Wireless Personal Communications (2018) 103:2957–2976
https://doi.org/10.1007/s11277-018-5987-8

Secure Relay Selection of Cognitive Two-Way Denoise-and-Forward Relaying Networks

Ruifeng Gao[1,2] · **Xiaodong Ji**[1] · **Zhihua Bao**[1]

Published online: 26 October 2018

Abstract

In this paper, secrecy performance of a cognitive two-way denoise-and-forward relaying network consisting of two primary user (*PT* and *PD*) nodes, two secondary source (*SA* and *SB*) nodes, multiple secondary relay (SR_i) nodes and an eavesdropper (*E*) node is considered, where *SA* and *SB* exchange their messages with the help of one of the relays using a two-way relaying scheme. The eavesdropper tries to wiretap the information transmitted between *SA* and *SB*. To improve secrecy performance of the network, two relay selection schemes called maximum sum rate and maximum secrecy capacity based relay selection (MSRRS and MSCRS) are proposed and analyzed in terms of intercept probability. It is proved that the MSRRS and MSCRS schemes have the same secrecy performance. Two parameters called average number gain and average cost gain are proposed to show the performance of the proposed relay selection schemes. Numerical results demonstrated that with 10 relay nodes, the proposed relay selection schemes can achieve, respectively, 3.7 dB and 1.9 dB's improvements in terms of the reduced intercept probability and the enhanced secrecy capacity compared to the traditional round-robin scheme.

Keywords Two-way relaying · Physical layer security · Cognitive wireless network · Relayselection · Denoise-and-forward relay · Intercept probability

1 Introduction

Cognitive radio (CR) has received much attention from the research community due to its improvement of spectrum utilization efficiency of wireless networks [1–3]. Generally, for a CR network, there exists two classes of users, namely, licensed and unlicensed (also called

✉ Zhihua Bao
bao.zh@ntu.edu.cn

Ruifeng Gao
grf@ntu.edu.cn

Xiaodong Ji
jxd@ntu.edu.cn

[1] School of Electronics and Information, Nantong University, Nantong 226019, China

[2] School of Transportation, Nantong University, Nantong 226019, China

primary and secondary) users using two types of spectrum sharing methods: overlay and underlay approaches. For the overlay approach, secondary users directly access the primary users' spectrum when the primary users are in the idle status. For the underlay approach, however, secondary users can utilize the primary users' spectrum without deteriorating the quality of service of the primary users. On the other hand, cooperative relay technologies can resist fading and path loss effects and have received much attention as well.

Physical-layer security is an emerging technique being able to secure the open communication environment against eavesdropping attacks at the physical layer [4]. Wyner proposed the wiretap channel model and studied its information-theoretic security in [5]. Leung-Yan-Cheong and Hellman [6] extended Wyner's work to the Guassian wiretap channel. Dong et al. [7] addressed the secure transmission issues by using cooperative relaying techniques, where different cooperative relaying protocols are considered, i.e., decode-and-forward (DF), amplify-and-forward (AF), and cooperative jamming (CJ). By using AF and DF relaying, Zou et al. [8] proposed an optimal relay selection scheme for physical-layer security. Chen et al. [9] and Zhao et al. [10] investigated the physical-layer security problem in the two-way relaying systems and proposed an effective relaying technology that can improve both the spectrum efficiency and the throughput simultaneously. Wang et al. [11] proposed a jammer selection scheme to enhance the secrecy performance of an DF two-way relaying network. Ding et al. [12] studied opportunistic relay selection scheme for the physical-layer security of artificial noise aided DF two-way relaying network.

However, most of the existing works regarding physical-layer security of two-way relaying do not consider cognitive radio settings. It is worth-mentioning that due to the interference between primary and secondary users, investigating secure techniques at the physical layer for a CR network becomes much more difficult. Zhang and Gursoy [13] studied secure communication in cognitive two-way relaying networks by using multi-relays beamforming designs. The authors of [14] investigated a new cooperative paradigm to provide information security for the primary network in cognitive two-way relaying networks. In [15], a joint resource allocation and relay selection scheme is proposed to secure the communication of CR networks via DF relays. Zhao et al. [16] investigated the physical-layer security problem of cognitive DF relay networks over Nakagami-*m* fading channels. Different from [13–16], we investigate secure techniques of secondary users for a two-way CR network by using denoise-and forward (DNF) relaying. It should be noted that, unlike DF relay, the DNF relay only detects and re-modulates the XOR of the two sources transmitted bits [17–19], and can result in more throughput than that of AF and DF relaying under low signal-noise-ratio (SNR) regime [20]. Table 1 gives a summarized comparison between the existing works and our work.

The network considered in this paper consists of two primary users (*PT* and *PD*), two secondary sources (*SA* and *SB*) and multiple secondary relays (SR_i) in the present of an eavesdropper (*E*). In the network, the secondary users transmit only when they detect a

Table 1 Existing works regarding physical-layer security of two-way relaying networks

Relaying protocol	Multiple relay selection	Secure beamforming	Cooperative jamming	In cognitive radio networks
AF	[9]	[10, 13]	[9, 14]	[13, 14]
DF	[11, 12, 15, 16]	–	[11, 12]	[15, 16]
DNF	This work	–	–	This work

spectrum hole. First, we propose two relay selection schemes called maximum secrecy capacity relay selection (MSCRS) and maximum sum rate relay selection (MSRRS) schemes. Second, closed-form expressions of intercept probability of the two proposed relay selection schemes are derived, where the missed detection of spectrum hole is considered. Moreover, we propose two parameters called ANG and ACG to show the performance of the proposed relay selection schemes. Our simulation results confirmed the efficiency of our propositions.

This paper is organized as follows. The system model under investigation is presented in Sect. 2. In Sect. 3, the intercept probabilities of the proposed MSCRS and MSRRS schemes as well as the traditional round-robin scheme are derived. ANG and ACG parameters are introduced in Sect. 4. The numerical results are presented in Sect. 5. Section 6 concludes the paper.

2 System Model

As shown in Fig. 1, the considered CTWDNFR network consists of two primary users PT and PD, two secondary users SA and SB, N relay nodes SR_i, $i \in \{1, 2, \dots, N\}$, and one eavesdropper E. For spectrum sharing, the overlay approach is employed. The two secondary users SA and SB use the two-way relaying scheme to exchange messages with each other. There are two time-slots in one round of transmission between SA and SB. In the first time-slot, SA and SB transmit their messages x_A and x_B to N relays, and then the selected relay uses the DNF protocol to decode the message into x_R, which is combined with x_A and x_B. In the second time-slot, the relay forwards x_R to SA and SB. During the first and the second time-slots, E aims to wiretap SA, SB and the relay's signals. Let x_P denote the signal transmitted by primary user PT. Without loss of generality, $E\left[\left|x_A\right|^2\right] = E\left[\left|x_B\right|^2\right] = E\left[\left|x_P\right|^2\right] = 1$ is assumed.

Suppose that there is no direct link between SA and SB because of deep channel fading. Furthermore, all the relays cannot communicate with each other. We use "H−L" to denote channel link from node H to L, where $H, L \in \left\{SA, SB, SR_i, PT, E\right\}$. The instantaneous

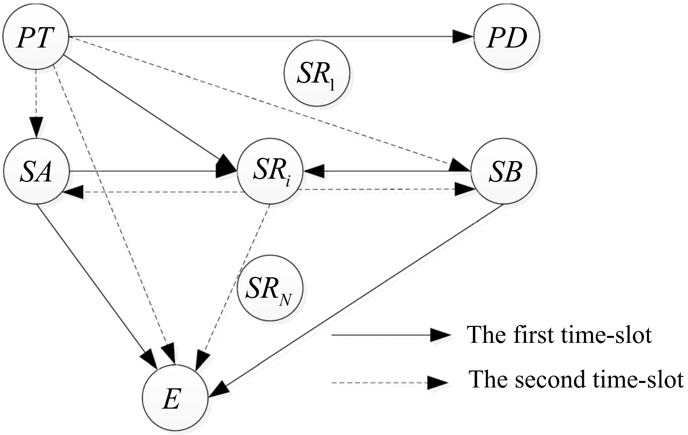

Fig. 1 System model

channel gain of link $H-L$ is denoted by h_{HL} and assumed to be zero mean complex Gaussian random variables with variance σ_{HL}^{2}. All the channels are assumed to undergo Rayleigh fading and to be independent and reciprocal. Thus, we have $h_{HL} = h_{LH}$. Let P_S denote the transmit power of SA, SB and SR_i, and P_P denote the transmit power of PT. Meanwhile, let N_0 denote the variance of the zero mean additive white Gaussian noise at all the receiving nodes. Furthermore, $E\left[P_S\left|h_{SBSR_i}\right|^2/N_0\right] = E\left[P_S\left|h_{SASR_i}\right|^2/N_0\right] = 1/\lambda_S$, $E\left[P_P\left|h_{PTSR_i}\right|^2/N_0\right] = E\left[P_P\left|h_{PTSA}\right|^2/N_0\right] = E\left[P_P\left|h_{PTSB}\right|^2/N_0\right] = E\left[P_P\left|h_{PTE}\right|^2/N_0\right] = 1/\lambda_P$ and $E\left[P_S\left|h_{SAE}\right|^2/N_0\right] = E\left[P_S\left|h_{SBE}\right|^2/N_0\right] = 1/\lambda_E$ are assumed. Let R_A and R_B denote the transmission rate of source SA and SB, respectively, and $R_A = R_B = R$ is assumed.

In this paper, SA and SB exchange their messages only when they detect a spectrum hole. Let $\hat{H}$ denote the result of spectrum detection, where $\hat{H} = H_0$ indicates that the licensed spectrum is unoccupied, while $\hat{H} = H_1$ represents the case that licensed spectrum is used. Moreover, $P_d = \Pr\left(\hat{H} = H_0 | H_0\right)$ and $P_f = \Pr\left(\hat{H} = H_0 | H_1\right)$ are used to denote the probabilities of correct detection and missed detection, respectively.

For the case of $\hat{H} = H_0$, SA and SB exchange messages via the selected relay SR_i. Thus, at the end of the first time-slot, the signal received at SR_i can be expressed as:

$$y_{SR_i}^{1\mathrm{st}} = \sqrt{P_S}h_{SASR_i}x_A + \sqrt{P_S}h_{SBSR_i}x_B + \sqrt{\alpha P_P}h_{PTSR_i}x_P + n_{R_i} \tag{1}$$

where $\alpha = \begin{cases} 0, & H_0 \\ 1, & H_1 \end{cases}$, n_{R_i} is the additive white Gaussian noise at the relay SR_i.

Here, the two sources' transmission rate R should follow the bellowing constraints.

$$\begin{aligned} R &\leqslant Ca\left(SNR_{SASR_i}^{1\mathrm{st}}\right) \\ R &\leqslant Ca\left(SNR_{SBSR_i}^{1\mathrm{st}}\right) \\ R &\leqslant \frac{1}{2}Ca\left(SNR_{SR_i}^{1\mathrm{st}}\right) \end{aligned} \tag{2}$$

where $Ca(x) = \frac{1}{2}\log_2(1+x)$, $SNR_{SASR_i}^{1\mathrm{st}} = \frac{\gamma_S\left|h_{SASR_i}\right|^2}{\alpha\gamma_P\left|h_{PTSR_i}\right|^2+1}$, $SNR_{SBSR_i}^{1\mathrm{st}} = \frac{\gamma_S\left|h_{SBSR_i}\right|^2}{\alpha\gamma_P\left|h_{PTSR_i}\right|^2+1}$, $SNR_{SR_i}^{1\mathrm{st}} = \frac{\gamma_S\left|h_{SBSR_i}\right|^2+\gamma_S\left|h_{SASR_i}\right|^2}{\alpha\gamma_P\left|h_{PTSR_i}\right|^2+1}$, $\gamma_S = \frac{P_S}{N_0}$, $\gamma_P = \frac{P_P}{N_0}$.

At the end of the first time-slot, the signal received at E can be expressed as:

$$y_E^{1\mathrm{st}} = \sqrt{P_S}h_{SAE}x_A + \sqrt{P_S}h_{SBE}x_B + \sqrt{\alpha P_P}h_{PTE}x_P + n_E \tag{3}$$

Thus, the maximum information that E obtains can be expressed as

$$I_{E-i}^{1\mathrm{st}} = \max\left(Ca\left(SNR_{SAE}\right), Ca\left(SNR_{SBE}\right)\right) \tag{4}$$

where $SNR_{SAE} = \frac{\gamma_S\left|h_{SAE}\right|^2}{\gamma_S\left|h_{SBE}\right|^2+\alpha\gamma_P\left|h_{PTE}\right|^2+1}$, and $SNR_{SBE} = \frac{\gamma_S\left|h_{SBE}\right|^2}{\gamma_S\left|h_{SAE}\right|^2+\alpha\gamma_P\left|h_{PTE}\right|^2+1}$.

In the second time-slot, SR_i forwards x_R to SA and SB, and the signal received at SA, SB and E can be, respectively, expressed as:

$$y_A^{\text{2nd}} = \sqrt{P_S} h_{SASR_i} x_R + \sqrt{\alpha P_P} h_{PTSA} x_P + n_A \tag{5}$$

$$y_B^{\text{2nd}} = \sqrt{P_S} h_{SBSR_i} x_R + \sqrt{\alpha P_P} h_{PTSB} x_P + n_B \tag{6}$$

$$y_E^{\text{2nd}} = \sqrt{P_S} h_{ESR_i} x_R + \sqrt{\alpha P_P} h_{PTE} x_P + n_E \tag{7}$$

From (5) and (6), *SA* and *SB* use their self-information being transmitted to the relay in the first time-slot to decode x_R. Thus, *R* should follow the bellowing constraints.

$$\begin{aligned} R &\leqslant Ca\left(SNR_{SR_iSA}^{\text{2nd}}\right) \\ R &\leqslant Ca\left(SNR_{SR_iSB}^{\text{2nd}}\right) \end{aligned} \tag{8}$$

where $SNR_{SR_iSA}^{\text{2nd}} = \frac{\gamma_S |h_{SASR_i}|^2}{\alpha\gamma_P |h_{PTSA}|^2 + 1}$, $SNR_{SR_iSB}^{\text{2nd}} = \frac{\gamma_S |h_{SBSR_i}|^2}{\alpha\gamma_P |h_{PTSB}|^2 + 1}$.

From (2) and (8), the maximum value of *R* is given by.

$$\begin{aligned} R_{DNF-i} = \min\Big(& Ca\left(SNR_{SASR_i}^{\text{1st}}\right), Ca\left(SNR_{SBSR_i}^{\text{1st}}\right), \frac{1}{2}Ca\left(SNR_{SR_i}^{\text{1st}}\right), \\ & Ca\left(SNR_{SR_iSA}^{\text{2nd}}\right), Ca\left(SNR_{SR_iSB}^{\text{2nd}}\right)\Big) \end{aligned} \tag{9}$$

It is worth-mentioning that, the eavesdropper *E* can decode x_A or x_B from x_R only when *E* has intercepted x_A or x_B in the first time-slot, meaning that *E* cannot intercept any information from the signal x_R if the $SA - SR_i$ and $SB - SR_i$ transmission in the first time-slot are kept secrecy.

3 Relay Selection Schemes and Intercept Probability Analysis

Here, we study two relay selection schemes called MSRRS and MSCRS schemes in addition to the traditional round-robin scheme.

3.1 MSCRS Scheme

For the MSCRS scheme, the relay having the maximum instantaneous secrecy capacity is selected as the optimal relay. Thus, the MSCRS criterion can be expressed as

$$o = \arg\begin{cases} \max\limits_{i\in\{1,2,\ldots,N\}} C_{S-i}^{proposed}, & if \max\limits_{i\in\{1,2,\ldots,N\}} C_{S-i}^{proposed} > 0 \\ \max\limits_{i\in\{1,2,\ldots,N\}} R_{DNF-i}, & if \max\limits_{i\in\{1,2,\ldots,N\}} C_{S-i}^{proposed} = 0 \end{cases} \tag{10}$$

where o denotes the subscript of the selected optimal relay. $C_{S-i}^{proposed}$ is the system secrecy capacity of relay SR_i, and can be expressed as

$$C_{S-i}^{proposed} = \left[R_{DNF-i} - I_{E-i}^{1st}\right]^{+} \tag{11}$$

where $[a]^{+} = \begin{cases} a, & if\ a > 0 \\ 0, & if\ a \leqslant 0 \end{cases}$.

It should be note that in the case of $C_{S-i}^{proposed} = 0$, $i \in \{1, 2, \ldots, N\}$, we will choose the optimal relay which can provide the maximum sum rate. Here, the global CSIs of all the channels are assumed to be available, which is a common assumption in the literature. However, CSIs of the wiretap channels, i.e., $SA - E$, $SB - E$, $SR_i - E$, $PT - E$ links, are not always easy to be estimated because the eavesdroppers are passive. Thus, we should consider a more practical scheme without requirement of CSI of the wiretap channel, which will be described in the next section.

3.2 MSRRS Scheme

For the MSRRS scheme, the relay having the maximum instantaneous sum rate is selected as the optimal relay. Thus, the MSRRS criterion can be expressed as

$$l = \arg \max_{i \in \{1,2,\ldots,N\}} R_{DNF-i} \tag{12}$$

where l denotes the subscript of the selected optimal relay.

According to (10) and (12), we have the following Proposition.

Proposition 1 For a CTWDNFR network, the MSCRS scheme equals to the MSRRS scheme. In other words, the CSI of wiretap channels has no effect on the MSCRS scheme.

Proof From (10) and (11), the MSCRS scheme equals to the MSRRS scheme if $\max_{i \in \{1,2,\ldots,N\}} C_{S-i}^{proposed} = 0$. In the case of $\max_{i \in \{1,2,\ldots,N\}} C_{S-i}^{proposed} > 0$, the MSCRS scheme can be rewritten as $o = \arg \max_{i \in \{1,2,\ldots,N\}} (R_{DNF-i} - I_{E-i}^{1st})$. From (4), $I_{E-i}^{1\text{st}}$ is always independent from the selected relay SR_i. Then MSCRS scheme can be rewritten as $o = \arg \max_{i \in \{1,2,\ldots,N\}} R_{DNF-i}$, which equals to the MSRRS scheme. This completes the proof.

Thus, we only analyze the MSRRS scheme in the rest of this paper. The intercept event is defined as that the eavesdropper can successfully decode x_A or x_B during the two transmission time-slots. However, E can decode x_A or x_B from x_R only when E has intercepted x_B or x_A in the first time-slot. With (12), the intercept probability of the network can be expressed as

$$P_{in-l}^{MSRRS} = \Pr\left(\max_{i \in \{1,2,\ldots,N\}} R_{DNF-i} \leqslant I_{E-i}^{1\text{st}} \middle| \hat{H} = H_0 \right) \tag{13}$$

Considering that the primary network still occupies the licensed spectrum while the secondary network detects a spectrum hole, which is a missed detection case, and by using the total probability law, (13) can be rewritten as

$$P_{in-l}^{MSRRS}=\underbrace{\Pr\left(\max_{i\in\{1,2,\ldots,N\}}R_{DNF-i}\leqslant I_{E-i}^{1\mathrm{st}}\middle|H_0,\hat{H}=H_0\right)}_{Q_1}\Pr\left(\hat{H}=H_0\middle|H_0\right)$$

$$+\underbrace{\Pr\left(\max_{i\in\{1,2,\ldots,N\}}R_{DNF-i}\leqslant I_{E-i}^{1\mathrm{st}}\middle|H_1,\hat{H}=H_0\right)}_{Q_2}\Pr\left(\hat{H}=H_0\middle|H_1\right) \tag{14}$$

where $Q_1=\Pr\left(\max_{i\in\{1,2,\ldots,N\}}R_{DNF-i}\leqslant I_{E-i}^{1\mathrm{st}}\middle|H_0,\hat{H}=H_0\right)$,
$Q_2=\Pr\left(\max_{i\in\{1,2,\ldots,N\}}R_{DNF-i}\leqslant I_{E-i}^{1\mathrm{st}}\middle|H_1,\hat{H}=H_0\right)$.

Here, $1/\lambda_S\gg 1$ and $1/\lambda_E\gg 1$ are assumed to simplify the derivation of (14). In the case of H_0 occurring, Q_1 can be rewritten as

$$Q_1=\Pr\left(\max_{i\in\{1,2,\ldots,N\}}\min\left(Ca\left(\gamma_S\left|h_{SASR_i}\right|^2\right),Ca\left(\gamma_S\left|h_{SBSR_i}\right|^2\right),\frac{1}{2}Ca\left(\gamma_S\left|h_{SASR_i}\right|^2+\gamma_S\left|h_{SBSR_i}\right|^2\right)\right)\right.$$
$$\left.\leqslant\max\left(Ca(\frac{\gamma_S\left|h_{SAE}\right|^2}{\gamma_S\left|h_{SBE}\right|^2}),Ca(\frac{\gamma_S\left|h_{SBE}\right|^2}{\gamma_S\left|h_{SAE}\right|^2})\right)\right) \tag{15}$$

According to “Appendix A”, we can obtain

$$Q_1=1+\sum_{m=0}^{N-1}\sum_{n=0}^{N-m}\sum_{k=0}^{2(N-m-n)}C_N^mC_{N-m}^nC_{2(N-m-n)}^k(-1)^{3N-3m-2n-k}\lambda_S^{N-m-n-(k-1)/2}z$$
$$\times(N-m)^{-(k-1)/2}e^{\lambda_S(N-m)}\int_{4\lambda_S(N-m)}^{+\infty}u^{\frac{(k-1)}{2}-1}e^{-u}du \tag{16}$$

where $\int_{4\lambda_S(N-m)}^{+\infty}u^{\frac{(k-1)}{2}-1}e^{-u}du=\begin{cases}\Gamma\left(\frac{k-1}{2},4\lambda_S(N-m)\right), & k>1\\ \mathrm{Ei}\left(1,4\lambda_S(N-m)\right), & k=1\\ 2\sqrt{\pi}\left(\mathrm{erf}\left(\sqrt{4\lambda_S(N-m)}\right)-1\right) & \\ +2e^{-4\lambda_S(N-m)}\left(4\lambda_S(N-m)\right)^{-1/2}, & k=0\end{cases}$

In the case of H_1 occurring, Q_2 can be rewritten as

$$Q_2 = \Pr\left(\begin{array}{l} \max\limits_{i\in\{1,2,\ldots,N\}} \min\left(\begin{array}{l} Ca\left(\frac{\gamma_S \left|h_{SASR_i}\right|^2}{\gamma_P \left|h_{PTSR_i}\right|^2+1} \right), Ca\left(\frac{\gamma_S \left|h_{SBSR_i}\right|^2}{\gamma_P \left|h_{PTSR_i}\right|^2+1} \right), \\ \frac{1}{2} Ca\left(\frac{\gamma_S \left|h_{SASR_i}\right|^2+\gamma_S \left|h_{SBSR_i}\right|^2}{\gamma_P \left|h_{PTSR_i}\right|^2+1} \right), \\ Ca\left(\frac{\gamma_S \left|h_{SASR_i}\right|^2}{\gamma_P \left|h_{PTSA}\right|^2+1} \right), Ca\left(\frac{\gamma_S \left|h_{SBSR_i}\right|^2}{\gamma_P \left|h_{PTSB}\right|^2+1} \right) \end{array} \right) \\ \leqslant \max\left(Ca\left(\frac{\gamma_S \left|h_{SAE}\right|^2}{\gamma_S \left|h_{SBE}\right|^2+\gamma_P \left|h_{PTE}\right|^2} \right), Ca\left(\frac{\gamma_S \left|h_{SBE}\right|^2}{\gamma_S \left|h_{SAE}\right|^2+\gamma_P \left|h_{PTE}\right|^2} \right) \right) \end{array} \right) \tag{17}$$

However, it is difficult to obtain a closed form solution to Q_2. Although finding a general closed-form expression for P_{in-l}^{MSRRS} is challenging, we can obtain the numerical results by computer simulations. □

3.3 Round-Robin Transmission Scheme

For the round-robin transmission scheme, N relays act as a DNF two-way relay to help the sources' transmission in turn [21]. The intercept event is defined as that the eavesdropper can successfully decode x_A or x_B during the two transmission time-slots. However, E can decode x_A or x_B from x_R only when E has intercepted x_B or x_A in the first time-slot. Thus, an intercept even in the first time-slot results in a system interception, giving

$$P_{in-i}^{round} = \Pr\left(R_{DNF-i} \leqslant I_{E-i}^{1\text{st}} \middle| \hat{H} = H_0 \right) \tag{18}$$

Considering the missed probability of the spectrum detection and by using the total probability law, (18) can be rewritten as

$$\begin{aligned} P_{in-i}^{round} = {} & \underbrace{\Pr\left(R_{DNF-i} \leqslant I_{E-i}^{1\text{st}} \middle| H_0, \hat{H} = H_0 \right)}_{G_1} \Pr\left(\hat{H} = H_0 \middle| H_0 \right) \\ & + \underbrace{\Pr\left(R_{DNF-i} \leqslant I_{E-i}^{1\text{st}} \middle| H_1, \hat{H} = H_0 \right)}_{G_2} \Pr\left(\hat{H} = H_0 \middle| H_1 \right) \end{aligned} \tag{19}$$

where $G_1 = \Pr\left(R_{DNF-i} \leqslant I_{E-i}^{1\text{st}} \middle| H_0, \hat{H} = H_0 \right), G_2 = \Pr\left(R_{DNF-i} \leqslant I_{E-i}^{1\text{st}} \middle| H_1, \hat{H} = H_0 \right).$

To simplify the derivation, $1/\lambda_S \gg 1$ and $1/\lambda_E \gg 1$ are assumed. By substituting $\alpha = 0$ to (2) and (8), G_1 can be rewritten as

$$G_1 = \Pr\left(\begin{array}{l} \min\left(Ca\left(\gamma_S \left|h_{SASR_i}\right|^2 \right), Ca\left(\gamma_S \left|h_{SBSR_i}\right|^2 \right), \frac{1}{2} Ca\left(\gamma_S \left|h_{SASR_i}\right|^2 + \gamma_S \left|h_{SBSR_i}\right|^2 \right) \right) \\ \leqslant \max\left(Ca\left(\frac{\gamma_S \left|h_{SAE}\right|^2}{\gamma_S \left|h_{SBE}\right|^2} \right), Ca\left(\frac{\gamma_S \left|h_{SBE}\right|^2}{\gamma_S \left|h_{SAE}\right|^2} \right) \right) \end{array} \right) \tag{20}$$

Substituting $\alpha = 1$ to (2) and (8), G_2 can be rewritten as

$$G_2 = \Pr\left(\min\left(\begin{array}{l} Ca\left(\frac{\gamma_S\left|h_{SASR_i}\right|^2}{\gamma_P\left|h_{PTSR_i}\right|^2+1}\right), Ca\left(\frac{\gamma_S\left|h_{SBSR_i}\right|^2}{\gamma_P\left|h_{PTSR_i}\right|^2+1}\right), \\ \frac{1}{2}Ca\left(\frac{\gamma_S\left|h_{SASR_i}\right|^2+\gamma_S\left|h_{SBSR_i}\right|^2}{\gamma_P\left|h_{PTSR_i}\right|^2+1}\right), \\ Ca\left(\frac{\gamma_S\left|h_{SASR_i}\right|^2}{\gamma_P\left|h_{PTSA}\right|^2+1}\right), Ca\left(\frac{\gamma_S\left|h_{SBSR_i}\right|^2}{\gamma_P\left|h_{PTSB}\right|^2+1}\right) \end{array} \right) \atop \leqslant \max\left(Ca\left(\frac{\gamma_S\left|h_{SAE}\right|^2}{\gamma_S\left|h_{SBE}\right|^2+\gamma_P\left|h_{PTE}\right|^2}\right), Ca\left(\frac{\gamma_S\left|h_{SBE}\right|^2}{\gamma_S\left|h_{SAE}\right|^2+\gamma_P\left|h_{PTE}\right|^2}\right)\right) \right) \tag{21}$$

According to “Appendix B”, we have

$$G_1 = 1 - e^{-3\lambda_S}\left(\left(2\sqrt{\pi}e^{4\lambda_S}\lambda_S^{3/2} + \sqrt{\pi}e^{4\lambda_S}\lambda_S^{1/2}\right)\left(\mathrm{erf}(2\sqrt{\lambda_S}) - 1\right) - 2\lambda_S e^{4\lambda_S}\mathrm{Ei}\left(1, 4\lambda_S\right) + \lambda_S + 1\right) \tag{22}$$

However, it is quite difficult to obtain a closed-form solution to G_2. Although finding a general closed-form expression for P_{in-i}^{round} is challenging, we can obtain the numerical results by computer simulations. As aforementioned, N relays act in turn as a DNF two-way relay in the round-robin transmission scheme. Thus, the intercept probability of the round-robin transmission scheme is the average intercept probability of N relays, given by.

$$P_{in}^{round} = \frac{1}{N}\sum_{i=1}^{N} P_{in-i}^{round} \tag{23}$$

4 Tradeoff Between Performance and Relay Numbers Analysis

It is well known that with increasing the number of relay nodes, more performance gain can be achieved. However, with the increment of relay numbers, the cost of relay deployment will also increase. Thus, it must exist a tradeoff between performance gain and relay numbers. Two parameters called ANG and ACG to study the performance improvement from the increment of the relay numbers. Here, ANG is defined as the ratio of intercept probability improvement to the relay numbers, which can be written as the following.

$$ANG(n) = \frac{1/P_{in-l}^{MSRRS}(n) - 1/P_{in-l}^{MSRRS}(1)}{n} \tag{24}$$

where n is the number of the relays, and $P_{in-l}^{MSRRS}(n)$ is the intercept probability of the network with n participated relays, which is given by (13). Here, we use $1/P_{in-l}^{MSRRS}(n) - 1/P_{in-l}^{MSRRS}(1)$ to show the improvement of the intercept probability.

ACG is defined as the ratio of intercept probability decrement to relay cost, which can be written as.

$$ACG(n) = \frac{1/P_{in-l}^{MSRRS}(n) - 1/P_{in-l}^{MSRRS}(1)}{1 + \varpi(n-1)} \tag{25}$$

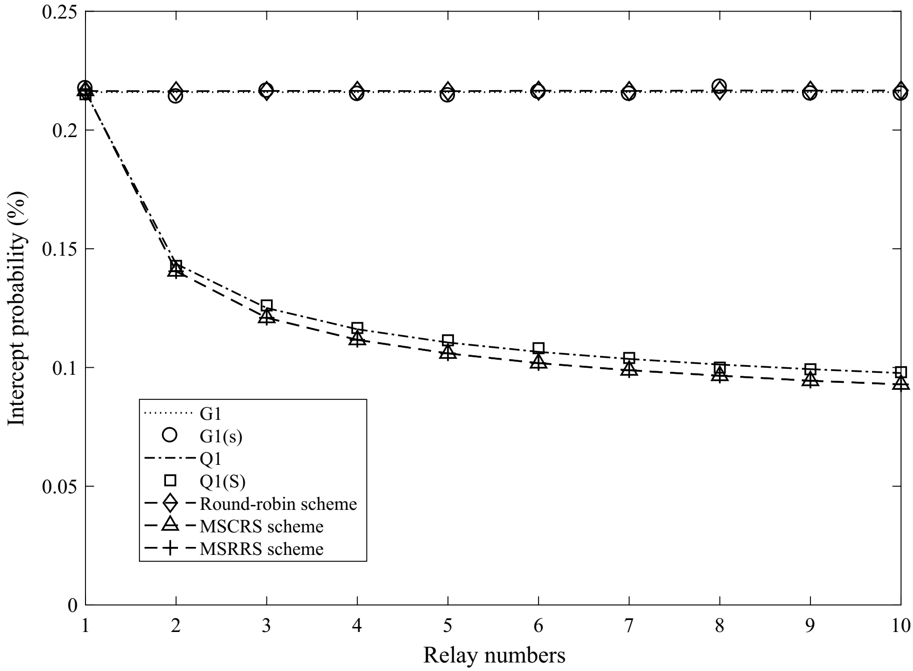

Fig. 2 Intercept probability verse N of G_1 and Q_1, round-robin and MSCRS schemes where $P_d = 0.9$, $P_f = 0.1$, $1/\lambda_S = 20$ dB, $1/\lambda_E = 10$ dB and $1/\lambda_P = 0$ dB

where ϖ is coefficient indicating the cost of the relays taking part in the cooperating but not being selected. The cost of the selected relay is assumed to be 1. Because the unselected relay nodes keep silence during the relaying phase, its cost will be smaller than the selected relay, thus we have $\varpi \in (0, 1)$.

From (13)–(17), we find it is difficult to obtain a closed-form solution for ANG and ACG, computer simulations will be conducted to analyze the tradeoff between the system security performance and the relay numbers.

5 Numerical Results

In this section, numerical results are presented to demonstrate the performance of the proposed schemes. According to the IEEE 802.22 standard, $P_d \geqslant 0.9$, indicates $P_f \leqslant 0.1$. Here, we assume $P_d = 0.9$ and $P_f = 0.1$. Moreover, $1/\lambda_E = 10\,\text{dB}$ is assumed. Figure 2 plots the intercept probabilities of the MSCRS, MSRRS and round-robin schemes as a function of the number of the available relay nodes. Here, we consider two cases, namely, the missed detection probability is zero and nonzero. $1/\lambda_P = 0\,\text{dB}$ and $1/\lambda_S = 20\,\text{dB}$ are assumed. Figure 2 shows that MSRRS scheme has the same performance as the MSCRS scheme which has been proved in Proposition 1 . It can be observed that as the relay number increases, the intercept probability of the MSCRS and MSRRS schemes decrease, meaning that the system secrecy performance can be improved by increasing the number of relays. Figure 2 also shows that with 10 relay nodes, the intercept probability of

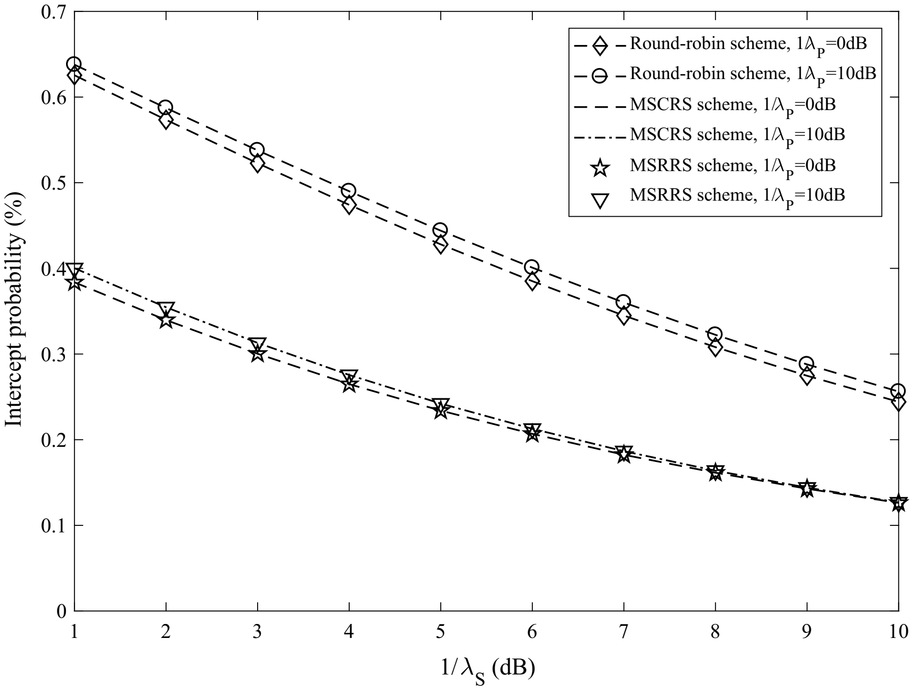

Fig. 3 Intercept probability verse $1/\lambda_S$ with round-robin and MSCRS schemes where $N = 4$, $P_d = 0.9$, $P_f = 0.1$ and $1/\lambda_E = 10$ dB

our proposed MSCRS and MSRRS schemes can be reduced by 3.7 dB compared to the traditional round-robin scheme. In addition, it can be seen that the simulation results of G_1 and Q_1 are extremely close to the theoretical values, confirming the correctness of our derived expressions. It should be pointed out that the intercept probability of the round-robin scheme stays unchanged when the number of relays increases. This is because that all the relay nodes serve as a DNF two-way relay to help the sources' transmission in turn and all relay-to-source links follow the same distribution. For the round-robin scheme, no diversity gain is achieved.

Figure 3 depicts the intercept probability against $1/\lambda_S$ of the round-robin, MSCRS and MSRRS schemes, where $1/\lambda_S$ is the exception of $P_S\left|h_{SBSR_i}\right|^2/N_0$ and $P_S\left|h_{SASR_i}\right|^2/N_0$. $N = 4$ and $1/\lambda_E = 10$ dB are assumed. Here, the following two cases are considered, i.e. (1) $1/\lambda_P = 0$ dB; (2) $1/\lambda_P = 10$ dB. Figure 3 shows that the intercept probabilities of the round-robin, MSCRS and MSRRS schemes decrease when $1/\lambda_S$ increases. Moreover, it shows that as $1/\lambda_P$ grows, the intercept probabilities of the three compared schemes increase simultaneously. It can be observed that the intercept probability of our proposed MSCRS and MSRRS schemes can be reduced by 2.6 dB compared to the traditional round-robin scheme when $1/\lambda_S = 5$ dB and $1/\lambda_P = 10$ dB. However, the performance of the considered two cases is very close because the primary user's interference only exists in the case that the licensed spectrum has been occupied, i.e., $P_f = 0.1$. Figure 3 also shows that the proposed MSCRS and MSRRS schemes have the similar performance.

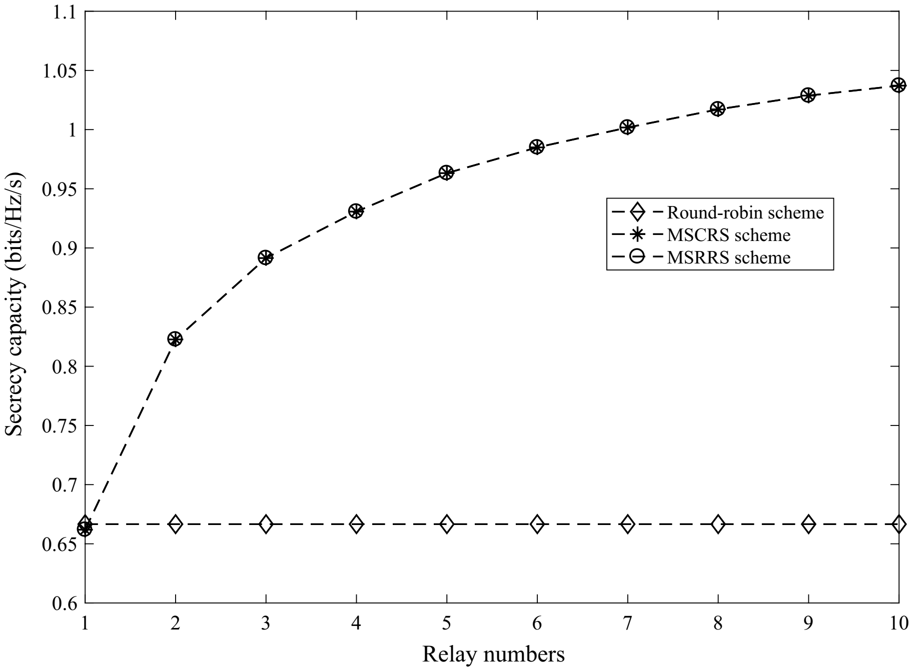

Fig. 4 Average secrecy capacity verse relay numbers of round-robin and MSCRS schemes where $P_d = 0.9$, $P_f = 0.1$, $1/\lambda_S = 20$ dB, $1/\lambda_E = 10$ dB and $1/\lambda_P = 0$ dB

In Figure 4, we plot the average secrecy capacity against the relay numbers. The secrecy capacity is defined as the gap between the main channel capacity and the wiretap channel capacity, giving in (11). Here, $1/\lambda_S = 20$ dB, $1/\lambda_E = 10$ dB and $1/\lambda_P = 0$ dB are assumed. From Fig. 4, it can be seen that the system gains more secrecy capacity with increasing the relay numbers. The proposed MSCRS and MSRRS schemes are shown to have the same performance, and they outperform the traditional round-robin scheme, achieving 1.9 dB secrecy capacity when the relay number is 10. However, the increment of the achieved secrecy capacity decreases when the relay numbers increase.

Figure 5 illustrates the average secrecy capacity against $1/\lambda_S$ of the round-robin, MSCRS and MSRRS schemes, where $N = 4$ and $1/\lambda_E = 10$ dB are assumed. The following two cases are considered, i.e., (1) $1/\lambda_P = 0$ dB; (2) $1/\lambda_P = 10$ dB. From Fig. 5, it can be seen that the average secrecy capacity of the round-robin, MSCRS and MSRRS schemes grow when $1/\lambda_S$ increases. Figure 5 also shows that the MSCRS and MSRRS schemes can gain 1.8 dB secrecy capacity than the traditional round-robin scheme when $1/\lambda_S = 5$ dB and $1/\lambda_P = 10$ dB. Compared with Fig. 3, the better channel state of the secondary users, the higher secrecy performance will be achieved.

To further show the secrecy performance of the system, we plot ANG and ACG verse relay numbers in Figs. 6 and 7, respectively. In Fig. 6, ANG against relay numbers of the round-robin, MSCRS and MSRRS schemes are plotted. Two cases are considered, i.e. (1) $1/\lambda_S = 10$ dB; (2) $1/\lambda_S = 20$ dB. In addition, $P_d = 0.9$, $P_f = 0.1$, $1/\lambda_E = 10$ dB and $1/\lambda_P = 0$ dB are assumed. Both the MSCRS and MSRRS schemes are shown to have the

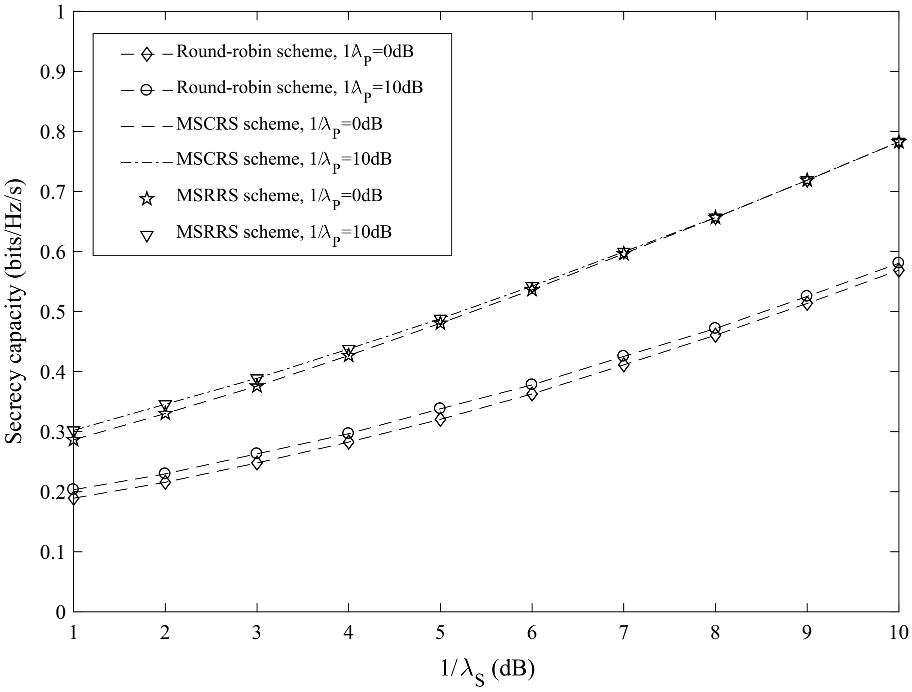

Fig. 5 Average secrecy capacity verse $1/\lambda_S$ of the round-robin and MSCRS schemes where $N = 4$, $P_d = 0.9$, $P_f = 0.1$ and $1/\lambda_E = 10$ dB

same performance in Fig. 6. It can be seen that for the MSCRS and MSRRS schemes, ANG grows first with the increment of relay numbers, then it drops down after the highest ANG point, indicating that we should consider both the relay numbers deployed and the system secrecy performance achieved in practical. It shows that the highest value where the ANG achieves of the MSCRS and MSRRS schemes are different in the two cases, which means that the highest ANG is achieved when the relay numbers is 2 in case (1) while it is achieved when the relay numbers is 3 in case (2). However, the ANG always stays zero in the round-robin scheme of both two cases. This is because that there is no system security performance improvement achieved by increasing the relay numbers.

Figure 7 plots the ACG against the relay numbers of the round-robin, MSCRS and MSRRS schemes. $P_d = 0.9$, $P_f = 0.1$, $1/\lambda_S = 20$ dB, $1/\lambda_E = 10$ dB and $1/\lambda_P = 0$ dB are assumed, and three cases are considered, i.e. (1) $\varpi = 0.1$; (2) $\varpi = 0.3$; (3) $\varpi = 0.5$. Figure 7 shows that ACG increases first, then decreases with the increment of relay numbers in the MSCRS and MSRRS schemes. Different values of ϖ indicate different costs of the unselected relays. With the higher ϖ, the lower ACG will be achieved, and the less relay numbers where the best ACG achieves. We can also obtain that the ACG always stays zero in the round-robin scheme of both two cases, which is also shown in Fig. 6.

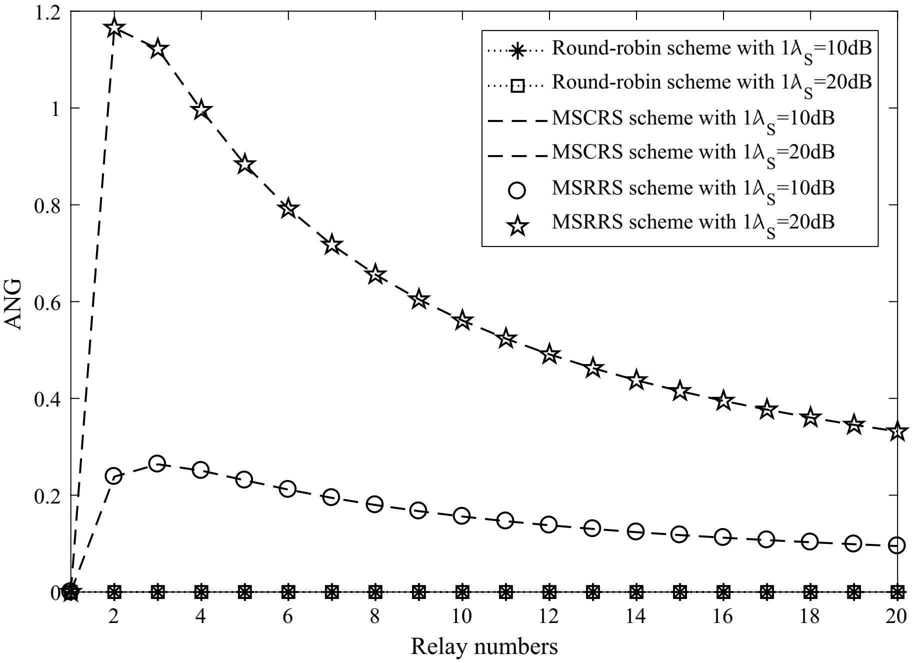

Fig. 6 ANG verse relay numbers of the round-robin and MSCRS schemes where $P_d = 0.9$, $P_f = 0.1$, $1/\lambda_E = 10$ dB and $1/\lambda_P = 0$ dB

6 Conclusions

In this paper, we studied the secrecy performance of a DNF protocol based two-way relaying in the cognitive radio network settings, where two secondary users try to communicate with each other when detecting a spectrum hole. Both the correct and missed detection events are considered. In order to improve the system secrecy performance, two relay selection schemes called MSRRS and MSCRS schemes are proposed. We proved that the MSRRS and MSCRS schemes have the same secrecy performance. Intercept probability of the proposed MSCRS scheme as well as the round-robin scheme were analyzed over Rayleigh fading channels, giving closed-form expressions in the correct detection event. We propose ANG and ACG to analyze the performance improvement from the increment of the relay numbers. Our simulation results show that the proposed schemes can significantly improve the secrecy performance and the network will become more secure either when the numbers of the relay increases or when the channel of the secondary users become better. Furthermore, the MSCRS and MSRRS schemes are shown to have the same performance, confirming the correctness of Proposition 1. It also shows that the ANG and the ACG not always grow with the increasing of the participated relay numbers, which

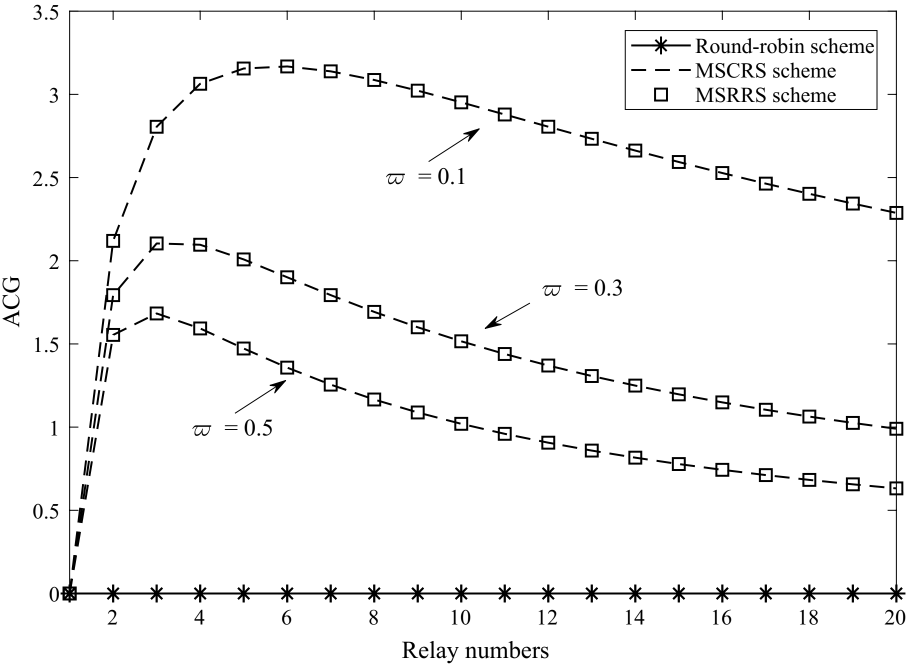

Fig. 7 ACG verse relay numbers of the round-robin and MSCRS schemes where $P_d = 0.9$, $P_f = 0.1$, $1/\lambda_S = 20$ dB, $1/\lambda_E = 10$ dB and $1/\lambda_P = 0$ dB

indicates that we should consider both the relay numbers deployed and the system secrecy performance achieved in practical.

Acknowledgements This work is supported in party by the National Natural Science Foundation of China (Grant Nos. 61771263, 61401238, 61371111), by the Nantong University-Nantong Joint Research Center for Intelligent Information Technology (Grant No. KFKT2017A03), by the Science and Technology Program of Nantong (Grant No. GY12016016), and by the Postgraduate Innovation Program of Scientific Research of Jiangsu Province (Grant No. KYZZ16-0353).

Appendix A

Derivation of Q_1

Let $K_{21} = \max\limits_{i} \min\left(Ca\left(\gamma_S\left|h_{SASR_i}\right|^2\right), Ca\left(\gamma_S\left|h_{SBSR_i}\right|^2\right), \frac{1}{2}Ca\left(\gamma_S\left|h_{SASR_i}\right|^2+\gamma_S\left|h_{SBSR_i}\right|^2\right)\right)$, $i \in \{1,2,\dots,N\}$, $K_{22} = \max\left(Ca\left(\frac{\gamma_S|h_{SAE}|^2}{\gamma_S|h_{SBE}|^2}\right), Ca\left(\frac{\gamma_S|h_{SBE}|^2}{\gamma_S|h_{SAE}|^2}\right)\right)$. Because all the CSIs are mutual independent, thus Q_1 can be rewritten as (26).

$$Q_1 = \Pr\left(K_{21} \leqslant K_{22}\right) = \oint \Pr\left(K_{21} \leqslant x\right) f_{K_{22}}(x)dx \tag{26}$$

We first derive $\Pr\left(K_{21} \leqslant x\right)$. Let $a_1 = \gamma_S\left|h_{SASR_i}\right|^2$ and $a_2 = \gamma_S\left|h_{SBSR_i}\right|^2$, we have (27).

$$\begin{aligned}
\Pr\left(K_{21} \leqslant x\right) &= \Pr\left(\max_{i\in\{1,2,\ldots,N\}} \min\left(Ca\left(a_1\right), Ca\left(a_2\right), \frac{1}{2}Ca\left(a_1{+}a_2\right)\right) \leqslant x\right)\\
&= \left(1-\Pr\left(\min\left(Ca\left(a_1\right), Ca\left(a_2\right), \frac{1}{2}Ca\left(a_1+a_2\right)\right) > x\right)\right)^N\\
&= \left(1-\Pr\left(a_1 > \underbrace{2^{2x}-1}_{z}, a_1 > 2^{2x}-1, a_1+a_2 > \left(2^{4x}-1\right)\right)\right)^N\\
&= \left(1-\left(1+\lambda_S z^2\right)e^{-\lambda_S z(z+2)}\right)^N\\
&= \sum_{m=0}^{N}\sum_{n=0}^{N-m} C_N^m(-1)^{N-m}C_{N-m}^n\lambda_S^{N-m-n}z^{2(N-m-n)}e^{-\lambda_S z(z+2)(N-m)}
\end{aligned} \tag{27}$$

The cumulative density function of K_{22} can be obtained from (28).

$$\begin{aligned}
F_{K_{22}}(x) &= \Pr\left(K_{12} < x\right)\\
&= \Pr\left(\max\left(Ca\left(\frac{\gamma_S\left|h_{SAE}\right|^2}{\gamma_S\left|h_{SBE}\right|^2}\right), Ca\left(\frac{\gamma_S\left|h_{SBE}\right|^2}{\gamma_S\left|h_{SAE}\right|^2}\right)\right) < x\right)\\
&= \Pr\left(\max\left(\frac{P_S\left|h_{SAE}\right|^2}{P_S\left|h_{SBE}\right|^2}, \frac{P_S\left|h_{SBE}\right|^2}{P_S\left|h_{SAE}\right|^2}\right) < 2^{2x}-1\right)\\
&= \begin{cases} \frac{2^{2x}-2}{2^{2x}} & x \geqslant 0.5\\ 0 & x < 0.5 \end{cases}
\end{aligned} \tag{28}$$

Thus, the probability density function of K_{22} can be expressed as (29).

$$f_{K_{22}}(x) = \frac{\partial F_{K_{22}}(x)}{\partial x} = \begin{cases} \frac{\ln(2)}{2^{2x-2}} & x \geqslant 0.5\\ 0 & x < 0.5 \end{cases} \tag{29}$$

Thus, we have (30).

$$\begin{aligned}
Q_1 = \int_{0.5}^{+\infty} & \sum_{m=0}^{N}\sum_{n=0}^{N-m} C_N^m(-1)^{N-m}C_{N-m}^n\lambda_S^{N-m-n}\left(2^{2x}-1\right)^{2(N-m-n)}\\
&\times e^{-\lambda_S\left(2^{2x}-1\right)\left(2^{2x}-1+2\right)(N-m)}\frac{\ln(2)}{2^{2x-2}}dx
\end{aligned} \tag{30}$$

Let $y = 2^{2x}-1$, (30) can be rewritten as (31).

$$Q_1 = 2\sum_{m=0}^{N}\sum_{j=0}^{N-m} C_N^m C_{N-m}^n(-1)^{N-m}\int_1^{+\infty}\lambda_S^{N-m-n}y^{2(N-m-n)}\frac{e^{-\lambda_S y(y+2)(N-m)}}{(y+1)^2}dy \tag{31}$$

Let $u = \lambda_S(y+1)^2(N-m)$, (31) can be rewritten as (32).

$$\begin{aligned}
Q_1 &= 1 + 2\sum_{m=0}^{N-1}\sum_{n=0}^{N-m} C_N^m C_{N-m}^n (-1)^{N-m} \lambda_S^{N-m-n} e^{\lambda_S(N-m)} \\
&\quad \times \int_{4\lambda_S(N-m)}^{+\infty} \left(\sqrt{\frac{u}{\lambda_S(N-m)}}-1\right)^{2(N-m-n)} \frac{e^{-u}}{\frac{u}{\lambda_S(N-m)}} d\left(\sqrt{\frac{u}{\lambda_S(N-m)}}-1\right) \\
&= 1 + 2\sum_{m=0}^{N-1}\sum_{n=0}^{N-m} C_N^m C_{N-m}^n (-1)^{N-m} \lambda_S^{N-m-n} e^{\lambda_S(N-m)} \\
&\quad \times \int_{4\lambda_S(N-m)}^{+\infty} \sum_{k=0}^{2(N-m-n)} C_{2(N-m-n)}^k \left(\frac{u}{\lambda_S(N-m)}\right)^{k/2} (-1)^{2(N-m-n)-k} \frac{e^{-u}}{\frac{u^{3/2}}{\sqrt{\lambda_S(N-m)}}} \frac{1}{2} du \\
&= 1 + \sum_{m=0}^{N-1}\sum_{n=0}^{N-m}\sum_{k=0}^{2(N-m-n)} C_{2(N-m-n)}^k C_N^m C_{N-m}^n (-1)^{3N-3m-2n-k} \lambda_S^{N-m-n} \\
&\quad \times \left(\frac{1}{\lambda_S(N-m)}\right)^{(k-1)/2} e^{\lambda_S(N-m)} \int_{4\lambda_S(N-m)}^{+\infty} u^{\frac{(k-1)}{2}-1} e^{-u} du \\
&= 1 + \sum_{m=0}^{N-1}\sum_{n=0}^{N-m}\sum_{k=0}^{2(N-m-n)} C_N^m C_{N-m}^n C_{2(N-m-n)}^k (-1)^{3N-3m-2n-k} \lambda_S^{N-m-n-(k-1)/2} \\
&\quad \times (N-m)^{-(k-1)/2} e^{\lambda_S(N-m)} \int_{4\lambda_S(N-m)}^{+\infty} u^{\frac{(k-1)}{2}-1} e^{-u} du
\end{aligned} \tag{32}$$

where

$$\begin{aligned}
&\int_{4\lambda_S(N-m)}^{+\infty} u^{\frac{(k-1)}{2}-1} e^{-u} du \\
&\quad = \begin{cases} \Gamma\left(\frac{k-1}{2}, 4\lambda_S(N-m)\right), & k > 1 \\ \mathrm{Ei}\left(1, 4\lambda_S(N-m)\right), & k = 1 \\ 2\sqrt{\pi}\left(\mathrm{erf}\left(\sqrt{4\lambda_S(N-m)}\right)-1\right) + 2e^{-4\lambda_S(N-m)}\left(4\lambda_S(N-m)\right)^{-1/2}, & k = 0 \end{cases}
\end{aligned}$$

Appendix B

Derivation of G_1

Let $K_{11} = \min\left(Ca\left(a_1\right), Ca\left(a_2\right), \frac{1}{2}Ca\left(a_1+a_2\right)\right)$ and $K_{12} = \max\left(Ca(b), Ca\left(\frac{1}{b}\right)\right)$, where $a_1 = \gamma_S\left|h_{SASR_i}\right|^2, a_2 = \gamma_S\left|h_{SBSR_i}\right|^2$ and $b = \frac{\gamma_S\left|h_{SAE}\right|^2}{\gamma_S\left|h_{SBE}\right|^2}$. Because all the CSIs are mutual independent, thus G_1 can be rewritten as (33).

$$G_1 = \Pr\left(K_{11} \leqslant K_{12}\right) = \oint \Pr\left(K_{11} \leqslant x\right) f_{K_{12}}(x) dx \tag{33}$$

We first drive $\Pr\left(K_{11} \leqslant x\right)$, given by (34).

$$\begin{aligned}
\Pr\left(K_{11} \leqslant x\right) &= \Pr\left(\min\left(Ca\left(a_1\right), Ca\left(a_2\right), \frac{1}{2}Ca\left(a_1{+}a_2\right)\right) \leqslant x\right)\\
&= 1 - \Pr\left(\min\left(Ca\left(a_1\right), Ca\left(a_2\right), \frac{1}{2}Ca\left(a_1{+}a_2\right)\right) \leqslant x\right)\\
&= 1 - \Pr\left(a_1 > \underbrace{2^{2x} - 1}_{z}, a_2 > 2^{2x} - 1, a_1{+}a_2 > \left(2^{4x} - 1\right)\right)\\
&= 1 - \int_{z}^{z(z+1)} \int_{z(z+2)-v}^{+\infty} \lambda_S e^{-\lambda_S u} \lambda_S e^{-\lambda_S v} du dv\\
&\quad - \int_{z(z+1)}^{+\infty} \int_{z}^{+\infty} \lambda_S e^{-\lambda_S u} \lambda_S e^{-\lambda_S v} du dv\\
&= 1 - \left(1 + \lambda_S\left(2^{2x} - 1\right)^2\right) e^{-\lambda_S\left(2^{4x}-1\right)}
\end{aligned} \tag{34}$$

The cumulative density function of K_{12} can be obtained from (35).

$$\begin{aligned}
F_{K_{12}}(x) &= \Pr\left(K_{12} < x\right)\\
&= \Pr\left(\max\left(Ca(b), Ca\left(\frac{1}{b}\right)\right) < x\right)\\
&= \Pr\left(\max\left(b, \frac{1}{b}\right) < 2^{2x} - 1\right)\\
&= \begin{cases} \frac{2^{2x}-2}{2^{2x}} & x \geqslant 0.5\\ 0 & x < 0.5 \end{cases}
\end{aligned} \tag{35}$$

Thus, the probability density function of K_{12} can be expressed as (36).

$$f_{K_{12}}(x) = \frac{\partial F_{K_{12}}(x)}{\partial x} = \begin{cases} \frac{\ln(2)}{2^{2x-2}} & x \geqslant 0.5\\ 0 & x < 0.5 \end{cases} \tag{36}$$

Let $y = 2^{2x} - 1$, (34) can be rewritten as (37).

$$\begin{aligned}
G_1 &= \Pr\left(K_{11} \leqslant K_{12}\right)\\
&= \int_{0.5}^{+\infty} 1 - \left(1 + \lambda_S\left(2^{2x} - 1\right)^2\right) e^{-\lambda_S\left(2^{2x}-1\right)\left(\left(2^{2x}-1\right)+2\right)} \frac{\ln(2)}{2^{2x-2}} dx\\
&= 2\int_{1}^{+\infty} \left(1 - \left(1 + \lambda_S y^2\right) e^{-\lambda_S y(y+2)}\right) \frac{1}{(y+1)^2} dy\\
&= 2\int_{1}^{+\infty} \frac{1}{(y+1)^2} dy - 2\int_{1}^{+\infty} \frac{\left(1 + \lambda_S y^2\right) e^{-\lambda_S y(y+2)}}{(y+1)^2} dy\\
&= 1 - e^{-3\lambda_S}\left(2\sqrt{\pi} e^{4\lambda_S} \lambda_S^{3/2} + \sqrt{\pi} e^{4\lambda_S} \lambda_S^{1/2}\right)\left(\operatorname{erf}(2\sqrt{\lambda_S}) - 1\right)\\
&\quad - e^{-3\lambda_S}\left(-2\lambda_S e^{4\lambda_S} \operatorname{Ei}\left(1, 4\lambda_S\right) + \lambda_S + 1\right)
\end{aligned} \tag{37}$$

References

1. Haykin, S. (2005). Cognitive radio: Brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications*, *23*(2), 201–220.
2. Mitola, J., & Maguire, G. (1999). Cognitive radio: Making software radios more personal. *IEEE Personal Communications*, *6*(4), 13–18.
3. Singh, J. S. P., Singh, R., & Rai, M. K. (2015). Cooperative sensing for cognitive radio: A powerful access method for shadowing environment. *Wireless Personal Communications*, *80*(4), 1363–1379.
4. Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, *104*(9), 1727–1765.
5. Wyner, A. D. (1975). The wire-tap channel. *The Bell System Technical Journal*, *54*(8), 1355–1387.
6. Leung-Yan-Cheong, S., & Hellman, M. (1978). The gaussian wire-tap channel. *IEEE Transactions on Information Theory*, *24*(4), 451–456.
7. Dong, L., Han, Z., Petropulu, A. P., & Poor, H. V. (2010). Improving wireless physical-layer security via cooperating relays. *IEEE Transactions on Signal Processing*, *58*(3), 1875–1888.
8. Zou, Y., Wang, X., & Shen, W. (2013). Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE Journal on Selected Areas in Communications*, *31*(10), 2099–2111.
9. Chen, J., Zhang, R., Song, L., Han, Z., & Jiao, B. (2012). Joint relay and jammer selection for secure two-way relay networks. *IEEE Transactions on Information Forensics and Security*, *7*(1), 310–320.
10. Zhao, S., Li, Q., & Zhang, Q. (2015). Optimal secure relay beamforming for non-regenerative multi-relay networks with energy harvesting constraint. *Wireless Personal Communications*, *85*(4), 2355–2365.
11. Wang, J., Chen, J., Duan, H., et al. (2014). Jammer selection for secure two-way DF relay communications with imperfect CSI. In *2014 16th international conference on advanced communication technology (ICACT)* (pp. 300–303). IEEE.
12. Ding, X., Song, T., & Zou, Y. (2017). Security-reliability tradeoff analysis of artificial noise aided two-way opportunistic relay selection. *IEEE Transactions on Vehicular Technology*, *66*(5), 3930–3941.
13. Zhang, J., & Gursoy, M. C. (2011). Secure relay beamforming over cognitive radio channels. In *2011 45th annual conference on information sciences and systems* (pp. 1–5).
14. Wang, D., Ren, P., Du, Q., Sun, L., & Wang, Y. (2016). Cooperative relaying and jamming for primary secure communication in cognitive two-way networks. In *2016 IEEE 83rd vehicular technology conference (VTC Spring)* (pp. 1–5).
15. Alavi, F., Mokari, N., & Saeedi, H. (2015). Secure resource allocation in OFDMA-based cognitive radio networks with two-way relays. In *Electrical engineering* (pp. 171–176). IEEE.
16. Zhao, R., Yuan, Y., & Fan, L. (2017). Secrecy performance analysis of cognitive decode-and-forward relay networks in Nakagami-*m* fading channels. *IEEE Transactions on Communications*, *65*(2), 549–563.
17. Fan, J., Li, L., Bao, T., & Zhang, H. (2015). Two-way relaying with differential MPSK modulation in virtual full duplexing system. In *IEEE/CIC international conference on communications in China (ICCC), 2015* (pp. 1–5).
18. Guan, W., & Liu, K. J. R. (2011). Two-way denoise-and-forward relaying with non-coherent differential modulation. In *IEEE global telecommunications conference—GLOBECOM, 2011* (pp. 1–5).
19. Masjedi, M., Hoseini, A. M. D., & Gazor, S. (2016). Non-coherent detection and denoise-and-forward two-way relay networks. *IEEE Transactions on Communications*, *64*(11), 4497–4505.
20. Popovski, P., & Yomo, H. (2006). The anti-packets can increase the achievable throughput of a wireless multi-hop network. In *2006 IEEE international conference on communications* (Vol. 9, pp. 3885–3890).
21. Zhang, Z., Lv, T., & Yang, S. (2013). Round-robin relaying with diversity in amplify-and-forward multisource cooperative communications. *IEEE Transactions on Vehicular Technology*, *62*(3), 1251–1266.
22. Alavi, F., & Saeedi, H. (2015). Radio resource allocation to provide physical layer security in relay-assisted cognitive radio networks. *IET Communications*, *9*(17), 2124–2130.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Ruifeng Gao is currently working toward the Ph.D. degree, under the supervision of Prof. Zhihua Bao, with the School of Electronics and Information, Nantong University.

Xiaodong Ji received the Ph.D. degree in signal and information processing from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2012. He is currently an Associate Professor with the School of Electronics and Information, Nantong University.

Zhihua Bao received the M.S. degree from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 1985. He is currently a Full Professor and Doctoral Advisor with the School of Electronics and Information, Nantong University.