Physical-Layer Security in Full-Duplex Multi-User Relay Networks

Saman Atapattu*, Nathan Ross†, Yindi Jing‡, Yuanyuan He*, and Jamie Evans*
*Department of Electrical and Electronic Engineering, University of Melbourne, Victoria, Australia
†School of Mathematics and Statistics, University of Melbourne, Victoria, Australia
‡Department of Electrical and Computer Engineering, University of Alberta, Edmonton, Canada
Email: *†{saman.atapattu, nathan.ross, yuanyuan.he, jse}@unimelb.edu.au, ‡yindi@ualberta.ca

***Abstract*—This paper studies the relay selection (RS) problem for full-duplex (FD) relay networks with multiple source-destination (SD) pairs under the attack of colluding eavesdroppers. Based on available channel state information (CSI), both optimal relay selection (ORS) and suboptimal relay selection (SRS) schemes are considered to maximize the minimum secrecy rate among all pairs in order to enhance the physical-layer security. The secrecy performance of the more practical SRS scheme is then evaluated in terms of intercept probability and diversity order. The SRS achieves full diversity when the gains of the main-to-eavesdropper and the main-to-interference channels increase asymptotically.**

***Index Terms*—Full-duplex communications, intercept probability, multi-user networks, physical-layer security, relay selection.**

I. Introduction

The physical-layer (PHY) security is becoming an essential requirement in multi-user networks which will be the fundamental network architecture of the fifth generation (5G) applications. Especially in multi-user cooperative relay networks, many transmitters can be exposed to adversarial users who may extract the legitimate user information [1]. The full-duplex (FD) communication which enables simultaneous transmission and reception on a common time-frequency channel is one of the promising technologies of new 5G configurations [2]. As the FD transceiver suffers from both residual self-interference (RSI) and eavesdroppers' attack, the relay selection (RS) techniques have great potential in achieving PHY security [3].

Most of existing work on PHY security in relay networks with RS focus on half-duplex (HD) relaying [4]–[6, and references therein]. Optimal RS schemes are studied in [4] for networks with single source-destination (SD) pair and multiple relays in the presence of single eavesdropper at the relay under both amplify-and-forward (AF) and decode-and-forward (DF) protocols, where full diversity is achieved. For a network of multiple-relays, -destinations and -eavesdroppers, but with single source, RS criteria are proposed for the best relay-user pair selection in [5]. However, eavesdroppers attack the relay transmission only but not the source transmission. Secure relay and jammer selections are also studied in [6].

This work is supported by the Australian Research Council (ARC) through the Discovery Early Career Researcher (DECRA) Award DE160100020.

The works in [7]–[9, and references therein] consider the PHY security for RS with FD relaying. For networks with single SD pair, in [7], a hybrid RS scheme is proposed that switches between HD and FD and the secrecy outage probability is analyzed. In [8], 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. [9] considers a network with multiple users, multiple relays, and single destination with an eavesdropper who can overhear the relay transmission, where a joint user and RS scheme is proposed for the PHY security.

The RS problem for PHY security in relay networks with multiple SD pairs where each source has its own destination is still an open problem for either HD or FD mode. This paper thus studies the RS problem in FD relay networks with multiple SD pairs, multiple common DF relays and two cooperative (or colluding) eavesdroppers who can attack both source and relay transmissions. Further, findings of this work can be easily extended to a similar HD relay network, which is still an unexplored problem. Based on the work in [10], [11], two RS schemes are proposed, the optimal relay selection (ORS) and the sub-optimal relay selection (SRS), in order to maximize the minimum secrecy rate among all SD pairs. Then, intercept probability is derived for the low-complex SRS scheme which requires channel state information (CSI) of the main channels and only the statistical information of self-interference channels. The SRS scheme is shown to provide full diversity when the gains of the main-to-eavesdropper and the main-to-interference channels increase asymptotically.

II. System Model

This work considers a multi-SD-pair dual-hop multi-relay wiretap network as shown in Fig. 1.

A. Network Model

In the wireless network, the K sources $S_1, \cdots, S_K$ send information to their corresponding destinations $D_1, \cdots, D_K$ via N intermediate relays $R_1, \cdots, R_N$ where $N \geq K$. There is no direct link from S_k to D_k for $k = 1, \cdots, K$. While S_k, R_n and D_k are legitimate nodes, S_k and R_n transmissions are exposed to eavesdroppers E_1 and E_2, respectively. Each

978-1-5386-3180-5/18/$31.00 ©2018 IEEE

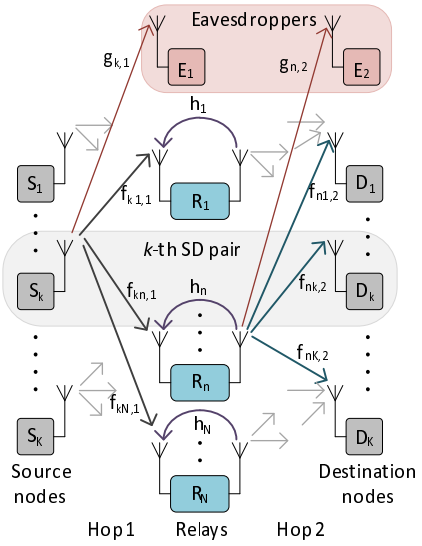

Fig. 1. A FD multi-SD-pair multi-relay wiretap network.

source has a transmit antenna. Each destination or eavesdropper has a single receive antenna. Each relay has one transmit antenna and one receive antenna. The relays are in the FD mode with DF.

The distances between S_k to R_n and R_n to D_k are the same, denoted as l_c. The distance between S_k to E_1 and R_n to E_2 are the same, 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 coefficients from S_k to R_n and R_n to D_k as $f_{kn,1}$ and $f_{nk,2}$, respectively. Thus $f_{kn,1}$ and $f_{nk,2}$ are independent and identically distributed (i.i.d.) with zero-mean complex Gaussian random variables, i.e., $f_{kn,1},\ f_{nk,2} \sim \mathcal{CN}(0,\sigma_c^2)$ where σ_c^2 is the variance of the main channel. Denote the small-scale fading coefficient of the wiretap channel from S_k to E_1 and from R_n to E_2 as $g_{k,1}$ and $g_{n,2}$, respectively. Thus, they are i.i.d. $\mathcal{CN}(0,\sigma_e^2)$, where σ_e^2 is the variance of the wiretap channel. 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 R_n is denoted as h_n.

B. Transceiver Model and Secrecy Rate

Now we elaborate the protocol and transceiver models for the communications from S_k to D_k. This work focuses on RS where 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.

For the main channels, if relay R_n is chosen for the transmission from S_k to D_k, the transceiver equations of the two hops are $y_{n,1}[t] = \sqrt{\frac{p}{l_c^\eta}} f_{kn,1} s_k[t] + i_n[t] + n_{n,1}[t]$ and $y_{k,2}[t] = \sqrt{\frac{p}{l_c^\eta}} f_{nk,2} \hat{s}_n[t] + n_{k,2}[t]$, respectively, where $y_{n,1}$ and $y_{k,2}$ are the received signals at R_n and D_k, η is the path-loss exponent, $s_k[t]$ is the source S_k symbol, $\hat{s}_n$ is the decoded and forwarded information symbol from R_n, $n_{n,1}[t]$ and $n_{k,2}[t]$ are additive white Gaussian noise (AWGN) at R_n and D_k, respectively, with zero-mean and σ_0^2-variance, and $i_n[t]$ is the self-interference. With self-interference cancellation (SIC) technique at the R_n, i_n's can be model as i.i.d. complex Gaussian random variables which have similar effect as the noise following $\mathcal{CN}(0,\sigma_i^2)$ and $\sigma_i^2 = \omega p^\nu$ where the two constants, $\omega > 0$ and $\nu \in [0,1]$, depend on the SIC scheme used at R_n [12]. The assumption implies that RSI variances are constants and identical for all relays. The received signal-to-interference-plus-noise ratio (SINR) at R_n for the first hop and the signal-to-noise-ratio (SNR) at the destination D_k for the second hop can be given respectively as

$$\gamma_{kn,1} = \frac{x_{kn}}{1+1/\alpha} \text{ and } \gamma_{nk,2} = y_{nk}, \tag{1}$$

where $x_{kn} = \frac{p}{l_c^\eta \sigma_0^2}|f_{kn,1}|^2$, $y_{nk} = \frac{p}{l_c^\eta \sigma_0^2}|f_{nk,2}|^2$, and $\alpha = \sigma_0^2/\sigma_i^2$. Define $\lambda = (l_c^\eta \sigma_0^2)/(p\,\sigma_c^2)$. It is obviously that $x_{kn}, y_{nk} \sim \mathcal{E}xp(\lambda)$, where the notation $X \sim \mathcal{E}xp(a)$ means that X follows the exponential distribution with $a > 0$.

For the wiretap channels, the received signal at E_1 and E_2 are $y_{k,e1}[t] = \sqrt{p/l_e^\eta} g_{k,1} s_k[t] + n_{e1}[t]$ and $y_{n,e2}[t] = \sqrt{p/l_e^\eta} g_{n,2} \hat{s}_n[t] + n_{e2}[t]$, respectively, where $n_{e1}[t]$ and $n_{e2}[t]$ are the Gaussian noise at E_1 and E_2, respectively, which follow $\mathcal{CN}(0,\sigma_0^2)$. It is assumed that the eavesdroppers know the encoding and decoding schemes at the sources and the destinations. The received SNRs at E_1 and E_2, denoted as $\gamma_{k,e1}$ and $\gamma_{n,e2}$, are given by

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

Again, $\gamma_{k,e1}, \gamma_{n,e2} \sim \mathcal{E}xp(\beta)$ where $\beta = (l_e^\eta \sigma_0^2)(p\,\sigma_e^2)$.

According to [13], [14], the achievable secrecy rate of the k-th SD pair via R_n with colluding eavesdroppers is

$$c_{kn} = \left[\log_2\left(\frac{1+\min(\gamma_{kn,1},\gamma_{nk,2})}{1+\gamma_{e,kn}}\right)\right]^+, \tag{3}$$

where $[x]^+ = \max(x,0)$ and $\gamma_{e,kn} = \gamma_{k,e1} + \gamma_{n,e2}$. Considering all possible relay choices for all SD pairs, we have the secrecy rate matrix as

$$\mathbf{C} = (c_{kn}) \in \mathbb{R}^{K\times N}, \tag{4}$$

whose (k,n)-th element c_{kn} is the secrecy rate of communications for the k-th SD pair if R_n is selected for the pair.

C. RS Schemes Based on Max-Min Fairness

Since a relay cannot be shared by more than one pair of SD, once a relay is assigned to one SD pair, there are $(N-1)$ possible relays remaining for any next SD pair. Likewise, there are $(N-K+1)$ possible relays remaining for the last SD pair. A straightforward greedy scheme may result in significant performance degradation for the final SD pair compared to others. Thus, a sophisticated RS scheme was proposed in [10] and modified in [11], which maximizes the minimum received SINR and guarantees the uniqueness/optimality of the solution.

1) The ORS Scheme: By considering individual performance and fairness, we aim to maximize the minimum secrecy rate of all SD pairs. The RS matrix for ORS is defined as

$$\mathbf{\Gamma}_o = (\tilde{\gamma}_{kn}) \in \mathbb{R}^{K\times N} \text{ where } \tilde{\gamma}_{kn} = \frac{1+\min(\gamma_{kn,1},\gamma_{nk,2})}{1+\gamma_{e,kn}}.$$

Thus $c_{kn} = [\log\tilde{\gamma}_{kn}]^+$ and $\mathbf{C} = ([\log\tilde{\gamma}_{kn}]^+)$. As the log-function is monotonically increasing, 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. Then, we apply the RS algorithm in [11]. Due to space limitation, details are omitted here and is referred to [11].

2) The SRS Scheme: From the practical point of view, it is reasonable to assume that the relay selector does not have any knowledge of eavesdroppers' channels. Further it may have only partial knowledge (i.e., the statistics) of the self-interference channels. Based on this, we propose to use the following RS matrix $\mathbf{\Gamma}_s$ based on the partial CSI:

$$\mathbf{\Gamma}_s = (\gamma_{kn}) \in \mathbb{R}^{K\times N} \text{ where } \gamma_{kn} = \min(\rho\, x_{kn}, y_{nk}) \quad (5)$$

and $\rho = \frac{\alpha}{1+\alpha}$. The same algorithm can be conducted with the RS matrix $\mathbf{\Gamma}_o$, and it is referred to as the SRS scheme.

3) RS Examples: An example is provided to help illustrate the RS schemes. For notational convenience, we define the following matrices $\mathbf{H_s} \triangleq (x_{kn}) \in \mathbb{R}^{K\times N}$, $\mathbf{H_d} \triangleq (y_{nk}) \in \mathbb{R}^{N\times K}$, $\mathbf{H_{e1}} \triangleq (\gamma_{k,e1}) \in \mathbb{R}^{K\times 1}$, $\mathbf{H_{e2}} \triangleq (\gamma_{n,e2}) \in \mathbb{R}^{N\times 1}$. which help to generate $\mathbf{C}$, $\mathbf{\Gamma_s}$, and $\mathbf{\Gamma_s}$. Let us consider a network with three SD pairs ($K=3$) and three relays ($N=3$) with $\alpha = 1$. A random channel realization results in the following network parameters:

$$\mathbf{H_s}=\begin{bmatrix}17.11 & 9.81 & 6.64\\ 6.26 & 11.78 & 3.33\\ 3.07 & 4.88 & 14.62\end{bmatrix};\mathbf{H_d^T}=\begin{bmatrix}0.69 & 5.65 & 0.80\\ 16.03 & 6.41 & 1.80\\ 11.13 & 13.89 & 0.27\end{bmatrix};$$

$$\mathbf{H_{e1}^T}=\begin{bmatrix}0.22 & 0.80 & 0.84\end{bmatrix};\mathbf{H_{e2}^T}=\begin{bmatrix}0.23 & 0.03 & 0.11\end{bmatrix}.$$

The corresponding secrecy rate matrix and the RS matrices for the two RS schemes are

$$\mathbf{C} = \begin{bmatrix}0.22 & 2.24 & 0.43\\ 1.02 & 1.91 & 0.48\\ 0.30 & 0.88 & 0\end{bmatrix};$$

$$\mathbf{\Gamma_o} = \begin{bmatrix}1.16 & 4.72 & \overset{(0.43)}{\mathbf{1.35}}\\ \overset{(1.02)}{\mathbf{2.03}} & 3.77 & 1.39\\ 1.23 & \overset{(0.88)}{\mathbf{1.85}} & 0.65\end{bmatrix};\ \mathbf{\Gamma_s} = \begin{bmatrix}0.69 & \overset{(2.24)}{\mathbf{4.90}} & 0.80\\ 3.13 & 5.89 & \overset{(0.48)}{\mathbf{1.67}}\\ \overset{(0.30)}{\mathbf{1.54}} & 2.44 & 0.27\end{bmatrix}.$$

When we run the ORS and SRS algorithms based on $\mathbf{\Gamma}_o$ and $\mathbf{\Gamma}_s$ respectively, the RS results are indicated by the elements in bold font in the matrices, and the corresponding secrecy rates are given on top of the bolded elements. For ORS and SRS, the minimum rates are 0.43 and 0.30, respectively. However, if we use naive RS based on $\mathbf{\Gamma_s}$, R_2, R_1 and R_3 are chosen for the first, second and last SD pairs, respectively. The effective secrecy rates are 2.24, 1.02, and 0 respectively for the three SD pairs, and the last pair is intercepted, i.e., $c_{(3)} = 0$.

III. Performance Analysis of SRS

This section analyzes the interception probability and diversity order of the SRS scheme proposed in Section II-B.

A. Intercept Probability of SRS

Denote the secrecy rate for the k-th SD pair after the SRS scheme as $c_{(k)}$. An intercept event occurs when the secrecy rate is less than a predefined rate τ, which is in general a non-negative value. Thus the intercept probability of the k-th SD pair may be given as

$$P_k(\tau) = \Pr[c_{(k)} < \tau]. \quad (6)$$

Recall that the RS matrix for SRS $\mathbf{\Gamma_s}$ is generated as in (5). We now sort γ_{kn}'s which are elements of $\mathbf{\Gamma_s}$ in descending order, and map with their corresponding secrecy rates. Then, $\gamma^{(j)}$ is the j-th largest element of $\mathbf{\Gamma_s}$ and $c^{(j)}$ is the corresponding secrecy rate in $\mathbf{C}$. It is important to note that $c^{(j)}$ is not necessarily the j-th largest element of $\mathbf{C}$. Each $c^{(j)}$ corresponds to a SD pair and a selected relay. Without loss of generality, we write $\gamma_{\mathrm{m}}^{(j)}$ to denote the value $\min(\gamma_{kn,1},\gamma_{nk,2})$ corresponding to $c^{(j)}$ as per (3). To help understand the computation of $P_k(\tau)$, in the following, we recite the three crucial quantities: γ_{kn}'s are the elements of the RS matrix, $c^{(j)}$'s are the secrecy rates corresponding to the ordered $\gamma^{(j)}$'s, and $\gamma_{\mathrm{m}}^{(j)}$ is a key intermediate term in computing probabilities for $c^{(j)}$. According to the RS algorithm, any selected entry $\gamma^{(j)}$ satisfies the property $j \in \{1,\cdots,(K-1)N+1\}$. Thus, the secrecy rate of the k-th SD pair, c_k, is in the set $\{c^{(1)},\cdots,c^{((K-1)N+1)}\}$. Now, let $L = L_k$ be the random index of the relay selected for the k-th SD pair, $\gamma_{e,\cdot} = \gamma_{k,e1} + \gamma_{n,e2}$ be a random variable in (3), and independent of $(\gamma^{(j)})_{j=1}^{NK}$, and $Z = (2^\tau - 1) + 2^\tau\gamma_{e,\cdot}$ whose density is denoted as f_Z. Then, the intercept probability of the k-th SD pair in (6) can be written as

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

where (a) follows from the definition of conditional probability, (b) is because L is independent of the values $(\gamma^{(j)})_{j=1}^{NK}$

(L only depends on their positions within the matrix $\mathbf{\Gamma_s}$), (c) follows from the definition of $c^{(j)}$, (d) comes from simple rearrangement using the monotonicity of the logarithm, and (e) is the continuous law of total probability. To this end, we need to calculate $\mathrm{P}_{(j)}$ and $\mathcal{J}_{(j)}$, the latter of which depends on $F_{\gamma_{\mathrm{m}}^{(j)}}(z)$ and $f_Z(z)$. The term $\mathrm{P}_{(j)}$ represents the probability that the relay with the j-th largest entry of $\mathbf{\Gamma_s}$. Since only the relay ordering matters, $\mathrm{P}_{(j)}$ depends on the dimensions of $\mathbf{\Gamma_s}$ and j. For a network with two SD pairs, these probabilities can be calculated analytically as given in [15], [16]. For the general case, calculating $\mathrm{P}_{(j)}$ may be difficult, however, we can easily evaluate these by simulations.

By using the fact that the PDF of the summation of two i.i.d. random variables each following $\mathcal{E}xp(a)$ is a^2xe^{-ax}, we can derive the PDF for $Z = (2^\tau - 1) + 2^\tau \gamma_{e,\cdot}$ as

$$f_Z(z) = (\beta/2^\tau)^2 \, e^{\frac{\beta(2^\tau-1)}{2^\tau}} (z - (2^\tau - 1)) e^{-\frac{\beta}{2^\tau} z} \tag{8}$$

Now, we calculate $F_{\gamma_{\mathrm{m}}^{(j)}}(x)$ in (7). According to the secrecy rate given in (3), we have $\gamma_{\mathrm{m}}^{(j)} = \min\left(\frac{x_{\cdot\cdot}^{(j)}}{1+1/\alpha}, y_{\cdot\cdot}^{(j)}\right)$. where the $x_{\cdot\cdot}^{(j)}$ and $y_{\cdot\cdot}^{(j)}$ are the variables corresponding to the induced index of $\gamma^{(j)}$. For brevity, we drop subscript indices. We have

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

where the last equality follows a simple rearrangement to help the application of the RS criterion in (5). To this end, we need the following. For a given $\gamma^{(j)}$ which is the j-th largest entry of $\mathbf{\Gamma_s}$, we have based on the RS in (5):

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

where 'w.p.' stands for *with probability* and $y^{(j)}_{>\gamma^{(j)}}$ and $\rho\, x^{(j)}_{>\gamma^{(j)}}$ have the same distribution as y_{nk} and $\rho\, x_{kn}$, given that they are greater than $\gamma^{(j)}$, respectively. Since random variables $\rho\, x_{kn}$ and y_{nk} are independent and they have exponential distributions, the PDF of the j-th largest element of $\mathbf{\Gamma_s}$, $\gamma^{(j)}$, can be given as

$$f_{\gamma^{(j)}}(z) = \frac{\lambda_c (NK)! \sum_{q=0}^{NK-j} (-1)^q \binom{NK-j}{q}}{(j-1)!(NK-j)!} e^{-\lambda_c (j+q) z}. \tag{11}$$

Now, to compute the joint distribution (and then the minimum) of $(\rho\, x^{(j)}, y^{(j)})$ from (10), we need distributions for $y^{(j)}_{>\gamma^{(j)}}$ and $\rho\, x^{(j)}_{>\gamma^{(j)}}$, conditional on $\gamma^{(j)}$. For notational convenience, we define $\hat{y}^{(j)} \triangleq y^{(j)}_{>\gamma^{(j)}}$ and $\hat{x}^{(j)} \triangleq \rho\, x^{(j)}_{>\gamma^{(j)}}$. Then, the PDFs of $\hat{x}^{(j)}$ and $\hat{y}^{(j)}$ conditional on $\gamma^{(j)}$ are

$$\begin{aligned} f_{\hat{x}^{(j)}}(z|\gamma^{(j)}) &= \frac{f_{x_{kn}}\left(\frac{z}{\rho}\right)}{\int_{\gamma^{(j)}}^{\infty} f_{x_{kn}}\left(\frac{t}{\rho}\right) dt} = \frac{\lambda}{\rho} e^{-\frac{\lambda}{\rho}\left(z-\gamma^{(j)}\right)} \\ f_{\hat{y}^{(j)}}(z|\gamma^{(j)}) &= \lambda e^{-\lambda\left(z-\gamma^{(j)}\right)}, \end{aligned} \tag{12}$$

respectively. Then, we can re-write (9) as

$$\begin{aligned} F_{\gamma_{\mathrm{m}}^{(j)}}(z) = 1 &- p_1 \int_z^\infty \int_{\max\{t,z\}}^\infty f_{\hat{y}^{(j)}}(w|\gamma^{(j)} = t) f_{\gamma^{(j)}}(t) dw dt \\ &- p_2 \int_z^\infty \int_{\max\{t,z\}}^\infty f_{\hat{x}^{(j)}}(w|\gamma^{(j)} = t) f_{\gamma^{(j)}}(t) dw dt \\ = 1 &- \sum_{q=0}^{NK-j} \frac{NK!(-1)^q \binom{NK-j}{q}}{(j-1)!(NK-j)!} \frac{e^{-\lambda(j+q)\left(\frac{1}{\alpha}+2\right)z}}{(j+q)}, \end{aligned} \tag{13}$$

where the last equality is obtained by substituting from (10), (11) and (12), and solving the double integrations. Subsequently we can calculate $\mathcal{J}_{(j)}$ in (7) by using (8) as

$$\begin{aligned} \mathcal{J}_{(j)} = 1 &- \sum_{q=0}^{NK-j} \frac{(NK)!(-1)^q \binom{NK-j}{q}}{(j-1)!(NK-j)!(j+q)} \\ &\left(\frac{\beta}{2^\tau}\right)^2 \frac{\varphi_1\left(1, \left(\frac{1}{\alpha}+2\right)\lambda(j+q), \frac{\beta}{2^\tau}, 2^\tau - 1\right)}{e^{-\frac{\beta(2^\tau-1)}{2^\tau}} \left(\left(\frac{1}{\alpha}+2\right)\lambda(j+q) + \frac{\beta}{2^\tau}\right)}; \end{aligned} \tag{14}$$

where $\varphi_1(a,b,c,t) = \int_t^\infty a e^{-(b+c)x}\, dx = \frac{a e^{-t(b+c)}}{b+c}$. With the aid of (7) and (14), we can calculate the intercept probability of the SRS scheme.

B. Diversity Order for High MER and MIR

We analyze the diversity order when the main-to-eavesdropper ratio (MER) and main-to-interference ratio (MIR) are high [4]. By following the notation in Section II-B, 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,

$$\text{MIR} = \begin{cases} \frac{p}{l_c^\eta \omega}\sigma_c^2; & \nu = 0, \\ \frac{1}{l_c^\eta \omega}\sigma_c^2; & \nu = 1, \end{cases}, \text{ and MER} = \frac{l_e^\eta}{l_c^\eta \sigma_e^2}\sigma_c^2. \tag{15}$$

We define the diversity order as $\delta \triangleq -\lim_{\lambda \to 0} \frac{\log P_k(\tau)}{\log(1/\lambda)}$. For fixed α and β, the diversity order shows how fast the intercept probability decreases with respect to the average gain of the main channel for high MIR and MER.

Theorem 1: For each SD pair, the diversity order of SRS in the FD wiretap network is N.

Proof: From (7) and the $\mathcal{J}_{(j)}$ expression in (14), we have

$$\begin{aligned} P_k(\tau) = 1 &- \sum_{j=1}^{N(K-1)+1} \frac{(KN)!\left(\frac{\beta}{2^\tau}\right)^2 \mathrm{P}_{(j)}}{(j-1)!(KN-j)!} \\ &\sum_{q=0}^{KN-j} \frac{(-1)^q \binom{KN-j}{q} e^{-(2^\tau-1)\left(\frac{1}{\alpha}+2\right)(j+q)\lambda}}{(j+q)\left(\left(\frac{1}{\alpha}+2\right)(j+q)\lambda + \frac{\beta}{2^\tau}\right)^2}. \end{aligned} \tag{16}$$

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

$$\begin{aligned} P_k(\tau) = 1 - \sum_{i=0}^{\infty} \frac{f^{(i)}(0)\lambda^i}{i!} &\sum_{j=1}^{N(K-1)+1} \frac{(KN)!\left(\frac{\beta}{2^\tau}\right)^2 \mathrm{P}_{(j)}}{(j-1)!(KN-j)!} \\ &\underbrace{\sum_{q=0}^{KN-j} (-1)^q \binom{KN-j}{q} (j+q)^{i-1}}_{=\mathcal{K}(K,N,\alpha,\beta,\lambda,\tau,i)}, \end{aligned} \tag{17}$$

where $f^{(i)}(0) = \frac{\partial^i}{\partial y^i}\left[\frac{e^{-(2^\tau-1)\left(\frac{1}{\alpha}+2\right)y}}{\left(\left(\frac{1}{\alpha}+2\right)y+\frac{\beta}{2^\tau}\right)^2}\right]\Bigg|_{y=0}$. To analyze (17) when $i=0$, we need the binomial identity for integers $m \geq 0$ and $s \geq 1$: $\sum_{q=0}^{m} \frac{(-1)^q\binom{m}{q}}{(s+q)} = \frac{(s-1)!m!}{(s+m)!}$. Now,

$$\mathcal{K}(K,N,\alpha,\beta,\lambda,\tau,0) = f^{(0)}(0)\sum_{j=1}^{(K-1)N+1} \frac{(KN)!\left(\frac{\beta}{2^\tau}\right)^2 \mathrm{P}_{(j)}}{(j-1)!(KN-j)!} \sum_{q=0}^{KN-j} \frac{(-1)^q\binom{KN-j}{q}}{(j+q)} \overset{(a)}{=} 1, \tag{18}$$

where (a) follows from $f^{(0)}(0) = \frac{4^\tau}{\beta^2}$, $m = KN-j$ and $s = j$, and $\sum_{j=1}^{(K-1)N+1} \mathrm{P}_{(j)} = 1$. To further analyze (17), we use the binomial identity for integer $m \geq 0$:

$$\sum_{q=0}^{m} q^s(-1)^q\binom{m}{q} = \begin{cases} 0; & s = 0,1,\ldots,m-1, \\ (-1)^m m!; & s = m. \end{cases} \tag{19}$$

Now, for $i = t$ where $t \in \{1,\cdots,N-1\}$,

$$\mathcal{K}(K,N,\alpha,\beta,\lambda,\tau,t) = \frac{f^{(t)}(0)\lambda^t}{t!}{}^{N(K-1)+1} \sum_{j=1} (KN)!\mathrm{P}_{(j)} \frac{\sum_{q=0}^{KN-j}(-1)^q\binom{KN-j}{q}(j+q)^{t-1}}{\left(\frac{\beta}{2^\tau}\right)^{-2}(j-1)!(KN-j)!} \overset{(a)}{=} 0, \tag{20}$$

where (a) is obtained by expanding $(j+q)^{t-1}$ and applying (19) with $m = NK-j$. For $i = N$,

$$\mathcal{K}(K,N,\alpha,\beta,\lambda,\tau,N) \overset{(a)}{=} \frac{f^{(N)}(0)\lambda^N \mathrm{P}_{((K-1)N+1)}\left(\frac{\beta}{2^\tau}\right)^2}{N!((K-1)N)!(N-1)!} \sum_{q=0}^{N-1}(-1)^q\binom{N-1}{q}(KN)!((K-1)N+1+q)^{N-1}, \tag{21}$$

where (a) is obtained by expanding $(j+q)^{N-1}$ and applying (19) with $m = NK-j$. With the aid of (18), (20) and (21), we have

$$P_k(\tau) = \frac{f^{(N)}(0)\mathrm{P}_{((K-1)N+1)}(KN)!\left(\frac{\beta}{2^\tau}\right)^2}{N!((K-1)N)!(N-1)!} \sum_{q=0}^{N-1} \frac{(-1)^{q+1}\binom{N-1}{q}\lambda^N}{((K-1)N+1+q)^{-(N-1)}} + \mathcal{O}\left(\lambda^{N+1}\right), \tag{22}$$

which proves that the k-th SD pair achieves full diversity. ■

IV. Numerical Results and Discussion

This section presents numerical results to show the performance of the proposed RS schemes and validate the analysis. In the legend, we denote the k-th SD pair as Uk, e.g., one can read the legend, 'SRS-U1' as the 1-st SD pair performance for SRS scheme. In Fig. 2, we normalize parameters σ_0^2, p, l_c, l_e, and vary σ_c^2, σ_e^2, ω in order to get MER and MIR in range 0-22 dB when $\tau = 0$ and $\sigma_i^2 = \omega p$, i.e., $\nu = 1$. For $K = 2$ and $N = 3$, the intercept probabilities of ORS and SRS are simulated together with naive RS and random RS scheme for comparison. In random RS, the SD pairs randomly choose relays, without replacement. In naive RS, the 1st SD pair first selects the best path. Then, the 2nd SD pair selects its best path that does not conflict with the 1st SD pair. As such, the intercept probabilities of the 1st SD pair and the 2nd SD pair are different. For the SRS, ORS, and random RS schemes, both pairs have the same intercept probability, thus only the intercept probability of the 1st SD pair is shown to keep the figure less busy. 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 III-A. The derived intercept probability approximations for large MER and MIR are accurate, which confirms the validity of our analysis for diversity order in Section III-B. ii) While the ORS, SRS and naive RS (the 1st SD pair) schemes achieve the full diversity order of three, the naive scheme (the 2nd SD pair) achieves diversity order two and the random RS provides a diversity order of only one. This demonstrates the unfairness of the naive RS scheme. At MER = MIR =16 dB, ORS outperforms SRS by 1.8 dB, and naive RS (the 1st SD pair) outperforms SRS by 2.4 dB. However, SRS outperforms naive RS (the 2nd SD pair) and random RS by 5.1 dB and 12.6 dB, respectively, which are very significant improvements on the PHY security aspect.

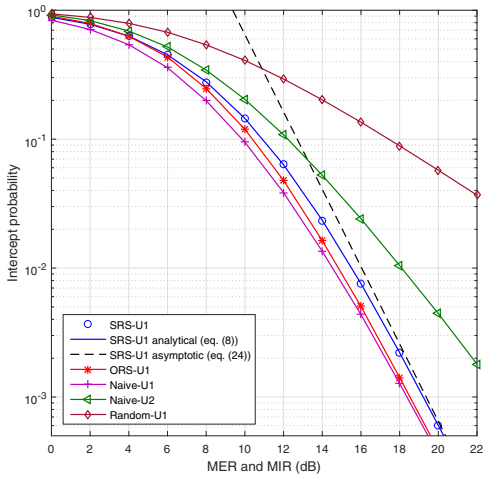

Fig. 2. Intercept probability for a relay network with $K = 2$ and $N = 3$.

In Fig. 3, we use more general settings, where the value of the path-loss is 140 dB for the first kilometer of each hop with path-loss exponent $\eta = 3$. We set $\tau = 0$, $\sigma_0^2 = 0.01$, $\omega = 0.01$, $\nu = 1$, $\sigma_c^2 = 1$, $\sigma_e^2 = 1$, $l_c = 500$ m, and $l_e = 2\,l_c$ m. The transmit power range is from 0 dBm to 20 dBm. We plot the intercept probability for the four cases: Case 1 - linearly increasing interference and wiretap channel gains; Case 2 - constant interference channel gain and linearly increasing wiretap channel gain; Case 3- linearly increasing interference channel gain and constant wiretap channel gain; and Case 4 - constant interference and wiretap channel gains. It can be seen that the first three cases have intercept probability floors for

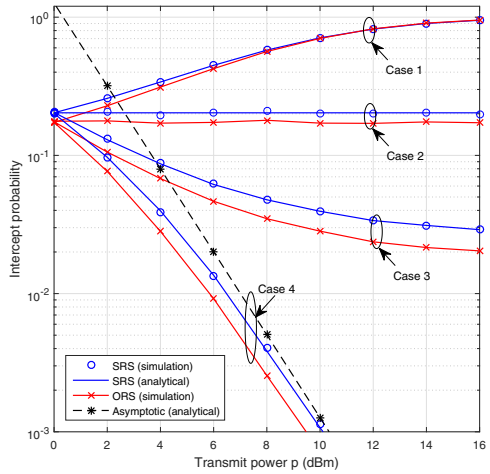

Fig. 3. Intercept probability for a relay network with $K = 2$ and $N = 3$.

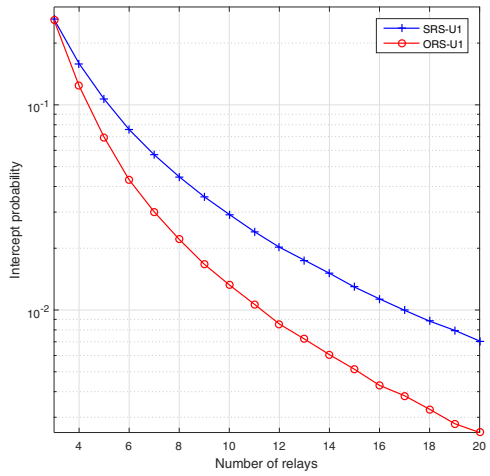

Fig. 4. Intercept probability for a network with $K = 3$.

both ORS and SRS, as self-interference and/or eavesdroppers SNR are proportional with p. Further, neither RS scheme can support securing user information unless we suppress the effective 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 $p = 10$ dBm. Fig. 4 plots the intercept probability versus the number of relays N when $l_c = 500$ m, $l_e = 1000$ m and $K = 3$. It shows that the ORS outperforms SRS. When the number of relays increases, intercept probability decreases dramatically. For example, 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.

V. Conclusion

This paper investigates the RS problem for an FD wireless network with multiple SD pairs, multiple DF relays, and two colluding eavesdroppers. To enhance the physical-layer security, two RS schemes, i.e., optimal RS (ORS) and suboptimal RS (SRS), are proposed based on global channel state information (CSI) and only SD pairs CSI, respectively. The exact intercept probability is derived for the SRS scheme which proves that it achieves full diversity when the gains of the main-to-eavesdropper and the main-to-interference channels increase asymptotically. Simulation results show that the proposed schemes provide user fairness in terms of secrecy rate compared with naive RS and random RS. Although the ORS outperforms SRS, the overhead cost for ORS also increases dramatically when the number of relays increases.

References

[1] 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 Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third 2014.

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

[3] S. Hong, J. Brand, J. I. Choi, M. Jain, J. Mehlman, S. Katti, and P. Levis, "Applications of self-interference cancellation in 5G and beyond," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 114–121, Feb. 2014.

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

[5] 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.

[6] 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.

[7] H. He, P. Ren, Q. Du, and L. Sun, "Full-duplex or half-duplex? hybrid relay selection for physical layer secrecy," in *Proc. IEEE Vehicular Technology Conf. (VTC)*, May 2016.

[8] 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.

[9] 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.

[10] 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. Networking*, vol. 19, no. 3, pp. 879–892, June 2010.

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

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

[13] 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.

[14] 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.

[15] R. Senanayake, S. Atapattu, P. L. Yeoh, and J. Evans, "Decentralized relay selection in two-user multihop decode-and-forward relay networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017.

[16] S. Atapattu, P. Dharmawansa, M. Di Renzo and J. Evans, "Relay selection in full-duplex multiple-user wireless networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017.