Secure Switch-and-Stay Combining (SSSC) for Cognitive Relay Networks

Lisheng Fan, Shengli Zhang, Trung Q. Duong, *Senior Member, IEEE*, and George K. Karagiannidis, *Fellow, IEEE*

***Abstract*—In this paper, we study a two-phase underlay cognitive relay network, where there exists an eavesdropper who can overhear the message. The secure data transmission from the secondary source to secondary destination is assisted by two decode-and-forward (DF) relays. Although the traditional opportunistic relaying technique can choose one relay to provide the best secure performance, it needs to continuously have the channel state information (CSI) of both relays, and may result in a high relay switching rate. To overcome these limitations, a secure switch-and-stay combining (SSSC) protocol is proposed where only one out of the two relays is activated to assist the secure data transmission, and the secure relay switching occurs when the relay cannot support the secure communication any longer. This security switching is assisted by either instantaneous or statistical eavesdropping CSI. For these two cases, we study the system secure performance of SSSC protocol, by deriving the analytical secrecy outage probability as well as an asymptotic expression for the high main-to-eavesdropper ratio (MER) region. We show that SSSC can substantially reduce the system complexity while achieving or approaching the full diversity order of opportunistic relaying in the presence of the instantaneous or statistical eavesdropping CSI.**

***Index Terms*—Secure switch-and-stay combining (SSSC), cognitive relay networks, secure communication, diversity order.**

Manuscript received March 5, 2015; revised July 18, 2015 and October 18, 2015; accepted October 22, 2015. Date of publication November 3, 2015; date of current version January 14, 2016. This work was supported in part by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22, in part by the NSF of China under Grant 61372129/61372078/61471229, in part by the NSF of Guangdong Province, China under Grant 2014A030306027, in part by the National 973 Project under Grant 2013CB336700, in part by the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (No. 2013D04), in part by the training program of Excellent Young Teachers in Higher Education Institutions of Guangdong Province (No. Yq2013070), in part by the Foundation of Shenzhen City (No. KQCX20140509172609163), and in part by the Natural Science Foundation of Shenzhen University (No. 00002501), and the high-quality University projects of Guangdong Province. This work was presented in part at the IEEE Global Communications Conference (GLOBECOM), San Diego, CA, December 2015. The associate editor coordinating the review of this paper and approving it for publication was H.-C. Yang. *(Corresponding author: Shengli Zhang.)*

L. Fan is with the Department of Electronic Engineering, Shantou University, Shantou, China, the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China, and also with the School of Computer Science and Educational Software, Guangzhou University, Guangzhou, China (e-mail: lsfan@stu.edu.cn).

S. Zhang is with College of Information Engineering, Shenzhen University, Shenzhen, China (e-mail: zsl@szu.edu.cn).

T. Q. Duong is with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast, U.K. (e-mail: trung.q.duong@qub.ac.uk).

G. K. Karagiannidis is with the Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, Thessaloniki 54 124, Greece (e-mail: geokarag@ieee.org).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2015.2497308

I. Introduction

DUE TO the broadcast nature, the wireless link from the source to destination may be overheard by some non-intended eavesdroppers, which causes the severe issue of wireless security. To prevent the wiretap, physical-layer security (PLS) as well as high-layer security has been proposed and extensively studied in the literature [1]–[5]. 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 extensively analyzed 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 demonstrated 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 techniques [6]–[9] 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 [10], and the opportunistic relaying technique 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 [11], where several users and relay selection schemes are proposed to enhance the system security. In addition, the asymptotic secure performance is investigated with the high main-to-eavesdropper ratio (MER), defined as the ratio of average channel gain from the relay to intended receiver to that from relay to eavesdropper. The secure characteristics of the DF relay network has been studied in [12], 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 [13], opportunistic relaying can be used to exploit the channel fluctuation among relays, and hence the full diversity of wireless system can be achieved. To further enhance the network security, the other techniques such as jamming, beamforming and resource allocation have been investigated for relay networks [14]–[24].

Due to the scarce radio frequency spectrum, the cognitive technique [25] is encouraged to be incorporated into relay networks to form a promising system for the next generation of wireless communications networks. Hence, the PLS of cognitive relay networks should be studied to guarantee the secure transmission. Various resource allocation strategies have been proposed to enhance the system security of cognitive relay networks. Specifically, power allocation can be applied to optimize the total transmit power among network nodes to improve the transmission security [26], [27]. For cognitive relay networks with multiple relays, opportunistic relaying can be used to choose the best relay to assist the secure transmission [28]–[30]. Although the opportunistic relaying can efficiently exploit the full system diversity, it has two major limitations [31]–[38]. The first limitation is the heavy load due to the system's needs to estimate the channel parameters of each relay continuously. The second limitation is the high relay switching rate, which is harmful to the network stability. Therefore, it is of vital importance to overcome these two limitations to ensure the security of the network.

Motivated by the aforementioned discussion, in this paper, we propose a secure switching-and-stay combining (SSSC) protocol for the cognitive relay networks with two DF relays, 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. The secure relay switching is assisted by the instantaneous eavesdropping CSI (I-ECSI) or statistical eavesdropping CSI (S-ECSI). In comparison with the conventional opportunistic relaying for secure cognitive relay networks [28]–[30], SSSC can reduce the channel estimation complexity, decrease the relay switching rate, and simultaneously maintain the secure performance. The key contributions of this paper are summarized as follow:

- We propose the SSSC protocol for the cognitive relay networks, in order to reduce the channel estimation complexity, keep the network stability, and simultaneously maintain the secure performance.
- For the SSSC with either I-ECSI or S-ECSI, we present an analytical expression for the system secrecy outage probability, in order to investigate the secure performance achieved by SSSC.
- We present new results for the asymptotic secrecy outage probability of SSSC. These asymptotic expressions enable us to determine the major factors that regulate the secure performance in the high transmit power and MER regions.
- Based on the asymptotic results, it is shown that SSSC with instantaneous eavesdropping CSI can achieve the system full diversity, and SSSC with statistical eavesdropping CSI can also approach this diversity.

The organization of this paper is as follows. After the introduction, Section II describes the model of a secure cognitive relay network with two DF relays, and Section III presents the SSSC protocol. For SSSC with either I-ECSI or S-ECSI, Section IV gives the secrecy outage probabilities, including the derivations for both the exact and asymptotic results. Numerical results are provided in Section V to offer valuable insights into the secure performance. Conclusions are drawn in Section VI.

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

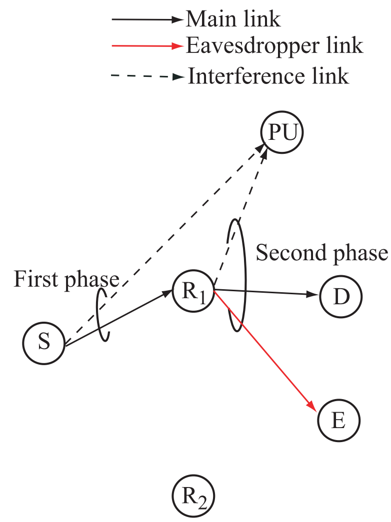


Fig. 1. Secure communication of two-phase underlay cognitive relay networks with two DF relays.

II. SYSTEM MODEL

Fig. 1 depicts the considered two-phase underlay cognitive relay network with two DF relays $\{R_i | i = 1, 2\}$ which can assist the communication from the secondary source S to the secondary destination D. In the underlay spectrum-sharing mode, the transmit power of both the secondary user and relays is constrained to limit the interference to the primary user PU, in order to guarantee the Quality-of-Service (QoS) of primary communications. The eavesdropper E in the network can overhear the message from the relays, which yields the issue of information wiretap. We consider severe shadowing environments, so that the direct links from the source S to D and E do not exist. While it is interesting to consider moderate shadowing environments and study the impact of direct links on the secure performance [14], [39], this is beyond the scope of this work. The considered system model in Fig. 1 can be applied to the communication of cognitive relay networks in unsecure environments, where the secondary information transmission may be wiretapped.

To provide the best secure performance, opportunistic relaying technique can be used to choose one relay out of two. However, opportunistic relaying needs continuous channel estimation, which leads to an increase in system complexity and may result in a high relay switching rate. To resolve these issues, the proposed SSSC protocol will be used, where one relay is activated while the other is silent[1]. 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 R_j ($j \neq i$) 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 independent 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 $h_{S,R_i} \sim \mathcal{CN}(0, \alpha_i)$ is 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 (1)–(2), the received SNR at R_i is 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 $\tilde{I}_P = I_P/\sigma^2$ is the maximum interference level-to-noise ratio. Suppose that R_i can correctly decode the message from the source with data rate R_d being 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 $h_{R_i,D} \sim \mathcal{CN}(0, \beta_i)$, $h_{R_i,E} \sim \mathcal{CN}(0, \varepsilon_i)$ 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 AWGNs at D and E, respectively. In addition, P_{R_i} is the transmit power of relay R_i, which is limited by

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

[1]Note that the main purpose of this work is to reduce the implementation complexity of the secure relay networks and simultaneously maintain the secure performance. Although the other relay can use the cooperative jamming to enhance the system security, it will cause an increase in the implementation complexity, such as synchronization and message exchange between the network nodes [14]–[16]. Hence jamming technique is not considered in this work.

to guarantee the QoS of primary communications, where $h_{R_i,PU} \sim \mathcal{CN}(0, \eta_i)$ is the instantaneous channel parameter of the R_i–PU link. From (5)–(7), the received SNRs at D and E are written respectively as

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

$$\mathsf{SNR}_E = \tilde{I}_P \frac{w_i}{t_i}, \tag{9}$$

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.

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

$$\frac{1}{2}\log_2(1 + \mathsf{SNR}_D) - \frac{1}{2}\log_2(1 + \mathsf{SNR}_E) < R_s. \tag{10}$$

From (10), we can find that the received SNR at eavesdropper E should not exceed the SNR at D to obtain a non-zero secrecy rate. This constraint is different from that at the primary user, and hence the eavesdropper cannot be assumed as another primary user. After some manipulations, (10) can be further written as

$$\frac{1 + \tilde{I}_P \frac{v_i}{t_i}}{1 + \tilde{I}_P \frac{w_i}{t_i}} < \gamma_s, \tag{11}$$

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

III. Description of the SSSC Protocol

Before the data transmission, the system needs to determine which relay to be activated for assisting the secure 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 from the help of pilot signals. Then R_i gathers all the channel parameters through some dedicated feedback channels. Specifically, the secondary R_i can gather the channel parameters of interference links from the primary user by using several techniques, e.g., direct feedback from PU, indirect feedback from band manager. More details about acquiring the channel information of interference links can be found in [40]–[43]. As to the channel parameters of eavesdropper links, the secondary R_i can obtain these parameters through some feedback when the eavesdropper is active, e.g., the eavesdropper is another active user in the network. On the other hand, when the eavesdropper is passive, R_i can still obtain the statistical information of eavesdropper links, by some ways, such as estimating the eavesdropper's location in the network. More details about acquiring the channel information of eavesdropper links can be found in [11], [44].

After obtaining the required channel information, SSSC will use the same relay R_i for the current data transmission when R_i can correctly decode the message from the source and more importantly, it can guarantee a secure transmission as

$$\frac{1 + \tilde{I}_P \frac{v_i}{t_i}}{1 + \tilde{I}_P \frac{w_i}{t_i}} \geq T, \tag{12}$$

where T is a given secure switching threshold. Otherwise, if R_i cannot correctly decode the message or fails to guarantee the secure transmission as described by (12), a 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 pilot signals. After that, the current data transmission starts through the help of R_j.

Note that in (12), the relay R_i needs to know the instantaneous CSI of the eavesdropper link, in order to determine whether the secure relay switching occurs or not. In some communication scenarios, the instantaneous CSI of eavesdropper link is however hard to obtain, and only its statistical information may be known. In this case, the secure relay switching metric in (12) becomes

$$\frac{1+\tilde{I}_P\frac{v_i}{t_i}}{1+\tilde{I}_P\frac{E\{w_i\}}{t_i}} \geq T, \tag{13}$$

where $E\{\cdot\}$ denotes the statistical expectation. If the above 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.

From (12) and (13), we can conclude that the relay switching of SSSC depends not only on the transmission quality of main links, but also on whether the relay can support a secure transmission or not. In contrast, the relay switching of SSC in non-secure networks [31]–[38] depends only on the transmission quality of main links. As such, the switching mechanism of SSSC is much more complicated than that of SSC in non-secure networks. More importantly, the mathematical analysis of the system performance becomes much more complex. In the following section, we study the secure performance of the SSSC protocol by analyzing SOP in the two cases of I-ECSI and S-ECSI.

IV. Secure Performance Analysis

A. Analytical SOP With I-ECSI

For a secure transmission system, the system SOP is defined as the probability that the difference in data rate between the main link and eavesdropper link drops below a predetermined data rate. From this definition and (10)–(11), we can write the SOP of SSSC with I-ECSI in (14), shown at the bottom of the page, where the notation || denotes the logical OR operation. p_1 and p_2 are 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 continue 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 vice versa, respectively. Also p_1 and p_2 are given by

$$p_1 = \frac{c_1}{c_1+c_2}, \tag{15}$$

$$p_2 = \frac{c_2}{c_1+c_2}, \tag{16}$$

where

$$c_1 = \Pr\left[\tilde{I}_P\frac{u_1}{t_0} \geq \gamma_0, \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1} \geq T\right], \tag{17}$$

$$c_2 = \Pr\left[\tilde{I}_P\frac{u_2}{t_0} \geq \gamma_0, \frac{t_2+\tilde{I}_P v_2}{t_2+\tilde{I}_P w_2} \geq T\right], \tag{18}$$

correspond to the probabilities that R_1 and R_2 continue to be used for the current data transmission, respectively. Note that the two relay branches share the common random variable of t_0 related to the transmit power P_S at the secondary source, when the secure relay switching occurs in J_2 and J_4. This causes the data transmission of both branches to be correlated and makes the mathematical analysis more complicated.

To solve this mathematical troublesome, we present the analytical expressions of c_1, J_1 and J_2 in the following proposition,

Proposition 1: An analytical expression of c_1 is given by

$$c_1 = L\left(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_1}\right)L\left(\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\right)L\left(\frac{T\varepsilon_1}{\beta_1}\right), \tag{19}$$

where $L(x) = (1+x)^{-1}$ and (19) is obtained by applying the probability density functions of $f_{u_1}(x) = \frac{1}{\alpha_1}e^{-\frac{x}{\alpha_1}}$, $f_{t_0}(x) = \frac{1}{\eta_0}e^{-\frac{x}{\eta_0}}$, $f_{t_1}(x) = \frac{1}{\eta_1}e^{-\frac{x}{\eta_1}}$, $f_{v_1}(x) = \frac{1}{\beta_1}e^{-\frac{x}{\beta_1}}$ and $f_{w_1}(x) = \frac{1}{\varepsilon_1}e^{-\frac{x}{\varepsilon_1}}$ [45]. The analytical expressions of J_1 and J_2 are given by

$$\begin{aligned} P_{out} = {} & p_1 \underbrace{\Pr\left[\tilde{I}_P\frac{u_1}{t_0} \geq \gamma_0, \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1} \geq T, \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1} < \gamma_s\right]}_{J_1} + p_1 \underbrace{\Pr\left[\tilde{I}_P\frac{u_1}{t_0} < \gamma_0 || \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1} < T, \tilde{I}_P\frac{u_2}{t_0} \geq \gamma_0, \frac{t_2+\tilde{I}_P v_2}{t_2+\tilde{I}_P w_2} < \gamma_s\right]}_{J_2} \\ & + p_2 \underbrace{\Pr\left[\tilde{I}_P\frac{u_2}{t_0} \geq \gamma_0, \frac{t_2+\tilde{I}_P v_2}{t_2+\tilde{I}_P w_2} \geq T, \frac{t_2+\tilde{I}_P v_2}{t_2+\tilde{I}_P w_2} < \gamma_s\right]}_{J_3} + p_2 \underbrace{\Pr\left[\tilde{I}_P\frac{u_2}{t_0} < \gamma_0 || \frac{t_2+\tilde{I}_P v_2}{t_2+\tilde{I}_P w_2} < T, \tilde{I}_P\frac{u_1}{t_0} \geq \gamma_0, \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1} < \gamma_s\right]}_{J_4}, \end{aligned} \tag{14}$$

$$J_1 = \begin{cases} L\left(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_1}\right)\left[L\left(\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\right)L\left(\frac{T\varepsilon_1}{\beta_1}\right)\right. \\ \left.-L\left(\frac{(\gamma_s-1)\eta_1}{\tilde{I}_P\beta_1}\right)L\left(\frac{\gamma_s\varepsilon_1}{\beta_1}\right)\right], & \text{If } T<\gamma_s \\ 0, & \text{If } T\geq\gamma_s \end{cases}. \quad (20)$$

$$J_2 = \left[1 - L\left(\frac{(\gamma_s-1)\eta_2}{\tilde{I}_P\beta_2}\right)L\left(\frac{\gamma_s\varepsilon_2}{\beta_2}\right)\right]\left[L\left(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_2}\right)\right. \\ \left. -L\left(\left(\frac{1}{\alpha_1}+\frac{1}{\alpha_2}\right)\frac{\gamma_0\eta_0}{\tilde{I}_P}\right)L\left(\frac{(T-1\eta_1)}{\tilde{I}_P\beta_1}\right)L\left(\frac{T\varepsilon_1}{\beta_1}\right)\right]. \quad (21)$$

Proof: See Appendix A. ■

By replacing α_1, β_1, η_1 and ε_1 by α_2, β_2, η_2 and ε_2 respectively, 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. Similarly, 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 with I-ECSI as $P_{out} = p_1(J_1 + J_2) + p_2(J_3 + J_4)$.

B. Analytical SOP With S-ECSI

According to the definition of SOP, we can write the SOP of SSSC with S-ECSI in (22), shown at the bottom of the page, where $\tilde{J}_1$ and $\tilde{J}_3$ represent the SOP when R_1 and R_2 continue to be used for the current data transmission, respectively, while $\tilde{J}_2$ and $\tilde{J}_4$ 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, $\tilde{p}_1$ and $\tilde{p}_2$ are given by

$$\tilde{p}_1 = \frac{\tilde{c}_1}{\tilde{c}_1+\tilde{c}_2}, \quad (23)$$

$$\tilde{p}_2 = \frac{\tilde{c}_2}{\tilde{c}_1+\tilde{c}_2}, \quad (24)$$

where

$$\tilde{c}_1 = \Pr\left[\tilde{I}_P\frac{u_1}{t_0}\geq\gamma_0, \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P E\{w_1\}}\geq T\right], \quad (25)$$

$$\tilde{c}_2 = \Pr\left[\tilde{I}_P\frac{u_2}{t_0}\geq\gamma_0, \frac{t_2+\tilde{I}_P v_2}{t_2+\tilde{I}_P E\{w_2\}}\geq T\right], \quad (26)$$

correspond to the probabilities that R_1 and R_2 continue to be used for the current data transmission, respectively. Similar to the analysis of J_2 and J_4, the two relay branches share the common random variable of t_0, when the secure relay switching occurs in $\tilde{J}_2$ and $\tilde{J}_4$. This makes the data transmission of both branches correlated, and the mathematical analysis becomes more complicated. Moreover, the secure switching metric $\frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P E\{w_1\}}$ is highly correlated with the outage metric $\frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1}$, but not the same. This correlation will also cause much difficulty to the mathematical analysis.

To resolve the complicated mathematical analysis, we give the analytical expressions of $\tilde{c}_1$, $\tilde{J}_1$ and $\tilde{J}_2$ in the following proposition,

Proposition 2: The analytical expression of $\tilde{c}_1$ is given by

$$\tilde{c}_1 = L(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_1})L\left(\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\right)e^{-\frac{\varepsilon_1 T}{\beta_1}}. \quad (27)$$

The analytical expressions of $\tilde{J}_1$ and $\tilde{J}_2$ are given by

$$\tilde{J}_1 = L\left(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_1}\right)\theta, \quad (28)$$

$$\tilde{J}_2 = \left[1 - L\left(\frac{(\gamma_s-1)\eta_2}{\tilde{I}_P\beta_2}\right)L\left(\frac{\gamma_s\varepsilon_2}{\beta_2}\right)\right]\left[L\left(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_2}\right)\right. \\ \left. -L\left(\left(\frac{1}{\alpha_1}+\frac{1}{\alpha_2}\right)\frac{\gamma_0\eta_0}{\tilde{I}_P}\right)L\left(\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\right)e^{-\frac{T\varepsilon_1}{\beta_1}}\right], \quad (29)$$

where θ is given by (30), shown at the bottom of the page, and

$$\begin{cases} q_0 = \frac{T}{\gamma_s} + \frac{T\varepsilon_1}{\beta_1} \\ q_1 = \left(\frac{1}{\eta_1} + \frac{T-1}{\tilde{I}_P\beta_1}\right)\frac{\tilde{I}_P}{\gamma_s - T} \\ q_2 = \left(\frac{1}{\eta_1} + \frac{\gamma_s-1}{\tilde{I}_P\beta_1}\right)\frac{\tilde{I}_P}{\gamma_s - T} \end{cases}. \quad (31)$$

$$P_{out} = \tilde{p}_1 \underbrace{\Pr\left[\tilde{I}_P\frac{u_1}{t_0}\geq\gamma_0, \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P E\{w_1\}}\geq T, \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1}<\gamma_s\right]}_{\tilde{J}_1} + \tilde{p}_1 \underbrace{\Pr\left[\tilde{I}_P\frac{u_1}{t_0}<\gamma_0 || \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P E\{w_1\}}<T, \tilde{I}_P\frac{u_2}{t_0}\geq\gamma_0, \frac{t_2+\tilde{I}_P v_2}{t_2+\tilde{I}_P w_2}<\gamma_s\right]}_{\tilde{J}_2}$$
$$+\tilde{p}_2 \underbrace{\Pr\left[\tilde{I}_P\frac{u_2}{t_0}\geq\gamma_0, \frac{t_2+\tilde{I}_P v_2}{t_2+\tilde{I}_P E\{w_2\}}\geq T, \frac{t_2+\tilde{I}_P v_2}{t_2+\tilde{I}_P w_2}<\gamma_s\right]}_{\tilde{J}_3} + \tilde{p}_2 \underbrace{\Pr\left[\tilde{I}_P\frac{u_2}{t_0}<\gamma_0 || \frac{t_2+\tilde{I}_P v_2}{t_2+\tilde{I}_P E\{w_2\}}<T, \tilde{I}_P\frac{u_1}{t_0}\geq\gamma_0, \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1}<\gamma_s\right]}_{\tilde{J}_4}, \quad (22)$$

$$\theta = \begin{cases} \left[L\left(\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\right) - L\left(\frac{\gamma_s\varepsilon_1}{\beta_1}\right)L\left(\frac{(\gamma_s-1)\eta_1}{\tilde{I}_P\beta_1}\right)\right]e^{-q_0} + L\left(\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\right)L(-q_1\gamma_s\varepsilon_1) \\ \times\left(e^{-\frac{T\varepsilon_1}{\beta_1}-q_1T\varepsilon_1} - e^{-q_0}\right) - L\left(\frac{(\gamma_s-1)\eta_1}{\tilde{I}_P\beta_1}\right)L\left(\left(\frac{\gamma_s}{\beta_1}-q_2\gamma_s\right)\varepsilon_1\right)\left(e^{-q_2T\varepsilon_1}-e^{-q_0}\right) & \text{If } T<\gamma_s \\ L\left(\frac{(T-\gamma_s)\eta_1}{\tilde{I}_P\varepsilon_1\gamma_s} + \frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\right)\left(1 - L\left(\frac{\gamma_s\varepsilon_1}{\beta_1}\right)\right)e^{-q_0}, & \text{If } T\geq\gamma_s \end{cases}. \quad (30)$$

Proof: See Appendix B. ■

Similarly, by replacing α_1 by α_2, β_1 with β_2, and η_1 with η_2, we can obtain the analytical expression of $\tilde{c}_2$ from the expression of $\tilde{c}_1$ in Proposition 2. This leads to the analytical expressions of $\tilde{p}_1$ and $\tilde{p}_2$. 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 $\tilde{J}_3$ and $\tilde{J}_4$ from the expressions of $\tilde{J}_1$ and $\tilde{J}_2$ in Proposition 2. In this way, we arrive at the analytical expression of SOP with S-ECSI as $P_{out} = \tilde{p}_1(\tilde{J}_1 + \tilde{J}_2) + \tilde{p}_2(\tilde{J}_3 + \tilde{J}_4)$.

C. Asymptotic SOP With I-ECSI

To obtain additional insights on the system performance, we now extend to analyze the asymptotic SOP performance of SSSC with I-ECSI, in high transmit power and high MER regions, where MER is defined as the ratio of average channel gain from the relay to intended receiver to that from relay to eavesdropper [11]. The asymptotic SOP with I-ECSI is given by the following proposition,

Proposition 3: The asymptotic c_1 and c_2 with high transmit power and high MER can be approximated from [36, eq. (1.112)] as

$$c_1 \simeq 1, \quad c_2 \simeq 1. \tag{32}$$

We further write the asymptotic SOP of SSSC with I-ECSI in high transmit power and high MER region as

$$P_{out} \simeq \begin{cases} \frac{\varepsilon_1+\varepsilon_2}{2\lambda_1\lambda_2} + \frac{\gamma_s - T}{2}\left(\frac{1+\zeta_1}{\lambda_1} + \frac{1+\zeta_2}{\lambda_2}\right), & \text{If } T < \gamma_s \\ \frac{\varepsilon_1+\varepsilon_2}{2\lambda_1\lambda_2}, & \text{If } T \geq \gamma_s \end{cases}, \tag{33}$$

where

$$\begin{cases} \zeta_1 = \frac{\rho_1\eta_1}{\beta_1}, \quad \zeta_2 = \frac{\rho_2\eta_2}{\beta_2} \\ \rho_1 = \frac{\lambda_1}{\tilde{I}_P}, \quad \rho_2 = \frac{\lambda_2}{\tilde{I}_P} \\ \varepsilon_1 = [\gamma_s + (\gamma_s - 1)\zeta_2] \cdot [T + (T-1)\zeta_1 + \gamma_0\eta_0\rho_1/\alpha_1] \\ \varepsilon_2 = [\gamma_s + (\gamma_s - 1)\zeta_1] \cdot [T + (T-1)\zeta_2 + \gamma_0\eta_0\rho_2/\alpha_2] \end{cases}. \tag{34}$$

Proof: See Appendix C. ■

In particular, when the transmit power is much larger than MER with $\tilde{I}_P \gg \lambda_i$ $(i = 1, 2)$, ρ_i approaches to zero, causing that $\zeta_i \simeq 0$ and $\varepsilon_i \simeq 0$. In this case, we can simplify the asymptotic SOP in (33) as

$$P_{out} \simeq \begin{cases} \frac{T\gamma_s}{\lambda_1\lambda_2} + \frac{\gamma_s - T}{2}\left(\frac{1}{\lambda_1} + \frac{1}{\lambda_2}\right), & \text{If } T < \gamma_s \\ \frac{T\gamma_s}{\lambda_1\lambda_2}, & \text{If } T \geq \gamma_s \end{cases}. \tag{35}$$

From the above asymptotic expressions, we can get the following insights on the system:

Remark 1: In high $\tilde{I}_P$ and MER region, both c_1 and c_2 approach to one, indicating that the same relay will continue to be used for a long time. Hence, the system only needs to estimate the channel parameters with a single relay. This can substantially reduce the implementation complexity in practice.

Remark 2: When $T \geq \gamma_s$, the system can achieve the full diversity order of two, as a large value of T can guarantee an effective secure relay switching. On the other hand, when $T < \gamma_s$, the system diversity order falls into $[1, 2)$, indicating that too small a value of T cannot effectively exploit the two relays to guarantee the secure transmission.

Remark 3: The optimal value of the secure switching threshold T^* is equal to the system secrecy threshold γ_s.

D. Asymptotic SOP With S-ECSI

To obtain some insights on the system of SSSC protocol with S-ECSI, we now derive the asymptotic SOP with large $\tilde{I}_P$ and MER, in the following proposition,

Proposition 4: The asymptotic $\tilde{c}_1$ and $\tilde{c}_2$ with large $\tilde{I}_P$ and MER can be written from [36, eq. (1.112)] as

$$\tilde{c}_1 \simeq 1, \tilde{c}_2 \simeq 1. \tag{36}$$

Then we approximate the SOP of SSSC with S-ECSI in high $\tilde{I}_P$ and high MER regions as

$$P_{out} \simeq \begin{cases} \frac{\varepsilon_1+\varepsilon_2}{2\lambda_1\lambda_2} + \frac{\gamma_s}{2}e^{-\frac{T}{\gamma_s}}\left[\frac{1-\varepsilon_3^2 e^{-\frac{T}{\gamma_s}\frac{1-\varepsilon_3}{\varepsilon_3}}}{(1-\varepsilon_3)\lambda_1} + \frac{1-\varepsilon_4^2 e^{-\frac{T}{\gamma_s}\frac{1-\varepsilon_4}{\varepsilon_4}}}{(1-\varepsilon_4)\lambda_2}\right], & \text{If } T < \gamma_s \\ \frac{\varepsilon_1+\varepsilon_2}{2\lambda_1\lambda_2} + \frac{\gamma_s}{2}e^{-\frac{T}{\gamma_s}}\left(\frac{1}{(1-\varepsilon_3)\lambda_1} + \frac{1}{(1-\varepsilon_4)\lambda_2}\right), & \text{If } T \geq \gamma_s \end{cases}, \tag{37}$$

with

$$\begin{cases} \varepsilon_3 = (\gamma_s - T)\zeta_1/\gamma_s \\ \varepsilon_4 = (\gamma_s - T)\zeta_2/\gamma_s \end{cases}. \tag{38}$$

Proof: See Appendix D. ■

In particular, when the transmit power is much larger than the value of MER with $\tilde{I}_P \gg \lambda_i$ $(i = 1, 2)$, both ε_3 and ε_4 approach to zero due to $\zeta_i \simeq 0$. In this condition, the asymptotic SOP of SSSC with S-ECSI is simplified as

$$P_{out} \simeq \frac{\gamma_s T}{\lambda_1\lambda_2} + \frac{\gamma_s}{2}\left(\frac{1}{\lambda_1} + \frac{1}{\lambda_2}\right)e^{-\frac{T}{\gamma_s}}. \tag{39}$$

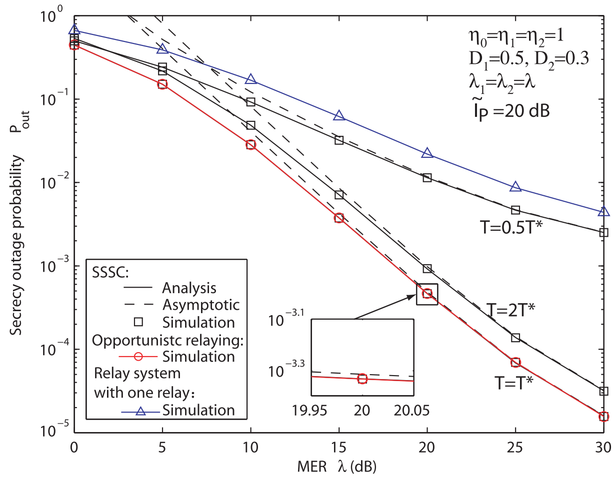
By setting the derivative of above P_{out} with respect to T into zero, we can readily obtain the minimum P_{out} as

$$P_{out,min} = \frac{\gamma_s^2}{\lambda_1\lambda_2}\left(1 + \ln\frac{\lambda_1 + \lambda_2}{2\gamma_s}\right). \tag{40}$$

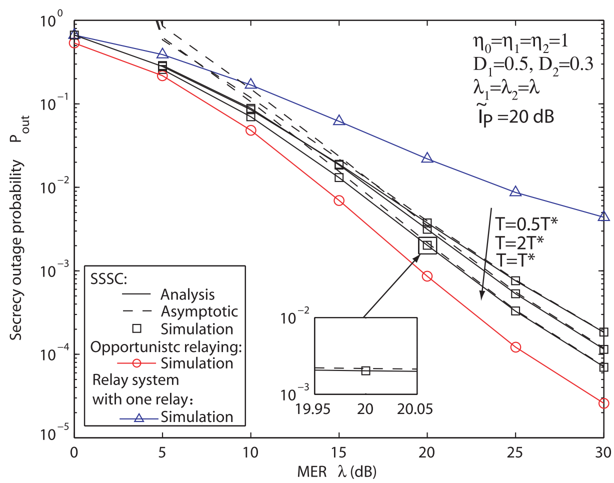
From these asymptotic results, we can achieve the following insights on the system performance with S-ECSI:

Remark 1: As both $\tilde{c}_1$ and $\tilde{c}_2$ 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, even with S-ECSI, the SSSC protocol can substantially reduce the system implementation complexity compared with the opportunistic relaying protocol.

Remark 2: From the above asymptotic results of P_{out}, we can find that the system diversity order falls between one and two. In particular, the system diversity order can approach to two for

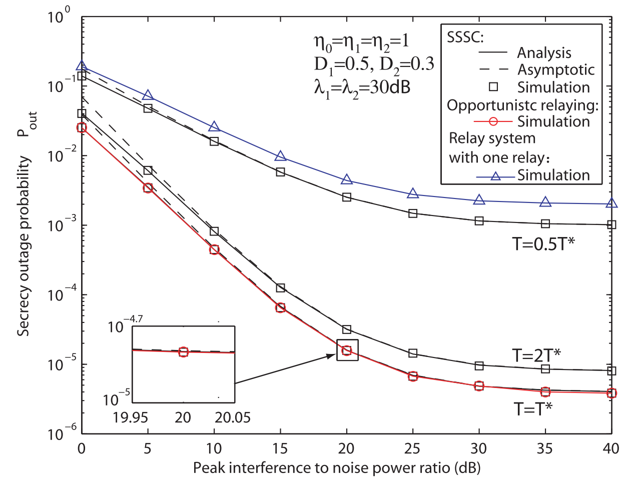


(a) I-ECSI

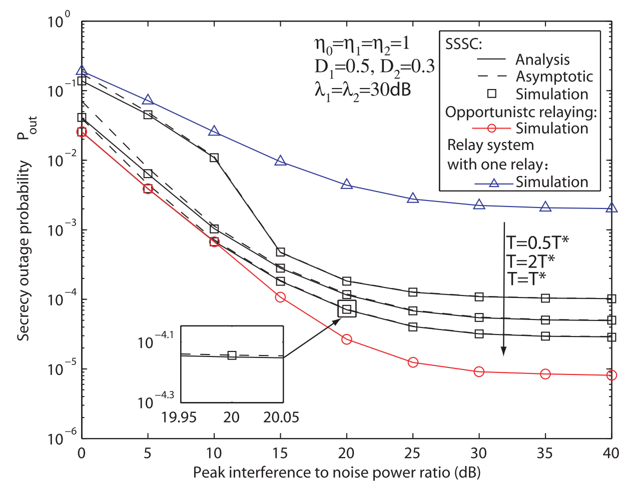


(b) S-ECSI

Fig. 2. Secrecy outage probability versus MER.



(a) I-ECSI



(b) S-ECSI

Fig. 3. Secrecy outage probability versus $\tilde{I}_P$.

a large value of T, which can effectively exploit the two relays to guarantee the secure transmission.

Remark 3: By comparing the minimum asymptotic P_{out} of S-ECSI with that of I-ECSI, we can find that the system performance is degraded, since the eavesdropping CSI is not fully known in the secure switching process.

E. Complexity Analysis

In this subsection, we briefly discuss the channel estimation complexity of the proposed SSSC protocol. When the secure relay switching does not occur, the system only needs to estimate the channel parameters of a single relay, and hence the channel estimation complexity of SSSC is just half of that of the opportunistic relaying. On the other hand, when the secure relay switching happens, the system needs to estimate the channel parameters of both relays, and SSSC requires the same channel estimation complexity as opportunistic relaying. In summary, the channel estimation complexity of SSSC with I-ECSI, normalized by that of opportunistic relaying, is given by

$$\mu_I = p_1\left[\frac{c_1}{2} + (1-c_1)\right] + p_2\left[\frac{c_2}{2} + (1-c_2)\right] = 1 - \frac{1}{2}\frac{c_1^2 + c_2^2}{c_1 + c_2}. \quad (41)$$

Similarly, for SSSC with S-ECSI, its normalized channel estimation complexity is given by

$$\mu_S = 1 - \frac{1}{2}\frac{\tilde{c}_1^2 + \tilde{c}_2^2}{\tilde{c}_1 + \tilde{c}_2}. \quad (42)$$

As the stay probabilities c_i and $\tilde{c}_i$ are both in the interval [0, 1] for $i = 1, 2$, one can find that the normalized complexity of SSSC falls into [0.5, 1]. Moreover, as both c_i and $\tilde{c}_i$ approach 1 with high transmit power and MER, SSSC protocol can reduce the channel estimation complexity of opportunistic relaying to almost half.

V. Simulation and Numerical Results

In this section, numerical and simulation results are presented to verify the proposed system. All the links in the system experience flat Rayleigh fading. The distance between the

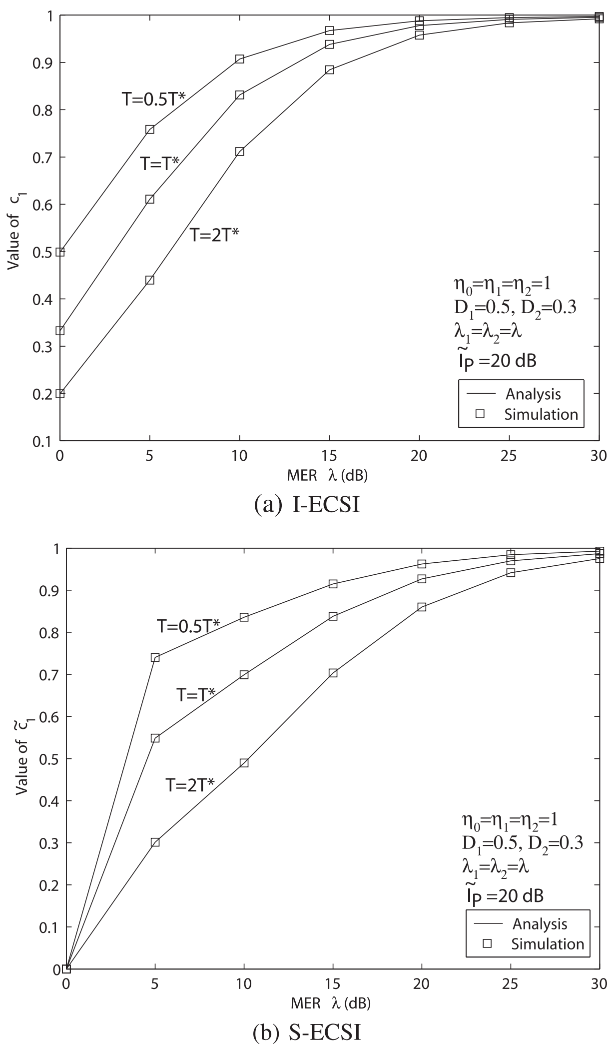


Fig. 4. Effect of T on c_1 and $\tilde{c}_1$ versus MER.

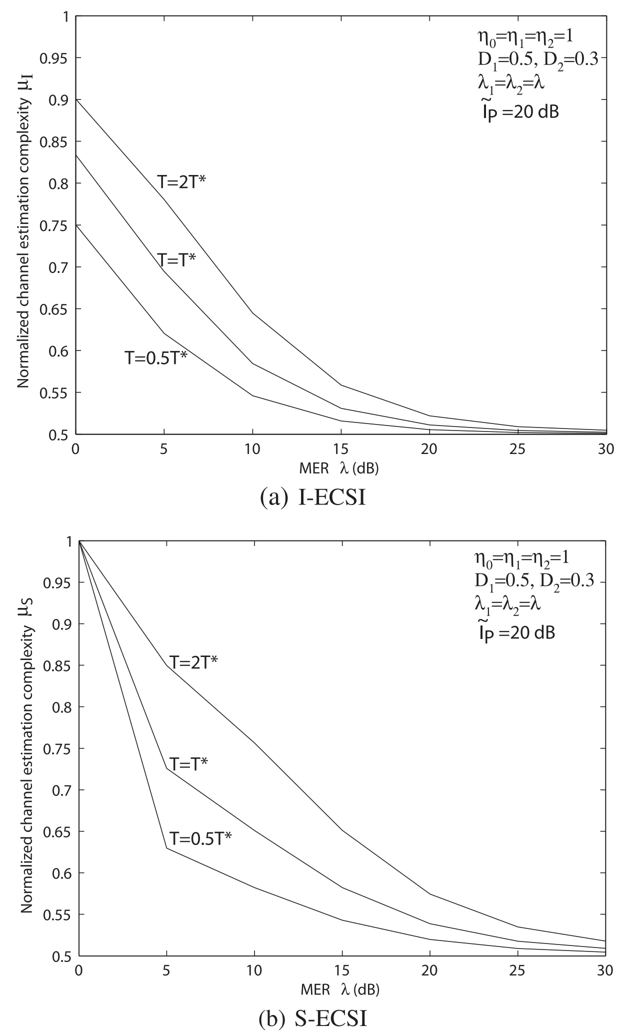


Fig. 5. Normalized channel estimation complexity of SSSC versus MER.

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 $\eta_0 = \eta_1 = \eta_2 = 1$. The source data rate R_d is set to 1 bps/Hz, so that the associated γ_0 is equal to 3. The secrecy data rate R_s is set to 0.5 bps/Hz, so that the secrecy SNR threshold γ_s is equal to 2.

Fig. 2 depicts the analytical, asymptotic and simulated SOPs of SSSC versus MER with $\lambda_1 = \lambda_2 = \lambda$ and $\tilde{I}_P = 20\text{dB}$[2], where the asymptotic results are computed from eqs. (33) and (37), respectively. The secure switching threshold T varies in $\{0.5, 1, 2\}T^*$ [3], where the optimal switching threshold T^* is set to γ_s for I-ECSI, while for S-ECSI, T^* can be obtained by some numerical methods from (37) [31]–[37]. Fig. 2 (a) and (b) correspond to the SSSC with I-ECSI and S-ECSI, respectively. For comparison, we plot the simulated secrecy outage probabilities of opportunistic relaying and the relay system with only one relay as the lower and upper bounds, respectively. As observed from Fig. 2 (a) and (b), we can find that for both cases of I-ECSI and S-ECSI, the analytical result of SSSC matches well with the simulation one, and the asymptotic result converges to the exact value with high MER more than 20dB. This verifies the validity of the derived analytical secrecy outage probability of SSSC and asymptotic expression. Moreover, SSSC with I-ECSI can have the same secure performance as opportunistic relaying when $T = T^*$, and hence achieve the full diversity order. For $T = 2T^*$, SSSC of I-ECSI can also achieve the system full diversity order of two. For $T = 0.5T^*$, the curve line of SSSC with I-ECSI is parallel with the relay system with only one relay, indicating that the system diversity degenerates into one. On the other hand, although SSSC with S-ECSI cannot achieve the same performance as opportunistic relaying, the lines with $T \in \{1, 2\}T^*$ are approximately parallel with opportunistic relaying, indicating that SSSC with S-ECSI can also

[2]We consider communication scenarios with $\tilde{I}_P = 20\text{dB}$, indicating that the primary user can tolerate a high interference level, which is widely used in cognitive relay networks [40]–[43].

[3]Besides the optimal secure switching threshold, two other typical values, $0.5T^*$ and $2T^*$, are set for T to show the impact of T on the system secure performance.

approach the system full diversity order of two in high MER region. This can be explained from the asymptotic analysis in (37), which contains two terms on the right hand side. Hence the diversity of SSSC falls between one and two, causing the curve of SSSC approximately parallel with opportunistic relaying. When the secure switching threshold becomes very large, SSSC with S-ECSI approaches to the system full diversity order of two, since the exponential decreasing term of (37) converges to zero.

Fig. 3 shows the effect of $\tilde{I}_P$ on the system secrecy outage probability of SSSC, where the secure switching threshold T varies in $\{0.5, 1, 2\}T^*$, $\lambda_1 = \lambda_2 = 30$dB. Specifically, Fig. 3 (a) and (b) correspond to the SSSC with I-ECSI and S-ECSI, respectively. We can see from this figure that for different values of T and $\tilde{I}_P$, the analytical result of SSSC is very close to the simulation one, and the asymptotic result converges to the exact value in high $\tilde{I}_P$ region. This also validates the derived analytical and asymptotic expressions of SOP for SSSC with I-ECSI and S-ECSI. Moreover, SSSC with I-ECSI and optimal secure switching threshold presents the same performance as opportunistic relaying. In contrast, there is a performance gap between SSSC and opportunistic relaying when S-ECSI is known, indicating that the secure relaying switching is more effective with I-ECSI.

Fig. 4 illustrates the effect of T on the simulation and analytical results of c_1 and $\tilde{c}_1$ [4] of SSSC versus MER with $\lambda_1 = \lambda_2 = \lambda$ and $\tilde{I}_P = 20$dB, where the secure switching threshold T varies in $\{0.5, 1, 2\}T^*$. Specifically, Fig. 4 (a) and (b) correspond to the SSSC with I-ECSI and S-ECSI, respectively. From this figure, we can find that for both I-ECSI and S-ECSI, c_1 and $\tilde{c}_1$ increase with larger $\tilde{I}_P$ and smaller T. In particular, c_1 and $\tilde{c}_1$ converge to unity 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 opportunistic relaying to almost half and meanwhile substantially reduce the relay switching rate.

Fig. 5 demonstrates the normalized channel estimation complexity of SSSC versus MER with $\lambda_1 = \lambda_2 = \lambda$ and $\tilde{I}_P = 20$dB, where the secure switching threshold T varies in $\{0.5, 1, 2\}T^*$. In particular, Fig. 5 (a) and (b) correspond to SSSC with I-ECSI and S-ECSI, respectively. We can observe from Fig. 5 that for both I-ECSI and S-ECSI, the channel estimation complexity of SSSC decreases with larger MER or smaller switching threshold, as the secure relay switching happens less. Moreover, SSSC can reduce the channel estimation complexity of opportunistic relaying to almost half in the high MER region, which validates the advantages of SSSC over opportunistic relaying.

VI. Conclusions

This paper proposed SSSC technique for the secure 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 with I-ECSI can exploit the system full diversity, and SSSC with S-ECSI can approach to the full diversity with large secure relaying switching threshold. Moreover, SSSC can reduce the channel estimation complexity of opportunistic relaying to almost half in high MER region, and provide a stable network configuration.

[4]As c_2 and $\tilde{c}_2$ show the similar behavior as c_1 and $\tilde{c}_1$, the results of c_2 and $\tilde{c}_2$ are not plotted in this figure for clarity.

Appendix A
Proof of Proposition 1

As the variable $\frac{u_1}{t_0}$ is independent of $\frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1}$, we can write c_1 from (17) as

$$c_1 = \Pr(\frac{u_1}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P}) \cdot \Pr\left(\frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1} \geq T\right). \tag{A.1}$$

By applying the probability density functions of $f_{u_1}(u_1) = \frac{1}{\alpha_1}e^{-\frac{u_1}{\alpha_1}}$, $f_{t_0}(t_0) = \frac{1}{\eta_0}e^{-\frac{t_0}{\eta_0}}$, $f_{t_1}(t_1) = \frac{1}{\eta_1}e^{-\frac{t_1}{\eta_1}}$, $f_{v_1}(v_1) = \frac{1}{\beta_1}e^{-\frac{v_1}{\beta_1}}$ and $f_{w_1}(w_1) = \frac{1}{\varepsilon_1}e^{-\frac{w_1}{\varepsilon_1}}$, we can compute $\Pr(\frac{u_1}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P})$ and $\Pr\left(\frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1} \geq T\right)$ as

$$\Pr\left(\frac{u_1}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P}\right) = \int_0^\infty f_{t_0}(t_0) \int_{\frac{\gamma_0}{\tilde{I}_P}t_0}^\infty f_{u_1}(u_1)du_1 dt_0 \tag{A.2}$$

$$= L\left(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_1}\right), \tag{A.3}$$

$$\tag{A.4}$$

$$\Pr\left(\frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1} \geq T\right) = \Pr\left(v_1 \geq \frac{T-1}{\tilde{I}_P}t_1 + Tw_1\right) \tag{A.5}$$

$$= \int_0^\infty f_{t_1}(t_1) \int_0^\infty f_{w_1}(w_1) \int_{\frac{T-1}{\tilde{I}_P}t_1+Tw_1}^\infty f_{v_1}(v_1)dv_1 dw_1 dt_1 \tag{A.6}$$

$$= L\left(\frac{T\varepsilon_1}{\beta_1}\right) L\left(\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\right), \tag{A.7}$$

where $L(x) = (1+x)^{-1}$. By combining eqs. (A.3) and (A.7), we can obtain the analytical expression of c_1, as shown in (19) of Proposition 1.

We now turn to derive the analytical expression of J_1. As the variable $\frac{u_1}{t_0}$ is independent of $\frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1}$, we can write J_1 as

$$J_1 = \Pr\left(\frac{u_1}{t_0} > \frac{\gamma_0}{\tilde{I}_P}\right) \cdot \Pr\left(\frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1} \geq T, \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1} < \gamma_s\right) \tag{A.8}$$

$$= L\left(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_1}\right) \Pr\left(\frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1} \geq T, \frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1} < \gamma_s\right), \tag{A.9}$$

where we apply the result of (A.3) in the last equality. When $T \geq \gamma_s$, $\frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1} \geq T$ contradicts with $\frac{t_1+\tilde{I}_P v_1}{t_1+\tilde{I}_P w_1} < \gamma_s$, causing that $J_1 = 0$. On the other hand, when $T < \gamma_s$, we can further write J_1 as

$$J_1 = L\left(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_1}\right)\left[\Pr\left(\frac{t_1+\tilde{I}_Pv_1}{t_1+\tilde{I}_Pw_1}\geq T\right) - \Pr\left(\frac{t_1+\tilde{I}_Pv_1}{t_1+\tilde{I}_Pw_1}\geq \gamma_s\right)\right] \quad (A.10)$$

$$= L\left(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_1}\right)\left[L\left(\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\right)L\left(\frac{T\varepsilon_1}{\beta_1}\right) - L\left(\frac{(\gamma_s-1)\eta_1}{\tilde{I}_P\beta_1}\right)L\left(\frac{\gamma_s\varepsilon_1}{\beta_1}\right)\right], \quad (A.11)$$

where we apply the result of (A.7) in the last equality.

We now turn to derive the analytical expression of J_2 as

$$J_2 = \Pr\left(\frac{t_2+\tilde{I}_Pv_2}{t_2+\tilde{I}_Pw_2}<\gamma_s\right) \times \Pr\left(\tilde{I}_P\frac{u_1}{t_0}<\gamma_0 || \frac{t_1+\tilde{I}_Pv_1}{t_1+\tilde{I}_Pw_1}<T, \tilde{I}_P\frac{u_2}{t_0}\geq\gamma_0\right) \quad (A.12)$$

$$= \left[1-L\left(\frac{(\gamma_s-1)\eta_2}{\tilde{I}_P\beta_2}\right)L\left(\frac{\gamma_s\varepsilon_2}{\beta_2}\right)\right] \times \underbrace{\Pr\left(\tilde{I}_P\frac{u_1}{t_0}<\gamma_0 || \frac{t_1+\tilde{I}_Pv_1}{t_1+\tilde{I}_Pw_1}<T, \tilde{I}_P\frac{u_2}{t_0}\geq\gamma_0\right)}_{J_{21}}, \quad (A.13)$$

where the last equality is obtained by applying the result of (A.7). We further write J_{21} as

$$J_{21} = \Pr\left(\frac{u_2}{t_0}\geq\frac{\gamma_0}{\tilde{I}_P}\right) - \Pr\left(\tilde{I}_P\frac{u_1}{t_0}\geq\gamma_0, \frac{t_1+\tilde{I}_Pv_1}{t_1+\tilde{I}_Pw_1}\geq T, \frac{u_2}{t_0}\geq\frac{\gamma_0}{\tilde{I}_P}\right) \quad (A.14)$$

$$= L(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_2}) - \Pr\left(\tilde{I}_P\frac{u_1}{t_0}\geq\gamma_0, \tilde{I}_P\frac{u_2}{t_0}\geq\gamma_0\right) \times \Pr\left(\frac{t_1+\tilde{I}_Pv_1}{t_1+\tilde{I}_Pw_1}\geq T\right) \quad (A.15)$$

$$= L(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_2}) - \Pr\left(\tilde{I}_P\frac{u_1}{t_0}\geq\gamma_0, \tilde{I}_P\frac{u_2}{t_0}\geq\gamma_0\right) \times L\left(\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\right)L\left(\frac{T\varepsilon_1}{\beta_1}\right), \quad (A.16)$$

where we apply the results of eqs. (A.3) and (A.7) into eqs. (A.15) and (A.16), respectively. In further, the probability of $\Pr\left(\tilde{I}_P\frac{u_1}{t_0}\geq\gamma_0, \tilde{I}_P\frac{u_2}{t_0}\geq\gamma_0\right)$ can be computed as

$$\Pr\left(\frac{u_1}{t_0}\geq\frac{\gamma_0}{\tilde{I}_P}, \frac{u_2}{t_0}\geq\frac{\gamma_0}{\tilde{I}_P}\right) = \int_0^\infty f_{t_0}(t_0)\int_{\frac{\gamma_0}{\tilde{I}_P}t_0}^\infty f_{u_1}(u_1)du_1\int_{\frac{\gamma_0}{\tilde{I}_P}t_0}^\infty f_{u_2}(u_2)du_2dt_0 \quad (A.17)$$

$$= L\left(\left(\frac{1}{\alpha_1}+\frac{1}{\alpha_2}\right)\frac{\gamma_0\eta_0}{\tilde{I}_P}\right). \quad (A.18)$$

By combining the above eqs. (A.13), (A.16) and (A.18), we can arrive at the analytical expression of J_2, as shown in (21) of Proposition 1. In this way, we have completed the proof of Proposition 1.

Appendix B
Proof of Proposition 2

From (25), we can write $\tilde{c}_1$ with S-ECSI as

$$\tilde{c}_1 = \Pr\left(\frac{u_1}{t_0}\geq\frac{\gamma_0}{\tilde{I}_P}\right)\cdot\Pr\left(\frac{t_1+\tilde{I}_Pv_1}{t_1+\tilde{I}_PE\{w_1\}}\geq T\right) \quad (B.1)$$

$$= L\left(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_1}\right)\Pr\left(\frac{t_1+\tilde{I}_Pv_1}{t_1+\tilde{I}_P\varepsilon_1}\geq T\right), \quad (B.2)$$

where we apply the result of (A.3) in the last equality. $\Pr\left(\frac{t_1+\tilde{I}_Pv_1}{t_1+\tilde{I}_P\varepsilon_1}\geq T\right)$ can be computed as

$$\Pr\left(\frac{t_1+\tilde{I}_Pv_1}{t_1+\tilde{I}_P\varepsilon_1}\geq T\right) = \Pr\left(v_1\geq\frac{T-1}{\tilde{I}_P}t_1+T\varepsilon_1\right) \quad (B.3)$$

$$= \int_0^\infty f_{t_1}(t_1)\int_{\frac{T-1}{\tilde{I}_P}t_1+T\varepsilon_1}^\infty f_{v_1}(v_1)dv_1dt_1 \quad (B.4)$$

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

By combining the results of eqs. (B.2) and (B.5), we can obtain the analytical expression of $\tilde{c}_1$, as shown in (27) of Proposition 2.

We now turn to derive the analytical expression of $\tilde{J}_1$ in (22) as

$$\tilde{J}_1 = \Pr\left(\frac{u_1}{t_0}\geq\frac{\gamma_0}{\tilde{I}_P}\right) \times \Pr\left(\frac{t_1+\tilde{I}_Pv_1}{t_1+\tilde{I}_PE\{w_1\}}\geq T, \frac{t_1+\tilde{I}_Pv_1}{t_1+\tilde{I}_Pw_1}<\gamma_s\right) \quad (B.6)$$

$$= L\left(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_1}\right) \times \underbrace{\Pr\left(v_1\geq\frac{T-1}{\tilde{I}_P}t_1+T\varepsilon_1, v_1<\frac{\gamma_s-1}{\tilde{I}_P}t_1+Tw_1\right)}_{\tilde{J}_{11}}, \quad (B.7)$$

where we apply the result of (A.3) in the last equality. In $\tilde{J}_{11}$, $\frac{\gamma_s-1}{\tilde{I}_P}t_1+Tw_1$ needs to be larger than $\frac{T-1}{\tilde{I}_P}t_1+T\varepsilon_1$, causing that

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

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

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

and $\tilde{J}_{11}$ is computed as

$$\begin{aligned}\tilde{J}_{11} &= \int_0^\infty f_{t_1}(t_1) \int_{\frac{T-1}{\tilde{I}_P\gamma_s}t_1+\frac{T\varepsilon_1}{\gamma_s}}^\infty f_{w_1}(w_1) \int_{\frac{T-1}{\tilde{I}_P}t_1+T\varepsilon_1}^{\frac{\gamma_s-1}{\tilde{I}_P}t_1+Tw_1} \\ &\quad f_{v_1}(v_1) dv_1 dw_1 dt_1 \qquad \text{(B.10)} \\ &= L\left(\frac{(T-\gamma_s)\eta_1}{\tilde{I}_P\varepsilon_1\gamma_s} + \frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\right)\left(1 - L(\frac{\gamma_s\varepsilon_1}{\beta_1})\right)e^{-q_0}, \qquad \text{(B.11)}\end{aligned}$$

where q_0 is defined in (31).

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

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

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 $t_1 \geq \frac{\tilde{I}_P T\varepsilon_1 - \tilde{I}_P\gamma_s w_1}{\gamma_s - T}$. Accordingly, we can compute $\tilde{J}_{11}$ as

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

where q_1 and q_2 are defined in (31). By combining eqs. (B.7), (B.11) and (B.14), we can arrive at the analytical expression of $\tilde{J}_1$, as shown in (28) of Proposition 2.

We now turn to derive the analytical expression of $\tilde{J}_2$. From (22), we can write $\tilde{J}_2$ as

$$\begin{aligned}\tilde{J}_2 &= \Pr\left(\frac{t_2 + \tilde{I}_P v_2}{t_2 + \tilde{I}_P w_2} < \gamma_s\right) \\ &\quad \times \Pr\left(\frac{u_1}{t_0} < \frac{\gamma_0}{\tilde{I}_P} || \frac{t_1 + \tilde{I}_P v_1}{t_1 + \tilde{I}_P\varepsilon_1} < T, \frac{u_2}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P}\right) \qquad \text{(B.15)} \\ &= \left[1 - L\left(\frac{(\gamma_s-1)\eta_2}{\tilde{I}_P\beta_2}\right)L\left(\frac{\gamma_s\varepsilon_2}{\beta_2}\right)\right] \\ &\quad \times \underbrace{\Pr\left(\frac{u_1}{t_0} < \frac{\gamma_0}{\tilde{I}_P} || \frac{t_1 + \tilde{I}_P v_1}{t_1 + \tilde{I}_P\varepsilon_1} < T, \frac{u_2}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P}\right)}_{\tilde{J}_{21}}, \qquad \text{(B.16)}\end{aligned}$$

where we apply the result of (A.7) in the last equality. In further, $\tilde{J}_{21}$ can be computed as

$$\begin{aligned}\tilde{J}_{21} &= \Pr\left(\frac{u_2}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P}\right) \\ &\quad - \Pr\left(\frac{u_1}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P}, \frac{t_1 + \tilde{I}_P v_1}{t_1 + \tilde{I}_P\varepsilon_1} \geq T, \frac{u_2}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P}\right) \qquad \text{(B.17)} \\ &= \Pr\left(\frac{u_2}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P}\right) - \Pr\left(\frac{u_1}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P}, \frac{u_2}{t_0} \geq \frac{\gamma_0}{\tilde{I}_P}\right) \\ &\quad \times \Pr\left(\frac{t_1 + \tilde{I}_P v_1}{t_1 + \tilde{I}_P\varepsilon_1} \geq T\right) \qquad \text{(B.18)} \\ &= L\left(\frac{\gamma_0\eta_0}{\tilde{I}_P\alpha_2}\right) - L\left(\left(\frac{1}{\alpha_1} + \frac{1}{\alpha_2}\right)\frac{\gamma_0\eta_0}{\tilde{I}_P}\right)L\left(\frac{(T-1)\eta_1}{\tilde{I}_P\beta_1}\right)e^{-\frac{T\varepsilon_1}{\beta_1}}, \qquad \text{(B.19)}\end{aligned}$$

where we apply the results of eqs. (A.3), (A.7) and (B.5) in the last equality. By combining the results in eqs. (B.16) and (B.19), we can obtain the analytical expression of $\tilde{J}_2$ with S-ECSI, as shown in (29) of Proposition 2. In this way, we have completed the proof of Proposition 2.

APPENDIX C
PROOF OF PROPOSITION 3

We first derive the asymptotic expressions of c_1 and c_2. To this end, we use the approximation of $(1+x)^{-1} \simeq 1 - x$ for small value of $|x|$ [36, eq. (1.112)] and obtain the asymptotic c_1 and c_2 as

$$c_1 \simeq 1, \quad c_2 \simeq 1, \tag{C.1}$$

which leads to $p_1 \simeq 0.5$ and $p_2 \simeq 0.5$. We now derive the asymptotic expressions of J_1, J_2, J_3 and J_4. When $T < \gamma_s$, we apply the approximation of $(1+x)^{-1} \simeq 1 - x$ and obtain the asymptotic expression of J_1 with high $\tilde{I}_P$ and MER as

$$J_1 \simeq \frac{\gamma_s - T}{\lambda_1}\left(1 + \frac{\eta_1\rho_1}{\beta_1}\right), \tag{C.2}$$

where ρ_1 is defined in (34). We further apply the approximation of $(1+x)^{-1} \simeq 1 - x$ into the expression of J_2, and obtain the asymptotic J_2 with high $\tilde{I}_P$ and MER as

$$J_2 \simeq \frac{\varepsilon_1}{\lambda_1\lambda_2}, \tag{C.3}$$

where ε_1 is defined in (34). Similarly, we can obtain the asymptotic expressions of J_3 and J_3. By combining the asymptotic results of J_1, J_2, J_3 and J_4, we can arrive at the asymptotic SOP with high $\tilde{I}_P$ and MER, as shown in (33). In this way, we have finished the proof of Proposition 3.

APPENDIX D
PROOF OF PROPOSITION 4

By applying the approximation of $(1+x)^{-1} \simeq 1-x$ for small value of $|x|$ [36, eq. (1.112)], we can approximate the expressions of $\tilde{c}_1$ and $\tilde{c}_2$ with large $\tilde{I}_P$ and MER as

$$\tilde{c}_1 \simeq 1, \quad \tilde{c}_2 \simeq 1. \tag{D.1}$$

Accordingly, the asymptotic $\tilde{p}_1$ and $\tilde{p}_2$ are given by

$$\tilde{p}_1 \simeq \frac{1}{2}, \tilde{p}_2 \simeq \frac{1}{2}. \tag{D.2}$$

We then extend to derive the asymptotic expressions of $\tilde{J}_1$, $\tilde{J}_2$, $\tilde{J}_3$ and $\tilde{J}_4$ with high $\tilde{I}_P$ and high MER. By applying the approximation of $(1+x)^{-1} \simeq 1-x$ for small value of $|x|$ [36, eq. (1.112)], we can obtain the asymptotic expression of $\tilde{J}_1$ and $\tilde{J}_2$ as

$$\tilde{J}_1 \simeq \begin{cases} \frac{\gamma_s}{\lambda_1} e^{-\frac{T}{\gamma_s}} \frac{1}{1-\varepsilon_3} \left(1 - \varepsilon_3^2 e^{-\frac{T}{\gamma_s}\frac{1-\varepsilon_3}{\varepsilon_3}}\right), & \text{If } T < \gamma_s \\ \frac{\gamma_s}{\lambda_1} e^{-\frac{T}{\gamma_s}} \frac{1}{1-\varepsilon_3}, & \text{If } T \geq \gamma_s \end{cases}, \tag{D.3}$$

$$\tilde{J}_2 \simeq \frac{\varepsilon_1}{\lambda_1 \lambda_2}, \tag{D.4}$$

where ε_3 is defined in (38). In a similar way, we can obtain the asymptotic expressions of $\tilde{J}_3$ and $\tilde{J}_4$ with high $\tilde{I}_P$ and high MER. By summarizing these asymptotic expressions, we can arrive at the asymptotic SOP of SSSC with S-ECSI. In this way, we have completed the proof of Proposition 4.

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 Signal Process. Lett.*, vol. 19, no. 8, pp. 479–482, Aug. 2012.

[4] W. Xu, Z. Peng, and S. Jin, "On secrecy of a multi-antenna system with eavesdropper in close proximity," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1525–1529, Oct. 2015.

[5] C. Wang and H.-M. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 11, pp. 1814–1827, Nov. 2014.

[6] S. Jin, M. R. McKay, C. Zhong, and K.-K. Wong, "Ergodic capacity analysis of amplify-and-forward MIMO dual-hop systems," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2204–2224, May 2010.

[7] X. Liang, S. Jin, X. Gao, and K.-K. Wong, "Outage performance for decode-and-forward two-way relay network with multiple interferers and noisy relay," *IEEE Trans. Commun.*, vol. 61, no. 2, pp. 521–531, Feb. 2013.

[8] C. Xing, S. Ma, Z. Fei, Y.-C. Wu, and H. V. Poor, "A general robust linear transceiver design for amplify-and-forward multi-hop MIMO relaying systems," *IEEE Trans. Signal Process.*, vol. 61, no. 5, pp. 1196–1209, Mar. 2013.

[9] M. Dai, C. W. Sung, and Y. Wang, "Distributed on-off power control for amplify-and-forward relays with orthogonal space-time block code," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1895–1903, Mar. 2013.

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

[11] 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, Sep. 2014.

[12] 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.

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

[14] S. Parsaeefard and T. Le-ngoc, "Full-duplex relay with jamming protocol for improving physical-layer security," in *Proc. IEEE 25th Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC'14)*, Washington DC, USA, 2014, pp. 129–133.

[15] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Trans. Signal Process.*, vol. 62, no. 9, pp. 2185–2199, May 2014.

[16] Q. Li, Q. Zhang, and J. Qin, "Secure relay beamforming for simultaneous wireless information and power transfer in nonregenerative relay networks," *IEEE Trans. Veh. Technol.*, vol. 63, no. 5, pp. 2462–2467, Jun. 2014.

[17] K. Jayasinghe, P. Jayasinghe, N. Rajatheva, and M. Latva-Aho, "Secure beamforming design for physical layer network coding based MIMO two-way relaying," *IEEE Commun. Lett.*, vol. 18, no. 7, pp. 1270–1273, Jul. 2014.

[18] Z. Ding, Z. Ma, and P. Fan, "Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 2189–2203, Apr. 2014.

[19] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 289–293, Jun. 2014.

[20] A. Jindal and R. Bose, "Resource allocation for secure multicarrier AF relay system under total power constraint," *IEEE Commun. Lett.*, vol. 19, no. 2, pp. 231–234, Feb. 2015.

[21] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[22] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 39–42, Jan. 2013.

[23] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 61, no. 5, pp. 3532–3545, Jul. 2012.

[24] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[25] F. G. ad Jiachen Li, T. Jiang, and W. Chen, "Sensing and recognition when primary user has multiple transmit power levels," *IEEE Trans. Signal Process.*, vol. 63, no. 10, pp. 2704–2717, May 2015.

[26] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, "Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 1058–1073, Feb. 2014.

[27] 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. Signal Process.*, vol. 63, no. 2, pp. 291–304, Jan. 2015.

[28] 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.

[29] 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. 4, no. 1, pp. 46–49, Feb. 2015.

[30] 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. 63, no. 1, pp. 215–228, Jan. 2015.

[31] 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.

[32] D. S. Michalopoulos and G. K. Karagiannidis, "Two-relay distributed switch and stay combining," *IEEE Trans. Commun.*, vol. 56, no. 11, pp. 1790–1794, Nov. 2008.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] V. N. Q. Bao, T. Q. Duong, A. Nallanathan, and G. K. Karagiannidis, "Distributed switch-and-stay combining in cognitive relay networks under spectrum sharing constraints," in *Proc. IEEE Global Commun. Conf. (GLOBECOM'13)*, Atlanta, GA, USA, Dec. 2013, pp. 1927–1932.

[39] S. Parsaeefard and T. Le-Ngoc, "Improving wireless secrecy rate via full-duplex relay-assisted protocols," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 10, pp. 2095–2107, Oct. 2015.

[40] J. M. Peha, "Approaches to spectrum sharing," *IEEE Commun. Mag.*, vol. 43, no. 2, pp. 10–12, Feb. 2005.

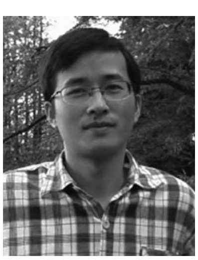
[41] H. Ding, J. Ge, D. B. da Costa, and Z. Jiang, "Asymptotic analysis of cooperative diversity systems with relay selection in a spectrum sharing scenario," *IEEE Trans. Veh. Technol.*, vol. 60, no. 2, pp. 457–472, Feb. 2011.

[42] S. Sagong, J. Lee, and D. Hong, "Capacity of reactive DF scheme in cognitive relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 1536–1276, Oct. 2011.

[43] L. Fan, X. Lei, T. Q. Duong, R. Q. Hu, and M. Elkashlan, "Multiuser cognitive relay networks: Joint impact of direct and relay communications," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 5043–5055, Sep. 2014.

[44] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[45] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic, 2007.



Lisheng Fan received the bachelor's degree in electronic engineering from Fudan University, Shanghai, China, the master's degree in electronic engineering from Tsinghua University, Beijing, China, and the Ph.D. degree in communications and integrated systems from Tokyo Institute of Technology, Tokyo, Japan, in 2002, 2005, and 2008, respectively. Since 2014, he has been a Professor. His research interests include the areas of wireless cooperative communications, physical-layer secure communications, interference modeling, and system performance evaluation. He has authored many papers in international journals such as the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTION ON VEHICULAR TECHNOLOGY, the IEEE COMMUNICATIONS LETTERS, and the IEEE WIRELESS COMMUNICATIONS LETTERS, as well as papers in conferences such as the IEEE ICC, the IEEE Globecom, and the IEEE WCNC. He has been a Guest Editor of *EURASIP Journal on Wireless Communications and Networking*, and served as the Chair of Wireless Communications and Networking Symposium for Chinacom 2014. He has also served as a member of technical program committees for IEEE conferences such as GLOBECOM, ICC, WCNC, and VTC.

Shengli Zhang received the B.Eng. degree in electronic engineering and the M.Eng. degree in communication and information engineering from the University of Science and Technology of China (USTC), Hefei, China, and the Ph.D. degree in information engineering from Chinese University of Hong Kong (CUHK), Hong Kong, in 2002, 2005, and 2008, respectively. After that, he worked as a Research Associate at CUHK. In May 2009, he joined the Department of Communication Engineering, Shenzhen University, Shenzhen, China, where he is currently an Associate Professor. From 2014 to 2015, he was a Visiting Associate Professor at Stanford University, Stanford, CA, USA. His research interests include physical layer network coding, known interference cancellation, and cooperative wireless networks.

Trung Q. Duong (S'05–M'12–SM'13) received the Ph.D. degree in telecommunications systems from Blekinge Institute of Technology (BTH), Blekinge, Sweden, in 2012. Since 2013, he has been a Lecturer (Assistant Professor) with Queen's University Belfast, Belfast, U.K. His research interests include cooperative communications, cognitive radio networks, physical layer security, massive MIMO, cross-layer design, mm-waves communications, and localization for radios and networks. He is the author or coauthor of 170 technical papers published in scientific journals and presented at international conferences. He currently serves as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE COMMUNICATIONS LETTERS, *IET Communications*, *Transactions on Emerging Telecommunications Technologies*, and *Electronics Letters*. He has also served as the Guest Editor of the special issue on some major journals including the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, *IET Communications*, *IEEE Wireless Communications Magazine*, *IEEE Communications Magazine*, *EURASIP Journal on Wireless Communications and Networking*, and *EURASIP Journal on Advances Signal Processing*. He was the recipient of Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013 and the IEEE International Conference on Communications (ICC) 2014.

George K. Karagiannidis (M'96–SM'03–F'14) was born in Pithagorion, Samos Island, Greece. He received the diploma (5 years) and Ph.D. degrees, both in electrical and computer engineering from the University of Patras, Patras, Greece, in 1987 and 1999, respectively. From 2000 to 2004, he was a Senior Researcher with the Institute for Space Applications and Remote Sensing, National Observatory of Athens, Athens, Greece. In June 2004, he joined the faculty of Aristotle University of Thessaloniki, Thessaloniki, Greece, where he is currently a Professor with the Department of Electrical & Computer Engineering and Director of Digital Telecommunications Systems and Networks Laboratory. His research interests include the broad area of digital communications systems with emphasis on communications theory, energy efficient MIMO and cooperative communications, satellite communications, cognitive radio, localization, smart grid, and optical wireless communications. He is the author or coauthor of more than 300 technical papers published in scientific journals and presented at international conferences, the author of the Greek edition of the book *Telecommunications Systems* and co-author of the book *Advanced Optical Wireless Communications Systems* (Cambridge Publications, 2012). He has been a member of technical program committees for several IEEE conferences such as ICC, GLOBECOM, VTC, etc. In the past, he was an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS and *EURASIP Journal of Wireless Communications and Networking*, and a Senior Editor of the IEEE COMMUNICATIONS LETTERS. He was the Lead Guest Editor of the special issue on Optical Wireless Communications of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS and Guest Editor of the special issue on Large-Scale Multiple Antenna Wireless Systems. Since January 2012, he has been the Editor-in Chief of the IEEE COMMUNICATIONS LETTERS. He has been selected as a 2015 Thomson Reuters Highly Cited Researcher.