Optimal Relay Selection with a Full-duplex Active Eavesdropper in Cooperative Wireless Networks

He Zhou, Dongxuan He, Hua Wang, and Dewei Yang
Beijing Institute of Technology, China

***Abstract*—In this paper, we investigate the physical layer security of a dual-hop cooperative network in the presence of a full-duplex active eavesdropper, which can overhear the confidential signals and transmit jamming signals simultaneously. We utilize the optimal relay selection scheme to improve the secrecy performance, where the relay maximizing the secrecy capacity will be selected to forward the information. To evaluate the secrecy performance of our system, we derive a compact closed-form expression of the secrecy outage probability. Besides, we also analyze the asymptotic performance related to the position of the nodes. Finally, we verify our analysis through the numerical results, and demonstrate that there exists a secrecy protection region where the secrecy outage probability is below a target probability.**

I. Introduction

Due to the broadcast nature of wireless medium, communications in wireless networks are vulnerable to be attacked by eavesdroppers, leading to severe threat to information security. Thus, as an alternative to the conventional cryptography-based methods at the upper layers, physical layer security (PLS), which is based on information-theoretic security, is becoming an effective way to combat the illegal interception [1].

To improve the security of the wireless networks, cooperative transmission has been regarded as an effective method to improve the security of the system. With the help of the external node, the difference of the channel capacity between legitimate link and wiretap link can be increased, thus improving the secrecy performance of the wireless networks. Among all the external node aided schemes, relay selection [3]-[9] has been regarded as a promising method due to its lower complexity and high diversity gain [2,3]. In [4], optimal relay selection schemes without power constraints and direct links had been proposed in terms of decreasing the intercept probability. In [5] and [6], the authors considered the situation that the decode-and-forward (DF) relays were not always able to decode the messages, and the secrecy outage probability (SOP) had been explored, where multiple eavesdroppers can overhear the messages from both source and relays with maximal ratio combining (MRC) [5] or selection combining (SC) [6] technique.

In addition, the relay selection scheme has also been combined with other techniques [7]-[9]. In [7], the joint relay selection and cooperative jamming scheme was studied to maximize the secrecy rate, where the source cooperated with the destination in the first phase and the selected relay cooperated with the source in the second phase to confound the eavesdropper. The authors of [8] used the idea of nodes cooperation by hybrid cooperative beamforming and jamming scheme in order to protect the data transmissions during the two phases. Moreover, [9] proposed to select a pair of opportunistic relays, where one was selected as a relay to forward the information and the other worked as a friendly jammer.

On the other hand, full-duplex has been regarded as a novel technique [10,11], which can double the spectral efficiency by transmitting and receiving simultaneously. [10] studied a full-duplex receiver scheme where an optimal jamming covariance matrix that maximized the secrecy rate was designed. The impact of full-duplex relay on the secrecy performance was analyzed in [11], and a full-duplex relay jamming scheme was proposed to improve the secrecy.

The aforementioned works all considered the passive eavesdroppers, where the eavesdroppers only try to overhear the confidential information. However, there exist some active eavesdroppers in practice who can eavesdrop and jam simultaneously, which are called full-duplex eavesdroppers in some works [12]-[14]. And the secure transmission without external nodes against the active eavesdropper has been explored. For example, [12] studied how to utilize the artificial noise to enhance the security in the presence of an active eavesdropper. In [13], the authors proposed to use a Game-Theoretic framework and derived the optimal transmission and jamming strategy to obtain equilibrium for the game. Besides, [14] considered the secrecy issue under an active eavesdropper in the multiple-input-multiple-output (MIMO) system.

Motivated by these studies, in this paper, we explore the secrecy transmission in the cooperative networks in the presence of a full-duplex active eavesdropper. Here, the optimal relay that leads to the maximum secrecy capacity is selected to forward the information in our system. To evaluate the secrecy performance, the expression of secrecy outage probability is derived, as well as the asymptotic performance. We also utilize the numerical simulation to validate our analysis.

The remainder of this paper is organized as follows. In Section II, we describe the system model of the multi-relay cooperative network. In Section III, we provide the secrecy outage probability and the asymptotic analysis. In Section IV, we give the numerical results. Finally, Section V concludes the paper.

II. System Model

As shown in Fig. 1, we consider a cooperative wireless network consisting of one source S, one destination D, and

978-1-7281-1217-6/19/$31.00 ©2019 IEEE

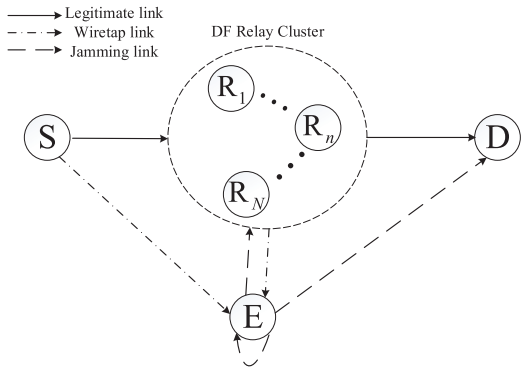

Fig. 1: System model of a multi-relay cooperative network under a full-duplex active eavesdropper.

N trusted DF relays R_n (n = 1,2, …,N) in the presence of an active eavesdropper E. We assume that the eavesdropper is a full-duplex node, which can perform eavesdropping and jamming simultaneously, and the source, destination, and relays all work in half-duplex mode with single antenna. We also assume that there is no direct link between S and D due to the deep fading and path-loss. Besides, we assume that all the relays are close together and have the same distance to other nodes.

It is assumed that all the channels in the system experience identical and independent distributed (i.i.d) Rayleigh fading together with a large-scale fading and the CSIs of all links are available. We denote $h_{ij}d_{ij}^{-\alpha/2}$ as the channel between the arbitrarily two nodes i and j, where h_{ij}, d_{ij} $(i \in (S, R_n, E), j \in (R_n, D, E))$ and α are the small-scale fading corresponding to a complex Gaussian random variable with zero mean and unit variance, the distance from node i to node j and the path-loss exponent, respectively. Due to the full-duplex characteristics, the eavesdropper remains a residual self-interference to itself, which can be modeled as link between the two antennas of E, denoted by $h_{EE} \sim \mathcal{CN}(0, 1)$. Moreover, $\rho \in (0, 1)$ is a linear coefficient after self-interference cancellation.

The transmission can be divided into two phases. The relays receive signal from the source in the first phase and then forward the received signal to the destination in the second phase. We assume the eavesdropper keeps eavesdropping and jamming during the two phases. Here, we define the transmit power of the source, the relays, and the eavesdropper as P_S, P_R, and P_E, respectively. As such, we express the received signal at node R_n and E in the first phase as

$$y_{R_n} = \sqrt{P_S} h_{SR_n} d_{SR_n}^{-\alpha/2} x_s + \sqrt{P_E} h_{ER_n} d_{ER_n}^{-\alpha/2} x_e + n_{R_n}, \quad (1)$$

$$y_{E,1} = \sqrt{P_S} h_{SE} d_{SE}^{-\alpha/2} x_s + \sqrt{\rho P_E} h_{EE} d_{EE}^{-\alpha/2} x_e + n_{E,1}, \quad (2)$$

where x_s and x_e are the information signal from the source and jamming signal from the eavesdropper, respectively. Here, we assume that $\mathbb{E}\left[|x_s|^2\right] = 1$ and $\mathbb{E}\left[|x_e|^2\right] = 1$. n_{R_n} and $n_{E,1}$ are AWGN at R_n and E in the first phase, respectively.

In the second phase, one relay is selected from the N relays to forward the information signal. To this end, we can formulate the received signal at node D and E in the second phase as

$$y_D = \sqrt{P_R} h_{R_n D} d_{R_n D}^{-\alpha/2} x_s + \sqrt{P_E} h_{ED} d_{ED}^{-\alpha/2} x_e + n_D, \quad (3)$$

$$y_{E,2} = \sqrt{P_R} h_{R_n E} d_{R_n E}^{-\alpha/2} x_s + \sqrt{\rho P_E} h_{EE} d_{EE}^{-\alpha/2} x_e + n_{E,2}, \quad (4)$$

where n_D and $n_{E,2}$ are AWGN at D and E in the second phase, respectively.

It is assumed that the noise received at any node has the same variance N_0. Consequently, from (1) and (2), the corresponding signal-to-interference-plus-noise ratio (SINR) at node R and E can respectively be expressed as

$$\gamma_{SR_n} = \frac{\gamma_S |h_{SR_n}|^2 d_{SR_n}^{-\alpha}}{\gamma_E |h_{ER_n}|^2 d_{ER_n}^{-\alpha} + 1}, \quad (5)$$

$$\gamma_{SE} = \frac{\gamma_S |h_{SE}|^2 d_{SE}^{-\alpha}}{\rho\gamma_E |h_{EE}|^2 d_{EE}^{-\alpha} + 1}, \quad (6)$$

where $\gamma_S = P_S/N_0$ and $\gamma_E = P_E/N_0$.

Similarly, according to (3) and (4), the obtained SINR at node D and E in the second phase can respectively be expressed as

$$\gamma_{R_n D} = \frac{\gamma_R |h_{R_n D}|^2 d_{R_n D}^{-\alpha}}{\gamma_E |h_{ED}|^2 d_{ED}^{-\alpha} + 1}, \quad (7)$$

$$\gamma_{R_n E} = \frac{\gamma_R |h_{R_n E}|^2 d_{R_n E}^{-\alpha}}{\rho\gamma_E |h_{EE}|^2 d_{EE}^{-\alpha} + 1}, \quad (8)$$

where $\gamma_R = P_R/N_0$.

In this work, we assume that the eavesdropper adopts the MRC [5] to decode the received signal. To this end, when the n-th relay is selected, the secrecy capacity can be formulated as

$$C_S(n) = \left[C_D(n) - C_E(n)\right]^+, \quad (9)$$

where $C_D(n) = \frac{1}{2}\log\left(1 + \min\left(\gamma_{SR_n}, \gamma_{R_n D}\right)\right)$, $C_E(n) = \frac{1}{2}\log\left(1 + \gamma_{SE} + \gamma_{R_n E}\right)$ are capacities of the legitimate link and the wiretap link when the n-th relay is selected to forward the information, respectively. And $[\cdot]^+ = \max(\cdot, 0)$.

III. Secrecy Performance Analysis

In this section, we quantify the system secrecy performance in terms of the secrecy outage probability (SOP). First, we derive the analytical expression of SOP in closed-form. Then, the asymptotic approximations will be derived, revealing the influence of node relative position intuitively. Specifically, we assume the relay that maximizes the secrecy capacity will be selected in the considered system. As such, we can express the relay selection scheme as

$$n^* = \arg \max_{n=1,\ldots,N} C_S(n). \quad (10)$$

A. Secrecy Outage Probability Analysis

Once $C_S(n^*) < R_s$, where R_s is a target secrecy transmission rate, the information can not be confidentially transmitted to D. As such, we define the secrecy outage probability as the probability that $C_S(n^*)$ is below R_s [15], which can be formulated as

$$\begin{aligned} P_{out} &= \Pr\left[C_S(n^*) < R_S\right] \\ &= \Pr\left[\arg \max_{n=1,\ldots,N} \left[\tfrac{1}{2}\log\left(\tfrac{1+min(\gamma_{SR_n},\gamma_{R_nD})}{1+\gamma_{SE}+\gamma_{R_nE}}\right)\right] < R_S\right]. \end{aligned} \tag{11}$$

For N independent relays are deployed in this system, we can further express the SOP as

$$\begin{aligned} P_{out} &= \prod_{n=1}^{N} \Pr\left[\frac{1+Z_1}{1+Z_2} < \gamma_{th}\right] \\ &= \prod_{n=1}^{N} \left(1 - \Pr\left[Z_2 < T(1+Z_1) - 1\right]\right) \\ &= \prod_{n=1}^{N} \left(1 - \underbrace{\int_0^{\infty} F_{Z_2}\left[T(1+x)-1\right] f_{Z_1}(x)dx}_{P}\right), \end{aligned} \tag{12}$$

where $r_{th} = 2^{2R_S}$, $T = 1/\gamma_{th}$, $Z_1 = min(\gamma_{SR_n}, \gamma_{R_nD})$ and $Z_2 = \gamma_{SE} + \gamma_{R_nE}$.

Since the channel is Rayleigh channel, we know that $|h_{ij}|^2$ (as well as $|h_{ij}|^2 d_{ij}^{-\alpha}$) follows exponential distribution. For the convenience of expression, we define $\sigma_{ij}^2 = d_{ij}^{-\alpha}$. As such, the cumulative distribution function (CDF) and probability density function (PDF) of $|h_{ij}|^2 d_{ij}^{-\alpha}$ can be respectively expressed as

$$F_{|h_{ij}|^2 d_{ij}^{-\alpha}}(x) = 1 - \exp(-\frac{x}{\sigma_{ij}^2}), \tag{13}$$

$$f_{|h_{ij}|^2 d_{ij}^{-\alpha}}(x) = \frac{1}{\sigma_{ij}^2}\exp(-\frac{x}{\sigma_{ij}^2}). \tag{14}$$

According to the above analysis, we can further obtain the PDF of variable Z_1 as

$$f_{Z_1}(x) = \frac{a_1 a_2}{a_2 - a_1}\left[\frac{a_3 x + a_1 a_3 + 1}{(x+a_1)^2} - \frac{a_3 x + a_2 a_3 + 1}{(x+a_2)^2}\right] \mathrm{e}^{-a_3 x}, \tag{15}$$

where $a_1 = \frac{\gamma_S \sigma_{SR_n}^2}{\gamma_E \sigma_{ER_n}^2}$, $a_2 = \frac{\gamma_R \sigma_{R_nD}^2}{\gamma_E \sigma_{ED}^2}$ and $a_3 = \frac{1}{\gamma_S \sigma_{SR_n}^2} + \frac{1}{\gamma_R \sigma_{R_nD}^2}$.

Proof: see Appendix. ∎

Meanwhile, from (6) and (8), the CDF of variable Z_2 can be expressed as

$$\begin{aligned} F_{Z_2}(x) &= \Pr\left(\frac{\omega_3 + \omega_4}{\omega_5} < x\right) \\ &= \Pr\left(\omega_3 < x\omega_5 - \omega_4\right) \\ &= \int_1^{\infty}\int_0^{x\omega_5} F_{\omega_3}\left(x\omega_5 - \omega_4\right) f_{\omega_4}\left(\omega_4\right) f_{\omega_5}\left(\omega_5\right) d\omega_4 d\omega_5, \end{aligned} \tag{16}$$

where $\omega_3 = \gamma_S |h_{SE}|^2 d_{SE}^{-\alpha}$, $\omega_4 = \gamma_R |h_{R_nE}|^2 d_{R_nE}^{-\alpha}$ and $\omega_5 = \rho\gamma_E |h_{EE}|^2 d_{EE}^{-\alpha} + 1$.

Substituting (13) and (14) into (16), we can re-express the CDF of Z_2 as

$$F_{Z_2}(x) = 1 - (b_1 - b_2)\frac{\exp(-b_3 x)}{x + b_1} - b_4 \frac{\exp(-b_6 x)}{x + b_5}, \tag{17}$$

with

$$\begin{cases} b_1 = \frac{\gamma_R \sigma_{RE}^2}{\rho\gamma_E \sigma_{EE}^2}, b_2 = \frac{\gamma_S \gamma_R \sigma_{SE}^2 \sigma_{RE}^2}{\rho\gamma_E \sigma_{EE}^2 (\gamma_S \sigma_{SE}^2 - \gamma_R \sigma_{RE}^2)} \\ b_3 = \frac{1}{\gamma_R \sigma_{RE}^2}, b_4 = \frac{(\gamma_S \sigma_{SE}^2)^2}{\rho\gamma_E \sigma_{EE}^2 (\gamma_S \sigma_{SE}^2 - \gamma_R \sigma_{RE}^2)} \\ b_5 = \frac{\gamma_S \sigma_{SE}^2}{\rho\gamma_E \sigma_{EE}^2}, b_6 = \frac{1}{\gamma_S \sigma_{SE}^2} \end{cases} \tag{18}$$

With the aid of the exponential integral function $\mathrm{Ei}(\cdot)$ [16, eq.(3.352.4),(3.353.3)], we can obtain the expression of P in (12) by substituting (15) and (17) into the P, which is now shown on the top of the next page. And the parameters in (19) can be expressed as follows

$$\begin{cases} c_1 = (T - 1 + b_1)/T\ ,\ c_2 = (T - 1 + b_5)/T \\ c_3 = a_3 + b_3 T\ \ ,\ \ c_4 = a_3 + b_6 T \\ d_1 = \frac{(b_1 - b_2)\exp(-b_3(T-1))}{T(c_1 - a_1)}, d_2 = \frac{(b_1 - b_2)\exp(-b_3(T-1))}{T(c_1 - a_2)} \\ d_3 = \frac{b_4 \exp(-b_6(T-1))}{T(c_2 - a_1)}\ \ \ \ , d_4 = \frac{b_4 \exp(-b_6(T-1))}{T(c_2 - a_2)} \end{cases} \tag{20}$$

Utilizing the above analysis, we can obtain a compact expression of the SOP as

$$P_{out} = \prod_{n=1}^{N}\left(1 - \mathrm{P}\right). \tag{21}$$

B. Asymptotic Analysis

In this subsection, we give out the asymptotic analysis of SOP, allowing us to observe the behavior of this metric intuitively.

Here, two asymptotic expressions, both of which are according to the distance relation, are discussing. Specifically, we first consider that either the destination or the source is closely located to the relays, and then we consider that the eavesdropper is close to the transmitters (either the source or the relays).

In the first case, we first assume the SNR of $R_n - D$ link is so high that $\sigma_{R_nD}^2 \to \infty$, due to the short distance between the relays and the destination. To this end, we can rewrite (21) as (22), which is shown on the top of the next page. To be noticed, this assumption implies the lower bound for the secrecy performance with fixed average SNR $\sigma_{SR_n}^2$. Next, we assume that $\sigma_{SR_n}^2 \to \infty$ for the situation that the distance between S and R_n is sufficiently short. As such, we set $\gamma_S \sigma_{SR_n}^2 = \gamma_R \sigma_{R_nD}^2$ and $a_1 = a_2$ in (22), which is observed tends to a constant value. The above analysis demonstrates that the quality of the $S - R_n$ link and that of the $R_n - D$ link have the similar impact on the secrecy performance.

In the second case, we first assume $\gamma_E \sigma_{SE}^2 \to \infty$ for the situation that the eavesdropper locates close to the source, causing the power of the received signal at the eavesdropper to

$$P = 1 + \frac{a_1 a_2}{a_2 - a_1}\{-d_1\left[\left(a_3 - \frac{1}{c_1 - a_1}\right)\exp(c_1 c_3)\mathrm{Ei}(-c_1 c_3) + (b_3 T + \frac{1}{c_1 - a_1})\exp(a_1 c_3)\mathrm{Ei}(-a_1 c_3) + \frac{1}{a_1}\right]$$
$$+d_2\left[\left(a_3 - \frac{1}{c_1 - a_2}\right)\exp(c_1 c_3)\mathrm{Ei}(-c_1 c_3) + (b_3 T + \frac{1}{c_1 - a_2})\exp(a_2 c_3)\mathrm{Ei}(-a_2 c_3) + \frac{1}{a_2}\right]$$
$$-d_3\left[\left(a_3 - \frac{1}{c_2 - a_1}\right)\exp(c_2 c_4)\mathrm{Ei}(-c_2 c_4) + (b_6 T + \frac{1}{c_2 - a_1})\exp(a_1 c_4)\mathrm{Ei}(-a_1 c_4) + \frac{1}{a_1}\right]$$
$$+d_4\left[\left(a_3 - \frac{1}{c_2 - a_2}\right)\exp(c_2 c_4)\mathrm{Ei}(-c_2 c_4) + (b_6 T + \frac{1}{c_2 - a_2})\exp(a_2 c_4)\mathrm{Ei}(-a_2 c_4) + \frac{1}{a_2}\right]\}. \quad (19)$$

$$P_{out} \simeq \prod_{n=1}^{N}\{a_1\{d_1\left[\left(\frac{1}{\gamma_S \sigma^2_{S R_n}} - \frac{1}{c_1 - a_1}\right)\exp(c_1 c_3)\mathrm{Ei}(-c_1 c_3) + (b_3 T + \frac{1}{c_1 - a_1})\exp(a_1 c_3)\mathrm{Ei}(-a_1 c_3) + \frac{1}{a_1}\right]$$
$$+d_3\left[\left(\frac{1}{\gamma_S \sigma^2_{S R_n}} - \frac{1}{c_2 - a_1}\right)\exp(c_2 c_4)\mathrm{Ei}(-c_2 c_4) + (b_6 T + \frac{1}{c_2 - a_1})\exp(a_1 c_4)\mathrm{Ei}(-a_1 c_4) + \frac{1}{a_1}\right]\}. \quad (22)$$

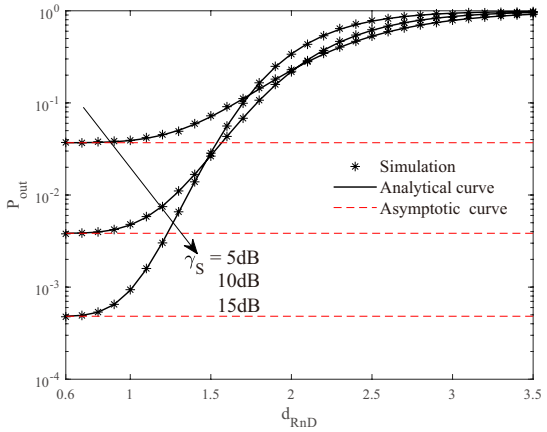

Fig. 2: P_{out} versus $d_{R_n D}$ for different values of γ_S with $\gamma_R = 20$ dB, $\gamma_E = 5$ dB, S (0, 0), R_n (0.5, 0), and E (-0.8, -1).

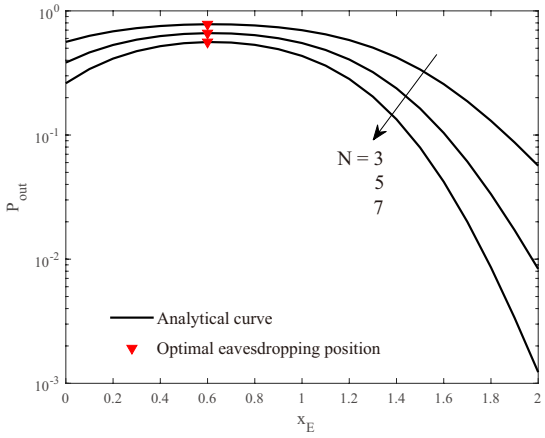

Fig. 3: P_{out} versus x_E for different values of N with $\gamma_S = 10$ dB, $\gamma_R = 20$ dB, $\gamma_E = 5$ dB, S (0, 0), R_n (0.7, 0), and D (1.2, 0.5).

be sufficiently high. Under this assumption, the SOP will be 1 without doubt. The similar conclusion can be drawn once the eavesdropper locates close to the relays. The above analysis indicates that it is crucial to establish a secrecy protection region to ensure the secure transmission.

IV. Numerical Results

In this section, we provide numerical results to validate our analysis. Specifically, we first detail the impact of the distance from the relays to the destination and the distance form the eavesdropper to the legitimate nodes, respectively. And then, we show the impact of the distribution of the eavesdropper on the secrecy outage probability. Throughout this section, we consider that $R_s = 0.1$ bits/s/Hz, $N = 3$, and $\rho = 0.01$. And we utilize the relative distance to represent the position relation, where the distance from the source to the relays is 1.

First, we show how the distance between R_n and D influences the secrecy outage probability in Fig. 2. We can see that the simulation points match with the analytical curve, which validates our derivation of the expression of the secrecy outage probability. We also observe that P_{out} increases as the increase of $d_{R_n D}$. When the distance tends to zero, P_{out} tends to a constant value which is determined by the quality of the channel between the source and the relays. And P_{out} tends to 1 when the distance is sufficiently large, this is because the relays can not forward the information to the destination successfully. Specifically, the short distance region corresponds to the high SNR regime, where $\sigma^2_{R_n D} \to \infty$. Here, we can see that the analytical curve and the asymptotic curve overlap, which demonstrates the effectiveness of our asymptotic analysis. In addition, we can find that P_{out} decreases drastically in the high SNR regime with the increase of γ_S, while it degrades slightly in the low SNR regime. This can be explained by the fact that the increasing transmit power enhances the wiretap link more than the legitimate link due to the large distance between R_n and D.

Then, we plot P_{out} versus x_E for different values of N in Fig. 3. To be noticed, the position of the eavesdropper here refers to the x-coordinate of the eavesdropper, where the y-coordinate of the eavesdropper always keeps to be -1. It is observed that we can improve the secrecy performance by increasing the number of the relays in this system. We can also see that P_{out} first increases and then decreases, and there exists an optimal eavesdropping position for the eavesdropper. To this end, we can evaluate the worst secrecy performance of our system by finding the optimal eavesdropping position.

Finally, we draw Fig. 4 to show how the P_{out} will be influenced by the position of the eavesdropper. We can see from this figure that once the eavesdropper is close to the

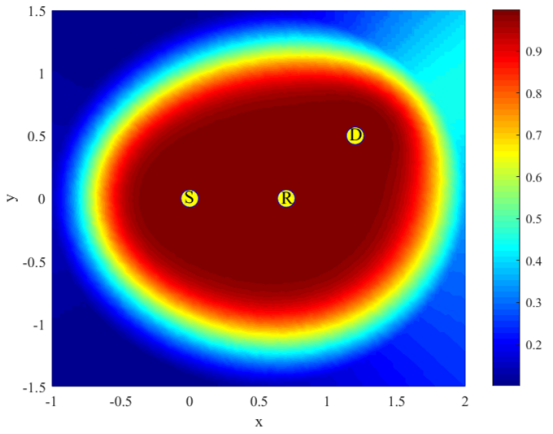

Fig. 4: P_{out} versus the position of E with $\gamma_S = 10$ dB, $\gamma_R = 20$ dB, $\gamma_E = 5$ dB, S (0, 0), R_n (0.7, 0), and D (1.2, 0.5).

legitimate nodes (including the source, the relays, and the destination), the secrecy outage probability will be sufficiently high. This demonstrates that there exists a secrecy protection region where P_{out} is below a target outage probability, and we can ensure the security by keeping the eavesdropper out of this region in our system. Besides, the positions of the legitimate nodes also influence the shape and scale of the secrecy protection region. As such, it will be significant to further design the deployment of the legitimate nodes, which will be investigated in the later works.

V. Conclusion

In this paper, we analyzed the secure transmission in the presence of a full-duplex active eavesdropper. To enhance the security, we considered the optimal relay selection scheme, where the relay corresponding to the maximum secrecy capacity is selected to forward the signal, is adopted in this system. To evaluate the secrecy performance, we derived the closed-form expression of the secrecy outage probability, as well as the asymptotic performance. Through our analysis, we found that there exists a secrecy protection region, where the secrecy performance will be ensured once we keep the eavesdropper out of this region. The simulation results validated our analysis and further demonstrated the existence of the secrecy protection region.

Appendix

Since $Z_1 = min\left(\gamma_{SR_n}, \gamma_{R_nD}\right)$, the CDF of Z_1 can be given by

$$\begin{aligned} F_{Z_1}(x) &= 1 - \Pr(\gamma_{SR_n} \geq x) \cdot \Pr(\gamma_{R_nD} \geq x) \\ &= 1 - (1 - F_{\gamma_{SR_n}}(x))(1 - F_{\gamma_{R_nD}}(x)). \end{aligned} \tag{23}$$

To derive the CDF of Z_1, we first rewrite the CDF of γ_{SR_n} by substituting (5) as

$$\begin{aligned} F_{\gamma_{SR_n}}(x) &= \Pr\left(\frac{\gamma_S |h_{SR_n}|^2 d_{SR_n}^{-\alpha}}{\gamma_E |h_{ER_n}|^2 d_{ER_n}^{-\alpha} + 1} < x\right) \\ &= \Pr(\omega_1 < x(\omega_2 + 1)) \\ &= \int_0^{\infty} F_{\omega_1}\left[x(\omega_2 + 1)\right] f_{\omega_2}(\omega_2) d\omega_2, \end{aligned} \tag{24}$$

where $\omega_1 = \gamma_S |h_{SR_n}|^2 d_{SR_n}^{-\alpha}$ and $\omega_2 = \gamma_E |h_{ER_n}|^2 d_{ER_n}^{-\alpha}$.

By substituting the CDF and PDF into (24) with (13) and (14), (24) can be calculated as

$$F_{\gamma_{SR_n}}(x) = 1 - \frac{\gamma_S \sigma_{SR_n}^2}{\gamma_S \sigma_{SR_n}^2 + \gamma_E \sigma_{ER_n}^2 x} \exp\left(-\frac{x}{\gamma_S \sigma_{SR_n}^2}\right). \tag{25}$$

Similarly, the CDF of γ_{R_nD} can be obtained in the same way. Next, we can derive the CDF of Z_1 as

$$F_{Z_1}(x) = 1 - \frac{a_1 a_2}{(x + a_1)(x + a_2)} \exp(-a_3 x). \tag{26}$$

Then, employing the derivative of $F_{Z_1}(x)$ in (26) with respect to x, we obtain the PDF of Z_1 as shown in (15).

Acknowledgement

This work was supported by the National Natural Science Foundation of China under Grant No. 61471037, No. 61771048, and No. 61201181.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[2] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[3] H. M. Wang and X. G. Xia, "Enhancing wireless secrecy via cooperation: signal design and optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 47–53, Dec. 2015.

[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] X. Lei, L. Fan, R. Q. Hu, and D. S. Michalopoulos, "Secure multiuser communications in multiple decode-and-forward relay networks with direct links," *in Proc. IEEE Globecom, Austin, USA*, Dec. 2014, pp. 3180–3185.

[6] J. Ding, Q. Yang, and J. Yang, "Secrecy outage probability of minimum relay selection in multiple eavesdroppers DF cognitive radio networks," *in Proc. IEEE VTC, Nanjing, China*, May. 2016, pp. 1–5.

[7] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[8] H. M. Wang, F. Liu, and M. Yang, "Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems," *IEEE Trans. Veh. Technol.*, vol. 64, no. 10, pp. 4893–4898, Oct. 2015.

[9] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay Selection for Security Enhancement in Cognitive Relay Networks," *IEEE Commun. Lett.*, vol. 4, no. 1, pp. 46–49, Feb. 2015.

[10] 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.

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

[12] C. Liu, J. Lee, and T. Q. S. Quek, "Secure Transmission in the Presence of Full-Duplex Active Eavesdropper," *in Proc. IEEE Globecom, Singapore, Singapore*, Dec. 2017.

[13] X. Tang, P. Ren, and Z. Han, "Power-Efficient Secure Transmission Against Full-Duplex Active Eavesdropper: A Game-Theoretic Framework," *IEEE Access*, vol. 5, pp. 24632–24645, Oct. 2017.

[14] L. Li, A. P. Petropulu, and Z. Chen, "MIMO Secret Communications Against an Active Eavesdropper," *IEEE Trans. Inf. Forensics and Security*, vol. 12, no. 10, pp. 2387–2401, Oct. 2017.

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

[16] I. S. Gradshteyn and I. M. Ryzhik, *Tabel of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic, 2007.