Secrecy Outage Probability Analysis for Cooperative Communication with Relay Selection Under Non-Identical Distribution

Esa R. Alotaibi and Khairi A. Hamdi.
School of Electrical and Electronic Engineering,
University of Manchester, Manchester M13 9PL, U.K.
Emails: esa.alotaibi@manchester.ac.uk, k.hamdi@manchester.ac.uk.

***Abstract*—In this paper, secrecy outage probability is analyzed in a cooperative network for an independent but non-identically distributed (i.n.i.d) Rayleigh fading channel. By using multi-trusted decode and forward relays, the model assumes direct links between a sender (Alice) and receiver nodes (Bob and an eavesdropper). The protocol employed herein selects the best relay with the highest signal-to-noise ratio (SNR) in relation to the destination (Bob). The eavesdropper's channel state information (CSI) is neither available to the sender nor to the best relay, while maximum ratio combining (MRC) is employed at Bob and the eavesdropper. Finally, the theoretical analysis is validated through simulation, and the results show that performance is enhanced with an increasing number of relays in the event of a direct link between the sender and the receiver's terminals.**

I. Introduction

The open environment in which wireless communication exists makes wireless networks highly vulnerable to active and passive eavesdroppers. Recently, security has been a key area of concern for researchers, and significant progress has been made in this regard. In the past, the focus was on securing upper layers of a communication by using traditional cryptographic techniques. However, more recently, security within physical layers has become more important, and has received a great deal of attention from researchers, with the prime motivating factors behind this move being the drawbacks associated with traditional approaches to achieving security [1], [2].

Cooperative communication, an interesting paradigm technology for wireless transmission, has been gaining ground over recent years [3]–[5]. Relay selection techniques are considered a significant and an effective approach for cooperative networks, as correctly designed schemes are able to support full spatial diversity with low complexity and overheads by operating as multiple input multiple output (MIMO) schemes, without using more conventional MIMO methods [4]. Recent developments in cooperative communication networks have led to renewed interest in relay selection schemes [6]–[8].

Many researchers have contributed to using the relay selection technique for cooperative transmission, in order to improve physical layer security [9]–[17]. The reason for this is that, if relay selection is not performed securely, the whole system may be unsecured in the physical layer. Krikidis, in his research [18], presented an opportunistic relay selection mechanism that offers an effective way to ensure the confidentiality and protection of the source's message against eavesdroppers, by taking into consideration a number of security constraints. The author analyzed his protection mechanism through three scenarios, namely conventional relay selection, which does not consider the relay-eavesdropper channels, optimal relay selection, where the instantaneous channel state information (CSI) of the eavesdropper link is assumed and achievable secrecy capacity is therefore maximized, and suboptimal relay selection, which presumes average CSI regarding the eavesdropper's channel. However, the researcher took into account two transmission phases, without assuming that direct links were available, in addition identically-distributed fading was considered.

Bao et al. [19] posited the concept of opportunistic relay selection schemes in cooperative networks, with multiple eavesdroppers under secrecy constraints. The researchers analyzed this scenario from the point of view of three protocols: minimum selection, conventional selection and secrecy relay selection. The first scheme minimized the message overheard by the eavesdropper, by selecting the relay with the lowest signal-to-noise ratio (SNR) in relation to the eavesdropper nodes. The second scheme maximized SNR at the destination terminal by choosing the best relay with the highest SNR in relation to the destination. In the third protocol, the best potential relay was selected according to its secrecy rate. The author's numerical results demonstrate that the optimal selection scheme's secrecy outage probability performs better than for both the conventional selection scheme and the minimum selection scheme, while the conventional selection scheme is better than the minimum selection scheme in relation to security performance. As a result, the authors proposed that increasing the number of relays is more effective than increasing transmit power at the relay nodes. However, they only considered a dual-hop cooperative system and assumed that the sender has no direct link with the receiver and the eavesdropper, thereby indicating that the direct links were in deep shadowing. In addition, they assumed that all of the distances between relay nodes and receiver terminals are identical.

978-1-4673-9814-5/16/$31.00 ©2016 IEEE

In [20], the authors appraised the lower bound, upper bound, and approximate expression for the secrecy outage probability of a dual-hop amplify-and-forward relay, in order to enhance physical layer security by selecting the best relay. They assumed no knowledge of the eavesdropper's instantaneous CSI, however in their system, direct communication from source to destination is not available, and identically-distributed fading was assumed.

In addition, many other study community organizations have investigated dual-hop cooperative communications through analysis and performance evaluations, by assuming that perfect CSI is available when performing relay selection, and that direct links are in deep shadowing in addition using identical distribution fading [18], [19], [21], [22] . Therefore, a real-life, practical scenario which includes direct links between a sender and receivers, and also the eavesdropper's CSI may not available to a source with diffident distances between cooperating nodes and receiver terminals.

A. Contributions

The main technical contributions of this paper are as follows: (1) We consider a relay selection scheme that selects the relay with the highest SNR in relation to the destination (Bob), by assuming that a direct link is available between the sender and the receiver terminals. (2) We investigate the effects of relay selection on system secrecy performance, by deriving analytical secrecy outage probability in an independent non-identically-distributed (i.n.i.d) Rayleigh fading channel scenario.(3) We extract a closed form expression for the secrecy outage probability, by assuming that the eavesdropper's CSI is not available to Alice and to the best relay.

B. Notations

Bold lower case symbols denote vectors, and $d_{i,j}$ represents the Euclidean distance between terminals i and j, while β refers to the path loss exponent, P_i denotes power at terminal i, h_i is the channel coefficient for channel i, n_i is the additive white Gaussian noise (AWGN) at i, and γ_i is the instantaneous signal-to-noise ratio at terminal i. In addition N_0 denotes the Variance of the AWGN, λ_i is the parameter of the distribution for channel i to Bob, μ_i is the parameter of the distribution for channel i to the eavesdropper, N represents the number of relays, and R_s the secrecy rate.

C. Organization

The rest of the paper is organized as follows: Section II discusses the proposed system model and provides a brief description thereof, before moving on to outline the relay selection technique and channel statistics. Section III analyzes the secrecy outage probability of the selection scheme. Next, Section IV displays the numerical results and discusses the proposed mechanism, while section V concludes the paper by presenting scope for future research.

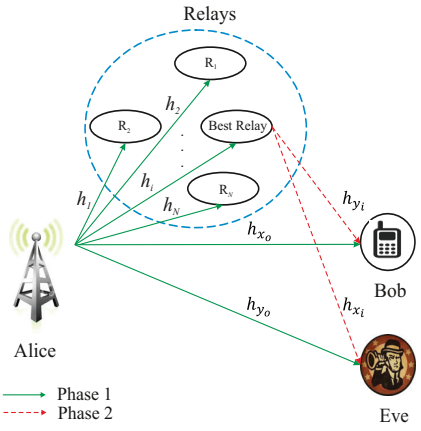

Fig. 1. System model of cooperative relay communications in the presence of an eavesdropper node with existing direct links

II. System Model

This section is split into three subsections. The first part explains the system model and provides a brief description thereof, the second part debates the relay selection technique, and the third part presents the channel statistics for Bob and the eavesdropper's links.

A. Description

The system model consists of one source (Alice), one destination (Bob), and a set of N decode-and-forward (DF) trusted relays which help to stop a passive eavesdropper from overhearing a transmission between the source and the destination. We assume that the source has a direct link with the destination and the eavesdropper terminals, all relays can successfully decode the Alice message, all nodes are equipped with a single antenna, and all of them operate in the half-duplex mode (a schematic diagram of the system model is shown in Fig. 1).

This paper focuses on the effect of relay selection schemes on a system's achievable secrecy outage probability, assuming an unknown eavesdropper's CSI at Alice and the best relay. In the first phase of the protocol, Alice broadcasts the transmitted signal to Bob, and to all of the relay nodes in the presence of a passive eavesdropper. In the second phase, the node with the highest SNR to Bob among the set of relays is chosen. It then re-encodes and forwards the re-encoded signal to Bob. The distances between nodes are arbitrary and not necessarily identical, in addition the signal experiences independent Rayleigh fading. As a result, the composite channel become independent but non-identical distribution (i.n.i.d). The channel remains static for one coherence interval (one slot), and changes independently at different coherence intervals with a variance of $\sigma_{i,j} = d_{i,j}^{-\beta}$. The symbol $d_{i,j}$ is the Euclidean distance between terminals i and j, while β is the path loss exponent. We assume that Alice remains silent in the second phase while the relays transmit [23]. After receiving the symbols from Alice and the best relay, Bob implements

a maximum ratio combining (MRC) process to unite the received signals and to maximize the SNR of Bob's channel. This permits Bob to take advantage of relay selection, and to use the direct link channel to improve the chances of achieving a secure transmission.

In the first phase, the signals received at Bob, the nth relay, and the eavesdropper, respectively, are

$$y_{B_1} = \sqrt{P_A} h_{x_o} s_1 + n_{B_1} \quad (1)$$

$$y_{n\text{th}_1} = \sqrt{P_A} h_{n\text{th}_1} s_1 + n_{n\text{th}_1} \quad (2)$$

$$y_{E_1} = \sqrt{P_A} h_{y_o} s_1 + n_{E_1} \quad (3)$$

where P_A is the transmitted power from Alice, and h_{x_o}, $h_{n\text{th}}$, and h_{y_o} are channel coefficients from Alice to Bob, the nth relay, and the eavesdropper, respectively. The symbols n_{B_1}, $n_{n\text{th}_1}$, and n_{E_1} represent added white Gaussian noise (AWGN) at Bob, the nth relay, and the eavesdropper nodes, respectively, while s_1 is the transmitted signal in the first phase.

In the second phase, the decoded messages at Bob and the eavesdropper are represented as

$$y_{B_2} = \sqrt{P_R} h_{x_i} s_2 + n_{B_2} \quad (4)$$

$$y_{E_2} = \sqrt{P_R} h_{y_i} s_2 + n_{E_2} \quad (5)$$

where P_R is the power at the best relay, and h_{x_i} and h_{y_i} are channel coefficients from the best relay to Bob and the eavesdropper, respectively. The symbols n_{B_2} and n_{E_2} are AWGN terms at Bob and the eavesdropper, respectively, while s_2 is the decode signal transmitted from the best relay in the second phase.

After employing MRC at Bob and at the eavesdropper, the instantaneous SNR at Bob (γ_{Bob}) is given by

$$\gamma_{\text{Bob}} = \frac{\left(P_A \mid h_{x_o} \mid^2 + P_R \mid h_{x_i} \mid^2\right)}{N_o}. \quad (6)$$

Correspondingly, the instantaneous SNR at the eavesdropper (γ_{E}) is specified as

$$\gamma_{\text{E}} = \frac{\left(P_A \mid h_{y_o} \mid^2 + P_R \mid h_{y_i} \mid^2\right)}{N_o} \quad (7)$$

where N_0 is a variance of AWGN.

B. Relay Selection Technique

In this subsection we present a suggested relay selection algorithm, that may be applied to enhance the physical layer security of cooperative relay communications in the presence of an eavesdropper node with existing direct links. The optimal relay is selected in order to maximize the signal-to-noise ratio at Bob

$$\arg \max_{1 \le n \le N} \gamma_n \quad (8)$$

where γ_n is the SNR between the nth relay and Bob, with perfect channels between the relays and Bob. Bob then feeds back the selected best relay via a low-rate feedback channel.

C. Channel Statistics

Here we present the statistics for γ_{Bob} and γ_{E}. Due to Rayleigh fading, the direct link channel from Alice to Bob (x_o) is an independent exponential with mean $\mathbb{E}[x_o] = 1/\lambda_o$. Also, the relay channels to Bob are $\{x_1, \ldots, x_N\}$, where x_i is an independent exponential with mean $\mathbb{E}[x_i] = 1/\lambda_i$. The direct link channel from Alice to the eavesdropper (y_o) is an independent exponential with mean $\mathbb{E}[y_o] = 1/\mu_o$, and the relay channels to the eavesdropper are $\{y_1, \ldots, y_N\}$, where y_i is an independent exponential with mean $\mathbb{E}[y_i] = 1/\mu_i$.

As mentioned in the previous section, after applying MRC at Bob, the instantaneous SNR at Bob is the summation of the two SNRs from the direct link and the best relay.

Thus

$$\gamma_{\text{Bob}} = \gamma_{h_{x_o}} + \max\left(\gamma_{h_{x_1}}, \ldots, \gamma_{h_{x_N}}\right). \quad (9)$$

The probability

$$\Pr\left(\max\left(\gamma_{h_{x_1}}, \ldots, \gamma_{h_{x_N}}\right) \le x\right) = \prod_{i=1}^{N} \left(1 - e^{-\lambda_i x}\right) \quad (10)$$

can then be rewritten in the following desirable form

$$\Pr\left(\max\left(\gamma_{h_{x_1}}, \ldots, \gamma_{h_{x_N}}\right) \le x\right) = \sum_{\boldsymbol{b} \in \mathcal{B}} (-1)^r e^{-x \boldsymbol{\lambda}^T \boldsymbol{b}} \quad (11)$$

where $\mathcal{B}$ is the set of all binary vectors of length of number of relays N and $r = \sum_{i=1}^{N} b_i$.

Let A_i be the event when x_i is selected, then

$$\begin{aligned} f(x, A_i) &= \lambda_i e^{-\lambda_i x} \prod_{n \ne i}^{N} \left(1 - e^{-\lambda_n x}\right) \\ &= \lambda_i \sum_{\boldsymbol{b} \in \mathcal{B}_i} (-1)^{r-1} e^{-x \boldsymbol{\lambda}^T \boldsymbol{b}} \end{aligned} \quad (12)$$

where $\mathcal{B}_i$ is the set of all binary vectors of the length of the number of relays N with $b_i = 1$.

It therefore follows that

$$\begin{aligned} \Pr(\gamma_{\text{Bob}} > x, A_i) &= \int_x^{\infty} \lambda_i \sum_{\boldsymbol{b} \in \mathcal{B}_i} (-1)^{r-1} e^{-x \boldsymbol{\lambda}^T \boldsymbol{b}} dx \\ &= \lambda_i \sum_{\boldsymbol{b} \in \mathcal{B}_i} (-1)^{r-1} \frac{1}{\boldsymbol{\lambda}^T \boldsymbol{b}} e^{-x \boldsymbol{\lambda}^T \boldsymbol{b}}. \end{aligned} \quad (13)$$

The probability distribution function (PDF) at Bob γ_{Bob} is provided in (14)

Proof: see Appendix A. ∎

$$f_{\gamma_{\text{Bob}}}(x) = \lambda_0 \sum_{\boldsymbol{b} \in \mathcal{B}} (-1)^r \frac{\lambda_0 e^{-\lambda_0 x} - \boldsymbol{\lambda}^T \boldsymbol{b} e^{-\boldsymbol{\lambda}^T \boldsymbol{b} x}}{\lambda_0 - \boldsymbol{\lambda}^T \boldsymbol{b}}. \quad (14)$$

Likewise, the PDF of γ_E is specified in (15)

Proof: see Appendix B. ∎

$$f_{\gamma_E}(x) = \frac{\mu_i \mu_o}{\mu_i - \mu_o} \left(e^{-\mu_o x} - e^{-\mu_i x}\right) \sum_{i=1}^{N} p_i \quad (15)$$

where p_i is the probability that the ith relay is selected, and is given by

$$p_i = \Pr(A_i) = \int_0^\infty f(x, A_i)\, dx = \lambda_i \sum_{b \in \mathcal{B}_i} \frac{(-1)^{r-1}}{\boldsymbol{\lambda}^T \boldsymbol{b}}. \quad (16)$$

III. Secrecy Outage Probability Analysis

In this section, we analyze the achievable secrecy outage probability performance of the system, according to the selection criteria set out in (8).

Secrecy capacity is defined as

$$C_s = \begin{cases} C_{Bob} - C_E & , \gamma_{\mathrm{Bob}} > \gamma_{\mathrm{E}} \\ 0 & , \gamma_{\mathrm{Bob}} \leq \gamma_{\mathrm{E}} \end{cases} \quad (17)$$

where the capacity of Bob's channel is expressed as

$$C_{Bob} = \log_2(1 + \gamma_{\mathrm{Bob}}) \quad (18)$$

and the capacity of the eavesdropper's channel is described as

$$C_E = \log_2(1 + \gamma_{\mathrm{E}}). \quad (19)$$

The performance of the system is characterized by the secrecy outage probability, which is defined as the probability that the instantaneous secrecy capacity C_s will be less than the target secrecy rate R_s [24]

$$P_{\mathrm{out}} = \Pr(C_s < R_s). \quad (20)$$

We can rewrite the ratio between the capacity of Bob's channel and the capacity of the eavesdropper's channel as

$$\eta = \frac{1 + \gamma_{\mathrm{Bob}}}{1 + \gamma_E} \quad (21)$$

and from (29) we can get

$$\Pr(\gamma_E > y|_{A_i}) = \frac{\mu_i e^{-\mu_o y} - \mu_o e^{-\mu_i y}}{\mu_i - \mu_o}. \quad (22)$$

Now consider the following conditional probability

$$\Pr(\eta < R_s|_{\gamma_{\mathrm{Bob}}}, A_i) = \Pr\left(\gamma_E > \left(\frac{1 + \gamma_{\mathrm{Bob}}}{R_s}\right) - 1|_{\gamma_{\mathrm{Bob}}}, A_i\right) \quad (23)$$

by applying (22) we can rewrite (23) as

$$\Pr(\eta < R_s|_{\gamma_{\mathrm{Bob}}}, A_i) = \begin{cases} (\zeta - \delta), & \gamma_{\mathrm{Bob}} > R_s - 1 \\ 1, & \gamma_{\mathrm{Bob}} \leq R_s - 1 \end{cases} \quad (24)$$

where $\zeta = \mu_i \exp\left(-\mu_o \left(\frac{1-R_s}{R_s}\right)\right) \exp\left(-\mu_o \frac{\gamma_{\mathrm{Bob}}}{R_s}\right) / (\mu_i - \mu_o)$ and $\delta = \mu_o \exp\left(-\mu_i \left(\frac{1-R_s}{R_s}\right)\right) \exp\left(-\mu_i \frac{\gamma_{\mathrm{Bob}}}{R_s}\right) / (\mu_i - \mu_o)$.

Therefore

$$\Pr(\eta \leq R_s) = \sum_{n=1}^{N} \int_{\gamma_{\mathrm{Bob}}} \Pr(\eta < R_s|_{\gamma_{\mathrm{Bob}}}, A_i) \times \Pr(\gamma_{\mathrm{Bob}}, A_i)\, \mathrm{d}\gamma_{\mathrm{Bob}} \quad (25)$$

and

$$\Pr(\eta \leq R_s) = \lambda_o \sum_{\boldsymbol{b} \in \mathcal{B}} (-1)^r \left(\frac{e^{-\boldsymbol{\lambda}^T \boldsymbol{b}(R_s - 1)} - e^{-\lambda_o (R_s - 1)}}{\lambda_o - \boldsymbol{\lambda}^T \boldsymbol{b}}\right) + \sum_{n=1}^{N} \int_{\gamma_{\mathrm{Bob}} > (\mathrm{R_s} - 1)} (\zeta - \delta)\, \mathrm{d}\gamma_{\mathrm{Bob}}. \quad (26)$$

By computing the integration in (26), a closed form expression for secrecy outage probability is obtained as shown in (27) at the top of the next page.

IV. Simulation Results and Discussion

In this section, we investigate the performance of the secrecy outage probability for decode and forward relay selection in cooperative network, with existing direct links over i.n.i.d. Rayleigh fading channels. The analytical results are validated using a Monte-Carlo simulation, which was executed over 10^5 independent trials. The results were computed for the special case where $\lambda_i = 1$ and $\mu_i = 0.7$.

Fig. 2 illustrates the secrecy outage probability of a cooperative relay communications system with existing direct links, versus average SNR in Rayleigh fading channels. Here, we set $R_s = 1$ bits/sec/Hz, $\lambda_o = 0.6$, $\mu_o = 0.8$, and the number of relays is set to 3, 5, and 9. The analytical results of (27), and the Monte-Carlo simulation results for secrecy outage probability performance for the i.n.i.d. Rayleigh fading channels, are depicted by solid lines and circle markers, respectively. The analytical results agree with the Monte-Carlo simulation, in that secrecy outage probability improves in accordance with an increased number of relays in the network. This finding could be attributed to the greater availability of potential decoding relays.

In order to assess the secrecy outage probability of a network with existing direct links, versus the number of relays, we also set $R_s = 1$ bits/sec/Hz, $\lambda_o = 0.6$, $\mu_o = 0.8$ and an average SNR resolved to 2, 5 and 10, the results are plotted in Fig. 3. It is evident that the analytical results match the simulation results, and we observed that when the average SNR increased in parallel with an increasing number of relays, the secrecy outage probability improved notably.

Fig. 4 shows the performance of the secrecy outage probability for a network with existing direct links, versus λ_o. A fixed number of five relays was used, and the secrecy rate was varied for different values: 0.5, 1, and 1.5. Other parameters were $\lambda_i = 1$, $\mu_i = 0.7$ and $\mu_o = 0.8$. It was noted that, when the quality of the direct link's channel to the legitimate user (Bob) increased, the secrecy outage probability improved

$$P_{\text{out}}(R_s) = \lambda_o \sum_{\boldsymbol{b}\in\mathcal{B}} (-1)^r \left(\frac{e^{-\boldsymbol{\lambda}^T \boldsymbol{b}(R_s-1)} - e^{-\lambda_o(R_s-1)}}{\lambda_o - \boldsymbol{\lambda}^T \boldsymbol{b}} \right) + \sum_{i=1}^{N} \sum_{\boldsymbol{b}\in B_i} (-1)^{r-1} \frac{\lambda_i}{\mu_i - \mu_o} \left(\frac{\mu_i}{\boldsymbol{\lambda}^T \boldsymbol{b} R_s + \mu_o} - \frac{\mu_i}{\boldsymbol{\lambda}^T \boldsymbol{b} R_s + \mu_i} \right) R_s e^{-\boldsymbol{\lambda}^T \boldsymbol{b}(R_s-1)}. \quad (27)$$

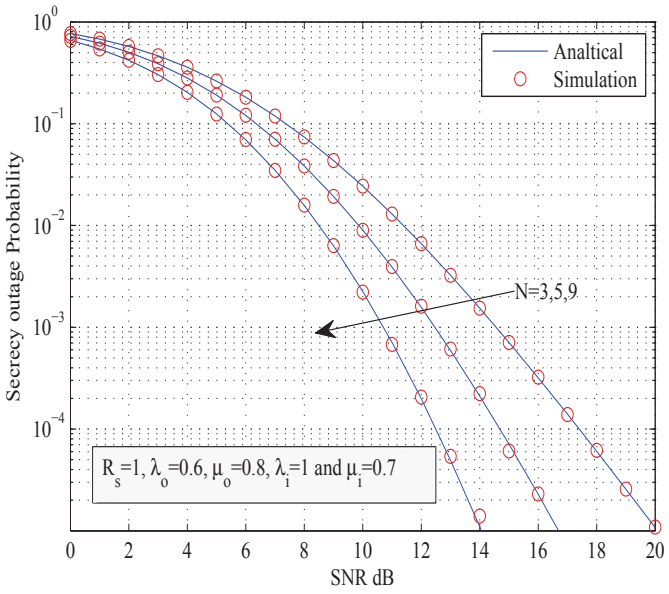

Fig. 2. Secrecy outage probability of a cooperative relay communications system versus an average SNR over Rayleigh fading channels for $R_s = 1$, $\lambda_0 = 0.6$, $\mu_0 = 0.8$, $\lambda_i = 1$, $\mu_i = 0.7$ and $N = 3, 5, 9$.

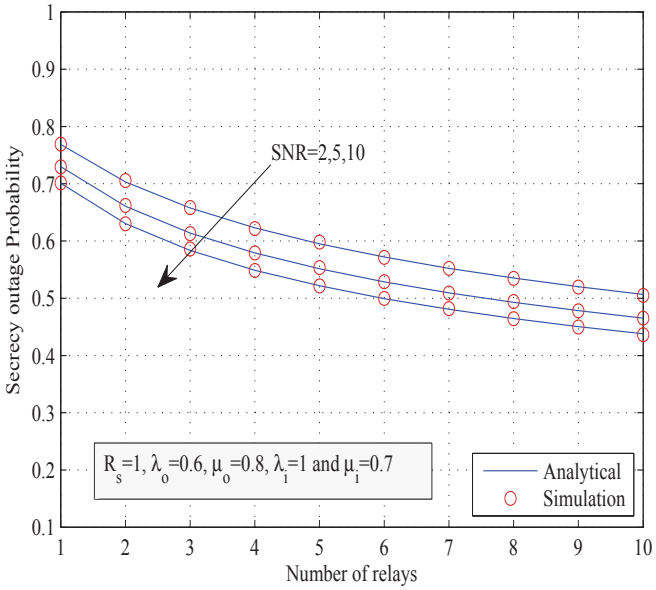

Fig. 3. Secrecy outage probability of a cooperative relay communications system versus a number of relays over Rayleigh fading channels for $R_s = 1$, $\lambda_0 = 0.6$, $\mu_0 = 0.8$, $\lambda_i = 1$, $\mu_i = 0.7$ and SNR $= 2, 5$ and 10.

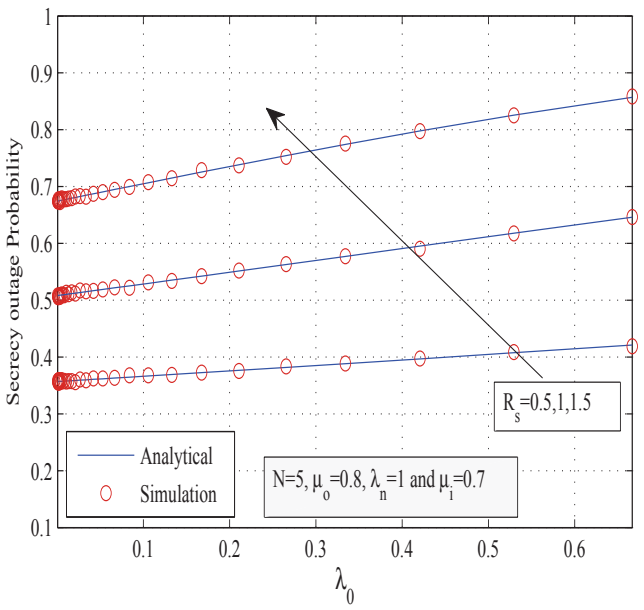

Fig. 4. Secrecy outage probability of a cooperative relay communications system versus λ_o values over Rayleigh fading channels for $N = 5$, $\mu_0 = 0.8$, $\lambda_i = 1$, $\mu_i = 0.7$, and $R_s = 0.5, 1$ and 1.5

somewhat. Similarly, when the secrecy rate increased from 0.5 to 1.5, the secrecy outage probability for the proposed system model decreased.

V. Conclusion

In this paper, a practical setting was considered in which pre-existing direct links between sender and receiver nodes were employed in order to improve the secrecy outage probability of a cooperative communication system with non-identical distribution. The model assumed the presence of trusted cluster relays implementing an MRC scheme at the receiver's terminal, with the eavesdropper's CSI unknown at the sender and the best relay. Analytical results were obtained in closed form, which aided computation. Future work will seek to determine ergodic secrecy capacity with full CSI and without being at the sender terminals.

Appendix A
Proof of Equation (14)

In this appendix, we aim to derive the probability distribution function for γ_{Bob}.

The instantaneous SNR at Bob is the summation of the two SNRs from the direct link and the best relay, accordingly

$$\begin{aligned}\Pr\left(\gamma_{\text{Bob}} \leq x\right) &= \Pr\left(\gamma_{x_o} + \max\left(\gamma_{h_{x_1}}, \ldots, \gamma_{h_{x_N}}\right) \leq x\right) \\ &= \Pr\left(\max\left(\gamma_{h_{x_1}}, \ldots, \gamma_{h_{x_N}}\right) \leq x - \gamma_{h_{x_o}}\right) \\ &= \begin{cases} \prod_{i=1}^{N}\left(1 - e^{-\lambda_i\left(x-\gamma_{h_{x_o}}\right)}\right), & x \geq \gamma_{h_{x_o}} \\ 0, & x < \gamma_{h_{x_o}} \end{cases}\end{aligned}$$

Therefore

$$\begin{aligned}\Pr\left(\gamma_{\text{Bob}} \leq x\right) &= \int_0^x \prod_{i=1}^{N}\left(1 - e^{-\lambda_i\left(x-\gamma_{h_{x_o}}\right)}\right) \\ &\quad \times \lambda_o e^{-\lambda_o \gamma_{h_{x_o}}} d\gamma_{h_{x_o}} \\ &= \sum_{\boldsymbol{b}\in\mathcal{B}} (-1)^r \lambda_o \int_0^x e^{-\left(x-\gamma_{h_{x_o}}\right)\boldsymbol{\lambda}^T\boldsymbol{b}} e^{-\lambda_o x} d\gamma_{h_{x_o}} \\ &= \lambda_o \sum_{\boldsymbol{b}\in\mathcal{B}} (-1)^r \frac{e^{-\boldsymbol{\lambda}^T\boldsymbol{b}x} - e^{-\lambda_o x}}{\lambda_o - \boldsymbol{\lambda}^T\boldsymbol{b}} \end{aligned} \tag{28}$$

We obtain the desired result of a probability distribution function for γ_{Bob} in (14) by differentiating (28).

APPENDIX B
PROOF OF EQUATION (15)

Consider the following conditional probability

$$\begin{aligned}\Pr\left(\gamma_E > y | A_i\right) &= \Pr\left(\gamma_{h_{y_o}} + \gamma_{h_{y_i}} > y\right) \\ &= \Pr\left(\gamma_{h_{y_o}} > y - \gamma_{h_{y_i}}\right) \\ &= \begin{cases} e^{-\mu_o\left(y-\gamma_{h_{y_i}}\right)}, & \gamma_{h_{y_o}} < y \\ 1, & \gamma_{h_{y_i}} > y \end{cases}\end{aligned}$$

where $\gamma_{h_{y_o}}$ is the SNR for the direct link from Alice to the eavesdropper and $\gamma_{h_{y_i}}$ is the SNR for the channel from the best relay to the eavesdropper. Accordingly,

$$\begin{aligned}\Pr\left(\gamma_E > y | A_i\right) &= \int_0^y \left(e^{-\mu_o\left(y-\gamma_{h_{y_i}}\right)}\right) \mu_i e^{-\mu_i \gamma_{h_{y_i}}} d\gamma_{h_{y_i}} \\ &\quad + \int_y^\infty \mu_i e^{-\mu_i \gamma_{h_{y_i}}} d\gamma_{h_{y_i}} \\ &= \frac{1}{\mu_i - \mu_o}\left(\mu_i e^{-\mu_o y} - \mu_o e^{-\mu_i y}\right) \end{aligned} \tag{29}$$

Therefore

$$\begin{aligned}\Pr\left(\gamma_E < y | A_i\right) &= 1 - \left(\frac{1}{\mu_i - \mu_o}\left(\mu_i e^{-\mu_o y} - \mu_o e^{-\mu_i y}\right)\right) \\ &= 1 + \left(\frac{1}{\mu_i - \mu_o}\left(\mu_o e^{-\mu_i y} - \mu_i e^{-\mu_o y}\right)\right) \end{aligned} \tag{30}$$

The corresponding PDF is

$$f_{\gamma_{\text{E}}}\left(x | A_i\right) = \frac{\mu_i \mu_o}{\mu_i - \mu_o}\left(e^{-\mu_o x} - e^{-\mu_i x}\right) \tag{31}$$

By applying (16) in (31) we can obtain the PDF of γ_E in (15).

REFERENCES

[1] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2515–2534, Jun. 2008.

[2] L. Lai and H. El Gamal, "The relay eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4005–4019, Sep. 2008.

[3] J. Laneman, D. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, pp. 3062–3080, Dec. 2004.

[4] Y. Zhao, R. Adve, and T. J. Lim, "Outage probability at arbitrary snr with cooperative diversity," *IEEE Commun. Lett.*, vol. 9, no. 8, pp. 700–702, Aug. 2005.

[5] S. Ikki and M. Ahmed, "Performance analysis of adaptive decode-and-forward cooperative diversity networks with best-relay selection," *IEEE Trans. Commun.*, vol. 58, pp. 68–72, Jan. 2010.

[6] A. Ibrahim, A. Sadek, W. Su, and K. Liu, "Cooperative communications with relay-selection: when to cooperate and whom to cooperate with," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2814–2827, Jul. 2008.

[7] L. Sun, T. Zhang, L. Lu, and H. Niu, "Cooperative communications with relay selection in wireless sensor networks," *IEEE Trans. Consum. Electron.*, vol. 55, pp. 513–517, May 2009.

[8] Y. Luo, J. Zhang, and K. Letaief, "Relay selection for energy harvesting cooperative communication systems," in *IEEE Global Commun. Conf.*, pp. 2514–2519, Dec. 2013.

[9] E. Alotaibi and K. Hamdi, "Secrecy outage probability of relay networking in multiple destination and eavesdropper scenarios," in *IEEE Wireless Commun. and Netw. Conf.*, pp. 2390–2395, Apr. 2014.

[10] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, pp. 5003–5011, Oct. 2009.

[11] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, pp. 2653–2661, Jul. 2014.

[12] M. Sarkar, T. Ratnarajah, and Z. Ding, "Beamforming with opportunistic relaying for wireless security," *IET Commun.*, vol. 8, pp. 1198–1210, May 2014.

[13] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, pp. 2653–2661, Jul. 2014.

[14] Z. Zhang, X. Chai, K. Long, A. Vasilakos, and L. Hanzo, "Full duplex techniques for 5g networks: self-interference cancellation, protocol design, and relay selection," *IEEE Commun. Mag.,*, vol. 53, pp. 128–137, May 2015.

[15] Z. Zhang, X. Wang, K. Long, A. Vasilakos, and L. Hanzo, "Large-scale mimo-based wireless backhaul in 5g networks," *IEEE Commun. Mag.,*, vol. 22, pp. 58–66, Oct. 2015.

[16] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless. Netw.*, vol. 21, no. 6, pp. 1835–1846, 2015.

[17] K. Liu, X. Chang, F. Liu, X. Wang, and A. V. Vasilakos, "A cooperative mac protocol with rapid relay selection for wireless ad hoc networks," *Comput. Netw.*, vol. 91, no. C, pp. 262–282, 2015.

[18] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Commun.*, vol. 4, pp. 1787–1791, Oct. 2010.

[19] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, pp. 6076–6085, Dec. 2013.

[20] A. Jindal, C. Kundu, and R. Bose, "Secrecy outage of dual-hop af relay system with relay selection without eavesdropper's csi," *IEEE Commun. Lett.*, vol. 18, pp. 1759–1762, Oct. 2014.

[21] A. Jindal, C. Kundu, and R. Bose, "Secrecy outage of dual-hop af relay system with relay selection without eavesdropper's csi," *IEEE Commun. Lett.*, vol. 18, pp. 1759–1762, Oct. 2014.

[22] L. Wang, K. J. Kim, T. Duong, M. Elkashlan, and H. Poor, "Security enhancement of cooperative single carrier systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 90–103, Jan. 2015.

[23] J. Hu and N. Beaulieu, "Performance analysis of decode-and-forward relaying with selection combining," *IEEE Commun. Lett.*, vol. 11, pp. 489–491, Jun. 2007.

[24] E. Alotaibi and K. Hamdi, "Relay selection for multi-destination in cooperative networks with secrecy constraints," in *IEEE 80th Veh. Technol. Conf. (VTC Fall)*, pp. 1–5, Sept. 2014.