \right] \\ = & \sum_{k=0}^{K_r-1} (-1)^k \binom{K_r-1}{k} \frac{K_r}{k\left(1-\rho_{RD}^2\right)+1} \\ & \times \frac{x}{\bar{\gamma}_{RD}} + \mathcal{O}\left(\frac{x}{\bar{\gamma}_{RD}}\right). \end{aligned} \tag{40}$$

Then, applying the upper bound of the receiver SNR, we may rewrite the COP and the SOP of the TBRS strategy at high SNRs as

$$\begin{aligned} P_{\text{co}}^{\text{TBRS},\infty} = & 1 - \left(1 - F_{\gamma_{SR^*}}\left(\gamma_{th}^D\right)\right)\left(1 - F_{\gamma_{R^*D}}\left(\gamma_{th}^D\right)\right) \\ = & \left[\frac{\left(1-\rho_{SR}^2\right)^{N_t-1}}{\sigma_{SR}^2} + \sum_{k=0}^{K_r-1} (-1)^k \right. \\ & \left. \times \binom{K_r-1}{k} \frac{K_r}{\left[k\left(1-\rho_{RD}^2\right)+1\right]\sigma_{RD}^2} \right] \frac{2^{2R_0}-1}{\eta} \end{aligned} \tag{41}$$

and according to the fact that γ_{R^*E} is exponentially distributed, we have

$$\begin{aligned} 1 - P_{\text{so}}^{\text{TBRS},\infty} = & 1 - \left(1 - F_{\gamma_{SR^*}}\left(\gamma_{th}^E\right)\right)\left(1 - F_{\gamma_{R^*E}}\left(\gamma_{th}^E\right)\right) \\ = & \left[\frac{\left(1-\rho_{SR}^2\right)^{N_t-1}}{\sigma_{SR}^2} + \frac{1}{\sigma_{RE}^2} \right] \frac{2^{2(R_0-R_s)}-1}{\eta}. \end{aligned} \tag{42}$$

Finally, substituting (41) and (42) into the definition of RSR in (16), we can obtain (17).

APPENDIX B
PROOF OF LEMMA 1

According to the description of COP and SOP, replacing $F_{\gamma_{R^*D}}(x)$ and $F_{\gamma_{R^*E}}(x)$ by $F_{\xi_D}(x)$ and $F_{\xi_E}(x)$ in (12) and (14) will involve a mathematically intractable integration of the form

$$\Upsilon(a,b,\mu,\nu)=\int_0^\infty \frac{z^a}{z+b}\exp\left(-\mu z-\frac{\nu}{z}\right)dz \tag{43}$$

which, to the best of our knowledge, does not have a closed-form solution. Alternatively, bearing in mind that the preceding integration has a great matter with ξ_D, we now focus our attention on the approximation of ξ_D. Based on the PDF results in (23), it may be seen that γ_{J^*D} obeys an exponential distribution. Then, we can approximate $\hat{\gamma}_{J^*D}=\gamma_{J^*D}+1$ by the exponential distribution as well, with an average value of $\mathbb{E}\{\hat{\gamma}_{J^*D}\}=([(K_r-1)(1-\rho_{RD}^2)+1]\bar{\gamma}_{RD}+K_r)/K_r$ by assuming that the AWGN term "1" is part of the stochastic mean terms. The approximation based on this method provides a very accurate analysis, and the accuracy of this method is verified by the numerical results of [34]. Thus, the CDF of $\hat{\xi}_D=\gamma_{R^*D}/\hat{\gamma}_{J^*D}$ can be derived as

$$F_{\hat{\xi}_D}(x)=\sum_{k=0}^{K_r-1}(-1)^k\binom{K_r-1}{k}\frac{K_r}{k+1}\frac{x}{x+\hat{\varphi}_k} \tag{44}$$

where $\hat{\varphi}_k=\mathbb{E}\{\gamma_{R^*D}\}\mathbb{E}/\{\hat{\gamma}_{J^*D}\}$.

Then, substituting (44) into (11), we have

$$\begin{aligned}F_{\gamma_D^{\mathrm{JRJS}}}(x)&\approx\sum_{n=0}^{N_t-1}\sum_{k=0}^{K_r-1}\sum_{m=0}^{N_t-1-n}\binom{N_t-1}{n}\binom{K_r-1}{k}\binom{N_t-1-n}{m}\\&\times\frac{(-1)^kK_r\rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n\varphi_kx^{N_t-1-n-m}e^{-\frac{x}{\bar{\gamma}_{SR}}}}{(N_t-1-n)!(k+1)\bar{\gamma}_{SR}^{N_t-n}(x+\varphi_k)}\\&\times\int_0^\infty\frac{z^{m+1}}{z+\frac{x(x+1)}{x+\varphi_k}}\exp\left(-\frac{z}{\bar{\gamma}_{SR}}\right)dz.\end{aligned} \tag{45}$$

Using [33, eq. (3.383.10)], we can obtain the CDF of γ_D^{JRJS} as

$$\begin{aligned}F_{\gamma_D^{\mathrm{JRJS}}}(x)\approx1-&\sum_{n=0}^{N_t-1}\sum_{k=0}^{K_r-1}\sum_{m=0}^{N_t-1-n}\binom{N_t-1}{n}\\&\times\binom{K_r-1}{k}\binom{N_t-1-n}{m}\\&\times\frac{(-1)^k(K_r+1)\rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n}{(N_t-1-n)!(k+1)\bar{\gamma}_{SR}^{N_t-n}}\\&\times\frac{\Gamma(m+2)\hat{\varphi}_kx^{N_t-n}(x+1)^{m+1}}{(x+\hat{\varphi}_k)^{m+2}}\\&\times\exp\left[-\frac{x(\hat{\varphi}_k-1)}{\bar{\gamma}_{SR}(x+\hat{\varphi}_k)}\right]\\&\times\Gamma\left(-m-1,\frac{x(x+1)}{\bar{\gamma}_{SR}(x+\hat{\varphi}_k)}\right).\end{aligned} \tag{46}$$

Finally, substituting $x=\gamma_{th}^D$ into (46), we obtain $P_{\mathrm{co}}^{\mathrm{JRJS}}$.

As far as the SOP is considered, we exploit the commonly used tight upper bound of $\gamma_E^{\mathrm{JRJS}}\geq(1/2)\min\{\gamma_{SR},\xi_E\}$ to calculate it, which may be rewritten as

$$\begin{aligned}P_{\mathrm{so}}^{\mathrm{JRJS}}&\approx\Pr\left\{\frac{1}{2}\min\{\gamma_{SR},\xi_E\}>\gamma_{th}^E\right\}\\&=\left[1-F_{\gamma_{SR}}\left(2\gamma_{th}^E\right)\right]\left[1-F_{\xi_E}\left(2\gamma_{th}^E\right)\right].\end{aligned} \tag{47}$$

Substituting (9) and (25) into (47), we obtain $P_{\mathrm{so}}^{\mathrm{JRJS}}$.

APPENDIX C
PROOF OF LEMMA 3

According to the definition of the RSCP in (18), we can calculate it by

$$\begin{aligned}P_{RS}^{\mathrm{JRJS}}=&\int_0^\infty\left[1-F_{\xi_D}\left(\gamma_{th}^D+\frac{\gamma_{th}^D\left(\gamma_{th}^D+1\right)}{z}\right)\right]\\&\times F_{\xi_E}\left(\gamma_{th}^E+\frac{\gamma_{th}^E\left(\gamma_{th}^E+1\right)}{z+\gamma_{th}^D-\gamma_{th}^E}\right)f_{\gamma_{SR^*}}\left(z+\gamma_{th}^D\right)dz.\end{aligned} \tag{48}$$

To make the integration mathematically tractable, we invoke a simple approximation for $F_{\xi_E}(x)$ by treating the AWGN term "1" in $\xi_E=\gamma_{R^*E}/(\gamma_{J^*E}+1)$ as part of the stochastic mean terms. Hence, we have

$$F_{\xi_E}(x)=\frac{x}{x+\hat{\phi}} \tag{49}$$

where $\hat{\phi}=\lambda\eta\sigma_{RE}^2/((1-\lambda)\eta\sigma_{RE}^2+1)$.

Then, replacing the corresponding CDFs of the second hop with $F_{\hat{\xi}_D}(x)$ and $F_{\hat{\xi}_E}(x)$ in (26), the integration can be derived as

$$\begin{aligned}P_{RS}^{\mathrm{JRJS}}\approx1-&\sum_{n=0}^{N_t-1}\sum_{k=0}^{K_r-1}\sum_{m=0}^{N_t-1-n}(-1)^k\binom{N_t-1}{n}\\&\times\binom{K_r-1}{k}\binom{N_t-1-n}{m}\\&\times\frac{(K_r+1)\rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n}{(N_t-1-n)!(k+1)\bar{\gamma}_{SR}^{N_t-n}}\\&\times\frac{\hat{\varphi}_k\left(\gamma_{th}^D\right)^{N_t-1-n-m}}{\gamma_{th}^D+\hat{\varphi}_k}\exp\left(-\frac{\gamma_{th}^D}{\bar{\gamma}_{SR}}-\frac{\gamma_{th}^D}{\omega_k\bar{\gamma}_{RD}}\right)\\&\times\int_0^\infty e^{\frac{-z}{\bar{\gamma}_{SR}}}z^{m+1}\Bigg[\frac{1}{z+\theta_{1,k}}-\frac{\hat{\phi}\left(z+\gamma_{th}^D-\gamma_{th}^E\right)e^{\frac{-\gamma_{th}^E}{\bar{\gamma}_{RE}}}}{\left(\gamma_{th}^E+\hat{\phi}\right)(\theta_{1,k}-\theta_2)}\\&\times\left(\frac{1}{z+\theta_2}-\frac{1}{z+\theta_{1,k}}\right)\Bigg]dz\end{aligned} \tag{50}$$

where $\hat{\varphi}_k$ and $\hat{\phi}$ are introduced by relying on the similar approximation as in Appendix B. Then, using [33, eq. (3.383.10)], we obtain $P_{R\&S}^{\mathrm{JRJS}}$.

REFERENCES

[1] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, Sep. 1998.

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

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[4] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[5] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[6] Y. W. P. Hong, P. C. Lan, and C. C. J. Kuo, "Enhancing physical-layer secrecy in multi-antenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.

[7] R. Bassily *et al.*, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[8] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[9] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[10] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[11] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2653–2661, Jul. 2014.

[12] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[13] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensic Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[14] Z. Ding, M. Xu, J. Lu, and F. Liu, "Improving wireless security for bidirectional communication scenarios," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2842–2848, Jul. 2012.

[15] C. Wang, H. M. Wang, and X. G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589–605, Feb. 2015.

[16] H. Deng, H. M. Wang, W. Guo, and W. Wang, "Secrecy transmission with a helper: To relay or to jam," *IEEE Trans. Inf. Forensic Security*, vol. 10, no. 2, pp. 293–307, Feb. 2015.

[17] B. He, X. Zhou, and T. D. Abhayapala, "Wireless physical layer security with imperfect channel state information: A survey," *ZTE Commun.*, vol. 11, no. 3, pp. 11–19, Sep. 2013.

[18] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[19] J. Zhang and M. C. Gursoy, "Relay beamforming strategies for physical-layer security," in *Proc. CISS*, Princeton, NJ, USA, Mar. 2010, pp. 1–6.

[20] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[21] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[22] J. Hu, Y. Cai, N. Yang, and W. Yang, "A new secure transmission scheme with outdated antenna selection," *IEEE Trans. Inf. Forensics Security*, to be published.

[23] J. Hu, W. Yang, N. Yang, X. Zhou, and Y. Cai, "On-off-based secure transmission design with outdated channel state information," *IEEE Trans. Veh. Technol.*, to be published.

[24] N. E. Wu and H. J. Li, "Effect of feedback delay on secure cooperative networks with joint relay and jammer selection," *IEEE Wireless Commun. Lett.*, vol. 2, no. 4, pp. 415–418, Aug. 2013.

[25] X. Guan Y. Cai and Y. Yang, "Secure transmission design and performance analysis for cooperation exploring outdated CSI," *IEEE Commun. Lett.*, vol. 18, no. 9, pp. 1637–1640, Sep. 2014.

[26] L. Wang, S. Xu, W. Yang, W. Yang, and Y. Cai, "Security performance of multiple antennas multiple relaying networks with outdated relay selection," in *Proc. WCSP*, Hefei, China, Oct. 2014, pp. 1–6.

[27] J. Huang and A. L. Swindlehurst, "Buffer-aided relaying for two-hop secure communication," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 152–164, Jan. 2015.

[28] S. I. Kim, I. M. Kim, and J. Heo, "Secure transmission for multiuser relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3724–3737, Jul. 2015.

[29] Y. Ma, D. Zhang, A. Leith, and Z. Wang, "Error performance of transmit beamforming with delayed and limited feedback," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1164–1170, Mar. 2009.

[30] Z. Rezki, A. Khisti, and M. S. Alouini, "Ergodic secret message capacity of the wirechannel with finite-rate feedback," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3364–3379, Jun. 2014.

[31] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.

[32] H. A. Suraweera, M. Soysa, C. Tellambura, and H. K. Garg, "Performance analysis of partial relay selection with feedback delay," *IEEE Signal Process. Lett.*, vol. 17, no. 6, pp. 531–534, Jun. 2010.

[33] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 6th ed. San Diego, CA, USA: Academic, 2000.

[34] S. Kim and J. Heo. "Outage probability of interference-limited amplify-and-forward relaying with partial relay selection," in *Proc. IEEE VTC*, Yokohama, Japan, May 2011, pp. 1–5.

Lei Wang (S'11) received the B.S. degree in electronics and information engineering from Central South University, Changsha, China, in 2004 and the M.S. degree in communications and information systems from PLA University of Science and Technology, Nanjing, China, in 2011. He is currently working toward the Ph.D. degree in communications and information systems with PLA University of Science and Technology.

His current research interests include cooperative communications, signal processing in communications, and physical layer security.

Yueming Cai (M'05–SM'12) received the B.S. degree in physics from Xiamen University, Xiamen, China, in 1982 and the M.S. degree in microelectronics engineering and the Ph.D. degree in communications and information systems from Southeast University, Nanjing, China, in 1988 and 1996, respectively.

He is currently with the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China. His current research interests include multiple-input–multiple-output systems, orthogonal frequency-division multiplexing systems, signal processing in communications, cooperative communications, and wireless sensor networks.

Yulong Zou (SM'13) received the B.Eng. degree in information engineering from Nanjing University of Posts and Telecommunications (NUPT), Nanjing, China, in July 2006; the Ph.D. degree in electrical engineering from Stevens Institute of Technology, Hoboken, NJ, USA, in May 2012; and the Ph.D. degree in signal and information processing from NUPT in July 2012.

He is currently a Professor with NUPT. His research interests span a wide range of topics in wireless communications and signal processing, including cooperative communications, cognitive radio, wireless security, and energy-efficient communications.

Dr. Zou has been a symposium chair, a session chair, and a technical program committee member for several IEEE-sponsored conferences, including the IEEE Wireless Communications and Networking Conference, the IEEE Global Communications Conference, the IEEE International Conference on Communications, the IEEE Vehicular Technology Conference, and the International Conference on Communications in China. He serves on the editorial board of *IEEE Communications Surveys and Tutorials*, *IEEE Communications Letters*, *IET Communications*, and the *EURASIP Journal on Advances in Signal Processing*. He was a received the 2014 IEEE Communications Society Asia-Pacific Best Young Researcher award.

Weiwei Yang (S'08–M'12) received the B.S., M.S., and Ph.D. degrees from PLA University of Science and Technology, Nanjing, China, in 2003, 2006, and 2011, respectively.

He is currently with the College of Communications Engineering, PLA University of Science and Technology. His research interests are orthogonal frequency-domain multiplexing systems, signal processing in communications, cooperative communications, cognitive networks, and network security.

Lajos Hanzo (M'91–SM'92–F'04) received the M.S. degree in electronics and the Ph.D. degree from the Technical University of Budapest, Budapest, Hungary, in 1976 and 1983, respectively; the D.Sc. degree from the University of Southampton, Southampton, U.K., in 2004; and the "Doctor Honoris Causa" degree from the Technical University of Budapest in 2009.

During his 38-year career in telecommunications, he has held various research and academic posts in Hungary, Germany, and the U.K. Since 1986, he has been with the School of Electronics and Computer Science, University of Southampton, where he holds the Chair in Telecommunications. He is currently directing an academic research team, working on a range of research projects in the field of wireless multimedia communications sponsored by industry, the Engineering and Physical Sciences Research Council (EPSRC), the European Research Council's Advanced Fellow Grant, and the Royal Society's Wolfson Research Merit Award. During 2008–2012, he was a Chaired Professor with Tsinghua University, Beijing, China. He is an enthusiastic supporter of industrial and academic liaison and offers a range of industrial courses. He has successfully supervised about 100 Ph.D. students, coauthored 20 John Wiley/IEEE Press books on mobile radio communications totaling in excess of 10 000 pages, and published more than 1400 research entries on IEEE Xplore.

Dr. Hanzo is a Fellow of the Royal Academy of Engineering, the Institution of Engineering and Technology, and the European Association for Signal Processing. He is also a Governor of the IEEE Vehicular Technology Society. During 2008–2012, he was the Editor-in-Chief of IEEE Press. He has served as the Technical Program Committee Chair and the General Chair of IEEE conferences, has presented keynote lectures, and has received a number of distinctions. His published work has more than 20 000 citations. Further information on research in progress and associated publications is available at http://www-mobile.ecs.soton.ac.uk.

AUTHOR QUERIES

AUTHOR PLEASE ANSWER ALL QUERIES

AQ1 = RV was expanded as "random variable." Please check if appropriate. Otherwise, please make the necessary changes.
AQ2 = Equations (29) and (30) are missing in the document. Please check.
AQ3 = Please provide publication update in Ref [22].
AQ4 = Please provide publication update in Ref [23].
AQ5 = Current affiliation of author Yueming Cai was provided as captured from the first footnote. Please check if appropriate. Otherwise, please make the necessary changes.
AQ6 = Please confirm that Dr. Zou has received two Ph.D. degrees.
AQ7 = Current affiliation of author Weiwei Yang was provided as captured from the first footnote. Please check if appropriate. Otherwise, please make the necessary changes.

END OF ALL QUERIES

Joint Relay and Jammer Selection Improves the Physical Layer Security in the Face of CSI Feedback Delays

Lei Wang, *Student Member, IEEE*, Yueming Cai, *Senior Member, IEEE*, Yulong Zou, *Senior Member, IEEE*, Weiwei Yang, *Member, IEEE*, and Lajos Hanzo, *Fellow, IEEE*

***Abstract*—We enhance the physical layer security (PLS) of amplify-and-forward (AF) relaying networks with the aid of joint relay and jammer selection (JRJS), despite the deleterious effect of channel state information (CSI) feedback delays. Furthermore, we conceive a new outage-based characterization approach for the JRJS scheme. The traditional best relay selection (TBRS) is also considered as a benchmark. We first derive closed-form expressions of both the connection outage probability (COP) and the secrecy outage probability (SOP) for both the TBRS and JRJS schemes. Then, a reliable and secure connection probability (RSCP) is defined and analyzed for characterizing the effect of the correlation between the COP and the SOP introduced by the corporate source–relay link. The reliability–security ratio (RSR) is introduced for characterizing the relationship between the reliability and the security through asymptotic analysis. Moreover, the concept of effective secrecy throughput is defined as the product of the secrecy rate and of the RSCP for the sake of characterizing the overall efficiency of the system, as determined by the transmit SNR, the secrecy codeword rate, and the power sharing ratio between the relay and the jammer. The impact of the direct source–eavesdropper link and additional performance comparisons with respect to other related selection schemes are also included. Our numerical results show that the JRJS scheme outperforms the TBRS method both in terms of the RSCP and in terms of its effective secrecy throughput, but it is more sensitive to the feedback delays. Increasing the transmit signal-to-noise ratio (SNR) will not always improve the overall throughput. Moreover, the RSR results demonstrate that, upon reducing the CSI feedback delays, the reliability improves more substantially than the security degrades, implying an overall improvement in terms of the security–reliability tradeoff. Additionally, the secrecy throughput loss due to the second-hop feedback delay is more pronounced than that due to the first-hop one.**

Manuscript received October 2, 2014; revised February 25, 2015 and July 27, 2015; accepted September 8, 2015. This work was supported in part by the National Natural Science Foundation of China under Grant 61371122, Grant 61471393, and Grant 61501512 and in part by the Natural Science Foundation of Jiangsu Province under Grant BK20150718 and Grant BK20150040. The review of this paper was coordinated by Prof. M. C. Gursoy.

L. Wang, Y. Cai, and W. Yang are with the College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China (e-mail: csu-wl@163.com; caiym@vip.sina.com; yww_1010@aliyun.com).

Y. Zou is with the School of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: yulong.zou@njupt.edu.cn).

L. Hanzo is with the Department of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (e-mail: lh@ecs.soton.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2015.2478029

***Index Terms*—Effective secrecy throughput, feedback delay, physical layer security (PLS), relay and jammer selection, reliability and security.**

I. Introduction

WIRELESS communications systems are particularly vulnerable to security attacks because of the inherent openness of the transmission medium. Traditionally, the information privacy of wireless networks has been focused on the higher layers of the protocol stack employing cryptographically secure schemes. However, these methods typically assume a limited computing power for the eavesdroppers and exhibit inherent vulnerabilities in terms of the inevitable secret key distribution and management [1]. In recent years, physical layer security (PLS) has emerged as a promising technique of improving the confidentiality wireless communications, which exploits the time-varying properties of fading channels, instead of relying on conventional cryptosystems. The pivotal idea of PLS solutions is to exploit the dynamically fluctuating random nature of radio channels for maximizing the uncertainty concerning the source messages at the eavesdropper [2], [3].

To achieve this target, several PLS-enhancement approaches have been proposed in the literature, including secrecy-enhancing channel coding [4], secure on–off transmission designs [5], secrecy-improving beamforming (BF)/precoding, and artificial-noise-aided techniques relying on multiple antennas [6], as well as secure relay-assisted transmission techniques [7]. Specifically, apart from improving the reliability and coverage of wireless transmissions, user cooperation also has a great potential in terms of enhancing the wireless security against eavesdropping attacks. There has been a growing interest in improving the security of cooperative networks at the physical layer [8]–[14]. To explore the spatial diversity potential of the relaying networks and to boost the secrecy capacity (the difference between the channel capacity of the legitimate main link and that of the eavesdropping link), most of the existing work has been focused on secrecy-enhancing BF [8], [9], as well as on intelligent relay node/jammer node (RN/JN) selection, etc. Notably, given the availability of multiple relays, appropriately designed RN/JN selection is capable of achieving a significant security improvement for cooperative networks, which is emerging as a promising research topic. In particular, Zou *et al.* investigated both amplify-and-forward (AF)- and decode-and-forward (DF)-based optimal relay selection conceived for

enhancing the PLS in cooperative wireless networks [10], [11], where the global channel state information (CSI) of both the main link and the eavesdropping link was assumed to be available. Similarly, jamming techniques, which impose artificial interference on the eavesdropper, have also attracted substantial attention [12]–[14]. More specifically, several sophisticated joint relay and jammer selection (JRJS) schemes were proposed in [12], where the beneficially selected relay increases the reliability of the main link, whereas the carefully selected jammer imposes interference on the eavesdropper and simultaneously protects the legitimate destination from interference. In [13] and [14], cooperative jamming has been studied in the context of bidirectional scenarios, and efficient RN/JN selection criteria have been developed for achieving improved secrecy rates with the aid of multiple relays. Furthermore, more effective relaying and jamming schemes, when taking the information leakage of the source–eavesdropper link into consideration, have been presented lately in [15] and [16].

Nevertheless, an idealized assumption of the previously reported research on PLS is the availability of perfect channel state information (CSI), which is regarded as a stumbling block in the way of invoking practical secrecy-enhancing Wyner coding, on–off design, BF/precoding, and RN/JN selection. However, this idealized simplifying assumption is not realistic, since practical channel estimation imposes CSI imperfections, which are aggravated by the feedback delay, limited-rate feedback, and channel estimation errors (CEEs) [17]. Generally, the related research has been focused on the issues of robust secure BF design from an average secrecy-rate-based optimization perspective for point-to-point multiantenna aided channels and relay channels [18], [19] supporting delay-tolerant systems. For systems imposing stringent delay constraints, particularly in imperfect CSI scenarios, perfect secrecy cannot always be achieved. Hence, the secrecy-outage-based characterization of systems is more appropriate, which provides a probabilistic performance measure of secure communication. The concept of secrecy outage was adopted in [20] for characterizing the probability of having both reliable and secure transmission, which, however, is inapplicable for the imperfect CSI case and fails to distinguish a connection outage from the secrecy outage. In [21], an alternative secrecy outage formulation is proposed for characterizing the attainable security level and provided a general framework for designing transmission schemes that meet specific target security requirements. To quantify both the reliability and security performance at both the legitimate and eavesdropper nodes separately, two types of outages, namely, the connection outage probability (COP) and the secrecy outage probability (SOP) are introduced. Then, considering the impact of time delay caused by the antenna selection process at the legitimate receiver, Hu *et al.* [22] proposed a new secure transmission scheme in the multiinput multioutput multieavesdropper wiretap channel. Much recently, considering the outdated CSI from the legitimate receiver, a new secure on–off transmission scheme was proposed for enhancing the secrecy throughput in [23].

Moreover, prior studies of the outage-based secure transmission design are limited to single-antenna-assisted single-hop systems and have not been considered for cooperative relaying systems. Hence, the issues of secure transmissions over cooperative relaying channels expressed in terms of the SOP, COP, and secrecy throughput constitute an open problem. On the other hand, apart from CEE, the CSI feedback delay results in critical challenges for the PLS of cooperative relaying systems, particularly when considering the specifics of RN/JN selection. In [15], the effects of outdated CSI knowledge concerning the legitimate links on the ergodic secrecy rate achieved by the proposed secure transmission strategy in the context of DF relaying is investigated. The impact of CSI feedback delay on the secure relay and jammer selection conceived for DF relaying was investigated in [24], albeit only in terms of the SOP. In our previous study [25], we considered the secure transmission design and the secrecy performance of an opportunistic DF system relying on outdated CSI, where only a single relay is invoked. Additionally, during the revision of this work, we investigated the security performance for outdated AF relay selection in [26]. Therefore, in this treatise, we extend our investigations to the PLS of multiple AF relaying assisted networks relying on RN/JN selection.

Explicitly, we focus our attention on the outage-based characterization of secure transmissions in cooperative relay-aided networks relying on realistic CSI feedback delay. To exploit the multirelay induced diversity gain and the associated jamming capabilities, joint AF relay node and jammer node selection is employed by the relay–destination link. We assume that, in line with the practical reality, the instantaneous eavesdropper's CSI is unavailable at the legitimate transmitter and that the RN/JN selections are performed based on the outdated CSI of the main links. Two types of cooperative strategies are invoked by our cooperative network operating under secrecy constraints, namely, the traditional best relay selection (TBRS) strategy and the JRJS strategy. Specifically, the main contributions of this paper can be summarized as follows.

- We develop an outage-based characterization for quantifying both the reliability and security performance of a two-hop AF relaying system. Specifically, in contrast to [21] and [22], we propose the novel definition of the reliable and secure connection probability (RSCP). Explicitly, closed-form expressions of the COP, the SOP, and the RSCP are derived for both the TBRS and for our JRJS strategies. Numerical results demonstrate that the JRJS scheme outperforms the TBRS scheme in terms of its RSCP.
- We also introduce the reliability–security ratio (RSR) for characterizing their direct relationship by a single parameter through the asymptotic analysis of the COP and the SOP in the high-SNR regime. We derive the RSR for both the TBRS and JRJS strategies for investigating the effect of secrecy codeword rate setting, as well as that of the feedback delay and that of the power sharing ratio between the relay and the jammer on the RSR.
- We then modify the definition of effective secrecy throughput by multiplying the secrecy rate with the RSCP, which results in an optimization problem of the transmit signal-to-noise ratio (SNR), secrecy codeword rate, and power sharing between the relay and the jammer.

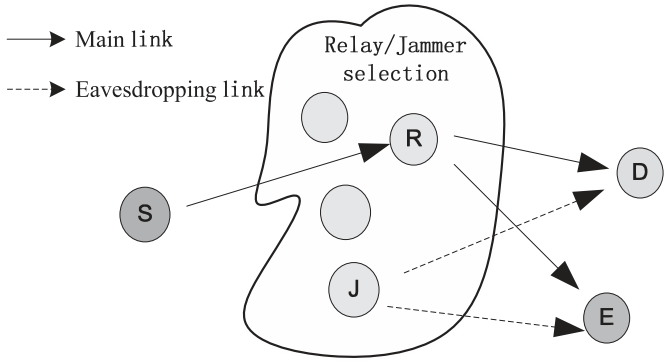

Fig. 1. Cooperative relaying network assisted by multiple relays in the presence of an eavesdropper.

It is shown that, compared with the TBRS strategy, JRJS achieves a significantly higher effective secrecy throughput, and the corresponding throughput loss is more sensitive to feedback delays. The impact of the direct source–eavesdropper link and additional throughput performance comparisons with respect to other related selection schemes are further discussed.

The remainder of this paper is organized as follows. Section II introduces our system model and describes both the TBRS and our JRJS strategies. In Sections III and IV, we present the mathematical framework of our performance analysis both for the TBRS strategy and for the JRJS strategy, respectively, including the COP, the SOP, the RSCP, the RSR, and the effective secrecy throughput. Our numerical results and discussions are provided in Section V. Finally, Section VI presents our concluding remarks.

II. System Model

A. System Description

Consider a cooperative relaying network consisting of a source S, a destination D, K_r relays R_k, $k = 1, \ldots, K_r$, and an eavesdropper E, as shown in Fig. 1, where all nodes are equipped with a single transmit antenna (TA), except for the source, which has N_t TAs. The cooperative relay architecture in Fig. 1 is generally applicable to diverse practical wireless systems in the presence of an eavesdropper, including the family of wireless sensor networks (WSNs), mobile ad hoc networks (MANETs), and the long-term evolution advanced cellular systems [11].

To exploit the diversity potential of multiple relay nodes over independently fading channels, AF relay/jammer selection is employed. All relays operate in the half-duplex AF mode, and data transmission is performed in two phases. More particularly, during the broadcast phase, the source node transmits its signal to a selected relay with the aid of BF, which is invoked for forwarding the signal received from S to D. An inherent assumption is that the transmit BF weights are based on the CSI estimates quantified and fed back by the selected relay. During the cooperative phase, a pair of appropriately selected relays transmit toward D and E, respectively. A conventional relay (denoted by R^*) forwards the source's message to the destination. Another relay (denoted by J^*) operates in the "jammer mode" and imposes intentional interference upon E in order confuse it. However, D is unable to mitigate the artificial interference emanating from the jammer node J^* due to its critical secrecy constraints [12]. It should be noted that both the process of RN/JN selection and the feedback of the transmit BF weights from R^* to S may impose a time lag between the data transmission and the channel estimation. These time delays are denoted by $T_{d_{SR}}$ and $T_{d_{RD}}$, respectively. Furthermore, we assume that the BF and RN/JN selection process is based on the perfectly estimated but outdated CSI. We employ the first-order autoregressive outdated CSI model of [20], while relying on the correlation coefficients of $\rho_{SR} = J_0(2\pi f_d T_{d_{SR}})$ and $\rho_{RD} = J_0(2\pi f_d T_{d_{RD}})$ for the two hops, where $J_0(\cdot)$ is the zero-order Bessel function of the first kind, and f_d is the Doppler frequency.

A slow flat block Rayleigh fading environment is assumed, where the channel remains static for the coherence interval (one slot) and changes independently in different coherence intervals, as denoted by $h_{i,j} \sim \mathcal{CN}(0, \sigma_{i,j}^2)$, $i, j \in \{S, R, J, D, E\}$. The direct communication links are assumed to be unavailable due to the presence of obstructions between S and D, as well as the eavesdropper.[1] This assumption follows the rationale of [12] and has been routinely exploited in previous literature (see [27] and [28] and the references therein), where the source and relays belong to the same cluster, whereas the destination and the eavesdropper are located in another. More specifically, this assumption is particularly valid in networks with broadcast and unicast transmission, where each terminal is a legitimate receiver for one signal and acts as an eavesdropper for some other signal. Therefore, the security concerns are only related to the cooperative relay-aided channel. Furthermore, additive white Gaussian noise (AWGN) is assumed with zero mean and unit variance N_0. Let P_i be the transmit power of node i, and the instantaneous SNR of the $i \to j$ link is given by $\gamma_{i,j} = P_i |h_{i,j}|^2 / N_0$.

We employ the constant-rate Wyner coding scheme for constructing wiretap codes of [2] to meet the PLS requirements due to the fact that the accurate global CSI is not available. Let $\mathbb{C}(R_0, R_s, N)$ denote the set of all possible Wyner codes of length N, where R_0 is the codeword transmission rate, and R_s is the confidential information rate ($R_0 > R_s$). The positive rate difference $R_e = R_0 - R_s$ is the cost of providing secrecy against the eavesdropper. A confidential message is encoded into a codeword at S and then transmitted to D.

B. Secure Transmission

In the broadcast phase, S transmits its BF signal $s(t)$ to the selected relay R^*, where the relay selection is performed before data transmission commences, and the selection criterion will be detailed later in the context of the cooperative phase. The transmit BF vector $\mathbf{w}(t|T_d)$ is calculated using the perfectly estimated but outdated CSI given by

[1] The case when the $S \to E$ link is introduced will be investigated separately in Section VI.

$\mathbf{w}(t|T_{d_{SR}}) = \mathbf{h}^H_{SR^*}(t-T_d)/|\mathbf{h}_{SR^*}(t-T_{d_{SR}})|$ [29], where we have $\mathbf{h}_{SR^*}(t) = [h_{SR^*,1}(t), \ldots, h_{SR^*,N_t}(t)]^T$, and the signal received by the relay R^* can be written as

$$y_{R^*}(t) = \sqrt{P_s}\mathbf{w}(t|T_d)\mathbf{h}_{SR^*}(t)s(t) + n_{SR^*}(t) \tag{1}$$

where $n_{SR^*}(t)$ is the AWGN at the relay. Then, we can define the received SNR at the relay node as $\gamma_{SR} = P_S|\mathbf{w}(t|T_{d_{SR}})\mathbf{h}_{SR^*}(t)|^2/N_0$.

In the cooperative phase, we consider two RN/JN selection schemes performed by D: relay selection without jamming and JRJS.

1) Traditional Best Relay Selection: The first category of solutions does not involve a jamming process, and therefore, only a conventional relay accesses the channel during the second phase of the protocol. The relay selection process is performed based on the highest instantaneous SNR of the second hop, which is formulated as

$$R^* = \arg\max_{R_k\in\mathcal{R}} \left\{ \frac{\tilde{\gamma}_{R_kD}}{\mathbb{E}\left[\gamma_{R_kE}\right]} = \frac{P_R\left|\tilde{h}_{R_kD}(t-T_d)\right|^2}{N_0\mathbb{E}\left[\gamma_{R_kE}\right]} \right\} \tag{2}$$

where $\tilde{\gamma}_{R_kD}$ is the instantaneous SNR in the relay selection process, and $\mathbb{E}[\gamma_{R_kE}]$ denotes the average SNR at E. We can model γ_{R_kD} and $\tilde{\gamma}_{R_kD}$ as two gamma distributed random variables having the correlation factor of ρ^2_{RD}.

During the second phase, the received signal $y_{R^*}(t)$ is multiplied by a time-variant AF-relay gain G and retransmitted to D, where we have $G = \sqrt{P_R/(P_S|\mathbf{w}_{\text{opt}}(t|T_{d_{SR}})\mathbf{h}_{SR^*}(t)|^2 + N_0)}$. After further mathematical manipulations, the mutual information (MI) between S and D, as well as the eavesdropper, can be written as

$$I_D^{\text{TBRS}} = \frac{1}{2}\log\left(1+\gamma_D^{\text{TBRS}}\right) = \frac{1}{2}\log\left(1+\frac{\gamma_{SR}\gamma_{R^*D}}{\gamma_{SR}+\gamma_{R^*D}+1}\right) \tag{3}$$

$$I_E^{\text{TBRS}} = \frac{1}{2}\log\left(1+\gamma_E^{\text{TBRS}}\right) = \frac{1}{2}\log\left(1+\frac{\gamma_{SR}\gamma_{R^*E}}{\gamma_{SR}+\gamma_{R^*E}+1}\right). \tag{4}$$

2) Joint Relay and Jammer Selection: Similarly, considering the unavailability of the instantaneous CSI regarding the eavesdropper, we adopt a suboptimal RN/JN selection metric conditioned on the outdated CSI as

$$\begin{aligned} R^* &= \arg\max_{R_k\in\mathcal{R}} \left\{ \frac{\tilde{\gamma}_{R_kD}}{\mathbb{E}\left[\gamma_{R_kE}\right]} \right\} \\ J^* &= \arg\min_{R_k\in\mathcal{R}-R^*} \left\{ \frac{\tilde{\gamma}_{R_kD}}{\mathbb{E}\left[\gamma_{R_kE}\right]} \right\} \end{aligned} \tag{5}$$

where J^* is selected for minimizing the interference imposed on D.

It should be noted that, to have the same transmit power as that of the TBRS case, we assume that $P_{R*} + P_{J^*} = P_R$ for our JRJS strategy and introduce $\lambda = P_{R^*}/(P_{R^*} + P_{J^*})$ as the ratio of the relay's transmit power to the total power required by the active relay and jammer.

In the cooperative phase, R^* will also amplify the received signal $y_{R^*}(t)$ by G and forward it to D. At the same time, the jammer J^* will generate intentional interference to confuse E, which will also cause interference at D. Consequently, the MI between the terminals is given by

$$I_D^{\text{JRJS}} = \frac{1}{2}\log\left(1+\gamma_D^{\text{JRJS}}\right) = \frac{1}{2}\log\left(1+\frac{\gamma_{SR}\frac{\gamma_{R^*D}}{\gamma_{J^*D}+1}}{\gamma_{SR}+\frac{\gamma_{R^*D}}{\gamma_{J^*D}+1}+1}\right) \tag{6}$$

$$I_E^{\text{JRJS}} = \frac{1}{2}\log\left(1+\gamma_E^{\text{JRJS}}\right) = \frac{1}{2}\log\left(1+\frac{\gamma_{SR}\frac{\gamma_{RE}}{\gamma_{JE}+1}}{\gamma_{SR}+\frac{\gamma_{RE}}{\gamma_{JE}+1}+1}\right). \tag{7}$$

Remark 1: Generally, the optimal RN/JN selection scheme should take into account the global SNR knowledge set $\{\gamma_{SR}, \gamma_{RD}, \gamma_{RE}\}$. However, given the potentially excessive implementational complexity overhead of the optimal selection schemes and the unavailability of the global CSI, we employ suboptimal selection schemes as in [12].[2] Furthermore, it is commonly assumed that the average SNR of the eavesdropper is available at the transmitter, which seems, somehow, not reasonable. However, as stated in most of the literature, such as [12]–[22], [24]–[28], and [30], provided that the eavesdropper belongs to the network, which is also the case in our paper, the related assumption might still be deemed reasonably. Additionally, as in [8], [11], [12], and [24], for mathematical convenience, we assume that the relaying channels are independent and identically distributed and that we have $\mathbb{E}[\gamma_{SR_k}] = \bar{\gamma}_{SR}$, $\mathbb{E}[\gamma_{R_kD}] = \bar{\gamma}_{RD}$, and $\mathbb{E}[\gamma_{R_kE}] = \bar{\gamma}_{RE}$. The distances between the relays are assumed to be much smaller than the distances between relays and source/destination/eavesdropper; hence, the corresponding path losses among the different relays are approximately the same. This assumption is reasonable both for WSNs and for MANETs associated with a symmetric clustered relay configuration, and it may be also satisfied as valid by classic cellular systems in a statistical sense [11].

III. Secure Transmission Without Jamming

Here, we endeavor to characterize both the reliability and security performance comprehensively of the TBRS scheme. We first derive closed-form expressions for both the COP and the SOP. Then, the RSR is introduced through the asymptotic analysis of the COP and the SOP. Furthermore, we propose the novel definition of the RSCP and the effective secrecy throughput.

[2]To further alleviate the cooperation-related overhead, the selection criterion is based on the $R \to D$ link, since the second hop plays a dominant role in determining the received SNR, because the first hop corresponds to a multiple-input–single-output channel with the aid of multiple antennas, and hence, it is more likely to be better than the second hop. The optimal selection based on both hops is beyond the scope of this work.

A. COP and SOP

When the perfect instantaneous CSI of the eavesdropper's channel and even the legitimate users' channel is unavailable, alternative definitions of the outage probability may be adopted for the statistical characterization of the attainable secrecy performance, particularly for delay-limited applications. Based on [31, Def. 2], perfect secrecy cannot be achieved, when we have $R_e < I_E$, where I_E denotes the MI between the source and the eavesdropper. Encountering this event is termed as a secrecy outage. Furthermore, the destination is unable to flawlessly decode the received codewords when $R_0 > I_D$, which is termed as a connection outage. The grade of reliability and the grade of security maintained by a transmission scheme may be then quantified by the COP and the SOP, respectively.

We continue by presenting our preliminary results versus the point-to-point SNRs. Let us denote the cumulative distribution function (CDF) and the probability density function (PDF) of a random variable X by $F_X(x)$ and $f_X(x)$, respectively. On one hand, the PDF of γ_{SR} using [29, eq. (15)] is given by

$$f_{\gamma_{SR}}(x) = \sum_{n=0}^{N_t-1} \binom{N_t-1}{n} \frac{\rho_{SR}^{2(N_t-1-n)} \left(\bar{\gamma}_{SR}\left(1-\rho_{SR}^2\right)\right)^n}{\bar{\gamma}_{SR}^{N_t}(N_t-1-n)!} \times x^{N_t-1-n} e^{\frac{-x}{\bar{\gamma}_{SR}}} \quad (8)$$

whereas its CDF is given by

$$F_{\gamma_{SR}}(x) = 1 - \sum_{n=0}^{N_t-1} \sum_{m=0}^{N_t-1-n} \binom{N_t-1}{n} \times \frac{\rho_{SR}^{2(N_t-1-n)} \left(1-\rho_{SR}^2\right)^n}{m!\bar{\gamma}_{SR}^m} x^m e^{\frac{-x}{\bar{\gamma}_{SR}}}. \quad (9)$$

On the other hand, for the instantaneous SNR of the $R \to D$ hop, according to the principles of concomitants or induced order statistics, the CDF of γ_{R^*D} can be derived as in [32]

$$F_{\gamma_{R^*D}}(y) = K_r \sum_{k=0}^{K_r-1} (-1)^k \binom{K_r-1}{k} \frac{1-e^{\frac{-(k+1)y}{\left(k\left(1-\rho_{RD}^2\right)+1\right)\bar{\gamma}_{RD}}}}{k+1}. \quad (10)$$

Thus, the COP of the TBRS strategy is given by

$$P_{\rm co}^{\rm TBRS}(R_0) = \Pr\left[I_D^{\rm TBRS} < R_0\right] = F_{\gamma_D^{\rm TBRS}}\left(\gamma_{th}^D\right) \quad (11)$$

where we have $\gamma_{th}^D = 2^{2R_0} - 1$, and the CDF of $\gamma_D^{\rm TBRS}$ can be calculated as

$$F_{\gamma_D^{\rm TBRS}}(x) = 1 - \int_0^\infty \left[1 - F_{\gamma_{R^*D}}\left(\frac{xz + x(x+1)}{z}\right)\right] f_{\gamma_{SR^*}}(z+x)dz. \quad (12)$$

Consequently, by substituting (8) and (10) into (12) and using [33, eq. (3.471.9)], we arrive at a closed-form expression for $F_{\gamma_D^{\rm TBRS}}(x)$ as

$$F_{\gamma_D^{\rm TBRS}}(x) = 1 - 2\sum_{n=0}^{N_t-1}\sum_{k=0}^{K_r-1}\sum_{m=0}^{N_t-1-n} (-1)^k K_r \binom{N_t-1}{n} \times \binom{K_r-1}{k}\binom{N_t-1-n}{m} \times \frac{\rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n x^{N_t-1-n-m}}{(N_t-1-n)!(k+1)\bar{\gamma}_{SR}^{N_t-n}} \times \left[\frac{\bar{\gamma}_{SR}x(x+1)}{\omega_k\bar{\gamma}_{RD}}\right]^{\frac{m+1}{2}} \times e^{-\left(\frac{\bar{\gamma}_{SR}+\omega_k\bar{\gamma}_{RD}}{\omega_k\bar{\gamma}_{SR}\bar{\gamma}_{RD}}\right)x} K_{m+1}\left(2\sqrt{\frac{x(x+1)}{\omega_k\bar{\gamma}_{SR}\bar{\gamma}_{RD}}}\right) \quad (13)$$

where we have $\omega_k = (k(1-\rho_{RD}^2)+1)/(k+1)$. Then, by substituting $x = \gamma_{th}^D$ into (13), we obtain $P_{\rm co}^{\rm TBRS}$.

Furthermore, the SOP of the TBRS strategy may be expressed as

$$P_{\rm so}^{\rm TBRS}(R_0, R_s) = \Pr\left[I_E^{\rm TBRS} > R_0 - R_s\right] = 1 - F_{\gamma_E^{\rm TBRS}}\left(\gamma_{th}^E\right) \quad (14)$$

where we have $\gamma_{th}^E = 2^{2(R_0-R_s)} - 1$. Similarly, we may calculate the CDF of $\gamma_E^{\rm TBRS}$ in (14) as

$$F_{\gamma_E^{\rm TBRS}}(x) = 1 - 2\sum_{n=0}^{N_t-1}\sum_{m=0}^{N_t-1-n} \binom{N_t-1}{n}\binom{N_t-1-n}{m} \times \frac{\rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n x^{N_t-1-n-m}}{(N_t-1-n)!\bar{\gamma}_{SR}^{N_t-n}} \times \left[\frac{\bar{\gamma}_{SR}x(x+1)}{\bar{\gamma}_{RE}}\right]^{\frac{m+1}{2}} \times e^{-\left(\frac{\bar{\gamma}_{SR}+\bar{\gamma}_{RE}}{\bar{\gamma}_{SR}\bar{\gamma}_{RE}}\right)x} K_{m+1}\left(2\sqrt{\frac{x(x+1)}{\bar{\gamma}_{SR}\bar{\gamma}_{RE}}}\right). \quad (15)$$

Then, by substituting $x = \gamma_{th}^E$ into (15), we can derive $P_{\rm so}^{\rm TBRS}$.

The COP and the SOP in (11) and (14) characterize the attainable reliability and security performance, respectively, and can be regarded as the detailed requirements of accurate system design. From the definition of COP and SOP, it is clear that the reliability of the main link can be improved by increasing the transmit SNR (or decreasing its data rate) to reduce the COP, which unfortunately increases the risk of eavesdropping. Thus, a tradeoff between reliability and security may be struck, despite the fact that closed-from expressions cannot be obtained as in [11]. Furthermore, we denote the minimal reliability and security requirements by υ and δ, where the feasible range of the reliability constraint is $0 < \upsilon < 1$. Bearing in mind that the COP is a monotonously increasing function of R_0, the corresponding threshold of the codeword transmission rate is $R_0^{th} = \arg\{P_{\rm co}^{\rm TBRS}(R_0) = \upsilon\}$, which leads to a lower bound of the SOP, when we have $(R_0 - R_s) \to R_0^{th}$. Thus, the feasible range of δ is $P_{\rm so}^{\rm TBRS}(R_0^{th}, 0) < \delta < 1$. The preceding analysis indicates that, given a reliability constraint υ, the lower bound of the security constraint is determined.

B. Reliability–Security Ratio

Here, we will focus our attention on the asymptotic analysis of the COP and the SOP in the high-SNR regime. Then, inspired by [25], we introduce the concept of the RSR for characterizing the direct relationship between reliability and security.

Proposition 1: Based on the asymptotic probabilities of $P_{\rm co}$ and $P_{\rm so}$ at high SNRs,[3] the RSR is defined as

$$P_{\rm co}(R_0) = \Lambda\left[1 - P_{\rm so}(R_0, R_s)\right] \tag{16}$$

where $\Lambda = \lim_{\eta\to\infty} P_{\rm co}/(1 - P_{\rm so})$, which represents the improvement in COP upon decreasing the SOP. More specifically, since the reduction of the SOP/COP must be followed by an improvement of COP/SOP, a lower Λ implies that, when the security is reduced, the reliability is improved, and *vice versa*. Thus, for the TBRS scheme studied earlier, the RSR is derived as (17), shown at the bottom of the page.

Proof: The proof is given in Appendix B.

Remark 2: It can be seen from the preceding expression that the factor Λ is independent of the transmit SNR, but directly depends on the channel gains, the rate pair (R_0, R_s), and the number of TAs and relays. For a given R_s, reducing R_0 to enhance the reliability may erode the security, because $(R_0 - R_s)$ is also reduced. Conversely, increasing R_0 provides more redundancy for protecting the security of the information, but simultaneously, the reliability is reduced. Hence, the RSR analysis underlines an important point of view concerning how to balance the reliability versus security tradeoff by adjusting (R_0, R_s). Furthermore, as long as a CSI feedback delay exists, the RSR has an intimate relationship with ρ_{SR} and ρ_{RD}. It is clear that the value of $\Lambda^{\rm TBRS}$ decreases as ρ_{RD} increases, which is due to the fact that the relay selection process only improves the reliability of the legitimate user. On the other hand, since we always have the conclusion that $\sum_{k=0}^{K_r-1}(-1)^k\binom{K_r-1}{k}(K_r/(k(1-\rho_{RD}^2)+1)) < 1$, when σ_{RD}^2 and σ_{RE}^2 are comparable, $\Lambda^{\rm TBRS}$ will be reduced as ρ_{SR} increases. This observation implies that, although both $P_{\rm co}$ and $(1 - P_{\rm so})$ are reduced when the first-hop CSI becomes better, the improvement of the reliability is more substantial than the security loss, as ρ_{SR} increases.

[3]Assume equal power allocation between S and the relay, yielding $P_S = P_R = P$, and define $\eta = P/N_0$ as the transmit SNR [24].

C. Effective Secrecy Throughput

It should be noted that the COP and SOP metrics ignore the correlation between these two outage events. More specifically, in contrast to the point-to-point transmission case, since the $S \to R$ link's SNR included in the MI expressions of (3) and (4), the secrecy outage and the connection outage are definitely not independent of each other. Therefore, it might be of limited benefit in evaluating the reliability or the security separately. We note furthermore that, although another metric referred to as the secrecy throughput was introduced as the product of the successful decoding probability and of the secrecy rate [21], [22], this definition ignores the fact that a reliable transmission may be insecure, and the SOP is not taken into consideration. Hence, this metric is unable to holistically characterize the efficiency of our scheme, while capable of achieving both reliable and secure transmission. Therefore, here, we redefine the effective secrecy throughput as the probability of a successful transmission (reliable and secure) multiplied by the secrecy rate, namely, as $\varsigma = R_s P_{R\&S}$, where the RSCP is defined as

$$P_{R\&S} = \Pr\{I_D > R_0, I_E < R_0 - R_s\}. \tag{18}$$

Upon substituting the expressions of I_D and I_E in (3) and (4) into (18), we can rewrite $P_{R\&S}$ for the TBRS strategy in (19), shown at the bottom of the page.

Finally, using the corresponding CDFs and PDFs of (8)–(10) from our previous analysis, we can obtain $P_{R\&S}^{\rm TBRS}$ in (20), shown at the bottom of the next page, as well as the secrecy throughput.

Furthermore, considering the asymptotic result for RSCP at high SNRs in (20) by applying the approximation $K_v(x) \approx (v-1)!/2(x/2)^v$ and closing the highest terms of η after invoking the McLaurin series representation for the exponential function, the asymptotic effective secrecy throughput can be approximated as

Remark 3: Given the definition of COP, SOP, and the secrecy throughput result of (21), shown at the bottom of the next page, it can be shown that, for a fixed R_s, if R_0 is too small, although

$$\Lambda^{\rm TBRS} = \frac{\left[\left(1-\rho_{SR}^2\right)^{N_t-1} + \sum_{k=0}^{K_r-1}(-1)^k\binom{K_r-1}{k}\frac{K_r\sigma_{SR}^2}{\left[k\left(1-\rho_{RD}^2\right)+1\right]\sigma_{RD}^2}\right]\left(2^{2R_0}-1\right)}{\left[N_t\left(1-\rho_{SR}^2\right)^{N_t-1} + \sigma_{SR}^2/\sigma_{RE}^2\right]\left(2^{2(R_0-R_s)}-1\right)} \tag{17}$$

$$\begin{aligned} P_{R\&S}^{\rm TBRS} &= \Pr\left\{\left\{\gamma_{SR} > \gamma_{th}^D, \gamma_{R^*D} > \frac{\gamma_{th}^D\gamma_{SR}+\gamma_{SR}}{\gamma_{SR}-\gamma_{th}^D}\right\} \cap \left[\left\{\gamma_{SR} > \gamma_{th}^E, \gamma_{R^*E} < \frac{\gamma_{th}^E\gamma_{SR}+\gamma_{SR}}{\gamma_{SR}-\gamma_{th}^E}\right\} \cup \left\{\gamma_{SR} < \gamma_{th}^E\right\}\right]\right\} \\ &= \Pr\left\{\gamma_{SR} > \gamma_{th}^D, \gamma_{R^*D} > \gamma_{th}^D + \frac{\gamma_{th}^D\left(\gamma_{th}^D+1\right)}{\gamma_{SR}-\gamma_{th}^D}, \gamma_{R^*E} < \gamma_{th}^E + \frac{\gamma_{th}^E\left(\gamma_{th}^E+1\right)}{\gamma_{SR}-\gamma_{th}^E}\right\} \end{aligned} \tag{19}$$

P_{RS} may be high (i.e., close to 1), the value of ς remains small. By contrast, if R_0 is too large, the value of $P_{\rm co}$ is close to 1, and therefore, ς will also become small. This observation is also suitable for R_s. Thus, as pointed out in the RSR analysis, it is elusive to improve both the reliability and the security simultaneously, but both of them are equally crucial in terms of the effective secrecy throughput, which depends on the rate pair (R_0, R_s).

Additionally, (21) also reveals that increasing the SNR would drastically reduce the effective secrecy throughput. For high transmit SNRs, a high reliability can indeed be perfectly guaranteed, but at the same time, the grade of the security is severely degraded. However, the probability of a reliable and simultaneously secure transmission will tend toward zero. Hence, we may conclude that there exists an optimal SNR, which achieves the maximal secrecy throughput.

In conclusion, adopting the appropriate code rate pair and transmit SNR is crucial for achieving the maximum effective secrecy throughput, which can be formulated as

$$\begin{aligned} &\max_{R_0,R_s,\eta} \varsigma(R_0,R_s) = R_s P_{R\&S}^{\rm TBRS} \\ &\text{s.t. } P_{\rm co} \le \upsilon, P_{\rm so} \le \delta, 0 < R_s < R_0 \end{aligned} \tag{22}$$

where υ and δ denote the system's reliability and security requirements. Unfortunately, it is quite a challenge to find the closed-form optimal solution to this problem due to the complexity of the expressions. Although suboptimal solutions can be found numerically (with the aid of gradient-based search techniques), the secrecy throughput optimization problem and the corresponding complexity analysis and performance comparisons are beyond the scope of this work.

IV. Secure Transmission With Jamming

Here, we consider the extension of the aforementioned relay selection approaches to systems additionally invoking relay-aided jamming. JRJS is based on the outdated but perfectly estimated CSI, and the details have been presented in Section II. We would also like to investigate the security performance from an outage-based perspective. The COP, SOP, RSCP, and effective secrecy throughput will be included.

A. COP and SOP

It is plausible that the main differences between the JRJS and TBRS schemes are determined by the instantaneous SNR of the $R \to D$ hop, where, now, a jammer is included. Based on our preliminary results detailed for the point-to-point SNRs in (8) and (10), we now focus our attention on the statistical analysis of the SNR, including J^*. As stated for the JRJS scheme in Section II, J^* corresponds to the lowest $\tilde{\gamma}_{R_k D}$ and is selected from the set $\{\mathcal{R} - R^*\}$. Recalling that R^* is the best relay of the second hop, we have $\tilde{\gamma}_{J^*D} = \min_{R_k \in \mathcal{R}-R^*}\{\tilde{\gamma}_{R_k D}\} \triangleq \min_{R_k \in \mathcal{R}}\{\tilde{\gamma}_{R_k D}\}$ for $K_r > 1$. Using the induced order statistics, the corresponding CDF of γ_{R^*D} is presented in (10), whereas the PDF of γ_{J^*D} can be formulated as

$$f_{\gamma_{J^*D}}(x) = \frac{K_r \exp\left(\frac{-K_r x}{\left[(K_r-1)\left(1-\rho_{RD}^2\right)+1\right]\bar{\gamma}_{JD}}\right)}{\left[\left(K_r-1\right)\left(1-\rho_{RD}^2\right)+1\right]\bar{\gamma}_{JD}}. \tag{23}$$

Although the relay and jammer selection processes are not entirely disjoint, we may exploit the assumption that γ_{R^*D} and γ_{J^*D} are independent of each other, which is valid when the number of relays is sufficiently high, as justified in [24]. Let us define the signal-to-interference-plus-noise ratio of the second hop as $\xi_D = \gamma_{R^*D}/(\gamma_{J^*D}+1)$, using (10) and (23), whose CDF can be formulated as

$$F_{\xi_D}(x) = 1 - K_r \sum_{k=0}^{K_r-1} (-1)^k \binom{K_r-1}{k} \frac{\varphi_k e^{\frac{-x}{\bar{\gamma}_{RD}\omega_k}}}{(k+1)(x+\varphi_k)} \tag{24}$$

where we have $\varphi_k = \lambda K_r \omega_k / ([(K_r-1)(1-\rho_{RD}^2)+1](1-\lambda))$.

$$\begin{aligned} P_{R\&S}^{\rm TBRS} = & \int_{\gamma_{th}^D}^{\infty} \left[1 - F_{\gamma_{R^*D}}\left(\gamma_{th}^D + \frac{\gamma_{th}^D\left(\gamma_{th}^D+1\right)}{x-\gamma_{th}^D}\right)\right] F_{\gamma_{R^*E}}\left(\gamma_{th}^E + \frac{\gamma_{th}^E\left(\gamma_{th}^E+1\right)}{x-\gamma_{th}^E}\right) f_{\gamma_{SR^*}}(x)dx \\ \approx & 2\sum_{n=0}^{N_t-1}\sum_{k=0}^{K_r-1}\sum_{m=0}^{N_t-1-n} (-1)^k \binom{K_r-1}{k}\binom{N_t-1}{n}\binom{N_t-1-n}{m} \frac{K_r \rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n \left(\gamma_{th}^D\right)^{N_t-1-n-m}}{(N_t-1-n)!(k+1)\bar{\gamma}_{SR}^{N_t-n-(m+1)/2}} \\ & \times \exp\left[-\left(\frac{\gamma_{th}^D}{\bar{\gamma}_{SR}} + \frac{\gamma_{th}^D}{\omega_k\bar{\gamma}_{RD}}\right)\right]\left[\left(\frac{\gamma_{th}^D\left(\gamma_{th}^D+1\right)}{\omega_k\bar{\gamma}_{RD}}\right)^{\frac{m+1}{2}} K_{m+1}\left(2\sqrt{\frac{\gamma_{th}^D\left(\gamma_{th}^D+1\right)}{\omega_k\bar{\gamma}_{SR}\bar{\gamma}_{RD}}}\right)\right. \\ & \left. - \exp\left(\frac{-\gamma_{th}^E}{\bar{\gamma}_{RE}}\right)\left(\frac{\gamma_{th}^D\left(\gamma_{th}^D+1\right)}{\omega_k\bar{\gamma}_{RD}} + \frac{\gamma_{th}^E\left(\gamma_{th}^E+1\right)}{\bar{\gamma}_{RE}+\gamma_{th}^D-\gamma_{th}^E}\right)^{\frac{m+1}{2}} K_{m+1}\left(2\sqrt{\frac{\gamma_{th}^D\left(\gamma_{th}^D+1\right)}{\omega_k\bar{\gamma}_{SR}\bar{\gamma}_{RD}} + \frac{\gamma_{th}^E\left(\gamma_{th}^E+1\right)}{\bar{\gamma}_{SR}\left(\bar{\gamma}_{RE}+\gamma_{th}^D-\gamma_{th}^E\right)}}\right)\right] \end{aligned} \tag{20}$$

$$\varsigma^{\rm TBRS}(R_0,R_s,\eta) = R_s\left\{1 - \left[\frac{N_t\left(1-\rho_{SR}^2\right)^{N_t-1}}{\sigma_{SR}^2} + \sum_{k=0}^{K_r-1}\frac{K_r(-1)^k}{\left[k\left(1-\rho_{RD}^2\right)+1\right]\sigma_{RD}^2}\binom{K_r-1}{k}\right] \times \frac{2^{2R_0}-1}{\eta}\right\}\frac{2^{2(R_0-R_s)}-1}{\sigma_{RE}^2\eta} \tag{21}$$

As far as the eavesdropper is concerned, γ_{R^*E} and γ_{J^*E} are independent and exponentially distributed. Furthermore, for $\xi_E = \gamma_{R^*E}/(\gamma_{J^*E}+1)$, we have

$$F_{\xi_E}(x) = 1 - \frac{\phi}{x+\phi} e^{\frac{-x}{\bar{\gamma}_{RE}}} \tag{25}$$

where $\phi = \lambda/(1-\lambda)$. According to the definition of COP and SOP in Section III-A, we can obtain the following closed-form approximations of the COP and the SOP.[4]

Lemma 1: The COP and the SOP of the JRJS strategy associated with feedback delays are approximated by

$$\begin{aligned} P_{\rm co}^{\rm JRJS}(R_0) \approx 1 - &\sum_{n=0}^{N_t-1}\sum_{k=0}^{K_r-1}\sum_{m=0}^{N_t-1-n}\binom{N_t-1}{n} \\ &\times \binom{K_r-1}{k}\binom{N_t-1-n}{m} \\ &\times \frac{(-1)^k(K_r+1)\rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n}{(N_t-1-n)!(k+1)\bar{\gamma}_{SR}^{N_t-n}} \\ &\times \frac{\Gamma(m+2)\hat{\varphi}_k\left(\gamma_{th}^D\right)^{N_t-n}\left(\gamma_{th}^D+1\right)^{m+1}}{\left(\gamma_{th}^D+\hat{\varphi}_k\right)^{m+2}} \\ &\times \exp\left[-\frac{\gamma_{th}^D(\hat{\varphi}_k-1)}{\bar{\gamma}_{SR}\left(\gamma_{th}^D+\hat{\varphi}_k\right)}\right] \\ &\times \Gamma\left(-m-1, \frac{\gamma_{th}^D\left(\gamma_{th}^D+1\right)}{\bar{\gamma}_{SR}\left(\gamma_{th}^D+\hat{\varphi}_k\right)}\right) \end{aligned} \tag{26}$$

where $\hat{\varphi}_k = K_r\lambda\omega_k\eta\sigma_{RD}^2/([(K_r-1)(1-\rho_{RD}^2)+1](1-\lambda)\eta\sigma_{RD}^2+K_r)$, and

$$\begin{aligned} P_{\rm so}^{\rm JRJS}(R_0,R_s) \approx &\sum_{n=0}^{N_t-1}\sum_{m=0}^{N_t-1-n}\binom{N_t-1}{n} \\ &\times \frac{\rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n}{m!\bar{\gamma}_{SR}^m} \\ &\times \frac{\left(2\gamma_{th}^E\right)^m\phi}{\left(2\gamma_{th}^E+\phi\right)}\exp\left[-\left(\frac{2\gamma_{th}^E}{\bar{\gamma}_{SR}}+\frac{2\gamma_{th}^E}{\bar{\gamma}_{RE}}\right)\right]. \end{aligned} \tag{27}$$

Proof: The proof is given in Appendix B.

The feasible range of the reliability constraint is similar to that of the TBRS strategy, and hence, it is omitted here.

B. Reliability–Security Ratio

Lemma 2: Recalling the definition in Section III, the RSR for the JRJS strategy may be expressed in (28), shown at the bottom of the page.

[4]When we have $\lambda \to 1$, (24) will degenerate into the TBRS case seen in (10). The performance analysis of the JRJS will be presented separately in the following, since several approximations have to be included.

It can be seen from the previous expression that, in contrast to the analysis of the TBRS strategy operating without jamming, for a fixed SNR threshold, the CDF of the second-hop SNR will converge to a nonzero limit. We also find that this limit is determined by the power sharing ratio between the relay and the jammer. Furthermore, according to the analysis of the TBRS strategy, for $\eta \to \infty$, we have $F_{\gamma_{SR^*}}(x) \to 0$. Thus, by exploiting the tight upper bound that $\gamma_D^{\rm TBRS} \le \min\{\gamma_{SR}, \gamma_{R^*D}\}$ and $\gamma_E^{\rm TBRS} \le \min\{\gamma_{SR}, \gamma_{R^*E}\}$, we have $P_{\rm co}^{\rm JRJS,\infty} \to F_{\gamma_{\xi_D}}(\gamma_{th}^D)$ and $1 - P_{\rm so}^{\rm JRJS,\infty} \to F_{\gamma_{\xi_E}}(\gamma_{th}^E)$. Finally, substituting the corresponding results into (16), we arrive at the RSR of the JRJS strategy.

Remark 4: It can be seen from the RSR expression of (28) again that the rate-pair setting (R_0, R_s) has an inconsistent influence on the RSR, and hence, we have to carefully adjust R_0 and R_s to balance the reliability versus security performance. Let us now focus our attention on the differences between the JRJS scheme and the TBRS arrangement.

First, we may find that the power sharing ratio λ between the relay and the jammer plays a very important role. The optimization of λ will be investigated from an effective secrecy throughput optimization point of view in the following.

Second, it is plausible that, in contrast to the behavior of the TBRS strategy, $\Lambda^{\rm JRJS}$ of (28) is only related to the delay of the second hop, but it is still a monotonically decreasing function of ρ_{RD}. This implies that the improvement of the channel quality of the JRJS will achieve a more pronounced COP improvement than the associated SOP improvement. Furthermore, recalling that the RSR is considered in the high-SNR region, it has no dependence on the first hop quality. This is due to the fact that if the first-hop channel quality is sufficiently high for ensuring a successful transmission, the asymptotic CDFs of ξ_D and ξ_E in (29) and (30) associated with $\eta \to \infty$ will converge to a nonzero limit at high SNRs, which ultimately dominates the COP and the SOP.

C. Effective Secrecy Throughput

Before proceeding to the effective secrecy throughput analysis, we also have to investigate the RSCP.

Lemma 3: The RSCP of our JRJS strategy may be approximated as in (31), shown at the bottom of the next page, where we have $\theta_{1,k} = (\gamma_{th}^D(\gamma_{th}^D+1))/(\gamma_{th}^D+\hat{\varphi}_k)$, $\theta_2 = \gamma_{th}^D - \gamma_{th}^E + (\gamma_{th}^E(\gamma_{th}^E+1)/(\gamma_{th}^E+\hat{\phi}))$, and $\hat{\phi} = \lambda\eta\sigma_{RE}^2/((1-\lambda)\eta\sigma_{RE}^2+1)$.

Proof: The proof is given in Appendix C.

Apart from the rate pair (R_0, R_s), the aforementioned $P_{R\&S}^{\rm JRJS}$ of (31) is also a function of the power sharing ratio λ between the selected relay and the jammer.

Given the complexity of the RSCP expression, it is quite a challenge to find a closed-form result for maximizing the

$$\Lambda^{\rm JRJS} = \frac{(2^{2R_0}-1)}{\left(2^{2(R_0-R_s)}-1\right)}\sum_{k=0}^{K_r-1}\binom{K_r-1}{k}\frac{(-1)^k K_r\left[(K_r-1)\left(1-\rho_{RD}^2\right)+1\right]\left[(\lambda^{-1}-1)\left(2^{2(R_0-R_s)}-1\right)+1\right]}{\left[(K_r-1)\left(1-\rho_{RD}^2\right)+1\right](k+1)(\lambda^{-1}-1)(2^{2R_0}-1)+K_r\left[k\left(1-\rho_{RD}^2\right)+1\right]} \tag{28}$$

effective secrecy throughput that $\max_{0<\lambda<1} \varsigma = R_s P_{R\&S}^{\mathrm{JRJS}}$. Alternatively, we can focus on the asymptotic analysis in the high-SNR region and try to find a general closed-form solution for λ. Specifically, when we have $\eta \to \infty$, $P_{R\&S}^{\mathrm{JRJS}}$ will be dominated by the channel quality of the second hop; hence, we have

$$P_{R\&S}^{\mathrm{JRJS},\infty}(R_0, R_s, \lambda) \approx \Pr\left\{\xi_D > \gamma_{th}^D, \xi_E < \gamma_{th}^E\right\} = \left[1 - F_{\xi_D}\left(\gamma_{th}^D\right)\right] F_{\xi_E}\left(\gamma_{th}^E\right) \quad (32)$$

where the approximation is based on the fact that, in contrast to both $F_{\xi_D}(\gamma_{th}^D)$ and $F_{\xi_E}(\gamma_{th}^E)$, which converge to a nonzero limit regardless of η, the first hop's $F_{\gamma_{SR}}(x)$ will tend to zero, and hence, it can be neglected. Substituting the asymptotic results of (29) and (30) into (33), we can obtain $P_{R\&S}^{\mathrm{JRJS},\infty}$. In contrast to the TBRS case operating without jamming, as the SNR tends to ∞, the RSCP will tend to a nonzero value and, upon increasing the transmit SNR beyond a certain limit, will no longer increase the effective secrecy throughput.

Then, based on (32), we arrive at the approximated optimal value λ_{opt}, which is the solution of the following equation:

$$\frac{\partial P_{R\&S}^{\mathrm{JRJS},\infty}(R_0, R_s, \lambda)}{\partial \lambda} = 0. \quad (33)$$

Then, by exploiting the approximation of $[k(1-\rho_{RD}^2)+1]/(k+1) \approx 1 - \rho_{RD}^2$ in (29) for a large ρ_{RD} (practically, the CSI delay is small, and $\rho_{RD} \to 1$), we have

$$\lambda_{\mathrm{subopt}} = \frac{\sqrt{\left[(K_r-1)\left(1-\rho_{RD}^2\right)+1\right]\gamma_{th}}}{\sqrt{\left[(K_r-1)\left(1-\rho_{RD}^2\right)+1\right]\gamma_{th}} + \sqrt{K_r\left(1-\rho_{RD}^2\right)}} \quad (34)$$

where $\gamma_{th} = (2^{2R_0}-1)(2^{2(R_0-R_s)}-1)$. It is clear that this value is determined by the number of relays and (R_0, R_s).

V. Numerical Results

Both our numerical and Monte Carlo simulation results are presented here for verifying the theoretical PLS performance analysis of the multiple-relay-aided network under CSI feedback delays. Explicitly, the COP, SOP, RSCP, and RSR are validated for both the TBRS and JRJS strategies. Furthermore, the effects of feedback delays and system parameters (including the transmission rate pair (R_0, R_s) and the power sharing ratio λ between the relay and the jammer) on the achievable effective secrecy throughput are evaluated. The Rayleigh fading model is employed for characterizing all communication links in our system. Additionally, we set the total power to $P = 1$ and $\sigma_{SR}^2 = \sigma_{RD}^2 = \sigma_{RE}^2 = 1$, and used $T_{d_{SR}} = T_{d_{RD}} = T_d$.

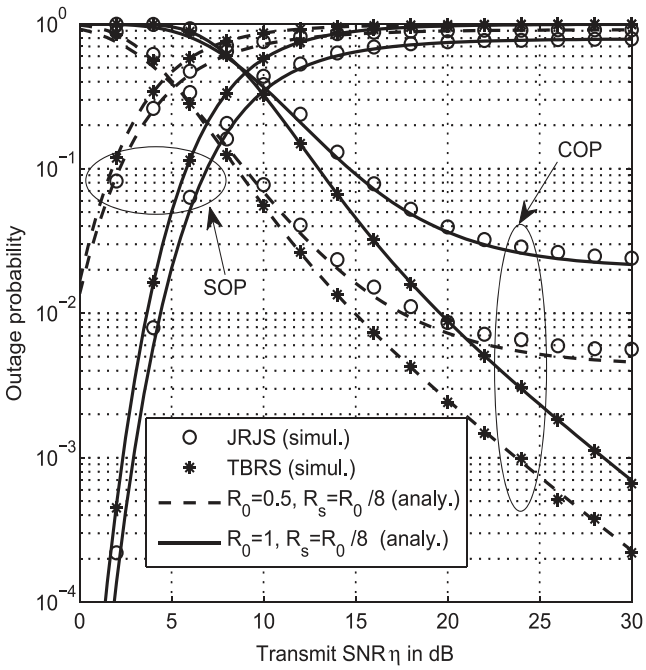

Fig. 2. COP and SOP versus transmit SNR for the TBRS and JRJS strategies in conjunction with different rate pairs, for $N_t = K_r = 3$, $f_d T_d = 0.1$, and $\lambda = 1/10$.

Fig. 2 plots the COP and the SOP versus the transmit SNR for both the TBRS and JRJS strategies in conjunction with different rate pairs. The analytical lines are plotted by using (11) and (14) for the TBRS strategy and by using (26) and (27) for the JRJS

$$P_{R\&S}^{\mathrm{JRJS}}(R_0, R_s, \lambda) \approx \sum_{n=0}^{N_t-1}\sum_{k=0}^{K_r-1}\sum_{m=0}^{N_t-1-n}(-1)^k \binom{N_t-1}{n}\binom{K_r-1}{k}\binom{N_t-1-n}{m} \times \frac{K_r \rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n \hat{\varphi}_k \left(\gamma_{th}^D\right)^{N_t-1-n-m}}{(N_t-1-n)!(k+1)\bar{\gamma}_{SR}^{N_t-n}\left(\gamma_{th}^D+\hat{\varphi}_k\right) e^{\frac{\gamma_{th}^D}{\bar{\gamma}_{SR}}+\frac{\gamma_{th}^D}{\bar{\gamma}_{RD}\omega_k}}} \times \left\{\theta_{1,k}^{m+1} e^{\frac{\theta_1}{\bar{\gamma}_{SR}}}\Gamma(m+2)\Gamma\left(-m-1, \frac{\theta_{1,k}}{\bar{\gamma}_{SR}}\right) - \frac{\hat{\phi} e^{-\gamma_{th}^E/\bar{\gamma}_{RE}}}{\left(\gamma_{th}^E+\phi\right)\left(\theta_{1,k}-\theta_2\right)}\Gamma(m+3) \times \left[\theta_2^{m+2} e^{\frac{\theta_2}{\bar{\gamma}_{SR}}}\Gamma\left(-m-2, \frac{\theta_2}{\bar{\gamma}_{SR}}\right) - \theta_{1,k}^{m+2} e^{\frac{\theta_1}{\bar{\gamma}_{SR}}}\Gamma\left(-m-2, \frac{\theta_{1,k}}{\bar{\gamma}_{SR}}\right)\right] + \Gamma(m+2)\left(\gamma_{th}^D - \gamma_{th}^E\right) \times \left[\theta_2^{m+1} e^{\frac{\theta_2}{\bar{\gamma}_{SR}}}\Gamma\left(-m-1, \frac{\theta_2}{\bar{\gamma}_{SR}}\right) - \theta_{1,k}^{m+1} e^{\frac{\theta_1}{\bar{\gamma}_{SR}}}\Gamma\left(-m-1, \frac{\theta_{1,k}}{\bar{\gamma}_{SR}}\right)\right]\right\} \quad (31)$$

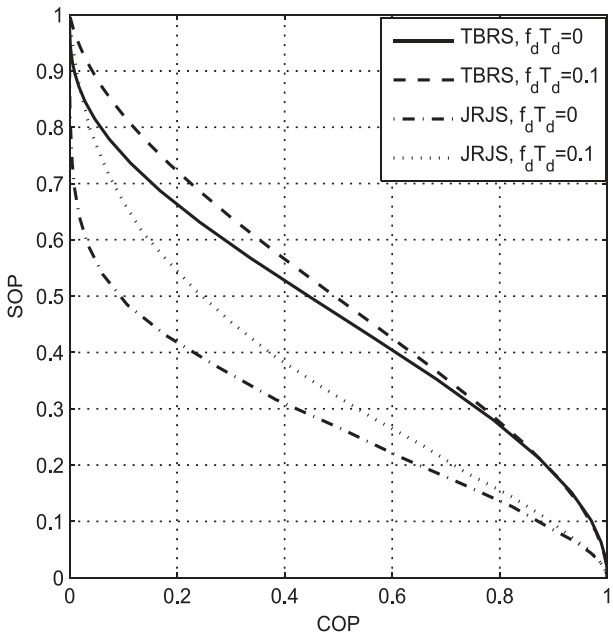

Fig. 3. SOP versus COP for the TBRS and JRJS strategies with different feedback delays for $N_t = K_r = 3$, $R_s = R_0/8$, and $\lambda = 1/10$.

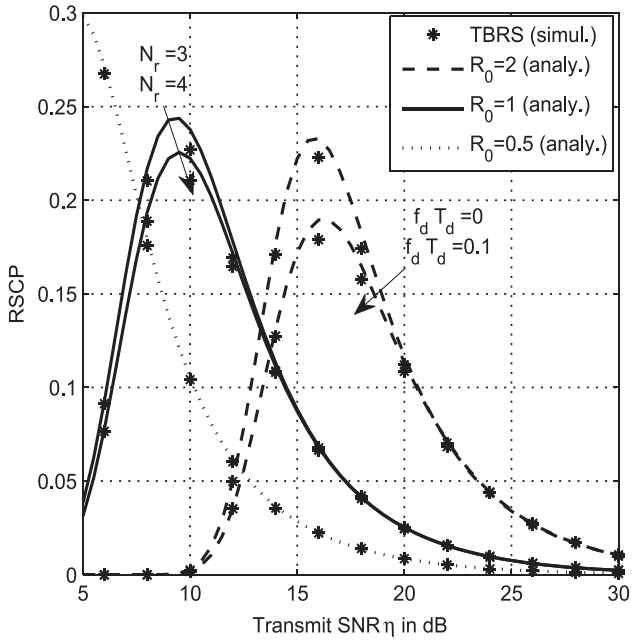

Fig. 4. RSCP versus transmit SNR for the TBRS strategy with different rate pairs for $N_t = K_r = 3$, $f_d T_d = 0.1$.

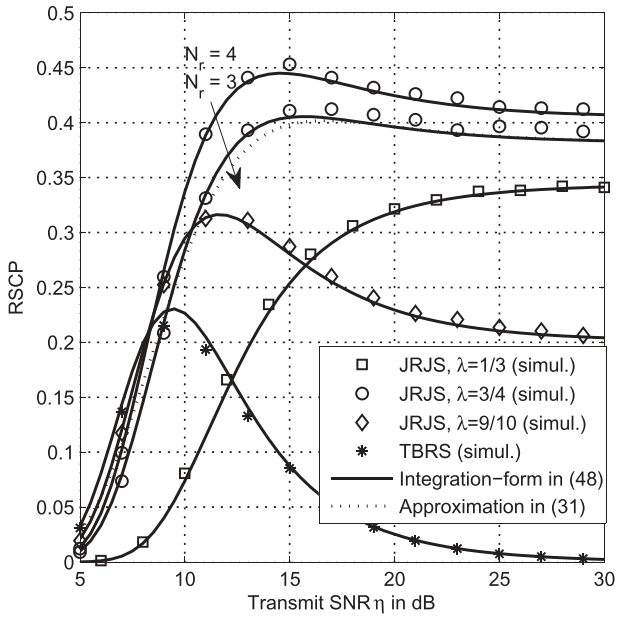

Fig. 5. RSCP versus transmit SNR for the JRJS strategy for different power sharing ratios λ and for $N_t = K_r = 3$, $f_d T_d = 0.1$, and $R_0 = 1$, $R_s = R_0/8$.

case, respectively. It can be clearly seen from the figure that the analytical and simulated outage probability curves match well, which confirms the accuracy of the mathematical analysis. As expected, compared with the TBRS strategy, the SOP of the JRJS strategy is much better, whereas the COP is worse. We can also find that both the COP and the SOP will converge to an outage floor at high SNRs for the JRJS strategy. The reason for this is that the jammer also imposes interference on the destination and the interference inflicted increases with the SNR. Thus, the designers have to take into account the tradeoff between the reliability and the security and the interference imposed on D, particularly when considering the JRJS strategy. Moreover, we can observe in Fig. 2 that increasing the transmission rate decreases the COP and increases the SOP.

Fig. 3 further characterizes the SOP versus COP for both the TBRS and JRJS strategies based on the numerical results in Fig. 2, which shows the tradeoff between the reliability and the security. It can be seen from the figure that the SOP decreases as the COP increases, and for a specific COP, the SOP of the JRJS scheme is strictly lower than that of TBRS. This confirms that the JRJS scheme performs better than the conventional TBRS scheme. Furthermore, the CSI feedback delay will also degrade the system tradeoff performance.

Fig. 4 illustrates the RSCP versus transmit SNR for the TBRS strategy in the context of different network configurations, including different rate pairs, different number of relays, and both perfect and outdated CSI feedback scenarios. The analytical lines are plotted by using the approximation in (20). We may conclude from the figure that the rate-pair setting (R_0, R_s) determines both the reliability and security transmission performance. These curves also show that the RSCP is a concave function of the transmit SNR, whereas the continued boosting of the SNR would only decrease the probability of a successful transmission. We can observe from Fig. 4 that, for a high transmit SNR, total reliability can be guaranteed, whereas the associated grade of security is severely eroded. Furthermore, increasing the number of relays and decreasing the feedback delay will improve both the reliability and security performance.

The RSCP of the JRJS strategy is presented in Fig. 5 for different power sharing ratios between relaying and jamming. Both the integration form (45) and the approximated closed form in (31) match well with the Monte Carlo simulations. The performance of the TBRS strategy is also included for comparison. The JRJS scheme outperforms the TBRS operating

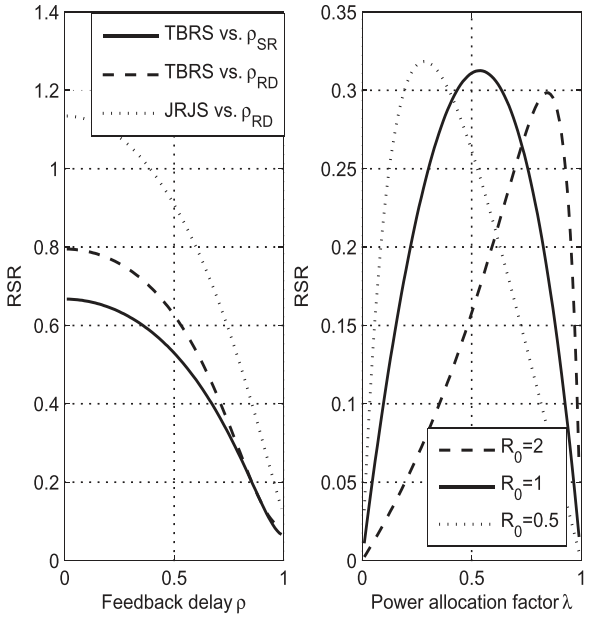

Fig. 6. RSR versus feedback delay coefficient ($R_0 = 1$, $R_s = R_0/8$, $\lambda = 3/4$) and power sharing ratio λ ($R_s = R_0/8$, $\rho_{SR} = \rho_{RD} = 0.9$) for the TBRS and JRJS strategies, with $N_t = K_r = 3$.

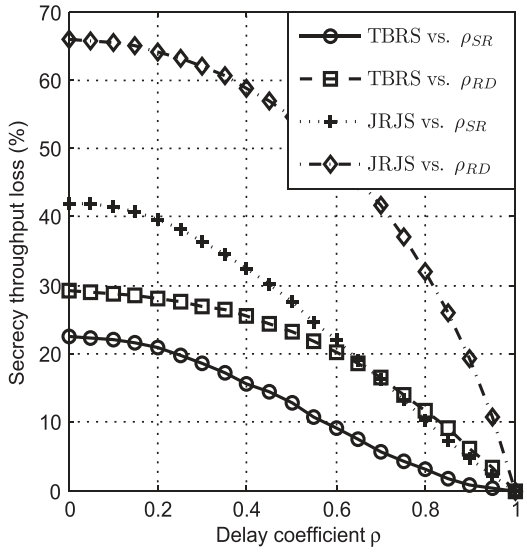

Fig. 7. Percentage secrecy throughput loss versus delay coefficients with $N_t = K_r = 3$, $R_0 = 1$, $R_s = R_0/8$, $\lambda = 3/4$, and $\eta = 10$ dB.

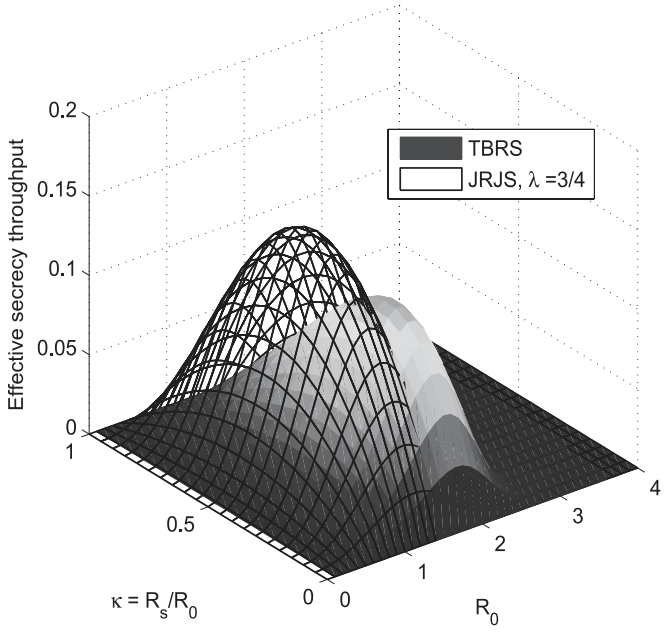

Fig. 8. Secrecy throughput versus R_0 and $\kappa = R_s/R_0$ for both the TBRS and JRJS strategies with $N_t = K_r = 3$, $f_d T_d = 0.1$, and $\eta = 15$ dB.

without jamming under the scenario considered when encountering comparable relay–destination and relay–eavesdropper channels. For some extreme configurations (when the relay–eavesdropper links are comparatively weak), this statement may not hold, but this scenario is beyond the scope of this paper. The maximum RSCP appears at about $\eta = 15$ dB for the JRJS strategy using $\lambda = 3/4$, whereas it is $\eta = 10$ dB for the TBRS strategy. Furthermore, as expected, increasing the number of available relays and jamming nodes will always be able to improve the reliability and security performance. However, the continued boosting of the jammer's power (decreasing λ) will not always improve the overall performance, because the interference improves initially the security, but then, it starts to reduce the reliability as λ decreases. This further motivates the designer to carefully take into account the power sharing between relaying and jamming. The effect of the rate-pair setting on the security and reliability of the JRJS strategy is neglected here, which follows a similar trend to that of the TBRS strategy.

Fig. 6 characterizes the RSR versus feedback delay and power sharing ratio for both TBRS and JRJS, in which the RSR curves are plotted by using (17) and (28), respectively. The first illustration shows that the RSR decreases as the delay coefficients (ρ_{SR} and ρ_{RD}), which confirms that the improvement of reliability becomes more pronounced than the reduction of the security as the feedback delay decreases. This observation implies an improvement in terms of the security–reliability tradeoff. In addition, the RSR versus ρ_{RD} is larger than that of ρ_{SR}, which indicates that the impact of the second-hop CSI feedback delay is more prominent. The other illustration in the right demonstrates that the RSR is a concave function of the power sharing ratio, which reflects the tradeoff between the reliability and the security struck by adjusting λ.

To further evaluate the effect of feedback delays on the secrecy performance, Fig. 7 plots the resultant percentage of secrecy throughput loss versus the delay, which is defined as

$$\varsigma_{\text{loss}} = \frac{\varsigma_{\text{no-delay}} - \varsigma_{\text{delay}}}{\varsigma_{\text{no-delay}}}. \tag{35}$$

It can be seen from the figure that, compared with the TBRS scheme, JRJS is more sensitive to the feedback delays. Furthermore, recalling that increasing the delay coefficient ρ_{SR} of the first hop improves the reliability, but at the same time also helps the eavesdropper, it is not surprising that the secrecy throughput loss due to the second-hop feedback delay is more pronounced.

Fig. 8 illustrates the achievable effective secrecy throughput for both the TBRS and JRJS strategies versus the codeword

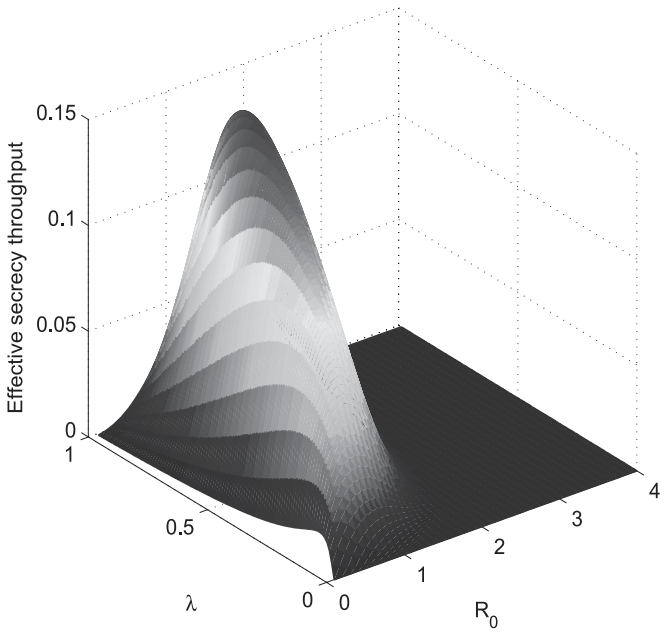

Fig. 9. Secrecy throughput versus R_0 and λ for the JRJS strategy with $N_t = K_r = 3$, $f_d T_d = 0.1$, $\eta = 15$ dB, and $R_s/R_0 = 1/8$.

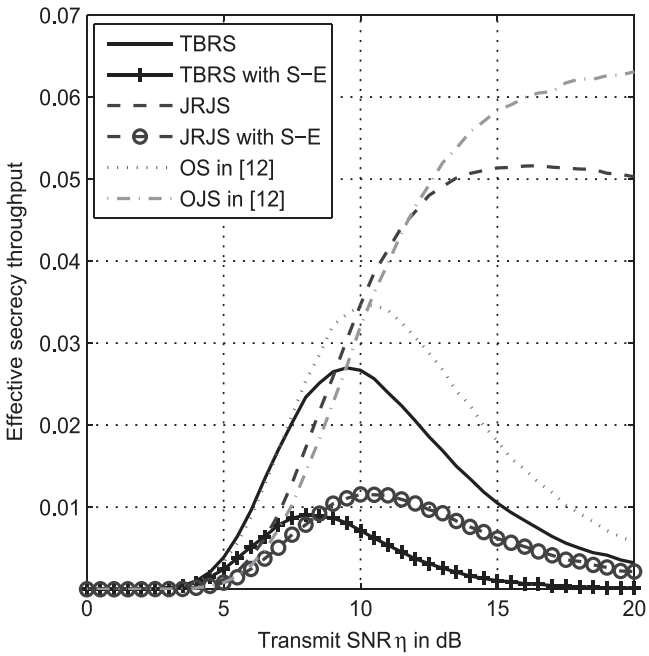

Fig. 10. Comparisons for different strategies with and without the S–E link, for $N_t = K_r = 3$, $R_0 = 1$, $R_s = R_0/8$, $f_d T_d = 0.1$, and $\lambda = 3/4$.

transmission rate R_0 and the secrecy code ratio $\kappa = R_s/R_0$ with no outage constraints ($\upsilon = \delta = 1$). The values of the effective secrecy throughput are plotted by using $\varsigma = R_s P_{R\&S}$. We can observe in Fig. 8 that, subject to a fixed code rate ratio κ, the effective secrecy throughput increases to a peak value as R_0 reaches its optimal value and then decreases. This phenomenon can be explained as follows. At a low transmission rate, although the COP increases with R_0, which has a negative effect on the effective secrecy throughput, both the secrecy rate and the SOP performance will benefit. However, after reaching the optimal R_0, the effective secrecy throughput drops since the main link cannot afford a reliable transmission, and the resultant COP increase becomes dominant. On the other hand, subject to a fixed R_0 (which results in a constant COP), the effective secrecy throughput is also a concave function of κ, and increasing the code rate ratio ultimately results in an increased secrecy information rate at the cost of an increased SOP.

The achievable effective secrecy throughput for the JRJS strategy is also presented in Fig. 8, and similar conclusions and trends can be observed to that of the TBRS case. Additionally, the comparison of the two strategies indicates that the JRJS scheme attains a higher effective secrecy throughput than the TBRS scheme operating without jamming, even if no power sharing optimization has been employed.

Fig. 9 further illustrates the impact of power sharing between the relay and the jammer on the achievable effective secrecy throughput of the JRJS strategy versus R_0 in the absence of outage constraints. Given a fixed code rate pair (R_0, R_s), the effective secrecy throughput follows the trend of the RSCP, which is a concave function of λ, as shown in Fig. 6. The interference introduced by the jammer initially improves both the reliability and the security as λ increases, but this trend is reversed beyond a certain point.

VI. Discussion

A. Impact of the S–E Link

We note that the introduction of the S–E link, i.e., the information leakage in the first phase, is very critical to the security. There are also some research studies focusing on the corresponding secure transmission design and performance evaluation for cooperative networks with the S–E link, such as [15] and [16]. Here, we assume that the eavesdropper can receive information directly from the source in the first phase. Thus, following the steps in the prior sections, for the TBRS and JRJS schemes, it is clear that the SNR experienced at the eavesdropper should be rewritten as

$$\tilde{\gamma}_E^{\tau} = \gamma_{SE} + \gamma_E^{\tau} \tag{36}$$

where $\gamma_{SE} = P_s |\mathbf{w}_{\rm opt}(t|T_{d_{SR}}) \mathbf{h}_{SE}(t)|^2 / N_0$ follows the exponential distribution with the average value $\bar{\gamma}_{SE}$, $\tau = \{\text{TBRS}, \text{JRJS}\}$, and γ_E^{τ} has been defined in (4) and (7).

Then, the corresponding SOP, RSCP, and effective secrecy throughput have to be reconsidered. Unfortunately, to the best of our knowledge, it is a mathematically intractable problem to obtain closed-form results for the related performance evaluations. Therefore, we resorted to numerical simulations for further investigating the impact of the S–E link. Fig. 10 compares the effective secrecy throughput of the TBRS and JRJS schemes both with and without considering the direct S–E link. It becomes clear that the information leakage in the first phase will lead to a severe security performance degradation, particularly for the JRJS scheme, which will no longer be capable of maintaining a steady throughput at high SNRs. The reason for this trend is that increasing the transmit SNR will help the eavesdropper in the presence of the direct S–E link.

B. Comparisons

Here, based on the outdated CSI assumption, we provide performance comparisons with a range of other schemes advocated in [12] with the aid of the proposed outage-based characterization. Fig. 10 also incorporates our effective secrecy throughput performance comparison, where the optimal selection (OS) regime and the optimal selection combined with jamming (OSJ) were proposed in [12]. They are formulated as

$$\text{OS}: R^* = \arg\max_{R_k \in \mathcal{R}} \left\{ \frac{\tilde{\gamma}_{R_k D}}{\tilde{\gamma}_{R_k E}} \right\} \tag{37}$$

$$\text{OSJ}: \begin{cases} R^* = \arg\max_{R_k \in \mathcal{R}} \left\{ \frac{\tilde{\gamma}_{R_k D}}{\tilde{\gamma}_{R_k E}} \right\} \\ J^* = \arg\min_{R_k \in \mathcal{R}-R^*} \left\{ \frac{\tilde{\gamma}_{R_k D}}{\tilde{\gamma}_{R_k E}} \right\} \end{cases} \tag{38}$$

where $\tilde{\gamma}_{R_k E}$ is the delayed version of the instantaneous CSI of the R–E link. It should be noted that this constitutes an entirely new performance characterization of these schemes from the perspective of the effective secrecy throughput. It is shown in Fig. 1 that the selection combined with jamming outperforms the corresponding nonjamming techniques at high SNRs, albeit this trend may no longer prevail at low SNRs. In comparison, compared with those selections relying on the average SNRs of the R–E link, the optimal selections relying on the idealized simplifying assumptions of having global CSI (OS and OSJ schemes) knowledge can only achieve throughput gains at high SNRs due to the inevitable feedback delay.

VII. Conclusion

An outage-based characterization of cooperative relay networks has been provided in the face of CSI feedback delays. Two types of relaying strategies were considered, namely, the TBRS strategy and the JRJS strategy. Closed-form expressions of the COP, the SOP, and the RSCP, as well as of the RSR, were derived. The RSR results demonstrated that the reliability is improved more substantially than the security performance when the CSI feedback delays are reduced. Furthermore, we presented a modified effective secrecy throughput definition and demonstrated that the JRJS strategy achieves a significant effective secrecy throughput gain over the TBRS strategy. The transmit SNR, the secrecy codeword rate setting, and the power sharing ratio between the relay and jammer nodes play important roles in striking a balance between the reliability and the security in terms of the secrecy throughput. The impact of the direct S–E link and the performance comparisons with other selection schemes were also included. Additionally, our results demonstrate that JRJS is more sensitive to the feedback delays and that the secrecy throughput loss due to the second-hop feedback delay is more pronounced than that due to the first-hop one.

Appendix A
Proof of Proposition 1

To simplify the asymptotic performance analysis, (3) can be expressed in a more mathematically tractable form by the commonly used tight upper bound of $\gamma_D^{\text{TBRS}} \leq \min\{\gamma_{SR}, \gamma_{R^*D}\}$ and $\gamma_E^{\text{TBRS}} \leq \min\{\gamma_{SR}, \gamma_{R^*E}\}$. When we have $\eta \to \infty$, based on the CDFs in (9) and (10) and closing the smallest order terms of x/η, we have

$$\begin{aligned} F_{\gamma_{SR}}(x) \to & 1 - \left[\sum_{n=0}^{N_t-1} \binom{N_t-1}{n} \rho_{SR}^{2(N_t-1-n)} \left(1-\rho_{SR}^2\right)^n \right. \\ & + \sum_{n=0}^{N_t-2} \binom{N_t-1}{n} \times \rho_{SR}^{2(N_t-1-n)} \\ & \left. \times \left(1-\rho_{SR}^2\right)^n \frac{x}{\bar{\gamma}_{SR}} + \mathcal{O}\left(\frac{x}{\bar{\gamma}_{SR}}\right) \right] \\ & \times \left[1 - \frac{x}{\bar{\gamma}_{SR}} + \mathcal{O}\left(\frac{x}{\bar{\gamma}_{SR}}\right) \right] \\ = & 1 - \left[1 + \left(1 - \left(1-\rho_{SR}^2\right)^{N_t-1} \right) \frac{x}{\bar{\gamma}_{SR}} + \mathcal{O}\left(\frac{x}{\bar{\gamma}_{SR}}\right) \right] \\ & \times \left[1 - \frac{x}{\bar{\gamma}_{SR}} + \mathcal{O}\left(\frac{x}{\bar{\gamma}_{SR}}\right) \right] \\ = & \left(1-\rho_{SR}^2\right)^{N_t-1} \frac{x}{\bar{\gamma}_{SR}} + \mathcal{O}\left(\frac{x}{\bar{\gamma}_{SR}}\right) \end{aligned} \tag{39}$$

where $\mathcal{O}(x)$ denotes the high-order infinitely small contributions as a function of x, and

$$\begin{aligned} F_{\gamma_{R^*D}}(x) \to & 1 - \sum_{k=0}^{K_r-1} (-1)^k \frac{K_r}{k+1} \binom{K_r-1}{k} \\ & \times \left[1 - \frac{k+1}{k\left(1-\rho_{RD}^2\right)+1} \frac{x}{\bar{\gamma}_{RD}} + \mathcal{O}\left(\frac{x}{\bar{\gamma}_{RD}}\right) \right] \\ = & \sum_{k=0}^{K_r-1} (-1)^k \binom{K_r-1}{k} \frac{K_r}{k\left(1-\rho_{RD}^2\right)+1} \\ & \times \frac{x}{\bar{\gamma}_{RD}} + \mathcal{O}\left(\frac{x}{\bar{\gamma}_{RD}}\right). \end{aligned} \tag{40}$$

Then, applying the upper bound of the receiver SNR, we may rewrite the COP and the SOP of the TBRS strategy at high SNRs as

$$\begin{aligned} P_{\text{co}}^{\text{TBRS},\infty} = & 1 - \left(1 - F_{\gamma_{SR^*}}\left(\gamma_{th}^D\right)\right)\left(1 - F_{\gamma_{R^*D}}\left(\gamma_{th}^D\right)\right) \\ = & \left[\frac{\left(1-\rho_{SR}^2\right)^{N_t-1}}{\sigma_{SR}^2} + \sum_{k=0}^{K_r-1} (-1)^k \right. \\ & \left. \times \binom{K_r-1}{k} \frac{K_r}{\left[k\left(1-\rho_{RD}^2\right)+1\right]\sigma_{RD}^2} \right] \frac{2^{2R_0}-1}{\eta} \end{aligned} \tag{41}$$

and according to the fact that γ_{R^*E} is exponentially distributed, we have

$$\begin{aligned} 1 - P_{\text{so}}^{\text{TBRS},\infty} = & 1 - \left(1 - F_{\gamma_{SR^*}}\left(\gamma_{th}^E\right)\right)\left(1 - F_{\gamma_{R^*E}}\left(\gamma_{th}^E\right)\right) \\ = & \left[\frac{\left(1-\rho_{SR}^2\right)^{N_t-1}}{\sigma_{SR}^2} + \frac{1}{\sigma_{RE}^2} \right] \frac{2^{2(R_0-R_s)}-1}{\eta}. \end{aligned} \tag{42}$$

Finally, substituting (41) and (42) into the definition of RSR in (16), we can obtain (17).

APPENDIX B
PROOF OF LEMMA 1

According to the description of COP and SOP, replacing $F_{\gamma_{R^*D}}(x)$ and $F_{\gamma_{R^*E}}(x)$ by $F_{\xi_D}(x)$ and $F_{\xi_E}(x)$ in (12) and (14) will involve a mathematically intractable integration of the form

$$\Upsilon(a,b,\mu,\nu)=\int_0^\infty \frac{z^a}{z+b}\exp\left(-\mu z-\frac{\nu}{z}\right)dz \tag{43}$$

which, to the best of our knowledge, does not have a closed-form solution. Alternatively, bearing in mind that the preceding integration has a great matter with ξ_D, we now focus our attention on the approximation of ξ_D. Based on the PDF results in (23), it may be seen that γ_{J^*D} obeys an exponential distribution. Then, we can approximate $\hat{\gamma}_{J^*D}=\gamma_{J^*D}+1$ by the exponential distribution as well, with an average value of $\mathbb{E}\{\hat{\gamma}_{J^*D}\}=([(K_r-1)(1-\rho_{RD}^2)+1]\bar{\gamma}_{RD}+K_r)/K_r$ by assuming that the AWGN term "1" is part of the stochastic mean terms. The approximation based on this method provides a very accurate analysis, and the accuracy of this method is verified by the numerical results of [34]. Thus, the CDF of $\hat{\xi}_D=\gamma_{R^*D}/\hat{\gamma}_{J^*D}$ can be derived as

$$F_{\hat{\xi}_D}(x)=\sum_{k=0}^{K_r-1}(-1)^k\binom{K_r-1}{k}\frac{K_r}{k+1}\frac{x}{x+\hat{\varphi}_k} \tag{44}$$

where $\hat{\varphi}_k=\mathbb{E}\{\gamma_{R^*D}\}\mathbb{E}/\{\hat{\gamma}_{J^*D}\}$.

Then, substituting (44) into (11), we have

$$\begin{aligned}F_{\gamma_D^{\mathrm{JRJS}}}(x)\approx&\sum_{n=0}^{N_t-1}\sum_{k=0}^{K_r-1}\sum_{m=0}^{N_t-1-n}\binom{N_t-1}{n}\binom{K_r-1}{k}\binom{N_t-1-n}{m}\\&\times\frac{(-1)^kK_r\rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n\varphi_k x^{N_t-1-n-m}e^{-\frac{x}{\bar{\gamma}_{SR}}}}{(N_t-1-n)!(k+1)\bar{\gamma}_{SR}^{N_t-n}(x+\varphi_k)}\\&\times\int_0^\infty\frac{z^{m+1}}{z+\frac{x(x+1)}{x+\varphi_k}}\exp\left(-\frac{z}{\bar{\gamma}_{SR}}\right)dz.\end{aligned} \tag{45}$$

Using [33, eq. (3.383.10)], we can obtain the CDF of γ_D^{JRJS} as

$$\begin{aligned}F_{\gamma_D^{\mathrm{JRJS}}}(x)\approx1-&\sum_{n=0}^{N_t-1}\sum_{k=0}^{K_r-1}\sum_{m=0}^{N_t-1-n}\binom{N_t-1}{n}\\&\times\binom{K_r-1}{k}\binom{N_t-1-n}{m}\\&\times\frac{(-1)^k(K_r+1)\rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n}{(N_t-1-n)!(k+1)\bar{\gamma}_{SR}^{N_t-n}}\\&\times\frac{\Gamma(m+2)\hat{\varphi}_k x^{N_t-n}(x+1)^{m+1}}{(x+\hat{\varphi}_k)^{m+2}}\\&\times\exp\left[-\frac{x(\hat{\varphi}_k-1)}{\bar{\gamma}_{SR}(x+\hat{\varphi}_k)}\right]\\&\times\Gamma\left(-m-1,\frac{x(x+1)}{\bar{\gamma}_{SR}(x+\hat{\varphi}_k)}\right).\end{aligned} \tag{46}$$

Finally, substituting $x=\gamma_{th}^D$ into (46), we obtain $P_{\mathrm{co}}^{\mathrm{JRJS}}$.

As far as the SOP is considered, we exploit the commonly used tight upper bound of $\gamma_E^{\mathrm{JRJS}}\geq(1/2)\min\{\gamma_{SR},\xi_E\}$ to calculate it, which may be rewritten as

$$\begin{aligned}P_{\mathrm{so}}^{\mathrm{JRJS}}&\approx\Pr\left\{\frac{1}{2}\min\{\gamma_{SR},\xi_E\}>\gamma_{th}^E\right\}\\&=\left[1-F_{\gamma_{SR}}\left(2\gamma_{th}^E\right)\right]\left[1-F_{\xi_E}\left(2\gamma_{th}^E\right)\right].\end{aligned} \tag{47}$$

Substituting (9) and (25) into (47), we obtain $P_{\mathrm{so}}^{\mathrm{JRJS}}$.

APPENDIX C
PROOF OF LEMMA 3

According to the definition of the RSCP in (18), we can calculate it by

$$\begin{aligned}P_{RS}^{\mathrm{JRJS}}=&\int_0^\infty\left[1-F_{\xi_D}\left(\gamma_{th}^D+\frac{\gamma_{th}^D\left(\gamma_{th}^D+1\right)}{z}\right)\right]\\&\times F_{\xi_E}\left(\gamma_{th}^E+\frac{\gamma_{th}^E\left(\gamma_{th}^E+1\right)}{z+\gamma_{th}^D-\gamma_{th}^E}\right)f_{\gamma_{SR^*}}\left(z+\gamma_{th}^D\right)dz.\end{aligned} \tag{48}$$

To make the integration mathematically tractable, we invoke a simple approximation for $F_{\xi_E}(x)$ by treating the AWGN term "1" in $\xi_E=\gamma_{R^*E}/(\gamma_{J^*E}+1)$ as part of the stochastic mean terms. Hence, we have

$$F_{\xi_E}(x)=\frac{x}{x+\hat{\phi}} \tag{49}$$

where $\hat{\phi}=\lambda\eta\sigma_{RE}^2/((1-\lambda)\eta\sigma_{RE}^2+1)$.

Then, replacing the corresponding CDFs of the second hop with $F_{\hat{\xi}_D}(x)$ and $F_{\hat{\xi}_E}(x)$ in (26), the integration can be derived as

$$\begin{aligned}P_{RS}^{\mathrm{JRJS}}\approx1-&\sum_{n=0}^{N_t-1}\sum_{k=0}^{K_r-1}\sum_{m=0}^{N_t-1-n}(-1)^k\binom{N_t-1}{n}\\&\times\binom{K_r-1}{k}\binom{N_t-1-n}{m}\\&\times\frac{(K_r+1)\rho_{SR}^{2(N_t-1-n)}\left(1-\rho_{SR}^2\right)^n}{(N_t-1-n)!(k+1)\bar{\gamma}_{SR}^{N_t-n}}\\&\times\frac{\hat{\varphi}_k\left(\gamma_{th}^D\right)^{N_t-1-n-m}}{\gamma_{th}^D+\hat{\varphi}_k}\exp\left(-\frac{\gamma_{th}^D}{\bar{\gamma}_{SR}}-\frac{\gamma_{th}^D}{\omega_k\bar{\gamma}_{RD}}\right)\\&\times\int_0^\infty e^{\frac{-z}{\bar{\gamma}_{SR}}}z^{m+1}\Bigg[\frac{1}{z+\theta_{1,k}}-\frac{\hat{\phi}\left(z+\gamma_{th}^D-\gamma_{th}^E\right)e^{\frac{-\gamma_{th}^E}{\bar{\gamma}_{RE}}}}{\left(\gamma_{th}^E+\hat{\phi}\right)(\theta_{1,k}-\theta_2)}\\&\times\left(\frac{1}{z+\theta_2}-\frac{1}{z+\theta_{1,k}}\right)\Bigg]dz\end{aligned} \tag{50}$$

where $\hat{\varphi}_k$ and $\hat{\phi}$ are introduced by relying on the similar approximation as in Appendix B. Then, using [33, eq. (3.383.10)], we obtain $P_{R\&S}^{\mathrm{JRJS}}$.

REFERENCES

[1] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, Sep. 1998.

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

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[4] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[5] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[6] Y. W. P. Hong, P. C. Lan, and C. C. J. Kuo, "Enhancing physical-layer secrecy in multi-antenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.

[7] R. Bassily *et al.*, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[8] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[9] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[10] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[11] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2653–2661, Jul. 2014.

[12] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[13] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensic Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[14] Z. Ding, M. Xu, J. Lu, and F. Liu, "Improving wireless security for bidirectional communication scenarios," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2842–2848, Jul. 2012.

[15] C. Wang, H. M. Wang, and X. G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589–605, Feb. 2015.

[16] H. Deng, H. M. Wang, W. Guo, and W. Wang, "Secrecy transmission with a helper: To relay or to jam," *IEEE Trans. Inf. Forensic Security*, vol. 10, no. 2, pp. 293–307, Feb. 2015.

[17] B. He, X. Zhou, and T. D. Abhayapala, "Wireless physical layer security with imperfect channel state information: A survey," *ZTE Commun.*, vol. 11, no. 3, pp. 11–19, Sep. 2013.

[18] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[19] J. Zhang and M. C. Gursoy, "Relay beamforming strategies for physical-layer security," in *Proc. CISS*, Princeton, NJ, USA, Mar. 2010, pp. 1–6.

[20] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[21] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[22] J. Hu, Y. Cai, N. Yang, and W. Yang, "A new secure transmission scheme with outdated antenna selection," *IEEE Trans. Inf. Forensics Security*, to be published.

[23] J. Hu, W. Yang, N. Yang, X. Zhou, and Y. Cai, "On-off-based secure transmission design with outdated channel state information," *IEEE Trans. Veh. Technol.*, to be published.

[24] N. E. Wu and H. J. Li, "Effect of feedback delay on secure cooperative networks with joint relay and jammer selection," *IEEE Wireless Commun. Lett.*, vol. 2, no. 4, pp. 415–418, Aug. 2013.

[25] X. Guan Y. Cai and Y. Yang, "Secure transmission design and performance analysis for cooperation exploring outdated CSI," *IEEE Commun. Lett.*, vol. 18, no. 9, pp. 1637–1640, Sep. 2014.

[26] L. Wang, S. Xu, W. Yang, W. Yang, and Y. Cai, "Security performance of multiple antennas multiple relaying networks with outdated relay selection," in *Proc. WCSP*, Hefei, China, Oct. 2014, pp. 1–6.

[27] J. Huang and A. L. Swindlehurst, "Buffer-aided relaying for two-hop secure communication," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 152–164, Jan. 2015.

[28] S. I. Kim, I. M. Kim, and J. Heo, "Secure transmission for multiuser relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3724–3737, Jul. 2015.

[29] Y. Ma, D. Zhang, A. Leith, and Z. Wang, "Error performance of transmit beamforming with delayed and limited feedback," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1164–1170, Mar. 2009.

[30] Z. Rezki, A. Khisti, and M. S. Alouini, "Ergodic secret message capacity of the wirechannel with finite-rate feedback," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3364–3379, Jun. 2014.

[31] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.

[32] H. A. Suraweera, M. Soysa, C. Tellambura, and H. K. Garg, "Performance analysis of partial relay selection with feedback delay," *IEEE Signal Process. Lett.*, vol. 17, no. 6, pp. 531–534, Jun. 2010.

[33] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 6th ed. San Diego, CA, USA: Academic, 2000.

[34] S. Kim and J. Heo. "Outage probability of interference-limited amplify-and-forward relaying with partial relay selection," in *Proc. IEEE VTC*, Yokohama, Japan, May 2011, pp. 1–5.

Lei Wang (S'11) received the B.S. degree in electronics and information engineering from Central South University, Changsha, China, in 2004 and the M.S. degree in communications and information systems from PLA University of Science and Technology, Nanjing, China, in 2011. He is currently working toward the Ph.D. degree in communications and information systems with PLA University of Science and Technology.

His current research interests include cooperative communications, signal processing in communications, and physical layer security.

Yueming Cai (M'05–SM'12) received the B.S. degree in physics from Xiamen University, Xiamen, China, in 1982 and the M.S. degree in microelectronics engineering and the Ph.D. degree in communications and information systems from Southeast University, Nanjing, China, in 1988 and 1996, respectively.

He is currently with the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China. His current research interests include multiple-input–multiple-output systems, orthogonal frequency-division multiplexing systems, signal processing in communications, cooperative communications, and wireless sensor networks.

Yulong Zou (SM'13) received the B.Eng. degree in information engineering from Nanjing University of Posts and Telecommunications (NUPT), Nanjing, China, in July 2006; the Ph.D. degree in electrical engineering from Stevens Institute of Technology, Hoboken, NJ, USA, in May 2012; and the Ph.D. degree in signal and information processing from NUPT in July 2012.

He is currently a Professor with NUPT. His research interests span a wide range of topics in wireless communications and signal processing, including cooperative communications, cognitive radio, wireless security, and energy-efficient communications.

Dr. Zou has been a symposium chair, a session chair, and a technical program committee member for several IEEE-sponsored conferences, including the IEEE Wireless Communications and Networking Conference, the IEEE Global Communications Conference, the IEEE International Conference on Communications, the IEEE Vehicular Technology Conference, and the International Conference on Communications in China. He serves on the editorial board of *IEEE Communications Surveys and Tutorials*, *IEEE Communications Letters*, *IET Communications*, and the *EURASIP Journal on Advances in Signal Processing*. He was a received the 2014 IEEE Communications Society Asia-Pacific Best Young Researcher award.

Weiwei Yang (S'08–M'12) received the B.S., M.S., and Ph.D. degrees from PLA University of Science and Technology, Nanjing, China, in 2003, 2006, and 2011, respectively.

He is currently with the College of Communications Engineering, PLA University of Science and Technology. His research interests are orthogonal frequency-domain multiplexing systems, signal processing in communications, cooperative communications, cognitive networks, and network security.

Lajos Hanzo (M'91–SM'92–F'04) received the M.S. degree in electronics and the Ph.D. degree from the Technical University of Budapest, Budapest, Hungary, in 1976 and 1983, respectively; the D.Sc. degree from the University of Southampton, Southampton, U.K., in 2004; and the "Doctor Honoris Causa" degree from the Technical University of Budapest in 2009.

During his 38-year career in telecommunications, he has held various research and academic posts in Hungary, Germany, and the U.K. Since 1986, he has been with the School of Electronics and Computer Science, University of Southampton, where he holds the Chair in Telecommunications. He is currently directing an academic research team, working on a range of research projects in the field of wireless multimedia communications sponsored by industry, the Engineering and Physical Sciences Research Council (EPSRC), the European Research Council's Advanced Fellow Grant, and the Royal Society's Wolfson Research Merit Award. During 2008–2012, he was a Chaired Professor with Tsinghua University, Beijing, China. He is an enthusiastic supporter of industrial and academic liaison and offers a range of industrial courses. He has successfully supervised about 100 Ph.D. students, coauthored 20 John Wiley/IEEE Press books on mobile radio communications totaling in excess of 10 000 pages, and published more than 1400 research entries on IEEE Xplore.

Dr. Hanzo is a Fellow of the Royal Academy of Engineering, the Institution of Engineering and Technology, and the European Association for Signal Processing. He is also a Governor of the IEEE Vehicular Technology Society. During 2008–2012, he was the Editor-in-Chief of IEEE Press. He has served as the Technical Program Committee Chair and the General Chair of IEEE conferences, has presented keynote lectures, and has received a number of distinctions. His published work has more than 20 000 citations. Further information on research in progress and associated publications is available at http://www-mobile.ecs.soton.ac.uk.

AUTHOR QUERIES

AUTHOR PLEASE ANSWER ALL QUERIES

AQ1 = RV was expanded as “random variable.” Please check if appropriate. Otherwise, please make the necessary changes.
AQ2 = Equations (29) and (30) are missing in the document. Please check.
AQ3 = Please provide publication update in Ref [22].
AQ4 = Please provide publication update in Ref [23].
AQ5 = Current affiliation of author Yueming Cai was provided as captured from the first footnote. Please check if appropriate. Otherwise, please make the necessary changes.
AQ6 = Please confirm that Dr. Zou has received two Ph.D. degrees.
AQ7 = Current affiliation of author Weiwei Yang was provided as captured from the first footnote. Please check if appropriate. Otherwise, please make the necessary changes.

END OF ALL QUERIES