Exploiting Direct Links for Physical Layer Security in Multi-User Multi-Relay Networks

Lisheng Fan, Nan Yang, *Member, IEEE*, Trung Q. Duong, *Senior Member, IEEE*, Maged Elkashlan, *Member, IEEE*, and George K. Karagiannidis, *Fellow, IEEE*

***Abstract*—We present two physical layer secure transmission schemes for multi-user multi-relay networks, where the communication from M users to the base station is assisted by direct links and by N decode-and-forward relays. In this network, we consider that a passive eavesdropper exists to overhear the transmitted information, which entails exploiting the advantages of both direct and relay links for physical layer security enhancement. To fulfill this requirement, we investigate two criteria for user and relay selection and examine the achievable secrecy performance. *Criterion I* performs a joint user and relay selection, while *Criterion II* performs separate user and relay selections, with a lower implementation complexity. We derive a tight lower bound on the secrecy outage probability for Criterion I and an accurate analytical expression for the secrecy outage probability for Criterion II. We further derive the asymptotic secrecy outage probabilities at high transmit signal-to-noise ratios and high main-to-eavesdropper ratios for both criteria. We demonstrate that the secrecy diversity order is $\min(MN, M+N)$ for Criterion I, and N for Criterion II. Finally, we present numerical and simulation results to validate the proposed analysis, and show the occurrence condition of the secrecy outage probability floor.**

***Index Terms*—Physical layer security, multi-user multi-relay networks, direct links, secrecy outage probability, secrecy diversity order.**

Manuscript received April 22, 2015; revised December 7, 2015; accepted January 28, 2016. The associate editor coordinating the review of this paper and approving it for publication was Prof. Dimitrie Popescu.

This work was supported by NSF of China (No. 61372129/61471229), Guangdong Natural Science Funds for Distinguished Young Scholar (No. 2014A030306027), training program of excellent young teachers in Higher Education Institutions of Guangdong Province (No. Yq2013070), the Open Research Fund of State Key Laboratory of Integrated Services Networks (No. ISN17-05), the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22 and by the Newton Institutional Link under Grant ID 172719890. The work of N. Yang was supported by the Australian Research Council Discovery Project under Grant DP150103905.

L. Fan is with the Department of Electronic Engineering, Shantou University, and is also with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, China (e-mail: lsfan@stu.edu.cn).

N. Yang is with Australian National University, Canberra ACT 0200, Australia (e-mail: yangnan1616@gmail.com).

T. Q. Duong is with Queen's University Belfast, Belfast BT7 1NN, United Kingdom (e-mail: trung.q.duong@qub.ac.uk).

M. Elkashlan is with Queen Mary University of London, London E1 4NS, United Kingdom (email: maged.elkashlan@qmul.ac.uk).

G. K. Karagiannidis is with Aristotle University of Thessaloniki, Thessaloniki 54 124, Greece (e-mail: geokarag@ieee.org).

Digital Object Identifier 10.1109/TWC.2016.2530068

I. Introduction

Over the past few years, the world of wireless communications has experienced unprecedented growth, driven by the vast increase in the number of intelligent devices, the amount of base stations (BSs), and the demand of multimedia content. Spurred by the ubiquitousness and necessity of wireless connections in the near future, an enormous volume of private and sensitive information, e.g., financial data, medical records, and customer files, will be wirelessly transmitted. It is widely accepted that wireless communications are inherently insecure, due to the broadcast nature of the medium. As such, providing an unrivalled security service is one of the top priorities in the design and implementation of the current and future wireless networks.

Differing from the traditional key-based cryptographic techniques, physical (PHY) layer security enhances the secrecy of wireless communications by exploiting the characteristics of wireless channels, without using secret keys and complex encryption/decryption algorithms [1]. As the seminal work that laid down the fundamentals of PHY layer security, the authors in [2] introduced the wiretap channel as the basic model and defined the secrecy capacity as the maximum rate at which messages are reliably transmitted to the legitimate receiver, without being intercepted by unintended parties. Inspired by early studies, PHY layer security over fading channel has been studied from both information-theoretic and practical perspectives. For example, [3], [4] considered a single-input single-output (SISO) wiretap channel over Rayleigh fading and analyzed the secrecy capacity. Built upon these studies, PHY layer security in multi-input multi-output (MIMO) communication systems has been intensively addressed, due to the benefits of multi-antenna techniques, such as high data rate and high link reliability. For instance, several MIMO secure techniques have been investigated, such as beamforming (e.g., [5]–[7]), precoding (e.g., [8]), artificial noise (e.g., [9]), and antenna selection (e.g., [10]–[12]).

Recently, PHY layer security in relay networks has attracted considerable attention, due to the fact that cooperative relaying is envisioned as a very promising technique to enhance the performance of the next-generation wireless communication networks [13]–[19]. In secure communications, researchers have investigated traditional relaying protocols [20]–[28], such as amplify-and-forward (AF) and decode-and-forward (DF), where DF can be further specified as fixed DF and selective DF

[29][1]. For example, [21] employed relay selection to enhance secrecy in a multi-AF-relay network and adopted the intercept probability as the secrecy performance metric. In [22]–[24], a selective-DF based multi-relay network was considered and one relay out of multiple relays was selected for secrecy improvement. Note that a common feature of [21]–[24] is that the direct link between the source and the destination (or the eavesdropper) is unavailable. To investigate the impact of the direct link on the secrecy performance, [25] studied the performance of relay selection in a fixed-DF based multi-relay network with maximal ratio combining (MRC) receiver, where the available direct link between the source and receiver is not involved in the system relay selection. Considering multiple relays used to facilitate the downlink of multi-user networks, [26] and [27] analyzed the secrecy performance for AF-relay and selective-DF-relay selection, respectively. Besides these works, the secure communications of full-duplex relay and large systems were also investigated in the literature [30]–[33].

This paper lays the groundwork for understanding the role of the direct link on the PHY layer security in the uplink of multi-user multi-relay networks, which stands as a major advancement over [26] and [27] which focused on the downlink[2]. We investigate secure user and relay selection schemes and analyze the achievable secrecy performance of the uplink where N fixed-DF relays assist the communication from M users to the BS. The BS adopts MRC to process the received signals through both the direct link and the relay link. We assume that a passive eavesdropper exists in this network to overhear the transmitted information. We note that although selective-DF based multiuser multi-relay networks have been extensively investigated, e.g., [27], [34], [35], fixed-DF based multiuser multi-relay networks with an MRC receiver have not been analyzed in the literature, regardless of secure or non-secure communications. The key contributions of this paper are summarized as follow:

- We propose two user and relay selection criteria that select the best user and relay pair, to exploit the advantages of both direct and relay links for PHY layer security enhancement. In Criterion I, a joint user and relay selection is performed to maximize the data rate of the main links, from the selected user to the BS. In Criterion II, separate user and relay selections are performed, based on direct and relay links, respectively, which reduces the implementation complexity.
- We derive novel expressions for the secrecy outage probability, in order to investigate the secrecy performance achieved by the proposed criteria. For Criterion I, we derive a tight lower bound on the secrecy outage probability, whereas for Criterion II, we present an accurate analytical expression.
- We present new results for the asymptotic secrecy outage probability for both criteria. These asymptotic expressions enable us to determine the main factors that regulate the secrecy performance in the transmit high signal-to-noise ratio (SNR) and the high main-to-eavesdropper ratio (MER) regimes.
- Based on the asymptotic results, we demonstrate that Criterion I achieves the secrecy diversity order of $\min(MN, M+N)$, while Criterion II achieves the secrecy diversity order of N. Notably, the number of users does not affect the secrecy diversity order for Criterion II. With the help of simulations, we verify our analysis and investigate the impact of the network parameters on the secrecy performance.
- Finally, we show that the secrecy outage probability floor occurs when the transmit power increases and the MER of either direct link or relay link is fixed.

The organization of this paper is as follows. After the introduction, Section II describes the model of a two-phase uplink multi-user multi-relay network and details the proposed criteria for user and relay selection. Section III presents the secrecy outage probabilities for the two criteria, including the derivations for both the exact and asymptotic results. Numerical results are provided in Section IV to offer valuable insights into the secrecy performance. Conclusions are drawn in Section V.

Notation: $X \sim \mathcal{CN}(0, \sigma^2)$ denotes a circularly symmetric complex Gaussian random variable X with zero mean and variance σ^2; $\Pr[\cdot]$ is the probability; $f_X(\cdot)$ and $F_X(\cdot)$ represent the probability density function (PDF) and cumulative distribution function (CDF) of the random variable X, respectively.

II. User and Relay Selection in Multi-User Multi-Relay Network

A. The Multi-user Multi-relay Network Model

Let us consider a secure multi-user multi-relay network, as depicted in Fig. 1, where the communication between M users S_m, $m \in \{1, \cdots, M\}$, and the BS D is assisted by N DF relays R_n, $n \in \{1, \cdots, N\}$[3]. In practice, this model represents the uplink of a multi-user cellular system with multiple relays, which assist the user–BS transmission. We assume that an eavesdropper E [4] exists in this network and overhears the transmitted messages, bringing out the important issue of information wiretap. We further assume that all nodes in the network are equipped with a single antenna, due to the size limitation, and operate in a half-duplex time-division mode.

[1]Compared with selective-DF relaying, fixed-DF relaying does not need additional feedback caused by notification, and hence is easier to implement in practice [29]. In the following, we use DF to denote fixed-DF if not specified.

[2]We clarify that there are several significant differences between this paper and [26] and [27]. First, the relaying protocol is different. This paper considers the fixed-DF relaying protocol whereas [26] and [27] consider AF and selective-DF relaying, respectively. Second, this paper exploits the direct link in both user selection and relay selection, whereas [26] did not consider the direct link and [27] performed the relay selection without using the direct link. These differences make the results of this paper fundamentally different from those in [26] and [27].

[3]We assume that the M users are relatively close together and in the same cluster, which have the same distance to the other nodes in the network. This assumption also holds for the N relays.

[4]If multiple eavesdroppers exist in the network, the secrecy performance will be degraded. This is caused by an increase in the success probability of eavesdropping, i.e., either by the best eavesdropper with the most favorable channel condition or by the collaboration of multiple eavesdroppers.

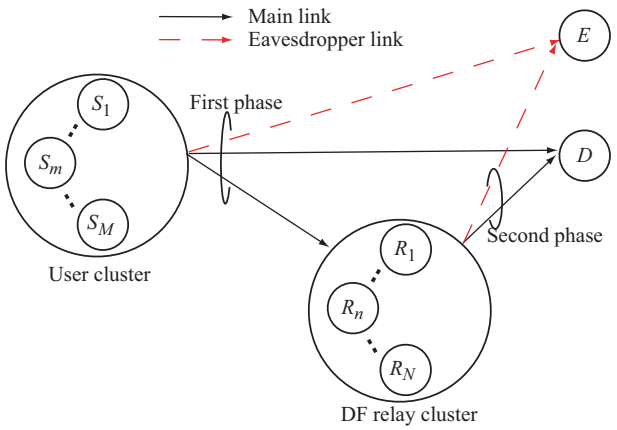


Fig. 1. The illustration of a two-phase secure multi-user multi-relay network with direct links.

To enhance the transmission security, both user selection and relay selection will be performed in this work to select one best user S_{m^*} among M users to communicate with D, with the help of a selected R_{n^*} out of N relays[5]. In practice, user selection can be applied in a multiuser LTE-Advanced cellular system to improve the system throughput [37], [38], whereas relay selection is feasible in IEEE 802.12j vehicular networks to improve the system capacity [34], [39]. We further assume that the direct link between the source and the destination is available. The adoption of this assumption is not to complicate the system model, but to address a practical scenario in wireless cellular networks. In practice, the direct link is available if the source and the destination are not placed remotely, or the destination does not fall within heavily shadowed areas. Motivated by this practicality, the impact of the direct link on the performance of relay-aided wireless systems has been examined in [34], [35] and [40]–[42]. Since the direct links can affect both the legitimate transmission and the illegitimate wiretap, the impact of both direct and relay links on the user and relay selection has to be considered for the secure transmission. To present the relay and user selection criteria, we first detail the two-phase transmission process, as follow:

Suppose that the user S_m and the relay R_n have been selected for data transmission. In the first phase, S_m sends the encoded signal of unit-variance, x_s, with transmit power P. The received signal at R_n, D, and E in the first phase are given by

$$y_{R_n} = h_{S_m,R_n}\sqrt{P}x_s + n_R, \tag{1}$$

$$y_D^{(1)} = h_{S_m,D}\sqrt{P}x_s + n_D^{(1)}, \tag{2}$$

$$y_E^{(1)} = h_{S_m,E}\sqrt{P}x_s + n_E^{(1)}, \tag{3}$$

[5]The residual users and relays are assumed to keep silent in this work. In some communication systems [24], [25], [28], [36], the residual users and relays can send jamming signals to confuse the eavesdropper, at the cost of an increased implementation complexity. The transmission of jamming signals will be addressed in future work.

respectively, where $h_{S_m,R_n} \sim \mathcal{CN}(0,\alpha)$, $h_{S_m,D} \sim \mathcal{CN}(0,\varepsilon_1)$, and $h_{S_m,E} \sim \mathcal{CN}(0,\varepsilon_2)$ denote the channel coefficients of the S_m–R_n link, S_m–D link, and S_m–E link, respectively. We also denote $n_R \sim \mathcal{CN}(0,\sigma^2)$, $n_D^{(1)} \sim \mathcal{CN}(0,\sigma^2)$, and $n_E^{(1)} \sim \mathcal{CN}(0,\sigma^2)$ as the additive white Gaussian noise (AWGN) at R_n, D, and E in the first phase. If R_n correctly decodes the message received in the first phase, it then re-encodes the signal with the same code book at S_m and forwards it to D in the second phase. Accordingly, the received signal at D and E in the second phase are given by

$$y_D^{(2)} = h_{R_n,D}\sqrt{P}x_s + n_D^{(2)} \tag{4}$$

$$y_E^{(2)} = h_{R_n,E}\sqrt{P}x_s + n_E^{(2)}, \tag{5}$$

respectively, where $h_{R_n,D} \sim \mathcal{CN}(0,\beta_1)$ and $h_{R_n,E} \sim \mathcal{CN}(0,\beta_2)$ denote the channel coefficients of the R_n–D link and R_n–E link, respectively. We also denote $n_D^{(2)} \sim \mathcal{CN}(0,\sigma^2)$ and $n_E^{(2)} \sim \mathcal{CN}(0,\sigma^2)$ as the AWGN at D and E, respectively, in the second phase. Here, although we assume that the selected relay has the same transmit power as the selected user, we highlight that this assumption does not lose generality. We denote $u_{mn} = |h_{S_m,R_n}|^2$, $v_{1n} = |h_{R_n,D}|^2$, $v_{2n} = |h_{R_n,E}|^2$, $w_{1m} = |h_{S_m,D}|^2$, and $w_{2m} = |h_{S_m,E}|^2$ as the channel gains of the S_m–R_n link, R_n–D link, R_n–E link, S_m–D link, and S_m–E link, respectively. The end-to-end SNR at D for the repetition-coded fixed DF relaying can be written as [29, Eq. (15)]

$$\mathsf{SNR}_D = \bar{\gamma}\min\left(u_{mn}, v_{1n} + w_{1m}\right), \tag{6}$$

where $\bar{\gamma} = P/\sigma^2$ is the transmit SNR. According to [25], [43], we note that the secrecy outage occurs when the system achievable secrecy data rate falls below a predetermined secrecy rate R_s, i.e.,

$$\frac{1}{2}\log_2\left(1+\bar{\gamma}\min\left(u_{mn}, v_{1n}+w_{1m}\right)\right) - \frac{1}{2}\log_2\left(1+\bar{\gamma}\left(v_{2n}+w_{2m}\right)\right) < R_s. \tag{7}$$

After some mathematical manipulations, we re-express (7) as

$$\frac{1+\bar{\gamma}\min\left(u_{mn}, v_{1n}+w_{1m}\right)}{1+\bar{\gamma}\left(v_{2n}+w_{2m}\right)} < \gamma_s, \tag{8}$$

where $\gamma_s = 2^{2R_s}$ is the secrecy SNR threshold.

B. User and Relay Selection Criteria

We consider a practical passive eavesdropping scenario, where only the statistical information of the eavesdropper's channel is known, while the instantaneous information of the eavesdropper's channel is unknown. This indicates that the eavesdropper's channel coefficients, i.e., $h_{S_m,E}$ and $h_{R_n,E}$, are not available at the users, relays, and BS. Accordingly, the values of v_{2n} and w_{2m} are not known and thus cannot be involved in the selection criterion. We highlight that the passive eavesdropping scenario is a practical consideration since in practice the eavesdropper is generally not cooperative and not willing to feedback its instantaneous channel coefficients to the legitimate nodes. Moreover, the assumption of known

statistical information of the eavesdropper's channel applies to the scenario where the eavesdropper is part of a multiuser system which in alternate time slots it becomes an active legitimate participant in the system. As such, the eavesdropper feeds back its channel state information to the transmitter for the time slot where it is being served. From this information, and assuming that the eavesdropper is static (or moving slowly), the statistical knowledge of the eavesdropper's channel in the time slots where it is not being served can be derived. Under this consideration, we propose two user and relay selection criteria that select the best user and relay pair to carry out the secure transmission in the network. These criteria are described as follow:

1) Criterion I: In this criterion, the joint user and relay selection is performed by maximizing the achievable rate of the main links. Mathematically, the indices of the selected user and the relay are expressed as

$$(m^*, n^*) = \arg \max_{1\leq m\leq M} \max_{1\leq n\leq N} \min\left(u_{mn}, v_{1n} + w_{1m}\right). \quad (9)$$

This criterion achieves the optimal secrecy performance in the passive eavesdropping scenario. We clarify that an assumption adopted in (9) is that the eavesdropper has the same average channel gain to the users and the relays. If we consider the scenario where the eavesdropper has different average channel gains to the users and the relays, the statistical information of eavesdropper's channel needs to be taken into account in the selection criterion. Specifically, the selection in this scenario cannot be performed by maximizing the data rate of main link, but can be performed by maximizing $\frac{1+\bar{\gamma}\min(u_{mn}, v_{1n}+w_{1m})}{1+\bar{\gamma}(E[v_{2n}]+E[w_{2m}])}$, where $E[\cdot]$ denotes the statistical expectation.

In Criterion I, the term w_{1m} from the direct link is incorporated into the term $\min(u_{mn}, v_{1n})$ from the relay links. As such, the two terms cannot be separated from each other. It follows that Criterion I is a joint selection scheme where the user selection interacts with the relay selection.

2) Criterion II: Differing from Criterion I, Criterion II involves separate user and relay selections. Specifically, the best user is firstly selected based on the direct links [44], and then the best relay is selected based on the two-hop relay links [45]. The indices of the selected user and the relay can be expressed as

$$m^* = \arg \max_{1\leq m\leq M} w_{1m}, \quad (10)$$

and

$$n^* = \arg \max_{1\leq n\leq N} \min\left(u_{m^*n}, v_{1n}\right). \quad (11)$$

It is evident from (10) and (11) that user selection and relay selection are performed separately in Criterion II. Compared with Criterion I which needs an adder and a comparator to perform joint selection, Criterion II only requires a simple comparator to perform separate selections, bringing about a lower implementation complexity. Hence, our work provides a flexible choice for system design as follows: If the system has a powerful computational capability, Criterion I is preferred to achieve the best secrecy performance; otherwise Criterion II can be used to reduce the implementation complexity.

We next detail the channel estimation procedure for both criteria. At the beginning of each transmission block, the network needs to determine which pair of user and relay is selected for data transmission. To this end, we assume that D estimates the required channel coefficients of main links with the help of pilot signals from users and relays. Then D performs user selection and relay selection according to either Criterion I or Criterion II, and notifies the indices of the selected user and relay through dedicated feedback channels. After selection, the two-phase data transmission commences at the selected user S_{m^*} and relay R_{n^*}.

Based on (8), the secrecy outage probability with the selected user S_{m^*} and relay R_{n^*} is given by

$$\begin{aligned} P_{out} &= \Pr\left[\frac{1+\bar{\gamma}\min\left(u_{m^*n^*}, v_{1n^*}+w_{1m^*}\right)}{1+\bar{\gamma}\left(v_{2n^*}+w_{2m^*}\right)} < \gamma_s\right], \\ &= \Pr\left[Z < \gamma_s\left(v_{2n^*}+w_{2m^*}\right)+\gamma_s'\right], \end{aligned} \quad (12)$$

where $\gamma_s' = (\gamma_s - 1)/\bar{\gamma}$ and $Z \triangleq \min\left(u_{m^*n^*}, v_{1n^*}+w_{1m^*}\right)$. Evidently, the statistical characterization of Z is the key for the evaluation of P_{out}.

III. Analysis of Secrecy Outage Probability

In this section, we derive new exact and asymptotic expressions for the secrecy outage probability, where both criteria are considered.

A. A Tight Lower Bound for Criterion I

For Criterion I, we first rewrite Z as

$$Z = \max_{1\leq m\leq M} \max_{1\leq n\leq N} \min\left(u_{mn}, v_{1n}+w_{1m}\right). \quad (13)$$

From (13), we can conclude that Z is the maximum of $M \times N$ non-independent variables, $\{\min\left(u_{mn}, v_{1n}+w_{1m}\right)\}$. This is due to the fact that M users share the common variable v_{1n}, while N relays share the common variable w_{1m}. Moreover, we see that the variable w_{1m} from the direct link affects both relay selection and user selection. This makes the mathematical derivation for the fixed-DF based multi-user multi-relay networks much more complicated than that for AF or selective-DF based multi-user multi-relay networks[6]. Therefore, it is mathematical difficult, if not impossible, to obtain an exact analytical expression for the secrecy outage probability for Criterion I. Motivated by this, we turn to derive two upper bounds on Z by exchanging the sequence of max and min operations. The first upper bound is given by

$$\begin{aligned} Z_1 &= \max_{1\leq m\leq M} \min\left(\max_{1\leq n\leq N}\left(u_{mn}, v_{1n}+w_{1m}\right)\right) \\ &= \max_{1\leq m\leq M} \min\left(\max_{1\leq n\leq N} u_{mn}, \left(\max_{1\leq n\leq N} v_{1n}\right)+w_{1m}\right), \end{aligned} \quad (14)$$

[6]For AF [26] or selective-DF based multi-user multi-relay networks with direct links [27], [35], [42], [46], the system relay selection is based on the two-hop relay links only with a given user S_m. This indicates that the direct links have no impact on the relay selection. Hence, the mathematical derivation in these studies cannot be applied to the proposed work.

and the second upper bound by

$$Z_2 = \max_{1\le n\le N} \min\left(\max_{1\le m\le M}(u_{mn}, v_{1n} + w_{1m})\right) = \max_{1\le n\le N} \min\left(\max_{1\le m\le M} u_{mn}, v_{1n} + \max_{1\le m\le M}(w_{1m})\right). \quad (15)$$

Built upon Z_1 in (14) and Z_2 in (15), we next derive the lower bounds on the secrecy outage probability, i.e., $P_{1,out}^{LB}$ and $P_{2,out}^{LB}$. We note that Z_1 is effective only when the relay selection does not dominate the joint user and relay selection, while Z_2 is effective only when the user selection does not dominate the joint selection. Hence, the maximal value of $P_{1,out}^{LB}$ and $P_{2,out}^{LB}$ provides a very tight lower bound on the secrecy outage probability, which will be demonstrated by the numerical and simulation results in Section IV.

We now begin to derive $P_{1,out}^{LB}$ associated with Z_1. Let

$$v_1 = \max_{1\le n\le N} v_{1n}, \quad (16)$$

$$u_m = \max_{1\le n\le N} u_{mn}, \quad (17)$$

and then we rewrite Z_1 as

$$Z_1 = \max_{1\le m\le M} \underbrace{\min\left(u_m, v_1 + w_{1m}\right)}_{Z_{1m}}. \quad (18)$$

From (18), Z_{1m} is correlated with each other, because of the common variable v_1. To deal with this, we first derive the conditional CDF of Z_{1m} with respect to v_1, i.e., $F_{Z_{1m}}(z|v_1)$. By statistically averaging $F_{Z_{1m}}^{M}(z|v_1)$ with respect to v_1, we then obtain the analytical CDF of Z_1, i.e., $F_{Z_1}(z)$. We further statistically average $F_{Z_1}(\gamma_s(v_{2n^*} + w_{2m^*}) + \gamma_s')$ with respect to both v_{2n^*} and w_{2m^*} to obtain $P_{1,out}^{LB}$. The CDF of Z_1 is derived and presented in the following theorem.

Theorem 1: The CDF of Z_1 can be expressed as

$$F_{Z_1}(z) = \sum_{n_1=1}^{N}\sum_{n_2=0}^{MN} b_{1,n_1,n_2} e^{-c_{1,n_1,n_2} z} + \sum_{m=0}^{M}\sum_{n=1}^{N}\widetilde{\sum_{\{i\}}} q_{1i} b_{2,m,n}\left(e^{-q_{2i}z} - e^{-(q_{2i}+c_{2,m,n})z}\right), \quad (19)$$

where

$$b_{1,n_1,n_2} = (-1)^{n_1+n_2+1}\binom{N}{n_1}\binom{MN}{n_2},$$

$$c_{1,n_1,n_2} = \frac{n_1}{\beta_1} + \frac{n_2}{\alpha},$$

$$\widetilde{\sum_{\{i\}}} = \sum_{i_1=0}^{m}\sum_{i_2=0}^{i_1}\cdots\sum_{i_{N-1}=0}^{i_{N-2}},$$

$$q_{1i} = \binom{m}{i_1}\binom{i_1}{i_2}\cdots\binom{i_{N-2}}{i_{N-1}} b_{3,1}^{m-i_1} b_{3,2}^{i_1-i_2}\cdots b_{3,N-1}^{i_{N-2}-i_{N-1}} b_{3,N}^{i_{N-1}}$$

$$b_{3,n} = \binom{N}{n}(-1)^{n-1},$$

$$b_{2,m,n} = (-1)^{m+n-1}\binom{N}{n}\binom{M}{m}\frac{n\varepsilon_1}{n\varepsilon_1 - m\beta_1},$$

$$q_{2i} = c_{3,1}(m - i_1) + c_{3,2}(i_1 - i_2) + \cdots + c_{3,N-1}(i_{N-2} - i_{N-1}) + c_{3,N} i_{N-1},$$

$$c_{3,n} = \frac{n}{\alpha} + \frac{1}{\varepsilon_1},$$

and

$$c_{2,m,n} = \frac{n}{\beta_1} - \frac{m}{\varepsilon_1}.$$

Proof: See Appendix A. ∎

From Theorem 1 and eq. (12), we can derive the first lower bound of P_{out} as

$$P_{1,out}^{LB} = \int_0^\infty\int_0^\infty F_{Z_1}\left(\gamma_s(v_{2n^*} + w_{2m^*}) + \gamma_s'\right) \times f_{v_{2n^*}}(v_{2n^*}) f_{w_{2m^*}}(w_{2m^*}) dv_{2n^*} dw_{2m^*}. \quad (20)$$

By using the PDF of v_{2n^*}, given by $f_{v_{2n^*}}(x) = \frac{1}{\beta_2}e^{-\frac{x}{\beta_2}}$, and the PDF of w_{2m^*}, given by $f_{w_{2m^*}}(x) = \frac{1}{\varepsilon_2}e^{-\frac{x}{\varepsilon_2}}$, and solving the integral in (20), we derive $P_{1,out}^{LB}$ as

$$P_{1,out}^{LB} = \sum_{n_1=1}^{N}\sum_{n_2=0}^{MN} b_{1,n_1,n_2}\mathcal{L}(c_{1,n_1,n_2}) + \sum_{m=0}^{M}\sum_{n=1}^{N}\widetilde{\sum_{\{i\}}} q_{1i} b_{2,m,n}\left(\mathcal{L}(q_{2i}) - \mathcal{L}(q_{2i} + c_{2,m,n})\right), \quad (21)$$

where $\mathcal{L}(x)$ is defined as

$$\mathcal{L}(x) = \frac{e^{-\gamma_s' x}}{(1 + \beta_2\gamma_s x)(1 + \varepsilon_2\gamma_s x)}. \quad (22)$$

The second lower bound of P_{out}, $P_{2,out}^{LB}$, has the same form as $P_{1,out}^{LB}$ in (21) after replacing M with N and β_1 with ε_1. This is because of the symmetry existed in (14) and (15). Finally, the tight lower bound on the secrecy outage probability for Criterion I can be obtained as

$$P_{out}^{LB} = \max\left(P_{1,out}^{LB}, P_{2,out}^{LB}\right). \quad (23)$$

We highlight that (23) consists of elementary functions only, and as such, it can be easily evaluated.

B. Exact Formula for Criterion II

To derive the secrecy outage probability for Criterion II, we first derive the CDFs of w_{1m^*}, $u_{m^*n^*}$, and v_{1n^*}, as per the selection criterion characterized by eqs. (10) and (11), and then we obtain the CDF of Z, $F_Z(z)$. Furthermore, by averaging $F_Z(z)$ with respect to w_{2m^*} and v_{2n^*}, we derive an exact expression for P_{out}.

Theorem 2: The CDF of Z can be expressed by

$$F_Z(z) = 1 - \sum_{m=1}^{M}\sum_{n_1=0}^{N-1}\sum_{n_2=0}^{N-1}\Big(t_{1,n_1}t_{3,m,n_2}e^{-\frac{z}{\zeta}} + t_{2,n_1}t_{3,m,n_2} \times e^{-(\frac{n_1+1}{\zeta}+\frac{1}{\beta_1})z} + t_{1,n_1}t_{4,m,n_2}e^{-(\frac{1}{\alpha}+\frac{m}{\varepsilon_1})z} + t_{1,n_1}t_{5,m,n_2}e^{-(\frac{1}{\alpha}+\frac{n_2+1}{\zeta})z} + t_{2,n_1}t_{4,m,n_2} \times e^{-(\frac{n_1+1}{\zeta}+\frac{m}{\varepsilon_1})z} + t_{2,n_1}t_{5,m,n_2}e^{-(\frac{n_1+n_2+2}{\zeta})z}\Big], \tag{24}$$

where

$$\zeta = \frac{\alpha\beta_1}{\alpha+\beta_1},$$

$$t_{1,n} = \frac{b_{4,n}\zeta}{\zeta+n\beta_1},$$

$$t_{2,n} = b_{4,n}\left(\frac{1}{n+1} - \frac{\zeta}{\zeta+n\beta_1}\right),$$

$$t_{3,m,n} = (-1)^{m-1}\binom{M}{m}\frac{b_{4,n}\zeta m\beta_1}{(\zeta+n\alpha)(m\beta_1-\varepsilon_1)},$$

$$t_{4,m,n} = (-1)^{m-1}\binom{M}{m}\left[\frac{1}{N} - \frac{b_{4,n}\zeta m\beta_1}{(\zeta+n\alpha)(m\beta_1-\varepsilon_1)} - b_{4,n}\left(\frac{1}{n+1}-\frac{\zeta}{\zeta+n\alpha}\right)\frac{m\zeta}{m\zeta-(n+1)\varepsilon_1}\right],$$

$$t_{5,m,n} = (-1)^{m-1}\binom{M}{m}\left(\frac{1}{n+1}-\frac{\zeta}{\zeta+n\alpha}\right)\frac{b_{4,n}m\zeta}{m\zeta-(n+1)\varepsilon_1},$$

and

$$b_{4,n} = N(-1)^n\binom{N-1}{n}.$$

Proof: See Appendix B. ∎

From Theorem 2 and (12), we can now derive an exact expression for P_{out} as

$$P_{out} = \int_0^\infty\int_0^\infty F_Z\left(\gamma_s(v_{2n^*}+w_{2m^*})+\gamma_s'\right) \times f_{v_{2n^*}}(v_{2n^*})f_{w_{2m^*}}(w_{2m^*})dv_{2n^*}dw_{2m^*}. \tag{25}$$

By using the PDFs $f_{v_{2n^*}}(x)$ and $f_{w_{2m^*}}(x)$ and solving the integral involved in (25), we further express P_{out} as

$$P_{out} = 1 - \sum_{m=1}^{M}\sum_{n_1=0}^{N-1}\sum_{n_2=0}^{N-1}\Big[t_{1,n_1}t_{3,m,n_2}\mathcal{L}\left(\frac{1}{\zeta}\right) + t_{2,n_1}t_{3,m,n_2} \times \mathcal{L}\left(\frac{n_1+1}{\zeta}+\frac{1}{\beta_1}\right) + t_{1,n_1}t_{4,m,n_2}\mathcal{L}\left(\frac{1}{\alpha}+\frac{m}{\varepsilon_1}\right) + t_{1,n_1}t_{5,m,n_2}\mathcal{L}\left(\frac{1}{\alpha}+\frac{n_2+1}{\zeta}\right) + t_{2,n_1}t_{4,m,n_2} \times \mathcal{L}\left(\frac{n_1+1}{\zeta}+\frac{m}{\varepsilon_1}\right) + t_{2,n_1}t_{5,m,n_2}\mathcal{L}\left(\frac{n_1+n_2+2}{\zeta}\right)\Big]. \tag{26}$$

Notably, (26) only consists of elementary functions and thus, can be easily evaluated.

C. Asymptotic P_{out} for Criterion I

We now derive the asymptotic secrecy outage probability for Criterion I, in the presence of high transmit SNRs and MERs. Using the approximation of $e^{-x} \simeq 1-x$ for small value of $|x|$, the asymptotic CDF of Z_1 can be written as,

Theorem 3: The asymptotic CDF of Z_1 can be expressed by

$$F_{Z_1}(z) \simeq \frac{\rho_{M,N}z^{M+N}}{\varepsilon_1^M\beta_1^N} + \left(\frac{z}{\alpha}\right)^{MN}, \tag{27}$$

where

$$\rho_{M,N} = \begin{cases} \sum_{m=0}^{M}\binom{M}{m}\frac{1}{m+1}\left(\frac{z}{\alpha}\right)^{M-m}, & \text{If } N=1, \\ \sum_{m=0}^{M}\frac{(-1)^m N}{m+N}\binom{M}{m}, & \text{If } N\geq 2. \end{cases} \tag{28}$$

Proof: See Appendix C. ∎

From the asymptotic expression for $F_{Z_1}(z)$, we can compute the asymptotic secrecy outage probability associated with Z_1 as

$$\begin{aligned} P_{1,out} &\simeq \int_0^\infty\int_0^\infty F_{Z_1}\left(\gamma_s(v_{2n^*}+w_{2m^*})+\gamma_s'\right)f_{v_{2n^*}}(v_{2n^*}) \times f_{w_{2m^*}}(w_{2m^*})dv_{2n^*}dw_{2m^*} \\ &\simeq \int_0^\infty\int_0^\infty F_{Z_1}\left(\gamma_s(v_{2n^*}+w_{2m^*})\right)f_{v_{2n^*}}(v_{2n^*}) \times f_{w_{2m^*}}(w_{2m^*})dv_{2n^*}dw_{2m^*} \\ &\simeq \frac{\gamma_s^{M+N}(M+N)!\rho_{M,N}}{\lambda_1^M\lambda_2^N}\sum_{k=0}^{M+N}\left(\frac{\beta_2}{\varepsilon_2}\right)^{M-k} + \frac{\gamma_s^{MN}(MN)!}{\lambda_2^{MN}}\left(\frac{\beta_1}{\alpha}\right)^{MN}\sum_{k=0}^{MN}\left(\frac{\varepsilon_2}{\beta_2}\right)^{MN-k}, \end{aligned} \tag{29}$$

where $\lambda_1 = \frac{\varepsilon_1}{\varepsilon_2}$ and $\lambda_2 = \frac{\beta_1}{\beta_2}$ are the MERs for the direct and relay links, respectively. Due to the symmetry between Z_1 and Z_2, we can readily obtain the asymptotic secrecy outage probability associated with Z_2, which has the same form as (29) after replacing M with N and β_1 with ε_1.

From these two asymptotic expressions, we conclude that the secrecy diversity order for Criterion I is equal to $\min(MN, M+N)$. This reveals that the security of the network can be significantly improved by increasing the number of users or the number of relays. In addition, we provide some valuable insights in the following two remarks:

Remark 1: For a single user or single relay communication system, the secrecy diversity order is MN. In particular, the secrecy diversity order is M for a single relay system with $N=1$. This is due to the fact that only multi-user diversity can be exploited. On the other hand, the secrecy diversity order is N for a single user system with $M=1$, since only the multi-relay diversity can be exploited.

Remark 2: For a multi-user and multi-relay communication system with $M\geq 2$ and $N\geq 2$, the secrecy diversity order is equivalent to $M+N$. This indicates that both multi-user diversity and multi-relay diversity can be fully exploited for secure communication.

D. Asymptotic P_{out} for Criterion II

Using the Taylor's series approximation of e^{-x} given by [47]

$$e^{-x} \simeq 1 - x + \frac{x^2}{2} + \cdots + \frac{(-x)^N}{N!}, \tag{30}$$

the asymptotic CDF of Z can be written as,

Theorem 4: The asymptotic CDF of Z can be expressed by

$$F_Z(z) \simeq \left(\frac{\beta_1}{\alpha+\beta_1}\right)\frac{z^N}{\zeta^N}, \tag{31}$$

Proof: See Appendix D. ∎

From this asymptotic CDF, we compute the asymptotic secrecy outage probability for Criterion II as

$$\begin{aligned} P_{out} &\simeq \int_0^\infty \int_0^\infty F_Z\left(\gamma_s(v_{2n^*}+w_{2m^*})+\gamma_s'\right) f_{v_{2n^*}}(v_{2n^*}) \\ &\quad \times f_{w_{2m^*}}(w_{2m^*}) dv_{2n^*} dw_{2m^*} \\ &\simeq \int_0^\infty \int_0^\infty F_Z\left(\gamma_s(v_{2n^*}+w_{2m^*})\right) f_{v_{2n^*}}(v_{2n^*}) \\ &\quad \times f_{w_{2m^*}}(w_{2m^*}) dv_{2n^*} dw_{2m^*} \\ &\simeq \frac{\gamma_s^N N!}{\lambda_2^N}\left(1+\frac{\alpha}{\beta_1}\right)^{N-1}\sum_{n=0}^{N}\left(\frac{\varepsilon_2}{\beta_2}\right)^n. \end{aligned} \tag{32}$$

From the asymptotic secrecy outage probability in (32), we provide some valuable insights in the following two remarks:

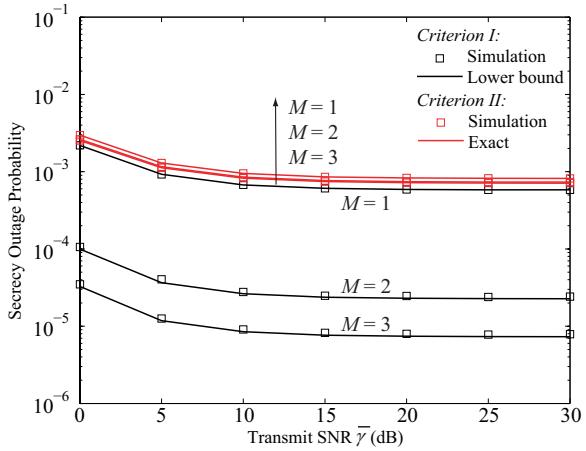
Remark 1: Criterion II achieves the secrecy diversity order of N, which comes from the multi-relay diversity. This indicates that the multi-user diversity is not efficiently exploited in Criterion II. In particular, increasing the number of users does not affect the secrecy diversity order nor the secrecy coding gain of Criterion II. This can be explained by the fact that the asymptotic secrecy outage probability is irrespective of M.

Remark 2: The secrecy performance of the network can be significantly enhanced by increasing the number of relays. This can be explained by the fact that the relay links are the bottleneck of the secure transmission in Criterion II.

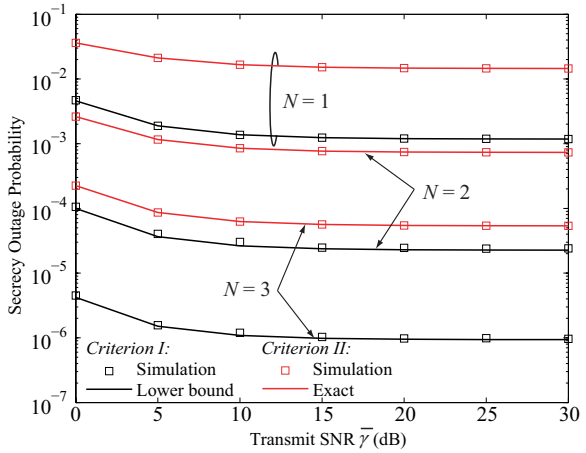
Observing the analytical and asymptotic results presented in (23), (26), (29) and (32), it is easy to find that our analysis is developed based on the statistical information of eavesdropping channels. This indicates that the statistical information of the eavesdropping channels is utilized to evaluate the secrecy outage probabilities for Criterion I and II.

IV. Numerical and Simulation Results

In this section, we provide numerical and simulation results to verify the presented analysis of the proposed selection criteria and to examine the impact of the network parameters on the secrecy outage probability. Throughout this section, we assume that all links in the network experience Rayleigh flat fading [7]. Without loss of generality, the distance between the users and the BS is set to unity, and the relays are placed between in them. Let d denote the distance from the users to relay. Accordingly, the average channel gains of the main links are set to $\alpha = d^{-4}$, $\beta_1 = (1-d)^{-4}$ and $\varepsilon_1 = 1$, where the path-loss model with a loss factor of 4 is used. The secrecy data rate R_s is set to 0.2 bps/Hz and thus, the secrecy SNR threshold γ_s is equal to 1.32.



(a) Impact of various M on the secrecy outage probability for $N = 2$.

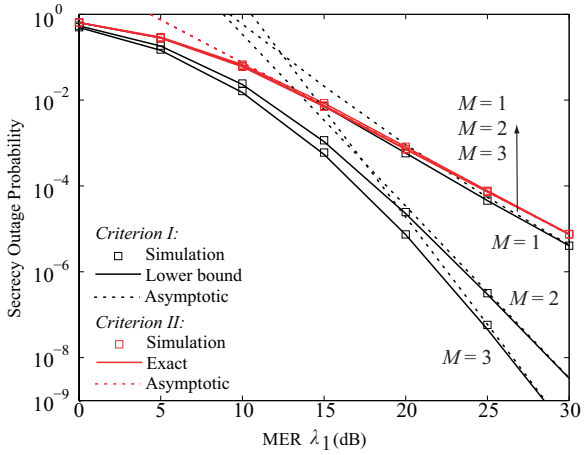


(b) Impact of various N on the secrecy outage probability for $M = 2$.

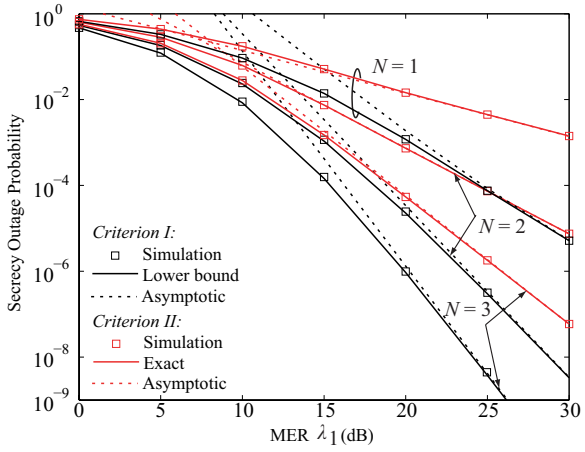
Fig. 2. Secrecy outage probability versus $\bar{\gamma}$ for $d = 0.5$ and $\lambda_1 = \lambda_2 = 20$ dB.

Figs. 2(a) and 2(b) plot the secrecy outage probabilities for Criterion I and II versus the transmit SNR $\bar{\gamma}$ for $d = 0.5$ and $\lambda_1 = \lambda_2 = 20$ dB. As observed from both figures, the analytical result for each criterion perfectly matches the corresponding simulation over the entire SNR regime for various values of M and N. This demonstrates the tightness of the lower bound derived for Criterion I and the correctness of the exact result proposed for Criterion II. Moreover, it is seen that the secrecy outage probability improves with the transmit SNR in the low SNR regime, but this improvement becomes saturated in the medium and high SNR regime. This is due to the fact that the MER is the bottleneck of the secrecy performance of the network. Furthermore, an increase in the number of relays brings a profound improvement in the secrecy outage probabilities for both criteria, which is due to

[7]The system secrecy performance will be affected if other channel scenarios are considered. For example, if we assume that the main channel experiences Nakagami-m fading with $m = 3$ (i.e., less severe fading), the achieved secrecy performance will be improved. Of course, we highlight that our developed analytical framework for secrecy performance evaluation in this paper is still valid even if a different channel scenario is considered.

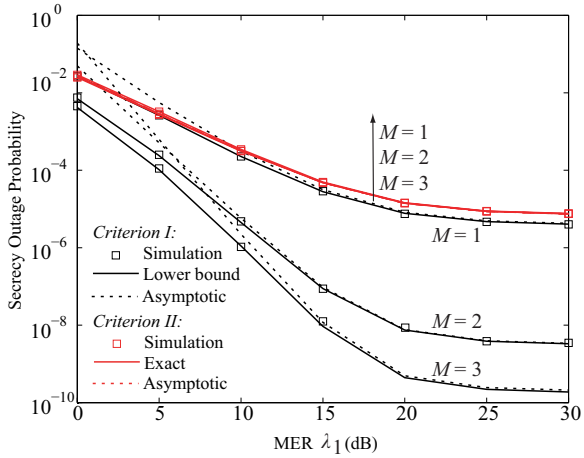


(a) Impact of various M on the secrecy outage probability for $N = 2$.

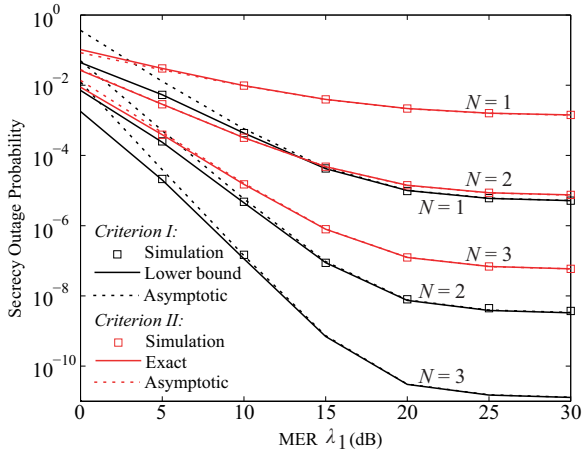


(b) Impact of various N on the secrecy outage probability for $M = 2$.

Fig. 3. Secrecy outage probability versus MER for $d = 0.5$, $\bar{\gamma} = 30$ dB, and $\lambda_1 = \lambda_2$.



(a) Impact of various M on the secrecy outage probability for $N = 2$.



(b) Impact of various N on the secrecy outage probability for $M = 2$.

Fig. 4. Secrecy outage probability versus MER for $d = 0.5$, $\bar{\gamma} = 30$ dB, and $\lambda_2 = 30$ dB.

the fact that the multi-relay diversity indeed helps the secure transmission for both of them. In addition, we can conclude that an increase in the number of users brings a profound improvement in the secrecy outage probability for Criterion I, but a minor improvement for Criterion II. This phenomenon can be explained by the fact that in Criterion II, the first hop of the relay link $u_{m^*n^*}$ is the bottleneck of the received SNR at the destination, $\bar{\gamma}\min(u_{m^*n^*}, v_{1n^*} + w_{1m^*})$. This bottleneck will not be improved profoundly by increasing the number of users, since the best user selected based on direct links is treated as a random user in the first hop of relay link.

Figs. 3(a) and 3(b) plot the secrecy outage probabilities for Criterion I and II versus the MER λ_1 for $d = 0.5$, $\bar{\gamma} = 30$ dB, and $\lambda_1 = \lambda_2$. To obtain the simulation results as low as 10^{-8} with $M = 2$ and $N = 3$ for Criterion I, we perform 10^{11} Monte Carlo runs. From both figures, the asymptotic result for each criterion accurately approximates the corresponding simulation result in the high MER regime for various values of M and N. This validates our asymptotic results derived for Criteria I and II. Moreover, the secrecy diversity order increases with N for both criteria. This implies that increasing the number of relays significantly improves the secrecy outage probability, especially in the medium and high MER regime. In contrast, the secrecy diversity order increases with M for Criterion I, but remains unchanged for Criterion II, as indicated by our asymptotic results. This implies that increasing the number of users leads to a prominent reduction in the secrecy outage probability for Criterion I, but a minor reduction in the secrecy outage probability for Criterion II.

Figs. 4(a) and 4(b) plot the secrecy outage probabilities for Criterion I and II versus the MER λ_1 for $d = 0.5$, $\bar{\gamma} = 30$ dB, and $\lambda_2 = 30$ dB. Again, here the accuracy of our asymptotic results in the high MER regime for various values of M and N. Moreover, we see that the network secrecy performance profoundly improves with λ_1 in the low and medium MER regime. Furthermore, we see that the network exhibits a secrecy performance floor in the high MER regime for both criteria. This is caused because that the relay links are the bottleneck of the secure transmission, when the MER of relay links is fixed.

Fig. 5 compares Criterion I and II with the selection schemes in [23] and [24] by plotting the secrecy outage proba-

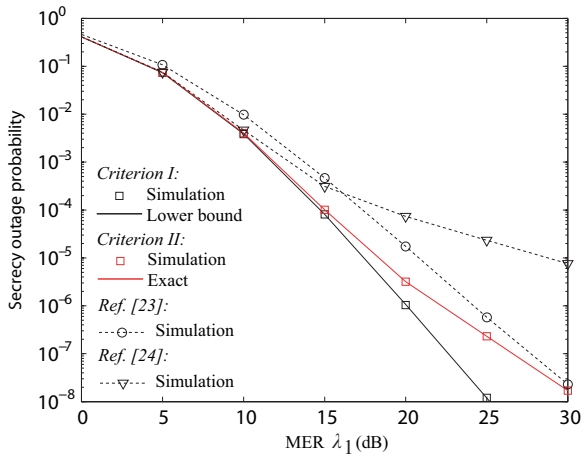


Fig. 5. Performance comparison of selection schemes versus MER for $d = 0.2$, $\bar{\gamma} = 30$ dB, $\lambda_1 = \lambda_2$, and $M = N = 2$.

bility versus the MER λ_1 with $d = 0.2$, $\bar{\gamma} = 30$ dB, $\lambda_1 = \lambda_2$, and $M = N = 2$. Recall that in [23] and [24], user and relay selection is performed by maximizing $\min(u_{mn}, v_{1n})$ and $(w_{1m} + v_{1n})$, respectively. From Fig. 5 we find that the secrecy outage probabilities of Criterion I and II are lower than the secrecy outage probabilities of the schemes in [23] and [24]. This is due to the fact that the system model and the relay protocol considered in [23] and [24] are different from those in our paper, leading to that the selection criteria in [23] and [24] cannot efficiently optimize the system performance. Hence, our proposed selection schemes outperform those in [23] and [24].

From Figs. 2–5 we find that the derived lower bound on the secrecy outage probability in Criterion I perfectly matches the simulation result over the entire regime of transmit SNR and MER. We also find that the matching is valid for various numbers of users and relays. This matching demonstrates the accuracy of the derived lower bound for Criterion I.

V. Conclusions

In this work we addressed the problem of secure communication in the multi-user and multi-relay network, where direct links from the users to the BS and from the users to the eavesdropper affect both information transmission and information wiretap. Taking into account the effect of both direct and relay links, we proposed two user and relay selection criteria that select one best user and relay pair to improve secure communication. For each criterion, we derived new analytical expressions for the secrecy outage probability. We confirmed from the asymptotic expressions that Criterion I achieves the secrecy diversity order of $M + N$ for $M \geq 2$ and $N \geq 2$, while Criterion II achieves the secrecy diversity order of N with a low implementation cost. Simulation results were also provided to validate the proposed analysis and to examine the impact of the network parameters on the secrecy performance.

Appendix A
Proof of Theorem 1

To derive the CDF of Z_1, we first derive the conditional CDF of Z_{1m} with respect to v_1 as

$$\begin{aligned} F_{Z_{1m}}(z|v_1) &= \Pr[\min(u_m, v_1 + w_{1m}) < z] \\ &= 1 - \Pr[u_m \geq z] \cdot \Pr[v_1 + w_{1m} \geq z]. \end{aligned} \quad (33)$$

Due to the fact that $u_m = \max_{1 \leq n \leq N} u_{mn}$, the CDF of u_m is given by [48]

$$F_{u_m}(x) = \left(1 - e^{-\frac{x}{\alpha}}\right)^N. \quad (34)$$

Accordingly, we obtain $\Pr[u_m \geq z]$ as

$$\Pr[u_m \geq z] = 1 - \left(1 - e^{-\frac{z}{\alpha}}\right)^N. \quad (35)$$

To derive $F_{Z_{1m}}(z|v_1)$, we consider $\Pr[v_1 + w_{1m} \geq z]$ for two cases, namely, $z < v_1$ and $z \geq v_1$. When $z < v_1$, $v_1 + w_{1m}$ is always larger than z. As such, we obtain

$$F_{Z_{1m}}(z|v_1) = (1 - e^{-\frac{z}{\alpha}})^N. \quad (36)$$

On the other hand, when $z \geq v_1$, we have

$$\Pr[v_1 + w_{1m} \geq z] = \Pr[w_{1m} \geq z - v_1] \quad (37)$$

$$= e^{-\frac{z - v_1}{\varepsilon_1}}. \quad (38)$$

Accordingly, we obtain

$$\begin{aligned} F_{Z_{1m}}(z|v_1) &= 1 - (1 - e^{-\frac{z}{\alpha}})^N e^{-\frac{z - v_1}{\varepsilon_1}} \\ &= 1 - e^{\frac{v_1}{\varepsilon_1}} \sum_{n=0}^{N} \binom{N}{n} (-1)^{n-1} e^{-(\frac{n}{\alpha} + \frac{1}{\varepsilon_1})z}. \end{aligned} \quad (39)$$

From (36) and (39), the CDF of Z_1 can be written as

$$\begin{aligned} F_{Z_1}(z) &= \int_0^\infty F_{Z_{1m}}^M(z|v_1) f_{v_1}(v_1) dv_1 \\ &= \int_0^z F_{Z_{1m}}^M(z|v_1) f_{v_1}(v_1) dv_1 \\ &\quad + \int_z^\infty F_{Z_{1m}}^M(z|v_1) f_{v_1}(v_1) dv_1. \end{aligned} \quad (40)$$

By using the PDF of v_1, given by $f_{v_1}(x) = \sum_{n=1}^{N} (-1)^{n-1} \binom{N}{n} \frac{n}{\beta_1} e^{-\frac{nx}{\beta_1}}$, and the binomial expansion into (40), we obtain the desired CDF of Z_1 as shown in (19) of Theorem 1, which completes the proof.

Appendix B
Proof of Theorem 2

Since w_{1m^*} is the maximum of M variables $\{w_{1m} | 1 \leq m \leq M\}$, as per the selection criterion characterized by (10), it holds that its distribution is given by [48]

$$f_{w_{1m^*}}(x) = \sum_{m=1}^{M} (-1)^{m-1} \binom{M}{m} \frac{m}{\varepsilon_1} e^{-\frac{mx}{\varepsilon_1}}. \quad (41)$$

We next derive the CDF of $u_{m^*n^*}$ and v_{1n^*}, as per the selection criterion characterized by (11). We first write the CDF of $u_{m^*n^*}$ as

$$\begin{aligned} F_{u_{m^*n^*}}(x) &= \Pr\left[u_{m^*n^*} < x\right] \\ &= \sum_{n=1}^{N} \Pr\left[u_{m^*n} < x, \min(u_{m^*n}, v_{1n}) > \theta_n\right], \end{aligned} \tag{42}$$

where θ_n is defined as

$$\theta_n = \max_{n_1=1,\cdots N, n_1 \neq n} \min(u_{m^*n_1}, v_{1n_1}). \tag{43}$$

Due to the symmetry among N end-to-end paths, $F_{u_{m^*n^*}}(x)$ in (42) is written as

$$\begin{aligned} F_{u_{m^*n^*}}(x) =& N \Pr\left[u_{m^*1} < x, u_{m^*1} > \theta_1, v_{11} > \theta_1\right] \\ =& N \int_0^x \int_{\theta_1}^x \int_{\theta_1}^{\infty} f_{\theta_1}(\theta_1) f_{u_{m^*1}}(u_{m^*1}) \\ & \times f_{v_{11}}(v_{11}) dv_{11} du_{m^*1} d\theta_1. \end{aligned} \tag{44}$$

We first note that u_{m^*1} and v_{11} follow exponential distribution with mean α and β_1, respectively. We also note that the CDF of θ_1 is given by

$$\begin{aligned} F_{\theta_1}(x) &= \Pr\left[\theta_1 < x\right] \\ &= \left(\Pr\left[\min(u_{m^*2}, v_{12}) < x\right]\right)^{N-1} \\ &= \sum_{n=0}^{N-1} (-1)^n \binom{N-1}{n} e^{-\frac{nx}{\zeta}}, \end{aligned} \tag{45}$$

where $\zeta = \alpha\beta_1/(\alpha+\beta_1)$. By applying these results and solving the integral in (44), we obtain $F_{u_{m^*n^*}}(x)$ as

$$\begin{aligned} F_{u_{m^*n^*}}(x) =& 1 - \sum_{n=0}^{N-1} b_{4,n} \left[\frac{\zeta}{\zeta + n\beta_1} e^{-\frac{x}{\alpha}} \right. \\ & \left. + \left(\frac{1}{n+1} - \frac{\zeta}{\zeta + n\beta_1} \right) e^{-\frac{(n+1)x}{\zeta}} \right], \end{aligned} \tag{46}$$

where $b_{4,n} = N(-1)^n \binom{N-1}{n}$.

Similarly, we derive the CDF of v_{1n^*} as

$$\begin{aligned} F_{v_{1n^*}}(x) =& 1 - \sum_{n=0}^{N-1} b_{4,n} \left[\frac{\zeta}{\zeta + n\alpha} e^{-\frac{x}{\beta_1}} \right. \\ & \left. + \left(\frac{1}{n+1} - \frac{\zeta}{\zeta + n\alpha} \right) e^{-\frac{(n+1)x}{\zeta}} \right]. \end{aligned} \tag{47}$$

Using (41), (46), and (47) the CDF of Z is given by

$$\begin{aligned} F_Z(z) &= \Pr\left[\min(u_{m^*n^*}, v_{1n^*} + w_{1m^*}) < z\right] \\ &= 1 - \Pr\left[u_{m^*n^*} \geq z\right] \cdot \Pr\left[v_{1n^*} + w_{1m^*} \geq z\right]. \end{aligned} \tag{48}$$

Note that $\Pr\left[u_{m^*n^*} \geq z\right] = 1 - F_{u_{m^*n^*}}(z)$ can be easily obtained using (46). Therefore, $\Pr\left[v_{1n^*} + w_{1m^*} \geq z\right]$ is calculated as

$$\begin{aligned} \Pr\left[v_{1n^*} + w_{1m^*} \geq z\right] &= 1 - \Pr\left[v_{1n^*} + w_{1m^*} < z\right] \\ &= 1 - \int_0^z F_{v_{1n^*}}(z - w_{1m^*}) f_{w_{1m^*}}(w_{1m^*}) dw_{1m^*}. \end{aligned} \tag{49}$$

Applying (41) and (47) into (49) we are able to obtain $\Pr\left[v_{1n^*} + w_{1m^*} \geq z\right]$. This leads to the analytical CDF of Z, as shown in (24) in Theorem 2. This completes the proof.

Appendix C
Proof of Theorem 3

By applying the approximation of $e^{-x} \simeq 1 - x$ for small value of $|x|$ into (36) and (39), we obtain the asymptotic $F_{Z_{1m}}(z)$ as

$$F_{Z_{1m}}(z) \simeq \left(\frac{z}{\alpha}\right)^N, \tag{50}$$

for $z < v_1$ and

$$F_{Z_{1m}}(z) \simeq \left(\frac{z}{\alpha}\right)^N + \frac{z - v_1}{\varepsilon_1}, \tag{51}$$

for $z \geq v_1$. Then the asymptotic CDF of Z_1 is derived as

$$\begin{aligned} F_{Z_1}(z) &\simeq \int_0^z \left(\left(\frac{z}{\alpha}\right)^N + \frac{z - v_1}{\varepsilon_1} \right)^M f_{v_1}(v_1) dv_1 \\ &\quad + \int_z^{\infty} \left(\frac{z}{\alpha}\right)^{MN} f_{v_1}(v_1) dv_1 \\ &\simeq \int_0^z \left(\left(\frac{z}{\alpha}\right)^N + \frac{z - v_1}{\varepsilon_1} \right)^M f_{v_1}(v_1) dv_1 + \left(\frac{z}{\alpha}\right)^{MN}. \end{aligned} \tag{52}$$

By applying the asymptotic $f_{v_1}(x) \simeq \frac{N x^{N-1}}{\beta_1^N}$ into (52) and then solving the resultant integral, we obtain the asymptotic CDF of Z_1 as shown in (27) of Theorem 3.

Appendix D
Proof of Theorem 4

By using Taylor's series approximation of $e^{-x} \simeq \sum_{n=0}^{N} \frac{(-x)^n}{n!}$ into (46) and (47), we obtain the asymptotic CDFs of $u_{m^*n^*}$ and v_{1n^*} as

$$F_{u_{m^*n^*}}(x) \simeq \left(\frac{x}{\zeta}\right)^N \frac{\beta_1}{\alpha + \beta_1}, \tag{53}$$

and

$$F_{v_{1n^*}}(x) \simeq \left(\frac{x}{\zeta}\right)^N \frac{\alpha}{\alpha + \beta_1}, \tag{54}$$

respectively, with the aid of [47, Eq. (0.154.3), (0.154.4)]. From (48), we then derive the asymptotic CDF of Z as

$$F_Z(z) \simeq 1 - \left(1 - \left(\frac{x}{\zeta}\right)^N \frac{\beta_1}{\alpha + \beta_1}\right) \Pr\left[v_{1n^*} + w_{1m^*} \geq z\right]. \tag{55}$$

We note that the asymptotic $\Pr\left[v_{1n^*} + w_{1m^*} \geq z\right]$ in (55) is computed as

$$\begin{aligned} \Pr\left[v_{1n^*} + w_{1m^*} \geq z\right] &= 1 - \int_0^z F_{v_{1n^*}}(z - w) f_{w_{1m^*}}(w) dw \\ &\simeq 1 - \frac{\alpha}{\alpha + \beta_1} \int_0^z \left(\frac{z - w}{\zeta}\right)^N f_{w_{1m^*}}(w) dw \\ &= 1 - \frac{z^{M+N}}{\zeta^N \varepsilon_1^M} \frac{M\alpha}{\alpha + \beta_1} \sum_{n=0}^{N} (-1)^n \binom{N}{n} \frac{1}{M+n}, \end{aligned} \tag{56}$$

where the asymptotic PDF $f_{w_{1m^*}}(x) \simeq \frac{M}{\varepsilon_1^M} x^{M-1}$ is applied to obtain the last equality. Combining the results in (55) and (56), we obtain the asymptotic CDF of Z as shown in (31) of Theorem 4.

REFERENCES

[1] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sept. 2013.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[3] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[4] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[5] S. Bashar, Z. Ding, and G. Y. Li, "On secrecy of codebook-based transmission beamforming under receiver limited feedback," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1212–1223, Apr. 2011.

[6] C. Liu, N. Yang, G. Geraci, J. Yuan, and R. Malaney, "Secrecy in MIMOME wiretap channels: Beamforming with imperfect CSI," in *Proc. IEEE Int. Commun. Conf. (ICC)*, Sydney, Australia, June 2014, pp. 4711–4716.

[7] D. Ng, E. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[8] G. Geraci, H. Dhillon, J. Andrews, J. Yuan, and I. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, June 2014.

[9] X. Zhang, M. McKay, X. Zhou, and R. Heath, "Artificial-noise-aided secure multi-antenna transmission with limited feedback," *IEEE Trans. Wireless Commun.*, accepted to appear.

[10] Y. Zou, J. Zhu, X. Wang, and V. C. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42–48, Jan. 2015.

[11] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1656–1667, Mar. 2014.

[12] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.

[13] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sept. 2013.

[14] S. Jin, M. R. McKay, C. Zhong, and K.-K. Wong, "Ergodic capacity analysis of amplify-and-forward MIMO dual-hop systems," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2204–2224, May 2010.

[15] C. Zhong, S. Jin, and K.-K. Wong, "Dual-hop systems with noisy relay and interference-limited destination," *IEEE Trans. Commun.*, vol. 58, no. 3, pp. 764–768, Mar. 2010.

[16] M. Dai, H. Y. Kwan, and C. W. Sung, "Linear network coding strategies for the multiple-access relay channel with packet erasures," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 218–227, Jan. 2013.

[17] M. Dai, K. W. Shum, and C. W. Sung, "Data dissemination with side information and feedback," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4708–4720, Sept. 2014.

[18] S. Zhang and S.-C. Liew, "Channel coding and decoding in a relay system operated with physical-layer network coding," *IEEE J. Select. Areas Commun.*, vol. 27, no. 5, pp. 788–796, Jun. 2009.

[19] S. Zhang, S. Liew, and J. Chen, "The capacity of known interference cancellation," *IEEE J. Select. Areas Commun.*, vol. 33, no. 6, pp. 1241–1252, Jun. 2015.

[20] L. Fan, S. Zhang, T. Q. Duong, and G. K. Karagiannidis, "Secure switch-and-stay combining (SSSC) for cognitive relay networks," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 70–82, Jan. 2016.

[21] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Select. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

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

[23] V. N. Q. Bao, N. L. Trung, and M. Debbah, "Relay selection scheme for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[24] N.-E. Wu and H.-J. Li, "Effect of feedback delay on secure cooperative networks with joint relay and jammer selection," *IEEE Wireless Commun. Lett.*, vol. 2, no. 4, pp. 415–418, Aug. 2013.

[25] C. Wang, H.-M. Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 589–605, Feb. 2015.

[26] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3299–3310, Sept. 2014.

[27] X. Lei, L. Fan, R. Q. Hu, D. S. Michalopoulos, and P. Fan, "Secure multiuser communications in multiple decode-and-forward relay networks with direct links," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Austin, TX, Dec 2014, pp. 3180–3185.

[28] Z. Ding, Z. Ma, and P. Fan, "Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 2189–2203, Apr. 2014.

[29] 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.

[30] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[31] G. Chen, Y. Gong, P. Xiao, and J. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Information Forensics and Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[32] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.

[33] J. Zhang, C. Yuen, C. K. Wen, S. Jin, K. K. Wong, and H. Zhu, "Large system secrecy rate analysis for SWIPT MIMO wiretap channels," *IEEE Trans. Information Forensics and Security*, vol. 11, no. 1, pp. 74–85, July 2015.

[34] J. Kim, D. S. Michalopoulos, and R. Schober, "Diversity analysis of multi-user multi-relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 7, pp. 2380–2389, July 2011.

[35] S. Chen, W. Wang, and X. Zhang, "Performance analysis of multiuser diversity in cooperative multi-relay networks under Rayleigh-fading channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 7, pp. 3415–3419, July 2009.

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

[37] M. S. Alam, J. W. Mark, and X. Shen, "Relay selection and resource allocation for multi-user cooperative LTE-A uplink," in *IEEE Inter. Conf. on Commun. (ICC)*, Ottawa, Canada, 2012.

[38] M. A.-T. J. Gomez, F. Blanquez-Casado, and F. Martin-Vega, "Channel inversion CoMP technique in cellular system: A user-selection algorithm," in *the Tenth International Conference on Wireless and Mobile Communications(ICWMC 2014)*, Spain, 2014.

[39] Y. Ge, S. Wen, Y.-H. Ang, and Y.-C. Liang, "Optimal relay selection in IEEE 802.16j multihop relay vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2198–2206, June 2010.

[40] M. A. B. de Melo and D. B. da Costa, "An efficient relay-destination selection scheme for multiuser multirelay downlink cooperative networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 5, pp. 2354–2360, June 2012.

[41] F. R. V. Guimaraes, D. B. da Costa, T. A. Tsiftsis, C. C. Cavalcante, and G. K. Karagiannidis, "Multiuser and multirelay cognitive radio networks under spectrum-sharing constraints," *IEEE Trans. Veh. Technol.*, vol. 63, no. 1, pp. 433–439, Jan. 2014.

[42] L. Sun, T. Zhang, L. Lu, and H. Niu, "On the combination of cooperative diversity and multiuser diversity in multi-source multi-relay wireless networks," *IEEE Sig. Proc. Lett.*, vol. 17, no. 6, pp. 535–538, June 2010.

[43] C. Jeong and I.-M. Kim, "Optimal power allocation for secure multicarrier relay systems," *IEEE Trans. Sig. Proc.*, vol. 59, no. 11, pp. 5428–5442, Nov. 2011.

[44] H. Ding, J. Ge, D. B. da Costa, and Z. Jiang, "Two birds with one stone: Exploiting direct links for multiuser two-way relaying systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, pp. 54–59, Jan. 2012.

[45] M. Ju, H.-K. Song, and I.-M. Kim, "Joint relay-and-antenna selection in multi-antenna relay networks," *IEEE Trans. Commun.*, vol. 58, no. 12, pp. 3417–3422, Dec. 2010.

[46] Z. Zhang, T. Lv, and X. Su, "Combining cooperative diversity and multiuser diversity: A fair scheduling scheme for multi-source multi-

relay networks," *IEEE Commun. Lett.*, vol. 15, no. 12, pp. 1353–1355, Dec. 2011.

[47] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA: Academic, 2007.

[48] M. K. Simon and M. S. Alouini, *Digital Communication over Fading Channels*, 2nd ed. John Wiley, 2005.