Secure Source-Relay Link Based Threshold DF Relaying Scheme

Jin Yao, Jia Ye, Danyang Wang, Hongjiang Lei, Gaofeng Pan

PII: S1434-8411(17)32403-2
DOI: https://doi.org/10.1016/j.aeue.2018.01.002
Reference: AEUE 52191

To appear in: *International Journal of Electronics and Communications*

Received Date: 10 October 2017
Accepted Date: 3 January 2018

Please cite this article as: J. Yao, J. Ye, D. Wang, H. Lei, G. Pan, Secure Source-Relay Link Based Threshold DF Relaying Scheme, *International Journal of Electronics and Communications* (2018), doi: https://doi.org/10.1016/j.aeue.2018.01.002

Secure Source-Relay Link Based Threshold DF Relaying Scheme

Jin Yao[1], Jia Ye[2], Danyang Wang[2], Hongjiang Lei[3],Gaofeng Pan[4]

1. Chongqing City Management College, Chongqing, 401331, China.

2. Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing, Southwest University, Chongqing, 400715, China.

3. Chongqing Key Lab of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China (email: leihj@cqupt.edu.cn).

4. School of Computing and Communications, Lancaster University, Lancaster, LA1 4WA, U.K. (e-mail: g.pan1@lancaster.ac.uk).

Abstract

In this work, a dual-hop cooperative system, in which there are a Source-Destination (S-D) pair, a relay node (R) and an eavesdropper (E), which attempts to eavesdrop the confidential message sent by S and forwarded by R, is considered. In order to enhance the system performance and save the system resource, we propose an $S-R$ link based threshold decode-and-forward (DF) relaying scheme for R to decide whether to aid S-D pair's information transmission or not, other than the traditional DF relaying scheme. The secrecy outage performance of the considered system is investigated and the closed-form analytical expression for secrecy outage probability is derived and verified via Monte-Carlo simulations.

Keywords:

Decode-and-forward, dual-hop, Rayleigh fading, secrecy outage.

1. Introduction

Due to the openness of wireless medium, the probability that the delivered information suffers eavesdropping will increase, when there is an eavesdropper trying to overhead the information transmission between the source and the destination. Then, the amount of secrecy information capacity of the data transmission between the source and the destination will degrade, resulting in poor physical layer security. [1] firstly described the wiretap channel, in which two legitimate terminals want to have secure communication with an eavesdropper appears in the channel.

Recently, plenty of works have been presented to study the security at the physical layer [2-8]. The author of [2] examined the security issue in the 5G network by considering the randomness of the communication terminals with disruptive technologies. [3] proposed a secure multiple-input multiple-output (MIMO) system consisting of a base station, an information-decoding user, and an energy-harvesting user, while considering simultaneous wireless information and power transfer (SWIPT). The authors of [4] and [5] investigated the secrecy performance of visible light communication system, while considering the randomness of the locations of the terminals. [6] presented a new key management mechanism which combines trusted-server scheme and key pre-distribution scheme to satisfy the security network architecture. The author of [7] also studied the secrecy outage performance for an underlay cognitive radio unit system over Nakagami-m fading channel. [8] studied a MIMO cognitive wiretap system, which adapts generalized selection combining over Nakagami-m channels in place of a multiple-antenna eavesdropper. Moreover, [9] investigated the secrecy capacity for classic Wyner's model over

α-μ fading channels.

Therefore, one can clearly see that physical layer security issue is quite important and urgent for wireless relay communication systems, as more information leakage might happen over the extended links [10]. In other words, the additional communication links from the source to relays can improve the system' coverage and throughput [11-12], however eavesdropping can also take place over these relaying links. Therefore, the security of the wireless cooperative/relay systems attracts more and more researchers' interests [13-24]. Several cooperation strategies were considered in [13] to derive the optimal rate-equivocation region for four-terminal relay-eavesdropper channel. A best decode-and-forward (DF) relay was selected by adopting selection combining (SC) technique to communicate with a destination [14]. In order to improve the security against eavesdroppers, an opportunistic selection scheme of two relay nodes was proposed in [15]. Partial relay selection schemes were proposed for cooperative systems with multi-relays in [16]. Hybrid decode-amplify-forward relay with three different selection schemes was introduced to enhance the secrecy performance of the considered wireless system in [17]. In [18], the outage and symbol error performance has been studied for a dual-hop conditional DF relay system. The influence of SWIPT at the relay on the outage of A dual-hop DF system was investigated in [19]. In [20], the authors studied the physical layer secrecy performance of multi-hop DF relay network was investigated in the presence of multiple passive eavesdroppers over Nakagami-m fading channels. For time-division multiple-access based DF cooperative protocols, the authors of [21] analyzed achievable secrecy rates with total and individual relay power constraints and

design relay beamforming weights to improve the secrecy rate. [22] presented and analyzed a jamming power allocation method that can effectively achieve the secrecy rate in cooperative network. An exponential-type integral representation for the logarithmic function was utilized to derive an approximate expression for the ergodic secrecy rates of cooperative DF relay networks only in terms of the moment generating function of signal-to-noise ratio (SNR) [23]. In order to provide security at the physical layer, [24] designed a cooperative protocol relying on both cooperative relaying and jamming.

However, to the best of our knowledge, the secrecy performance has not been well studied for cooperative systems, as most of the existing works focus on traditional relay schemes, e.g., amplify-to-forward and DF schemes. In this work, a dual-hop cooperative system, in which there are a Source-Destination (S-D) pair, a relay node (R) and an eavesdropper (E), which attempts to eavesdrop the confidential message sent by S and forwarded by R, is considered. R tries to coordinate the processes of information decoding from the received signal, by recoding and forwarding the received messages to D. Further, R adopts threshold DF relaying scheme to decide whether to aid S-D pair's information transmission or not, aiming to enhancing the system performance and save the system resource. The main contributions of this work are listed as follows:

1) In this work, we propose S-R link based threshold DF scheme, which can improve the secrecy outage performance and system resource consumption when the quality of S-R link is not good;

2) The secrecy outage performance of S-R link based threshold DF scheme is studied and the closed-form expression for secrecy outage probability has

been derived.

The rest of the paper is structured as follows. In Section 2, the system model is introduced. The secrecy outage performance is studied for threshold DF scheme by deriving the closed-form analytical expressions for the secrecy outage probability of the considered system, in Section 3. Monte-Carlo simulations are conducted to verify the proposed analytical models in Section 4. Finally, Section 5 concludes the paper.

2. System model

In this section, a cooperation group including a S-D pair, R and E, which attempts to eavesdrop the confidential message sent by S and forwarded by R, is considered. All links experience independent and identically Rayleigh fading. An S-R link based threshold relay scheme is considered in this work in order to enhance the system performance and save the system resource. Namely, R will decide to forward the decoded information bits according to the transmission over S-R link: if it is not successful, R will not take any action and keep silence; otherwise, R will forward its decoded information to D [1]. Therefore, one can clearly see that, compare to the traditional DF relay

[1] Once R can successfully decode the received signal from S, it will forward the received signal to D. Under this case, there will be two copies of the transmitted signal at both D and E. However, for practical scenarios, the main channels (including $S-R$ and $R-D$ links) should outperform the eavesdropping channels (including $S-E$ and $R-E$ links); otherwise, the secrecy capacity will be zero and the information delivery will be meaningless. So even under this case, the secrecy performance of the system will be improved as the improvement at D benefited from diversity receiving schemes (like maximal ratio combining and SC) outperforms the one at E.

scheme, under the considered threshold DF relay scheme system source can be saved while the information transmission over S-R link is not successful. Moreover, it is also assumed that each terminal has a single antenna and operates in half-duplex mode.

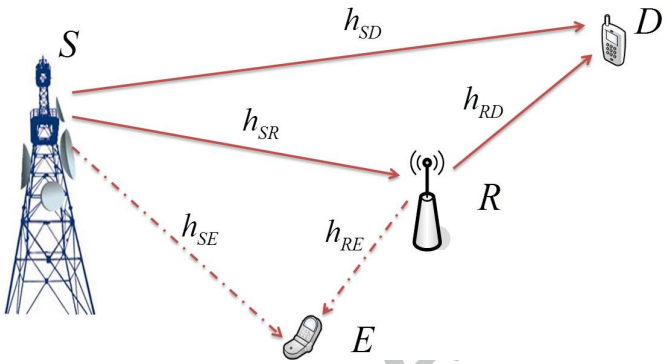

Figure 1: Secure cooperative system model

Then, we can divide the information transmission process into the following two phases:

1) S broadcasts the information to R and D;

2) Under threshold DF relay scheme, R adopts its instantaneous SNR of the received signal over S-R link as an indication of the reliability of the relaying transmission. If the SNR is larger than a predefined threshold (γ_0), the probability of an error at R is small. Hence R will forward the signal after decoding. Otherwise, R remains silent.

3. Secrecy outage analysis

If R forwards the message, there will be two copies of the transmitted signals at both of D and E. In this work we assume SC scheme is adopted

at both of D and E to process the received two copies of the signals.

In Phase 2, the received signals at R, D and E are given by

$$y_R = \sqrt{P_S} h_{SR} s + n_R \tag{1-a}$$

$$y_{D1} = \sqrt{P_S} h_{SD} s + n_D \tag{1-b}$$

$$y_{E1} = \sqrt{P_S} h_{SE} s + n_E \tag{1-c}$$

respectively, where P_i ($i \in \{S, R, D\}$) is the transmit power at node i, h_{ij} ($i, j \in \{S, D, R, E\}$) is the link channel gain between node i and j, s denotes the transmitted symbols from S, n_i ($i \in \{D, R, E\}$) denotes the independent complex Gaussian noise at R, D and E. In this work, to simplify the analysis, we assume that n_R, n_D and n_E are with zero means and a same variances, N_0.

Therefore, the SNR of the received signal at R, D and E can be written as

$$\gamma_R = \frac{P_S |h_{SR}|^2}{N_0} \tag{2-a}$$

$$\gamma_{D1} = \frac{P_S |h_{SD}|^2}{N_0} \tag{2-b}$$

$$\gamma_{E1} = \frac{P_S |h_{SE}|^2}{N_0} \tag{2-c}$$

respectively.

The probability density function (PDF) of $|h_{SR}|^2$, $|h_{SD}|^2$ and $|h_{SE}|^2$ can be given as

$$f_{|h_{SR}|^2}(x) = \frac{1}{h_{SR}} \exp\left(-\frac{x}{h_{SR}}\right) \tag{3-a}$$

$$f_{|h_{SD}|^2}(x) = \frac{1}{h_{SD}} \exp\left(-\frac{x}{h_{SD}}\right) \tag{3-b}$$

$$f_{|h_{SE}|^2}(x) = \frac{1}{h_{SE}} \exp\left(-\frac{x}{h_{SE}}\right) \qquad (3-c)$$

respectively, where h_{SR}, h_{SD} and h_{SE} are the expectation of channel power gain $|h_{SR}|^2$, $|h_{SD}|^2$ and $|h_{SE}|^2$, respectively.

Further, we can obtain $\gamma_R \sim \text{Exp}(\lambda_{SR})$, $\gamma_{D1} \sim \text{Exp}(\lambda_{SD})$ and $\gamma_{E1} \sim \text{Exp}(\lambda_{SE})$, respectively, where $\lambda_{SR} = \frac{N_0}{h_{SR}P_S}$, $\lambda_{SD} = \frac{N_0}{h_{SD}P_S}$ and $\lambda_{SE} = \frac{N_0}{h_{SE}P_S}$, respectively.

In the second phase, if R decides to forward the detected symbol, s_R, to D after regenerating, the received signal at D and E is

$$y_{D2} = \sqrt{P_R} h_{RD} s_R + n_D \qquad (4-a)$$

$$y_{E2} = \sqrt{P_R} h_{RE} s_R + n_E \qquad (4-b)$$

respectively.

Therefore, the SNR of the received signal at D and E can be written as

$$\gamma_{D2} = \frac{P_R |h_{RD}|^2}{N_0} \qquad (5-a)$$

$$\gamma_{E2} = \frac{P_R |h_{RE}|^2}{N_0}, \qquad (5-b)$$

respectively.

The PDF of $|h_{RD}|^2$ and $|h_{RE}|^2$ can be written as $f_{|h_{RD}|^2}(x) = \frac{1}{h_{RD}} \exp\left(-\frac{x}{h_{RD}}\right)$ and $f_{|h_{RE}|^2}(x) = \frac{1}{h_{RE}} \exp\left(-\frac{x}{h_{RE}}\right)$, respectively, where h_{RD} and h_{RE} is the expectation of channel power gain $|h_{RD}|^2$ and $|h_{RE}|^2$, respectively. Then, we can also obtain $\gamma_{D2} \sim \text{Exp}(\lambda_{RD})$ and $\gamma_{E2} \sim \text{Exp}(\lambda_{RE})$, respectively.

Then, when SC scheme is adopted, we can have

$$\gamma_D = \begin{cases} \gamma_{D1} & \text{if} \gamma_{SR} \leq \gamma_0 \\ \max\{\gamma_{D1}, \gamma_{D2D}\} & \text{else} \end{cases} \qquad (6-a)$$

$$\gamma_E = \begin{cases} \gamma_{E1} & \text{if} \gamma_{SR} \leq \gamma_0 \\ \max\{\gamma_{E1}, \gamma_{E2}\} & \text{else} \end{cases}, \qquad (6-b)$$

respectively, where $\gamma_{D2D} = \min\{\gamma_{SR}, \gamma_{D2}\}$ is the end-to-end SNR of $S-R-D$ link under DF scheme, the cumulative distribution function (CDF) of which can be written as $F_{\gamma_{D2D}}(x) = 1 - \exp(-(\lambda_{SR} + \lambda_{RD.})x)$.

Therefore, the instantaneous secrecy capacity of the considered system can be written as

$$C_s = \begin{cases} \log_2(1+\gamma_D) - \log_2(1+\gamma_E) & \text{if} \gamma_E \leq \gamma_D \\ 0 & \text{else} \end{cases} \qquad (7-a)$$

If $\gamma_{SR} \leq \gamma_0$, we can have

$$C_s = \begin{cases} \log_2(1+\gamma_{D1}) - \log_2(1+\gamma_{E1}) & \text{if} \gamma_{D1} \geq \gamma_{E1} \\ 0 & \text{else} \end{cases} \qquad (7-b)$$

If $\gamma_{SR} \geq \gamma_0$,it deduces

$$C_s = \begin{cases} \log_2(1+\max\{\gamma_{D1}, \gamma_{D2D}\}) - \log_2(1+\max\{\gamma_{E1}, \gamma_{E2}\}) & \text{if} \gamma_D \geq \gamma_E \\ 0 & \text{else} \end{cases} \qquad (7-c)$$

where $\gamma_D = \max\{\gamma_{D1}, \gamma_{D2D}\}$ and $\gamma_E = \max\{\gamma_{E1}, \gamma_{E2}\}$.

Therefore, the secrecy outage probability for the considered system using threshold can be expressed as

$$\begin{aligned} \Pr_{\text{out}}(C_{\text{th}}) = &\Pr\{\gamma_{SR} > \gamma_0\} \Pr\{C_s \leq C_{\text{th}} | \gamma_{SR} > \gamma_0\} \\ &+ \Pr\{\gamma_{SR} \leq \gamma_0\} \Pr\{C_s \leq C_{\text{th}} | \gamma_{SR} \leq \gamma_0\} \end{aligned} \qquad (8)$$

In the following, we derive the terms in (8), respectively.

The probability that the SNR of the S-R link γ_0 is below the threshold can be given as

$$\Pr\{\gamma_{SR} \leq \gamma_0\} = \int_0^{\gamma_0} \lambda_{SR} \exp(-\lambda_{SR} x)\, dx = 1 - \exp(-\lambda_{SR}\gamma_0) \tag{9}$$

Then, it is easy to obtain

$$\Pr\{\gamma_{SR} > \gamma_0\} = 1 - \Pr\{\gamma_{SR} \leq \gamma_0\} = \exp(-\lambda_{SR}\gamma_0) \tag{10}$$

When $\gamma_{SR} \leq \gamma_0$, the probability that the instantaneous secrecy capacity C_s drops below C_{th} can be presented as

$$\begin{aligned}
\Pr\{C_s \leq C_{\rm th} |\, \gamma_{SR} \leq \gamma_0\} &= \Pr\{C_s \leq C_{\rm th}\} \\
&= \Pr\{\log_2(1+\gamma_{D1}) - \log_2(1+\gamma_{E1}) \leq C_{\rm th}\} \\
&= \Pr\left\{\log_2\left(\tfrac{1+\gamma_{D1}}{1+\gamma_{E1}}\right) \leq C_{\rm th}\right\} \\
&= \Pr\left\{\tfrac{1+\gamma_{D1}}{1+\gamma_{E1}} \leq 2^{C_{\rm th}}\right\} \\
&= \Pr\{\gamma_{D1} \leq \lambda\gamma_{E1} + \lambda - 1\} \\
&= \int_0^{\infty} \lambda_{SE} \exp(-\lambda_{SE}\gamma_{E1}) \int_0^{\lambda\gamma_{E1}+\lambda-1} \lambda_{SD} \exp(-\lambda_{SD}\gamma_{D1})\, d\gamma_{D1} d\gamma_{E1} \\
&= \int_0^{\infty} \lambda_{SE} \exp(-\lambda_{SE}\gamma_{E1}) \left[1 - \exp(-\lambda_{SD}(\lambda\gamma_{E1} + \lambda - 1))\right] d\gamma_{E1} \\
&= 1 - \int_0^{\infty} \lambda_{SE} \exp\left(-(\lambda_{SE} + \lambda_{SD}\lambda)\gamma_{E1} - \lambda_{SD}(\lambda - 1)\right) d\gamma_{E1} \\
&= 1 - \tfrac{\lambda_{SE}\exp(-\lambda_{SD}(\lambda-1))}{\lambda_{SE}+\lambda_{SD}\lambda}
\end{aligned} \tag{11}$$

where $\lambda = 2^{C_{\rm th}}$.

When $\gamma_{SR} > \gamma_0$, the probability that the instantaneous secrecy capacity

C_s drops below C_{th} can be presented as

$$\begin{aligned}\Pr\left\{C_s \le C_{\rm th}\right\} &= \Pr\left\{\log_2\left(1+\gamma_D\right) - \log_2\left(1+\gamma_E\right) \le C_{\rm th}\right\} \\ &= \Pr\left\{\gamma_D \le \lambda\gamma_E + \lambda - 1\right\} \\ &= \int_0^{\infty} f_{\gamma_E}\left(\gamma_E\right) \int_0^{\lambda\gamma_E+\lambda-1} f_{\gamma_D}\left(\gamma_D\right) d\gamma_D d\gamma_E \\ &= \int_0^{\infty} f_{\gamma_E}\left(\gamma_E\right) F_{\gamma_D}\left(\lambda\gamma_E + \lambda - 1\right) d\gamma_E\end{aligned} \tag{12}$$

where $f_{\gamma_D}(x)$ and $f_{\gamma_E}(x)$ are the PDF of γ_D and γ_E, respectively, $F_{\gamma_D}(x)$ denotes the CDF of γ_D.

As $\gamma_D = \max\left\{\gamma_{D1}, \gamma_{D2D}\right\}$ and $\gamma_E = \max\left\{\gamma_{E1}, \gamma_{E2}\right\}$, $f_{\gamma_E}(x)$ and $F_{\gamma_D}(x)$ can be presented as

$$\begin{aligned}f_{\gamma_E}\left(x\right) = {} & \lambda_{SE}\exp\left(-\lambda_{SE}x\right)\left[1-\exp\left(-\lambda_{RE}x\right)\right] \\ & + \lambda_{RE}\exp\left(-\lambda_{RE}x\right)\left[1-\exp\left(-\lambda_{SE}x\right)\right]\end{aligned} \tag{13-a}$$

$$F_{\gamma_D}\left(x\right) = \left[1-\exp\left(-\lambda_{SD}x\right)\right]\left[1-\exp\left(-\left(\lambda_{SR}+\lambda_{RD}\right)x\right)\right] \tag{13-b}$$

Substituting Eq. (13) into (12), we can obtain

$$\begin{aligned}\Pr\left\{C_s \le C_{\rm th}\right\} = {} & \int_0^{\infty} \lambda_{SE}\exp\left(-\lambda_{SE}\gamma_E\right)\left[1-\exp\left(-\lambda_{RE}\gamma_E\right)\right] \\ & \times\left[1-\exp\left(-\lambda_{SD}\left(\lambda\gamma_E+\lambda-1\right)\right)\right] \\ & \times\left[1-\exp\left(-\left(\lambda_{SR}+\lambda_{RD}\right)\left(\lambda\gamma_E+\lambda-1\right)\right)\right]d\gamma_E \\ & + \int_0^{\infty} \lambda_{RE}\exp\left(-\lambda_{RE}\gamma_E\right)\left[1-\exp\left(-\lambda_{SE}\gamma_E\right)\right] \\ & \times\left[1-\exp\left(-\lambda_{SD}\left(\lambda\gamma_E+\lambda-1\right)\right)\right] \\ & \times\left[1-\exp\left(-\left(\lambda_{SR}+\lambda_{RD}\right)\left(\lambda\gamma_E+\lambda-1\right)\right)\right]d\gamma_E\end{aligned} \tag{14}$$

In order to facilitate the following analysis, we will consider a new integral $I = \int_0^{\infty} \exp\left(-ax\right)\left[1-\exp\left(-bx\right)\right]\left[1-\exp\left(-cx-e\right)\right]\left[1-\exp\left(-dx-f\right)\right]dx$ (where

a, b, c, d, e and f are constant, and $a > 0$, $b > 0$, $c > 0$ and $d > 0$), which can be calculated as

$$\begin{aligned} I = & \int_0^\infty \exp\left(-ax\right) dx - \int_0^\infty \exp\left(-\left(a+b\right)x\right) dx \\ & - \int_0^\infty \exp\left(-\left(a+c\right)x - e\right) dx - \int_0^\infty \exp\left(-\left(a+d\right)x - f\right) dx \\ & + \int_0^\infty \exp\left(-\left(a+b+c\right)x - e\right) dx + \int_0^\infty \exp\left(-\left(a+b+d\right)x - f\right) dx \\ & + \int_0^\infty \exp\left(-\left(a+c+d\right)x - e - f\right) dx \\ & - \int_0^\infty \exp\left(-\left(a+b+c+d\right)x - e - f\right) dx \\ = & \tfrac{1}{a} - \tfrac{1}{a+b} - \tfrac{1}{a+c}\exp(-e) - \tfrac{1}{a+d}\exp(-f) \\ & + \tfrac{1}{a+b+c}\exp(-e) + \tfrac{1}{a+b+d}\exp(-f) \\ & + \tfrac{1}{a+c+d}\exp(-e-f) - \tfrac{1}{a+b+c+d}\exp(-e-f) \end{aligned} \tag{15}$$

By using Eq. (15) into (14), we obtain

$$\begin{aligned} \Pr\left\{C_s \le C_{th}\right\} = & 1 - \left(\tfrac{\lambda_{SE}}{\lambda_{SE}+\lambda_{SD}\lambda} + \tfrac{\lambda_{RE}}{\lambda_{RE}+\lambda_{SD}\lambda}\right)\exp\left(\lambda_{SD}\left(1-\lambda\right)\right) \\ & - \left(\tfrac{\lambda_{SE}}{\lambda_{SE}+(\lambda_{SR}+\lambda_{RD})\lambda} + \tfrac{\lambda_{RE}}{\lambda_{RE}+(\lambda_{SR}+\lambda_{RD})\lambda}\right)\exp\left(\left(\lambda_{SR}+\lambda_{RD}\right)\left(1-\lambda\right)\right) \\ & + \tfrac{\lambda_{SE}+\lambda_{RE}}{\lambda_{SE}+\lambda_{RE}+\lambda_{SD}\lambda}\exp\left(\lambda_{SD}\left(1-\lambda\right)\right) \\ & + \tfrac{\lambda_{SE}+\lambda_{RE}}{\lambda_{SE}+\lambda_{RE}+(\lambda_{SR}+\lambda_{RD})\lambda}\exp\left(\left(\lambda_{SR}+\lambda_{RD}\right)\left(1-\lambda\right)\right) \\ & + \left(\tfrac{\lambda_{SE}}{\lambda_{SE}+\lambda_{SD}\lambda+(\lambda_{SR}+\lambda_{RD})\lambda} + \tfrac{\lambda_{RE}}{\lambda_{RE}+\lambda_{SD}\lambda+(\lambda_{SR}+\lambda_{RD})\lambda}\right) \\ & \times \exp\left(\left(\lambda_{SD}+\lambda_{SR}+\lambda_{RD}\right)\left(1-\lambda\right)\right) \\ & - \tfrac{\lambda_{SE}+\lambda_{RE}}{\lambda_{SE}+\lambda_{RE}+\lambda_{SD}\lambda+(\lambda_{SR}+\lambda_{RD})\lambda}\exp\left(\left(\lambda_{SD}+\lambda_{SR}+\lambda_{RD}\right)\left(1-\lambda\right)\right) \end{aligned} \tag{16}$$

Therefore, the SOP for the threshold DF scheme can be obtained by substituting Eqs. (9), (10), (11) and (16) into (8).

4. Numerical and simulation results

In order to confirm our proposed model, in this section we compare Monte-Carlo simulation and analytical results corresponding to the secrecy outage over independent Rayleigh fading channels. During each simulation, S sends 10^6 bits to D.

Figure 2 presents the result of the SOP versus (h_{RD}/h_{RE}). Unless otherwise explicitly specified, the parameters are set as $P_s = 5$ dB, $P_r = 5$ dB, $N_0 = 1$ dB, $C_{th} = 3$ dB, $\gamma_0 = 0.05$. It is obvious that SOP can be improved while (h_{RD}/h_{RE}) increases, because a larger (h_{RD}/h_{RE}) means a better R-D link with high security. Further, it can also be seen that simulation results match very well with analytical ones. In Figure 2 simulation and analytical results are presented for $h_{SD} = 2$, 4, 6. It could be observed that the SOP for a higher h_{SD} outperforms that of a smaller h_{SD} as a higher h_{SD} represents a better S-D link.

Figure 3 presents the results of the SOP versus (h_{SR}/h_{RD}). Unless otherwise explicitly specified, the parameters are set as $P_s = 5$ dB, $P_r = 5$ dB, $N_0 = 1$ dB, $C_{th} = 3$ dB, $\gamma_0 = 0.05$. It is obvious that SOP can be improved while (h_{SR}/h_{RD}) increases, because a larger (h_{SR}/h_{RD}) represents a better S-R link. Further, one can also be seen that simulation results match very well with analytical ones. In Figure 3, we can also see that simulation and analytical results of SOP are given while $h_{RE} = 0.1$, 0.3 and 0.5. It could be observed that the SOP for a higher h_{RE} outperforms that of a smaller h_{RE} as a smaller h_{RE} represents a worse R-E link.

Figure 4 and 5 present the results of the SOP versus P_s. We find that SOP can be improved with the increasing of P_s, as larger P_s indicates that

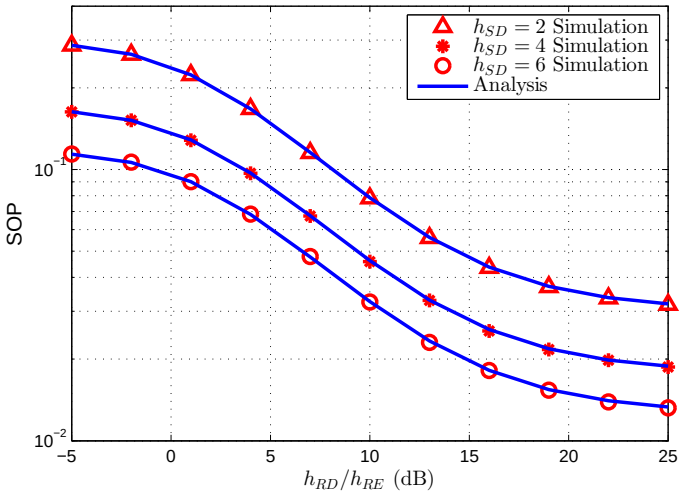

Figure 2: SOP versus (h_{RD}/h_{RE}) for different h_{SD}

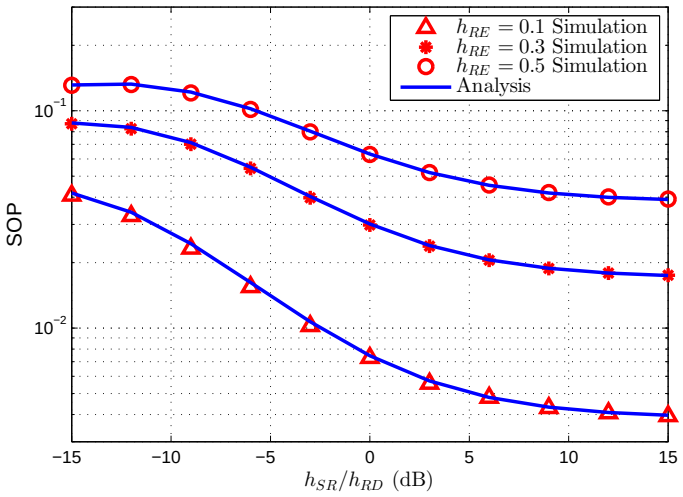

Figure 3: SOP versus (h_{SR}/h_{RD}) for different h_{RE}

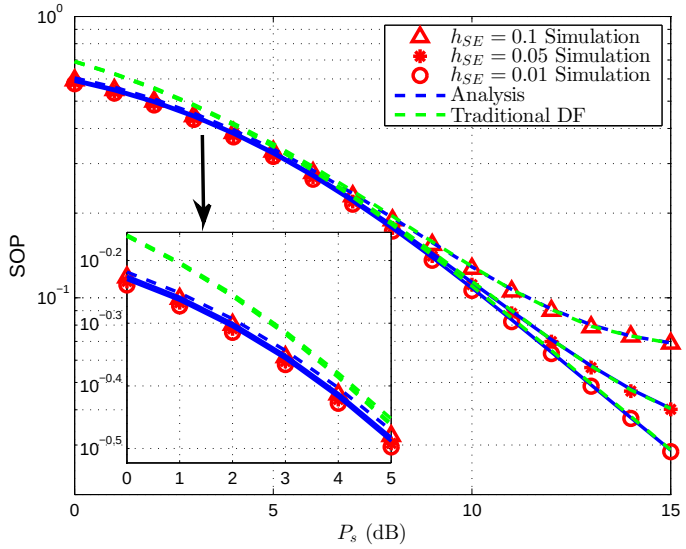

Figure 4: SOP versus P_s for different h_{SE}

a larger success probability of the transmission over S-R and S-D links. In Figure 4, we compare simulation and analytical results while $h_{SE} = 0.1$, 0.05 and 0.01 with $P_r = 10$ dB, $N_0 = 0.5$ dB, $C_{th} = 1$, $\gamma_0 = 0.5$. It is observed that SOP can be improved with the decreasing of h_{SE} in the high P_s region, while no more improvement can be found in the low P_s region. Because, when P_s is low, the probability that $\gamma_{SR} \leq \gamma_0$ will increase, as suggested by Eq. (11).

In Figure 5, we present the simulation and analytical results of SOP while $h_{RD} = 2$, 4 and 6 with $P_r = 10$ dB, $N_0 = 1$ dB, $C_{th} = 1.5$, $\gamma_0 = 1$. It is observed that SOP can be enhanced with the increase of h_{RD} in the high P_s region. One can also clearly observe that there exists a fluctuation and the SOP for different h_{RD} will approach to a constant. Because when P_s is high, the SNR of S-D link will be improved, which indicates that the data

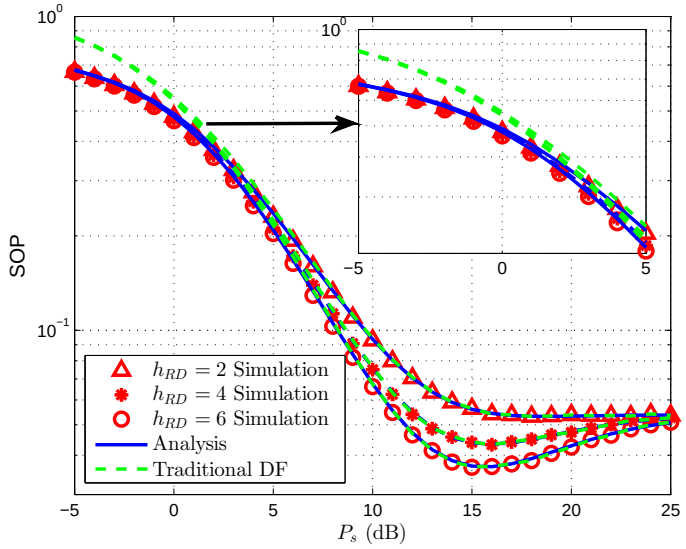

Figure 5: SOP versus P_s for different h_{RD}

transmission over S-R link will succeed. Then R will aid the information delivery between S and D, finally resulting in the diversity gain at D. So under this case the proposed threshold DF scheme will be degrade to the traditional DF scheme, and the secrecy outage performance of the target system will tend to a constant in high h_{RD}.

Moreover, as observed in Figs. 4 and 5, the proposed threshold DF scheme outperforms the traditional DF scheme in low P_s region. It can be explained by the following fact: Under the proposed threshold DF scheme, R will not forward the information for S and D, as R find the S-R transmission does not satisfy the requirement of quality. Then, in low P_s region only S-D transmission happens and E only can overhear the data transmission for one time, leading to the improved secrecy outage performance. The performance of the proposed threshold DF scheme approaches to the one of the traditional

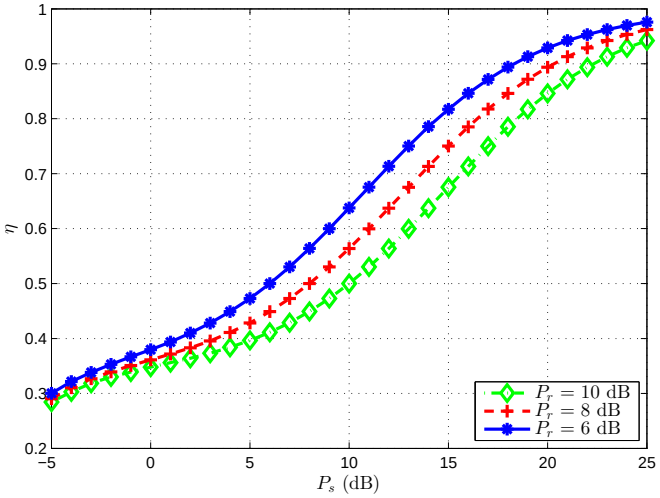

Figure 6: η versus P_s for different P_r

DF scheme in high P_s region. Because R will play as the relay for S-D transmission to forward the information over R-D link, which inevitably increases the eavesdropping probability of the data transmission.

In the following, we define the total consumption power of the considered system with the proposed threshold DF relaying scheme as P_{SUM} and the total consumption power of the considered system with traditional DF system as P_{SUM}^{DF}, respectively. In Figure 6, we define a new performance index $\eta = \frac{P_{SUM}}{P_{SUM}^{DF}}$ to illustrate the proposed threshold DF system can significantly save the consumed power. We can see from Figure 6 that $\eta \leq 1$, which means that the proposed threshold DF scheme can significantly save more consumed power than the traditional DF scheme, especially in low P_s region. Because when S-R link is poor, R will keep silent and save the transmit power consumed over the relay link from R to D.

5. Conclusions

In this work, we have investigated the secrecy outage performance of a dual-hop DF cooperative network. We derived the closed-form analytical expressions for SOP while considering the proposed $S-R$ link based threshold DF relay scheme, which is verified via Monte-Carlo simulations. By observing these numerical results, we can conclude that lower transmit power at the source can obtain lower secrecy outage probability. However, when the transmit power at the source increases, the data forwarding offered by threshold DF relay from the relay to the destination will inevitably increase the probability of the data transmission being eavesdropped, and then SOP will degrade and approaches to a constant, as the traditional DF scheme.

6. Acknowledgment

This research was supported in part by the National Science Foundation under Grants 61401372, the Project of Fundamental and Frontier Research Plan of Chongqing under Grant cstc2017jcyjAX0204, and the Scientific and Technological Research Program of Chongqing Municipal Education Commission under Grant KJ1600413, the Fundamental Research Funds for the Central Universities under Grant XDJK2015B023 and XDJK2016A011.

References

[1] C. E. Shannon. (1949). Communication theory of secrecy systems. Bell Syst. Tech. J, 28(4): 656-715.

[2] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo. (2015). Safeguarding 5G wireless communication networks using physical layer security. IEEE Commun. Mag, 53(4): 20-27.

[3] J. Zhang, C. Yuen, C. K. Wen, et al. (2015). Large system secrecy rate analysis for SWIPT MIMO wiretap channels. IEEE Trans. Inf. Forensics Sec, 11(1): 74-85.

[4] G. Pan, J. Ye and Z. Ding. (2017). Secure hybrid VLC-RF systems with light energy harvesting. IEEE Trans. Commun., 65(10): 4348-4359

[5] G. Pan, J. Ye and Z. Ding. (2017). On secure VLC systems with spatially random terminals. IEEE Commun. Lett, 21(3): 492-495.

[6] S. Yang, J. Liu, C. Fan, X. Zhang and J. Zou. (2010). A new design of security wireless sensor network using efficient key management scheme. 2010 2nd IEEE International Conference on Network Infrastructure and Digital Content, Beijing, 2010, pp. 504-508.

[7] C. Tang, G. Pan and T. Li. (2014). Secrecy outage analysis of underlay cognitive radio unit over Nakagami-m fading channels, IEEE Wirel. Commun. Lett, 3(6): 609-612.

[8] H. Lei et al. (2017). Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-m channels. IEEE Trans. Veh. Technol, 66(3): 2237-2250.

[9] H. Lei, I. S. Ansari, G. Pan, B. Alomair and M. S. Alouini. (2017). Secrecy capacity analysis over α-μ fading channels. IEEE Commun. Lett, 21(6): 1445-1448.

[10] R. Peng, H. Yu. (2014). Distributed estimation scheme based on cooperative communication in wireless sensor networks. IET Wirel. Sens. Syst, 4(4): 206-212.

[11] A. Bletsas, H. Shin, and M. Z. Win. (2007). Cooperative communications with outage-optimal opportunistic relaying. IEEE Trans. Wirel. Commun, 6: 3450-3460.

[12] J. N. Laneman, D. N. C. Tse, and G. W. Wornell. (2004). Cooperative diversity in wireless networks: efficient protocols and outage behavior. IEEE Trans. Inform. Theory, 50: 3062-3080.

[13] L. Lai and H. El Gamal. (2008). The relay-eavesdropper channel: Cooperation for secrecy. IEEE Trans. Inform. Theory, 54: 4005-4019.

[14] D. K. Sarker, M. Z. I. Sarkar and M. S. Anower. (2016). Wireless security in selection decode-and-forward relay networks. 2016 2nd International Conference on Electrical, Computer & Telecommunication Engineering (ICECTE), Rajshahi, 2016, pp. 1-4.

[15] I. Krikidis, J. Thompson, S. Mclaughlin. (2009). Relay selection for secure cooperative networks with jamming. IEEE Trans. Wirel. Commun, 8(10): 5003-5011.

[16] Y. Zhou, G. Pan, T. Li, H. Liu, C. Tang and Y. Chen. (2015). Secrecy outage performance for partial relay selection schemes in cooperative systems. IET Communications, 9(16): 1980-1987.

[17] T. Divya, K. K. Gurrala and S. Das. (2015). Performance analysis of hybrid decode-amplify-forward (HDAF) relaying for improving security

in cooperative wireless network. 2015 Global Conference on Communication Technologies (GCCT), Thuckalay, 2015, pp. 682-687.

[18] W. He, H. Lei, G. Pan. (2016). Performance analysis on conditional DF relaying schemes over Nakagami-m fading channels with integral m, AEÜ-International Journal of Electronics and Communications, 70(6): 743-749.

[19] G. Pan, C. Tang. (2017). Outage performance on threshold AF and DF relaying schemes in simultaneous wireless information and power transfer systems, AEÜ-International Journal of Electronics and Communications, 71(1): 175-180.

[20] D. D. Tran, N. S. Vo, T. L. Vo and D. B. Ha (2015). Physical layer secrecy performance of multi-hop decode-and-forward relay networks with multiple eavesdroppers. 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, Gwangiu, 2015, pp. 430-435.

[21] J. H. Lee. (2015). Cooperative relaying protocol for improving physical layer security in wireless decode-and-forward relaying networks. Wireless Personal Communications, 83(4): 3033-3044.

[22] P. Mangayarkarasi, R. Revathi, Dr. S. Jayashri. (2014). Secured power allocation for decode and forward relay in wireless relay networks. International Journal of Innovative Research in Science, Engineering and Technology. 3(1): 1611-1617.

[23] P. Adebo, E. Adebola and A. Annamalai. (2014). On the ergodic secrecy rate of cooperative decode-and-forward relay networks. 2014 IEEE Military Communications Conference, Baltimore, MD, 2014, pp. 1595-1600.

[24] N. Kolokotronis and M. Athanasakos. (2016). Improving physical layer security in DF relay networks via two-stage cooperative jamming. 2016 24th European Signal Processing Conference (EUSIPCO), Budapest, 2016, pp. 1173-1177.