Joint Antenna and User Selection for Untrusted Relay Networks

Bingtao He*, Qiang Ni†, Jian Chen*, Long Yang* and Lu Lv*
*State Key Laboratory of Integrated Services Networks, Xidian University, P. R. China
E-mail:{hebingtao, lulv}@stu.xidian.edu.cn, jianchen@mail.xidian.edu.cn, lyang@xidian.edu.cn
†School of Computing and Communications, Lancaster University, UK
E-mail: q.ni@lancaster.ac.uk

***Abstract*—In this paper, we investigate secure communication for an untrusted relay network, in which a source equipped with N_S antennas communicates to M users with the help of an untrusted relay. To protect the data confidentially while concurrently relying on the untrusted relays, joint antenna and user selection scheme has been proposed with the aid of cooperative jamming. Furthermore, the impacts of both the number of antennas and the number of users on system performance are studied. Both the secrecy outage probability (SOP) and ergodic secrecy rate (ESR) are derived in closed form, and the secrecy diversity order of the considered networks is proved to be $\min(N_S, M/2)$. Compared with the traditional single antenna and single source-destination scenario, both SOP and ESR can achieve a great improvement owing to the mutual effects of antenna diversity and user diversity. In addition, numerical results are conducted to demonstrate the validity of the proposed scheme.**

***Index Terms*—Physical layer security, untrusted relay networks, antenna selection, user selection.**

I. Introduction

By exploiting randomness properties of wireless channels, physical layer security (PLS) has been recognized as an efficient method for the secure data transmission, which has drawn great interests on different kinds of wireless networks [1], [2]. As one of the most significate applications, secure communication for the cooperative networks is widely investigated in [3]–[6]. In these works, a friendly relay is usually used to enhance the main channel capacity [3], [4] or acts as a jammer to deteriorate the wiretap channel capacity [5], [6].

However, sometimes the relay may not have the same level of access to the information as the destination users, which may become a potential eavesdropper to decode the information signal, i.e. the relay is untrustworthy [7]. The achievable secrecy rate for the untrusted relay channel is analyzed in [8]. In [9], the authors propose the joint secure beamforming at both source and relay to achieve the secrecy rate maximization. The opportunistic transmission scheme is proposed in [10], in which the secrecy outage performance is studied. The aforementioned works [8]–[10] for the secure communication rely on the existing of the direct link between the source and destination. However, when the direct link is nonexistent, source-destination communication can be performed only by utilizing the untrusted relay, thus making the secure transmission even more challenging.

To enjoy the connectivity of the cooperation as well as keeping confidential information from leaking, destination based cooperative jamming scheme has been proposed in [11]. In [12], the optimal power allocation for data transmission and cooperative jamming has been studied, and joint source and destination precoding is designed for the MIMO untrusted relay networks in [13]. The ergodic secrecy rate (ESR) [7] and the secrecy outage probability (SOP) [14] are fully investigated for the multiple untrusted relay networks, which indicate that the secrecy performance cannot be further improved by increasing the number of untrusted relays.

In this paper, we investigate secure communication for the multi-antenna and multiuser untrusted relay networks. By taking the advantage of antenna diversity for the security enhancement [15], we propose a joint antenna and user selection scheme for the considered system. Different from [15], [16], the direct link cannot be exploited to improve the security in our considered system due to the long distance or high attenuation of the signals. Therefore, cooperative jamming is introduced to avoid the overhearing of the untrusted relay. Meanwhile, multiple destination users are considered in our work and user scheduling is investigated to further ensure the secure transmission. To evaluate the performance of the proposed scheme, we derive both the lower bound and the upper bound of SOP, asymptotic expression of SOP, and the lower bound of ESR in closed form, and some simulations are provided to validate their effectiveness. The analytical results and simulations show that, compared with the traditional single antenna and single source-destination scenario, the considered networks with the proposed scheme can achieve a great improvement on both secrecy outage performance i.e. $\min(N_S, \frac{M}{2})$, and secrecy rate performance.

II. System Model

As it is shown in Fig. 1, we consider a cooperative wireless network, in which a source node S communicates with M destination nodes with the help of an amplify-and-forward half-duplex relay R. We assume that S is equipped with an array of N_S antennas, while R and each destination user D_m, $m = 1, ..., M$, are equipped with a single antenna. Due to the long distance or high attenuation, there is no direct link between S and D_m. It is assumed that R is untrustworthy which also attempts to intercept the received signal[1]. All the channels are assumed to be quasi-static block-fading channels, where channel fading coefficients remain unchanged during a single time slot. The additive white Gaussian noise (AWGN) at each receiver is modeled as a zero-mean complex Gaussian random variable with variance N_0.

A. Transmission Protocol

In each time slot, the data transmission procedure can be described as two phases. In the first phase, S sends the m-th destination user's information signal x_m to the relay R, meanwhile, the m-th destination user sends a jamming signal w_m to R. Consider that the n-th, $n = 1, ..., N_S$, antenna is selected for this transmission, the signal received at R can be expressed as

$$y_R = \sqrt{P} h_{n,R} x_m + \sqrt{P} g_{m,R} w_m + n_R, \tag{1}$$

where P is the transmit power and each node has the same transmit power. $h_{n,R}$ and $g_{m,R}$ denote the instantaneous channels fading coefficients of the n-th antenna to R and the m-th destination user to R respectively. It assumes that $h_{n,R}$ and $g_{m,R}$ are independent, and they follow complex Gaussian distributions with zero means and different variances Ω_X and Ω_Y. n_R denotes the AWGN at the relay.

In the second phase, R forwards its received signal y_R to the selected user with the amplifying coefficient $\alpha_{n,m} = \sqrt{1/(P|h_{n,R}|^2 + P|g_{m,R}|^2 + N_0)}$. Therefore, the received signal at the selected user D_m is given by

$$y_{D_m} = \alpha_{n,m} \sqrt{P} g_{m,R} y_R + n_m, \tag{2}$$

where n_m is the noise observed by D_m. Here, $g_{m,R}$ is also used to denote the R to D_m link due to the reciprocity of channel.

Consider the eavesdropping of R, from (1), the achievable rate at R is given by

$$R_E(n,m) = \frac{1}{2} \log_2 \left(1 + \frac{\rho |h_{n,R}|^2}{\rho |g_{m,R}|^2 + 1} \right), \tag{3}$$

where $\rho = P/N_0$. Since the jamming signal w_m is sent by D_m, after the self-interference cancelation, the achievable rate at D_m is given by

$$R_D(n,m) = \frac{1}{2} \log_2 \left(1 + \frac{\rho^2 |h_{n,R}|^2 |g_{m,R}|^2}{\rho |h_{n,R}|^2 + 2\rho |g_{m,R}|^2 + 1} \right). \tag{4}$$

Above all, the secrecy rate of the system can be expressed as

$$R_S(n,m) = \left[R_D(n,m) - R_E(n,m) \right]^+. \tag{5}$$

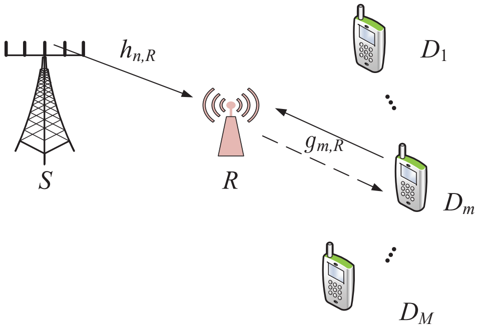

Fig. 1. System model of an untrusted relay network with a multi-antenna source node and multiple destination nodes.

B. Joint Antenna and User Selection

For the considered system, we select the best antenna n^* for the best user D_{m^*} in order to maximize the instantaneous secrecy rate:

$$(n^*, m^*) = \arg \max_{n=1,\ldots,N_S} \max_{m=1,\ldots,M} R_S(n,m). \tag{6}$$

With the observation of the term (3) and (4), since $R_D(n,m)$ increases as $|g_{m,R}|^2$ increases while $R_E(n,m)$ decreases as $|g_{m,R}|^2$ increases, it is easy to verify that the secrecy rate increases as $|g_{m,R}|^2$ increases for any n-th antenna. Therefore, the secrecy rate of the joint antenna and user selection scheme can be reformulated as

$$\hat{R_S} = \arg \max_{n=1,\ldots,N_S} R_S(n, m^*), \tag{7}$$

where $m^* = \arg \max_{m=1,\ldots,M} |g_{m,R}|^2$. Therefore, the user selection can be easily performed at each destination user in a distributed way with the help of the virtual timer. In the following sections, we will provide the performance analysis of the proposed selection scheme.

III. Secrecy Outage Probability Analysis

We will present the secrecy outage performance in this section. The SOP can be expressed as

$$p_{out} = \Pr \left\{ \max_{n=1,\ldots,N_S} \frac{1}{2} \log_2 \left(\frac{1 + \frac{X_n Y}{X_n + 2Y + 1}}{1 + \frac{X_n}{Y+1}} \right) < R_{th} \right\}, \tag{8}$$

where $X_n = \rho |h_{n,R}|^2, Y = \rho |g_{m^*,R}|^2$ and R_{th} denotes the threshold of secrecy rate. For the high signal-to-noise ratio (SNR), the following approximation can be obtained

$$\begin{aligned} p_{out} &\simeq \Pr \left\{ \max_{n=1,\ldots,N_S} \tfrac{1}{2} \log_2 \left(\frac{1 + \frac{X_n Y}{X_n + 2Y}}{1 + \frac{X_n}{Y}} \right) < R_{th} \right\} \\ &= \Pr \left\{ \max_{n=1,\ldots,N_S} \frac{\frac{X_n Y}{X_n + Y} + \frac{1}{2} \frac{X_n Y \cdot X_n 2Y}{(X_n + Y)(X_n + 2Y)}}{X_n} < \gamma_{th} \right\}, \end{aligned} \tag{9}$$

where $\gamma_{th} = 2^{2R_{th}}$. With the acknowledgement that $\min(a,b)$ $\geq \frac{ab}{a+b} \geq \frac{1}{2} \min(a,b)$, the secrecy outage can be further given

[1] Like [7], we assume that the cooperative relay is trusted at the service level while it is untrusted at the data level. In this assumption, the relay is authorized to help data forwarding (i.e. cognitive relay) and some required information (i.e. channel state information, control signaling, etc.) can be feedback to source accurately. However, it is unauthorized to access the content of the data, therefore, it is necessary to consider the potential eavesdropping for the confidential information.

by

$$p_{out} \simeq \Pr\left\{ \max_{n=1,\ldots,N_S} \frac{\min(X_n,Y)+\frac{\min(X_n,Y)\min(X_n,2Y)}{2}}{X_n} < \theta\gamma_{th} \right\}, \tag{10}$$

where $\theta \in [1,2]$. The lower bound of SOP can be obtained when $\theta = 1$, and the upper bound can be acquired when $\theta = 2$. After some mathematical manipulations, we can obtain the following theorem.

Theorem 1: For the considered untrusted relay networks, the SOP achieved by the proposed scheme can be given by (11), presented at the top of next page.

Here, $\zeta = \frac{\rho\theta\gamma_{th}\Omega_X}{4n}$, $\eta = \frac{n}{\rho\theta\gamma_{th}\Omega_X} + \frac{m+1}{\rho\Omega_Y}$, $\Psi(a,b) = e^{\frac{na}{\rho\Omega_X}+\frac{(m+1)b}{\rho\Omega_Y}}$, $\mathrm{erfc}(x)$ is the complementary error function defined in [18, eq.(8.250.4)], $a_1 = 2\theta\gamma_{th} - 1$, $a_2 = 2\theta\gamma_{th} - 2$, $t_k = \frac{1}{2}\left(1 - \cos\left(\frac{2k-1}{K}\right)\right)$, and K is the Gauss-Chebyshev integral approximated sum term.

Proof: Owing to the independence of X_n, the term (10) can be rewritten as (12), presented at the top of next page. $f_Y(y)$ is the probability density function (PDF) of the random variable Y, which is given by

$$f_Y(y) = \sum_{m=0}^{M-1} \binom{M-1}{m} \frac{M(-1)^m}{\rho\Omega_Y} e^{-\frac{(m+1)y}{\rho\Omega_Y}}. \tag{13}$$

Consider the different relationship between X_n and Y, we can further express the term (12) as

$$\begin{aligned} p_{out} \simeq \int_y \Big[&\Pr\left(X_n < a_2, X_n < y\right) \\ &+ \Pr\left(X_n > \tfrac{y}{\theta\gamma_{th} - \frac{1}{2}y}, y \le X_n < 2y\right) \\ &+ \Pr\left(X_n > \tfrac{y^2+y}{\theta\gamma_{th}}, 2y \le X_n\right) \Big]^{N_S} f_Y(y)\mathrm{d}y \\ = I_0^{a_2} + I_{a_2}^{a_1} + I_{a_1}^{\infty}, \end{aligned} \tag{14}$$

where

$$I_0^{a_2} = \int_0^{a_2} \left(\int_0^y f_X(x)\mathrm{d}x + \int_y^{2y} f_X(x)\mathrm{d}x + \int_{2y}^{\infty} f_X(x)\mathrm{d}x \right)^{N_S} f_Y(y)\mathrm{d}y, \tag{15}$$

$$I_{a_2}^{a_1} = \int_{a_2}^{a_1} \left(\int_0^{a_2} f_X(x)\mathrm{d}x + \int_{\frac{y}{\theta\gamma_{th} - \frac{1}{2}y}}^{2y} f_X(x)\mathrm{d}x + \int_{2y}^{\infty} f_X(x)\mathrm{d}x \right)^{N_S} f_Y(y)\mathrm{d}y, \tag{16}$$

$$I_{a_1}^{\infty} = \int_{a_1}^{\infty} \left(\int_0^{a_2} f_X(x)\mathrm{d}x + 0 + \int_{\frac{y^2+y}{\theta\gamma_{th}}}^{\infty} f_X(x)\mathrm{d}x \right)^{N_S} f_Y(y)\mathrm{d}y, \tag{17}$$

and

$$f_X(x) = \frac{1}{\rho\Omega_X} e^{-\frac{x}{\rho\Omega_X}}. \tag{18}$$

$I_0^{a_2}$ can be calculated as

$$I_0^{a_2} = \left(1 - e^{-\frac{a_2}{\rho\Omega_Y}}\right)^M. \tag{19}$$

Then, we rewrite $I_{a_2}^{a_1}$ as

$$\begin{aligned} I_{a_2}^{a_1} = &\sum_{n=1}^{N_S} \sum_{m=0}^{M-1} \binom{N_S}{n} \binom{M-1}{m} (-1)^m \frac{M(1-e^{-\frac{a_2}{\rho\Omega_X}})^{N_S-n}}{\rho\Omega_Y} \\ &\Psi\left(2, -2\theta\gamma_{th}\right) \underbrace{\int_{\frac{1}{2}}^{1} 2\Psi\left(\frac{-2\theta\gamma_{th}}{u}, 2u\right)\mathrm{d}u}_{Q_1} \\ &+ \underbrace{\left(1 - e^{-\frac{a_2}{\rho\Omega_X}}\right)^{N_S} \int_{a_2}^{a_1} f_Y(y)\mathrm{d}y}_{Q_2}. \end{aligned} \tag{20}$$

With the aid of [17, eq.(55)], after some algebraic transformations Q_1 can be calculated as

$$Q_1 \simeq \sum_{k=1}^{K} \frac{\pi\left|\sin\frac{2k-1}{K}\right|}{K} \left(\Psi\left(\frac{-2\theta\gamma_{th}}{t_k}, 2t_k\right) - \frac{1}{2}\Psi\left(\frac{-4\theta\gamma_{th}}{t_k}, t_k\right) \right). \tag{21}$$

$I_{a_1}^{\infty}$ can be reformulated as

$$\begin{aligned} I_{a_1}^{\infty} = &\sum_{n=1}^{N_S} \sum_{m=0}^{M-1} \binom{N_S}{n} \binom{M-1}{m} (-1)^m \frac{M(1-e^{-\frac{a_2}{\rho\Omega_X}})^{N_S-n}}{\rho\Omega_Y} \\ &\underbrace{\int_{a_1}^{\infty} e^{-\frac{n}{\rho\theta\gamma_{th}\Omega_X}u^2 - (\frac{m+1}{\rho\Omega_Y} + \frac{n}{\rho\theta\gamma_{th}\Omega_X})u}\mathrm{d}u}_{Q_3} \\ &+ \underbrace{\left(1 - e^{-\frac{a_2}{\rho\Omega_X}}\right)^{N_S} \int_{a_1}^{\infty} f_Y(y)\mathrm{d}y}_{Q_4}. \end{aligned} \tag{22}$$

With the aid of [18, eq.(3.322.1)], Q_3 can be given by

$$Q_3 = \sqrt{\pi\zeta} e^{\zeta\eta^2} \mathrm{erfc}\left(\eta\sqrt{\zeta} + \frac{a_1}{2\sqrt{\zeta}}\right). \tag{23}$$

$$\begin{aligned} Q_2 + Q_4 &= \left(1 - e^{-\frac{a_2}{\rho\Omega_X}}\right)^{N_S} \int_{a_2}^{\infty} f_Y(y)\mathrm{d}y \\ &= \left(1 - \left(1 - e^{-\frac{a_2}{\rho\Omega_Y}}\right)^M\right)\left(1 - e^{-\frac{a_2}{\rho\Omega_X}}\right)^{N_S}. \end{aligned} \tag{24}$$

By combining $I_0^{a_2}$, $I_{a_2}^{a_1}$ and $I_{a_1}^{\infty}$, we can readily obtain the Theorem 1. ■

Corollary 1: The diversity order of the consider networks is $\min\left(N_S, \frac{M}{2}\right)$.

Proof: By using the fact that $e^x \simeq 1 + x$ if $x \to 0$, when $\rho \to \infty$ we have

$$\begin{aligned} p_{out} \overset{\rho\to\infty}{\simeq} &\sum_{\substack{m=0,\\ n=N_S}}^{M-1} \binom{M-1}{m} (-1)^m \frac{M\sqrt{\pi\zeta}e^{\zeta\eta^2}}{\rho\Omega_Y} \mathrm{erfc}\left(\eta\sqrt{\zeta} + \frac{a_1}{2\sqrt{\zeta}}\right) \\ &+ \sum_{\substack{m=0,\\ n=N_S}}^{M-1} \binom{M-1}{m} (-1)^m \frac{M\pi \sum_{k=1}^{K} \left|\sin\frac{2k-1}{K}\right|}{\rho\Omega_Y 2K} \Psi\left(2, -2\theta\gamma_{th}\right) \\ &+ \frac{a_2}{\Omega_Y}\left(\frac{1}{\rho}\right)^M + \frac{a_2}{\Omega_X}\left(\frac{1}{\rho}\right)^{N_S}. \end{aligned} \tag{25}$$

We first give the following two sums of the binomial coefficients

$$\sum_{k=0}^{N} \binom{N}{k} (-1)^k k^n = 0, \quad 0 \le n \le N-1, \tag{26}$$

$$p_{out} \simeq \left(1-e^{-\frac{a_2}{\rho\Omega_Y}}\right)^M + \left(1-(1-e^{-\frac{a_2}{\rho\Omega_Y}})^M\right)\left(1-e^{-\frac{a_2}{\rho\Omega_X}}\right)^{N_S} + \sum_{n=1}^{N_S}\sum_{m=0}^{M-1}\tbinom{N_S}{n}\tbinom{M-1}{m}(-1)^m \frac{M(1-e^{-\frac{a_2}{\rho\Omega_X}})^{N_S-n}}{\rho\Omega_Y}$$
$$\times\left\{\sqrt{\pi\zeta}e^{\zeta\eta^2}\mathrm{erfc}\left(\eta\sqrt{\zeta}+\frac{a_1}{2\sqrt{\zeta}}\right)+\frac{\pi\Psi(2,-2\theta\gamma_{th})}{K}\sum_{k=1}^{K}\left|\sin\frac{2k-1}{K}\right|\left(\Psi\left(\frac{-2\theta\gamma_{th}}{t_k},2t_k\right)-\frac{1}{2}\Psi\left(\frac{-4\theta\gamma_{th}}{t_k},t_k\right)\right)\right\} \tag{11}$$

$$p_{out} \simeq \int_y \prod_{n=1}^{N_S} \Pr\left\{ \frac{\min(X_n,y)+\frac{\min(X_n,y)\min(X_n,2y)}{2}}{X_n} < \theta\gamma_{th} \middle| Y=y \right\} f_Y(y)\mathrm{d}y \tag{12}$$

and

$$\sum_{k=0}^{N}\tbinom{N}{k}(-1)^k k^N = (-1)^N N!. \tag{27}$$

With the help of above two equations, the asymptotic results can be given by

$$p_{out} \overset{\rho\to\infty}{\simeq} \frac{a_2}{\Omega_Y}\left(\frac{1}{\rho}\right)^M + \frac{a_2}{\Omega_X}\left(\frac{1}{\rho}\right)^{N_S} + \delta\frac{M!(\frac{\theta\gamma_{th}\Omega_X}{4N_S})^{\frac{M}{2}}}{(\Omega_Y)^M}\left(\frac{1}{\rho}\right)^{\frac{M}{2}}$$
$$+\frac{M\pi(2\theta\gamma_{th})^{M-1}\sum_{k=1}^{K}\left|\sin\frac{2k-1}{K}\right|}{2K(\Omega_Y)^M}\left(\frac{1}{\rho}\right)^M, \tag{28}$$

where δ equals to $\frac{\pi}{a_3!}$ if M is odd, δ equals to $\sum_{l=0}^{a_4}\frac{(-1)^l 2}{(a_4-l)!l!(2l+1)}$ if M is even, $a_3=\frac{M-1}{2}$ and $a_4=\frac{M-2}{2}$. Note that the diversity order dominated by the smaller one of $\left(N_S, \frac{M}{2}\right)$, then the prove is completed. ■

From the asymptotic expression, it reveals that the security performance can be improved by the mutual effects of the increased number of antennas and the increased number of users. This phenomenon also indicates that, increasing the number of antennas in the high-density user networks ($M \gg N_S$) can achieve a better outage performance gain than increasing the number of users when the number of antennas is much more than the number of users case ($N_S \gg M$).

IV. Ergodic Secrecy Rate Analysis

This section will investigate secrecy rate performance by using the proposed scheme. The ESR of considered system can be given as

$$\begin{aligned}\bar{R}_S &= E\left\{[R_D(n^*,m^*)-R_E(n^*,m^*)]^+\right\}.\\ &\geq E\left\{\left[\max_{i=1,\ldots,N_S}R_D(i,m^*)-\max_{j=1,\ldots,N_S}R_E(j,m^*)\right]^+\right\}\\ &\geq E\left[\left\{\max_{i=1,\ldots,N_S}R_D(i,m^*)-\max_{j=1,\ldots,N_S}R_E(j,m^*)\right\}\right]^+\\ &\triangleq \bar{R}_S^{LB}.\end{aligned} \tag{29}$$

The lower bound of ESC ($\bar{R}_S^{LB}$) can be characterized by

$$\bar{R}_S^{LB} = \frac{1}{2\ln 2}\left[E\left\{\ln\left(1+\frac{\hat{X}Y}{\hat{X}+2Y+1}\right)\right\}-E\left\{\ln\left(1+\frac{\hat{X}}{Y+1}\right)\right\}\right]^+, \tag{30}$$

where $\hat{X}=\max_{i=1,\ldots,N_S}\rho|h_{i,R}|^2$, and Y has been defined before. With the help of [7, eq.(8)], we have

$$\begin{aligned}\bar{R}_S^{LB} &= \frac{1}{2\ln 2}\left[E\left\{\ln\left(1+e^{\ln(\hat{X}Y)-\ln(\hat{X}+2Y+1)}\right)\right\}\right.\\ &\qquad\left.-E\left\{\ln\left(1+\frac{\hat{X}}{Y+1}\right)\right\}\right]^+\\ &\overset{(a)}{\geq}\frac{1}{2\ln 2}\left[\ln\left(1+e^{E\left\{\ln\hat{X}+\ln Y\right\}-E\{\ln(Z_1+1)\}}\right)\right.\\ &\qquad\left.-E\left\{\ln\left(1+Z_2\right)\right\}\right]^+,\end{aligned} \tag{31}$$

where $Z_1=\hat{X}+2Y$, $Z_2=\frac{\hat{X}}{Y+1}$ and step (a) is obtained from the Jensen's inequality. To obtain the expectations in (31), we first give the PDF of $\hat{X}$, Z_1 and the cumulative distribution function (CDF) of Z_2 as follows

$$f_{\hat{X}}(x)=\sum_{n=0}^{N_S-1}\tbinom{N_S-1}{n}\frac{N_S(-1)^n}{\rho\Omega_X}e^{-\frac{(n+1)x}{\rho\Omega_X}}, \tag{32}$$

$$\begin{aligned}&f_{Z_1}(z)=\\ &\sum_{n=0}^{N_S}\sum_{m=0}^{M-1}\frac{\binom{N_S}{n}\binom{M-1}{m}(-1)^{n+m}M}{\rho\Omega_Y}\left\{\underset{b_2=2b_1}{\Delta}\left\{\frac{1}{2}e^{-b_1 z}(1-b_1 z)\right\}\right.\\ &\qquad\left.+\underset{b_2\neq 2b_1}{\Delta}\left\{\frac{\frac{b_2}{2}e^{-\frac{b_2}{2}z}-b_1 e^{-b_1 z}}{b_2-2b_1}\right\}\right\},\end{aligned} \tag{33}$$

$$F_{Z_2}(z)=1+\sum_{n=1}^{N_S}\sum_{m=0}^{M-1}\frac{\binom{N_S}{n}\binom{M-1}{m}(-1)^{n+m}Mb_2 e^{-b_1 z}}{(m+1)(b_1 z+b_2)}, \tag{34}$$

where $b_1=\frac{n}{\rho\Omega_X}$, and $b_2=\frac{m+1}{\rho\Omega_Y}$. Here, we define the operation $\underset{B}{\Delta}\{A\}$ as: $\underset{B}{\Delta}\{A\}=A$ if the condition B holds, and $\underset{B}{\Delta}\{A\}=0$ otherwise.

With the aid of [18, eq.(4.331.1)], we have

$$\begin{aligned}&E\{\ln\hat{X}+\ln Y\}=\\ &\qquad\int_0^\infty \ln(x)f_{\hat{X}}(x)\mathrm{d}x+\int_0^\infty \ln(y)f_Y(y)\mathrm{d}y\\ &\quad=\sum_{n=0}^{N_S-1}\tbinom{N_S-1}{n}(-1)^{n+1}N_S\frac{\mathcal{C}+\ln(\frac{n+1}{\rho\Omega_X})}{n+1}\\ &\qquad+\sum_{m=0}^{M-1}\tbinom{M-1}{m}(-1)^{m+1}M\frac{\mathcal{C}+\ln(\frac{m+1}{\rho\Omega_Y})}{m+1}\triangleq T_1,\end{aligned} \tag{35}$$

where $\mathcal{C}$ is the Euler constant. Following [18, eq.(4.337.5)], we have

$$E\left\{\ln\left(1+Z_1\right)\right\} = \int_0^\infty \ln(1+z) f_{Z_1}(z)\mathrm{d}z = \sum_{n=0}^{N_S}\sum_{m=0}^{M-1} \frac{\binom{N_S}{n}\binom{M-1}{m}(-1)^{n+m}M}{\rho\Omega_Y}\left\{\underset{b_2=2b_1}{\Delta}\left\{-\tfrac{1}{2}e^{b_1}E_i(-b_1) -\tfrac{1}{b_1}\right\} + \underset{b_2\neq 2b_1}{\Delta}\left\{\frac{\underset{n\neq 0}{\Delta}\left\{e^{b_1}E_i(-b_1)\right\} - e^{\frac{b_2}{2}}E_i(-\frac{b_2}{2})}{b_2-2b_1}\right\}\right\} \triangleq T_2, \tag{36}$$

where $E_i(x)$ is the exponential integral function defined in [18, eq.(8.212.1)]. By using [18, eq.(3.353.3), eq.(3.352.4)], we have

$$E\left\{\ln\left(1+Z_2\right)\right\} = \int_0^\infty \frac{1-F_{Z_2}(z)}{1+z}\mathrm{d}z = \sum_{n=1}^{N_S}\sum_{m=0}^{M-1} \frac{\binom{N_S}{n}\binom{M-1}{m}(-1)^{n+m+1}M}{m+1}\left\{\underset{b_1=b_2}{\Delta}\left\{b_1 e^{b_1}E_i(-b_1) +1\right\} + \underset{b_2\neq b_1}{\Delta}\left\{\frac{b_2\left(e^{b_2}E_i(-b_2)-e^{b_1}E_i(-b_1)\right)}{b_2-b_1}\right\}\right\} \triangleq T_3. \tag{37}$$

With the given T_1, T_2 and T_3, the following theorem can be obtained.

Theorem 2: For the considered untrusted relay networks, the ESR achieved by the proposed scheme is lower bounded by

$$\bar{R}_S \geq \tfrac{1}{2\ln 2}\left[\ln\left(1+e^{T_1-T_2}\right) - T_3\right]^+. \tag{38}$$

V. Numerical Results

In this section, simulation results are presented to demonstrate the performance of the proposed scheme. We assume that the target secrecy rate R_{th} is 1 bps/Hz for the outage performance analysis. We use the lower bound of SOP ($\theta = 1$) for the whole section, and it can be shown that it is a tighten bound in high SNR regime. The Gaussian-Chebyshev parameter is chosen as $K = 10$. We assume that $\Omega_X = \Omega_Y = 1$, but extension using different Ω_X and Ω_Y values is straightforward. The parameter N_S and M will be defined individually for each figure.

Fig. 2 shows the SOP of the proposed joint antenna and user selection scheme for different N_S and M. It can be observed that our analysis results agree well with the simulations, and the lower bound of SOP is tight in the high SNR regime. When $N_S = 1$ and $M = 1$, it can be regarded as the traditional three nodes scenario (i.e. source-relay-destination). It can be observed that, by introducing the multiple source antennas or multiple users will benefit the outage performance for the traditional three node scenario. For a fixed number of antennas, as the number of users M increases, the slope of the curve will first increase then remain stable. The multiuser diversity promises a better outage performance as M increase. However, this enhancement will become less due to the limitation of the number of antennas. This phenomenon is also in agreement with the Corollary 1.

Fig. 3 shows the ESR versus ρ for the different number of antennas N_S with the different number of users M, which demonstrates the accuracy of the derived lower bound of ESR of the proposed scheme. We denote (a, b) as the curve of $N_S = a$ and $M = b$. Comparing the traditional three nodes case $(1, 1)$ with the multiuser and multi-antenna case, a great performance gain can be found, which shows the effectiveness of the proposed scheme. Compared $(2, 2)$ with $(2, 4)$, a great enhancement on ESC can be achieved due to the multiuser diversity. Compared $(6, 4)$ with $(2, 4)$, a large enhancement on the number of antennas meets a small improvement on ESR. These observations indicate that, to set N_S and M at a proper number will make the enhancement on ESR more

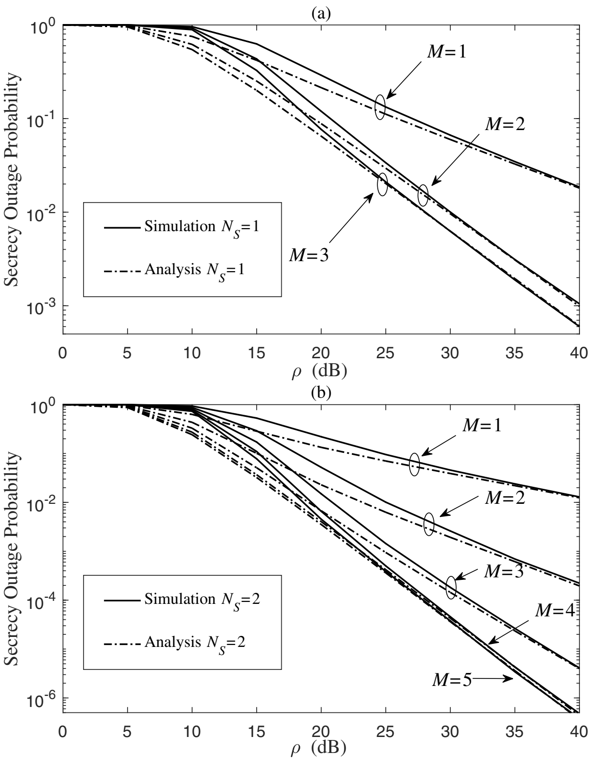

Fig. 2. Secrecy outage probability versus ρ for different number of antennas N_S with different number of users M.

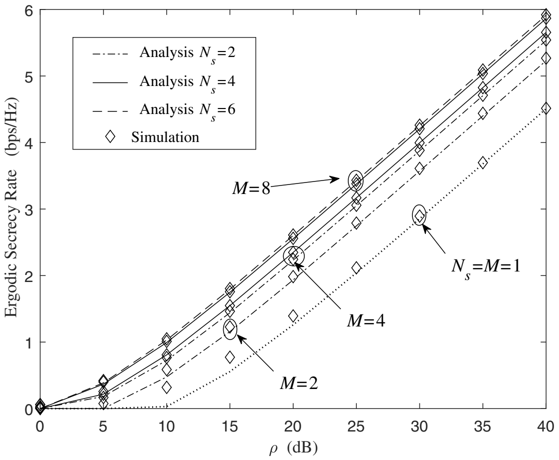

Fig. 3. Ergodic secrecy rate versus ρ for the different number of antennas N_S with the different number of users M.

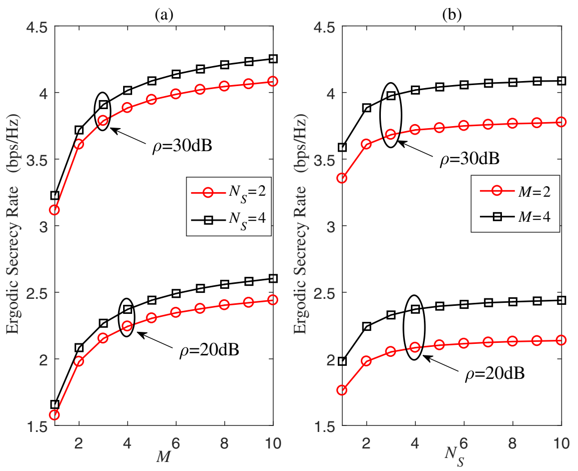

Fig. 4. The effect of the number of antennas N_S and the number of users M on the ergodic secrecy rate, (a) ESR-M case; (b) ESR-N_S case.

efficient.

In Fig. 4, we fix the SNR ρ to investigate the effects of N_S and M on the ESR. When $N_S = M$, ESR-M case can obtain a larger ESR than ESR-N_S case for both $\rho = 20$dB and $\rho = 30$dB. By increasing N_S for the ESR-M case and M for the ESR-N_S case will improve the ESR of the system, and the enhancement of ESR-N_S case is much more than ESR-M case. These observations are mainly because that, the increased number of users can provide a higher main channel rate and bring the untrusted relay higher interference, however, increased number of users will benefit not only destination users but also untrusted relay with different degree.

VI. Conclusion

In this paper, we introduce cooperative jamming for the secure communication in the untrusted relay networks with multi-antenna and multiuser. The joint antenna and user selection scheme has been proposed to further improve the security. To evaluate the performance of the proposed scheme, we derive both the lower bound and the upper bound of SOP, asymptotic expression of SOP, and the lower bound of ESR in closed form. From the asymptotic expressions and the simulation results, we can obtain that the secrecy diversity order of the proposed scheme is $\min(N_S, M/2)$. It reveals that, increasing the number of antennas and users will improve the diversity of the system, however, the secrecy order achieved by traditional single antenna single source-destination untrusted relay network is limited to one even with the aid of multiple relays.

Acknowledgement

This work was supported in part by the National Natural Science Foundation of China under Grants 61771366 and 61601347, in part by the Royal Society Project under Grant IEC/NSFC/170324, in part by the EU FP7 CROWN Project under Grant PIRSES-GA-2013-610524, in part by the Natural Science Basic Research Plan in Shaanxi Province of China under Grant 2017JQ6055, in part by the 111 Project of China under Grant B08038, and in part by the Innovation Fund of Xidian University.

References

[1] L. Yang, J. Chen, H. Jiang, S. A. Vorobyov, and H. Zhang, "Optimal relay selection for secure cooperative communications with an adaptive eavesdropper," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 26-42, Jan. 2017.

[2] L. Lv, Z. Ding, Q. Ni and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Trans. Veh. Technol.*, pp.1-1, Mar. 2018.

[3] Z. Ding, K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359-368, Feb. 2012.

[4] Y. Feng, S. Yan, Z. Yang, N. Yang and W. P. Zhu, "TAS-based incremental hybrid decode-amplify-forward relaying for physical layer security enhancement," *IEEE Trans. Commun*, vol. 65, no. 9, pp. 3876-3891, Sep. 2017.

[5] J. Chen, R. Zhang, L. Song, Z. Han and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310-320, Feb. 2012.

[6] C. Wang, H. M. Wang and X. G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589-605, Feb. 2015.

[7] L. Sun, T. Zhang, Y. Li and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801-3807, Oct. 2012.

[8] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807-3827, Aug. 2010.

[9] C. Jeong, I.-M. Kim, and D. I. Kim,"Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310-325, Jan. 2012.

[10] M. Ju, D. H. Kim and K. S. Hwang, "Opportunistic transmission of nonregenerative network with untrusted relay," *IEEE Trans. Veh. Technol.*, vol. 64, no. 6, pp. 2703-2709, June 2015.

[11] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *Proc. IEEE Global Telecommun. Conf.*, New Orleans, LO, 2008, pp. 1-5.

[12] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 289-292, Jun. 2014.

[13] J. Xiong, L. Cheng, D. Ma and J. Wei, "Destination-aided cooperative jamming for dual-hop amplify-and-forward MIMO untrusted relay systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7274-7284, Sep. 2016.

[14] J.-B. Kim, J. Lim, and J. M. Cioffi, "Capacity scaling and diversity order for secure cooperative relaying with untrustworthy relays," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3866-3876, Jul. 2015.

[15] L. Lv, Q. Ni, Z. Ding and J. Chen, "Cooperative non-orthogonal relaying for security enhancement in untrusted relay networks," in *Proc. IEEE International Conference on Communications (ICC)*, Paris, 2017, pp. 1-6.

[16] D. Deng, W. Zhou and L. Fan, "Secrecy outage probability of multiuser untrusted amplify-and-forward relay networks," in *Proc. IEEE Vehicular Technology Conference (VTC Spring)*, Sydney, 2017, pp. 1-5.

[17] Z. Yang, Z. Ding, Y. Wu and P. Fan, "Novel relay selection strategies for cooperative NOMA," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10114-10123, Nov. 2017.

[18] A. Jeffrey and D. Zwillinger, *Table of Integrals, Series, and Products*. New York, NY, USA: Academic, 2007.