Hindawi
Wireless Communications and Mobile Computing
Volume 2017, Article ID 9580639, 11 pages
https://doi.org/10.1155/2017/9580639

Research Article

Secrecy Analysis of Multiuser Untrusted Amplify-and-Forward Relay Networks

Dan Deng,[1] Xutao Li,[2] Lisheng Fan,[3] Wen Zhou,[4] Rose Qingyang Hu,[5] and Zhili Zhou[6]

[1]*School of Information Engineering, Guangzhou Panyu Polytechnic, Guangzhou 511483, China*
[2]*Department of Electronic Engineering, Shantou University, Shantou 515063, China*
[3]*School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China*
[4]*College of Information Science and Technology, Nanjing Forestry University, Nanjing 210037, China*
[5]*Department of Electrical and Computer Engineering, Utah State University, Logan, UT 84322-4120, USA*
[6]*Jiangsu Engineering Centre of Network Monitoring and School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China*

Correspondence should be addressed to Lisheng Fan; lsfan@gzhu.edu.cn

Received 16 July 2016; Revised 18 September 2016; Accepted 13 October 2016; Published 15 January 2017

Academic Editor: Gonzalo Vazquez-Vilar

Copyright © 2017 Dan Deng et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper investigates the secure communications of multiuser untrusted amplify-and-forward relay networks in the presence of direct links. In the considered system, one user is selected among multiple ones for secure transmission to the destination node with the help of an untrusted relay node. To reduce the information leakage to the untrusted relay, the paper considers two selection criteria to select the user based on the direct and the relaying links, respectively. The impact of direct and the relaying link on the system secrecy performance is studied by deriving the close-form ergodic secrecy rate (ESR) as well as the asymptotic expression. From the asymptotic expression, it can be found that the asymptotic ESR increases linearly with the logarithm of the average channel gain ratio of the direct link to the relaying link.

1. Introduction

The information transmission and processing have been attracting much attention in recent years [1–8], during which the security plays an important role [9–12]. Due to the broadcast nature of wireless channel, physical layer security in cooperative relay networks has attracted great interests. Secure MIMO communication was investigated in [13, 14] within the framework of Wyners wiretap channel [15]. In order to prevent the information leakage, some useful schemes such as artificial noise [16–18] and antenna/user selection [19, 20] have been proposed and comprehensively analyzed. The secure relay beamforming problems are investigated in [21], and rank-1 relay beamformer has been proved to be globally optimal with imperfect channel state information (CSI). As an improvement, [22] analyzed the globally optimal relay beamformer with complete CSI as well as with partial eavesdroppers CSI. Specifically, under a stochastic geometry framework, authors in [23] studied the secure multiantenna transmission coexisting with randomly located eavesdroppers.

Besides, user selection, which can efficiently exploit the multiuser diversity in the wireless communication system, has been widely adopted to enhance the system performance. In [24–27], the impact of outdated channel state information on secrecy outage probability (SOP) was studied. In [28], three criteria were proposed to select the best relay and user pair, and the corresponding analytical expressions for the secrecy outage probability were derived. For a multiuser scheme with cooperative jamming, authors in [29] revealed that the ergodic secrecy rate (ESR) for the optimal user selection scheme can be increased as the number of users. Also, in [30] two relay and jammer selection methods were developed for SOP minimization. Authors in [31] considered the joint impact of direct and relaying links on the user selection criterion in multiuser cognitive relay networks by deriving an exact closed-form expression for outage probability. The

secure communications with full-duplex relaying and large scale system were studied in [32–35].

Moreover, in some application scenarios, the user-destination pair attempts to keep secret from an untrusted relay, despite that the cooperation relaying is still needed [36]. He and Yener [37] provided an achievable secrecy rate analysis for the general untrusted relay channel. Authors in [38] proposed an iterative algorithm for the jointly design of user and relay beamformers with an untrusted relay. In [39], with multiple untrusted relay nodes, the lower bound and the asymptotic analysis of ESR for suboptimal relay selection strategy were derived by using the extreme value theory. Considering the optimal power allocation in untrusted relay networks, [40] analyzed the asymptotic ESR for large antenna number. Authors in [41] concerned about joint design of secure beamforming at the source and the relay for an amplify-and-forward (AF) MIMO untrusted relay system. Based on linear beamforming, [42] presented an imbalanced beamforming for secure utilization of an untrusted relay networks.

Most of existing literatures investigated the impact of the relaying links. However, few attentions are paid to the effects of the direct links for the untrusted relay networks. Authors in [43] derived the exact secrecy outage probability of an opportunistic transmission scheme with an untrusted relay in single user networks. In this model, there are two transmission modes in the system model: the direct link and the triangular link. Our paper extends to a multiuser scenario with two-phase signals directly combined by the destination. Moreover, we derive analytical expression of the secrecy capacity for two suboptimal criteria, which is applicable for delay-tolerant communication. To the best of our knowledge, no prior work has considered the joint impact of the direct and relaying links for multiuser untrusted relay networks.

This paper studies the secure communications of multiuser untrusted amplify-and-forward relay networks in the presence of direct links. In the considered systems, one user is selected among multiple ones for secure transmission to the destination node with the help of an untrusted relay node, while the relay may wiretap the signals sent from the selected user. To reduce the information leakage, we consider two selection criteria for user selection based on direct and relaying links, respectively. We study the impact of the direct and relaying links on the system secrecy performance by deriving the analytical ESR as well as the asymptotic expression. Numerical simulation results are provided to validate the theoretical analysis.

Notations. We use $A \triangleq B$ to denote that A, by definition, equals B. $\log_2(\cdot)$ and $\ln(\cdot)$ denote the base-2 and natural logarithms, respectively. For a random variable X, $f_X(x)$ denotes the probability density function of X, and $\mathbb{E}(X)$ denotes the expectation of a random variable X. Also, $x \sim \mathcal{CN}(\mu, \sigma^2)$ indicates that random variable x is a circularly symmetric complex-valued Gaussian random variable with mean μ and variance σ^2. The notation R-D denotes the link from R to D.

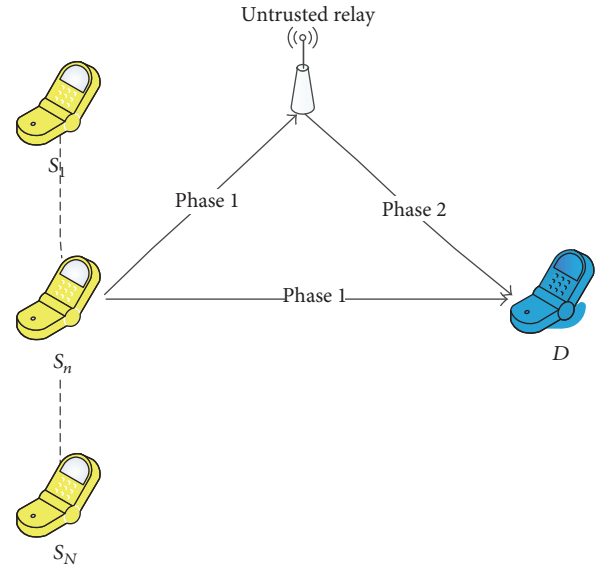


Figure 1: Two-phase untrusted amplify-and-forward relay networks with user selection.

2. System Model

Figure 1 depicts the system model of two-phase untrusted amplify-and-forward relay networks with user selection, which consists of N user nodes $(S_1, S_2, \ldots, S_N)$, an untrusted AF relay node (R), and a destination node (D). There exist direct links between the users and the destination, as well as a relaying link. All the nodes are assumed to be equipped with a single antenna and operate in the half-duplex time-division mode.

We consider that the relay system works in two-phase mode as follows. In the first phase, one of the *best* user is selected for information transmission, while the relay and the destination receive the wireless signal from the selected user node, respectively. Besides, the relay can intercept the signal simultaneously. The aim of the selection criteria is to prevent the information leakage by the untrusted relay as well as to increase the capacity of the legitimate link. In the second phase, the relay amplifies and forwards the received signal to the destination.

The destination node D and the relay node can easily estimate their channel parameters, with the help of some pilot signals for users. Then D gathers the CSI of S_n-R through some dedicated feedback channels. After that, D performs user selection and broadcasts the index of the selected user to other nodes in the network.

To recover the original information from the user, the destination combines the direct link signal and relaying link signal by MRC receiver. The received noise of every link is modelled as an independent additive white Gaussian noise (AWGN) with zero mean and variance equals N_0. Let $h_{S_nR} \sim \mathcal{CN}(0, \alpha)$, $h_{S_nD} \sim \mathcal{CN}(0, \beta)$ and $h_{RD} \sim \mathcal{CN}(0, \varepsilon)$ denote the instantaneous channel fading coefficients of S_n-R, S_n-D, and R-D links, respectively, where $\mathcal{CN}(a, b)$ denotes the Complex Gaussian random distribution with mean a and variance b. We assume that all links between different nodes are

quasistatic Rayleigh fading and stochastically independent between each other. The channel fading coefficient of each link remains constant within each transmission, while varies independently from one frame to another. Different from [43] where only one source node is considered, we address on the secure multiuser communication in amplify-and-forward relay networks. More importantly, we utilize both the direct and the relay links simultaneously, which makes our schemes better than the opportunistic transmission scheme. Specifically, [43] analyzed the secrecy outage probability behavior, while this paper studies the secrecy capacity, which is applicable for delay-tolerant communication and give us new insights into the secrecy performance.

Given that S_n is selected in the first phase, the signal received at relay can be written as

$$r_{S_nR} = \sqrt{P_S} x_n h_{S_nR} + n_R, \tag{1}$$

where P_S is the transmission power of the user station, x_n denotes the transmission signal from S_n with constant unit power, and $n_R \sim \mathcal{CN}(0, N_0)$ is the AWGN received at relay with power N_0. Then the signal-to-noise ratio (SNR) at relay in the first phase is

$$\mathrm{SNR}_R^{(n)} = \rho_s \gamma_{S_nR}, \tag{2}$$

where $\rho_s \triangleq P_S/N_0$ and $\gamma_{S_nR} \triangleq |h_{S_nR}|^2$ is the instantaneous power of channel fading coefficients of the S_n-R link. The untrusted relay intercepts messages from the wireless channel just as an eavesdropper, and the capacity of the illegal link is

$$C_R^{(n)} = \frac{1}{2}\log_2\left(1 + \mathrm{SNR}_R^{(n)}\right). \tag{3}$$

Similarly, the signal received at destination can be expressed as

$$r_{S_nD} = \sqrt{P_S} x_n h_{S_nD} + n_{D,1}, \tag{4}$$

where $n_{D,1} \sim \mathcal{CN}(0, N_0)$ is the AWGN received at destination with power N_0 in the first phase. Then the SNR at destination is

$$\mathrm{SNR}_{D,1}^{(n)} = \rho_s \gamma_{S_nD}, \tag{5}$$

where $\gamma_{S_nD} \triangleq |h_{S_nD}|^2$ is the instantaneous power of channel fading coefficients of the S_n-D link.

In the second phase, the relay amplifies and forwards the received signal in the previous phase with transmission power P_R, and the power amplifier factor is

$$\kappa_n = \sqrt{\frac{P_R}{P_S \gamma_{S_nR} + N_0}}. \tag{6}$$

For the sake of fairness, it is assumed that the total transmission power of system is fixed as P_T. Then we can give the following definitions:

$$\begin{aligned} P_R &= \eta P_T, \\ P_S &= (1 - \eta) P_T, \end{aligned} \tag{7}$$

where $\eta \in [0, 1)$ is the normalized power allocation factor for the relay.

Then the received signal at destination in the second phase is given by

$$r_{RD} = \kappa_n r_{S_nR} h_{RD} + n_{D,2}, \tag{8}$$

where $n_{D,2} \sim \mathcal{CN}(0, N_0)$ is the AWGN received at destination with power N_0 in the second phase. Then the corresponding SNR at destination is expressed as

$$\mathrm{SNR}_{D,2}^{(n)} = \frac{\rho_s \gamma_{S_nR} \cdot \rho_r \gamma_{RD}}{\rho_s \gamma_{S_nR} + \rho_r \gamma_{RD} + 1}, \tag{9}$$

where $\rho_r \triangleq P_R/N_0$, $\gamma_{RD} \triangleq |h_{RD}|^2$. Using MRC receiver to combining the two-phase signals from the selected user and the relay, the equivalent SNR at destination is given by

$$\mathrm{SNR}_D^{(n)} = \mathrm{SNR}_{D,1}^{(n)} + \mathrm{SNR}_{D,2}^{(n)}. \tag{10}$$

Then the capacity of the legitimate link can be calculated as

$$C_M^{(n)} = \frac{1}{2}\log_2\left(1 + \mathrm{SNR}_D^{(n)}\right). \tag{11}$$

Then the secrecy rate of the system can be expressed as the difference between C_M and C_R. According to [44], the secrecy rate of the system, with S_n being the selected user node, is given by

$$C_S^{(n)} = \left[C_M^{(n)} - C_R^{(n)}\right]^+ = \frac{1}{2}\left[\log_2 M_n\right]^+, \tag{12}$$

where $M_n \triangleq (1 + \rho_s \gamma_{S_nD} + \rho_s \gamma_{S_nR} \cdot \rho_r \gamma_{RD}/(\rho_s \gamma_{S_nR} + \rho_r \gamma_{RD} + 1))/(1 + \rho_s \gamma_{S_nR})$ and $[x]^+ \triangleq \max\{x, 0\}$.

3. Secrecy-Enhanced User Selection

From the secrecy rate given in (12), the optimal user can be selected based on

$$n^* = \arg\max_{1 \le n \le N} M_n \tag{13}$$

which however requires continuously monitoring the channel parameters of both the direct and relaying links. This imposes a severe load on the system. Moreover, in some specific practical communication scenarios such as ad hoc or sensor networks in [45], the system may only know the channel parameters of either direct links or relaying links of users. For example, if the feedback signaling of the direct (relaying) links is unavailable due to the limited bandwidth or equipment complexity, only the CSI of the relaying (direct) links can be obtained. In this case, we need to consider the user selection criterion based on the relaying links or direct links only.

Considering the scenarios where the system only knows CSI of the direct links, the optimal selection criterion in (13) can be implemented as

$$n_1^* = \arg\max_{1 \le n \le N} \gamma_{S_nD}. \tag{14}$$

This criterion selects the user with optimal channel gain of the direct links, which also guarantees the maximization of instantaneous secrecy rate when only the channel parameters of direct links are obtained by the system.

For other scenarios where the system only knows CSI of the relaying links, the optimal selection criterion in (13) can be implemented as

$$n_2^* = \arg\min_{1\le n\le N} \gamma_{S_nR}. \tag{15}$$

This criterion selects the user with the minimal channel gain of the S_n-R links, which results in maximization of instantaneous secrecy rate by reducing the capacity of the eavesdropping channel.

For convenience of notation, we will refer to the selection criterion in (14) and (15) as Criterion I and Criterion II, respectively. In the following, we will investigate the ergodic secrecy rate (ESR) as well as the asymptotic ESR for Criterion I and Criterion II.

Note the expression of the secrecy rate in (12), when the total transmission power of system P_T is large enough, we observed that the secrecy rate is a monotone decreasing function with respect to γ_{S_nR} and a monotone increasing function with respect to γ_{S_nD}. In the case that only the CSI of the direct links is available, the proposed Criterion I is preferred, while in the case that only the CSI of the relaying links is available, the proposed Criterion II leads to the maximization of the system secrecy rate, since the secrecy rate is decreasing with respect to γ_{S_nR}.

4. Secrecy Rate Analysis

First, to reduce the complexity of the theoretical analysis, an approximation approach [46, Eq. 6] [47, Eq. 2] [48, Eq. 2] should be adopted for (12); namely,

$$C_S^{(n)} \approx \frac{1}{2\ln 2}\left[\ln G_n\right]^+, \tag{16}$$

where $G_n \triangleq (1+\rho_s\gamma_{S_nD}+\min(\rho_s\gamma_{S_nR},\rho_r\gamma_{RD}))/(1+\rho_s\gamma_{S_nR})$.

Note that the approximation in (16) is widely used in existing literatures such as [46–48].

4.1. Criterion I. The probability distribution function of γ_{S_nD} can be written as

$$f_{\gamma_{S_nD}}(y) = \frac{1}{\beta}e^{-y/\beta}. \tag{17}$$

According to the order statistics [49], for Criterion I in (14), the probability distribution function of $\gamma_{S_{n_1}D}$ can be expressed as

$$f_{\gamma_{S_{n_1}D}}(v) = \sum_{n=1}^{N}\binom{N}{n}(-1)^{n-1}\frac{n}{\beta}e^{-nv/\beta}. \tag{18}$$

The ESR of Criterion I can be derived from (16) and written as

$$\overline{R}_1 \triangleq \mathbb{E}\left\{C_S^{(n_1)}\right\} \approx \frac{1}{2\ln 2}\mathbb{E}\left[\ln G_{n_1}\right]^+. \tag{19}$$

Similar to [50, Eq. 16], the operator $[]^+$ can be ignored. Then the tight approximation can be used for the expression of ESR as

$$\overline{R}_1 \approx \frac{1}{2\ln 2}\left\{\mathbb{E}\ln\left[\frac{1}{\rho_s}+\gamma_{S_{n_1}D} + \min\left(\gamma_{S_{n_1}R},\frac{\rho_r}{\rho_s}\gamma_{RD}\right)\right] - \mathbb{E}\ln\left[\frac{1}{\rho_s}+\gamma_{S_{n_1}R}\right]\right\}. \tag{20}$$

Note that the approximation in (20) is a necessary approximation for capacity analysis, such as [50]. Furthermore, both of the approximations in (16) and (20) will be confirmed by the simulation results in the later part of this paper. It is seen that the approximation results match the simulation results very well. In a word, since it is hard to obtain the exact analysis, we have to use the two approximations to derive the results.

Since n_1 is selected only based on γ_{S_nD}, due to the statistical independence between γ_{S_nD} and γ_{S_nR}, the distribution of $\gamma_{S_{n_1}R}$ keeps the same with γ_{S_nR}. Then the ESR of Criterion I can be rewritten as

$$\overline{R}_1 \approx \frac{1}{2\ln 2}\left\{\mathbb{E}\ln\left[\frac{1}{\rho_s}+\gamma_{S_{n_1}D}+\min\left(\gamma_{S_nR},\frac{\rho_r}{\rho_s}\gamma_{RD}\right)\right] - \mathbb{E}\ln\left[\frac{1}{\rho_s}+\gamma_{S_nR}\right]\right\}. \tag{21}$$

According to the full probability formula [46, Eq. 7], the ESR can be written as

$$\begin{aligned}\overline{R}_1 \approx \frac{1}{2\ln 2}\Bigg\{&\underbrace{\mathbb{E}\left[\ln\left(\frac{1}{\rho_s}+\gamma_{S_{n_1}D}+\gamma_{S_nR}\right),\gamma_{S_nR}\le\frac{\rho_r}{\rho_s}\gamma_{RD}\right]}_{H_1}\\ &+\underbrace{\mathbb{E}\left[\ln\left(\frac{1}{\rho_s}+\gamma_{S_{n_1}D}+\frac{\rho_r}{\rho_s}\gamma_{RD}\right),\gamma_{S_nR}>\frac{\rho_r}{\rho_s}\gamma_{RD}\right]}_{H_2}\\ &-\underbrace{\mathbb{E}\ln\left(\frac{1}{\rho_s}+\gamma_{S_nR}\right)}_{H_3}\Bigg\}.\end{aligned} \tag{22}$$

Lemma 1. *Given that $Ei(x)$ is the exponential integral function [51, Eq. 8.211], the definite integral of $Ei(\cdot)$ combined with the exponential function can be written as*

$$\begin{aligned}G_0(a,b,p) &\triangleq \int_0^{+\infty} Ei\left[-(a+bx)\right]e^{-px}dx\\ &= \frac{1}{p}\left[Ei(-a)-e^{ap/b}Ei\left(-a-\frac{ap}{b}\right)\right],\end{aligned} \tag{23}$$

where $a, b, p > 0$.

The proof of Lemma 1 is given in Appendix A.

Theorem 2. *The ESR of Criterion I can be written as*

$$\overline{R}_1 \approx \frac{1}{2\ln 2}\left\{E_2\left(\frac{1}{\alpha\rho_s}\right) - E_2\left(\frac{g_1}{\rho_r}\right) - \sum_{n=1}^{N}\binom{N}{n}(-1)^{n-1}\frac{E_2\left(n/\beta\rho_s\right) - E_2\left(g_1/\rho_r\right)}{1 - n\rho_r/\beta\rho_s g_1}\right\}, \tag{24}$$

with

$$g_1 \triangleq \frac{\rho_r}{\alpha\rho_s} + \frac{1}{\varepsilon}$$
$$E_2(x) \triangleq e^x Ei(-x), \quad x > 0. \tag{25}$$

The proof of Theorem 2 is given in Appendix B.

4.2. Criterion II. Considering the Criterion II in (15), the cumulative distribution function of $\gamma_{S_{n_2}R}$ can be expressed as

$$\begin{aligned} F_{\gamma_{S_{n_2}R}}(u) &= \Pr\left[\min_n\left\{\gamma_{S_nR}\right\} \le u\right] \\ &= 1 - \Pr\left[\min_n\left\{\gamma_{S_nR}\right\} > u\right] \\ &= 1 - \prod_{n=1}^{N}\Pr\left[\gamma_{S_nR} > u\right] \\ &= 1 - \left[1 - \Pr\left(\gamma_{S_nR} \le u\right)\right]^N = 1 - e^{-Nu/\alpha}, \end{aligned} \tag{26}$$

and the corresponding probability distribution function can be written as

$$f_{\gamma_{S_{n_2}R}}(u) = \frac{N}{\alpha}e^{-Nu/\alpha}. \tag{27}$$

Similar to the derivation in (19) and (20), due to the statistical independence between γ_{S_nD} and γ_{S_nR}, the ESR of Criterion II can be derived from (16) and can be written as

$$\begin{aligned} \overline{R}_2 &\triangleq \mathbb{E}\left\{C_S^{(n_2)}\right\} \\ &\approx \frac{1}{2\ln 2}\left\{\mathbb{E}\ln\left[\frac{1}{\rho_s} + \gamma_{S_{n_2}D} + \min\left(\gamma_{S_{n_2}R}, \frac{\rho_r}{\rho_s}\gamma_{RD}\right)\right] - \mathbb{E}\ln\left[\frac{1}{\rho_s} + \gamma_{S_{n_2}R}\right]\right\} \\ &= \frac{1}{2\ln 2}\left\{\mathbb{E}\ln\left[\frac{1}{\rho_s} + \gamma_{S_nD} + \min\left(\gamma_{S_{n_2}R}, \frac{\rho_r}{\rho_s}\gamma_{RD}\right)\right] - \mathbb{E}\ln\left[\frac{1}{\rho_s} + \gamma_{S_{n_2}R}\right]\right\}. \end{aligned} \tag{28}$$

Using the full probability formula [46, Eq. 7] yields

$$\begin{aligned} \overline{R}_2 &\approx \frac{1}{2\ln 2}\left\{\underbrace{\mathbb{E}\left[\ln\left(\frac{1}{\rho_s} + \gamma_{S_nD} + \gamma_{S_{n_2}R}\right), \gamma_{S_{n_2}R} \leqslant \frac{\rho_r}{\rho_s}\gamma_{RD}\right]}_{F_1}\right. \\ &\quad + \underbrace{\mathbb{E}\left[\ln\left(\frac{1}{\rho_s} + \gamma_{S_nD} + \frac{\rho_r}{\rho_s}\gamma_{RD}\right), \gamma_{S_{n_2}R} > \frac{\rho_r}{\rho_s}\gamma_{RD}\right]}_{F_2} \\ &\quad \left. - \underbrace{\mathbb{E}\ln\left(\frac{1}{\rho_s} + \gamma_{S_{n_2}R}\right)}_{F_3}\right\}. \end{aligned} \tag{29}$$

Similar to Theorem 2, substituting (27) and (17) into F_1 in (29) and using Lemma 1, we obtain

$$\begin{aligned} F_1 &= \frac{N\rho_r}{\alpha\rho_s}\left\{\frac{\ln\left(1/\rho_s\right) - E_2\left(g_3/\rho_r\right)}{g_3} - \frac{E_2\left(1/\beta\rho_s\right) - E_2\left(g_3/\rho_r\right)}{g_2}\right\}, \\ F_2 &= \frac{\alpha\rho_s}{N\varepsilon\rho_r}F_1, \end{aligned} \tag{30}$$

where $g_2 \triangleq N\rho_r/\alpha\rho_s - \rho_r/\beta\rho_s + 1/\varepsilon$, $g_3 \triangleq N\rho_r/\alpha\rho_s + 1/\varepsilon$, and $E_2(\cdot)$ is defined in (25).

For the third item of $\overline{R}_2$, substituting (27) into F_3 in (29) and using [51, Eq. 4.337] yield

$$F_3 = \ln\left(\frac{1}{\rho_s}\right) - E_2\left(\frac{N}{\alpha\rho_s}\right). \tag{31}$$

Substituting (30) and (31) into (29), the ESR of Criterion II can be written as

$$\overline{R}_2 \approx \frac{1}{2\ln 2}\left[E_2\left(\frac{N}{\alpha\rho_s}\right) + \frac{\rho_r}{\beta g_2\rho_s}E_2\left(\frac{g_3}{\rho_r}\right) - \frac{g_3}{g_2}E_2\left(\frac{1}{\beta\rho_s}\right)\right]. \tag{32}$$

4.3. Asymptotic Analysis. To reveal the insights into the secrecy performance of different selection criteria with untrusted relay, we will focus on the asymptotic behavior of ESR, where the total transmission power of the system is high and the channel gain of the direct links is large enough.

Lemma 3. *The difference of $E_2(x \to 0)$ and $E_2(y \to 0)$ can be written as*

$$\lim_{x,y\to 0^+}\left[E_2(x) - E_2(y)\right] = \ln\left(\frac{x}{y}\right). \tag{33}$$

The proof of Lemma 3 is given in Appendix C.

Applying Lemma 3 on (24), using the equation $\sum_{n=1}^{N}\binom{N}{n}(-1)^{n-1} = 1$, and removing the infinitesimal, the asymptotic ESR for Criterion I can be rewritten as

$$\overline{R}_1^{\infty} \triangleq \lim_{P_T\to\infty,\beta\to\infty} \overline{R}_1 \approx \frac{1}{2\ln 2}\left[\ln\left(\frac{\beta}{\alpha}\right) - A_N\right], \tag{34}$$

where $A_N \triangleq \sum_{n=1}^{N}\binom{N}{n}(-1)^{n-1}\ln n$.

It is shown that the asymptotic ESR remains linearly with the logarithm of the average channel gain ratio of the the direct link to the relaying link.

Similarly, by using Lemma 3, the asymptotic ESR of Criterion II in (32) can be derived as

$$\overline{R}_2^{\infty} \triangleq \lim_{P_T\to\infty,\beta\to\infty} \overline{R}_2 \approx \frac{1}{2\ln 2}\ln\left(\frac{N\beta}{\alpha}\right). \tag{35}$$

Obviously, the asymptotic ESR of Criterion II increases linearly with the logarithm of the number of users, as well as the average channel gain ratio of the direct link to the relaying link.

Furthermore, when the number of users approaches infinity, the behavior of the ESR performance is investigated. Consider Criterion II, when the number of users $N \to \infty$, the CDF of $\gamma_{S_{n_2}R}$ can be written as

$$\lim_{N\to\infty} F_{\gamma_{S_{n_2}R}}(u) = \lim_{N\to\infty}\left[1 - e^{-Nu/\alpha}\right] = 1. \tag{36}$$

That is to say, when the number of users approaches infinity, $\gamma_{S_{n_2}R} \to 0$. According to (28), the ESR of Criterion II can be derived as

$$\begin{aligned}\lim_{N\to\infty}\overline{R}_2 = {} & \lim_{N\to\infty} \\ & \cdot\frac{1}{2\ln 2}\left\{\mathbb{E}\ln\left[\frac{1}{\rho_s} + \gamma_{S_nD} + \min\left(\gamma_{S_{n_2}R}, \frac{\rho_r}{\rho_s}\gamma_{RD}\right)\right]\right. \\ & \left. - \mathbb{E}\ln\left[\frac{1}{\rho_s} + \gamma_{S_{n_2}R}\right]\right\} = \frac{1}{2\ln 2}\left\{\mathbb{E}\ln\left[\frac{1}{\rho_s} + \gamma_{S_nD}\right]\right. \\ & \left. - \mathbb{E}\ln\left[\frac{1}{\rho_s}\right]\right\} = \frac{1}{2\ln 2}\left\{\mathbb{E}\ln\left[1 + \rho_s\gamma_{S_nD}\right]\right\}.\end{aligned} \tag{37}$$

Using (17) and [51, Eq. 4.337.2], the ESR of Criterion II can be rewritten as

$$\lim_{N\to\infty}\overline{R}_2 = \frac{1}{2\ln 2}e^{1/\beta\rho_s}\mathrm{Ei}\left(-\frac{1}{\beta\rho_s}\right). \tag{38}$$

We can conclude that the ESR of Criterion II is only related to the quality of the main links when the number of users approaches infinity.

5. Numerical Simulation

In this section, numerical simulation results are provided to validate the theoretical analysis for the considered system model. We consider the effects of total transmission power (P_T), the number of user nodes (N), and the distance between the relay and destination (d) on the ergodic secrecy rate as well as the asymptotic ESR, respectively.

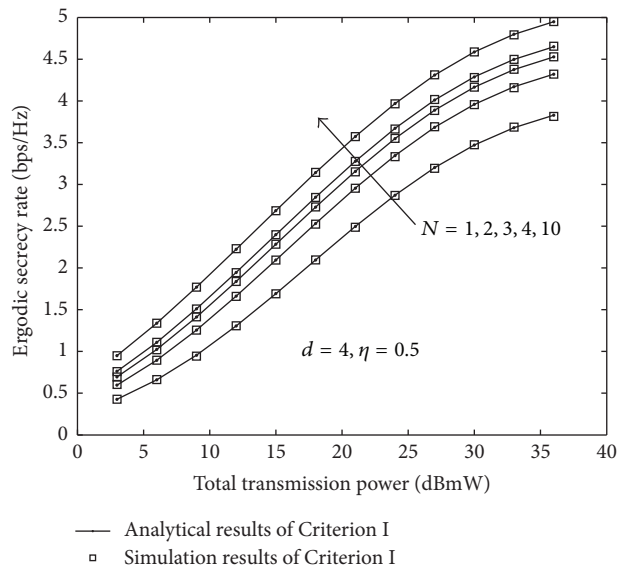


Figure 2: Ergodic secrecy rate of Criterion I versus P_T.

Without loss of generality, it is assumed that three types of nodes constitute a two-dimensional topology. The destination lies at the origin, and the user nodes are placed along x-axis, where the distance between the users and destination is fixed to one. The relay is located along y-axis, and the normalized distance between the relay and destination is denoted by d. As mentioned before, we assume that all links between different nodes are quasistatic Rayleigh fading and stochastically independent between each other. The path loss factor of the wireless channel is set as 4; that is, $\beta = 1, \varepsilon = d^{-4}$, and $\alpha = (1 + d^2)^{-2}$. Note that this assumption can be easily extended to other general topologies. Furthermore, the power of AWGN is assumed to be fixed as $N_0 = 0$ dBmW.

Figure 2 presents the results of analytical ESR for Criterion I in (24) as a function of P_T. For a considerable well condition, we set $d = 4$ and $\eta = 0.5$ and N increases from 1 to 10. We can see from this figure that the analytical ESR curves match the simulation ESR curves well in all regions. In addition, we investigate the effects of number of users on the ESR. Note that the ESR increases with the number of users, as more users can achieve more multiuser diversity because of the independent channel fading. Specifically, the system gain on secrecy capacity grows more slowly as N increases. Similar results can be observed for Criterion II from Figure 3, in which system parameters remain the same as Figure 2.

Figure 4 gives a comparison of ESR performance between the proposed selection criteria and the optimal user selection criterion in (13), with system parameters $d = 2, \eta = 0.5$, and $N = 10$. It is seen from Figure 4 that Criterion I outperforms Criterion II in the low P_T region, while Criterion II gives capacity gain in the high P_T region. Furthermore, the analytical ESR tends to converge to the asymptotic ESR for both Criterion I and Criterion II. We can find that, with low and medium P_T regions, Criterion I approaches the

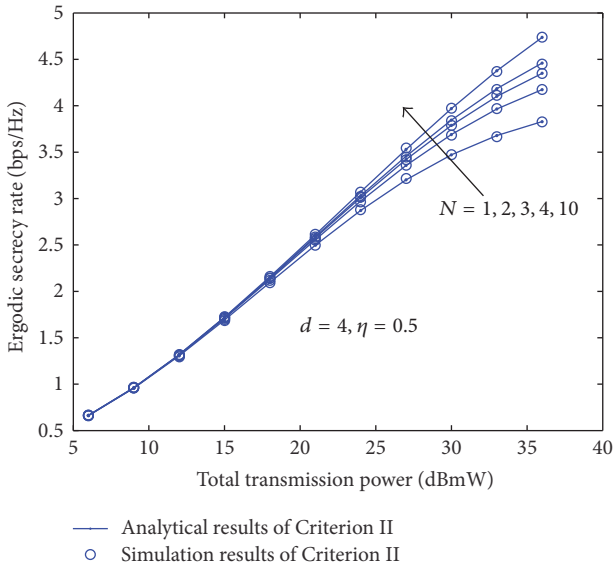


FIGURE 3: Ergodic secrecy rate of Criterion II versus P_T.

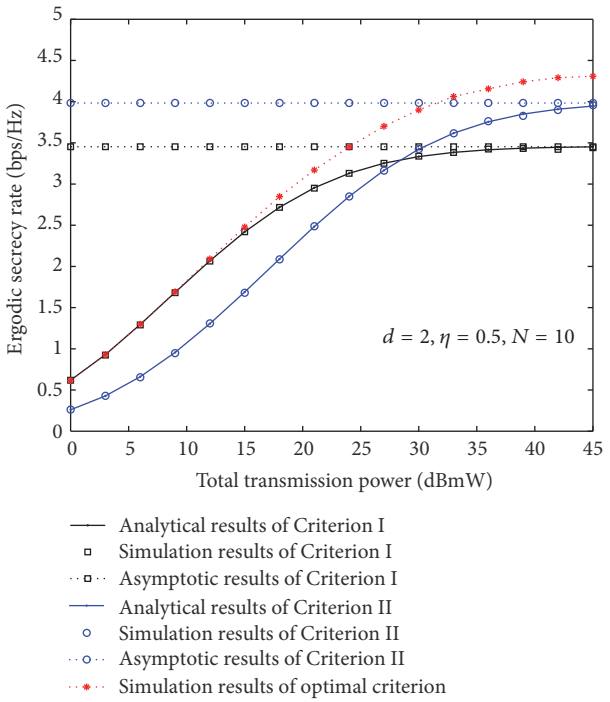


FIGURE 4: Ergodic secrecy rate comparison of Criterion I and Criterion II with $N = 10$.

secure performance of the optimal selection. Also, simulation results validate the analytical results as well as the asymptotic analysis.

Figure 5 demonstrates the effects of the number of users on ESR for Criterion I and Criterion II and the optimal criterion with $P_T = 36$ dBmW, $\eta = 0.5$, and $d = 4$. The number of users changes from 1 to 10. We can see from this figure that the system performance improves rapidly with N. Furthermore, Criterion I holds obvious secrecy

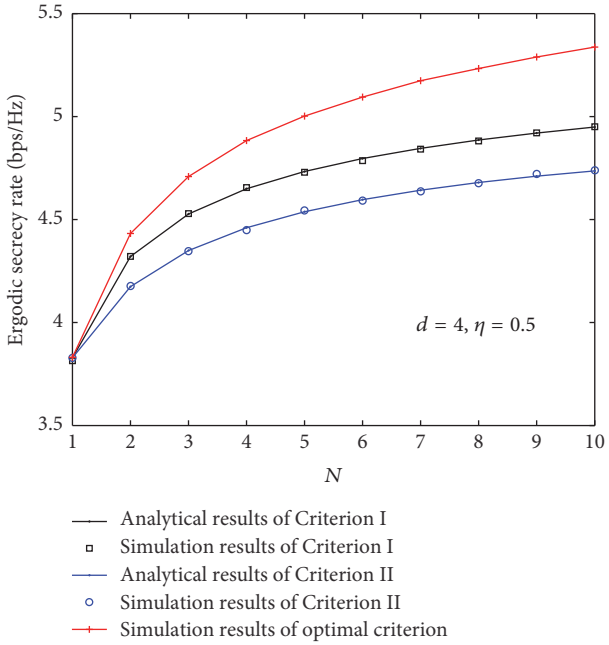


FIGURE 5: Effects of the number of users on ESR with $P_T = 36$ dBmW.

capacity gain than Criterion II for all N values. Similarly, the asymptotic ESR curves match well with the analytical ESR curves, as well as the simulation curves. On the other hand, the optimal criterion, which needs the CSI of both the direct and relaying links, shows better performance than Criterion I and Criterion II, especially when N is large enough. The reason is that Criterion I and Criterion II only utilize either the CSI of the direct links or that of the relaying links, while the optimal criterion benefits from both two types of links. Then the optimal strategy outperforms Criterion I and Criterion II.

Generally speaking, when the direct links are more reliable than the relaying links, Criterion I will be preferred. Conversely, when the relaying links are stronger, Criterion II will be a good choice. In Figure 5, the distance between the relay and destination (d) is large enough; hence the average channel gain of the direct links is much larger than that of the relaying links. In this case, Criterion I has superiority over Criterion II in high P_T region. On the contrary, the average channel gain of the relaying links in Figure 4 is much larger than that of the Figure 5. In high P_T region, Criterion II exhibits better ESR performances, while in low and medium P_T regions, both of the links are interferenced by the noise, Criterion I, which directly increases the capacity of the main channel, leads to the better ESR performance.

Figure 6 depicts the effects of the distance between the relay node and the destination node on ESR for Criterion I and Criterion II and the optimal criterion with $P_T = 36$ dBmW, $\eta = 0.5$, and $N = 10$. The distance parameter d changes from 2 to 10. From the figure, we can see that ESR steadily increases with d, which fits with normal intuitions. Moreover, we find that the optimal criterion outperforms Criterion I and Criterion II, as it utilizes both the direct

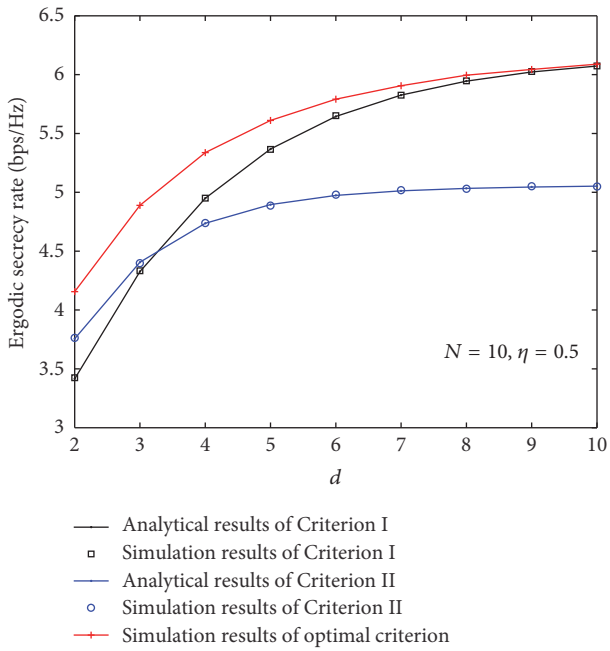


Figure 6: Effects of the distance between destination and relay on ESR with $P_T = 36$ dBmW.

and relay links for the secure transmission. With the system configuration, if the relay node is close to the destination node, that is, $d < 3.2$, Criterion II gives better ESR performance than Criterion I. The reason is that more information can be intercepted if d is within small region, and the eavesdropping channel plays a key role on ESR. Then Criterion II, which can directly reduce the gain of the eavesdropping channel, becomes a better scheme. Due to the pass loss, if the relay node is far from the destination, the average gain of the eavesdropping channel deteriorates rapidly, and the direct link plays more important role than the eavesdropping channel. In this case, Criterion I will be preferable.

6. Conclusion

In this paper, we analyze the effect of untrusted relay on the ergodic secrecy rate of amplify-and-forward relay networks in the presence of direct links and multiple users, where the best user is selected to transmit signal to the relay as well as the destination. To reduce the complexity of implementation, we consider two suboptimal selection criteria which are based on the direct and relaying link, respectively. We investigate the impact of both the direct and relaying links on secrecy performance by deriving the close-form analytical ESR as well as the asymptotic expressions. Simulation results are provided to confirm the theoretical analysis. From the asymptotic expressions and simulation results, it can be found that the asymptotic ESR increases linearly with with the logarithm of the average channel gain ratio of the direct link to the relaying link.

Appendix

A. Proof of Lemma 1

Considering the definition of $G_0(a, b, p)$, we can have

$$\begin{aligned} G_0(a,b,p) &= \int_0^{+\infty} \mathrm{Ei}\left[-(a+bx)\right] e^{-px}\,dx \\ &\overset{(a)}{=} \frac{e^{ap/b}}{b} \int_a^{+\infty} \mathrm{Ei}(-y)\, e^{-(p/b)y}\,dy \\ &\overset{(b)}{=} -\frac{e^{ap/b}}{b} \int_{y=a}^{+\infty} \int_{x=1}^{+\infty} \frac{e^{-yx}}{x}\,dx\, e^{-(p/b)y}\,dy \\ &= -\frac{1}{b} \int_{x=1}^{+\infty} \frac{e^{-ax}\,dx}{x(x+p/b)} \\ &\overset{(c)}{=} \frac{1}{p}\left[\mathrm{Ei}(-a) - e^{ap/b}\mathrm{Ei}\left(-a-\frac{ap}{b}\right)\right], \end{aligned} \tag{A.1}$$

where (a) can be easily fulfilled by the variables substitution, (b) is obtained by using [51, Eq. 8.211], and (c) is decided by using [51, Eq. 3.352.3].

Lemma 1 is proved.

B. Proof of Theorem 2

First, consider the first item of ESR of Criterion I in (22); using probability distribution function $f_{\gamma_{RD}}(z) = (1/\varepsilon)e^{-z/\varepsilon}$ and substituting (17) and (18) into (22), H_1 can be rewritten as

$$\begin{aligned} H_1 &= \mathbb{E}\left\{\ln\left(\frac{1}{\rho_s} + \gamma_{S_{n_1}D} + \gamma_{S_nR}\right), \gamma_{S_nR} \leqslant \frac{\rho_r}{\rho_s}\gamma_{RD}\right\} \\ &= \int_{x=0}^{+\infty} f_{\gamma_{S_nR}}(x) \int_{v=0}^{+\infty} f_{\gamma_{S_{n_1}D}}(v) \int_{z=(\rho_s/\rho_r)x}^{+\infty} f_{\gamma_{RD}}(z) \\ &\cdot \ln\left(\frac{1}{\rho_s} + v + x\right) dz\,dv\,dx \\ &= \int_{x=0}^{+\infty} \frac{1}{\alpha} e^{-x/\alpha} \int_{v=0}^{+\infty} \sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} \frac{n}{\beta} e^{-nv/\beta} \\ &\cdot \ln\left(\frac{1}{\rho_s} + v + x\right) dv \int_{z=(\rho_s/\rho_r)x}^{+\infty} \frac{1}{\varepsilon} e^{-z/\varepsilon} dz\,dx \\ &\overset{(a)}{=} \sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} \int_{x=0}^{+\infty} \frac{1}{\alpha} e^{-x/\alpha} e^{-x\rho_s/\varepsilon\rho_r} \\ &\cdot \left[\ln\left(\frac{1}{\rho_s} + x\right)\right. \\ &\left. - e^{n/\beta\rho_s} e^{nx/\beta} \mathrm{Ei}\left(-\left(\frac{n}{\beta\rho_s} + \frac{nx}{\beta}\right)\right)\right] dx, \end{aligned} \tag{B.1}$$

where (a) is obtained by using [51, Eq. 4.337]. Therefore, substituting (23) into (B.1) and performing basic mathematical manipulations, we obtain the expression of H_1 in (B.2).

The first item of ESR of Criterion I can be written as

$$H_1 = \frac{\rho_r}{\rho_s \alpha} \sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} \cdot \left[\frac{\ln(1/\rho_s)}{g_1} - \frac{E_2(g_1/\rho_r)}{g_1} - \frac{E_2(n/\beta\rho_s) - E_2(g_1/\rho_r)}{g_1 - n\rho_r/\beta\rho_s} \right], \tag{B.2}$$

where g_1 and $E_2(\cdot)$ are defined in (25).

Similarly, by using [51, Eq. 4.337] and (23), the second item of ESR of Criterion I can be expressed as

$$H_2 = \frac{1}{\varepsilon} \sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} \cdot \left[\frac{\ln(1/\rho_s)}{g_1} - \frac{E_2(g_1/\rho_r)}{g_1} - \frac{E_2(n/\beta\rho_s) - E_2(g_1/\rho_r)}{g_1 - n\rho_r/\beta\rho_s} \right]; \tag{B.3}$$

that is, $H_1 = (\rho_r \varepsilon / \rho_s \alpha) H_2$.

Consider the third item of ESI of Criterion I in (22); using probability distribution function $f_{\gamma_{S_n R}}(x) = (1/\alpha) e^{-x/\alpha}$ and substituting [51, Eq. 4.337] into H_3 yield

$$\begin{aligned} H_3 &= \int_0^{+\infty} \ln\left(\frac{1}{\rho_s} + x\right) f_{\gamma_{S_n R}}(x)\, dx \\ &= \int_0^{+\infty} \ln\left(\frac{1}{\rho_s} + x\right) \frac{1}{\alpha} e^{-x/\alpha} dx \\ &= \ln\left(\frac{1}{\rho_s}\right) - e^{1/\alpha\rho_s} \mathrm{Ei}\left(-\frac{1}{\alpha\rho_s}\right). \end{aligned} \tag{B.4}$$

By using the equation $\sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} = 1$ and substituting (B.2), (B.3), and (B.4) into (22), we obtain (24) in Theorem 2.

C. Proof of Lemma 3

By using [51, eq. 8.214] and [51, Eq. 1.121], the series expansion of Ei$(\cdot)$ and e^x can be expressed as

$$\begin{aligned} \mathrm{Ei}(x) &= C + \ln(-x) + \sum_{k=1}^{\infty} \frac{x^k}{k \cdot k!}, \quad x < 0 \\ e^x &= 1 + \sum_{k=1}^{\infty} \frac{x^k}{k!}, \end{aligned} \tag{C.1}$$

where C is a constant parameter.

Substituting (C.1) into (33) and removing the first order infinitesimal, we can obtain

$$\begin{aligned} &\lim_{x,y \to 0^+} [E_2(x) - E_2(y)] = \lim_{x,y \to 0^+} [e^x \mathrm{Ei}(-x) \\ &\quad - e^y \mathrm{Ei}(-y)] = \lim_{x,y \to 0^+} \left\{ \left(1 + \sum_{k=1}^{\infty} \frac{x^k}{k!}\right) \right. \\ &\quad \cdot \left[C + \ln(-x) + \sum_{k=1}^{\infty} \frac{x^k}{k \cdot k!} \right] - \left(1 + \sum_{k=1}^{\infty} \frac{y^k}{k!}\right) \\ &\quad \left. \cdot \left[C + \ln(-y) + \sum_{k=1}^{\infty} \frac{y^k}{k \cdot k!} \right] \right\} \\ &\quad = \lim_{x,y \to 0^+} \left\{ \left[C + \ln(-x) + \sum_{k=1}^{\infty} \frac{x^k}{k \cdot k!} \right] \right. \\ &\quad \left. - \left[C + \ln(-y) + \sum_{k=1}^{\infty} \frac{y^k}{k \cdot k!} \right] \right\} = \lim_{x,y \to 0^+} \{C \\ &\quad + \ln(-x) - C - \ln(-y)\} = \ln\left(\frac{x}{y}\right). \end{aligned} \tag{C.2}$$

Lemma 3 is proved.

Competing Interests

The authors declare that the mentioned received fundings did not lead to any conflict of interests regarding the publication of this manuscript. Also, the authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported by Science and Technology Program of Guangzhou, China (no. 201605131408424), the Scientific Research Project of Guangzhou Municipal University (no. 1201620439), Guangzhou Science of Education Research Program in the 12th Five-Year Plan (no. 1201431075), Qingshanhu Young Scholar Program in GZPYP (no. 2016Q001), the National Science Foundation grants ECCS-1308006, the National Science Foundation of China (no. 61372129/61471229/61601275), and Guangdong Natural Science Funds for Distinguished Young Scholar (no. 2014A030306027).

References

[1] Z. Zhou, Y. Wang, Q. J. Wu, C. N. Yang, and X. Sun, "Effective and effcient global context verifcation for image copy detection," *IEEE Transactions on Information Forensicsand Security*, vol. 12, no. 1, pp. 48–63, 2016.

[2] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 507–518, 2015.

[3] B. Gu, V. S. Sheng, K. Y. Tay, W. Romano, and S. Li, "Incremental support vector learning for ordinal regression," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 26, no. 7, pp. 1403–1416, 2015.

[4] C. Yuan, X. Sun, and R. Lv, "Fingerprint liveness detection based on multi-scale LPQ and PCA," *China Communications*, vol. 13, no. 7, pp. 60–65, 2016.

[5] Y. Zhang, X. Sun, and W. Baowei, "Efficient algorithm for k-barrier coverage based on integer linear programming," *China Communications*, vol. 13, no. 7, pp. 16–23, 2016.

[6] Z. Xia, X. Wang, X. Sun, and B. Wang, "Steganalysis of least significant bit matching using multi-order differences," *Security and Communication Networks*, vol. 7, no. 8, pp. 1283–1291, 2014.

[7] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual verifiable provable data auditing in public cloud storage," *Journal of Internet Technology*, vol. 16, no. 2, pp. 317–323, 2015.

[8] S. Xie and Y. Wang, "Construction of tree network with limited delivery latency in homogeneous wireless sensor networks," *Wireless Personal Communications*, vol. 78, no. 1, pp. 231–246, 2014.

[9] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 340–352, 2016.

[10] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," *Journal of Internet Technology*, vol. 16, no. 1, pp. 171–178, 2015.

[11] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing," *IEICE Transactions on Communications*, vol. 98, no. 1, pp. 190–200, 2015.

[12] Y. Zheng, B. Jeon, D. Xu, Q. M. J. Wu, and H. Zhang, "Image segmentation by generalized hierarchical fuzzy C-means algorithm," *Journal of Intelligent and Fuzzy Systems*, vol. 28, no. 2, pp. 961–973, 2015.

[13] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas Part I: the MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[14] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—part II: the MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[15] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[16] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[17] H.-M. Wang, T. Zheng, and X.-G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: artificial noise vs. artificial fast fading," *IEEE Transactions on Wireless Communications*, vol. 14, no. 1, pp. 94–106, 2015.

[18] N. Romero-Zurita, D. McLernon, and M. Ghogho, "Physical layer security by robust masked beamforming and protected zone optimisation," *IET Communications*, vol. 8, no. 8, pp. 1248–1257, 2014.

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

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

[21] X. Wang, K. Wang, and X.-D. Zhang, "Secure relay beamforming with imperfect channel side information," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2140–2155, 2013.

[22] X. Wang, Z. Zhang, and K. Long, "Secure beamforming for multiple-antenna amplify-and-forward relay networks," *IEEE Transactions on Signal Processing*, vol. 64, no. 6, pp. 1477–1492, 2016.

[23] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Transactions on Communications*, vol. 63, no. 11, pp. 4347–4362, 2015.

[24] L. Fan, X. Lei, P. Fan, and R. Q. Hu, "Outage probability analysis and power allocation for two-way relay networks with user selection and outdated channel state information," *IEEE Communications Letters*, vol. 16, no. 5, pp. 638–641, 2012.

[25] D. S. Michalopoulos, H. A. Suraweera, G. K. Karagiannidis, and R. Schober, "Amplify-and-forward relay selection with outdated channel estimates," *IEEE Transactions on Communications*, vol. 60, no. 5, pp. 1278–1290, 2012.

[26] H. Cui, R. Zhang, L. Song, and B. Jiao, "Relay selection for bidirectional AF relay network with outdated CSI," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 9, pp. 4357–4365, 2013.

[27] D. Deng, L. Fan, R. Zhao, and R. Q. Hu, "Secure communications in multiple amplify-and-forward relay networks with outdated channel state information," *Transactions on Emerging Telecommunications Technologies*, vol. 27, no. 4, pp. 494–503, 2016.

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

[29] S.-I. Kim, I.-M. Kim, and J. Heo, "Secure transmission for multiuser relay networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 3724–3737, 2015.

[30] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Processing Letters*, vol. 22, no. 8, pp. 1147–1151, 2015.

[31] L. Fan, X. Lei, T. Q. Duong, R. Q. Hu, and M. Elkashlan, "Multiuser cognitive relay networks: joint impact of direct and relay communications," *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 5043–5055, 2014.

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

[33] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physicallayer security for full duplex communications with self-interference mitigation," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 329–340, 2016.

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

[35] J. Zhang, C. Yuen, C.-K. Wen, S. Jin, K.-K. Wong, and H. Zhu, "Large system secrecy rate analysis for SWIPT MIMO wiretap channels," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 74–85, 2016.

[36] S. Zhang, L. Fan, M. Peng, and H. V. Poor, "Near-optimal modulo-and-forward scheme for the untrusted relay channel," *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2545–2556, 2016.

[37] X. He and A. Yener, "Cooperation with an untrusted relay: a secrecy perspective," *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, vol. 56, no. 8, pp. 3807–3827, 2010.

[38] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Transactions on Signal Processing*, vol. 62, no. 9, pp. 2185–2199, 2014.

[39] L. Sun, P. Ren, Q. Du, Y. Wang, and Z. Gao, "Security-aware relaying scheme for cooperative networks with untrusted relay nodes," *IEEE Communications Letters*, vol. 19, no. 3, pp. 463–466, 2015.

[40] 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 Communications Letters*, vol. 3, no. 3, pp. 289–292, 2014.

[41] 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 Transactions on Signal Processing*, vol. 60, no. 1, pp. 310–325, 2012.

[42] A. Mukherjee, "Imbalanced beamforming by a multi-antenna source for secure utilization of an untrusted relay," *IEEE Communications Letters*, vol. 17, no. 7, pp. 1309–1312, 2013.

[43] M. Ju, D.-H. Kim, and K.-S. Hwang, "Opportunistic transmission of nonregenerative network with untrusted relay," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 6, pp. 2703–2709, 2015.

[44] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[45] I. Krikidis, J. Thompson, S. Mclaughlin, and N. Goertz, "Amplify-and-forward with partial relay selection," *IEEE Communications Letters*, vol. 12, no. 4, pp. 235–237, 2008.

[46] B. V. Nguyen and K. Kim, "Secrecy outage probability of optimal relay selection for secure AnF cooperative networks," *IEEE Communications Letters*, vol. 19, no. 12, pp. 2086–2089, 2015.

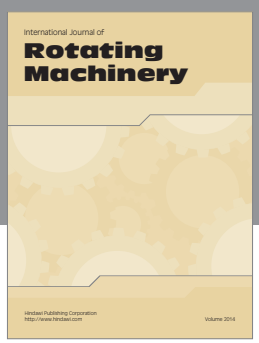
[47] G. Amarasuriya, M. Ardakani, and C. Tellambura, "Output-threshold multiple-relay-selection scheme for cooperative wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 6, pp. 3091–3097, 2010.

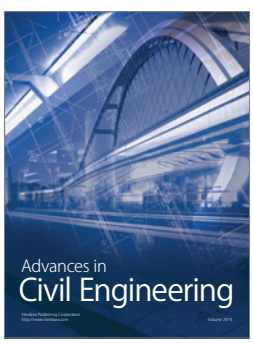
[48] S. Ikki and M. H. Ahmed, "Performance analysis of cooperative diversity wireless networks over Nakagami-m fading channel," *IEEE Communications Letters*, vol. 11, no. 4, pp. 334–336, 2007.

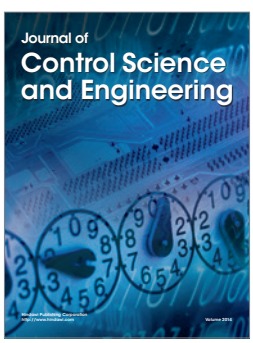
[49] H. A. David and H. N. Nagaraja, *Order Statistics*, John Wiley & Sons, New York, NY, USA, 3rd edition, 2003.

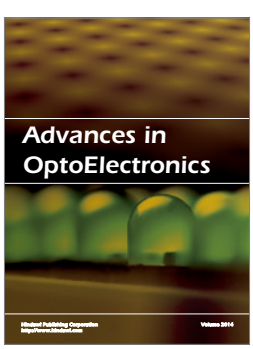
[50] H. Jeon, N. Kim, J. Choit, H. Lee, and J. Ha, "On multiuser secrecy rate in flat fading channel," in *Proceedings of the IEEE Military Communications Conference (MILCOM '09)*, pp. 1–7, Boston, Mass, USA, October 2009.

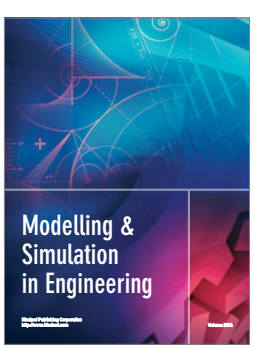
[51] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press, Elsevier, San Diego, Calif, USA, 7th edition, 2007.

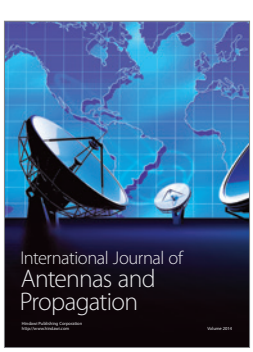


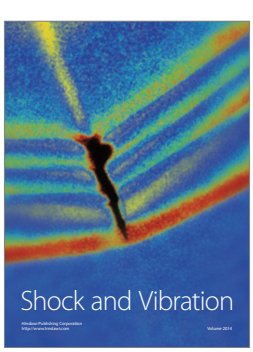


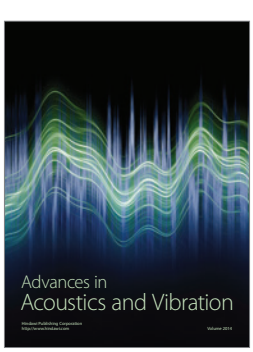












Hindawi

Submit your manuscripts at
https://www.hindawi.com