Secure Multiuser Multiple Amplify-and-Forward Relay Networks in Presence of Multiple Eavesdroppers

Lisheng Fan[1,2], Xianfu Lei[3], Trung Q. Duong[4], Maged Elkashlan[5], and George K. Karagiannidis[6,7]
[1]Department of Electronic Engineering, Shantou University, Shantou, China (email: lsfan@stu.edu.cn)
[2] National Mobile Communications Research Laboratory, Southeast University
[3]Department of Electrical & Computer Engineering, Utah State University, USA (email: xflei81@gmail.com)
[4]Queen's University Belfast, UK (email: trung.q.duong@qub.ac.uk)
[5]Queen Mary University of London, London, UK (email: maged.elkashlan@qmul.ac.uk)
[6]Department of Electrical and Computer Engineering, Khalifa University, PO Box 127788, Abu Dhabi, UAE
[7] Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, 54 124, Thessaloniki, Greece
(e-mail: geokarag@ieee.org)

***Abstract*—In this paper, we study the information-theoretical security of a downlink multiuser cooperative relaying network with multiple intermediate amplify-and-forward (AF) relays, where there exist multiple eavesdroppers which can overhear the message. To prevent the wiretap and strength the network security, we select one best relay and user pair, so that the selected user can receive the message from the base station assisted by the selected relay. The relay and user selection is performed by maximizing the ratio of the received signal-to-noise ratio (SNR) at the user to the eavesdroppers, which is based on both the main and eavesdropper links. For the considered system, we derive the closed-form expression of the secrecy outage probability, and provide the asymptotic expression in high main-to-eavesdropper ratio (MER) region. From the asymptotic analysis, we can find that the system diversity order is equivalent to the number of relays regardless of the number of users and eavesdroppers.**

I. Introduction

Due to the broadcast nature of wireless transmission, the eavesdroppers in wireless networks can overhear the message, which is illegal and brings out the severe issue of information security. To strength the network security, the physical layer security has been studied to implement the secure communications. Wyner firstly introduced a classical wiretap model in [1], and pointed out that there existed a secrecy data rate below which an approximately perfect secure data transmission could be achieved. Pioneered by this work, researchers have extended to analyze the secrecy performances over different fading channels [2]–[8]. In particular, Bloch *et.al* and Gopala *et.al* have studied the system secrecy capacity where the main and eavesdropper links experience independent Rayleigh flat fading [2], [3]. Jeon *et.al* and Sun *et.al* have studied the Rayleigh fading correlation between the main and eavesdropper links in [4], [5], and found out that the system secrecy performance seriously degraded with the channel correlation. In further, the authors in [6]–[8] have studied the secrecy performances over Rician and Nakagami-m fading channels.

To increase the network security of wireless transmission, user selection technique can be applied for multiuser communication systems. Luo *et.al* have considered a secure multiuser MISO-OFDMA system in [9], and performed the user selection to maximize the system secrecy data rate by exploiting the channel fluctuation among users. Besides the user selection, antenna selection technique can be used for communication systems with multiple antennas to enhance the network security. Alves *et.al* has considered the physical-layer security of a multiple-input single-output (MISO) system in [10], and studied the effect of transmit antenna selection on the system security by exploiting the channel fluctuation among antennas. For MIMO systems [11], [12], Yang *et.al* applied the transmit antenna selection to prevent the wiretap, and presented the analytical secrecy outage probability as well as the asymptotic expression with high main-to-eavesdropper ratio (MER).

Besides the selection technique, relaying technique is encouraged to incorporate into the secure communication systems [13], which provides a powerful tool for enhancing the transmission security. Some fundamental relaying protocols such as amplify-and-forward (AF) and decode-and-forward (DF) have been applied in the information-theoretical security systems [14]–[19]. Mo *et.al* studied the physical layer security of a cooperative DF relaying network in [14], and pointed out that the relay placement could affect the system secrecy outage probability substantially. The authors in [15]–[17] studied the information-theoretical security of cooperative networks with multiple DF relays, and applied relay selection to enhance the system security by exploiting the channel fluctuation among relays. For relay networks with multiple AF relays [18], Yang *et.al* proposed the secure beamforming to prevent the wiretap caused by multiple eavesdroppers. Recently, Zou *et.al* in [19] studied the physical layer security of the cooperative relaying networks with multiple AF relays, and applied the relay selection to improve the system intercept probability. However, the intercept probability is a special case of the system secrecy outage probability when the target secrecy date rate is set to zero, and it only relies on the second-hop relaying channels of the main and eavesdropper links. In other words, the first-hop relaying channels are not involved in the relay selection criterion [19], which simplifies the selection criterion

978-1-4799-3512-3/14/$31.00 ©2014 IEEE

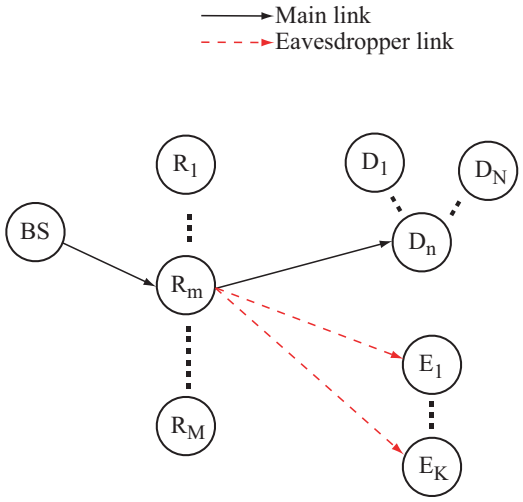

Fig. 1. Two-phase multiuser multi-relay cooperative network with multiple eavesdroppers.

and related performance analysis substantially. So far, no prior work has studied the effect of multiple AF relay selection on the secrecy outage probability of relaying networks, to the best of our knowledge.

In this paper, we consider a downlink multiuser cooperative relaying network, where there exist multiple intermediate AF trusted relays which can assist the data transmission. There are multiple eavesdroppers in the network which can overhear the message and bring out the issue of information security. In order to enhance the system security, we select one best relay and user pair by maximizing the ratio of the received signal-to-noise ratio (SNR) at the user to the eavesdroppers. We firstly derive the closed-form expression for the secrecy outage probability. We then provide the asymptotic secrecy outage probability in high MER region, from which we can find that the system diversity order is equal to number of relays, regardless of the number of users and eavesdroppers. Numerical and simulation results are illustrated 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 [20], and ${}_2F_1(\cdot)$ is the Gauss hypergeometric function [20]. 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. 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. To prevent the wiretap, we select the best relay and user pair (R_{m^*}, D_{n^*}) to enhance the system security performance. All nodes in the network are equipped with a single antenna due to size limitation, and they operate in a half-duplex mode.

Suppose that the m-th relay and n-th user have been selected for data transmission, and P 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

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

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

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

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

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

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 $\mathrm{R}_m\rightarrow\mathrm{D}_n$ and $\mathrm{R}_m\rightarrow\mathrm{E}_k$ 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)–(4), the received SNRs at D_n and E_k are obtained as

$$\mathsf{SNR}_{m,n}^{\mathsf{D}} = \frac{P P_R u_m v_{m,n}}{P u_m + P_R v_{m,n} + 1}, \tag{5}$$
$$\mathsf{SNR}_{m,k}^{\mathsf{E}} = \frac{P P_R u_m w_{m,k}}{P u_m + P_R w_{m,k} + 1}, \tag{6}$$

where $u_m = |h_{BS,R_m}|^2$, $v_{m,n} = |h_{R_m,D_n}|^2$ and $w_{m,k} = |h_{R_m,E_k}|^2$ denote the instantaneous channel gains of the BS$\rightarrow\mathrm{R}_m$, $\mathrm{R}_m\rightarrow\mathrm{D}_n$ and $\mathrm{R}_m\rightarrow\mathrm{E}_k$ links, respectively.

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

$$P_{out,m,n} = \Pr\left[\frac{1}{2}\log_2(1+\mathsf{SNR}_{m,n}^{\mathsf{D}}) - \frac{1}{2}\log_2(1+\max_{k=1,\cdots,K}\mathsf{SNR}_{m,k}^{\mathsf{E}}) < R_s\right] \tag{7}$$
$$= \Pr\left(\frac{1+\mathsf{SNR}_{m,n}^{\mathsf{D}}}{1+\max_{k=1,\cdots,K}\mathsf{SNR}_{m,k}^{\mathsf{E}}} < \gamma_{th}\right), \tag{8}$$

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

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,

$$(m^*, n^*) = \arg \min_{m=1,\cdots,M} \min_{n=1,\cdots,N} P_{out,m,n} \quad (9)$$

$$= \arg \min_{m=1,\cdots,M} \min_{n=1,\cdots,N} \Pr\left(\frac{1+\mathsf{SNR}^{\mathsf{D}}_{m,n}}{1+\max_{k=1,\cdots,K}\mathsf{SNR}^{\mathsf{E}}_{m,k}} < \gamma_{th}\right). \quad (10)$$

Since $\frac{xy}{x+y+1}$ increases with x when $x \geq 0$ and $y \geq 0$, we can rewrite $\max_{k=1,\cdots,K}\mathsf{SNR}^{\mathsf{E}}_{m,k}$ as

$$\max_{k=1,\cdots,K}\mathsf{SNR}^{\mathsf{E}}_{m,k} = \max_{k=1,\cdots,K}\left(\frac{PP_R u_m w_{m,k}}{Pu_m + P_R w_{m,k} + 1}\right) \quad (11)$$

$$= \frac{PP_R u_m w_m}{Pu_m + P_R w_m + 1}, \quad (12)$$

where $w_m = \max_{k=1,\cdots,K} w_{m,k}$ denotes the largest channel gain among the K eavesdropper links. In high SNR region, it holds that

$$\frac{1+\mathsf{SNR}^{\mathsf{D}}_{m,n}}{1+\max_{k=1,\cdots,K}\mathsf{SNR}^{\mathsf{E}}_{m,k}} \simeq \frac{\mathsf{SNR}^{\mathsf{D}}_{m,n}}{\max_{k=1,\cdots,K}\mathsf{SNR}^{\mathsf{E}}_{m,k}} \quad (13)$$

$$\simeq \frac{PP_R u_m v_{m,n}/(Pu_m + P_R v_{m,n})}{PPR u_m w_m/(Pu_m + P_R w_m)} \quad (14)$$

$$= \frac{(u_m + \eta w_m)v_{m,n}}{(u_m + \eta v_{m,n})w_m}, \quad (15)$$

where $\eta = \frac{P_R}{P}$ is the transmit power ratio of the base station to the relay. From (15), we can approximate $P_{out,m,n}$ as

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

$$= \Pr\left[u_m v_{m,n} < (\gamma_{th}u_m + (\gamma_{th}-1)\eta v_{m,n})w_m\right] \quad (17)$$

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

We then devise a relay and user pair selection criterion as

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

From (16)–(18), we find that the above criterion is equivalent to maximizing the received SNR ratio at 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.

In the following, we will first derive analytical expression 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 secrecy outage probability as well as the asymptotic expression for the considered system. From (18), the system secrecy outage probability with selected R_{m^*} and D_{n^*} for high transmit power is given by

$$P_{out,m^*,n^*} \simeq \Pr(Z_{m^*,n^*} < w_{m^*}), \quad (20)$$

with

$$Z_{m,n} = \frac{u_m v_{m,n}}{\gamma_{th}u_m + (\gamma_{th}-1)\eta v_{m,n}}. \quad (21)$$

A. Analytical secrecy outage probability

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 first need to study the secrecy outage probability for a given relay R_m with only user selection.

Note that $Z_{m,n}$ in (21) increases with $v_{m,n}$, the best user $\mathrm{D}_{n^*_m}$ conditioned on a given relay R_m should be selected to maximize $v_{m,n}$,

$$n^*_m = \arg \max_{n=1,\cdots,N} v_{m,n}. \quad (22)$$

The probability density function (PDF) of v_{m,n^*_m} is

$$f_{v_{m,n^*_m}}(v) = \sum_{n=1}^{N}(-1)^{n-1}\binom{N}{n}\frac{n}{\beta}e^{-\frac{nv}{\beta}}. \quad (23)$$

We now extend to analyze the cumulative density function (CDF) of Z_{m,n^*_m} as

$$F_{Z_{m,n^*_m}}(z) = \Pr\left(\frac{u_m v_{m,n^*_m}}{\gamma_{th}u_m + (\gamma_{th}-1)\eta v_{m,n^*_m}} < z\right) \quad (24)$$

$$= \Pr\left[u_m(v_{m,n^*_m} - \gamma_{th}z) < (\gamma_{th}-1)\eta v_{m,n^*_m}z\right] \quad (25)$$

$$= \Pr(v_{m,n^*_m} \leq \gamma_{th}z) + \Pr\left(v_{m,n^*_m} > \gamma_{th}z, u_m < \frac{(\gamma_{th}-1)\eta v_{m,n^*_m}z}{v_{m,n^*_m} - \gamma_{th}z}\right). \quad (26)$$

By applying the PDFs of u_m and v_{m,n^*_m} into the above equation, we obtain the CDF of Z_{m,n^*_m} as

$$F_{Z_{m,n^*_m}}(z) = 1 - \sum_{n=1}^{N}(-1)^{n-1}\binom{N}{n}b_n e^{-(\frac{n\gamma_{th}}{\beta} + \frac{\eta(\gamma_{th}-1)}{\alpha})z} \times z\mathcal{K}_1(b_n z), \quad (27)$$

where we apply [20, eq. (3.324)] and

$$b_n = \sqrt{\frac{4n\eta\gamma_{th}(\gamma_{th}-1)}{\alpha\beta}}. \quad (28)$$

From (27), we derive the closed-form expression of the secrecy outage probability with the m-th relay for large transmit power as

$$P_{out,m,n_m^*} \simeq \Pr(Z_{m,n_m^*} < w_m) \quad (29)$$

$$= \int_0^\infty f_{w_m}(w) F_{Z_{m,n_m^*}}(w) dw, \quad (30)$$

where $f_{w_m}(w) = \sum_{k=1}^{K}(-1)^{k-1}\binom{K}{k}\frac{k}{\varepsilon}e^{-\frac{kw}{\varepsilon}}$ is the PDF of w_m. By applying [20, eq. (6.621.3)], we can obtain the secrecy outage probability with the m-th relay as

$$P_{out,m,n_m^*} \simeq 1 - \sum_{k=1}^{K}\sum_{n=1}^{N}(-1)^{n+k}\binom{K}{k}\binom{N}{n}\frac{16kb_n^2}{3\varepsilon(b_n+c_{n,k})^3} \times {}_2F_1(3,\frac{3}{2},\frac{5}{2};\frac{c_{n,k}-b_n}{c_{n,k}+b_n}), \quad (31)$$

with

$$c_{n,k} = \frac{k}{\varepsilon} + \frac{n\gamma_{th}}{\beta} + \frac{\eta(\gamma_{th}-1)}{\alpha}. \quad (32)$$

As mentioned above, 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 analytical secrecy outage probability with high transmit power as

$$P_{out,m^*,n^*} \simeq \left[1 - \sum_{k=1}^{K}\sum_{n=1}^{N}(-1)^{n+k}\binom{K}{k}\binom{N}{n} \times \frac{16kb_n^2}{3\varepsilon(b_n+c_{n,k})^3}\ {}_2F_1(3,\frac{3}{2},\frac{5}{2};\frac{c_{n,k}-b_n}{c_{n,k}+b_n})\right]^M. \quad (33)$$

B. Asymptotic secrecy outage probability

In this subsection, we derive the asymptotic expression of the system secrecy outage probability with high MER, from which we obtain the system diversity order. We firstly consider the lower and upper bounds of Z_{m,n_m^*} as

$$0.5\min\left(\frac{u_m}{(\gamma_{th}-1)\eta}, \frac{v_{m,n_m^*}}{\gamma_{th}}\right) \le Z_{m,n_m^*} \le \min\left(\frac{u_m}{(\gamma_{th}-1)\eta}, \frac{v_{m,n_m^*}}{\gamma_{th}}\right). \quad (34)$$

The above bounds can be written in a unified form as

$$Z^b_{m,n_m^*} = \delta\min\left(\frac{u_m}{(\gamma_{th}-1)\eta}, \frac{v_{m,n_m^*}}{\gamma_{th}}\right), \quad (35)$$

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 1: The asymptotic expression of P_{out,m,n_m^*} with high MER is given by

$$P^{asy}_{out,m,n_m^*} = \begin{cases} \left[\frac{(\gamma_{th}-1)\eta\beta}{\delta\alpha} + \frac{\gamma_{th}}{\delta}\right]\left(\sum_{k=1}^{K}\frac{1}{k}\right)\frac{1}{\lambda}, & \text{If } N=1 \\ \frac{(\gamma_{th}-1)\eta\beta}{\delta\alpha}\left(\sum_{k=1}^{K}\frac{1}{k}\right)\frac{1}{\lambda}, & \text{If } N\ge 2 \end{cases}, \quad (36)$$

where $\lambda = \frac{\beta}{\varepsilon}$ denotes the MER [19], 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 A.*

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

$$P^{asy}_{out,m^*,n^*} = \begin{cases} \left[\left(\frac{(\gamma_{th}-1)\eta\beta}{\alpha} + \gamma_{th}\right)\left(\sum_{k=1}^{K}\frac{1}{k}\right)\right]^M \times\frac{1}{(\delta\lambda)^M}, & \text{If } N=1 \\ \left(\frac{(\gamma_{th}-1)\eta\beta}{\alpha}\left(\sum_{k=1}^{K}\frac{1}{k}\right)\right)^M\frac{1}{(\delta\lambda)^M}, & \text{If } N\ge 2 \end{cases}, \quad (37)$$

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 is equal to M. Hence, we can conclude from the squeeze theorem that the diversity order 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.

V. 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. Without loss of generality, we set the average channel gains of main links to unity with $\alpha = \beta = 1$. In addition, we set a high transmit power at the base station with $P = 40$ dB, since we focus on the effect of MER on the system secrecy outage probability. The target secrecy data rate R_s is set to 0.5 bps/Hz, so that the associated secrecy SNR threshold is equal to 2.

Fig. 2 demonstrates the effect of the number of relays on the system secrecy outage probability versus MER, where $R_s = 0.5$ bps/Hz, $N = 2$, $K = 2$, and M varies from 1 to 3. For comparison, we plot the simulation results of the proposed selection criterion as well as the optimal selection performed in (10). We also plot the asymptotic results which

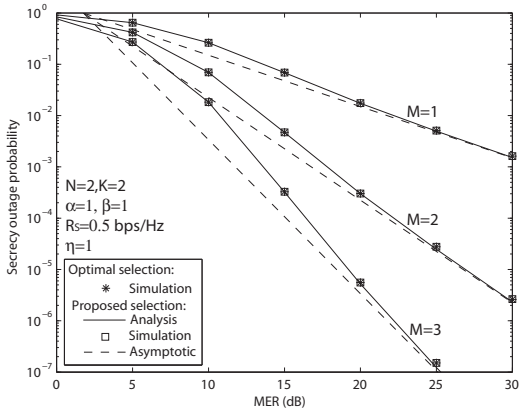

Fig. 2. Effect of number of relays on the secrecy outage probability versus MER.

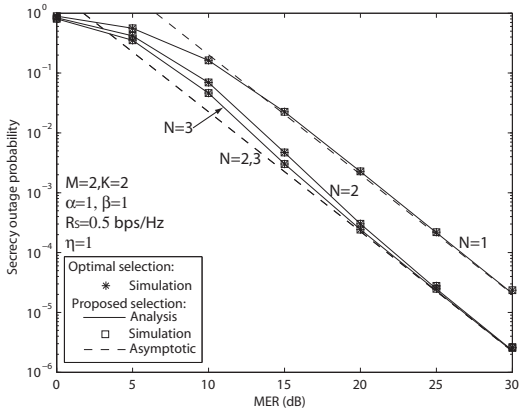

Fig. 3. Effect of number of users on the secrecy outage probability versus MER.

are from the lower bound of secrecy outage probability with $\delta = 1$ [1]. As observed from the figure, we can find that for different values of MER and M, the analytical result is close to the simulation one in whole MER region, which validates the derived analytical expressions of the secrecy outage probability in (33). In addition, the asymptotic result converges to the exact value at high MER, which verifies the derived asymptotic expression. Moreover, the slopes of the curve of the secrecy outage probability are in parallel with M, which verifies the system diversity order of M.

Fig. 3 shows 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. We find from this figure 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

[1] In this work, we do not plot the asymptotic results from the upper bound of the secrecy outage probability, since one can verify that the upper bound is loose while the lower bound is tight in the high MER region.

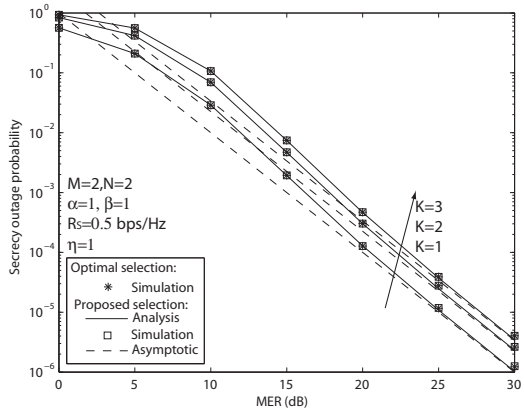

Fig. 4. Effect of number of eavesdroppers on the secrecy outage probability versus MER.

indicates that users have no impact on the system diversity order.

Fig. 4 illustrates 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 3. As observed from Fig. 4, 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 share the same slope, indicating that the system diversity order is independent of the number of eavesdroppers. Moreover, the analytical result matches well with the simulation for different values of K, and the asymptotic result converges with the exact in high MER region. This further verifies the derived analytical expression for the secrecy outage probability as well as the asymptotic expression.

VI. Conclusions

In this paper, we proposed relay selection to secure the physical layer communication in multiuser cooperative relay networks with multiple AF relays, against the wiretap channel with multiple eavesdroppers. In order to strengthen the network security, we selected the best relay and user pair by maximizing the SNR ratio at the user to eavesdroppers. We derived analytical expression 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 number of users and eavesdroppers.

VII. Acknowledgement

This work was supported by the National Basic Research Program of China (973 Program No.2012CB316100), NSF of China (No. 61372129/61002015/61032002), NSF of Guangdong Province, China (No. S2012010010062), the 111 Project (No.111-2-14), 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).

APPENDIX A
PROOF OF THEOREM 1

For Z^b_{m,n^*_m} in (35), we derive its CDF as

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

$$= 1 - \Pr\left(u_m \geq \frac{(\gamma_{th}-1)\eta z}{\delta}\right) \times \Pr\left(v_{m,n^*_m} \geq \frac{\gamma_{th} z}{\delta}\right). \quad \text{(A.2)}$$

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

$$F_{Z^b_{m,n^*_m}}(z) = 1 - \sum_{n=1}^{N}(-1)^{n-1}\binom{N}{n} e^{-[\frac{(\gamma_{th}-1)\eta}{\delta\alpha} + \frac{\eta\gamma_{th}}{\delta\beta}]z}. \quad \text{(A.3)}$$

Similar to eqs. (29)-(30), we can obtain the asymptotic expression of P_{out,m,n^*_m} as

$$P_{out,m,n^*_m} \simeq \sum_{k=1}^{K}(-1)^{k-1}\binom{K}{k}\frac{k}{\varepsilon}\int_0^\infty F_{Z^b_{m,n^*_m}}(w) e^{-\frac{kw}{\varepsilon}} dw \quad \text{(A.4)}$$

$$= 1 - \sum_{k=1}^{K}\sum_{n=1}^{N}(-1)^{n+k}\binom{K}{k}\binom{N}{n}\frac{k}{\varepsilon} \times \int_0^\infty e^{-[\frac{k}{\varepsilon} + \frac{(\gamma_{th}-1)\eta}{\delta\alpha} + \frac{\eta\gamma_{th}}{\delta\beta}]w} dw \quad \text{(A.5)}$$

$$= 1 - \sum_{k=1}^{K}\sum_{n=1}^{N}(-1)^{n+k}\binom{K}{k}\binom{N}{n} \times \left(1 + \frac{(\gamma_{th}-1)\eta}{k\delta}\frac{\varepsilon}{\alpha} + \frac{n\gamma_{th}}{k\delta}\frac{\varepsilon}{\beta}\right)^{-1}. \quad \text{(A.6)}$$

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

$$P^{asy}_{out,m,n^*_m} = \frac{1}{\delta}\sum_{k=1}^{K}\sum_{n=1}^{N}(-1)^{n+k}\binom{K}{k}\binom{N}{n} \times [\frac{(\gamma_{th}-1)\eta}{k}\frac{\varepsilon}{\alpha} + \frac{n\gamma_{th}}{k}\frac{\varepsilon}{\beta}] \quad \text{(A.7)}$$

$$= \begin{cases} \left[\frac{(\gamma_{th}-1)\eta\beta}{\delta\alpha} + \frac{\gamma_{th}}{\delta}\right]\left(\sum_{k=1}^{K}\frac{1}{k}\right)\frac{1}{\lambda}, \text{ If } N = 1 \\ \frac{(\gamma_{th}-1)\eta\beta}{\delta\alpha}\left(\sum_{k=1}^{K}\frac{1}{k}\right)\frac{1}{\lambda}, \text{ If } N \geq 2 \end{cases} \quad \text{(A.8)}$$

where we apply [20, eq. (0.154.2)] and [20, eq. (0.155.4)] in the last equality. Hence, the proof of Theorem 2 is completed.

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] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

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

[18] 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.

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

,