Intercept Outage Probability Analysis of Cognitive Relay Networks in Presence of Eavesdropping Attack

Jing Yang*†, Lei Chen*, Jie Ding*, Xuelong Hu*
* School of Information Engineering
Yangzhou University, China
{E-mails: jingyang@yzu.edu.cn, leichen092@163.com,
coolanding@hotmail.com, xlhu@yzu.edu.cn}
† School of Information Science and Engineering
Southeast University, China

P. Takis Mathiopoulos
Department of Informatics and Telecommunications
National and Kapodistrian University of Athens
15784 Athens, GREECE
mathio@di.uoa.gr

***Abstract*—In this paper, we study the physical-layer security of amplify-and-forward relaying networks under a spectrum-sharing mechanism over independent non-identically distributed Rayleigh fading channels. Relay selection is presented to select the best relay, which can guarantee the security performance by minimizing the received signal-to-noise ratio at the eavesdropper. In order to guarantee the quality-of-service of primary networks, both the maximum tolerable peak interference power at the primary users and maximum allowable transmit power at secondary users are considered. Closed-form lower and upper bounds as well as asymptotic expressions for the intercept outage probability (OP) are derived. From the asymptotic expressions, it can be observed that the diversity order of intercept OP equals to two. Our analysis results are validated by Monte-Carlo simulation.**

***Keywords*—Intercept outage probability; amplify-and-forward; cognitive radio network; relay selection**

I. Introduction

In future wireless communication systems, cognitive radio with spectrum sharing has been regarded as a promising technique to improve spectral efficiency and solve the problem of spectrum scarcity [1]. Data security transmission in cognitive radio networks (CRNs) is mainly a sever problem, due to the open and dynamic nature of CRNs where various unknown wireless devices are allowed to opportunistically access the licensed spectrum, which makes cognitive radio systems vulnerable to eavesdropping attacks [2]. In order to prevent the wiretap and improve the security performance, physical layer security has attracted intense interest to secure data transmission without the need for complex cryptographic protocols.

In 1975, Wyner firstly proposed the wiretap model and investigated the secrecy rate [3], which has become a cornerstone in the field of the physical security research. Recently, research efforts have been devoted to exploiting the characteristics of wireless channels to provide secure data transmission [4]–[11]. In cooperative relaying communication utilizing decode-and-forward (DF) and amplify-and-forward (AF) protocols, the secrecy capacity, secrecy outage probability (OP) and relay selection scheme have been studied in [4], [6]–[8]. While in these works, the system models are normally assumed as the cooperative wireless networks [4]–[8], [10], without taking account into cognitive radio technology.

Recently, considerable research efforts have been devoted to the physical layer security in CRNs [12]–[16]. The authors in [12], [13] investigated the secret communication through cognitive relay assisted interference channels in the presence of an eavesdropper. For multi-relay cognitive DF relaying networks, [14] proposed a relay selection scheme which selected the best relay by maximizing the achievable secrecy rate without harming the primary user. For a CRN that consists of one cognitive base station and multiple cognitive users in the presence of multiple eavesdroppers, [15] proposed a user scheduling scheme to achieve multiuser diversity and improve system security. For multiple-input multiple-output CRN, [16] studied secrecy OP of the considered system.

In this paper, we investigate the security performance of multi-relay AF cognitive relaying networks in the presence of eavesdropping attacks which has not explored in the open technical literature. Differing from the relay selection criterion by maximizing the achievable secrecy rate in [14] where multi-relay cognitive DF relaying networks is considered, we here consider multi-relay cognitive AF relaying networks and the best relay node among K candidates is selected to guarantee the security performance by minimizing the received signal-to-noise ratio (SNR) at the eavesdropper. Specifically, we study intercept OP for the considered system over independent non-identically distributed (i.n.i.d.) Rayleigh fading channels. Closed-form lower and upper bounds for the intercept OP are presented which are quite tight at high SNRs. In order to provide further insights, asymptotic analysis for the intercept OP are also derived. Finally, simulation is presented to verify the correctness of our analysis.

The remainder of this paper is organized as follows. In Section II, system model and relay selection scheme are

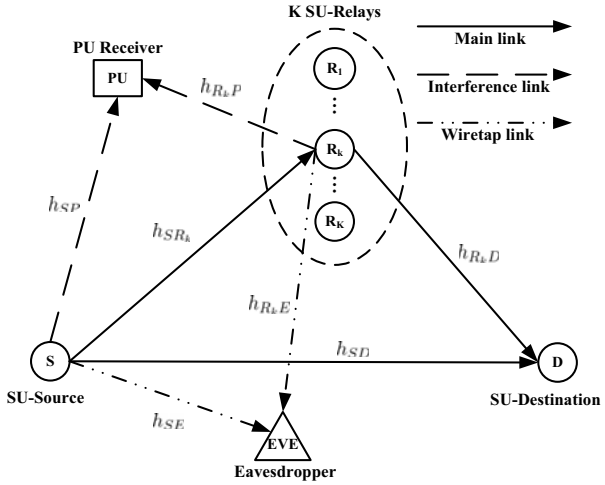

Fig. 1. System model.

presented. In Section III, closed-form lower and upper bounds as well as high-SNRs asymptotic expressions for the intercept OP are derived. Section IV presents various performance evaluation results and their interpretations. Finally, Section V concludes this paper.

II. System Model and Relay Selection Scheme

Consider a dual-hop cognitive AF relaying network including one secondary-user (SU) source S, K SU relays R_k $(k = 1, 2, \ldots, K)$, one SU destination D, one primary-user (PU) receiver and one eavesdropper EVE, as shown in Fig. 1. It is assumed that the eavesdropper intercepts the cognitive transmissions from S to R_k and D, from R_k to D, where all nodes are equipped with single antenna and operate in half-duplex mode. The channel coefficients h_{MT} experience i.n.i.d. Rayleigh fading, with M and T denoting two arbitrary nodes and all the noise components are additive white Gaussian noise (AWGN) with zero mean and variance N_0. In order to ensure the QoS provision at PU, i.e., total accumulated interference at PU cannot exceed the maximum tolerable interference power $\mathcal{Q}$. Let P_S and P_{R_k} be the maximum transmit power at S and R_k, respectively. Thus, the transmit powers at S and R_k are strictly governed by

$$\overline{P_S} = \min\left(\mathcal{Q}/|h_{SP}|^2, P_S\right),$$

and

$$\overline{P_{R_k}} = \min\left(\mathcal{Q}/|h_{R_kP}|^2, P_{R_k}\right),$$

respectively. In order to improve the physical-layer security, relay selection is presented to select the best relay node R_{k^*} which can minimize the end-to-end SNR at the eavesdropper EVE. Assume R_k is selected to help communication. The communication from S to D is performed into two times slots. During the first time slot, S transmits its information to R_k and D, while simultaneously the EVE intercepts the information. During the second time slot, R_k amplifies its received signal in the first time slot and forwards it to D, while the EVE also can wiretap the signal transmitted from R_k. Based upon this procedure, the received SNR from the relaying transmission at EVE, i.e., γ_{SR_kE}, can be expressed as

$$\gamma_{SR_kE} = \frac{\gamma_{SR_k}\gamma_{R_kE}}{\gamma_{SR_k} + \gamma_{R_kE} + 1}, \tag{1}$$

where

$$\gamma_{SR_k} = \min\left(\mathcal{Q}/|h_{SP}|^2, P_S\right)\frac{d_{SR_k}^{-\rho}|h_{SR_k}|^2}{N_0},$$
$$\gamma_{R_kE} = \min\left(\mathcal{Q}/|h_{R_kP}|^2, P_{R_k}\right)\frac{d_{R_kE}^{-\rho}|h_{R_kE}|^2}{N_0},$$

and d_{MT} is the distance between two arbitrary nodes M and T, ρ represents the path loss coefficient.

The best relay, i.e., R_{k^*}, is selected based on the following criterion

$$k^* = \arg\min_{k\in K}\left\{\gamma_{SR_kE}\right\}, \tag{2}$$

Assuming MRC strategy is employed by the eavesdropper EVE. Therefore, the received SNR at EVE can be given as

$$\gamma_E = \min_{k\in K}\left\{\frac{\gamma_{SR_k}\gamma_{R_kE}}{\gamma_{SR_k} + \gamma_{R_kE} + 1}\right\} + \gamma_{SE}, \tag{3}$$

where $\gamma_{SE} = \min\left(\mathcal{Q}/|h_{SP}|^2, P_S\right)\frac{|h_{SE}|^2}{N_0}$.

III. Intercept Outage Probability Analysis

In this section, the intercept OP of cognitive AF relaying system over i.n.i.d. Rayleigh fading channels after selecting the best relay, i.e., R_{k^*}, will be presented. The intercept OP $P_{\text{iout}}(\gamma_{\text{th}})$, is defined as the probability that the end-to-end SNR γ_E at the eavesdropper EVE falls below a specified SNR threshold γ_{th}, i.e.,

$$P_{\text{iout}}(\gamma_{\text{th}}) = \Pr\{\gamma_E \leqslant \gamma_{\text{th}}\}.$$

Without any loss of generality, it will be assumed that $P_{R_k} = P_S = P_t$. Define $\beta_{SP} \triangleq 1/E\{|h_{SP}|^2\}$, $\beta_{R_kP} \triangleq 1/E\{|h_{R_kP}|^2\}$, $\beta_{SR_k}^P \triangleq 1/E\{P_t d_{SR_k}^{-\rho}|h_{SR_k}|^2/N_0\}$, $\beta_{ME}^P \triangleq 1/E\{P_t|h_{ME}|^2/N_0\}$, $\beta_{SR_k}^Q \triangleq 1/E\{\mathcal{Q}d_{SR_k}^{-\rho}|h_{SR_k}|^2/N_0\}$ and $\beta_{ME}^Q \triangleq 1/E\{\mathcal{Q}|h_{ME}|^2/N_0\}$ with $M \in \{S, R_k\}$. Hereinafter, we assume that the interference links from R_k to the PU receiver undergo independent identically distributed (i.i.d.) Rayleigh fading, i.e., $\beta_{R_kP} = \beta_{RP}, \forall k$.

Since $\Pr\{X + Y \leq c\} < \Pr\{X \leq c\}\Pr\{Y \leq c\}$ if $X > 0, Y > 0$ and $c > 0$, using (3), an upper bound of intercept OP can be obtained by

$$P_{\text{iout,ub}}(\gamma_{\text{th}}) = \Pr\left\{\gamma_{SE} \leq \gamma_{\text{th}}\right\} \times \Pr\left\{\min_{k\in K}\left[\frac{\gamma_{SR_k}\gamma_{R_kE}}{\gamma_{SR_k} + \gamma_{R_kE} + 1}\right] \leq \gamma_{\text{th}}\right\}. \tag{4}$$

It can be observed that the two terms in (3) are correlated since they have a common random variable $|h_{SP}|^2$. Now, let

$X = |h_{SP}|^2$ and $Y = |h_{RP}|^2$, the upper bound of conditional intercept OP can be written as [17]

$$P_{\text{iout,ub}}(\gamma_{\text{th}}|X,Y) = \overbrace{\Pr\{\gamma_{SE} \le \gamma_{\text{th}}|X\}}^{\xi_1} \times \underbrace{\Pr\left\{\min_{k\in K}\left[\frac{\gamma_{SR_k}\gamma_{R_kE}}{\gamma_{SR_k}+\gamma_{R_kE}+1}\right] \le \gamma_{\text{th}}|X,Y\right\}}_{\xi_2}. \quad (5)$$

Since all the links from SU S to EVE experience i.n.i.d. Rayleigh fading, ξ_1 can be expressed as

$$\begin{aligned}\xi_1 &= \Pr\{\gamma_{SE} \le \gamma_{\text{th}}|X\} = F_{\gamma_{SE}}(\gamma_{\text{th}}|X) \\ &= 1 - \exp(\gamma_{\text{th}}\beta_{SE}),\end{aligned} \quad (6)$$

where $\beta_{MT} = 1/E\{\gamma_{MT}\}$ with $M \in \{S, R_k\}$ and $T \in \{R_k, E\}$. Furthermore, ξ_2 in (5) can be expressed as

$$\begin{aligned}\xi_2 &= \Pr\left\{\min_{k\in K}\left[\frac{\gamma_{SR_k}\gamma_{R_kE}}{\gamma_{SR_k}+\gamma_{R_kE}+1}\right] \le \gamma_{\text{th}}|X,Y\right\} \\ &= 1 - \prod_{k=1}^{K}\left(1 - \underbrace{\Pr\left\{\frac{\gamma_{SR_k}\gamma_{R_kE}}{\gamma_{SR_k}+\gamma_{R_kE}+1} \le \gamma_{\text{th}}|X,Y\right\}}_{\zeta}\right),\end{aligned} \quad (7)$$

Similar to [18, eq. (19)], ζ in (7) can be evaluated

$$\begin{aligned}\zeta = 1 - \beta_{SR_k}\exp\left[-\gamma_{\text{th}}(\beta_{SR_k}+\beta_{R_kE})\right]\sqrt{\frac{\gamma_{\text{th}}(\gamma_{\text{th}}+1)\beta_{R_kE}}{\beta_{SR_k}}} \\ \times 2K_1\left(2\sqrt{\gamma_{\text{th}}(\gamma_{\text{th}}+1)\beta_{SR_k}\beta_{R_kE}}\right),\end{aligned} \quad (8)$$

where $K_1(\cdot)$ denotes the first-order modified Bessel function of the second kind [19, eq. (8.432)]. Then, the upper bound of intercept OP can be obtained by [20]

$$P_{\text{iout,ub}}(\gamma_{\text{th}}) = \int_0^\infty\int_0^\infty \overbrace{F_{\gamma_{SE}}(\gamma_{\text{th}}|X)F_{\gamma_{SR_{k^*}E}}(\gamma_{\text{th}}|X,Y)}^{\mathcal{P}_1} \times f_X(x)f_Y(y)\mathrm{d}x\mathrm{d}y. \quad (9)$$

From (6) and (7), $\mathcal{P}_1$ can be obtained. Because $|h_{SP}|^2$ and $|h_{RP}|^2$ are Rayleigh distribution, the probability density function (PDF) of $|h_{SP}|^2$ and $|h_{RP}|^2$ can be expressed as

$$f_X(x) = \beta_{SP}\exp(-x\beta_{SP}), f_Y(y) = \beta_{RP}\exp(-y\beta_{RP}), \quad (10)$$

respectively. In addition, it is true that

$$\min\left(\frac{\mathcal{Q}}{X}, P_S\right) = \begin{cases} P_S, & \text{if } X \le \mathcal{Q}/P_S, \\ \mathcal{Q}/X, & \text{if } X > \mathcal{Q}/P_S. \end{cases} \quad (11)$$

$$\min\left(\frac{\mathcal{Q}}{Y}, P_{R_k}\right) = \begin{cases} P_{R_k}, & \text{if } Y \le \mathcal{Q}/P_{R_k}, \\ \mathcal{Q}/Y, & \text{if } Y > \mathcal{Q}/P_{R_k}. \end{cases} \quad (12)$$

Note that $P_{R_k} = P_S = P_t$. Therefore, the upper bound of intercept OP in (9) can be split according to the four combined cases in (11) and (12) as $P_{\text{iout,ub}}(\gamma_{\text{th}}) = \theta_1(\gamma_{\text{th}}) + \theta_2(\gamma_{\text{th}}) + \theta_3(\gamma_{\text{th}}) + \theta_4(\gamma_{\text{th}})$, where

$$\begin{aligned}\theta_1(\gamma_{\text{th}}) &= \int_0^{Q/P_t}\int_0^{Q/P_t} \mathcal{P}_1 f_X(x)f_Y(y)\mathrm{d}x\mathrm{d}y, \\ \theta_2(\gamma_{\text{th}}) &= \int_0^{Q/P_t}\int_{Q/P_t}^{\infty} \mathcal{P}_1 f_X(x)f_Y(y)\mathrm{d}x\mathrm{d}y, \\ \theta_3(\gamma_{\text{th}}) &= \int_{Q/P_t}^{\infty}\int_0^{Q/P_t} \mathcal{P}_1 f_X(x)f_Y(y)\mathrm{d}x\mathrm{d}y, \\ \theta_4(\gamma_{\text{th}}) &= \int_{Q/P_t}^{\infty}\int_{Q/P_t}^{\infty} \mathcal{P}_1 f_X(x)f_Y(y)\mathrm{d}x\mathrm{d}y.\end{aligned}$$

Then, making some appropriate substitutions and utilizing the following approximation $\lim_{x\to 0} K_1(x) = 1/x$ [21, eq. (9.6.9)], one have

$$\begin{aligned}\theta_1(x) = &\left[1 - \exp\left(-\frac{\mathcal{Q}}{P_t}\beta_{SP}\right)\right]\left[1 - \exp\left(-\frac{\mathcal{Q}}{P_t}\beta_{RP}\right)\right] \\ &\times \left[1 - \exp\left(-x\beta_{SE}^P\right)\right]\Bigg[1 - \prod_{k=1}^{K}\Big(\beta_{SR_k}^P\exp\left[-x(\beta_{SR_k}^P + \beta_{R_kE}^P)\right] \\ &\times 2\sqrt{\frac{x(x+1)\beta_{R_kE}^P}{\beta_{SR_k}^P}}K_1\left(2\sqrt{x(x+1)\beta_{SR_k}^P\beta_{R_kE}^P}\right)\Big)\Bigg],\end{aligned} \quad (13)$$

$$\begin{aligned}\theta_2(x) = &\left[1 - \exp\left(-x\beta_{SE}^P\right)\right]\left[1 - \exp\left(-\frac{\mathcal{Q}}{P_t}\beta_{SP}\right)\right]\exp\left(-\frac{\mathcal{Q}}{P_t}\beta_{RP}\right) \\ &\times \left(1 - \frac{\beta_{RP}\exp\left[-x\sum_{k=1}^{K}\left(\beta_{SR_k}^P + \frac{\mathcal{Q}}{P_t}\beta_{R_kE}^Q\right)\right]}{x\sum_{k=1}^{K}\beta_{R_kE}^Q + \beta_{RP}}\right),\end{aligned} \quad (14)$$

$$\begin{aligned}\theta_3(x) = &\left[1 - \exp\left(-\frac{\mathcal{Q}}{P_t}\beta_{RP}\right)\right]\exp\left(-\frac{\mathcal{Q}}{P_t}\beta_{SP}\right) \\ &\times \left(1 - \frac{\beta_{SP}\exp\left(-x\frac{\mathcal{Q}}{P_t}\beta_{SE}^Q\right)}{x\beta_{SE}^Q + \beta_{SP}}\right. \\ &+ \frac{\beta_{SP}\exp\left[-x\left(\sum_{k=1}^{K}\left(\frac{\mathcal{Q}}{P_t}\beta_{SR_k}^Q + \beta_{R_kE}^P\right) + \frac{\mathcal{Q}}{P_t}\beta_{SE}^Q\right)\right]}{x\sum_{k=1}^{K}(\beta_{SE}^Q + \beta_{SR_k}^Q) + \beta_{SP}} \\ &\left. - \frac{\beta_{SP}\exp\left[-x\sum_{k=1}^{K}\left(\frac{\mathcal{Q}}{P_t}\beta_{SR_k}^Q + \beta_{R_kE}^P\right)\right]}{x\sum_{k=1}^{K}\beta_{SR_k}^Q + \beta_{SP}}\right),\end{aligned} \quad (15)$$

$$\theta_4(x)=\exp\left[-\frac{\mathcal{Q}}{P_t}(\beta_{SP}+\beta_{RP})\right]\Bigg\{1-\frac{\beta_{SP}\exp\left(-x\frac{\mathcal{Q}}{P_t}\beta_{SE}^{Q}\right)}{x\beta_{SE}^{Q}+\beta_{SP}} + \left(\frac{\exp\left(-x\frac{\mathcal{Q}}{P_t}\beta_{SE}^{Q}\right)}{x(\beta_{SE}^{Q}+\sum_{k=1}^{K}\beta_{SR_k}^{Q})+\beta_{SP}}-\frac{1}{x\sum_{k=1}^{K}\beta_{SR_k}^{Q}+\beta_{SP}}\right) \times\frac{\beta_{SP}\beta_{RP}\exp\left[-x\frac{\mathcal{Q}}{P_t}\sum_{k=1}^{K}(\beta_{SR_k}^{Q}+\beta_{R_kE}^{Q})\right]}{x\sum_{k=1}^{K}\beta_{R_kE}^{Q}+\beta_{RP}}\Bigg\}. \quad (16)$$

It can be observed that γ_E in (3) is upper bounded by $\gamma_E \leqslant 2\max\{\gamma_{SE},\gamma_{SR_kE}\}$, as a result, the lower bound of intercept OP can be obtained by

$$P_{\text{iout,lb}}(\gamma_{\text{th}}) = \Pr\left\{\gamma_{SE}\leq\frac{\gamma_{\text{th}}}{2}\right\} \times\Pr\left\{\min_{k\in K}\left[\frac{\gamma_{SR_k}\gamma_{R_kE}}{\gamma_{SR_k}+\gamma_{R_kE}+1}\right]\leq\frac{\gamma_{\text{th}}}{2}\right\}. \quad (17)$$

Following a similar line of arguments as in the proof of $P_{\text{iout,ub}}(\gamma_{\text{th}})$, the lower bound of intercept OP can be derived as

$$P_{\text{iout,lb}}(\gamma_{\text{th}}) =\theta_1\left(\frac{\gamma_{\text{th}}}{2}\right)+\theta_2\left(\frac{\gamma_{\text{th}}}{2}\right) +\theta_3\left(\frac{\gamma_{\text{th}}}{2}\right)+\theta_4\left(\frac{\gamma_{\text{th}}}{2}\right). \quad (18)$$

In order to obtain further insights on the system performance of security, a high-SNRs asymptotic expression for intercept OP will be derived. Without loss of generality, let $\overline{\gamma}=1/N_0$ be the system SNR and assume $Q/P_t=\mu$, where μ is a positive constant. Thus, $\beta_{SR_k}^{P}=1/\left(\overline{\gamma}E\{P_t d_{SR_k}^{-\rho}|h_{SR_k}|^2\}\right)$, $\beta_{R_kE}^{Q}=1/\left(\overline{\gamma}E\{\mathcal{Q}|h_{R_kE}|^2\}\right)$, and $\beta_{ME}^{P}=1/\left(\overline{\gamma}E\{P_t|h_{ME}|^2\}\right)$ with $M\in\{S,R_k\}$. Consider the facts (1) $\lim_{a\to 0}e^{-ax}=1-ax$; (2) $\lim_{x\to 0}K_1(x)=1/x$. When $\overline{\gamma}\to\infty$, after making some algebraic manipulations, $\theta_1(x)$, $\theta_2(x)$, $\theta_3(x)$ and $\theta_4(x)$ become

$$\theta_1^{\infty}(x)\simeq x\beta_{SE}^{P}\left[1-\exp\left(-\mu\beta_{SP}\right)\right]\left[1-\exp\left(-\mu\beta_{RP}\right)\right] \times\sum_{k=1}^{K}\left[x(\beta_{SR_k}^{P}+\beta_{R_kE}^{P})\right]\propto\left(\frac{1}{\overline{\gamma}}\right)^2, \quad (19)$$

$$\theta_2^{\infty}(x)\simeq x\beta_{SE}^{P}\left[1-\exp\left(-\mu\beta_{SP}\right)\right]\exp\left(-\mu\beta_{RP}\right) \times\sum_{k=1}^{K}\left[x(\beta_{SR_k}^{P}+\mu\beta_{R_kE}^{Q})\right]\propto\left(\frac{1}{\overline{\gamma}}\right)^2, \quad (20)$$

$$\theta_3^{\infty}(x)=\theta_4^{\infty}(x)\simeq 0. \quad (21)$$

Finally, utilizing these results and performing the appropriate substitutions, the asymptotic approximation for the upper and lower bounds of intercept OP can be obtained as when $\overline{\gamma}\to\infty$

$$P_{\text{iout,ub}}^{\infty}(\gamma_{\text{th}})\simeq\theta_1^{\infty}(\gamma_{\text{th}})+\theta_2^{\infty}(\gamma_{\text{th}}), \quad (22)$$

$$P_{\text{iout,lb}}^{\infty}(\gamma_{\text{th}})\simeq\theta_1^{\infty}\left(\frac{\gamma_{\text{th}}}{2}\right)+\theta_2^{\infty}\left(\frac{\gamma_{\text{th}}}{2}\right), \quad (23)$$

respectively.

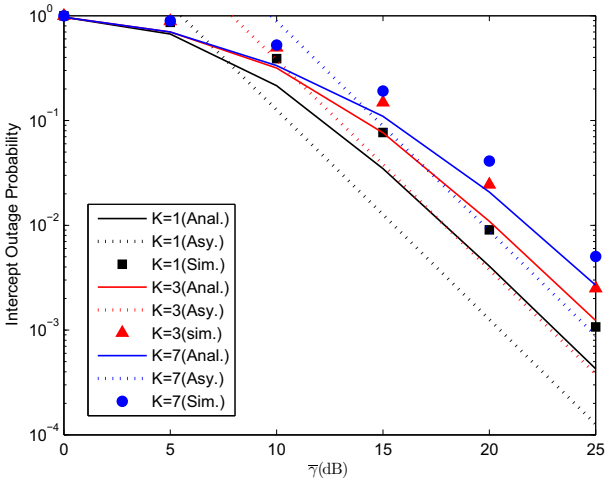

Fig. 2. Intercept OP and asymptotic behavior versus system SNR $\overline{\gamma}$ for different numbers of SU relays with $P_t=\mathcal{Q}=0.5$.

As it can be observed that the asymptotic expressions for the intercept OP are analyzed indicating that the diversity order is two, which means the diversity order in this considered network is independent of the number of secondary relays K.

IV. Numerical and Computer Simulation Results

In this section, various performance evaluation results obtained using the intercept OP expressions presented in Sections III are presented. In order to validate the accuracy of the proposed analytical framework, complimentary performance evaluation results obtained by computer simulated experiments using Monte-Carlo error counting techniques, will be also presented.

Without loss of generality, the statistical average of the channel gains is determined by the distance among the nodes, the threshold $\gamma_{\text{th}}=5$ dB for all considered analysis, and the path loss coefficient $\rho=4$. It is assumed that all SUs are located in a straight line. The SU source is located at (0,0), the SU destination is located at (1,0), the SU relays are also clustered together and collocated at (1/2,0), the PU receiver is located at (0,1), and the eavesdropper EVE is located at (1/2,1). For Fig. 2, the "Anal." curves represent the lower bound of the intercept OP, given in (18). To avoid entanglement, the upper bound of the OP is not shown in Fig. 2. From Figs. 2 and 3, it can be observed that the derived lower and upper bounds of intercept are both very tight with their corresponding simulation results, respectively, thus validating the correctness of the proposed analysis.

Fig. 2 depicts the impact of the number of SU relays K on the intercept OP of the CRN with $P_t=\mathcal{Q}=0.5$. As it can be observed, the security performance improves as the number of SU relays K increases. In other words, when the number of SU relays K increases, higher intercept OP can be observed, so that the security performance improves. Moreover, as expected, the diversity order is unchanged, just as our preceding analysis.

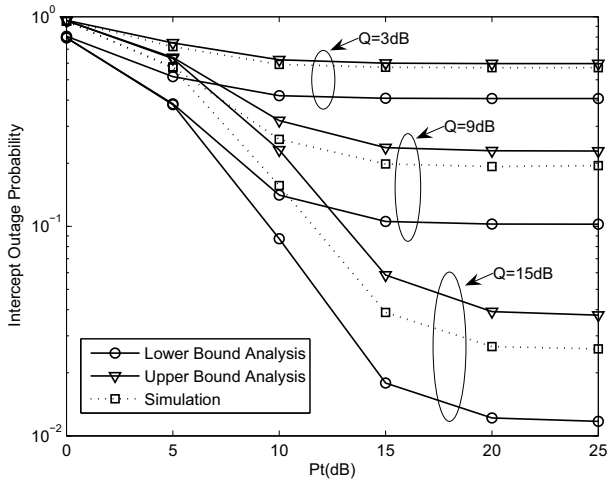

Fig. 3. Impact of P_t on the intercept outage probability with $K = 2$.

Fig. 3 displays the impact of maximum transmit power P_t on the intercept OP when $K = 2$ with interference temperature $\mathcal{Q} = [3, 9, 15]$ dB. It is observed that when $\mathcal{Q}$ is a certain value, outage performance tends to be stable with the increase in P_t. This is because, when P_t is large enough, $\mathcal{Q}$ will limit the transmit power of SUs thus determining the outage performance.

V. Conclusion

In this paper, a comprehensive analytical framework for the performance evaluation of security in multi-relay AF CRNs operating over i.n.i.d. Rayleigh fading channels has been presented. In addition, in order to improve the physical-layer security, relay selection is employed to select the best relay node R_{k^*} which can minimize the end-to-end SNR at the eavesdropper EVE. To ensure the QoS provision at the primary network, both the maximum tolerable interference power at PU and maximum allowable transmit power at SU have been taken into account. Closed-form lower and upper bounds as well as asymptotic expressions of intercept OP have been obtained. Based on the newly derived formulae, our findings reveal that the diversity order of intercept OP is two. Simulation results are provided to validate the analysis.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (Grant No. 61301111/61472343/61401387), China Postdoctoral Science Foundation (Grant No. 2014M56074), the Universities Natural Science Research Project of Jiangsu Province (Grant No. 14KJB510035).

References

[1] J. Mitola and G. Q. Maguire, "Cognitive radio: Making software radios more personal," IEEE Pers. Commun., vol. 6, no. 4, pp. 13C18, Aug. 1999.

[2] Z. Shu, Y. Qian and S. Ci, "On physical layer security for cognitive radio networks," IEEE NetWork, vol. 27, no. 3, pp. 28C33, May 2013.

[3] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355C1387, Oct. 1975.

[4] H. Long, W. Xiang, Y. Zhang, Y. Liu and W. Wang, "Secrecy capacity enhancement with distributed precoding in multirelay wiretap systems," IEEE Trans. Inf. Forensics And Security, vol. 8, no. 1, pp. 229C238, Jan. 2013.

[5] A. Jindal, C. Kundu and R. Bose, "Secrecy outage of dual-hop AF relay system with relay selection without eavesdropper's CSI," IEEE Commun. Lett., vol. 18, no. 10, pp. 1759C1762, Oct. 2014.

[6] Y. Zou, X. Wang and W. Shen, "Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack," Proc. IEEE ICC 2013 (Communication and Information Systems Security Symposium), Budapest, Hungary, Jun. 2013, pp. 2183C2187.

[7] V. N. Q. Bao, N. L.-Trung and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," IEEE Trans Commun., vol. 12, no. 12, pp. 6076C6085, Dec. 2013.

[8] 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. 3299C3310, Sep. 2014.

[9] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," IEEE Trans. Commun., vol. 61, no. 1, pp. 144C154, Jan. 2013.

[10] Y. Zou, X. Wang, W. Shen and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," IEEE Trans. Veh. Technol., vol. 63, no. 6, pp. 2653C2661, Jul. 2014.

[11] G. Wang, Y. Zou, F. Gao and Z. Zhong, "Security-reliability tradeoff for secure wireless communications with channel estimation error," Proc. High Mobility Wireless Communications (HMWC 2013), Shanghai, China, Nov. 2013, pp. 44C47.

[12] M. Z. I. Sarkar and T. Ratnarajah, "Aspect of security in the cognitive relay assisted interference channels," Proc. 2012 IEEE Information Theory Workshop (ITW), Lausanne, Switzerland, Sep. 2012, pp. 652C656.

[13] M. Z. I. Sarkar and T. Ratnarajah, "Enhancing security in the cognitive relay assisted co-existing radio systems with interferences," Proc. IEEE ICC 2013 (Signal Processing for Communications Symposium), Budapest, Hungary, Jun. 2013, pp. 4729C4733.

[14] H. Sakran, M. Shokair, O. Nasr, S. E.-Rabaie and A. A. E.-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," IET Commun., vol. 6, no. 16, pp. 2676C2687, Nov. 2012.

[15] Y. Zou, X. Wang and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," IEEE Trans Commun., vol. 61, no. 12, pp. 5103C5113, Dec. 2013.

[16] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis and A. Nallanathan, "On the security of cognitive radio networks," IEEE Trans. Veh. Technol., 2014, accepted for publication.

[17] T. Q. Duong, V. N. Q. Bao, G. C. Alexandropoulos and H.-J. Zepernick, "Cooperative spectrum sharing networks with AF relay and selection diversity," Electron. Lett., vol. 47, no. 20, pp. 1149C1151, Sep. 2011.

[18] M. A. B. d. Melo and D. B. da Costa, "An efficient relay-destination selection scheme for multiuser multirelay downlink cooperative networks," IEEE Trans. Veh. Technol., vol. 61, no. 5, pp. 2354C2360, Jun. 2012.

[19] I. S. Gradshteyn and I. M. Ryzhik, Table of Integrals, Series, and Products, 7th ed. San Diego, CA: Academic Press, 2007.

[20] F. R. V. Guimarães, D. B. da Costa, T. A. Tsiftsis, C. C. Cavalcante and G K Karagiannidis, "Multiuser and Multirelay Cognitive Radio Networks Under Spectrum-Sharing Constraints," IEEE Trans. Veh. Technol., vol. 63, no. 1, pp. 433C439, Jan. 2014.

[21] M. Abramowitz and I. A. Stegun, Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables, New York, NY, USA: U.S. Dept. Commerce, 1972.