RESEARCH

CrossMark

Secrecy outage of threshold-based cooperative relay network with and without direct links

Khyati Chopra[1*] iD, Ranjan Bose[1] and Anupam Joshi[2]

Abstract

In this paper, we investigate the secrecy outage performance of a dual-hop decode-and-forward (DF) threshold-based cooperative relay network, both with and without the direct links between source-eavesdropper and source-destination. Without assuming that all the relays can always perfectly decode, here we consider that only those relays who satisfy predetermined threshold can correctly decode the message. We have investigated the outage probability of optimal relay selection scheme, when either full instantaneous channel state information (ICSI) or statistical channel state information (SCSI) of all the links is available. We have shown that CSI knowledge at the transmitter can improve secrecy, and the amount of improvement for the outage probability is more when the required rate is low and for low operating SNR. Asymptotic and diversity gain analysis of the secrecy outage for both the single relay and multi-relay system is obtained, when average SNRs of source-relay and relay-destination links are equal or unequal. We have shown that the improvement in predetermined threshold, eavesdropper channel quality, direct links, and required secrecy rate significantly affects the secrecy performance of the system.

Keywords: Decode-forward relay, Dual-hop, Relay selection, Secrecy outage probability, Secrecy capacity, Threshold based

1 Introduction

Cooperative communication plays a promising role to expand the coverage of wireless networks, save uplink transmit power of source due to highly constrained wireless resources [1–3], and increase the spatial diversity without increasing the number of antennas [4]. Due to the broadcast nature of wireless medium, these cooperative networks are susceptible to eavesdropping, where the unintended receiver (eavesdropper) might overhear transmissions from the source and hence, can potentially cause great threat to secure wireless communication [1, 5]. Wireless security has traditionally relied on data encryption and decryption techniques at various layers, but key distribution becomes a major challenge in these cryptographic algorithms [6]. Recently, physical layer security (PLS) or information-theoretic security has emerged as an

alternate paradigm for secure wireless cooperative communications [3, 6]. This line of work was pioneered by Wyner [5], where he introduced the degraded wiretap channel (DWTC) model by exploiting the physical characteristics of wireless channels [1, 6] and defined the concept of secrecy capacity. A positive secrecy capacity can only be achieved when an eavesdropper's channel is a degraded version of the main (or legitimate) channel. A survey on PLS is presented in [7], with technical challenges and recent advances. Authors in [8] have investigated the PLS for a wireless ad hoc network with numerous eavesdroppers and legitimate transmitter-receiver pairs. The PLS for a spectrum-sharing system has been examined in [9], which consists of multiple source-destination pairs. Physical layer security for full duplex communications is discussed in [10], with self-interference mitigation.

Node cooperation is also introduced in PLS to improve the performance of secure communication by overcoming the wireless channel impairments [1, 2, 11]. Authors in [12] have investigated cooperative beamforming and user

*Correspondence: khyatichopra134@gmail.com
[1]Dept. of Electrical Engineering, Indian Institute of Technology, Delhi, New Delhi-110016, India
Full list of author information is available at the end of the article

Chopra *et al. EURASIP Journal on Information Security* (2018) 2018:7

Page 2 of 12

selection techniques to improve the security of a cooperative relaying network and have explored the concept of cooperative diversity gain, namely, adapted cooperative diversity gain (ACDG), which can be used to evaluate the security level. Authors in [11] have investigated secrecy outage of dual-hop amplify-and-forward (AF) relay system with relay selection without the knowledge of eavesdropper's instantaneous channel state information (ICSI). Authors in [13] have presented the secrecy outage probability of AF multi-antenna relay network in presence of an eavesdropper. Comprehensive study of secrecy transmission in decode-and-forward (DF) relay networks subjected to slow fading is presented in [3], and secrecy throughput of the two-hop transmission is maximized under secrecy outage constraint. Diversity is an effective technique to combat the performance degradation in wireless communication systems caused due to fading. Cooperative diversity is incorporated in a multi-path fading environment with the help of relay nodes, to improve the communication reliability and throughput [14]. Maximal ratio combining (MRC) and selection combining (SC) are two diversity combining techniques, where the relayed signal, as well as, the signal from the source are combined to obtain the diversity gain [14], and to enable higher transmission rates and robustness against channel variations due to fading.

Cooperative jamming is introduced in [6, 15] where, in order to confuse the eavesdroppers, the source transmits the encoded signal and weighted jamming signal is transmitted by relays. The optimal routing policy that minimizes the cost with secrecy outage probability constraint over multi-hop fading wiretap networks is discussed in [16]. Authors in [17] have investigated physical layer secrecy performance of multi-hop decode-and-forward relay networks with multiple passive eavesdroppers over Nakagami-m fading channels. Cooperative multicast scheme which allows the users to function as relays is presented in [18], and the secure outage behavior of this scheme is studied. Secrecy outage probability of multicast cooperative relay network is also studied in [19], in the presence of multi-destination and multi-eavesdropper nodes. Authors in [15] have discussed the outage probability and outage secrecy rate in wireless relay channels using cooperative jamming, assuming that the eavesdropper channels follow a zero-mean Gaussian distribution with known covariance. The problem of physical layer security in a large-scale multiple-input multiple-output (LSMIMO) relaying system is studied in [20], and the impact of imperfect channel state information (CSI) in AF and DF classical relaying schemes is also investigated. Secrecy performance of full-duplex relay (FDR) networks is explored in [21].

Relay selection schemes are introduced based on ICSI to improve the diversity gain in secure cooperative multi-relay system [1, 2, 22]. The combined use of relays and jamming for AF and DF protocols [1, 6] to improve security has also been addressed extensively by authors in [2]. For secure communication in DF relay networks, outage optimal relay selection strategy using destination-based jamming is discussed in [6]. Authors in [23] have studied the impact of both maximal ratio combining and relay selection on the physical layer security in wireless communication systems over Rayleigh fading channel. The average secrecy rate was analyzed in [24] for the optimal relay selection scheme in DF relaying systems. Authors in [25] have investigated secrecy outage performance for partial relay selection schemes in cooperative systems. Authors in [26] have analyzed the secrecy outage performance of underlay cognitive radio networks with optimal relay selection over Nakagami-m fading channels. Secrecy performance of threshold-based DF cooperative cognitive networks is extensively discussed in [27], with optimal relay selection scheme. The opportunistic relay selection schemes were proposed in [2, 28, 29] taking into account the quality of relay-eavesdropper links, and it was demonstrated that the proposed relay selection schemes can significantly improve the secrecy outage probability. Single opportunistic relay selection scheme, which selects the relay that maximizes the system secrecy capacity for secure communication, in a cooperative system with multiple full-duplex decode-and-forward relays is presented in [30]. The PLS problem of cognitive DF relay networks is presented in [31], for Nakagami-m fading channels by using an opportunistic relay selection. Beamforming scheme with opportunistic relaying for wireless security under AF and DF strategies have been discussed in [32].

In most of the prior works, neither threshold-based relaying nor direct link between source-eavesdropper and source-destination is taken into account [1, 2, 6, 22, 29]. However, due to the broadcast nature of wireless medium, the direct link is likely to exist in practice. Hence, in contrast to the above study, our work investigates the secrecy outage for a dual-hop threshold-based cooperative DF relay network, both with and without the direct link between source-eavesdropper and source-destination. Also, threshold-based relaying is taken into account, where without assuming that all the relays can always perfectly decode, we consider that only those relays who meets predetermined threshold can correctly decode the message [27]. We have used DF protocol instead of AF in our study for the secrecy performance analysis of dual-hop threshold-based cooperative relay system. The study on DF and AF protocols has been done in the prior literature [33–35]. In comparison to AF, the bit error rate (BER) performance of DF scheme is better [33–35]. On the other hand, AF relaying technique is much simpler as compared to DF, as the complexity of a DF scheme is significantly higher due to its full processing

Chopra *et al. EURASIP Journal on Information Security* (2018) 2018:7

Page 3 of 12

capability [33–35]. Since we have considered threshold-based relaying in our paper, DF protocol is employed, such that the relay first decodes the source message, then compares it with the required threshold, and only if the threshold is met, the message is correctly decoded and forwarded by the relay node. AF protocol is not applicable for threshold-based schemes.

The main contributions of our study are summarized as follows:

- Outage probability analysis of the cooperative threshold-based DF relay system is presented without assuming that all the relays can always correctly decode. We have shown that the secrecy outage performance can be affected by link quality of both source-relay and relay-destination.
- Without assuming that the direct transmissions are absent owing to deep shadow fading or large distance between nodes, the expression for secrecy outage of DF threshold-based cooperative relay network is derived, both with and without the direct link between source-eavesdropper and source-destination.
- We have shown that the improvement in predetermined threshold, eavesdropper channel quality, and required secrecy rate significantly affects the outage performance of the system.
- Secrecy outage probability is evaluated for optimal relay selection scheme, when either ICSI or SCSI is known for cooperative DF threshold-based dual-hop relay system.
- We have shown that CSI knowledge at the transmitter can improve secrecy, and the amount of improvement for the outage probability is more when the required rate is low and for low operating SNR.
- Asymptotic and diversity gain analysis of the secrecy outage for both the single relay and multi-relay cooperative system with optimal relay selection is obtained, when average SNRs of source-relay and relay-destination links are equal or unequal.

The remainder of this study is organized as follows. The system model is described in Section 2. Outage probability expressions are evaluated for threshold-based single cooperative relay system, both with and without direct link in Section 3. In Section 4, outage probability is studied for optimal relay selection scheme. Asymptotic and diversity gain analysis is presented in Section 5. In Section 6, numerical results are discussed and finally, we conclude this study in Section 7.

2 System model
We consider the system model, consisting of a source S, a destination D, an eavesdropper E and N number of DF

relays R_i, $i \in [1, 2.., N]$ which work in a dual-hop mode as depicted in the Fig. 1. We assume there is also a direct $S - D$ and $S - E$ link due to the broadcast nature of wireless medium, and the communication takes place with the help of a single cooperative relay. We have derived the expression for secrecy outage probability of this dual-hop DF threshold-based cooperative relay network, both with and without the direct link between source-eavesdropper and source-destination. Threshold-based relaying is taken into account, where without assuming that the relay can always perfectly decode, we consider that only if the the received SNR at the relay meets predetermined threshold, illustrated as γ-th for $S - R_i$ link, it can correctly decode the message from the source [27, 36]. When none of the relays could perfectly decode the message from source, i.e, all relays have $S - R_i$ link SNR lower than the threshold, then, only direct communication between $S - D$ and $S - E$ takes place. The links between various nodes works in half-duplex mode and are modeled as flat Rayleigh flat fading channels, which are mutually independent but not identical [2, 22].

The SNR between any two arbitrary nodes a and b, denoted as Γ_{ab}, is given by [36]

$$\Gamma_{ab} = \frac{P_a |h_{ab}|^2}{N_{0_b}}, \tag{1}$$

where P_a is the transmitted power at node a, N_{0_b} is the noise variance of the additive white Gaussian noise (AWGN) at b. As h_{ab} is Rayleigh distributed, Γ_{ab} is exponentially distributed with mean $1/\beta_{ab}$ [37], expressed as $\Gamma_{ab} \sim \mathcal{E}(\beta_{ab})$, where β_{ab} is the parameter of the exponentially distribution.

For the random variable Z, which is exponentially distributed with parameter β_{ab}, the CDF is given as

$$\begin{aligned} F_Z(z) &= \mathbb{P}[Z \le z] \\ &= 1 - e^{-z\beta_{ab}}, \end{aligned} \tag{2}$$
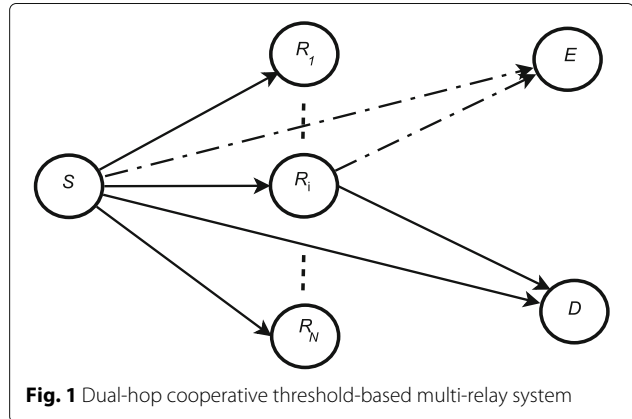

Fig. 1 Dual-hop cooperative threshold-based multi-relay system

Chopra *et al. EURASIP Journal on Information Security* (2018) 2018:7

Page 4 of 12

and the corresponding PDF is obtained by differentiating (2) with respect to z as

$$f_Z(z) = \beta_{ab} e^{-z\beta_{ab}}. \tag{3}$$

For MRC, the random variable Z is the sum of two random variables A and B, i.e., $Z = A + B$ where A and B are exponentially distributed with parameters β_{ab} and $\beta_{a'b'}$, the CDF is given as

$$\begin{aligned}
F_Z(z) &= \mathbb{P}[A + B \leq z] \\
&= \mathbb{P}[A \leq z - B] \\
&= 1 - \frac{\beta_{a'b'} e^{-z\beta_{ab}}}{\beta_{a'b'} - \beta_{ab}} - \frac{\beta_{ab} e^{-z\beta_{a'b'}}}{\beta_{ab} - \beta_{a'b'}},
\end{aligned} \tag{4}$$

and the corresponding PDF is obtained by differentiating (4) with respect to z as

$$f_Z(z) = \frac{\beta_{a'b'}\beta_{ab} e^{-z\beta_{ab}}}{\beta_{a'b'} - \beta_{ab}} + \frac{\beta_{ab}\beta_{a'b'} e^{-z\beta_{a'b'}}}{\beta_{ab} - \beta_{a'b'}}. \tag{5}$$

The $S - R_i$ channels h_{sr_i}, $R_i - D$ channels h_{r_id}, $R_i - E$ channels h_{r_ie}, $S - D$ channels h_{sd}, and $S - E$ channels h_{se}, $\forall i \in [1, 2.., N]$, are slowly varying Rayleigh flat fading channels [38]. Let P_s and P_{r_i} denote the average powers used at source and relay R_i, respectively. Also, let N_{sr_i}, N_{r_id}, N_{r_ie}, N_{sd}, and N_{se} denote the variances of additive white Gaussian noise of $S - R_i$, $R_i - D$, $R_i - E$, $S - D$ and $S - E$ links, respectively. The SNRs Γ_{sr_i}, Γ_{r_id}, Γ_{r_ie}, Γ_{sd} and Γ_{se} are exponentially distributed given as $\Gamma_{sr_i} = \frac{P_s|h_{sr_i}|^2}{N_{sr_i}}$, $\Gamma_{r_id} = \frac{P_{r_i}|h_{r_id}|^2}{N_{r_id}}$, $\Gamma_{r_ie} = \frac{P_{r_i}|h_{r_ie}|^2}{N_{r_ie}}$, $\Gamma_{sd} = \frac{P_s|h_{sd}|^2}{N_{sd}}$ and $\Gamma_{se} = \frac{P_s|h_{se}|^2}{N_{se}}$ with average values $1/\beta_{sr_i}$, $1/\beta_{r_id}$, $1/\alpha_{r_ie}$, $1/\beta_{sd}$, and $1/\alpha_{se}$, respectively where β_{sr_i}, β_{r_id}, α_{r_ie}, β_{sd}, and α_{se} are the parameters of the exponential distribution. An outage event occurs when the instantaneous secrecy rate is lower than the required secrecy rate of the cooperative relay system, given as R_s where, $R_s > 0$ and $\rho = 2^{2R_s}$ [6, 22, 27]. We have used ρ for direct mapping of required secrecy rate R_s, and the probability of successful occurrence of this outage event is called outage probability P_o, which is a key metric in evaluating the performance of physical-layer security [38].

The achievable secrecy rate is the difference between the capacity of main link and that of wiretap link [1, 5, 38]

$$C_s^d \triangleq \frac{1}{2}\left[\log_2\left(\frac{1 + \Gamma_M^d}{1 + \Gamma_E^d}\right)\right]^+ \tag{6}$$

where C_s^d is the secrecy capacity when both $S-D$ and $S-E$ direct link exists, $\Gamma_M^d = \Gamma_{r_id} + \Gamma_{sd}$ is the maximal ratio combined SNR of the main link at D and $\Gamma_E^d = \Gamma_{r_ie} + \Gamma_{se}$ is the maximal ratio combined SNR of the eavesdropper link at E. The term $1/2$ here denotes that to complete this dual-

hop transmission process, two time phase are required. The message transmitted by the source is decoded at the relay, whose threshold is satisfied in the first phase. In the second phase, one of the relay is selected to re-encode and forward the message to the destination. From (6), when the relay node does not meet the predetermined threshold due to shadow fading [39], the secrecy capacity is defined as $C_s^{d'}$ where $\Gamma_M^{d'} = \Gamma_{sd}$ is the combined SNR of the main link at D, and $\Gamma_E^{d'} = \Gamma_{se}$ is the SNR of the eavesdropper link at E.

We have investigated three scenarios in our study where first is when the direct link between both source-eavesdropper and source-destination exists, as discussed above. The second is when the direct link only between S and E is considered assuming that the direct link between S and D is absent owing to deep shadow fading or large distance between nodes. From (6), when the relay node meets the predetermined threshold, the secrecy capacity is defined as C_s^{se} where $\Gamma_M^{se} = \Gamma_{r_id}$ is the SNR of the main link at D, and $\Gamma_E^{se} = \Gamma_{r_ie} + \Gamma_{se}$ is the maximal ratio combined SNR of the eavesdropper link at E and when the relay node does not meet the predetermined threshold due to shadow fading [39], the secrecy capacity is defined as $C_s^{se'}$, where only direct link between source-eavesdropper exists and $\Gamma_E^{se'} = \Gamma_{se}$ is the SNR of the eavesdropper link at E.

The third scenario is when no direct link between $S - D$ and $S - E$ is considered assuming that the direct links between $S-D$ and $S-E$ are absent owing to deep shadow fading or large distance between nodes [1, 2, 22]. From (6), when the relay node meets the predetermined threshold, the secrecy capacity is defined as C_s^{nd} where $\Gamma_M^{nd} = \Gamma_{r_id}$ is the SNR of the main link at D, and $\Gamma_E^{nd} = \Gamma_{r_ie}$ is the SNR of the eavesdropper link at E and when the relay node does not meet the predetermined threshold due to shadow fading [39], no relay is selected for communication.

3 Secrecy outage probability analysis of single relay system

This section deals with the evaluation of the expression for secrecy outage probability of DF threshold-based dual-hop cooperative relay network, in the three scenarios discussed in our study. Each scenario is divided into two probabilistic instances where in the first instance, we consider that the message is decoded successfully [28, 29], as the SNR at the relay node satisfies the predetermined threshold while, in the second instance we consider that the SNR at the relay node does not meet the predetermined threshold.

3.1 Direct link between both $S - D$ and $S - E$
We evaluate outage probability for single ith relay in the first scenario where the direct link between both $S-D$ and $S - E$ exists as

$$P_o^i(R_s)$$
$$= \mathbb{P}\left[C_s^d < R_s | \Gamma_{sr_i} \geq \gamma_{\text{th}}\right] \mathbb{P}\left[\Gamma_{sr_i} \geq \gamma_{\text{th}}\right]$$
$$+ \mathbb{P}\left[C_s^{d'} < R_s | \Gamma_{sr_i} < \gamma_{\text{th}}\right] \mathbb{P}\left[\Gamma_{sr_i} < \gamma_{\text{th}}\right]$$
$$= \mathbb{P}\left[\frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_M^d}{1+\Gamma_E^d}\right)\right] < R_s \mid \Gamma_{sr_i} \geq \gamma_{\text{th}}\right]$$
$$\times \mathbb{P}\left[\Gamma_{sr_i} \geq \gamma_{\text{th}}\right] + \mathbb{P}\left[\frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_M^{d'}}{1+\Gamma_E^{d'}}\right)\right] < R_s \mid \Gamma_{sr_i} < \gamma_{\text{th}}\right]$$
$$\times \mathbb{P}\left[\Gamma_{sr_i} < \gamma_{\text{th}}\right]$$
$$= \mathbb{P}[\underbrace{(\Gamma_{r_id} + \Gamma_{sd})}_{\text{MRC}} < (\rho-1) + \rho\underbrace{(\Gamma_{r_ie} + \Gamma_{se})}_{\text{MRC}} | \Gamma_{sr_i} \geq \gamma_{\text{th}}]\left(e^{-\gamma_{\text{th}}\beta_{sr_i}}\right)$$
$$+ \mathbb{P}[\Gamma_{sd} < (\rho-1) + \rho\Gamma_{se} | \Gamma_{sr_i} < \gamma_{\text{th}}]\left(1 - e^{-\gamma_{\text{th}}\beta_{sr_i}}\right) \tag{7}$$

By substituting the PDF and CDF of MRC diversity scheme from (4) and (5) in (7) and after some algebraic simplifications, the outage probability expression is obtained as

$$P_o^i(R_s) = \left(1 - \frac{e^{-(\rho-1)\beta_{r_id}}\beta_{sd}\alpha_{r_ie}\alpha_{se}}{(\beta_{sd}-\beta_{r_id})(\alpha_{se}-\alpha_{r_ie})(\rho\beta_{r_id}+\alpha_{r_ie})}\right.$$
$$- \frac{e^{-(\rho-1)\beta_{sd}}\beta_{r_id}\alpha_{r_ie}\alpha_{se}}{(\beta_{r_id}-\beta_{sd})(\alpha_{se}-\alpha_{r_ie})(\rho\beta_{sd}+\alpha_{r_ie})}$$
$$- \frac{e^{-(\rho-1)\beta_{r_id}}\beta_{sd}\alpha_{r_ie}\alpha_{se}}{(\beta_{sd}-\beta_{r_id})(\alpha_{r_ie}-\alpha_{se})(\rho\beta_{r_id}+\alpha_{se})}$$
$$\left. - \frac{e^{-(\rho-1)\beta_{sd}}\beta_{r_id}\alpha_{r_ie}\alpha_{se}}{(\beta_{r_id}-\beta_{sd})(\alpha_{r_ie}-\alpha_{se})(\rho\beta_{sd}+\alpha_{se})}\right)\left(e^{-\gamma_{\text{th}}\beta_{sr_i}}\right)$$
$$+ \left(1 - e^{-\gamma_{\text{th}}\beta_{sr_i}}\right)\left(1 - \frac{\alpha_{se}e^{-\beta_{sd}(\rho-1)}}{\rho\beta_{sd}+\alpha_{se}}\right). \tag{8}$$

3.2 Direct link only between *S* and *E*
We evaluate outage probability for single *i*th relay in the second scenario where only the direct link between *S* and *E* exists as

$$P_o^i(R_s) = \mathbb{P}\left[C_s^{se} < R_s | \Gamma_{sr_i} \geq \gamma_{\text{th}}\right] \mathbb{P}[\Gamma_{sr_i} \geq \gamma_{\text{th}}]$$
$$+ \mathbb{P}\left[C_s^{se'} < R_s | \Gamma_{sr_i} < \gamma_{\text{th}}\right] \mathbb{P}\left[\Gamma_{sr_i} < \gamma_{\text{th}}\right]$$
$$= \mathbb{P}\left[\frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_M^{se}}{1+\Gamma_E^{se}}\right)\right] < R_s \mid \Gamma_{sr_i} \geq \gamma_{\text{th}}\right] \times$$
$$\mathbb{P}\left[\Gamma_{sr_i} \geq \gamma_{\text{th}}\right] + \mathbb{P}\left[\frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_M^{se'}}{1+\Gamma_E^{se'}}\right)\right] < R_s \mid \Gamma_{sr_i} < \gamma_{\text{th}}\right]$$
$$\times \mathbb{P}\left[\Gamma_{sr_i} < \gamma_{\text{th}}\right]$$
$$= \mathbb{P}[(\Gamma_{r_id}) < (\rho-1) + \rho\underbrace{(\Gamma_{r_ie} + \Gamma_{se})}_{\text{MRC}} | \Gamma_{sr_i} \geq \gamma_{\text{th}}]\left(e^{-\gamma_{\text{th}}\beta_{sr_i}}\right)$$
$$+ \left(1 - e^{-\gamma_{\text{th}}\beta_{sr_i}}\right) \tag{9}$$

By substituting the PDF and CDF of MRC diversity scheme from (4) and (5) in (9) and after some algebraic simplifications, the outage probability expression is obtained as

$$P_o^i(R_s) = \left(1 - \frac{e^{-(\rho-1)\beta_{r_id}}\alpha_{r_ie}\alpha_{se}}{(\alpha_{se}-\alpha_{r_ie})(\rho\beta_{r_id}+\alpha_{r_ie})} - \frac{e^{-(\rho-1)\beta_{r_id}}\alpha_{r_ie}\alpha_{se}}{(\alpha_{r_ie}-\alpha_{se})(\rho\beta_{r_id}+\alpha_{se})}\right)$$
$$\times \left(e^{-\gamma_{\text{th}}\beta_{sr_i}}\right) + \left(1 - e^{-\gamma_{\text{th}}\beta_{sr_i}}\right) \tag{10}$$

3.3 No direct link between both *S − D* and *S − E*
We have evaluated the outage probability of a threshold-based DF relaying system without any direct links for the two cases. The two cases discussed in this section are as follows. In the first case, no CSI knowledge is available at the transmitter. The transmission rate cannot thus be adapted by the transmitter to get the positive secrecy. The condition of positive secrecy, i.e., $\Gamma_M > \Gamma_E$ is not imposed in this case and $P_o^i(R_s)$ evaluation is independent of CSI. In the second case, CSI is completely known at the transmitter. The transmission rate can thus be adapted by the transmitter to get the positive secrecy. When CSI knowledge is available at the transmitter, the condition of positive secrecy, i.e., $\Gamma_M > \Gamma_E$ is imposed while evaluating the $P_o^i(R_s)$ for cooperative system. Usually, through a feedback link from the receiver to the transmitter, there can be the availability of channel information for a particular link at the transmitter. However, this feedback channel has to be of high-capacity, which cannot be always maintained. Each case is further divided into two probabilistic instances. The relay can decode correctly in the first instance, as the predetermined threshold SNR is achieved [27]. The predetermined threshold SNR is not achieved in the second instance by the relay, and thus the source information is not forwarded [27]. When $\Gamma_{sr_i} < \gamma_{\text{th}}$, the $P_o^i(R_s)$ becomes unity; irrespective of the full CSI knowledge available at the transmitter or not, i.e., $\mathbb{P}\left[C_s < R_s \cap \Gamma_M > \Gamma_E | \Gamma_{sr_i} < \gamma_{\text{th}}\right] = 1$.

3.3.1 No knowledge of CSI at transmitter
We evaluate outage probability for single *i*th relay in the third scenario where, no direct link between $S − D$ and $S − E$ exists and full CSI knowledge is not available at the transmitter

$$P_o^i(R_s) = \mathbb{P}\left[C_s^{nd} < R_s | \Gamma_{sr_i} \geq \gamma_{\text{th}}\right] \mathbb{P}[\Gamma_{sr_i} \geq \gamma_{\text{th}}]$$
$$+ \mathbb{P}\left[C_s^{nd'} < R_s | \Gamma_{sr_i} < \gamma_{\text{th}}\right] \mathbb{P}\left[\Gamma_{sr_i} < \gamma_{\text{th}}\right]$$
$$= \mathbb{P}\left[\frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_M^{nd}}{1+\Gamma_E^{nd}}\right)\right] < R_s \mid \Gamma_{sr_i} \geq \gamma_{\text{th}}\right]$$
$$\times \mathbb{P}\left[\Gamma_{sr_i} \geq \gamma_{\text{th}}\right] + \mathbb{P}\left[\Gamma_{sr_i} < \gamma_{\text{th}}\right]$$
$$= \mathbb{P}[(\Gamma_{r_id}) < (\rho-1) + \rho(\Gamma_{r_ie}) | \Gamma_{sr_i} \geq \gamma_{\text{th}}]\left(e^{-\gamma_{\text{th}}\beta_{sr_i}}\right)$$
$$+ \left(1 - e^{-\gamma_{\text{th}}\beta_{sr_i}}\right)$$
$$= \left(e^{-\gamma_{\text{th}}\beta_{sr_i}}\right)\left(1 - \frac{\alpha_{r_ie}e^{-\beta_{r_id}(\rho-1)}}{\rho\beta_{r_id}+\alpha_{r_ie}}\right)$$
$$+ \left(1 - e^{-\gamma_{\text{th}}\beta_{sr_i}}\right) \tag{11}$$

3.3.2 CSI completely known at transmitter

We evaluate outage probability for single ith relay in the third scenario where no direct link between $S - D$ and $S - E$ exists, and full CSI knowledge is available at the transmitter as

$$
\begin{aligned}
P_o^i(R_s) &= \mathbb{P}\left[C_s^{nd} < R_s \cap \Gamma_M > \Gamma_E | \Gamma_{sr_i} \geq \gamma_{\text{th}} \right] \mathbb{P}\left[\Gamma_{sr_i} \geq \gamma_{\text{th}} \right] \\
&\quad + \mathbb{P}\left[C_s^{nd'} < R_s \cap \Gamma_M > \Gamma_E | \Gamma_{sr_i} < \gamma_{\text{th}} \right] \mathbb{P}\left[\Gamma_{sr_i} < \gamma_{\text{th}} \right] \\
&= \mathbb{P}\left[\frac{1}{2} \left[\log_2\left(\frac{1 + \Gamma_M^{nd}}{1 + \Gamma_E^{nd}} \right) \right] < R_s \cap \Gamma_M > \Gamma_E \mid \Gamma_{sr_i} \geq \gamma_{\text{th}} \right] \\
&\quad \times \mathbb{P}\left[\Gamma_{sr_i} \geq \gamma_{\text{th}} \right] + \mathbb{P}\left[\Gamma_{sr_i} < \gamma_{\text{th}} \right] \\
&= \mathbb{P}[(\Gamma_{r_i d}) < (\rho - 1) + \rho (\Gamma_{r_i e}) \cap \Gamma_M > \Gamma_E | \Gamma_{sr_i} \geq \gamma_{\text{th}}] \left(e^{-\gamma_{\text{th}} \beta_{sr_i}} \right) \\
&\quad + \left(1 - e^{-\gamma_{\text{th}} \beta_{sr_i}} \right) \\
&= \left(e^{-\gamma_{\text{th}} \beta_{sr_i}} \right) \left(\frac{\alpha_{r_i e}}{\beta_{r_i d} + \alpha_{r_i e}} - \frac{\alpha_{r_i e} e^{-\beta_{r_i d}(\rho - 1)}}{\rho \beta_{r_i d} + \alpha_{r_i e}} \right) \\
&\quad + \left(1 - e^{-\gamma_{\text{th}} \beta_{sr_i}} \right)
\end{aligned}
\tag{12}
$$

In contrast to the prior literature, where the direct link between the source-eavesdropper and source-destination is not taken into account [1, 2, 22], we have derived the expression for secrecy outage probability of DF threshold-based dual-hop cooperative relay network, both with and without the direct link between source-eavesdropper and source-destination as discussed in our study.

4 Secrecy outage analysis of relay selection scheme

In this section, the secrecy outage probability analysis of optimal relay selection (OS) scheme for dual-hop threshold-based DF cooperative multi-relay system is presented, under the no direct link scenario [27].

4.1 Optimal selection: ICSI of all the links is known

In the optimal relay selection scheme for cooperative multi-relay system [22, 29], the relay that maximizes the secrecy capacity of system is selected to forward the source data. In this case, ICSI of all the links is available. The relay is taken to be selected if predetermined threshold is satisfied, and P is taken as the number of relays which are selected. When the predetermined threshold is not satisfied, the relay is not selected and Q is taken as the number of relays which are not selected. The probability that the maximum of some independent random variable is less than some quantity, is the probability that all the independent random variables are less than that quantity [27]. The final summation is done over the set S, where S is the set of all possible combinations of relay $i \in [1, 2.., N]$. Considering the fact that an outage event occurs when the secrecy capacity becomes less than the desired secrecy rate R_s, we can evaluate the outage probability of this OS scheme in the third scenario where no direct link between

$S - D$ and $S - E$ exists and full CSI knowledge is not available at the transmitter as

$$
\begin{aligned}
P_o^{OS}(R_s) &= \sum_S \left[\left(\prod_{\substack{\forall i \in [1,P] \\ \text{selected}}} \mathbb{P}[\Gamma_{sr_i} \geq \gamma_{\text{th}}] \right) \left(\prod_{\substack{\forall j \in [1,Q] \\ \text{not selected}}} \mathbb{P}[\Gamma_{sr_j} < \gamma_{\text{th}}] \right) \right. \\
&\quad \left. \times \mathbb{P}\left[\max_{\substack{\forall i \in [1,P] \\ \text{selected}}} \{C_s\} < R_s | \Gamma_{sr_i} \geq \gamma_{\text{th}} \right] \right] \\
&= \sum_S \left[\left(\prod_{i=1}^{P} \left(e^{-\gamma_{\text{th}} \beta_{sr_i}} \right) \right) \left(\prod_{j=1}^{Q} \left(1 - e^{-\gamma_{\text{th}} \beta_{sr_j}} \right) \right) \right. \\
&\quad \left. \times \prod_{i=1}^{P} \mathbb{P}\left[C_s < R_s | \Gamma_{sr_i} \geq \gamma_{\text{th}} \right] \right] \\
&= \sum_S \left[\left(\prod_{i=1}^{P} \left(e^{-\gamma_{\text{th}} \beta_{sr_i}} \right) \right) \left(\prod_{j=1}^{Q} \left(1 - e^{-\gamma_{\text{th}} \beta_{sr_j}} \right) \right) \right. \\
&\quad \left. \times \prod_{i=1}^{P} \left(1 - \frac{\alpha_{r_i e} e^{-\beta_{r_i d}(\rho - 1)}}{\rho \beta_{r_i d} + \alpha_{r_i e}} \right) \right]
\end{aligned}
\tag{13}
$$

Similarly, we can also evaluate the outage probability of this OS scheme in the third scenario where no direct link between $S - D$ and $S - E$ exists and full CSI knowledge is available at the transmitter as

$$
\begin{aligned}
P_o^{OS}(R_s) &= \sum_S \left[\left(\prod_{i=1}^{P} \left(e^{-\gamma_{\text{th}} \beta_{sr_i}} \right) \right) \left(\prod_{j=1}^{Q} \left(1 - e^{-\gamma_{\text{th}} \beta_{sr_j}} \right) \right) \right. \\
&\quad \left. \times \prod_{i=1}^{P} \left(\frac{\alpha_{r_i e}}{\beta_{r_i d} + \alpha_{r_i e}} - \frac{\alpha_{r_i e} e^{-\beta_{r_i d}(\rho - 1)}}{\rho \beta_{r_i d} + \alpha_{r_i e}} \right) \right]
\end{aligned}
\tag{14}
$$

4.2 Optimal selection: SCSI of all the links is known

We have examined another relay selection scheme where no knowledge of instantaneous channel state information is required [22, 27]. This relay selection method has been proposed in [22], and it requires only the statistical information of all the links for secrecy outage probability measurement. This relay selection method is the optimal one, only when no knowledge of ICSI is available except statistical information. In this scheme, the relay for which the secrecy outage probability of system becomes minimum is selected [22]. The secrecy outage probabilities, $P_o^i(R_s)$ of all the individual single relay systems can be first measured, and then we can find the optimal relay i^* [22].

It can be expressed mathematically as

$$
i^* = \arg \min_{i \in [1, \cdots, N]} \left(P_o^i(R_s) \right).
\tag{15}
$$

Since ICSI is not required, power consumption is reduced as no complex channel measurements are necessary. Compared to the ICSI, channel statistics does not considerably change over time and thus, this is a one-time process. Under severe resource constraint like power and computational complexity, this selection scheme can improve the secrecy performance [22]. The

Chopra *et al. EURASIP Journal on Information Security* (2018) 2018:7

Page 7 of 12

performance of optimal relay selection scheme will be better, as improvement is achieved by utilizing the knowledge of ICSI of the system in OS scheme [22], while only SCSI of the system is available for this scheme. This scheme can be useful in the networks, where there is no availability of CSI of the eavesdropper at all the time instants and due to power limitations, the ICSI of other nodes cannot be fed back at all instants to the decision making node.

5 Asymptotic and diversity analysis

In this section, asymptotic and diversity analysis of dual-hop threshold-based DF cooperative relay network is presented, under the scenario when there is no direct link between both $S - D$ and $S - E$. When link SNRs of $S - R_i$ and or $R_i - D$ are asymptotically increased in comparison to eavesdropper's link, the behavior of secrecy outage becomes important for the system design. We have discussed the following two significant cases: (1) when $S - R_i$ and $R_i - D$ link average SNRs are equal, for all i, and they together tends to infinity, i.e., $1/\beta_{sr_i} = 1/\beta_{r_id} = 1/\beta \to \infty$, it is called as balanced case, and (2) when either of the $S - R_i$ or $R_i - D$ for all i, link average SNR tends to infinity, i.e., $1/\beta_{sr_i}$ is fixed and $1/\beta_{r_id} = 1/\beta \to \infty$ or $1/\beta_{r_id}$ is fixed and $1/\beta_{sr_i} = 1/\beta \to \infty$, it is called as unbalanced case [22, 27].

5.1 Single balanced relay case

The $P_o^i(R_s)$ for single DF relaying system is evaluated, both when full CSI knowledge is not available and when available at the transmitter.

5.1.1 No knowledge of CSI at transmitter

For the balanced case, when $1/\beta_{sr_i} = 1/\beta_{r_id} = 1/\beta \to \infty$, the $P_o^i(R_s)$ for single DF relaying balanced system without CSI knowledge at the transmitter in (11) is expressed as

$$
\begin{aligned}
P_o^i(R_s) &= \frac{\beta_{r_id}\left(\rho + \alpha_{r_ie}(\rho - 1)\right)}{\alpha_{r_ie}} + \gamma_{\text{th}}\beta_{sr_i} \\
&= \beta\left[\frac{\rho + \alpha_{r_ie}(\rho - 1)}{\alpha_{r_ie}} + \gamma_{\text{th}}\right] \\
&= \frac{1}{\frac{1}{\beta}}\left[\frac{\rho}{\alpha_{r_ie}} + (\rho - 1) + \gamma_{\text{th}}\right]
\end{aligned} \tag{16}
$$

5.1.2 CSI completely known at transmitter

For the balanced case, when $1/\beta_{sr_i} = 1/\beta_{r_id} = 1/\beta \to \infty$, the $P_o^i(R_s)$ for single DF relaying balanced system with CSI knowledge at the transmitter in (12) is expressed as

$$
\begin{aligned}
P_o^i(R_s) &= \frac{\beta_{r_id}\left((\rho - 1) + \alpha_{r_ie}(\rho - 1)\right)}{\alpha_{r_ie}} + \gamma_{\text{th}}\beta_{sr_i} \\
&= \beta\left[\frac{(\rho - 1) + \alpha_{r_ie}(\rho - 1)}{\alpha_{r_ie}} + \gamma_{\text{th}}\right] \\
&= \frac{1}{\frac{1}{\beta}}\left[\frac{(\rho - 1)}{\alpha_{r_ie}} + (\rho - 1) + \gamma_{\text{th}}\right]
\end{aligned} \tag{17}
$$

We can interpret from (16) and (17) that secrecy outage probability is inversely proportional to $1/\beta$ and it tends

to zero, when main channel SNR $(1/\beta)$ tends to infinity. It is directly proportional to the required threshold γ_{th}, eavesdropper channel SNR $(1/\alpha_{r_ie})$, and desired secrecy rate R_s.

Diversity order is a critical measure to observe how fast the outage probability decreases when SNR tends to infinity. Hence, the effect of the increase in number of relays on the outage probability can also be intuitively understood. The diversity order [1] can be defined as

$$
D = -\lim_{\text{SNR}\to\infty} \frac{\log P_o(\text{SNR})}{\log(\text{SNR})}, \tag{18}
$$

where $P_o(\text{SNR})$ is the secrecy outage probability given by function of $\text{SNR} = 1/\beta$. We can show that using this definition, diversity order of (16) and (17) can be obtained as one. The power of SNR in the denominator of (16) and (17) is same as the diversity order D. It is also depicted by the slope of curve in the log graph. As there is no relay selection, it is intuitive that diversity order of one is achieved by this single cooperative relay system.

5.2 Single unbalanced relay case

The behavior of outage probability is studied for this unbalanced case, both when full CSI knowledge is not available and when available at the transmitter.

5.2.1 No knowledge of CSI at transmitter

The $P_o^i(R_s)$ is evaluated by asymptotically increasing the average SNR of the $R_i - D$ link and keeping the average SNR of the $S - R_i$ link fixed, i.e., when $1/\beta_{sr_i}$ is fixed and $1/\beta_{r_id} = 1/\beta \to \infty$. The $P_o^i(R_s)$ for single DF relaying unbalanced system without CSI knowledge at the transmitter in (11) is expressed as

$$
P_o^i(R_s) = \left[1 - e^{-\gamma_{\text{th}}\beta_{sr_i}}\right] + \frac{1}{\frac{1}{\beta}}\left[\frac{e^{-\gamma_{\text{th}}\beta_{sr_i}}\left(\rho + (\rho - 1)\alpha_{r_ie}\right)}{\alpha_{r_ie}}\right] \tag{19}
$$

Also, the behavior of outage probability is studied by asymptotically increasing the average SNR of the $S - R_i$ link and keeping the average SNR of the $R_i - D$ link fixed, i.e., when $1/\beta_{r_id}$ is fixed and $1/\beta_{sr_i} = 1/\beta \to \infty$. The $P_o^i(R_s)$ is given as

$$
P_o^i(R_s) = \left[1 - \frac{\alpha_{r_ie}e^{-\beta_{r_id}(\rho - 1)}}{\rho\beta_{r_id} + \alpha_{r_ie}}\right] + \frac{1}{\frac{1}{\beta}}\left[\frac{\gamma_{\text{th}}\alpha_{r_ie}e^{-\beta_{r_id}(\rho - 1)}}{\rho\beta_{r_id} + \alpha_{r_ie}}\right] \tag{20}
$$

5.2.2 CSI completely known at transmitter

The $P_o^i(R_s)$ is evaluated by asymptotically increasing the average SNR of the $R_i - D$ link and keeping the average SNR of the $S - R_i$ link fixed, i.e., when $1/\beta_{sr_i}$ is fixed and $1/\beta_{r_id} = 1/\beta \to \infty$. The $P_o^i(R_s)$ for single DF relaying unbalanced system with CSI knowledge at the transmitter in (12) is expressed as

$$
P_o^i(R_s) = \left[1 - e^{-\gamma_{\text{th}}\beta_{sr_i}}\right] + \frac{1}{\frac{1}{\beta}}\left[\frac{e^{-\gamma_{\text{th}}\beta_{sr_i}}\left((\rho - 1) + (\rho - 1)\alpha_{r_ie}\right)}{\alpha_{r_ie}}\right] \tag{21}
$$

Chopra *et al. EURASIP Journal on Information Security*   (2018) 2018:7

Page 8 of 12

Also, the behavior of outage probability is studied by asymptotically increasing the average SNR of the $S-R_i$ link and keeping the average SNR of the $R_i - D$ link fixed, i.e., when $1/\beta_{r_id}$ is fixed and $1/\beta_{sr_i} = 1/\beta \to \infty$. The $P_o^i(R_s)$ is given as

$$P_o^i(R_s) = \left[\frac{\alpha_{r_ie}}{\beta_{r_id} + \alpha_{r_ie}} - \frac{\alpha_{r_ie}e^{-\beta_{r_id}(\rho-1)}}{\rho\beta_{r_id} + \alpha_{r_ie}} \right]$$
$$+ \frac{1}{\frac{1}{\beta}} \left[\frac{\gamma_{\text{th}}\alpha_{r_ie}e^{-\beta_{r_id}(\rho-1)}}{\rho\beta_{r_id} + \alpha_{r_ie}} + \frac{\gamma_{\text{th}}\beta_{r_id}}{\alpha_{r_ie} + \beta_{r_id}} \right] \quad (22)$$

The asymptotic outage probability is expressed as a summation of an asymptotically varying term with $1/\beta$ and a constant quantity. We can observe that asymptotically varying term is dominating at low SNR, but at high SNR it vanishes. We can also infer from (19) to (22) that due to fixing average SNR of any hop, unbalance is caused in dual-hop cooperative relay system . Hence, the secrecy outage is limited to a constant, even if we infinitely increase the average SNR of the other hop [22, 27].

5.3 Optimal balanced relay selection case
Asymptotic expression of the outage probability for optimal relay selection in the balanced case can be evaluated both when full CSI knowledge is not available and when available at the transmitter.

5.3.1 No knowledge of CSI at transmitter
The $P_o^{OS}(R_s)$ for DF optimal relaying balanced system without CSI knowledge at the transmitter in (13) is expressed as

$$P_o^{OS}(R_s) = \prod_{i=1}^{N} P_o^i(R_s)$$
$$= \frac{1}{\frac{1}{\beta^N}} \prod_{i=1}^{N} \left[\frac{\rho}{\alpha_{r_ie}} + (\rho - 1) + \gamma_{\text{th}} \right]. \quad (23)$$

5.3.2 CSI completely known at transmitter
The $P_o^{OS}(R_s)$ for DF optimal relaying balanced system with CSI knowledge at the transmitter in (14) is expressed as

$$P_o^{OS}(R_s) = \prod_{i=1}^{N} P_o^i(R_s)$$
$$= \frac{1}{\frac{1}{\beta^N}} \prod_{i=1}^{N} \left[\frac{(\rho - 1)}{\alpha_{r_ie}} + (\rho - 1) + \gamma_{\text{th}} \right]. \quad (24)$$

Comparing (23) and (24) with (16) and (17), we can see that for optimal relay selection scheme, asymptotic expression for secrecy outage probability is given by the product of asymptotic expressions of individual single cooperative relay system. We can also see that the denominator in (23) and (24) contains power of N at main channel SNR = $1/\beta$ and thus, using (18) diversity order $D = N$ is obtained. We conclude that, when we choose a single cooperative relay from a set of N relays, the diversity order of N is achieved, which is also intuitive [22, 27].

5.4 Optimal unbalanced relay selection case
The outage probability for DF optimal relaying unbalanced system can be evaluated both when full CSI knowledge is not available and when available at the transmitter.

5.4.1 No knowledge of CSI at transmitter
When $1/\beta_{sr_i}$ is fixed and $1/\beta_{r_id} = 1/\beta \to \infty$, for all $i = 1, \cdots, N$, for optimal relay selection scheme, the outage probability tends to be a constant value in the unbalanced case. The $P_o^{OS}(R_s)$ for DF optimal relaying unbalanced system without CSI knowledge at the transmitter in (13) is expressed as

$$P_o^{OS}(R_s) = \prod_{i=1}^{N} P_o^i(R_s)$$
$$= \prod_{i=1}^{N} \left[1 - e^{-\gamma_{\text{th}}\beta_{sr_i}} \right]. \quad (25)$$

Also, when $1/\beta_{r_id}$ is fixed and $1/\beta_{sr_i} = 1/\beta \to \infty$, for all $i = 1, \cdots, N$, for optimal relay selection scheme, the outage probability tends to be a constant value in the unbalanced case and is given as

$$P_o^{OS}(R_s) = \prod_{i=1}^{N} P_o^i(R_s)$$
$$= \prod_{i=1}^{N} \left[1 - \frac{\alpha_{r_ie}e^{-\beta_{r_id}(\rho-1)}}{\rho\beta_{r_id} + \alpha_{r_ie}} \right]. \quad (26)$$

5.4.2 CSI completely known at transmitter
When $1/\beta_{sr_i}$ is fixed and $1/\beta_{r_id} = 1/\beta \to \infty$, for all $i = 1, \cdots, N$, for optimal relay selection scheme, the outage probability tends to be a constant value in the unbalanced case. The $P_o^{OS}(R_s)$ for DF optimal relaying unbalanced system with CSI knowledge at the transmitter in (14) is expressed as

$$P_o^{OS}(R_s) = \prod_{i=1}^{N} P_o^i(R_s)$$
$$= \prod_{i=1}^{N} \left[1 - e^{-\gamma_{\text{th}}\beta_{sr_i}} \right]. \quad (27)$$

Also, when $1/\beta_{r_id}$ is fixed and $1/\beta_{sr_i} = 1/\beta \to \infty$, for all $i = 1, \cdots, N$, for optimal relay selection scheme, the outage probability tends to be a constant value in the unbalanced case and is given as

$$P_o^{OS}(R_s) = \prod_{i=1}^{N} P_o^i(R_s)$$
$$= \prod_{i=1}^{N} \left[\frac{\alpha_{r_ie}}{\beta_{r_id} + \alpha_{r_ie}} - \frac{\alpha_{r_ie}e^{-\beta_{r_id}(\rho-1)}}{\rho\beta_{r_id} + \alpha_{r_ie}} \right]. \quad (28)$$

Here, asymptotic varying terms are not shown, which can also be obtained as in (19)–(22). Comparing (25)–(28) with (19)–(22), we can observe that the constant value of secrecy outage probability is the product of constant values of individual single cooperative relay system for

Chopra *et al. EURASIP Journal on Information Security* (2018) 2018:7

Page 9 of 12

optimal relay selection scheme. As each constant value of the outage probability in (19)–(22) is less than unity, the performance is always improved by optimal relay selection [22, 27].

The prior literature does not take into account the effect of $S - R_i$ link quality, but in our study, we have considered the effect of both $S - R_i$ and $R_i - D$ link quality for complete performance analysis [27].

6 Numerical analysis

This section presents the analytical results of a threshold-based dual-hop DF cooperative relay network that exactly matches with the simulation results. Noise power is assumed to be the same at all the nodes. To cover feasible range of required secrecy rate, both low and high desired rate of $R_s = 0.1$ and $R_s = 2.0$ are considered.

Figure 2 shows the comparative analysis of the outage probability $P_o(R_s)$ of single ith relay with total SNR $1/\beta$, as expressed in (11) and (12) for the balanced case under the scenario when no direct link is present, both with and without the availability of channel knowledge at the transmitter. The figure is plotted with different $R_s = 0.1, 1.0,$ and 2.0 and fixed $\gamma_{th} = 3$ dB and $1/\alpha_{re} = 1/\alpha = 3$ dB. It can be observed that CSI knowledge can improve secrecy; the amount of improvement for the $P_o(R_s)$ is more when the required rate is low and for low operating SNR. Also, outage probability increases in function of R_s. Corresponding asymptotic analysis as expressed in (16) and (17) is also shown by solid straight lines passing through the curves.

Figure 3 shows the comparison of outage probability $P_o(R_s)$ of single ith relay with total SNR $1/\beta$, as expressed in (8), (10) and (11) under three scenarios: (1) with direct link between both $S - D$ and $S - E$, (2) with direct link only
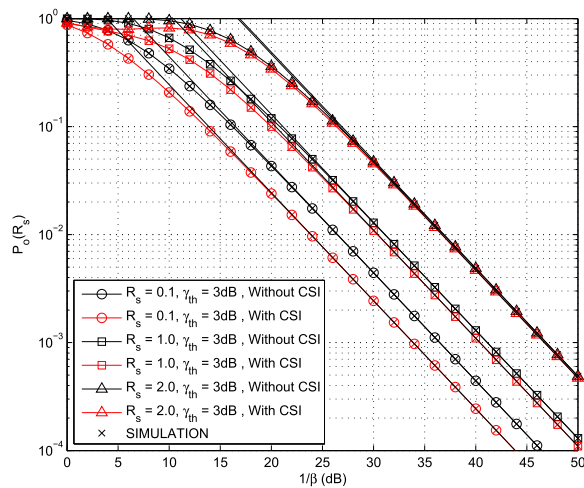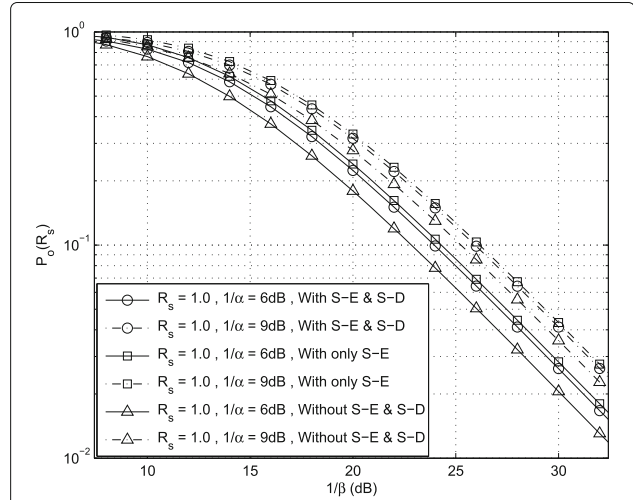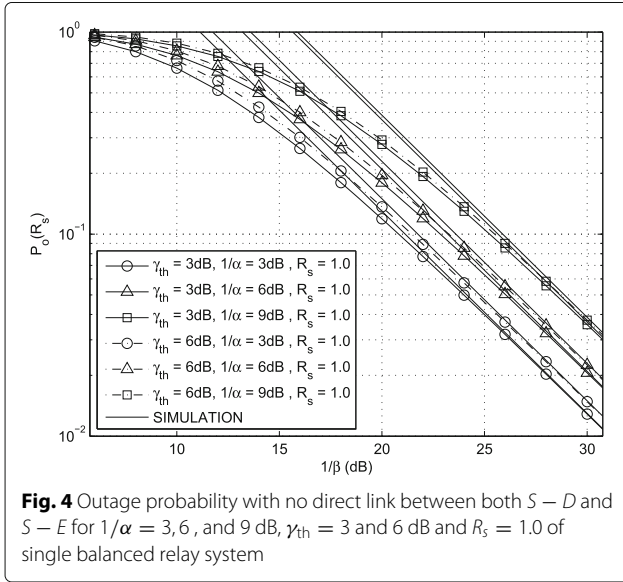

Fig. 3 Comparison of outage probability under three scenarios: (1) with direct link between both $S - D$ and $S - E$, (2) with direct link only between S and E, and (3) with no direct link between both $S - D$ and $S - E$ for $1/\alpha = 6$ and 9 dB, $R_s = 1.0$, and $\gamma_{th} = 3$ dB of single balanced relay system

between S and E, and (3) with no direct link between both $S - D$ and $S - E$. This figure has been plotted with different relays to eavesdropper average SNR $1/\alpha_{r_ie} = 1/\alpha = 6$ and 9 dB, desired secrecy rate $R_s = 1.0$, and fixed $\gamma_{th} = 3$ dB. It is observed from the figure that the outage probability is maximum for the case when only $S-E$ link is present which is intuitive and least for the case when there is no direct link between both $S - D$ and $S - E$. Also, increase in eavesdropper channel quality increases the outage probability of the system for all three scenarios.

Figure 4 shows the outage probability $P_o(R_s)$ of single ith relay with total SNR $1/\beta$, as expressed in (11) under the scenario when direct link is not present between both $S-D$ and $S-E$. This figure has been plotted with different relays to eavesdropper average SNR $1/\alpha_{r_ie} = 1/\alpha = 3, 6,$ and 9 dB, $\gamma_{th} = 3$ and 6 dB, and fixed desired secrecy rate $R_s = 1.0$. It is observed from the figure that the improvement in predetermined threshold value γ_{th}, increases the outage probability of the system. This observation holds true for other two scenarios also. The corresponding asymptotic analysis as given in (16) is depicted by straight solid lines crossing through the curves. It can be observed from the plot that the spacing between asymptotic solid straight lines for $\gamma_{th} = 3$ dB and $\gamma_{th} = 6$ dB, at a given $P_o(R_s)$, is more for low eavesdropper average SNR $1/\alpha = 3$ dB and subsequently decreases for $1/\alpha = 6$ dB and $1/\alpha = 9$ dB. Hence, we can interpret that increase in predetermined threshold value γ_{th} degrades the outage probability more, when eavesdropper average SNR is low, than when eavesdropper average SNR is high. Also, it is observed that
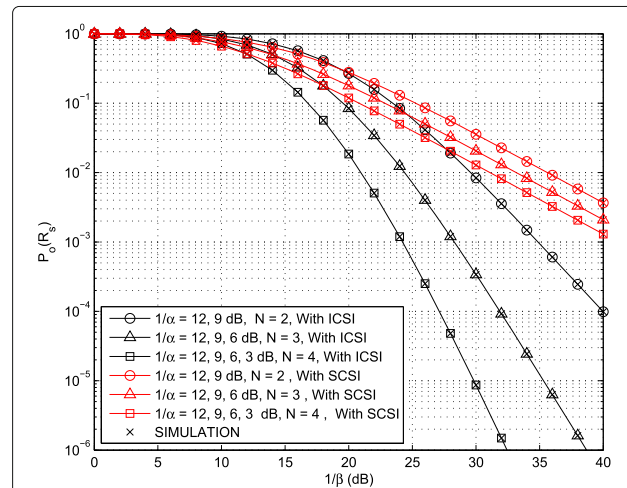

Fig. 2 Comparison of outage probability with $1/\beta$ under no direct link scenario both with and without CSI for $R_s = 0.1, 1.0,$ and 2.0; and $\gamma_{th} = 3$ dB of single balanced relay system

Chopra *et al. EURASIP Journal on Information Security*   (2018) 2018:7

Page 10 of 12

Fig. 4 Outage probability with no direct link between both $S - D$ and $S - E$ for $1/\alpha = 3, 6$, and 9 dB, $\gamma_{\text{th}} = 3$ and 6 dB and $R_s = 1.0$ of single balanced relay system

increase in eavesdropper channel quality increases the outage probability of the system.

Figure 5 shows the outage probability $P_o(R_s)$ of single ith relay, as expressed in (11) for the unbalanced case under the scenario when direct link is not present between both $S - D$ and $S - E$ with average SNR of $1/\beta_{sr_i} = 1/\beta$ at different $1/\beta_{r_id} = 25, 30$, and 35 dB with $1/\alpha_{r_ie} = 1/\alpha = 6$ dB, $\gamma_{\text{th}} = 3$ dB, desired secrecy rate $R_s = 1.0$, and it is also plotted for the unbalanced case with average SNR of $1/\beta_{r_id} = 1/\beta$ at different $1/\beta_{sr_i} = 25, 30$, and 35 dB with $1/\alpha_{r_ie} = 1/\alpha = 6$ dB and fixed $\gamma_{\text{th}} = 3$ dB, desired secrecy rate $R_s = 1.0$. It is observed that $P_o(R_s)$ tends to be a fixed constant, which is derived in (19) and (20) for a given $1/\beta_{r_id}$ or $1/\beta_{sr_i}$ even if $1/\beta$ increases.
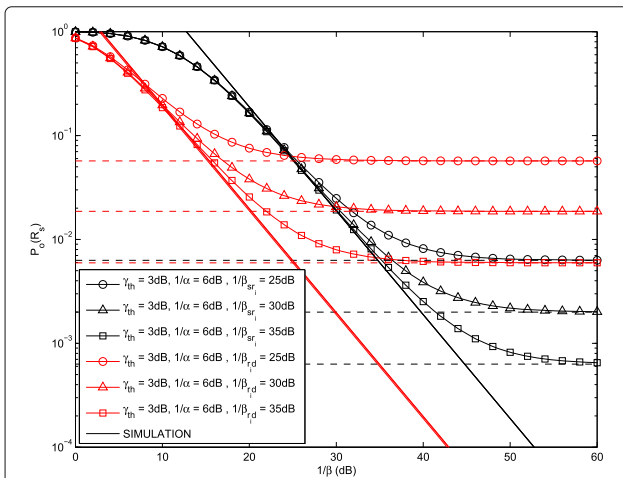
The fixed constants which are derived in (19) and (20) are shown with horizontal dashed line. From the flooring of curves, we can interpret that outage probability is constrained by either of $S - R_i$ or $R_i - D$ link quality. Also, we can observe from the plot that the asymptotically varying term of (19) and (20) depicted by straight solid line have crossed the dashed lines exactly at the point, whereafter average SNR of one hop exceeds the other hop [22, 27]. The flooring of curves can also be analysed using the results of [40], where it is shown that since the average secrecy capacity has a ceiling when the transmit SNR improves, the secrecy outage probability has a floor.

Figure 6 shows the outage probability $P_o(R_s)$ of optimal relay selection scheme when either ICSI or SCSI is known as given in (13) and (15) for the cooperative relay system. The figure is plotted with different number of relays $N = 2, 3$, and 4 for the balanced case under the scenario when direct link is not present between both $S - D$ and $S - E$ with total SNR $1/\beta$. This figure has been plotted with fixed desired secrecy rate $R_s = 1.0$, $\gamma_{\text{th}} = 3$ dB and different relay to eavesdropper average SNR $1/\alpha_{r_ie} = 1/\alpha == 12, 9, 6$, and 3 dB. It is clearly observed from the figure that $P_o(R_s)$ decreases with the increase in number of relays N. The relay selection will improve the performance of multi-relay cooperative system, when the number of relays is increased, for the case when ICSI of the system is known. Whereas, when ICSI of the system is not available, while only SCSI of the system is known, the secrecy performance can either remain same or increase, when the number of relays is increased, depending on the channel characteristics. Particularly for this numerical analysis, we have shown that when only SCSI of the system is known, the secrecy performance is increasing with the increase in

Fig. 5 Outage probability with no direct link between both $S - D$ and $S - E$ for $1/\alpha = 6$ dB, $\gamma_{\text{th}} = 3$ dB, and $R_s = 1.0$ with $1/\beta_{sr_i} = 25, 30$, and 35 dB and $1/\beta_{r_id} = 25, 30$, and 35 dB of single unbalanced relay system

Fig. 6 Outage probability of balanced optimal relay selection scheme when either ICSI or SCSI is known with no direct link between both $S - D$ and $S - E$ for $N = 2, 3$, and 4; $R_s = 1.0$; $1/\alpha = 12, 9, 6$, and 3 dB; and $\gamma_{\text{th}} = 3$ dB

Chopra *et al. EURASIP Journal on Information Security* (2018) 2018:7

Page 11 of 12

the number of relays. Here, out of N relays, we select the relay for which the secrecy outage probability of the system becomes minimum. The secrecy performance with only SCSI of the system will be less, as compared to the one with ICSI of the system, which is also intuitive as improvement is achieved by utilizing the knowledge of instantaneous channel information of the system.

7 Conclusions

In this paper, we have evaluated the secrecy outage probability of the cooperative threshold-based DF dual-hop relay system, both with and without the direct link between source-eavesdropper and source-destination and also without assuming that all the relays can always perfectly decode. We have shown that improvement in desired secrecy rate, eavesdropper channel quality, and predetermined threshold has a significant impact on outage performance of the system. We have provided the asymptotic and diversity gain analysis of the secrecy outage for both the single relay and multi-relay system with OS, when average SNRs of source-relay and relay-destination links are equal or unequal. Secrecy outage probability is evaluated for OS scheme, when either ICSI or SCSI is known and we have examined that the secrecy performance improves with increase in the number of relays. We have also demonstrated that CSI knowledge at the transmitter can improve secrecy, and the amount of improvement for the outage probability is more when the required rate is low and for low operating SNR.

Authors' contributions
KC conceived this diversity combining study and participated in its numerical analysis. RB participated in the analysis of this algorithm study and performed the simulations. AJ also participated in the analysis of this algorithm study and coordination. All authors read and approved the final manuscript.

Competing interests
The authors declare that they have no competing interests.

Publisher's Note
Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Author details
[1]Dept. of Electrical Engineering, Indian Institute of Technology, Delhi, New Delhi-110016, India. [2]Dept. of Computer Science, University of Maryland, Baltimore County, Baltimore, MD 21250, USA.

References
1. Y Zou, X Wang, W Shen, Optimal relay selection for physical-layer security in cooperative wireless networks. IEEE J. Sel. Areas Commun. **31**(10), 2099–2111 (2013)
2. VNQ Bao, N Linh-Trung, M Debbah, Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers. IEEE Trans. Wirel. Commun. **12**(12), 6076–6085 (2013)
3. T-X Zheng, H-M Wang, F Liu, MH Lee, Outage constrained secrecy throughput maximization for DF relay networks. IEEE Trans. Commun. **63**(5), 1741–1755 (2015)
4. TE Hunter, S Sanayei, A Nosratinia, Outage analysis of coded cooperation. IEEE Trans. Inf. Theory. **52**(2), 375–391 (2006)
5. AD Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
6. I Krikidis, JS Thompson, S McLaughlin, Relay selection for secure cooperative networks with jamming. IEEE Trans. Wirel. Commun. **8**(10), 5003–5011 (2009)
7. Y Zou, J Zhu, X Wang, L Hanzo, A survey on wireless security: technical challenges, recent advances, and future trends.Proc. IEEE. **104**(9), 1727–1765 (2016)
8. TX Zheng, HM Wang, J Yuan, Z Han, MH Lee, Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy. IEEE Trans. Wirel. Commun. **16**(6), 3827–3839 (2017)
9. Y Zou, Physical-layer security for spectrum sharing systems. IEEE Trans. Wirel. Commun. **16**(2), 1319–1329 (2017)
10. F Zhu, F Gao, T Zhang, K Sun, M Yao, Physical-layer security for full duplex communications with self-interference mitigation. IEEE Trans. Wirel. Commun. **15**(1), 329–340 (2016)
11. A Jindal, C Kundu, R Bose, Secrecy outage of dual-hop AF relay system with relay selection without eavesdropper's CSI. IEEE Commun. Lett. **18**(10), 1759–1762 (2014)
12. TM Hoang, TQ Duong, HA Suraweera, C Tellambura, HV Poor, Cooperative beamforming and user selection for improving the security of relay-aided systems. IEEE Trans. Commun. **12**, 5039–5051 (2015)
13. K-S Hwang, M Ju, in *Proceedings IEEE International Conference on Communications (ICC)*. Secrecy outage probability of amplify-and-forward transmission with multi-antenna relay in presence of eavesdropper (IEEE, 2014), pp. 5408–5412
14. J Hu, NC Beaulieu, Performance analysis of decode-and-forward relaying with selection combining. IEEE Commun. Lett. **11**(6), 489–491 (2007)
15. J Li, S Luo, AP Petropulu, in *Proceedings IEEE Global Communications Conference (GLOBECOM)*. Outage secrecy rate in wireless relay channels using cooperative jamming (IEEE, 2012), pp. 2438–2443
16. S Tomasin, Routing over multi-hop fading wiretap networks with secrecy outage probability constraint. IEEE Commun. Lett. **18**(10), 1811–1814 (2014)
17. D-D Tran, N-S Vo, T-L Vo, D-B Ha, in *Proceedings IEEE 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*. Physical layer secrecy performance of multi-hop decode-and-forward relay networks with multiple eavesdroppers (IEEE, 2015), pp. 430–435
18. X Wang, YXu M Tao, Outage analysis of cooperative secrecy multicast transmission. IEEE Wirel. Commun. Lett. **2**(3), 161–164 (2014)
19. ER Alotaibi, KA Hamdi, in *Proceedings IEEE Wireless Communications and Networking Conference (WCNC)*. Secrecy outage probability of relay networking in multiple destination and eavesdropper scenarios (IEEE, 2014), pp. 2390–2395
20. X Chen, L Lei, H Zhang, C Yuen, in *Proceedings IEEE International Conference on Communications (ICC)*. On the secrecy outage capacity of physical layer security in large-scale MIMO relaying systems with imperfect CSI (IEEE, 2014), pp. 2052–2057
21. H Alves, G Brante, R Demo Souza, DB da Costa, M Latva-aho, in *Proceedings IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. On the performance of full-duplex relaying under phy security constraints (IEEE, 2014), pp. 3978–3981
22. C Kundu, S Ghose, R Bose, Secrecy outage of dual-hop regenerative multi-relay system with relay selection. IEEE Trans. Wirel. Commun. **14**(8), 4614–4625 (2015)
23. T Li, T Zhang, B Zhong, Z Zhang, AV Vasilakos, in *Proceedings IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. Physical layer security via maximal ratio

Chopra *et al. EURASIP Journal on Information Security* (2018) 2018:7

Page 12 of 12

combining and relay selection over Rayleigh fading channel (IEEE, 2015), pp. 612–616

24. C Cai, Y Cai, W Yang, W Yang, in *Proceedings International Conference on Wireless Communications and Signal Processing*. Average secrecy rate analysis with relay selection using decode-and-forward strategy in cooperative networks (IEEE, 2013), pp. 1–4

25. Y Zhou, G Pan, T Li, H Liu, C Tang, Y Chen, Secrecy outage performance for partial relay selection schemes in cooperative systems. IET Commun. **9**(16), 1980–1987 (2015)

26. H Lei, H Zhang, IS Ansari, Z Ren, G Pan, KA Qaraqe, MS Alouini, On Secrecy Outage of Relay Selection in Underlay Cognitive Radio Networks Over Nakagami-m Fading Channels. IEEE Trans. Cogn. Commun. Netw. **3**(4), 614–627 (2017)

27. K Chopra, R Bose, A Joshi, Secrecy performance of threshold-based decode-and-forward cooperative cognitive radio network. IET Commun. **11**(9), 1396–1406 (2017)

28. FS Al-Qahtani, C Zhong, HM Alnuweiri, Opportunistic relay selection for secrecy enhancement in cooperative networks. IEEE Trans. Commun. **63**(5), 1756–1770 (2015)

29. I Krikidis, Opportunistic relay selection for cooperative networks with secrecy constraints. IET Commun. **4**(15), 1787–1791 (2010)

30. B Van Nguyen, K Kim, in *Proceedings IEEE International Workshop on Information Forensics and Security (WIFS)*. Single relay selection for secure communication in a cooperative system with multiple full-duplex decode-and-forward relays (IEEE, 2015), pp. 1–6

31. R Zhao, Y Yuan, L Fan, YC He, Secrecy performance analysis of cognitive decode-and-forward relay networks in Nakagami-m fading channels. IEEE Trans. Commun. **65**(2), 549–563 (2017)

32. MZI Sarkar, T Ratnarajah, Z Ding, Beamforming with opportunistic relaying for wireless security. IET Commun. **8**(8), 1198–1210 (2014)

33. Z Pengyu, Y Jian, C Jianshu, W Jian, Y Jin, in *Proceedings IEEE Wireless Communications and Networking Conference (WCNC)*. Analyzing Amplify-and-Forward and Decode-and-Forward Cooperative Strategies in Wyner's Channel Model (IEEE, 2009), pp. 1–5

34. T Wang, in *Proceedings 5th IEEE International Conference on Broadband Network & Multimedia Technology (IC-BNMT)*. Comparison of the energy efficiency for decode-and-forward and amplify-and-forward two-way relaying (IEEE, 2013), pp. 232–236

35. G Levin, S Loyka, in *Proceedings 22nd International Zurich Seminar on Communications (IZS)*. Amplify-and-forward versus decode-and-forward relaying: which is better? (Eidgenössische Technische Hochschule Zurich, 2012), pp. 123–126

36. S Ghose, C Kundu, R Bose, Secrecy performance of dual-hop decode-and-forward relay system with diversity combining at the eavesdropper. IET Commun. **10**(8), 904–914 (2016)

37. J Proakis, *Digital Communications*, 4th edn. (McGraw-Hill, New York, 2001)

38. J Barros, MR Rodrigues, in *Proceedings IEEE International Symposium on Information Theory*. Secrecy capacity of wireless channels (IEEE, 2006), pp. 356–360

39. T Lu, P Liu, S Panwar, in *Proceedings IEEE 81st Vehicular Technology Conference (VTC Spring)*. Shining a light into the darkness: How cooperative relay communication mitigates correlated shadow fading (IEEE, 2015), pp. 1–7

40. H Lei, IS Ansari, G Pan, B Alomair, M-S Alouini, Secrecy capacity analysis over $\alpha - \mu$ fading channels. IEEE Commun. Lett. **21**(6), 1445–1448 (2017)