Secrecy Outage of Cooperative Relay Network With and Without Eavesdropper's Direct Link

Khyati Chopra
Dept. of Electrical Engineering
Indian Institute of Technology, Delhi
New Delhi-110016, India
Email: eez148071@ee.iitd.ac.in

Ranjan Bose
Dept. of Electrical Engineering
Indian Institute of Technology, Delhi
New Delhi-110016, India
Email: rbose@ee.iitd.ac.in

Anupam Joshi
Dept. of Computer Science
University of Maryland, Baltimore County
Baltimore, MD 21250, United States
Email: joshi@cs.umbc.edu

Abstract—In this paper, a source communicates to the destination with the cooperation of a relay, in the presence of an eavesdropper. All the links undergo Rayleigh fading and perfect decoding at the relays is not considered. The secrecy outage probability expression is evaluated for a decode-and-forward (DF) dual-hop cooperative relay network, both with and without the presence of direct source to eavesdropper transmission link. The performance of the maximal ratio combining (MRC) and selection combining (SC) diversity at the eavesdropper is investigated. Asymptotic and diversity gain analysis for both the single relay and multi-relay system is obtained, when average SNRs of source-relay and relay-destination links are balanced or unbalanced. We have shown that the increase in target secrecy rate and eavesdropper channel quality significantly affects the outage performance of the system. 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 and have shown that there is improvement in the secrecy performance with the increase in the number of relays.

I. INTRODUCTION

PHYSICAL layer security, has become a promising strategy to ensure secure transmission of information over wireless channels, without the use of cryptographic protocols [1], [2]. Due to the broadcast nature of the wireless medium, it is vulnerable to unintended eavesdropping. The pioneer work [3] on physical layer security of wiretap channels have proved that a positive secrecy capacity can be achieved when the main (or legitimate) channel is the improved version of an eavesdropper's channel.

Cooperative relay communication has received much attention for increasing spectral efficiency, extending radio coverage, and providing a better immunity against signal fading in the wireless networks [4], [5]. Amplify-and-forward (AF) and decode-and-forward (DF) are some fundamental relaying protocols that have been exploited for secure communications [4], [5]. Diversity gain is obtained by combining the relayed signals as well as the signal from the source using a variety of diversity combining techniques such as maximal ratio combining (MRC) and selection combining (SC) [6]. The outage probability performance is analyzed for SC [6], with an arbitrary number of relays in dual-hop scenario and compared

with that of MRC case, but an eavesdropper is not considered in their system model.

Physical layer security of MRC is presented in [7] for wiretap two-wave with diffuse power fading channels, in which MRC scheme is employed by the receiver and the eavesdropper to maximize the probability of secure transmission and successful eavesdropping respectively. Authors in [8] have analyzed the secrecy outage probability with MRC for Rayleigh fading, taking into consideration the single-input multi-output (SIMO) wiretap channel at the receiver and the eavesdropper. The secrecy mutual information for generalized Nakagami-m fading was characterized considering the same channel in [9].

Physical layer security enhancement of a wireless communication system is investigated in [10] with generalized selection diversity combining scheme. Transmit antenna selection for security enhancement in MIMO wiretap channels is discussed in [11], where the legitimate receiver and the eavesdropper use either the MRC or the SC. Bounds on the secrecy capacity is studied in [12] with diversity combining techniques. MRC technique is employed at the receivers in [13], to combine the signals from the direct and relaying links. Authors in [14] have discussed in correlated Rayleigh fading channel with MRC diversity to enhance security.

The motivation behind our work is to incorporate cooperative diversity, which with the help of relay node can improve the throughput and communication reliability, in a multi-path fading environment. We assume that owing to large distance between nodes or deep shadow fading, the source to destination link is not present. On the other hand, source to eavesdropper link is considered, as the eavesdropper can be anywhere in the system to overhear transmission from both the direct and relayed path, and thus can achieve the benefit of diversity gain. We have investigated the secrecy performance of the system with diversity schemes implemented only at the eavesdropper when DF relay is considered for relaying.

The remainder of this paper is organized as follows. The system model is described in Section II. In Section III, secrecy outage probability expressions are evaluated for single cooperative relay system, both with and without direct link. Secrecy outage probability is studied for the optimal relay selection in Section IV. Asymptotic and diversity analysis is
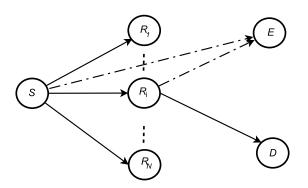
Fig. 1. Dual-hop cooperative DF multi-relay system.

presented in Section V. Numerical results are discussed to support the analytical result in Section VI. Conclusions are drawn in Section VII.

II. SYSTEM MODEL

As shown in the Fig.1, we have considered a dual-hop cooperative relay network 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 . Due to the broadcast nature of wireless medium, we have assumed that there a direct $S-E$ transmission link is also present. We have derived the expression for secrecy outage probability, both with and without the presence of direct $S-E$ transmission link for this dual-hop DF cooperative relay network. The links between various nodes are modeled as Rayleigh flat fading channels and works in half-duplex mode, which are mutually independent but not identical. The ICSI of the eavesdropper channel, as well as, of the main channel is assumed to be known [15].

The SNR between any two arbitrary nodes a and b, denoted as Γ_{ab}, is given by [15]

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

where P_a is the node a transmitted power, 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 $1/\beta_{ab}$ [16], expressed as $\Gamma_{ab} \sim \mathcal{E}(\beta_{ab})$, where β_{ab} is the parameter of the exponentially distribution. The probability density function (PDF), $f_A(z)$ of random variable A for the exponential distribution with β_{ab} as the parameter , is given by

$$f_A(z) = \beta_{ab} e^{-z\beta_{ab}}, \tag{2}$$

and corresponding cumulative distribution function (CDF) $F_A(z)$ of random variable A is given by

$$F_A(z) = 1 - e^{-z\beta_{ab}}. \tag{3}$$

The PDF for SC, where $A = \max(X, Y)$ and X, Y are the exponential distribution with β_{ab} and $\beta_{a'b'}$ as parameters, is

given by

$$f_A(z) = \beta_{ab} e^{-z\beta_{ab}} + \beta_{a'b'} e^{-z\beta_{a'b'}}$$
$$- (\beta_{ab} + \beta_{a'b'}) e^{-z(\beta_{ab} + \beta_{a'b'})} \tag{4}$$

The PDF of the sum of exponential distribution $A = X + Y$ with β_{ab} and $\beta_{a'b'}$ as parameters, is given by

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

The $S - R_i$ channels h_{sr_i}, $R_i - D$ channels h_{r_id}, $R_i - E$ channels h_{r_ie} and $S - E$ channels h_{se}, are slowly varying Rayleigh flat fading channels [15], [17]. Let P_s and P_{r_i} denote the source and relay R_i average powers respectively. Also, let N_{sr_i}, N_{r_id}, N_{r_ie} and N_{se} denote the variances of additive white Gaussian noise of $S - R_i$, $R_i - D$, $R_i - E$ and $S - E$ links respectively. The SNRs Γ_{sr_i}, Γ_{r_id} , Γ_{r_ie} and Γ_{se} are exponentially distributed given as $\Gamma_{sr_i} = \frac{P_s |h_{sr_i}|^2}{N_{sr_i}}$, $\Gamma_{r_id} = \frac{P_{r_i} |h_{r_id}|^2}{N_{r_id}}$, $\Gamma_{r_ie} = \frac{P_{r_i} |h_{r_ie}|^2}{N_{r_ie}}$ and $\Gamma_{se} = \frac{P_s |h_{se}|^2}{N_{se}}$ with average values $1/\beta_{sr_i}$, $1/\beta_{r_id}$, $1/\alpha_{r_ie}$ and $1/\alpha_{se}$ respectively where β_{sr_i} , β_{r_id} , α_{r_ie} and α_{se} are the parameters of the exponential distribution. An outage event occurs when the instantaneous secrecy rate is lower than the target secrecy rate of the cooperative relay system, given as R_s where, $R_s > 0$ and $\rho = 2^{2R_s}$ [15]. We have used ρ for direct mapping of target secrecy rate R_s, and the probability that this outage event occurs successfully is called the outage probability P_o [15], [17]. For this dual-hop system, the capacity is limited by the minimum of the individual hop capacities, which corresponds to the minimum SNRs of the individual hop. This assumption takes care of the fact that perfect decoding at DF relays is not always possible and decoding errors can be there. In our study, we have investigated three scenarios. In the first scenario, the direct $S - E$ link exists with MRC diversity scheme employed at E. In the second scenario, the direct $S-E$ link exists with SC diversity scheme employed at E. In the third scenario, no direct $S - E$ link is considered, assuming that the direct $S - E$ link is absent owing to deep shadow fading or large distance between nodes [15], [18]. Assuming that the optimal Gaussian code-book is used at the source, the secrecy capacity of the system is given as [3], [15], [17], [18]

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

where $(x)^+ \triangleq \max(x, 0)$, $C_s^{MRC(i)}$ is the secrecy capacity of the ith relay in the first scenario with MRC at E, $\Gamma_M = \min(\Gamma_{sr_i}, \Gamma_{r_id})$ is the main link SNR at D and $\Gamma_E^{MRC} = \Gamma_{r_ie} + \Gamma_{se}$ is the eavesdropper link SNR at E. In the second scenario with SC at E, from (6), the secrecy capacity of the ith relay is defined as $C_s^{SC(i)}$ where, $\Gamma_M = \min(\Gamma_{sr_i}, \Gamma_{r_id})$ is the main link SNR at D , $\Gamma_E^{SC} = \max(\Gamma_{r_ie}, \Gamma_{se})$ is the eavesdropper link SNR at E. In the third scenario, from (6), the secrecy capacity of the ith relay is defined as $C_s^{ne(i)}$ where, $\Gamma_M = \min(\Gamma_{sr_i}, \Gamma_{r_id})$ is the main link SNR at D and $\Gamma_E^{NE} = \Gamma_{r_ie}$ is the eavesdropper link SNR at E. The term 1/2 here

denotes that two time phase are required, to complete this dual-hop transmission process. The message transmitted by the source is decoded at the relay, in the first phase. In the second phase, one of the relay is selected to re-encode and forward the message to the destination.

III. Secrecy Outage Probability Analysis of Single Relay System

This section finds the secrecy outage probability expression of DF dual-hop cooperative relay network, in the three scenarios as discussed in our study.
Outage probability for single i^{th} relay is evaluated for the first scenario using (1)-(6) where, the direct $S - E$ link exists with MRC at E as

$$
\begin{aligned}
P_o^i &= \mathbb{P}\left[C_s^{MRC(i)} < R_s\right] = \mathbb{P}\left[\left(\frac{1+\Gamma_M}{1+\Gamma_E^{MRC}}\right) < \rho\right] \\
&= \mathbb{P}\left[\min(\Gamma_{sr_i}, \Gamma_{r_id}) < \rho(1+\lambda) - 1\right] \\
&= 1 - \mathbb{P}\left[\min(\Gamma_{sr_i}, \Gamma_{r_id}) \geq \rho(1+\lambda) - 1\right] \\
&= 1 - \left[\mathbb{P}\left[\Gamma_{sr_i} \geq \rho(1+\lambda) - 1\right] \times \right. \\
&\qquad \left. \mathbb{P}\left[\Gamma_{r_id} \geq \rho(1+\lambda) - 1\right]\right] \\
&= 1 - \left[(1 - \mathbb{P}\left[\Gamma_{sr_i} < \rho(1+\lambda) - 1\right]) \times \right. \\
&\qquad \left. (1 - \mathbb{P}\left[\Gamma_{r_id} < \rho(1+\lambda) - 1\right])\right] \\
&= \mathbb{P}\left[\Gamma_{sr_i} < \rho(1+\lambda) - 1\right] + \mathbb{P}\left[\Gamma_{r_id} < \rho(1+\lambda) - 1\right] \\
&\quad - \mathbb{P}\left[\Gamma_{sr_i} < \rho(1+\lambda) - 1\right]\mathbb{P}\left[\Gamma_{r_id} < \rho(1+\lambda) - 1\right] \\
&= \int_0^\infty \left(1 - e^{-\left(\beta_{sr_i}+\beta_{r_id}\right)\left(\rho(1+\lambda)-1\right)}\right) \times \\
&\qquad \left(\frac{\alpha_{r_ie}\alpha_{se}e^{-\lambda\alpha_{r_ie}}}{\alpha_{se} - \alpha_{r_ie}} + \frac{\alpha_{r_ie}\alpha_{se}e^{-\lambda\alpha_{se}}}{\alpha_{r_ie} - \alpha_{se}}\right)d\lambda \\
&= 1 - \frac{\alpha_{r_ie}\alpha_{se}e^{-\left(\beta_{sr_i}+\beta_{r_id}\right)(\rho-1)}}{\left(\rho\left(\beta_{sr_i}+\beta_{r_id}\right)+\alpha_{r_ie}\right)\left(\rho\left(\beta_{sr_i}+\beta_{r_id}\right)+\alpha_{se}\right)},
\end{aligned}
\tag{7}
$$

where $\lambda = \Gamma_{r_ie} + \Gamma_{se}$.
Outage probability for single i^{th} relay is evaluated for the second scenario using (1)-(6) where, the direct $S - E$ link exists with SC at E as

$$
\begin{aligned}
P_o^i &= \mathbb{P}\left[C_s^{SC(i)} < R_s\right] = \mathbb{P}\left[\left(\frac{1+\Gamma_M}{1+\Gamma_E^{SC}}\right) < \rho\right] \\
&= \mathbb{P}\left[\min(\Gamma_{sr_i}, \Gamma_{r_id}) < \rho(1+\lambda') - 1\right] \\
&= 1 - \mathbb{P}\left[\min(\Gamma_{sr_i}, \Gamma_{r_id}) \geq \rho(1+\lambda') - 1\right] \\
&= 1 - \left[\mathbb{P}\left[\Gamma_{sr_i} \geq \rho(1+\lambda') - 1\right] \times \right. \\
&\qquad \left. \mathbb{P}\left[\Gamma_{r_id} \geq \rho(1+\lambda') - 1\right]\right] \\
&= 1 - \left[(1 - \mathbb{P}\left[\Gamma_{sr_i} < \rho(1+\lambda') - 1\right]) \times \right. \\
&\qquad \left. (1 - \mathbb{P}\left[\Gamma_{r_id} < \rho(1+\lambda') - 1\right])\right] \\
&= \mathbb{P}\left[\Gamma_{sr_i} < \rho(1+\lambda') - 1\right] + \mathbb{P}\left[\Gamma_{r_id} < \rho(1+\lambda') - 1\right] \\
&\quad - \mathbb{P}\left[\Gamma_{sr_i} < \rho(1+\lambda') - 1\right]\mathbb{P}\left[\Gamma_{r_id} < \rho(1+\lambda') - 1\right] \\
&= \int_0^\infty \left(1 - e^{-\left(\beta_{sr_i}+\beta_{r_id}\right)\left(\rho(1+\lambda')-1\right)}\right) \times \\
&\qquad \left(\alpha_{se}e^{-\alpha_{se}\lambda'} + \alpha_{r_ie}e^{-\alpha_{r_ie}\lambda'} - \right.
\end{aligned}
$$

$$
\left. (\alpha_{se} + \alpha_{r_ie})\, e^{-(\alpha_{se}+\alpha_{r_ie})\lambda'}\right)d\lambda'
\tag{8}
$$

$$
\begin{aligned}
&= 1 - \frac{\alpha_{se}e^{-\left(\beta_{sr_i}+\beta_{r_id}\right)(\rho-1)}}{\left(\rho\left(\beta_{sr_i}+\beta_{r_id}\right)+\alpha_{se}\right)} - \frac{\alpha_{r_ie}e^{-\left(\beta_{sr_i}+\beta_{r_id}\right)(\rho-1)}}{\left(\rho\left(\beta_{sr_i}+\beta_{r_id}\right)+\alpha_{r_ie}\right)} \\
&\quad + \frac{\left(\alpha_{se}+\alpha_{r_ie}\right)e^{-\left(\beta_{sr_i}+\beta_{r_id}\right)(\rho-1)}}{\left(\rho\left(\beta_{sr_i}+\beta_{r_id}\right)+\left(\alpha_{se}+\alpha_{r_ie}\right)\right)},
\end{aligned}
\tag{9}
$$

where $\lambda' = \max(\Gamma_{r_ie}, \Gamma_{se})$.
Outage probability for single i^{th} relay is evaluated for the third scenario using (1)-(6) where, no direct $S - E$ link exists as

$$
\begin{aligned}
P_o^i &= \mathbb{P}\left[C_s^{NE(i)} < R_s\right] = \mathbb{P}\left[\left(\frac{1+\Gamma_M}{1+\Gamma_E^{NE}}\right) < \rho\right] \\
&= \mathbb{P}\left[\min(\Gamma_{sr_i}, \Gamma_{r_id}) < \rho(1+\lambda'') - 1\right] \\
&= 1 - \mathbb{P}\left[\min(\Gamma_{sr_i}, \Gamma_{r_id}) \geq \rho(1+\lambda'') - 1\right] \\
&= 1 - \left[\mathbb{P}\left[\Gamma_{sr_i} \geq \rho(1+\lambda'') - 1\right] \times \right. \\
&\qquad \left. \mathbb{P}\left[\Gamma_{r_id} \geq \rho(1+\lambda'') - 1\right]\right] \\
&= 1 - \left[(1 - \mathbb{P}\left[\Gamma_{sr_i} < \rho(1+\lambda'') - 1\right]) \times \right. \\
&\qquad \left. (1 - \mathbb{P}\left[\Gamma_{r_id} < \rho(1+\lambda'') - 1\right])\right] \\
&= \mathbb{P}\left[\Gamma_{sr_i} < \rho(1+\lambda'') - 1\right] + \mathbb{P}\left[\Gamma_{r_id} < \rho(1+\lambda'') - 1\right] \\
&\quad - \mathbb{P}\left[\Gamma_{sr_i} < \rho(1+\lambda'') - 1\right]\mathbb{P}\left[\Gamma_{r_id} < \rho(1+\lambda'') - 1\right] \\
&= \int_0^\infty \left(1 - e^{-\left(\beta_{sr_i}+\beta_{r_id}\right)\left(\rho(1+\lambda'')-1\right)}\right) \times \\
&\qquad \alpha_{r_ie}e^{-\lambda''\alpha_{r_ie}}d\lambda'' \\
&= 1 - \frac{\alpha_{r_ie}e^{-\left(\beta_{sr_i}+\beta_{r_id}\right)(\rho-1)}}{\rho\left(\beta_{sr_i}+\beta_{r_id}\right)+\alpha_{r_ie}},
\end{aligned}
\tag{10}
$$

where $\lambda'' = \Gamma_{r_ie}$.
Contrary to prior literature, where the source-eavesdropper direct link is not taken into account [15], [18], [19], we have derived the outage probability expression for the DF relay network, both with and without the direct source-eavesdropper link.

IV. Secrecy Outage Analysis of Relay Selection Scheme

In this section, outage probability analysis of DF relay network with MRC diversity scheme at E, for optimal relay selection scheme is presented [15], [19].

A. Optimal Selection: ICSI of All the Links is Available

For the optimal relay selection scheme, [15], [18], [19], the relay for which the secrecy capacity of the cooperative system becomes maximum is selected. We can obtain outage probability by evaluating the probability for which the maximum secrecy capacity becomes less than the target secrecy rate, R_s [15], [18]. We can evaluate this by the multiplication of CDFs of the corresponding random variables. Here, the individual secrecy outage probabilities of single cooperative relay system are basically taken as the CDFs. We have hence evaluated the secrecy outage probability of optimal relay selection as

$$
P_o^{OS}(R_s) = \mathbb{P}\left[\max_{i \in [1,N]}\{C_s^{MRC(i)}\} < R_s\right]
$$

$$= \prod_{i=1}^{N} \mathbb{P}\left[C_s^{MRC(i)} < R_s\right] = \prod_{i=1}^{N} P_o^i(R_s). \quad (11)$$

We can examine that (10) is obtained by simply multiplying the individual outage probabilities of single cooperative relay system, which is derived in (7). There is requirement of ICSI of all the links in this relay selection scheme.

B. Optimal Selection: SCSI of All the Links is Available

We have examined this relay selection scheme where, no knowledge of ICSI is required. This selection method requires only the statistical information of all the links for outage probability measurement. In this scheme, the relay for which the outage probability of system with direct $S-E$ transmission link becomes minimum is selected [15]. The outage probabilities, $P_o^i(R_s)$ of all the individual single relay systems as obtained in (7) can be first measured, and then we can find the optimal relay i^* [15].
It can be expressed mathematically as

$$i^* = \arg \min_{i \in [1,..,N]} \left(P_o^i(R_s)\right). \quad (12)$$

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. 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 [15].

V. ASYMPTOTIC AND DIVERSITY ANALYSIS

In this section, asymptotic and diversity analysis is presented for DF relay network [15].

A. Single Balanced Relay Case

When $1/\beta_{sr_i} = 1/\beta_{r_id} = 1/\beta \to \infty$ in the balanced case, the outage probability of single cooperative relay system in (7)-(9) is given, with MRC at E, SC at E and without $S-E$ link respectively as

$$P_o^i(R_s) = \frac{2}{\frac{1}{\beta}}\left[\frac{\rho}{\alpha_{r_ie}} + \frac{\rho}{\alpha_{se}} + (\rho - 1)\right] \quad (13)$$

$$P_o^i(R_s) = \frac{2}{\frac{1}{\beta}}\left[\frac{\rho(\alpha_{r_ie}^2 + \alpha_{r_ie}\alpha_{se} + \alpha_{se}^2)}{\alpha_{r_ie}\alpha_{se}(\alpha_{r_ie} + \alpha_{se})} + (\rho - 1)\right] \quad (14)$$

$$P_o^i(R_s) = \frac{2}{\frac{1}{\beta}}\left[\frac{\rho}{\alpha_{r_ie}} + (\rho - 1)\right]. \quad (15)$$

We can interpret from (12)-(14) that the outage probability is inversely proportional to $1/\beta$ and when main channel SNR $(1/\beta)$ tends to infinity, it tends to zero. It is directly proportional to the eavesdropper channel SNR and target secrecy rate R_s.
Diversity order is a measure to observe that how fast secrecy outage probability decreases, when we tend SNR to infinity. Hence, we can intuitively understand the effect on the outage

probability, when the number of relays are increased. The diversity order [18] is given as

$$D = -\lim_{\text{SNR} \to \infty} \frac{\log P_o(\text{SNR})}{\log(\text{SNR})}, \quad (16)$$

where $P_o(\text{SNR})$ is the outage probability given by function of $\text{SNR} = 1/\beta$. We can show that using this definition, diversity order of (12)-(14) can be obtained as one. The power of SNR in the denominator of (12)-(14), is same as the diversity order, D. It is intuitive that the diversity order of one is obtained by the single relay system, as relay selection is not there.

B. Single Unbalanced Relay Case

The outage probability behavior is discussed, when MRC is considered at E for this unbalanced case, by increasing the average $R_i - D$ link SNR asymptotically and keeping the average $S - R_i$ link SNR fixed, i.e. when $1/\beta_{sr_i}$ is fixed and $1/\beta_{r_id} = 1/\beta \to \infty$.

$$P_o^i(R_s) = \left[1 - \frac{\alpha_{r_ie}\alpha_{se}e^{-\beta_{sr_i}(\rho-1)}}{(\rho\beta_{sr_i} + \alpha_{r_ie})(\rho\beta_{sr_i} + \alpha_{se})}\right]$$
$$+ \frac{1}{\frac{1}{\beta}}\left[\frac{\rho\alpha_{r_ie} + \rho\alpha_{se} + (\rho - 1)\alpha_{r_ie}\alpha_{se}e^{-\beta_{sr_i}(\rho-1)}}{(\rho\beta_{sr_i} + \alpha_{r_ie})(\rho\beta_{sr_i} + \alpha_{se})}\right]. \quad (17)$$

Also, the behavior of secrecy outage probability is discussed, when MRC is considered at E by increasing the average $S-R_i$ link SNR asymptotically and keeping the average $R_i - D$ link SNR fixed, i.e. when $1/\beta_{r_id}$ is fixed and $1/\beta_{sr_i} = 1/\beta \to \infty$. The asymptotic secrecy outage probability can be expressed same as in (16) with β_{sr_i} replaced with β_{r_id} because it is symmetric.
The asymptotic outage probability is given as the summation of a constant quantity and an asymptotically varying term with $1/\beta$. We can observe that asymptotically varying term vanishes at high SNR and is dominating at low SNR. We can also infer from (16) 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 [15].

C. Optimal Balanced Relay Selection Case

Asymptotic expression for the outage probability as given in (7)-(9), in the balanced case can be evaluated for the optimal relay selection, with MRC at E, SC at E and without $S-E$ link respectively as

$$P_o^{OS}(R_s) = \frac{2^N}{\frac{1}{\beta^N}} \prod_{i=1}^{N}\left[\frac{\rho}{\alpha_{r_ie}} + \frac{\rho}{\alpha_{se}} + (\rho - 1)\right] \quad (18)$$

$$P_o^{OS}(R_s) = \frac{2^N}{\frac{1}{\beta^N}} \prod_{i=1}^{N}\left[\frac{\rho(\alpha_{r_ie}^2 + 2\alpha_{r_ie}\alpha_{se} + \alpha_{se}^2)}{\alpha_{r_ie}\alpha_{se}(\alpha_{r_ie} + \alpha_{se})} + (\rho - 1)\right] \quad (19)$$

$$P_o^{OS}(R_s) = \frac{2^N}{\frac{1}{\beta^N}} \prod_{i=1}^{N}\left[\frac{\rho}{\alpha_{r_ie}} + (\rho - 1)\right]. \quad (20)$$

Comparing (17)-(19) with (12)-(14) 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 (17)-(19) contains power of N at main channel SNR $= 1/\beta$ and thus, using (15) diversity order $D = N$ is obtained [15]. We can conclude that we achieve the diversity order of N, when a single cooperative relay is chosen from a set of N relays, which is also intuitive.

D. Optimal Unbalanced Relay Selection Case

When $1/\beta_{r_id} = 1/\beta \to \infty$ and $1/\beta_{sr_i}$ is fixed, for all $i = 1, \cdots, N$, for optimal relay selection scheme in (10), the outage probability tends to a constant value in the unbalanced case and is given, when MRC is considered at E as

$$P_o^{OS}(R_s) = \prod_{i=1}^{N} \left(1 - \frac{\alpha_{r_ie}\alpha_{se}e^{-\beta_{sr_i}(\rho-1)}}{(\rho\beta_{sr_i} + \alpha_{r_ie})(\rho\beta_{sr_i} + \alpha_{se})} \right). \quad (21)$$

Also, $1/\beta_{sr_i} = 1/\beta \to \infty$ and when $1/\beta_{r_id}$ is fixed, for all $i = 1, \cdots, N$, for optimal relay selection scheme in (10), the outage probability tends to a constant value in the unbalanced case. The asymptotic secrecy outage probability can be expressed same as in (20) with β_{sr_i} replaced with β_{r_id} because it is symmetric. Here asymptotic varying terms are not shown, which can also be obtained as in (16). Comparing (20) with (16), it can be observed that the constant value of the secrecy outage probability for the optimal relay selection, is product of the constant values of the individual single cooperative DF relay system. As each constant value of the outage probability in (16) is less than unity, the optimal relay selection always improve the secrecy performance of the system [15]. 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 [15], [19].

VI. NUMERICAL ANALYSIS

This section presents the analytical results of a dual-hop DF cooperative relay network, that matches with the simulation results. At all the nodes, noise power is assumed to be same. For covering feasible range of target secrecy rate, both low and high target rate of $R_s = 0.1$ and $R_s = 1.0$ are considered. Fig. 2 shows the comparison of outage probability $P_o(R_s)$ of single i^{th} relay with total SNR $1/\beta$, as expressed in (7)-(9) for the balanced case under three scenarios, 1) with MRC at E 2) with SC at E and 3) with no direct $S - E$ link. This figure has been plotted with different target secrecy rate $R_s = 0.1, 1.0$ and fixed relay to eavesdropper average SNR $1/\alpha_{r_ie} = 1/\alpha = 6$ dB. It can be observed from the figure that the outage performance is better when no direct link available as compared with the case of direct link available. This proves that direct link has a significant impact on the system secrecy. It is also found that the system secrecy performance is better for SC at the E than MRC, as MRC has better diversity performance than SC. The corresponding asymptotic analysis as given in (12)-(14) is depicted by straight solid lines crossing
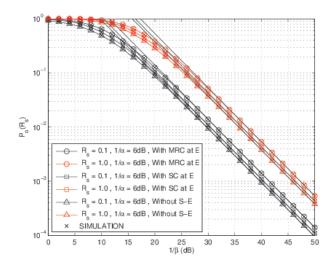

Fig. 2. Comparison of outage probability under three scenarios, 1) with MRC at E 2) with SC at E and 3) with no direct $S - E$ link for $1/\alpha = 6$ dB and $R_s = 0.1, 1.0$ of single balanced relay system.
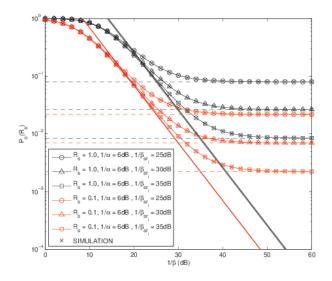

Fig. 3. Outage probability with MRC at E for $1/\alpha = 6$ dB and $R_s = 0.1, 1.0$ with $1/\beta_{sr_i} = 25, 30, 35$ dB of single unbalanced relay system.

through the curves. Also, secrecy outage probability increases with the increase in target secrecy rate R_s in all the three scenarios.

Fig. 3 shows the outage probability $P_o(R_s)$ of single i^{th} relay, as expressed in (7) for the unbalanced case under the scenario when MRC at E is considered, with average SNR of $1/\beta_{r_id} = 1/\beta$ at different $1/\beta_{sr_i} = 25, 30, 35$ dB, target secrecy rate $R_s = 0.1, 1.0$ and fixed $1/\alpha_{r_ie} = 1/\alpha = 6$ dB. It is observed that $P_o(R_s)$ tends to a fixed constant, which is derived in (16) for a given $1/\beta_{r_id}$ or $1/\beta_{sr_i}$, even if $1/\beta$ increases. The fixed constants which are derived in (16) 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
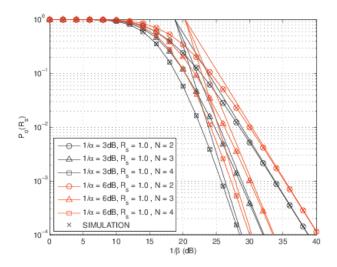
Fig. 4. Outage probability of balanced optimal relay selection scheme with MRC at E for $N = 2, 3, 4$, $R_s = 1.0$ and $1/\alpha = 3, 6$ dB.

observe from the plot that the asymptotically varying term of (16) depicted by straight solid line, have crossed the dashed lines exactly at the point, whereafter average SNR of one hop exceeds the other hop [15].

Fig. 4 shows the secrecy outage probability $P_o(R_s)$ of optimal relay selection scheme with different number of relays $N = 2, 3, 4$ as given in (10) for the balanced case under the scenario when MRC at E is considered, with total SNR $1/\beta$. This figure has been plotted with different relay to eavesdropper average SNR $1/\alpha_{r_i e} = 1/\alpha = 3, 6$ dB and fixed target secrecy rate $R_s = 1.0$. It is clearly observed from the figure that increase in number of relays N from $N = 2$ to $N = 4$ improves the outage probability as diversity increases. The corresponding asymptotic analysis as given in (17) is depicted by straight solid lines crossing through the curves. Also, secrecy outage probability of the system increases with increase in eavesdropper channel quality. These observations hold true for the other two scenarios also.

VII. Conclusion

In this paper, we have discussed the secrecy outage probability of the cooperative DF dual-hop relay system, both with and without the direct source-eavesdropper link. We have investigated the performance of the MRC and SC diversity at the eavesdropper have shown that the system secrecy performance is better for SC at the E than MRC, as MRC has better diversity performance than SC. We observe that increase in target secrecy rate and eavesdropper channel quality has a significant impact on outage performance of the system. We have provided the asymptotic and diversity gain analysis, when average SNRs of source-relay and relay-destination links are balanced or unbalanced. Outage probability is evaluated for optimal relay selection scheme, when either full ICSI or SCSI of all the links is available and have shown that the secrecy performance improves with increase in the number of relays.

References

[1] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[2] Y. Liang, H. V. Poor *et al.*, "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[3] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[4] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, 2010.

[5] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4985–4997, 2011.

[6] J. Hu and N. C. Beaulieu, "Performance analysis of decode-and-forward relaying with selection combining," *IEEE Communications Letters*, vol. 11, no. 6, pp. 489–491, 2007.

[7] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 247–258, 2014.

[8] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Communications Letters*, vol. 15, no. 5, pp. 509–511, 2011.

[9] M. Z. I. Sarkar and T. Ratnarajah, "On the secrecy mutual information of Nakagami-*m* fading SIMO channel," in *Proc. IEEE International Conference on Communications (ICC)*, 2010, pp. 1–5.

[10] L. Chen, Y. Yang, and G. Wei, "Physical layer security enhancement with generalized selection diversity combining," in *Proc. IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2013, pp. 518–521.

[11] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Transactions on Communications*, vol. 61, no. 1, pp. 144–154, 2013.

[12] M. Z. I. Sarkar and T. Ratnarajah, "Bounds on the secrecy capacity with diversity combining techniques," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, 2012, pp. 2847–2851.

[13] X. Lei, L. Fan, R. Q. Hu, D. S. Michalopoulos, and P. Fan, "Secure multiuser communications in multiple decode-and-forward relay networks with direct links," in *Proc. IEEE Global Communications Conference*, 2014, pp. 3180–3185.

[14] M. Z. I. Sarkar and T. Ratnarajah, "Enhancing security in correlated channel with maximal ratio combining diversity," *IEEE Transactions on Signal Processing*, vol. 60, no. 12, pp. 6745–6751, 2012.

[15] C. Kundu, S. Ghose, and R. Bose, "Secrecy outage of dual-hop regenerative multi-relay system with relay selection," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4614–4625, 2015.

[16] J. Proakis, *Digital Communications*, 4th ed. New York, NY, USA: McGraw-Hill, 2001.

[17] J. Barros and M. R. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE International Symposium on Information Theory*, 2006, pp. 356–360.

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

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