Mou *et al. EURASIP Journal on Wireless Communications and Networking* (2017) 2017:144
DOI 10.1186/s13638-017-0923-2

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

On the security of cooperative cognitive radio networks with distributed beamforming

Weifeng Mou, Weiwei Yang*, Yuzhen Huang, Xiaoming Xu, Yueming Cai and Kaihua Wang

Abstract

This paper investigates the secrecy performance of amplify-and-forward (AF)-relaying cooperative cognitive radio networks (CCRNs) over Rayleigh-fading channels. Specifically, we consider practical passive eavesdropping scenarios, where the channel state information of the eavesdropper's link is not available at the secondary transmitter. In order to avoid interfering with the primary receiver and enhance the secrecy performance, collaborative distributed beamforming is adopted at the secondary relays. Closed-form and asymptotic expressions for the secrecy outage probability of CCRNs in the presence of single and multiple non-colluding eavesdroppers are derived. The asymptotic analysis reveals that the achievable secrecy diversity order of collaborative distributed beamforming with M AF relays is $M - 1$ regardless of the number of eavesdroppers. In addition, simulations are conducted to validate the accuracy of our analytical results.

Keywords: Cooperative cognitive radio networks (CCRNs), Physical layer security, Distributed beamforming

1 Introduction

Cognitive radio has been regarded as a potential means to improve spectral efficiency by allowing secondary users (SUs) to share the spectrum originally allocated to the primary users (PUs), as long as the generated interference aggregated at the primary receivers is below acceptable levels [1]. In order to enhance system performance and extend the coverage of secondary transmission, cooperative relay techniques have been further introduced into cognitive radio networks (CRNs), and thus, a novel network model, cooperative cognitive radio networks (CCRNs), has attracted significant interests in the research community [2]. On the other hand, due to the broadcast nature of wireless medium and the openness of cognitive radio architecture, CRNs face a more serious challenge of security, and higher layer cryptographic authentication and identification have become expensive and vulnerable to attacks [3]. Recently, a promising approach towards achieving secure communications has been developed by Wyner in [4] termed as physical layer security, the key idea of which lies in exploiting the randomness of wireless channels to ensure the security of confidential information.

*Correspondence: wwyang1981@163.com
College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China

Due to the advantages of physical layer security, many researchers have devoted efforts to investigate the physical layer security issues in CRNs [5–10]. In [5], the secrecy performance of CRNs in terms of the secrecy outage probability and the probability of non-zero secrecy capacity was analyzed. In [6], the authors investigated the achievable secrecy rates of multiple-input single-output (MISO) CRNs with different beamforming schemes. Later, the secrecy outage performance of single-input multiple-output (SIMO) CRNs using selection combining (SC) and generalized selection combining (GSC) was investigated in [7] and [8], respectively. The authors in [9] investigated the secrecy outage and diversity performance for multi-user multi-eavesdropper CRNs. The exact and asymptotic expressions of the secrecy outage probability in multiple-input multiple-output (MIMO) CRNs with transmit antenna selection (TAS)/maximal ratio combining (MRC) were derived in [10].

In addition to the multi-antenna diversity, user cooperation can also be exploited to enhance the security of wireless transmission. The authors in [11] proposed an opportunistic decode-and-forward (DF)-relaying scheme for CCRNs against eavesdropping. In [12], we investigated the secrecy outage performance for DF-relaying CCRNs with outdated channel state information. Different joint relay and jammer selection policies were developed to

enhance the secrecy outage performance for DF-relaying CCRNs in [13]. The security-reliability trade-off performance of single-relay and multi-relay selection strategies for DF-relaying CCRNs was investigated in [14]. However, very few research has considered the secrecy performance of amplify-and-forward (AF)-relaying CCRNs except [15], in which the authors investigated the security and the reliability performance of CCRNs with single AF relay in terms of the intercept probability. It is worth noting that the intercept probability is a special case of secrecy outage probability when the target secrecy data rate is set to zero. To the best of the authors' knowledge, no works have considered the secrecy outage probability of CCRNs with multiple AF relays. Besides, various advanced techniques have been employed to enhance the physical layer security of CRNs, such as multiple antenna diversity in [7–10], relay selection in [11–14], artificial noise in [13], and secrecy beamforming/precoding in [6]. However, collaborative distributed beamforming-based security enhancement in CCRNs has not been investigated yet.

Different from the aforementioned works, in this paper, we investigate the secrecy outage performance of multiple AF relay-assisted CCRNs with distributed beamforming against passive eavesdropping attacks. The main contributions of our work are summarized as follows:

1) Compared with [11–14] that only considered the relay selection for DF-relaying CCRNs and [15] that only considered the intercept probability for single AF-relaying CCRNs, we investigate the physical layer security in terms of the probability of non-zero secrecy capacity, the secrecy outage probability, the secrecy array gain, and the secrecy diversity order for multiple AF-relaying CCRNs with collaborative distributed beamforming in the presence of single and multiple non-colluding eavesdroppers, respectively, where distributed zero-forcing beamforming (D-ZFB) is employed at the relays without interfering with the primary users.
2) We derive the closed-form expressions of the probability of non-zero secrecy capacity and the secrecy outage probability as well as the asymptotic expression at high SNR regimes. Our asymptotic results accurately predict the secrecy diversity order of M AF relay CCRNs with collaborative distributed beamforming, i.e., $M-1$, which is different from the results obtained in [11] and [13]. This is due to the fact that the proposed collaborative distributed beamforming scheme is designed at relays to avoid the interference at PUs at the expense of one spatial degree. In addition, numerical and simulation results are provided to verify the correctness of the proposed scheme.

2 System model

Let us consider a spectrum-sharing cognitive relay network [16], which consists of one secondary source (S), M AF relays ($R_1, \cdots, R_M$), one secondary destination (D), one primary receiver (P), and one passive eavesdropper (E), as shown in Fig. 1. All the nodes are equipped with a single antenna and operate in half-duplex mode. We assume that the direct links from S to D and from S to E do not exist due to severe shadowing environment. The data transmission from S to D can only be done with the help of relays, with the possible wiretap from the eavesdropper. We assume that all channels experience slow block fading and additive white Gaussian noise (AWGN) with variance of σ_0^2, where the fading coefficients are invariant during one fading block and the corresponding channel gains follow independent Rayleigh distribution. Let h_{ab} denote the channel coefficient between a and b. The channel power gains $|h_{SR_i}|^2$, $|h_{R_iD}|^2$, $|h_{R_iE}|^2$, $|h_{R_iP}|^2$, and $|h_{SP}|^2$ are independent and exponentially distributed with parameters λ_{SR_i}, λ_{R_iD}, λ_{R_iE}, λ_{R_iP}, and λ_{SP}, respectively. Without loss of generation, all the secondary relays are close to each other and forming a cluster, i.e., $\lambda_{SR_i} = \lambda_{SR}$, $\lambda_{R_iD} = \lambda_{RD}$, $\lambda_{R_iE} = \lambda_{RE}$, and $\lambda_{R_iP} = \lambda_{RP}$ for all i. $\mathbf{h}_{SR} = \left[h_{SR_1}, \cdots, h_{SR_M}\right]^T$, $\mathbf{h}_{RD} = \left[h_{R_1D}, \cdots, h_{R_MD}\right]^T$, $\mathbf{h}_{RE} = \left[h_{R_1E}, \cdots, h_{R_ME}\right]^T$, and $\mathbf{h}_{RP} = \left[h_{R_1P}, \cdots, h_{R_MP}\right]^T$ represent the channel vectors between the secondary source and the relays, between the relays and the secondary destination, between the relays and the eavesdropper, and between the relays and the primary receiver, respectively. It is worth mentioning that we focus on a passive eavesdropper scenario, where the instantaneous channel state information (CSI) of the eavesdropper's link $\mathbf{h}_{RE}$ is not known at the secondary source. In addition, the CSI of interference links, e.g., $|h_{R_iP}|^2$ and $|h_{SP}|^2$, can be acquired through a spectrum-band manager that mediates between the primary and secondary networks. However, for those

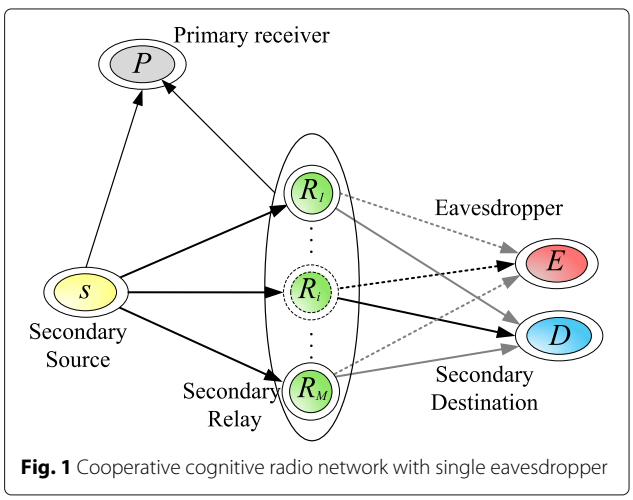

Fig. 1 Cooperative cognitive radio network with single eavesdropper

cases where the secondary network has no knowledge of the interference channel, our results serve as performance bounds for the considered CCRNs and represent efficient system design tools [17].

The transmission is divided into two slots. In the first phase, the secondary source broadcasts the encoded confidential data. According to the underlaying spectrum-sharing approach, the secondary source adjusts its transmit power P_S under a predefined threshold I to guarantee the quality of service of the primary user. Hence, the transmit power at the secondary source is constrained as $P_S = I \Big/ |h_{sp}|^2$ [7]. In the second phase, the relays amplify and forward the received signals to the destination with the transmit power P_R. In order to avoid interfering with the primary transmission and maximize the mutual information of the secondary system, the D-ZFB scheme is applied to null the interference to the primary receiver, and the $M \times 1$ D-ZFB weight vector is the solution of the following problem, mathematically, $\max_{\mathbf{w}_{ZF}} |\mathbf{h}_{RD}^H \mathbf{w}_{ZF}|$ $s.t.\ |\mathbf{h}_{RP}^H \mathbf{w}_{ZF}| = 0$, $\|\mathbf{w}_{ZF}\|^2 = 1$

By applying a standard Lagrangian multiplier method, the optimal weight vector is given as $\mathbf{w}_{ZF} = \mathbf{T}^{\perp}\mathbf{h}_{RD} \big/ \left\|\mathbf{T}^{\perp}\mathbf{h}_{RD}\right\|$, where $\mathbf{T}^{\perp} = \mathbf{I} - \mathbf{h}_{RP}\left(\mathbf{h}_{RP}^H \mathbf{h}_{RP}\right)\mathbf{h}_{RP}^H$ is the projection idempotent matrix with rank $(M-1)$.

Thus, the equivalent received signal-to-noise ratio (SNR) at D and E is given as

$$\gamma_D^{AF} = \frac{\gamma_1 \gamma_2}{\gamma_1 + \gamma_2 + 1} \tag{1}$$

$$\gamma_E^{AF} = \frac{\gamma_1 \gamma_E}{\gamma_1 + \gamma_E + 1} \tag{2}$$

where $\gamma_1 = \left(I/\sigma_0^2\right)\|\mathbf{h}_{SR}\|^2 \big/ |h_{SP}|^2$, $\gamma_2 = \left(P_R/\sigma_0^2\right)\left|\mathbf{T}^{\perp}\mathbf{h}_{RD}\right|^2$, and $\gamma_E = \left(P_R/\sigma_0^2\right)\left|\mathbf{h}_{RE}^H \mathbf{w}_{ZF}\right|^2$ denote the equivalent instantaneous SNRs at the *S-R*, *R-D*, and *R-E* links, respectively.

Considering that $\|\mathbf{h}_{SR}\|^2$ is a chi-square random variable with $2M$ degrees of freedom with parameter λ_{SR} due to $h_{SR_i}, i = 1, \cdots, M$ being i.i.d exponential distribution variables with parameter λ_{SR}, and $|h_{SP}|^2$ is an exponential random variable with parameter λ_{SP}, then the cumulative distribution function (CDF) of γ_1 is given by

$$F_{\gamma_1}(\gamma) = \left(\frac{\gamma}{\bar{\gamma}_1 + \gamma}\right)^M \tag{3}$$

where $\bar{\gamma}_1 = (I\lambda_{SR}) \big/ \left(\lambda_{SP}\sigma_0^2\right)$.

Let $\mathbf{h}_{RD} = \mathbf{h}_{RD} \big/ \sqrt{\lambda_{RD}}$, then each entry of $\mathbf{h}_{RD} = \mathbf{h}_{RD} \big/ \sqrt{\lambda_{RD}}$ is i.i.d. $\mathcal{CN}(0,1)$. Considering $\mathbf{T}^{\perp} = \mathbf{I} - \mathbf{h}_{RP}\left(\mathbf{h}_{RP}^H \mathbf{h}_{RP}\right)\mathbf{h}_{RP}^H$ is the projection idempotent matrix with rank $(M-1)$, $\left(\mathbf{T}^{\perp}\right)^H \mathbf{T}^{\perp}$ is a Hermitian matrix with rank $(M-1)$. Based on [18, Theorem 2], $\mathbf{h}_{RD}^H \left(\mathbf{T}^{\perp}\right)^H \mathbf{T}^{\perp} \mathbf{h}_{RD}$ is a chi-square random variable with $2(M-1)$ degrees of freedom. Then, the CDF of $\gamma_2 = \left(P_R/\sigma_D^2\right)\left|\mathbf{T}^{\perp}\mathbf{h}_{RD}\right|^2 = \left(P_R\lambda_{RD}/\sigma_D^2\right)\mathbf{h}_{RD}^H\left(\mathbf{T}^{\perp}\right)^H \mathbf{T}^{\perp}\mathbf{h}_{RD}$ is given by

$$F_{\gamma_2}(\gamma) = 1 - \frac{1}{\Gamma(M-1)}\Gamma\left(M-1, \frac{\gamma}{\bar{\gamma}_2}\right) \tag{4}$$

where $\bar{\gamma}_2 = P_R\lambda_{RD}/\sigma_0^2$, $\Gamma(\cdot)$ is the gamma function [19, (8.310.1)], and $\Gamma(\cdot,\cdot)$ is the incomplete gamma function [19, (8.350.2)].

3 Secrecy performance analysis with single eavesdropper

In this section, we characterize secrecy performance of the multiple AF-relaying cooperative cognitive radio network with collaborative distributed beamforming in terms of the probability of non-zero secrecy capacity, the secrecy outage probability, the secrecy array gain, and the secrecy diversity order.

Based on (1) and (2), the instantaneous secrecy capacity of the considered network is given by [8]

$$C_S = \max\left\{\frac{1}{2}\log_2\left(1+\gamma_D^{AF}\right) - \frac{1}{2}\log_2\left(1+\gamma_E^{AF}\right), 0\right\} \tag{5}$$

Throughout this work, we focus on the passive eavesdropping scenario, where the secondary source does not have the channel information of the equivalent *S-R-E* link and has no choice but to encode the confidential data with a constant codeword rate $R_S > 0$, which is the target secrecy data rate for the considered system. If R_S is less than secrecy capacity, perfect secrecy can be guaranteed. Otherwise, E can eavesdrop on the confidential data; therefore, perfect secrecy is compromised.

3.1 The probability of non-zero secrecy capacity

In this subsection, we examine the condition for the existence of non-zero secrecy capacity. According to (5), the probability of non-zero secrecy capacity is formulated as

$$\Pr\{C_S > 0\} = \Pr\{\gamma_2 > \gamma_E\} = 1 - \int_0^{\infty} F_{\gamma_2}(\gamma) f_{\gamma_E}(\gamma)\, d\gamma \tag{6}$$

where the probability density function (PDF) of γ_E is $f_{\gamma_E}(\gamma) = \exp\left(-\gamma/\bar{\gamma}_E\right)/\bar{\gamma}_E$ and $\bar{\gamma}_E = P_R\lambda_{RE}/\sigma_0^2$.

Substituting (4) into (6) and using $\Gamma(n+1,x) = \Gamma(n+1)\exp(-x)\sum_{m=0}^{n}\frac{x^m}{\Gamma(m+1)}$, we can derive the closed-form expression of the probability of non-zero secrecy capacity with the aid of [19, 3.351.3] as

$$\begin{aligned}&\Pr\{C_S>0\}=\tfrac{1}{\Gamma(M-1)}\int_0^\infty\Gamma\left(M-1,\tfrac{\gamma}{\bar{\gamma}_2}\right)\exp\left(-\gamma/\bar{\gamma}_E\right)/\bar{\gamma}_E d\gamma\\&=\sum_{m=0}^{M-2}\tfrac{1}{\Gamma(m+1)\bar{\gamma}_E}\left(\tfrac{1}{\bar{\gamma}_2}\right)^m\int_0^\infty\gamma^m\exp\left(-\tfrac{\bar{\gamma}_2+\bar{\gamma}_E}{\bar{\gamma}_2\bar{\gamma}_E}\gamma\right)d\gamma\\&=\sum_{m=0}^{M-2}\tfrac{\bar{\gamma}_2}{\bar{\gamma}_E}\left(\tfrac{\bar{\gamma}_E}{\bar{\gamma}_2+\bar{\gamma}_E}\right)^{m+1}\end{aligned}\tag{7}$$

It is obvious that the probability of non-zero secrecy capacity is independent of the tolerable interference level I in the primary network, which is due to the fact that D-ZFB is employed to null the interference to PUs in the second phase.

3.2 Secrecy outage probability

The secrecy outage probability is defined as the probability of $C_S < R_S$ and can be expressed as

$$P_{\text{out}}=\Pr\left\{\tfrac{1}{2}\log_2\left(1+\gamma_D^{AF}\right)-\tfrac{1}{2}\log_2\left(1+\gamma_E^{AF}\right)<R_S\right\}\tag{8}$$

Substituting (1) and (2) into (8), the secrecy outage probability is rewritten as

$$P_{\text{out}}=\Pr\left\{\frac{1+\frac{\gamma_1\gamma_2}{\gamma_1+\gamma_2+1}}{1+\frac{\gamma_1\gamma_E}{\gamma_1+\gamma_E+1}}<\gamma_{th}\right\}\tag{9}$$

where $\gamma_{th}=2^{2R_S}$ denotes the secrecy SNR threshold.

Furthermore, in order to be mathematically tractable, we apply some approximations into (10) as follows

$$\begin{aligned}P_{\text{out}}&\overset{a}{\approx}\Pr\left\{\frac{\frac{\gamma_1\gamma_2}{\gamma_1+\gamma_2+1}}{\frac{\gamma_1\gamma_E}{\gamma_1+\gamma_E+1}}<\gamma_{th}\right\}\\&\overset{b}{\approx}\Pr\left\{\tfrac{(\gamma_1+\gamma_E)\gamma_2}{(\gamma_1+\gamma_2)\gamma_E}<\gamma_{th}\right\}\\&\overset{c}{\approx}\Pr\left\{\min\left(\tfrac{\gamma_1}{(\gamma_{th}-1)},\tfrac{\gamma_2}{\gamma_{th}}\right)<\gamma_E\right\}\end{aligned}\tag{10}$$

where we employ the approximations of $(1+x)/(1+y)\approx x/y$ in (a), $xy/(1+x+y)\approx xy/(x+y)$ in (b), and $\frac{xy}{x+y}\approx\min(x,y)$ in (c). These approximations have been used in [20, 21], and the effect of the approximation error can be neglected in the medium and high SNR regimes.

Let $Z=\min\left(\frac{\gamma_1}{(\gamma_{th}-1)},\frac{\gamma_2}{\gamma_{th}}\right)$, and the secrecy outage probability is further expressed as

$$P_{\text{out}}\approx\int_0^\infty\Pr\{Z<\gamma\}f_{\gamma_E}(\gamma)\,d\gamma\tag{11}$$

To solve the above integral, we first give the CDF of Z as follows:

$$\begin{aligned}&F_Z(\gamma)=\Pr\{Z<\gamma\}\\&=1-\left[1-F_{\gamma_1/(\gamma_{th}-1)}(\gamma)\right]\left[1-F_{\gamma_2/\gamma_{th}}(\gamma)\right]\\&=\sum_{k=1}^{M}\sum_{m=0}^{M-2}\tbinom{M}{k}\tfrac{(-1)^k}{\Gamma(m+1)}\left(\tfrac{\gamma_{th}\gamma}{\bar{\gamma}_2}\right)^m\left[1+\tfrac{(\gamma_{th}-1)\gamma}{\bar{\gamma}_1}\right]^{-k}\exp\left(-\tfrac{\gamma_{th}\gamma}{\bar{\gamma}_2}\right)\end{aligned}\tag{12}$$

Now, substituting (12) into (11), and using $\left(\frac{x}{\alpha+x}\right)^M=\sum_{k=0}^{M}\binom{M}{k}(-1)^k\left(1+\frac{x}{\alpha}\right)^{-k}$, the secrecy outage probability is given by

$$\begin{aligned}P_{\text{out}}&\approx1+\tfrac{1}{\bar{\gamma}_E}\sum_{k=1}^{M}\sum_{m=0}^{M-2}\tbinom{M}{k}\tfrac{(-1)^k}{\Gamma(m+1)}\left(\tfrac{\gamma_{th}}{\bar{\gamma}_2}\right)^m\\&\times\int_0^\infty\left(1+\tfrac{(\gamma_{th}-1)\gamma}{\bar{\gamma}_1}\right)^{-k}\gamma^m\exp\left(-\left(\tfrac{\gamma_{th}}{\bar{\gamma}_2}+\tfrac{1}{\bar{\gamma}_E}\right)\gamma\right)d\gamma\end{aligned}\tag{13}$$

Then, with the help of [19, (9.222.1)], the approximated expressions of the secrecy outage probability can be derived as

$$\begin{aligned}P_{\text{out}}&\approx1+\tfrac{1}{\bar{\gamma}_E}\sum_{k=1}^{M}\sum_{m=0}^{M-2}\tbinom{M}{k}(-1)^k\left(\tfrac{\gamma_{th}}{\bar{\gamma}_2}\right)^m\\&\times\tfrac{\alpha^{(m+k)/2}}{\beta^{(m-k)/2+1}}\exp\left(\alpha\beta/2\right)W_{-(k+m)/2,(m-k)/2+0.5}(\alpha\beta)\end{aligned}\tag{14}$$

where $\alpha=\bar{\gamma}_1/(\gamma_{th}-1)$, $\beta=\gamma_{th}/\bar{\gamma}_2+1/\bar{\gamma}_E$ and $W_{m,n}(x)$ is the Whittaker function [19, (9.222.1)]. It is noted from (14) that the secrecy outage probability expression is derived in closed form and can be easily applied to evaluate the secrecy performance with arbitrary numbers of relays, arbitrary average SNRs, and arbitrary interference constraint level.

3.3 Asymptotic secrecy outage probability

In this subsection, in order to exploit a novel insight of design, the asymptotic analysis for the secrecy outage probability was provided to characterize the behavior under the high SNR of legitimate links. The asymptotic result enables us to explicitly examine the impact of collaborative distributed beamforming on the secrecy performance in terms of the secrecy diversity order. Without loss of generation, let $\lambda_{SR}=\lambda_{RD}=\lambda\to\infty$, namely $\bar{\gamma}_2=\kappa\bar{\gamma}_1=\bar{\gamma}\to\infty$, where $\kappa=P_R\lambda_{SP}/I$. Here, $\bar{\gamma}\to\infty$ corresponds to the scenario where the relays have high received SNRs at the first phase and the secondary destination are located much closer to the relays than the eavesdropper, which is a practical scenario of interest. It is obvious that $\bar{\gamma}/\bar{\gamma}_E=\lambda/\lambda_{RE}\to\infty$ for a given $\bar{\gamma}_E$ when $\bar{\gamma}\to\infty$. Similar to [7], we denote $MER=\lambda_{SD}/\lambda_{RE}$ as the ratio of average channel gain from the relays to the secondary destination to that from the relays to the eavesdropper.

With the aid of the Maclaurin series expansion [19, (1.211.1)], we can rewrite (12) as

$$F_Z^{\infty}(\gamma) \overset{\bar{\gamma}\to\infty}{=} \frac{1}{\Gamma(M)}\left(\frac{\gamma_{th}\gamma}{\bar{\gamma}}\right)^{M-1} + o\left(\frac{\gamma}{\bar{\gamma}}\right) \tag{15}$$

where $o(\cdot)$ denotes higher order terms.

Substituting (15) and the PDF of $\gamma_E f_{\gamma_E}$ into (11), and using [19, (3.351.3)], the asymptotic secrecy outage probability is calculated as

$$\begin{aligned} P_{\text{out}}^{\infty} &= \int_0^{\infty} \frac{1}{\Gamma(M)}\left(\frac{\gamma_{th}\gamma}{\bar{\gamma}}\right)^{M-1} \frac{1}{\bar{\gamma}_E}\exp\left(-\frac{\gamma}{\bar{\gamma}_E}\right) d\gamma \\ &= \gamma_{th}^{M-1} MER^{-(M-1)} \end{aligned} \tag{16}$$

Obviously, one can observe from (16) that the secrecy outage probability behaves as $MER^{-(M-1)}$ for $MER \to \infty$. Thus, the achievable secrecy diversity order of the proposed collaborative distributed beamforming yields to

$$d_{\text{single}} = M - 1, \tag{17}$$

and the achievable secrecy array gain is given by

$$\Theta_{\text{single}} = \gamma_{th}^{-1} \tag{18}$$

which implies that as the number of relays increases, the slope of the secrecy outage probability curve becomes steeper when $MER \to \infty$ in the geometric sense. Therefore, collaborative distributed beamforming can effectively improve the physical layer security of cognitive transmission to defend against eavesdropping attacks. However, comparing with the relay selection scheme in [11] and [13], the proposed collaborative distributed beamforming scheme cannot achieve the full diversity order, i.e., $d = M$. This is because the proposed collaborative distributed beamforming scheme allocates the power into the projected channels to enforce zero interference to the PUs, which reduces the achievable secrecy diversity order to $M - 1$.

4 Secrecy performance with multiple eavesdroppers

In this section, we extend our cooperative cognitive system model to K non-colluding eavesdroppers, as shown in Fig. 2. We assume that all the eavesdroppers are located close to each other, which implies the same average received SNR at eavesdroppers. We denote $\mathbf{h}_{RE_k} = \left[h_{R_1E_k}, \cdots, h_{R_ME_k}\right]^T$ as the channel vector between the relays and the kth eavesdropper. Then, the equivalent instantaneous SNR between the relays and the kth eavesdropper can be denoted by $\gamma_{E_k} = \left(P_R/\sigma_0^2\right)\left|\mathbf{h}_{RE_k}^H \mathbf{w}_{ZF}\right|^2$, which is exponentially distributed with the same parameter $\bar{\gamma}_E$.

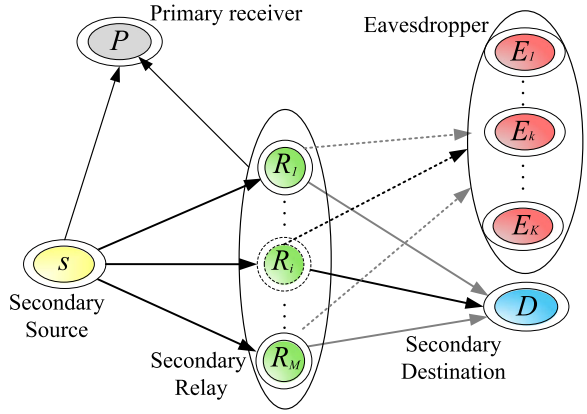

Fig. 2 Cooperative cognitive radio network with K eavesdroppers

Under this scenario, the instantaneous secrecy capacity should be rewritten as

$$\begin{aligned} C_S^K = \max\Bigg\{&\tfrac{1}{2}\log_2\left(1 + \frac{\gamma_1\gamma_2}{\gamma_1+\gamma_2+1}\right) \\ &- \max_{k=1,\cdots,K}\left(\tfrac{1}{2}\log_2\left(1 + \frac{\gamma_1\gamma_{E_k}}{\gamma_1+\gamma_{E_k}+1}\right)\right), 0\Bigg\} \end{aligned} \tag{19}$$

Similar to (6), the probability of non-zero secrecy capacity with K non-colluding eavesdroppers can be formulated as

$$\begin{aligned} \Pr\left\{C_S^K > 0\right\} &= \Pr\left\{\gamma_2 > \max_{k=1,\cdots,K}\gamma_{E_k}\right\} \\ &= 1 - \int_0^{\infty} F_{\gamma_2}(\gamma) f_{\gamma_E^K}(\gamma)\, d\gamma \end{aligned} \tag{20}$$

where $f_{\gamma_E^K}(\gamma)$ denotes the PDF of $\gamma_E^K = \max_{k=1,\cdots,K}\gamma_{E_k}$.

Considering that $\gamma_{E_k}, k = 1, \cdots, K$ are i.i.d exponential distribution variables, the CDF and PDF of γ_E^K can be expressed as

$$F_{\gamma_E^K}(\gamma) = \sum_{K=0}^{K}\binom{K}{k}(-1)^k \exp\left(-\frac{k\gamma}{\bar{\gamma}_E}\right) \tag{21}$$

and

$$f_{\gamma_E^K}(\gamma) = \sum_{K=0}^{K-1}\binom{K-1}{k}\frac{K}{\bar{\gamma}_E}(-1)^k \exp\left(-\frac{(k+1)\gamma}{\bar{\gamma}_E}\right) \tag{22}$$

Substituting (4) and (22) into (20), the probability of non-zero secrecy capacity with K non-colluding eavesdroppers can be derived as

$$\Pr\{C_S > 0\} = \sum_{m=0}^{M-2}\sum_{k=0}^{K-1}\binom{K-1}{k}(-1)^k \frac{K\bar{\gamma}_2}{\bar{\gamma}_E}\left[\frac{\bar{\gamma}_E}{(k+1)\bar{\gamma}_2 + \bar{\gamma}_E}\right]^{m+1} \tag{23}$$

Similarly, the secrecy outage probability with K non-colluding eavesdroppers is further expressed as

$$\begin{aligned}
P_{\text{out}}^{K} &\approx \int_0^\infty \Pr\{Z<\gamma\} f_{\gamma_E^K}(\gamma)\, d\gamma \\
&= 1+\sum_{l=1}^{M}\sum_{m=0}^{M-2}\sum_{k=0}^{K-1}\binom{K-1}{k}\binom{M}{1}\frac{K(-1)^{k+l}}{\Gamma(m+1)\bar{\gamma}_E}\left(\frac{\gamma_{th}}{\bar{\gamma}_2}\right)^m \\
&\quad\times\int_0^\infty\left(1+\tfrac{\gamma}{\alpha}\right)^{-l}\gamma^m\exp\left(-\left(\frac{\gamma_{th}}{\bar{\gamma}_2}+\frac{(k+1)}{\bar{\gamma}_E}\right)\gamma\right)d\gamma \\
&\overset{t=\gamma/\alpha}{=} 1+\sum_{l=1}^{M}\sum_{m=0}^{M-2}\sum_{k=0}^{K-1}\binom{K-1}{k}\binom{M}{1}\frac{K(-1)^{k+l}\alpha^{m+1}}{\Gamma(m+1)\bar{\gamma}_E}\left(\frac{\gamma_{th}}{\bar{\gamma}_2}\right)^m \\
&\quad\times\int_0^\infty(1+t)^{-l}t^m\exp(-\eta\alpha t)\,dt \\
&= 1+\sum_{l=1}^{M}\sum_{m=0}^{M-2}\sum_{k=0}^{K-1}\binom{K-1}{k}\binom{M}{1}\frac{K(-1)^{k+l}}{\bar{\gamma}_E}\left(\frac{\gamma_{th}}{\bar{\gamma}_2}\right)^m \\
&\quad\times\frac{\alpha^{(m+l)/2}}{\eta^{(m-l)/2+1}}\exp\left(\alpha\eta/2\right)W_{-(m+l)/2,(m-l)/2+0.5}(\alpha\eta)
\end{aligned} \tag{24}$$

where $\eta=\gamma_{th}/\bar{\gamma}_2+(k+1)/\bar{\gamma}_E$.

The asymptotic secrecy outage probability with K non-colluding eavesdroppers can be derived as

$$\begin{aligned}
P_{\text{out}}^{K,\infty} &\approx \sum_{K=0}^{K-1}\binom{K-1}{k}\frac{K}{\bar{\gamma}_E}(-1)^k\frac{1}{\Gamma(M)}\left(\frac{\gamma_{th}}{\bar{\gamma}_2}\right)^{M-1} \\
&\quad\times\int_0^\infty\gamma^{M-1}\exp\left(-\tfrac{(k+1)\gamma}{\bar{\gamma}_E}\right)d\gamma \\
&= \left[\sum_{k=0}^{K-1}\binom{K-1}{k}(-1)^k K(k+1)^{-M}\gamma_{th}^{M-1}\right]MER^{-(M-1)}
\end{aligned} \tag{25}$$

It is clear that the achievable secrecy diversity order in the presence of K non-colluding eavesdroppers is still $M-1$, which means that the secrecy diversity performance is independent of the number of eavesdroppers. However, the achievable secrecy array gain is different due to the presence of multiple non-colluding eavesdroppers, which can be yielded as

$$\Theta_{\text{multiple}}=\left[\sum_{k=0}^{K-1}\binom{K-1}{k}(-1)^k K(k+1)^{-M}\right]^{-1/(M-1)}\gamma_{th}^{-1} \tag{26}$$

It is indicated from (18) and (26) that the achievable secrecy array gain decreases with increasing K, which results in a decrease in the secrecy outage performance.

5 Numerical and simulation results

In this section, Monte Carlo simulations are provided to validate our analytical expressions over Rayleigh-fading channels. We assume that $R_s=0.1$ bit/s/Hz, $P_R=20$ dB, $\sigma_0^2=1$, $\lambda_{SR}=\lambda_{RD}=1$, and $\lambda_{SP}=\lambda_{RP}=0.3$. It is worth noting that the primary and secondary users are spatially separated in two different wireless networks. As such, an average channel gain (λ_{SP} and λ_{RP}) between two heterogeneous users from the different networks is set to be smaller than that (λ_{SR} and λ_{RD}) between two heterogeneous users from the same networks.

Figure 3 plots the secrecy outage probability versus I for various M over Rayleigh-fading channels. The analytical results based on (14) are in precise agreement with the Monte Carlo simulations. It is shown that for a fixed M, the secrecy outage probability decreases with increasing I, which increases the transmitting power at the secondary source and improves the transmission reliability of S-R links. We can also see that there exists a secrecy outage performance floor in the high I region. It is because the secrecy outage performance is determined by second hop links when $I\to\infty$. On the other hand, the secrecy outage performance is improved with larger M, as more relays do not only help improve the communication quality of S-R links but also enhance security of R-D links. As shown in Fig. 3, as the number of relays increases from $M=3$ to 5, the secrecy outage performance floor is significantly reduced.

Figures 4 and 5 plot the secrecy outage probability and the probability of non-zero secrecy capacity versus *MER* for various M in the presence of a single eavesdropper. The exact curves precisely agree with the Monte Carlo simulation results, which validates the correctness of our analysis. As shown in the figures, as the number of relays increases from $M=2$ to 5, the secrecy outage probability and the probability of non-zero secrecy capacity are significantly improved. The reason is that more relays do not only help improve the communication quality of S-R links but also enhance the security of the R-D links. In order to predict the secrecy diversity order and the secrecy array gain, the asymptotic secrecy outage probability curves based on (16) are also drawn in Fig. 5. We can see that the asymptotic curves well approximate the analytical curves in the high *MER* region, which verifies

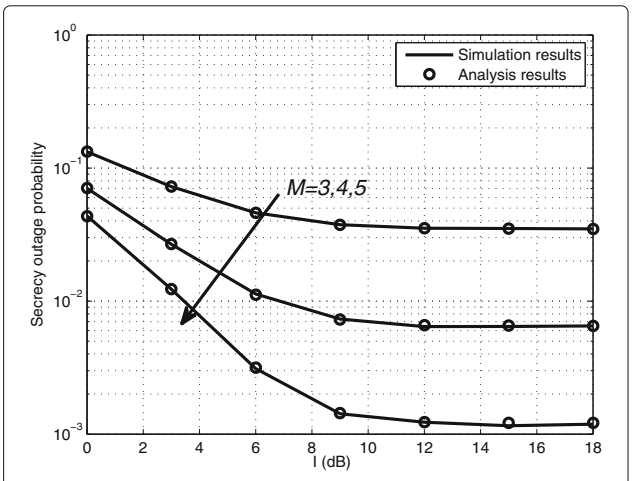

Fig. 3 Secrecy outage probability versus *MER* for various I ($\lambda_{RE}=0.2$)

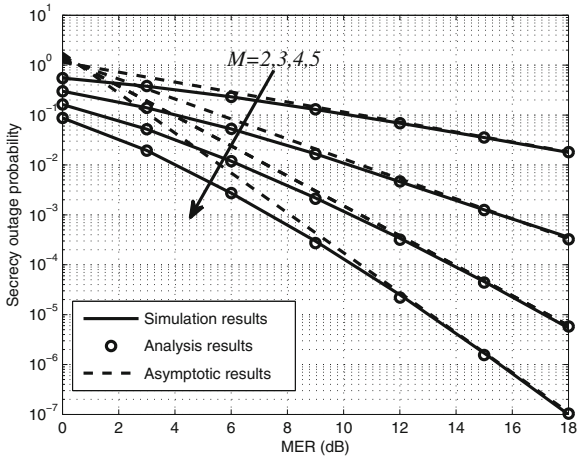

Fig. 4 Secrecy outage probability versus *MER* for various *M* ($K = 1$ and $I = 10$ dB)

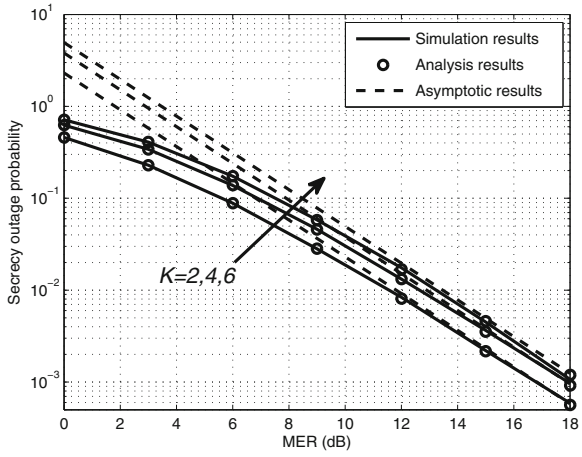

Fig. 6 Secrecy outage probability versus *MER* for various *K* ($M = 3$ and $I = 10$ dB)

the derived asymptotic expressions. As $MER \to \infty$, the secrecy outage probability decreases at a faster speed with an increasing number of relays M. This is because the achievable secrecy diversity order is $M - 1$.

Figures 6 and 7 plot the secrecy outage probability and the probability of non-zero secrecy capacity versus *MER* in the presence of K non-colluding eavesdroppers ($M = 3$ and $I = 10$ dB). As observed from the figure, we can find that for different values of *MER* and K, the analytical results match well the simulation. In addition, the asymptotic secrecy outage probability curves based on (25) converge exactly in the high *MER* region in Fig. 6. Moreover, the slopes of the curves of the secrecy outage probability are in parallel, which verifies the secrecy diversity order of $M - 1$ regardless of the number of eavesdroppers K. From Fig. 7, it is evident that the probability of non-zero secrecy capacity improves with increasing *MER*. In addition, the probability of non-zero secrecy capacity improves at a faster speed with smaller K.

6 Conclusions

In this paper, we have investigated the security performance of multiple AF-relaying CCRNs with collaborative distributed beamforming scheme against passive eavesdropping attacks. To show the advantages of the collaborative distributed beamforming scheme, we have derived closed-form expressions of the probability of non-zero secrecy capacity and secrecy outage probability as well as the asymptotic expression over Rayleigh-fading channels, which provide an efficient means to evaluate the impact of key parameters on the security performance. Moreover,

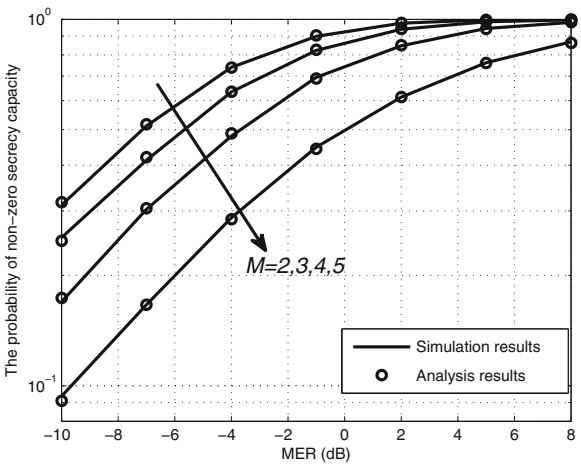

Fig. 5 Probability of non-zero secrecy capacity versus *MER* for various *M* ($K = 1$ and $I = 10$ dB)

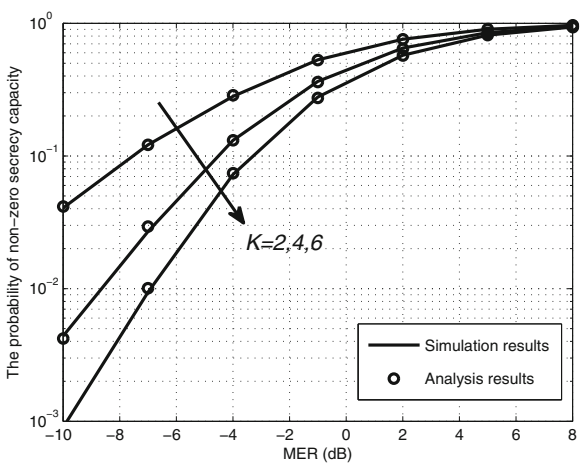

Fig. 7 Probability of non-zero secrecy capacity versus *MER* for various *K* ($M = 3$ and $I = 10$ dB)

our asymptotic results demonstrated that the achievable secrecy diversity order of collaborative distributed beamforming with M AF relays is $M - 1$ regardless of the number of eavesdroppers.

Acknowledgements
This work is supported by the National Natural Science Foundation of China (No. 61471393 and 61501507) and the Jiangsu Provincial Natural Science Foundation of China (No. BK20150719) and the China Postdoctoral Science Foundation under a Special Financial (No. 2013T60912).

Competing interests
The authors declare that they have no competing interests.

Publisher's Note

Received: 10 October 2016 Accepted: 28 July 2017
Published online: 29 August 2017

References

1. D Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1367 (1975)
2. A Jovicic, P Viswanath, Cognitive radio: an information-theoretic perspective. IEEE Trans. Inf. Theory. **55**(9), 3945–3958 (2009)
3. X Chen, H-H Chen, W Meng, Cooperative communication for cognitive radio networks—from theory to application. IEEE Commun. Surv. Tutor. **16**(3), 1180–1192 (2014)
4. Z Shu, Y Qian, S Ci, On physical layer security for cognitive radio networks. IEEE Netw. **27**(3), 28–33 (2013)
5. C Tang, G Pan, T Li, Secrecy outage analysis of underlay cognitive radio unit over Nakagami-m fading channels. IEEE Wirel. Commun. Lett. **3**(6), 609–612 (2014)
6. Y Pei, Y-C Liang, L Zhang, KC Teh, KH Li, Secure communication over MISO cognitive radio channels. IEEE Trans. Wirel. Commun. **9**(4), 1494–1502 (2010)
7. Y Zou, X Li, Y-C Liang, Secrecy outage and diversity analysis of cognitive radio systems. IEEE J. Sel. Areas Commun. **32**(11), 2222–2236 (2014)
8. M Elkashlan, L Wang, TQ Duong, GK Karagiannidis, A Nallanathan, On the security of cognitive radio networks. IEEE Trans. Veh. Techol. **64**(8), 3790–3795 (2015)
9. H Lei, H Zhang, IS Ansari, C Gao, Y Guo, G Pan, KA Qaraqe, Secrecy outage performance for SIMO underlay cognitive radio systems with generalized selection combining over Nakagami-m channels. IEEE Trans. Veh. Techol. **65**(12), 10126–10132 (2016)
10. H Zhao, Y Tan, G Pan, Y Chen, N Yang, Secrecy outage on transmit antenna selection/maximal ratio combining in MIMO cognitive radio networks. IEEE Trans. Veh. Techol. **65**(12), 10236–10242 (2016)
11. Y Zou, J Zhu, L Yang, Y-C Liang, Y-D Yao, Securing physical layer communications for cognitive radio networks. IEEE Commun. Mag. **53**(9), 48–54 (2015)
12. W Yang, X Xu, Y Cai, in *IEEE WCNC 2014*. Secrecy outage analysis for DF underlay CRNs with outdate CSI (Wireless Communications and Networking Conference (WCNC), 2014 IEEE, Istanbul, 2014)
13. Y Liu, L Wang, TT Duy, M Elkashlan, TQ Duong, Relay selection for security enhancement in cognitive relay networks. IEEE Wirel. Commun. Lett. **4**(1), 46–49 (2015)
14. Y Zou, B Champagne, W-P Zhu, L Hanzo, Relay-selection improves the security-reliability trade-off in cognitive radio systems. IEEE Trans. Commun. **63**(1), 215–228 (2015)
15. Q Gu, G Wang, L Gao, M Peng, Security-reliability performance of cognitive AF relay-based wireless communication system with channel estimation error. EURASIP J. Adv. Signal Process. **2014**, 1–11 (2015)
16. W Yang, K Wang, X Xu, J Zhou, in *WOCC 2016*. Secure transmission for AF relaying spectrum-sharing systems with collaborative distributed beamforming (Wireless and Optical Communication Conference (WOCC), 2016 25th, Chengdu, 2016)
17. A Afana, V Asghari, A Ghrayeb, S Affes, On the performance of cooperative relaying spectrum-sharing system with collaborative distributed beamforming. IEEE Trans. Commun. **62**(3), 857–871 (2014)
18. RJ Pavur, Quadratic forms involving the complex Gaussian. M.Sc. dissertation, Math. Dept., Texas Tech Univ.Lubbock, TX, (1980)
19. IS Gradshteyn, IM Ryzhik, *Table of integrals, series, and products*, sixth ed. (Academic Press, London, 2000)
20. I Krikidis, Opportunistic relay selection for cooperative networks with secrecy constraints. IET Commun. **4**(15), 1787–1791 (2010)
21. A Behnad, X Wang, Accuracy of harmonic mean approximation in performance analysis of multihop amplify-and-forward relaying. IEEE Wirel. Commun. Lett. **3**(2), 125–128 (2014)