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


Published in:
IEEE Transactions on Communications

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

Publisher rights
© 2015 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.
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.

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 relay 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:

1. 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.
2. 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.
3. 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.
4. 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 $\mathcal{C}_N(0, \sigma^2)$ denotes a circularly symmetric complex Gaussian random variable with zero mean and variance $\sigma^2$. We use $f_X(\cdot)$ to represent the probability density function of random variable $X$. Notation $\Pr[\cdot]$ returns the probability.

## 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 wiretapping. 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\textsuperscript{1}. Before presenting the SSSC protocol, we first detail the two-phase data transmission process, as follows.

Assume that the relay \( R_i \) \((i = 1, \text{or} 2) \) 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
\[
y_{R_i} = \sqrt{P_S} h_{S,R_i} x_S + n_{R_i},
\]
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
\[
P_S = \frac{I_P}{|h_{S,PU}|^2},
\]
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
\[
\text{SNR}_{R_i} = \frac{I_P u_i}{I_0},
\]
where \( u_i = |h_{S,R_i}|^2 \) and \( I_0 = |h_{S,PU}|^2 \) 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
\[
\frac{1}{2} \log_2 (1 + \text{SNR}_{R_i}) \geq R_d,
\]
which is equivalent to \( \text{SNR}_{R_i} \geq \gamma_0 \) 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
\[
y_D = \sqrt{P_R} h_{R_i,D} x_S + n_D,
\]
\[
y_E = \sqrt{P_R} h_{R_i,E} x_S + n_E,
\]
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, \( P_R \) is the transmit power of relay \( R_i \), which is limited by
\[
P_R = \frac{I_P}{|h_{R_i,PU}|^2},
\]
to guarantee the QoS of primary communications, where \( h_{R_i,PU} \sim \mathcal{CN}(0, \eta_i) \) is the instantaneous channel parameter
\textsuperscript{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.

of the \( R_i-PU \) link. From (5)-(7), the received SNRs at \( D \) and \( E \) are written respectively as
\[
\text{SNR}_D = \frac{I_P u_i}{I_0},
\]
\[
\text{SNR}_E = \frac{I_P w_i}{I_0},
\]
where \( u_i = |h_{R_i,D}|^2 \), \( w_i = |h_{R_i,E}|^2 \) 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
\[
\frac{1}{2} \log_2 (1 + \text{SNR}_D) - \frac{1}{2} \log_2 (1 + \text{SNR}_E) < R_s,
\]
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
\[
\frac{1 + \tilde{I}_P w_i}{1 + \tilde{I}_P u_i} < \gamma_s,
\]
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 \( R_i \) \((i = 1, \text{or} 2) \) 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
\[
\frac{1 + \tilde{I}_P w_i}{1 + \tilde{I}_P u_i} \geq T,
\]
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

$$
\frac{1 + \hat{I}_{P, w_i}}{1 + \hat{I}_{P, E(w_i)}} \geq T, \quad (13)
$$

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) at the top of this page, where the notation $\parallel$ 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

$$p_1 = \frac{c_1}{c_1 + c_2}, \quad (15)$$
$$p_2 = \frac{c_2}{c_1 + c_2}, \quad (16)
$$

where

$$c_1 = \Pr \left[ \hat{I}_{P, w_1} \geq \gamma_0, \frac{t_1 + \hat{I}_{P,v_1}}{t_1 + \hat{I}_{P,w_1}} \geq T \right], \quad (17)$$
$$c_2 = \Pr \left[ \hat{I}_{P, w_2} \geq \gamma_0, \frac{t_2 + \hat{I}_{P,v_2}}{t_2 + \hat{I}_{P,w_2}} \geq T \right], \quad (18)
$$

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 $P_0$ 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

$$c_1 = L\left(\frac{\gamma_0}{I_{P, \alpha_1}}\right) L\left(\frac{(T-1)\eta_1}{I_{P, \beta_1}}\right) L\left(\frac{T\epsilon_1}{\beta_1}\right), \quad (19)
$$

where $L(x) = (1 + x)^{-1}$ and (19) is obtained by applying the probability density functions of $f_{w_1}(x) = \frac{1}{\gamma_0} e^{-\frac{\gamma_0}{\gamma_0}}$, $f_{t_1}(x) = \frac{1}{\eta_1} e^{-\frac{x}{\eta_1}}$, $f_{v_1}(x) = \frac{1}{\beta_1} e^{-\frac{x}{\beta_1}}$ and $f_{w_1}(x) = \frac{1}{\epsilon_1} e^{-\frac{x}{\epsilon_1}}$ [45]. The analytical expressions of $J_1$ and $J_2$ are given by

$$J_1 = \begin{cases} L\left(\frac{\gamma_0}{I_{P, \alpha_1}}\right) L\left(\frac{(T-1)\eta_1}{I_{P, \beta_1}}\right) L\left(\frac{T\epsilon_1}{\beta_1}\right), & \text{if } T < \gamma_s, \\ 0, & \text{if } T \geq \gamma_s. \end{cases} \quad (20)
$$

$$J_2 = \left[ 1 - L\left(\frac{(\gamma_s-1)\eta_2}{I_{P, \beta_2}}\right) L\left(\frac{\gamma_s\epsilon_2}{\beta_2}\right) \right] L\left(\frac{\gamma_0}{I_{P, \alpha_2}}\right) L\left(\frac{(T-1)\eta_1}{I_{P, \beta_1}}\right) L\left(\frac{T\epsilon_1}{\beta_1}\right) \quad (21)
$$

**Proof:** See Appendix A.
\[
P_{out} = \tilde{p}_1 \Pr \left[ \frac{I_P u_1}{t_0} \geq \gamma_0, \frac{t_1 + \tilde{I}_P v_1}{t_1 + I_P E(w_1)} \geq T, \frac{t_1 + \tilde{I}_P v_1}{t_1 + I_P w_1} < \gamma_s \right] + \tilde{p}_2 \Pr \left[ \frac{I_P u_2}{t_0} \geq \gamma_0, \frac{t_2 + \tilde{I}_P v_2}{t_2 + I_P E(w_2)} \geq T, \frac{t_2 + \tilde{I}_P v_2}{t_2 + I_P w_2} < \gamma_s \right]
\]

\[
+ \tilde{p}_1 \Pr \left[ \frac{I_P u_1}{t_0} \geq \gamma_0, \frac{t_1 + \tilde{I}_P v_1}{t_1 + I_P E(w_1)} < T, \frac{t_1 + \tilde{I}_P v_1}{t_1 + I_P w_1} \geq \gamma_s \right] + \tilde{p}_2 \Pr \left[ \frac{I_P u_2}{t_0} \geq \gamma_0, \frac{t_2 + \tilde{I}_P v_2}{t_2 + I_P E(w_2)} < T, \frac{t_2 + \tilde{I}_P v_2}{t_2 + I_P w_2} \geq \gamma_s \right]
\]

(22)

By replacing \(\alpha_1, \beta_1, \eta_1\) and \(\varepsilon_1\) by \(\alpha_2, \beta_2, \eta_2\) and \(\varepsilon_2\) 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 \(\alpha_1\) with \(\alpha_2\), \(\beta_1\) with \(\beta_2\), and \(\eta_1\) with \(\eta_2\), 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) at the top of the next page, where \(J_1\) 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 that from \(R_2\) to \(R_1\), respectively. Also, \(\tilde{p}_1\) and \(\tilde{p}_2\) are given by

\[
\tilde{p}_1 = \frac{\tilde{c}_1}{\tilde{c}_1 + \tilde{c}_2}, \quad \tilde{p}_2 = \frac{\tilde{c}_2}{\tilde{c}_1 + \tilde{c}_2},
\]

(23)

(24)

where

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

(25)

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

(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 \(J_2\) and \(J_4\). This makes the data transmission of both branches correlated, and the mathematical analysis becomes more complicated. Moreover, the secure switching metric \(\frac{t_1 + \tilde{I}_P v_1}{t_1 + I_P E(w_1)}\) is highly correlated with the outage metric \(\frac{t_1 + \tilde{I}_P v_1}{t_1 + I_P w_1}\), 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 \(c_1\), \(J_1\) and \(J_2\) in the following proposition.

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

\[
\tilde{c}_1 = L \left( \frac{\gamma_0 \eta_1}{I_P \alpha_1} \right) L \left( \frac{(T - 1) \eta_1}{I_P \beta_1} \right) e^{-\frac{T \varepsilon_1}{\beta_1}}.
\]

(27)

The analytical expressions of \(J_1\) and \(J_2\) are given by

\[
J_1 = L \left( \frac{\gamma_0 \eta_1}{I_P \alpha_1} \right) \theta,
\]

(28)

\[
J_2 = \left[ 1 - L \left( \frac{(T - 1) \eta_1}{I_P \beta_1} \right) L \left( \frac{\gamma_0 \eta_2}{I_P \alpha_2} \right) \right] L \left( \frac{\gamma_0 \eta_2}{I_P \alpha_2} \right) e^{-\frac{T \varepsilon_1}{\beta_1}},
\]

(29)

where \(\theta\) is given by (30) at the top of this page, and

\[
\begin{align*}
q_0 &= \frac{T}{\eta_1} + \frac{T \varepsilon_1}{\beta_1}, \\
q_1 &= \left( \frac{1}{\eta_1} + \frac{T - 1}{I_P \beta_1} \right) \frac{\tilde{I}_P}{\gamma_0}, \\
q_2 &= \left( \frac{1}{\eta_1} + \frac{\gamma_0 - 1}{I_P \beta_1} \right) \frac{\tilde{I}_P}{\gamma_0}.
\end{align*}
\]

(31)

**Proof:** See Appendix B.

Similarly, by replacing \(\alpha_1\) by \(\alpha_2\), \(\beta_1\) with \(\beta_2\), and \(\eta_1\) with \(\eta_2\), we can obtain the analytical expression of \(c_2\) from the expression of \(c_1\) in Proposition 2. This leads to the analytical expressions of \(\tilde{p}_1\) and \(\tilde{p}_2\). By swapping \(\alpha_1\) with \(\alpha_2\), \(\beta_1\) with \(\beta_2\), and \(\eta_1\) with \(\eta_2\), we can obtain the analytical expressions of \(J_3\) and \(J_4\) from the expressions of \(J_1\) and \(J_2\) in Proposition 2. In this way, we arrive at the analytical expression of SOP with S-ECSI as \(P_{out} = \tilde{p}_1(J_1 + J_2) + \tilde{p}_2(J_3 + J_4)\).
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

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

where

\[
  \zeta_1 = \frac{\rho_1 \eta_1}{\beta_1}, \quad \zeta_2 = \frac{\rho_2 \eta_2}{\beta_2},
\]

\[
  \rho_1 = \frac{\lambda_1}{I_P}, \quad \rho_2 = \frac{\lambda_2}{I_P}.
\]

\[
  \varepsilon_1 = [\gamma_s + (\gamma_s - 1)\zeta_2] \cdot [T + (T - 1)\zeta_1 + \gamma_0 \rho_1 \rho_1 / \alpha_1]
\]

\[
  \varepsilon_2 = [\gamma_s + (\gamma_s - 1)\zeta_1] \cdot [T + (T - 1)\zeta_2 + \gamma_0 \rho_2 / \alpha_2]. \tag{34}
\]

Proof: See Appendix C.

In particular, when the transmit power is much larger than MER with \( I_P \gg \lambda_i \) (\( i = 1, 2 \)), \( \rho_1 \) approaches to zero, causing that \( \zeta_1 \simeq 0 \) and \( \varepsilon_1 \simeq 0 \). In this case, we can simplify the asymptotic SOP in (33) as

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

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

Remark 1: In high \( I_P \) 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 \( \gamma_s \).

D. Asymptotic SOP with S-ECSI

To obtain some insights on the system of SSSC with I-ECSI, we now derive the asymptotic SOP with large \( I_P \) and MER, in the following proposition.

Proposition 4: The asymptotic \( c_1 \) and \( c_2 \) with large \( I_P \) and MER can be written from [36, eq. (1.112)] as

\[
  c_1 \simeq 1, \quad c_2 \simeq 1. \tag{36}
\]

Then we approximate the SOP of SSSC with S-ECSI in high \( I_P \) and high MER regions as

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

with

\[
  \begin{align*}
    \varepsilon_3 &= (\gamma_s - T)\zeta_1 / \gamma_s, \\
    \varepsilon_4 &= (\gamma_s - T)\zeta_2 / \gamma_s. \tag{38}
  \end{align*}
\]

Proof: See Appendix D.

In particular, when the transmit power is much larger than the value of MER with \( I_P \gg \lambda_i \) (\( i = 1, 2 \)), both \( \varepsilon_3 \) and \( \varepsilon_4 \) approach to zero due to \( \zeta_i \simeq 0 \). In this condition, the asymptotic SOP of SSSC with S-ECSI is simplified as

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

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

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

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 one in high \( I_P \) 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 \( P_{\text{out}} \), 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 large value of \( T \), which can effectively exploit the two relays to guarantee the secure transmission.

Remark 3: By comparing the minimum asymptotic \( P_{\text{out}} \) 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

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

(41)

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

\[ \mu_S = 1 - \frac{c_1^2 + c_2^2}{2c_1 + c_2}. \]  

(42)

As the stay probabilities \( c_i \) and \( \bar{c}_i \) 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 \( \bar{c}_i \) 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 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 \( \gamma_0 = \gamma_1 = \gamma_2 = 1 \). The source data rate \( R_s \) is set to 1 bps/Hz, so that the associated \( \gamma_0 \) is equal to 3. The secrecy data rate \( R_s \) is set to 0.5 bps/Hz, so that the secrecy SNR threshold \( \gamma_s \) is equal to 2.

Fig. 2 depicts the analytical, asymptotic and simulated SOPs of SSSC versus MER with \( \lambda_1 = \lambda_2 = \lambda \) and \( I_p = 20 \)dB\(^2\), where the asymptotic results are computed from eqs. (33) and (37), respectively. The secure switching threshold \( T \) varies in \([0.5, 1, 2]T^* \), where the optimal switching threshold \( T^* \) is set to \( \gamma_s \) 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 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 $\{0.5, 1.2\} T^*$. $\lambda_1 = \lambda_2 = 30 \text{dB}$ 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 $I_P$ 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 $\tilde{c}_1$ of SSSC versus MER with $\lambda_1 = \lambda_2 = \lambda$ and $\tilde{I}_P = 20 \text{dB}$, 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 $\tilde{I}_P = 20 \text{dB}$, where the secure switching threshold $T$ varies in $\{0.5, 1.2\} T^*$. In particular, Fig. 5 (a) and (b) correspond to

\begin{align*}
\eta_1 = \eta_2 &= 1 \\
D_1 &= 0.5, D_2 = 0.3 \\
\lambda_1 &= \lambda_2 = 30 \text{dB}
\end{align*}

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.
transmission; otherwise the secure relay switching occurred
transmission when the relay could support the secure data
destination. The same relay continued to be used for data
relaying switching threshold. Moreover, SSSC can reduce the
S-ECSI can approach to the full diversity with large secure
ECSI can exploit the system full diversity, and SSSC with
over opportunistic relaying.

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

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 cog-
nitive 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.

APPENDIX A

PROOF OF PROPOSITION 1

As the variable \( R_t \) is independent of \( \frac{t_1 + I_P v_1}{t_1 + I_P w_1} \), we can write \( c_1 \) from (17) as

\[
c_1 = P_t(\frac{R_t}{t_0} \geq \frac{\gamma_0}{I_P}) \cdot P_t(\frac{t_1 + I_P v_1}{t_1 + I_P w_1} \geq T) \tag{A.1}
\]

By applying the probability density functions of \( f_{u_1}(u_1) = \frac{1}{\beta_1} e^{-\frac{u_1}{\beta_1}}, f_{v_1}(t_1) = \frac{1}{\beta_1} e^{-\frac{t_1}{\beta_1}}, f_{v_1}(v_1) = \frac{1}{\beta_1} e^{-\frac{v_1}{\beta_1}} \) and \( f_{w_1}(w_1) = \frac{1}{\beta_1} e^{-\frac{w_1}{\beta_1}} \), we can compute \( P_t(\frac{R_t}{t_0} \geq \frac{2\gamma_0}{I_P}) \) and \( P_t(\frac{t_1 + I_P v_1}{t_1 + I_P w_1} \geq T) \) as

\[
P_t(\frac{R_t}{t_0} \geq \frac{\gamma_0}{I_P}) = \int_0^{\infty} f_{v_1}(t_1) \int_{t_1 + I_P w_1}^{\infty} f_{u_1}(u_1) du_1 dt_0 \tag{A.2}
\]

\[
= L(\frac{\gamma_0}{I_P}) \int_0^{\infty} f_{v_1}(t_1) \int_{t_1 + I_P w_1}^{\infty} f_{u_1}(u_1) du_1 dt_0 \tag{A.3}
\]

\[
P_t(\frac{t_1 + I_P v_1}{t_1 + I_P w_1} \geq T) = P_t(\frac{v_1}{t_1 + I_P w_1} \geq \frac{T - 1}{I_P} \frac{t_1 + T w_1}{T}) \tag{A.5}
\]

\[
= \int_0^{\infty} f_{t_1}(t_1) \int_0^{\infty} f_{w_1}(w_1) \int_{t_1 + I_P w_1}^{\infty} f_{v_1}(v_1) dv_1 dw_1 dt_1 \tag{A.6}
\]

\[
= L(\frac{T \varepsilon_1}{\beta_1}) L\left(\frac{(T - 1) \eta_1}{I_P \beta_1}\right) \tag{A.7}
\]

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 \( \frac{\gamma_0}{I_P t_0} \) is independent of \( \frac{1 + I_P v_1}{t_1 + I_P w_1} \), we can write \( J_1 \) as

\[
J_1 = P_t(\frac{R_t}{t_0} \geq \frac{\gamma_0}{I_P}) \cdot P_t(\frac{t_1 + I_P v_1}{t_1 + I_P w_1} \geq T, \frac{t_1 + I_P v_1}{t_1 + I_P w_1} < \gamma_s) \tag{A.8}
\]

\[
= L(\frac{\gamma_0}{I_P \alpha_1}) P_t\left(\frac{t_1 + I_P v_1}{t_1 + I_P w_1} \geq T, \frac{t_1 + I_P v_1}{t_1 + I_P w_1} < \gamma_s\right), \tag{A.9}
\]

where we apply the result of (A.3) in the last equality. When \( T \geq \gamma_s \), \( \frac{1 + I_P v_1}{t_1 + I_P w_1} \geq T \) contradicts with \( \frac{t_1 + I_P v_1}{t_1 + I_P w_1} < \gamma_s \), causing that \( J_1 = 0 \). On the other hand, when \( T < \gamma_s \), we can further write \( J_1 \) as

\[
J_1 = L(\frac{\gamma_0}{I_P \alpha_1}) \left[ P_t\left(\frac{t_1 + I_P v_1}{t_1 + I_P w_1} \geq T\right)
- P_t\left(\frac{t_1 + I_P v_1}{t_1 + I_P w_1} \geq \gamma_s\right)\right] \tag{A.10}
\]

\[
= L(\frac{\gamma_0}{I_P \alpha_1}) \left[ L\left(\frac{(T - 1) \eta_1}{I_P \beta_1}\right) L\left(\frac{T \varepsilon_1}{\beta_1}\right)
- L\left(\frac{(\gamma_s - 1) \eta_1}{I_P \beta_1}\right) L\left(\frac{T \varepsilon_1}{\beta_1}\right)\right] \tag{A.11}
\]
where we apply the result of (A.7) in the last equality.
We now turn to derive the analytical expression of \( J_2 \) as
\[
J_2 = \Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P u_2} < \gamma_s \right) \\
\times \Pr \left( \tilde{I}_P u_1 < \gamma_0 \left| \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} < T, \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} \geq \gamma_0 \right. \right) \\
\times \Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} < T, \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} \geq \gamma_0 \right)
\]  
where we apply the result of (A.3) in the last equality. \( \Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} \geq T \right) \) can be computed as
\[
\Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} \geq T \right) = \Pr \left( \frac{v_1}{\tilde{I}_P} \geq \frac{T - 1}{\tilde{I}_P} t_1 + T \varepsilon_1 \right)
\]  
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 1.
We now turn to derive the analytical expression of \( \tilde{J}_1 \) in (22) as
\[
\tilde{J}_1 = \Pr \left( \frac{u_1}{t_0} \geq \gamma_0 \right) \\
\times \Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} \geq T \right) \\
\times \Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} \geq \gamma_0 \right)
\]  
where we apply the result of eqs. (A.3) and (A.7) into eqs. (A.15) and (A.16), respectively. In further, the probability of \( \Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} \geq \gamma_0 \right) \) can be computed as
\[
\Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} \geq \gamma_0 \right) = \int_0^\infty f_{t_1}(t_1) \int_0^\infty f_{u_1}(t_0) \int_0^\infty f_{u_2}(u_2) du_1 du_0 du_2
\]  
where we apply the result of (A.7) in the last equality. \( \Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} \geq T \right) \) can be computed as
\[
\Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} \geq T \right) = \Pr \left( \frac{v_1}{\tilde{I}_P} \geq \frac{T - 1}{\tilde{I}_P} t_1 + T \varepsilon_1 \right)
\]  
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
\[
\tilde{c}_1 = \Pr \left( \frac{u_1}{t_0} \geq \gamma_0 \right) \cdot \Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} \geq T \right) + \Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} < T \right)
\]  
\[
\tilde{c}_1 = \Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} \geq T \right)
\]  
\[
\tilde{c}_1 = \Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} \geq T \right) + \Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_0 + \tilde{I}_P w_1} < T \right)
\]  
where \( \tilde{c}_1 \) is defined in (31).
On the other hand, when \( T < \gamma_s \) holds, the condition of (B.8) becomes
\[
w_1 + \frac{\gamma_s - T}{\tilde{I}_P \gamma_s} t_1 \geq \frac{T \varepsilon_1}{\gamma_s}
\]  
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 \( t_1 \geq \frac{\tilde{I}_P T \varepsilon_1 - \tilde{I}_P \varepsilon_1 w_1}{\gamma_s - T} \).
Accordingly, we can compute $\tilde{J}_{11}$ as

$$\tilde{J}_{11} = \int_0^\infty f_{v_1}(t_1) \int_{\frac{\gamma_s}{P} t_1 + \gamma_1}^{\infty} f_{w_1}(w_1) \int_{\frac{\gamma_s}{P} t_1 + \gamma_2}^{\infty} f_{v_1}(t_1) \int_{\frac{\gamma_s}{P} t_1 + \gamma_2}^{\infty} f_{v_1}(v_1) dv_1 dw_1 dt_1$$

$$= \frac{2\pi}{\sqrt{P}} \int_0^\infty f_{w_1}(w_1) \int_{\frac{\gamma_s}{P} t_1 + \gamma_1}^{\infty} f_{v_1}(t_1) \int_{\frac{\gamma_s}{P} t_1 + \gamma_2}^{\infty} f_{v_1}(v_1) dv_1 dw_1 dt_1$$

$$= \left[ L \left( \frac{(T-1)\eta_1}{Ip_{1\beta_1}} \right) - L \left( \frac{\gamma_s - 1}{Ip_{2\beta_1}} \right) \right] e^{-\gamma_0}$$

$$+ \left[ L \left( \frac{(T-1)\eta_1}{Ip_{1\beta_1}} \right) L \left( -q_I \gamma_s \xi \right) e^{-\frac{\rho_1}{P} - q_I T \xi - e^{-\gamma_0}} \right]$$

$$- L \left( \frac{(\gamma_s - 1)\eta_1}{Ip_{2\beta_1}} \right) L \left( \frac{(T-1)\eta_1}{Ip_{2\beta_1}} \right) e^{-q_I T \xi - e^{-\gamma_0}},$$

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

$$\tilde{J}_2 = \Pr \left( \frac{t_2 + \tilde{I}_P v_2}{t_2 + \tilde{I}_P v_2} < \gamma_s \right)$$

$$\times \Pr \left( \frac{u_1}{t_0} < \frac{\gamma_0}{I_p} \frac{l_1 + \tilde{I}_P v_1}{l_1 + \tilde{I}_P v_1} < \gamma_0 \frac{u_2}{t_0} \gamma_0 \frac{t_0}{I_p} \right)$$

$$= \left[ 1 - L \left( \frac{(\gamma_s - 1)\eta_1}{Ip_{2\beta_2}} \right) \right]$$

$$\times \Pr \left( \frac{u_1}{t_0} < \frac{\gamma_0}{I_p} \frac{l_1 + \tilde{I}_P v_1}{l_1 + \tilde{I}_P v_1} < \gamma_0 \frac{u_2}{t_0} \gamma_0 \frac{t_0}{I_p} \right),$$

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

$$\tilde{J}_{21} = \Pr \left( \frac{w_2}{t_0} \frac{\gamma_0}{I_p} \frac{l_1 + \tilde{I}_P v_1}{l_1 + \tilde{I}_P v_1} \gamma_0 \frac{t_0}{I_p} \right)$$

$$= \Pr \left( \frac{w_2}{t_0} \frac{\gamma_0}{I_p} \frac{l_1 + \tilde{I}_P v_1}{l_1 + \tilde{I}_P v_1} \gamma_0 \frac{t_0}{I_p} \right)$$

$$= \left[ 1 - L \left( \frac{(\gamma_s - 1)\eta_1}{Ip_{2\beta_2}} \right) \right]$$

$$\times \Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_1 + \tilde{I}_P v_1} \gamma_0 \frac{t_0}{I_p} \right)$$

$$= L \left( \frac{\gamma_0}{I_p} \frac{l_1 + \tilde{I}_P v_1}{l_1 + \tilde{I}_P v_1} \right)$$

$$\times \Pr \left( \frac{t_1 + \tilde{I}_P v_1}{t_1 + \tilde{I}_P v_1} \gamma_0 \frac{t_0}{I_p} \right)$$

$$= \frac{2\pi}{\sqrt{P}} \int_0^\infty f_{w_1}(w_1) \int_{\frac{\gamma_s}{P} t_1 + \gamma_1}^{\infty} f_{v_1}(v_1) dv_1 dw_1 dt_1$$

$$= \left[ L \left( \frac{(T-1)\eta_1}{Ip_{1\beta_1}} \right) - L \left( \frac{\gamma_s - 1}{Ip_{2\beta_1}} \right) \right] e^{-\gamma_0}$$

$$+ \left[ L \left( \frac{(T-1)\eta_1}{Ip_{1\beta_1}} \right) L \left( -q_I \gamma_s \xi \right) e^{-\frac{\rho_1}{P} - q_I T \xi - e^{-\gamma_0}} \right]$$

$$- L \left( \frac{(\gamma_s - 1)\eta_1}{Ip_{2\beta_1}} \right) L \left( \frac{(T-1)\eta_1}{Ip_{2\beta_1}} \right) e^{-q_I T \xi - e^{-\gamma_0}},$$

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

$$c_1 \simeq 1, \quad c_2 \simeq 1,$$

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 $I_p$ and MER as

$$J_1 \simeq \frac{\gamma_s}{\lambda_1} \left( 1 + \frac{\eta_1 \rho_1}{\beta_1} \right),$$

where $\rho_1$ 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 $I_p$ and MER as

$$J_2 \simeq \frac{\varepsilon_1}{\lambda_1 \lambda_2},$$

where $\varepsilon_1$ is defined in (34). Similarly, we can obtain the asymptotic expressions of $J_3$ and $J_4$. By combining the asymptotic results of $J_1$, $J_2$, $J_3$ and $J_4$, we can arrive at the asymptotic SOP with high $I_p$ 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 $I_p$ and MER as

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

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

$$\tilde{p}_1 \simeq 1, \quad \tilde{p}_2 \simeq 1.$$  

We then extend to derive the asymptotic expressions of $\tilde{J}_1$, $\tilde{J}_2$, $\tilde{J}_3$ and $\tilde{J}_4$ with high $I_p$ 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

$$\tilde{J}_1 \simeq \frac{\gamma_s}{\lambda_1} \left( 1 - \frac{1}{1 - \varepsilon_3} \right) \left( 1 - \frac{1}{1 - \varepsilon_3} \right),$$

$$\tilde{J}_2 \simeq \frac{\varepsilon_1}{\lambda_1 \lambda_2}.$$  

where $\varepsilon_3$ is defined in (38). In a similar way, we can obtain the asymptotic expressions of $J_3$ and $J_4$ with high $I_p$ 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.
Lisheng Fan received the bachelor and master degrees from Fudan University and Tsinghua University, China, in 2002 and 2005, respectively, both from Department of Electronic Engineering. He received the Ph.D. degree from Department of Communications and Integrated Systems of Tokyo Institute of Technology, Japan, in 2008. From 2014, he has been an Associate Professor. His research interests span in the areas of wireless cooperative communications, physical-layer secure communications, interference modeling, and system performance evaluation. Lisheng Fan has published many papers in international journals such as IEEE Transaction on Wireless Communications, IEEE Transaction on Vehicular Technology, IEEE Communications Letters and IEEE Wireless Communications Letters, as well as papers in conferences such as IEEE ICC, IEEE Globecom, and IEEE WCNC. He is a guest editor of EURASIP Journal on Wireless Communications and Networking, and served as the chair of Wireless Communications and Networking Symposium for Chinaacom 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 his 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, in 2002 and 2005, respectively. He received his Ph.D. in the Department of Information Engineering, the Chinese University University of Hong Kong (CUHK), in 2008. After that, he worked as a research associate in CUHK. In May, 2009, he joined the Communication Engineering Department, Shenzhen University. Now, he holds an associate professor there. From 2014 to 2015, he was a visiting associate professor at Stanford University. 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 his Ph.D. degree in Telecommunications Systems from Blekinge Institute of Technology (BTH), Sweden in 2012. Since 2013, he has joined Queen’s University Belfast, UK as a Lecturer (Assistant Professor). His current research interests include cooperative communications, cognitive radio networks, physical layer security, massive MIMO, cross-layer design, mm-wave communications, and localization for radars and networks. He is the author or co-author of more than 170 technical papers published in scientific journals and presented at international conferences.

Dr. Duong currently serves as an Editor for the IEEE Transactions on Communications, IEEE Communications Letters, IET Communications, Wiley 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 IEEE Journal in Selected Areas on Communications, IET Communications, IEEE Wireless Communications Magazine, IEEE Communications Magazine, EURASIP Journal on Wireless Communications and Networking, EURASIP Journal on Advances in Signal Processing. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, 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 University Diploma (5 years) and PhD degree, both in electrical and computer engineering from the University of Patras, in 1987 and 1999, respectively. From 2000 to 2004, he was a Senior Researcher at the Institute for Space Applications and Remote Sensing, National Observatory of Athens, Greece. In June 2004, he joined the faculty of Aristotle University of Thessaloniki, Greece where he is currently Professor in the Electrical Computer Engineering Dept. and Director of Digital Telecommunications Systems and Networks Laboratory. His research interests are in 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 co-author of more than 300 technical papers published in scientific journals and presented at international conferences. He is also author of the Greek edition of a book on “Telecommunications Systems” and co-author of the book “Advanced Optical Wireless Communications Systems”, Cambridge Publications, 2012. Dr. Karagiannidis has been a member of Technical Program Committees for several IEEE conferences such as ICC, GLOBECOM, VTC, etc. In the past he was Editor in IEEE Transactions on Communications, Senior Editor of IEEE Communications Letters and Editor of the EURASIP Journal of Wireless Communications Networks. He was 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”. Dr. Karagiannidis has been selected as a 2015 Thomson Reuters Highly Cited Researcher and since January 2012 he is the Editor-in-Chief of IEEE Communications Letters.