Secure Multiple Amplify-and-Forward Relaying with Co-Channel Interference

Secure Multiple Amplify-and-Forward Relaying with Co-Channel Interference

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

***Abstract*—We investigate the impact of co-channel interference on the security performance of multiple amplify-and-forward (AF) relaying networks, where N intermediate AF relays assist the data transmission from the source to the destination. The relays are corrupted by multiple co-channel interferers, and the information transmitted from the relays to destination can be overheard by the eavesdropper. In order to deal with the interference and wiretap, the best out of N relays is selected for security enhancement. To this end, we derive a novel lower bound on the secrecy outage probability (SOP), which is then utilized to present two best relay selection criteria, based on the instantaneous and statistical channel information of the interfering links. For these criteria and the conventional max-min criterion, we quantify the impact of co-channel interference and relay selection by deriving the lower bound on the SOP. Furthermore, we derive the asymptotic SOP for each criterion, to explicitly reveal the impact of transmit power allocation among interferers on the secrecy performance, which offers valuable insights into practical design. We demonstrate that all selection criteria achieve full secrecy diversity order N, while the proposed in this paper two criteria outperform the conventional max-min scheme.**

***Index Terms*—Secure communications, co-channel interference, relay selection, secrecy diversity order.**

I. Introduction

Due to its broadcast nature, wireless transmission may be overheard by eavesdroppers in the network, which brings out the risk of information leakage. To prevent this leakage, secure techniques, such as encryption and physical-layer security (PLS) [1], have been widely investigated in the literature. In the pioneering work by Wyner [2], the classical wiretap model was proposed to analyze the secure communication. Then the study on PLS has been extended over fading channels, such as Rayleigh and Nakagami-m [3]–[6]. In these works, important metrics of secrecy performance, such as secrecy outage probability (SOP) and secrecy capacity, have been studied. To enhance the transmission security for multi-antenna systems, antenna selection technique can be used to exploit the dynamic nature among the multi-antenna fading channels [7].

Relaying technique has attracted increasingly attention in the literature, since it extends the radio coverage and improves the system capacity, without raising the transmit power [8]–[11]. Hence, it is of vital importance to study the PLS in relay networks [12]–[15]. There are two fundamental relaying protocols: amplify-and-forward (AF) and decode-and-forward (DF). For DF-aided relay networks, the system secure communication has been extensively studied, by deriving analytical expressions for the SOP in [16]–[18]. In order to enhance the security for multi-DF relay networks, these works [16]–[18] used relay selection techniques to exploit the dynamic nature among multi-relay fading channels. Compared with DF relaying, it is, however, much more complicated to obtain analytical SOP expressions for AF relay networks, since the received signal-to-noise ratios (SNRs) at the destination and eavesdroppers are represented in complex forms. In order to deal with this issue, the authors in [19] analyzed the intercept probability, which depends on the second-hop relay channels only. However, this probability is just a special case of the SOP, where the target secrecy data rate is set to zero. Furthermore, the authors in [20] investigated the PLS of multiuser multi-AF relay networks, and presented closed-form expressions for the limiting behavior of SOP, assuming a large transmit power.

One of the utmost concerns arising in wireless networks is the existence of co-channel interference, due to the excessive frequency reuse [21]–[25]. In [26], the authors studied a relay network in the presence of co-channel interference and analyzed the effect of interference power distribution[1] on the network performance. For multi-AF relay networks with co-channel interference, the relay selection aided by the interfering channel parameters can be used to improve the network transmission performance [27]. Recently, the impact of co-channel interference on the secure communications has received much attention. In [28], the authors studied the PLS of multi-DF relay networks in the presence of co-channel interference, by deriving the analytical and asymptotic SOP expressions. To the best of our knowledge, no prior work

This work was supported by the NSF of China (No. 61372129/61471229/61501382), Guangdong Natural Science Funds for Distinguished Young Scholar (No. 2014A030306027). This work of T. Q. Duong was supported in part by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22 and by the Newton Institutional Link under Grant ID 172719890.

L. Fan is with the School of Computer Science and Educational Software, Guangzhou University, Guangzhou, China, and is also with National Mobile Communications Research Laboratory, Southeast University (e-mail: lsfan@gzhu.edu.cn).

X. Lei is with the Provincial Key Lab of Information Coding and Transmission, Southwest Jiaotong University, Chengdu, China, and is also with National Mobile Communications Research Laboratory, Southeast University (e-mail: xflei@home.swjtu.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).

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

[1]As shown in [26], the interference power distribution refers to the transmit power allocation among interferers, for a given total transmit power.

has considered the secure communications of multi-AF relay networks, taking into account the impact of co-channel interference and relay selection.

In this paper, we study the secure communications of multi-AF relay networks in the presence of an eavesdropper, assuming that the N relays are disturbed by multiple co-channel interferers. To tackle with the co-channel interference and wiretap, relay selection is performed, such that the best relay is chosen to enhance the network security. We study the network secrecy performance by deriving the analytical and asymptotic SOP expressions. The key contributions of this paper are summarized as follows,

- To facilitate the secure performance evaluation, we derive a novel lower bound on the SOP, which is valid for an arbitrary transmit power.
- Besides the traditional max-min criterion, we utilize the newly derived lower bound on the SOP to present two relay selection criteria, based on the instantaneous and statistical channel information of the interfering links, respectively.
- For each criterion, we derive an analytical lower bound on the SOP, in order to investigate the system secrecy performance.
- We present novel asymptotic results for the SOP with high main-to-eavesdropper ratio (MER), which can be efficiently used to determine the factors governing the secrecy performance.
- Based on these asymptotic expressions, we provide key insights into the network secrecy diversity order and the impact of interference power distribution on the network security.

The rest of the paper is organized as follows. Section II introduces the system model of the secure multi-AF relay networks in the presence of co-channel interference. In Section III, we first derive a novel lower bound expression for the SOP, and then we present the relay selection criteria. For each criterion, Section IV provides the analytical lower bound of SOP as well as the asymptotic expression, assuming high value of MER. Simulations and numerical results are presented in Section V to show the impact of co-channel interference and relay selection on the network security. Finally, conclusions are drawn in Section VI.

Notations: 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 density function (CDF) of the RV X, respectively. The function, $E_1(x) = \int_x^\infty \frac{e^{-t}}{t} dt$, is the exponential integral function [29], while $\Pr[\cdot]$ returns the probability, and $E[\cdot]$ denotes statistical average.

II. System Model

Fig. 1 depicts the system model of a two-phase multiple AF relay network with co-channel interference, where the source S communicates with the destination D with the help of N intermediate AF relays, $\{R_n | 1 \leq n \leq N\}$. Apart from the additive white Gaussian noise (AWGN), the relays are

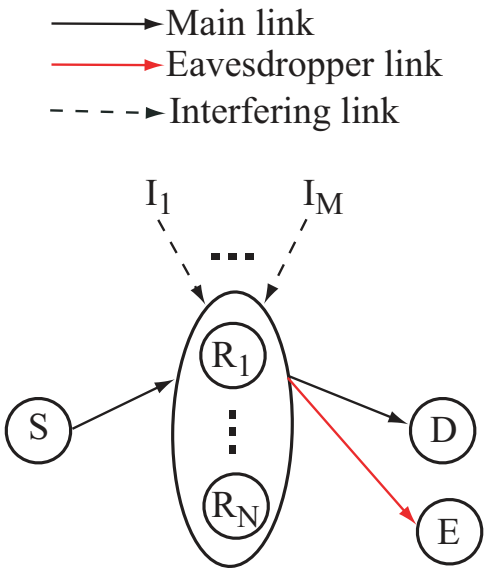

Fig. 1. A network consisting of multiple AF relays with co-channel interference and an eavesdropper.

corrupted by M co-channel interferers, $\{I_m | 1 \leq m \leq M\}$. An eavesdropper, E, can overhear the message forwarded from relays, which indicates a great threat to the communication from S to D. Note that the network secrecy performance becomes worse if multiple eavesdroppers exist in the network, no matter whether the eavesdroppers decode the messages in a colluding or non-colluding manner [20]. However, the relay selection criteria and the secrecy performance analytical framework proposed in this work can be easily extended to the case of multiple eavesdroppers. We assume that D and E are disturbed by the AWGN only. A severe shadowing environment is considered, so that there is no direct link from S to D or from S to E. Due to the size limitation, all nodes in the network are equipped with a single antenna. To deal with the wiretap channel and co-channel interference, the best relay, R_{n^*}, needs to be selected among N relays for enhancing the network security. Before presenting the relay selection criterion, we first formulate the two-phase data transmission with co-channel interference at relays.

Suppose that R_n is selected for data transmission. In the first phase, S sends signal x_S to R_n in co-channel interference environments. The received signal at R_n is given by

$$y_{R_n} = \sqrt{P} h_{S,R_n} x_S + \sum_{m=1}^{M} \sqrt{P_{I_m}} h_{I_m,R_n} x_{I_m} + n_R, \quad (1)$$

where P is the transmit power at S, $h_{S,R_n} \sim \mathcal{CN}(0,\alpha)$ is the channel coefficient of the S–R_n link, P_{I_m} and x_{I_m} are the transmit power and signal of the interferer I_m, $h_{I_m,R_n} \sim \mathcal{CN}(0,\varepsilon)$ is the channel coefficient of the interfering I_m–R_n link, and $n_R \sim \mathcal{CN}(0,N_o)$ is the AWGN at R_n. As per the rules of AF relaying, R_n amplifies y_{R_n} using the factor

$$\kappa_n = \sqrt{\frac{P}{P|h_{S,R_n}|^2 + \sum_{m=1}^{M} P_{I_m} |h_{I_m,R_n}|^2 + N_o}}. \quad (2)$$

The received signals at D and E from R_n in the second phase can be respectively written as

$$y_D = h_{R_n,D}\kappa_n y_{R_n} + n_D, \tag{3}$$

$$y_E = h_{R_n,E}\kappa_n y_{R_n} + n_E, \tag{4}$$

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 and R_n–E links, respectively, and $n_D \sim \mathcal{CN}(0,N_o)$ and $n_E \sim \mathcal{CN}(0,N_o)$ are the AWGN at D and E, respectively. Note that D and E only receive signals, but not transmit. Hence, there is no channel link between D and E. Using (1)–(4), the end-to-end signal-to-interference-plus-noise ratios (SINRs) at D and E can be written as

$$\gamma_n^D = \frac{\frac{\tilde{P}u_n}{1+\sum_{m=1}^{M}\tilde{P}_{I_m}w_{mn}}\tilde{P}v_{1n}}{1+\frac{\tilde{P}u_n}{1+\sum_{m=1}^{M}\tilde{P}_{I_m}w_{mn}}+\tilde{P}v_{1n}}, \tag{5}$$

$$\gamma_n^E = \frac{\frac{\tilde{P}u_n}{1+\sum_{m=1}^{M}\tilde{P}_{I_m}w_{mn}}\tilde{P}v_{2n}}{1+\frac{\tilde{P}u_n}{1+\sum_{m=1}^{M}\tilde{P}_{I_m}w_{mn}}+\tilde{P}v_{2n}}, \tag{6}$$

where $\tilde{P} = P/N_o$ and $\tilde{P}_{I_m} = P_{I_m}/N_o$ denote the average SNR at the source and interferer I_m, respectively. For the simplification of notation, let us denote $u_n = |h_{S,R_n}|^2$, $v_{1n} = |h_{R_n,D}|^2$, $v_{2n} = |h_{R_n,E}|^2$, and $w_{mn} = |h_{I_m,R_n}|^2$ as the associated channel gains.

The SOP with R_n is defined as the probability that the difference of the data rate between the main and eavesdropper links falls below a given threshold R_s, which is formulated as

$$\mathcal{P}_{n,out} = \Pr\left[\frac{1}{2}\log_2(1+\gamma_n^D) - \frac{1}{2}\log_2(1+\gamma_n^E) < R_s\right] \tag{7}$$

$$= \Pr\left[\frac{1+\gamma_n^D}{1+\gamma_n^E} < \gamma_s\right], \tag{8}$$

where the term $\frac{1}{2}$ in (7) is due to the two-phase data transmission, and $\gamma_s = 2^{2R_s}$ denotes the secrecy SNR threshold.

III. Relay Selection

A. A Novel Lower Bound on the SOP

As observed from (5) and (6), the received SINRs, γ_n^D and γ_n^E, share two common RVs, namely, u_n and w_{mn}. As such, it is not trivial to derive an exact analytical expression for the SOP, since γ_n^D and γ_n^E are correlated RVs. To deal with this issue, we note that the authors in [20] presented simplified expressions for γ_n^D and γ_n^E, by assuming large transmit power P. However, this is not applicable in practical scenarios, where the terminals are limited powered, e.g., mobile devices or sensor nodes. Next, we derive a novel lower bound on the SOP. We first write $\mathcal{P}_{n,out}$ as

$$\mathcal{P}_{n,out} = \Pr\left[\frac{1+\frac{\tilde{P}u_n}{1+z_n}\tilde{P}v_{1n}}{1+\frac{\tilde{P}u_n}{1+z_n}+\tilde{P}v_{1n}} < \gamma_s\right], \tag{9}$$

where $z_n = \sum_{m=1}^{M}\tilde{P}_{I_m}w_{mn}$. Based on the following equalities

$$1+\frac{\frac{\tilde{P}u_n}{1+z_n}\tilde{P}v_{1n}}{1+\frac{\tilde{P}u_n}{1+z_n}+\tilde{P}v_{1n}} = \frac{(1+\frac{\tilde{P}u_n}{1+z_n})(1+\tilde{P}v_{1n})}{1+\frac{\tilde{P}u_n}{1+z_n}+\tilde{P}v_{1n}}, \tag{10}$$

$$1+\frac{\frac{\tilde{P}u_n}{1+z_n}\tilde{P}v_{2n}}{1+\frac{\tilde{P}u_n}{1+z_n}+\tilde{P}v_{2n}} = \frac{(1+\frac{\tilde{P}u_n}{1+z_n})(1+\tilde{P}v_{2n})}{1+\frac{\tilde{P}u_n}{1+z_n}+\tilde{P}v_{2n}}, \tag{11}$$

we rewrite $\mathcal{P}_{n,out}$ in a more compact form as

$$\mathcal{P}_{n,out} = \Pr\left[\frac{(1+\tilde{P}v_{1n})(1+\frac{\tilde{P}u_n}{1+z_n}+\tilde{P}v_{2n})}{(1+\tilde{P}v_{2n})(1+\frac{\tilde{P}u_n}{1+z_n}+\tilde{P}v_{1n})} < \gamma_s\right],$$

$$= \Pr\left[1+\frac{\frac{\tilde{P}u_n}{1+z_n}}{1+\tilde{P}v_{2n}} < \gamma_s(1+\frac{\frac{\tilde{P}u_n}{1+z_n}}{1+\tilde{P}v_{1n}})\right],$$

$$= \Pr\left[\frac{\frac{\tilde{P}u_n}{1+z_n}}{1+\tilde{P}v_{2n}} < (\gamma_s-1)+\frac{\gamma_s\cdot\frac{\tilde{P}u_n}{1+z_n}}{1+\tilde{P}v_{1n}}\right]. \tag{12}$$

Since

$$\frac{1}{1+\tilde{P}v_{2n}} < \frac{\gamma_s-1}{\frac{\tilde{P}u_n}{1+z_n}} + \frac{\gamma_s}{1+\tilde{P}v_{1n}}, \tag{13}$$

we further rewrite $\mathcal{P}_{n,out}$ as

$$\mathcal{P}_{n,out} = \Pr\left[\frac{1}{\frac{\gamma_s-1}{\frac{\tilde{P}u_n}{1+z_n}}+\frac{\gamma_s}{1+\tilde{P}v_{1n}}} < 1+\tilde{P}v_{2n}\right]. \tag{14}$$

By applying the inequality[2] [30]

$$\frac{1}{\frac{1}{x_1}+\frac{1}{x_2}} = \frac{x_1x_2}{x_1+x_2} \le \min(x_1,x_2) \tag{15}$$

into (14), a new lower bound expression of $\mathcal{P}_{n,out}$ is obtained as

$$\mathcal{P}_{n,out}^{\mathsf{LB}} = \Pr\left[\min\left(\frac{\tilde{P}u_n}{(\gamma_s-1)(1+z_n)}, \frac{1+\tilde{P}v_{1n}}{\gamma_s}\right) < 1+\tilde{P}v_{2n}\right]$$

$$= \Pr\left[\min\left(\frac{u_n}{(\gamma_s-1)(1+z_n)}, \frac{\tilde{P}_r+v_{1n}}{\gamma_s}\right) < \tilde{P}_r+v_{2n}\right], \tag{16}$$

where $\tilde{P}_r = \frac{1}{\tilde{P}}$. It is worthwhile to note that the lower bound derived above can be used for the entire regime of transmit power, thus being more applicable than the method given by [20] for secrecy performance evaluation.

B. Selection Criterion

Relying on the newly derived lower bound on $\mathcal{P}_{n,out}$ in (16), we next present the relay selection criterion to choose the best relay R_{n^*} in order to deal with the co-channel interference and wiretap. In practical communication scenarios with passive eavesdroppers, it is hard to acquire the instantaneous channel coefficients of eavesdropper links, and only the channel coefficients of main and interfering links can be utilized to

[2]Note that the accuracy of the bound in (15) depends on the values of x_1 and x_2. Specifically, it is quite accurate when x_1 is far from x_2, while the accuracy becomes worse when x_1 is close to x_2.

perform relay selection. From (16), the best relay, R_{n^*}, is selected according to

$$n^* = \arg \max_{1\le n\le N} \min\Big(\frac{u_n}{(\gamma_s-1)(1+z_n)}, \frac{\tilde{P}_r+v_{1n}}{\gamma_s}\Big). \quad (17)$$

According to this criterion, the system needs to know the instantaneous channel coefficients of the interfering links, which can be obtained in some communication systems through dedicated feedback channels from the interferers. However, in some other communication systems without such feedback, the system is only able to know the statistical channel information of interfering links. In this case, the best relay R_{n^*} is selected according to

$$n^* = \arg \max_{1\le n\le N} \min\Big(\frac{u_n}{(\gamma_s-1)(1+E(z_n))}, \frac{\tilde{P}_r+v_{1n}}{\gamma_s}\Big). \quad (18)$$

Apart from the proposed selection criteria, the conventional max-min criterion can also be used to select the best relay. This criterion is mathematically expressed as

$$n^* = \arg \max_{1\le n\le N} \min(u_n, v_{1n}), \quad (19)$$

which maximizes the minimum channel gain of the dual-hop main link.

After relay selection, the lower bound on the SOP with selected R_{n^*} is given by

$$\mathcal{P}_{out}^{\mathsf{LB}} = \Pr\Bigg[\min\Bigg(\frac{u_{n^*}}{(\gamma_s-1)(1+z_{n^*})}, \frac{\tilde{P}_r+v_{1n^*}}{\gamma_s}\Bigg) < \tilde{P}_r+v_{2n^*}\Bigg]. \quad (20)$$

For the reader's convenience, we next refer to the selection criterion in (17), (18) and (19) as criterion I, II, and III, respectively. For these three criteria, we will derive the analytical expression for the SOP and the asymptotic SOP in the high regime of MER.

IV. Secrecy Outage Probability

A. Lower Bound for Criterion I

Based on the selection criterion in (17), we write the lower bound on the SOP as

$$\mathcal{P}_{out}^{\mathsf{LB}} = \Pr\Bigg[\Bigg(\max_{1\le n\le N}\min\Big(\frac{u_n}{(\gamma_s-1)(1+z_n)}, \frac{\tilde{P}_r+v_{1n}}{\gamma_s}\Big)\Bigg) < \tilde{P}_r+v_{2n^*}\Bigg]. \quad (21)$$

By defining θ_n as,

$$\theta_n = \min\Big(\frac{u_n}{(\gamma_s-1)(1+z_n)}, \frac{\tilde{P}_r+v_{1n}}{\gamma_s}\Big), \quad (22)$$

we rewrite $\mathcal{P}_{out}^{\mathsf{LB}}$ as

$$\mathcal{P}_{out}^{\mathsf{LB}} = \Pr\Big(\max_{1\le n\le N}\theta_n < \tilde{P}_r+v_{2n^*}\Big). \quad (23)$$

Note that both u_n and v_{1n} follow exponential distribution with mean α and β_1, respectively. The PDF of z_n is given by [31]

$$f_{z_n}(z) = \sum_{(i,j)} \chi_{i,j}\frac{(\varepsilon P_{I<i>})^{-j}}{(j-1)!}z^{j-1}e^{-\frac{z}{\varepsilon P_{I<i>}}}, \quad (24)$$

where

$$\sum_{(i,j)} = \sum_{i=1}^{\rho(\mathbf{A})}\sum_{j=1}^{\tau_i(\mathbf{A})}, \quad (25)$$

and $\mathbf{A} = \mathrm{diag}(\varepsilon\tilde{P}_{I1}, \varepsilon P_{I2}, \cdots, \varepsilon\tilde{P}_{IM})$. We denote $\rho(\mathbf{A})$ as the number of distinct diagonal elements, $\varepsilon\tilde{P}_{I<1>} > \varepsilon\tilde{P}_{I<2>} > \cdots > \varepsilon\tilde{P}_{I<\rho(\mathbf{A})>}$ as the distinct diagonal elements in decreasing order, $\tau_i(\mathbf{A})$ as the multiplicity of $\varepsilon\tilde{P}_{I<i>}$, and $\chi_{i,j}$ as the (i,j)-th characteristic coefficient of $\mathbf{A}$. From the above, we obtain the CDF of $\theta_{n^*} = \max_{1\le n\le N}\theta_n$ in the following theorem.

Theorem 1: The CDF of θ_{n^*} is

$$F_{\theta_{n^*}}(\theta) = 1 - \sum_{n=1}^{N}\sum_{(i,j)}\sum_{k=1}^{n\tau_i(\mathbf{A})}\binom{N}{n}(-1)^{n-1}d_{i,k}e^{\frac{n}{\tilde{P}\beta_1}} \times \exp\Bigg[-\Bigg(-(\frac{\gamma_s}{\beta_1}+\frac{\gamma_s-1}{\alpha})n\theta\Bigg)\Bigg]\Big(\theta+\frac{\alpha}{(\gamma_s-1)\varepsilon\tilde{P}_{I<i>}}\Big)^{-k}, \quad (26)$$

where

$$d_{i,k} = \frac{1}{[n\tau_i(\mathbf{A})-k]!}\frac{d^{n\tau_i(\mathbf{A})-k}}{dx^{n\tau_i(\mathbf{A})-k}}\Big[g(x) \times\Big(x+\frac{\alpha}{(\gamma_s-1)\varepsilon\tilde{P}_{I<i>}}\Big)^{k}\Big]_{|x=-\frac{\alpha}{(\gamma_s-1)\varepsilon\tilde{P}_{I<i>}}}, \quad (27)$$

with

$$g(x) = \Big[\sum_{(i,j)}\chi_{i,j}\big[1+\frac{(\gamma_s-1)\varepsilon\tilde{P}_{I<i>}}{\alpha}\theta\big]^{-j}\Big]^{n}. \quad (28)$$

Proof: *See Appendix A*.

From Theorem 1 and (23), we can write the lower bound on the SOP for criterion I in eqs. (29)-(30), as shown at the top of the next page, where [24, eq.(3.352.4)] and [24, eq.(3.353.2)] are used to achieve the last equality and $\Xi(a,b,k)$ is given by

$$\Xi(a,b,k) = \begin{cases} e^{ab}E_1(ab), & k=1 \\ \frac{1}{(k-1)!}\sum_{n=1}^{k-1}(n-1)!(-a)^{k-n-1}b^{-n} & \\ \quad +\frac{(-a)^{k-1}}{(k-1)!}e^{ab}E_1(ab), & k\ge 2 \end{cases}. \quad (31)$$

B. Lower Bound for Criteria II and III

We firstly express criterion II of (18) and III of (19) in a unified way as

$$n^* = \arg \max_{1\le n\le N} \min(u_n, \frac{v_{1n}+c_1}{c_2}), \quad (32)$$

where $c_1 = \tilde{P}_r$ and $c_2 = \frac{\gamma_s}{(\gamma_s-1)(1+\varepsilon P_{IA})}$ correspond to criterion II, while $c_1 = 0$ and $c_2 = 1$ correspond to criterion III. Note that in the existing works such as [20] and [32],

$$\mathcal{P}_{out}^{\mathsf{LB}} = 1 - \sum_{n=1}^{N}\sum_{(i,j)}\sum_{k=1}^{n\tau_i(\mathbf{A})}\binom{N}{n}(-1)^{n-1}\frac{d_{i,k}}{\beta_2}\exp\left[-\left(-\frac{n(\gamma_s-1)}{\tilde{P}}(\frac{1}{\alpha}+\frac{1}{\beta_1})\right)\right] \times \int_0^{\infty} e^{-[\frac{1}{\beta_2}+n(\frac{1}{\beta_2}+\frac{\gamma_s-1}{\alpha})]v_2}\frac{1}{\left(v_2+\tilde{P}_r+\frac{\alpha}{(\gamma_s-1)\varepsilon\tilde{P}_{I<i>}}\right)^k}dv_2 \tag{29}$$

$$= 1 - \sum_{n=1}^{N}\sum_{(i,j)}\sum_{k=1}^{n\tau_i(\mathbf{A})}\binom{N}{n}(-1)^{n-1}\frac{d_{i,k}}{\beta_2}\exp\left[-\left(-\frac{n(\gamma_s-1)}{\tilde{P}}(\frac{1}{\alpha}+\frac{1}{\beta_1})\right)\right]\Xi\Big[\frac{1}{\beta_2}+n(\frac{1}{\beta_2}+\frac{\gamma_s-1}{\alpha}),\tilde{P}_r+\frac{\alpha}{(\gamma_s-1)\varepsilon\tilde{P}_{I<i>}},k\Big], \tag{30}$$

$$\begin{aligned}\mathcal{P}_{out}^{\mathsf{LB}} =& 1 - b_1 b_3 e^{-\frac{\gamma_s-1}{\tilde{P}}(\frac{1}{\alpha}+\frac{1}{\beta_1})}\sum_{(i,j)}\chi_{i,j}\left(\frac{\alpha}{\vartheta_i}\right)^j\Xi\left[\frac{\gamma_s-1}{\alpha}+\frac{\gamma_s}{\beta_1},\tilde{P}_r+\frac{\alpha}{\vartheta_i},j\right] - \sum_{n=0}^{N-1}\sum_{(i,j)}b_{2n}b_3\chi_{i,j}e^{-\frac{\gamma_s-1}{\tilde{P}}(\frac{1}{\beta_1}+\frac{n+1}{\zeta})}\left(\frac{\zeta}{(n+1)\vartheta_i}\right)^j \\ &\times\Xi\left[\frac{\gamma_s}{\beta_1}+\frac{(n+1)(\gamma_s-1)}{\zeta},\tilde{P}_r+\frac{\zeta}{(n+1)\vartheta_i},j\right] - \sum_{n=0}^{N-1}\sum_{(i,j)}b_1b_{4n}\chi_{i,j}e^{-\frac{\gamma_s-1}{\tilde{P}}(\frac{1}{\alpha}+\frac{n+1}{c_2\zeta})}\left(\frac{\alpha}{\vartheta_i}\right)^j \\ &\times\Xi\left[\frac{\gamma_s-1}{\alpha}+\frac{(n+1)\gamma_s}{c_2\zeta},\tilde{P}_r+\frac{\alpha}{\vartheta_i},j\right] - \sum_{n_1=0}^{N-1}\sum_{n_2=0}^{N-1}\sum_{(i,j)}b_{2n_1}b_{4n_2}\chi_{i,j}e^{-\frac{\gamma_s-1}{\tilde{P}\zeta}(1+n_1+\frac{n_2+1}{c_2})}\left(\frac{\zeta}{(n_2+1)\vartheta_i}\right)^j \\ &\times\Xi\left[\frac{(n_1+1)(\gamma_s-1)}{\zeta}+\frac{(n_2+1)\gamma_s}{c_2\zeta},\tilde{P}_r+\frac{\zeta}{(n_2+1)\vartheta_i},j\right],\end{aligned} \tag{43}$$

u_{n^*} and v_{1n^*} were selected when $c_1 = 0$, which means that they are special cases of the present work. Using (32), we can obtain the CDFs of u_{n^*} and v_{1n^*} in the following theorem.

Theorem 2: The CDFs of u_{n^*} and v_{1n^*} are given by

$$F_{u_{n^*}}(x) = 1 - b_1 e^{-\frac{x}{\alpha}} - \sum_{n=0}^{N-1} b_{2n} e^{-\frac{(n+1)x}{\zeta}}, \tag{33}$$

$$F_{v_{1n^*}}(x) = 1 - b_3 e^{-\frac{x}{\beta_1}} - \sum_{n=0}^{N-1} b_{4n} e^{-\frac{(n+1)x}{c_2\zeta}}, \tag{34}$$

where

$$\zeta = \frac{\alpha\beta_1}{c_2\alpha+\beta_1}, \tag{35}$$

$$b_1 = \sum_{n=0}^{N-1} N\binom{N-1}{n}(-1)^n\frac{c_2\zeta}{c_2\zeta+n\beta_1}e^{-\frac{c_1 n}{c_2\alpha}}, \tag{36}$$

$$b_{2n} = N\binom{N-1}{n}(-1)^n\Big(\frac{1}{n+1}-\frac{c_2\zeta}{c_2\zeta+n\beta_1}\Big)e^{\frac{(n+1)c_1}{\beta_1}}, \tag{37}$$

$$b_3 = 1 - \sum_{n=0}^{N-1} N\binom{N-1}{n}(-1)^n\Big(\frac{1}{n+1}-\frac{\zeta}{\zeta+n\alpha}\Big)e^{-\frac{c_1(n+1)}{c_2\alpha}}, \tag{38}$$

$$b_{4n} = N\binom{N-1}{n}(-1)^n\Big(\frac{1}{n+1}-\frac{\zeta}{\zeta+n\alpha}\Big)e^{-\frac{c_1(n+1)}{c_2\alpha}}. \tag{39}$$

Proof: *See Appendix B.*

From Theorem 2, we write the lower bound on the SOP for criteria II and III as

$$\mathcal{P}_{out}^{\mathsf{LB}} = \Pr\left[\min\Big(\frac{u_{n^*}}{(\gamma_s-1)(1+z_{n^*})},\frac{\tilde{P}_r+v_{1n^*}}{\gamma_s}\Big) < \tilde{P}_r+v_{2n^*}\right] \tag{40}$$

$$= 1 - \Pr[u_{n^*}\geq(\gamma_s-1)(1+z_{n^*})(\tilde{P}_r+v_{2n^*}), v_{1n^*}\geq\gamma_s(\tilde{P}_r+v_{2n^*})-\tilde{P}_r] \tag{41}$$

$$= 1 - \int_0^{\infty}\int_0^{\infty}\Big[1-F_{u_{n^*}}[(\gamma_s-1)(1+z_{n^*}) \times(\tilde{P}_r+v_{2n^*})]\Big]\Big[1-F_{v_{1n^*}}(\gamma_s(\tilde{P}_r+v_{2n^*})-\tilde{P}_r)\Big] \times f_{v_{2n^*}}(v_{2n^*})f_{z_{n^*}}(z_{n^*})dv_{2n^*}dz_{n^*}. \tag{42}$$

By using the PDF of z_{n^*} in (24) and $f_{v_{2n^*}}(v_{2n^*}) = \frac{1}{\beta_2}e^{-\frac{v_{2n^*}}{\beta_2}}$, and solving the integral, we obtain the analytical lower bound on the SOP for criteria II and III in (43), as shown at the top of this page, where $\vartheta_i = (\gamma_s-1)\,\varepsilon P_{I<i>}$. By setting $c_1 = \tilde{P}_r$ with $c_2 = \frac{\gamma_s}{(\gamma_s-1)(1+\varepsilon P_{IA})}$ and $c_1 = 0$ with $c_2 = 1$ into the above equation, we obtain the lower bound on the SOP for criteria II and III, respectively.

C. Asymptotic SOP for Criterion I

In order to get insights into the system behavior for criterion I, we present an asymptotic expression for the SOP, when high MER is assumed. By applying the approximation of $e^{-x} \simeq 1-x$ and $(1+x)^{-n} \simeq 1-nx$ for small value of $|x|$, we obtain the asymptotic CDF of θ_n as

$$F_{\theta_n}(\theta) \simeq \big(\frac{\gamma_s}{\beta_1}+\frac{(\gamma_s-1)(1+\varepsilon\tilde{P}_{IA})}{\alpha}\big)\theta, \tag{44}$$

where we also assume a large transmit power P, and $\tilde{P}_{IA} = \sum_{m=1}^{M} \tilde{P}_{Im}$ denotes the total transmit power of interferers. From the asymptotic $F_{\theta_n}(\theta)$, we write the asymptotic SOP for criterion I as

$$\mathcal{P}_{out} \simeq \Big(\frac{\gamma_s}{\beta_1} + \frac{(\gamma_s - 1)(1 + \varepsilon \tilde{P}_{IA})}{\alpha}\Big)^N \int_0^\infty v_2^N f_{v_2}(v_2) dv_2 \tag{45}$$

$$= \frac{N!}{\lambda^N}\Big(\gamma_s + \frac{\beta_1(\gamma_s - 1)(1 + \varepsilon \tilde{P}_{IA})}{\alpha}\Big)^N, \tag{46}$$

where $\lambda = \frac{\beta_1}{\beta_2}$ is the MER, defined as the average channel gain ratio of the main to the eavesdropper link. From (46), we conclude that the secrecy diversity order is equal to the number of relays, where the secrecy diversity order can be defined as $\lim_{\lambda \to \infty} \frac{-\log \mathcal{P}_{out}}{\log \lambda}$. Hence, the network security can be profoundly enhanced by increasing the number of relays. Moreover, it is find that the asymptotic SOP depends on the total transmit power of interferers, but not on the interference power distribution.

D. Asymptotic SOP for Criteria II and III

We now provide the asymptotic SOP for criteria II and III with high MER. By applying the approximation of $e^{-x} \simeq \sum_{n=0}^{N} \frac{(-1)^n}{n!} x^n$ [29] for small value of $|x|$, we obtain the asymptotic distributions of u_{n^*} and v_{1n^*} as

$$F_{u_{n^*}}(x) \simeq \big(\frac{x}{\zeta}\big)^N \frac{\beta_1}{\beta_1 + c_2\alpha}, \tag{47}$$

$$F_{v_{1n^*}}(x) \simeq \big(\frac{x}{c_2\zeta}\big)^N \frac{c_2\alpha}{\beta_1 + c_2\alpha}, \tag{48}$$

where we also assume a large transmit power P. Then the asymptotic SOP for criteria II and III can be written by

$$\mathcal{P}_{out} \simeq \Pr\Big[\min\big(\frac{u_{n^*}}{(\gamma_s - 1)(1 + z_{n^*})}, \frac{v_{1n^*}}{\gamma_s}\big) < v_{2n^*}\Big] \tag{49}$$

$$= 1 - \Pr\big[u_{n^*} \geq (\gamma_s - 1)(1 + z_{n^*})v_{2n^*}, v_{1n^*} \geq \gamma_s v_{2n^*}\big] \tag{50}$$

$$= \frac{(\gamma_s - 1)^N}{\zeta^N} \frac{\beta_1}{\beta_1 + c_2\alpha} \int_0^\infty \int_0^\infty (1 + z_{n^*})^N v_{2n^*}^N \times f_{v_{2n^*}}(v_{2n^*}) f_{z_{n^*}}(z_{n^*}) dz_{n^*} dv_{2n^*} + \frac{\gamma_s^N}{\zeta^N} \frac{\alpha}{(\beta_1 + c_2\alpha)c_2^{N-1}} \int_0^\infty v_{2n^*}^N f_{v_{2n^*}}(v_{2n^*}) dv_{2n^*}. \tag{51}$$

By applying the PDFs of z_{n^*} and v_{2n^*}, and then solving the integral, we obtain the asymptotic SOP for criteria II and III as

$$\mathcal{P}_{out} \simeq \frac{N!}{\lambda^N}\Big(\frac{\beta_1 + c_2\alpha}{\alpha}\Big)^{N-1}\Big(\frac{\beta_1(\gamma_s - 1)^N}{\alpha} T_z + \frac{\gamma_s^N}{c_2^{N-1}}\Big), \tag{52}$$

where $T_z = E\{(1 + z_{n^*})^N\} = \sum_{n=0}^{N} \sum_{(i,j)} \binom{N}{n} \chi_{i,j} \frac{(n+j-1)!}{(j-1)!} (\varepsilon P_{I<i>})^n$. By setting c_2 to $\frac{\gamma_s}{(\gamma_s - 1)(1 + \varepsilon P_{IA})}$ and 1, we obtain the asymptotic SOP of criteria II and III, respectively.

From the asymptotic expression, it is evident that criteria II and III achieve the full secrecy diversity of order N. Hence, the system secrecy performance is significantly enhanced by increasing the number of relays. Moreover, it is found from [33]–[35] that T_z is a Schur-convex function with respect to the interference power vector $[P_{I_1}, P_{I_2}, \cdots, P_{I_M}]$. Hence, the interference power distribution affects the SOP of criteria II and III as follows: for a given total interference power, the optimal secrecy performance is achieved with equal-power interferers, while only one effective interferer[3] leads to the worst secrecy performance.

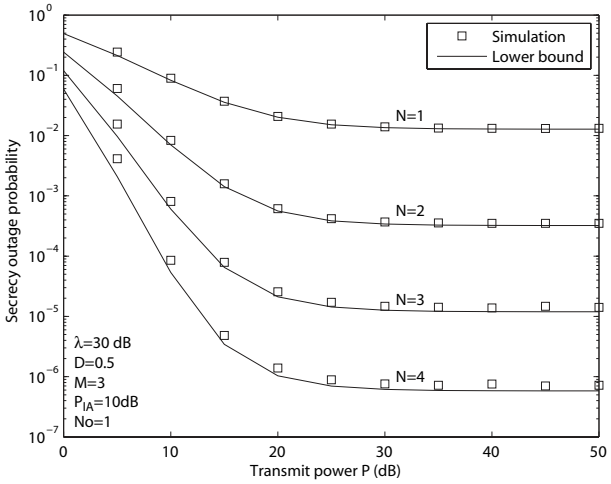

Fig. 2. Secrecy outage probability versus the transmit power P: Criterion I

V. Numerical and Simulation Results

In this section, we present some simulation and numerical results to demonstrate the impact of co-channel interference and relay selection on the secrecy performance. All links in the network experience Rayleigh flat fading. Without loss of generality, the distance between the source S and destination D is normalized to unity, and the relays are in between. Let D denote the distance between the relays and D, so that $\alpha = (1 - D)^{-4}$ and $\beta_1 = D^{-4}$, where the path loss model with the exponent of 4 is used. Note that the path loss model can be used for the average channel gains of eavesdropping links. Let D_E denote the distance between the relays and E. Then ε is set to D_E^{-4}, and the associated MER is $(D/D_E)^{-4}$. Since MER is related to D_E, and is a key factor that regulates the secrecy performance, we prefer to use MER as a key parameter in the simulations, which can actually reflect the value of D_E since $D_E = D \cdot \text{MER}^{1/4}$. The average channel gain of interfering links is set to one, and the target secrecy data rate R_s is set to 0.5 bps/Hz, so that the associated secrecy SNR threshold γ_s is 2.

Figs. 2-4 illustrate the effect of transmit power P on the SOP with $\lambda = 30$dB, where $D = 0.5$, $N_o = 1$, $M = 3$, and N varies from 1 to 4. Specifically, Figs. 2, 3 and 4 correspond to criteria I, II and III, respectively. The total transmit power of interferers P_{IA} is set to 10 dB, and un-equal interference power distribution is used with $P_{I_1} = 7$, $P_{I_2} = 2$ and $P_{I_3} = 1$. In this work, we consider the transmit power of the source

[3]As shown in [26], one effective interferer indicates that one interferer uses the total interference power to transmit signal, while the other interferes do not transmit signals.

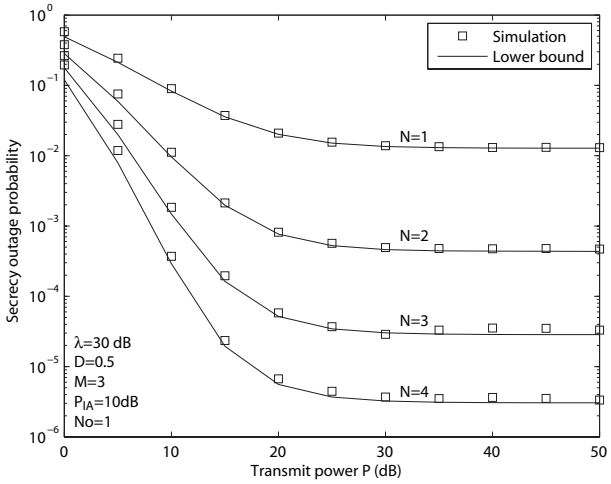

Fig. 3. Secrecy outage probability versus the transmit power P: Criterion II

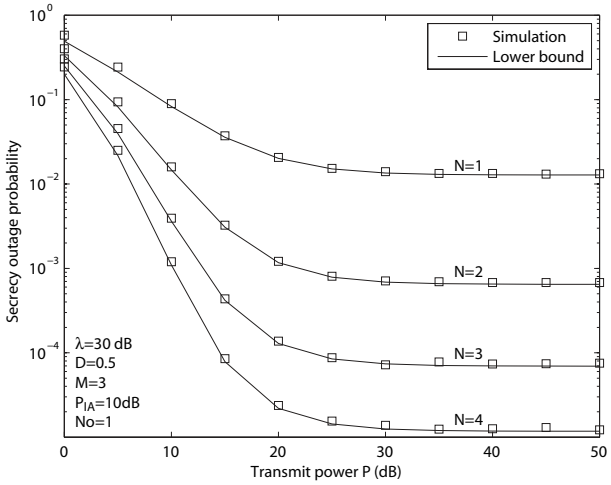

Fig. 4. Secrecy outage probability versus the transmit power P: Criterion III

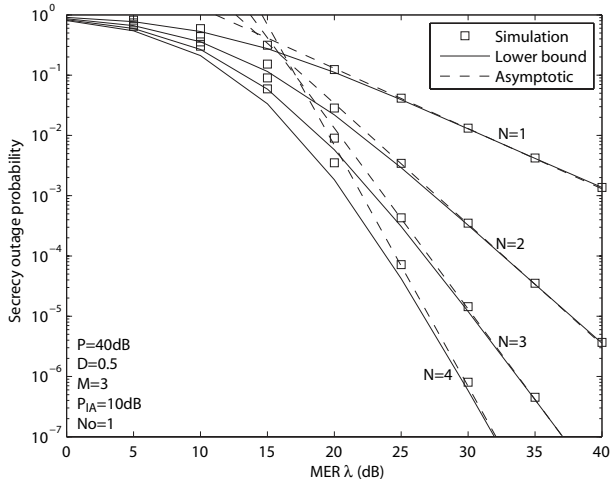

Fig. 5. Secrecy outage probability versus the MER λ: Criterion I

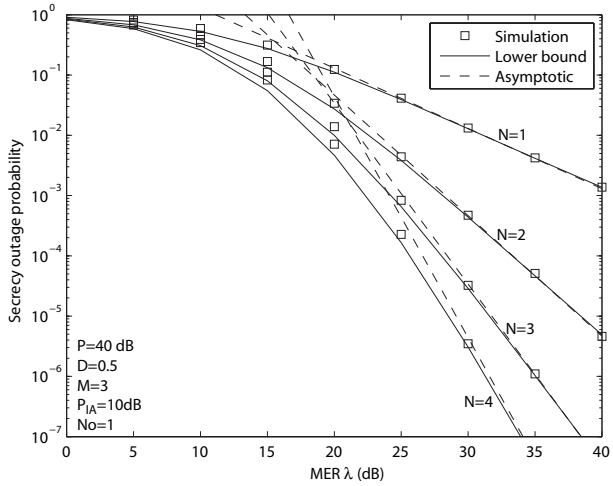

Fig. 6. Secrecy outage probability versus the MER λ: Criterion II

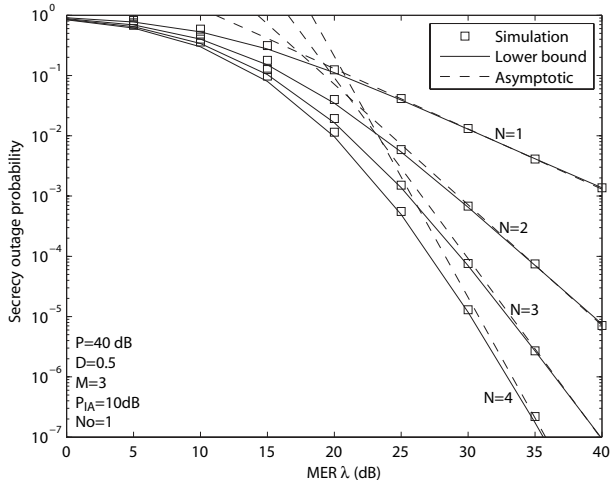

Fig. 7. Secrecy outage probability versus the MER λ: Criterion III

and interferers normalized by the noise power, and hence the relative unit of P_{IA} is dB. As it is observed from these figures, for each criterion and each number of relays, the lower bound on SOP is close to the simulation results in the entire region of P. This validates the effectiveness of the derived lower bound expression. Moreover, the SOP for each criterion is profoundly improved by increasing the number of relays, as more relays can help strengthen the secure transmission. The SOP can be also improved by increasing P. However, this improvement is almost saturated for large P, since the fixed main-to-eavesdropper ratio becomes the bottleneck of the network security.

Figs. 5-7 demonstrate the impact of relay selection and MER on the SOP with $P = 40$ dB, where $M = 2$ and the unequal interference power distribution is used with $P_{I_1} = 7$, $P_{I_2} = 2$ and $P_{I_3} = 1$. Specifically, Figs. 5, 6 and 7 correspond to criteria I, II and III, respectively. As can be seen, for each criterion, the lower bound on SOP matches well with the simulation result in the entire region of MER. This also validates the effectiveness of the derived lower bound expression. Moreover, the asymptotic result approaches the exact result with high MER, which corroborates the derived asymptotic expression for each criterion. Furthermore, the curve slope of SOP is in parallel with the number of relays, indicating that the network secrecy diversity order is equal to

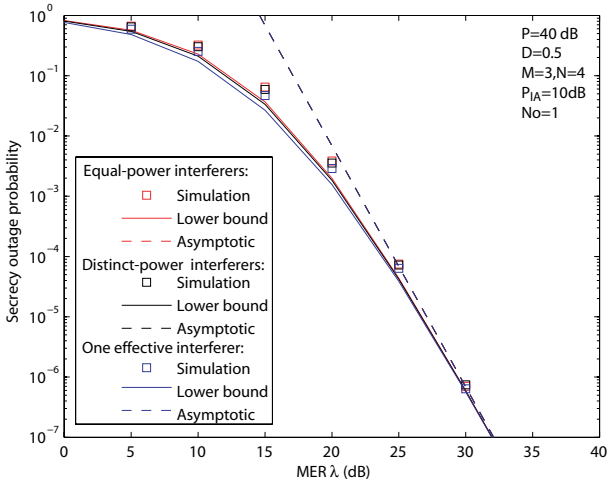

Fig. 8. Impact of interference power distribution on SOP: Criterion I

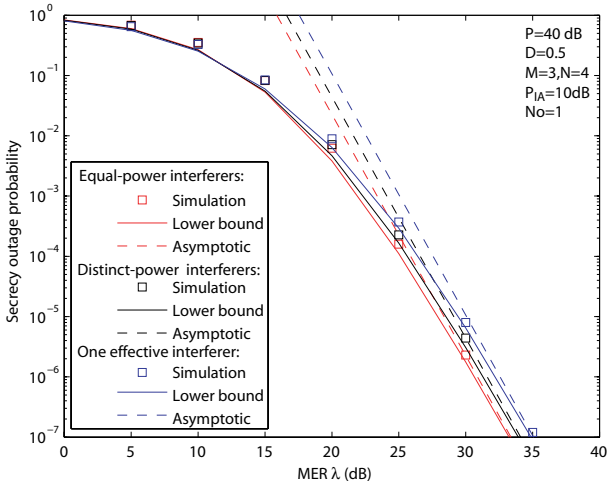

Fig. 9. Impact of interference power distribution on SOP: Criterion II

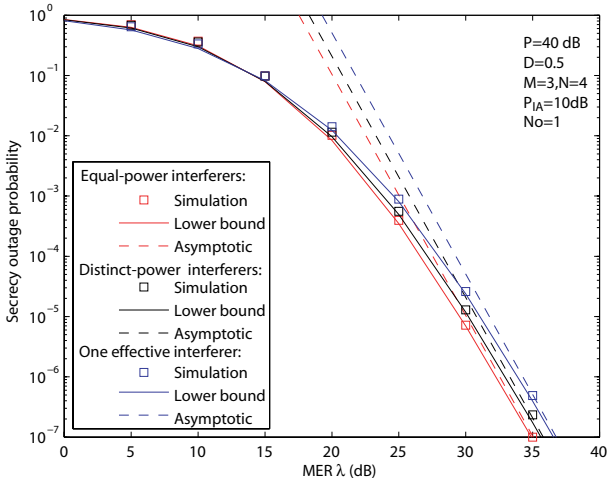

Fig. 10. Impact of interference power distribution on SOP: Criterion III

N for each criterion.

Figs. 8-10 show the impact of interference power distribution on the network SOPs of the three selection criteria, where $N = 4$, $M = 3$ and the total interference power P_{IA} is

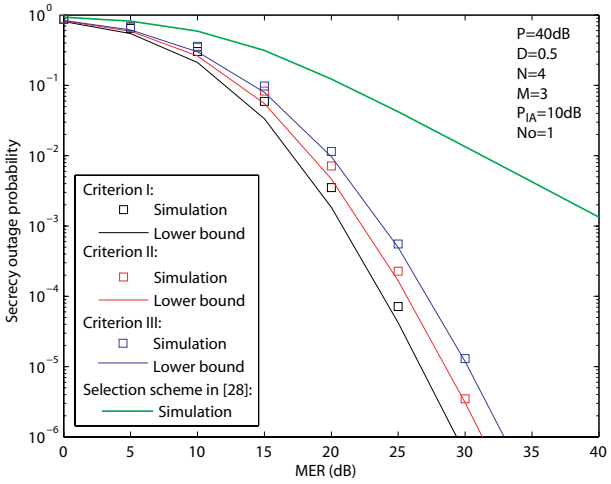

Fig. 11. Performance comparison among relay selection schemes.

fixed to 10 dB. Specifically, Figs. 8, 9 and 10 correspond to criteria I, II and III, respectively. For comparison, we consider three interference scenarios: the equal-power interferers with $P_{I_1} = P_{I_2} = P_{I_3} = \frac{10}{3}$, the distinct-power interferers with $[P_{I_1}, P_{I_2}, P_{I_3}] = [7, 2, 1]$, and the only one effective interferer with $[P_{I_1}, P_{I_2}, P_{I_3}] = [10, 0, 0]$. As can be clearly observed from Figs. 8-10 that the SOP of criterion I remains almost unchanged with the three interference scenarios, indicating that the network security is not affected by the interference power distribution. In contrast, the secrecy outage probabilities of criteria II and III are both affected by the interference scenarios. In particular, the optimal secrecy performances of criterion II and III can be achieved for the equal-power interferers, while the secrecy performances become worst for the only one effective interferer. Such observation validates the insights into the asymptotic SOP expressions of criteria II and III. We note that the interference power distribution imposes a noticeable impact on the secrecy performance of criteria II and III only in the high MER regime. This motivates us to use the asymptotic SOP to evaluate the impact of interference power distribution on the secrecy performances.

Fig. 11 compares the secrecy performances of the three selection criteria versus MER, where $N = 4$, $M = 3$ and the total interference power P_{IA} is set to 10 dB. The un-equal interference power distribution with $P_{I_1} = 7$, $P_{I_2} = 2$ and $P_{I_3} = 1$ is used. For comparison, we also present the simulated SOP result of the relay selection scheme in [22]. As observed from Fig. 11, we find that criterion I outperforms criterion II by achieving lower secrecy outage probability, since the former employs the instantaneous information of interfering links in the relay selection. We then find that criterion II outperforms criterion III, since the former incorporates different impact from the two hops into the network security. Furthermore, the selection scheme in [28] achieves higher secrecy outage probability than the three selection investigated in this work. This is because that the selection scheme proposed in [28] is a partial relay selection scheme that relies on the second-hop main channel only, for the sake of low complexity.

Fig. 12 illustrates the secrecy outage probabilities of the

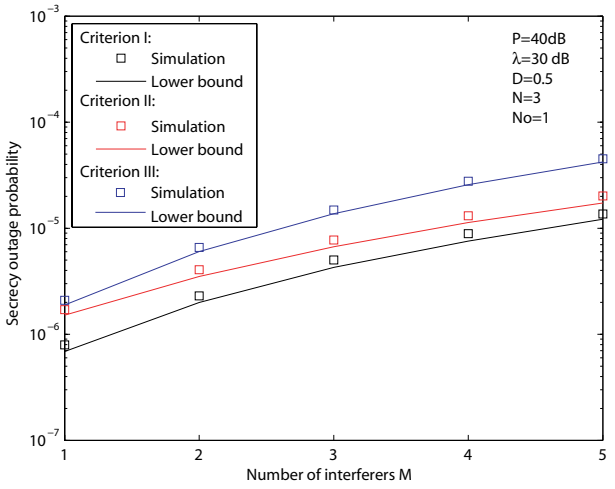

Fig. 12. Impact of the number of interferers on the secrecy performance.

three selection criteria with respect to the number of interferers M, where $N = 3$, $P = 40$ dB and $\lambda = 30$ dB. The number of interferers varies from 1 to 5, and each interferer has the equal transmit power of 3 dB. From this figure, we find that for different number of interferers, criterion I outperforms criterion II, and criterion II outperforms criterion III, which is in accordance with the results in Fig. 11. Moreover, the network secrecy performance becomes worse when M increases, since more interferers deteriorate the forwarding ability of relays.

VI. Conclusions

In this paper, we studied the communication security of multi-AF relay networks with co-channel interference. A novel lower bound expression was developed for the network secrecy outage probability, and then three selection criteria were presented to select the best relay among multiple ones, in order to deal with the co-channel interference and wiretap. For each criterion, we derived an analytical lower bound on SOP and also provided an asymptotic expression in the high MER region. From this expression, we found that each criterion achieves the full secrecy diversity order, and the interference power distribution affects the SOP of criterion II and III. Simulations and numerical results were presented to validate the proposed studies and verify the obtained insights on the system.

Appendix A
Proof of Theorem 1

The CDF of $\theta_n = \min\left(\frac{u_n}{(\gamma_s-1)(1+z_n)}, \frac{\tilde{P}_r+v_{1n}}{\gamma_s}\right)$ is given by

$$F_{\theta_n}(\theta) = \Pr\left[\min\left(\frac{u_n}{(\gamma_s-1)(1+z_n)}, \frac{\tilde{P}_r+v_{1n}}{\gamma_s}\right) \le \theta\right] \tag{A.1}$$

$$= 1 - \Pr\left[\frac{u_n}{(\gamma_s-1)(1+z_n)} > \theta, \frac{\tilde{P}_r+v_{1n}}{\gamma_s} > \theta\right]. \tag{A.2}$$

Since v_{1n} is independent of u_n and z_n, we can further write $F_{\theta_n}(\theta)$ as

$$F_{\theta_n}(\theta) = 1 - \Pr\left[u_n > (\gamma_s-1)(1+z_n)\theta\right] \times \Pr\left[v_{1n} > (\gamma_s\theta - \tilde{P}_r)\right] \tag{A.3}$$

$$= 1 - \left[\int_0^\infty \int_{(\gamma_s-1)(1+z_n)\theta}^\infty f_{u_n}(u_n) f_{z_n}(z_n) du_n dz_n\right] \times \int_{\gamma_s\theta-\tilde{P}_r}^\infty f_{v_{1n}}(v) dv. \tag{A.4}$$

By applying the PDFs of u_n, z_n and v_{1n} into the above equation and then solving the integral, we can obtain the CDF of θ_n as

$$F_{\theta_n}(\theta) = 1 - e^{\frac{1}{\tilde{P}\beta_1} - \left(\frac{\gamma_s}{\beta_1} + \frac{\gamma_s-1}{\alpha}\right)\theta} \sum_{(i,j)} \chi_{i,j} \left[1 + \frac{\theta(\gamma_s-1)\varepsilon\tilde{P}_{I<i>}}{\alpha}\right]^{-j}. \tag{A.5}$$

Since θ_n is independent of each other, we can write the CDF of $\theta_{n^*} = \max_{1\le n\le N} \theta_n$ by using the order statistics as,

$$F_{\theta_{n^*}}(\theta) = \left[1 - e^{\frac{1}{\tilde{P}\beta_1} e^{-\left(\frac{\gamma_s}{\beta_1} + \frac{\gamma_s-1}{\alpha}\right)\theta} \widetilde{\sum_{(i,j)}} \chi_{i,j}} \times \left[1 + \frac{(\gamma_s-1)\varepsilon\tilde{P}_{I<i>}}{\alpha}\theta\right]^{-j}\right]^N \tag{A.6}$$

$$= 1 - \sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} e^{\frac{n}{\tilde{P}\beta_1}} e^{-\left(\frac{\gamma_s}{\beta_1} + \frac{\gamma_s-1}{\alpha}\right)n\theta} \times \left[\widetilde{\sum_{(i,j)}} \chi_{i,j} \left[1 + \frac{(\gamma_s-1)\varepsilon\tilde{P}_{I<i>}}{\alpha}\theta\right]^{-j}\right]^n. \tag{A.7}$$

By applying [24, eq. (2.102)] into the above equation, we can arrive at the CDF of $F_{\theta_{n^*}}(\theta)$, as shown in (26) of Theorem 1.

Appendix B
Proof of Theorem 2

From the selection criterion in (32), we now compute the CDF of u_{n^*} as

$$F_{u_{n^*}}(x) = \sum_{n=1}^{N} \Pr\left[u_n \le x, \min(u_n, \frac{v_{1n}+c_1}{c_2}) \ge \max_{1\le m\le N, m\ne n} \phi_m\right], \tag{B.1}$$

where $\phi_m = \min(u_m, \frac{v_{1m}+c_1}{c_2})$. Due to the symmetry among N relays, we can rewrite $F_{u_{n^*}}(x)$ as

$$F_{u_{n^*}}(x) = N \Pr\left[u_1 \le x, \min(u_1, \frac{v_{11}+c_1}{c_2}) \ge \phi_{m^*}\right], \tag{B.2}$$

where $\phi_{m^*} = \max_{2\le m\le N} \phi_m$. The CDF of ϕ_m is derived as

$$F_{\phi_m}(\phi) = \Pr\left[\min(u_m, \frac{v_{1m}+c_1}{c_2}) \le \phi\right] \tag{B.3}$$

$$= 1 - \Pr(u_m > \phi) \cdot \Pr(v_{1m} > c_2\phi - c_1). \tag{B.4}$$

We now consider the two cases of $0 < \phi < \frac{c_1}{c_2}$ and $\phi \ge \frac{c_1}{c_2}$, respectively. When $0 < \phi < \frac{c_1}{c_2}$, $c_2\phi - c_1 < 0$ and hence $v_{1m} > c_2\phi - c_1$ always holds. In this case, $F_{\phi_m}(\phi)$ becomes

$$F_{\phi_m}(\phi) = 1 - e^{-\frac{\phi}{\alpha}}. \tag{B.5}$$

On the other hand, when $\phi \geq \frac{c_1}{c_2}$, $c_2\phi - c_1 \geq 0$ holds, and $F_{\phi_m}(\phi)$ becomes

$$F_{\phi_m}(\phi) = 1 - e^{-\frac{\phi}{\alpha}} e^{-\frac{c_2\phi - c_1}{\beta_1}}. \tag{B.6}$$

From the above CDF of ϕ_m, we can write the CDF of ϕ_{m^*} as

$$F_{\phi_{m^*}}(\phi) = \begin{cases} (1 - e^{-\frac{\phi}{\alpha}})^{N-1} = \sum_{n=0}^{N-1} \binom{N-1}{n} (-1)^n e^{-\frac{n\phi}{\alpha}}, \\ \qquad 0 < \phi < \frac{c_1}{c_2} \\ (1 - e^{-\frac{\phi}{\alpha}} e^{-\frac{c_2\phi - c_1}{\beta_1}})^{N-1} = \sum_{n=0}^{N-1} \binom{N-1}{n} \\ \times (-1)^n e^{\frac{nc_1}{\beta_1}} e^{-\frac{n\phi}{\zeta}}, \quad \phi \geq \frac{c_1}{c_2} \end{cases},$$

where ζ is defined in (35). From (B.2), we can further write $F_{u_{n^*}}(x)$ as

$$F_{u_{n^*}}(x) = N \int_0^{\frac{c_1}{c_2}} f_{\phi_{m^*}}(\phi) \int_\phi^x f_{u_1}(u_1) du_1 d\phi + N \int_{\frac{c_1}{c_2}}^\infty f_{\phi_{m^*}}(\phi) \Big[\int_\phi^x f_{u_1}(u_1) du_1 \cdot \int_{c_2\phi - c_1}^\infty f_{v_1}(v_1) dv_1 \Big] d\phi. \tag{B.7}$$

By applying the distributions of ϕ_{m^*}, u_1 and v_1 into the above equation, and then solving the integral, we can arrive at the CDF of u_{n^*}, as shown in (33) of Theorem 2. Similarly, we can obtain the CDF of v_{1n^*}, as shown in Theorem 2. In this way, we have completed the proof of Theorem 2.

REFERENCES

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[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] 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] 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.

[7] 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.

[8] 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.

[9] S. Jin, X. Liang, K.-K. Wong, X. Gao, and Q. Zhu, "Ergodic rate analysis for multipair massive MIMO two-way relay networks," *IEEE Trans. Wireless Commun.*, vol. 3, no. 14, pp. 1480–1491, Mar. 2015.

[10] 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.

[11] 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.

[12] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State-of-the-art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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

[19] 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.

[20] 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.

[21] K. W. Sowerhy and A. G. Williamson, "Outage probability calculations for mobile radio systems with multiple interferers," *Elec. Lett.*, vol. 24, no. 17, pp. 1073–1075, Aug. 1988.

[22] J. H. Winter, "Optimum combining in digital mobile radio with cochannel interference," *IEEE J. Select. Areas Commun.*, vol. 2, no. 4, pp. 528–539, July 1984.

[23] A. Shah and A. M. Haimovich, "Performance analysis of optimum combining in wireless communications with Rayleigh fading and cochannel interference," *IEEE Trans. Commun.*, vol. 46, no. 4, pp. 473–479, Apr. 1998.

[24] G. Zhu, C. Zhong, H. A. Suraweera, Z. Zhang, and C. Yuen, "Outage probability of dual-hop multiple antenna AF systems with linear processing in the presence of co-channel interference," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 2308–2321, Apr. 2014.

[25] G. Zhu, C. Zhong, H. A. Suraweera, Z. Zhang, C. Yuen, and R. Yin, "Ergodic capacity comparison of different relay precoding schemes in dual-hop af systems with co-channel interference," *IEEE Trans. Commun.*, vol. 62, no. 7, pp. 2314–2328, July 2014.

[26] 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.

[27] J. M. Moualeu, W. Hamouda, and F. Takawira, "Outage analysis of relay selection in AF with outdated channel information in the presence of co-channel interference," in *Proc. IEEE WCNC*, New Orleans, LA, Mar. 2015, pp. 498–503.

[28] T. T. Duy, T. Q. Duong, T. L. Thanh, and V. N. Q. Bao, "Secrecy performance analysis with relay selection methods under impact of co-channel interference," *IET Commun.*, vol. 9, no. 11, pp. 1427–1435, July 2015.

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

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

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

[32] D. S. Michalopoulos, H. A. Suraweera, and G. K. Karagiannidis, "Amplify-and-forward relay selection with outdated channel estimates," *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1278–1290, May 2012.

[33] S. LI and Y. Fan, "An adaptive control with optimal disturbances rejection," *Science China*, vol. 55, no. 7, pp. 1704–1714, July 2012.

[34] S. Li, "Robust adaptive control of uncertain systems with guaranteed robust stability and asymptotic performance," *International Journal of Systems Science*, vol. 42, no. 6, pp. 1007–1022, June 2011.

[35] H. Boche and E. A. Jorswieck, "On Schur-convexity of expectation of weighted sum of random variables with applications," *J. Inequalities Pure App. Math.*, vol. 5, no. 2, pp. 1–14, 2004.

Lisheng Fan received the bachelor and master degrees from Fudan University and Tsinghua University, China, in 2002 and 2005, respectively, both from the Department of Electronic Engineering. He received the Ph.D degree from the Department of Communications and Integrated Systems of Tokyo Institute of Technology, Japan, in 2008. He is now a Professor with GuangZhou University. His research interests span in the areas of wireless cooperative communications, physical-layer secure communications, interference modeling, and system performance evaluation. Lisheng Fan has published many papers in international journals such as IEEE Transactions on Wireless Communications, IEEE Transactions on Communications, IEEE Transactions on Information Theory, as well as papers in conferences such as IEEE ICC, IEEE Globecom, and IEEE WCNC. He is a guest editor of EURASIP Journal on Wireless Communications and Networking, and served as the chair of Wireless Communications and Networking Symposium for Chinacom 2014. He has also served as a member of Technical Program Committees for IEEE conferences such as Globecom, ICC, WCNC, and VTC.

Xianfu Lei was born in December 1981. From 2012 to 2014, he worked as a research fellow in the Department of Electrical and Computer Engineering at Utah State University, USA. Since 2015, he has been an associate professor with the School of Information Science and Technology at Southwest Jiaotong University, China. His current research interests include 5G wireless communications, cooperative communications, cognitive radio, physical layer security, energy harvesting, etc. He has published nearly 70 journal and conference papers on these topics. He currently serves on the Editorial Board of IEEE Communications Letters, IEEE Access, Wireless Communications and Mobile Computing, Security and Communication Networks, KSII Transactions on Internet and Information Systems, and Telecommunication Systems. He has served as a Guest Editor of the special issue on Non-orthogonal Multiple Access for 5G Systems in IEEE Journal on Selected Areas in Communications in 2016 as well as the Lead Guest Editor of the special issue on Energy Harvesting Wireless Communications in EURASIP Journal on Wireless Communications and Networking in 2014. He has also served as TPC member for major international conferences such as IEEE ICC, IEEE GLOBECOM, IEEE WCNC, IEEE VTC Spring/Fall, IEEE PIMRC, etc. Dr. Lei received an Exemplary Reviewer Certificate of the IEEE Communications Letters and an Exemplary Reviewer Certificate of the IEEE Wireless Communications Letters in 2013.

Nan Yang (S'09–M'11) received the B.S. degree in electronics from China Agricultural University in 2005, and the M.S. and Ph.D. degrees in electronic engineering from the Beijing Institute of Technology in 2007 and 2011, respectively. He is currently a Future Engineering Research Leadership Fellow and Lecturer in the Research School of Engineering at the Australian National University. Prior to this, he was a Postdoctoral Research Fellow the University of New South Wales (UNSW) from 2012 to 2014, a Postdoctoral Research Fellow at the Commonwealth Scientific and Industrial Research Organization from 2010 to 2012, and a visiting Ph.D. student at UNSW from 2008 to 2010. He received the Exemplary Reviewer Award of the IEEE Transactions on Communications and the Top Reviewer Award from the IEEE Transactions on Vehicular Technology in 2015, the IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award and the Exemplary Reviewer Award of the IEEE Wireless Communications Letters in 2014, the Exemplary Reviewer Award of the IEEE Communications Letters in 2013 and 2012, and the Best Paper Award at the IEEE 77th Vehicular Technology Conference in 2013. He is currently serving in the Editorial Board of the IEEE Transactions on Vehicular Technology and the Transactions on Emerging Telecommunications Technologies. His general research interests lie in the areas of communications theory and signal processing, with specific interests in heterogeneous networks, massive multi-antenna systems, millimeter wave communications, cyber-physical security, and molecular communications.

Trung Q. Duong (S'05, M'12, SM'13) received his Ph.D. degree in Telecommunications Systems from Blekinge Institute of Technology (BTH), Sweden in 2012. Since 2013, he has joined Queen's University Belfast, UK as a Lecturer (Assistant Professor). His current research interests include physical layer security, energy-harvesting communications, cognitive relay networks. He is the author or co-author of more than 200 technical papers published in scientific journals (105 articles) and presented at international conferences.

Dr. Duong currently serves as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE COMMUNICATIONS LETTERS, IET COMMUNICATIONS, WILEY TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES, and ELECTRONICS LETTERS. He has also served as the Guest Editor of the special issue on some major journals including IEEE JOURNAL IN SELECTED AREAS ON COMMUNICATIONS, IET COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS MAGAZINE, IEEE COMMUNICATIONS MAGAZINE, EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, EURASIP JOURNAL ON ADVANCES SIGNAL PROCESSING. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, IEEE International Conference on Communications (ICC) 2014. He is the recipient of prestigious Royal Academy of Engineering Research Fellowship (2015-2020)

George K. Karagiannidis (M'96-SM'03-F'14) was born in Pithagorion, Samos Island, Greece. He received the University Diploma (5 years) and PhD degree, both in electrical and computer engineering from the University of Patras, in 1987 and 1999, respectively. From 2000 to 2004, he was a Senior Researcher at the Institute for Space Applications and Remote Sensing, National Observatory of Athens, Greece. In June 2004, he joined the faculty of Aristotle University of Thessaloniki, Greece where he is currently Professor in the Electrical & Computer Engineering Dept. and Director of Digital Telecommunications Systems and Networks Laboratory. He is also Honorary Professor at South West Jiaotong University, Chengdu, China.

His research interests are in the broad area of Digital Communications Systems with emphasis on Wireless Communications, Optical Wireless Communications, Wireless Power Transfer and Applications, Molecular Communications, Communications and Robotics and Wireless Security.

He is the author or co-author of more than 400 technical papers published in scientific journals and presented at international conferences. He is also author of the Greek edition of a book on "Telecommunications Systems" and co-author of the book "Advanced Optical Wireless Communications Systems", Cambridge Publications, 2012.

Dr. Karagiannidis has been involved as General Chair, Technical Program Chair and member of Technical Program Committees in several IEEE and non-IEEE conferences. In the past he was Editor in IEEE Transactions on Communications, Senior Editor of IEEE Communications Letters, Editor of the EURASIP Journal of Wireless Communications & Networks and several times Guest Editor in IEEE Selected Areas in Communications. From 2012 to 2015 he was the Editor-in Chief of IEEE Communications Letters.

Dr. Karagiannidis has been selected as a 2015 Thomson Reuters Highly Cited Researcher and he Listed in Thomson Reuters 2015 World's Most Influential Scientific Minds.