Secure Multiuser Communications in Multiple Amplify-and-Forward Relay Networks

Secure Multiuser Communications in Multiple Amplify-and-Forward Relay Networks

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

***Abstract*— This paper proposes relay selection in order to increase the physical layer security in multiuser cooperative relay networks with multiple amplify-and-forward (AF) relays, in the presence of multiple eavesdroppers. To strengthen the network security against eavesdropping attack, we present three criteria to select the best relay and user pair. Specifically, criterion I and II study the received signal-to-noise ratio (SNR) at the receivers, and perform the selection by maximizing the SNR ratio of the user to the eavesdroppers. To this end, criterion I relies on both the main and eavesdropper links, while criterion II relies on the main links only. Criterion III is the standard max-min selection criterion, which maximizes the minimum of the dual-hop channel gains of main links. For the three selection criteria, we examine the system secrecy performance by deriving the analytical expressions for the secrecy outage probability. We also derive the asymptotic analysis for the secrecy outage probability with high main-to-eavesdropper ratio (MER). From the asymptotic analysis, an interesting observation is reached: for each criterion, the system diversity order is equivalent to the number of relays regardless of the number of users and eavesdroppers.**

***Index Terms*— Multiuser communications, multi-relay cooperative networks, multiple eavesdroppers, physical layer security, secrecy outage probability**

I. Introduction

Due to the broadcast nature of wireless transmission, the eavesdroppers in the wireless communications can overhear the message and hence bring out the severe issue of security. To prevent the wiretap, the physical layer security has been considered to implement the information-theoretical secure transmission. In [1], the wiretap model was first introduced by Wyner to study the secrecy rate. After this work, research in this direction picked up momentum by extending and analyzing the secrecy performance over different fading channels [2]–[8]. Specifically, the authors in [2] and [3] have considered that the main and eavesdropper links undergo independent Rayleigh fading, and studied the secrecy capacity. In [4] and [5], the authors have considered the correlated Rayleigh fading between the main and eavesdropper links, and analyzed the impact of channel correlation on the secrecy capacity and outage probability. In [6]–[8], the authors have studied the secrecy performance over Rician and Nakagami-m fading channels.

To enhance the secrecy performance of wireless communications, selection technique has been widely used [9]–[12]. For the communication system with multiple antennas at the transmitter, antenna selection can be used to exploit the fluctuation of fading channels among antennas. Specifically, the authors in [9] have studied the effect of transmit antenna selection on the security of a multiple-input single-output (MISO) system, and developed analytical expression of the secrecy outage probability. The results in [9] have shown that the transmit antenna selection can considerably enhance the system security. In [10] and [11], the authors have proposed transmit antenna selection in a multiple-input multiple-output (MIMO) system to enhance the system security, and presented the analytical and asymptotic expressions of secrecy outage probability. For the multiuser communication system, user selection can be performed to exploit the channel fluctuation among users, in order to enhance the system security. For example, the authors in [12] have investigated the problem of user selection and resource allocation for the secure multiuser downlink MISO orthogonal frequency division multiple access (MISO-OFDMA) system, and devised the system by maximizing the secrecy rate.

Besides selection technique, relaying technique can also improve the secrecy performance of wireless communications [13]–[25]. Some fundamental relaying protocols such as amplify-and-forward (AF) and decode-and-forward (DF) relaying can be applied in the physical layer security systems [26]–[31]. In [26], the authors have studied the secrecy performance of the cooperative DF relaying networks, and analyzed the impact of relay placement on the secrecy outage probability. For cooperative relaying networks with multiple

Manuscript received February 06, 2014; revised June 06, 2014; accepted July 31, 2014. Part of this paper will be presented at the IEEE Global Communications Conference (Globecom), Austin, USA, December 8-12 2014. The associate editor coordinating the review of this paper and approving it for publication was Dr. Jinhong Yuan.

L. Fan is with the Department of Electronic Engineering, Shantou University, Shantou, China, and is also with National Mobile Communications Research Laboratory, Southeast University. (email: lsfan@stu.edu.cn)

X. Lei is with Department of Electrical & Computer Engineering, Utah State University, USA. (email: xflei81@gmail.com)

T. Q. Duong is with Queen's University Belfast, UK (email: trung.q.duong@qub.ac.uk)

M. Elkashlan is with Queen Mary University of London, London, UK (email: maged.elkashlan@qmul.ac.uk)

G. K. Karagiannidis is with the Department of Electrical and Computer Engineering, Khalifa University, PO Box 127788, Abu Dhabi, UAE and with the Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, 54 124, Thessaloniki, Greece (e-mail: geokarag@ieee.org)

This work was supported by the NSF of China (No. 61372129/61002015/61301182), NSF of Guangdong Province, China (No. S2012010010062/S2013040016857), Vietnam's National Foundation for Science and Technology Development (Nafosted, Project No.: 102.04-2013.13), FDYT 2013 (2013LYM-0077), the open research fund of National Mobile Communications Research Laboratory, Southeast University (No. 2013D04), training program of outstanding young teachers in Higher Education Institutions of Guangdong Province (No. Yq2013070), the Academic Innovation Team of Shantou University (No. ITC12002), and the Opening Project of Key Lab of Digital Signal and Image Processing of Guangdong (No. 201203 and 2013GDDSIPL-05).

DF relays, relay selection can be applied to enhance the system security performance [27]–[30]. In [31], the authors have studied the cooperative secure beamforming for AF relaying networks in the presence of multiple eavesdroppers. In [22]–[24], H.-M. Wang et.al proposed *joint* beamforming and jamming schemes to enhance the security of both one-way and two-way relay networks., which led to a breakthrough in the field of physical-layer secure design for cooperative relay systems. Recently, the authors in [30] have studied the secrecy performance of the cooperative relaying networks with multiple AF relays, and analyzed the effect of relay selection on the intercept probability. However, the intercept probability is a special case of secrecy outage probability when the target secrecy date rate is set to zero, and it only depends on the second-hop relaying channels of the main and eavesdropper links. In other words, the first-hop relaying channels do not affect the relay selection criterion in [30], which simplifies the selection criterion and related performance analysis. To the best of our knowledge, no prior work has considered the effect of multiple AF relay selection on the secrecy outage probability of relaying networks.

In this paper, we consider a multiuser cooperative relaying network with M trusted AF relays in the presence of multiple eavesdroppers, and we study the effect of relay selection on the system secrecy outage probability. We present three selection criteria to select one best relay and user pair, in order to enhance the system security. Specifically, criterion I and II study the received signal-to-noise ratio (SNR) at the receivers, and perform the selection by maximizing the SNR ratio of the user to the eavesdroppers. To this end, criterion I relies on both the main and eavesdropper links, while criterion II relies on the main links only. Criterion III is the standard max-min selection criterion, which maximizes the minimum of the dual-hop channel gains of main links. For each criterion, we derive the analytical expression for the secrecy outage probability as well as the asymptotic expression with high main-to-eavesdropper ratio (MER). The asymptotic analysis reveals that the system diversity order is equal to M, regardless of the selection criterion. The diversity order is also independent of the number of users and eavesdroppers. Numerical and simulation results are demonstrated to verify the proposed studies.

Notation: The notation $\mathcal{CN}(0,\sigma^2)$ denotes a circularly symmetric complex Gaussian random variable (RV) with zero mean and variance σ^2. We use $f_X(\cdot)$ and $F_X(\cdot)$ to represent the probability density function (PDF) and cumulative distribution function (CDF) of RV X, respectively. The function $\mathcal{K}_1(x)$ denotes the first-order modified Bessel function of the second kind [32, (8.407)] and $\Gamma(x)$ is the Gamma function [32]. Notation $\Pr[\cdot]$ returns the probability.

II. System Model

Fig. 1 depicts the system model of the two-phase multiuser multi-relay cooperative network with multiple eavesdroppers

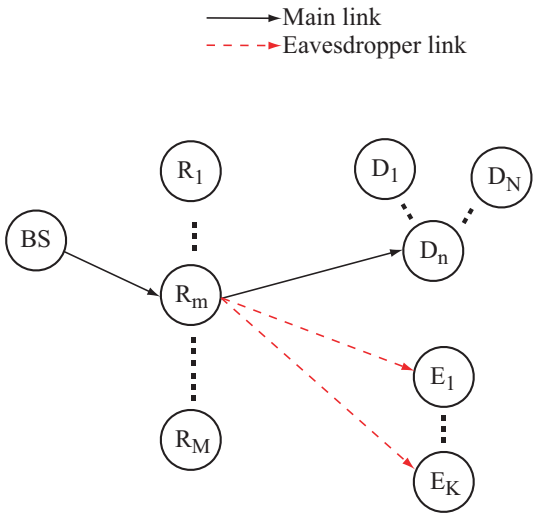

Fig. 1. Two-phase multiuser multi-relay cooperative network with multiple eavesdroppers.

[1]. The system consists of a base station BS, M trusted AF relays, and N desired users as well as K eavesdroppers. We consider severe shadowing environment so that the direct links do not exist. The data transmission from the BS to the users can only travel via the relays, with the possible wiretap from K eavesdroppers. We assume that the eavesdroppers can cooperate with each other by employing maximal ratio combining (MRC) technique to increase the wiretap probability. Although this assumption may involve an increased complexity, particularity in distributed scenarios of eavesdroppers, it presents the extreme case from the secure communication viewpoint [35]. To prevent the wiretap, we select the best relay and user pair (R_{m^*}, D_{n^*}) to enhance the system security performance, while the other relays and users keep silent [2]. All nodes in the network are equipped with a single antenna due to size limitation, and they operate in a half-duplex mode. In this work, we assume the error-free channel estimation, where the estimation method can be found the literature such as [15]–[17], [36], [37].

Suppose that the m-th relay and n-th user have been selected for data transmission, and P_S and P_R denote the transmit power at the BS and relay, respectively. In the first phase, BS sends normalized signal s to R_m, while R_m receives

$$y_m^R = \sqrt{P_S} h_{BS,R_m} s + n_R, \tag{1}$$

where $h_{BS,R_m} \sim \mathcal{CN}(0,\alpha)$ denotes the channel of the BS$\rightarrow\mathrm{R}_m$ link, and $n_R \sim \mathcal{CN}(0,1)$ is the additive white noise

[1]The considered system model is practically applicable for the downlink communication of cellular networks. The utilization of multi-relay and multiuser provides both cooperative and multiuser diversity, which significantly improve the system outage probability and throughput [33], [34]. Moreover, multiple eavesdroppers may arise from realistic scenarios in which the malicious nodes are attempting to attack the legitimate destinations [25], [31].

[2]In this work, we assume that the residual $(M-1)$ relays and $(N-1)$ users keep silent. This assumption has been widely used in the existing literature such as [9]–[11], [15], [17]–[18]. In some communication scenarios, these silent nodes can be active to send artificial noise to enhance the system security, at the cost of more implementation complexity. The utilization of artificial noise is beyond the scope of this paper and will be investigated in our future work.

at the relay. Then relay R_m amplifies the received signal y_m^R by a factor κ,

$$\kappa = \sqrt{\frac{P_R}{P_S|h_{BS,R_m}|^2+1}}, \tag{2}$$

and forwards the resultant signal in the second phase. User D_n and eavesdropper E_k respectively receive

$$y_{m,n}^D = h_{R_m,D_n}\kappa y_m^R + n_D, \tag{3}$$
$$y_{m,k}^E = h_{R_m,E_k}\kappa y_m^R + n_E, \tag{4}$$

where $h_{R_m,D_n} \sim \mathcal{CN}(0,\beta)$ and $h_{R_m,E_k} \sim \mathcal{CN}(0,\varepsilon)$ denote the channels of $\mathrm{R}_m \to \mathrm{D}_n$ and $\mathrm{R}_m \to \mathrm{E}_k$ links, respectively. Notations $n_D \sim \mathcal{CN}(0,1)$ and $n_E \sim \mathcal{CN}(0,1)$ are the additive white noise at the user and eavesdropper, respectively. From (1)–(3), the received SNR at D_n is obtained as

$$\mathsf{SNR}_{m,n}^{\mathsf{D}} = \frac{P_S P_R u_m v_{m,n}}{P_S u_m + P_R v_{m,n} + 1}, \tag{5}$$

where $u_m = |h_{BS,R_m}|^2$ and $v_{m,n} = |h_{R_m,D_n}|^2$ denote the instantaneous channel gains of the $\mathrm{BS}\to\mathrm{R}_m$ and $\mathrm{R}_m\to\mathrm{D}_n$ links, respectively. To increase the wiretap probability, the eavesdroppers combine the received signals $y_{m,k}^E$ with MRC [3] to obtain a scalar symbol as [38]

$$y_n^E = \sum_{k=1}^{K} h_{R_m,E_k}^{\dagger} y_{m,k}^E = \sum_{k=1}^{K} |h_{R_m,E_k}|^2 \kappa y_m^R + h_{R_m,E_k}^{\dagger} n_E, \tag{6}$$

where † denotes the conjugate transpose operation. From the above equation, we can obtain the received SNR of K eavesdroppers with MRC as [38]

$$\mathsf{SNR}_m^{\mathsf{E}} = \frac{P_S P_R u_m w_m}{P_S u_m + P_R w_m + 1}, \tag{7}$$

where $w_m = \sum_{k=1}^{K} |h_{R_m,E_k}|^2$ denotes the sum channel gain of the K eavesdropper links.

For the considered system with target secrecy data rate R_s, the secrecy outage event occurs when the instantaneous capacity difference between the main and eavesdropper links falls below R_s. Accordingly, the secrecy outage probability with the m-th relay and n-th user is given by

$$P_{out,m,n} = \Pr\left[\frac{1}{2}\log_2(1+\mathsf{SNR}_{m,n}^{\mathsf{D}}) - \frac{1}{2}\log_2(1+\mathsf{SNR}_m^{\mathsf{E}}) < R_s\right] \tag{8}$$
$$= \Pr\left(\frac{1+\mathsf{SNR}_{m,n}^{\mathsf{D}}}{1+\mathsf{SNR}_m^{\mathsf{E}}} < \gamma_{th}\right), \tag{9}$$

where $\gamma_{th} = 2^{2R_s}$ denotes the secrecy SNR threshold.

[3]In this paper, we consider a worse-case scenario where malicious nodes can cooperate via MRC to form a group of colluding eavesdroppers [35]. The MRC technique can be implemented by gathering all the received signals and required channel information from eavesdroppers through a dedicated feedback channel.

III. Relay and user selection

For the considered system, we select the best relay and user pair (R_{m^*}, D_{n^*}) to minimize the secrecy outage probability,

$$(m^*,n^*) = \arg\min_{m=1,\cdots,M}\min_{n=1,\cdots,N} P_{out,m,n} \tag{10}$$
$$= \arg\min_{m=1,\cdots,M}\min_{n=1,\cdots,N} \Pr\left(\frac{1+\mathsf{SNR}_{m,n}^{\mathsf{D}}}{1+\mathsf{SNR}_m^{\mathsf{E}}} < \gamma_{th}\right). \tag{11}$$

It holds that

$$\frac{1+\mathsf{SNR}_{m,n}^{\mathsf{D}}}{1+\mathsf{SNR}_m^{\mathsf{E}}} \simeq \frac{\mathsf{SNR}_{m,n}^{\mathsf{D}}}{\mathsf{SNR}_m^{\mathsf{E}}} \tag{12}$$
$$= \frac{P_S P_R u_m v_{m,n}/(P_S u_m + P_R v_{m,n} + 1)}{P_S P_R u_m w_m/(P_S u_m + P_R w_m + 1)} \tag{13}$$
$$\simeq \frac{P_S P_R u_m v_{m,n}/(P_S u_m + P_R v_{m,n})}{P_S P_R u_m w_m/(P_S u_m + P_R w_m)} \tag{14}$$

where in (12) we apply the approximation of $(1+x)/(1+y) \simeq x/y$. This approximation has been used in [4], [28], [29], and the effect of approximation error can be neglected in high SNR region. In addition, we apply the approximation of $xy/(1+x+y) \simeq xy/(x+y)$ in (14), where the effect of approximation error can be also ignored for large transmit power [39]. Let $\eta = \frac{P_R}{P_S}$ denote the transmit power ratio of the relay to the BS. Then we can summarize

$$\frac{1+\mathsf{SNR}_{m,n}^{\mathsf{D}}}{1+\mathsf{SNR}_m^{\mathsf{E}}} \simeq \frac{(u_m+\eta w_m)v_{m,n}}{(u_m+\eta v_{m,n})w_m}, \tag{15}$$

Accordingly, we can approximate $P_{out,m,n}$ using (15) as

$$P_{out,m,n} \simeq \Pr\left[\frac{(u_m+\eta w_m)v_{m,n}}{(u_m+\eta v_{m,n})w_m} < \gamma_{th}\right]. \tag{16}$$

Note that $\frac{(u_m+\eta w_m)v_{m,n}}{(u_m+\eta v_{m,n})w_m} < \gamma_{th}$ is equivalent to $(u_m+\eta w_m)v_{m,n} < (u_m+\eta v_{m,n})\gamma_{th} w_m$, which can be simplified as $u_m v_{m,n} < (\gamma_{th}u_m + (\gamma_{th}-1)\eta v_{m,n})w_m$. Hence, we can further write $P_{out,m,n}$ as

$$P_{out,m,n} \simeq \Pr\left[u_m v_{m,n} < (\gamma_{th}u_m + (\gamma_{th}-1)\eta v_{m,n})w_m\right] \tag{17}$$
$$= \Pr\left[\frac{u_m v_{m,n}}{\gamma_{th}u_m + (\gamma_{th}-1)\eta v_{m,n}} < w_m\right]. \tag{18}$$

We then devise a relay and user pair selection criterion as

$$(m^*,n^*) = \arg\max_{m=1,\cdots,M}\max_{n=1,\cdots,N} \left(\frac{u_m v_{m,n}/(\gamma_{th}u_m + (\gamma_{th}-1)\eta v_{m,n})}{w_m}\right). \tag{19}$$

From (16)–(18), one can easily conclude that the criterion in (19) is equivalent to maximizing the received SNR ratio of the user to the eavesdroppers based on both the main and eavesdropper links, and hence it achieves a near-optimal secrecy outage performance with large transmit power.

Note that the near-optimal selection in (19) mandates the knowledge of the instantaneous channel parameters of both the main and eavesdropper links. In some communication

scenarios, it may be however impractical or cost-consuming to acquire the instantaneous channel parameters of the eavesdropper links. In this case, the relay and user selection can only depend on the instantaneous channel parameters of main links. By applying

$$u_m v_{m,n}/(\gamma_{th}u_m + (\gamma_{th}-1)\eta v_{m,n}) \leq \min(\frac{u_m}{(\gamma_{th}-1)\eta}, \frac{v_{m,n}}{\gamma_{th}}) \tag{20}$$

into (19), we can devise a sub-optimal relay and user selection criterion as

$$(m^*, n^*) = \arg \max_{m=1,\cdots,M} \max_{n=1,\cdots,N} \min\left(\frac{u_m}{(\gamma_{th}-1)\eta}, \frac{v_{m,n}}{\gamma_{th}}\right), \tag{21}$$

which maximizes the received SNR ratio of the user to the eavesdroppers based only on the main links.

In addition, according to the standard max-min criterion, we select the relay and user pair by maximizing the minimum of the dual-hop channel gains of main links as

$$(m^*, n^*) = \arg \max_{m=1,\cdots,M} \max_{n=1,\cdots,N} \min(u_m, v_{m,n}). \tag{22}$$

For convenience of notation, we will refer to the selection criterion in (19), (21) and (22) as criterion I, II, and III, respectively. For each of the three criteria, we will first derive analytical expressions for the secrecy outage probability, we then provide asymptotic expressions with high MER, from which we obtain the system diversity order.

IV. Secrecy outage Probability

In this section, we will derive the analytical expression of secrecy outage probability for criterion I, II and III. From (18), the system secrecy outage probability with selected R_{m^*} and D_{n^*} for high transmit power is given by

$$P_{out,m^*,n^*} \simeq \Pr(Z_{m^*,n^*} < w_{m^*}), \tag{23}$$

where the approximation sign comes from the assumption of large transmit power which was previously used in eq. (15), and $Z_{m,n}$ is

$$Z_{m,n} = \frac{u_m v_{m,n}}{\gamma_{th}u_m + (\gamma_{th}-1)\eta v_{m,n}}. \tag{24}$$

A. Criterion I

According to the selection criterion in (19), we find that the statistic $Z_{m^*,n^*}/w_{m^*}$ is the maximum of the $M \times N$ variables $\{Z_{m,n}/w_m\}$. However, these $M \times N$ variables are not independent of each other, since N users share the common BS-relay link for a given relay. This non-independence causes some difficulty to the performance analysis. To solve this troublesome, we turn our attention to view $Z_{m^*,n^*}/w_{m^*}$ as the maximum of M variables $\{Z_{m,n_m^*}/w_m\}$, where $\mathrm{D}_{n_m^*}$ is the best user conditioned on a given relay R_m. These M variables are independent of each other, since each relay has independent links with other nodes in the network. Hence, we need first to study the secrecy outage probability for a given relay R_m with only user selection.

Note that $Z_{m,n}$ in (24) increases with $v_{m,n}$, the best user $\mathrm{D}_{n_m^*}$ conditioned on a given relay R_m should be selected to maximize $v_{m,n}$,

$$n_m^* = \arg \max_{n=1,\cdots,N} v_{m,n}. \tag{25}$$

The probability density function (PDF) of v_{m,n_m^*} is [40, (9E.2)]

$$f_{v_{m,n_m^*}}(v) = \sum_{n=1}^{N} (-1)^{n-1} \binom{N}{n} \frac{n}{\beta} e^{-\frac{nv}{\beta}}. \tag{26}$$

Using (26), the cumulative density function (CDF) of Z_{m,n_m^*} can be written as

$$F_{Z_{m,n_m^*}}(z) = \Pr\left(\frac{u_m v_{m,n_m^*}}{\gamma_{th}u_m + (\gamma_{th}-1)\eta v_{m,n_m^*}} < z\right) \tag{27}$$

$$= \Pr\left[u_m(v_{m,n_m^*} - \gamma_{th}z) < (\gamma_{th}-1)\eta v_{m,n_m^*} z\right]. \tag{28}$$

By considering two cases of $v_{m,n_m^*} \leq \gamma_{th}z$ and $v_{m,n_m^*} > \gamma_{th}z$ respectively, we can further write $F_{Z_{m,n_m^*}}(z)$ as

$$F_{Z_{m,n_m^*}}(z) = \Pr(v_{m,n_m^*} \leq \gamma_{th}z) + \Pr\left(v_{m,n_m^*} > \gamma_{th}z, u_m < \frac{(\gamma_{th}-1)\eta v_{m,n_m^*} z}{v_{m,n_m^*} - \gamma_{th}z}\right). \tag{29}$$

By applying the PDF of v_{m,n_m^*} in eq. (26) and $f_{u_m}(u) = \frac{1}{\alpha}e^{-\frac{u}{\alpha}}$ into the above equation, and then solving the required integral, we obtain the CDF of Z_{m,n_m^*} as

$$F_{Z_{m,n_m^*}}(z) = 1 - \sum_{n=1}^{N} (-1)^{n-1} \binom{N}{n} b_n e^{-(\frac{n\gamma_{th}}{\beta} + \frac{\eta(\gamma_{th}-1)}{\alpha})z} \times z\mathcal{K}_1(b_n z), \tag{30}$$

where we apply [32, (3.324)] and

$$b_n = \sqrt{\frac{4n\eta\gamma_{th}(\gamma_{th}-1)}{\alpha\beta}}. \tag{31}$$

From eqs. (23) and (30), we derive the closed-form expression of the secrecy outage probability with the m-th relay for large transmit power as

$$P_{out,m,n_m^*} \simeq \Pr(Z_{m,n_m^*} < w_m) \tag{32}$$

$$= \int_0^\infty f_{w_m}(w) F_{Z_{m,n_m^*}}(w) dw, \tag{33}$$

where the approximation sign in eq. (32) comes from the assumption of large transmit power which was previously used in eq. (15). Note that $f_{w_m}(w) = \frac{w^{K-1}}{\Gamma(K)\varepsilon^K} e^{-\frac{w}{\varepsilon}}$ is the PDF of w_m [40, (9.5)], we can obtain the secrecy outage probability with the m-th relay by applying [32, (6.621.3)] as

$$P_{out,m,n_m^*} \simeq 1 - \sum_{n=1}^{N} (-1)^{n-1} \binom{N}{n} \frac{2\sqrt{\pi}b_n^2 \Gamma(K+2)}{\varepsilon^K (b_n + c_n)^{K+2} \Gamma(K+\frac{3}{2})} \times {}_2F_1(K+2, \frac{3}{2}, K+\frac{3}{2}; \frac{c_n - b_n}{c_n + b_n}), \tag{34}$$

where $c_n = \frac{1}{\varepsilon} + \frac{n\gamma_{th}}{\beta} + \frac{\eta(\gamma_{th}-1)}{\alpha}$ and ${}_2F_1(\cdot)$ denotes the Gauss hypergeometric function [32, (9.100)] [4].

As mentioned at the beginning of Sec. IV. A, the statistic $Z_{m^*,n^*}/w_{m^*}$ is the maximum of M independent variables of $\{Z_{m,n_m^*}/w_m\}$, and hence we can obtain the secrecy outage probability for criterion I with high transmit power as

$$P_{out,m^*,n^*} \simeq \left[1 - \sum_{n=1}^{N} \binom{N}{n} \frac{2(-1)^{n-1}\sqrt{\pi} b_n^2 \Gamma(K+2)}{\varepsilon^K (b_n + c_n)^{K+2} \Gamma(K+\frac{3}{2})} \times {}_2F_1(K+2, \frac{3}{2}, K+\frac{3}{2}; \frac{c_n - b_n}{c_n + b_n})\right]^M. \quad (35)$$

B. Criterion II and III

In this subsection, we derive the secrecy outage probability for criterion II and III in a unified manner. Note that criterion II and III in (21) and (22) can be unified as

$$(m^*, n^*) = \arg \max_{m=1,\cdots,M} \max_{n=1,\cdots,N} \min(u_m, \rho v_{m,n}), \quad (36)$$

where $\rho = \rho_{II}$ and $\rho = \rho_{III}$ correspond to criterion II and III, respectively, with $\rho_{II} = \frac{(\gamma_{th}-1)\eta}{\gamma_{th}}$ and $\rho_{III} = 1$. According to (36), we obtain the CDFs of u_{m^*} and v_{m^*,n^*} in the following theorem.

Theorem 1: The CDFs of u_{m^*} and v_{m^*,n^*} are given by

$$\begin{cases} F_{u_{m^*}}(x) = 1 - \sum_{n=1}^{N} \widetilde{\sum_i} \left(q_{1i} e^{-q_{2i}x} + q_{3i} e^{-\frac{x}{\alpha}}\right) \\ F_{v_{m^*,n^*}}(x) = 1 - \sum_{n=1}^{N} \widetilde{\sum_i} \left(\frac{q_{4i}}{q_{2i}\rho} e^{-q_{2i}\rho x} + \frac{q_{5i}\beta}{n} e^{-\frac{n}{\beta}x}\right) \end{cases} \quad (37)$$

where

$$\begin{cases} q_{1i} = M(-1)^{n-1}\binom{N}{n} \frac{d_i e_i}{\alpha(e_i + \frac{n}{\rho\beta})(e_i + \frac{1}{\alpha} + \frac{n}{\rho\beta})} \\ q_{2i} = e_i + \frac{1}{\alpha} + \frac{n}{\rho\beta} \\ q_{3i} = M(-1)^{n-1}\binom{N}{n} \frac{n d_i}{n + e_i\rho\beta} \\ q_{4i} = M(-1)^{n-1}\binom{N}{n} \frac{n d_i e_i}{\beta(e_i + \frac{1}{\alpha})} \\ q_{5i} = M(-1)^{n-1}\binom{N}{n} \frac{n d_i}{\beta(1 + \alpha e_i)} \end{cases}, \quad (38)$$

with

$$\begin{cases} \widetilde{\sum_i} = \sum_{i_1=0}^{M-1} \sum_{i_2=0}^{i_1} \sum_{i_3=0}^{i_2} \cdots \sum_{i_N=0}^{i_{N-1}} \\ d_i = (-1)^{i_1+i_2+\cdots+i_N} \binom{M-1}{i_1}\binom{i_1}{i_2}\cdots\binom{i_{N-1}}{i_N} \\ \quad \times (\binom{N}{1})^{i_1-i_2} (\binom{N}{2})^{i_2-i_3} \cdots (\binom{N}{N-1})^{i_{N-1}-i_N} \\ e_i = \frac{i_1}{\alpha} + \frac{i_1 + \cdots + i_N}{\rho\beta} \end{cases}. \quad (39)$$

Proof: *See Appendix I.*

From Theorem 1, we now extend to analyze the CDF of $Z_{m^*,n^*} = \frac{u_{m^*} v_{m^*,n^*}}{\gamma_{th} u_{m^*} + (\gamma_{th}-1)\eta v_{m^*,n^*}}$ as

$$F_{Z_{m^*,n^*}}(z) = \Pr\left(\frac{u_{m^*} v_{m^*,n^*}}{\gamma_{th} u_{m^*} + (\gamma_{th}-1)\eta v_{m^*,n^*}} < z\right) \quad (40)$$

$$= \Pr\left[u_{m^*}(v_{m^*,n^*} - \gamma_{th} z) < (\gamma_{th}-1)\eta v_{m^*,n^*} z\right] \quad (41)$$

$$= \Pr(v_{m^*,n^*} \le \gamma_{th} z) + \Pr\left[v_{m^*,n^*} > \gamma_{th} z, u < \frac{(\gamma_{th}-1)\eta v_{m^*,n^*} z}{v_{m^*,n^*} - \gamma_{th} z}\right]. \quad (42)$$

Applying the results of Theorem 1 into the above equation yields the CDF of Z_{m^*,n^*} as

$$F_{Z_{m^*,n^*}}(z) = 1 - \sum_{n_1}^{N} \sum_{n_2=1}^{N} \widetilde{\sum_i} \widetilde{\sum_j} \Bigg[\frac{q_{5i} q_{1j} \beta \psi_1}{n_1} z \times e^{-[\frac{\eta_1\gamma_{th}}{\beta} + q_{2j}\eta(\gamma_{th}-1)]z} \mathcal{K}_1(\psi_1 z) + \frac{q_{5i} q_{3j} \beta \psi_2}{n_1} z e^{-[\frac{n_1\gamma_{th}}{\beta} + \frac{(\gamma_{th}-1)\eta}{\alpha}]z} \mathcal{K}_1(\psi_2 z) + \frac{q_{4i} q_{1j} \psi_3}{\rho q_{2i}} z e^{-[q_{2i}\rho\gamma_{th} + q_{2j}\eta(\gamma_{th}-1)]z} \mathcal{K}_1(\psi_3 z) + \frac{q_{4i} q_{3j} \psi_4}{\rho q_{2i}} z e^{-[\rho q_{2i}\gamma_{th} + \frac{(\gamma_{th}-1)\eta}{\alpha}]z} \mathcal{K}_1(\psi_4 z)\Bigg], \quad (43)$$

with

$$\begin{cases} \psi_1 = \sqrt{\frac{4 n_1 q_{2j} \eta \gamma_{th}(\gamma_{th}-1)}{\beta}} \\ \psi_2 = \sqrt{\frac{4 n_1 \eta \gamma_{th}(\gamma_{th}-1)}{\alpha\beta}} \\ \psi_3 = \sqrt{4 q_{2i} q_{2j} \rho \eta \gamma_{th}(\gamma_{th}-1)} \\ \psi_4 = \sqrt{\frac{4\rho q_{2i} \eta \gamma_{th}(\gamma_{th}-1)}{\alpha}} \end{cases}. \quad (44)$$

The system secrecy outage probability is then derived as

$$P_{out,m^*,n^*} \simeq \Pr(Z_{m^*,n^*} < w_{m^*}) \quad (45)$$

$$= \int_0^\infty f_{w_{m^*}}(w) F_{Z_{m^*,n^*}}(w) dw. \quad (46)$$

Note that for criterion II and III, the eavesdropper links are not involved in the relay and user selection. Hence we obtain

[4]Note that the Gauss hypergeometric function can be computed in Matlab or Mathematica. This function can be also efficiently calculated by the representation of some elementary functions. For example, ${}_2F_1(K+2, \frac{3}{2}, K+\frac{3}{2}; z)$ with $K=1$ can be calculated as $\frac{3[\sqrt{z}(z+1) - (z-1)^2 \tanh^{-1}(\sqrt{z})]}{8(z-1)^2 z^{\frac{3}{2}}}$ [32], [41].

that $f_{w_{m^*}}(w) = \frac{w^{K-1}}{\Gamma(K)\varepsilon^K} e^{-\frac{w}{\varepsilon}}$ [40, (9.5)]. Applying $f_{w_{m^*}}(w)$ into (46) yields

$$\begin{aligned} P_{out,m^*,n^*} \simeq 1 - \sum_{n_1=1}^{N} \sum_{n_2=1}^{N} \widetilde{\sum_i}\widetilde{\sum_j} \frac{2\sqrt{\pi}\Gamma(K+2)}{\Gamma(K+\frac{3}{2})\varepsilon^K} \\ \times \Bigg[\frac{q_{5i} q_{1j} \beta \psi_1^2}{n_1(\psi_1+\tau_1)^{K+2}} \ {}_2F_1(K+2, \frac{3}{2}, K+\frac{3}{2}; \frac{\tau_1-\psi_1}{\tau_1+\psi_1}) \\ + \frac{q_{5i} q_{3j} \beta \psi_2^2}{n_1(\psi_2+\tau_2)^{K+2}} \ {}_2F_1(K+2, \frac{3}{2}, K+\frac{3}{2}; \frac{\tau_2-\psi_2}{\tau_2+\psi_2}) \\ + \frac{q_{4i} q_{1j} \psi_3^2}{\rho q_{2i}(\psi_3+\tau_3)^{K+2}} \ {}_2F_1(K+2, \frac{3}{2}, K+\frac{3}{2}; \frac{\tau_3-\psi_3}{\tau_3+\psi_3}) \\ + \frac{q_{4i} q_{3j} \psi_4^2}{\rho q_{2i}(\psi_4+\tau_4)^{K+2}} \ {}_2F_1(K+2, \frac{3}{2}, K+\frac{3}{2}; \frac{\tau_4-\psi_4}{\tau_4+\psi_4}) \Bigg], \end{aligned} \tag{47}$$

where

$$\begin{cases} \tau_1 = \dfrac{1}{\varepsilon} + \dfrac{n_1\gamma_{th}}{\beta} + q_{2j}\eta(\gamma_{th}-1) \\ \tau_2 = \dfrac{1}{\varepsilon} + \dfrac{n_1\gamma_{th}}{\beta} + \dfrac{(\gamma_{th}-1)\eta}{\alpha} \\ \tau_3 = \dfrac{1}{\varepsilon} + q_{2i}\rho\gamma_{th} + q_{2j}\eta(\gamma_{th}-1) \\ \tau_4 = \dfrac{1}{\varepsilon} + q_{2i}\rho\gamma_{th} + \dfrac{(\gamma_{th}-1)\eta}{\alpha} \end{cases}. \tag{48}$$

By setting $\rho = \rho_{II}$ and $\rho = \rho_{III}$ into (47), we can obtain the analytical expression of secrecy outage probability for criterion II and III, respectively.

V. Asymptotic Analysis

In this section, we analyze the asymptotic secrecy outage probability for the three selection criteria with high MER. From the asymptotic expressions, we further reveal the system diversity order for the three criteria.

A. Criterion I

To analyze the diversity gain of criterion I, we firstly consider the lower and upper bounds of Z_{m,n_m^*} as

$$\begin{aligned} 0.5 \min\left(\frac{u_m}{(\gamma_{th}-1)\eta}, \frac{v_{m,n_m^*}}{\gamma_{th}}\right) \le Z_{m,n_m^*} \\ \le \min\left(\frac{u_m}{(\gamma_{th}-1)\eta}, \frac{v_{m,n_m^*}}{\gamma_{th}}\right). \end{aligned} \tag{49}$$

The above bounds can be written in a unified form as

$$Z^b_{m,n_m^*} = \delta \min\left(\frac{u_m}{(\gamma_{th}-1)\eta}, \frac{v_{m,n_m^*}}{\gamma_{th}}\right), \tag{50}$$

where $\delta = 0.5$ and $\delta = 1$ correspond to the lower and upper bounds of Z_{m,n_m^*}, respectively. From Z^b_{m,n_m^*}, we can derive the asymptotic P_{out,m,n_m^*} with high MER in the following theorem,

Theorem 2: The asymptotic expression of P_{out,m,n_m^*} in the high MER region is given by

$$P^{asy}_{out,m,n_m^*} = \begin{cases} \dfrac{K}{\lambda}\left[\dfrac{(\gamma_{th}-1)\eta\beta}{\delta\alpha} + \dfrac{\gamma_{th}}{\delta}\right], & \text{If } N = 1 \\ \dfrac{K}{\lambda}\dfrac{(\gamma_{th}-1)\eta\beta}{\delta\alpha}, & \text{If } N \ge 2 \end{cases}, \tag{51}$$

where $\lambda = \frac{\beta}{\varepsilon}$ denotes the MER [30], defined as the ratio of average channel gain from the relay to the users to that from the relay to the eavesdroppers.

Proof: *See Appendix II.*

It follows from Theorem 2 that we can obtain the asymptotic secrecy outage probability with high MER for criterion I as

$$P^{asy}_{out,m^*,n^*} = \begin{cases} \dfrac{K^M}{\lambda^M}\left[\dfrac{(\gamma_{th}-1)\eta\beta}{\delta\alpha} + \dfrac{\gamma_{th}}{\delta}\right]^M, & \text{If } N = 1 \\ \dfrac{K^M}{\lambda^M}\left(\dfrac{(\gamma_{th}-1)\eta\beta}{\delta\alpha}\right)^M, & \text{If } N \ge 2 \end{cases}, \tag{52}$$

where $\delta = 0.5$ and $\delta = 1$ correspond to asymptotic expressions derived from the upper and lower bounds of the secrecy outage probability, respectively. Inspired by the asymptotic expression from either lower or upper bound of the secrecy outage probability, we find that the diversity order for criterion I is equal to M. Hence, we can conclude from the squeeze theorem that the diversity order for criterion I is equal to M, regardless of the number of users and eavesdroppers. Moreover, the asymptotic secrecy outage probability is irrespective of the number of users when $N \ge 2$, indicating that no gain is achieved from increasing the number of users with high MER. This is due to the fact that when $N \ge 2$, the first hop from the BS to the relays becomes the bottleneck for the dual-hop data transmission.

B. Criterion II and III

To derive the asymptotic secrecy outage probability for criterion II and III, we first give the asymptotic CDFs of u_{m^*} and v_{m^*,n^*} in the following theorem.

Theorem 3: The asymptotic CDFs of u_{m^*} and v_{m^*,n^*} are

$$F_{u_{m^*}}(x) \simeq \begin{cases} (1+\dfrac{\rho\beta}{\alpha})^{M-1}\dfrac{\rho\beta}{\alpha}\dfrac{x^M}{(\rho\beta)^M}, & \text{If } N = 1 \\ \dfrac{x^M}{\alpha^M}, & \text{If } N \ge 2 \end{cases}, \tag{53}$$

$$F_{v_{m^*,n^*}}(x) \simeq \begin{cases} (1+\dfrac{\rho\beta}{\alpha})^{M-1}\dfrac{x^M}{\beta^M}, & \text{If } N = 1 \\ \dfrac{MN}{M+N-1}\dfrac{\rho^{M-1}x^{M+N-1}}{\alpha^{M-1}\beta^N}, & \text{If } N \ge 2 \end{cases}. \tag{54}$$

Proof: *See Appendix III.*

We then derive the CDFs of $Z^b_{m^*,n^*}$ from (50) as

$$F_{Z^b_{m^*,n^*}}(z) = \Pr\left[\delta \min\left(\frac{u_{m^*}}{(\gamma_{th}-1)\eta}, \frac{v_{m^*,n^*}}{\gamma_{th}}\right) < z\right] \quad (55)$$

$$= 1 - \Pr\left(u_{m^*} \geq \frac{(\gamma_{th}-1)\eta z}{\delta}\right) \times \Pr\left(v_{m^*,n^*} \geq \frac{\gamma_{th} z}{\delta}\right). \quad (56)$$

Applying the results of Theorem 3 into the above equation yields the asymptotic CDF of $Z^b_{m^*,n^*}$ as

$$F_{Z^b_{m^*,n^*}}(z) \simeq \begin{cases} \mu_1 (\frac{z}{\delta\beta})^M, & \text{If } N = 1 \\ \mu_{21}(\frac{z}{\delta\beta})^M + \mu_{22}(\frac{z}{\delta\beta})^{M+N-1}, & \text{If } N \geq 2 \end{cases}, \quad (57)$$

with

$$\begin{cases} \mu_1 = (1+\frac{\rho\beta}{\alpha})^{M-1}\left[\frac{\rho\beta}{\alpha}\left(\frac{(\gamma_{th}-1)\eta}{\rho}\right)^M + \gamma_{th}^M\right] \\ \mu_{21} = \frac{\beta^M}{\alpha^M}\left((\gamma_{th}-1)\eta\right)^M \\ \mu_{22} = \frac{MN}{M+N-1}(\frac{\rho\beta}{\alpha})^{M-1}\gamma_{th}^{M+N-1} \end{cases}. \quad (58)$$

By applying the asymptotic CDF of $Z^b_{m^*,n^*}$ into (46) and then solving the resultant equation, we can obtain the asymptotic secrecy outage probability with high MER for criterion II and III as,

$$P^{asy}_{out,m^*,n^*} \simeq \begin{cases} \frac{\mu_1\Gamma(M+K)}{\Gamma(K)}\frac{1}{(\delta\lambda)^M}, & \text{If } N = 1 \\ \frac{\mu_{21}\Gamma(M+K)}{\Gamma(K)}\frac{1}{(\delta\lambda)^M} + \frac{\mu_{22}\Gamma(M+N+K-1)}{\Gamma(K)} \times \frac{1}{(\delta\lambda)^{M+N-1}}, & \text{If } N \geq 2 \end{cases} \quad (59)$$

where $\rho = \rho_{II}$ and $\rho = \rho_{III}$ correspond to the asymptotic secrecy outage probabilities of criterion II and III, respectively, and $\delta = 0.5$ and $\delta = 1$ correspond to the asymptotic expressions derived from the upper and lower bounds of the secrecy outage probability, respectively. Note that when $N \geq 2$, the first term on the right hand side (RHS) of (59) will dominate with large MER, while the second term will become marginal. Hence we can conclude from the squeeze theorem that for criterion II and III, the system diversity order is also equal to M, regardless of the number of users and eavesdroppers. Moreover, the first term in RHS of (59) is irrespective of the number of users when $N \geq 2$, indicating that no gain can be achieved from increasing the number of users with high MER. Once again this is due to the bottleneck effect of the first hop from the BS to the relays when $N \geq 2$.

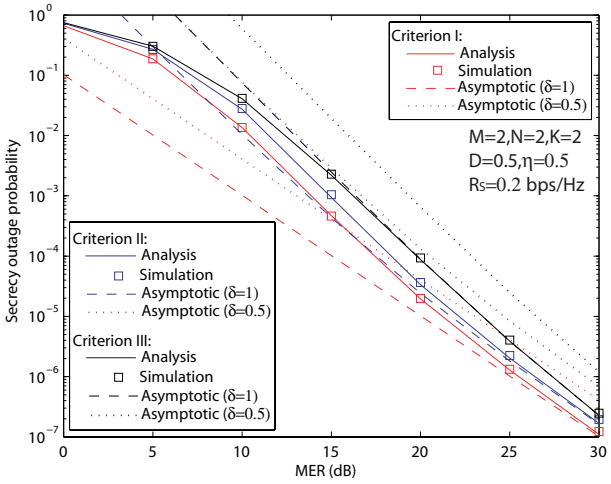

Fig. 2. Asymptotic secrecy outage probability versus MER.

VI. Numerical and Simulation Results

In this section, we present numerical and simulation results to verify the proposed studies. All the links in the system experience Rayleigh flat fading. We adopt the pathloss model with loss factor of four to determine the average channel gains. The distance between the base station and the desired users is set to unity. The relays are between the base station and desired users, and the distance between the base station and relays is denoted by D, so that $\alpha = D^{-4}$ and $\beta = (1-D)^{-4}$. In addition, we set a high transmit power at the base station with $P_S = 30$ dB, since we focus on the effect of MER on the system secrecy outage probability.

Fig. 2 shows the asymptotic secrecy outage probability versus MER, where $D = 0.5$, $R_s = 0.2$ bps/Hz, $M = 2$, $N = 2$, and $K = 2$. As observed from this figure, the asymptotic result from the lower bound of secrecy outage probability has the same curve slope with that from the upper bound. Moreover, the asymptotic secrecy outage probability from the lower bound converges to the exact value, while that from the upper bound is not tight even in high MER region. As such, in the following, we only show the asymptotic secrecy outage probability from the lower bound with $\delta = 1$.

Fig. 3 demonstrates the effect of the number of relays on the secrecy outage probability of criterion I, II, and III versus MER, where $D = 0.5$, $R_s = 0.2$ bps/Hz, $N = 2$, $K = 2$, and M varies from 1 to 3. For comparison, we plot the simulation results of the three selection criteria as well as the optimal selection performed in (11). As observed from the figure, we can find that for different values of MER and M, the analytical results for criterion I – III match well the simulation, which validates the derived analytical expressions of the secrecy outage probability in (35) and (47). In addition, the asymptotic results converge with the exact at high MER, which verifies the derived asymptotic expressions. Moreover, the slopes of the curve of the secrecy outage probability are in parallel with M, which verifies the system diversity order of M for all three criteria. Further, criterion I achieves a comparable performance to the optimal selection, and outperforms criterion II and III. This is because criterion I performs the selection by

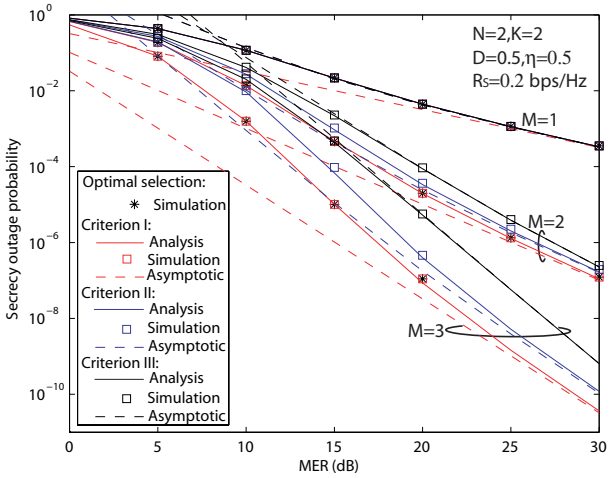

Fig. 3. Effect of number of relays on the secrecy outage probability versus MER.

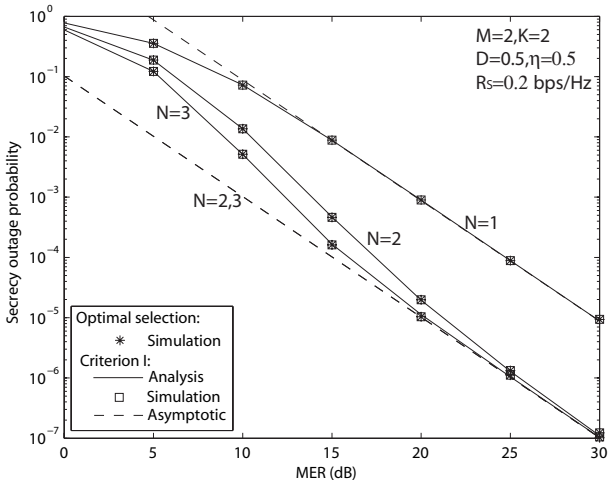

Fig. 4. Effect of number of users on the secrecy outage probability versus MER: Criterion I.

incorporating both the main and eavesdropper links. Criterion II exhibits better performance than criterion III, as the former incorporates different impact from the two relay hops on the system security. One can also find that the performance gap between the three criteria increases with the number of relays.

Figs. 4 – 6 demonstrate the effect of the number of users on the system secrecy outage probability, where $M = 2$, $K = 2$, and N varies from 1 to 3. Specifically, Figs. 4 – 6 correspond to criterion I, II, and III, respectively. We find from the figures that the system secrecy outage probability improves with larger N, as more users help improve the link quality of the relays to users. However, this improvement becomes marginal for $N \geq 2$ when MER is high, since the first hop of the BS to relays becomes the bottleneck of the dual-hop data transmission. Moreover, curves with different N share the same slope, which indicates that users have no impact on the system diversity order for each criterion.

Figs. 7 – 9 demonstrate the effect of the number of eavesdroppers on the system secrecy outage probability versus MER, where $M = 2$, $N = 2$, and K varies from 1 to 4. Specif-

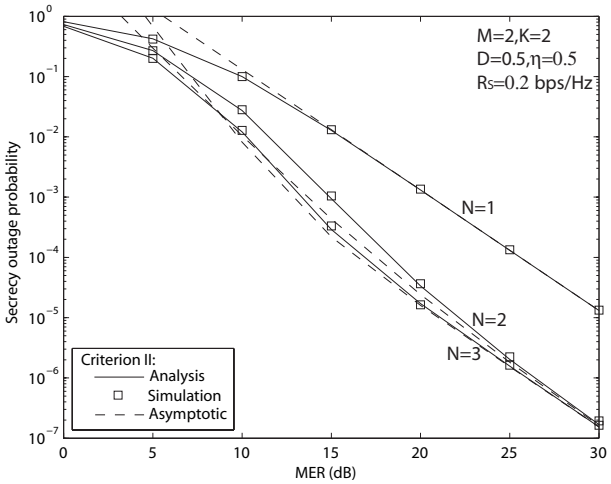

Fig. 5. Effect of number of users on the secrecy outage probability versus MER: Criterion II.

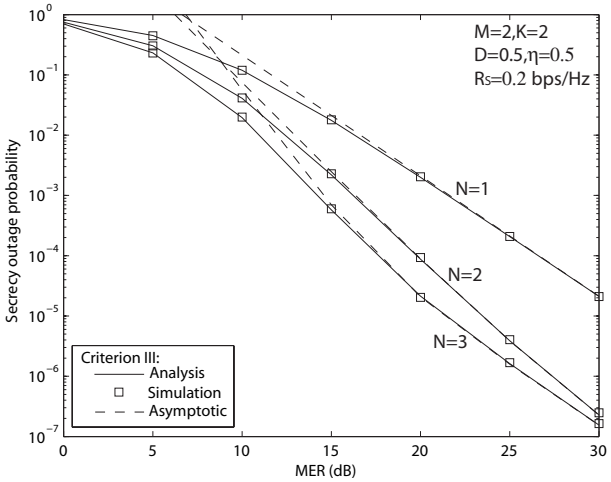

Fig. 6. Effect of number of users on the secrecy outage probability versus MER: Criterion III.

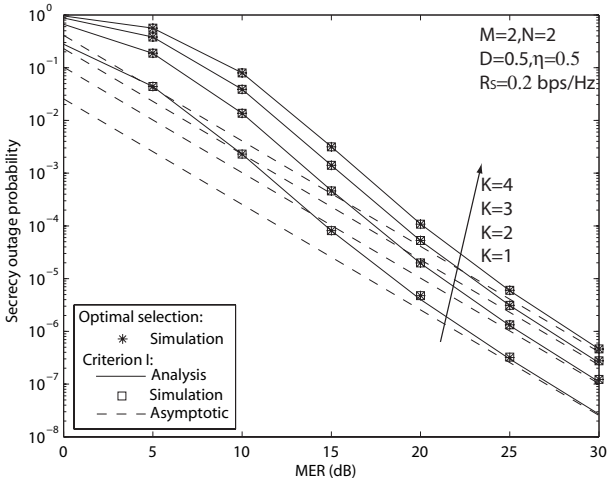

Fig. 7. Effect of number of eavesdroppers on the secrecy outage probability versus MER: Criterion I.

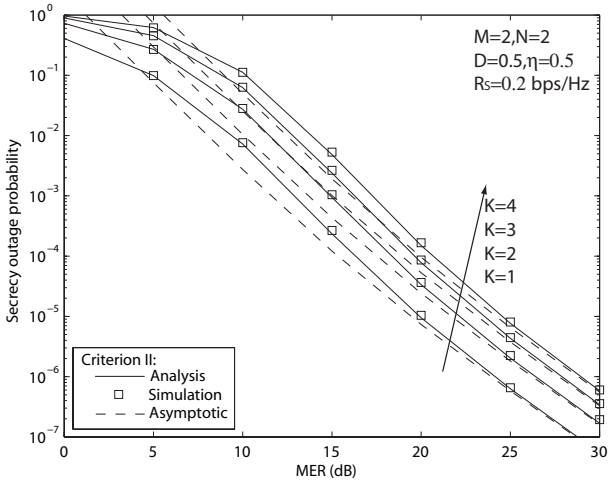

Fig. 8. Effect of number of eavesdroppers on the secrecy outage probability versus MER: Criterion II.

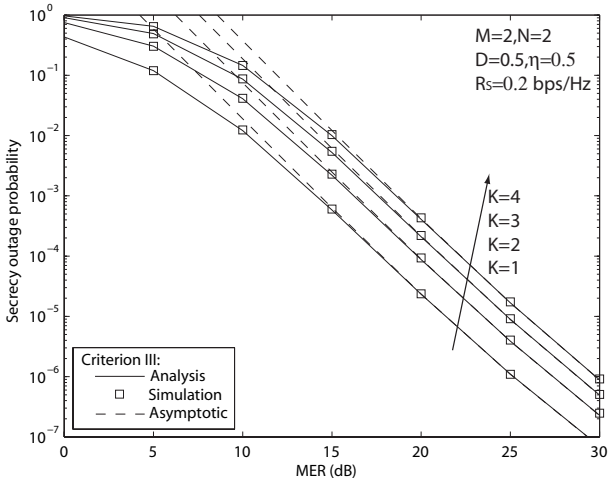

Fig. 9. Effect of number of eavesdroppers on the secrecy outage probability versus MER: Criterion III.

ically, Figs. 7 – 9 are associated with criterion I, II, and III, respectively. As observed from these three figures, we can find that the system secrecy outage probability deteriorates with larger K, as more eavesdroppers help strengthen the link of the relays to eavesdroppers. We see that curves with different values of K have the same slope, indicating that the system diversity order is independent of the number of eavesdroppers. Moreover, the analytical results match well with the simulation for different values of K, and the asymptotic results converge with the exact at high MER. This further verifies the derived analytical expressions for the secrecy outage probability as well as the asymptotic expressions for each criterion.

VII. Conclusions

In this paper, we proposed relay selection to secure the physical layer communication in multiuser cooperative relay networks with multiple amplify-and-forward (AF) relays, against the wiretap channel with multiple eavesdroppers. We presented three selection criteria to select the best relay and user pair, in order to strengthen the network security. For each of the three criteria, we derived analytical expressions for the secrecy outage probability with large transmit power. We also derived the asymptotic analysis for the secrecy outage probability with high MER. An interesting conclusion is that the system diversity order is equal to the number of relays, regardless of the selection criterion. The diversity order is also independent of the number of users and eavesdroppers.

Appendix I
Proof of Theorem 1

The CDF of u_{m^*} is defined as

$$F_{u_{m^*}}(x) = \Pr(u_{m^*} < x) \tag{A.1}$$

$$= \sum_{m=1}^{M} \Pr[u_m < x, \min(u_m, \rho v_{m,n_m^*}) > \max_{m_1=1,\cdots,M,m_1\neq m} \min(u_{m_1}, \rho v_{m_1,n_{m_1}^*})]. \tag{A.2}$$

Due to the symmetry, we can rewrite $F_{u_{m^*}}(x)$ as

$$F_{u_{m^*}}(x) = M \Pr[u_1 < x, \min(u_1, \rho v_{1,n_1^*}) > \theta], \tag{A.3}$$

where $\theta = \max_{m=2,\cdots,M} \min(u_m, \rho v_{m,n_m^*})$. The CDF of θ is equivalent to the $(M-1)$-th power of the CDF of $\min(u_m, \rho v_{m,n_m^*})$, given by

$$F_\theta(\theta) = \left[1 - \sum_{n=1}^{N} (-1)^{n-1} \binom{N}{n} e^{-(\frac{1}{\alpha} + \frac{n}{\rho\beta})\theta}\right]^{M-1} \tag{A.4}$$

$$= \widetilde{\sum_i} d_i e^{-e_i\theta}, \tag{A.5}$$

where $\widetilde{\sum_i}$, d_i and e_i are defined in (39). By setting $F_\theta(\theta)$ derivative with respect to θ, we can obtain the PDF of θ as

$$f_\theta(\theta) = -\widetilde{\sum_i} d_i e_i e^{-e_i\theta}. \tag{A.6}$$

Then, we further derive $F_{u_{m^*}}(x)$ from (A.3) as

$$F_{u_{m^*}}(x) = M \Pr\left(\theta < u_1 < x, v_{1,n_1^*} > \frac{\theta}{\rho}, 0 < \theta < x\right) \tag{A.7}$$

$$= M \int_0^x f_\theta(\theta) \left[\int_\theta^x f_{u_1}(u_1) du_1 \int_{\frac{\theta}{\rho}}^{\infty} f_{v_{1,n_1^*}}(v_1) dv_1\right] d\theta. \tag{A.8}$$

Applying the PDFs of θ, u_1 and v_{1,n_1^*} into the above equation leads to the CDF of u_{m^*}, as shown in (37) of Theorem 1.

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

$$F_{v_{m^*,n^*}}(x) = \Pr(v_{m^*,n^*} < x) \tag{A.9}$$

$$= \sum_{m=1}^{M} \Pr\left[v_{m,n_m^*} < x, \min(u_m, \rho v_{m,n_m^*}) > \max_{m_1=1,\cdots,M,m_1\neq m} \min(u_{m_1}, \rho v_{m_1,n_{m_1}^*})\right] \tag{A.10}$$

$$= M \Pr[v_{1,n_1^*} < x, \min(u_1, \rho v_{1,n_1^*}) > \theta]. \tag{A.11}$$

Note that the condition of $v_{1,n_1^*} < x$ and $\min(u_1, \rho v_{1,n_1^*}) > \theta$ can be written as $u_1 > \theta$, $v_{1,n_1^*} > \frac{\theta}{\rho}$ and $v_{1,n_1^*} < x$, which is equivalent to $u_1 > \theta$, $\frac{\theta}{\rho} < v_{1,n_1^*} < x$ and $0 < \theta < \rho x$. Hence, we can further write $F_{v_{m^*,n^*}}(x)$ as

$$F_{v_{m^*,n^*}}(x) = M \Pr\left(u_1 > \theta, \frac{\theta}{\rho} < v_{1,n_1^*} < x, 0 < \theta < \rho x\right) \tag{A.12}$$

$$= M \int_0^{\rho x} f_\theta(\theta) \left[\int_\theta^\infty f_{u_1}(u_1) du_1 \int_{\frac{\theta}{\rho}}^x f_{v_{1,n_1^*}}(v_1) dv_1\right] d\theta. \tag{A.13}$$

By applying the PDFs of θ, u_1 and v_{1,n_1^*} into the above equation, we can obtain the CDF of v_{m^*,n^*}, as shown in (37) of Theorem 1. Hence, we complete the proof of Theorem 1.

Appendix II
Proof of Theorem 2

For Z^b_{m,n_m^*} in (50), we derive its CDF as

$$F_{Z^b_{m,n_m^*}}(z) = \Pr\left[\delta \min\left(\frac{u_m}{(\gamma_{th}-1)\eta}, \frac{v_{m,n_m^*}}{\gamma_{th}}\right) < z\right] \tag{B.1}$$

$$= 1 - \Pr\left[\min\left(\frac{u_m}{(\gamma_{th}-1)\eta}, \frac{v_{m,n_m^*}}{\gamma_{th}}\right) \geq \frac{z}{\delta}\right] \tag{B.2}$$

$$= 1 - \Pr\left(u_m \geq \frac{(\gamma_{th}-1)\eta z}{\delta}\right) \times \Pr\left(v_{m,n_m^*} \geq \frac{\gamma_{th} z}{\delta}\right). \tag{B.3}$$

Applying the PDFs of u_m and v_{m,n_m^*} into the above equation yields the CDF of Z^b_{m,n_m^*} as

$$F_{Z^b_{m,n_m^*}}(z) = 1 - \sum_{n=1}^N (-1)^{n-1} \binom{N}{n} e^{-[\frac{(\gamma_{th}-1)\eta}{\delta\alpha} + \frac{n\gamma_{th}}{\delta\beta}]z}. \tag{B.4}$$

Similar to eqs. (32)-(33), we can obtain the asymptotic expression of P_{out,m,n_m^*} as

$$P_{out,m,n_m^*} \simeq \frac{1}{\Gamma(K)\varepsilon^K} \int_0^\infty F_{Z^b_{m,n_m^*}}(w) w^{K-1} e^{-\frac{w}{\varepsilon}} dw \tag{B.5}$$

$$= 1 - \frac{1}{\Gamma(K)\varepsilon^K} \sum_{n=1}^N (-1)^{n-1} \binom{N}{n} \times \int_0^\infty w^{K-1} e^{-(\frac{1}{\varepsilon} + \frac{(\gamma_{th}-1)\eta}{\delta\alpha} + \frac{n\gamma_{th}}{\delta\beta})w} dw \tag{B.6}$$

$$= 1 - \sum_{n=1}^N (-1)^{n-1} \binom{N}{n} \left(1 + \frac{(\gamma_{th}-1)\eta\varepsilon}{\delta\alpha} + \frac{n\gamma_{th}\varepsilon}{\delta\beta}\right)^{-K} \tag{B.7}$$

Applying the series approximation of $(1+x)^{-1} \simeq 1 - x$ for small value of $|x|$, we can further obtain the asymptotic expression of P_{out,m,n_m^*} with high MER as

$$P^{asy}_{out,m,n_m^*} = \frac{K}{\lambda\delta} \left(\frac{(\gamma_{th}-1)\eta\beta}{\alpha} + \sum_{n=1}^N (-1)^{n-1} \binom{N}{n} n\gamma_{th}\right) \tag{B.8}$$

$$= \begin{cases} \frac{K}{\lambda}\left[\frac{(\gamma_{th}-1)\eta\beta}{\delta\alpha} + \frac{\gamma_{th}}{\delta}\right], & \text{If } N = 1 \\ \frac{K}{\lambda}\frac{(\gamma_{th}-1)\eta\beta}{\delta\alpha}, & \text{If } N \geq 2 \end{cases}, \tag{B.9}$$

where we apply [32, (0.154.2)] in the last equality. Hence, the proof of Theorem 2 is completed.

Appendix III
Proof of Theorem 3

By applying the series approximation of $e^{-x} \simeq 1 - x$ for small value of $|x|$ into (A.4), we obtain the asymptotic CDF of θ with small value of $|\theta|$ as

$$F_\theta(\theta) \simeq \begin{cases} (\frac{1}{\alpha} + \frac{1}{\rho\beta})^{M-1} \theta^{M-1}, & \text{If } N = 1 \\ \frac{\theta^{M-1}}{\alpha^{M-1}}, & \text{If } N \geq 2 \end{cases}. \tag{C.1}$$

Then the asymptotic PDF of θ is given by

$$f_\theta(\theta) \simeq \begin{cases} (M-1)(\frac{1}{\alpha} + \frac{1}{\rho\beta})^{M-1} \theta^{M-2}, & \text{If } N = 1 \\ (M-1)\frac{\theta^{M-2}}{\alpha^{M-1}}, & \text{If } N \geq 2 \end{cases}. \tag{C.2}$$

From (A.8), we can derive the asymptotic $F_{u_{m^*}}(x)$ as

$$F_{u_{m^*}}(x) = M \int_0^x f_\theta(\theta) \left[\int_\theta^x f_{u_1}(u_1) du_1 \int_{\frac{\theta}{\rho}}^\infty f_{v_{1,n_1^*}}(v_1) dv_1\right] d\theta \tag{C.3}$$

$$\simeq M \int_0^x f_\theta(\theta)(e^{-\frac{\theta}{\alpha}} - e^{-\frac{x}{\alpha}}) d\theta \tag{C.4}$$

$$\simeq \frac{M}{\alpha} \int_0^x f_\theta(\theta)(x - \theta) d\theta. \tag{C.5}$$

By applying the asymptotic expression of $f_\theta(\theta)$ in (C.2) into the above equation, we can arrive at the asymptotic expression of $F_{u_{m^*}}(x)$, as shown in (53) of Theorem 3.

In a similar way, we can derive the asymptotic expression of $F_{v_{m^*,n^*}}(x)$ by applying (C.2) into (A.13). The result is shown in (54) of Theorem 3. In this way, we have completed the proof of Theorem 3.

References

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

[2] 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.

[3] 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.

[4] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 4005–4019, Apr. 2011.

[5] X. Sun, J. Wang, W. Xu, , and C. Zhao, "Performance of secure communications over correlated fading channels," *IEEE Sig. Proc. Lett.*, vol. 19, no. 8, pp. 479–482, Aug. 2012.

[6] J. Li and A. P. Petropulu, "Ergodic secrecy rate for multiple-antenna wiretap channels with Rician fading," *IEEE Trans. Information Forensics and Security*, vol. 6, no. 3, pp. 861–867, Sept. 2011.

[7] X. Liu, "Probability of strictly positive secrecy capacity of the Rician-Rician fading channel," *IEEE Wireless Commun. Lett.*, vol. 2, no. 1, pp. 50–53, Feb. 2013.

[8] M. Z. I. Sarkar and T. Ratnarajah, "Secure communication through Nakagami-m fading MISO channel," in *IEEE Inter. Conf. on Commun. (ICC)*, Kyoto, Japan, 2011.

[9] H. Alves, R. DemoSouza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Sig. Proc. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[10] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[11] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754–1757, Sept. 2013.

[12] W. Y. Luo, L. Jin, K. Z. Huang, and Z. Zhong, "User selection and resource allocation for secure multiuser MISO-OFDMA systems," *Elec. Lett.*, vol. 47, no. 15, pp. 884–886, July 2011.

[13] L. Fan, X. Lei, R. Q. Hu, and W. Seah, "Outdated relay selection in two-way relay network," *IEEE Trans. Veh. Technol.*, vol. 62, no. 8, pp. 4051–4057, Oct. 2013.

[14] L. Fan, X. Lei, T. Q. Duong, R. Q. Hu, and M. Elkashlan, "Multiuser cognitive relay networks: Joint impact of direct and relay communications," *IEEE Trans. Wireless Commun.*, To appear, 2014 (DOI:10.1109/TWC.2014.2322627).

[15] F. Gao, B. Jiang, X. Gao, and X.-D. Zhang, "Superimposed training based channel estimation for OFDM modulated amplify-and-forward relay networks," *IEEE Trans. Commun.*, vol. 59, no. 7, pp. 2029–2039, July 2011.

[16] F. Gao, R. Zhang, and Y.-C. Liang, "Channel estimation for OFDM modulated two-way relay networks," *IEEE Trans. Sig. Proc.*, vol. 57, no. 11, pp. 4443–4455, Nov. 2009.

[17] H. Zhang, L. Shu-hung, S. Gao, F. Gao, D. Pan, and X. Dai, "Doubly selective channel estimation for OFDM modulated amplify-and-forward relay networks using superimposed training," *EURASIP J. Wireless Commun. and Netw.*, Aug. 2012, 12 pages.

[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, June 2009.

[19] S. Zhang, S.-C. Liew, and H. Wang, "Blind known interference cancellation," *IEEE J. Select. Areas Commun.*, vol. 31, no. 8, pp. 1572–1582, Aug. 2013.

[20] S. Huang, H. Chen, Y. Zhang, and F. Zhao, "Energy-efficient cooperative spectrum sensing with amplify-and-forward relaying," *IEEE Commun. Lett.*, vol. 16, no. 4, pp. 450–453, Apr. 2012.

[21] S. Huang, H. Chen, Y. Zhang, and H.-H. Chen, "Sensing-energy tradeoff in cognitive radio networks with relays," *IEEE Systems Journal*, vol. 7, pp. 68–76, Mar. 2013.

[22] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Sig. Proc.*, vol. 61, no. 5, pp. 3532–3545, Jul. 2012.

[23] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's csi," *IEEE Sig. Proc. Lett.*, vol. 20, no. 1, pp. 39–42, Jan. 2013.

[24] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Information Forensics and Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[25] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Sig. Proc.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[26] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, Jun. 2012.

[27] 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.

[28] 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, Oct. 2009.

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

[30] 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.

[31] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. C. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Sig. Proc. Lett.*, vol. 20, no. 1, pp. 35–38, Jan. 2013.

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

[33] M. A. B. de Melo and D. B. da Costa, "Downlink performance of multiuser multi-relay cooperative networks: A low-complexity relay-destination selection scheme," in *18th European Wireless Conference*, Poznan, Poland, 2012.

[34] X. Zhang, W. Wang, and X. Ji, "Multiuser diversity in multiuser two-hop cooperative relay wireless networks: System model and performance analysis," *IEEE Trans. Veh. Technol.*, vol. 58, no. 2, pp. 1031–1036, Feb. 2009.

[35] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.

[36] X. Li, J. Sun, L. Jin, and M. Liu, "Bi-parameter CGM model for approximation of α-stable PDF," *Elec. Lett.*, vol. 44, no. 18, pp. 1096–1097, August 2008.

[37] X. Li, S. Wang, and L. Wu, "Generator and parameters estimation for IID general alpha stable random series," *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 7, pp. 2071–2080, 2009.

[38] P. L. Yeoh, M. Elkashlan, and I. B. Collings, "Exact and asymptotic SER of distributed TAS/MRC in MIMO relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 751–756, Mar. 2011.

[39] A. Behnad and X. Wang, "Accuracy of harmonic mean approximation in performance analysis of multihop amplify-and-forward relaying," *IEEE Wireless Commun. Lett.*, vol. 3, no. 2, pp. 125–128, Apr. 2014.

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

[41] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals and Series: More special functions*, 1st ed. CRC, 1990.