Relay Selection for Improved Physical Layer Security in Cognitive Relay Networks Using Artificial Noise

Shaobo Jia, Jiayan Zhang, Honglin Zhao, Yi Lou and Yao Xu
Email: jiashaobo2007@126.com, jyzhang, hlzhao@hit.edu.cn, louyi8733@gmail.com, xuyao_hit@sina.com

Abstract—In this paper, the physical layer security of underlay cognitive decode-and-forward (DF) relay networks is investigated, wherein one secondary transmitter (ST) exchanges confidential information with one secondary destination (SD) with the assistance of multiple cognitive decode-and-forward (DF) relays by sharing the licensed spectrum of an primary user (PU), and the relayed transmission is intercepted by multiple passive eavesdroppers. To provide security guarantee for secondary transmission, we propose a novel cooperative scheme aided by artificial noise (AN). In the absence of the eavesdroppers’ channel state information (CSI), two opportunistic relay selection schemes, namely best relay selection (BRS) and conventional relay selection (CRS), are proposed as an incentive to further enhance the physical layer security. To be specific, only the CSI of the main channel is employed in the CRS scheme, whereas the BRS scheme invokes both the CSI of the main channel and interference channel. We address the secrecy performance in terms of secrecy outage probability (SOP), for which the closed-form expressions for both the relay selection schemes are derived. Simulation results are provided to verify our analysis, and show that the proposed BRS scheme significantly achieves better secrecy outage performance, as compared with the CRS scheme, as well as the conventional scheme without jamming.

Index Terms—Physical layer security, relay selection, cognitive radio network, secrecy outage probability.

I. INTRODUCTION

Over the past few years, cognitive radio networks (CRNs) have attracted ever growing interest from the wireless community due to its potential in addressing the conflict between the stringent requirement and spectrum scarcity in the next generation of wireless communications [1]-[4]. In CRNs for dynamic spectrum sharing, secondary users (SUs) are allowed to access the licensed radio spectrum provided that the quality of service (QoS) of primary network is maintained, thereby offering the spectrum efficiency improvement.

Due to the dynamic nature of access mechanism and the openness of radio propagation medium, legitimate cognitive radio (CR) users are vulnerable to potential eavesdropping attacks. Therefore, the security aspects in CRNs [5], [6] are of the utmost importance and have sparked widespread interest. Traditionally, cryptographic technologies implemented at upper-layer are employed to achieve communication confidentiality against eavesdropping attacks, which heavily rely on the computational complexity. However, with the rapid advancement of the computation techniques, these cryptographic methods are not perfectly secure and can be deciphered by malicious nodes. As a complementary approach, physical layer security (PLS) is envisioned as a promising technique by smartly exploiting intrinsic randomness of the communications media.

A. Related Works

Recently, numerous works focusing on the PLS in CRNs are available [7]-[10]. The authors in [7] investigated the PLS for CRNs over Nakagami-m fading channels subject to the interference power constraint. Extensions of the system model in [7] to the multi-antenna spectrum sharing environments were presented in [8], in which the closed-form expressions for the exact and asymptotic SOP were derived. In [9], the outage probability and intercept probability were derived for an energy-harvesting underlay CR system adopting energy-aware multiuser scheduling scheme. In [10], the PLS of cognitive DF relay networks over Nakagami-m fading channels was studied with outdated CSI.

To ensure the existence of a nonzero secrecy rate when the channel quality of the wiretap link is superior to that of the legitimate link, Goel et al. in [11] proposed to employ artificial noise (AN) to improve PLS. Motivated by [11], a numerous body of works have studied PLS based on AN in CRNs. In [12], antenna selection schemes were proposed to secure full-duplex multi-antenna CRNs using AN. In [13], a multiuser CR network is considered, where an idle secondary user serves as a friendly jammer to provide security guarantee for secondary network. Exploiting the primary-secondary networks’ cross interference as a collaboration incentive to enhance the PLS of CRNs was addressed [14]-[16]. In [17], secure multiple-antenna transmission schemes with AN for throughput maximization were proposed to guarantee the security of PUs in CRNs. In [18], dual antenna selection was applied to improve the secondary transmission and primary secrecy performance in CRNs, respectively.

Significantly recent research efforts such as [19]-[24] have been devoted to improving the PLS for cognitive relay networks by employing relay selection. With different level of CSI available, relay selection schemes were addressed for secure underlay CRNs over Rayleigh fading channels [19]-[21], Nakagami-m fading channels [22]. In [23], relay selection schemes were proposed and examined to secure DF cognitive relay networks relying on realistic spectrum sensing. In [24], relay selection scheme was proposed for security constrained CRNs aiming to maximize the achievable secrecy rate. Coop-
erative jamming (CJ), as an extension of the idea of AN to cooperative relaying systems with jammers, is widely used to enhance the PLS of cooperative networks [25], [26]. However, only a few studies investigated relay selection schemes for secrecy enhancement in cognitive relay networks considering CJ. The authors in [27] studied the secrecy outage performance of a cognitive relay network with several relay and jammer selection schemes. The selection schemes adopted in this work are based on precise knowledge of global CSI, and the jammer is forced to share the jamming signal with the destination. These constraints incur high feedback overhead, especially for large number of relays, and these selection schemes are not applicable in the presence of passive eavesdropping. In our previous work [28], two relay selection schemes were investigated for DF CRNs in the absence of the eavesdroppers’ CSI, targeting to improve the secure secondary transmission via CJ, however, both the broadcast phase and the maximum transmit power constraint were not addressed.

We remark that this paper is the substantial extension of our previous work [29]. To be specific, this work is different from [29] in three aspects. First, only the cooperative phase is studied in [29], while in this paper, we pursue a more detailed investigation on the secrecy performance of the cognitive relay network considering both the broadcast phase and cooperative phase. Second, [29] studies the multiple eavesdroppers scenario relying on the assumption that the eavesdroppers are located in a cluster, while in this work we drop this assumption as an incentive to address a more practical scenario. Third, in addition to deriving the expressions of SOP for the CRS and BRS schemes, we also provide that for the corresponding relay selection schemes without jamming for comparison purpose. Moreover, numerical results are conducted to exhibit the superiority of our proposed relay selection schemes as compared to the schemes without jamming.

### B. Contributions and Organization

In this work, we investigate the secrecy performance of an underlay cognitive relay network in the presence of multiple passive eavesdroppers via exploiting CJ. The main contributions of this paper are summarized as follows:

- We propose an AN-assisted cooperative scheme, whereby one of the cognitive relays succeeding in source decoding is selected as the forwarding relay to retransmit the confidential signal, while the other relays emit AN attempt to confound the eavesdropper without impairing the channel quality of the legitimate receivers. Provided that the CSI of the wiretap channel is absent, two relay selection schemes, namely BRS and CRS schemes, are proposed to further improve the secrecy performance for the secondary network. Specifically, in the CRS scheme, only the CSI of the main channel is employed, whereas the BRS scheme combines both the CSI of the main channel and interference channel.
- We derive novel closed-form expressions of the exact and asymptotic SOP in the considered CRNs under the BRS and CRS schemes. The analytical results for the corresponding relay selection schemes with no jamming are also presented for comparison purpose.

- Our numerical results demonstrate that by making full use of the CSI of the interference link, the proposed BRS scheme can significantly achieve better secrecy performance than the CRS scheme, as well as the relay selection schemes without jamming. Moreover, we provide insights into the effect of various system parameters, i.e., the peak interference power, the number of relays and eavesdroppers, and the channel parameters, on the secrecy performance of the considered system.

The remainder of this paper is organized as follows. We introduce the mathematical model for the cognitive relay networks in section II. In section III and IV, the detailed analysis of exact and asymptotic SOP for the secondary network under both the two relay selection schemes are carried out, respectively. Some useful remarks is also provided in this section. In section V, numerical results are provided to verify the correctness of the proposed results. Finally, the conclusions of this work are drawn in section VI.

### II. System Model

We consider secure secondary transmission in an underlay cognitive relay network as shown in Fig. 1, where one secondary transmitter (ST) intends to achieve secure communication with one secondary destination (SD) via $N \geq 4$ DF cognitive relays $R_k$ ($k = 1, 2, ..., N$), and be granted to share the licensed spectrum of one primary user (PU), while $M$ passive eavesdroppers $E_m$ ($m = 1, 2, ..., M$) attempt to overhear the secondary transmission. Due to cost limitation, all nodes in the whole network are equipped with a single antenna and operate in the half-duplex mode. Like [10], [27], [28], etc., it is assumed that that direct links between ST and SD/E_m do not exist due to path loss and severe shadowing. Clustered relay configuration is assumed [10], [26], [27], where all the relays are located in the same cluster to ensure equal average

![Fig. 1. System model consisting of a primary user (PU), a secondary transmitter (ST), a collection of cognitive DF relays, a secondary destination (SD), and multiple eavesdroppers.](image-url)
SNR from the secondary relays to other nodes. Furthermore, zero-mean additive white Gaussian noise (AWGN) encounters at each receiver with variance $\sigma^2$. We highlight that the considered cognitive transmission model in Fig. 1 can be applied to diverse practical wireless scenarios in the presence of eavesdropping, e.g., mobile ad hoc networks (MANETs) and wireless sensor networks.

All wireless links are modeled as slow, flat, block Rayleigh fading, where the channel coefficients are complex Gaussian random variables (RVs). We denote $h_{SR_k}$, $h_{SP}$ as the channel coefficients between ST and $R_k$, ST and PU with variances $1/\lambda_{SR}$ and $1/\lambda_{SP}$, respectively. Likewise, we denote $h_{kP}$ and $g_{kP}$ ($h_{kD}$ and $g_{kD}$, $h_{kEm}$ and $g_{kEm}$) as the channel coefficients between $R_k$ and PU ($R_k$ and SD, $R_k$ and $E_m$), $R_k$ and PU ($R_k$ and SD, $R_k$ and $E_m$), respectively, each element of them has variance $1/\lambda_{RP}$ ($1/\lambda_{RD}$, $1/\lambda_{RE_m}$). Note that $g_{kP}$, $g_{kD}$ and $g_{kEm}$ are all $1 \times (N-1)$ vectors.

Under the DF relaying protocol, the transmission duration is equally divided into two phases. We assume that the perfect CSI of all legitimate links are available\(^1\). During the first phase (termed as "broadcast phase"), ST broadcasts its information signal to all the $N$ secondary relays at the transmit power $P_S$. Due to the QoS requirement of primary network in underlay spectrum sharing environments, the transmit power $P_S$ is constrained by [8], [10], [12], [13], [22]

$$P_S = \min\left(P_{th}, \frac{I_{th}}{|h_{SP}|^2}\right),$$

where $P_{th}$ is the maximum transmit power at both phases. $I_{th}$ is the peak interference power constraint at PU. The instantaneous received SNR at $R_k$ is given by

$$\gamma_k = \left|h_{SR_k}\right|^2 \min\left(\frac{\bar{\gamma}_p}{|h_{SP}|^2}\right),$$

where $\bar{\gamma}_p = I_{th}/\sigma^2$ and $\gamma_p = I_{th}/\sigma^2$. The channel capacity between ST and the $k$th relay is given by

$$C_{SR_k} = \frac{1}{2} \log_2 \left(1 + \gamma_k\right),$$

where the factor $1/2$ arises from the fact that two equal phases are required to complete the secondary transmission. With the aid of [30, eq. (2)], the $k$th relay can successfully decode the received signal provided that $C_{SR_k}$ is greater than the target data rate $R_k$. In this case, $R_k$ is said to belong to a decoding set $\Phi$, and $|\Phi|$ is defined as the number of relays in $\Phi$.

During the second phase (termed as "cooperative phase"), one forwarding relay denoted as $R_kF$ is optimally selected from the decoding set $\Phi$ to retransmit the decoded confidential information $u$ with variance $\gamma_{ku}$, which can be overheard by $E_m$ for interception purpose, and the remaining $N-1$ relays denoted as $R_kJ$ simultaneously emit jamming signal $z_k$ to impair the channel quality of the eavesdroppers. We consider the passive eavesdroppers scenario where the CSI between the relays and $E_m$ is absent, whereas its channel statistics information is available. We employ AN proposed in [11] and [32] to guarantee transmission confidentiality for SD. Now we first define an $2 \times (N-1)$ channel matrix, i.e., $H_k = [g_{kD}, g_{kP}]$. The jamming signal can be expressed as $z_k = W_k v_k$, where $W_k ((N-1)\times(N-3))$ is the null space of $H_k$. Hence, we have $W_k = [g_{kF}^H, g_{kD}^H, g_{kP}^H, g_{kEm}^H, g_{kD}^H, g_{kEm}^H, g_{kD}^H, g_{kEm}^H]$, which is the maximum transmit power constraint $P_{th}$, $\sigma_{ku}^2$ and $\sigma_{v}^2$ should be designed to ensure the interference at PU does not exceed a threshold $I_{th}$. Bearing this in mind, we have

$$\sigma_{ku}^2 = \min\left(\frac{I_{th}}{|h_{kD}|^2}, \alpha P_{th}\right), \quad \sigma_{v}^2 = \frac{(1-\alpha)P_{th}}{N-3},$$

where $\alpha \in (0,1]$ is the power allocation factor, representing the fraction of total transmit power allocated to the information signal. Based on this, the instantaneous SNRs at SD and $E_m$ are respectively given by

$$\gamma_{kD} = \frac{\sigma_{ku}^2 |h_{kD}|^2}{\sigma^2}, \quad \gamma_{kEm} = \frac{\sigma_{ku}^2 |h_{kEm}|^2}{\sigma_{v}^2 \gamma_{kD} + \sigma^2},$$

where $G_k = g_{kEm} W_k$.

Based on the proposed cooperative scheme above, if the decoding set $|\Phi| = 0$, then there will be no relay can be selected to forward confidential information, so that the information transmission from ST to SD is interrupted. Mathematically, the instantaneous secrecy capacity of the considered cognitive system can be expressed as [27, eq. (4)]

$$C_S = \begin{cases} \frac{1}{2} \log_2 (1 + \gamma_{kD}) & \text{for } |\Phi| > 0, \\ 0 & \text{for } |\Phi| = 0, \end{cases}$$

where $[x]^+ = \max\{x, 0\}$, $C_{kD} = \frac{1}{2} \log_2 (1 + \gamma_{kD})$ and $C_{kE} = \frac{1}{2} \log_2 (1 + \gamma_{max})$ with $\gamma_{max} = \max_{m=1,2,\ldots,M} \{\gamma_{kEm}\}$.

### III. Secrecy outage performance analysis

In this section, the secrecy performance of the system characterized by the SOP is analyzed under two opportunistic relay selection schemes, for which closed-form expressions are derived. SOP which is defined as the probability that the instantaneous secrecy rate falls below a given threshold secrecy rate $R_S$ can be expressed as

$$P_{out} = \Pr\left(C_S \leq R_S\right) = \sum_{K=0}^{N} \Pr\left(|\Phi| = K| \Pr\left(C_S < R_S\right) |\Phi| = K\right),$$

where $P_{out}$ is the probability that the secrecy rate falls below a given threshold secrecy rate $R_S$. The above expression can be further simplified as

$$P_{out} = \sum_{K=0}^{N} \frac{p_k}{p_\Phi} \Pr\left(C_S < R_S\right) |\Phi| = K, \quad p_k = \Pr\left(|\Phi| = K\right),$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2878058, IEEE Access.
where $P_K$ represents the probability that there are $K$ relays in the decoding set $\Phi$ which can decode the source signal successfully, and $P_{\Phi^K}$ represents the conditional SOP. The exact expression of $P_K$ is given by the following lemma.

**Lemma 1:** The exact expression of $\Pr(|\Phi| = K)$ in (7) can be computed as (8)

$$P_K = \sum_{l=0}^{K} \binom{N}{K} \binom{K}{l} (-1)^l \left( \left( 1 - \exp \left(-\lambda_{SR} \frac{\bar{\gamma}_{th}}{\bar{\gamma}} \right) \right)^{N-K+l} \right) \times \left( 1 - \exp \left(-\lambda_{SP} \frac{\bar{\gamma}_p}{\bar{\gamma}} \right) \right) \sum_{p=0}^{N-K+l} \binom{N-K+l}{p} (-1)^p \times \frac{\lambda_{SP}}{\lambda_{SR}} \frac{\bar{\gamma}_p}{\bar{\gamma}_{th} \bar{\gamma}_p + \lambda_{SP} \frac{\bar{\gamma}_p}{\bar{\gamma}}} \right).$$

(8)

where $\bar{\gamma}_{th} = 2^{2R_{th}} - 1$ and $\binom{K}{l} = K! / ((K-k!)k!)$.

**Proof:** See appendix A.

Next, we will proceed to derive the condition SOP for CRS and BRS schemes, respectively.

### A. Conventional relay selection (CRS)

We first consider the CRS scheme. In this case, the forwarding relay is selected from the decoding set $\Phi$ relying on the most channel power gain between the DF relays and SD such that the resulting information signal arrives at SD is maximized [10, eq. (5)]. Mathematically, the relay selection criterion for CRS scheme is given by

$$k^* = \arg\max_{k \in \Phi} |h_{kD}|^2.$$

(9)

Utilizing (4), (6) and (7), the conditional SOP using the CRS scheme $P_{\Phi^K}$ can be expressed as

$$P_{\Phi^K} = \Pr\left(C^{\text{CRS}} < R_S | |\Phi| = K \right) = \Pr\left(C_{k^*D} - C_{k^*E} < R_S, \sigma_{k^*u}^2 = I_{th}/|h_{k^*D}|^2 \right) + \Pr\left(C_{k^*D} - C_{k^*E} < R_S, \sigma_{k^*u}^2 = \alpha P_{th} \right).$$

(10)

Substituting (4) and (5) into (10), we have

$$P_{\Phi^K} = \Pr\left(X_D < \frac{(e-1)}{\bar{\gamma}_p} X_P + \varepsilon Z, \frac{I_{th}}{X_P} \leq \alpha P_{th} \right) + \Pr\left(X_D < \frac{(e-1)}{\bar{\gamma}_p} X_P + \varepsilon Z, \frac{I_{th}}{X_P} > \alpha P_{th} \right)$$

$$= \int_{0}^{\infty} \int_{0}^{\frac{I_{th}}{\alpha \bar{\gamma}}} F_{X_D}(\frac{(e-1)}{\bar{\gamma}_p} z + \varepsilon z) f_{\varepsilon}(\varepsilon) \frac{f_\mu(x) f_\gamma(z) dxdz}{I_1} + \int_{0}^{\infty} \int_{\frac{I_{th}}{\alpha \bar{\gamma}}}^{\infty} F_{X_D}(\frac{(e-1)}{\bar{\gamma}_p} z + \varepsilon z) f_{\varepsilon}(\varepsilon) \frac{f_\mu(x) f_\gamma(z) dxdz}{I_2}.$$

(11)

where $X_D = \max_{k \in \Phi} |h_{kD}|^2$, $X_P = |h_{k^*D}|^2$, $\varepsilon = \pm 2^{2R_S}$, and

$$Z = \max_{m=1,2,...,M} \left\{ \frac{|h_{E_m}|^2}{\Theta G_{k} G_{k}^2 + 1} \right\}.$$

(12)

with $\Theta = \frac{\sigma^2}{\sigma^2}$.

In what follows, we will proceed to derive $I_1$ and $I_2$, respectively. Here, $|h_{kD}|^2$ and $|h_{k^*D}|^2$ are both exponentially distributed RVs. Therefore, the PDF of $X$ is $f_X(x) = \lambda_{RP} \exp(-\lambda_{RP})$, and the CDF of $X_D$ can be expressed as

$$F_{X_D}(x) = \prod_{n=1}^{K} \Pr(|h_{kD}|^2 < x) = (1 - \exp(-\lambda_{RD} x))^K.$$

(13)

Substituting $F_{X_D}(x)$ and $f_X(x)$ into $I_1$, after some algebraic manipulations, we have

$$I_1 = \exp(-\lambda_{RP} A) + \sum_{n=1}^{K} \binom{K}{n} (-1)^n \omega_1$$

$$\times \int_{0}^{\infty} \exp(-\lambda_{RD} \varepsilon z) f_Z(z) dz,$$

(14)

where

$$\omega_1 = \frac{\lambda_{RP} \bar{\gamma}_p}{\lambda_{RD} (e-1) + \lambda_{RP} \bar{\gamma}_p} \exp \left( -\left( \frac{\lambda_{RD} (e-1)}{\bar{\gamma}_p} + \lambda_{RP} \right) A \right).$$

(15)

Relying on a similar method proposed in [34, eq. (10)], we can expand the item in (15) as

$$\int_{m=1}^{M} \left( 1 - \exp(-\lambda_{E,m} z) \right) = 1 + \sum_{p=1}^{M} (-1)^p \sum_{m=1}^{(\lfloor M/p \rfloor)}$$

$$\times \exp \left( -\lambda_{E,m}^T \frac{I_{p,m}}{z} \right) (1 + \Theta z)^{(N-3)}$$

$$= 1 + \sum_{p} \sum_{m} \exp \left( -\lambda_{E,m}^T \frac{I_{p,m}}{z} \right) (1 + \Theta z)^{(N-3)}.$$

(16)
Using integration by parts, $I_1$ can be further written as

$$I_1 = \exp(-\lambda_{RP} A) + \sum_{n=1}^{K} \left(\frac{K}{n}\right)(-1)^n \omega_1 \times \left(1 - \lambda_{RD} n e \int_0^\infty R_Z(z) \exp(-\lambda_{RD} n e z) dz\right).$$  \hspace{1cm} (17)

Substituting (15) and (16) into (17), applying the binomial theorem and with the aid of [35, eq.(3.382.4)], $I_1$ can be finally attained as

$$I_1 = \exp(-\lambda_{RP} A) + \sum_{n=1}^{K} \left(\frac{K}{n}\right)(-1)^n \omega_1 \times \left(1 + \lambda_{RD} n e \sum_p \sum_m \Theta^{p(3-N)}(\Xi_{n,p,m}) p^{(N-3)} - 1 \times \exp(\Xi_{n,p,m} \Theta^{-1}) \Gamma \left(p(3-N) + 1, \Xi_{n,p,m} \Theta^{-1}\right)\right).$$  \hspace{1cm} (18)

where $\Xi_{n,p,m} = \lambda_{F} m I_{p} + \lambda_{RD} n e$ for ease of description, and $\Gamma(\alpha, x) = \int_{x}^{\infty} \exp(-t) t^{\alpha-1} dt$ denotes the upper incomplete Gamma function [35, eq.(8.350.2)].

Following a similar approach to that we derive $I_1$, the expression of $I_2$ can be evaluated as

$$I_2 = 1 - \exp(-\lambda_{RP} A) \left(1 + \exp(-\lambda_{RP} A) \sum_{n=1}^{K} \left(\frac{K}{n}\right)(-1)^n \omega_2 \times \left(1 - \lambda_{RD} n e \int_0^\infty R_Z(z) \exp(-\lambda_{RD} n e z) dz\right)\right).$$  \hspace{1cm} (19)

where $\omega_2 = \exp(-\lambda_{RD} n e^{-1} \frac{e}{\gamma})$. Plugging (15) and (16) into (19), $I_2$ can be attained as

$$I_2 = 1 - \exp(\lambda_{RP} A) \left(1 + \exp(-\lambda_{RP} A) \sum_{n=1}^{K} \left(\frac{K}{n}\right)(-1)^n \times \omega_2 \left(1 + \lambda_{RD} n e \sum_p \sum_m \Theta^{p(3-N)}(\Xi_{n,p,m}) p^{(N-3)} - 1 \times \exp(\Xi_{n,p,m} \Theta^{-1}) \right) \times \Gamma \left(p(3-N) + 1, \Xi_{n,p,m} \Theta^{-1}\right)\right).$$  \hspace{1cm} (20)

Substituting (18) and (20) into (11), after some algebraic manipulations, we can obtain the closed-form expression of the conditional SOP using the CRS scheme as

$$P_{\Phi_K}^{CRS} = 1 + \sum_{n=1}^{K} \left(\frac{K}{n}\right)(-1)^n W_n \times \left(1 + \lambda_{RD} n e \sum_p \sum_m \Theta^{p(3-N)}(\Xi_{n,p,m}) p^{(N-3)} - 1 \times \exp(\Xi_{n,p,m} \Theta^{-1}) \right) \times \Gamma \left(p(3-N) + 1, \Xi_{n,p,m} \Theta^{-1}\right).$$  \hspace{1cm} (21)

where

$$W_n = \exp(-\lambda_{RD} n e^{-1} \frac{e}{\gamma}) \times \left(1 - \frac{\lambda_{RD} n e^{-1}}{\lambda_{RD} n e^{-1} + \lambda_{RP} \gamma_p} \exp(-\lambda_{RP} A)\right).$$  \hspace{1cm} (22)

**Remark 1:** For comparison purpose, we also provide the expression of the convention relay selection scheme with no jamming (CRSNJ) as in [10] for the considered cognitive relay network.

**Lemma 2:** The exact expression of conditional SOP for the CRSNJ can be computed as (23)

$$P_{\Phi_K}^{CRSNJ} = 1 + \sum_{n=1}^{K} \left(\frac{K}{n}\right)(-1)^n \exp(-\lambda_{RD} n e - 1) \times \left(1 - \frac{\lambda_{RD} n e^{-1}}{\lambda_{RD} n e^{-1} + \lambda_{RP} \gamma_p} \exp(-\lambda_{RP} A)\right) \times \left(1 + \lambda_{RD} n e \sum_p \sum_m (\Xi_{n,p,m})^{-1}\right).$$  \hspace{1cm} (23)

**Proof:** See appendix B.

**B. Best relay selection (BRS)**

As aforementioned, the CSI of the inference channel are not considered in the CRS scheme. Hence, it is reasonable to employ the channel gain of the interference link to participate in implementing the relay selection. With this in mind, we attempt to select the forwarding relay $R_{kF}$ by taking all available CSI into account for the BRS scheme. Utilizing (5), (6), (7) and (12), and with a slight organization, the expression of conditional SOP $P_{\Phi_K}$ can be recast as

$$P_{\Phi_K} = \Pr(X < Z),$$  \hspace{1cm} (24)

where $X \triangleq (1 - \frac{\sigma^2}{N_0} |h_{kD}|^2) \frac{N_0}{\sigma^2}$. As shown in (24), $X$ only requires the CSI between the secondary relays and PU, secondary relays and SD, which are prior knowledge to us. $Z$ only comprises of the CSI between the secondary relays and $\bar{E}_m$, which is actually unavailable. Motivated by this observation, we propose to maximize $X$ to minimize the conditional SOP. Mathematically, the forwarding relay $R_{kF}$ is selected according to the following criterion

$$k^o = \arg \max_{k \in \Phi} \{X\}. $$  \hspace{1cm} (25)

Thus, the conditional SOP of the BRS scheme $P_{\Phi_K}^{BRS}$ can be formulated as

$$P_{\Phi_K}^{BRS} = \Pr(\bar{X} < Z) = \Pr(\bar{X} < 0) + \Pr(\bar{X} < Z, \bar{X} > 0).$$  \hspace{1cm} (26)

where $\bar{X} \triangleq \max_{k \in \Phi} X$. To obtain $P_{\Phi_K}^{BRS}$, the PDF of $\bar{X}$ is required. Resorting to (4), the CDF of $\bar{X}$ is given by

$$F_{\bar{X}}(x) = \Pr(x < \bar{X})
= \underbrace{\Pr(X < x, \sigma_{k^o}^2 = \frac{I_{th}}{|h_{k^o} p|^2})}_{B_1} + \underbrace{\Pr(X < x, \sigma_{k^o}^2 = \alpha P)}_{B_2}.$$  \hspace{1cm} (27)
Substituting $X$ into (27), $B_1$ and $B_2$ can be respectively rewritten as

$$B_1 = \int_0^\infty F_X(x) \left( e^{\frac{(e-1)}{\bar{\gamma} p}} - \frac{\lambda_{RD} (e-1)}{\lambda_{RD} (e-1) + \lambda_{RP} \bar{\gamma} p} \right) \frac{\lambda_{RD} (e-1)}{\lambda_{RD} (e-1) + \lambda_{RP} \bar{\gamma} p} \times \exp \left( \left( \frac{\lambda_{RD} (e-1)}{\lambda_{RD} (e-1) + \lambda_{RP} \bar{\gamma} p} \right) A \exp(-\lambda_{RD} x), \right)$$

$$B_2 = \left( 1 - \exp \left( \left( \frac{\lambda_{RD} (e-1)}{\lambda_{RD} (e-1) + \lambda_{RP} \bar{\gamma} p} \right) x \right) \right) \left( 1 - \exp(-\lambda_{RD} A) \right).$$

Substituting (29) into (27), after some algebraic manipulations, the CDF of $X$ can be expressed as

$$F_X(x) = 1 - \omega_3 \exp(-\lambda_{RD} x).$$

where

$$\omega_3 = \left( 1 - \exp(-\lambda_{RP} A) \right) \frac{\lambda_{RD} (e-1)}{\lambda_{RD} (e-1) + \lambda_{RP} \bar{\gamma} p} \times \exp \left( \left( \frac{\lambda_{RD} (e-1)}{\lambda_{RD} (e-1) + \lambda_{RP} \bar{\gamma} p} \right) A \exp(-\lambda_{RD} x), \right).$$

Therefore, the CDF of $X$ can be obtained as

$$F_X(x) = \left( 1 - \omega_3 \exp(-\lambda_{RD} x) \right)^K.$$

By taking the derivation of $F_X(x)$ w.r.t. $x$, we obtain the PDF of $X$ as

$$f_X(x) = \Delta(1 - \omega_3 \exp(-\lambda_{RD} x))^{K-1} \exp(-\lambda_{RD} x).$$

where $\Delta = \lambda_{RD} \epsilon_3 K$. Utilizing formula of total probability, the expression of $I$ can be reformulated as

$$I = \int_0^\infty R_Z(x) f_X(x)dx.$$

Then, plugging (15), (16) and (32) into (33), applying the binomial theorem, we can obtain $I$. Substituting $I$ and (31) into (26), we can finally obtain the conditional SOP for the proposed BRS scheme as

$$P_{\Phi_K}^{BRS} = (1 - \omega_3)^K - \Delta \sum_p \sum_m \sum_{n=0}^{K-1} \frac{\lambda_{RD} (e-1)}{\lambda_{RD} (e-1) + \lambda_{RP} \bar{\gamma} p} \times \exp \left( \left( \frac{\lambda_{RD} (e-1)}{\lambda_{RD} (e-1) + \lambda_{RP} \bar{\gamma} p} \right) A \exp(-\lambda_{RD} x), \right)$$

Remark 2: In order to better assess the performance gain result from utilizing the CSI of the inference channel, we also present the conditional SOP for the CRS scheme with no jamming (BRSNJ), which is given by the following lemma.

Lemma 3: The conditional SOP of the considered cognitive radio network using the BRSNJ scheme can be derived as

$$P_{\Phi_K}^{BRSNJ} = (1 - \omega_3)^K - \Delta \sum_p \sum_m \sum_{n=0}^{K-1} \frac{\lambda_{RD} (e-1)}{\lambda_{RD} (e-1) + \lambda_{RP} \bar{\gamma} p} \exp(-\lambda_{RD} x).$$

Proof: See appendix C.

C. Optimal power allocation (OPA)

In this subsection, the OPA problem is addressed to further improve the SOP performance for both the BRS and CRS schemes. Note that both the conditional SOP $P_{\Phi_K}^i$ ($i \in \{CRSNJ, BRSNJ\}$) are single-variable functions of $\alpha$, which belongs to the interval $(0, 1]$, and our aim is to minimize the SOP. Henceforth, we can formulate the optimization problem as

$$\min_{\alpha} P_{\Phi_K}^i \quad \text{s.t.} \quad \alpha \in (0, 1].$$

Solving (36) directly is challenging as a result that $P_{\Phi_K}^i$ is a complex function of $\alpha$. Instead of deriving the closed-form expression of $\alpha$, a simple one-dimensional search technique, e.g., grid search or golden search, can be employed to handle the single-variable optimization problem (36), and choosing the one that leads to the minimum as an optimal solution of (36).

IV. ASYMPTOTIC ANALYSIS

In this section, we evaluate asymptotic $P_{\text{out}}$ expressions $P_{\text{out}}^{\infty}$ ($P_{\text{out}}$ for $P_{\text{th}} \to \infty$), which denotes the secrecy outages for fully cognitive (transmit power only limited by interference constraint) regime. As $P_{\text{th}} \to \infty$, $\bar{\gamma} \to \infty$, thus $P_K$ in (8) can be reduced to

$$P_{\Phi_K}^{\infty} = \frac{K}{\bar{\gamma}} \sum_{p=0}^{K-1} \left( \sum_{n=0}^{N-K} \frac{\lambda_{RD} (e-1)}{\lambda_{RD} (e-1) + \lambda_{RP} \bar{\gamma} p} \exp(-\lambda_{RD} x) \right) \left( \sum_{n=0}^{N-K} \frac{\lambda_{RD} (e-1)}{\lambda_{RD} (e-1) + \lambda_{RP} \bar{\gamma} p} \exp(-\lambda_{RD} x) \right).$$

A. Conventional relay selection

According to (21), the asymptotic conditional SOP of the considered cognitive radio network using the CRS scheme can be derived as

$$P_{\Phi_K}^{\infty} = 1 + \sum_{n=1}^{K} \left( \frac{K}{n} \right) \left( \frac{\lambda_{RD} (e-1)}{\lambda_{RD} (e-1) + \lambda_{RP} \bar{\gamma} p} \right)^n \exp(-\lambda_{RD} x).$$

Similarly, resorting to (23), the asymptotic conditional SOP of the considered cognitive radio network using the CRSNJ scheme can be derived as

$$P_{\Phi_K}^{\infty} = 1 + \sum_{n=1}^{K} \left( \frac{K}{n} \right) \left( \frac{\lambda_{RD} (e-1)}{\lambda_{RD} (e-1) + \lambda_{RP} \bar{\gamma} p} \right)^n \exp(-\lambda_{RD} x).$$
the considered cognitive radio network using the BRS scheme

B. Best relay selection

With the help of (35), the asymptotic conditional SOP of the considered cognitive radio network using the BRS scheme can be derived as

\[ p_{\Phi_K}^{\text{BRS}, P_{th} \to \infty} = \left( \frac{\lambda_{RD}(e-1)}{\lambda_{RD}(e-1) + \lambda_{RP} \bar{\gamma}_p} \right)^K. \] (40)

V. Numerical results

In this section, numerical results are provided for validation of the derived expressions. All simulation results are based on the proposed AN-assisted cooperative scheme with OPA using BRS and CRS. In our simulations, all channel are assumed to undergo Rayleigh fading. We set the target data rate \( R_h = 0.1 \) bits/s/Hz, the threshold secrecy rate \( R_S = 1 \) bits/s/Hz. Without loss of generality, the noise variance \( \sigma^2 \) is normalized to be 1, \( \lambda_{SR} = \lambda_{RP} = \lambda_{RD} \) and \( \lambda_{KE} = \lambda_{KE_m} \). For the purpose of comparison, the conventional relay selection scheme with no jamming (labeled as CRSNJ) in [10] is also presented as a benchmark method. As shown in Figs. 2-6, the Monte Carlo simulation points are in excellent match with analytical curves, which corroborates the accuracy of our derivations.

In Fig. 2, we present the exact and asymptotic SOP of the proposed cognitive system using three different schemes versus transmit SNR \( \bar{\gamma} \) for different \( \bar{\gamma}_p \). Firstly, it is evident that the SOP of the BRS scheme significantly outperforms the ones of the CRS and CRSNJ schemes for \( \bar{\gamma}_p \) greater than 5dB, which confirms that BRS is the most effective scheme. This is because the BRS scheme performs relay selection by making full use of all available CSI, thus results in a better performance. On the other hand, it is observed that for the CRSNJ scheme, the SOP saturates from very low \( \bar{\gamma} \), and both the proposed BRS and CRS schemes perform better than the CRSNJ scheme, demonstrating that jamming is rather an effective approach to enhance the secrecy performance for the wireless transmissions. As expected, we can find that the SOP decreases with increasing \( \bar{\gamma} \), because a higher \( \bar{\gamma} \)
implies a larger transmit power at both the ST and the relays. Furthermore, the SOP exhibits a floor in the higher $\gamma$ region. It is because as $\gamma$ goes to infinity, the transmit power at ST and the secondary relays are limited only by the interference power constraint from the PU leading the system to falling into a full-cognitive scenario. Thus for a given system setting, the secrecy performance cannot be enhanced unless $\gamma_p$ is increased.

In Fig. 3, we depict the SOP versus the number of relays $N$ using four different schemes. As shown in Fig. 3, we can observe that the SOP decreases with $N$ increasing, it can be explained by the following two reasons. Larger $N$ means that there will be more relays can decode the confidential messages successfully, which reduces the outage probability in the broadcast phase. On the other hand, more relays can jam the eavesdroppers more efficiently, which yields a performance gain in the cooperative phase. Besides, the SOP of BRS decreases faster than the ones of CRS and CRSNJ schemes, which means BRS is the most effective scheme with increasing $N$. It is also seen that the SOP of BRSNJ scheme outperforms that the one of CRSNJ scheme, demonstrating that even with no jamming, utilizing the CSI of PU can still result in a performance gain.

In Figs. 4-5, we depict the exact and asymptotic SOP of the proposed cognitive system using three different schemes versus $\gamma$ for various values of $M$ and $\lambda_{KE}$. As shown in Fig. 4, we can find that the secrecy performance decreases with increasing $M$, because more eavesdroppers will increase the information leakage, thereby degrading the overall secrecy performance of this cognitive radio network in terms of SOP. From Fig. 5, it can be seen that the SOP with a larger $\lambda_{KE}$ outperforms the one with a smaller $\lambda_{KE}$. It is due to the fact that a larger $\lambda_{KE}$ means a worse channel quality between the forwarding relay and $E_m$. It is also seen that in the high $\gamma$ range ($\gamma \to \infty$), different $M$ and $\lambda_{KE}$ achieve the same secrecy outage performance, which is in accordance with (38) and (40).

Fig. 6 illustrates the impact of $\lambda_P$ on the secrecy outage performance with $N$ varying. It is seen that with $\lambda_P$ increasing, the secrecy outage performance is enhanced. This is because a higher $\lambda_P$ implies a worse channel condition from the ST and the forwarding relay to PU, and thus less interference will be imposed on PU. It can be also observed that the performance gap between the BRS scheme and CRS scheme becomes smaller for higher $\lambda_P$. This is because the performance gain results from exploring the CSI of interference channel eventually vanishes when $\lambda_P$ goes larger.

Fig. 7 shows the optimal power allocation factor $\alpha$ versus $\gamma$ using BRS and CRS schemes with different $M$. It is seen that $\alpha$ decreases with $\gamma$, which means that more power should be allocated to generate interference when the transmit SNR increases. Furthermore, BRS scheme always maintains a lower $\alpha$ value than CRS scheme. It signifies that, to achieve the optimal secrecy outage performance at a same $\gamma$ value, the BRS scheme requires less power to produce jamming signal than the CRS one. Besides, it can be also seen that $\alpha$ decreases with $M$ increasing, which implies that more power should be allocated to the jamming signal to cover the secondary transmission when the number of eavesdroppers increases.

VI. Conclusion

In this work, we considered the secure secondary transmission of an underlay cognitive relay network coexisting with multiple passive eavesdroppers using AN. Provided that the CSI of the eavesdroppers is unavailable, two opportunistic relay selection schemes, namely BRS and CRS schemes, were proposed to further improve the secrecy performance of the considered system. New closed-form expressions of the SOP were derived for both the relay selection schemes. The analytical results were verified by performing Monte-Carlo simulations. It was shown that the proposed BRS and CRS schemes exhibit better performance compared with the scheme without jamming, i.e., CRSNJ scheme. On the other hand, the BRS scheme significantly outperforms than the CRS one without increasing overhead. Besides, the secrecy outage performance of the considered system can significantly
benefit from loosing the peak interference power constraint and increasing the number of cooperative relays. More number of eavesdroppers will pose greater threats to the security of the considered system. Moreover, the fading parameters of interference and wiretap channels also have great effects on the secrecy performance of the secondary transmission.

APPENDIX A

PROOF OF LEMMA 1

For ease of description, let $X_P = |h_{SP}|^2$ and $X_{R_k} = |h_{SR_k}|^2$. Resorting to (3) and based on the binomial theorem, the probability that there exist any $K$ out of $N$ relays that can correctly decode the source signal can be attained as

$$P_K = \int_0^\infty \left( \sum_{k=0}^{K} \binom{N}{k} \left[ \Pr(C_{SR_k} > R_{th}) \right]^k \times \left[ \Pr(C_{SR_k} \leq R_{th}) \right]^{N-K} f_{X_P}(x) \right) dx$$

$$= \sum_{l=0}^{K} \binom{N}{K} \binom{K}{l} (-1)^l \int_0^\infty \left( \int_0^{2\pi} F_{X_{R_k}} \left( \frac{\gamma_{th}}{\gamma} \right) \right)^{N-K+l} f_{X_P}(x) dx$$

$$+ \int_0^\infty \left( \int_0^{2\pi} F_{X_{R_k}} \left( \frac{\gamma_{th}}{\gamma} \right) \right)^{N-K+l} f_{X_P}(x) dx$$  \hspace{1cm} (A.1)

Here, both $|h_{SP}|^2$ and $|h_{SR_k}|^2$ are exponentially distributed RVs, then the probability density function (PDF) of $|h_{SP}|^2$ is $f_{X_P}(x) = \lambda_{SP} \exp(-\lambda_{SP} x)$ and the cumulative density function (CDF) of $|h_{SR_k}|^2$ is $F_{X_{R_k}}(x) = 1 - \exp(-\lambda_{SR} x)$. Substituting $f_{X_P}(x)$ and $F_{X_{R_k}}(x)$ into (A.1), the integral terms $\mathcal{A}_1$ and $\mathcal{A}_2$ can be respectively derived as

$$\mathcal{A}_1 = \left( 1 - \exp\left( -\lambda_{SR} \frac{\gamma_{th}}{\gamma} \right) \right)^{N-K+l} \left( 1 - \exp\left( -\lambda_{SP} \frac{\gamma_{th}}{\gamma} \right) \right)^{K-l}$$  \hspace{1cm} (A.2)

and

$$\mathcal{A}_2 = \sum_{p=0}^{N-K+l} \binom{N-K+l}{p} (-1)^p \lambda_{SP} \frac{\gamma_{th} \gamma}{\lambda_{SR} \gamma_{th} \gamma + \lambda_{SP} \gamma} \times \exp\left( -\lambda_{SR} \frac{\gamma_{th} \gamma}{\lambda_{SP} \gamma} + \lambda_{SP} \frac{\gamma}{\lambda_{SP} \gamma} \right).$$  \hspace{1cm} (A.3)

Then, substituting (A.2) and (A.3) into (A.1), we can obtain the exact expression of $\Pr(|\Phi| = K)$ as (8).

APPENDIX B

PROOF OF LEMMA 2

For the CRSNJ scheme, no power will be allocated to the jamming signals, i.e., the power allocation factor is $\alpha = 1$, therefore, the conditional SOP for the CRSNJ scheme can be formulated as

$$P_{\Phi_k}^{CRSNJ} = \Pr(C_{SR}^{CRS} < R_s) | \Phi = K$$

$$= \Pr\left( \left| C_{k} \cdot D - C_{k} \cdot E \right| \leq R_s, \sigma_{k-u}^2 = I_{th}/|h_{k} \cdot p|^2 \right) + \Pr\left( |C_{k} \cdot D - C_{k} \cdot E| > R_s, \sigma_{k-u}^2 = \alpha I_{th} \right).$$  \hspace{1cm} (B.1)

Observing (B.1) and (10), we can obtain that the positive random variable $Z$ in (12) becomes $\tilde{Z} = \max_{m=1,2,...,M} \{ |h_{k} \cdot E_{m}|^2 \}$, the CCDF of $\tilde{Z}$ can be written as

$$R_{2}(z) = 1 - \sum_{m=1}^{M} \left( 1 - \exp(-\lambda_{E,m} z) \right) = - \sum_{m=1}^{M} \sum_{l=0}^{\infty} \exp(-\lambda_{E,m} z).$$  \hspace{1cm} (B.2)

Substituting (B.2) into (17) and (19), then $I_1$ and $I_2$ can be derived as

$$I_1 = \exp\left( -\lambda_{RF} \frac{I_{th}}{P_{th}} + \sum_{n=1}^{K} \binom{K}{n} (-1)^n \omega_1 \right)$$

$$\times \left( 1 + \lambda_{RD} \sum_{p=0}^{K} \sum_{m=1}^{\infty} \left( \Xi_{n,p,m} \right)^{-1} \right).$$  \hspace{1cm} (B.3)

and

$$I_2 = 1 - \exp\left( -\lambda_{RF} \frac{I_{th}}{P_{th}} + \sum_{n=1}^{K} \binom{K}{n} (-1)^n \lambda_{RD} k \epsilon \sum_{p=0}^{K} \sum_{m=1}^{\infty} \left( \Xi_{n,p,m} \right)^{-1} \right).$$  \hspace{1cm} (B.4)

respectively. Substituting (B.3) and (B.4) into (11), and with a slight organization, we can obtain the closed form expression of the conditional SOP for the BRSNJ scheme as (23).

APPENDIX C

PROOF OF LEMMA 3

In this regard, the conditional SOP of the BRSNJ scheme $P_{\Phi_k}^{BRS}$ can be formulated as

$$P_{\Phi_k}^{BRSNJ} = \Pr(\tilde{X} < \tilde{Z})$$

$$= \Pr(\tilde{X} < 0) + \Pr(\tilde{X} < \tilde{Z}, \tilde{X} > 0),$$  \hspace{1cm} (C.1)

Utilizing formula of total probability, we can further evaluate $P_{\Phi_k}^{BRSNJ}$ as

$$P_{\Phi_k}^{BRSNJ} = F_{\tilde{X}}(0) + \int_0^{\infty} R_{2}(x) f_{\tilde{X}}(x) dx.$$  \hspace{1cm} (C.2)

Substituting (31), (32) and (B.2) into (C.2), the exact expression of $P_{\Phi_k}^{BRSNJ}$ can be finally attained as (35).