Relay Selection for Security Enhancement in Cognitive Relay Networks

Liu, Y., Wang, L., Duy, T. T., Elkashlan, M., & Duong, T. Q. (2015). Relay Selection for Security Enhancement in Cognitive Relay Networks. *IEEE Wireless Communications Letters*, *4*(1), 46-49. https://doi.org/10.1109/LWC.2014.2365808

Published in:
IEEE Wireless Communications Letters

Document Version:
Peer reviewed version

Relay Selection for Security Enhancement in Cognitive Relay Networks

Yuanwei Liu, Lifeng Wang, Tran Trung Duy, Maged Elkashlan, and Trung Q. Duong

***Abstract*—This letter proposes several relay selection policies for secure communication in cognitive decode-and-forward (DF) relay networks, where a pair of cognitive relays are opportunistically selected for security protection against eavesdropping. The first relay transmits the secrecy information to the destination, and the second relay, as a friendly jammer, transmits the jamming signal to confound the eavesdropper. We present new exact closed-form expressions for the secrecy outage probability. Our analysis and simulation results strongly support our conclusion that the proposed relay selection policies can enhance the performance of secure cognitive radio. We also confirm that the error floor phenomenon is created in the absence of jamming.**

***Index Terms*—Cognitive radio, cooperative networks, physical layer security**

I. Introduction

Cognitive radio networks are confronted with new privacy and security risks, due to the broadcast nature of wireless channels. Such security threats of eavesdropping are further escalated by the distributed nature of future multi-tier cognitive radio deployments. Physical (PHY) layer security, as an appealing approach to achieve secure transmission, has aroused wide-spread interest [1]. With this in mind, PHY layer security has been considered in cognitive radio networks [2]. Also, several recent efforts have considered PHY layer security in cooperative communications [3–8]. Among them [3] introduced cooperative transmission for security enhancement with single antenna and with multiple antennas. In [4], several cooperative relaying schemes were proposed to increase the secrecy rate, including decode-and-forward (DF), amplify-and-forward (AF), and cooperative jamming (CJ). In [5], collaborative relay weights for CJ were optimized to maximize the secrecy rate. In [6], two secrecy transmission schemes were proposed in opportunistic relaying. Joint relay and jammer selection for security enhancement was examined in one-way DF relay networks [7] and in two-way AF relay networks [8], where jamming was considered as a useful approach to resist security attacks.

Contrary to previous efforts, we focus on the security of cognitive relay networks where the transmit power of the cognitive relay is constrained. In this network, a pair of cognitive relays are selected. The first relay, as a helper, transmits the confidential messages to the legitimate destination, while the malicious eavesdropper tries to overhear the communication. The second relay, as a friendly jammer, transmits a jamming signal to corrupt the received signals at the eavesdropper. Our contributions are at least two-fold: 1) we propose and compare four relay selection policies, namely random relay and random jammer (RRRJ), random jammer and best relay (RJBR), best relay and best jammer (BRBJ), and best relay and no jammer (BRNJ); and 2) we characterize the joint impact of the proposed relay selection policies and the interference power constraint on the secrecy performance by deriving new exact closed-form expressions for the secrecy outage probability. We show that the proposed policies offer a secrecy performance/implementation trade-off. We also show that the absence of the jammer gives rise to the outage saturation phenomenon.

II. Network Model

We consider the secure communication in a cognitive relay network consisting of one secondary user (SU) source ($\mathtt{S}$), $M+1$ DF cognitive relays $\{\mathtt{R}_m\}$ ($m = 1, 2, \cdots, M+1$), one primary user (PU) receiver ($\mathtt{P}$), one SU destination ($\mathtt{D}$), and one eavesdropper ($\mathtt{E}$). All the nodes are equipped with a single antenna and operate in half-duplex mode. In such a network, the cognitive relays are allowed to share the same spectrum as the PU under interference power constraint. Because of the absence of the direct links, the signal transmitted by $\mathtt{S}$ cannot be received by the eavesdropper, hence the transmission during broadcast phase is secure. Assuming that the source and the relays are located in the same cluster, yielding high received SNRs at the DF relays for successful decoding of messages [7], we concentrate on the cooperative phase in the presence of eavesdropping[1]. A pair of relays are selected among $M+1$ relays, such that the first relay, denoted as $\mathtt{R}_c$, transmits the secrecy information; and the second relay, denoted as $\mathtt{R}_j$, transmits the jamming signal as a jammer. We consider the active eavesdropper scenario where the channel state information (CSI) between the relays and the eavesdropper is available[2] [4, 9]. Such a scenario is particularly applicable in multicast and unicast networks where the users play dual roles as legitimate receivers for some signals and eavesdroppers for others [4].

All the channels are subject to slow, flat, block Rayleigh fading, where the fading coefficients are constant during a codeword transmission. Let us denote $\gamma_m^{\mathtt{D}}$, $\gamma_m^{\mathtt{P}}$, and $\gamma_m^{\mathtt{E}}$ as the channel power gains of $\mathtt{R}_m \to \mathtt{D}$, $\mathtt{R}_m \to \mathtt{P}$, and $\mathtt{R}_m \to \mathtt{E}$ links, respectively. The channel power gains $\gamma_m^{\mathtt{D}}$, $\gamma_m^{\mathtt{P}}$, and

Y. Liu, L. Wang, and M. Elkashlan are with Queen Mary University of London, London, UK.

T. T. Duy is with Posts and Telecommunications Institute of Technology, Vietnam.

T. Q. Duong is with Queen's University Belfast, Belfast, UK.

[1]In DF relay networks, the transmission of the broadcast phase has little effect on our proposed schemes of the secure transmission in the cooperative phase.

[2]The CSI among all the nodes can be obtained at the SU source with the assistance of the relays.

$\gamma_m^{\mathtt{E}}$ are exponentially distributed random variables (RVs) with parameters $\lambda_{\mathtt{D}} = (d_{\mathtt{D}})^{\eta}$, $\lambda_{\mathtt{P}} = (d_{\mathtt{P}})^{\eta}$, and $\lambda_{\mathtt{E}} = (d_{\mathtt{E}})^{\eta}$, respectively, where $d_{\mathtt{D}}$, $d_{\mathtt{P}}$, and $d_{\mathtt{E}}$ denote the distance of $\mathtt{R}_m \to \mathtt{D}$, $\mathtt{R}_m \to \mathtt{P}$, and $\mathtt{R}_m \to \mathtt{E}$ links, respectively, and η represents the path-loss exponent.

In this underlay network, the SU terminals must limit their transmit powers so that the interference inflicted at the PU does not exceed the maximum allowable interference power limit $\mathtt{I}_{\mathtt{th}}$. To deal with this, the transmit powers at the relay $\mathtt{R}_c$ and the jammer $\mathtt{R}_j$ are given as

$$\mathtt{P}_c = \frac{\alpha \mathtt{I}_{\mathtt{th}}}{\gamma_c^{\mathtt{P}}} \qquad \text{and} \qquad \mathtt{P}_j = \frac{(1-\alpha)\mathtt{I}_{\mathtt{th}}}{\gamma_j^{\mathtt{P}}}, \tag{1}$$

respectively, where α is the power allocation factor, $0 < \alpha \leqslant 1$. Note that $\alpha = 1$ corresponds to no jamming. We assume that the interfering signal from the cooperative jammer $\mathtt{R}_j$ can be shared by the destination with specific method (e.g. use the seed of the random noise generator in a secure fashion [10]). This assumption helps us understand the performance limits and properties of cooperative jamming, and has been seen in prior works such as [10, 11]. After canceling the interference component, the instantaneous received SNR at the destination is given by

$$\Psi_{\mathtt{D}} = \frac{\mathtt{P}_c}{N_0}\gamma_c^{\mathtt{D}} = \frac{\alpha Q_{\mathtt{t}}}{\gamma_c^{\mathtt{P}}}\gamma_c^{\mathtt{D}} \,, \tag{2}$$

where N_0 is the noise power and $Q_{\mathtt{t}} = \mathtt{I}_{\mathtt{th}}/N_0$ is the transmit SNR of the network. Since the interfering signal is unknown at the eavesdropper, the instantaneous received signal-to-interference-plus-noise ratio (SINR) at the eavesdropper is given by

$$\Psi_{\mathtt{E}} = \frac{\mathtt{P}_c\gamma_c^{\mathtt{E}}}{N_0 + \mathtt{P}_j\gamma_j^{\mathtt{E}}} = \frac{\alpha Q_{\mathtt{t}}\gamma_c^{\mathtt{E}}}{\gamma_c^{\mathtt{P}}\left(1 + (1-\alpha)\, Q_{\mathtt{t}}\gamma_j^{\mathtt{E}}/\gamma_j^{\mathtt{P}}\right)} \,. \tag{3}$$

III. Secrecy Outage Probability

In this section, we focus on several relay selection policies with low implementation complexity. We consider constant secret rate applications that operate under short-term power constraints, typically found in device to device networks (i.e., ad hoc networks) and sensor networks. Such networks can suffer from outage despite CSI known at the transmitter. In this scenario, the secrecy outage probability is a meaningful metric to characterize the secrecy performance and has been considered in several prior works including the well-known [**?**]. Given the expected secrecy rate $\mathtt{R}_{\mathtt{th}}$, a secrecy outage is declared when the instantaneous secrecy rate drops below $\mathtt{R}_{\mathtt{th}}$. As such, we provide new closed-form expressions for the secrecy outage probability. These new results will enable us to examine and compare the benefits of the proposed policies. Based on (2) and (3), the secrecy rate is expressed as [7–9]

$$I = \left[\log_2(1+\Psi_{\mathtt{D}}) - \log_2(1+\Psi_{\mathtt{E}})\right]^{+} , \tag{4}$$

where $[x]^{+} = \max\{x, 0\}$. From (4), on the one hand, we find that increasing the instantaneous received SNR at the destination increases the secrecy rate. On the other hand, decreasing the instantaneous received SINR at the eavesdropper increases the secrecy rate. With this in mind, we propose and analyze four different relay selection policies in cognitive relay networks, namely random relay and random jammer (RRRJ), random jammer and best relay (RJBR), best relay and best jammer (BRBJ), and best relay and no jammer (BRNJ).

A. Random Relay and Random Jammer (RRRJ)

We first consider the RRRJ policy as a baseline for comparison purposes. In this case, the relay $\mathtt{R}_c$ and the jammer $\mathtt{R}_j$ are selected randomly. As such, the secrecy outage probability for RRRJ is formulated as

$$\begin{aligned} P_{\mathtt{RRRJ}}^{\mathtt{out}} &= \Pr\left(I_{\mathtt{RRRJ}} < R_{\mathtt{th}}\right) \\ &= \Pr\left(\frac{1 + \alpha Q_{\mathtt{t}}\gamma_c^{\mathtt{D}}/\gamma_c^{\mathtt{P}}}{1 + \frac{\alpha Q_{\mathtt{t}}\gamma_c^{\mathtt{E}}}{\gamma_c^{\mathtt{P}}\left(1+(1-\alpha)Q_{\mathtt{t}}\gamma_j^{\mathtt{E}}/\gamma_j^{\mathtt{P}}\right)}} < \rho\right) \,, \end{aligned} \tag{5}$$

where $R_{\mathtt{th}}$ is the expected secrecy rate and $\rho = 2^{R_{\mathtt{th}}}$.

Theorem 1: The secrecy outage probability for RRRJ is given by

$$\begin{aligned} P_{\mathtt{RRRJ}}^{\mathtt{out}} =& 1 - \frac{\omega_1\lambda_E\left(1-\omega_2\right)}{\lambda_{\mathtt{E}}\left(1-\omega_2\right) + \lambda_{\mathtt{D}}\rho} \\ & - \frac{\omega_1\lambda_{\mathtt{E}}\lambda_{\mathtt{D}}\omega_2\rho}{\left(\lambda_{\mathtt{E}}\left(1-\omega_2\right) + \lambda_{\mathtt{D}}\rho\right)^2} \ln\left(\frac{\lambda_{\mathtt{E}} + \lambda_{\mathtt{D}}\rho}{\lambda_{\mathtt{E}}\omega_2}\right) \,, \end{aligned} \tag{6}$$

where $\omega_1 = \lambda_{\mathtt{P}}\alpha Q_{\mathtt{t}}/\left(\lambda_{\mathtt{P}}\alpha Q_{\mathtt{t}} + \lambda_{\mathtt{D}}\left(\rho - 1\right)\right)$ and $\omega_2 = \lambda_{\mathtt{P}}\left(1-\alpha\right)Q_{\mathtt{t}}/\lambda_{\mathtt{E}}$.

Proof: See Appendix A. ∎

From (6), we see that the secrecy outage probability for RRRJ is independent of the number of relays.

B. Random Jammer and Best Relay (RJBR)

In this policy, we first select a random jammer $\mathtt{R}_j$. Without loss of the generality, we assume that the jammer is $\mathtt{R}_j = \mathtt{R}_{M+1}$. As such, the instantaneous secrecy rate at the relay $\mathtt{R}_m\,(m = 1, 2, \cdots, M)$ is calculated as

$$I_{\mathtt{RJBR}}^{m} = \log_2\left(\frac{1 + \alpha Q_{\mathtt{t}}\gamma_m^{\mathtt{D}}/\gamma_m^{\mathtt{P}}}{1 + \frac{\alpha Q_{\mathtt{t}}\gamma_m^{\mathtt{E}}}{\gamma_m^{\mathtt{P}}(1+Y_1)}}\right), \tag{7}$$

where $Y_1 = \left(1-\alpha\right)Q_{\mathtt{t}}\gamma_j^{\mathtt{E}}/\gamma_j^{\mathtt{P}}$. Then, the best relay $\mathtt{R}_c$ is selected to maximize the instantaneous secrecy rate as $R_c = \underset{m=1,2,\cdots,M}{\arg\max}\ I_{\mathtt{RJBR}}^{m}$. Therefore, the secrecy outage probability for RJBR is formulated as

$$P_{\mathtt{RJBR}}^{\mathtt{out}} = \Pr\left(\max_{m=1,2,\cdots,M}\left(\frac{1 + \alpha Q_{\mathtt{t}}\gamma_m^{\mathtt{D}}/\gamma_m^{\mathtt{P}}}{1 + \frac{\alpha Q_{\mathtt{t}}\gamma_m^{\mathtt{E}}}{\gamma_m^{\mathtt{P}}(1+Y_1)}}\right) < \rho\right) \,. \tag{8}$$

Theorem 2: The secrecy outage probability for RJBR is given by

$$\begin{aligned} P_{\mathtt{RJBR}}^{\mathtt{out}} =& \left(1-\omega_1\right)^M + \sum_{m=1}^{M}\binom{M}{m}\left(1-\omega_1\right)^{M-m}\omega_2(\omega_1(\omega_3-1))^m \\ & \times\left[a_1\ln\left(\frac{\omega_2}{\omega_3}\right) + \frac{a_2}{\omega_2} + \sum_{t=2}^{m}\frac{a_t}{\left(t-1\right)\left(\omega_3\right)^{t-1}}\right] \,, \end{aligned} \tag{9}$$

where $\omega_3 = 1 + \lambda_{\mathtt{D}}\rho/\lambda_{\mathtt{E}}$, $a_1 = \frac{m}{(\omega_3-\omega_2)^{m+1}}$, $a_2 = \frac{1}{(\omega_3-\omega_2)^m}$, and $a_t = \frac{m-t+1}{(\omega_3-\omega_2)^{m-t+2}}$.

Proof: See Appendix B. ∎

C. Best Relay and Best Jammer (BRBJ)

In this policy, we first select the best relay that maximizes the channel power gain between the relay and the destination. Without loss of generality, we assume that the best relay $\mathtt{R}_c$ is $\mathtt{R}_{M+1}$, i.e., $\gamma^{\mathtt{D}}_{M+1} = \max\limits_{m=1,2,\cdots,M+1}(\gamma^{\mathtt{D}}_m)$. Then, the best jammer $\mathtt{R}_j$ is selected among the remaining M relays to maximize the interference power at the eavesdropper, such that $R_j : \arg\max\limits_{m=1,2,\cdots,M}((1-\alpha)\,Q_{\mathtt{t}}\gamma^{\mathtt{E}}_m/\gamma^{\mathtt{P}}_m)$. In such a policy, the instantaneous secrecy rate is expressed as

$$I_{\mathtt{BRBJ}} = \log_2\left(\frac{1+\alpha Q_{\mathtt{t}}Y_2/\gamma^{\mathtt{P}}_{M+1}}{1+\frac{\alpha Q_{\mathtt{t}}\gamma^{\mathtt{E}}_{M+1}}{\gamma^{\mathtt{P}}_{M+1}(1+Y_3)}}\right), \tag{10}$$

where $Y_2 = \max\limits_{m=1,2,\cdots M+1}(\gamma^{\mathtt{D}}_m)$ and $Y_3 = \max\limits_{n=1,2,\cdots,M}((1-\alpha)\,Q_{\mathtt{t}}\gamma^{\mathtt{E}}_n/\gamma^{\mathtt{P}}_n)$ are statistically independent. The secrecy outage probability for BRBJ is formulated as

$$P^{\mathtt{out}}_{\mathtt{BRBJ}} = \Pr\left(Y_2 < \frac{\rho-1}{\alpha Q_{\mathtt{t}}}\gamma^{\mathtt{P}}_{M+1} + \rho\frac{\gamma^{\mathtt{E}}_{M+1}}{(1+Y_3)}\right). \tag{11}$$

Theorem 3: The secrecy outage probability for BRBJ is given in (12) at the top of next page, where $\vartheta = \frac{\lambda_{\mathtt{E}}(1-\omega_2)+m\lambda_{\mathtt{D}}\rho}{\lambda_{\mathtt{E}}+m\lambda_{\mathtt{D}}\rho}$ and ${}_2F_1(\cdot,\cdot;\cdot;\cdot)$ is the Gauss hypergeometric function [12, Eq. (9.142)].

Proof: The proof can be done in the similar way as the proof of Theorem 1. ■

D. Best Relay and No Jammer (BRNJ)

In this policy, no jamming protection is utilized. As such, the instantaneous secrecy rate at relay $\mathtt{R}_m$ $(m = 1, 2, \cdots, M+1)$ is calculated as

$$I^m_{\mathtt{BRNJ}} = \log_2\left(\frac{1+Q_{\mathtt{t}}\gamma^{\mathtt{D}}_m/\gamma^{\mathtt{P}}_m}{1+Q_{\mathtt{t}}\gamma^{\mathtt{E}}_m/\gamma^{\mathtt{P}}_m}\right). \tag{13}$$

The best relay $\mathtt{R}_c$ is selected so as to maximize the secrecy rate, such that $\mathtt{R}_c : \arg\max\limits_{m=1,2,\cdots,M+1} I^m_{\mathtt{BRNJ}}$. Therefore, the secrecy outage probability for BRNJ is derived as

$$\begin{aligned} P^{\mathtt{out}}_{\mathtt{BRNJ}} &= \Pr\left(\max_{m=1,2,\cdots,M+1}\left(\frac{1+Q_{\mathtt{t}}\gamma^{\mathtt{D}}_m/\gamma^{\mathtt{P}}_m}{1+Q_{\mathtt{t}}\gamma^{\mathtt{E}}_m/\gamma^{\mathtt{P}}_m}\right) < \rho\right) \\ &= \left(1 - \frac{\lambda_{\mathtt{E}}\lambda_{\mathtt{P}}Q_{\mathtt{t}}}{(\lambda_{\mathtt{E}}+\lambda_{\mathtt{D}}\rho)(\lambda_{\mathtt{P}}Q_{\mathtt{t}}+\lambda_{\mathtt{D}}(\rho-1))}\right)^{M+1}. \end{aligned} \tag{14}$$

IV. Numerical Results

Numerical results are presented to highlight the impact of relay selection on secure transmission of cognitive DF relay networks. The secrecy outage probability analytical curves for different relay selection policies are obtained from (6), (9), (12), and (14), respectively. In a two-dimensional topology, we assume that the co-ordinates of the relays (R), the destination (D), PU (P) and the eavesdropper (E), are $(x_{\mathtt{R}};0)$, $(1;0)$, $(x_{\mathtt{P}};y_{\mathtt{P}})$, and $(x_{\mathtt{E}};y_{\mathtt{E}})$, respectively. Hence, the distances are calculated as $d_{\mathtt{D}} = 1 - x_{\mathtt{R}}$, $d_{\mathtt{P}} = \sqrt{(x_{\mathtt{R}}-x_{\mathtt{P}})^2 + y^2_{\mathtt{P}}}$, and $d_{\mathtt{E}} = \sqrt{(x_{\mathtt{R}}-x_{\mathtt{E}})^2 + y^2_{\mathtt{E}}}$. In the simulations, we assume the path-loss exponent $\eta = 3$.

Fig. 1 plots the secrecy outage probability versus $Q_{\mathtt{t}}$ for $M = 2$. We assume that there are 3 relays ($M+1 = 3$). We place the relays, PU, and eavesdropper at positions $\{x_{\mathtt{R}};0\} = \{0.5;0\}$, $\{x_{\mathtt{P}};y_{\mathtt{P}}\} = \{0.5;-0.5\}$, and $\{x_{\mathtt{E}};y_{\mathtt{E}}\} = \{0.75;0.6\}$, respectively. We see that there is an error floor for BRNJ without jammer. This discouraging phenomenon is avoided by using jamming protection for RRRJ, RJBR, and BRBJ. We also see that BRBJ enhances the secrecy performance and achieves the lowest secrecy outage probability among the four proposed policies, however, it demands more instantaneous feedbacks and system overhead.

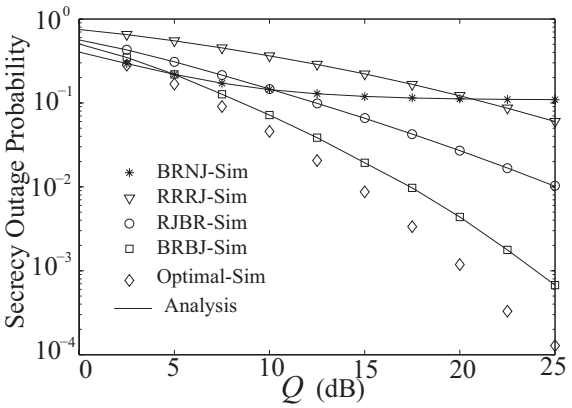

Fig. 1. Secrecy outage probability with $M = 2$, $R_{\mathtt{th}} = 1$, and $\alpha = 0.75$.

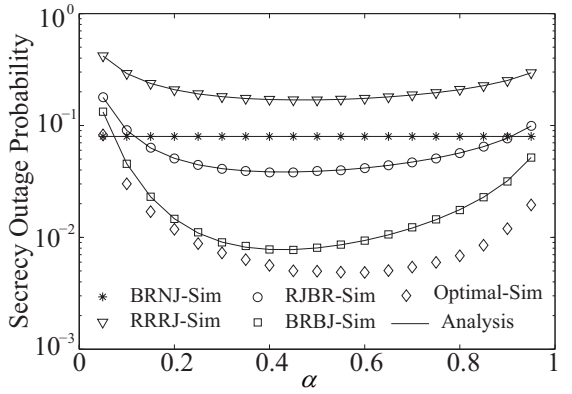

Fig. 2. Secrecy outage probability with $M = 2$, $R_{\mathtt{th}} = 0.75$, and $Q_{\mathtt{t}} = 5$ dB.

Fig. 2 plots the secrecy outage probability versus α for different relay selection policies. We place the relays, PU and the eavesdropper at the positions $\{x_{\mathtt{R}};0\} = \{0.5;0\}$, $\{x_{\mathtt{P}};y_{\mathtt{P}}\} = \{0.5;-0.5\}$, $\{x_{\mathtt{E}};y_{\mathtt{E}}\} = \{1;0.5\}$, respectively. We see that different power allocations have a direct impact on the secrecy outage probability except BRNJ (no jammer with $\alpha = 1$). For a given α, BRBJ offers the lowest secrecy outage probability among the four proposed policies. In addition, RJBR outperforms RRRJ. We also see that the optimal α lies in the medium region of (0,1]. This is due to the fact that a certain amount of energy needs to be allocated to the relay to deliver the source messages, and the remainder is allocated to the jammer to improve the security.

In Fig. 1 and Fig. 2, we also provide Monte Carlo simulations of the optimal relay selection policy which jointly selects the best relay and the best jammer to maximize the

$$P_{\mathtt{BRBJ}}^{\mathtt{out}}=\sum_{m=0}^{M+1}(-1)^m\binom{M+1}{m}\frac{\lambda_{\mathtt{P}}\alpha Q_{\mathtt{t}}}{\lambda_{\mathtt{P}}\alpha Q_{\mathtt{t}}+m\lambda_{\mathtt{D}}(\rho-1)}\sum_{n=1}^{M}\binom{M}{n}(\omega_2)^n\Bigg[\left(\frac{\lambda_{\mathtt{E}}}{\lambda_{\mathtt{E}}+m\lambda_{\mathtt{D}}\rho}\right)^n\Bigg[{}_2F_1\Big(1,n;n+1;\vartheta\Big)-\frac{n}{n+1}\frac{\lambda_{\mathtt{E}}(1-\omega_2)}{\lambda_{\mathtt{E}}+m\lambda_{\mathtt{D}}\rho}{}_2F_1\Big(1,n+1;n+2;\vartheta\Big)-1\Bigg]-\frac{(-1)^n\lambda_{\mathtt{E}}}{(\lambda_{\mathtt{E}}+m\lambda_{\mathtt{D}}\rho)(\omega_2)^n}+\sum_{k=1}^{n-1}\frac{(-1)^{k+n}k!}{\prod_{p=0}^{k}(n-p)}\frac{mn\lambda_{\mathtt{D}}\rho(\lambda_{\mathtt{E}})^k}{(\omega_2)^{n-k}(\lambda_{\mathtt{E}}+m\lambda_{\mathtt{D}}\rho)^{k+1}}\Bigg], \quad (12)$$

secrecy rate. From the simulation results, we see that optimal relay selection achieves the lowest secrecy outage probability. However, to the best of our knowledge, the analytical result of this policy is mathematically intractable, therefore we leave this policy for further investigation.

V. Conclusion

We considered relay and jammer selection in cognitive decode-and-forward (DF) relay networks with security constraints. We proposed four relay selection policies. Based on these policies, we derived new closed-form expressions for secrecy outage probability. The performance behavior of the proposed relay selection policies are showcased. Further study may consider other relay selection policies including the optimal relay selection policy which jointly selects the best relay and the best jammer to maximize the secrecy rate.

Appendix A: Proof of Theorem 1

Let $Z=\gamma_c^{\mathtt{E}}/(1+Y_1)$ with $Y_1=(1-\alpha)Q_{\mathtt{t}}\gamma_j^{\mathtt{E}}/\gamma_j^{\mathtt{P}}$, we rewrite (5) as

$$P_{\mathtt{RRRJ}}^{\mathtt{out}}=\int_0^\infty\int_0^\infty F_{\gamma_c^{\mathtt{D}}}\left(\frac{\rho-1}{\alpha Q_{\mathtt{t}}}x+\rho z\right)f_{\gamma_c^{\mathtt{P}}}(x)\,f_Z(z)\,dxdz\ . \quad (A.1)$$

Here, $f_Z(z)$ is the PDF of Z, we remind that the cumulative density function (CDF) and probability density function (PDF) of the random variables (RVs) γ_m^X, $X\in\{\mathtt{D},\mathtt{P},\mathtt{E}\}$ are $F_{\gamma_m^X}(x)=1-e^{-\lambda_X x}$ and $f_{\gamma_m^X}(x)=\lambda_X e^{-\lambda_X x}$, respectively. By substituting the CDF $F_{\gamma_c^{\mathtt{D}}}(x)$ and PDF $f_{\gamma_c^{\mathtt{P}}}(x)$ into (A.1), after some manipulations, (A.1) is given by

$$P_{\mathtt{RRRJ}}^{\mathtt{out}}=\int_0^\infty\left(1-\omega_1 e^{-\lambda_{\mathtt{D}}\rho z}\right)f_Z(z)\,dz\ , \quad (A.2)$$

where $\omega_1=\lambda_{\mathtt{P}}\alpha Q_{\mathtt{t}}/(\lambda_{\mathtt{P}}\alpha Q_{\mathtt{t}}+\lambda_{\mathtt{D}}(\rho-1))$. To obtain $f_Z(z)$, we first calculate the CDF of Y_1 as $F_{Y_1}(y)=1-\frac{\omega_2}{y+\omega_2}$ with $\omega_2=\lambda_{\mathtt{P}}(1-\alpha)Q_{\mathtt{t}}/\lambda_{\mathtt{E}}$. Taking the derivative of $F_{Y_1}(y)$ with respect to (w.r.t.) y, we obtain the PDF of Y_1 as

$$f_{Y_1}(y)=\frac{\omega_2}{(y+\omega_2)^2}. \quad (A.3)$$

Then, the CDF of Z can be formulated as

$$F_Z(z)=\int_0^\infty\left(1-e^{-\lambda_{\mathtt{E}}(z+zy)}\right)f_{Y_1}(y)\,dy\ . \quad (A.4)$$

By substituting (A.3) into (A.4), the CDF of Z is derived as

$$F_Z(z)=1-e^{-\lambda_{\mathtt{E}}z}+\lambda_{\mathtt{E}}\omega_2 z e^{-\lambda_{\mathtt{E}}(1-\omega_2)z}E_1(\lambda_{\mathtt{E}}\omega_2 z)\,, \quad (A.5)$$

where $E_1(x)$ is the exponential integral function given by $E_1(x)=\int_1^\infty e^{-xt}t^{-1}dt$ [12]. Taking the derivative of $F_Z(z)$ given in (A.5) w.r.t. z, we obtain the PDF of Z. Then substituting the PDF of Z into (A.2) and using [12, Eq. (6.227.1)], we obtain the desired result in (6).

Appendix B: Proof of Theorem 2

Based on (8), we first calculate the secrecy outage probability conditioned on Y_1 as

$$P_{\mathtt{RJBR}}^{\mathtt{out}}(Y_1)=\prod_{m=1}^{M}\Pr\left(\gamma_m^{\mathtt{D}}<\frac{\gamma_m^{\mathtt{P}}}{\alpha Q_{\mathtt{t}}}(\rho-1)+\frac{\gamma_m^{\mathtt{E}}\rho}{1+Y_1}\right)$$
$$=(1-\omega_1)^M+\sum_{m=1}^{M}\binom{M}{m}(1-\omega_1)^{M-m}\frac{(\omega_1(\omega_3-1))^m}{(Y_1+\omega_3)^m}\ . \quad (B.1)$$

The $P_{\mathtt{RJBR}}^{\mathtt{out}}$ is derived as

$$P_{\mathtt{RJBR}}^{\mathtt{out}}=\int_0^\infty f_{Y_1}(y)\,P_{\mathtt{RJBR}}^{\mathtt{out}}(y)\,dy\ . \quad (B.2)$$

Substituting (A.3) and (B.1) into (B.2), we get the desired result in (9).

References

[1] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas–part I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[2] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[3] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359–368, Feb. 2012.

[4] 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.

[5] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[6] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1725–1729, June 2011.

[7] I. Krikidis, J. 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.

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

[9] 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, June 2008.

[10] 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, July 2013.

[11] R. Zhang, L. Song, Z. Han, B. Jiao, and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in *Proc. Global Telecommun. Conf. (GLOBECOM)*, Miami, USA, 2010, pp. 1–6.

[12] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 6th ed. New York, NY, USA: Academic Press, 2000.