Distributed Secure Switch-and-Stay Combining Over Correlated Fading Channels

Xiazhi Lai, Lisheng Fan, Xianfu Lei, Jin Li, Nan Yang, *Member, IEEE*, and George K. Karagiannidis, *Fellow, IEEE*

***Abstract*— In this paper, we study decode-and-forward relaying networks in the presence of direct links, where they are used by the eavesdropper to overhear the confidential message from the source and relay. The secure data transmission can go through from either the direct or the relaying branch, and we focus on the practical communication scenarios, where the main and eavesdropper channels are correlated. Although traditional opportunistic selection techniques can choose one better branch to ensure the secure performance, it needs to continuously know the channel state information (CSI) of both branches and may result in a high branch switching rate. To overcome these limitations, we propose a distributed secure switch-and-stay combining (DSSSC) protocol, where only one between direct and relaying branches is activated to assist the secure data transmission, and the switching occurs when the branch cannot support the secure communication any longer. The DSSSC protocol uses either the instantaneous or the statistics of the eavesdropping CSI. For both cases, we quantify the impact of correlated fading on secure communication by deriving an analytical expression for the secrecy outage probability (SOP) as well as an asymptotic expression for the high main-to-eavesdropper ratio region. From the asymptotic SOP, we can conclude that the DSSSC can achieve the optimal secure performance of opportunistic selection with less implementation complexity, and the channel correlation can further enhance the transmission security.**

***Index Terms*— Secure transmission, correlated fading, DSSSC, secrecy outage probability.**

Manuscript received August 15, 2018; revised December 8, 2018; accepted December 24, 2018. Date of publication January 10, 2019; date of current version May 9, 2019. This work was supported in part by NSFC under Grant 61871139, Grant 61722203, and Grant 61801132, in part by the Guangdong Natural Science Funds for Distinguished Young Scholar under Grant 2014A030306027, in part by the Innovation Team Project of Guangdong Province University under Grant 2016KCXTD017, and in part by the Science and Technology Program of Guangzhou under Grant 201807010103. The work of X. Lei was supported in part by NSFC under Grant 61501382, in part by the Sichuan Science and Technology Program under Grant 2017HH0035, in part by the Fundamental Research Funds for the Central Universities under Grant 2682018CX27, and in part by the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University, under Grant 2017D15. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Walid Saad. *(Corresponding author: Lisheng Fan.)*

X. Lai, L. Fan, and J. Li are with the School of Computer Science, Guangzhou University, Guangzhou 510006, China (e-mail: laixzh@mail2.sysu.edu.cn; lsfan@gzhu.edu.cn; lijin@gzhu.edu.cn).

X. Lei is with the Provincial Key Lab of Information Coding and Transmission, Southwest Jiaotong University, Chengdu 610031, China, and also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: xflei@home.swjtu.edu.cn).

N. Yang is with the Research School of Electrical, Energy and Materials Engineering, The Australian National University, Canberra, ACT 2600, Australia (e-mail: nan.yang@anu.edu.au).

G. K. Karagiannidis is with the Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece (e-mail: geokarag@auth.gr).

Digital Object Identifier 10.1109/TIFS.2019.2891932

I. Introduction

DUE to the broadcast nature of wireless channels, the transmission of confidential message may be wiretapped by eavesdroppers in the networks, which causes the severe issue of information leakage [1]. To safeguard the secure transmission, physical-layer security (PLS) and encryption algorithms should be applied, from the physical to application layer, respectively. Compared with the traditional encryption algorithms, PLS can achieve the perfect secrecy in theory and its implementation complexity is much lower [2]. Hence, it can serve as an important complement to the traditional encryption algorithms [3]. In recent years, PLS has attracted a lot of attention from the researchers in both academic and industrial fields.

A. Previous Work

For the PLS, the pioneering work was done by Wyner [4], where a wiretap channel model was proposed, and it is found that perfect secrecy can be achieved with properly designed encoder and decoder. Then, other researchers extended Wyner's work to fading channel environments, and studied the important secrecy performance metrics, such as secrecy data rate and secrecy outage probability (SOP) [5]–[8]. Specifically, Bloch *et al.* [6] investigated the secure communications over Rayleigh fading channels, and derived the analytical expressions of secrecy data rate and SOP. Moreover, Li and Petropulu [7] and Liu [8] investigated the secure communications over Rician fading channels, and studied the effect of Rician factor on the secrecy performance. For the smart attacker, Li *et al.* [9], Xiao *et al.* [10], and Xu *et al.* [11] used the the reinforcement learning to proposed efficient anti-wiretap schemes in order to maximize the secrecy data rate, and it found that the wiretap and jamming of the attacker can be efficiently suppressed. For the secondary networks, Cao *et al.* [12] designed an effective secure transmission scheme to optimize the network secrecy performance.

In order to improve the transmission security, cooperative relaying technique can be incorporated into wireless communications, where there are two fundamental relaying protocols, i.e., amplify-and-forward (AF) and decode-and-forward (DF) [13], [14]. The secrecy performance of relaying networks has been widely studied by analyzing and optimizing the network secrecy data rate and SOP [15]–[18]. An effective secure transmission scheme based on joint beamforming and time switching was proposed to maximize the secrecy data rate in

wireless-powered relaying systems [19], and a novel two-phase secure transmission protocol was presented for the wireless-powered relay systems with the assistance of partial eavesdropper CSI [20]. For multi-relay networks, secure transmission can be rapidly improved by exploiting the channel fluctuation among relay channels. For example, Fan *et al.* [21] studied the secure transmission of relay networks with multiple AF relays, and provided an analytical expression for the SOP, as well as an asymptotic expression in the high regime of main-to-eavesdropper ratio (MER) which indicates that the average channel gain of main links is much larger than that of the eavesdropping links. Fan *et al.* [22] investigated the secure communication of multiple DF relay networks and studied the secrecy performance by deriving the analytical and asymptotic expression for SOP. In [21] and [22], the opportunistic relay selection is used, which requires to continuously know the channel parameters of all relays and results in frequent relay switching. To overcome these limitations, a secure switch-and-stay combining (SSSC) protocol was proposed for two-relay networks [23], and distributed switch-and-stay combining (DSSC) was investigated for the relaying networks with direct links, where the channel information of eavesdropper links was however not exploited for DSSC [24].

Most of the existing research on the PLS assume that the main and eavesdropper channels experience independent fading. However, due to the practical factors, such as locations of eavesdropper and legitimate nodes, radio scattering environments and antenna deployments [25], [26], channel correlation becomes inevitable and it is of vital importance to investigate the channel correlation on the network secrecy performance. To this end, Jeon *et al.* [27] and Sun *et al.* [28] evaluated the secrecy performance with correlated main and eavesdropper's channels, and suggested that the channel correlation had adverse effect on the secrecy performance at low MER region. Moreover, the works in [29] and [30] proposed that when the MER is sufficiently high, channel correlation could help strengthen secure transmissions in the relay networks.

Note that in [29] and [30], only the relaying links were considered for the secure transmission. However, in the practical moderate shadowing environments, the direct links between the source and destination may also exist, which yield a significant impact on the transmission security. Specifically, the eavesdropper in the network can overhear the secure message through the direct links, and hence it is of vital importance to design an efficient secure transmission protocol with low implementation complexity. Moreover, besides the channel correlation of relaying links between the main and eavesdropper channels, the correlation of direct links may also exist between the main and eavesdropper channels, and these correlations on the network security should be revealed.

B. Contribution of This Paper

In this paper, we study the secure transmission of the DF relaying networks in the presence of direct link, where the main and eavesdropper channels are correlated. The main contribution of this paper lies in the following two aspects.

The first aspect is one critical question: "How to reduce the implementation complexity, while maintaining the secure performance in the presence of direct link?" In tackling this, we propose to utilize distributed secure switch-and-stay combining (DSSSC), aided by the instantaneous eavesdropping channel state information (I-ECSI) or statistics of eavesdropping channel state information (S-ECSI). In this protocol, only one between direct and relaying branches is activated to assist the secure data transmission, and the secure branch switching occurs when the branch cannot support the secure communication any longer.

The second aspect is another critical question: "How the channel correlation between the main and eavesdropper channels affects the secure communications of relaying networks?", by taking into account the practical communication scenarios, where the main and eavesdropper channels are correlated due to factors e.g. radio scattering environments and antenna deployments. In doing this, we quantify the impact of correlated fading on secure communication by deriving an analytical expression for the SOP as well as an asymptotic expression for the high MER region. From the asymptotic SOP, we conclude that with the assistance of instantaneous eavesdropping CSI, DSSSC can achieve the secure performance of opportunistic selection and obtain the diversity order of two. Moreover, for DSSSC with either I-ECSI or S-ECSI, the channel correlation between the main and eavesdropper channels can help to strengthen the transmission security.

C. Notations

We denote a zero-mean circularly symmetric complex Gaussian random variable (RV) X with variance σ^2 by $X \sim \mathcal{CN}(0, \sigma^2)$, and we denote an exponential RV Y with parameter λ by $Y \sim \mathbb{E}(\lambda)$. Also, we denote the probability density function (PDF) of RV X by $f_X(x)$ and the joint PDF of RVs X and Y by $f_{X,Y}(x, y)$. In addition, $I_0(x)$ is the modified Bessel function of the first kind of order zero [31], and $\Pr[X]$ is the probability that event X occurs. We use $[x]^+$ to represent a $\max(0, x)$ operation.

II. System Model

Fig. 1 depicts the system model of DF relaying networks[1] in the presence of direct link, where the direct and relaying branches are activated for the secure data transmission in Fig. 1 (a) and (b), respectively. The relay R assists the secure transmission from the source S to the destination D, and it operates in half-duplex frequency-division mode.[2] In practice,

[1] Although AF relaying is easy to be implemented, it may amplify the received noise when amplifying the desired signal. Differently, DF relaying does not amplify the received noise at the relay, thus achieving a better reliability performance than the AF relaying. Hence, DF relaying is adopted in this paper.

[2] Note that the half-duplex relay can operate in either time-division or frequency-division mode. In the time-division relaying, two different time slots and a single frequency band are used. In the frequency-division relaying, a single time slot and two different frequency bands are used. As the spectral efficiency accounts for both the time and frequency resources, the time-division and frequency-division modes yield the same spectral efficiency.

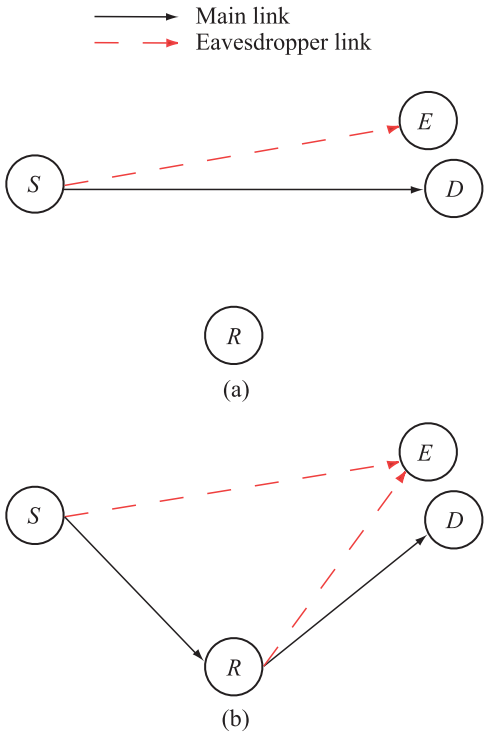


Fig. 1. DSSSC aided DF relaying networks in the presence of direct link. (a) Direct branch. (b) Relaying branch.

this model represents the downlink of a cellular system with one relay, which assists the wireless transmission from the base station to the user. We consider the moderate shadowed environments, so that the direct link from the source S to the destination D exists. The eavesdropper E in the network can overhear the confidential message from the source S and relay R, which yields the secure issue of information wiretap. Due to factors, such as radio scattering environments and antenna deployments, the eavesdropper channel is correlated with the main channel. To ensure secure communication, the system needs to choose either direct branch or relaying branch to assist the data transmission, as shown in Fig. 1 (a) and (b), respectively. Although the opportunistic selection can guarantee the secrecy performance, it requires to continuously know the channel parameters of both branches, and results in a high branch switching rate. To overcome these limitations, we propose to use the DSSSC protocol, where the same branch continues to be used for the secure data transmission as long as it can support the secure transmission. The branch switching occurs only when the branch cannot support the secure transmission any longer. Although the conventional maximal ratio combining (MRC) receiver [32] can exploit the signals of both branches to achieve the optimal transmission performance of main links, it has the following several limitations in practice, compared with the SSC-based protocol. Firstly, MRC requires to continuously estimate the channel parameters of both branches, while SSC-based protocol only needs to estimate the channel parameters of a single branch when the branch switching does not occur. Secondly, the receiver structure of MRC is more complicated than that of SSC-based protocol, since MRC needs to combine the signals from both branches. Thirdly, the spectral efficiency of MRC is smaller than that of the distributed SSC-based protocol, since the distributed SSC can accomplish the data transmission within one phase when the direct branch is activated. Overall, compared with MRC receiver, the SSC-based protocol can achieve a fine balance among the transmission performance, implementation complexity and spectral efficiency. Hence, we adopt the distributed secure switch-and-stay combining protocol in this paper.

In order to describe the DSSSC protocol, we first present the secure data transmission process in the following. Suppose that the direct branch is activated for the data transmission as depicted in Fig. 1 (a). Then S transmits the normalized signal x_S to D with transmit power P through the direct link. The destination D and eavesdropper E respectively receive

$$y_D = \sqrt{P} h_{S,D} x_S + n_D, \tag{1}$$

$$y_E = \sqrt{P} h_{S,E} x_S + n_E, \tag{2}$$

where $h_{S,D} \sim \mathcal{CN}(0, \varepsilon_1)$ and $h_{S,E} \sim \mathcal{CN}(0, \varepsilon_2)$ are the channel coefficients of the S–D and S–E links, respectively. In addition, the notations $n_D \sim \mathcal{CN}(0, \sigma^2)$ and $n_E \sim \mathcal{CN}(0, \sigma^2)$ are the additive white Gaussian noise (AWGN) at D and E, respectively.

Let $w_1 = |h_{S,D}|^2$ and $w_2 = |h_{S,E}|^2$ denote the instantaneous channel gains of the direct S–D and S–E links, respectively. The secrecy outage event happens when the secrecy data rate falls below a given target secrecy data rate R_S,

$$\log_2\left(1 + \frac{P}{\sigma^2} w_1\right) - \log_2\left(1 + \frac{P}{\sigma^2} w_2\right) \leq R_S, \tag{3}$$

which is equivalent to

$$\frac{1 + \bar{P} w_1}{1 + \bar{P} w_2} \leq \gamma_{th}, \tag{4}$$

where $\gamma_{th} = 2^{R_S}$ is the secrecy signal-to-noise ratio (SNR) threshold, and $\bar{P} = \frac{P}{\sigma^2}$ denotes the transmit SNR. In this work, we consider the practical communication scenarios where the effects of radio scattering environments and antenna deployments are taken into account, so that the channel coefficients of the S–D and S–E links are correlated with power correlation coefficient $\rho_1 \in [0, 1]$. The correlation is characterized by the joint PDF of RVs w_1 and w_2, $f_{w_1,w_2}(w_1, w_2)$, given by [28]

$$f_{w_1,w_2}(w_1, w_2) = \frac{I_0\left(\frac{2}{1-\rho_1}\sqrt{\frac{\rho_1 w_1 w_2}{\varepsilon_1 \varepsilon_2}}\right)}{(1-\rho_1)\varepsilon_1 \varepsilon_2} e^{-\frac{\frac{w_1}{\varepsilon_1} + \frac{w_2}{\varepsilon_2}}{1-\rho_1}}. \tag{5}$$

By using the infinite binomial expansion of $I_0(x) = 1 + \sum_{n=1}^{\infty} \frac{x^{2n}}{(\Gamma(n+1))^2}$ [31], we can rewrite $f_{w_1,w_2}(w_1, w_2)$ as

$$f_{w_1,w_2}(w_1, w_2) \approx \sum_{q_1=0}^{N_1} c_{0,q_1} w_1^{q_1} w_2^{q_2} e^{-c_1 w_1} e^{c_2 w_2}, \tag{6}$$

where N_1 is the number of first truncated term and

$$c_{0,q_1} = \frac{\rho_1^{q_1}}{(1-\rho_1)^{2q_1+1} (\varepsilon_1 \varepsilon_2)^{q_1+1} (q_1!)^2}, \tag{7}$$

$$c_1 = \frac{1}{(1-\rho_1)\varepsilon_1}, \quad c_2 = \frac{1}{(1-\rho_1)\varepsilon_2}. \tag{8}$$

As given in [28] and [29], the truncation error in (6) decays exponentially with N_1, and with a sufficient number of terms, the approximate expression fits the exact expression very well. Thus, we ignore the truncation error and use the approximate expression of $f_{w_1,w_2}(w_1, w_2)$ in (6) for the subsequent derivation.

When the relaying branch is activated for the secure transmission as shown in Fig. 1 (b), S sends the normalized signal x_S through the help of the fixed DF relay R within two phases. Let $h_{S,R} \sim \mathcal{CN}(0, \alpha)$, $h_{R,D} \sim \mathcal{CN}(0, \beta_1)$ and $h_{R,E} \sim \mathcal{CN}(0, \beta_2)$ denote the channel parameters of the S–R, R–D and R–E links, respectively. We further use $u = |h_{S,R}|^2$, $v_1 = |h_{R,D}|^2$ and $v_2 = |h_{R,E}|^2$ to represent the associated channel gains. For the fixed DF relaying, the received end-to-end SNRs at the D and E are given by [22]

$$\mathrm{SNR}_D = \bar{P} \min(u, v_1), \tag{9}$$

$$\mathrm{SNR}_E = \bar{P}(w_2 + v_2), \tag{10}$$

where the transmit power at the relay is P and the variance of the AWGN at the relay is σ^2. Note that the destination D can also receive the direct signal through the S–D link, when the relaying branch is activated for secure data transmission. However, we do not use MRC receiver at D to exploit the direct signal, since MRC has several limitations such as channel estimation complexity, receiver structure and spectral efficiency, which has been explained in the first paragraph of Sec. II. Compared with the MRC receiver, the DSSSC protocol can achieve a fine balance among the transmission performance, implementation complexity and spectral efficiency. Hence, in (9), the direct link is not used for the legitimate communication, and only the relaying links are used. In contrast, in (10), both the relaying and direct links are used for the eavesdropping, and the MRC receiver is employed at the E. This is because that we consider the worst-case eavesdropping scenarios, i.e., the eavesdropper has the best capability to overhear the secure message, no matter the implementation complexity. Moreover, this worst-case can be viewed as an important benchmark for the other eavesdropping scenarios.

From (9) and (10), the secrecy outage event with activated relaying branch occurs when the following equation holds,

$$\frac{1}{2}\log_2[1+\bar{P}\min(u, v_1)] - \frac{1}{2}\log_2[1+\bar{P}(v_2 + w_2)] < \frac{1}{2}R_s, \tag{11}$$

which is equivalent to

$$\frac{1 + \bar{P}\min(u, v_1)}{1 + \bar{P}(v_2 + w_2)} < \gamma_{th}. \tag{12}$$

Note that the factor $\frac{1}{2}$ on the left-hand side (LHS) of (11) comes from the two-phase transmission. The factor $\frac{1}{2}$ on the right-hand side (RHS) of (11) is due to both the two-phase transmission and the fixed data rate at the nodes in the network. The data rate is fixed because that in some practical communication scenarios such as wireless sensing networks, the wireless nodes may not have complicated functions such as adaptive modulation, i.e., they may be equipped with a single modulation scheme. This is particularly applicable when the wireless nodes are of low price. Also, we consider the practical communication scenarios in which the impacts of radio scattering environments and antenna deployment are considered, and thus the channel gains of R–D and R–E links are correlated. The correlation is characterized by the joint PDF of RVs v_1 and v_2, $f_{v_1,v_2}(v_1, v_2)$, which can be presented in the following forms [28],

$$\begin{aligned} f_{v_1,v_2}(v_1, v_2) &= \frac{I_0\left(\frac{2}{1-\rho_2}\sqrt{\frac{\rho_2 v_1 v_2}{\beta_1\beta_2}}\right)}{(1-\rho_2)\beta_1\beta_2} e^{-\frac{\frac{v_1}{\beta_1}+\frac{v_2}{\beta_2}}{1-\rho_2}} \\ &\approx \sum_{q_2=0}^{N_2} b_{0,q_2} v_1^{q_2} v_2^{q_2} e^{-b_1 v_1} e^{-b_2 v_2}, \end{aligned} \tag{13}$$

where $\rho_2 \in [0, 1]$ is the power correlation coefficient regarding R–D and R–E links, N_2 is the number of first truncated terms, and

$$b_{0,q_2} = \frac{\rho_2^{q_2}}{(1-\rho_2)^{2q_2+1}(\beta_1\beta_2)^{q_2+1}(q_2!)^2}, \tag{14}$$

$$b_1 = \frac{1}{(1-\rho_2)\beta_1}, \quad b_2 = \frac{1}{(1-\rho_2)\beta_2}. \tag{15}$$

Also, the truncation error in (13) decreases with N_2 in an exponential manner. Thus the truncation error can be ignored with a large number of N_2 [29], and we utilize the approximate expression of $f_{v_1,v_2}(v_1, v_2)$ in (13) for the subsequent derivations.

Here, we highlight that the channel correlation exists between the main and eavesdropping channels of direct links, or between the main and eavesdropping channels of relaying links. Since the frequency-division half-duplex relaying is adopted in this paper, i.e., the source and relay use orthogonal frequency bands to transmit signals, there is no channel correlation over the dual-hop relaying channels. In a word, we only consider the channel correlation between $h_{S,D}$ and $h_{S,E}$, or between $h_{R,D}$ and $h_{R,E}$.

III. Description of the DSSSC Protocol

Before the secure data transmission, the system needs to activate one branch between the direct and relaying branches to assist the data transmission for the current time slot. Suppose that the direct (or relay) branch was used in the previous time slot. Then at the beginning of the current time slot, the destination D estimates the channel parameters of the main links associated with the direct (or relay) branch, through some pilot signals from the source and relay [33]. Similarly, the eavesdropper E can estimate its channel parameters with the help of pilot signals from the source and relay. Then the system can gather the instantaneous channel state information of eavesdropper links if the eavesdropper is active, i.e., another active user in the networks. When the eavesdropper is passive, the system can still acquire the statistics CSI of the eavesdropper links by some ways, such as estimating the eavesdropper's location in the network [23], [34], [35]. Note that the secure transmission with the instantaneous or statistical CSI of eavesdropper links in this paper can be viewed as two

important benchmarks for the secure communications with a general CSI knowledge of the eavesdropper links.

After obtaining the CSI of the main and eavesdropper links, DSSSC will continue to use the direct branch for the secure data transmission in the current time slot, as long as the branch can support the secure transmission as

$$\frac{1+\bar{P}w_1}{1\bar{P}w_2} \geq T, \tag{16}$$

or

$$\frac{1+\bar{P}w_1}{1+\bar{P}E\{w_2\}} \geq T, \tag{17}$$

where $E\{\ \}$ means statistical expectation, and T is a given secure switching threshold, in which (16) and (17) employ the instantaneous eavesdropping CSI and statistics of eavesdropping CSI to assist the DSSSC protocol, respectively. When (16) and (17) cannot hold, secure branch switching occurs and the relaying branch is activated for the current data transmission. Similarly, when the relaying branch was used in the previous time slot, the switching check in (16) and (17) becomes

$$\frac{1+\bar{P}v_1}{1+\bar{P}(v_2+w_2)} \geq T, \tag{18}$$

or

$$\frac{1+\bar{P}w_1}{1+\bar{P}E\{v_2+w_2\}} \geq T. \tag{19}$$

If (18) or (19) holds, the relaying branch continues to be used for the current data transmission. Otherwise, the secure branch switching occurs and the direct branch is activated for the current data transmission.

IV. Performance Analysis

In this section, we evaluate the secure performance of DSSSC protocol, and quantify the impact of correlated fading channels. For DSSSC with I-ECSI and S-ECSI, we first give the analytical expression of SOP, and then provide the asymptotic SOP expression in the high regime of MER.

A. Analytical SOP With I-ECSI

According to the DSSC protocol with I-ECSI, we write the secrecy outage probability as [3]

$$\begin{aligned} P_{out} &= \underbrace{\Pr\left[\frac{1+\bar{P}\min(u,v_1)}{1+\bar{P}(v_2+w_2)} < \gamma_{th}, \frac{1+\bar{P}\min(u,v_1)}{1+\bar{P}(v_2+w_2)} \geq T\right]}_{J_1} P_R \\ &\quad + \underbrace{\Pr\left[\frac{1+\bar{P}w_1}{1+\bar{P}w_2} < \gamma_{th}, \frac{1+\bar{P}\min(u,v_1)}{1+\bar{P}(v_2+w_2)} < T\right]}_{J_2} P_R \\ &\quad + \underbrace{\Pr\left[\frac{1+\bar{P}w_1}{1+\bar{P}w_2} < \gamma_{th}, \frac{1+\bar{P}w_1}{1+\bar{P}w_2} \geq T\right]}_{J_3} P_D \\ &\quad + \underbrace{\Pr\left[\frac{1+\bar{P}\min(u,v_1)}{1+\bar{P}(v_2+w_2)} < \gamma_{th}, \frac{1+\bar{P}w_1}{1+\bar{P}w_2} \leq T\right]}_{J_4} P_D, \end{aligned} \tag{20}$$

where J_1 and J_3 correspond to the SOP when the relay and direct branches continue to be used for the current data transmission, respectively, while J_2 and J_4 represent the SOP when the relaying branch switches to direct branch, and vice versa, respectively. Notations P_R and P_D are the probabilities that the system utilizes relay and direct branch, respectively, given by

$$P_R = \frac{C_R}{C_R+C_D}, \quad P_D = \frac{C_D}{C_R+C_D}, \tag{21}$$

where

$$C_R = \Pr\left(\frac{1+\bar{P}w_1}{1+\bar{P}w_2} \leq T\right), \tag{22}$$

$$C_D = \Pr\left(\frac{1+\bar{P}\min(u,v_1)}{1+\bar{P}(v_2+w_2)} \leq T\right) \tag{23}$$

are the probabilities that direct branch switches to relaying branch, and vice versa, respectively. By applying the joint PDF of w_1 and w_2 in (6), and then solving the required integral, we can compute C_R as

$$C_R = \varphi_1(T), \tag{24}$$

where

$$\begin{aligned} \varphi_1(T) = 1 - \sum_{q_1=0}^{N_1}\sum_{m_1=0}^{q_1}\sum_{n_1=0}^{m_1} c_{0,m} d_{q_1,m_1n_1}(T)(q_1+m_1)! \\ \times (c_1T+c_2)^{-(q_1+m_1+1)}, \end{aligned} \tag{25}$$

with

$$d_{q_1,m_1n_1}(x) = \frac{q_1!}{m_1!}\binom{m_1}{n_1}\frac{e^{-c_1\frac{x-1}{\bar{P}}}}{c_1^{q_1-m_1+1}}x^{n_1}\left(\frac{x-1}{\bar{P}}\right)^{m_1-n_1}. \tag{26}$$

Then, by applying the PDFs of RV u and w_2, $f_u(u) = \frac{1}{\alpha}e^{-\frac{u}{\alpha}}$ and $f_{w_2} = \frac{1}{\varepsilon_2}e^{-\frac{w_2}{\varepsilon_2}}$, as well as the joint PDF of RVs v_1 and v_2 in (13), C_D can be calculated as

$$C_D = \varphi_2(T), \tag{27}$$

where $\varphi_2(T)$ is defined as

$$\begin{aligned} \varphi_2(T) = 1 - \frac{1}{\varepsilon_2}e^{-\frac{T-1}{\alpha\bar{P}}}\sum_{q_2=0}^{N_2}\sum_{m=0}^{q_2}\sum_{n=0}^{m}\sum_{t=0}^{n}\binom{n}{t}d_{q_2,mn}(T) \\ \times \frac{(n-t)!}{(\frac{1}{\varepsilon_2}+\frac{T}{\alpha}+b_1T)^{n-t+1}}\frac{(q_2+t)!}{(b_2+\frac{T}{\alpha}+b_1T)^{q_2+t+1}}, \end{aligned} \tag{28}$$

with

$$d_{q_2,mn}(x) = \frac{q_2!}{m!}\binom{m}{n}\frac{e^{-b_1\frac{x-1}{\bar{P}}}}{b_1^{q-m+1}}x^n\left(\frac{x-1}{\bar{P}}\right)^{m-n}. \tag{29}$$

[3] For the derivation of the secrecy outage probability, the joint probability density functions (PDFs) of the main and eavesdropper channels are needed. These PDFs require to know not only the channel distribution such as Rayleigh distribution, but also the statistics of the channels such as the average channel gain and the correlation coefficient.

$$J_2 = \varphi_1(\gamma_{th}) + e^{-\frac{T-1}{\bar{P}\alpha}} \sum_{q_1=0}^{N_1} \sum_{q_2=0}^{N_2} \sum_{m=0}^{q} \sum_{n=0}^{m} \sum_{t=0}^{m-n} \frac{\hat{d}_{q_2,mnt}(\gamma_{th}, T) b_{0,q_2}(n+q_2)!}{[(b_1+\alpha^{-1})T + b_2]^{n+q_2+1}} \frac{c_{0,q_1} q_1! c_1^{-q_1-1}(t+q_1!)}{[c_2 + (b_1+\alpha^{-1})\gamma_{th}]^{t+q_1+1}}$$
$$- e^{-\frac{T-1}{\bar{P}\alpha}} \sum_{q_1=0}^{N_1} \sum_{m_1=0}^{q_1} \sum_{n_1=0}^{m_1} \sum_{q_2=0}^{N_2} \sum_{m=0}^{q_2} \sum_{n=0}^{m} \sum_{t=0}^{m-n} \frac{c_{0,q_1} d_{q_1,m_1 n_1}(\gamma_{th})(n+q_2)!}{[(b_1+\alpha^{-1})T + b_2]^{n+q_2+1}} \frac{b_{0,q_2} \hat{d}_{q_2,mnt}(T,T)(t+q_1+n_1)!}{[(b_1+\alpha^{-1})T + c_2 + c_1\gamma_{th}]^{t+q_1+n_1+1}}. \quad (32)$$

Accordingly, J_1 and J_3 can be computed as

$$J_1 = \begin{cases} \varphi_2(\gamma_{th}) - \varphi_2(T), & \text{If } T < \gamma_{th} \\ 0, & \text{If } T \geq \gamma_{th}, \end{cases} \quad (30)$$

$$J_3 = \begin{cases} \varphi_1(\gamma_{th}) - \varphi_1(T), & \text{If } T < \gamma_{th} \\ 0, & \text{If } T \geq \gamma_{th}. \end{cases} \quad (31)$$

From (30) and (31), we can see that when $T \geq \gamma_{th}$, J_1 and J_3 become zero, since a large switching threshold results in the effective secure branch switching. Moreover, by applying the PDF $f_u(u)$ for RV u, and the joint PDFs $f_{w_1,w_2}(w_1, w_2)$ for RVs w_1 and w_2, as well as $f_{v_1,v_2}(v_1, v_2)$ for RVs v_1 and v_2 from (6) and (13), J_2 can be computed as shown in (32) at the top of this page, where

$$\hat{d}_{q_2,mnt}(x,y) = \frac{q_2!}{m!}\binom{m}{n}\binom{m-n}{t} \frac{e^{-b_1\frac{x-1}{\bar{P}}}}{b_1^{q_2-m+1}} x^n y^t \times \left(\frac{x-1}{\bar{P}}\right)^{m-n-t}. \quad (33)$$

Then exchanging T with γ_{th}, we obtain the exact analytical expression of J_4. By summarizing the results in (30)-(32), we achieve the analytical expression of SOP for DSSSC with I-ECSI as $P_{out} = P_R(J_1 + J_2) + P_D(J_3 + J_4)$. In particular, when the secure branch switching threshold is large with $T \geq \gamma_{th}$, the analytical P_{out} becomes $P_R J_2 + P_D J_4$, which relies on the SOP only when the secure branch switching occurs. Moreover, the analytical result for SOP is composed of elementary functions only, and hence it is easy to be evaluated.

B. Analytical SOP With S-ECSI

According to the DSSSC protocol with S-ECSI, we can write the secrecy outage probability as

$$\begin{aligned} P_{out} &= \underbrace{\Pr\left[\frac{1+\bar{P}\min(u,v_1)}{1+\bar{P}(v_2+w_2)} < \gamma_{th}, \frac{1+\bar{P}\min(u,v_1)}{1+\bar{P}(E\{v_2+w_2\})} \geq T\right]}_{\tilde{J}_1} \tilde{P}_R \\ &+ \underbrace{\Pr\left[\frac{1+\bar{P}w_1}{1+\bar{P}w_2} < \gamma_{th}, \frac{1+\bar{P}\min(u,v_1)}{1+\bar{P}(E\{v_2+w_2\})} < T\right]}_{\tilde{J}_2} \tilde{P}_R \\ &+ \underbrace{\Pr\left[\frac{1+\bar{P}w_1}{1+\bar{P}w_2} < \gamma_{th}, \frac{1+\bar{P}w_1}{1+\bar{P}E\{w_2\}} \geq T\right]}_{\tilde{J}_3} \tilde{P}_D \\ &+ \underbrace{\Pr\left[\frac{1+\bar{P}\min(u,v_1)}{1+\bar{P}(v_2+w_2)} < \gamma_{th}, \frac{1+\bar{P}w_1}{1+\bar{P}E\{w_2\}} \leq T\right]}_{\tilde{J}_4} \tilde{P}_D. \end{aligned} \quad (34)$$

Here, $\tilde{J}_1$ and $\tilde{J}_3$ are the SOP when relay and direct branches continue to be employed for secure data transmission, while $\tilde{J}_2$ and $\tilde{J}_4$ represent the SOP when the secure transmission switches from the relaying branch to the direct branch, and that from the direct branch to the relaying branch, respectively. Also, $\tilde{P}_R$ and $\tilde{P}_D$ correspond to the probabilities that direct and relaying branches are employed, respectively, which can be written as

$$\tilde{P}_R = \frac{\tilde{C}_R}{\tilde{C}_R + \tilde{C}_D}, \quad \tilde{P}_D = \frac{\tilde{C}_D}{\tilde{C}_R + \tilde{C}_D}. \quad (35)$$

where

$$\tilde{C}_R = \Pr\left[\frac{1+\bar{P}w_1}{1+\bar{P}E\{w_2\}} \leq T\right], \quad (36)$$

$$\tilde{C}_D = \Pr\left[\frac{1+\bar{P}\min(u,v_1)}{1+\bar{P}(E\{v_2\}+E\{w_2\})} \leq T\right], \quad (37)$$

represent the probabilities that direct branch switches to relaying branch and relaying branch switches to direct branch, respectively.

By using the PDFs of RVs u, v_1 and w_1, and then solving the required integral, we have

$$\tilde{C}_R = 1 - e^{-\frac{T(1+\bar{P}\varepsilon_2)-1}{\bar{P}\varepsilon_1}}, \quad (38)$$

$$\tilde{C}_D = 1 - e^{-\left(\frac{T[1+\bar{P}(\beta_2+\varepsilon_2)]-1}{\bar{P}\alpha} + \frac{T[1+\bar{P}(\beta_2+\varepsilon_2)]-1}{\bar{P}\beta_1}\right)}. \quad (39)$$

From (38) and (39), we observe that the channel correlation between the main and eavesdropper channels does not affect the value of $\tilde{C}_R$ and $\tilde{C}_D$, indicating that the secure branch switching with S-ECSI is not effective as that with I-ECSI. Then, by applying the joint PDF of RV v_1 and v_2, $f_{v_1,v_2}(v_1, v_2)$ from (13), as well as the PDFs of RV u and w_2, $f_u(u)$ and $f_{w_2}(w_2)$, we can compute $\tilde{J}_1$ as shown in (40), at the top of the next page, where $\Xi_{n,q_2}(b_2)$ and Φ are given in (41) and (42), at the top of the next page, and

$$\tilde{\theta}_{q_2,mt}(x) = \frac{(x)^{m-q_2-1} q_2!}{m!}\binom{m}{t}\left(\frac{1}{\gamma_{th}\bar{P}} + \frac{1}{\bar{P}}\right)^{m-t} \gamma_{th}^{-t}, \quad (43)$$

$$\theta_{q_2,mn}(x) = \frac{q_2!}{m!}\binom{m}{n}(x)^{m-q_2-1}\left(\frac{1}{\gamma_{th}\bar{P}} - \frac{1}{\bar{P}}\right)^{m-n} \gamma_{th}^{-n}. \quad (44)$$

Similarly, we can calculate $\tilde{J}_2$ as

$$\tilde{J}_2 = \varphi_1(\gamma_{th})\tilde{C}_R. \quad (45)$$

The analytical expressions of $\tilde{J}_3$ and $\tilde{J}_4$ are given by (46) and (47) at the top of the next page, where $\Gamma(x, y)$ is the upper incomplete gamma function [31, eq. (8.350.2)]. Note that different from the results of J_1 and J_3 in (30) and (31), $\tilde{J}_1$ and $\tilde{J}_3$ are not equal to zero even with a large value of T,

$$\tilde{J}_1 = \sum_{q_2=0}^{N_2}\sum_{n=0}^{q_2}(b_2-\varepsilon_2^{-1})^{-q_2-1}b_1^{n-q_2-1}\frac{(q_2!)^2}{n!}\alpha^{-1}\Xi_{n,0}\left(\frac{1}{\varepsilon_2}\right) - \sum_{q_2=0}^{N_2}\sum_{m=0}^{q_2}\sum_{n=0}^{q_2}\sum_{t=0}^{m} e^{-\frac{b_2(1-\alpha)}{\gamma_{th}\bar{P}\alpha}+\frac{b_2(1-\alpha)}{\bar{P}\alpha}}\alpha^{-1}b_1^{n-q_2-1}\frac{q_2!}{n!}$$
$$\times\tilde{\theta}_{q_2,mt}(b_2-\varepsilon_2^{-1})\Xi_{t,n}(b_2) + \sum_{q_2=0}^{N_2}\sum_{m=0}^{q_2}\sum_{n=0}^{q_2}\sum_{t=0}^{n} q_2!b_1^{-q_2-1}\alpha^{-1}\frac{b_1^m}{m!}\theta_{q_2,mn}(b_2)\Xi_{t,m}(b_2) + \sum_{q_2=0}^{N_2} q_2!(b_2-\varepsilon_2^{-1})^{-q_2-1}$$
$$\times\Xi_{0,q_2}\left(\frac{1}{\varepsilon_2}\right) - \sum_{q_2=0}^{N_2}\sum_{m=0}^{q_2}\sum_{n=0}^{m}\theta_{m,n,(b_2-\varepsilon_2^{-1})}\Xi_{n,q_2}(b_2) + \sum_{q_2=0}^{N_2}\sum_{m=0}^{q_2}\sum_{n=0}^{m}\theta_{m,n,b_2}\Xi_{n,q_2}(b_2) + \Phi. \tag{40}$$

$$\Xi_{n,q_2}(b_2) = \begin{cases} b_{0,q_2}e^{-\frac{b_2}{\gamma_{th}\bar{P}}+\frac{b_2}{\bar{P}}}\left(\frac{b_2}{\gamma_{th}}+b_1+\alpha^{-1}\right)^{-n-q_2-1}\Gamma\left[n+q_2+1,\frac{\gamma_{th}-1}{\bar{P}}\left(\frac{b_2}{\gamma_{th}}+b_1+\alpha^{-1}\right)\right], \\ \qquad\qquad \text{If } T<\dfrac{\gamma_{th}}{1+\bar{P}(\beta_2+\varepsilon_2)} \\ b_{0,q_2}e^{-\frac{b_2}{\gamma_{th}\bar{P}}+\frac{b_2}{\bar{P}}}\left(\frac{b_2}{\gamma_{th}}+b_1+\alpha^{-1}\right)^{-n-q_2-1}\Gamma\left[n+q_2+1,\frac{T\left[1+\bar{P}(\beta_2+\varepsilon_2)\right]-1}{\bar{P}}\left(\frac{b_2}{\gamma_{th}}+b_1+\alpha^{-1}\right)\right], \quad \text{Else.} \end{cases} \tag{41}$$

$$\Phi = \begin{cases} e^{-\frac{T\left[1+\bar{P}(\varepsilon_2+\beta_2)\right]-1}{\alpha\bar{P}}-\frac{T\left[1+\bar{P}(\varepsilon_2+\beta_2)\right]-1}{\beta_1\bar{P}}} - e^{-\frac{\gamma_{th}-1}{\alpha\bar{P}}-\frac{\gamma_{th}-1}{\beta_1\bar{P}}}, & \text{If } T<\dfrac{\gamma_{th}}{1+\bar{P}(\beta_2+\varepsilon_2)} \\ 0 & \text{Else.} \end{cases} \tag{42}$$

$$\tilde{J}_3 = \sum_{q_1=0}^{N_1} c_{0,q_1}\left[(c_1c_2)^{-q_1-1}\Gamma\left(q_1+1,c_1\frac{T(1+\bar{P}\varepsilon_2)-1}{\bar{P}}\right)\Gamma\left[q_1+1,\left(\frac{T(1+\bar{P}\varepsilon_2)}{\gamma_{th}\bar{P}}-\frac{1}{\bar{P}}\right)c_2\right]\right.$$
$$\left. - \sum_{m=0}^{q_1}\sum_{n=0}^{m} d_{q_1,m_1n_1}(T)\frac{\Gamma\left[n+q_1+1,\left(\frac{T(1+P\varepsilon_2)}{\gamma_{th}\bar{P}}-\frac{1}{\bar{P}}\right)(c_2+c_1\gamma_{th})\right]}{(c_2+c_1\gamma_{th})^{n+q_1+1}}\right]. \tag{46}$$

$$\tilde{J}_4 = \sum_{q_1=0}^{N_1} c_{0,q_1}c_1^{-q_1-1}\left[q_1!-\Gamma\left(q_1+1,c_1\frac{T(1+P\varepsilon_2)-1}{\bar{P}}\right)\right]\left[q_1!c_2^{-q_1-1}-q_1!\frac{e^{-\frac{\gamma_{th}-1}{\bar{P}\alpha}}\beta_2^{-1}}{\frac{\gamma_{th}}{\alpha}+\frac{1}{\beta_2}}(c_2+\frac{\gamma_{th}}{\alpha})^{-q_1-1}+\sum_{q=0}^{N_2}b_{0,q_2}b_1^{-q_2-1}\right.$$
$$\left.\times\frac{e^{-\frac{\gamma_{th}-1}{\bar{P}\alpha}}(q_2!)^2q_1!}{(b_2+\frac{\gamma_{th}}{\alpha})^{q_2+1}}(c_2+\frac{\gamma_{th}}{\alpha})^{-q_1-1} - \sum_{q=0}^{N_2}\sum_{m=0}^{q}\sum_{n=0}^{m}\sum_{t=0}^{m-n} b_{0,q_2}\frac{\hat{d}_{q_2,mnt}(\gamma_{th},\gamma_{th})(n+q_2)!}{(b_2+\frac{\gamma_{th}}{\alpha}+b_1\gamma_{th})^{n+q_2+1}}\frac{e^{-\frac{\gamma_{th}-1}{\bar{P}\alpha}}(q_1+t)!}{(c_2+\frac{\gamma_{th}}{\alpha}+b_1\gamma_{th})^{q_1+t+1}}\right]. \tag{47}$$

indicating that the secure branch switching cannot be efficiently exploited with the assistance of S-ECSI. Summarizing the results in (40)-(47), we achieve the analytical expression of SOP for DSSSC with S-ECSI as $P_{out} = \tilde{P}_R(\tilde{J}_1+\tilde{J}_2)+\tilde{P}_D(\tilde{J}_3+\tilde{J}_4)$, which is easy to be computed, since all the expressions involved comprise elementary functions and gamma function only.

C. Asymptotic SOP With I-ECSI

In this section, we turn to analyze the asymptotic expression of SOP with I-ECSI, in the high regime of SNR and MER. We first rewrite the expression of w_2, according to the work in [36], which defines the correlated complex RVs as

$$w_2 = \frac{\rho_1 w_1+(1-\rho_1)n_1+2\sqrt{\rho_1(1-\rho_1)}(w_{11}n_{11}+w_{12}n_{12})}{\lambda_1}, \tag{48}$$

in which w_{11}, w_{12}, n_{11} and n_{12} are independent complex Gaussian distributed RVs with mean 0 and variance $\frac{\varepsilon_1}{2}$, and n_1 is subject to the exponential distribution with mean ε_1. Let $\lambda_1 = \frac{\varepsilon_1}{\varepsilon_2}$ and $\lambda_2 = \frac{\beta_1}{\beta_2}$ denote the MER of the direct and relaying branches, respectively. We present the asymptotic expression w_2 in the following proposition,

Proposition 1: When λ_1 is large and $w_1 \le \phi w_2$ holds with $\phi \ll \lambda_1$, w_2 can be efficiently approximated by $\frac{(1-\rho_1)n_1}{\lambda_1}$.

Proof: See Appendix A. ∎

From Proposition 1 and the approximation of $e^{-x} \simeq 1-x$ for small value of $|x|$, we can write the asymptotic C_R with high SNR and MER as

$$C_R \simeq \Pr\left(w_1 \le \frac{T(1-\rho_1)n_1}{\lambda_1}\right) \tag{49}$$
$$\simeq \widetilde{\varphi}_1(T), \tag{50}$$

where $\widetilde{\varphi}_1(T)$ is defined as

$$\widetilde{\varphi}_1(T) = \frac{(1-\rho_1)T}{\lambda_1}. \tag{51}$$

We next derive the asymptotic expression of C_D with high SNR and MER. We first rewrite C_D as

$$C_D = \Pr\left[u \le \gamma_{th}(v_2+w_2)\right] + \underbrace{\Pr\left[v_1 \le \gamma_{th}(v_2+w_2) \le u\right]}_{L_1}. \tag{52}$$

$$P_{out} \simeq \begin{cases} \dfrac{\widetilde{\varphi}_1(T)\left[\widetilde{\varphi}_2(\gamma_{th}) - \widetilde{\varphi}_2(T) + \widetilde{\varphi}_1(T)\widetilde{\varphi}_3(\gamma_{th})\right] + \widetilde{\varphi}_2(T)\left[\widetilde{\varphi}_1(\gamma_{th}) - \widetilde{\varphi}_1(T) + \widetilde{\varphi}_1(\gamma_{th})\widetilde{\varphi}_3(T)\right]}{\widetilde{\varphi}_1(T) + \widetilde{\varphi}_2(T)}, & \text{If } T < \gamma_{th} \\ \widetilde{\varphi}_1(T)\left[\dfrac{\widetilde{\varphi}_1(\gamma_{th})\widetilde{\varphi}_3(T)}{\widetilde{\varphi}_1(T) + \widetilde{\varphi}_2(T)} + \dfrac{\widetilde{\varphi}_2(T)\widetilde{\varphi}_3(\gamma_{th})}{\widetilde{\varphi}_1(T) + \widetilde{\varphi}_2(T)}\right], & \text{If } T \geq \gamma_{th}. \end{cases} \tag{60}$$

From Proposition 1, L_1 can be approximated by

$$L_1 \simeq \Pr\left[v_1 \leq \gamma_{th}\left(\tfrac{(1-\rho_2)n_2}{\lambda_2} + w_2\right) < u\right], \tag{53}$$

where $n_2 \sim \mathbb{E}(\beta_1)$ is an exponential RV independent of v_1. From (53) and by applying the approximation of $(1+x)^{-1} \simeq 1 - x$ for small value of $|x|$, we further write the asymptotic C_D as

$$C_D \simeq \widetilde{\varphi}_2(T), \tag{54}$$

where $\widetilde{\varphi}_2(T)$ is defined as

$$\widetilde{\varphi}_2(T) = \frac{T}{\lambda_1}\left[\frac{\varepsilon_1}{\alpha}\left(1+\frac{\beta_2}{\varepsilon_2}\right)+\frac{\varepsilon_1}{\beta_1}\left(1+\frac{\beta_2(1-\rho_2)}{\varepsilon_2}\right)\right]. \tag{55}$$

From the asymptotic C_R and C_D in (50) and (54), we can find that when the channel correlation between the main and eavesdropper channels of the direct (or relaying) links increases, the direct (or relaying) branch tends to be used more often for data transmission. Moreover, when the main and eavesdropper channels of direct links are completely correlated with $\rho_1 = 1$, C_R reaches zero and the relaying branch is rarely used by the system. Accordingly, we can obtain the asymptotic expressions of J_1 and J_3 as

$$J_1 = \begin{cases} \widetilde{\varphi}_2(\gamma_{th}) - \widetilde{\varphi}_2(T), & \text{If } T < \gamma_{th} \\ 0, & \text{If } T \geq \gamma_{th}, \end{cases} \tag{56}$$

$$J_3 = \begin{cases} \widetilde{\varphi}_1(\gamma_{th}) - \widetilde{\varphi}_1(T), & \text{If } T < \gamma_{th} \\ 0, & \text{If } T \geq \gamma_{th}. \end{cases} \tag{57}$$

Similar to the approaches in (50)-(54), we obtain the asymptotic expression of J_2 with high SNR and MER as

$$J_2 \simeq \widetilde{\varphi}_1(\gamma_{th})\widetilde{\varphi}_3(T), \tag{58}$$

where $\widetilde{\varphi}_3(T)$ is given by

$$\widetilde{\varphi}_3(T) = \frac{T}{\lambda_1}\Big[\frac{\varepsilon_1}{\alpha}\Big(2(1-\rho_1)+\frac{\beta_2}{\varepsilon_2}\Big)+\frac{\varepsilon_1}{\beta_1}\Big(2(1-\rho_1) + \frac{\beta_2(1-\rho_2)}{\varepsilon_2}\Big)\Big]. \tag{59}$$

Then, by exchanging γ_{th} and T in (58), the asymptotic expression of J_4 can be obtained. From (57)-(58), we see that when $\rho_1 = 1$, J_2, J_3 and J_4 are equal to zero, indicating that when the main and eavesdropper channels of direct links are completely correlated, the direct branch can provide a perfect secure transmission. Combining these asymptotic results, we achieve the asymptotic expression of SOP for DSSSC with I-ECSI, as shown in (60) at the top of this page.

From the asymptotic expression of P_{out}, some key insights about the impact of channel correlation and secure switching threshold on the network secrecy performance are given as follows,

Remark 1: When $T \geq \gamma_{th}$, since

$$\widetilde{\varphi}_1(\gamma_{th})\widetilde{\varphi}_3(\gamma_{th}) \leq P_{out} \leq \widetilde{\varphi}_1(T)\widetilde{\varphi}_3(T), \tag{61}$$

holds, we can obtain from the squeeze theorem [32] that the system diversity order is equal to two, indicating that both direct and relaying branches can be efficiently exploited for the secure data transmission thanks to a large value of secure switching threshold. However, when the secure switching threshold T becomes smaller with $T < \gamma_{th}$, the system diversity order degrades into the range of [1, 2], since a small T cannot efficiently utilize the secure branch switching.

Remark 2: The optimal secure switching threshold T^* which minimizes the SOP is equal to γ_{th}, and the associated minimum P_{out} is given by

$$P_{out}^{min} \simeq \widetilde{\varphi}_1(\gamma_{th})\widetilde{\varphi}_3(\gamma_{th}). \tag{62}$$

Remark 3: As Proposition 1 suggested, the correlation between the main and eavesdropper channels is helpful for the transmission security in the high SNR and MER region. This phenomenon is consistent to the results in [29], [30], and [37].

Remark 4: When the main and eavesdropper channels of the direct links are completely correlated with $\rho_1 = 1$, the secrecy data transmission relies on the direct link only, resulting in a perfect secure transmission. On the contrary, when the relay links between the main and eavesdropper channels are completely correlated with $\rho_2 = 1$, the secrecy outage event still occurs as the eavesdropper can still exploit the direct link due to the usage of MRC receiver.

D. Asymptotic SOP With S-ECSI

In the high SNR and MER region, based on Proposition 1 and the approximation $e^{-x} \simeq 1-x$ which holds well for small value of $|x|$, we can achieve

$$\tilde{C}_R \simeq \frac{T}{\lambda_1}, \tag{63}$$

$$\tilde{C}_D \simeq \frac{T}{\lambda_1}\left[\frac{\varepsilon_1}{\alpha}\left(1+\frac{\beta_2}{\varepsilon_2}\right)+\frac{\varepsilon_1}{\beta_1}\left(1+\frac{\beta_2}{\varepsilon_2}\right)\right]. \tag{64}$$

Note that different from the asymptotic value of C_R and C_D in (50) and (54), the asymptotic value of $\tilde{C}_R$ and $\tilde{C}_D$ is not affected by the channel correlation between the main and eavesdropper links. Similar to the approaches in deriving the asymptotic expressions of $\tilde{C}_R$ and $\tilde{C}_D$, the asymptotic $\tilde{J}_1$, $\tilde{J}_2$, $\tilde{J}_3$ and $\tilde{J}_4$ can be accordingly derived as follows,

$$\begin{aligned}\tilde{J}_1 \simeq \frac{\gamma_{th}}{\lambda_1}\Big[&e^{-\frac{T(\beta_1+\varepsilon_2)}{\gamma_{th}\varepsilon_2}}\Big(\frac{\beta_1}{\alpha}+\frac{\varepsilon_2}{\beta_2}\frac{\beta_1}{\alpha}-\frac{\varepsilon_2}{\varepsilon_2-\beta_2}\frac{\beta_1}{\alpha} \\ &+\frac{\varepsilon_2}{\varepsilon_2-\beta_2(1-\rho_2)}\frac{\varepsilon_2}{\beta_2}\Big)+e^{-\frac{T(\beta_2+\varepsilon_2)}{\gamma_{th}\beta_2}}\frac{\beta_2}{\beta_2-\varepsilon_2}\frac{\beta_1}{\alpha} \\ &+e^{-\frac{Tb_2(\beta_2+\varepsilon_2)}{\gamma_{th}}}\Big(\frac{\beta_1(1-\rho_2)}{\alpha}-\frac{\varepsilon_2(1-\rho_2)}{\varepsilon_2-\beta_2(1-\rho_2)}\Big)\Big],\end{aligned} \tag{65}$$

$$\tilde{J}_2 \simeq \frac{T\gamma_{th}(1-\rho_1)}{\lambda_1^2}\left[\frac{\varepsilon_1}{\alpha}\left(1+\frac{\beta_2}{\varepsilon_2}\right)+\frac{\varepsilon_1}{\beta_1}\left(1+\frac{\beta_2}{\varepsilon_2}\right)\right], \tag{66}$$

$$\tilde{J}_3 \simeq e^{-\frac{T}{\gamma_{th}(1-\rho_1)}}\frac{\gamma_{th}(1-\rho_1)}{\lambda_1}, \tag{67}$$

$$\tilde{J}_4 \simeq \frac{T\gamma_{th}}{\lambda_1^2}\left[\frac{\varepsilon_1}{\alpha}(1+\beta_2 c_2)+\frac{\varepsilon_1}{\beta_1}(1+c_2\beta_2(1-\rho_2))\right]. \tag{68}$$

Summarizing the results in (63)-(68), the asymptotic SOP for DSSSC with S-ECSI can be obtained. From this asymptotic expression of SOP, a few insights about the impact of channel correlation and secure switching on the network performance are obtained as follows,

Remark 5: The diversity order of DSSSC with S-ECSI falls between one and two, which suggests that both direct and relaying branches can be exploited for secure transmission. However, the secure branch switching is not as effective as the DSSSC with I-ECSI, since only the statistical channel information of eavesdropper channel can be used, which leads to some diversity order loss.

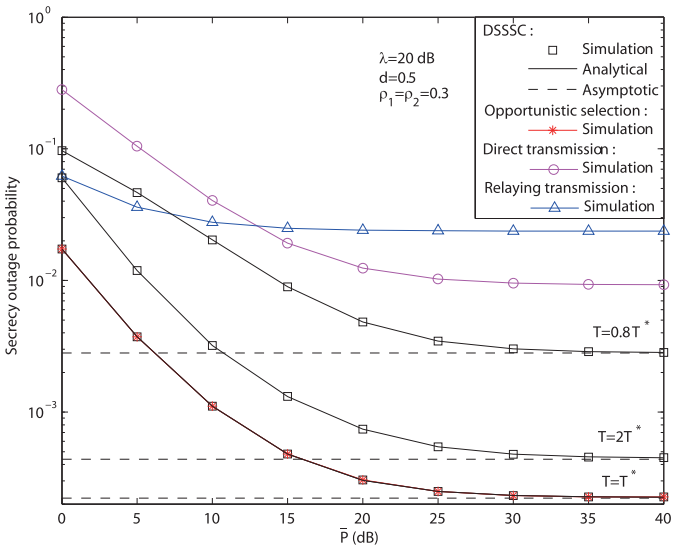
Remark 6: Although it is difficult to analytically obtain the optimal secure switching threshold T^* with the minimum SOP, we can employ some numerical methods such as the dichotomy method to efficiently find the optimal value of T^* [23], [38].

Remark 7: As $\tilde{J}_1$, $\tilde{J}_2$, $\tilde{J}_3$ and $\tilde{J}_4$ become smaller with increasing ρ_1 and ρ_2, we can find that higher channel correlation can help suppress the wiretap in the network. However, $\tilde{C}_R$ and $\tilde{C}_D$ are not affected by the channel correlation between the main and eavesdropper channels, due to the ineffective secure branch switching. In particular, $\rho_1 = 1$ does not result in $\tilde{C}_R = 0$, which is different from the result of DSSSC with I-ECSI.

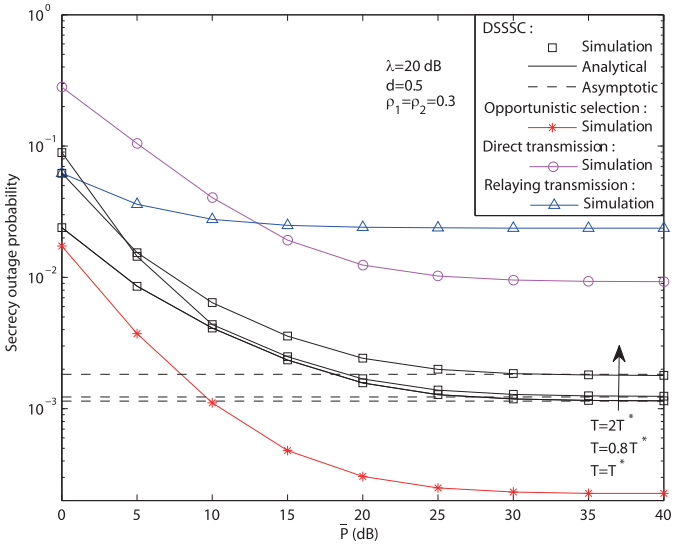
Remark 8: From (66) and (67), we see that when the main and eavesdropper channels of direct links are completely correlated, $\tilde{J}_2$ and $\tilde{J}_3$ are both equal to zero, which suggests that the direct branch can provide a perfect secure transmission. However, when $\rho_1 = 1$, $\tilde{C}_R > 0$ holds which indicates that the relaying branch is still used for data transmission. Accordingly, DSSSC with S-ECSI cannot achieve a perfect secure transmission, which is different from DSSSC with I-ECSI. This is because that the benefit of channel correlation cannot be fully exploited with the inefficient utilization of secure branch switching.

V. Numerical and Simulation Results

In this section, we aim to verify the proposed analysis with numerical and simulation results. All links are assumed to experience the Rayleigh flat fading, and a path loss model with loss factor of four is adopted. Without loss of generality, we normalize the distance between S and D to unity. Let d denote the distance between the source and relay, and accordingly, we have $\alpha = d^{-4}$, $\beta_1 = (1-d)^{-4}$. If not specified, the target secrecy data rate R_s is set to 0.4 bps/Hz as a reference value, and the associated γ_{th} is equal to 1.32. Moreover, we assume the MERs regarding both direct and relaying branches are equal with $\lambda_1 = \lambda_2 = \lambda$. In order accurately compute the analytical approximations of SOP with I-ECSI and S-ECSI, we set the exponentially bounded truncation error to a very small value of 10^{-10}, leading to $N_1 = \text{round}(\frac{-10}{\log_{10}\rho_1})$ and $N_2 = \text{round}(\frac{-10}{\log_{10}\rho_2})$. Accordingly, only the first N_1 and N_2 terms are kept in the analytical approximations.



(a) I-ECSI



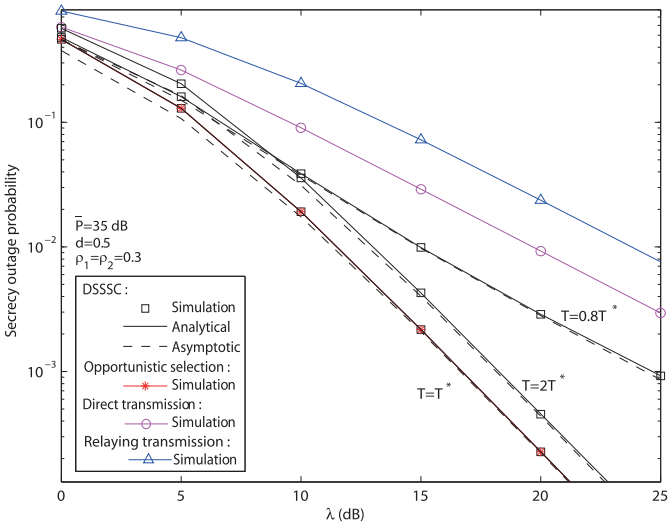
(b) S-ECSI

Fig. 2. Secrecy outage probability of DSSSC versus the transmit SNR $\bar{P}$. (a) I-ECSI. (b) S-ECS.

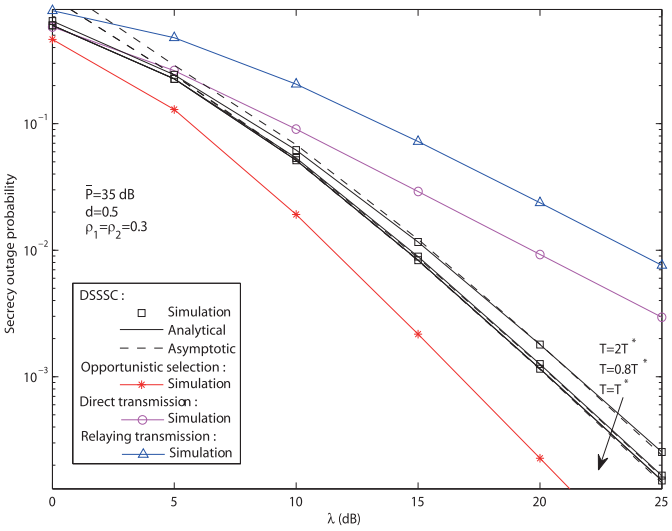
Fig. 2 demonstrates how the secrecy outage probability of DSSSC varies with the transmit SNR $\bar{P}$, where $d = 0.5$, MER = 20 dB, $\rho_1 = \rho_2 = 0.3$ and $\bar{P}$ varies from 0 dB to 40 dB. Specifically, Fig. 2 (a) and (b) correspond to DSSSC with I-ECSI and S-ECSI, respectively. For performance comparison, we also give the simulated secrecy outage probabilities of opportunistic selection, the direct transmission where only the direct branch is used, and the relaying transmission where only the relaying branch is used. The optimal secure

switching thresholds T^* for DSSSC with I-ECSI is equal to γ_{th}, while the optimal T^* for the DSSSC with S-ECSI can be obtained by applying some numerical methods in (34). We set several typical values of the secure switching threshold T, with $T = \{0.8, 1, 2\}T^*$. As observed from Fig. 2, we can find that for both I-ECSI and S-ECSI, the analytical result of DSSSC fits the simulation one perfectly, and approaches to asymptotic result in the high SNR region, which verifies the derived analytical and asymptotic SOP of DSSSC. Moreover, for I-ECSI, DSSC with the optimal T can achieve the best performance of opportunistic selection, which outperforms the transmission through the direct branch only and through the relaying branch only. The performance of DSSSC with I-ECSI degrades with $T = 2T^*$ or $T = 0.8T^*$, as large or small secure switching threshold cannot utilize the branch switching effectively. In further, for S-ECSI, although DSSSC with the optimal T cannot achieve the secrecy performance of the opportunistic selection, it is still better than the secrecy performance of direct transmission and relaying transmission. Furthermore, by comparing the results in Fig. 2 (a) and (b), we should highlight that there are two major differences in SOP performance between the DSSSC with I-ECSI and that with S-ECSI. One difference is that DSSSC with I-ECSI can achieve the optimal performance of the opportunistic selection, while DSSSC with S-ECSI cannot. Another difference is that DSSSC with S-ECSI performs worse than DSSSC with I-ECSI, due to the ineffective secure branch switching. The performance gap becomes larger with increasing value of transmit SNR. In particular, the secrecy outage probability of DSSSC with S-ECSI is about 5 times that of DSSSC with I-ECSI, when the transmit SNR is 30 dB.

Fig. 3 shows the secrecy outage probabilities of DSSSC versus MER, where $\bar{P}$=35dB, d=0.5, $\rho_1 = \rho_2 = 0.3$ and T varies in $\{0.8, 1, 2\}T^*$. In particular, Fig. 3 (a) and (b) correspond to DSSSC with I-ECSI and S-ECSI, respectively. We can see from Fig. 3 that for both I-ECSI and S-ECSI, the analytical result of DSSSC matches well with the simulation one, and the asymptotic result converge to the exact one in the high MER regime, which also verifies the derived analytical and asymptotic expressions of DSSSC. Moreover, for I-ECSI, DSSSC with the optimal T achieves the same best performance with the opportunistic selection, and DSSSC with $T = 2T^*$ has the same slope with the opportunistic selection. This indicates that the diversity order of DSSSC with I-ECSI is equal to two when $T \geq \gamma_{th}$. On the other hand, when $T \leq \gamma_{th}$, DSSSC with I-ECSI has the same slope with that of secure transmission through direct branch and relaying branch, indicating that DSSSC with I-ESCI has the diversity order of one when the secure switching threshold is small. In further, although DSSSC cannot achieve the same secure performance of opportunistic selection, it still outperforms the transmission through direct or relaying branch only. The asymptotic slope of DSSSC with S-ECSI are between those of opportunistic selection and the direct transmission, which verifies that the diversity order of the DSSSC with S-ECSI falls into $[1, 2]$. Furthermore, by comparing the results in Fig. 3 (a) and (b), we can also find the two major differences in SOP performance between the DSSSC with I-ECSI and



(a) I-ECSI

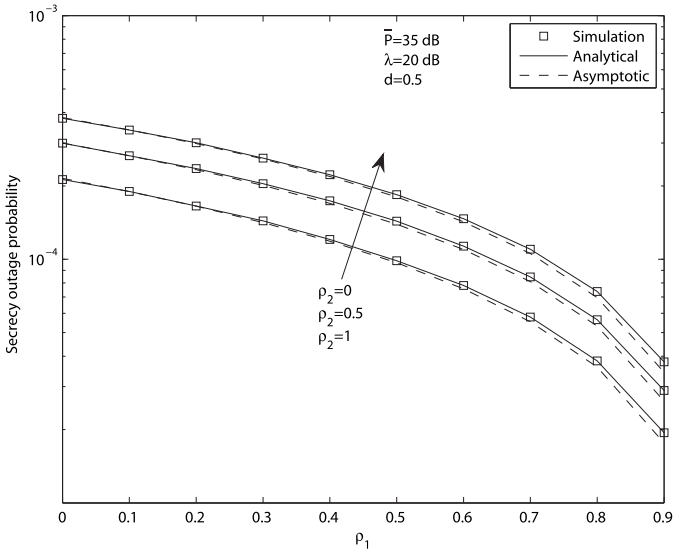


(b) S-ECSI

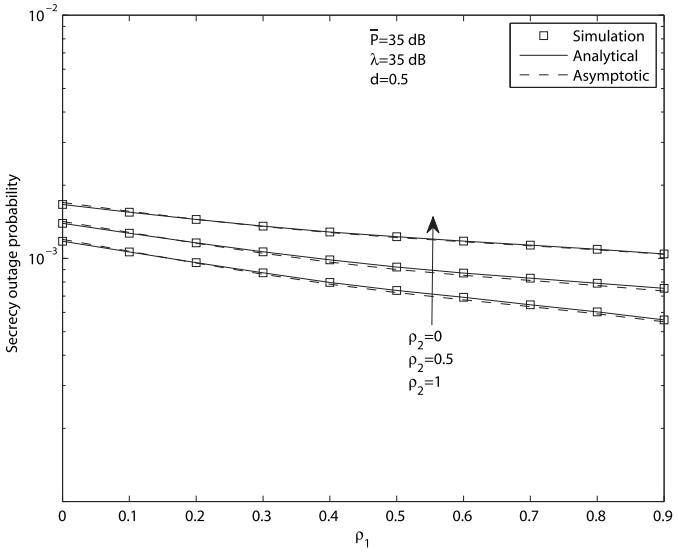
Fig. 3. Secrecy outage probability of DSSSC versus MER λ. (a) I-ECSI. (b) S-ECSI.

DSSSC with S-ECSI, similar to the comparison result in Fig. 2 (a) and (b).

Fig. 4 illustrates the effect of channel correlation on the secrecy performance of DSSSC, where $d = 0.5$, $\bar{P} = 35$ dB, $\lambda = 20$ dB, ρ_1 varies from 0 to 0.9 and ρ_2 varies in $\{0, 0.5, 1\}$. Specifically, Fig. 4 (a) and (b) are associated with DSSSC with I-ECSI and S-ECSI, respectively. We can find from Fig. 4 that for DSSSC with I-ECSI and S-ECSI, the secrecy performance improves with increasing ρ_1 and ρ_2, as larger channel correlation helps suppress the wiretap. Moreover, when ρ_1 approaches to one where the direct S–D and S–E links are completely correlated, the SOP of DSSSC with I-ECSI decreases drastically. This is because that when $\rho_1 = 1$, the secure transmission can relay on the direct branch and the perfect secure transmission can be achieved. On the contrary, when $\rho_1 = 1$, the secrecy performance of DSSSC with S-ECSI improves much more slowly than that of DSSSC with I-ESCI,

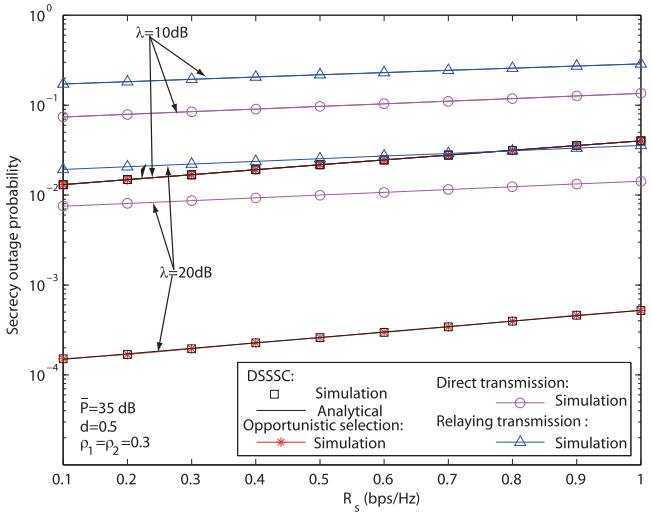


(a) I-ECSI

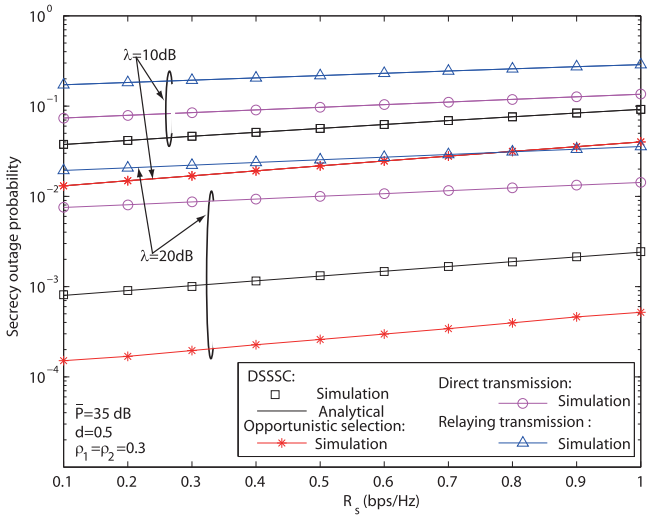


(b) S-ECSI

Fig. 4. Impact of ρ_1 and ρ_2 on the secrecy outage probability of DSSSC. (a) I-ECSI. (b) S-ECSI



(a) I-ECSI



(b) S-ECSI

Fig. 5. Secrecy outage probability versus the target secrecy data rate R_s. (a) I-ECSI. (b) S-ECSI.

since utilization of statistical information of eavesdropper channel cannot fully exploit the benefit of channel correlation. In further, the effect of ρ_2 on the secrecy performance of DSSSC is less obvious than that of ρ_1, since the MRC receiver at the eavesdropper combines the signals from both the direct and relaying links. Even for $\rho_2 = 1$ where the relaying R–D and R–E links are completely correlated, the eavesdropper can still use the direct link for wiretap.

Fig. 5 depicts how the secrecy outage probability varies with the target secrecy data rat R_s, where $\bar{P} = 35$ dB, $\lambda = \{10, 20\}$ dB, $\rho_1 = \rho_2 = 0.3$, and R_s varies from 0.1 bps/Hz to 1 bps/Hz. Specifically, Figs. 5 (a) and (b) are associated with DSSSC with I-ECSI and S-ECSI, respectively. As expected, we see that with increasing R_s, the SOP becomes worse, since the secrecy SNR threshold γ_{th} becomes larger. Moreover, the SOP performance improves with larger value of λ, as higher MER can help suppress the wiretap from the eavesdropper. Furthermore, for a wide range of R_s, DSSSC with either I-ECSI or S-ECSI outperforms the direct transmission and relaying transmission, which further demonstrates the advantages of our DSSSC protocol.

VI. Conclusions

In this paper, the secure transmission of the DF relaying networks was analyzed, where the channel correlation between the main and eavesdropper channels was taken into consideration. We proposed the DSSSC protocol with I-ECSI or S-ECSI to reduce the implementation complexity while maintain the secure performance in the presence of direct link. In further, we evaluated the impact of correlated fading on secure communication by deriving the analytical expression of secrecy outage probability as well as the high-MER asymptotic expression. Form the asymptotic results, we conclude that the DSSSC can achieve the secure performance of opportunistic

selection and obtain the diversity order of two with less implementation complexity. Moreover, the channel correlation between the main and eavesdropper channels is helpful for the transmission security. In the future works, we will employ multi-antenna at the nodes and the associated techniques such as beamforming [19], [20] to further enhance the physical-layer security for the considered networks. In addition, we will adopt the time-division half-duplex relaying and study how the channel correlation over the dual-hop relaying channels affects the network secrecy performance.

APPENDIX A
PROOF OF PROPOSITION 1

From (48), we rewrite ϕw_2 as

$$\phi w_2 = \frac{\phi\rho_1 w_1}{\lambda_1} + \frac{2\phi\sqrt{\rho_1(1-\rho_1)}(w_{11}n_{11} + w_{12}n_{12})}{\lambda_1} + \frac{\phi(1-\rho_1)n_1}{\lambda_1}. \tag{A.1}$$

When $w_1 \le \phi w_2$ holds, we see that

$$\frac{\phi\rho_1 w_1}{\lambda_1} \ll w_1 \le \phi w_2 \tag{A.2}$$

holds and hence the first term on the RHS of (A.1) is negligible compared with ϕw_2. Moreover, from Cauchy-Schwarz inequality [31], the upper bound of $2\sqrt{\rho_1(1-\rho_1)}(w_{11}n_{11} + w_{12}n_{12})$ on the third term of the RHS of (48) is obtained as

$$\begin{aligned} &2\sqrt{\rho_1(1-\rho_1)}(w_{11}n_{11} + w_{12}n_{12}) && \text{(A.3)}\\ &\le \rho_1(w_{11}^2 + w_{12}^2) + (1-\rho_1)(n_{11}^2 + n_{12}^2) && \text{(A.4)}\\ &= \rho_1 w_1 + (1-\rho_1)n_1. && \text{(A.5)} \end{aligned}$$

When $w_1 \le \phi w_2$ holds, we combine (48) and (A.3)-(A.5), and then we have

$$w_1 \le \frac{2\phi\,[\rho_1 w_1 + (1-\rho_1)n_1]}{\lambda_1}, \tag{A.6}$$

which is equivalent to

$$w_1 \le \frac{2\phi(1-\rho_1)n_1}{\lambda_1 - 2\phi\rho_1}. \tag{A.7}$$

From (A.7) and Cauchy-Schwarz inequality, we write the upper bound of the second term on the RHS of (A.1) as

$$\begin{aligned} &\frac{2\phi\sqrt{\rho_1(1-\rho_1)}(w_{11}n_{11} + w_{12}n_{12})}{\lambda_1}\\ &\le \left(\frac{(2\phi)^{\frac{3}{2}}}{\lambda_1(\lambda_1 - 2\phi\rho_1)^{\frac{1}{2}}}\right)(1-\rho_1)\sqrt{\rho_1}n_1 && \text{(A.8)}\\ &\overset{a}{\ll} \frac{\phi(1-\rho_1)n_1}{\lambda_1} && \text{(A.9)}\\ &< \phi w_2. && \text{(A.10)} \end{aligned}$$

where step (a) holds when λ_1 is large and $\phi \ll \lambda_1$. Also, the last two inequalities suggest that the second term on the RHS of (A.1) is negligible compared with ϕw_2. As observed, when $w_1 \le \phi w_2$ and $\phi \ll \lambda_1$, only the third term is left in ϕw_2 and the proof of Proposition 1 is completed.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] N. Zhao, F. R. Yu, M. Li, Q. Yan, and V. C. M. Leung, "Physical layer security issues in interference-alignment-based wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 162–168, Aug. 2016.

[3] N. Zhao, Y. Cao, F. R. Yu, Y. Chen, M. Jin, and V. C. M. Leung, "Artificial noise assisted secure interference networks with wireless power transfer," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1087–1098, Feb. 2018.

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

[5] L. Sun and H. Xu, "Unequal secrecy protection for untrusted two-way relaying systems: Constellation overlapping and noise aggregation," *IEEE Trans. Veh. Technol.*, vol. 67, no. 10, pp. 9681–9695, Oct. 2018.

[6] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[7] J. Li and A. P. Petropulu, "Ergodic secrecy rate for multiple-antenna wiretap channels with Rician fading," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 861–867, Sep. 2011.

[8] X. Liu, "Probability of strictly positive secrecy capacity of the Rician–Rician fading channel," *IEEE Wireless Commun. Lett.*, vol. 2, no. 1, pp. 50–53, Feb. 2013.

[9] C. Li, Y. Xu, J. Xia, and J. Zhao, "Protecting secure communication under UAV smart attack with imperfect channel estimation," *IEEE Access*, vol. 6, pp. 76395–76401, 2019.

[10] L. Xiao, Y. Li, C. Dai, H. Dai, and H. V. Poor, "Reinforcement learning-based NOMA power allocation in the presence of smart jamming," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3377–3389, Apr. 2018.

[11] Y. Xu, J. Xia, H. Wu, and L. Fan, "Q-learning based physical-layer secure game against multiagent attacks," *IEEE Access*, to be published.

[12] Y. Cao *et al.*, "Optimization or alignment: Secure primary transmission assisted by secondary networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 905–917, Apr. 2018.

[13] C. Zhong, H. A. Suraweera, G. Zheng, I. Krikidis, and Z. Zhang, "Wireless information and power transfer with full duplex relaying," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3447–3461, Oct. 2014.

[14] L. Fan, N. Zhao, X. Lei, Q. Chen, N. Yang, and G. K. Karagiannidis, "Outage probability and optimal cache placement for multiple amplify-and-forward relay networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12373–12378, Dec. 2018.

[15] M. Zhang and Y. Liu, "Secure beamforming for untrusted MISO cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4861–4872, Jul. 2018.

[16] F. Shi, J. Xia, Z. Na, X. Liu, Y. Ding, and Z. Wang, "Secure probabilistic caching in random multi-user multi-UAV relay networks," *Phys. Commun.*, vol. 32, pp. 31–40, Feb. 2019.

[17] H. Xu, L. Sun, P. Ren, Q. Du, and Y. Wang, "Cooperative privacy preserving scheme for downlink transmission in multiuser relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 825–839, Apr. 2017.

[18] X. Lin, J. Xia, and Z. Wang, "Probabilistic caching placement in UAV-assisted heterogeneous wireless networks," *Phys. Commun.*, vol. 33, pp. 54–61, Apr. 2019.

[19] J. Qiao, H. Zhang, X. Zhou, and D. Yuan, "Joint beamforming and time switching design for secrecy rate maximization in wireless-powered FD relay systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 567–579, Jan. 2018.

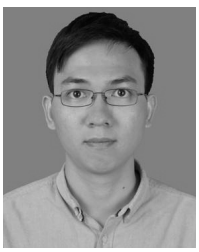
[20] J. Qiao, H. Zhang, F. Zhao, and D. Yuan, "Secure transmission and self-energy recycling with partial eavesdropper CSI," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1531–1543, Jul. 2018.

[21] 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.

[22] L. Fan, N. Yang, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Exploiting direct links for physical layer security in multiuser multirelay networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3856–3867, Jun. 2016.

[23] L. Fan, S. Zhang, T. Q. Duong, and G. K. Karagiannidis, "Secure switch-and-stay combining (SSSC) for cognitive relay networks," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 70–82, Jan. 2016.

[24] F. S. Al-Qahtani, C. Zhong, and H. M. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1756–1770, May 2015.
[25] W. C.-Y. Lee, "Effects on correlation between two mobile radio base-station antennas," *IEEE Trans. Veh. Technol.*, vol. VT-22, no. 4, pp. 130–140, Nov. 1973.
[26] S.-B. Rhee and G. Zysman, "Results of suburban base station spatial diversity measurements in the UHF band," *IEEE Trans. Commun.*, vol. COMM-22, no. 10, pp. 1630–1636, Oct. 1974.
[27] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1975–1983, Apr. 2011.
[28] 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.
[29] L. Fan, R. Zhao, F.-K. Gong, N. Yang, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying over correlated fading channels," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2811–2820, Jul. 2017.
[30] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy cooperative networks with outdated relay selection over correlated fading channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7599–7603, Aug. 2017.
[31] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.
[32] M. K. Simon and M.-S. Alouini, *Digital Communication Over Fading Channels*, 2nd ed. Hoboken, NJ, USA: Wiley, 2005.
[33] F. Gao, T. Cui, and A. Nallanathan, "Optimal training design for channel estimation in decode-and-forward relay networks with individual and total power constraints," *IEEE Trans. Signal Process.*, vol. 56, no. 12, pp. 5937–5949, Dec. 2008.
[34] Q. Li, Q. Zhang, and J. Qin, "Robust beamforming for cognitive multi-antenna relay networks with bounded channel uncertainties," *IEEE Trans. Commun.*, vol. 62, no. 2, pp. 478–487, Feb. 2014.
[35] C. Zhong, X. Jiang, F. Qu, and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: Design and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4585–4599, Jul. 2017.
[36] R. E. Mortensen, *Random Signals and Systems*. Hoboken, NJ, USA: Wiley, 1987.
[37] N. S. Ferdinand, D. B. da Costa, A. L. F. de Almeida, and M. Latva-Aho, "Physical layer secrecy performance of TAS wiretap channels with correlated main and eavesdropper channels," *IEEE Wireless Commun. Lett.*, vol. 3, no. 1, pp. 86–89, Feb. 2014.
[38] 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.



Xiazhi Lai is currently pursuing the Ph.D. degree with the School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou, China. He is also with the School of Computer Science, Guangzhou University, under the supervision of Prof. L. Fan. His research interests include cooperative communications, physical-layer security, and non-orthogonal multiple access.

Lisheng Fan received the bachelor's degree from the Department of Electronic Engineering, Fudan University, China, in 2002, the master's degree from the Department of Electronic Engineering, Tsinghua University, China, in 2005, and the Ph.D. degree from the Department of Communications and Integrated Systems, Tokyo Institute of Technology, Japan, in 2008. He is currently a Professor with Guangzhou University. He has published many papers in international journals such as the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON INFORMATION THEORY, and papers in conferences such as IEEE ICC, IEEE Globecom, and IEEE WCNC. His research interests span in the areas of wireless cooperative communications, physical-layer secure communications, interference modeling, and system performance evaluation. He has also served as a member for technical program committees of the IEEE conferences such as Globecom, ICC, WCNC, and VTC. He is a Guest Editor of the *EURASIP Journal on Wireless Communications and Networking* and served as the Chair for the Wireless Communications and Networking Symposium for Chinacom 2014.

Xianfu Lei was born in 1981. From 2012 to 2014, he was a Research Fellow with the Department of Electrical and Computer Engineering, Utah State University, USA. Since 2015, he has been an Associate Professor with the School of Information Science and Technology, Southwest Jiaotong University, China. His current research interests include 5G wireless communications, cooperative communications, cognitive radio, physical layer security, and energy harvesting. He has published nearly 70 journal and conference papers on these topics. He has also served as a TPC member for major international conferences such as IEEE ICC, IEEE GLOBECOM, IEEE WCNC, IEEE VTC Spring/Fall, and IEEE PIMRC. He received Exemplary Reviewer Certificates from the IEEE COMMUNICATIONS LETTERS, and the IEEE WIRELESS COMMUNICATIONS LETTERS in 2013. He currently serves on the Editorial Board for IEEE COMMUNICATIONS LETTERS, IEEE ACCESS, *Wireless Communications and Mobile Computing*, *Security and Communication Networks*, the *KSII Transactions on Internet and Information Systems*, and *Telecommunication Systems*. He has served as a Guest Editor for the Special Issue on Non-orthogonal Multiple Access for 5G Systems in the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS in 2016 and the Lead Guest Editor of the Special Issue on Energy Harvesting Wireless Communications in the *EURASIP Journal on Wireless Communications and Networking* in 2014.

Jin Li received the B.S. degree in mathematics from Southwest University in 2002 and the M.S. degree in mathematics and the Ph.D. degree in information security from Sun Yat-sen University in 2004 and 2007, respectively. He was a Senior Researcher and a Visiting Professor with the Korea Advanced Institute of Technology and Illinois Institute of Technology and VirginaTech, respectively. He is currently a Professor and a Vice Dean of the School of Computer Science, Guangzhou University. He has published more than 100 papers in international conferences and journals, including IEEE TDSC, IEEE INFOCOM, IEEE TIFS, IEEE TPDS, IEEE TC, and ESORICS. Three papers have been selected as the best paper in the international conferences. His research has been cited more than 11 000 times at Google Scholar and the h-index is 42. His research interests include design of secure protocols in computing and privacy protection in various new computing environments. He also served as a program chair/publicity chair for many international conferences such as IEEE Blockchain 2018, ICA3PP2018, IEEE CNS 2015, IEEE CSE 2017, IEEE EUC 2017, and ISICA 2015. He is an Associate Editor of *Information Sciences* and a guest editor of several journals such as MONET, JNCA, and FGCS.

Nan Yang (S'09–M'11) received the B.S. degree in electronics from China Agricultural University in 2005 and the M.S. and Ph.D. degrees in electronic engineering from the Beijing Institute of Technology in 2007 and 2011, respectively. He was a Post-Doctoral Research Fellow with The University of New South Wales from 2012 to 2014 and also with the Commonwealth Scientific and Industrial Research Organization from 2010 to 2012. He has been with the Research School of Electrical, Energy and Materials Engineering, The Australian National University, since 2014, where he is currently a Senior Lecturer. His general research interests include massive multi-antenna systems, millimeter-wave and terahertz communications, ultra-reliable low latency communications, cyber-physical security, and molecular communications. He received the Top Editor Award from the *Transactions on Emerging Telecommunications Technologies* in 2017, the Exemplary Reviewer Award from the IEEE TRANSACTIONS ON COMMUNICATIONS in 2016 and 2015, the Top Reviewer Award from the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY in 2015, the IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award, the Exemplary Reviewer Award from IEEE WIRELESS COMMUNICATIONS LETTERS in 2014, and the Exemplary Reviewer Award from IEEE COMMUNICATIONS LETTERS in 2013 and 2012. He was a co-recipient of best paper awards from IEEE GlobeCOM 2016 and IEEE VTC 2013-Spring. He currently serves on the Editorial Board for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and the *Transactions on Emerging Telecommunications Technologies*.

George K. Karagiannidis (M'96–SM'03–F'14) was born in Pythagorion, Greece. He received the University Diploma and Ph.D. 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 with the Institute for Space Applications and Remote Sensing, National Observatory of Athens, Greece. In 2004, he joined the Aristotle University of Thessaloniki, Greece, as a Faculty Member, where he is currently a Professor with the Electrical and Computer Engineering Department and Director of the Digital Telecommunications Systems and Networks Laboratory. He is also an Honorary Professor with South West Jiaotong University, Chengdu, China.

His research interests are in the broad area of digital communications systems and signal processing, with emphasis on wireless communications, optical wireless communications, wireless power transfer and applications, communications for biomedical engineering, stochastic processes in biology, and wireless security. He has authored or co-authored more than 500 technical papers published in scientific journals and presented at international conferences. He has also authored the Greek edition of a book on *Telecommunications Systems* and co-authored the book *Advanced Optical Wireless Communications Systems* (Cambridge Publications, 2012).

Dr. Karagiannidis is involved as the General Chair, the Technical Program Chair, and a member of technical program committees in several IEEE and non-IEEE conferences. He was an Editor of IEEE TRANSACTIONS ON COMMUNICATIONS and the *EURASIP Journal of Wireless Communications and Networks*, a Senior Editor of IEEE COMMUNICATIONS LETTERS, and several times as a Guest Editor of IEEE SELECTED AREAS IN COMMUNICATIONS. From 2012 to 2015, he was the Editor-in Chief of IEEE COMMUNICATIONS LETTERS. He is one of the highly cited authors across all areas of electrical engineering, recognized from Clarivate Analytics as a Web-of-Science Highly-Cited Researcher from 2015 to 2018.