Open access • Journal Article • DOI:10.1109/TWC.2013.110813.121671

Relay Selection Schemes for Dual-Hop Networks under Security Constraints with Multiple Eavesdroppers — Source link

Vo Nguyen Quoc Bao, Nguyen Linh-Trung, Merouane Debbah

Institutions: University of Engineering and Technology, Lahore, Supélec

Published on: 11 Nov 2013 - IEEE Transactions on Wireless Communications (IEEE)

Topics: Relay channel and Relay

Relay Selection Schemes for Dual-Hop Networks under Security Constraints with Multiple Eavesdroppers

Vo Nguyen Quoc Bao, Nguyen Linh-Trung, Mérouane Debbah

Relay Selection Schemes for Dual-Hop Networks under Security Constraints with Multiple Eavesdroppers

Vo Nguyen Quoc Bao, *Member, IEEE,* Nguyen Linh-Trung, *Senior Member, IEEE,* and Mérouane Debbah, *Senior Member, IEEE*

***Abstract*—In this paper, we study opportunistic relay selection in cooperative networks with secrecy constraints, where a number of eavesdropper nodes may overhear the source message. To deal with this problem, we consider three opportunistic relay selection schemes. The first scheme tries to reduce the overheard information at the eavesdroppers by choosing the relay having the lowest instantaneous signal-to-noise ratio (SNR) to them. The second scheme is conventional selection relaying that seeks the relay having the highest SNR to the destination. In the third scheme, we consider the ratio between the SNR of a relay and the maximum among the corresponding SNRs to the eavesdroppers, and then select the optimal one to forward the signal to the destination. The system performance in terms of probability of non-zero achievable secrecy rate, secrecy outage probability and achievable secrecy rate of the three schemes are analyzed and confirmed by Monte Carlo simulations.**

***Index Terms*—Rayleigh fading, security constraints, achievable secrecy rate, secrecy outage probability, Shannon capacity, relay selection.**

I. Introduction

Cooperative communication has been considered as one of the most interesting paradigms in future wireless networks. By encouraging single-antenna equipped nodes to cooperatively share their antennas, spatial diversity can be achieved in the fashion of multi-input multi-output (MIMO) systems [1], [2]. Recently, this cooperative concept has increased interest in the research community as a mean to ensure secrecy for wireless systems [3]–[8]. The basic idea is that the system achievable secrecy rate can be significantly improved with the help of relays considering the spatial diversity characteristics of cooperative relaying.

While relay selection schemes have been intensively studied (see, e.g., [9]–[13] and references therein), there has been little research to date that focuses on relay selection with security purposes and related performance evaluation. In particular, Dong *et al.* investigated repetition-based decode-and-forward (DF) cooperative protocols and considered the design problem of transmit power minimization in [5]. Relay selection and cooperative beamforming were proposed for physical layer security in [14]. For the same system model, destination assisted jamming was considered in [15], showing an increase of the system achievable secrecy rate with the total transmit power budget. Investigating physical layer security in cognitive radio networks was carried out by Sakran *et al.* in [16] where a secondary user sends confidential information to a secondary receiver on the same frequency band of a primary user in the presence of an eavesdropper receiver. For amplify-and-forward (AF) relaying, the secure performance, based on channel state information (CSI) of the two hops, of different relay selection schemes was investigated in [17]. For orthogonal frequency division multiplexing (OFDM) networks using DF, a close-form expression of the secrecy rate was derived in [18]. In a large system of collaborating relay nodes, the problem of secrecy requirements with a few active relays was investigated in [19], aimed at reducing the communication and synchronization needs by using the model of a knapsack problem. To simultaneously improve the secure performance and quality of service (QoS) of mobile cooperative networks, an optimal secure relay selection was proposed in [20] by overlooking the changing property for the wireless channels. Effects of cooperative jamming and noise forwarding were studied in [21] to improve the achievable secrecy rates of a Gaussian wiretap channel. In [22], Krikidis *et al.* proposed a new relay selection scheme to improve the Shannon capacity of confidential links by using a jamming technique. Then, in [23], by taking into account of the relay-eavesdropper links in the relay selection metric, they also introduced an efficient way to select the best relay and its performance in terms of secrecy outage probability.

In the last paper above, the performance study is limited to only one eavesdropper. Such a network model may be inadequate in practice since many eavesdroppers could be available. In addition, the system achievable secrecy rate is still an open question, whereas it is the most important measure to characterize relay selection schemes under security constraints.

In this paper, we investigate the effects of relay selection with *multiple* eavesdroppers under Rayleigh fading and with security constraints. Three relay selection schemes are considered: minimum selection, conventional selection [24], and secrecy relay selection [23]. For the first scheme, the

Manuscript received October 28, 2012; revised May 2, 2013. The associate editor coordinating the review of this paper and approving it for publication was Dr. Daniela Tuninetti.

V. N. Q. Bao is with the Department of Telecommunications, Posts and Telecommunications Institute of Technology, 11 Nguyen Dinh Chieu Str., District 1, Ho Chi Minh City, Vietnam, email: baovnq@ptithcm.edu.vn.

N. Linh-Trung is with the Faculty of Electronics and Telecommunications, University of Engineering and Technology, Vietnam National University, G2-206, 144 Xuan Thuy road, Cau Giay, Hanoi, Vietnam, email: linhtrung@vnu.edu.vn.

M. Debbah is with the Alcatel-Lucent Chair on Flexible Radio, SUPELEC, 3 rue Joliot-Curie, 91192 Gif-sur-Yvette, France, email: merouane.debbah@supelec.fr.

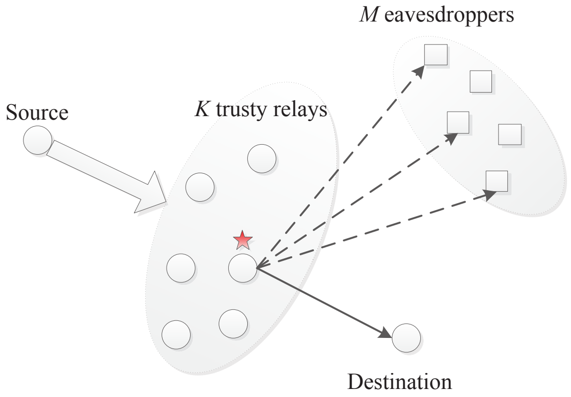

Fig. 1. The system model with K relays and M eavesdroppers.

relay to be selected is the one that has the lowest SNR to the eavesdroppers. For the second scheme, it is the relay that provides the highest signal-to-noise ratio (SNR) to the destination. In the third scheme, the best potential relay gets selected according to its secrecy rate.

We also study the performance of the three relay selection schemes in terms of the probability of non-zero achievable secrecy rate, secrecy outage probability and achievable secrecy rate of three selection schemes. These will first be analytically described by investigating the probability density functions (PDF) of the end-to-end system SNR. Then, the asymptotic approximations for the system achievable secrecy rate, which reveal the system behavior, will be provided. We will show that previously known results in [5] and [23] are special cases of our obtained results. Monte Carlo simulations will finally be conducted for confirming the correctness of the mathematical analysis.

II. System Model and Relay Selection Schemes

A. System model

The system model consists of one source, S, one destination, D, and a set of K decode-and-forward (DF) relays [2], R_k (for $k = 1, \ldots, K$), which help the transmission between the source and the destination to avoid overhearing attacks of M malicious eavesdroppers, E_m (for $m = 1, \ldots, M$). The schematic diagram of the system model is shown in Figure 1. In order to focus our study on the cooperative slot, we assume that the source has no direct link with the destination and eavesdroppers, i.e., the direct links are in deep shadowing, and the communication is carried out through a reactive DF protocol [9]. It is worth noting that this assumption is well-known in the literature for cooperative systems, whether or not taking into account of secrecy constraints [5], [6], [9]. More specifically, this assumption refers to cooperative systems with a secure broadcast phase [6] or clustered relay configurations, wherein the source node communicates with relays via a local connection [25].

As in [23], this paper focuses on the effect of relay selection schemes on the system achievable secrecy rate under the assumption of perfect CSI. In practice, this corresponds to, for example, the scenario where eavesdroppers are other active users of the network with time division multiple access (TDMA) channelization. As a result, both centralized and distributed relay selection mechanisms are both applicable. For the centralized mechanism, a central base station is dedicated to collect the necessary CSI and then select the best relay. For the distributed mechanism, the best relay is selected a priori using the distributed timer fashion as proposed in [24]. The problem of imperfect CSI is beyond the scope of this paper.

In the first phase of this protocol, the source broadcasts its signal to all the relay nodes. In the second phase, one potential relay node, which is chosen among the relays that successfully decodes the source message[1], forwards the re-encoded signal towards the destination.

The channels between nodes $i \in \{1, \ldots, K\}$ and $j \in \{m, D\}$ are modelled as independent and slowly varying flat Rayleigh fading random variables. Due to Rayleigh fading, the channel fading gains, denoted by $|h_{i,j}|^2$, are independent and exponential random variables with means of $\lambda_{i,j}$. For simplicity, we assume that $\lambda_{k,m} = \lambda_E$ and $\lambda_{k,D} = \lambda_D$ for all m and k. The general case where all the $\lambda_{k,m}$ and $\lambda_{k,D}$ are distinct is shown in Appendix A. The average transmit power for the relays is denoted by $\mathcal{P}_{\mathrm{R}}$, then instantaneous SNRs for the links from relay k to the destination can be written as $\gamma_{k,D} = \mathcal{P}_{\mathrm{R}}|h_{k,D}|^2/\mathcal{N}_0$ and to each eavesdropper m as $\gamma_{k,m} = \mathcal{P}_{\mathrm{R}}|h_{k,m}|^2/\mathcal{N}_0$, where $\mathcal{N}_0$ is the variance of the additive white Gaussian noise at all receiving terminals. As a result, the expected values for $\gamma_{k,D}$ and $\gamma_{k,m}$, denoted by $\bar{\gamma}_D$ and $\bar{\gamma}_E$, are $\mathcal{P}_{\mathrm{R}}\lambda_D/\mathcal{N}_0$ and $\mathcal{P}_{\mathrm{R}}\lambda_E/\mathcal{N}_0$, respectively.

For each relay R_k, the channel capacity from it to D is given by [26]

$$\mathcal{C}_{k,D} = \log_2(1 + \gamma_{k,D}). \tag{1}$$

Similarly, the Shannon capacity of the channel from relay k to eavesdropper m is given by

$$\mathcal{C}_{k,m} = \log_2(1 + \gamma_{k,m}). \tag{2}$$

The system model is assuming the presence of M non-colluding eavesdroppers. Therefore, by leveraging the wiretap coding techniques for the compound wiretap channel, secrecy rates that are supported by picking the eavesdropper with the highest SNR when considering the other eavesdroppers are also achievable, which is given by [27]

$$\begin{aligned}\mathcal{C}_{k,E} &\triangleq \max_m \mathcal{C}_{k,m} \\ &= \log_2(1 + \gamma_{k,E}),\end{aligned} \tag{3}$$

where $\gamma_{k,E}$ denotes the instantaneous SNR of the link from relay k to the eavesdropper group and is defined as

$$\gamma_{k,E} \triangleq \max_m \gamma_{k,m}. \tag{4}$$

Then, the achievable secrecy rate at relay k can be defined

[1] In this paper, for simplicity we assume that all the relays can decode the signal correctly.

as [4]

$$\begin{aligned}\mathcal{C}_k &\triangleq \left[\mathcal{C}_{k,D} - \mathcal{C}_{k,E}\right]^+ \\ &= \left[\log_2(1+\gamma_{k,D}) - \log_2(1+\gamma_{k,E})\right]^+ \\ &= \left[\log_2\left(\frac{1+\mathcal{P}_{\mathrm{R}}\gamma_{k,D}}{1+\mathcal{P}_{\mathrm{R}}\gamma_{k,E}}\right)\right]^+, \end{aligned} \tag{5}$$

where

$$[x]^+ = \max(x,0) = \begin{cases} x, & x \geq 0 \\ 0, & x < 0 \end{cases}.$$

B. Relay selection schemes

In physical communication security with cooperative relaying, how to maximize the capacity of the wireless link to the destination and how to minimize the capacity of the channel to the malicious eavesdroppers are two main concerns. It is observed that, on a one hand, the relay which has a good channel to the destination may also have good channels to eavesdroppers and, on the other hand, the relay having bad channels to eavesdroppers may also have a bad channel to the destination. Therefore, relay selection depends on some selection criterion and the optimization of such a criterion is the main objective of this paper. To facilitate the relay selection process, we assume perfect knowledge of the required channel-based parameters. In this paper, the following three relay selection schemes, namely minimum selection, conventional selection and optimal selection, will be considered. For the minimum scheme, the best relay is chosen based on full CSI of the relay-eavesdropper links, that is the selected relay is the relay having the minimum the SNR towards eavesdroppers. For the conventional scheme, the selected relay is the relay providing the best instantaneous capacity toward the destination [24]. It is noted that to choose the best relay for the conventional selection scheme, the full CSI of the relay-destination links are required. Although the above schemes of relay selection are natural, they are not optimal ones since a part of CSI related to the end-to-end system achievable secrecy rate, i.e., either the SNR towards to eavesdroppers or the SNR towards to the destination, is utilized. The third scheme, as first proposed in [23] for the case of one eavesdropper, is the optimal one in view of the utilization of full CSI. It is expected that this scheme will provide a better secrecy performance as compared to the other schemes. In the following, we will go into detail.

1) Minimum Selection: In this relay selection scheme, the relay that has the lowest equivalent instantaneous SNR to the eavesdropper group will be selected to forward the signal to the destination. Denoting R_{k^*} the selected relay, we have

$$k^* = \arg\min_k \gamma_{k,E}. \tag{6}$$

The problem about how to select the relay having the lowest instantaneous SNR to the eavesdroppers can be solved by using the distributed timer approach suggested by Bletsas *et al.* in [9]. Then, the achievable secrecy rate for minimum selection can be generally written as

$$\mathcal{C}_{\min} = \left[\mathcal{C}_{k^*,D} - \min_k \mathcal{C}_{k,E}\right]^+. \tag{7}$$

2) Conventional Selection: In conventional selection, the relay that has the highest equivalent instantaneous SNR to the destination will be selected to become the sender of the next hop. For the selected relay R_{k^*}, we have

$$k^* = \arg\max_k \gamma_{k,D}. \tag{8}$$

The achievable secrecy rate of this selection scheme is expressed by

$$\mathcal{C}_{\max} = \left[\max_k \mathcal{C}_{k,D} - \mathcal{C}_{k^*,E}\right]^+. \tag{9}$$

3) Optimal Selection: We recognize that, when full CSI is assumed, minimum selection considers only relay-eavesdropper links while conventional selection considers only the relay-destination links. Optimal selection incorporates the quality of both links in the selection decision metric. In particular, the relay that has the highest achievable secrecy rate to the destination and eavesdroppers gets selected. As a result, the optimal selection scheme is expected to provide a better performance than that of the others. Mathematically, the proposed selection technique selects relay R_{k^*} with

$$k^* = \arg\max_k \left\{\frac{\gamma_{k,D}+1}{\gamma_{k,E}+1}\right\}. \tag{10}$$

The corresponding achievable secrecy rate is expressed by

$$\mathcal{C}_{\text{opt}} = \left[\mathcal{C}_{k^*,D} - \mathcal{C}_{k^*,E}\right]^+. \tag{11}$$

The new selection metric is related to the maximization of the achievable secrecy rate and therefore it is considered as the optimal solution for reactive DF protocols with secrecy constraints.

III. Performance Analysis

In order to analyze the achievable secrecy rate of the three schemes, we first derive the probability density function of the SNR of each link from the selected relay to the destination and to the eavesdroppers. Such the PDFs are then used for obtaining the non-zero achievable secrecy rate, the secrecy outage probability and the system achievable secrecy rate[2] in closed-forms.

A. Minimum selection performance

Considering a Rayleigh fading distribution, the PDF of the equivalent SNR from the selected relay to the destination, $\gamma_{k^*,D}$, is given by

$$f_{\gamma_{k^*,D}}(\gamma) = \frac{1}{\bar{\gamma}_D} e^{-\frac{\gamma}{\bar{\gamma}_D}}, \tag{12}$$

where $\bar{\gamma}_D = \mathcal{P}_{\mathrm{R}}\lambda_D$. Following (7), the equivalent SNR of the channel from the selected relay to the eavesdroppers is

$$\gamma_{k^*,E} = \min_k \gamma_{k,E}. \tag{13}$$

[2] It is in fact the average achievable secrecy rate, where the average is done with respect to the channel statistics.

Assuming that all fading channels are independent, the PDF of $\gamma_{k^*,E}$ can be written as

$$f_{\gamma_{k^*,E}}(\gamma) = \sum_{k=1}^{K} f_{\gamma_{k,E}}(\gamma) \prod_{n=1,n\neq k}^{K} \left[1 - F_{\gamma_{k,E}}(\gamma)\right]. \qquad (14)$$

The following lemma is of important when it provides the closed-form expression of the PDF of the $\gamma_{k^*,E}$.

Lemma 1: The PDF of the $\gamma_{k^*,E}$ can be expressed in a compact and elegant form as follows:

$$\begin{aligned} f_{k^*,E}(\gamma) &= K\left[\sum_{m=1}^{M}(-1)^{m-1}\binom{M}{m}e^{-\frac{m\gamma}{\bar\gamma_E}}\right]^{K-1} \\ &\quad \times \sum_{m=1}^{M}(-1)^{m-1}\binom{M}{m}\frac{m}{\bar\gamma_E}e^{-\frac{m\gamma}{\bar\gamma_E}} \\ &= \overset{\sim}{\sum}\mathcal{K}\chi e^{-\gamma\chi}, \qquad (15) \end{aligned}$$

where

$$\begin{aligned} \overset{\sim}{\sum} &\triangleq \sum_{m_1=1}^{M}\cdots\sum_{m_K=1}^{M}, \\ \mathcal{K} &\triangleq (-1)^{-K+\sum_{p=1}^{K}m_p}\prod\nolimits_{q=1}^{K}\binom{M}{m_q}, \\ \chi &\triangleq \tfrac{1}{\bar\gamma_E}\sum\nolimits_{k=1}^{M}m_k. \end{aligned}$$

Proof: The proof of Lemma 1 is given in Appendix A. ■

The PDF of $\gamma_{k^*,E}$ in (15) has an exponential form with respect to γ making it become mathematical tractability. We shall soon see that such a form will play a very important role in simplifying the evaluation of system performance over Rayleigh fading channels.

1) Probability of non-zero achievable secrecy rate: By invoking the fact that the secrecy rate is zero when the highest eavesdropper SNR is higher than the SNR from the chosen relay to the destination, i.e., $\mathcal{C}_{\min} = 0$ if $\gamma_{k^*,D} < \gamma_{k^*,E}$, and assuming the independence between the main channel and the eavesdropper channel, the probability of system non-zero achievable secrecy rate is given by

$$\begin{aligned} \Pr(\mathcal{C}_{\min} > 0) &= \Pr(\gamma_{k^*,D} > \gamma_{k^*,E}) \\ &= \int_0^\infty F_{\gamma_{k^*,E}}(\gamma) f_{\gamma_{k^*,D}}(\gamma)d\gamma. \qquad (16) \end{aligned}$$

Substituting (12) and (15) into (17), and then taking the integral with respect to $\gamma_{k^*,D}$, we have

$$\begin{aligned} \Pr(\mathcal{C}_{\min} > 0) &= \int_0^\infty \overset{\sim}{\sum}\mathcal{K}\left(1 - e^{-\gamma\chi}\right)\frac{1}{\bar\gamma_D}e^{-\frac{\gamma}{\bar\gamma_D}}d\gamma \\ &= \overset{\sim}{\sum}\mathcal{K}\frac{\chi\bar\gamma_D}{1+\chi\bar\gamma_D}. \qquad (17) \end{aligned}$$

2) Secrecy outage probability: Under the security constraint, the system is in outage whenever a message transmission is neither perfectly secure nor reliable. For a given secure rate (R), the secrecy outage probability is therefore defined as

$$\begin{aligned} &\Pr(\mathcal{C}_{\min} < R) = \\ &\quad \Pr(\gamma_{k^*,E} \geq \gamma_{k^*,D})\Pr\left(\mathcal{C}_{\min} < R \,|\, \gamma_{k^*,E} \geq \gamma_{k^*,D}\right) \\ &\quad + \Pr(\gamma_{k^*,E} < \gamma_{k^*,D})\Pr\left(\mathcal{C}_{\min} < R | \gamma_{k^*,E} < \gamma_{k^*,D}\right). \qquad (18) \end{aligned}$$

Making use the fact that $\Pr(\mathcal{C}_{\min} < R \,|\, \gamma_{k^*,E} \geq \gamma_{k^*,D}) = 1$ and recalling (7), we can write

$$\begin{aligned} \Pr(\mathcal{C}_{\min} < R) &= \int_0^\infty F_{\gamma_{k^*,D}}\left[2^{2R}(1+\gamma) - 1\right] f_{\gamma_{k^*,E}}(\gamma)d\gamma \\ &\overset{(a)}{=} \overset{\sim}{\sum}\mathcal{K}\left[1 - e^{-\frac{2^{2R}-1}{\bar\gamma_D}}\frac{\chi\bar\gamma_D}{\chi\bar\gamma_D + 2^{2R}}\right], \qquad (19) \end{aligned}$$

where (a) immediately follows after plugging (12) and (15) into (19) then taking the integral with respect to $\gamma_{k^*,E}$.

3) Asymptotic achievable secrecy rate: It is useful to examine the asymptotic behavior of the achievable secrecy rate, which reveals the effects of channel and network settings on the system performance. Different from the Shannon capacity, which increases according to the average SNRs, the achievable secrecy rate likely approaches a constant limit which is determined by the average channel powers of the main and eavesdropper channels. To obtain the system achievable secrecy rate, we first introduce the following lemma.

Lemma 2: Under Rayleigh fading, the CDF and PDF of γ_{k^*} are respectively given by

$$F_{\gamma_{k^*}}(\gamma) = \overset{\sim}{\sum}\mathcal{K}\frac{\gamma}{\gamma + \chi\bar\gamma_D}, \qquad (20)$$

$$f_{\gamma_{k^*}}(\gamma) = \overset{\sim}{\sum}\mathcal{K}\frac{\chi\bar\gamma_D}{(\gamma + \chi\bar\gamma_D)^2}. \qquad (21)$$

The proof of Lemma 2 is given in Appendix B. Having the PDF and CDF of γ_{k^*} in hands allows us to derive the asymptotic system achievable secrecy rate, which is stated in the following theorem.

Proposition 1: In the high SNR regime, the achievable secrecy rate of dual-hop DF networks under the minimum selection scheme is given by

$$\bar{\mathcal{C}}_{\min} \to \frac{1}{\ln 2}\overset{\sim}{\sum}\mathcal{K}\ln(\chi\bar\gamma_D + 1). \qquad (22)$$

Proof: Starting from (7), it is possible to write

$$\begin{aligned} \bar{\mathcal{C}}_{\min} &= \mathbb{E}\{\mathcal{C}_{\min}\} \\ &\to \frac{1}{\ln 2}\int_1^\infty \ln(x) f_{\gamma_{k^*}}(x)dx \\ &= \frac{1}{\ln 2}\overset{\sim}{\sum}\mathcal{K}\int_1^\infty \ln(\gamma)\frac{\chi\bar\gamma_D}{(\gamma + \chi\bar\gamma_D)^2}d\gamma. \end{aligned}$$

With the help of [28, eq. (2.727.3)], we can obtain the closed-form expression for $\bar{\mathcal{C}}_{\min}$ as in (22). ■

B. Conventional selection performance

Following [9], the PDF of the channel gain from the selected relay to the destination in this scheme can be given as

$$f_{\gamma_{k^*,D}}\left(\gamma\right) = \sum_{k=1}^{K} \left(-1\right)^{k-1} \binom{K}{k} \frac{k}{\bar{\gamma}_D} e^{-\frac{k\gamma}{\bar{\gamma}_D}}. \tag{23}$$

Next, we consider the PDF of SNR for the best link from the selected relay to the eavesdroppers, which can be written as follows:

$$f_{\gamma_{k^*,E}}\left(\gamma\right) = \sum_{m=1}^{M} \left(-1\right)^{m-1} \binom{M}{m} \frac{m}{\bar{\gamma}_E} e^{-\frac{m\gamma}{\bar{\gamma}_E}}. \tag{24}$$

1) Probability of non-zero achievable secrecy rate: Now we focus on deriving the probability of non-zero achievable secrecy rate. Mathematically, we have

$$\begin{aligned}\Pr(\mathcal{C}_{\max} > 0) =& \Pr(\gamma_{k^*,E} < \gamma_{k^*,D}) \\ =& \int\limits_0^\infty \left[\sum_{m=1}^{M} (-1)^{m-1} \binom{M}{m} \left(1 - e^{-\frac{m\gamma}{\gamma_E}}\right)\right] \\ & \times \sum_{k=1}^{K} (-1)^{k-1} \binom{K}{k} \frac{k}{\gamma_D} e^{-\frac{k\gamma}{\gamma_D}} d\gamma \qquad (25) \\ =& \sum_{m=1}^{M}\sum_{k=1}^{K} (-1)^{m+k-2} \binom{M}{m}\binom{K}{k} \frac{\frac{m\bar{\gamma}_D}{k\bar{\gamma}_E}}{1+\frac{m\bar{\gamma}_D}{k\bar{\gamma}_E}}.\end{aligned}$$

2) Secrecy outage probability: Making use of the same steps as for (19), we can write the secrecy outage probability as

$$\begin{aligned}\Pr(\mathcal{C}_{\max} < R) =& \Pr(\gamma_{k^*,E} \geq \gamma_{k^*,D}) \qquad (26) \\ & + \Pr[\gamma_{k^*,E} < \gamma_{k^*,D} < 2^{2R}(1+\gamma_{k^*,E}) - 1].\end{aligned}$$

Integrating both sides of (26) with respect to $\gamma_{k^*,E}$ yields

$$\begin{aligned}&\Pr(\mathcal{C}_{\max} < R) = \mathbb{E}_{\gamma_{k^*,E}} \left\{\Pr[\gamma_{k^*,D} < 2^{2R}(1+\gamma_{k^*,E}) - 1]\right\} \\ &= \sum_{k=1}^{K}\sum_{m=1}^{M} (-1)^{k+m-2} \binom{K}{k}\binom{M}{m} \left[1 - \frac{e^{-\frac{k(2^{2R}-1)}{\bar{\gamma}_D}}}{1+2^{2R}\frac{k}{m}\frac{\bar{\gamma}_E}{\bar{\gamma}_D}}\right]. \qquad (27)\end{aligned}$$

In (27), we use the CDF of $\gamma_{k^*,D}$, which is derived from (23) as

$$\begin{aligned}F_{\gamma_{k^*,D}}\left(\gamma\right) &= \int\limits_0^\gamma f_{\gamma_{k^*,D}}\left(\gamma\right) d\gamma \\ &= \sum_{k=1}^{K} (-1)^{k-1} \binom{K}{k} \left(1 - e^{-\frac{k\gamma}{\gamma_D}}\right). \qquad (28)\end{aligned}$$

3) Asymptotic achievable secrecy rate: We now analyze the asymptotic achievable secrecy rate when the relay providing the best Shannon capacity toward the destination is selected. To approximate $\mathbb{E}\{\mathcal{C}_{\max}\}$, we need to calculate the PDF of $\gamma_{k^*} = \frac{\gamma_{k^*,D}}{\gamma_{k^*,E}}$, given by

$$\begin{aligned}f_{\gamma_{k^*}}(\gamma) &= \frac{dF_{\gamma_{k^*}}(\gamma)}{d\gamma} \\ &= \frac{d}{d\gamma}\left[\int\limits_0^\infty \Pr(\gamma_{k^*,D} < \gamma x) f_{\gamma_{k^*,E}}(x) dx\right] \\ &= \frac{d}{d\gamma}\left[\sum_{k=1}^{K}\sum_{m=1}^{M} (-1)^{m+k-2} \binom{M}{m}\binom{K}{k} \frac{\gamma}{\gamma + \frac{m}{k}\frac{\bar{\gamma}_D}{\bar{\gamma}_E}}\right] \\ &= \sum_{k=1}^{K}\sum_{m=1}^{M} (-1)^{m+k-2} \binom{M}{m}\binom{K}{k} \frac{\frac{m}{k}\frac{\bar{\gamma}_D}{\bar{\gamma}_E}}{\left(\gamma + \frac{m}{k}\frac{\bar{\gamma}_D}{\bar{\gamma}_E}\right)^2}. \qquad (29)\end{aligned}$$

We are now in a position to derive the asymptotic achievable secrecy rate, which is provided in the following theorem.

Theorem 1: The achievable secrecy rate of DF relay networks with the best relay scheme is tightly approximated at high SNRs as

$$\begin{aligned}\bar{\mathcal{C}}_{\max} &\to \int\limits_1^\infty \log_2(x) f_{\gamma_{k^*}}(x) dx \qquad (30) \\ &= \frac{1}{\ln 2}\sum_{k=1}^{K}\sum_{m=1}^{M} (-1)^{m+k-2} \binom{K}{k}\binom{M}{m} \ln\left(1 + \frac{m}{k}\frac{\bar{\gamma}_D}{\bar{\gamma}_E}\right).\end{aligned}$$

Proof: It is easy to show that from (23), and with the help of [29, eq. (2.727.3)], the theorem follows after some manipulations. ■

C. Optimal selection performance

Considering relay k, we have the equivalent secrecy channel SNR as follows:

$$\gamma_k = \frac{\gamma_{k,D} + 1}{\gamma_{k,E} + 1}. \tag{31}$$

To facilitate the analysis, γ_k can be approximated at high SNRs as [23]

$$\gamma_k \approx \frac{\gamma_{k,D}}{\gamma_{k,E}}. \tag{32}$$

leading to $\gamma_{k^*} \approx \max_k \frac{\gamma_{k,D}}{\gamma_{k,E}}$.

For Rayleigh fading channels, the CDF of γ_k can be derived as

$$\begin{aligned}F_{\gamma_k}(\gamma) \;&=\; \Pr\left(\frac{\gamma_{k,D}}{\gamma_{k,E}} \leq \gamma\right) \\ &= \int\limits_0^\infty \Pr(\gamma_{k,D} \leq \gamma\gamma_{k,E}) f_{\gamma_{k,E}}(\gamma_{k,E}) d\gamma_{k,E} \\ &= \int\limits_0^\infty \left(1 - e^{-\frac{\gamma\gamma_{k,E}}{\bar{\gamma}_D}}\right) \sum_{m=1}^{M} (-1)^{m-1} \binom{M}{m} \frac{m}{\bar{\gamma}_E} e^{-\frac{m\gamma_{k,E}}{\bar{\gamma}_E}} d\gamma_{k,E} \\ &= 1 - \sum_{m=1}^{M} (-1)^{m-1} \binom{M}{m} \frac{m\Omega}{\gamma + m\Omega}. \qquad (33)\end{aligned}$$

where $\Omega = \bar{\gamma}_D/\bar{\gamma}_E$. After using the identity [29, eq. 3.1.7], i.e.,

$$\sum_{m=1}^{M} (-1)^{m-1} \binom{M}{m} = 1, \tag{34}$$

(33) is rewritten as

$$F_{\gamma_k}(\gamma) = \sum_{m=1}^{M} (-1)^{m-1} \binom{M}{m} \frac{\gamma}{\gamma + \alpha_m}, \tag{35}$$

where $\alpha_m = m\Omega$. To obtain the PDF of γ_k, we differentiate (35), namely

$$f_{\gamma_k}(\gamma) = \sum_{m=1}^{M} (-1)^{m-1} \binom{M}{m} \frac{\alpha_m}{(\gamma + \alpha_m)^2}. \tag{36}$$

Having the CDF and PDF of γ_k at hands allows ones to derive the PDF of γ_{k^*}, which is given in Lemma 3.

Lemma 3: Under Rayleigh fading channels, the PDF of $\gamma_{k^*} = \max_k \gamma_k$ is given by

$$f_{\gamma_{k^*}}(\gamma) = \sum^{\sim} \sum_{p=1}^{L} \sum_{q=1}^{r_p} \frac{\mathcal{K}\mathcal{A}_{p,q}}{(\gamma + \Theta_p)^q}, \tag{37}$$

where Θ_p are L distinct elements of the set of $\{\alpha_k\}_{k=1}^{K}$ in decreasing order, and $\mathcal{A}_{p,q}$ are the coefficients of the partial-fraction expansion, given by

$$\mathcal{A}_{p,q} = \frac{1}{(r_p - q)!} \left\{ \frac{\partial^{(r_p - q)}}{\partial \gamma^{(r_n - q)}} [(\gamma + \Theta_p)^{r_p} f_{\gamma_{k^*}}(\gamma)] \right\} \Bigg|_{\gamma = -\Theta_p}. \tag{38}$$

The proof of Lemma 3 is given in Appendix C.

1) Probability of non-zero achievable secrecy rate: Making use the fact that $\log_2\left(\frac{1+x}{1+y}\right) > 0 \Leftrightarrow x > y$ for positive random variables x and y, the probability of non-zero achievable secrecy rate is given as

$$\begin{aligned} \Pr(\mathcal{C}_{\text{opt}} > 0) &= \Pr(\gamma_{k^*} > 1) \\ &= 1 - F_{\gamma_k^*}(1) \\ &= 1 - \left[\sum_{m=1}^{M} (-1)^{m-1} \binom{M}{m} \frac{1}{\alpha_m + 1} \right]^K \end{aligned} \tag{39}$$

2) Secrecy outage probability: Since there is no visibly mathematical relationship between the $\gamma_{k^*,E}$ with γ_k, it is likely impossible to obtain the exact form expression for $\Pr(\mathcal{C}_{\text{opt}} < R)$. To deal with this problem, the approximation approach should be used, namely

$$\Pr(\mathcal{C}_{\text{opt}} < R) = \Pr[\gamma_{k^*,D} < 2^{2R}(1 + \gamma_{k^*,E}) - 1] \tag{40}$$

$$\begin{aligned} &\approx \Pr\left(\gamma_{k^*} < 2^{2R}\right) \\ &= \left[\sum_{m=1}^{M} (-1)^{m-1} \binom{M}{m} \frac{2^{2R}}{\alpha_m + 2^{2R}} \right]^K. \end{aligned} \tag{41}$$

3) Asymptotic achievable secrecy rate: In this subsection, by using Lemma 3 we derive the asymptotic achievable secrecy rate, which is reported in Theorem 2.

Theorem 2: At high SNR regime, the limit for the achievable secrecy rate is of the following form:

$$\bar{\mathcal{C}}_{\text{sec}} = \sum^{\sim} \frac{\mathcal{K}}{\ln 2} \sum_{p=1}^{L} \left[\mathcal{A}_{p,1} \left\{ -\frac{(\ln \Theta_p)^2}{2} - \text{Li}_2\left(-\frac{1}{\Theta_p}\right) \right\} + \right.$$
$$\left. \sum_{q=2}^{r_p} \mathcal{A}_{p,q} \left\{ \frac{\ln(\Theta_p + 1)}{(\Theta_p)^{q-1}} - \sum_{n=2}^{q-1} \left(\frac{1}{\Theta_p}\right)^{q-n} \frac{1}{(n-1)(\Theta_p + 1)^{n-1}} \right\} \right] \tag{42}$$

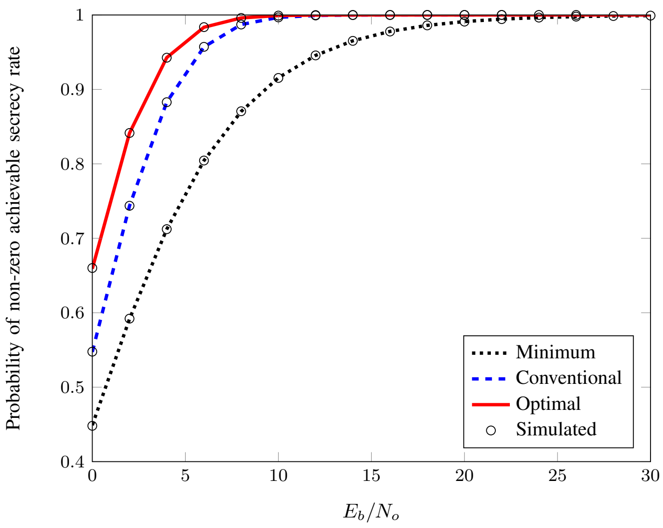

Fig. 2. Probability of non-zero achievable secrecy rate of the three relay selection schemes, with $K = 4$ and $M = 3$.

In (42), $\text{Li}_2(-x) = \int_1^x \frac{\ln t}{t-1} dt$ [29, eq. (27.7.1)]. The proof of Theorem 2 is given in Appendix D. It is worth noting that our derived method for the system achievable secrecy rate (i.e., (22), (30), and (42)) is highly precise at high SNRs and very simple with the determination of the appropriate parameters being done straightforwardly. Additionally, they are given in a closed-form fashion, its evaluation is instantaneous regardless of the number of trusted relays, the number of eavesdroppers and the value of the fading channels. Observing their final form, we easily recognize that the system capacities at high SNR regime only depend on $\Omega = \lambda_D/\lambda_E$ suggesting that the system achievable secrecy rate will keep the same regardless of the increase of the average SNR.

IV. Numerical Results and Discussion

Computer (Monte Carlo) simulations are used to demonstrate the performance of the three relay selection scheme under security conditions. The number of trials for each simulation results is 10^6.

In Figures 2 and 3, three relay selection schemes are compared in terms of probability of non-zero achievable secrecy rate, secrecy outage probability and achievable secrecy rate by fixing $\bar{\gamma}_E = 5$ dB and varying $\bar{\gamma}_D$ in steps of 5 dB in the range from 0 to 30 dB. It can be observed in these figures that there is excellent agreement between the simulation and the analysis results, confirming the correctness of our derivations. In Figure 2, the theoretical curves for the probability of non-zero achievable secrecy rate of the three schemes were plotted using equations (17), (25) and (39), respectively. At high $\bar{\gamma}_D$, all schemes yield nearly indistinguishable probabilities of non-zero achievable secrecy rate with unity value. However, at low $\bar{\gamma}_D$, the optimal selection scheme outperforms the others while the minimum selection scheme provides the lowest probability of non-zero achievable secrecy rate. Figure 3 plots the secrecy outage probability for the three schemes. For a given R, increasing SNR leads to a different increase in the shape of secrecy outage probabilities. In particular, the curves for

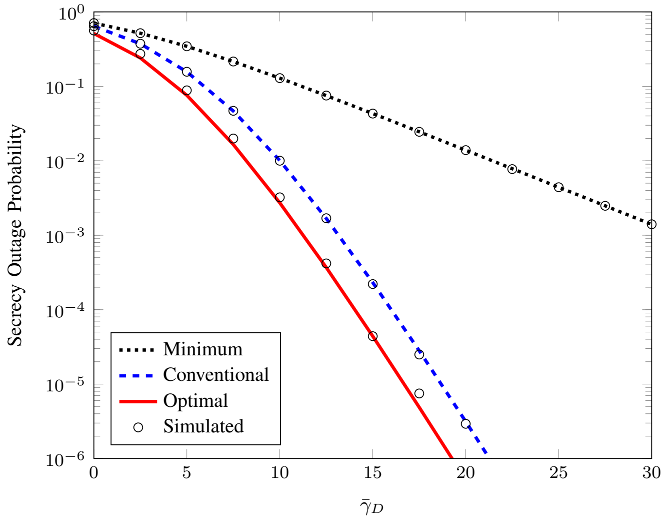

Fig. 3. Secrecy outage probability of the three relay selection schemes, with $K = 4$, $M = 3$, and $R = 0.5$.

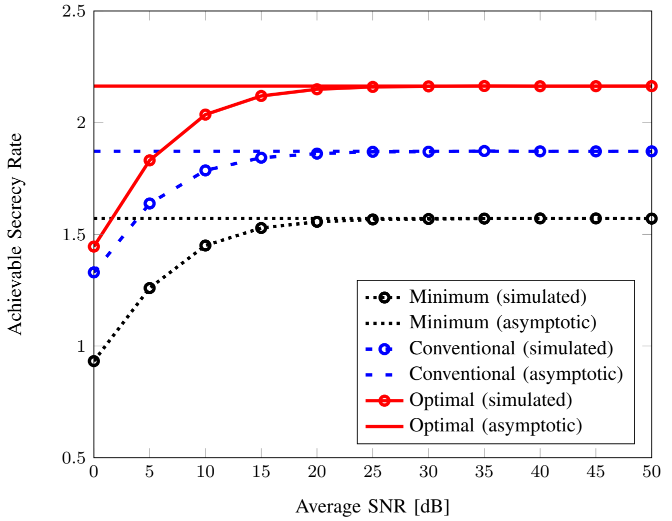

Fig. 4. Achievable secrecy rate versus average SNRs.

optimal selection and conventional selection have the same slope while that for minimum selection exhibits the smallest slope. This is due to the fact that the minimum selection scheme selects the relay having the worst channels towards the eavesdropper group. In addition, this scheme does not take into account the relay-destination links on the relay selection metric. In terms of diversity gain, this will not provide any diversity gain since it selects the relay that has the worst channels to the eavesdroppers.

The impact of the achievable secrecy rates of three relay selection schemes versus the average SNR is shown in Figure 4. The optimal selection scheme provides the best performance as compared to the others. In addition, there is significant gaps between the capacities achieved by the schemes. In the high SNR regime, these gaps become constant regardless of the increased transmit power of the relays. Because of the limit of large $\mathcal{P}_{\mathrm{R}}$, the system achievable secrecy rates approach a finite value, which represents an "upper floor". This phenomenon suggests that at high SNRs the secrecy probability remains the same regardless of how large the average SNR is. We also observe that the simulation and the exact analysis results are in excellent agreement.

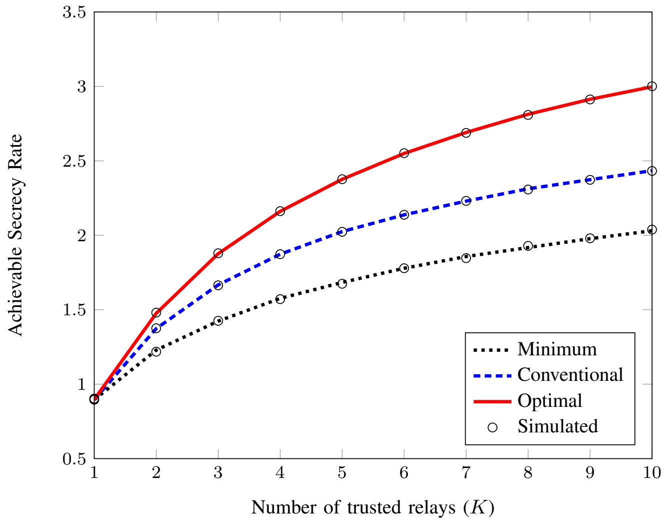

Fig. 5. Achievable secrecy rate versus the number of the relays, with $\bar{\gamma}_D = \bar{\gamma}_E = 30$ dB and $M = 3$.

Figure 5 illustrates the achievable secrecy rates of the three relay selection schemes versus the number of relays in the network. It can be seen that the optimal selection scheme again achieves the highest achievable secrecy rate. The curves indicate that for a fixed number of eavesdroppers, a non-negligible performance improvement can be obtained by increasing the number of trusted relays. This is due to the fact that when the number of relays increases, the network has more opportunities to choose the most appropriate relay for security purposes. The result also confirms that the conventional selection scheme always outperforms the minimum selection scheme; in terms of secrecy efficiency, improving the data links is better than improving the eavesdropper links. This can be explained by the concept of diversity gain. The conventional selection scheme provides a diversity gain for the relay-eavesdropper links while the minimum selection scheme keeps the diversity gain the same when the number of relays and the number of eavesdroppers are respectively increased.

Figure 6 shows the impact of the achievable secrecy rates of the three schemes against the number of the eavesdroppers. Contrary to the results in Figure 5, the achievable secrecy rates now decrease when the number of the malicious nodes increases. This is expected because the chance of overhearing will increase when the number of eavesdroppers increases.

V. Conclusion

In this paper, we have studied the effects of three relay selection schemes, which are minimum selection, conventional selection, and optimal selection (which is optimal with respect to secrecy), under security constraints in the presence of multiple eavesdroppers. Based on the closed-form expressions of the PDF and the CDF of the eavesdropper links and data links, three key performance metrics under Rayleigh fading

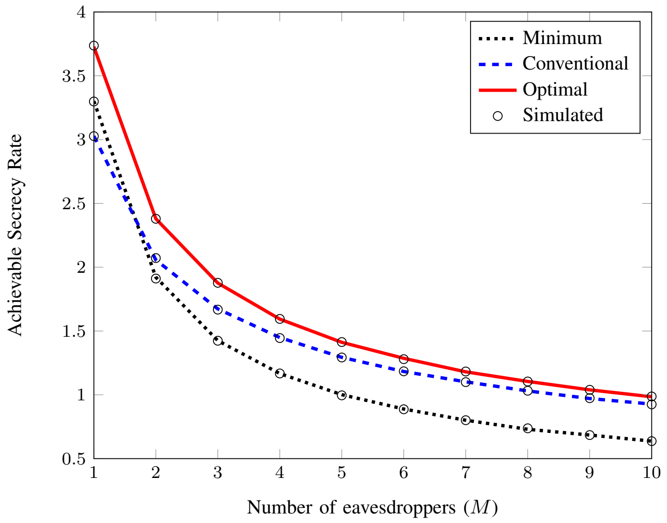

Fig. 6. Achievable secrecy rate versus the number of the eavesdroppers, with $\bar{\gamma}_D = \bar{\gamma}_E = 30$ dB and $K = 4$.

were derived: the probability of non-zero secrecy capacity, the secrecy outage probability and the achievable secrecy rate. The numerical results have shown that optimal selection outperforms conventional selection, which in turns outperforms minimum selection. Furthermore, conventional selection always provides better secure performance than minimum selection, thus suggesting that increasing the number of cooperative relays is more efficient than increasing the transmit power at relays. The simulation results are in excellent agreement with the analysis results confirming the correctness of our derivation approach.

Appendix A
Proof of Lemma 1

We start the proof by exploiting the independent channel assumption of eavesdropper channels, leading to

$$f_{k^*,E}(\gamma) = \sum_{k=1}^{K} f_{\gamma_{kE}}(\gamma) \prod_{n=1, n\neq k}^{K} [1 - F_{\gamma_{kE}}(\gamma)]. \tag{A.1}$$

In (A.1), $F_{\gamma_{k,E}}(\gamma)$ is the cumulative distribution function (CDF) of $\gamma_{k,E}$ and can be computed according to the binomial theorem [30] as

$$\begin{aligned} F_{\gamma_{k,E}}(\gamma) &= \prod_{m=1}^{M} F_{\gamma_{k,m}}(\gamma) \\ &= \left(1 - e^{-\frac{\gamma}{\bar{\gamma}_E}}\right)^M \\ &= \sum_{m=0}^{M} \binom{M}{m} (-1)^m e^{-\frac{m\gamma}{\bar{\gamma}_E}} \\ &= 1 - \sum_{m=1}^{M} \binom{M}{m} (-1)^{m-1} e^{-\frac{m\gamma}{\bar{\gamma}_E}}, \end{aligned} \tag{A.2}$$

where $\bar{\gamma}_E = \mathcal{P}_{\mathrm{R}}\lambda_E$, and hence the PDF of $\gamma_{k,E}$ is obtained by

$$\begin{aligned} f_{\gamma_{k,E}}(\gamma) &= \frac{dF_{\gamma_{k,E}}(\gamma)}{d\gamma} \\ &= \sum_{m=1}^{M} (-1)^{m-1} \binom{M}{m} \frac{m}{\bar{\gamma}_E} e^{-\frac{m\gamma}{\bar{\gamma}_E}}. \end{aligned} \tag{A.3}$$

Since $\bar{\gamma}_{k,E} = \bar{\gamma}_E$ for all k, (A.1) is simplified as

$$f_{k^*,E}(\gamma) = K[1 - F_{\gamma_{kE}}(\gamma)]^{K-1} f_{\gamma_{kE}}(\gamma), \tag{A.4}$$

Plugging (A.2) and (A.3) into (A.4) and after arranging and grouping terms in an appropriate order, we can express (A.4) in a compact and elegant form as (15).

Since $\bar{\gamma}_{k,1} \neq \bar{\gamma}_{k,1} \neq \cdots \neq \bar{\gamma}_{k,M}$, the CDF and the PDF of $\gamma_{k,E}$ can be respectively expressed as

$$\begin{aligned} F_{\gamma_{k,E}}(\gamma) &= \prod_{m=1}^{M} F_{\gamma_{k,m}}(\gamma) \\ &= \prod_{m=1}^{M} \left(1 - e^{-\frac{\gamma}{\bar{\gamma}_{E,m}}}\right) \\ &= \sum_{k=1}^{M} (-1)^{k-1} \sum_{\substack{m_1=\cdots=m_k=1 \\ m_1<\cdots<m_k}}^{M} (1 - e^{-\gamma\chi_k}) \\ &= 1 - \sum_{k=1}^{M} (-1)^{k-1} \sum_{\substack{m_1=\cdots=m_k=1 \\ m_1<\cdots<m_k}}^{M} e^{-\gamma\chi_k} \end{aligned} \tag{A.5}$$

and

$$f_{\gamma_{k,E}}(\gamma) = \sum_{k=1}^{M} (-1)^{k-1} \sum_{\substack{m_1=\cdots=m_k=1 \\ m_1<\cdots<m_k}}^{M} \chi_k e^{-\gamma\chi_k} \tag{A.6}$$

where $\chi_k = \left(\sum_{\ell=1}^{k} \frac{1}{\bar{\gamma}_{E,m_\ell}}\right)^{-1}$. Noting that the form of (A.5) and (A.6) take the similar form of (A.2) and (A.3) in the revised manuscript, i.e., they are also of the summation form of exponential distribution leading to the fact that the same approach suggested our papers could be used to solve for the generalized case. Therefore, the assumption $\lambda_{k,m} = \lambda_E$ will not affect on the results and conclusions made in the paper, especially on the effects of relay selections.

Appendix B
Proof of Lemma 2

Here we derive the CDF and PDF of $\gamma_{k^*,D}$. Using conditional probability [30], $F_{\gamma_{k^*}}(\gamma)$ is given by

$$\begin{aligned} F_{\gamma_{k^*}}(\gamma) &= \Pr\left(\frac{\gamma_{k^*,D}}{\gamma_{k^*,E}} \leq \gamma\right) \\ &= \int_0^\infty \Pr(\gamma_{k^*,D} \leq \gamma\gamma_{k^*,E}) f_{\gamma_{k^*,E}}(\gamma_{k^*,E}) d\gamma_{k^*,E} \\ &= 1 - \sum^{\sim} \mathcal{K} \frac{\bar{\gamma}_D \chi}{\gamma + \bar{\gamma}_D \chi}. \end{aligned} \tag{B.1}$$

Since the PDF and the CDF are related by $f_{\gamma_{k^*}}(\gamma) = \frac{dF_{\gamma_{k^*}}(\gamma)}{d\gamma}$, we have

$$f_{\gamma_{k^*}}(\gamma) = \overset{\sim}{\sum} \mathcal{K} \frac{\bar{\gamma}_D \chi}{(\gamma + \bar{\gamma}_D \chi)^2}. \tag{B.2}$$

Appendix C
Proof of Lemma 3

Under the assumption of channel independence and then using order statistics, we are able to derive the PDF of $\gamma_{k^*} = \max_k \gamma_k$ by getting the maximum value from K secrecy channel gains as

$$f_{\gamma_{k^*}}(\gamma) = \frac{dF_{\gamma_{k^*}}(\gamma)}{d\gamma} = \frac{d}{d\gamma}[F_{\gamma_k}(\gamma)]^K. \tag{C.1}$$

Plugging (35) and (36) into (C.1), we have [30, p. 246]

$$\begin{aligned} f_{\gamma_{k^*}}(\gamma) &= K[F_{\gamma_k}(\gamma)]^{K-1} f_{\gamma_k}(\gamma) \\ &= K\left[\sum_{m=1}^{M} (-1)^{m-1} \binom{M}{m} \frac{\gamma}{\gamma + \alpha_m}\right]^{K-1} \\ &\times \left[\sum_{m=1}^{M} (-1)^{m-1} \binom{M}{m} \frac{\alpha_m}{(\gamma + \alpha_m)^2}\right] \end{aligned} \tag{C.2}$$

After tedious manipulation, we have the compact form of the PDF for γ_{k^*} as follows:

$$f_{\gamma_{k^*}}(\gamma) = \sum_{m_1=1}^{M} \cdots \sum_{m_K=1}^{M} \mathcal{K} \frac{\alpha_1 \gamma^{K-1}}{(\gamma + \alpha_1) \prod_{k=1}^{K} (\gamma + \alpha_k)}. \tag{C.3}$$

Here, we recall that

$$\overset{\sim}{\sum} = \sum_{m_1=1}^{M} \cdots \sum_{m_K=1}^{M}$$

and

$$\mathcal{K} = K(-1)^{-K + \sum_{p=1}^{K} m_p} \prod\nolimits_{q=1}^{K} \binom{M}{m_q}.$$

With the current form of γ_{k^*}, it seems impossible to derive the system achievable secrecy rate. For that matter, we employ the residue theorem [31] by first expressing the product form of $f_{\gamma_{k^*}}(\gamma)$ in the following partial-fraction expansion where in the each resulting terms can be integrable, namely

$$\frac{\alpha_1 \gamma^{K-1}}{(\gamma + \alpha_1) \prod_{k=1}^{K} (\gamma + \alpha_k)} = \sum_{p=1}^{L} \sum_{q=1}^{r_p} \frac{\mathcal{A}_{p,q}}{(\gamma + \Theta_p)^q}, \tag{C.4}$$

In the above, Θ_p are L distinct elements of the set of $\{\alpha_k\}_{k=1}^{K}$ in decreasing order and $\mathcal{A}_{p,q}$ are the coefficients of the partial-fraction expansion, readily determined as [32][3]

$$\mathcal{A}_{p,q} = \frac{1}{(r_p - q)!} \left\{ \frac{\partial^{(r_p - q)}}{\partial \gamma^{(r_n - q)}} [(\gamma + \Theta_p)^{r_p} f_{\gamma_{k^*}}(\gamma)] \right\} \Bigg|_{\gamma = -\Theta_p} \tag{C.6}$$

Pulling everything together, we complete the proof.

Appendix D
Proof of Theorem 2

By proceeding in a similar way, the asymptotic achievable secrecy rate of the optimal selection scheme is approximated by

$$\begin{aligned} \overline{\mathcal{C}}_{\text{opt}} &\approx \int_{1}^{\infty} \log_2(\gamma) f_{\gamma_{k^*}}(\gamma) d\gamma \\ &= \overset{\sim}{\sum} \sum_{p=1}^{L} \sum_{q=1}^{r_p} \frac{\mathcal{K} \mathcal{A}_{p,q}}{\ln 2} \int_{0}^{\infty} \frac{\ln(\gamma)\, d\gamma}{(\gamma + \Theta_p)^q}. \end{aligned} \tag{D.1}$$

It should be noted that the integral $\int_1^\infty \frac{\ln(\gamma) d\gamma}{\gamma + \Theta_p}$ (i.e., when $q = 1$) cannot be evaluated in a closed form. To deal with such problem, we partition the inner integral into two parts

$$\overline{\mathcal{C}}_{\text{opt}} \overset{\mathcal{P}_{\text{R}} \to \infty}{\to} \overset{\sim}{\sum} \frac{\mathcal{K}}{\ln 2} \left[\mathcal{I}_1 + \sum_{p=1}^{L} \sum_{q=2}^{r_p} \mathcal{A}_{p,q} \mathcal{I}_2 \right]. \tag{D.2}$$

where $\mathcal{I}_1$ and $\mathcal{I}_2$ are of the following forms:

$$\mathcal{I}_1 = \sum_{p=1}^{L} \mathcal{A}_{p,1} \int_{1}^{\infty} \frac{\ln(\gamma)\, d\gamma}{\gamma + \Theta_p} \tag{D.3}$$

$$\mathcal{I}_2 = \int_{1}^{\infty} \frac{\ln(\gamma)\, d\gamma}{(\gamma + \Theta_p)^q}, \quad q \geq 2. \tag{D.4}$$

By using the fact that $\sum_{p=1}^{L} \mathcal{A}_{p,1} = 0$ and recognizing the integral representation of the dilogarithm function[4], that is, $\text{Li}_2(-x) = \int_1^x \frac{\ln t}{t-1} dt$, $\mathcal{I}_1$ can be derived to [28, eq. (2.727.1)]

$$\mathcal{I}_1 = -\sum_{p=1}^{L} \mathcal{A}_{p,1} \left[\frac{(\log \Theta_p)^2}{2} + \text{Li}_2\left(-\frac{1}{\Theta_p}\right) \right]. \tag{D.5}$$

For $\mathcal{I}_2$, using integration by parts yields

$$\mathcal{I}_2 = \underbrace{-\frac{\ln \gamma}{(q-1)(\gamma + \Theta_p)^{q-1}} \Bigg|_{\gamma=1}^{\infty}}_{\to 0} + \underbrace{\frac{1}{q-1} \int_{1}^{\infty} \frac{d\gamma}{\gamma(\gamma + \Theta_p)^{q-1}}}_{\mathcal{I}_3}. \tag{D.6}$$

Applying partial fraction technique and then grouping together appropriate terms, we have

$$\begin{aligned} \mathcal{I}_3 &= \left(\frac{1}{\Theta_p}\right)^{q-1} \int_{1}^{\infty} \left(\frac{1}{\gamma} - \frac{1}{\gamma + \Theta_p} \right) d\gamma - \sum_{n=2}^{q-1} \left(\frac{1}{\Theta_p}\right)^{q-n} \int_{1}^{\infty} \frac{d\gamma}{(\gamma + \Theta_p)^n} \\ &= \left(\frac{1}{\Theta_p}\right)^{q-1} \ln(\Theta_p + 1) - \sum_{n=2}^{q-1} \left(\frac{1}{\Theta_p}\right)^{q-n} \frac{1}{(n-1)(\Theta_p + 1)^{n-1}}. \end{aligned} \tag{D.7}$$

[3] For convenience, coefficients $\mathcal{A}_{p,q}$ can be obtained more easily by solving the system of $K+1$ equations which is established by randomly choosing $K+1$ distinct values of γ but not equal to any Θ_p [33]. Denoting $K+1$ values of γ as B_u with $u = 1, \ldots, K+1$, we can obtain the following linear system of equations

$$\sum_{p=1}^{L} \sum_{q=1}^{r_p} \frac{\mathcal{A}_{p,q}}{(\gamma + \Theta_p)^q} = \frac{1}{(\gamma + \alpha_1) \prod_{k=1}^{K} (\gamma + \alpha_k)}, \tag{C.5}$$

where $\mathbf{A} = [\ \mathcal{A}_{1,1} \ \cdots \ \mathcal{A}_{p,q} \ \cdots \ \mathcal{A}_{L,r_L}\ ]^T$ is obtained by $\mathbf{A} = \mathbf{C}^{-1}\mathbf{D}$ where $[.]^T$ is a transpose operator; $\mathbf{C}$ is a $K+1 \times K+1$ matrix whose entries are $C_{u,v} = \frac{1}{(B_u + \Theta_p)^q}$ with $v = q + \sum\limits_{m=1}^{p-1} r_m$; $\mathbf{D} = [\ D_1 \ \cdots \ D_u \ \cdots \ D_{K+1}]^T$ with $D_u = \frac{1}{(B_u + \alpha_1) \prod_{n=1}^{K} (B_u + \alpha_n)}$ and $u, v = 1, \ldots, K$.

[4] The dilogarithm function is a special case of the polylogarithm.

Finally, combining (D.5), (D.6) and (D.2), we have the final approximated closed-form expression for the achievable secrecy rate.

Acknowledgment

This work was supported by Project 39/2012/HD/NDT granted by the Ministry of Science and Technology of Vietnam.

References

[1] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 74–80, Oct. 2004.

[2] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[3] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

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

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

[6] V. Aggarwal, L. Sankar, A. Calderbank, and H. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," *EURASIP J. Wirel. Comm.*, vol. 2009, pp. 1–14, 2009.

[7] P. Popovski and O. Simeone, "Wireless secrecy in cellular systems with infrastructure-aided cooperation," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 2, pp. 242–256, Feb. 2009.

[8] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[9] A. Bletsas, H. Shin, and M. Win, "Outage analysis for cooperative communication with multiple amplify-and-forward relays," *Electron. Lett.*, vol. 43, no. 6, Mar. 2007.

[10] I. Krikidis, J. Thompson, S. McLaughlin, and N. goertz, "Amplify-and-forward with partial relay selection," *IEEE Commun. Lett.*, vol. 12, no. 4, pp. 235–237, Apr. 2008.

[11] J. Lopez Vicario, A. Bel, J. A. Lopez-Salcedo, and G. Seco, "Opportunistic relay selection with outdated CSI: Outage probability and diversity analysis," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 2872–2876, Jun. 2009.

[12] M. Seyfi, S. Muhaidat, and J. Liang, "Performance analysis of relay selection with feedback delay," *IEEE Signal Process. Lett.*, vol. 18, no. 1, pp. 67–70, Jan. 2010.

[13] W. Zhang, D. Duan, and L. Yang, "Relay selection from a battery energy efficiency perspective," *IEEE Trans. Commun.*, vol. 59, no. 6, pp. 1525 – 1529, Jun. 2011.

[14] K. Junsu, A. Ikhlef, and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," *J. Commun. Netw.*, vol. 14, no. 4, pp. 364–373, Aug. 2012.

[15] L. Yupeng and A. P. Petropulu, "Relay selection and scaling law in destination assisted physical layer secrecy systems," in *Proc. 2012 IEEE Statistical Signal Processing Workshop (SSP'12)*, 2012, pp. 381–384.

[16] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Commun.*, vol. 6, no. 16, pp. 2676–2687, Nov. 2012.

[17] Y. Shi, P. Mugen, W. Wenbo, D. Liang, and M. Ahmed, "Relay self-selection for secure cooperative in amplify-and-forward networks," in *Proc. 2012 7th International ICST Conference on Communications and Networking in China (CHINACOM'12)*, 2012, pp. 581–585.

[18] C. Chunxiao, C. Yueming, and Y. Weiwei, "Secrecy rates for relay selection in OFDMA networks," in *Proc. 2011 Third International Conference on Communications and Mobile Computing (CMC'11)*, 2011, pp. 158–160.

[19] S. Luo, H. Godrich, A. Petropulu, and H. V. Poor, "A knapsack problem formulation for relay selection in secure cooperative wireless communication," in *Proc. 2011 IEEE International Conference onAcoustics, Speech and Signal Processing (ICASSP'11)*, 2013, pp. 2512–2515.

[20] W. Li, K. Tenghui, S. Mei, W. Yifei, and T. Yinglei, "Research on secrecy capacity oriented relay selection for mobile cooperative networks," in *Proc. 2011 IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS'11)*, 2011, pp. 443–447.

[21] R. Bassily and S. Ulukus, "Deaf cooperation and relay selection strategies for secure communication in multiple relay networks," vol. 61, no. 6, pp. 1544–1554, Dec. 2013.

[22] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Aug. 2009.

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

[24] A. Bletsas, H. Shin, and M. Z. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, pp. 3450–3460, Jun. 2007.

[25] A. Ozgur, O. Leveque, and D. Tse, "Hierarchical cooperation achieves optimal capacity scaling in ad hoc networks," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3549–3572, Oct. 2007.

[26] E. Biglieri, J. Proakis, and S. Shamai, "Fading channels: information-theoretic and communications aspects," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2619–2692, Oct. 1998.

[27] L. Yingbin, K. Gerhard, P. H Vincent, and S. Shamai, "Compound wiretap channels," *EURASIP J. Wirel. Comm.*, vol. 2009, pp. 1–12, 2009.

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

[29] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, 10th ed., Washington: U.S. Govt. Print. Off., 1972.

[30] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*, 4th ed., Boston: McGraw-Hill, 2002.

[31] M. J. Roberts, *Signals and Systems: Analysis Using Transform Methods and MATLAB*, 1st ed., Dubuque, Iowa: McGraw-Hill, 2004.

[32] S. V. Amari and R. B. Misra, "Closed-form expressions for distribution of sum of exponential random variables," *IEEE Trans. Rel.*, vol. 46, no. 4, pp. 519–522, Apr. 1997.

[33] H. V. Khuong and H. Y. Kong, "General expression for pdf of a sum of independent exponential random variables," *IEEE Commun. Lett.*, vol. 10, no. 3, pp. 159–161, Mar. 2006.

Vo Nguyen Quoc Bao received the B.Eng. and M.Eng. degrees in electrical engineering from Ho Chi Minh City University of Technology, Vietnam, in 2002 and 2005, respectively, and the Ph.D. degree in electrical engineering from University of Ulsan, South Korea, in 2009. 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 systems, combining techniques, 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). He is also a Guest Editor of EURASIP Journal on Wireless Communications and Networking, special issue on “Cooperative Cognitive Networks” and IET Communications, special issue on “Secure Physical Layer Communications”.

Nguyen Linh-Trung received both the B.Eng. and Ph.D. degrees in Electrical Engineering from Queensland University of Technology, Brisbane, Australia. From 2003 to 2005, he had been a postdoctoral research fellow at the French National Space Agency (CNES). He joined the University of Engineering and Technology within Vietnam National University, Hanoi, in 2006 and is currently an associate professor at its Faculty of Electronics and Telecommunications. He has held visiting positions at Telecom ParisTech, Vanderbilt University, Ecole Supérieure d’Electricité (Supelec) and the Université Paris 13 Sorbonne Paris Cité. His research focuses on methods and algorithms for data dimensionality reduction, with applications to biomedical engineering and wireless communications. The methods of interest include time-frequency analysis, blind source separation, compressed sensing, and network coding. He was co-chair of the technical program committee of the annual International Conference on Advanced Technologies for Communications (ATC) in 2011 and 2012.

Mérouane Debbah entered the Ecole Normale Supérieure de Cachan (France) in 1996 where he received his M.Sc and Ph.D. degrees respectively. He worked for Motorola Labs (Saclay, France) from 1999-2002 and the Vienna Research Center for Telecommunications (Vienna, Austria) until 2003. He then joined the Mobile Communications department of the Institut Eurecom (Sophia Antipolis, France) as an Assistant Professor until 2007. He is now a Full Professor at Supelec (Gif-sur-Yvette, France), holder of the Alcatel-Lucent Chair on Flexible Radio and a recipient of the ERC starting grant MORE (Advanced Mathematical Tools for Complex Network Engineering). His research interests are in information theory, signal processing and wireless communications. He is a senior area editor for IEEE Transactions on Signal Processing and an Associate Editor in Chief of the journal Random Matrix: Theory and Applications. Mérouane Debbah is the recipient of the ”Mario Boella” award in 2005, the 2007 General Symposium IEEE GLOBECOM best paper award, the Wi-Opt 2009 best paper award, the 2010 Newcom++ best paper award, the WUN CogCom Best Paper 2012 and 2013 Award as well as the Valuetools 2007, Valuetools 2008, Valuetools 2012 and CrownCom2009 best student paper awards. He is a WWRF fellow and an elected member of the academic senate of Paris-Saclay. In 2011, he received the IEEE Glavieux Prize Award. He is the co-founder of Ximinds.