Switch-and-Stay Combining Relaying for Security Enhancement in Cognitive Radio Networks

Lisheng Fan[1], Shengli Zhang[2], Trung Q. Duong[3], George K. Karagiannidis[4], and Arumugam Nallanathan[5]
[1]Shantou University, Shantou, China. (e-mail:lsfan@stu.edu.cn)
[2]Shenzhen University, China. (e-mail:zsl@szu.edu.cn)
[3]Queen's University Belfast, UK. (e-mail: trung.q.duong@qub.ac.uk)
[4]Aristotle University of Thessaloniki, 54 124, Thessaloniki, Greece. (e-mail: geokarag@ieee.org)
[5]King's College London, London, UK. (e-mail: arumugam.nallanathan@kcl.ac.uk)

***Abstract*—Opportunistic relaying scheme (ORS), where the best relay is selected for dual-hop communication, has been widely considered as the global optimum relaying technique. However, due to the requirement of acquiring the full channel state information (CSI) of all links, ORS has increased the system's complexity and might be harmful to the network stability, especially for the large-scale networks. In this paper, we therefore proposed an alternative scheme, namely, secure switch-and-stay combining (SSSC) protocol for providing the best secure performance. In particular, a two-phase underlay cognitive relay network, where one out of two decode-and-forward (DF) is activated to assist the secure data transmission. The secure relay switching occurs when the relay cannot support the secure communication any longer. We study the system secure performance of SSSC protocol by deriving an analytical secrecy outage probability as well as an asymptotic expression in the high main-to-eavesdropper ratio (MER) region. It is shown that SSSC can substantially reduce the switching rate with lower channel estimation complexity, and approach the full diversity meanwhile.**

I. Introduction

Due to the broadcast nature, the wireless link from the source to destination may be overhear by some non-intended receivers (eavesdroppers), which causes the severe issue of information leakage. To prevent the wiretap, physical-layer security (PLS) as well as high-layer security has been extensively studied in the literature. In this field, Wyner firstly introduced the wiretap model to analyze the secure transmission [1], and pointed out that perfect secrecy can be achieved with properly designed encoder and decoder. Pioneered by this work, many researchers have extended to analyze the PLS performance in fading channels. In [2], the authors studied the secure transmission by analyzing the secrecy capacity with full or partial channel state information (CSI), and found that the channel fading has a positive impact on the secrecy capacity. Furthermore, the authors in [3] studied the secure performance over correlated fading channels by analyzing the secrecy capacity and secrecy outage probability (SOP), and showed that the channel correlation severely degrades the secure transmission. To enhance the system security, antenna selection can be applied for multiple-input multiple-output (MIMO) wiretap channels, where the channel fluctuation among antennas can be exploited to obtain the full system diversity gain.

As relaying technique can increase the transmission reliability, system capacity, and coverage area without additional transmit power at the transmitter, the secure transmission in relay networks has attracted much attention in recent works. There are two fundamental relaying protocols, i.e., amplify-and-forward (AF) and decode-and-forward (DF) relaying. The intercept probability of multiple AF relay networks has been studied in [4], and the opportunistic relaying scheme (ORS) is used to exploit the full diversity gain for enhancing the security. As an extension of intercept probability, the SOP is studied for multiuser multiple AF relay networks in [5], where several user and relay selection schemes are proposed to enhance the system security. The characteristic of the secure DF relay network has been studied in [6], and it is found that the placement of the DF relay can also affect the system secure metrics, such as secrecy capacity and SOP. For multiuser DF relay networks [7], ORS can be used to exploit the channel fluctuation among relays, and hence the system full diversity can be achieved to enhance the secure transmission.

Due to the scarce radio frequency spectrum, the cognitive technique is encouraged to be incorporated into relay networks to form a promising system for the next-generation wireless communications [8], [9]. Hence, the PLS of cognitive relay networks should be studied to guarantee the secure transmission. For an orthogonal frequency-division multiple access based cognitive relay network, the power and subcarrier allocations can be used to enhance the system security [10], while for cognitive relay networks with multiple relays, ORS can be used to choose the best relay to assist the secure transmission [11]–[13]. However, although ORS can efficiently exploit the full system diversity, it has two major limitations [14]–[20]. The first is the heavy load due to that the system needs to estimate the channel parameters of each relay continuously. The second limitation is the frequent relay switching rate, which is harmful to the network stability. Therefore, it is of vital importance to overcome these two limitations in order to ensure the security of the network.

In this paper, we propose a secure switch-and-stay combining (SSSC) protocol for the cognitive relay networks with

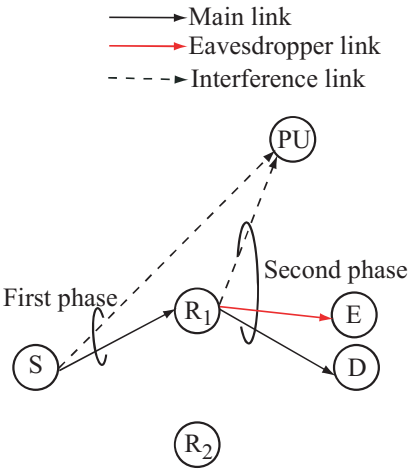

Fig. 1. Secure communication of two-phase cognitive relay networks with two DF relays.

two DF relays[1], in the presence of an eavesdropper. In SSSC, one relay out of two is chosen to be activated to assist the secure data transmission for the secondary source to secondary destination. The relay switching occurs if the relay cannot support the secure transmission any longer; otherwise, the same relay continues to be used. We study the system secure communication by analyzing the SOP. We also provide an asymptotic expression of SOP in the high main-to-eavesdropper ratio (MER) region. From this asymptotic expression, we can conclude that SSSC can approach to the system full diversity. Numerical and simulation results are demonstrated to verity the merits of SSSC.

Notation: The notation $\mathcal{CN}(0,\sigma^2)$ denotes a circularly symmetric complex Gaussian random variable (RV) with zero mean and variance σ^2. We use $f_X(\cdot)$ and $F_X(\cdot)$ to represent the probability density function (PDF) and cumulative distribution function (CDF) of RV X, respectively. Notation $\Pr[\cdot]$ returns the probability.

II. System Model

Fig. 1 depicts the considered two-phase cognitive relay network, where there are two DF relays $\{R_i|i=1,2\}$ which can assist the communication from the secondary source S to the secondary destination D. To guarantee the quality of the primary communication, the transmit power of both the secondary user and relays is constrained to limit the interference to the primary user PU. The eavesdropper E in the network can overhear the message from the relays, which brings out the issue of security. To provide the best secure performance, opportunistic relaying scheme (ORS) can be used to choose one relay out of two. However, ORS needs continuous channel estimation, which leads to an increase in system complexity. Moreover, ORS may result in a frequent relay switching rate, which is harmful to the network stability. To resolve these issues, the proposed SSSC protocol will be used for the secure communication of the considered system, where one relay will be chosen to be activated while the other is silent. Before presenting the SSSC protocol, we first detail the two-phase data transmission process, as follows.

Assume that the relay R_i ($i=1$, or 2) is activated while the other relay is silent. All nodes in the network are equipped with a single antenna due to the size limitation, and operate in a time-division half-duplex mode. Moreover, all the links in the network experience Rayleigh fading. In the first phase, the secondary user S transmits its signal x_S of unit-variance, and R_i receives y_{R_i} as

$$y_{R_i} = \sqrt{P_S} h_{S,R_i} x_S + n_{R_i}, \tag{1}$$

where $h_{S,R_i} \sim \mathcal{CN}(0,\alpha_i)$ denotes the instantaneous channel parameter of the S–R_i link and $n_{R_i} \sim \mathcal{CN}(0,\sigma^2)$ is the additive white Gaussian noise (AWGN) at the relay R_i. We denote P_S as the transmit power of S, and to guarantee the quality of primary communication, it is limited by

$$P_S = \frac{I_P}{|h_{S,PU}|^2}, \tag{2}$$

where I_P is the maximum interference level and $h_{S,PU} \sim \mathcal{CN}(0,\eta_0)$ is the instantaneous channel parameter of the S-PU link. From eqs. (1)-(2), the received SNR at R_i given by

$$\mathsf{SNR}_{R_i} = \tilde{I}_P \frac{u_i}{t_0}, \tag{3}$$

where $u_i = |h_{S,R_i}|^2$ and $t_0 = |h_{S,PU}|^2$ are the associated channel gains of the S–R_i and S–PU links, respectively, and $\tilde{I}_P = \frac{I_P}{\sigma^2}$ is the ratio of maximum interference level to noise. Suppose that R_i can correctly decode the message form the source with data rate R_d constrained by

$$\frac{1}{2}\log_2(1+\mathsf{SNR}_{R_i}) \geq R_d, \tag{4}$$

which is equivalent to $\mathsf{SNR}_{R_i} \geq \gamma_0$, with $\gamma_0 = 2^{2R_d}-1$ being a given SNR threshold. In this case, R_i forwards the correctly decoded signal, and the received signals at D and E are respectively given by

$$y_D = \sqrt{P_{R_i}} h_{R_i,D} x_S + n_D, \tag{5}$$

$$y_E = \sqrt{P_{R_i}} h_{R_i,E} x_S + n_E, \tag{6}$$

where $h_{R_i,D} \sim \mathcal{CN}(0,\beta_i)$ and $h_{R_i,E} \sim \mathcal{CN}(0,\varepsilon_i)$ are the instantaneous channel parameters of R_i–D and R_i–E links, respectively, while $n_D \sim \mathcal{CN}(0,\sigma^2)$ and $n_E \sim \mathcal{CN}(0,\sigma^2)$ are the AWGN at D and E. Moreover, P_{R_i} is the transmit power of relay R_i, and it is limited by

$$P_{R_i} = \frac{I_P}{|h_{R_i,PU}|^2}, \tag{7}$$

to guarantee the quality of service (QoS) of primary communications, where $h_{R_i,PU} \sim \mathcal{CN}(0,\eta_i)$ is the instantaneous

[1]If there exist more than two relays, we can extend the proposed SSSC to the secure switch-and-examine combining, where the extension of the derivation will be straightforward.

$$P_{out} = p_1 \underbrace{\Pr\Big[\frac{u_1}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P}, \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P E\{w_1\}} \geq T, \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1} < \gamma_s\Big]}_{J_1} + p_1 \underbrace{\Pr\Big[\frac{u_1}{t_0} < \frac{\gamma_0}{\tilde{I}_P} || \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P E\{w_1\}} < T, \frac{u_2}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P}, \frac{t_2+\tilde{I}_P v_2}{t_2+\tilde{I}_P w_2} < \gamma_s\Big]}_{J_2}$$
$$+ p_2 \underbrace{\Pr\Big[\frac{u_2}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P}, \frac{t_2+\tilde{I}_P v_2}{t_2+\tilde{I}_P E\{w_2\}} \geq T, \frac{t_2+\tilde{I}_P v_2}{t_2+\tilde{I}_P w_2} < \gamma_s\Big]}_{J_3} + p_2 \underbrace{\Pr\Big[\frac{u_2}{t_0} < \frac{\gamma_0}{\tilde{I}_P} || \frac{t_2+\tilde{I}_P v_2}{t_2+\tilde{I}_P E\{w_2\}} < T, \frac{u_1}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P}, \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1} < \gamma_s\Big]}_{J_4}, \tag{12}$$

channel parameter of the R_i–PU link. From eqs. (5)-(7), the received SNRs at D and E are written respectively as,

$$\mathsf{SNR}_D = \tilde{I}_P \frac{v_i}{t_i}, \quad \mathsf{SNR}_E = \tilde{I}_P \frac{w_i}{t_i}, \tag{8}$$

where $v_i = |h_{R_i,D}|^2$, $w_i = |h_{R_i,E}|^2$ and $t_i = |h_{R_i,PU}|^2$ are the associated channel gains.

For a predetermined secure data rate R_s, the system secure transmission will be in outage if

$$\frac{1}{2}\log_2(1+\mathsf{SNR}_D) - \frac{1}{2}\log_2(1+\mathsf{SNR}_E) < R_s, \tag{9}$$

which is equivalent to

$$\frac{1+\tilde{I}_P \frac{v_i}{t_i}}{1+\tilde{I}_P \frac{w_i}{t_i}} < \gamma_s, \tag{10}$$

where $\gamma_s = 2^{2R_s}$ is the secrecy threshold.

III. The SSSC Protocol

Before the data transmission, the system needs to determine which relay to be activated for assisting the transmission. Suppose that the relay R_i ($i = 1$, or 2) was used in the previous data transmission. Then at the beginning of the current data transmission, the system first estimates the channel parameters of the links with R_i, with the help of pilot signals. Then R_i gathers all the channel parameters through some dedicated feedback channel to determine whether or not the relay switching occurs or not. The same relay R_i will continue to be used for the current data transmission when it can correctly decode the message from the source and more importantly, it can guarantee a secure transmission. Otherwise, if R_i cannot correctly decode the message or fails to guarantee the secure transmission, the relay switching occurs, which is notified to the other nodes in the network through a dedicated feedback channel. Then the other relay R_j will be activated, and the system needs to estimate the channel parameters of main and interference links with R_j, with the help of some pilot signals. After that, the current data transmission starts through the help of R_j.

From eq. (10), we can find that a natural way to perform the security check in the above procedure is to compare $\frac{1+\tilde{I}_P \frac{v_i}{t_i}}{1+\tilde{I}_P \frac{w_i}{t_i}}$ with a given secure switching threshold T. However, the instantaneous channel parameters of eavesdropping links are hard to obtain in many practical communications, and only the statistical information may be known. In this condition, the secure relay switching condition becomes

$$\frac{1+\tilde{I}_P \frac{v_i}{t_i}}{1+\tilde{I}_P \frac{E\{w_i\}}{t_i}} \geq T, \tag{11}$$

where $E\{\cdot\}$ denotes the statistical expectation. If this equation holds and R_i can correctly decode the message, the same relay R_i will continue to be used for the current data transmission. Otherwise, the secure relay switching occurs and the other relay R_j will be activated to assist the current data transmission.

In the following section, we will study the secure performance of the SSSC protocol by deriving the analytical SOP and the asymptotic expression in high MER region.

IV. Secure Performance Analysis

A. Analytical SOP

According to the definition of SOP, we can write the SOP of SSSC in eq. (12), shown at the top of this page, where p_1 and p_2 denote the probabilities that the relay R_1 and R_2 are activated, respectively. Note that J_1 and J_3 represent the SOP when R_1 and R_2 continues to be used for the current data transmission, respectively; while J_2 and J_4 correspond to the SOP when the relay switching occurs from R_1 to R_2, and that from R_2 to R_1, respectively. Also, p_1 and p_2 are given by

$$p_1 = \frac{c_1}{c_1+c_2}, \tag{13}$$
$$p_2 = \frac{c_2}{c_1+c_2}, \tag{14}$$

where

$$c_1 = \Pr\Big[\tilde{I}_P \frac{u_1}{t_0} \geq \gamma_0, \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P E\{w_1\}} \geq T\Big], \tag{15}$$
$$c_2 = \Pr\Big[\tilde{I}_P \frac{u_2}{t_0} \geq \gamma_0, \frac{t_2+\tilde{I}_P v_2}{t_2+\tilde{I}_P E\{w_2\}} \geq T\Big], \tag{16}$$

correspond to the probabilities that R_1 and R_2 continue to be used for the current data transmission, respectively. The analytical expression of c_1, J_1 and J_2 are presented in the following proposition,

Proposition 1: An analytical expression of c_1 in eq. (15) is given by

$$c_1 = L(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_1}) L\Big(\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\Big) e^{-\frac{\varepsilon_1 T}{\beta_1}}, \tag{17}$$

where $L(x) = (1+x)^{-1}$.

$$\theta = \begin{cases} \Big[L\Big(\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\Big) - L(\frac{\gamma_s\varepsilon_1}{\beta_1})L\Big(\frac{(\gamma_s-1)\eta_1}{\tilde{I}_P\beta_1}\Big)\Big]e^{-q_0} + L\Big(\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\Big)L(-q_1\gamma_s\varepsilon_1) \\ \quad \times\Big(e^{-\frac{T\varepsilon_1}{\beta_1}-q_1T\varepsilon_1} - e^{-q_0}\Big) - L\Big(\frac{(\gamma_s-1)\eta_1}{\tilde{I}_P\beta_1}\Big)L\Big((\frac{\gamma_s}{\beta_1}-q_2\gamma_s)\varepsilon_1\Big)\Big(e^{-q_2T\varepsilon_1} - e^{-q_0}\Big) & \text{If } T<\gamma_s \\ L\Big(\frac{(T-\gamma_s)\eta_1}{\tilde{I}_P\varepsilon_1\gamma_s} + \frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\Big)\Big(1-L(\frac{\gamma_s\varepsilon_1}{\beta_1})\Big)e^{-q_0}, & \text{If } T\geq\gamma_s \end{cases} . \quad (20)$$

The analytical expressions of J_1 and J_2 are given by

$$J_1 = L(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_1})\theta, \quad (18)$$

$$J_2 = \Big[1 - L\Big(\frac{(\gamma_s-1)\eta_2}{\tilde{I}_P\beta_2}\Big)L(\frac{\gamma_s\varepsilon_2}{\beta_2})\Big] \times \Big[L(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_2}) - L\Big((\frac{1}{\alpha_1}+\frac{1}{\alpha_2})\frac{\gamma_0\eta_0}{\tilde{I}_P}\Big)L\Big(\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\Big)e^{-\frac{T\varepsilon_1}{\beta_1}}\Big], \quad (19)$$

where θ is given by eq. (20), shown at the top of this page, and

$$\begin{cases} q_0 = \dfrac{T}{\gamma_s} + \dfrac{T\varepsilon_1}{\beta_1} \\ q_1 = (\dfrac{1}{\eta_1} + \dfrac{T-1}{\tilde{I}_P\beta_1})\dfrac{\tilde{I}_P}{\gamma_s - T} \\ q_2 = (\dfrac{1}{\eta_1} + \dfrac{\gamma_s-1}{\tilde{I}_P\beta_1})\dfrac{\tilde{I}_P}{\gamma_s - T} \end{cases} . \quad (21)$$

Proof: See Appendix A. ■

Through replacing α_1 by α_2, β_1 with β_2, and η_1 with η_2, we can obtain the analytical expression of c_2 from the expression of c_1 in Proposition 1. This leads to the analytical expressions of p_1 and p_2. By swapping α_1 with α_2, β_1 with β_2, and η_1 with η_2, we can obtain the analytical expressions of J_3 and J_4 from the expressions of J_1 and J_2 in Proposition 1. In this way, we arrive at the analytical expression of SOP as $P_{out} = p_1(J_1 + J_2) + p_2(J_3 + J_4)$.

B. Asymptotic SOP

To obtain some insights on the system with SSSC protocol, we now derive the asymptotic SOP in large $\tilde{I}_P$ and MER regions. By applying the approximation of $(1+x)^{-1} \simeq 1-x$ for small value of $|x|$ [21], we can obtain the asymptotic c_1 and c_2 with large $\tilde{I}_P$ and MER as

$$c_1 \simeq 1, \quad c_2 \simeq 1. \quad (22)$$

Accordingly, the asymptotic p_1 and p_2 are given by

$$p_1 \simeq \frac{1}{2}, \quad p_2 \simeq \frac{1}{2}. \quad (23)$$

In further, the asymptotic expressions of J_1, J_2, J_3 and J_4 are

$$J_1 \simeq \frac{\gamma_s}{\lambda_1}e^{-\frac{T}{\gamma_s}}, \quad J_2 \simeq \frac{\gamma_s T}{\lambda_1\lambda_2}, \quad (24)$$

$$J_3 \simeq \frac{\gamma_s}{\lambda_2}e^{-\frac{T}{\gamma_s}}, \quad J_4 \simeq \frac{\gamma_s T}{\lambda_1\lambda_2}, \quad (25)$$

where $\lambda_1 = \frac{\beta_1}{\varepsilon_1}$ and $\lambda_2 = \frac{\beta_2}{\varepsilon_2}$ are the MER with relay R_1 and R_2, respectively. By summarizing the above asymptotic expressions, we can obtain the asymptotic SOP as

$$P_{out} \simeq \frac{\gamma_s T}{\lambda_1\lambda_2} + \frac{\gamma_s}{2}\Big(\frac{1}{\lambda_1} + \frac{1}{\lambda_2}\Big)e^{-\frac{T}{\gamma_s}}. \quad (26)$$

By setting the derivative of P_{out} with respect to T into zero, we can obtain the optimal value of the secure switching threshold T^* as

$$T^* = \gamma_s \ln\frac{\lambda_1+\lambda_2}{2\gamma_s}, \quad (27)$$

which can lead to the minimum P_{out},

$$P_{out,min} = \frac{\gamma_s^2}{\lambda_1\lambda_2}\Big(1 + \ln\frac{\lambda_1+\lambda_2}{2\gamma_s}\Big). \quad (28)$$

From these asymptotic results, we can achieve the following insights on the system:

Remark 1: As both c_1 and c_2 approach to 1 in high $\tilde{I}_P$ and MER region, the same relay will continue to be used for data transmission in a long time. Hence, the SSSC protocol can substantially reduce the system implementation complexity compared with ORS.

Remark 2: From the asymptotic P_{out} in eq.(26), we can find that the system diversity order falls between one and two. In particular, the system diversity order can approach to two for a large value of T, which can effectively exploit the two relays to guarantee the secure transmission.

V. Simulation and Numerical Results

In this section, numerical and simulation results are presented to verify the proposed studies. All the links in the system experience Rayleigh flat fading. The distance between the secondary source and destination is set to unity, and the two relays are between in them. Let D_1 and D_2 denote the distance from the secondary source to relay R_1 and R_2, respectively. Accordingly, the average channel gains of the two-hop main links are set to $\alpha_1 = D_1^{-4}$, $\alpha_2 = D_2^{-4}$, $\beta_1 = (1-D_1)^{-4}$, and $\beta_2 = (1-D_2)^{-4}$, where the path-loss model with loss factor of four is used. Without loss of generality, we set the average channel gains of interference links to unity, so that $\eta_0 = \eta_1 = \eta_2 = 1$.

Fig. 2 depicts the system secrecy outage probability of SSSC versus MER with $\lambda_1 = \lambda_2 = \lambda$ and $\tilde{I}_P = 40$dB, where the secure switching threshold T varies in $\{0.5, 1, 2\}T^*$ and the optimal switching threshold T^* is set to $\gamma_s \ln\frac{\lambda_1+\lambda_2}{2\gamma_s}$. For comparison, we plot the simulated secrecy outage probabilities of ORS and the relay system with only one relay as the lower

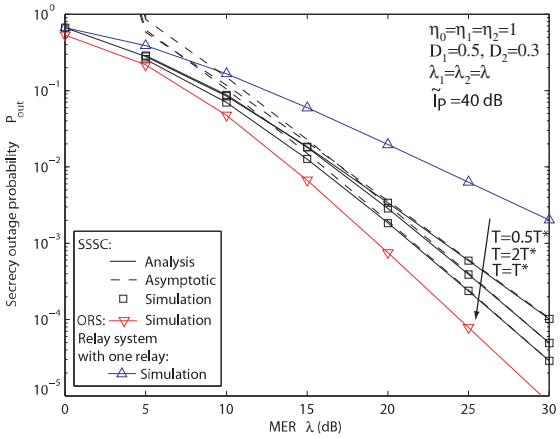

Fig. 2. Secrecy outage probability versus MER

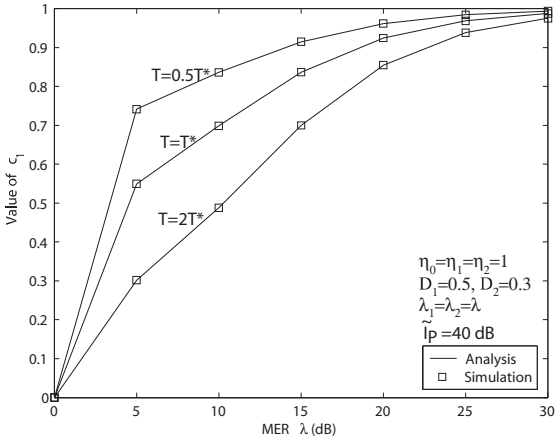

Fig. 3. Effect of T on c_1 versus MER

and upper bounds, respectively. As observed from Fig. 2, we can find that the analytical result of SSSC matches well with the simulation one, and the asymptotic result converges to the exact value in high MER region. This verifies the validity of the derived analytical secrecy outage probability of SSSC and asymptotic expression. Moreover, the lines with $T \in \{1,2\}T^*$ are approximately parallel with ORS, indicating that SSSC protocol can approach the system full diversity order of two in high MER region.

Fig. 3 illustrates the effect of T on the simulation and analytical results of c_1[2] of SSSC versus MER with $\lambda_1 = \lambda_2 = \lambda$ and $\tilde{I}_P = 40$dB, where the secure switching threshold T varies in $\{0.5, 1, 2\}T^*$. From this figure, we can find that c_1 increases with larger $\tilde{I}_P$ and smaller T. In particular, c_1 converges to one with large value of $\tilde{I}_P$, indicating that the secure relay switching seldom occurs and the system needs to estimate the channel parameters of only one relay. In other words, the SSSC technique can reduce the channel estimation complexity of ORS to almost half and meanwhile substantially reduce the relay switching rate.

[2]As c_2 shows the similar behavior as c_1, the result of c_2 is not plotted in this figure for clarity.

VI. Conclusions

To achieve the secure performance of ORS with less system's complexity, this paper proposed an alternative secure switch-and-stay combining (SSSC) for cognitive relay networks with two DF relays. In SSSC, one relay out of two was chosen to be activated to assist the data transmission from the secondary source to secondary destination. The same relay continued to be used for data transmission when the relay could support the secure data transmission; otherwise the secure relay switching occurred and the other relay would be activated. It has been shown by the simulation and numerical results that SSSC can not only approach to the secure diversity as ORS, but also reduce the switching rate with less channel estimation complexity.

Appendix A
Proof of Proposition 1

From eq. (15), we can write the expression of c_1 as

$$c_1 = \Pr\Big(\frac{u_1}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P}\Big) \cdot \Pr\Big(\frac{t_1 + \tilde{I}_P v_1}{t_1 + \tilde{I}_P E\{w_1\}} \geq T\Big) \quad \text{(A.1)}$$

$$= L\Big(\frac{\gamma_0 \eta_0}{\tilde{I}_P \alpha_1}\Big) \Pr\Big(\frac{t_1 + \tilde{I}_P v_1}{t_1 + \tilde{I}_P \varepsilon_1} \geq T\Big), \quad \text{(A.2)}$$

where we apply the the PDFs of $f_{u_1}(x) = \frac{1}{\alpha_1} e^{-\frac{x}{\alpha_1}}$ and $f_{t_0}(x) = \frac{1}{\eta_0} e^{-\frac{x}{\eta_0}}$ in the last equality. $\Pr\Big(\frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P \varepsilon_1} \geq T\Big)$ can be computed as

$$\Pr\Big(\frac{t_1 + \tilde{I}_P v_1}{t_1 + \tilde{I}_P \varepsilon_1} \geq T\Big) = \Pr\Big(v_1 \geq \frac{T-1}{\tilde{I}_P} t_1 + T\varepsilon_1\Big) \quad \text{(A.3)}$$

$$= \int_0^\infty f_{t_1}(t_1) \int_{\frac{T-1}{\tilde{I}_P} t_1 + T\varepsilon_1}^\infty f_{v_1}(v_1) dv_1 dt_1 \quad \text{(A.4)}$$

$$= L\Big(\frac{(T-1)\eta_1}{\tilde{I}_P \beta_1}\Big) e^{-\frac{\varepsilon_1 T}{\beta_1}}, \quad \text{(A.5)}$$

By combining the results of eqs. (A.2) and (A.5), we can obtain the analytical expression of c_1, as shown in eq. (17) of Proposition 1.

We now turn to derive the analytical expression of J_1 in eq. (12) as

$$J_1 = \Pr\Big(\frac{u_1}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P}\Big) \cdot \Pr\Big(\frac{t_1 + \tilde{I}_P v_1}{t_1 + \tilde{I}_P E\{w_1\}} \geq T, \frac{t_1 + \tilde{I}_P v_1}{t_1 + \tilde{I}_P w_1} < \gamma_s\Big) \quad \text{(A.6)}$$

$$= L\Big(\frac{\gamma_0 \eta_0}{\tilde{I}_P \alpha_1}\Big) \underbrace{\Pr\Big(v_1 \geq \frac{T-1}{\tilde{I}_P} t_1 + T\varepsilon_1, v_1 < \frac{\gamma_s - 1}{\tilde{I}_P} t_1 + T w_1\Big)}_{J_{11}}, \quad \text{(A.7)}$$

Note that in J_{11} above, $\frac{\gamma_s-1}{\tilde{I}_P}t_1+Tw_1$ needs to be larger than $\frac{T-1}{\tilde{I}_P}t_1+T\varepsilon_1$, causing that

$$\gamma_s w_1 \geq \frac{T-\gamma_s}{\tilde{I}_P}t_1+T\varepsilon_1. \tag{A.8}$$

Hence we now consider the two cases of $T \geq \gamma_s$ and $T < \gamma_s$. If $T \geq \gamma_s$, the condition of eq. (A.8) becomes

$$w_1 \geq \frac{T-1}{\tilde{I}_P\gamma_s}t_1+\frac{T\varepsilon_1}{\gamma_s}, \tag{A.9}$$

and J_{11} is computed as

$$\begin{aligned} J_{11} &= \int_0^\infty f_{t_1}(t_1)\int_{\frac{T-1}{\tilde{I}_P\gamma_s}t_1+\frac{T\varepsilon_1}{\gamma_s}}^\infty f_{w_1}(w_1) \\ &\quad\times\int_{\frac{T-1}{\tilde{I}_P}t_1+T\varepsilon_1}^{\frac{\gamma_s-1}{\tilde{I}_P}t_1+Tw_1} f_{v_1}(v_1)dv_1dw_1dt_1 \qquad (A.10)\\ &= L\Big(\frac{(T-\gamma_s)\eta_1}{\tilde{I}_P\varepsilon_1\gamma_s}+\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\Big)\Big(1-L(\frac{\gamma_s\varepsilon_1}{\beta_1})\Big)e^{-q_0}, \qquad (A.11)\end{aligned}$$

where q_0 is defined in eq. (21).

On the other hand, when $T < \gamma_s$ holds, the condition of eq. (A.8) becomes

$$w_1+\frac{\gamma_s-T}{\tilde{I}_P\gamma_s}t_1 \geq \frac{T\varepsilon_1}{\gamma_s}. \tag{A.12}$$

This condition can be specified into two integral regions of $w_1 \geq \frac{T\varepsilon_1}{\gamma_s}$ and $w_1 < \frac{T\varepsilon_1}{\gamma_s}$ with $t_1 \geq \frac{\tilde{I}_PT\varepsilon_1-\tilde{I}_P\gamma_sw_1}{\gamma_s-T}$. Accordingly, we can compute J_{11} as

$$\begin{aligned} J_{11} &= \int_0^\infty f_{t_1}(t_1)\int_{\frac{T\varepsilon_1}{\gamma_s}}^\infty f_{w_1}(w_1)\int_{\frac{T-1}{\tilde{I}_P}t_1+T\varepsilon_1}^{\frac{\gamma_s-1}{\tilde{I}_P}t_1+Tw_1} f_{v_1}(v_1)dv_1dw_1dt_1 \\ &\quad+\int_0^{\frac{T\varepsilon_1}{\gamma_s}} f_{w_1}(w_1)\int_{\frac{\tilde{I}_PT\varepsilon_1-\tilde{I}_P\gamma_sw_1}{\gamma_s-T}}^\infty f_{t_1}(t_1) \\ &\quad\times\int_{\frac{T-1}{\tilde{I}_P}t_1+T\varepsilon_1}^{\frac{\gamma_s-1}{\tilde{I}_P}t_1+Tw_1} f_{v_1}(v_1)dv_1dt_1dw_1 \qquad (A.13)\\ &= \Big[L\Big(\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\Big)-L(\frac{\gamma_s\varepsilon_1}{\beta_1})L\Big(\frac{(\gamma_s-1)\eta_1}{\tilde{I}_P\beta_1}\Big)\Big]e^{-q_0} \\ &\quad+L\Big(\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\Big)L(-q_1\gamma_s\varepsilon_1)\Big(e^{-\frac{T\varepsilon_1}{\beta_1}-q_1T\varepsilon_1}-e^{-q_0}\Big) \\ &\quad-L\Big(\frac{(\gamma_s-1)\eta_1}{\tilde{I}_P\beta_1}\Big)L\Big((\frac{\gamma_s}{\beta_1}-q_2\gamma_s)\varepsilon_1\Big)\Big(e^{-q_2T\varepsilon_1}-e^{-q_0}\Big), \qquad (A.14)\end{aligned}$$

where q_1 and q_2 are defined in eq. (21). By combining eqs. (A.7), (A.11) and (A.14), we can arrive at the analytical expression of J_1, as shown in eq. (18) of Proposition 1. In a similar way, we can obtain the analytical expression of J_2, and hence we complete the proof of Proposition 1.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[2] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[3] X. Sun, J. Wang, W. Xu, , and C. Zhao, "Performance of secure communications over correlated fading channels," *IEEE Sig. Proc. Lett.*, vol. 19, no. 8, pp. 479–482, Aug. 2012.

[4] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Select. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[5] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3299–3310, Sept. 2014.

[6] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, Jun. 2012.

[7] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Commun.*, vol. 4, no. 15, pp. 1787–1791, Oct. 2010.

[8] T. Q. Duong, P. L. Yeoh, V. N. Q. Bao, M. Elkashlan, and N. Yang, "Cognitive relay networks with multiple primary transceivers under spectrum-sharing," *IEEE Signal Processing Lett.*, vol. 19, no. 11, pp. 741–744, Nov. 2012.

[9] T. Q. Duong, D. B. da Costa, T. A. Tsiftsis, C. Zhong, and A. Nallanathan, "Outage and diversity of cognitive relaying systems under spectrum sharing environments in Nakagami-m fading," *IEEE Commun. Lett.*, vol. 16, no. 12, pp. 2075–2078, Dec. 2012.

[10] N. Mokari, S. Parsaeefard, H. Saeedi, P. Azmi, and E. Hossain, "Secure robust ergodic uplink resource allocation in relay-assisted cognitive radio networks," *IEEE Trans. Sig. Proc.*, vol. 63, no. 2, pp. 291–304, Jan. 2015.

[11] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Commun.*, vol. 6, no. 16, pp. 2676–2687, Nov. 2012.

[12] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Commun. Lett.*, vol. pp, no. 99, 2015.

[13] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. Commun.*, vol. pp, no. 99, 2015.

[14] D. S. Michalopoulos and G. K. Karagiannidis, "Distributed switch and stay combining (DSSC) with a single decode and forward relay," *IEEE Commun. Lett.*, vol. 11, no. 5, pp. 408–410, May 2007.

[15] ——, "Two-relay distributed switch and stay combining," *IEEE Trans. Commun.*, vol. 56, no. 11, pp. 1790–1794, Nov. 2008.

[16] V. N. Q. Bao and H. Y. Kong, "Distributed switch and stay combining for selection relay networks," *IEEE Commun. Lett.*, vol. 13, no. 12, pp. 914–916, Dec. 2009.

[17] C. Xiao and N. C. Beaulieu, "Node switching rates of opportunistic relaying and switch-and-examine relaying in Rician and Nakagami-m fading," *IEEE Trans. Commun.*, vol. 60, no. 2, pp. 488–498, Feb. 2012.

[18] D. S. Michalopoulos, A. S. Lioumpas, G. K. Karagiannidis, and R. Schober, "Selective cooperative relaying over time-varying channels," *IEEE Trans. Commun.*, vol. 48, no. 8, pp. 2402–2412, Aug. 2010.

[19] M. Yan, Q. Chen, X. Lei, T. Q. Duong, and P. Fan, "Outage probability of switch and stay combining in two-way amplify-and-forward relay networks," *IEEE Wirelss Commun. Lett.*, vol. 1, no. 4, pp. 296–299, Aug. 2012.

[20] L. Fan, X. Lei, R. Q. Hu, and S. Zhang, "Distributed two-way switch and stay combining with a single amplify-and-forward relay," *IEEE Wirelss Commun. Lett.*, vol. 2, no. 4, pp. 379–382, Aug. 2013.

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