Secrecy Outage Performance of Cooperative Relay Network With Diversity Combining

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, the secrecy outage probability of threshold-based decode-and-forward (DF) cooperative relay network is evaluated. Unlike other works to date, we assume combining of direct and relayed signals both at the destination and the eavesdropper. All the links undergo Rayleigh fading and the relay can perfectly decode the message, only if the received SNR meets a particular threshold. The secrecy performance is compared for the system with either selection combining (SC), or with maximal ratio combining (MRC) or with the combination of both, at the destination and eavesdropper. We have shown that the eavesdropper channel quality, required secrecy rate, pre-defined threshold and the choice of diversity scheme significantly affects the secrecy performance of the system.**

***Keywords*—decode-forward relay; maximal ratio combining; selection combining; secrecy outage probability; threshold-based**

I. Introduction

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 [1]–[3]. Maximal ratio combining (MRC) and selection combining (SC) are the diversity combining techniques, where the relayed signals as well as the signal from the source is combined to obtain the diversity gain [1]. Due to the open and dynamic nature of these cooperative networks, they are vulnerable to unintended eavesdropping. Hence, for secure communications in these cooperative networks, physical layer security has arisen as a promising strategy [2], [4]. The classical wiretap model was proposed by Wyner in [5], which can facilitate the security analysis without the use of cryptographic protocols for communication systems [4].

The performance analysis of the decode-and-forward (DF) relaying system, with MRC and SC is investigated in [1]. A system may use SC which simply requires SNR measurements, instead of using MRC which requires exact knowledge of the channel state information (CSI). Authors have shown that the MRC system outperforms the SC system, but unlike our system model, the presence of an eavesdropper is not considered. However, non-zero secrecy capacity with diversity combining techniques over log-normal fading channel is discussed in [6]. Secrecy Outage on transmit antenna selection/maximal ratio combining over Rayleigh fading channels is presented in [7], for multiple input multiple output (MIMO) cognitive radio networks. Transmit antenna selection for security enhancement in MIMO wiretap channels is discussed in [8], where the legitimate receiver and the eavesdropper use either the MRC or the SC. Bounds on the secrecy capacity is studied in [9] with diversity combining techniques. MRC technique is employed at the receivers in [10], to combine the signals from the direct and relaying links. Authors in [11] have discussed in correlated Rayleigh fading channel with MRC diversity to enhance security.

In the existing literature, typically it is assumed that in high SNR scenario, a relay can correctly decode the message [12]. However, this is not always a practical assumption, as the signal strength might be degraded due to fading. In such scenario, the relay is not able to correctly decode the message [2]. Correct decoding over a particular threshold SNR is thus a better assumption and is considered in our paper. In [2], secrecy performance of such threshold-based DF relay system is explored, but with the diversity combining only at the eavesdropper. Contrary to [2], [4], direct link between both source-destination and source-eavesdropper is considered in our study, that requires diversity combining at destination and eavesdropper. Threshold-based relaying is also taken into account, where the relay is able to fully decode the message, only if the pre-defined SNR is met. The closed-form secrecy outage probability expressions are obtained for this threshold-based cooperative DF relay system.

The remainder of this paper is organized as follows. The system model is described in Section II. Secrecy outage probability expressions are evaluated for threshold-based single cooperative DF relay system in Section III. In Section IV, simulation results are discussed to corroborate the analytical results. Finally, we conclude this study in Section V.

Notation: $\mathcal{E}(x)$ defines exponential distribution with parameter x, $\mathbb{P}[\cdot]$ is the probability of an event. $\max\{\cdot\}$ denotes the maximum of its arguments and $(x)^+ \triangleq \max(0, x)$. Generally $F_X(\cdot)$, in capital letter, denotes the cumulative distribution function (CDF) of a RV X. $f_X(\cdot)$, in small letter, denotes the corresponding probability density function (PDF).

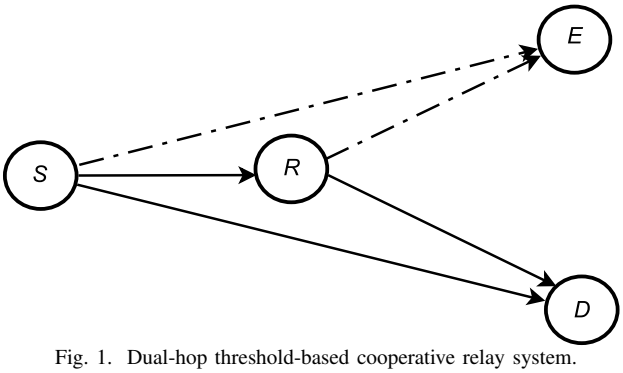

Fig. 1. Dual-hop threshold-based cooperative relay system.

II. System Model

We consider a dual-hop cooperative relay system consisting of a source S, a destination D, an eavesdropper E and a DF relay R , which works in a dual-hop mode as shown in Fig. 1. We assume direct transmission links $S-D$ and $S-E$ are also present, due to the broadcast nature of wireless medium. Without assuming that the relay can always perfectly decode, we consider that the relay can correctly decode the message, only if the received SNR meets the pre-defined threshold, illustrated as γ_{th} for $S-R$ link [2]. 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 main channel, as well as, of the eavesdropper channel is not known at the transmitter [2], [4]. The SNR between any two arbitrary nodes a and b, denoted as Γ_{ab}, is given by [2]

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

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 $1/\beta_{ab}$ [13], expressed as $\Gamma_{ab} \sim \mathcal{E}(\beta_{ab})$, where β_{ab} is the parameter of the exponentially distribution. The PDF, given as $f_A(z)$ of random variable A for the exponential distribution with β_{ab} as the parameter is

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

and the corresponding CDF is given as

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

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

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

and the corresponding CDF is given as

$$F_X(z) = 1 - e^{-z\beta_{ab}} - e^{-z\beta_{a'b'}} + e^{-z(\beta_{ab}+\beta_{a'b'})}. \tag{5}$$

The PDF for MRC, where $A = X + Y$, and X, Y are the random variables with exponential distribution with β_{ab} and $\beta_{a'b'}$ as parameters, is given as

$$f_A(z) = \frac{\beta_{a'b'}\beta_{ab} e^{-z\beta_{ab}}}{\beta_{a'b'} - \beta_{ab}} + \frac{\beta_{ab}\beta_{a'b'} e^{-z\beta_{a'b'}}}{\beta_{ab} - \beta_{a'b'}}, \tag{6}$$

and the corresponding CDF is given as

$$F_X(z) = 1 - \frac{\beta_{x'y'} e^{-z\beta_{xy}}}{\beta_{x'y'} - \beta_{xy}} - \frac{\beta_{xy} e^{-z\beta_{x'y'}}}{\beta_{xy} - \beta_{x'y'}}. \tag{7}$$

The $S-R$ channel h_{sr}, $R-D$ channel h_{rd}, $R-E$ channel h_{re}, $S-D$ channel h_{sd} and $S-E$ channel h_{se}, are slowly varying Rayleigh flat fading channels [2]. Let P_s and P_r denote the average powers used at source and relay R respectively. Also, let N_{sr}, N_{rd}, N_{re}, N_{sd} and N_{se} denote the variances of additive white Gaussian noise of $S-R$, $R-D$, $R-E$, $S-D$ and $S-E$ links respectively. The SNRs Γ_{sr}, Γ_{rd} , Γ_{re}, Γ_{sd} and Γ_{se} are exponentially distributed given as $\Gamma_{sr} = \frac{P_s|h_{sr}|^2}{N_{sr}}$, $\Gamma_{rd} = \frac{P_r|h_{rd}|^2}{N_{rd}}$, $\Gamma_{re} = \frac{P_r|h_{re}|^2}{N_{re}}$, $\Gamma_{sd} = \frac{P_s|h_{sd}|^2}{N_{sd}}$ and $\Gamma_{se} = \frac{P_s|h_{se}|^2}{N_{se}}$ with average values $1/\beta_{sr}$, $1/\beta_{rd}$, $1/\alpha_{re}$, $1/\beta_{sd}$ and $1/\alpha_{se}$ respectively where β_{sr} , β_{rd} , α_{re}, 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 $\rho = 2^{2R_s}$ [2], [14]. We have used ρ for direct mapping of required secrecy rate R_s, and the outage probability P_o is the probability of successful occurrence of this outage event [2], [4].

Achievable secrecy rate is the difference of the main channel information rate and the eavesdropper channel information rate of the system given as [2], [5]

$$C_s \triangleq \frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_M}{1+\Gamma_E}\right)\right]^+, \tag{8}$$

where Γ_M, Γ_E are the SNRs at D and E respectively. 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, in the first phase. In the second phase, the relay re-encodes and forwards the message to the destination.

We have investigated four scenarios in our study. First is when SC diversity scheme is employed at both D and E, such that when $\Gamma_{sr} \geq \gamma_{th}$, the relay correctly decodes the message and $\Gamma_M^{SC} = \max(\Gamma_{rd}, \Gamma_{sd})$ is the SNR at D and $\Gamma_E^{SC} = \max(\Gamma_{re}, \Gamma_{se})$ is the SNR at E. The second is when SC diversity scheme is employed at D and MRC diversity scheme is employed at E, such that when $\Gamma_{sr} \geq \gamma_{th}$, the relay correctly decodes the message and $\Gamma_M^{SC} = \max(\Gamma_{rd}, \Gamma_{sd})$ is the SNR at D and $\Gamma_E^{MRC} = \Gamma_{re} + \Gamma_{se}$ is the SNR at E. The third is when MRC diversity scheme is employed at D and SC diversity scheme is employed at E, such that when $\Gamma_{sr} \geq \gamma_{th}$, the relay correctly decodes the message and $\Gamma_M^{MRC} = \Gamma_{rd} + \Gamma_{sd}$ is the SNR at D and $\Gamma_E^{SC} = \max(\Gamma_{re}, \Gamma_{se})$ is the SNR at E. The fourth is when MRC diversity scheme is employed at both D and E, such that when $\Gamma_{sr} \geq \gamma_{th}$, the relay correctly decodes the message and $\Gamma_M^{MRC} = \Gamma_{rd} + \Gamma_{sd}$ is the SNR at D and $\Gamma_E^{MRC} = \Gamma_{re} + \Gamma_{se}$

is the SNR at E. When $\Gamma_{sr} < \gamma_{th}$, the relay does not transmit at all, thus only direct $S-D$ and $S-E$ communication link exists, where $\Gamma_M = \Gamma_{sd}$ is the SNR of the main link at D and $\Gamma_E = \Gamma_{se}$ is the SNR of the eavesdropper link at E for all the four scenarios.

III. 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 by following the law of total probability, in the four scenarios as discussed in our study. The secrecy outage probability of the system can be evaluated by finding the conditional secrecy outage probability when relay correctly decodes the message and when it does not [2], [14]. We have evaluated secrecy outage probability for single relay system using (1)-(7), in the first scenario as

$$\begin{aligned}
P_o &= \mathbb{P}\left[C_s < R_s | \Gamma_{sr} \geq \gamma_{th}\right] \mathbb{P}[\Gamma_{sr} \geq \gamma_{th}] \\
&\quad + \mathbb{P}\left[C_s < R_s | \Gamma_s < \gamma_{th}\right] \mathbb{P}\Big[\Gamma_s < \gamma_{th}\Big] \\
&= \mathbb{P}\left[\frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_M^{SC}}{1+\Gamma_E^{SC}}\right)\right] < R_s \Big| \Gamma_{sr} \geq \gamma_{th}\right] \times \\
&\quad \mathbb{P}\Big[\Gamma_{sr} \geq \gamma_{th}\Big] + \mathbb{P}\left[\frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_M}{1+\Gamma_E}\right)\right] < R_s \Big| \Gamma_{sr} < \gamma_{th}\right] \\
&\quad \times \mathbb{P}\Big[\Gamma_{sr} < \gamma_{th}\Big] \\
&= \mathbb{P}[\max(\Gamma_{rd}, \Gamma_{sd}) < (\rho-1) + \\
&\quad \rho(\max(\Gamma_{re}, \Gamma_{se}))|\Gamma_{sr} \geq \gamma_{th}] \left(e^{-\gamma_{th}\beta_{sr}}\right) \\
&\quad + \mathbb{P}[\Gamma_{sd} < (\rho-1) + \rho\Gamma_{se}|\Gamma_{sr} < \gamma_{th}] \left(1 - e^{-\gamma_{th}\beta_{sr}}\right) \\
&= \Bigg(1 - \frac{\alpha_{se}e^{-(\rho-1)\beta_{sd}}}{(\rho\beta_{sd}+\alpha_{se})} - \frac{\alpha_{re}e^{-(\rho-1)\beta_{sd}}}{(\rho\beta_{sd}+\alpha_{re})} \\
&\quad + \frac{(\alpha_{se}+\alpha_{re})\, e^{-(\rho-1)\beta_{sd}}}{(\rho\beta_{sd}+\alpha_{se}+\alpha_{re})} - \frac{\alpha_{se}e^{-(\rho-1)\beta_{rd}}}{(\rho\beta_{rd}+\alpha_{se})} \\
&\quad - \frac{\alpha_{re}e^{-(\rho-1)\beta_{rd}}}{(\rho\beta_{rd}+\alpha_{re})} + \frac{(\alpha_{se}+\alpha_{re})\, e^{-(\rho-1)\beta_{rd}}}{(\rho\beta_{rd}+\alpha_{se}+\alpha_{re})} \\
&\quad + \frac{\alpha_{se}e^{-(\rho-1)(\beta_{sd}+\beta_{rd})}}{(\rho\,(\beta_{sd}+\beta_{rd})+\alpha_{se})} + \frac{\alpha_{re}e^{-(\rho-1)(\beta_{sd}+\beta_{rd})}}{(\rho\,(\beta_{sd}+\beta_{rd})+\alpha_{re})} \\
&\quad - \frac{(\alpha_{se}+\alpha_{re})\, e^{-(\rho-1)(\beta_{sd}+\beta_{rd})}}{(\rho\,(\beta_{sd}+\beta_{rd})+\alpha_{se}+\alpha_{re})}\Bigg)\left(e^{-\gamma_{th}\beta_{sr}}\right) \\
&\quad + \left(1 - e^{-\gamma_{th}\beta_{sr}}\right)\left(1 - \frac{\alpha_{se}e^{-\beta_{sd}(\rho-1)}}{\rho\beta_{sd}+\alpha_{se}}\right). \qquad (9)
\end{aligned}$$

We have evaluated secrecy outage probability for single relay system using (1)-(7), in the second scenario as

$$\begin{aligned}
P_o &= \mathbb{P}\left[C_s < R_s | \Gamma_{sr} \geq \gamma_{th}\right] \mathbb{P}[\Gamma_{sr} \geq \gamma_{th}] \\
&\quad + \mathbb{P}\left[C_s < R_s | \Gamma_s < \gamma_{th}\right] \mathbb{P}\Big[\Gamma_s < \gamma_{th}\Big] \\
&= \mathbb{P}\left[\frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_M^{SC}}{1+\Gamma_E^{MRC}}\right)\right] < R_s \Big| \Gamma_{sr} \geq \gamma_{th}\right] \times \\
&\quad \mathbb{P}\Big[\Gamma_{sr} \geq \gamma_{th}\Big] + \mathbb{P}\left[\frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_M}{1+\Gamma_E}\right)\right] < R_s \Big| \Gamma_{sr} < \gamma_{th}\right] \\
&\quad \times \mathbb{P}\Big[\Gamma_{sr} < \gamma_{th}\Big] \\
&= \mathbb{P}[\max(\Gamma_{rd}, \Gamma_{sd}) < (\rho-1) + \\
&\quad \rho(\Gamma_{re}+\Gamma_{se})|\Gamma_{sr} \geq \gamma_{th}] \left(e^{-\gamma_{th}\beta_{sr}}\right) \\
&\quad + \mathbb{P}[\Gamma_{sd} < (\rho-1) + \rho\Gamma_{se}|\Gamma_{sr} < \gamma_{th}] \left(1 - e^{-\gamma_{th}\beta_{sr}}\right) \\
&= \Bigg(1 - \frac{\alpha_{re}\alpha_{se}e^{-(\rho-1)\beta_{sd}}}{(\rho\beta_{sd}+\alpha_{re})\,(\alpha_{se}-\alpha_{re})} \\
&\quad - \frac{\alpha_{se}\alpha_{re}e^{-(\rho-1)\beta_{sd}}}{(\rho\beta_{sd}+\alpha_{se})\,(\alpha_{re}-\alpha_{se})} - \frac{\alpha_{re}\alpha_{se}e^{-(\rho-1)\beta_{rd}}}{(\rho\beta_{rd}+\alpha_{re})\,(\alpha_{se}-\alpha_{re})} \\
&\quad - \frac{\alpha_{se}\alpha_{re}e^{-(\rho-1)\beta_{rd}}}{(\rho\beta_{rd}+\alpha_{se})\,(\alpha_{re}-\alpha_{se})} \\
&\quad + \frac{\alpha_{re}\alpha_{se}e^{-(\rho-1)(\beta_{sd}+\beta_{rd})}}{(\rho(\beta_{sd}+\beta_{rd})+\alpha_{re})\,(\alpha_{se}-\alpha_{re})} \\
&\quad + \frac{\alpha_{se}\alpha_{re}e^{-(\rho-1)(\beta_{sd}+\beta_{rd})}}{(\rho(\beta_{sd}+\beta_{rd})+\alpha_{se})\,(\alpha_{re}-\alpha_{se})}\Bigg)\left(e^{-\gamma_{th}\beta_{sr}}\right) \\
&\quad + \left(1 - e^{-\gamma_{th}\beta_{sr}}\right)\left(1 - \frac{\alpha_{se}e^{-\beta_{sd}(\rho-1)}}{\rho\beta_{sd}+\alpha_{se}}\right). \qquad (10)
\end{aligned}$$

We have evaluated secrecy outage probability for single relay system using (1)-(7), in the third scenario as

$$\begin{aligned}
P_o &= \mathbb{P}\left[C_s < R_s | \Gamma_{sr} \geq \gamma_{th}\right] \mathbb{P}[\Gamma_{sr} \geq \gamma_{th}] \\
&\quad + \mathbb{P}\left[C_s < R_s | \Gamma_s < \gamma_{th}\right] \mathbb{P}\Big[\Gamma_s < \gamma_{th}\Big] \\
&= \mathbb{P}\left[\frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_M^{MRC}}{1+\Gamma_E^{SC}}\right)\right] < R_s \Big| \Gamma_{sr} \geq \gamma_{th}\right] \times \\
&\quad \mathbb{P}\Big[\Gamma_{sr} \geq \gamma_{th}\Big] + \mathbb{P}\left[\frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_M}{1+\Gamma_E}\right)\right] < R_s \Big| \Gamma_{sr} < \gamma_{th}\right] \\
&\quad \times \mathbb{P}\Big[\Gamma_{sr} < \gamma_{th}\Big] \\
&= \mathbb{P}[(\Gamma_{rd} + \Gamma_{sd}) < (\rho-1) + \\
&\quad \rho(\max(\Gamma_{re}, \Gamma_{se}))|\Gamma_{sr} \geq \gamma_{th}] \left(e^{-\gamma_{th}\beta_{sr}}\right) \\
&\quad + \mathbb{P}[\Gamma_{sd} < (\rho-1) + \rho\Gamma_{se}|\Gamma_{sr} < \gamma_{th}] \left(1 - e^{-\gamma_{th}\beta_{sr}}\right) \\
&= \Bigg(1 - \frac{\alpha_{se}\beta_{sd}e^{-(\rho-1)\beta_{rd}}}{(\rho\beta_{rd}+\alpha_{se})\,(\beta_{sd}-\beta_{rd})} \\
&\quad - \frac{\alpha_{se}\beta_{rd}e^{-(\rho-1)\beta_{sd}}}{(\rho\beta_{sd}+\alpha_{se})\,(\beta_{rd}-\beta_{sd})} - \frac{\alpha_{re}\beta_{sd}e^{-(\rho-1)\beta_{rd}}}{(\rho\beta_{rd}+\alpha_{re})\,(\beta_{sd}-\beta_{rd})} \\
&\quad - \frac{\alpha_{re}\beta_{rd}e^{-(\rho-1)\beta_{sd}}}{(\rho\beta_{sd}+\alpha_{re})\,(\beta_{rd}-\beta_{sd})} + \frac{(\alpha_{se}+\alpha_{re})\beta_{sd}e^{-(\rho-1)\beta_{rd}}}{(\rho\beta_{rd}+\alpha_{se}+\alpha_{re})\,(\beta_{sd}-\beta_{rd})} \\
&\quad + \frac{(\alpha_{se}+\alpha_{re})\beta_{rd}e^{-(\rho-1)\beta_{sd}}}{(\rho\beta_{sd}+\alpha_{se}+\alpha_{re})\,(\beta_{rd}-\beta_{sd})}\Bigg)\left(e^{-\gamma_{th}\beta_{sr}}\right) \\
&\quad + \left(1 - e^{-\gamma_{th}\beta_{sr}}\right)\left(1 - \frac{\alpha_{se}e^{-\beta_{sd}(\rho-1)}}{\rho\beta_{sd}+\alpha_{se}}\right). \qquad (11)
\end{aligned}$$

We have evaluated secrecy outage probability for single relay system using (1)-(7), in the fourth scenario as

$$\begin{aligned}
P_o &= \mathbb{P}\left[C_s < R_s | \Gamma_{sr} \geq \gamma_{th}\right] \mathbb{P}[\Gamma_{sr} \geq \gamma_{th}] \\
&\quad + \mathbb{P}\left[C_s < R_s | \Gamma_s < \gamma_{th}\right] \mathbb{P}\Big[\Gamma_s < \gamma_{th}\Big]
\end{aligned}$$

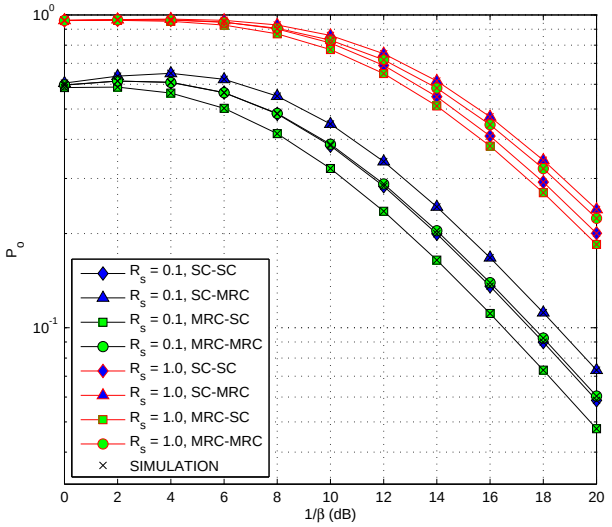

Fig. 2. Comparative analysis of secrecy outage probability with $1/\beta$ under four scenarios for $R_s = 1.0, 0.1$, $1/\alpha = 6$ dB and $\gamma_{th} = 3$ dB of single relay system.

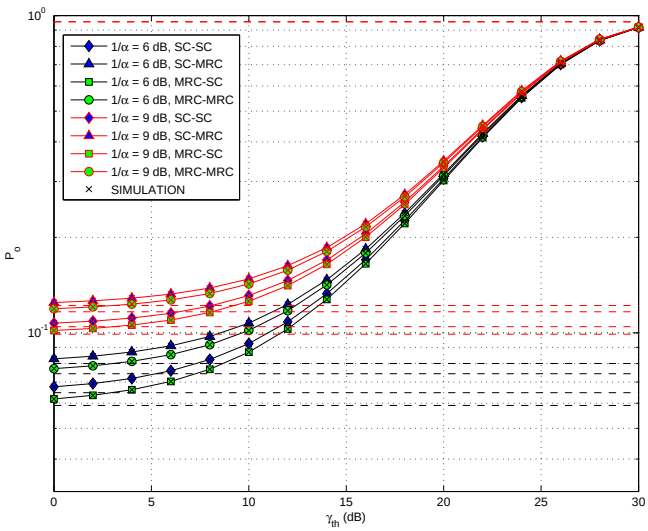

Fig. 3. Comparative analysis of secrecy outage probability with γ_{th} under four scenarios for $1/\alpha = 6, 9$ dB , $R_s = 1.0$ of single relay system.

$$
\begin{aligned}
&= \mathbb{P}\left[\frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_M^{MRC}}{1+\Gamma_E^{MRC}}\right)\right] < R_s \middle| \Gamma_{sr} \geq \gamma_{th}\right] \times \\
&\mathbb{P}\Big[\Gamma_{sr} \geq \gamma_{th}\Big] + \mathbb{P}\left[\frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_M}{1+\Gamma_E}\right)\right] < R_s \middle| \Gamma_{sr} < \gamma_{th}\right] \\
&\times \mathbb{P}\Big[\Gamma_{sr} < \gamma_{th}\Big] \\
&= \mathbb{P}[(\Gamma_{rd} + \Gamma_{sd}) < (\rho - 1) + \\
&\quad \rho((\Gamma_{re} + \Gamma_{se}))|\Gamma_{sr} \geq \gamma_{th}]\left(e^{-\gamma_{th}\beta_{sr}}\right) \\
&\quad + \mathbb{P}[\Gamma_{sd} < (\rho-1) + \rho\Gamma_{se}|\Gamma_{sr} < \gamma_{th}]\left(1 - e^{-\gamma_{th}\beta_{sr}}\right) \\
&= \Bigg(1 - \frac{e^{-(\rho-1)\beta_{rd}}\beta_{sd}\alpha_{re}\alpha_{se}}{(\beta_{sd}-\beta_{rd})(\alpha_{se}-\alpha_{re})(\rho\beta_{rd}+\alpha_{re})} \\
&\quad - \frac{e^{-(\rho-1)\beta_{sd}}\beta_{rd}\alpha_{re}\alpha_{se}}{(\beta_{rd}-\beta_{sd})(\alpha_{se}-\alpha_{re})(\rho\beta_{sd}+\alpha_{re})} \\
&\quad - \frac{e^{-(\rho-1)\beta_{rd}}\beta_{sd}\alpha_{re}\alpha_{se}}{(\beta_{sd}-\beta_{rd})(\alpha_{re}-\alpha_{se})(\rho\beta_{rd}+\alpha_{se})} \\
&\quad - \frac{e^{-(\rho-1)\beta_{sd}}\beta_{rd}\alpha_{re}\alpha_{se}}{(\beta_{rd}-\beta_{sd})(\alpha_{re}-\alpha_{se})(\rho\beta_{sd}+\alpha_{se})}\Bigg)\left(e^{-\gamma_{th}\beta_{sr}}\right) \\
&\quad + \left(1 - e^{-\gamma_{th}\beta_{sr}}\right)\left(1 - \frac{\alpha_{se}e^{-\beta_{sd}(\rho-1)}}{\rho\beta_{sd}+\alpha_{se}}\right). \qquad (12)
\end{aligned}
$$

In contrast to the prior literature [2], [12], we have done the comparative secrecy performance analysis with threshold-based relaying, and diversity schemes employed both at destination and eavesdropper.

IV. Simulation Results

In this section, we present the simulation results to validate the derived expressions. Noise power is assumed to be same at all the nodes. To cover the feasible range of required secrecy rate, both low and high required rate of $R_s = 0.1$ and $R_s = 1.0$ are considered.

Fig. 2 shows the comparison of outage probability P_o of single cooperative relay for the four scenarios, as expressed in (9), (10), (11) and (12) with total SNR $1/\beta$. This figure has been plotted with different required secrecy rate $R_s = 0.1, 1.0$, and fixed relay to eavesdropper average SNR $1/\alpha_{re} = 1/\alpha = 6$ dB , $\gamma_{th} = 3$ dB, $1/\beta_{sd} = 3$ dB , $1/\alpha_{se} = 3$ dB. It is observed from the figure that the secrecy performance of the system is best, when diversity scheme MRC is used at D and SC is used at E. The performance is worst, when diversity scheme SC is used at D and MRC is used at E. At lower secrecy rates, the performance difference of the system with MRC or SC diversity scheme at both D and E is comparable. However, at higher secrecy rates, SC system performs better than the MRC system. Also, it is shown that P_o increases in function of the required secrecy rate R_s, which is intuitive.

Fig. 3 shows the effect of γ_{th} on the outage probability P_o, as given in (9), (10), (11) and (12). This figure has been plotted with different relay to eavesdropper average SNR $1/\alpha_{re} = 1/\alpha = 6, 9$ dB and fixed required secrecy rate $R_s = 1.0$, main link average SNR $1/\beta_{sr} = 1/\beta_{rd} = 25$ dB, $1/\beta_{sd} = 3$ dB , $1/\alpha_{se} = 3$ dB. It can be observed from the plot that when γ_{th} tends to zero, all curves saturate to a particular value shown by using horizontal dashed line, which can be evaluated by substituting $\gamma_{th} = 0$ in (9), (10), (11) and (12). This shows that a fixed least outage probability could be achieved depending on the input parameters, when the message is perfectly decoded by the relay. When threshold tends to infinity, due to high SNR threshold relay cannot decode the message, and as both $S-E$ and $S-D$ links exist, outage probability tends to $\left(1 - \frac{\alpha_{se}e^{-\beta_{sd}(\rho-1)}}{\rho\beta_{sd}+\alpha_{se}}\right)$. This shows that the direct links have a significant impact on the system secrecy. Also, it is shown that P_o increases in function

of the relay to eavesdropper average SNR $1/\alpha_{re}$.

V. Conclusion

We have derived the exact closed-form expressions for secrecy outage probability of cooperative threshold-based DF relay system. Unlike other works, that neglect the direct source to destination and source to eavesdropper link assuming it to be weak, we assume combining of direct and relayed signals both at the destination and the eavesdropper. We have shown that the eavesdropper channel quality, pre-defined threshold, required secrecy rate and the choice of diversity scheme (MRC/SC), significantly affects the secrecy performance of the system.

References

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

[2] S. Ghose, C. Kundu, and R. Bose, "Secrecy performance of dual-hop decode-and-forward relay system with diversity combining at the eavesdropper," *IET Commun.*, vol. 10, no. 8, pp. 904–914, 2016.

[3] A. Jindal, C. Kundu, and R. Bose, "Secrecy outage of dual-hop AF relay system with relay selection without eavesdropper's CSI," *IEEE Communications Letters*, vol. 18, no. 10, pp. 1759–1762, 2014.

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

[5] A. D. Wyner, "The wire-tap channel," *The Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[6] M. Z. I. Sarkar and T. Ratnarajah, "Secrecy capacity over log-normal fading channel with diversity combining techniques," in *Proc. IEEE Wireless Communications and Networking Conf. (WCNC)*, 2013, pp. 2457–2461.

[7] H. Zhao, Y. Tan, G. Pan, and Y. Chen, "Secrecy outage on transmit antenna selection/maximal ratio combining in MIMO cognitive radio networks," in *Proc. IEEE Int. Conf. on Wireless Communications & Signal Processing (WCSP)*, 2015, pp. 1–6.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

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

[14] F. S. Al-Qahtani, C. Zhong, and H. M. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Trans. on Commun.*, vol. 63, no. 5, pp. 1756–1770, 2015.