Physical-Layer Security in Full-Duplex Multi-Hop Multi-User Wireless Network With Relay Selection

Saman Atapattu, *Member, IEEE*, Nathan Ross, Yindi Jing, *Member, IEEE*, Yuanyuan He, *Member, IEEE*, and Jamie S. Evans, *Senior Member, IEEE*

***Abstract*— This paper investigates the relay selection (RS) problem for multi-hop full-duplex relay networks where multiple source–destination (SD) pairs compete for the same pool of relays, under the attack of multiple eavesdroppers. To enhance the physical-layer security, within a given coherence time, our objective is to jointly assign the available relays at each hop to different SD pairs to maximize the minimum secrecy rate among all pairs. Two RS schemes, optimal RS and suboptimal RS (SRS), are proposed for two-hop networks based on global channel state information (CSI) and only SD pairs CSI, respectively. Since all users can communicate within the same coherence time, our joint RS schemes are important for the user-fairness and ultra-reliable low-latency communications. To evaluate the performance, the exact secrecy outage probability of the SRS scheme is derived under two residual self-interference models. The asymptotic analysis shows that the SRS scheme achieves full diversity. A relay-based jamming scheme is also proposed by using unassigned relays for user communications. Finally, the two-hop RS schemes and the analysis are extended to the general multi-hop network with multiple eavesdroppers. The numerical results reveal interesting fundamental trends where the proposed schemes can significantly enhance the secrecy performance.**

***Index Terms*— Full-duplex communications, intercept probability, multi-user networks, physical-layer security, multi-hop relay networks, relay selection, residual self-interference, secrecy outage probability.**

I. Introduction

DUE to the broadcast nature of wireless channels, reliable communications can be challenging in the presence of adversarial users who may either extract or degrade (jamming) the legitimate user information [1]. While data encryption techniques have traditionally been used to alleviate eavesdroppers' attacks, recently, there have been expanding research on physical-layer (PHY) security, which exploits the physical characteristics of a wireless network. Especially in multi-user networks, PHY security is becoming an essential requirement [2]. From the information theoretic perspective, key performance measures of PHY security are 1) the *secrecy rate*, defined as the difference between the rate of the source to the destination (or main channel) and the rate of the source to the eavesdropper (or the wiretap channel); and 2) the *intercept probability*, defined as the probability that the eavesdropper succeeds in intercepting the information [3], [4]. As wireless systems evolve to the fifth generation (5G), the numbers of legitimate users and eavesdroppers at a given geographical area are expected to increase dramatically, making legitimate users more vulnerable to attackers. Thus, there are increasing needs for research in addressing PHY security issues for multiuser networks with various new 5G applications, such as massive multiple-input multiple-output (MIMO), mm-wave, cognitive radio, Internet of Things (IoT), and full-duplex (FD) communications, to mention but a few [5]–[8].

FD communications enable simultaneous transmission and reception on a common time-frequency channel. Compared to the half-duplex (HD) communications, it provides significant improvement in spectrum efficiency as spectrum splitting is not necessary between forward and reverse links [9]. Its advantage is even more apparent for relay networks where communications take multiple hops. While HD relaying has the capability of scaling up the system performance in terms of extending the coverage and reducing power consumption, effective FD relaying techniques can further enhance the overall performance due to the improved spectral efficiency [10]. However, for FD communications, the residual self-interference (RSI) is usually stronger than the intended receive signal. Thus proper self-interference cancellation is necessary and some recent breakthroughs can be found in [11].

This paper is on the PHY security of relay networks with FD communications, where the nodes suffer from attacks of multiple eavesdroppers who operate either cooperatively (i.e., colluding) or non-cooperatively (i.e., non-colluding) [12]. While relay selection (RS) is considered for traditional multi-user relay network for both HD and FD relaying, e.g., [13]–[15], the RS is also applied for secure transmission because it has

Manuscript received April 13, 2018; revised July 24, 2018 and November 22, 2018; accepted December 17, 2018. Date of publication January 9, 2019; date of current version February 11, 2019. This work was supported in part by the Australian Research Council through the Discovery Early Career Researcher Award under Grant DE160100020 and in part by the Discovery Project under Grant DP180101205. The associate editor coordinating the review of this paper and approving it for publication was T. Q. Duong. *(Corresponding author: Saman Atapattu.)*

S. Atapattu, Y. He, and J. S. Evans are with the Department of Electrical and Electronic Engineering, The University of Melbourne, Parkville, VIC 3010, Australia (e-mail: saman.atapattu@unimelb.edu.au; yuhe@unimelb.edu.au; jse@unimelb.edu.au).

N. Ross is with the School of Mathematics and Statistics, The University of Melbourne, Parkville, VIC 3010, Australia (e-mail: nathan.ross@unimelb.edu.au).

Y. Jing is with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB T6G 2V4, Canada (e-mail: yindi@ualberta.ca).

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/TWC.2018.2890609

great potential in achieving PHY security by exploiting spatial diversity among relays and jamming adversarial users [16]. The remainder of this section has an overview of related work, followed by a summary on contributions of this work.

A. Related Work

Most existing work on PHY security in relay networks with RS focus on two-hop HD relaying [4], [17]–[23], and references therein. Among them, optimal RS schemes are studied in [4] for networks with single source-destination (SD) pair and multiple relays in the presence of an eavesdropper under both amplify-and-forward (AF) and decode-and-forward (DF) protocols, where full diversity is achieved. For networks with single source, multiple AF relays, destinations and eavesdroppers, in [17], three criteria to select the best relay-user pair are proposed and shown to achieve full diversity. In the network model, the eavesdropper is assumed to attack the relay transmission only but not the source transmission. The work in [18] investigates the joint and separate user-relay selections under DF with the presence of a direct link. Unlike in [4] and [17], both source and relay transmissions are assumed to be exposed to eavesdroppers. Moreover, in [20] and [21], secure relay and jammer selections are studied in wireless networks with multiple intermediate nodes and eavesdroppers, where each intermediate node either helps message forwarding as a relay, or broadcasts noise as a jammer. Further, in [22] and [23], PHY security is investigated for two-way relay networks with single SD-pair and multiple relays, where the eavesdropper taps the transmissions of both the end-users and the relays.

Recently, there has been some work on PHY security in two-hop FD relaying [24]–[29] with focus on the secrecy rate performance and the advantages of FD over HD. For a single SD pair, in [27], a hybrid RS scheme is proposed that switches between HD and FD and the secrecy outage probability (SOP) is analyzed. In [28], partial, optimal, and minimal self-interference RS schemes are proposed for FD heterogeneous networks with single transmitter in the presence of multiple cognitive radio eavesdroppers. Reference [29] considers multiple users, multiple relays, and single destination with an eavesdropper who can overhear the relay transmission, where a joint user and relay selection is proposed to enhance the PHY security. Research results on the PHY security of multi-hop (more than two hops) relaying or multiple SD pairs have been very limited in the literature for either HD or FD. A tree-formation game to choose secure paths for the uplink of a multi-hop network is proposed in [30]. In [31], secure routing is studied in a single-user multi-hop ad-hoc network with randomly distributed eavesdroppers. The combination of PHY security and quality-of-service for route selection is investigated for multi-hop ad-hoc networks in [32]. While [33] is on three-hop networks with FD, the model is limited to a single SD pair. Recently, in [34], a cross-layer optimization approach is used to maximize the secrecy rate in multi-hop networks.

On the other hand, the concept of cooperative jamming can effectively benefit the security of relay networks by sending jamming signals (e.g., artificial noises) from the source, destination or relays, e.g., [35], [36] and references therein. On the notion of RS, a relay and jammer selection in cooperative HD systems is proposed in [37], where one relay forwards the data of the source and the other relay transmits jamming signal in order to confuse the eavesdropper. An optimal single-user selection scheme is considered for a multi-user HD relay scheme with cooperative jamming in [38]. A minimum energy routing in the presence of multiple malicious jammers is proposed for multi-hop relaying in [39] and [40].

B. Summary of Contributions

According to the above review, the RS problem for PHY security in relay networks with multiple SD pairs is still wide open for either HD or FD mode, even for the simple two-hop case. In current and future wireless systems, concurrent communications between multiple SD pairs is a typical scenario and has general applications in ultra-reliable low latency communication (URLLC) services. Further, emerging 5G and beyond communications require device-to-device multi-hop interactions to extend the coverage of small-cell network architectures in a dense urban environment. Applications including multi-tier cellular networks may perform traffic offloading and relaying from one network/operator to another [41]. To facilitate secure communications in such an environment, the exploitation of RS schemes and the corresponding performance analysis for such networks are important, but at the same time highly challenging due to possible conflicts among users and the intertwined system parameters. A recent paper [42] considers RS for a FD two-hop relay network with multiple users under the attack of colluding eavesdroppers where Gaussian RSI channels are assumed. There has not been results for systems with non-cooperative eavesdroppers, random block-fading RSI channels, and multiple hops. To help fill this research gap, this paper studies the RS problem in more general FD relay networks. The key technical contributions are summarized in the following.

1) The traditional two-hop FD relay network is considered with two eavesdroppers. Two RS schemes are proposed, namely the optimal relay selection (ORS) and sub-optimal relay selection (SRS). The ORS scheme maximizes the minimum secrecy rate among all SD pairs but requires channel state information (CSI) of all nodes including the eavesdroppers. The SRS scheme, a more practical one, depends on the CSI of the main channels only along with the statistical information of the eavesdropper channels. Although the ORS scheme assumes full CSI knowledge, it can be used to benchmark the practical SRS scheme. Since the secrecy outage/intercept probability of ORS is a lower bound for that of SRS, the performance limit of the ORS scheme can provide guidance for SRS design.
2) The SOP of the SRS scheme is derived for two-hop FD relay networks under two RSI models for both non-colluding and colluding eavesdroppers. The scheme is shown to provide full diversity when the gains of the main-to-eavesdropper and the main-to-interference channels increase asymptotically. Further, a relay-based jamming scheme is proposed to effectively exploit the multiuser diversity for secure relaying.

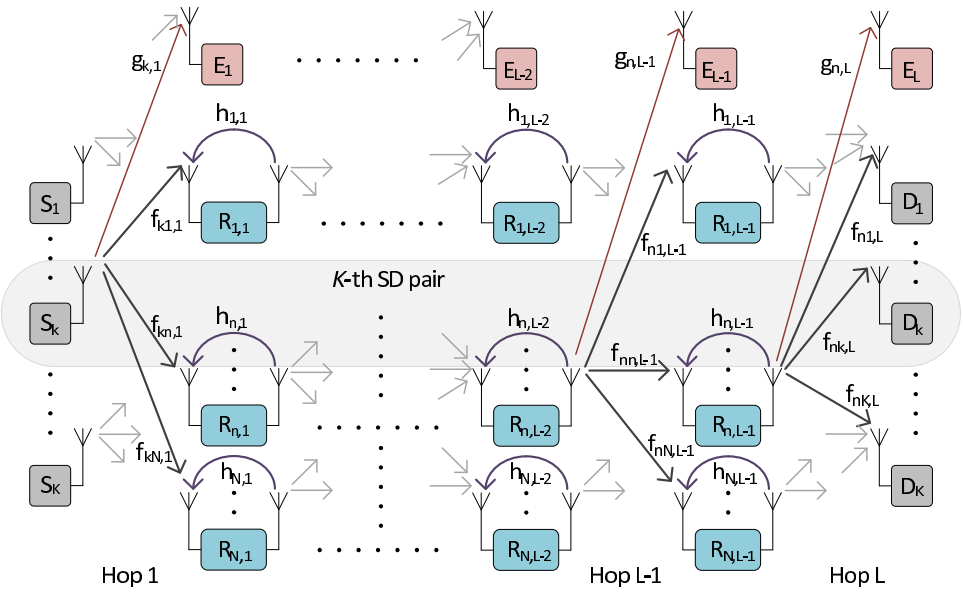


Fig. 1. A full-duplex multi-source-destination-pair multi-relay multi-hop wiretap network.

3) With the focus on 5G and beyond applications, the two-hop network is extended to a general multi-hop relay network. Two RS schemes, namely locally-ORS and locally-SRS, are proposed by considering locally optimal selection and locally sub-optimal selection schemes. The SOP of the locally-SRS scheme is derived along with asymptotic diversity results.

II. Multi-Hop FD Relay Network With Multiple SD Pairs and Eavesdroppers

A. Network Model

This work considers a general multi-SD-pair multi-hop multi-relay wiretap network as shown in Fig. 1, where the K sources $S_1, \ldots, S_K$ send information to their corresponding destinations $D_1, \ldots, D_K$ via $L-1$ layers of relays and each layer contains N relays where $N \geq K$. Denote the n-th relay at the ℓ-th layer as $R_{n,\ell}$. To help the presentation, the K sources together is denoted as the 0-th layer while the K destinations together is denoted as the L-th layer. The (n,ℓ)-th node of the network refers to the n-th node of the ℓ-th layer, where the node is a relay when $\ell = 1, \ldots, L-1$, a source when $\ell = 0$, and a destination when $\ell = L$.

Direct wireless links only exist from the ℓ-th layer to the subsequent $(\ell+1)$-th layer for $\ell = 0, \ldots, L-1$. We assume that the direct links from the ℓ-th layer to the $(\ell+2)$-th layer and beyond for $\ell = 0, \ldots, L-2$ are sufficiently weak and can be ignored due to obstacles and/or deep fading. Thus communications from the sources to the destinations take L hops. While S_k, $R_{n,\ell}$ and D_k are legitimate nodes, the transmitters of the ℓ-th layer is exposed to an eavesdropper $E_{\ell+1}$ for $\ell = 0, \ldots, L-1$.[1] Each source S_k has a transmit antenna. Each destination D_k or eavesdropper E_ℓ has a single receive antenna. Each relay $R_{n,\ell}$ is assumed to have one transmit antenna and one receive antenna. The relays are in the FD mode with DF.

It is assumed that the $(L-1)$ relay clusters are equally spaced from the source to the destination, as shown in Fig. 1. Then the distances between the $(i,\ell-1)$-th node to the (j,ℓ)-th node are the same for all i, j, ℓ, denoted as l_c. The distances between the (i,ℓ)-th node to E_ℓ are the same for all ℓ, denoted as l_e. The wireless channels follow independent small-scale multi-path Rayleigh fading along with large-scale path-loss fading. Denote the small-scale channel coefficient from the $(i,\ell-1)$-th node to the (j,ℓ)-th node as $f_{ij,\ell}$. Based on the aforementioned distance setup and the assumption of similar multipath propagation characteristics for all hops, $f_{ij,\ell}$'s are i.i.d. with zero-mean circularly symmetric complex Gaussian distribution, i.e., $f_{ij,\ell} \sim \mathcal{CN}(0, \sigma_c^2)$ where σ_c^2 is the variance of the main channel. Denote the small-scale fading coefficient of the wiretap channel from the $(i,\ell-1)$-th node to E_ℓ, the eavesdropper at the ℓ-th layer, as $g_{i,\ell}$. Thus $g_{i,\ell}$'s are i.i.d. $\mathcal{CN}(0, \sigma_e^2)$, where σ_e^2 is the variance of the wiretap channel. While a more general non-identical distance/channel variance model is very attractive, it is highly challenging in terms of performance analysis. The resulting non-identical random variables do not facilitate rigorous analytical treatment. Further, non-identical parameters produce cumbersome analytical expressions due to nested summations and products which occupy more space. For the sake of brevity and simplicity of analysis, we thus assume identical parameters for channels of the same hop to help the derivations and insightful analytical expressions in the sequel. The transmit power of all transmitting nodes (sources or relays) is denoted as p. Under FD mode where the relay transmission and reception are simultaneous, each relay receives a self-interference component in addition to the information signal from the transmitter. The self-interference channel of the (n,ℓ)-th FD node is denoted as $h_{n,\ell}$.

[1]To systematically develop the analytical framework, we assume only one eavesdropper per layer. The models and derived results of this paper can be straightforwardly extended to an arbitrary number of eavesdroppers.

B. Communication Model

We now elaborate the protocol and transceiver models for the communications from S_k to D_k. This work focuses on RS where at each relay layer, only one relay is chosen to help each SD pair, and each relay can help at most one SD pair. To avoid interference, the SD pairs are assigned orthogonal channels using frequency- or time-division multiple access. The k-th channel is the channel allocated for the communications of the k-th SD pair.

1) The Main Channel: At the ℓ-th network layer for $\ell = 1 \ldots, L$, the received signal at the (n, ℓ)-th node on the k-th channel for $k = 1, \ldots, K$ at time t, can be written as $y_{n,\ell}[t] = \sqrt{p/l_c^{\eta}} f_{kn,\ell} s_{k,\ell-1}[t] + i_{n,\ell}[t] + n_{n,\ell}[t]$, where η is the path-loss exponent, $s_{k,\ell-1}[t]$ is the decoded and forwarded information symbol of S_k at the $(\ell-1)$-th layer, $n_{n,\ell}[t]$ is additive white Gaussian noise (AWGN) at the (n, ℓ)-th node with zero mean and σ_0^2 variance, and $i_{n,\ell}[t]$ is the self-interference. When $\ell = L$ (the last communication hop), there is no self-interference, i.e., $i_{n,L}[t] = 0$.

2) Self-Interference Models: Without applying self-interference cancellation (SIC) technique at the (n, ℓ)-th node (which is $R_{n,\ell}$), we have for $\ell = 1, \ldots, L-1$, $i_{n,\ell}[t] = \sqrt{p} h_{n,\ell} s_{n,\ell}[t]$. As self-interference is usually the bottleneck for FD communications, SIC techniques are essential at the FD relays for desirable performance. In this work, we assume that some SIC technique is implemented at the relays and thus with slight abuse of notation, $i_{n,\ell}$ is used to represent the residual self-interference (RSI) at the (n, ℓ)-th node. The following two RSI models are adopted.

- RSI Model I: $i_{n,\ell}$'s are i.i.d. complex Gaussian random variables following $\mathcal{CN}(0, \sigma_i^2)$, which have a similar effect as the noise [10].
- RSI Model II: $i_{n,\ell}$'s are i.i.d. complex Gaussian random variables following $\mathcal{CN}(0, \sigma_i^2)$, and are block fading random variables [26].

By including the impacts of p, $h_{n,\ell}$ and $s_{k,\ell}$ into the RSI variance, we assume that $\sigma_i^2 = \omega p^{\nu}$ where the two constants, $\omega > 0$ and $\nu \in [0, 1]$, depend on the SIC schemes used at the (n, ℓ)-th node [10]. It implies that RSI variances are constants and identical for all relays.

3) The Wiretap Channel: The received signal at E_ℓ, the eavesdropper at the ℓ-th layer, on the k-th channel at time t is $y_{k,e\ell}[t] = \sqrt{p/l_e^{\eta}} g_{k,\ell} s_k[t] + n_{e,\ell}[t]$, for $k = 1, \ldots, K$, where $n_{e,\ell}[t]$ is the Gaussian noise at E_ℓ, which follows $\mathcal{CN}(0, \sigma_0^2)$. It is assumed that the eavesdroppers know the encoding and decoding schemes at the sources and the destinations.

III. RS Schemes for Two-Hop Networks

This section is on the two-hop network with a single layer of relays, denoted as $R_{n,1}$'s for $n = 1, \ldots, N$, and two eavesdroppers E_1 and E_2 one for each hop. The RS problem is to choose one relay for each SD pair. Two RS schemes are proposed based on the secrecy rate and the received signal-to-interference-plus-noise ratios (SINRs).

A. Received SINR and Secrecy Rate

If Relay $R_{n,1}$ is chosen for the transmission from S_k to D_k, the transceiver equations of the two hops are $y_{n,1}[t] = \sqrt{\frac{p}{l_c^{\eta}}} f_{kn,1} s_k[t] + i_{n,1}[t] + n_{n,1}[t]$ and $y_{k,2}[t] = \sqrt{\frac{p}{l_c^{\eta}}} f_{nk,2} s_{n,1}[t] + n_{k,2}[t]$, where $y_{k,2}[t]$ is the received signal at D_k and $n_{k,2}[t]$ is the noise at D_k at time t. The received SINR at $R_{n,1}$ for the first hop and the signal-to-noise-ratio (SNR) at D_k for the second hop can be given respectively as

$$\gamma_{kn,1} = \frac{p}{l_c^{\eta}\sigma_0^2} \frac{|f_{kn,1}|^2}{(1+u_n)} \quad \text{and } \gamma_{nk,2} = \frac{p}{l_c^{\eta}\sigma_0^2} |f_{nk,2}|^2, \tag{1}$$

where $u_n = \frac{\sigma_i^2}{\sigma_0^2}$ for RSI Model I and $u_n = \frac{|h_{n,1}|^2}{\sigma_0^2}$ RSI Model II. For the wiretap channels, the received SNRs at E_1 and E_2 are given by

$$\gamma_{k,e1} = \frac{p}{l_e^{\eta}\sigma_0^2} |g_{k,1}|^2 \quad \text{and } \gamma_{n,e2} = \frac{p}{l_e^{\eta}\sigma_0^2} |g_{n,2}|^2, \tag{2}$$

respectively. To help the presentation, we use 'C' and 'NC' for cases with colluding eavesdroppers and non-colluding eavesdroppers, respectively. Define

$$\tilde{\gamma}_{kn} \triangleq \frac{1 + \min(\gamma_{kn,1}, \gamma_{nk,2})}{1 + \gamma_{e,kn}}, \tag{3}$$

where

$$\gamma_{e,kn} \triangleq \begin{cases} \gamma_{k,e1} + \gamma_{n,e2}; & \text{for C} \\ \max(\gamma_{k,e1}, \gamma_{n,e2}); & \text{for NC.} \end{cases}$$

All possible user achievable secrecy rates connected via any relay can be given as [12], [31]

$$\mathcal{C} = (c_{kn}) \in \mathbb{R}^{K \times N} \quad \text{where } c_{kn} = [\log \tilde{\gamma}_{kn}]^+ \tag{4}$$

and $[x]^+ = \max(x, 0)$.

B. RS Schemes Based on Max-Min Fairness

In this section, two RS schemes are presented, one is based on the global information of all nodes and the other is based on the information of the legitimate nodes only.

1) The ORS Scheme: By considering individual performance as well as fairness, we aim to maximize the minimum secrecy rate of all SD pairs. The ORS scheme is adopted, originally proposed for HD relay network in [13], which maximizes the minimum received SINR and guarantees the uniqueness of the solution. The RS matrix for ORS is defined as $\mathbf{\Gamma}_o = (\tilde{\gamma}_{kn})$, which is a $K \times N$ real matrix whose (k, n)-th entry is defined in (3). Due to the relationship between c_{kn} and $\tilde{\gamma}_{kn}$, entries of the matrix $\mathbf{\Gamma}_o$ fully represent the achievable secrecy rate performance of the K SD pairs with all possible choices of the N relays. More specifically, the k-th row determines the achievable secrecy rates of the k-th SD pair via each of the N relays, and the n-th column determines the achievable secrecy rates of all SD pair transmissions through $R_{n,1}$.

The ORS scheme is presented in Algorithm 1. In this algorithm, for each m, the while-loop finds the solution that maximizes the m-th minimal secrecy rate of all SD pairs. The key step is in Line 7, where a better selection is one that has a higher m-th minimal secrecy rate than the previous selection result. In the search for a better selection, all "unmarked" relays that can lead to a higher performance for the m-th worst SD pair is checked in the order of decreasing rate. If a checked relay has already been assigned to another SD pair, the process of checking if a better relay selection exists

Algorithm 1 The ORS Scheme for Two-Hop Wiretap Networks

1: Calculate the RS matrices $\mathbf{\Gamma}_o$.
2: Make a random initialization for the relay assignment: R_k^* for $k = 1, \ldots, K$. That is, the R_k^*-th relay is assigned for the k-th SD pair.
3: **for** $m = 1 : K$ **do**
4: Set flag=1.
5: **while** flag==1 **do**
6: Find the index k_m whose value is the m-th lowest among $[\mathbf{\Gamma}_o]_{1,R_1^*}, \ldots, [\mathbf{\Gamma}_o]_{K,R_K^*}$.
7: Check if a better relay selection exists for the k_m-th SD pair by calling function `find_another_relay(`k_m`)`.
8: **if** a better selection can be found **then**
9: Update the relay selection to the found one.
10: **else**
11: flag=0.

needs to be conducted for that new pair, i.e., the function `find_another_relay` will be recursively called for the new pair. Once checked, a relay will be remembered as "marked" to avoid endless loop. Thus, in finding a new relay selection for one SD pair, the relay selections for other pairs may also be adjusted accordingly. This scheme was originally proposed in [43] and modified in [13]. For more details on how the function `find_another_relay` can be realized, please refer to [13]. With the for-loop, such relay searching is conducted from the worst SD pair to the second worst and finally the best SD pair. If we sort elements in the RS matrix $\mathbf{\Gamma}_o$ in descending order, after the RS, the end-to-end performance metric of every SD pair is among the first $(K-1)N+1$ of the ordered values. The worst-case complexity of the ORS scheme is $\mathcal{O}(K^2N^2)$ [13], [43]. Global CSI information of all legitimate users as well as the eavesdroppers is needed for the ORS scheme.

2) The SRS Scheme: In wiretap networks, the eavesdroppers secretly listen to the main channels without legitimate nodes' consent, and therefore the relay selector may be unaware of their presence. Moreover, to obtain information of the time-varying self-interference channels, estimation and reporting to the relay selector are usually done periodically with manageable overhead. Thus, from the practical point of view, it is reasonable to assume that the relay selector does not have any knowledge of eavesdroppers' channels, and has only partial knowledge (i.e., the statistics) of the self-interference channels. Based on this, we propose an SRS scheme. When only the knowledge of the main channels is known along with the statistics of the self-interference channels, the following value can be calculated:

$$\gamma_{kn} \triangleq \min\left(\rho\, x_{kn}, y_{nk}\right), \tag{5}$$

where

$$\rho \triangleq \frac{\sigma_0^2/\sigma_i^2}{1+\sigma_0^2/\sigma_i^2},\ x_{kn} \triangleq \frac{p}{l_c^\eta \sigma_0^2}|f_{kn,1}|^2,\ y_{nk} \triangleq \frac{p}{l_c^\eta \sigma_0^2}|f_{nk,2}|^2.$$

Here, x_{kn} is the received signal power of the first hop at the nth relay, and y_{nk} is the received SNR of the second hop via the nth relay. The $K \times N$ real RS matrix $\mathbf{\Gamma}_s$ is defined as $\mathbf{\Gamma}_s = (\gamma_{kn})$. The same algorithm as in the ORS case can be conducted with the RS matrix being replaced by $\mathbf{\Gamma}_s$. While ORS achieves the maximum-minimal secrecy rate, SRS is suboptimal as the RS matrix $\mathbf{\Gamma}_s$ is based on the CSI of partial of the network.

IV. Secrecy Outage Probability (SOP) of SRS for Two-Hop Networks

Denote the secrecy rate for the k-th SD pair after the SRS scheme as $c_{(k)}$. The SOP is the probability that the secrecy rate of the k-th SD pair is not higher than the target secrecy rate τ, i.e., $P_k(\tau) = \Pr\left(c_{(k)} \le \tau\right)$, where τ is an arbitrary positive value. If the secrecy rate is zero, i.e., $c_{(k)} = 0$, or equivalently, $\gamma_{kn} \le 1$ when Relay $R_{n,1}$ is chosen for the k-th SD pair, one or both eavesdroppers can succeed in intercepting the signal on the k-th channel and an intercept event occurs. Thus, an intercept event occurs when the secrecy capacity becomes negative, and the intercept probability can be calculated as $\Pr\left(c_{(k)} = 0\right) = P_k(0)$. In this paper, the SOP instead of the intercept probability is analyzed for the SRS scheme proposed in Section III for more general results.

To help understand the computation of $P_k(\tau)$ in what follows, we define and recite some crucial quantities:

- Since all channels are Rayleigh fading, we have $x_{kn}, y_{nk} \sim \mathcal{E}xp(\lambda)$, where $\lambda \triangleq \frac{l_c^\eta \sigma_0^2}{p\,\sigma_c^2}$, $\gamma_{k,e1}, \gamma_{n,e2} \sim \mathcal{E}xp(\beta)$ where $\beta \triangleq \frac{l_e^\eta \sigma_0^2}{p\,\sigma_e^2}$ and $u_n \sim \mathcal{E}xp(\sigma_0^2/\sigma_i^2)$ for RSI Model II. The notation $X \sim \mathcal{E}xp(a)$ means that X follows the exponential distribution with rate parameter $a > 0$;
- The entries γ_{kn}'s are the elements of the RS matrix $\mathbf{\Gamma_s}$;
- The j-th largest element of $\mathbf{\Gamma_s}$ is denoted as $\gamma^{(j)}$, and it has the probability density function (p.d.f.) as [44]

$$f_{\gamma^{(j)}}(z) = \lambda_c \sum_{q=0}^{NK-j} \Xi\left(N,K,j,q\right) e^{-\lambda_c(j+q)z} \tag{6}$$

where $\lambda_c \triangleq \lambda(\rho+1)/\rho$ and $\Xi\left(N,K,j,q\right) \triangleq \frac{(NK)!(-1)^q\binom{NK-j}{q}}{(j-1)!(NK-j)!}$;
- The secrecy rates corresponding to the ordered $\gamma^{(j)}$'s are $c^{(j)}$'s;
- The notation $\gamma_{\mathrm{m}}^{(j)}$ which represents the value of $\min(\gamma_{kn,1}, \gamma_{kn,2})$ corresponding to $c^{(j)}$ as per (3) is a key intermediate term in computing probabilities for $c^{(j)}$; and
- According to the RS algorithm, the secrecy rate of the k-th SD pair, $c_{(k)}$, is in the set $\{c^{(1)}, \ldots, c^{((K-1)N+1)}\}$.

Now, let L_k be the index of the relay selected for the k-th SD pair, which is an independent random variable of the values $(\gamma^{(j)})_{j=1}^{NK}$. The SOP of the k-th SD pair is

$$\begin{aligned} P_k(\tau) &= \Pr[c_{(k)} \le \tau] \\ &= \sum_{j=1}^{(K-1)N+1} \Pr[L_k = j] \Pr[c^{(j)} \le \tau | L_k = j] \\ &= \sum_{j=1}^{(K-1)N+1} \mathrm{P}_{(j)} \Pr[c^{(j)} \le \tau]. \end{aligned}$$

Unlike the traditional RS in FD communications [15], here we have an additional set of random variables due to eavesdroppers' channels. Thus, the analytical approach will be different.

Let $\gamma_{e,\cdot}$ be the corresponding effective SNR of the eavesdroppers as defined in (3). Further we define $\mathrm{P}_{(j)} \triangleq \Pr[L_k = j]$ and $Z \triangleq (2^\tau - 1) + 2^\tau \gamma_{e,\cdot}$. By following the definition of $c^{(j)}$, $P_k(\tau)$ can then be written as

$$\begin{aligned} P_k(\tau) &= \sum_{j=1}^{(K-1)N+1} \mathrm{P}_{(j)} \Pr\left[\log_2\left(\frac{1+\gamma_{\mathrm{m}}^{(j)}}{1+\gamma_{e,\cdot}}\right) \le \tau\right] \\ &= \sum_{j=1}^{(K-1)N+1} \mathrm{P}_{(j)} \Pr\left[\gamma_{\mathrm{m}}^{(j)} \le (2^\tau - 1) + 2^\tau \gamma_{e,\cdot}\right] \\ &= \sum_{j=1}^{(K-1)N+1} \mathrm{P}_{(j)} \underbrace{\int_{2^\tau-1}^{\infty} \underbrace{\Pr\left[\gamma_{\mathrm{m}}^{(j)} \le z\right]}_{\triangleq F_{\gamma_{\mathrm{m}}^{(j)}}(z)} f_Z(z) dz}_{=\mathcal{J}_{(j)}}, \quad (7) \end{aligned}$$

where the last two equalities come by using the monotonicity of the logarithm and the continuous law of total probability. To this end, we need to calculate $\mathrm{P}_{(j)}$ and $\mathcal{J}_{(j)}$.

The term $\mathrm{P}_{(j)}$ represents the probability that the relay with the j-th largest entry of $\mathbf{\Gamma_s}$ corresponds to the k-th SD pair. Only the relay ordering matters, $\mathrm{P}_{(j)}$ depends on the dimensions of $\mathbf{\Gamma_s}$ and j. For some cases, these probabilities are calculated analytically in [45]. In general, they can be evaluated by simulations.

The term $\mathcal{J}_{(j)}$ depends on $f_Z(z)$ and $F_{\gamma_{\mathrm{m}}^{(j)}}(z)$. As the p.d.f. s of the maximum and summation of two i.i.d. random variables each following $\mathcal{E}xp(a)$ are $2\,a\left(e^{-ax} - e^{-2\,ax}\right)$ and $a^2\,xe^{-ax}$, respectively, we derive the p.d.f. for Z with the aid of (3), as[2]

$$f_Z(z) = \begin{cases} \left(\frac{\beta}{2^\tau}\right)^2 \frac{e^{\frac{\beta(2^\tau-1)}{2^\tau}}}{e^{\frac{\beta}{2^\tau}z}} (z - (2^\tau - 1)); & \text{C;} \\ \frac{2\beta}{2^\tau} \frac{e^{\frac{\beta(2^\tau-1)}{2^\tau}}}{e^{\frac{\beta}{2^\tau}z}} \left(1 - \frac{e^{\frac{\beta(2^\tau-1)}{2^\tau}}}{e^{\frac{\beta}{2^\tau}z}}\right); & \text{NC.} \end{cases} \quad (8)$$

To calculate $F_{\gamma_{\mathrm{m}}^{(j)}}(x)$ in (7), we need to develop two different analytical frameworks for RSI Models I and II because of the different random variables involved. Moreover, for each model, we need to analyze the SRS scheme under colluding and non-colluding cases. Thus, our subsequent analysis for $\mathcal{J}_{(j)}$ yields four expressions.

A. Analysis for RSI Model I

According to the definition in (3), we have $\gamma_{\mathrm{m}}^{(j)} = \min\left(\gamma_{\cdot,1}^{(j)}, \gamma_{\cdot,2}^{(j)}\right) = \min\left(\frac{x_{\cdot\cdot}^{(j)}}{1+\sigma_i^2/\sigma_0^2}, y_{\cdot\cdot}^{(j)}\right)$ where the $\gamma_{\cdot,1}^{(j)}, \gamma_{\cdot,2}^{(j)}, x_{\cdot\cdot}^{(j)}, y_{\cdot\cdot}^{(j)}$ are the variables corresponding to the induced index of $\gamma^{(j)}$. For brevity, we drop the subscript indices for $\gamma_{\cdot,1}^{(j)}, \gamma_{\cdot,2}^{(j)}, x_{\cdot\cdot}^{(j)}, y_{\cdot\cdot}^{(j)}$ without sacrificing the readability to have $\gamma_1^{(j)}$, $\gamma_2^{(j)}$, $x^{(j)}$, $u^{(j)}$, $y^{(j)}$. Now, we calculate $F_{\gamma_{\mathrm{m}}^{(j)}}(x)$ in (7) as

$$\begin{aligned} F_{\gamma_{\mathrm{m}}^{(j)}}(z) &= \Pr\left[\min\left(\frac{x^{(j)}}{1+\sigma_i^2/\sigma_0^2}, y^{(j)}\right) \le z\right] \\ &= 1 - \Pr\left[\rho\, x^{(j)} > \rho\left(1 + \frac{\sigma_i^2}{\sigma_0^2}\right) z,\, y^{(j)} > z\right] \quad (9) \end{aligned}$$

where the second step follows a simple rearrangement to help the application of the RS criterion. The probability calculation needs the distribution of $(\rho\, x^{(j)}, y^{(j)})$ for the situation that $\gamma^{(j)}$ is the j-th largest entry of $\mathbf{\Gamma_s}$. To this end, we first write the following:

$$\left(\rho\, x^{(j)}, y^{(j)}\right) = \begin{cases} \left(\gamma^{(j)}, \hat{y}^{(j)}\right); & \text{w.p. } p_1 = \dfrac{1}{\rho+1} \\ \left(\rho\, \hat{x}^{(j)}, \gamma^{(j)}\right); & \text{w.p. } p_2 = \dfrac{\rho}{\rho+1}, \end{cases} \quad (10)$$

where 'w.p.' stands for *with probability*, $\hat{y}^{(j)}$ equals $y^{(j)}$ when it is larger than $\gamma^{(j)}$, and $\rho\,\hat{x}^{(j)}$ equals $\rho\, x_{kn}$ when it is larger than $\gamma^{(j)}$. With the aid of (10) and (6), we can re-write (9) as

$$\begin{aligned} F_{\gamma_{\mathrm{m}}^{(j)}}(z) &= 1 - p_1 \int_z^\infty \int_{\max\{t,z\}}^\infty f_{\hat{y}^{(j)}}(w|\gamma^{(j)} = t) f_{\gamma^{(j)}}(t) dw dt \\ &\quad - p_2 \int_z^\infty \int_{\max\{t,z\}}^\infty f_{\hat{x}^{(j)}}(w|\gamma^{(j)} = t) f_{\gamma^{(j)}}(t) dw dt \\ &\overset{(a)}{=} 1 - \frac{\int_z^\infty \int_t^\infty f_{\hat{y}^{(j)}}(w|\gamma^{(j)} = t) f_{\gamma^{(j)}}(t) dw dt}{\left(1 + \frac{\sigma_0^2}{\sigma_i^2}\right)^{-1}\left(1 + 2\frac{\sigma_0^2}{\sigma_i^2}\right)} \\ &\quad - \frac{\sigma_0^2}{\sigma_i^2} \frac{\int_z^\infty \int_t^\infty f_{\hat{x}^{(j)}}(w|\gamma^{(j)} = t) f_{\gamma^{(j)}}(t) dw dt}{\left(1 + 2\frac{\sigma_0^2}{\sigma_i^2}\right)} \\ &\overset{(b)}{=} 1 - \sum_{q=0}^{NK-j} \frac{\Xi(N,K,j,q)}{(j+q)} e^{-\lambda(j+q)\left(\frac{\sigma_i^2}{\sigma_0^2}+2\right)z}, \quad (11) \end{aligned}$$

where (a) is obtained by substituting the values of p_1, p_2, and changing the limits of the integrations, and (b) is obtained by first using (6); then averaging over the conditional distributions $f_{\hat{x}^{(j)}}(z|\gamma^{(j)}) = \lambda/\rho\, e^{-\frac{\lambda}{\rho}\left(z-\gamma^{(j)}\right)}$ and $f_{\hat{y}^{(j)}}(z|\gamma^{(j)}) = \lambda e^{-\lambda\left(z-\gamma^{(j)}\right)}$; and finally solving the double integrations. With this result and (8), $\mathcal{J}_{(j)}$ in (7) can be calculated for both colluding and non-colluding cases as follows:

$$\begin{aligned} \mathcal{J}_{(j)} &= 1 - \sum_{q=0}^{NK-j} \frac{\Xi(N,K,j,q)}{(j+q)} \\ &\quad \times \begin{cases} \left(\frac{\beta}{2^\tau}\right)^2 \frac{\varphi_1\left(1, \left(\frac{\sigma_i^2}{\sigma_0^2}+2\right)\lambda(j+q), \frac{\beta}{2^\tau}, 2^\tau - 1\right)}{e^{-\frac{\beta(2^\tau-1)}{2^\tau}}\left(\left(\frac{\sigma_i^2}{\sigma_0^2}+2\right)\lambda(j+q) + \frac{\beta}{2^\tau}\right)}; & \text{C} \\ \frac{2\beta}{2^\tau}\left[\frac{\varphi_1\left(1, \left(\frac{\sigma_i^2}{\sigma_0^2}+2\right)\lambda(j+q), \frac{\beta}{2^\tau}, 2^\tau - 1\right)}{e^{-\frac{\beta(2^\tau-1)}{2^\tau}}}\right. \\ \left. \quad - \frac{\varphi_1\left(1, \left(\frac{\sigma_i^2}{\sigma_0^2}+2\right)\lambda(j+q), \frac{2\beta}{2^\tau}, 2^\tau - 1\right)}{e^{-\frac{2\beta(2^\tau-1)}{2^\tau}}}\right]; & \text{NC,} \end{cases} \end{aligned} \quad (12)$$

where $\varphi_1(a,b,c,t) = \int_t^\infty a e^{-(b+c)x}\, dx = a e^{-t(b+c)}/(b+c)$.

[2]For systems with multiple eavesdroppers at each hop, say M_1 and M_2 at the two hops respectively, $\gamma_{e,kn}$ can be modified as $\gamma_{e,kn} = \sum_{j=1}^{M_1} \gamma_{k,e1}^j + \sum_{j=1}^{M_2} \gamma_{k,e2}^j$ for C and $\gamma_{e,kn} = \max\left(\sum_{j=1}^{M_1} \gamma_{k,e1}^j, \sum_{j=1}^{M_2} \gamma_{k,e2}^j\right)$ or $\max\left(\gamma_{k,e1}^1, \ldots, \gamma_{k,e1}^{M_1}, \gamma_{k,e2}^1, \ldots, \gamma_{k,e2}^{M_2}\right)$ for NC. As $\gamma_{k,\cdot\cdot}^m$'s are i.i.d. $\mathcal{E}xp(a)$, we can derive $f_{\gamma_{e,kn}}(x)$ and $f_{\gamma_Z}(z)$ accordingly.

$$
\begin{aligned}
F_{\gamma_{\mathrm{m}}^{(j)}}(z) &= \Pr\left[\min\left(\frac{x^{(j)}}{1+u^{(j)}}, y^{(j)}\right) \le z\right] = 1 - \Pr\left[\frac{x^{(j)}}{1+u^{(j)}} > z, y^{(j)} > z\right] \\
&= 1 - \mathbb{E}\left[\Pr\left[u^{(j)} < \frac{x^{(j)}}{z} - 1 \middle| \left(x^{(j)}, y^{(j)}\right)\right] \Pr\left[y^{(j)} > z \middle| \left(x^{(j)}, y^{(j)}\right)\right]\right] \\
&= 1 - \mathbb{E}\left[F_{u^{(j)}}\left(\frac{x^{(j)}}{z} - 1\right) \mathbb{1}_{x^{(j)}>z} \mathbb{1}_{y^{(j)}>z}\right] = 1 - \mathbb{E}\left[F_{u^{(j)}}\left(\frac{\rho\, x^{(j)}}{\rho\, z} - 1\right) \mathbb{1}_{\rho x^{(j)}>\rho z} \mathbb{1}_{y^{(j)}>z}\right] \\
&= 1 - p_1 \int_{\rho z}^{\infty} \int_{\max\{t,z\}}^{\infty} F_{u^{(j)}}\left(\frac{t}{\rho\, z} - 1\right) f_{\hat{y}^{(j)}}(w|\gamma^{(j)} = t) f_{\gamma^{(j)}}(t) dw dt \\
&\quad - p_2 \int_{z}^{\infty} \int_{\max\{t,\rho z\}}^{\infty} F_{u^{(j)}}\left(\frac{w}{\rho\, z} - 1\right) f_{\hat{x}^{(j)}}(w|\gamma^{(j)} = t) f_{\gamma^{(j)}}(t) dw dt \\
&= 1 - p_1 \int_{\rho z}^{z} \int_{z}^{\infty} F_{u^{(j)}}\left(\frac{t}{\rho\, z} - 1\right) f_{\hat{y}^{(j)}}(w|\gamma^{(j)} = t) f_{\gamma^{(j)}}(t) dw dt \\
&\quad - p_1 \int_{z}^{\infty} \int_{t}^{\infty} F_{u^{(j)}}\left(\frac{t}{\rho\, z} - 1\right) f_{\hat{y}^{(j)}}(w|\gamma^{(j)} = t) f_{\gamma^{(j)}}(t) dw dt \\
&\quad - p_2 \int_{z}^{\infty} \int_{t}^{\infty} F_{u^{(j)}}\left(\frac{w}{\rho\, z} - 1\right) f_{\hat{x}^{(j)}}(w|\gamma^{(j)} = t) f_{\gamma^{(j)}}(t) dw dt. \qquad (13)
\end{aligned}
$$

B. Analysis for RSI Model II

According to the definition in (3), we have $\gamma_{\mathrm{m}}^{(j)} = \min\left(\gamma_{\cdot,1}^{(j)}, \gamma_{\cdot,2}^{(j)}\right) = \min\left(\frac{x_{\cdot}^{(j)}}{1+u_{\cdot}^{(j)}}, y_{\cdot}^{(j)}\right)$. The major difference in the analysis of RSI Model II to that of RSI Model I is the additional random variable $u^{(j)}$. Then, we have $F_{\gamma_{\mathrm{m}}^{(j)}}(z)$ as given in (13), shown at the top of this page. The derivation follows straightforward algebra and general probability rules.

The distributions of $\gamma^{(j)}$, $\hat{x}^{(j)}$, $\hat{y}^{(j)}$ are given in (6) and under (11), respectively. Since all distribution functions $F_{u^{(j)}}(\cdot)$, $f_{\hat{x}^{(j)}}(\cdot)$, $f_{\hat{y}^{(j)}}(\cdot)$ and $f_{\gamma^{(j)}}(\cdot)$ include only exponential functions, the integrals in (13) can be solved in closed-forms. Due to space limitations, we omit the details of the calculations. Define

$$
\begin{aligned}
\varphi_2(a,b,c,d,t) &= \int_t^{\infty} \frac{a e^{-(b+c)x}}{x+d} dx \\
&= -a e^{d(b+c)} \mathrm{Ei}(-(d+t)(b+c)) \\
\varphi_3(a,b,c,d,t) &= \int_t^{\infty} \frac{a(x-t) e^{-(b+c)x}}{x+d} dx \\
&= \varphi_1(a,b,c,t) - (d+t)\varphi_2(a,b,c,d,t)
\end{aligned}
$$

where $\varphi_1(a,b,c,t)$ is given below (12). By combining (13) with (8), the $\mathcal{J}_{(j)}$ for both cases can be as what follows:

$$
\begin{aligned}
\mathcal{J}_{(j)} = 1 - &\sum_{q=0}^{NK-j} \Xi(N,K,j,q) \\
&\times \begin{cases} \left(\frac{\beta}{2^{\tau}}\right)^2 e^{\frac{\beta(2^{\tau}-1)}{2^{\tau}}} \pi(j,q); & \text{for C} \\ \frac{2\beta}{2^{\tau}} \left(\psi(\beta,j,q) - \psi(2\beta,j,q)\right); & \text{for NC,} \end{cases} \qquad (14)
\end{aligned}
$$

where $\pi(j,q) = \Bigg[\frac{\varphi_1(t_1,t_6,\beta/2^{\tau},2^{\tau}-1)}{t_6+\beta/2^{\tau}} + \varphi_3(t_2,t_7,\beta/2^{\tau},t_8,2^{\tau}-1) + \varphi_3(t_3,t_6,\beta/2^{\tau},t_{10},2^{\tau}-1) + \varphi_3(t_4,t_6,\beta/2^{\tau},t_9,2^{\tau}-1) - \varphi_3(t_5,t_6,\beta/2^{\tau},t_8,2^{\tau}-1)\Bigg]$; $t_1 = \frac{\left(1-e^{-1}\right)\rho(j+q-1)}{(j+q)(\rho(j+q-1)+j+q)}$; $t_{10} = \frac{\sigma_0^2/\sigma_i^2}{\lambda}$; $t_2 = \frac{\sigma_0^2/\sigma_i^2(\rho(j+q-1)+j+q)^{-1}}{\lambda(\rho(j+q-1)+j+q)}$; $t_3 = \frac{e^{-1}\rho\sigma_0^2/\sigma_i^2}{\lambda(\rho(j+q)+j+q-1)}$; $t_4 = \frac{e^{-1}\sigma_0^2/\sigma_i^2}{(j+q-1)} \frac{\lambda(\rho+1)(j+q)^2}{(\rho(j+q)+j+q-1)^{-1}}$; $t_5 = \frac{e^{-1}\sigma_0^2/\sigma_i^2}{\lambda(\rho(j+q-1)+j+q)^2}$; $t_6 = \frac{\lambda(\rho+1)(j+q)}{\rho}$; $t_7 = \lambda(\rho(j+q-1)+j+q+1)$; $t_8 = \frac{\sigma_0^2/\sigma_i^2}{\lambda(\rho(j+q-1)+j+q)}$; $t_9 = \frac{\sigma_0^2/\sigma_i^2}{\lambda(\rho+1)(j+q)}$; and $\psi(\beta,j,q) = e^{\frac{\beta(2^{\tau}-1)}{2^{\tau}}} \Bigg[\varphi_1(t_1,t_6,\beta/2^{\tau},2^{\tau}-1) + \varphi_2(t_2,t_7,\beta/2^{\tau},t_8,2^{\tau}-1) + \varphi_2(t_3,t_6,\beta/2^{\tau},t_1 0,2^{\tau}-1) + \varphi_2(t_4,t_6,\beta/2^{\tau},t_9,2^{\tau}-1) - \varphi_2(t_5,t_6,\beta/2^{\tau},t_8,2^{\tau}-1)\Bigg]$.

V. Asymptotic Analysis for the SRS in Two-Hop Networks

In this section, we provide two asymptotic analysis for i) high main-to-eavesdropper and main-to-interference ratios, and ii) high transmit power. Due to space limitations, this analysis is based on Model-I, however Model-II follows a similar characteristic.

A. Diversity Order for High MER and MIR

For traditional MIMO and virtual MIMO systems, diversity order is defined based on the SNR. For networks with eavesdroppers, due to wiretap channels, it is based on the ratio of average gains of the main channels and the eavesdropper channels, called the main-to-eavesdropper-ratio (MER). Further, in our network model, we have self-interference channels apart from main and eavesdroppers channels. Thus, other than MER, the main-to-interference-ratio (MIR) is also needed, which is the ratio of average gains of the main channels and the interference channels. Define $\alpha \triangleq \sigma_0^2/\sigma_i^2$. By following the notation in Section III-A, the average gains of the main, interference, and eavesdroppers channels are respectively, $1/\lambda = p\sigma_c^2/(l_c^{\eta}\sigma_0^2)$, $1/\alpha = \sigma_i^2/\sigma_0^2$, and $1/\beta = p\sigma_e^2/(l_e^{\eta}\sigma_0^2)$.

Thus,

$$\text{MIR} = \frac{(1/\lambda)}{(1/\alpha)} = \begin{cases} \left(\frac{p}{l_c^\eta \omega}\right)\sigma_c^2; & \text{if } \nu = 0, \\ \left(\frac{1}{l_c^\eta \omega}\right)\sigma_c^2; & \text{if } \nu = 1, \end{cases}$$

$$\text{MER} = \frac{(1/\lambda)}{(1/\beta)} = \left(\frac{l_e^\eta}{l_c^\eta \sigma_e^2}\right)\sigma_c^2.$$

Diversity order is defined as the negative ratio of the average intercept probability or SOP versus the MER curve (in log-scale) when the MIR and MER [4] approaches infinity, i.e., $\delta \triangleq -\lim_{\lambda\to 0} \frac{\log P_k(\tau)}{\log(1/\lambda)}$. For fixed α and β, the diversity order shows how fast the intercept probability or SOP decreases with respect to the average gain of the main channel.

Theorem 1: For each SD pair, the diversity order of SRS in two-hop network is N.

Proof: We start with the proof for RSI Model I with colluding eavesdroppers. In this case, from (7) and the $\mathcal{J}_{(j)}$ expression in (12), we have

$$P_k(\tau) = 1 - \sum_{j=1}^{N(K-1)+1} \sum_{q=0}^{KN-j} \frac{\Xi(N,K,j,q)\left(\frac{\beta}{2^\tau}\right)^2}{(j+q)} \times \frac{\mathrm{P}_{(j)} e^{-(2^\tau-1)\left(\frac{1}{\alpha}+2\right)(j+q)\lambda}}{\left(\left(\frac{1}{\alpha}+2\right)(j+q)\lambda + \frac{\beta}{2^\tau}\right)^2} \quad (15)$$

By Taylor series expansion when $(j+q)\lambda \to 0$, the SOP can be written as

$$P_k(\tau) = 1 - \sum_{j=1}^{N(K-1)+1} \sum_{q=0}^{KN-j} \frac{\mathrm{P}_{(j)}\Xi(N,K,j,q)}{(j+q)} \times \sum_{i=0}^{\infty} \frac{f^{(i)}(0)(j+q)^i\lambda^i}{i!} \quad (16)$$

where

$$f^{(i)}(0) = \left(\frac{\beta}{2^\tau}\right)^2 \frac{\partial^i}{\partial y^i}\left[\frac{e^{-(2^\tau-1)\left(\frac{1}{\alpha}+2\right)y}}{\left(\left(\frac{1}{\alpha}+2\right)y + \frac{\beta}{2^\tau}\right)^2}\right]\Bigg|_{y=0} = \left(\left(\frac{1}{\alpha}+2\right)(1-2^\tau)\right)^i {}_2F_0\left(2,-i;;\frac{2^\tau}{\beta(1-2^\tau)}\right).$$

By decomposing the infinite sum as $i=0$, $i=1,\ldots,N-1$, $i=N$ and $i=N+1,\ldots$, we have

$$\begin{aligned} P_k(\tau) \;=\; & 1 - \sum_{j=1}^{(K-1)N+1} \sum_{q=0}^{KN-j} \frac{\mathrm{P}_{(j)}\Xi(N,K,j,q)\, f^{(0)}(0)}{(j+q)} \\ & + \sum_{i=1}^{N-1} \sum_{j=1}^{N(K-1)+1} \sum_{q=0}^{KN-j} \frac{\mathrm{P}_{(j)}\Xi(N,K,j,q)\, f^{(i)}(0)}{i!(j+q)^{1-i}\lambda^{-t}} \\ & + \frac{\mathrm{P}_{((K-1)N+1)}(KN)! f^{(N)}(0)\lambda^N}{N!((K-1)N)!(N-1)!} \\ & \times \sum_{q=0}^{N-1} \frac{(-1)^q\binom{N-1}{q}}{((K-1)N+1+q)^{-(N-1)}} + \mathcal{O}\left(\lambda^{N+1}\right) \\ \overset{(a)}{=} \; & \frac{f^{(N)}(0)\mathrm{P}_{((K-1)N+1)}(KN)!}{N!((K-1)N)!(N-1)!} \\ & \times \sum_{q=0}^{N-1} \frac{(-1)^{q+1}\binom{N-1}{q}\lambda^N}{((K-1)N+1+q)^{-(N-1)}} + \mathcal{O}\left(\lambda^{N+1}\right), \end{aligned} \quad (17)$$

where (a) comes by using the binomial identities, and then due to the fact that the term corresponding to $i=0$ equals one and the terms corresponding to $i=1,\ldots,N-1$ equal zero. This proves that the k-th SD pair achieves full diversity. The diversity result for networks with RSI Model II and non-colluding eavesdroppers can be proved similarly. ■

B. High Transmit Power

For analysis with asymptotically high transmit power, we also illustrate the results for networks with RSI Model I and colluding eavesdroppers, where $P_k(\tau)$ is given in (15). The same results can be obtained for other network settings similarly. Define $\hat{\lambda} \triangleq l_c^\eta \sigma_0^2/\sigma_c^2$, $\hat{\alpha} \triangleq \sigma_0^2/\omega$, $\hat{\beta} \triangleq l_e^\eta \sigma_0^2/\sigma_e^2$, and $x \triangleq 1/p$, based on which $\lambda = \hat{\lambda}x$, $\alpha = \hat{\alpha}x^\nu$ and $\beta = \hat{\beta}x$. Further, infinite transmit power $p \to \infty$ is equivalent to $x \to 0$. We assume $\hat{\lambda}$ is a constant thus the main channel gain is linear in p. The following four cases are considered for different scalings of interference and wiretap channel gains.

1) Case 1 - Linearly Increasing Interference and Wiretap Channel Gains: This case corresponds to networks where $\nu = 1$ and $\hat{\beta}$ is a constant. From (15), by substituting $\lambda = \hat{\lambda}x$, $\alpha = \hat{\alpha}x$ and $\beta = \hat{\beta}x$ we have

$$P_k(\tau) = 1 - \sum_{j=1}^{N(K-1)+1} \sum_{q=0}^{KN-j} \frac{\mathrm{P}_{(j)}\Xi(N,K,j,q)}{(j+q)} \times \frac{\hat{\alpha}^2\hat{\beta}^2x^2 e^{-\frac{\hat{\lambda}(2^\tau-1)(j+q)(2\hat{\alpha}x+1)}{\hat{\alpha}}}}{\left(2^\tau(j+q)\hat{\lambda}(2\hat{\alpha}x+1) + \hat{\alpha}\hat{\beta}x\right)^2} \overset{x\to 0}{\longrightarrow} 1. \quad (18)$$

When $x \to 0$, the double summation term which scales as $\mathcal{O}(x^2)$ diminishes. This shows that when the transmit power affects all three channels, i.e., main, eavesdropper and interference, with linear scaling, the eavesdroppers succeed in interception with probability one.

2) Case 2 - Constant Interference Channel Gain and Linearly Increasing Wiretap Channel Gain: This case corresponds to networks with $\nu = 1$ and constant $\hat{\beta}$. From (15), we have

$$P_k(\tau) \overset{x\to 0}{\longrightarrow} 1 - \sum_{j=1}^{N(K-1)+1} \sum_{q=0}^{KN-j} \frac{\mathrm{P}_{(j)}\Xi(N,K,j,q)}{(j+q)} \times \frac{\hat{\alpha}^2\hat{\beta}^2}{\left(\hat{\alpha}\hat{\beta} + (2\hat{\alpha}+1)\hat{\lambda}2^\tau(j+q)\right)^2} \quad (19)$$

by using the Taylor series expansion at $x = 0$: $e^{-\left(\frac{1}{\hat{\alpha}}+2\right)\hat{\lambda}(2^\tau-1)(j+q)x} = 1 + \left(\frac{1}{\hat{\alpha}}+2\right)\hat{\lambda}(1-2^\tau)(j+q)x + \mathcal{O}\left(x^2\right)$. The result shows that an SOP floor as in (19) exists when the transmit power affects the main and eavesdropper channel gains only.

3) Case 3 - Linearly Increasing Interference Channel Gain and Constant Wiretap Channel Gain: This corresponds to the case of $\nu = 1$ and β is fixed for increasing p. It happens when the increment of the transmit power does not affect eavesdroppers' channels. From (15), we have

$$P_k(\tau) \xrightarrow{x\to 0} 1 - \sum_{j=1}^{N(K-1)+1} \sum_{q=0}^{KN-j} \frac{\mathrm{P}_{(j)}\Xi\left(N,K,j,q\right)}{(j+q)} \times \frac{\hat{\alpha}^2\hat{\beta}^2 e^{-\frac{\hat{\lambda}\left(2^\tau-1\right)(j+q)}{\hat{\alpha}}}}{\left(\hat{\alpha}\hat{\beta}+\hat{\lambda}2^\tau(j+q)\right)^2}, \quad (20)$$

where the limit is also from the Taylor series expansion at $x = 0$: $\frac{e^{-\frac{\hat{\lambda}\left(2^\tau-1\right)(j+q)(2\hat{\alpha}x+1)}{\hat{\alpha}}}}{\left(\hat{\alpha}\hat{\beta}+\hat{\lambda}2^\tau(j+q)(2\hat{\alpha}x+1)\right)^2} = \frac{e^{-\frac{\hat{\lambda}\left(2^\tau-1\right)(j+q)}{\hat{\alpha}}}}{\left(\hat{\alpha}\hat{\beta}+\hat{\lambda}2^\tau(j+q)\right)^2} + \mathcal{O}\left(x\right)$. The result also shows an SOP floor when the transmit power affects the main and interference channel gains only.

4) Case 4 - Constant Interference and Wiretap Channel Gains: In this case, only the average gain of the main channel increases with p while keeping other channel gains constants, which implies high MER and MIR. This case can thus be analyzed the similar way as in Section V-A, i.e., both α and β are fixed while $\lambda \to 0$.

VI. Analysis for Two-Hop Networks With Relay-Based Jamming

In this section, we consider the RS for two-hop networks with relay-based jamming and analyze the SOP. The key idea of relay-based jamming is to have relays that are not assigned for any SD-pair to transmit jamming signals to degrade the receive SINR at the eavesdroppers. The jamming signals can be artificial noises known to the destinations but unknown to the eavesdroppers. Recall that every user is supported by only one relay. For the case of $K = N$, there is no spare relay for jamming. For the case of $K < N$, there are $N - K$ spare relays after the RS and all of them intentionally send artificial jamming noises in the second hop of communications. Denote the index set of all available relays as $\mathcal{R} = \{R_1, \ldots, R_N\}$, the index set of the K relays selected for information transmissions as $\mathcal{R}^{(\mathrm{T})} = \{R_1^{(\mathrm{T})}, \ldots, R_K^{(\mathrm{T})}\}$, and the remaining index set of $N - K$ jamming relays as $\mathcal{R}^{(\mathrm{J})} = \{R_1^{(\mathrm{J})}, \ldots, R_{N-K}^{(\mathrm{J})}\}$. Thus, $\mathcal{R} = \mathcal{R}^{(\mathrm{T})} \cup \mathcal{R}^{(\mathrm{J})}$ and $\mathcal{R}^{(\mathrm{T})} \cap \mathcal{R}^{(\mathrm{J})} = \emptyset$. The average transmit power of each relay in $\mathcal{R}^{(\mathrm{J})}$ on each of the K channels is assumed to be p/K. The total average transmit power of each jamming relay is thus p, which is the same as the selected relays.

Since the destination nodes have knowledge of the jamming signals, they can cancel the jamming signals perfectly. Thus, even with relay jamming, expressions in (1) still hold for the received SINR at $R_{n,1}$ in the first hop and the SNR at D_k in the second hop. For the wiretap channels, the received SNR at E_1 is the same as $\gamma_{k,e1}$ in (2) as there is no source-based jamming. The received SINR at E_2 is however different due to jamming, which can be given as

$$\gamma_{n,e2}^{(\mathrm{J})} = \frac{\frac{p}{l_e^\eta\sigma_0^2}|g_{n,2}|^2}{\frac{p}{Kl_e^\eta\sigma_0^2}\sum_{m\in\mathcal{R}^{(\mathrm{J})}}|g_{m,2}|^2 + 1} = \frac{X}{\frac{1}{K}\sum_{m\in\mathcal{R}^{(\mathrm{J})}} X_m + 1}, \quad (21)$$

where $X \triangleq \frac{p}{l_e^\eta\sigma_0^2}|g_{n,2}|^2$ and $X_m \triangleq \frac{p}{l_e^\eta\sigma_0^2}|g_{m,2}|^2$. Notice that $X, X_m \sim \mathcal{E}xp(\beta)$ where $\beta = \frac{l_e^\eta\sigma_0^2}{p\,\sigma_e^2}$. The cumulative distribution function (c.d.f.) of $\gamma_{n,e2}^{(\mathrm{J})}$ can be derived as

$$F_{\gamma_{n,e2}^{(\mathrm{J})}}(t) = 1 - \frac{e^{-\beta t}}{\left(1+\frac{t}{K}\right)^{N-K}}. \quad (22)$$

A. Relay Selection

As discussed in Section III, with no jamming, we can develop the ORS scheme based on $\mathbf{\Gamma}_o = (\tilde{\gamma}_{kn})$ and the SRS scheme based on $\mathbf{\Gamma}_s = (\gamma_{kn})$ since the performance of each SD pair only depends on the relay chosen for the pair and is independent of the RS of other pairs when there is no conflict between relays. This is not the case for the network with relay jamming, since the performance of every SD pair depends on the RS of the other pairs via the set of jamming relays $\mathcal{R}^{(\mathrm{J})}$. There are $\frac{N!}{(N-K)!K!}$ possible RS sets and every possibility provides a different SINR value $\gamma_{n,e2}^{(\mathrm{J})}$ in (21). Thus the possible end-to-end SINRs for different RS sets cannot be represented with a matrix similar to $\mathbf{\Gamma}_o$ or $\mathbf{\Gamma}_s$. Thus, the development of the RS schemes and the corresponding performance analysis considering the concatenated effect of the relay jamming is left as future work. In this work, we use the SRS scheme proposed in Section III-B.2 to find the relay set for signal transmissions $\mathcal{R}^{(\mathrm{T})}$, and thus the remaining relay set $\mathcal{R}^{(\mathrm{J})}$ is used for jamming. The focus is to compare the performance between networks with and without relay jamming.

B. SOP Analysis

The SOP of the k-th SD pair can be calculated as in (7) where we now have a different p.d.f. for Z to (8) due to the different received SINR expression for E_2 in (21). Recall that $Z \triangleq (2^\tau - 1) + 2^\tau\gamma_{e,\cdot}$ and define $\Delta \triangleq \frac{2^\tau-1}{2^\tau K}$. With the aid of (22) and general probability rules, the p.d.f. of Z can be derived for colluding eavesdroppers as

$$f_Z(z) = \begin{cases} \frac{\beta}{2^\tau}e^{\beta\Delta K}e^{-\frac{\beta z}{2^\tau}}\left[1-\left(\frac{z}{2^\tau K}-\Delta+1\right)^{K-N} - \frac{\beta K\left(1-\left(\frac{z}{2^\tau K}-\Delta+1\right)^{K-N+1}\right)}{K-N+1}\right]; & \text{if } N-K>1; \\ \frac{\beta e^{\beta\Delta K}e^{-\frac{\beta z}{2^\tau}}}{2^\tau\left(\frac{z}{2^\tau K}-\Delta+1\right)}\left[\beta K\left(\frac{z}{2^\tau K}-\Delta+1\right)\right. \\ \left.\log\left(\frac{z}{2^\tau K}-\Delta+1\right)-\Delta+\frac{z}{2^\tau K}\right]; & \text{if } N-K=1. \end{cases} \quad (23)$$

For non-colluding eavesdroppers, we have

$$f_Z(z) = \frac{e^{2\beta\Delta K}}{e^{\frac{2\beta z}{2^\tau}}}\left[\left(\frac{e^{\frac{\beta z}{2^\tau}}}{e^{\beta\Delta K}}-1\right)\left(\frac{z}{2^\tau K}-\Delta+1\right)^{K-N-1} \times\left(\frac{\beta z}{2^\tau K}+(\beta-1)-\beta\Delta+\frac{N}{K}\right) +\beta\left(\frac{e^{\frac{\beta z}{2^\tau}}}{e^{\beta\Delta K}}-\left(\frac{z}{2^\tau K}-\Delta+1\right)^{K-N}\right)\right]. \quad (24)$$

$$\begin{aligned}\mathcal{J}_{(j)} &= 1-\sum_{q=0}^{NK-j}\frac{\Xi\left(N,K,j,q\right)}{(j+q)}\frac{\beta}{2^{\tau}}e^{\beta\Delta K}\int_{2^{\tau}-1}^{\infty}e^{-\lambda(j+q)\left(\frac{\sigma_i^2}{\sigma_0^2}+2\right)z}e^{-\frac{\beta z}{2^{\tau}}}\\ &\quad\times\left(1-\left(\frac{z}{2^{\tau}K}-\Delta+1\right)^{K-N}-\frac{\beta K\left(1-\left(\frac{z}{2^{\tau}K}-\Delta+1\right)^{K-N+1}\right)}{K-N+1}\right)dz.\\ &= 1-\sum_{q=0}^{NK-j}\frac{\Xi\left(N,K,j,q\right)}{(j+q)}\frac{\beta}{2^{\tau}}e^{\beta\Delta K}\left[\left(1-\frac{\beta K}{K-N+1}\right)\varpi_1\left(2^r-1,\left(\frac{1}{\alpha}+2\right)\lambda(j+q)+\frac{\beta}{2^r}\right)\right.\\ &\quad-\frac{\varpi_2\left(2^r-1,\left(\frac{1}{\alpha}+2\right)\lambda(j+q)+\frac{\beta}{2^r},K2^r(1-\Delta),K-N\right)}{\left(K2^r\right)^{K-N}}\\ &\quad\left.+\frac{\beta K\varpi_2\left(2^r-1,\left(\frac{1}{\alpha}+2\right)\lambda(j+q)+\frac{\beta}{2^r},K2^r(1-\Delta),K-N+1\right)}{(K-N+1)\left(K2^r\right)^{K-N+1}}\right],\end{aligned}\tag{25}$$

By using (23) and (24) in (7) and noticing that $F_{\gamma_{\mathrm{m}}^{(j)}}(z)$ has been derived for both RSI models in (11) and (13), $\mathcal{J}_{(j)}$ and the SOP for the network with relay jamming can be calculated.

For instance, for RSI Model I with colluding eavesdroppers when $N-K>1$, we can derive $\mathcal{J}_{(j)}$ as (25), shown at the top of this page, where we define $\varpi_1(a,b)\triangleq e^{-ab}/b$ and $\varpi_2(a,b,d,n)\triangleq e^{bd}b^{-n-1}\Gamma(n+1,b(a+d))$. The SOP for RSI Model I with colluding eavesdroppers and relay jamming when $N-K>1$ can be given as $P_k^{(\mathrm{j})}(\tau)=\sum_{j=1}^{(K-1)N+1}\mathrm{P}_{(j)}\mathcal{J}_{(j)}$. Other cases can be analyzed similarly.

VII. RS Schemes and Performance Analysis for Multi-Hop Networks

In this section, the general L-hop network is considered. As shown in Fig. 1 and explained in Section II, the network has $L+1$ layers of nodes, where the 0-th layer is composed of the K sources, the L-th layer is composed of the K destinations, and each layer in between is composed of N relays. In each hop, K relays out of N available ones are selected, one for each SD pair. Without loss of generality, we elaborate the communications of the k-th SD pair at the ℓ-th hop. If the $(n,\ell-1)$-th node is the selected node at the $(\ell-1)$-th layer for the k-th SD pair, it has N possible connections to the N relays at the ℓ-th layer.

A. Multi-Hop Relay Selection Schemes

The goal of RS is to maximize the minimum performance among all SD pairs to take into account the individual performance as well as fairness. While exhaustive search achieves the optimal solution, it is prohibitive in computations even for small networks. In addition, the use of exhaustive search requires a centralized system with a master node that has access to global CSI of all channels. The overhead for channel training/estimation and feedback are also dramatically large. It is more desirable and practical to design decentralized RS schemes with independent RS at each layer.

For HD multi-hop networks with two SD pairs and no eavesdroppers, a decentralized scheme was proposed in [45], where the RS for each hop are conducted independently. In this scheme, the selection of the relays in the ℓ-layer for $\ell=1,\ldots,L-2$ is based on the local CSI of the ℓ-th hop only (i.e., channels between the nodes of the $(\ell-1)$-th layer and the ℓ-th layer), while for the last relay layer, the CSI of both the last two hops (i.e., the $(L-1)$-th and L-th hops) is used, which is essential in achieving diversity. Following this idea, we propose two decentralized RS schemes, namely locally-ORS and locally-SRS, for the general multi-hop FD wiretap network with multiple SD pairs. The locally ORS scheme uses the secrecy rate values for RS and the locally SRS scheme uses the SINR values of the main channels for RS.

For the ℓ-th hop of the k-th SD pair, define $x_{kn,\ell}\triangleq\frac{p}{l_c^{\eta}\sigma_0^2}|f_{kn,\ell}|^2$, $u_{n,\ell}\triangleq\frac{1}{\sigma_0^2}|h_{n,\ell}|^2$, $\gamma_{kn,\ell}\triangleq\frac{x_{kn,\ell}}{1+u_{n,\ell}}$, $\gamma_{e\ell,k}\triangleq\frac{p}{l_e^{\eta}\sigma_0^2}|h_{k,\ell}|^2$, where $\gamma_{kn,\ell}$ and $\gamma_{e\ell,k}$ are the SINR of the main channel and the SNR of the wiretap channel. Thus, for the ℓ-th hop, the possible user secrecy rates for th k-th SD pair via the n-th relay is

$$c_{kn,\ell}=\left[\log_2\left(\frac{1+\gamma_{kn,\ell}}{1+\gamma_{e\ell,k}}\right)\right]^{+}.$$

1) Locally-ORS: For the locally-ORS scheme, the RS matrix for the ℓ-th layer is defined as

$$\mathbf{\Gamma}_{o,\ell}=(\tilde{\gamma}_{kn,\ell})\in\mathbb{R}^{K\times N},$$

where

$$\tilde{\gamma}_{kn,\ell}\triangleq\begin{cases}\dfrac{1+\gamma_{kn,\ell}}{1+\gamma_{e\ell,k}}; & \ell=1,\ldots,L-2;\\ \dfrac{1+\min\left(\gamma_{kn,L-1},\gamma_{nk,L}\right)}{1+\gamma_{e(L-1),k}}; & \ell=L-1.\end{cases}$$

where $\gamma_{e(L-1),k}$ depends on colluding or non-colluding case as given in (3). Denote the selected relay for S_k at the ℓ-th layer as $R_{l,k}^*$. To help the presentation, for the 0-th layer, let $R_{0,k}^*=S_k$ and for the L-th layer, let $R_{L,k}^*=D_k$. The proposed locally-ORS algorithm is given in Algorithm 2, where the RS is conducted layer-by-layer sequentially based on $\mathbf{\Gamma}_{o,\ell}$ and for each layer, the ORS scheme for the two-hop case in Algorithm 1 is used. Since $c_{kn,\ell}=[\log_2(\tilde{\gamma}_{kn,\ell})]^{+}$ for $\ell=1,\ldots,L-2$, the RS of each of the first $L-2$ relay layers is conducted independently based on maximizing the

minimum secrecy rate of all SD pairs. The RS of the last relay layer is based on the end-to-end secrecy rate of the last two hops, also following the max-min sense. This scheme needs local CSI of the main, eavesdropper, and interference channels at each layer.

Algorithm 2 The Locally-ORS Scheme for Multi-Hop Wiretap Networks

1: Calculate the RS matrices for the multiple communication hops: $\mathbf{\Gamma}_{s,1},\ldots,\mathbf{\Gamma}_{s,L-2},\mathbf{\Gamma}_{s,L-1}$.
2: Initialize the 0-th layer node selection, i.e., $R^*_{0,k}=S_k$ for $\forall k$.
3: **for** $\ell=1:L-1$ **do**
4: Make a random initialization for the relay assignment of the ℓ-th layer: $R^*_{\ell,k}$ for $\forall k$.
5: **for** $m=1:K$ **do**
6: Set flag=1;
7: **while** flag==1 **do**
8: Find the index $k_{\ell,m}$ whose value is the m-th lowest among $[\mathbf{\Gamma}_{s,\ell}]_{R^*_{\ell-1,1},R^*_{\ell,1}},\ldots,[\mathbf{\Gamma}_{s,\ell}]_{R^*_{\ell-1,K},R^*_{\ell,K}}$.
9: Check if a better RS exists for the $k_{\ell,m}$-th SD pair by calling function `find_another_relay`$(k_{\ell,m})$.
10: **if** a better selection can be found **then**
11: Update the relay selection to the found one for the ℓ-th layer.
12: **else**
13: flag=0;

The RS within a given hop has the worst-case complexity that is quadratic in both the number of relays and the number of users $\mathcal{O}\left(K^2N^2\right)$ which is the complexity for the two-hop network and the individual hop complexity in a general multi-hop network. Since the output of the ℓ-th hop selection depends on the previous $(\ell-1)$-th hop selection, the overall complexity of locally-ORS or locally-SRS is $\mathcal{O}\left((L-1)K^2N^2\right)$.

2) Locally-SRS: For the locally-SRS scheme, the RS matrix is defined as

$$\mathbf{\Gamma}_{s,\ell}\triangleq(\gamma_{kn,\ell})\in\mathbb{R}^{K\times N},$$

where

$$\gamma_{kn,\ell}\triangleq\begin{cases}\rho x_{kn,\ell}; & \ell=1,\ldots,L-2;\\ \min\left(\rho x_{kn},y_{nk}\right); & \ell=L-1.\end{cases}$$

It follows the same algorithm as locally-ORS with the RS matrix being replaced by $\mathbf{\Gamma}_{s,\ell}$. This scheme requires local CSI of the main channels and only the statistics of the interference channels. No information is needed for the wiretap channels.

B. The SOP of the Locally-SRS Scheme

For the multi-hop network, the effective end-to-end secrecy rate of the k-th SD pair, denoted as $c_{(k)}$, can be given as

$$c_{(k)}=\log_2\left(\frac{1+\min\limits_{\ell=1,\ldots,L-1}\gamma_{\ell,(k)}}{1+\gamma_{e,(k)}}\right),\tag{26}$$

where

$$\gamma_{e,(k)}=\begin{cases}\sum_{\ell=1}^{L}\gamma_{e\ell,(k)}; & \text{C};\\ \max\limits_{\ell=1,\ldots,L}\gamma_{e\ell,(k)}; & \text{NC},\end{cases}$$

$\gamma_{\ell,(k)}$ is the effective SINR of the k-th SD pair and $\gamma_{e\ell,(k)}$ is the eavesdropper SNR affected on the k-th SD pair, at the ℓ-th hop after RS. The $\gamma_{e,(k)}$'s defined in (26) have identical distribution for different k and are independent to $\gamma_{\ell,(k)}$'s. By defining $Z\triangleq(2^\tau-1)+2^\tau\gamma_{e,\cdot}$, the SOP of the k-th SD pair can be derived as follows.

$$\begin{aligned}P_k(\tau)&=\Pr[c_{(k)}\le\tau]\overset{(a)}{=}\Pr\left[\min_{\ell=1,\ldots,L-1}\gamma_{\ell,(k)}\le Z\right]\\&\overset{(b)}{=}1-\prod_{\ell=1}^{L-1}\left(1-\Pr[\gamma_{\ell,(k)}\le Z]\right)\\&\overset{(c)}{=}1-\int_{2^\tau-1}^{\infty}(1-\underbrace{\Pr[\gamma_{\ell,(k)}\le z|Z=z]}_{\triangleq F_{\ell,(k)}(z)})^{L-2}\\&\quad\times(1-\underbrace{\Pr[\gamma_{L-1,(k)}\le z|Z=z)}_{\triangleq F_{L-1,(k)}(z)}f_Z(z)dz,\end{aligned}\tag{27}$$

where (a) follows the definition of Z; (b) follows the independence of $\gamma_{\ell,(k)}$'s for $l=1,\ldots,L-1$; and (c) is obtained as the first $(L-1)$ hops are homogeneous with random variables associated to each hop identically distributed. The random variables associated to the last two hops, i.e, with the index $(L-1)$, are different from others as the last two hops involve joint selection.

It is important to note that $F_{L-1,(k)}(z)$ is derived exactly as in the two-hop case in Section IV as per (7) and is restated below:

$$F_{L-1,(k)}(z)=\sum_{j=1}^{(K-1)N+1}\mathrm{P}_{(j)}F_{\gamma_{\mathrm{m}}^{(j)}}(z).\tag{28}$$

In the following, we derive $F_{\ell,(k)}(z)$'s for $\ell=1,\ldots,L-2$ for locally-SRS.

1) RSI Model I: With the properties of the RS algorithm, we have

$$\begin{aligned}F_{\ell,(k)}(z)&=\sum_{j=1}^{(K-1)N+1}\mathrm{P}_{(j)}\Pr\left[\rho x^{(j)}\le z\right]\\&\overset{(a)}{=}1-\sum_{j=1}^{(K-1)N+1}\sum_{q=0}^{KN-j}\frac{\mathrm{P}_{(j)}\Xi\left(N,K,j,q\right)}{(j+q)e^{\frac{(\alpha+1)\lambda(j+q)}{\alpha}z}},\end{aligned}\tag{29}$$

where (a) follows the derivation result in (6) with λ_c set as λ/ρ. Further, as we expect, $F_{\ell,(k)}(z)$ is independent of ρ.

2) RSI Model II: Following similar steps in (29), we get for RSI Model II,

$$\begin{aligned}F_{\ell,(k)}(z)&=\sum_{j=1}^{(K-1)N+1}\mathrm{P}_{(j)}\Pr\left[\frac{x^{(j)}}{1+u^{(j)}}\le z\right]\\&=1-\sum_{j=1}^{(K-1)N+1}\mathrm{P}_{(j)}\mathbb{E}\left[F_{u^{(j)}}\left(\frac{\rho\,x^{(j)}}{\rho\,z}-1\right)\mathbb{1}_{\rho x^{(j)}\ge\rho z}\right]\\&=1-\sum_{j=1}^{(K-1)N+1}\sum_{q=0}^{KN-j}\frac{\mathrm{P}_{(j)}\Xi\left(N,K,j,q\right)}{(j+q)}\\&\quad\times\frac{\alpha\,e^{\lambda z(-(j+q))}}{(\alpha+\lambda z(j+q))},\end{aligned}\tag{30}$$

$$P_k(\tau) \overset{(a)}{=} 1 - \sum_{i=1}^{(K-1)N+1} \sum_{j=1}^{(K-1)N+1} \sum_{s=0}^{KN-i} \sum_{q=0}^{KN-j} \frac{\alpha^3\beta^3 (KN)!^2 (-1)^{s+q} \mathrm{P}_{(i)} \mathrm{P}_{(j)} \binom{KN-i}{s} \binom{KN-j}{q}}{(i+s)(j+q)(KN-i)!(KN-j)!}$$
$$\times \frac{1}{(i-1)!(j-1)!} \frac{e^{-\frac{\lambda\left(2^r-1\right)(\alpha(i+2\ j+s+2\ q)+i+j+s+q)}{\alpha}}}{\left(\alpha\beta + \lambda 2^r(\alpha(i+2\ j+s+2\ q)+i+j+s+q)\right)^3}$$
$$\overset{(b)}{=} \sum_{i=1}^{(K-1)N+1} \sum_{j=1}^{(K-1)N+1} \sum_{s=0}^{KN-i} \sum_{q=0}^{KN-j} \frac{(KN)!^2 (-1)^{s+q+1} \mathrm{P}_{(i)} \mathrm{P}_{(j)} \binom{KN-i}{s} \binom{KN-j}{q}}{N!(i+s)(j+q)(KN-i)!(KN-j)!}$$
$$\times \frac{\left(\frac{1-2^r}{\alpha}\right)^N {}_2F_0\left(3, -N; ; \frac{2^r}{\beta - 2^r\beta}\right)}{(i-1)!(j-1)!(\alpha(i+2\ j+s+2\ q)+i+j+s+q)^{-N}} \lambda^N + \mathcal{O}\left(\lambda^{N+1}\right). \tag{32}$$

which is also independent of ρ. By using the fact that p.d.f. s of summation and maximum of n i.i.d. random variables having distribution $\mathcal{E}xp(a)$ are $a^n x^{n-1} e^{-ax}/(n-1)!$ and $nae^{-ax}(1-e^{-ax})^{n-1}$, respectively, we can derive the p.d.f. for $Z = (2^\tau - 1) + 2^\tau \gamma_{e,\cdot}$ with the aid of (26) as

$$f_Z(z) = \begin{cases} \left(\frac{\beta}{2^\tau}\right)^L e^{\frac{\beta(2^\tau-1)}{2^\tau}} \frac{(z-(2^\tau-1))^{L-1}}{(L-1)! e^{\frac{\beta}{2^\tau}z}}; & \text{for C;} \\ \frac{L\beta}{2^\tau} \frac{e^{\frac{\beta(2^\tau-1)}{2^\tau}}}{e^{\frac{\beta}{2^\tau}z}} \left(1 - \frac{e^{\frac{\beta(2^\tau-1)}{2^\tau}}}{e^{\frac{\beta}{2^\tau}z}}\right)^{L-1}; & \text{for NC.} \end{cases} \tag{31}$$

Now, by substituting (29), (30), and (31) into (27) together with results in Section IV, one can derive $P_k(\tau)$ in closed-form for either RSI model under locally-SRS scheme. However, the derivations are tedious and lengthy although it involves straightforward mathematical manipulations with multinomial/binomial expansions. Therefore, we provide an example instead.

Example: Consider a three-hop ($L = 3$) network with K SD pairs, N relays and three colluding eavesdroppers. By following (27), the SOP can be derived as in (32), shown at the top of this page. In (32), (a) is obtained by substituting (29) for $F_{1,(k)}(z)$, (11) and (28) for $F_{2,(k)}(z)$, and (31) with $L = 3$ for $f_Z(z)$; and then by solving the integral. This is the SOP in closed-form for $L = 3$. To analyze the diversity order, we then consider the case of $\lambda \to 0$ and use in Step (b) the Taylor series expansion at $\lambda = 0$. The constant 1 gets canceled and the $\mathcal{O}(\lambda^i)$-terms for $i = 1, \ldots, N-1$ are zero (as explained in the proof of Theorem 1). Thus, the first non-zero term for $P_k(\tau)$ scales as λ^N, meaning that full diversity order N is achieved. We may extend the analysis for any L-hop network to show that the diversity order is N.

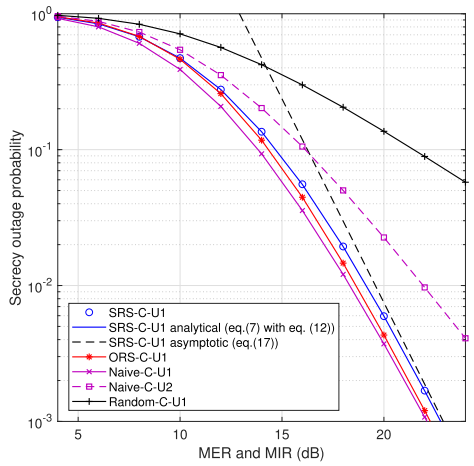
VIII. Numerical Results and Discussion

This section presents numerical results to show the performance in term of the SOP or the intercept probability, i.e., $P_k(\tau = 0)$. In the figure legend, we denote the k-th SD pair as Uk, e.g., one can read the curve with the legend 'SRS-C-U1' as the result of the 1-st SD pair for the SRS scheme with colluding eavesdroppers. The performance of our proposed SRS scheme is compared against the performance benchmark that is identified based on our proposed ORS scheme. In some cases, we also compare their performance with the naive and random RS schemes.

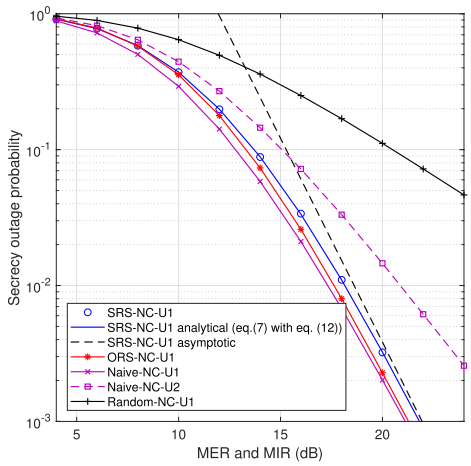
A. Two-Hop Networks

In Fig. 2, two-hop networks are considered with $K = 2$ and $N = 3$. We normalize parameters σ_0^2, p, l_c, $l_{e,\ell}$ and set $\tau = 1$ [bits/sec/Hz] and $\sigma_i^2 = \omega p$, i.e., $\nu = 1$. The parameters σ_c^2, σ_e^2, ω are varied in order to get MER and MIR in range 0-24 dB. In Fig. 2, the SOP is shown for ORS and SRS, together with naive and random RS schemes for comparison. In naive RS, the 1st SD pair first selects their best relay, then the 2nd SD pair select their relay from the remaining relays. As such, the SOPs of the two pairs are different. For the SRS, ORS, and random RS schemes, both pairs have the same SOP, thus only the intercept probability of the 1st SD pair is shown. We also provide analytical results for SRS in the figure. Several observations are gained from Fig. 2. i) For the entire simulated power range, our exact analytical results (based on (7)) closely match the simulation results for SRS, which confirms the accuracy of our analysis in Section IV. The derived SOP approximations for large MER and MIR are accurate (only provided for RSI Model I), which confirms the validity of our analysis for diversity order in Section V-A. ii) While the ORS and SRS schemes achieve the full diversity order of three for both SD pairs, the naive scheme achieves full diversity for the 1st SD pair but diversity order two for the 2nd SD pair. The random RS provides a diversity order of one only. This demonstrates the unfairness of the naive RS scheme and undesired performance of the random RS. For RSI Model I with colluding at $\mathrm{MER} = \mathrm{MIR} = 16$ dB, ORS outperforms SRS by 1 dB, and naive RS (the 1st SD pair) outperforms SRS by 1.9 dB. However, SRS outperforms naive RS (the 2nd SD pair) and random RS by 2.8 dB and 7.3 dB, respectively, which are significant improvements on the PHY security aspect. Similar observations can be seen for RSI Model II. iii) For all RS schemes, the network with non-colluding eavesdroppers outperforms the network with colluding eavesdroppers because colluding eavesdroppers cooperate with each other.

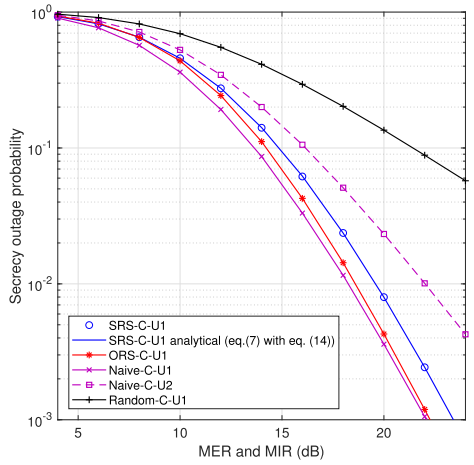
In Fig. 3, we use more general settings, where the path-loss is 140 dB for the first kilometer of each hop with $\eta = 3$, $\tau = 0$, $\sigma_0^2 = 0.01$, $\omega = 0.01$, $\nu = 1$, $\sigma_c^2 = 1$, $\sigma_e^2 = 1$, $l_c = 500$ m, and $l_e = 2\, l_c$ m. The transmit power range is from 0 dBm to 20 dBm. For $K = 2$ and $N = 3$, we plot the intercept probability for the four cases discussed in Section V-B. Again, the analytical results in (18)-(20) closely match the simulation results, and asymptotic results in (18)-(20) approach



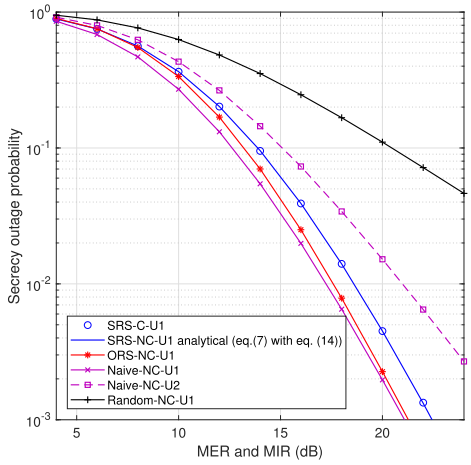
(a) RSI Model I with colluding eavesdroppers.



(b) RSI Model I with non-colluding eavesdroppers.

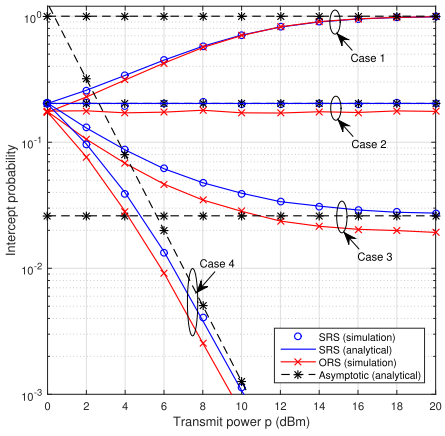


(c) RSI Model II with colluding eavesdroppers.

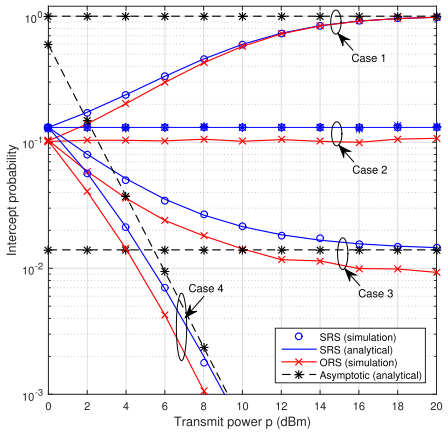


(d) RSI Model II with non-colluding eavesdroppers.

Fig. 2. The SOP for two-hop network with two SD pairs and three relays.



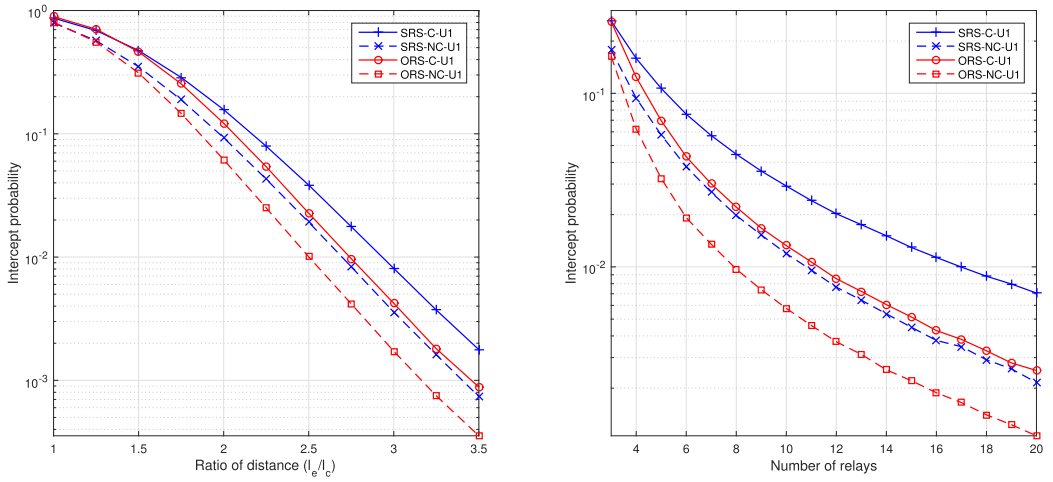
(a) Colluding eavesdroppers.



(b) Non-colluding eavesdroppers.

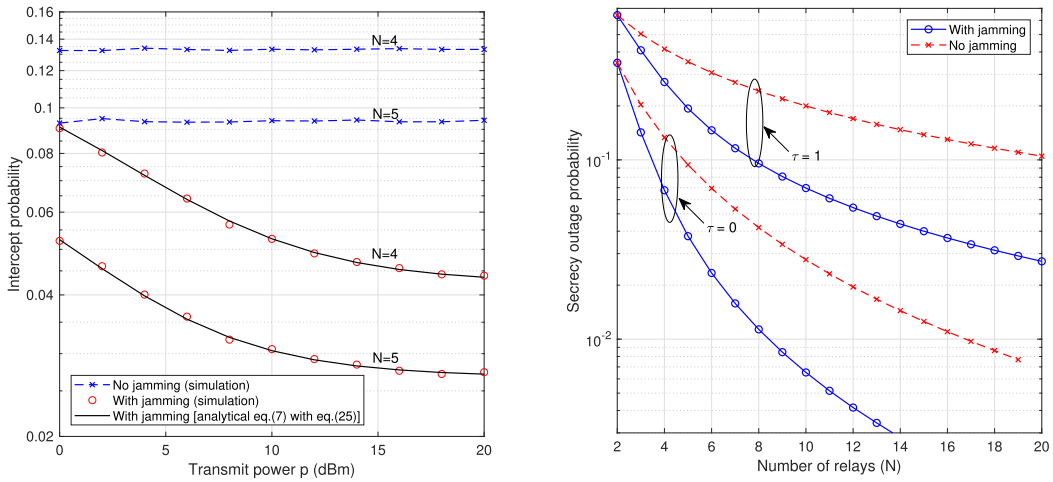
Fig. 3. Intercept probability for two-hop networks with two SD pairs and three relays under RSI Model-I.

the exact ones at high transmit power region which confirms the accuracy of our analysis in Section V-B. The first three cases have intercept probability floors for both ORS and SRS, as self-interference and/or eavesdroppers SNR are proportional with p. As shown in Case 1, neither RS scheme can support securing user information unless we suppress the effective



(a) With ratio of distance l_c/l_e for $N = 4$. (b) With number of relays N for $l_c = 0.5l_e = 500\,\text{m}$.

Fig. 4. Intercept probability for two-hop networks with three SD pairs under RSI Model I.



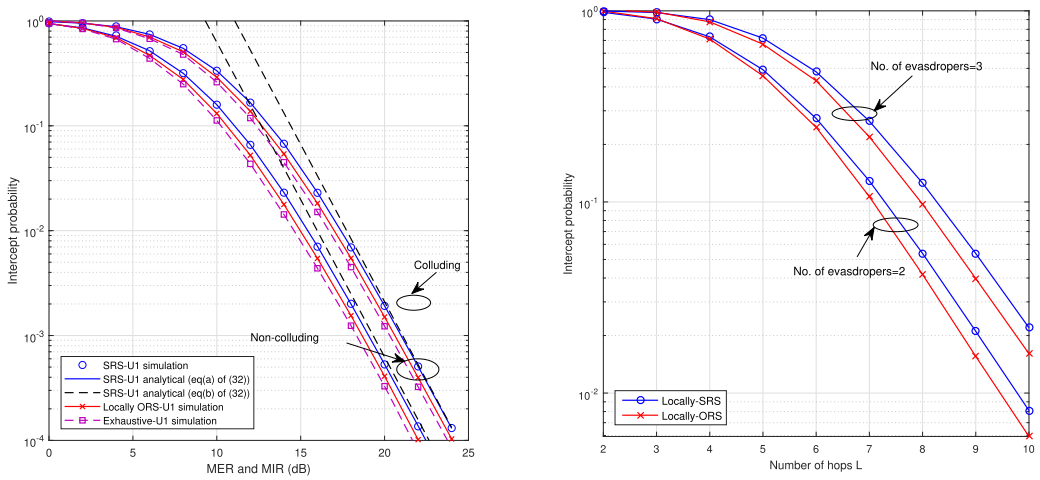
(a) With transmit power p for $N = 4$ and $N = 5$. (b) With number of relays N for $\tau = 0$ and $\tau = 1$.

Fig. 5. Intercept probability and SOP for two-hop networks with two SD pairs under RSI Model I and colluding eavesdroppers.

power level by some wireless techniques, e.g., beamforming, jamming, etc.. For Case 2, the intercept probability is a constant for all p, as both rates of the main and wiretap channels increases with p. The intercept probability of Case 3 depends on the capability of self-interference mitigation ω.

In Fig. 4, we use the same path-loss model as in Fig. 3 where $\tau = 0$, $\sigma_0^2 = 0.01$, $\omega = 0.01$, $\nu = 0$, $\sigma_c^2 = 1$, $\sigma_e^2 = 1$, and $p = 10\,\text{dBm}$. Fig. 4a plots the intercept probability versus the ratio of distance l_c/l_e when $l_c = 500\,\text{m}$, $K = 3$, and $N = 4$. Fig. 4b plots the intercept probability versus the number of relays N when $l_c = 500\,\text{m}$, $l_e = 1000\,\text{m}$ and $K = 3$. While observing that ORS outperforms SRS, non-colluding also outperforms the colluding eavesdropper case from both plots. As shown in Fig. 4a, when the distance l_e increases, a significant performance improvement can be observed. For example, for the colluding case, when l_e/l_c increases from 2 to 3, the performance improves by 12.9 dB and 14.6 dB for SRS and ORS, respectively. This observation also reveals the importance of considering PHY security with distance-dependent path-loss. Further, performance improvements of ORS with respect to SRS are 1.1 dB and 2.8 dB for $l_e/l_c = 2$ to $l_e/l_c = 3$, respectively, which come from having additional knowledge of the instantaneous CSI of the eavesdropper channels. Similarly, as shown in Fig. 4b, when the number of relays increases, intercept probability decreases dramatically. For example, for the colluding case, when we increase N from 5 to 15, the performance improves by 9.2 dB and 11.3 dB for SRS and ORS, respectively. However, the overhead cost also increases.

Next, we compare the performance of networks with and without relay jamming in Fig. 5, where the same systems parameters are used as those in Fig. 3. Fig. 5a is for intercept probability vs transmit power when $K = 2$ and $N = 4, 5$. For no jamming, since both the eavesdropper and the user rates



(a) With MER and MIR.

(b) With number of hops L

Fig. 6. Intercept probability for multi-hop networks with RSI Model I and colluding eavesdroppers.

increase with the same rate as p changes, Fig. 5a shows an almost constant intercept-probability floor for all p, similar to Case 2 in Fig. 3. With jamming, since the transmit power has more impact on the interference to eavesdroppers, the intercept probability approaches its floor only at high p. This figure shows the advantage of relay-based jamming. For instance at $p = 10$ dB, we achieve 4.0 dB and 4.8 dB performance gain with jamming over no jamming when $N = 4$ and $N = 5$, respectively. Further, the derived analytical results on the SOP tightly match the simulation. Fig. 5b is for the SOP vs transmit power when $\tau = 0$ and $\tau = 1$. While the SOP of all cases decreases with N, it increases when the threshold τ increases. It is important to note that the SOP of systems with jamming decreases with N dramatically, e.g., when N increases from 4 to 10, we achieve 10 dB and 6.8 dB performance gains with jamming and without jamming, respectively, where we have additional 3.2 dB gain with jamming.

B. Multi-Hop Network

In this subsection, a multi-hop network is considered where $K = 2$, $N = 3$ and $L = 3$. RSI Model I is assumed. Other parameters are the same as the ones in Fig. 2. As can be seen from Fig. 6a, our exact analytical results (given in (32)) closely match the simulation results for locally-SRS and the derived approximations are also accurate for large MER and MIR. This confirms the validity of our analysis in Section VII. Further, we compare the simulated intercept probabilities of locally-SRS with the optimal RS (via exhaustive search) and locally-ORS. All schemes achieve full diversity order of three. As expected, the exhaustive search outperforms both locally-ORS and locally-SRS. For example, for the colluding case, its advantage over the two local schemes is 0.8 dB and 1.8 dB, respectively. However, considering the significant extra costs complexity which is exponential in the number of hops and overhead for the global channel knowledge, the proposed local RS schemes are apparently more desirable.

In Fig. 6b, we consider a network where $K = 3$ and $N = 4$, and use the same general parameters as in Fig. 3. RSI Model I and colluding eavesdroppers are adopted. We consider two scenarios where the first scenario has 2 eavesdroppers and the second has 3 eavesdroppers. Although our system model is set up for one eavesdropper on each layer, the model and corresponding analysis can be extended to any number of eavesdroppers per layer, including the case of no eavesdropper on some layers. Regardless of the number of hops, the distance between the SD pairs is fixed as 3 km. The distance of an eavesdropper to its attacking transmitting node-layer is fixed as 1 km. In practice, this fixed distance may vary by placing more intermediate layers. However, we neglect such variations. Then, we increase L by placing more layers of relays between the sources and destinations and each layer has equal distance. For the first scenario with 2 eavesdroppers, the information may be intercepted with probability one for a two-hop ($L = 2$) network. However, if we can insert more relay layers between the SD pairs without any notice for eavesdropper network (i.e., same number of eavesdroppers), the figure shows that the intercept probability can be decreased significantly. For example, we have 5.5 dB and 6.1 dB improvement with six hops for locally-SRS and locally-ORS, respectively. Similar observation can be seen with three eavesdroppers which always underperforms the two-eavesdropper scenario.

IX. Conclusion

In this work, the RS problem was considered for a FD wireless network with multiple source-destination pairs, multiple DF relays, and multiple colluding and non-colluding eavesdroppers. RS schemes were designed to maximize the minimum secrecy rate among all source-destination pairs under two self-interference models. For two-hop networks, optimal RS and sub-optimal RS schemes were proposed based on available CSI. The exact secrecy outage probability for the more practical sub-optimal RS scheme was derived, and subsequent analysis proves that full diversity can be achieved when the gains of the main-to-eavesdropper and the main-to-interference channels increase asymptotically. With the help of unallocated relays for user communications, a relay-based

jamming scheme was proposed to enhance the secrecy. The schemes were extended to general multi-hop FD relay network with multiple eavesdroppers with analytical results on the intercept probability. Simulation results illustrated that the secrecy performance of multi-hop FD relay network can be boosted significantly with the proposed schemes. Since multi-user two-hop or multi-user multi-hop has not even been considered for the HD relaying, the proposed RS schemes and analytical framework can easily be applied for HD networks.

Further, our joint RS scheme can be implemented in future wireless applications focused on the security, user-fairness and URLLC. There are several directions for future works. First, *optimal* RS schemes for either source-based or relay-based jamming can be considered to further enhance the robustness and PHY-security in multi-user networks. Second, implementing non-orthogonal multiple-access transmission schemes can improve the throughput and transmission time. Third, RS designs for the more general case of non-identical channels is attractive and important.

REFERENCES

[1] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2119–2123, Sep. 2004.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[3] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[4] 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.

[5] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[6] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[7] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Netw.*, vol. 27, no. 3, pp. 28–33, May/Jun. 2013.

[8] X. Chen, Z. Zhang, H.-H. Chen, and H. Zhang, "Enhancing wireless information and power transfer by exploiting multi-antenna techniques," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 133–141, Apr. 2015.

[9] M. Duarte and A. Sabharwal, "Full-duplex wireless communications using off-the-shelf radios: Feasibility and first results," in *Proc. 40th Asilomar Conf. Signals Syst. Comput.*, Nov. 2010, pp. 1558–1562.

[10] L. J. Rodríguez, N. H. Tran, and T. Le-Ngoc, "Performance of full-duplex AF relaying in the presence of residual self-interference," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1752–1764, Sep. 2014.

[11] S. Hong *et al.*, "Applications of self-interference cancellation in 5G and beyond," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 114–121, Feb. 2014.

[12] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.

[13] S. Atapattu, Y. Jing, H. Jiang, and C. Tellambura, "Relay selection and performance analysis in multiple-user networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 8, pp. 1517–1529, Aug. 2013.

[14] A. Zappone, S. Atapattu, M. Di Renzo, J. Evans, and M. Debbah, "Energy-efficient relay assignment and power control in multi-user and multi-relay networks," *IEEE Wireless Commun. Lett.*, vol. 7, no. 6, pp. 1070–1073, Dec. 2018.

[15] S. Atapattu, P. Dharmawansa, M. Di Renzo, C. Tellambura, and J. Evans, "Multi-user relay selection for full-duplex radio," *IEEE Trans. Commun.*, to be published.

[16] 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.

[17] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3299–3310, Sep. 2014.

[18] L. Fan, N. Yang, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Exploiting direct links for physical layer security in multiuser multirelay networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3856–3867, Jun. 2016.

[19] W. Cao, Y. Zou, and Z. Yang, "Joint source-relay selection for improving wireless physical-layer security," in *Proc. IEEE Global Commn. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–5.

[20] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1147–1151, Aug. 2015.

[21] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Power-constrained secrecy rate maximization for joint relay and jammer selection assisted wireless networks," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2180–2193, May 2017.

[22] X. Ding, T. Song, Y. Zou, X. Chen, and L. Hanzo, "Security-reliability tradeoff analysis of artificial noise aided two-way opportunistic relay selection," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3930–3941, May 2017.

[23] A. H. A. El-Malek, A. M. Salhab, and S. A. Zummo, "New bandwidth efficient relaying schemes in cooperative cognitive two-way relay networks with physical layer security," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5372–5386, Jun. 2017.

[24] S. Parsaeefard and T. Le-Ngoc, "Improving wireless secrecy rate via full-duplex relay-assisted protocols," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2095–2107, Oct. 2015.

[25] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

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

[27] H. He, P. Ren, Q. Du, and L. Sun, "Full-duplex or half-duplex? Hybrid relay selection for physical layer secrecy," in *Proc. IEEE Veh. Technol. Conf. (VTC)*, May 2016, pp. 1–5.

[28] N.-P. Nguyen, C. Kundu, H. Q. Ngo, T. Q. Duong, and B. Canberk, "Secure full-duplex small-cell networks in a spectrum sharing environment," *IEEE Access*, vol. 4, pp. 3087–3099, 2016.

[29] Y. Feng, Z. Yang, S. Yan, N. Yang, and B. Lv, "Physical layer security enhancement in multi-user multi-full-duplex-relay networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–7.

[30] W. Saad, X. Zhou, B. Maham, T. Basar, and H. V. Poor, "Tree formation with physical layer security considerations in wireless multi-hop networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 3980–3991, Nov. 2012.

[31] J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 753–764, Feb. 2016.

[32] Y. Xu, J. Liu, Y. Shen, X. Jiang, and T. Taleb, "Security/QoS-aware route selection in multi-hop wireless ad hoc networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.

[33] J. H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525–528, Apr. 2015.

[34] F. Tian *et al.*, "Secrecy rate optimization in wireless multi-hop full duplex networks," *IEEE Access*, vol. 6, pp. 5695–5704, 2018.

[35] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[36] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, "Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8286–8297, Dec. 2016.

[37] 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.

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

[39] A. Sheikholeslami, M. Ghaderi, H. Pishro-Nik, and D. Goeckel, "Jamming-aware minimum energy routing in wireless networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 2313–2318.
[40] M. Ghaderi, D. Goeckel, A. Orda, and M. Dehghan, "Minimum energy routing and jamming to thwart wireless network eavesdroppers," *IEEE Trans. Mobile Comput.*, vol. 14, no. 7, pp. 1433–1448, Jul. 2015.
[41] A. Mishra and T. Alexander, "Radio communications: Components, systems, and networks [Series Editorial]," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 142–143, Jun. 2015.
[42] S. Atapattu, N. Ross, Y. Jing, Y. He, and J. Evans, "Physical-layer security in full-duplex multi-user relay networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.
[43] S. Sharma, Y. Shi, Y. T. Hou, and S. Kompella, "An optimal algorithm for relay node assignment in cooperative ad hoc networks," *IEEE/ACM Trans. Netw.*, vol. 19, no. 3, pp. 879–892, Jun. 2010.
[44] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Processes*, 4th ed. New York, NY, USA: McGraw-Hill, 2002.
[45] R. Senanayake, S. Atapattu, J. S. Evans, and P. J. Smith, "Decentralized relay selection in multi-user multihop decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 5, pp. 3313–3326, May 2018.

Saman Atapattu (M'14) received the B.Sc. degree in electrical and electronics engineering from the University of Peradeniya, Sri Lanka, in 2003, the M.Eng. degree in telecommunications from the Asian Institute of Technology, Thailand, in 2007, and the Ph.D. degree in electrical engineering from the University of Alberta, Canada, in 2013. He is currently a Research Fellow with the Department of Electrical and Electronic Engineering, The University of Melbourne, Australia. His research interests include wireless communications and signal processing.

Nathan Ross received the Ph.D. degree in mathematics from the University of Southern California in 2009. From 2009 to 2013, he held a Post-doctoral research position with the Department of Statistics, UC Berkeley. He is currently a Senior Lecturer with the School of Mathematics and Statistics, The University of Melbourne.

Yindi Jing received the B.Eng. and M.Eng. degrees in automatic control from the University of Science and Technology of China, Hefei, China, in 1996 and 1999, respectively, and the M.Sc. and Ph.D. degrees in electrical engineering from the California Institute of Technology, Pasadena, CA, USA, in 2000 and 2004, respectively. From 2004 to 2005, she was a Post-doctoral Scholar with the Department of Electrical Engineering, California Institute of Technology. From 2006 to 2008, she was a Post-doctoral Scholar with the Department of Electrical Engineering and Computer Science, University of California at Irvine, Irvine. In 2008, she joined the Electrical and Computer Engineering Department, University of Alberta, where she is currently a Professor.

Her research interests are in wireless communications, focusing on massive MIMO, cooperative relay networks, and channel estimation. She has been a member of the IEEE Signal Processing Society Signal Processing for Communications and Networking Technical Committee, since 2015, and a member of the NSERC Discover Grant Evaluation Group for Electrical and Computer Engineering since 2017. She was an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2011 to 2016. She currently serves as a Senior Area Editor for the IEEE SIGNAL PROCESSING LETTERS.

Yuanyuan He (S'08–M'12) received the Ph.D. degree from the Department of Electrical and Electronic Engineering, The University of Melbourne, Melbourne, Australia. In 2017, she was a Visiting Researcher with the Department of Electrical and Computer Engineering, University of Alberta, Canada. She is currently a Research Fellow with The University of Melbourne. Her current research interests lie in the area of wireless communications, including resource allocation, spatial modulation, and full-duplex communications.

Jamie S. Evans (S'93–M'98–SM'17) was born in Newcastle, Australia, in 1970. He received the B.S. degree in physics and the B.E. degree in computer engineering from The University of Newcastle, in 1992 and 1993, respectively, and the M.S. and Ph.D. degrees in electrical engineering from The University of Melbourne, Australia, in 1996 and 1998, respectively. He was awarded the Chancellor's Prize for excellence for his Ph.D. thesis. He received the University Medal upon graduation from The University of Newcastle.

From 1998 to 1999, he was a Visiting Researcher with the Department of Electrical Engineering and Computer Science, University of California at Berkeley, Berkeley. Since returning to Australia in 1999, he has held academic positions at the University of Sydney, The University of Melbourne, and Monash University. He is currently a Professor and the Deputy Dean with the Melbourne School of Engineering, The University of Melbourne. His research interests are in communications theory, information theory, and statistical signal processing with a focus on wireless communications networks.