Regular Article

Multihop Decode-and-Forward Relay Networks: Secrecy Analysis and Relay Position Optimization

Vo Nguyen Quoc Bao[1], **Nguyen Linh-Trung**[2]

[1] Dept. Telecommunications, Posts and Telecommunication Institute of Technology, Vietnam.
[2] Fac. Electronics & Telecommunications, VNU University of Engineering & Technology, Hanoi, Vietnam.

Correspondence: Vo Nguyen Quoc Bao, baovnq@ptithcm.edu.vn

Manuscript communication: received 23 November 2011, accepted 10 July 2012

Abstract– **Relay communication has advantages over direct transmission in terms of secrecy capacity. In this paper, the performance of secrecy, offered by multihop decode-and-forward relaying, is investigated and compared to its counterpart in direct transmission. Three key performance measures are derived over Rayleigh fading channels: probability of non-zero secrecy capacity, secure outage probability and secrecy capacity, which are valid for an arbitrary number of hops. Based on the tractable form of the probability of non-zero secrecy capacity, the optimization problem of trusty relay replacement is also studied. Numerical results indicate that a proper relay replacement can increase the network security without extra network resources. The correctness of analytical results is confirmed by using a MATLAB-based independent simulation model.**

Keywords– **Secrecy capacity, decode-and-forward, multihop networks, probability of non-zero secrecy capacity, secure outage probability.**

This work was supported under Project 39/2012/HĐ/NĐT granted by the Ministry of Science and Technology of Vietnam.

1 Introduction

Multihop communication has been shown to be an effective way to extend the coverage of a wireless network as well as to combat the adverse effects of wireless fading channels without using more network resources [1]. The basic idea is that the communication from a source node to a destination node in the network is allowed to be relayed by the assistance of intermediate nodes [2], [3].

A concept of perfect secrecy was introduced by Shannon in 1949 when dealing with secure communication [4]. This is the ability of a communication system to be secure against cryptanalysis when an eavesdropper has unlimited time and manpower available for the analysis of intercepted cryptograms. Recently, relayed transmission is particularly attractive in physical (PHY) layer security, which exploits the physical characteristics of wireless channels for secure transmission [5]. In particular, while direct transmission leads to zero secrecy capacity in some network scenarios, it was shown that by introducing one or more relays a positive secrecy capacity can be achieved in such scenarios.

In [6], three cooperation strategies relay-eavesdropper channels were proposed, including noise-forwarding (NF), compress-and-forward (CF), and amplify-and-forward (AF) and the corresponding achievable performance bounds were provided. Secrecy capacity optimization was studied for AF-based and decode-and-forward (DF)-based cooperative networks in the presence of one eavesdropper or more [7], [8]. Under secrecy constraints, relay and jammer selection in cooperative systems were dealt with in [9] wherein jamming was shown to be an efficient technique for networks with strong eavesdropper links. Considering the environment where multiple trusty relays are available, an efficient relay selection scheme was proposed in [10], taking into account both legitimate and eavesdropper channels in the relay selection metric and, hence, resulting in a significant system secrecy capacity. For two-way relay networks, secure performance analysis in terms of symbol error rate confirms that the eavesdropper has more chance to eavesdrop the message when it is located close to one of the transmitters [11]. Recently, relays which are untrusted have been studied and it has been shown that they could be used to help the source and the destination to communicate despite being subjected to the secrecy constraints [12]. By assuming the correlation between the legitimate and eavesdropper channels, a closed-form expression of the asymptotic secrecy capacity has been derived and its behaviors in various situations have been extensively studied [13]. Non-cooperative secure beamforming and cooperative secure beamforming, as two ways to transmit confidential information of the source to the destination via an untrusted relay, were proposed in [14]. It was shown that the cooperative scheme should only be deployed if the transmit power of the relay is high, the number of relay antennas is large, and the distance between the source and the relay is small as compared to that between the source and the destination.

Above, most of the performance analysis of wireless systems under PHY layer security has been concentrated on *two-hop* relaying. In this paper, we investigate the information-theoretic security of *multihop* DF relay networks for the first time. Three secure performance measures, which are the non-zero secrecy capacity probability, the secrecy outage probability and the secrecy capacity, are analyzed over the most generalized channel model which includes independently identically distributed (i.i.d.) and independently non-identically distributed (i.n.d.) Rayleigh fading channels as special cases. Closed-form expressions as well as easy-to-evaluate asymptotic solutions for the above secure performance measures are provided for an arbitrary number of hops. From the analysis, we can gain important insights in the design of a relay network and realize the impact of some key network parameters on the behavior of the network. For example, we can determine the optimal number of hops so as to have the best secrecy capacity or the optimal trusty relay positions under given fixed positions of the source, destination and eavesdropper. In particular, based on the tractable form of the non-zero secrecy capacity probability, the optimization problem of relay placement is solved.

In detailing the above contributions, the paper is divided into the following sections. The system and channel models are first described in Section 2. To obtain the secure performance metrics, the cumulative distribution function (CDF) and probability density function (PDF) of the equivalent end-to-end secrecy signal-to-noise ratio (SNR) are also established. Next, in Section 3, the secure performance is analyzed in terms of the probability of non-zero secrecy capacity, the secrecy outage probability and the secrecy capacity. Then, in Section 4, the optimization problem of trusty relay positions is solved. In Section 5, the performance analysis is verified by Monte-Carlo simulation, together with a study of the system behaviors at high SNR regime. Finally, conclusions are drawn in Section 6.

2 System Model

Consider a multihop DF network under security constraints as shown in Figure 1. The network consists of one source denoted by T_0 and one destination denoted by T_K, in the existence of an eavesdropper denoted by E. Suppose that no direct link between the source and the destination is available and the communication is performed by the assistance of $K-1$ trusty relays, denoted by T_1, ..., and T_{K-1}. In particular, each intermediate relay fully decodes the received confidential signal and then forwards the re-encoded signal to the next legitimate node over a wireless fading channel, which is referred to hereafter as a main channel. Meanwhile, at each hop, the eavesdropper also attempts to decode the message over an eavesdropper channel. For simplicity, we assume that the eavesdropper cannot do joint decoding. In practice, this assumption can be realized by using randomized code-books at each hop to confuse the eavesdropper [12]. We further assume that a transmitter (source or relay) has full channel state information (CSI) of both the corresponding main and eavesdropper channels. It is a widely adopted assumption in the literature for communication systems under secrecy constraints (see for examples [9], [10]).

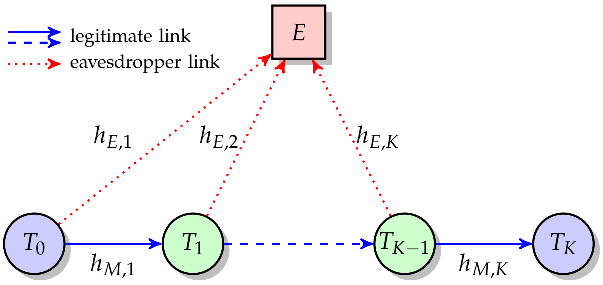

Figure 1. Multihop DF relay network under secrecy constraints.

Denote by $h_{M,k}$ and $h_{E,k}$ the channel coefficients of the main and eavesdropper links in hop k, respectively. Under Rayleigh fading, the corresponding channel gains, $|h_{M,k}|^2$ and $|h_{E,k}|^2$, are exponentially distributed with distribution parameters $\lambda_{M,k}$ and $\lambda_{E,k}$. As a result, the instantaneous signal-to-noise ratios (SNRs) of the main and eavesdropper link are respectively

$$\gamma_{M,k} = \frac{P_k |h_{M,k}|^2}{\mathcal{N}_0}, \tag{1}$$

$$\gamma_{E,k} = \frac{P_k |h_{E,k}|^2}{\mathcal{N}_0}, \tag{2}$$

where P_k denotes the average transmit power at hop k and $\mathcal{N}_0$ is the variance of additive white Gaussian noise (AWGN) at the receivers. By introducing the general notation $Z \in \{M, E\}$, the PDF and CDF of $\gamma_{Z,k}$ are given by

$$f_{\gamma_{Z,k}}(\gamma) = \frac{1}{\bar{\gamma}_{Z,k}} e^{-\frac{\gamma}{\bar{\gamma}_{Z,k}}}, \tag{3}$$

$$F_{\gamma_{Z,k}}(\gamma) = 1 - e^{-\frac{\gamma}{\bar{\gamma}_{Z,k}}}, \tag{4}$$

where $\bar{\gamma}_{Z,k} = P_k \lambda_{Z,k}$.

3 Secure Performance Analysis

In this section, we derive exact and asymptotic closed-form expressions of key secure performance measures for the network scenario under consideration. We start with the definition of the secrecy capacity at hop k, which is given by [4]

$$C_k \triangleq \left[\log_2\left(\frac{1+\gamma_{M,k}}{1+\gamma_{E,k}}\right)\right]^+, \tag{5}$$

where $[x]^+ \triangleq \max(x, 0)$. To facilitate the analysis, we denote by

$$\gamma_k = \frac{1+\gamma_{M,k}}{1+\gamma_{E,k}}, \tag{6}$$

the secrecy SNR of hop k and present the following lemma.

Lemma 1 *Under Rayleigh fading, the CDF of γ_k is given by*

$$F_{\gamma_k}(\gamma) = 1 - e^{-\frac{\gamma-1}{\bar{\gamma}_{M,k}}} \frac{\alpha_k}{\gamma + \alpha_k}, \tag{7}$$

where $\alpha_k = \bar{\gamma}_{M,k}/\bar{\gamma}_{E,k}$.

Proof: The CDF of γ_k can be expressed as

$$\begin{aligned} F_{\gamma_k}(\gamma) &= \Pr\left[\frac{1+\gamma_{M,k}}{1+\gamma_{E,k}} < \gamma\right] \\ &= \int_0^\infty F_{\gamma_{M,k}}\left(\gamma(1+\gamma_{E,k}) - 1\right) f_{\gamma_{E,k}}(\gamma_{E,k}) d\gamma_{E,k}. \end{aligned}$$

Plugging (3) and (4) into the above result yields

$$F_{\gamma_k}(\gamma) = \int_0^\infty \left[1 - e^{-\frac{\gamma(1+\gamma_{E,k})-1}{\bar{\gamma}_{M,k}}}\right] \frac{1}{\bar{\gamma}_{E,k}} e^{-\frac{\gamma_{E,k}}{\bar{\gamma}_{E,k}}} d\gamma_{E,k}.$$

By making use of $\int_0^\infty f_{\gamma_{E,k}}(\gamma) d\gamma = 1$ and with the help of the integral expression $\int_0^\infty e^{-px} dx = 1/p$ [15, Eq. (3.310)], we can obtain (7). ■

For multihop DF relaying under security constraints, the system is defined to be in outage whenever the data transmission in any hop is either unsuccessfully decoded or imperfectly secure. In addition, under the assumption that the direct link between the source and the destination is not available and considering the fact that the secure outage decisions are taken on a per hop basis, the secrecy SNR of the system can be expressed as

$$\gamma_{\text{e2e}} = \min_k \gamma_k. \tag{8}$$

It is worth mentioning that such a form is similar to that of conventional multihop DF relay networks. However, secrecy SNR is used here instead of instantaneous SNR. It is due to the fact that in view of security the weakest hop dominates the secrecy system performance.

We now derive the CDF of γ_{e2e}, which will be useful later for the derivation of the performance metrics. Assuming that all γ_k are independent of each other, we have

$$\begin{aligned} F_{\gamma_{\text{e2e}}}(\gamma) &= 1 - \Pr[\gamma_1 > \gamma, \ldots, \gamma_K > \gamma] \\ &= 1 - \prod_{k=1}^K (1 - F_{\gamma_k}(\gamma)). \end{aligned} \tag{9}$$

Inserting (7) into (9) gives

$$F_{\gamma_{\text{e2e}}}(\gamma) = 1 - e^{\chi(1-\gamma)} \prod_{k=1}^K \frac{\alpha_k}{\gamma + \alpha_k}, \tag{10}$$

where $\chi = \sum_{k=1}^K 1/\bar{\gamma}_{M,k}$.

3.1 Probability of Non-zero Secrecy Capacity

The probability of nonzero secrecy capacity represents the probability that Shannon capacity of the main channel is greater than that of the eavesdropper channel. For multihop DF relay networks, it is given by

$$\Pr[\mathcal{C} > 0] = \Pr\left[\frac{1}{K}\log_2(\gamma_{\text{e2e}}) > 0\right]. \tag{11}$$

In (11), the factor $1/K$ accounts for the fact that the overall transmission is split into K phases. In addition, since $\log_2(\gamma_{\text{e2e}}) > 0$ is equivalent to $\gamma_{\text{e2e}} > 1$, Eq. (11) can be rewritten as

$$\begin{aligned} \Pr[\mathcal{C} > 0] &= \Pr[\gamma_{\text{e2e}} > 1] \\ &= 1 - F_{\gamma_{\text{e2e}}}(1) \\ &= \prod_{k=1}^K \frac{\alpha_k}{\alpha_k + 1}. \end{aligned} \tag{12}$$

It is clearly recognized that the probability of nonzero secrecy capacity is determined by the channel gain ratios between the legitimate and eavesdropper channels rather than the average channel powers. Such a fact will be the motivating point to investigate the optimal relay positions, which will be presented in detail in Section 4.

To gain further insights, we study here two limiting cases: $\alpha_k \gg 1$ and $\alpha_k \ll 1$, corresponding to the cases wherein the eavesdropper is located very far or very closely to the trusty nodes, respectively. From (12), it is straightforward to arrive at

$$\Pr[\mathcal{C} > 0] \to \begin{cases} 1, & \alpha_k \gg 1, \\ \prod\limits_{k=1}^K \alpha_k, & \alpha_k \ll 1. \end{cases} \tag{13}$$

From (13), we can see that if the channel gain ratios between the legitimate and eavesdropper channels are large the probability of nonzero secrecy capacity reaches to 100%. On the other hand, if these ratios are relatively small, the probability of non-zero secrecy capacity will depend not only on them but also on the number of hops.

3.2 Secure Outage Probability

Having obtained the CDF of γ_{e2e}, we can now derive the secrecy outage probability. According to [6], the secure outage probability is defined as the probability that information-theoretic security of the multihop relay system is compromised. For a given secure target rate R, and with $\mathcal{C} > 0$, the secrecy outage probability $\Pr[\mathcal{C} < R]$ can be expressed as follows using the total probability theorem:

$$\begin{aligned} \Pr[\mathcal{C} < R] =& \Pr[\mathcal{C} < 0] \Pr[\mathcal{C} < R | \mathcal{C} < 0] \\ &+ \Pr[\mathcal{C} > 0] \Pr[\mathcal{C} < R | \mathcal{C} > 0]. \end{aligned} \tag{14}$$

Using the positivity notion in the definition of the secrecy capacity, we can see that $\Pr(\mathcal{C} < R | \mathcal{C} < 0) = 1$. Hence,

$$\begin{aligned} \Pr(\mathcal{C} < R) &= \Pr(\mathcal{C} < 0) + \Pr(0 < \mathcal{C} < R) \\ &= F_{\gamma_{\text{e2e}}}(2^{KR}) \\ &= 1 - \prod_{k=1}^K e^{-\frac{2^{KR}-1}{\bar{\gamma}_{M,k}}} \frac{\alpha_k}{2^{KR} + \alpha_k}. \end{aligned} \tag{15}$$

3.3 Secrecy Capacity

We now turn our attention to the system secrecy capacity, which is defined as

$$\overline{\mathcal{C}} \triangleq \frac{1}{K} \int_1^\infty \log_2(\gamma) f_{\gamma_{\text{e2e}}}(\gamma) d\gamma. \tag{16}$$

To obtain $\overline{\mathcal{C}}$, we first need to derive $f_{\gamma_{\text{e2e}}}(\gamma)$, which is related to $F_{\gamma_{\text{e2e}}}(\gamma)$ by $f_{\gamma_{\text{e2e}}}(\gamma) = \frac{d}{d\gamma}\left[F_{\gamma_{\text{e2e}}}(\gamma)\right]$. By partial fraction expansion, $F_{\gamma_{\text{e2e}}}(\gamma)$ can be written as

$$F_{\gamma_{\text{e2e}}}(\gamma) = 1 - e^{\chi(1-\gamma)}\sum_{i=1}^{N}\sum_{j=1}^{r_i}\frac{A_{ij}}{(\gamma+\beta_i)^j}, \tag{17}$$

where $\beta_1, \beta_2, \ldots, \beta_N$ denote N distinct elements in decreasing order of $\alpha_1, \ldots, \alpha_K$, the numerators

$$A_{ij} = \frac{1}{(r_i-j)!}\frac{d^{(r_i-j)}}{d\gamma^{(r_i-j)}}\left[(\gamma+\alpha_i)^{r_i}\prod_{k=1}^{K}\frac{\alpha_k}{\gamma+\alpha_k}\right]\Bigg|_{\gamma=-\alpha_i},$$

and $\sum\limits_{i=1}^{N} r_i = K$. As a result of (17), the PDF of γ_{e2e} is given in the following form:

$$f_{\gamma_{\text{e2e}}}(\gamma) = e^{\chi}\sum_{i=1}^{N}\sum_{j=1}^{r_i}A_{ij}\left[\frac{\chi e^{-\chi\gamma}}{(\gamma+\beta_i)^j} + \frac{je^{-\chi\gamma}}{(\gamma+\beta_i)^{j+1}}\right]. \tag{18}$$

This form enables us to obtain a closed-form expression of the secrecy capacity. In particular, inserting (18) into (16), we have

$$\overline{\mathcal{C}} = \frac{e^{\chi}}{K}\sum_{i=1}^{N}\sum_{j=1}^{r_i}A_{ij}\left[\int_1^{\infty}\frac{\chi e^{-\chi\gamma}\log_2\gamma}{(\gamma+\beta_i)^j}d\gamma + \int_1^{\infty}\frac{je^{-\chi\gamma}\log_2\gamma}{(\gamma+\beta_i)^{j+1}}d\gamma\right]. \tag{19}$$

Direct solving (19) is a challenging problem since both integrands do not have a closed-form expression; the integrand for $j = 1$ in (19) does not converge. To overcome this challenge, integration by parts can be applied, as follows:

$$\int_1^{\infty}\frac{je^{-\chi\gamma}\log_2\gamma}{(\gamma+\beta_i)^{j+1}}d\gamma = -\underbrace{\frac{e^{-\chi\gamma}\log_2\gamma}{(\gamma+\beta_i)^j}\Bigg|_1^{\infty}}_{\mathcal{J}_1} - \int_1^{\infty}\frac{\chi e^{-\chi\gamma}\log_2\gamma}{(\gamma+\beta_i)^j}d\gamma$$
$$+\frac{1}{\log 2}\int_1^{\infty}\frac{e^{-\chi\gamma}}{\gamma(\gamma+\beta_i)^j}d\gamma. \tag{20}$$

Then, by using l'Hopital's rule, J_1 is shown to be

$$\begin{aligned}\mathcal{J}_1 &= \lim_{\gamma\to\infty}\frac{\log_2\gamma}{e^{\chi\gamma}(\gamma+\beta_i)^j} - \underbrace{\lim_{\gamma\to 1}\frac{e^{-\chi\gamma}\log_2\gamma}{(\gamma+\beta_i)^j}}_{\to 0}\\ &= \lim_{\gamma\to\infty}\frac{1}{\ln 2\left[\chi e^{\chi\gamma}(\gamma+\beta_i)^j + je^{\chi\gamma}(\gamma+\beta_i)^{j-1}\right]}\\ &= 0.\end{aligned}$$

Hence, by combining (19) and (20) with $J_1 = 0$, $\overline{\mathcal{C}}$ can be written as

$$\overline{\mathcal{C}} = \frac{e^{\chi}}{2}\sum_{i=1}^{N}\sum_{j=1}^{r_i}\frac{A_{ij}}{\ln 2}\underbrace{\int_1^{\infty}\frac{e^{-\chi\gamma}}{\gamma(\gamma+\beta_i)^j}d\gamma}_{\mathcal{J}_2}. \tag{21}$$

To proceed further with J_2, partial fraction expansion can be applied again

$$\mathcal{J}_2 = \frac{1}{\beta_i{}^j}\int_1^{\infty}\frac{e^{-\chi\gamma}d\gamma}{\gamma} - \sum_{\ell=1}^{j}\frac{1}{\beta_i{}^{j+1-\ell}}\int_1^{\infty}\frac{e^{-\chi\gamma}d\gamma}{(\gamma+\beta_i)^{\ell}}. \tag{22}$$

With the help of the identity $\int_1^{\infty}\frac{e^{-ax}}{x}dx = -\text{Ei}(-\text{a})$ [15, Eq. (3.351.5)] and the result proved in Appendix A, a closed-form expression for the system secrecy capacity is finally obtained as shown in Equation (23) at the top of the next page. This closed-form expression can be simplifed for different types of channels. For i.i.d. channels ($\alpha_1 = \cdots = \alpha_K = \alpha$), it is simplified to expression (24) at the top of the next page, and for i.n.d. channels ($\alpha_1 \neq \cdots \neq \alpha_K$), expression (25).

It is obvious that by using (23), (24), and (25), the system secrecy capacity over Rayleigh fading channel can be easily obtained in closed-form. Though the system secrecy capacity can be evaluated at arbitrary SNR values, it hardly offers any insights. Instead, taking into account the fact that the secrecy capacity of a single hop over a Gaussian channel is bounded by a finite value when the SNR approaches to infinity, it is more meaningful to study the asymptotic system security behavior at high SNR regime over Rayleigh fading channels. The asymptotic secrecy capacity at the high SNR regime will be derived next.

Theorem 2 *At high SNR regime, the system secrecy capacity, $\overline{\mathcal{C}}$, reaches an upper limit of*

$$\frac{1}{K}\sum_{k=1}^{K}\prod_{\ell=1,\ell\neq k}^{K}\frac{\alpha_\ell}{\alpha_k-\alpha_\ell}\log_2(1+\alpha_k), \tag{26}$$

for i.n.d. channels, or

$$\frac{\log_2(\alpha+1)}{K} - \frac{1}{K\log 2}\sum_{k=2}^{K}\frac{\alpha^{k-1}}{(k-1)(1+\alpha)^{k-1}}, \tag{27}$$

for i.i.d. channels, or

$$-\sum_{i=1}^{N}\frac{B_{i1}\log_2(1+\beta_i)}{K} + \frac{1}{K\log 2}\sum_{i=1}^{N}\sum_{j=2}^{r_i}\frac{B_{ij}}{(j-1)(\gamma+\beta_i)^{j-1}}, \tag{28}$$

for generalized channels.

Proof: We start the proof by writing the definition of the system secrecy capacity over Rayleigh fading channels

$$\overline{\mathcal{C}} = \frac{1}{K}\mathbb{E}\left\{\min_k\left(\log_2\left[\frac{1+\gamma_{M,k}}{1+\gamma_{E,k}}\right]\right)\right\}, \tag{29}$$

where $\mathbb{E}\{.\}$ denotes the expectation operator. Since $\gamma_{M,k}, \gamma_{E,k} \gg 1$, we have $\frac{1+\gamma_{M,k}}{1+\gamma_{E,k}} \approx \frac{\gamma_{M,k}}{\gamma_{E,k}}$, and hence

$$\begin{aligned}\overline{\mathcal{C}} &\to \frac{1}{K}\mathbb{E}\left\{\log_2\left[\min_k\left(\frac{\gamma_{M,1}}{\gamma_{E,1}}\right)\right]\right\}\\ &= \frac{1}{K}\int_1^{\infty}\log_2(\gamma)f_{\tilde{\gamma}_{e2e}}(\gamma)d\gamma,\end{aligned} \tag{30}$$

where $\tilde{\gamma}_{e2e} = \min_k\frac{\gamma_{M,k}}{\gamma_{E,k}}$.

$$\overline{\mathcal{C}} = \frac{e^{\chi}}{K}\sum_{i=1}^{N}\sum_{j=1}^{r_i}\frac{A_{ij}}{\log 2}\left[\frac{\mathrm{Ei}(-\chi)}{{\beta_i}^{j}} + \sum_{\ell=1}^{j}\frac{1}{{\beta_i}^{j+1-\ell}}\left(e^{-\chi}\sum_{n=1}^{\ell-1}\frac{(n-1)!(-\chi)^{\ell-n-1}}{(\ell-1)!(\beta_i+1)^{n}} - \frac{(-\chi)^{\ell-1}}{(\ell-1)!}e^{\beta_i\chi}\mathrm{Ei}[-(\beta_i+1)\chi]\right)\right] \tag{23}$$

$$\overline{\mathcal{C}} = \frac{e^{\chi}}{K\log 2}\left[\mathrm{Ei}(-\chi) + \sum_{\ell=1}^{K}\alpha^{\ell-1}\left(e^{-\chi}\sum_{n=1}^{\ell-1}\frac{(n-1)!(-\chi)^{\ell-n-1}}{(\ell-1)!(\alpha+1)^{n}} - \frac{(-\chi)^{\ell-1}}{(\ell-1)!}e^{\alpha\chi}\mathrm{Ei}[-(\alpha+1)\chi]\right)\right] \tag{24}$$

$$\overline{\mathcal{C}} = \frac{e^{\chi}\prod_{m=1}^{K}\alpha_m}{K\log 2}\sum_{k=1}^{K}\prod\nolimits_{\ell=1,\ell\neq k}^{K}\frac{1}{\alpha_\ell-\alpha_k}\left[\mathrm{Ei}(-\chi) - e^{\alpha_k\chi}\mathrm{Ei}(-\chi[1+\alpha_k])\right]. \tag{25}$$

To compute (30), we first derive $F_{\tilde{\gamma}_{\mathrm{e2e}}}(\gamma)$, which is given by

$$\begin{aligned} F_{\tilde{\gamma}_{\mathrm{e2e}}}(\gamma) &= 1 - \Pr\left(\frac{\gamma_{M,1}}{\gamma_{E,1}} > \gamma, \ldots, \frac{\gamma_{M,K}}{\gamma_{E,K}} > \gamma\right) \\ &= 1 - \prod_{k=1}^{K}\left[1 - \Pr\left(\frac{\gamma_{M,k}}{\gamma_{E,k}} < \gamma\right)\right] \\ &= 1 - \prod_{k=1}^{K}\frac{\alpha_k}{\gamma+\alpha_k}, \end{aligned} \tag{31}$$

where $\Pr\left(\frac{\gamma_{M,k}}{\gamma_{E,k}} < \gamma\right)$ is of the form

$$F_{\gamma_k}(\gamma) = \frac{\gamma}{\gamma+\alpha_k}.$$

Then, by using integration by parts, (30) can be now rewritten in terms of $F_{\tilde{\gamma}_{\mathrm{e2e}}}(\gamma)$ as

$$\overline{\mathcal{C}} \to \frac{1}{K}\left[\log_2(\gamma)F_{\tilde{\gamma}_{\mathrm{e2e}}}(\gamma)\Big|_{\gamma=1}^{\infty} - \frac{1}{\log 2}\int_{1}^{\infty}\frac{F_{\tilde{\gamma}_{\mathrm{e2e}}}(\gamma)}{\gamma}d\gamma\right]. \tag{32}$$

By inserting (31) and into (32) and carrying out some manipulations, the following yields

$$\begin{aligned} \overline{\mathcal{C}} \to{}& \frac{\log_2(\gamma)}{K}\left(1 - \prod_{k=1}^{K}\frac{\alpha_k}{\gamma+\alpha_k}\right)\Bigg|_{\gamma=1}^{\infty} \\ &- \frac{1}{K\log 2}\int_{1}^{\infty}\frac{1}{\gamma}\left(1 - \prod_{k=1}^{K}\frac{\alpha_k}{\gamma+\alpha_k}\right)d\gamma. \end{aligned} \tag{33}$$

After canceling like terms in (33) and applying the L'Hopistal rule, it is straightforward to obtain

$$\overline{\mathcal{C}} \to \frac{1}{K\log 2}\int_{1}^{\infty}\frac{1}{\gamma}\prod_{k=1}^{K}\frac{\alpha_k}{\gamma+\alpha_k}d\gamma. \tag{34}$$

From (34), three cases of channels will be now considered separately. For the i.n.d channels, that is, $\alpha_1 \neq \cdots \neq \alpha_K$, $\overline{\mathcal{C}}$ is re-written as

$$\overline{\mathcal{C}} \to \frac{1}{K\log 2}\int_{1}^{\infty}\left[\frac{1}{\gamma} - \sum_{k=1}^{K}\frac{\prod_{\ell=1,\ell\neq k}^{K}\frac{\alpha_\ell}{\alpha_k-\alpha_\ell}}{\gamma+\alpha_k}\right]d\gamma. \tag{35}$$

Knowing that $\sum_{k=1}^{K}\prod_{\ell=1,\ell\neq k}^{K}\frac{\alpha_\ell}{\alpha_k-\alpha_\ell} = 1$, the closed-form expression of (35) is then expressed as

$$\overline{\mathcal{C}} \to \frac{1}{K\log 2}\sum_{k=1}^{K}\prod_{\ell=1,\ell\neq k}^{K}\frac{\alpha_\ell}{\alpha_k-\alpha_\ell}\log(1+\alpha_k), \tag{36}$$

which is the limit of (26).

Next, for the i.i.d. channels, that is, $\alpha_1 = \cdots = \alpha_K = \alpha$, (34) is simplified to

$$\overline{\mathcal{C}} \to \frac{1}{K\log 2}\int_{1}^{\infty}\frac{1}{\gamma}\left(\frac{\alpha}{\gamma+\alpha}\right)^{K}d\gamma. \tag{37}$$

By means of partial fraction expansion, (37) reads

$$\overline{\mathcal{C}} \to \frac{1}{K\log 2}\int_{1}^{\infty}\left[\frac{1}{\gamma} - \frac{1}{\gamma+\alpha} - \sum_{k=2}^{K}\frac{\alpha^{k-1}}{(\gamma+\alpha)^{k}}\right]d\gamma. \tag{38}$$

Using the identity [15, Eq. (2.111)], we have

$$\overline{\mathcal{C}} \to \frac{1}{K\log 2}\left[\log(\alpha+1) - \sum_{k=2}^{K}\frac{\alpha^{k-1}}{(k-1)(1+\alpha)^{k-1}}\right], \tag{39}$$

proving the limit of (27).

Finally, for the generalized channels, recall that $\beta_1, \beta_2, \ldots, \beta_N$ are N distinct elements in decreasing order of $\alpha_1, \ldots, \alpha_K$. Then, (34) is re-expressed according to the residue theorem as

$$\overline{\mathcal{C}} \to \frac{1}{K\log 2}\int_{1}^{\infty}\left[\frac{1}{\gamma} + \sum_{i=1}^{N}\sum_{j=2}^{r_i}\frac{\mathcal{B}_{ij}}{(\gamma+\beta_i)^{j}}\right]d\gamma, \tag{40}$$

where $\sum_{i=1}^{N} r_i = K$ and

$$B_{ij} = \frac{1}{(r_i-j)!}\frac{d^{(r_i-j)}}{d\gamma^{(r_i-j)}}\left[(\gamma+\alpha_i)^{r_i}\prod_{k=1}^{K}\frac{\alpha_k}{\gamma+\alpha_k}\right]\Bigg|_{\gamma=-\alpha_i} \tag{41}$$

Similarly, taking the integral with respect to γ, we have

$$\begin{aligned} \overline{\mathcal{C}} \to{}& \frac{1}{K\log 2}\int_{1}^{\infty}\left[\frac{1}{\gamma} + \sum_{i=1}^{N}\frac{B_{i1}}{\gamma+\beta_i} + \sum_{i=1}^{N}\sum_{j=2}^{r_i}\frac{B_{ij}}{(\gamma+\beta_i)^{j}}\right]d\gamma \\ &\overset{(a)}{=} -\sum_{i=1}^{N}\frac{B_{i1}\log_2(1+\beta_i)}{K} \\ &\quad + \frac{1}{K\log 2}\sum_{i=1}^{N}\sum_{j=2}^{r_i}\frac{B_{ij}}{(j-1)(\gamma+\beta_i)^{j-1}}, \end{aligned} \tag{42}$$

where (a) follows from the fact that $\sum_{i=1}^{N} B_{i1} = -1$. The limit in (42) is that in (27); this completes the proof of the theorem. ■

4 Maximizing The Probability of Non-zero Secrecy Capacity

In this section, the optimal positions of trusty relays, which maximize the probability of non-zero secrecy capacity, will be studied. It will later be shown that the system secrecy capacity is then improved at no extra network resource. For ease of analysis, the linear network model is considered where the trusty relays are assumed to be in sequence and located on a straight line connecting the source and the destination, as shown in 1. Without loss of generality, it is further assumed that the source, the destination and the eavesdropper are placed at coordinates $(0,0)$, $(1,0)$, and (x_E, y_E), respectively. Such a model is well adopted in the literature in studies related to multihop networks because it is mathematically tractable and, more importantly, it can be straightforwardly extended to the more general case of two dimension (2-D) networks.

The single slope distance-dependent path loss model in [16] is used where the average channel gain between any two nodes primarily depends on the corresponding distance between them; that is, $\lambda_{Z,k} = d_{Z,k}^{-\eta}$ with $Z \in \{M, K\}$, where η is the path-loss exponent[1] and $d_{Z,k}$ is the physical distance of hop k. Based on that model, we have

$$\frac{\alpha_k}{\alpha_k + 1} = \frac{d_{M,k}^{-\eta}}{d_{M,k}^{-\eta} + d_{E,k}^{-\eta}}. \tag{43}$$

From (12) and (43), the optimization problem is given by

$$\text{maximize} \prod_{k=1}^{K} \frac{d_{M,k}^{-\eta}}{d_{M,k}^{-\eta} + d_{E,k}^{-\eta}} \quad \text{subject to} \quad \sum_{k=1}^{K} d_{M,k} = 1. \tag{44}$$

The constraint in (44) indicates that the overall distance between the source (T_0) and the destination (T_K) is normalized to one. A conventional approach adopted in solving the above optimization problem is the Lagrange method. But with the current form of (44) the challenge is the high computational complexity when dealing with the Lagrange conditions.

Since $\alpha_1, \ldots, \alpha_K$ are all positive numbers, by using the arithmetic-geometric inequality [15, Eq. (11.116)], we have

$$\prod_{k=1}^{K} \frac{\alpha_k}{\alpha_k + 1} \leq \left(\frac{1}{K} \sum_{k=1}^{K} \frac{\alpha_k}{\alpha_k + 1} \right)^K. \tag{45}$$

The probability of non-zero secrecy capacity attains its maximum if and only if

$$\frac{\alpha_1}{\alpha_1 + 1} = \frac{\alpha_2}{\alpha_2 + 1} = \cdots = \frac{\alpha_K}{\alpha_K + 1}, \tag{46}$$

which yields

$$\alpha_1 = \alpha_2 = \cdots = \alpha_K, \tag{47}$$

or equivalently

$$\frac{d_{E,1}^*}{d_{M,1}^*} = \frac{d_{E,2}^*}{d_{M,2}^*} = \cdots = \frac{d_{E,K}^*}{d_{M,K}^*}, \tag{48}$$

where $d_{M,k}^*$ and $d_{E,k}^*$ denote the optimal distance of main and eavesdropper link in hop k, respectively. In addition, for a given coordination of the eavesdropper (x_E, y_E), $d_{E,k}$ can be expressed in terms of $d_{M,k}$ via the help of the Pythagorean theorem as

$$d_{E,k} = \sqrt{\left(\sum_{\ell=1}^{k-1} d_{M,\ell} - x_E \right)^2 + {y_E}^2}. \tag{49}$$

Combining (44), (48) and (49), a nonlinear system of equations can be built

$$\begin{cases} d_{M,1} + \cdots + d_{M,k} - 1 = 0 \\ \dfrac{\sqrt{(x_E - d_{M,1})^2 + {y_E}^2}}{d_{M,2}} - \dfrac{\sqrt{x_E^2 + y_E^2}}{d_{M,1}} = 0 \\ \vdots \\ \dfrac{\sqrt{\left(x_E - \sum_{\ell=1}^{K-1} d_{M,\ell} \right)^2 + {y_E}^2}}{d_{M,K}} - \dfrac{\sqrt{x_E^2 + y_E^2}}{d_{M,1}} = 0 \end{cases} \tag{50}$$

where $d_{E,1} = \sqrt{x_E^2 + y_E^2}$.

The roots of the above equation system, which are $d_{M,1}^*, \ldots, d_{M,K}^*$, will provide the optimal x-coordinates for trusty relays. In general, solving (50) is not easy and one has to resort to numerical methods. Here, we adopt the well-known Newton method where the optimal distance of hop k can be determined by means of recursion [17]. It is noted that the solution to this problem solely depends on the number of hops and the coordinate of the eavesdropper, regardless the operational environment (the value of pathloss exponent).

5 Numerical Results

This section presents MATLAB simulations to verify the analytical results. In our plots, we adopt the network model where all nodes are located on a two-dimensional plane as in Section 4. Unless otherwise stated, a uniform relay placement scheme is used, that is, $d_{M,k} = 1/K$ for all k. Furthermore, the secure target rate is chosen as $R = 1$.

First, the the effect of the number of hops on the system performance is investigated. Figures 2, 3 and 4 respectively show the probability of non-zero secrecy capacity, the secure outage probability and the secrecy capacity versus average SNRs of legitimate links, while the average SNR of eavesdropper links is fixed at 5 dB ($\bar{\gamma}_{E,k} = 5$ dB for all k). As the figures reveal, the system performance in terms of the probability of non-zero secrecy capacity improve as K increases. In particular, the proposed scheme shows its advantage in terms of secrecy capacity gain over the direct transmission scheme at low SNRs, $\bar{\gamma}_{M,k} < 10$ dB, which can be explained partly by the increase of path loss gain.

[1] The path-loss exponent, η, normally takes values from 2 to 6 depending the operating environments.

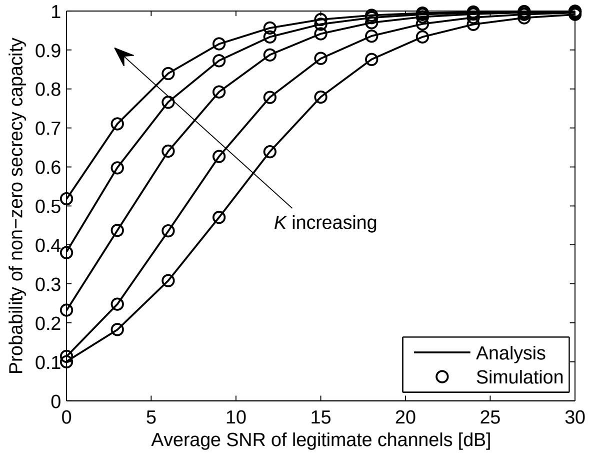

Figure 2. Probability of non-zero secrecy capacity versus K, $(x_E, y_E) = (0.5, 0.5)$, $\eta = 3$, $\overline{\gamma}_{E,k} = 5$ dB for all k.

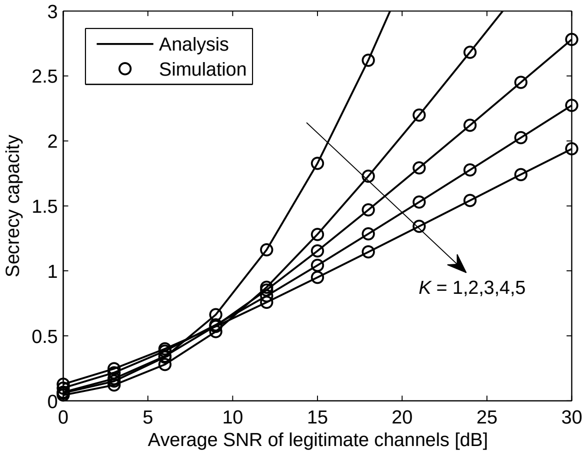

Figure 4. Secrecy capacity versus K, $(x_E, y_E) = (0.5, 0.5)$, $\eta = 3$, $\overline{\gamma}_{E,k} = 5$ dB for all k.

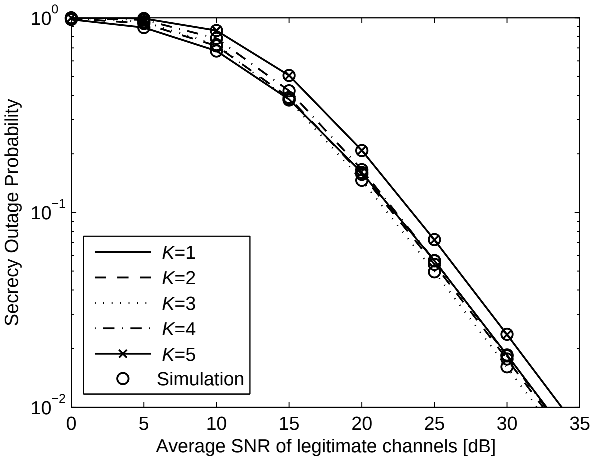

Figure 3. Secure Outage Probability versus K, $(x_E, y_E) = (0.5, 0.5)$, $\eta = 3$, $\overline{\gamma}_{E,k} = 5$ dB for all k.

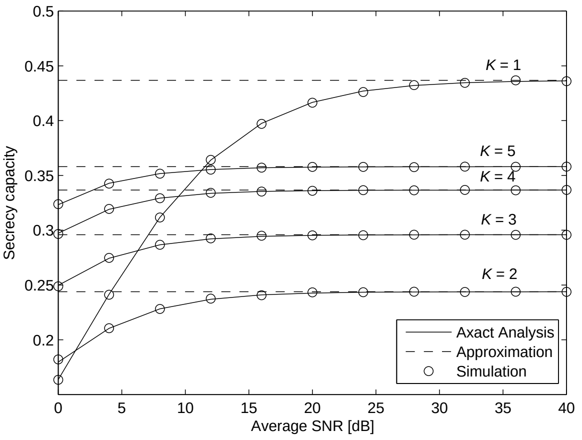

Figure 5. Effect of number of hops on the secrecy capacity, $(x_E, y_E) = (0.5, 0.5)$, $\eta = 4$.

However, increasing K does not always return a performance improvement for secure outage probability. For examples, the networks with $K = 3$ and $K = 5$ provide the best and the worst secure outage probability, respectively. Such an observation suggests that for a given fixed R, there exists an optimal number of hops, which will provide the best secure performance.

Next, the behaviors of the system at high SNR is shown in Figure 5. Clearly, the system secrecy capacity at high SNR regime approaches an upper limit, which is determined by the number of hops and the average SNR ratios between the legitimate link and the eavesdropper link. It is worth noting that, in the low SNR regime, increasing the number of hops offers better performance but with diminishing returns. However, in the high SNR regime, a direct transmission is more favorable since it provides the best secrecy capacity. Such a phenomenon can be explained by the fact that communicating over short distance in the low SNR regime is equivalent to increasing the effective SNRs.

The effect of the position of the eavesdropper on the system secrecy capacity is studied. For illustration, a dual-hop relay network is considered. Figure 6 shows three different positions of the eavesdropper with coordinates at (0.1,0.3), (0.5, 0.3) and (0.9,0.3), denoted as case A, case B and case C, correspondingly. It is straightforward to see that the eavesdropper is located closely to the source, the relay and the destination in case A, case B and case C, respectively. Among them, case C outperforms case B, which, in turns, outperforms case A. It can also be seen that the system secrecy capacity will improve if the eavesdropper is located farther away from all transmitters.

Figures 8 and 9 show the effect of path loss exponent on the probability of non-zero secrecy capacity and the secrecy capacity, respectively. It can be seen that using more hops provides a better probability of non-zero secrecy capacity, which is also consistent with the results reported above. However, with resepct to the secrecy capacity, there exists the optimal number of hops, which seems to be a complicated function of K. For example, the optimal number of hops for $\eta = 2, 3$ and 4 is 3, 2, and 2, respectively.

Up to this point, the optimal relay positions have not been considered. Figure 7 shows the advantage of multihop relay networks in conjunction with optimal

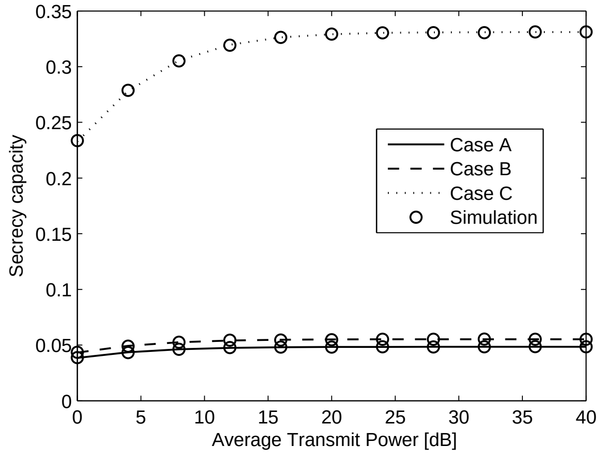

Figure 6. Effect of the eavesdropper position, $\eta = 3$, $K = 2$.

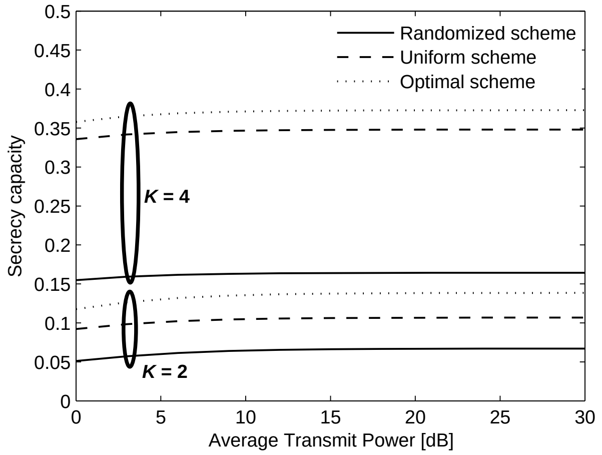

Figure 7. Comparison of relay replacement schemes, $(x_E, y_E) = (0.25, 0.25)$, $\eta = 4$.

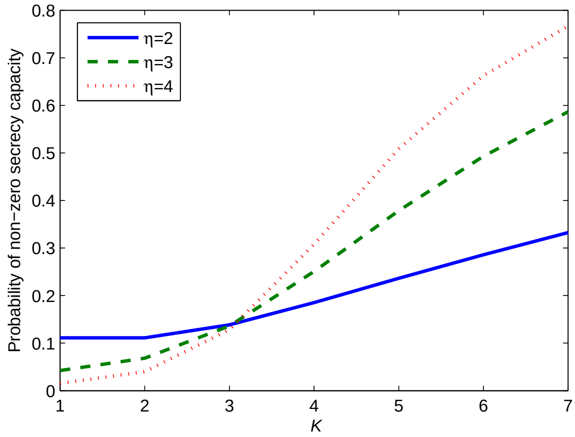

Figure 8. Effect of path loss exponent on the probability of non-zero secrecy capacity, $(x_E, y_E) = (0.25, 0.25)$.

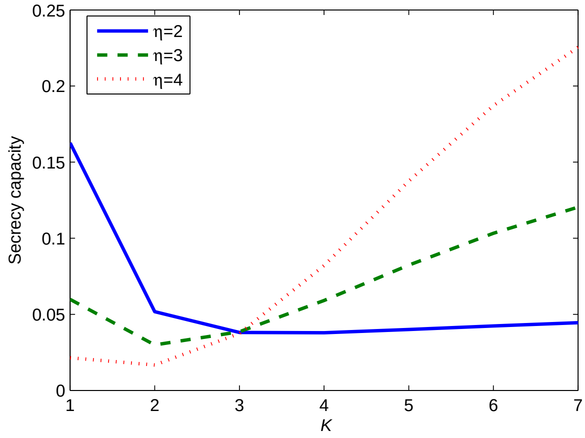

Figure 9. Effect of pathloss exponent on the secrecy capacity, $(x_E, y_E) = (0.25, 0.25)$.

relay replacement. For comparison purposes, the results provided by the uniform and randomized relay placement schemes are illustrated. We can see that in terms of secrecy capacity, the optimal relay placement provides the best performance as compared to the others. Furthermore, such a gain is more pronounced when the number of hops increases.

6 Conclusions

In this work, the information-theoretic security of multihop DF relay networks has been considered. New exact closed-form expressions for the probability of non-zero secrecy capacity, the secure outage probability and the secrecy capacity, assuming Rayleigh fading channels. The asymptotic analysis for the secrecy capacity at the high SNR regime was also provided. The numerical results have illustrated that multihop DF relay networks can provide better performance in comparison with direct transmission under the secrecy constraints. An optimal solution to the problem of trusty relay replacement was also investigated and it was shown that the system secrecy performance significantly improved without any network resource requirement. Finally, it was shown that the uniform relay replacement scheme gives an acceptable performance as compared to the randomized one.

Appendix

The purpose of this appendix is to calculate

$$\mathcal{I}_\ell = \int_1^\infty \frac{e^{-\chi\gamma}d\gamma}{(\gamma+\beta_i)^\ell}. \tag{51}$$

For ℓ integer with $\ell \geq 2$, using integral by parts, we obtain

$$\begin{aligned}
\mathcal{I}_\ell &= -\left.\frac{e^{-\chi\gamma}}{(\ell-1)(\gamma+\beta_i)^{\ell-1}}\right|_{\gamma=1}^{\infty} \\
&\quad - \frac{\chi}{\ell-1}\underbrace{\int_1^\infty \frac{\chi e^{-\chi\gamma}}{(\gamma+\beta_i)^{\ell-1}}d\gamma}_{\mathcal{I}_{\ell-1}} \\
&= \frac{e^{-\chi}}{(\ell-1)(\beta_i+1)^{\ell-1}} - \frac{\chi}{\ell-1}\mathcal{I}_{\ell-1}.
\end{aligned} \tag{52}$$

It can be clearly seen that (52) is expressed in a recursive form. Then, after $\ell - 2$ times of repeated integration by parts and using the same procedure as for (52), we have

$$\int_1^\infty \frac{e^{-\chi\gamma}d\gamma}{(\gamma+\beta_i)^\ell} = e^{-\chi}\sum_{n=1}^{\ell-1}\frac{(n-1)!(-\chi)^{\ell-n-1}}{(\ell-1)!(\beta_i+1)^n} + \frac{(-\chi)^{\ell-1}}{(\ell-1)!}e^{\beta_i\chi}\mathrm{Ei}[-(\beta_i+1)\chi], \quad (53)$$

where $\mathcal{I}_1 = e^{\chi\beta_1}\mathrm{Ei}[-\chi(\beta_i+1)]$ [15, Eq. (3.352.2)].

References

[1] J. Boyer, D. Falconer, and H. Yanikomeroglu, "A theoretical characterization of the multihop wireless communications channel without diversity," in *Proc. 12th IEEE Int Symp. Personal, Indoor and Mobile Radio Communications (PIRMC 2001)*, vol. 2, 2001, pp. E–116–E–120.

[2] M. O. Hasna and M.-S. Alouini, "End-to-end performance of transmission systems with relays over Rayleigh-fading channels," *IEEE Transactions on Wireless Communications*, vol. 2, no. 6, pp. 1126–1131, 2003.

[3] ——, "Outage probability of multihop transmission over Nakagami fading channels," *IEEE Communications Letters*, vol. 7, no. 5, pp. 216–218, 2003.

[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[5] 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.

[6] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[7] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. 46th Annual Allerton Conf. Communication, Control, and Computing*, 2008, pp. 1132–1138.

[8] ——, "Amplify-and-forward based cooperation for secure wireless communications," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP 2009)*, 2009, pp. 2613–2616.

[9] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5003–5011, 2009.

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

[11] S. Fu, T. Zhang, and M. Colef, "Secrecy in two-way relay systems," in *Proc. IEEE Global Telecommunications Conf. (GLOBECOM 2010)*, 2010, pp. 1–5.

[12] X. He and A. Yener, "End-to-end secure multi-hop communication with untrusted relays is possible," in *Proc. 42nd Asilomar Conf. Signals, Systems and Computers*, 2008, pp. 681–685.

[13] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high snr," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 1975–1983, 2011.

[14] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Transactions on Signal Processing*, vol. 60, no. 1, pp. 310–325, 2012.

[15] I. S. Gradshteyn, I. M. Ryzhik, A. Jeffrey, and D. Zwillinger, *Table of integrals, series and products*, 7th ed. Amsterdam ; Boston: Elsevier, 2007.

[16] A. Goldsmith, *Wireless communications*. Cambridge ; New York: Cambridge University Press, 2005.

[17] E. K. P. Chong and S. H. Zak, *An introduction to optimization*, 2nd ed., ser. Wiley-Interscience series in discrete mathematics and optimization. New York: Wiley, 2001.

Vo Nguyen Quoc Bao was born in Khanh Hoa, Vietnam, in 1979. He received the B.E. and M.Eng. degree in electrical engineering from Ho Chi Minh City University of Technology (HCMUT), Vietnam, in 2002 and 2005, respectively, and Ph.D. degree in electrical engineering from University of Ulsan, South Korea, in 2010.

In 2002, he joined the Department of Electrical Engineering, Posts and Telecommunications Institute of Technology (PTIT), as a lecturer. Since February 2010, he has been with the Department of Telecommunications, PTIT, where he is currently an Assistant Professor. His major research interests are modulation and coding techniques, MIMO system, combining technique, cooperative communications and cognitive radio. Dr. Bao is a Member of Korea Information and Communications Society (KICS), The Institute of Electronics, Information and Communication Engineers (IEICE) and the Institute of Electrical and Electronics Engineers (IEEE).

Nguyen Linh Trung received the B.Eng. and Ph.D. degrees in electrical engineering from the Queensland University of Technology, Brisbane, Australia, in 1997 and 2005, respectively. From 2003 to 2005, he was a postdoctoral research fellow with the Centre National d'Études Spatiales (CNES), Toulouse, France. Since 2006, he joined the Faculty of Electronics and Telecommunications, University of Engineering and Technology, Vietnam National University, Vietnam. He has held visiting positions with Vanderbilt University, the Ecole Supérieure d'Eléctricité (SUPELEC) and the Université Paris 13, Sorbonne Paris Cité. He is interested in data dimensionality reduction methods, which are related to time-frequency analysis, underdetermined blind source separation, compressed sensing and network coding, and their applications to biomedical engineering and wireless communications.