This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2882178, IEEE Transactions on Vehicular Technology

User-Pair Selection in Multiuser Cooperative Networks With an Untrusted Relay

Bingtao He, Qiang Ni, *Senior Member, IEEE,* Jian Chen, *Member, IEEE,* Long Yang, *Member, IEEE,* and Lu Lv

***Abstract*—This paper investigates the physical-layer security of an amplify-and-forward wireless cooperative network where N source nodes communicate with their corresponding destination nodes under the help of an untrusted relay. In each slot only one user-pair is scheduled to transmit the information, and the destination aided cooperative jamming is adopted to protect information from being intercepted by the untrusted relay. Three user-pair selection schemes have been proposed for the considered system, namely opportunistic user-pair selection (OUS) scheme, greedy user-pair selection (GUS) scheme and genie-aided user-pair selection (GAUS) scheme. Both the secrecy outage probability and average secrecy rate have been studied to evaluate the performance of the OUS and GUS schemes, and the asymptotic analysis has also been obtained. It reveals that, the proposed schemes can improve the secrecy performance for the cooperative multiuser networks as the number of user-pairs increases. We also prove that the achievable diversity order of both OUS scheme and GUS scheme is $\frac{N}{2}$. Finally, numerical and simulation results are presented to validate the accuracy of the developed analytical results.**

***Index Terms*—Physical layer security, untrusted relay networks, cooperative jamming, user-pair selection, multiuser diversity, secrecy outage probability, average secrecy rate.**

I. Introduction

OWING to the broadcast nature of wireless medium, it is a challenging work to ensure the secure transmission in wireless communications, especially for the multiuser systems [1]–[3]. Physical layer security (PLS) is becoming increasingly recognized as a promising technique to safeguard data transmissions by exploiting the randomness of wireless channels [4]–[6]. Therefore, by taking the advantage of the multiuser diversity, user selection and transmission scheduling for secure communications have been widely investigated in [7]–[9]. Recently, cooperative relay has been adopted in multiuser networks not only for the enhancement of reliability and connectivity but also an effective physical layer method to improve the security [10]–[14].

From the perspective of PLS, a friendly relay may protect the confidential message from leaking. However, in public or financial networks, the relay may not always be trusted since the different security clearances of each node and the different levels of access to the information [15], [16]. Therefore, it is necessary to avoid the potential overhearing of the information signal, while utilizing the untrusted relay to improve the reliability of wireless communications. In [17], the achievable secrecy rate for the untrusted relay channel with confidential information is first investigated. The secure communication for a single untrusted multiple-input-multiple-output (MIMO) relay network is considered in [18], where the joint source/relay beamforming scheme has been designed to maximize secrecy rate. In [19], the achievable secrecy rate is presented for the three-node cooperative networks with the consideration of the existing of the source-destination link, and the performance of secrecy outage probability (SOP) is studied in [20]. A novel modulo-and-forward scheme has been proposed in [21] to achieve a full generalized secure diversity gain. In [22], the physical-layer network coding scheme has been proposed in the two-way relay scenario to enhance throughput and guarantee data confidentiality.

As an effective approach among the PLS techniques, cooperative jamming can degrade the channel quality of the eavesdroppers for ensuring security [23], which has attracted many interests in many wireless applications as well as untrusted relay networks [18-26]. In [24], the source based jamming scheme has been proposed to achieve a positive secrecy rate, however, this scheme relies on the random seeds sharing between source and destination. A friendly node can act as a jammer to improve the security by utilizing a proper jamming power [25], [26]. Destination itself can also contribute to deteriorating the received signal at the relay, and the intentional jamming can be subtracted from the received signal at destination by applying the self-interference cancellation [27]. Destination-based jamming (DBJ) promises a positive secrecy rate without the help of external nodes, which has been paid a lot of attention in untrusted relay networks [20-26]. DBJ has been first proposed in [28], in which the upper bound of secrecy rate is obtained. In [29], the optimal power allocation between source and destination has been investigated. In [30], DBJ and precoding schemes have been jointly considered

Manuscript received February 26, 2018; revised July 9, 2018 and October 20, 2018; accepted November 1, 2018. This work was supported in part by the National Natural Foundation of China under grants 61601347 and 61771366, in part by the Royal Society project under Grant IEC\NSFC\170324, in part by the EPSRC IAA project under Grant CSA7114, in part by the EPSRC project under Grant EP/K011693/1, in part by the EU FP7 CROWN project under Grant PIRSES-GA-2013-610524, in part by the Natural Science Basic Research Plan in the Shaanxi Province of China under grant 2017JQ6055, in part by the Fundamental Research Funds for the Central University, in part by the Innovation Fund of Xidian University, in part by the International Postdoctoral Exchange Fellowship Program 2017 from the Office of China Postdoctoral Council, and in part by the "111" Project of China (Grant No. B08038). The associate editor coordinating the review of this paper and approving it for publication was Prof. Wei Song. *(Corresponding Author: Jian Chen)*.

B. He, J. Chen, L. Yang and L. Lv are with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China (e-mail: hebingtao@stu.xidian.edu.cn; jianchen@mail.xidian.edu.cn; lyang@xidian.edu.cn; lulv_xidian@hotmail.com).

Q. Ni is with the School of Computing and Communications, Lancaster University, Lancaster LA1 4WA, U.K. (e-mail: q.ni@lancaster.ac.uk).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2882178, IEEE Transactions on Vehicular Technology

in MIMO untrusted relay networks. The authors in [31] analyze ergodic secrecy rate (ESR) for cooperative multicast networks, in which the energy harvesting destination nodes are considered. For multi-relay scenario, the lower bound of the ergodic secrecy capacity for a single source-destination pair is derived in [32]. It reveals that increasing the number of untrusted relays cannot improve but decrease the achievable secrecy rate. In [33], the secrecy order for both distributed beamforming and opportunistic relaying is obtained. It shows that, as the number of relay increases, the diversity order for the two schemes is limited to one.

In this paper, we consider the secure communication for an untrusted relay network with multiple source-destination pairs. Although a lot of research has been done in multiple source-destination pairs scenario [34], [35], there is a little work investigating for the PLS. In [36], the authors propose an user-pair selection scheme to achieve a better security-reliability tradeoff. For the cooperative communications, In [14], the authors consider a multiuser scenario consisting of one user pair with security requirement and several unclassified user pairs, in which the transmit power of multiple sources and the relay beamformer are jointly designed to maximize the achievable secrecy rate. In [37], the authors consider a relay-aided multiple-source multiple-destination network with the presence of multiple eavesdroppers, and propose two algorithms to maximize the sum secrecy rate. The existing work on cooperative networks with multiple source-destination nodes mainly considers that the relay is trusted, so it can be used to improve the security. However, if the relay is untrusted, especially when the direct link between source and destination does not exist due to the blockage or high attenuation, things will become difficult. To be more specific, we cannot use the direct links to improve the secrecy performance as in [20]. Further, it is well known that for an AF protocol, the signal-to-noise ratio (SNR) of the source-relay-destination link is always lower than that of the source-relay link. How to enjoy the connectivity of the cooperation as well as keeping confidential information from being intercepted by the untrusted relay is deserved to be further studied. Therefore, we introduce DBJ to promise the secure communication. On the other hand, as a low overhead and power saving method, we also introduce the user-pair selection in our work to further improve the security of the considered system. It should be pointed out that, the problem of the best user-pair selection can be regarded as the best relay selection for the single source-destination scenario with multiple relays under the assumption that the relay nodes are trustworthy [35]. When the relay is untrusted, although some solid work [32], [33] reveals that relay selection cannot improve the security, things will become different for the user-pair selection. Hence, we focus our attention on the following two aspects in this paper: 1) The secrecy performance of the considered networks; 2) Whether the secrecy performance can be improved through the multiuser diversity? Our contribution can be summarized as follows:

- We introduce the cooperative jamming technique into an untrusted relay network with N source-destination pairs, and propose three user-pair selection schemes $\big($i.e., 1. opportunistic user-pair selection (OUS); 2. greedy user-pair selection (GUS); 3. genie-aided user-pair selection (GAUS) $\big)$ to improve the secrecy performance for the considered system.
- To evaluate the performance of the proposed the OUS scheme and the GUS scheme, both the SOP and the average secrecy rate (ASR) have been derived in closed-form expressions.
- Asymptotic analysis is presented, which shows that the achievable diversity order for both OUS and GUS is $\frac{N}{2}$. Increasing the number of N will increase the secrecy performance owing to the multiuser diversity, however, the diversity order for the single user-pair with N untrusted relay scenario is limited to one.
- Some simulation results are made to help us analyze the effectiveness of the proposed schemes and the accuracy of the analytical results. Compared with the round-robin user-pair selection scheme, the proposed schemes can achieve a better performance on SOP and ASR due to taking the advantage of multiuser diversity.

The rest of this paper is organized as follows. The system model is described in Section II. The user-pair selection schemes are described in Section III. In Section IV, the performance analysis for the OUS scheme is studied. The analysis of the GUS is given in Section V. Simulation results for the two schemes are presented in Section VI. Finally, Section VII concludes this paper.

Notation: Throughout this paper, $X \sim \mathcal{CN}(a,b)$ denotes that X is a complex Gaussian random variable with mean a and variance b. $[x]^+ \triangleq \max\{0,x\}$, $\Pr(\cdot)$ denotes probability. $f_X(\cdot)$, $F_X(\cdot)$, $F_{X|Y}(\cdot)$ denote the probability density function (PDF), the cumulative distribution function (CDF) and conditional CDF of a random variable X, respectively. $E[X]$ denotes the expectation of a random variable X.

II. System Model

We consider a cooperative network with N legitimate source-destination pairs and one untrusted relay[1], and all of them share the same wireless medium. Time is slotted and each time slot is divided into two phases, only one user-pair with the best secrecy performance is scheduled in a single time slot. Slow fading channels are considered, where the channel coefficient of each wireless link remains static within each slot but varied from one slot to another. It is assumed that the channels are reciprocal. The channel coefficient between source i and relay is denoted by $h_i \sim \mathcal{CN}(0,\sigma_1)$ and $g_i \sim \mathcal{CN}(0,\sigma_2)$ is the channel coefficient between relay and destination i. All the nodes are equipped with a single antenna and all of them are working in a half-duplex mode. We assume that the direct links between sources and destinations are non-existent, due to the long distance or high attenuation of the signals [13], [32]. The noise at relay and destinations has been modeled as independent additive white Gaussian noise (AWGN) with zero mean and unit variance.

[1]We assume that the relay is trusted at the service level and untrusted at the data level.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2882178, IEEE Transactions on Vehicular Technology

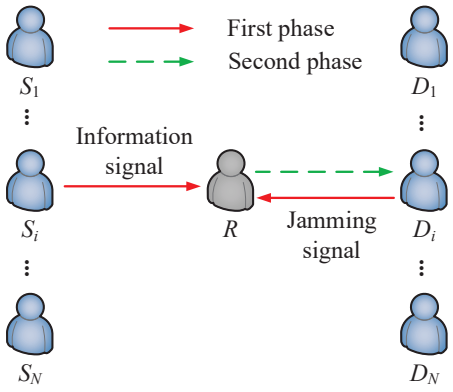


Fig. 1. Two-phase multiple user-pairs cooperative network with an untrusted relay.

For the acquisition of CSI, like the method in [32], source i first broadcasts the request-to-send (RTS) signal to the relays. After receiving the RTS, the relay performs channel estimation to obtain h_i. After that, clear-to-send (CTS) is transmitted from the relay to all sources and all destinations. A pilot signal and the value of h_i are included in the CTS packet. Finally, each destination can obtain the channel state information (CSI) between relay and itself, and CSI of all source-relay links. Besides, a two-step training scheme can also be adopted for the CSI acquirement as in [38, Section II-D].

During the first phase, we assume that the user-pair U_i is scheduled to transmit information, $i \in \{1, ..., N\}$. The source broadcasts information signal x_i to the relay, while the destination sends jamming signal d_i (i.e., artificial noise) to prevent the confidential information from leaking with the same transmission power P. The received signal at the relay is given by

$$y_R = h_i\sqrt{P}x_i + g_i\sqrt{P}d_i + n_R, \tag{1}$$

where n_R is the AWGN at the relay. The signal-to-interference-and-noise-ratio (SINR) at the relay is given by

$$\gamma_{R,i} = \frac{P|h_i|^2}{P|g_i|^2 + 1}. \tag{2}$$

In the second phase, the relay forwards the received signal to the destination with the amplifying coefficient φ_i which is given by $\varphi_i = \sqrt{P/(P|h_i|^2 + P|g_i|^2 + 1)}$. The received signal at destination i can be expressed as

$$\begin{aligned} y_i &= g_i\varphi_i y_R + n_i \\ &= \sqrt{P}\varphi_i h_i g_i x_i + \sqrt{P}\varphi_i g_i g_i d_i + \varphi_i g_i n_R + n_i, \end{aligned} \tag{3}$$

where n_i is the AWGN at the destination. The jamming signal d_i is transmitted by destination i, meanwhile, both h_i and g_i are known at the destination. Thus, destination i can subtract the term $\sqrt{P}\varphi_i g_i g_i d_i$ from its received signal. After the interference cancelation, the received SNR at destination i is given by

$$\gamma_{d,i} = \frac{P^2|h_i|^2|g_i|^2}{P|h_i|^2 + 2P|g_i|^2 + 1}. \tag{4}$$

III. User-Pair Selection

In this section, we propose two user-pair selection schemes which are described as follows.

A. Opportunistic User-pair Selection

In the OUS scheme, the best user-pair which maximizes the instantaneous secrecy rate will be selected in each slot. The achievable secrecy rate can be expressed as

$$R^{OUS} = \left[\max_{i\in\{1,...,N\}} \frac{1}{2}\left(\log_2\left(1 + \frac{P^2|h_i|^2|g_i|^2}{P|h_i|^2+2P|g_i|^2+1}\right) - \log_2\left(1 + \frac{P|h_i|^2}{P|g_i|^2+1}\right)\right)\right]^+. \tag{5}$$

Here, since the other destinations are trusted, the potential overhearing of the destination nodes is not considered in our work. We only focus on the secure communication at the untrusted relay node, and utilize the proper selection scheme to enhance the security for the user-pair system.

On the basis of (5), the SOP can be given by

$$P_{\text{out}}^{OUS} = \Pr\left(\max_{i\in\{1,...,N\}} \frac{1 + \frac{P^2|h_i|^2|g_i|^2}{P|h_i|^2+2P|g_i|^2+1}}{1 + \frac{P|h_i|^2}{P|g_i|^2+1}} < \psi\right), \tag{6}$$

where $\psi = 2^{2R_{\text{th}}}$ and R_{th} is the target secrecy rate. In the high SNR regime, it holds that

$$\begin{aligned} P_{\text{out}}^{OUS} &\approx \Pr\left(\max_{i\in\{1,...,N\}} \frac{\frac{P^2|h_i|^2|g_i|^2}{P|h_i|^2+2P|g_i|^2}}{1+\frac{P|h_i|^2}{P|g_i|^2}} < \psi\right) \\ &= \Pr\left(\max_{i\in\{1,...,N\}} \frac{\alpha_i\beta_i^2}{(\alpha_i+2\beta_i)(\alpha_i+\beta_i)} < \psi\right), \end{aligned} \tag{7}$$

where $\alpha_i = P|h_i|^2$ and $\beta_i = P|g_i|^2$.

B. Greedy User-pair Selection

The GUS scheme is to select the best source node j^* and the best destination node i^* to maximize the instantaneous secrecy rate:

$$R^{GUS} = \left[\max_{j\in\{1,...,N\}}\max_{i\in\{1,...,N\}} \frac{1}{2}\log_2\left(\frac{1+\frac{\alpha_j\beta_i}{\alpha_j+2\beta_i+1}}{1+\frac{\alpha_j}{\beta_i+1}}\right)\right]^+. \tag{8}$$

The GUS scheme for a single transmission slot can be easily implemented as follows:

- The destination user which has the maximum channel gain between destination and relay will be scheduled to receive its information[2], i.e., $i^* = \arg\max_{i\in\{1,...,N\}} |g_i|^2$.
- With the settled destination i^*, the source which can achieve the maximum secrecy rate will be selected to transmit the information, i.e., $j^* =$

[2]The destination node selection can be decoupled from the source node selection due to the following observations. For any source $\bar{j}$ The term $\frac{P^2|h_{\bar{j}}|^2|g_i|^2}{P|h_{\bar{j}}|^2+2P|g_i|^2+1}$ increases as $|g_i|^2$ increases, and the term $\frac{P|h_{\bar{j}}|^2}{P|g_i|^2+1}$ decreases as $|g_i|^2$ increases. Thus, the achievable secrecy rate increases as $|g_i|^2$ increases, which means that selecting the best relay-destination link will always benefit the achievable secrecy rate.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2882178, IEEE Transactions on Vehicular Technology

$\arg \max_{j\in\{1,\ldots,N\}} \frac{1}{2}(\log_2(1+\frac{\mu_j\nu}{\mu_j+2\nu+1})-\log_2(1+\frac{\mu_j}{\nu+1}))$, where $\mu_j = P|h_j|^2$ and $\nu = \max_{i\in\{1,\ldots,N\}} P|g_i|^2$.

For the OUS scheme, each source node only has some information to be transmitted to a specific destination. While, if each source has different data to be transmitted to all destinations (i.e., eHealth [39], social networking [40]), the scheduled destinations are not necessarily the partners of the scheduled sources as in OUS scheme. Therefore, we can use the GUS scheme to achieve a better performance, which can be also regarded as an upper bound of performance for any other situations in considered system. Besides, the topology and the analysis for the scheme can also fit for the secrecy communication between a single source with multiple antennas and multiple destinations via an untrusted relay, and the source node selection can be regarded as the antenna selection.

The achievable secrecy rate for the GUS scheme is given by

$$R^{GUS} = \left[\max_{j\in\{1,\ldots,N\}} \frac{1}{2}\log_2\left(\frac{1+\frac{\mu_j\nu}{\mu_j+2\nu+1}}{1+\frac{\mu_j}{\nu+1}}\right)\right]^+. \quad (9)$$

Following the same operation in (7), the SOP of GUS scheme can be also obtained as

$$P_{\text{out}}^{GUS} \approx \Pr\left(\max_{j\in\{1,\ldots,N\}} \frac{\mu_j\nu^2}{(\mu_j+2\nu)(\mu_j+\nu)} < \psi\right). \quad (10)$$

C. Genie-aided User-pair Selection

For the GAUS scheme, the destination k^* can be selected to help the information receiver (i.e., destination i^*) to send the jamming signal in the first phase. If the jamming signal can be subtracted by destination i^* in the second phase, the optimal instantaneous secrecy rate can be achieved as follow

$$R^{GA} = \left[\max_{\substack{i\in\{1,\ldots,N\};j\in\{1,\ldots,N\}\\ k\in\{1,\ldots,N\}}} \frac{1}{2}\log_2\left(\frac{1+\frac{\alpha_j\beta_i}{\alpha_j+\beta_i+\beta_k+1}}{1+\frac{\alpha_j}{\beta_k+1}}\right)\right]^+. \quad (11)$$

It is worth pointing out that, to ensure the jamming signal d_{k^*} can be subtracted by destination i^*, it is necessary to take the additional operations (i.e., the pseudo-random code sharing between each destination but not opening to the untrusted relay [25], or random seeds sharing by utilizing the reciprocity of the channels [24], [31]). Meanwhile, the CSI between relay and destination k^* should also be provided to the destination i^*. On the other hand, unlike the OUS scheme and the GUS scheme, the term (11) is more complicated and hard for us to give a further analysis. Therefore, we only present the simulation result as a benchmark in Section VI.

In the following two sections, we will investigate the analytical expressions of SOP, secrecy diversity order and ASR for the OUS and GUS schemes. Here, we mainly focus on two types of situations: Case 1. The CSI between relay and selected destination can be fed back to the selected source; Case 2. The CSI between relay and selected destination cannot be fed back to the selected source. For the first case, the source has the knowledge of both the main channel fading coefficient and wiretap channel fading coefficients. Therefore, the coding scheme can be adapted to every realization of the fading coefficient. We characterize the ASR as the fundamental security metric. For the second case, the source cannot know the whole main channel fading coefficient, so there is no choice but to encode the confidential information at a constant rate. Under this circumstance, we characterize the SOP as the fundamental security metric.

IV. Performance Analysis for OUS Scheme

This section provides a comprehensive performance analysis for the OUS scheme.

A. Outage Performance

To derive the SOP of the OUS, we first rewrite the term (7) as follow

$$P_{\text{out}}^{OUS} = \prod_{i=1}^{N} \Pr\left(\frac{X_i\beta_i}{(X_i+2)(X_i+1)} < \psi\right), \quad (12)$$

where $X_i = \frac{\alpha_i}{\beta_i}$, $Z_i = \frac{X_i\beta_i}{(X_i+2)(X_i+1)}$. The PDF of α_i and β_i are $f_{\alpha_i}(x) = \lambda_1 e^{-\lambda_1 x}$, $f_{\beta_i}(x) = \lambda_2 e^{-\lambda_2 x}$, where $\lambda_1 = \frac{1}{P\sigma_1}$, $\lambda_2 = \frac{1}{P\sigma_2}$. The conditional CDF $F_{X_i|\beta_i}$ can be obtain as follows

$$F_{X_i|\beta_i}(x|y) = 1 - e^{-\lambda_1 yx}. \quad (13)$$

The CDF of Z_i takes the form

$$\begin{aligned} F_{Z_i}(z) &= \int_0^\infty F_{Z_i}(z|y) f_{\beta_i}(y)\mathrm{d}y \\ &\overset{(a)}{=} \int_0^\infty \Pr\left(X_i^2 + (3-\frac{y}{z})X_i + 2 \geq 0|y\right) f_{\beta_i}(y)\mathrm{d}y, \end{aligned} \quad (14)$$

where (a) holds when $z > 0$. Since the value range of ψ is 1 to ∞, the obtained expression can fit for any nonnegative target rate R_{th}. Define equation: $X_i^2 + (3-\frac{y}{z})X_i + 2 = 0$ and $\Delta = (\frac{y}{z}-3)^2 - 8$. Then the probability $\Pr\left(X_i^2 + (3-\frac{y}{z})X_i + 2 \geq 0|y\right)$ can be expressed as the summation of three events, corresponding to the following cases

1) $z\epsilon^- \leq \beta_i \leq z\epsilon^+$ ($\Delta \leq 0$);
2) $0 \leq \beta_i < z\epsilon^-$ (the equation has two negative roots);
3) $z\epsilon^+ < \beta_i$ (the equation has two positive roots).

Here $\epsilon^\pm = 3 \pm 2\sqrt{2}$. We have

$$\begin{aligned} &F_{Z_i}(z) \\ &= \int_0^{z\epsilon^-} f_{\beta_i}(y)\mathrm{d}y + \int_{z\epsilon^-}^{z\epsilon^+} f_{\beta_i}(y)\mathrm{d}y + \int_{z\epsilon^+}^{\infty} f_{\beta_i}(y) \\ &\quad \cdot\left[F_{X_i|\beta_i}\left(\frac{\frac{y}{z}-3-\sqrt{\Delta}}{2}\right) + \left(1 - F_{X_i|\beta_i}\left(\frac{\frac{y}{z}-3+\sqrt{\Delta}}{2}\right)\right)\right]\mathrm{d}y \\ &= 1 - e^{-\lambda_2\epsilon^+ z} + \int_{z\epsilon^+}^{\infty} f_{\beta_i}(y)\cdot\left[F_{X_i|\beta_i}\left(\frac{\frac{y}{z}-3-\sqrt{\Delta}}{2}\right)\right. \\ &\qquad \left. + \left(1 - F_{X_i|\beta_i}\left(\frac{\frac{y}{z}-3+\sqrt{\Delta}}{2}\right)\right)\right]\mathrm{d}y \\ &= \int_0^\infty \left[1 - e^{\frac{-\lambda_1 z}{2\lambda_2}(y+\sqrt{\lambda_2}\epsilon^+)\left(y+2\sqrt{2\lambda_2}-\sqrt{y^2+4\sqrt{2\lambda_2}y}\right)}\right. \\ &\qquad \left. + e^{\frac{-\lambda_1 z}{2\lambda_2}(y+\sqrt{\lambda_2}\epsilon^+)\left(y+2\sqrt{2\lambda_2}+\sqrt{y^2+4\sqrt{2\lambda_2}y}\right)}\right] \\ &\qquad \cdot z\sqrt{\lambda_2}e^{-\sqrt{\lambda_2}(y+\sqrt{\lambda_2}\epsilon^+)z}\mathrm{d}y + 1 - e^{-\lambda_2\epsilon^+ z}. \end{aligned} \quad (15)$$

Neither integration formulas nor techniques in the literature can be utilized to solve (15) in closed-form. Fortunately,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2882178, IEEE Transactions on Vehicular Technology

an approximation can be given with the help of Gaussian-Chebyshev quadrature [41]. Then we have the following theorem.

Theorem 1: The SOP of the OUS scheme can be approximated as

$$P_{\text{out}}^{OUS} \approx \left(1 - e^{-\lambda_2 \epsilon^+ \psi} + \psi \sum_{g=1}^{G} a_g \sqrt{\lambda_2} e^{-b_1(\tau_g)\psi} \cdot \left(1 - e^{-b_2(\tau_g)^- \psi} + e^{-b_2(\tau_g)^+ \psi}\right)\right)^N, \tag{16}$$

where $b_1(x) = \sqrt{\lambda_2}(x + \sqrt{\lambda_2}\epsilon^+)$, $b_2(x)^{\pm} = \frac{\lambda_1}{2\lambda_2}(x + \sqrt{\lambda_2}\epsilon^+)\left(x + 2\sqrt{2\lambda_2} \pm \sqrt{x^2 + 4\sqrt{2\lambda_2}x}\right)$, $\tau_g = \left(\frac{\sqrt{t_g}}{1-\sqrt{t_g}}\right)^2$, $\omega_g = \frac{2\pi}{2G+1} t_g$, $a_g = \omega_g \frac{\sqrt{1-t_g}/\sqrt{t_g}}{(1-\sqrt{t_g})^3}$, $t_g = \cos^2\left(\frac{2g-1}{2G+1}\frac{\pi}{2}\right)$ and G is a complexity-accuracy tradeoff parameter.

Proof: Please see Appendix A. ∎

Then, we will provide the following proposition.

Proposition 1: The SOP of the OUS scheme is bounded by

$$\underbrace{\left\{1 - e^{\xi_1 2\psi}\left[\Gamma(1, \xi_2\psi) - \xi_3\sqrt{\psi}\Gamma(\frac{1}{2}, \xi_2\psi)\right]\right\}^N}_{P_{\text{UB}}^{OUS}} \geq P_{\text{out}}^{OUS} \geq \underbrace{\left\{1 - e^{\xi_1 \frac{\psi}{2}}\left[\Gamma(1, \xi_2\frac{\psi}{4}) - \xi_3\sqrt{\frac{\psi}{4}}\Gamma(\frac{1}{2}, \xi_2\frac{\psi}{4})\right]\right\}^N}_{P_{\text{LB}}^{OUS}}, \tag{17}$$

where $\xi_1 = -\lambda_2 + \frac{\lambda_1}{2} + \frac{(\lambda_2)^2}{2\lambda_1}$, $\xi_2 = \lambda_1(3 + \frac{\lambda_2}{\lambda_1})^2$, $\xi_3 = \frac{\lambda_2}{\sqrt{\lambda_1}}$ and $\Gamma(a, x)$ is the incomplete gamma function defined in [42, eq.(8.350.2)].

Proof: Please see Appendix B. ∎

With the help of **Proposition 1**, we can also analyze the diversity gain achieved by the OUS scheme. The diversity order of the secure communication is defined by $d = \lim_{P\to\infty} \frac{-\log P_{\text{out}}}{\log P}$, then the diversity order can be obtained as follows.

Theorem 2: The diversity order of the OUS scheme is $\frac{N}{2}$.

Proof: Please see Appendix C. ∎

In trusted relay networks, the best relay selection for the "N *relays with a single user-pair*" scenario can achieve the same diversity order as the best user-pair selection for the "N *user-pairs with a single relay*" scenario, namely both of them can achieve a diversity order of N. When the relay is untrusted, the diversity order of "N *user-pairs with a single relay*" scenario reduces to $\frac{N}{2}$. However, the diversity order of "N *relays with a single user-pair*" scenario is limited to one. This phenomenon is mainly because of the following reasons:

1) For "N *relays with a single user-pair*" scenario, relay selection can only improve the main channel capacity (end-to-end capacity for the source-destination pair), while making no effort to the wiretap channel capacity (maximum capacity of all untrusted relays). For "N *user-pairs with a single relay*" scenario, both main channel capacity and wiretap channel capacity will be influenced by user-pair selection. Selecting the proper user-pair can improve the main channel capacity while impairing the wiretap channel capacity, thus improving the secrecy capacity.
2) With the increasing N, more relays can be utilized to improve the main channel capacity in "N *relays with a single user-pair*" scenario. However, it will also increase the wiretap channel capacity due to the increased number of eavesdroppers. Therefore, increasing the number of relay will make no contribution for relay selection to improve the secrecy order. On the other hand, in "N *user-pairs with a single relay*" scenario the increased user-pairs will provide the selection more chances to achieve a higher user diversity gain.

B. Average secrecy rate

ASR is the maximum achievable rate averaged over all realizations of the fading coefficients. Following [43], the ASR of the OUS scheme can be given by

$$\begin{aligned} R_{\text{ASR}}^{OUS} &= E\left\{\left[\frac{1}{2}\log_2\left(\max_{i\in\{1,\ldots,N\}} \frac{\alpha_i\beta_i^2}{(\alpha_i+2\beta_i)(\alpha_i+\beta_i)}\right)\right]^+\right\} \\ &= \frac{1}{2\ln 2}\int_1^\infty \ln(z) f_{Z_{i^*}}(z)\mathrm{d}z \\ &= \frac{1}{2\ln 2}\int_1^\infty \frac{1-F_{Z_{i^*}}(z)}{z}\mathrm{d}z. \end{aligned} \tag{18}$$

The CDF of Z_i in (15) can be rewrite as follows

$$F_{Z_i}(z) = 1 - \int_0^\infty \left(e^{-b_2(y)^- z} - e^{-b_2(y)^+ z}\right) z\sqrt{\lambda_2} e^{-b_1(y)z}\mathrm{d}y. \tag{19}$$

Then we can also obtain the approximation of $F_{Z_{i^*}}(z)$ as follow

$$F_{Z_{i^*}}(z) = 1 + \sum_{n=1}^{N} \sum_{k_1+\ldots+k_G=n} \sum_{\substack{m_1+\ldots+m_G\leq n;\\ m_g\leq k_g,\forall g}} \binom{N}{n} \frac{n!(z\sqrt{\lambda_2})^n}{k_1!,\ldots,k_G!} (-1)^{\sum_{g=1}^{G} m_g+n} \prod_{g=1}^{G} \binom{k_g}{m_g} a_g{}^{k_g} e^{-\Lambda_1 z}, \tag{20}$$

where $\Lambda_1 = \sum_{g=1}^{G} k_g\left(b_1(\tau_g) + b_2(\tau_g)^-\right) + m_g b_3(\tau_g)$ and $b_3(x) = \frac{\lambda_1}{\lambda_2}(x + \sqrt{\lambda_2}\epsilon^+)\sqrt{x^2 + 4\sqrt{2\lambda_2}x}$. By using [42, eq.(3.381.3)], we have

Theorem 3: The ASR of the OUS scheme can be obtained as

$$R_{\text{ASR}}^{OUS} \approx \sum_{n=1}^{N} \sum_{k_1+,\ldots,+k_G=n} \sum_{\substack{m_1+,\ldots,+m_G\leq n;\\ m_g\leq k_g,\forall g}} \binom{N}{n} \frac{n!(\sqrt{\lambda_2})^n}{k_1!,\ldots,k_G!} \frac{(-1)^{\sum_{g=1}^{G} m_g+n+1}}{2\ln 2} \prod_{g=1}^{G} \binom{k_g}{m_g} a_g{}^{k_g} \Lambda_1^{-n}\Gamma(n, \Lambda_1). \tag{21}$$

Then we will provide the lower bound of ASR for the OUS scheme.

Proposition 2: The ASR of the OUS scheme is lower

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2882178, IEEE Transactions on Vehicular Technology

bounded by

$$R_{ASR}^{OUS} \geq \frac{1}{2\ln 2}\Bigg[\sum_{n=0}^{N-1}\Big(\frac{c_{n,1}^{s,2}\lambda_2}{\lambda_1}+\frac{2c_{n,2}^{s,2}\lambda_1}{\lambda_2}\Big)\Upsilon_{\lambda_1}-\frac{n(c_{n,1}^{s,2}+2c_{n,2}^{s,2})}{n+1}\Upsilon_{\lambda_{n+1}^{s,2}} - \sum_{n_1=0}^{N-1}\sum_{n_2=0}^{N-1} c_{n_1,1}^{s,2}c_{n_2,2}^{s,2}\Big\{\Psi_1(\lambda_1,\lambda_2,n_1)+\Psi_1(\lambda_2,\lambda_1,n_2) +\Psi_2(2)+\Psi_3(2)\Big\}+c_{n_1,1}^{s,3}c_{n_2,3}^{s,3}\Big\{\Psi_1(\lambda_1,\lambda_3,n_1) +\Psi_1(\lambda_3,\lambda_1,n_2)+\Psi_2(3)+\Psi_3(3)\Big\}\Bigg]^+, \tag{22}$$

where $\Psi_2(x)=\underset{\lambda_1=\lambda_x}{\Delta}\{1+\Upsilon_{\lambda_1}\}+\underset{\lambda_1\neq\lambda_x}{\Delta}\left\{\frac{\lambda_x\Upsilon_{\lambda_1}-\lambda_1\Upsilon_{\lambda_x}}{\lambda_x-\lambda_1}\right\}$, $\Psi_1(x,y,n)=\frac{nx(x+y)}{(n+1)(x+y)-y}\left(\frac{\Upsilon_y}{y}-\frac{\Upsilon_{(n+1)(x+y)}}{(n+1)(x+y)}\right)$, $\Psi_3(x)=\underset{n_1=n_2}{\Delta}\left\{1+\Upsilon_{\lambda_{n_1+1}^{s,x}}\right\}+\underset{n_1\neq n_2}{\Delta}\left\{\frac{\lambda_{n_2+1}^{s,x}\Upsilon_{\lambda_{n_1+1}^{s,x}}-\lambda_{n_1+1}^{s,x}\Upsilon_{\lambda_{n_2+1}^{s,x}}}{\lambda_{n_2-n_1}^{s,x}}\right\}$, $c_{n,x}^{s,y}=\frac{N\binom{N-1}{n}(-1)^n\lambda_x}{\lambda_1\lambda_y/\lambda_x+\lambda_n^{s,y}}$, $\Upsilon_x=-\mathcal{C}-\ln(x)$, $\lambda_n^{s,x}=n(\lambda_1+\lambda_x)$, $\lambda_3=\frac{\lambda_2}{2}$, $\mathcal{C}$ is the Euler constant defined in [42, eq.(8.367.1)], and we define $\underset{B}{\Delta}\{A\}$ as: $\underset{B}{\Delta}\{A\}=A$ if the condition B holds and $\underset{B}{\Delta}\{A\}=0$ otherwise.

Proof: Please see Appendix D. ∎

V. Performance Analysis for GUS Scheme

The analysis of the GUS scheme will be presented in this section.

A. Outage Performance

Following the term (10), the SOP of GUS can be rewritten as

$$P_{\text{out}}^{GUS}=\underbrace{\int_0^\infty\prod_{j=1}^{N}\Pr\left(\frac{\hat{X}_j y}{(\hat{X}_j+2)(\hat{X}_j+1)}<\psi\right)f_\nu(y)\mathrm{d}y}_{F_{\widehat{Z}}(\psi)}, \tag{23}$$

where $\hat{X}_j=\frac{\alpha_j}{\nu}$. The PDF of ν can be given by

$$f_\nu(y)=N\sum_{n=0}^{N-1}\binom{N-1}{n}(-1)^n\lambda_2 e^{-(n+1)\lambda_2 y}. \tag{24}$$

The CDF $F_{\widehat{Z}}(z)$ can be obtained as

$$F_{\widehat{Z}}(z)=\int_0^\infty\left[1-e^{-b_2(y)^- z}+e^{-b_2(y)^+ z}\right]^N z\sqrt{\lambda_2}b_4(y,z)\mathrm{d}y+\int_0^{z\epsilon^+}f_\nu(y)\mathrm{d}y, \tag{25}$$

where $b_4(y,z)=N\sum_{n=0}^{N-1}\binom{N-1}{n}(-1)^n e^{-(n+1)\sqrt{\lambda_2}(x+\sqrt{\lambda_2}\epsilon^+)z}$. With the help of Gaussian-Chebyshev quadrature [41, eq. (25.4.42)], we can get the following theorem.

Theorem 4: The SOP of the GUS scheme can be approximated as

$$P_{\text{out}}^{GUS}\approx(1-e^{-\lambda_2\epsilon^+\psi})^N+\psi\sum_{g=1}^{G}a_g\sqrt{\lambda_2}b_4(\tau_g,\psi)\cdot\left[1-e^{-b_2(\tau_g)^-\psi}+e^{-b_2(\tau_g)^+\psi}\right]^N, \tag{26}$$

where a_g and τ_g have been defined before. The bound of SOP for GUS scheme is provided as follows.

Proposition 3: The SOP of the GUS scheme is bounded by

$$\underbrace{A(4\psi)+\widetilde{\sum_{k,n}}\zeta_{4\psi}{}^{N-k}\lambda_2 l_k^{4\psi}e^{(\theta_k^n l_k^{4\psi})^2}\mathrm{erfc}\left(\theta_k^n l_k^{4\psi}+\frac{4\psi}{l_k^{4\psi}}\right)}_{P_{\text{UB}}^{GUS}}\geq P_{\text{out}}^{GUS}\geq\underbrace{A(\psi)+\widetilde{\sum_{k,n}}\zeta_{\psi}{}^{N-k}\lambda_2 l_k^{\psi}e^{(\theta_k^n l_k^{\psi})^2}\mathrm{erfc}\left(\theta_k^n l_k^{\psi}+\frac{\psi}{l_k^{\psi}}\right)}_{P_{\text{LB}}^{GUS}}, \tag{27}$$

where $\widetilde{\sum_{k,n}}=\sum_{k=1}^{N}\sum_{n=0}^{N-1}\binom{N}{k}\binom{N-1}{n}(-1)^n N\sqrt{\pi}$, $\zeta_x=1-e^{-\lambda_1 2x}$, $l_k^x=\sqrt{\frac{x}{4\lambda_1 k}}$, $\theta_k^n=\lambda_2(n+1)-\lambda_1 k$, $A(x)=(1-e^{-\lambda_1 2x})^N\left(1-(1-e^{-\lambda_2 2x})^N\right)+(1-e^{-\lambda_2 2x})^N$ and $\mathrm{erfc}(x)\triangleq 1-\frac{2}{\sqrt{\pi}}\int_0^x\exp(-t^2)\mathrm{d}t$ is the complementary error function defined in [42, eq.(8.250.4)].

Proof: Please see Appendix E. ∎

Following the **Proposition 3**, the diversity order can be obtained as follows.

Theorem 5: The diversity order of the GUS scheme is $\frac{N}{2}$.

Proof: Please see Appendix F. ∎

It can be noticed that the achievable diversity orders for the OUS and GUS schemes are the same. That is to say, although more flexibility is introduced to the GUS scheme, the existing of the untrusted relay will be the bottleneck for GUS to achieve a better diversity performance.

B. Average secrecy rate

The ASR of the GUS scheme can be given by

$$R_{\text{ASR}}^{GUS}=E\left\{\left[\frac{1}{2}\log_2\left(\max_{j\in\{1,\ldots,N\}}\frac{\alpha_j\nu^2}{(\alpha_j+2\nu)(\alpha_j+\nu)}\right)\right]^+\right\}=\frac{1}{2\ln 2}\int_1^\infty\frac{1-F_{\widehat{Z}}(z)}{z}\mathrm{d}z. \tag{28}$$

First, we rewrite $F_{\widehat{Z}}(z)$ as

$$F_{\widehat{Z}}(z)=z\int_0^\infty\sum_{n_1=1}^{N}\binom{N}{n_1}\left(e^{-b_2(y)^+ z}-e^{-b_2(y)^- z}\right)^{n_1}\cdot\sqrt{\lambda_2}b_4(y,z)\mathrm{d}y+1. \tag{29}$$

Then the approximation of $F_{\widehat{Z}}(z)$ can be also given by

$$F_{\widehat{Z}}(z)\approx 1+z\sum_{g=1}^{G}a_g\sum_{n_1=1}^{N}\binom{N}{n_1}\left(e^{-b_2(\tau_g)^+ z}-e^{-b_2(\tau_g)^- z}\right)^{n_1}\cdot N\sum_{n_2=0}^{N-1}\binom{N-1}{n_2}(-1)^{n_2}\sqrt{\lambda_2}e^{-(n_2+1)b_1(\tau_g)z}. \tag{30}$$

After taking some manipulations for the gotten $F_{\widehat{Z}}(z)$, the following theorem can be obtained.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2882178, IEEE Transactions on Vehicular Technology

Theorem 6: The ASR of the GUS scheme is approximated as

$$R_{\rm ASR}^{GUS} \approx N \sum_{n_1=1}^{N} \sum_{n_2=0}^{N-1} \sum_{n_3=0}^{n_1} \sum_{g=1}^{G} \binom{N}{n_1}\binom{N-1}{n_2}\binom{n_1}{n_3} (-1)^{n_2+n_3+1} \frac{\sqrt{\lambda_2 a_g}}{2\ln 2\Phi(\tau_g)} e^{-\Phi(\tau_g)}, \tag{31}$$

where $\Phi(x) = (n_1 - n_3)b_2(x)^+ + n_3 b_2(x)^- + (n_2+1)b_1(x)$. Then we will also provide the lower bound for GUS.

Proposition 4: The ASR of the GUS scheme is lower bounded by

$$R_{\rm ASR}^{GUS} \geq \left[\sum_{n=0}^{N-1} \binom{N-1}{n}(-1)^n \frac{\Upsilon_{(n+1)\lambda_1} + \Upsilon_{(n+1)\lambda_2} - \Upsilon_{(n+1)\frac{\lambda_2}{2}}}{2\ln 2 \cdot (n+1)/N} - \sum_{n_1=1}^{N} \sum_{n_2=0}^{N-1} \frac{\binom{N}{n_1}\binom{N-1}{n_2}(-1)^{n_1+n_2+1}\lambda_2}{2\ln 2/N} \left\{ \Delta_{\xi_5=2\xi_4} \left\{ \frac{1}{2\xi_4} \right\} + \Delta_{\xi_5 \neq 2\xi_4} \left\{ \frac{\Upsilon_{\xi_4} - \Upsilon_{\frac{\xi_5}{2}}}{\xi_5 - 2\xi_4} \right\} + \frac{\ln(\xi_4) - \ln(\xi_5)}{\xi_6} \right\} \right]^+, \tag{32}$$

where $\xi_4 = n_1\lambda_1$, $\xi_5 = (n_2+1)\lambda_2$, and $\xi_6 = \xi_4(\ln(\xi_4) - \ln(\xi_5))$ if $\xi_4 = \xi_5$, $\xi_6 = \xi_4 - \xi_5$ otherwise.

Proof: Please see Appendix G. ■

VI. Numerical Results

This section presents some numerical results to demonstrate the performance of the proposed schemes. Without loss of generality, the following parameters will be used throughout this section. The target secrecy rate is set to be $R_{\rm th} = 1$ bit per channel use (BPCU), and $\sigma_1 = \sigma_2 = 1$ if there is no additional description in the figure. The Gaussian-Chebyshev parameter is chosen as $G = 11$. We use "SNR" to denote the power levels in all figures, since the unit variance of noise is considered at the relay node and each destination. The simulation results of the GAUS scheme will be provided in this section. We also present 3 benchmark schemes as the comparisons: 1. the round-robin user-pair selection (RRUS) in the considered networks; 2. conventional maximum transmission rate user-pair selection without cooperative jamming (CUS) [35]; 3. the best relay selection (BRS) in "N *untrusted relays with a single user-pair*" scenario [32].

A. Outage Performance

Fig. 2 and Fig. 3, show the outage performance of the OUS and GUS schemes for $N = 2$ and 3. Besides, some benchmark schemes are presented dispersedly in the two figures. The derived approximated results agree well with the simulations, and the lower bound of SOP also presents a good match for a large SNR. It can be observed that, the GUS scheme achieves almost the same secrecy performance of the GAUS scheme, which indicates that the GUS scheme can provide the near-optimal secrecy performance without the collaboration among destinations. From the curve of the CUS scheme, we can observe that conventional user-pair selection scheme without cooperative jamming cannot ensure the secure communication due to the overhearing of the untrusted relay. All of the proposed schemes outperform the round-robin scheme since their diversity gain can be improved when more users can be scheduled. It can be seen from the BRS scheme that, increasing the number of N makes little effect on the best relay selection scheme in "N *relays with a single user-pair*" scenario, which is in agreement with our previous analysis in Section IV. Comparing Fig. 2 and Fig. 3, it can be found that GUS outperforms OUS at the outage performance. The reason is that, there are N^2 combinations of source-relay link and relay-destination link for GUS to choose from, however, there are only N combinations for OUS. Therefore, there is more likely for the GUS scheme to achieve a lower secrecy outage.

Fig. 4 shows the diversity order of the OUS and GUS schemes. Since the effectiveness of the derived lower bound and the approximation expression have already been verified in Fig. 2 and Fig. 3, we only provide theoretical curves in this figure. The lower bounds perfectly match the derived

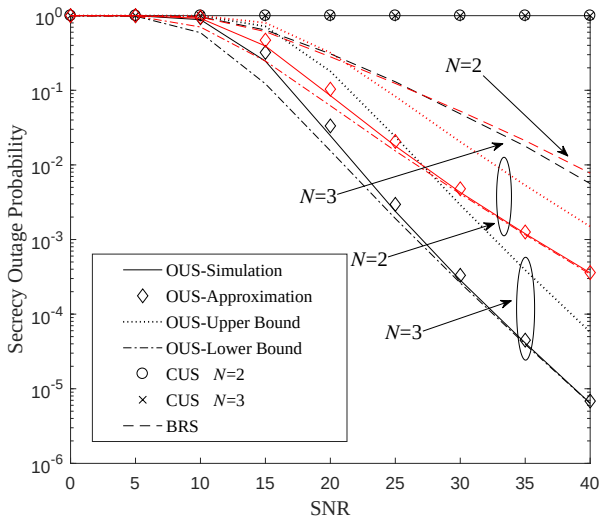


Fig. 2. Secrecy outage probability vs SNR for the OUS scheme, with user-pair number $N = 2$, 3.

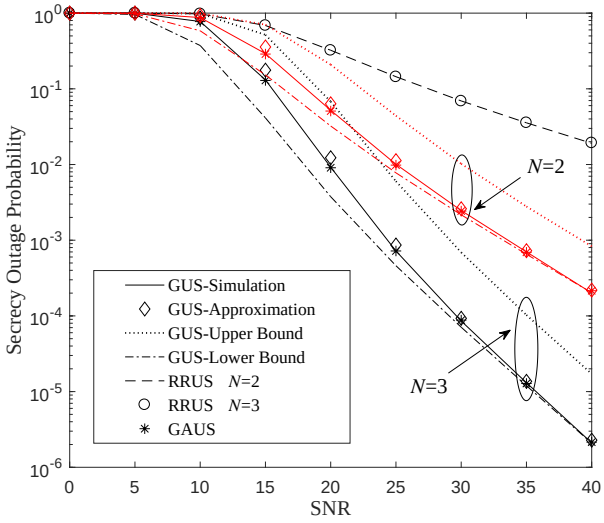


Fig. 3. Secrecy outage probability vs SNR for the GUS scheme, with user-pair number $N = 2$, 3.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2882178, IEEE Transactions on Vehicular Technology

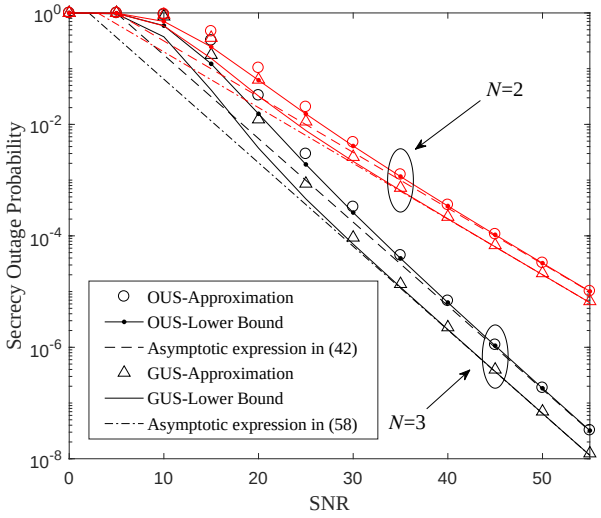


Fig. 4. Asymptotic secrecy outage probability vs SNR for the two schemes, with user-pair number $N = 2, 3$.

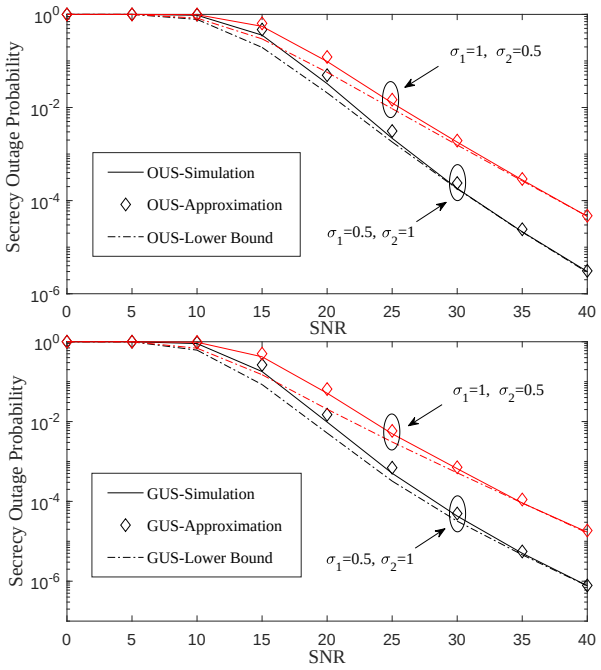


Fig. 5. Secrecy outage probability vs SNR for the two schemes, with different σ_1, σ_2 and user-pair number $N = 3$.

asymptotic results in (42) and (58), which confirms that the diversity order of the OUS scheme and the GUS scheme is $\frac{N}{2}$. There is another interesting observation in the figure. As N increases, the SOP curves of the two schemes can achieve the same slop, however, the gap between the OUS scheme and the GUS scheme becomes larger with the increased N. That is to say, increasing the transmission power P can achieve the same enhancement of the secrecy outage performance for the two schemes, while increasing the number of user-pair N will boost the enhancement of secrecy outage performance for the GUS scheme.

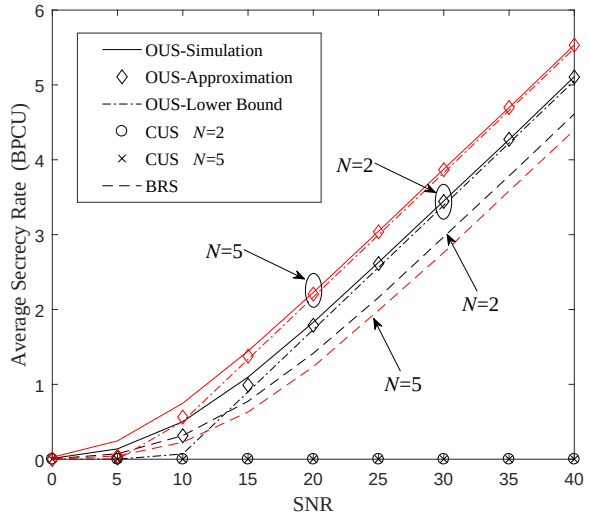


Fig. 6. Average secrecy rate vs SNR for the OUS schemes, with user-pair number $N = 2, 5$.

Fig. 5 presents the secrecy outage probability of the two schemes with different σ_1, σ_2. It can be observed that, there is a great performance loss for the two schemes as the decrease in σ_2. This phenomenon is due to the following two reasons: 1) With the decreasing σ_2, the main channel will be deteriorated due to the deterioration of the general relay-destination link condition. 2) The wiretap channels are not impeded by the decreasing σ_2, while the impact of the jamming signal is crippled. In contrast, for the decreased σ_1, there is less performance loss or even better outage performance in the high SNR regimes. As the σ_1 decreases, both the main channel and the wiretap channel will be influenced. The performance loss in the small SNR regimes is caused by the transmission outage due to the poor source-relay link condition. On the other hand, since the general condition of the relay-destination link is better than the source-relay link, the jamming signal can be used more effectively in the high SNR regimes.

B. Secrecy rate performance

Fig. 6 and Fig. 7 present the simulated ASR, the derived approximated results and the lower bound of ASR for the OUS and GUS schemes. From the curve of the CUS scheme, we can also obtain that the conventional user-pair selection scheme without DBJ cannot achieve positive secrecy rate at any SNR. Comparing the four user-pair selection schemes in the considered system, we can find that, all of the proposed schemes are better than the round-robin scheme, which shows the effectiveness of proposed schemes for improving the ASR. The ASR of the GUS scheme is very close to the GAUS scheme. We can also observe that, the increasing N gives better performance for the proposed schemes. Therefore, the secrecy performance of the considered system can benefit from the increased user-pairs as long as taking full advantage of multiuser diversity. In contrast, from the curve of the BRS scheme, we can see that the secrecy rate of the best relay selection in "N *relays with a single user-pair*" scenario

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2882178, IEEE Transactions on Vehicular Technology

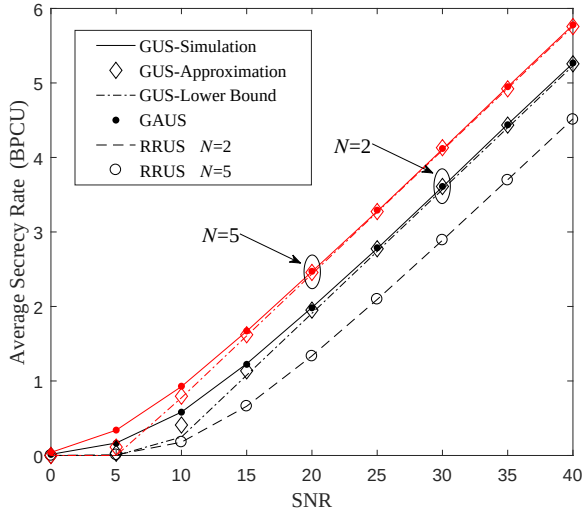


Fig. 7. Average secrecy rate vs SNR for the GUS schemes, with user-pair number $N = 2, 5$.

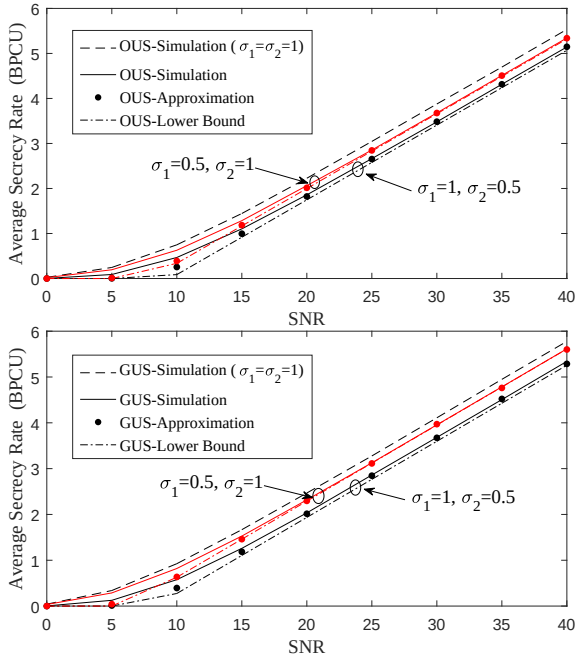


Fig. 8. Average secrecy rate vs SNR for the two schemes, with different σ_1, σ_2 and user-pair number $N = 5$.

reduces as N increases, such observation can also be obtained in [32]. It reveals that, exploiting the multiuser diversity, instead of cooperative diversity, is an efficient method of enhancing the secrecy performance for the untrusted relay networks.

In Fig. 8, the ASR of the OUS and GUS schemes with different σ_1, σ_2 is plotted. The present results show that the ASR will decrease as the decrease in σ_1 or σ_2. The decreased σ_2 will result in a great performance loss, since the deterioration of relay-destination link will only worsen the main channel condition.

VII. Conclusion

In this paper, we investigate secure communication for untrusted relay networks with multiple source-destination pairs. Three DBJ aided user-pair selection schemes have been proposed to prevent information from being intercepted. Analytical expressions of both SOP and ASR have been derived for the OUS and GUS schemes in closed-forms. Some theoretic and simulation results have been also presented. It can be obtained that, the proposed schemes outperform the round-robin scheme, which shows the effectiveness of using multiuser diversity gain in the considered networks. The GUS scheme outperforms the OUS scheme due to the additional flexibility provided by the source cooperation, whereas, the OUS scheme can achieve the same diversity order (namely $\frac{N}{2}$) as GUS scheme. We can also conclude that, although increasing the number of relays (cooperative diversity) cannot benefit the considered untrusted relay networks, the secrecy performance can be improved by increasing the number of user-pairs (multiuser diversity).

Appendix A
Proof of Theorem 1

By changing the value $y = \left(\frac{1}{1-t^{\frac{1}{2}}} - 1\right)^2$, the term (15) can be expressed as

$$F_1(z) = z\int_0^1 \sqrt{\frac{t}{1-t}}\left(1 - e^{-b_2(y)^- z} + e^{-b_2(y)^+ z}\right) \cdot\sqrt{\lambda_2} e^{-b_1(y)z}\sqrt{\tfrac{1-t}{t}}\tfrac{\mathrm{d}y}{\mathrm{d}t}\mathrm{d}t. \tag{33}$$

Then, with the help of Gaussian-Chebyshev quadrature [41, eq. (25.4.42)], we have

$$F_1(z) \approx z\sum_{g=1}^{G}\omega_g\sqrt{\tfrac{1-t_g}{t_g}}\tfrac{1}{(1-\sqrt{t_g})^3}\sqrt{\lambda_2}e^{-b_1\left((\frac{\sqrt{t_g}}{1-\sqrt{t_g}})^2\right)z} \cdot\left(1 - e^{-b_2\left((\frac{\sqrt{t_g}}{1-\sqrt{t_g}})^2\right)^- z} + e^{-b_2\left((\frac{\sqrt{t_g}}{1-\sqrt{t_g}})^2\right)^+ z}\right). \tag{34}$$

Due to the independent and identical distribution of each channel, we can obtain that

$$F_{Z_{i^*}}(z) = \left(1 - e^{-\lambda_2\epsilon^+ z} + F_1(z)\right)^N, \tag{35}$$

where $i^* = \arg\max_{i\in\{1,\ldots,N\}} Z_i$. $P_{\text{out}}^{OUS} = F_{Z_{i^*}}(\psi)$. It completes the proof.

Appendix B
Proof of Proposition 1

Based on (7), following the fact that $\frac{1}{2}\min(x,y) \le \frac{xy}{x+y} \le \min(x,y)$, we have

$$P_{\text{out}}^{OUS} \ge \Pr\left(\max_{i\in\{1,\ldots,N\}}\tfrac{\frac{1}{2}\beta_i}{\alpha_i+\beta_i}\min(\alpha_i, 2\beta_i) < \psi\right) \ge \underbrace{\Pr\left(\max_{i\in\{1,\ldots,N\}}\frac{1}{2}\min\left(\min(\alpha_i,\beta_i), \frac{2\beta_i^2}{\alpha_i+\beta_i}\right) < \psi\right)}_{P_{\text{LB}}^{OUS}}, \tag{36}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2882178, IEEE Transactions on Vehicular Technology

$$
\begin{aligned}
P_{\text{out}}^{OUS} &\leq \Pr\left(\max_{i\in\{1,\ldots,N\}} \tfrac{\frac{1}{4}\beta_i}{\alpha_i+\beta_i}\min(\alpha_i,2\beta_i) < \psi\right) \\
&\leq \Pr\left(\max_{i\in\{1,\ldots,N\}} \tfrac{1}{4}\min\left(\tfrac{1}{2}\min(\alpha_i,\beta_i), \tfrac{2\beta_i^2}{\alpha_i+\beta_i}\right) < \psi\right) \\
&= \Pr\left(\max_{i\in\{1,\ldots,N\}} \tfrac{1}{8}\min\left(\min(\alpha_i,\beta_i), \tfrac{4\beta_i^2}{\alpha_i+\beta_i}\right) < \psi\right) \\
&\leq \underbrace{\Pr\left(\max_{i\in\{1,\ldots,N\}} \frac{1}{8}\min\left(\min(\alpha_i,\beta_i), \frac{2\beta_i^2}{\alpha_i+\beta_i}\right) < \psi\right)}_{P_{\text{UB}}^{OUS}}.
\end{aligned} \tag{37}
$$

Reformulating (36), we have

$$
\begin{aligned}
P_{\text{LB}}^{OUS} &= \prod_{i=1}^{N}\Bigg[\Pr\left(\frac{1}{2}\alpha_i < \psi, \alpha_i \leq \beta_i\right) \\
&\qquad +\Pr\left(\tfrac{\beta_i^2}{\alpha_i+\beta_i} < \psi, \alpha_i > \beta_i\right)\Bigg] \\
&= \Bigg(\int_0^{2\psi}\int_x^{\infty}\lambda_1 e^{-\lambda_1 x}\lambda_2 e^{-\lambda_2 y}\mathrm{d}y\mathrm{d}x \\
&\qquad +\int_0^{2\psi}\int_0^{x}\lambda_1 e^{-\lambda_1 x}\lambda_2 e^{-\lambda_2 y}\mathrm{d}y\mathrm{d}x + \\
&\quad \int_{2\psi}^{\infty}\int_0^{\sqrt{\psi x+(\frac{\psi}{2})^2}+\frac{\psi}{2}}\lambda_1 e^{-\lambda_1 x}\lambda_2 e^{-\lambda_2 y}\mathrm{d}y\mathrm{d}x\Bigg)^N \\
&= \left(1-\lambda_1 e^{-\lambda_2\frac{\psi}{2}}\int_{2\psi}^{\infty} e^{-\lambda_2\sqrt{\psi x+(\frac{\psi}{2})^2}}e^{-\lambda_1 x}\mathrm{d}x\right)^N \\
&= \left(1-2\lambda_1 e^{\xi_1 2\psi}\int_{\frac{3\sqrt{\psi}}{2}}^{\infty} e^{-\lambda_1(u+\frac{\lambda_2}{2\lambda_1}\sqrt{\psi})^2}u\mathrm{d}u\right)^N.
\end{aligned} \tag{38}
$$

Using the results in [42, eq.(3.326.3)] and [42, eq.(3.326.4)], we have

$$
P_{\text{LB}}^{OUS} = \left\{1-e^{\xi_1\frac{\psi}{2}}\left[\Gamma(1,\xi_2\tfrac{\psi}{4}) - \xi_3\sqrt{\tfrac{\psi}{4}}\Gamma(\tfrac{1}{2},\xi_2\tfrac{\psi}{4})\right]\right\}^N, \tag{39}
$$

and it is straightforward to obtain the P_{UB}^{OUS} by substituting ψ in (39) for 4ψ. It completes the proof.

Appendix C
Proof of Theorem 2

Since $e^x = \sum_{n=0}^{\infty}\frac{x^n}{n!}$, with the aid of [42, eq.(8.352.7)] and [42, eq.(8.354.2)], we have

$$
\begin{aligned}
e^{\xi_1\frac{\psi}{2}}\Gamma(1,\xi_2\tfrac{\psi}{4}) &= e^{\xi_1\frac{\psi}{2}}e^{-\xi_2\frac{\psi}{4}} = e^{-2(\lambda_1+\lambda_2)\psi} \\
&= 1-2\psi(\tfrac{1}{\sigma_1}+\tfrac{1}{\sigma_2})\tfrac{1}{P}+O(\tfrac{1}{P^2}),
\end{aligned} \tag{40}
$$

and

$$
\begin{aligned}
\Gamma(\tfrac{1}{2},\xi_2\tfrac{\psi}{4}) &= \sqrt{\pi}-\sum_{n=0}^{\infty}\frac{(-1)^n(\xi_2\frac{\psi}{4})^{n+\frac{1}{2}}}{n!(n+\frac{1}{2})} \\
&= \sqrt{\pi}-(3+\tfrac{\sigma_1}{\sigma_2})\sqrt{\tfrac{\psi}{\sigma_1}}(\tfrac{1}{P})^{\frac{1}{2}}+O\left(\tfrac{1}{P^{\frac{3}{2}}}\right).
\end{aligned} \tag{41}
$$

Thus, we can obtain that

$$
\begin{aligned}
P_{\text{LB}}^{OUS} &\overset{P\to\infty}{\simeq} \left(e^{\xi_1\frac{\psi}{2}}\xi_3\sqrt{\tfrac{\psi}{4}}\sqrt{\pi}\right)^N \\
&= \left(\sqrt{\tfrac{\psi\pi}{4}}\tfrac{\sqrt{\sigma_1}}{\sigma_2}\right)^N(\tfrac{1}{P})^{\frac{N}{2}}.
\end{aligned} \tag{42}
$$

As same as the above operation, we can easily verify that the diversity order for upper bound case is also equal to $\frac{N}{2}$. Hence, it can be concluded that the diversity order of OUS scheme is equal to $\frac{N}{2}$. It completes the proof.

Appendix D
Proof of Proposition 2

From the expression of ASR in (18), we have

$$
\begin{aligned}
R_{\text{ASR}}^{OUS} &\geq \tfrac{1}{2\ln 2}\left[E\left\{\ln\left(\max_{i\in\{1,\ldots,N\}}\tfrac{\alpha_i\beta_i^2}{(\alpha_i+2\beta_i)(\alpha_i+\beta_i)}\right)\right\}\right]^+ \\
&\geq \tfrac{1}{2\ln 2}\left[E\left\{\ln\left(\tfrac{\alpha_k\beta_k^2}{(\alpha_k+2\beta_k)(\alpha_k+\beta_k)}\right)\right\}\right]^+ \\
&= \tfrac{1}{2\ln 2}\Big[E\left\{\ln(\alpha_k)\right\}+2E\left\{\ln(\beta_k)\right\} \\
&\qquad -E\left\{\ln(\alpha_k+\beta_k)\right\}-E\left\{\ln(\alpha_k+2\beta_k)\right\}\Big]^+,
\end{aligned} \tag{43}
$$

where $k = \arg\max_{i\in\{1,\ldots,N\}}(\alpha_i,\beta_i)$. To obtain the expectations, it is necessary to get the PDF of α_k and β_k. Following [44, eq.(38)], we have

$$
f_{\alpha_k}(x) = \sum_{n=0}^{N-1}\tfrac{\binom{N-1}{n}(-1)^n N}{(\lambda_2+n\lambda^{\text{s}})/\lambda_1}\left(\lambda_2 e^{-\lambda_1 x} - n\lambda^{\text{s}}e^{-(n+1)\lambda^{\text{s}}x}\right), \tag{44}
$$

where $\lambda^{\text{s}} = \lambda_1+\lambda_2$. Due to the symmetry, we can also obtain the PDF of β_k from (44). With the derived $f_{\alpha_k}(x)$ and $f_{\beta_k}(x)$, the PDF of $\alpha_k+\bar{\chi}\beta_k$, $\bar{\chi}=\{1,2\}$ can be given by

$$
\begin{aligned}
f_{\alpha_k+\bar{\chi}\beta_k}(x) &= \sum_{n_1=0}^{N-1}\sum_{n_2=0}^{N-1} c_{n_1,1}^{\text{s},\bar{\chi}+1}c_{n_2,1}^{\text{s},\bar{\chi}+1}\Bigg[\tfrac{\lambda_1(e^{-\frac{\lambda_2}{\bar{\chi}}x}-e^{-\lambda_{n_1+1}^{\text{s},\bar{\chi}+1}x})}{(\lambda_{n_1+1}^{\text{s},\bar{\chi}+1}-\lambda_2/\bar{\chi})/\lambda_{n_1}^{\text{s},\bar{\chi}+1}} \\
&+\tfrac{\frac{\lambda_2}{\bar{\chi}}(e^{-\lambda_1 x}-e^{-\lambda_{n_2+1}^{\text{s},\bar{\chi}+1}x})}{(\lambda_{n_2+1}^{\text{s},\bar{\chi}+1}-\lambda_1)/\lambda_{n_2}^{\text{s},\bar{\chi}+1}} + \underset{\lambda_1\neq\frac{\lambda_2}{\bar{\chi}}}{\Delta}\left\{\tfrac{\lambda_1\frac{\lambda_2}{\bar{\chi}}(e^{-\lambda_1 x}-e^{-\frac{\lambda_2}{\bar{\chi}}x})}{\frac{\lambda_2}{\bar{\chi}}-\lambda_1}\right\}+ \\
&\underset{\lambda_1=\frac{\lambda_2}{\bar{\chi}}}{\Delta}\left\{\lambda_1\tfrac{\lambda_2}{\bar{\chi}}xe^{-\lambda_1 x}\right\}+\underset{n_1=n_2}{\Delta}\left\{\lambda_{n_1}^{\text{s},\bar{\chi}+1}\lambda_{n_2}^{\text{s},\bar{\chi}+1}xe^{-\lambda_{n_1+1}^{\text{s},\bar{\chi}+1}x}\right\} \\
&+\underset{n_1\neq n_2}{\Delta}\left\{\tfrac{\lambda_{n_1}^{\text{s},\bar{\chi}+1}\lambda_{n_2}^{\text{s},\bar{\chi}+1}(e^{-\lambda_{n_1+1}^{\text{s},\bar{\chi}+1}x}-e^{-\lambda_{n_2+1}^{\text{s},\bar{\chi}+1}x})}{\lambda_{n_2-n_1}^{\text{s},\bar{\chi}+1}}\right\}\Bigg].
\end{aligned} \tag{45}
$$

With the help of [42, eq.(4.331.1)] and [42, eq.(4.352.2)], we can obtain (22). It completes the proof.

Appendix E
Proof of Proposition 3

Similar to the expressions (36) and (37), we can also obtain the upper bound and the lower bound of SOP for the GUS scheme as follows

$$
P_{\text{LB}}^{GUS} = \Pr\left(\max_{j\in\{1,\ldots,N\}}\tfrac{1}{2}\min\left(\min(\mu_j,\nu),\tfrac{2\nu^2}{\mu_j+\nu}\right)<\psi\right), \tag{46}
$$

and

$$
P_{\text{UB}}^{GUS} = \Pr\left(\max_{j\in\{1,\ldots,N\}}\tfrac{1}{8}\min\left(\min(\mu_j,\nu),\tfrac{2\nu^2}{\mu_j+\nu}\right)<\psi\right). \tag{47}
$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2882178, IEEE Transactions on Vehicular Technology

We rewrite (46) as

$$\begin{aligned}P_{\mathrm{LB}}^{GUS} =& \int_{2\psi}^{\infty}\left(\int_{0}^{2\psi}\lambda_1 e^{-\lambda_1 x}dx+\int_{\frac{y^2}{\psi}-y}^{\infty}\lambda_1 e^{-\lambda_1 x}\mathrm{d}x\right)^N f_\nu(y)\mathrm{d}y\\ &+\int_{0}^{2\psi}\left(\int_{0}^{y}\lambda_1 e^{-\lambda_1 x}\mathrm{d}x+\int_{y}^{\infty}\lambda_1 e^{-\lambda_1 x}\mathrm{d}x\right)^N f_\nu(y)\mathrm{d}y\\ =& \underbrace{\int_{2\psi}^{\infty}\sum_{k=0}^{N}\binom{N}{k}(1-e^{-\lambda_1 2\psi})^{N-k}e^{-\lambda_1(\frac{y^2}{\psi}-y)k}f_\nu(y)\mathrm{d}y}_{J_1}\\ &+(1-e^{-\lambda_2 2\psi})^N.\end{aligned} \tag{48}$$

After some manipulations, we have

$$\begin{aligned}J_1 =& \sum_{k=1}^{N}\tbinom{N}{k}(1-e^{-\lambda_1 2\psi})^{N-k}\sum_{n=0}^{N-1}\tbinom{N}{n}(-1)^n N\lambda_2\\ &\cdot\underbrace{\int_{2\psi}^{\infty}e^{-\frac{\lambda_1 k}{\psi}y^2-[\lambda_2(n+1)-\lambda_1 k]y}\mathrm{d}y}_{J_2}\\ &+(1-e^{-\lambda_1 2\psi})^N(1-(1-e^{-\lambda_2 2\psi})^N).\end{aligned} \tag{49}$$

With the aid of [42, eq.(3.322.1)], we have

$$\begin{aligned}J_2 =& \sqrt{\pi\cdot\tfrac{\psi}{4\lambda_1 k}}e^{\frac{\psi}{4\lambda_1 k}[\lambda_2(n+1)-\lambda_1 k]^2}\\ &\cdot\mathrm{erfc}\left\{[\lambda_2(n+1)-\lambda_1 k]\sqrt{\tfrac{\psi}{4\lambda_1 k}}+\sqrt{4\lambda_1\psi k}\right\}.\end{aligned} \tag{50}$$

Combining (48), (49) and (50), the lower bound P_{LB}^{GUS} is acquired. After variable substitution, the upper bound P_{UB}^{GUS} can also be obtained. It completes the proof.

Appendix F
Proof of Theorem 5

First, it can be obtained that

$$\begin{aligned}A(\psi) =& (1-e^{-\lambda_1 2\psi})^N-(1-e^{-\lambda_1 2\psi})^N(1-e^{-\lambda_2 2\psi})^N\\ &+(1-e^{-\lambda_2 2\psi})^N\\ \overset{P\to\infty}{\simeq}& (\tfrac{2\psi}{\sigma_1}\tfrac{1}{P})^N-(\tfrac{2\psi}{\sigma_1}\tfrac{1}{P})^N(\tfrac{2\psi}{\sigma_2}\tfrac{1}{P})^N+(\tfrac{2\psi}{\sigma_2}\tfrac{1}{P})^N\\ \simeq& \left((\tfrac{2\psi}{\sigma_1})^N+(\tfrac{2\psi}{\sigma_2})^N\right)(\tfrac{1}{P})^N=I_1.\end{aligned} \tag{51}$$

After some manipulations, we have

$$\begin{aligned}P_{\mathrm{LB}}^{GUS}\overset{P\to\infty}{\simeq}& I_1+\tfrac{\sqrt{N\pi\psi}}{2}\tfrac{\lambda_2}{\sqrt{\lambda_1}}\sum_{n=0}^{N-1}\tbinom{N-1}{n}(-1)^n e^{(l_N^\psi\theta_N^n)^2}\\ &\cdot\mathrm{erfc}\left(\theta_N^n l_N^\psi+\tfrac{\psi}{l_N^\psi}\right)\\ =& \tfrac{\sqrt{N\pi\psi}}{2}\tfrac{\sqrt{\sigma_1}}{\sigma_2}\sqrt{\tfrac{1}{P}}\sum_{n=0}^{N-1}\tbinom{N-1}{n}(-1)^n(1-\mathrm{erf}(\theta_N^n l_N^\psi+\tfrac{\psi}{l_N^\psi}))\\ &\cdot\sum_{m=0}^{\infty}\frac{\left(\sqrt{\frac{\psi\sigma_1}{4N}}(\frac{n}{\sigma_2}+\frac{1}{\sigma_2}-\frac{N}{\sigma_1})\sqrt{\frac{1}{P}}\right)^{2m}}{m!}+I_1\\ =& I_1+I_2+I_3,\end{aligned} \tag{52}$$

where I_2 and I_3 are defined as follows

$$\begin{aligned}I_2 =& \tfrac{\sqrt{N\pi\psi}}{2}\tfrac{\sqrt{\sigma_1}}{\sigma_2}\sum_{m=0}^{\infty}\tfrac{(\frac{\psi\sigma_1}{4N})^m(\frac{1}{P})^{m+\frac{1}{2}}}{m!}\sum_{n=0}^{N-1}\tbinom{N-1}{n}(-1)^n\\ &\cdot\sum_{q=0}^{2m}\tbinom{2m}{q}(\tfrac{1}{\sigma_2}-\tfrac{N}{\sigma_1})^{2m-q}(\tfrac{n}{\sigma_2})^q,\end{aligned} \tag{53}$$

and

$$\begin{aligned}I_3 =& \tfrac{-\sqrt{N\pi\psi}}{2}\tfrac{\sqrt{\sigma_1}}{\sigma_2}\sum_{m=0}^{\infty}\tfrac{(\frac{\psi\sigma_1}{4N})^m(\frac{1}{P})^{m+\frac{1}{2}}}{m!}\sum_{n=0}^{N-1}\tbinom{N-1}{n}(-1)^n\\ &\cdot\mathrm{erf}(\theta_N^n l_N^\psi+\tfrac{\psi}{l_N^\psi})\sum_{q=0}^{2m}\tbinom{2m}{q}(\tfrac{1}{\sigma_2}-\tfrac{N}{\sigma_1})^{2m-q}(\tfrac{n}{\sigma_2})^q,\end{aligned} \tag{54}$$

where $\mathrm{erf}(x)\triangleq 1-\mathrm{erfc}(x)$ is the error function defined in [42, eq.(8.250.1)].

Recall the following sums of the binomial coefficients [42, eq.(0.154.3)]

$$\sum_{n=0}^{N-1}\tbinom{N-1}{n}(-1)^n n^q=0, \tag{55}$$

for $N-2\geq q\geq 0$ and

$$\sum_{n=0}^{N-1}\tbinom{N-1}{n}(-1)^n n^{N-1}=(-1)^{N-1}(N-1)!. \tag{56}$$

Following (53), in I_2 all the terms with n^q for $q\leq N-2$ can be removed. At high SNR, when N is odd, all the factors with $(\frac{1}{P})^{m+\frac{1}{2}}$ for $m>\frac{N-1}{2}$ can be ignored, the dominant factor of I_2 will be the one order of $(\frac{1}{P})^{\frac{N-1}{2}+\frac{1}{2}}$. When N is even, the dominant factor of I_2 is $(\frac{1}{P})^{\frac{N}{2}+\frac{1}{2}}$. With the aid of [42, eq.(3.321.1)], we have

$$\begin{aligned}&\mathrm{erf}(\theta_N^n l_N^\psi+\tfrac{\psi}{l_N^\psi})=\tfrac{2}{\sqrt{\pi}}\sum_{k=0}^{\infty}\frac{(-1)^k\left(\theta_N^n l_N^\psi+\frac{\psi}{l_N^\psi}\right)^{2k+1}}{k!(2k+1)}\\ &=\tfrac{2}{\sqrt{\pi}}\left(\sqrt{\tfrac{\psi\sigma_1}{4N}}(\tfrac{n}{\sigma_2}+\tfrac{1}{\sigma_2}-\tfrac{N}{\sigma_1})+\sqrt{\tfrac{4N\psi}{\sigma_1}}\right)\sqrt{\tfrac{1}{P}}+O\left(\tfrac{n^3}{P^{\frac{3}{2}}}\right)\\ &\approx\tfrac{2}{\sqrt{\pi}}\sum_{k=0}^{\infty}\frac{(-1)^k\left(\sqrt{\frac{\psi\sigma_1}{4N}}(\frac{n}{\sigma_2}\sqrt{\frac{1}{P}})\right)^{2k+1}}{k!(2k+1)}.\end{aligned} \tag{57}$$

Therefore, all the terms with $n^{\bar{q}}$ for $\bar{q}\leq N-2$ can be removed from I_3, where $\bar{q}=q+2k+1$. Then, the dominant factor of I_3 is $(\frac{1}{P})^{\frac{N-2k-1}{2}+\frac{1}{2}+\frac{2k+1}{2}}$ when N is odd, and the dominant factor of I_3 is $(\frac{1}{P})^{\frac{N-2k-2}{2}+\frac{1}{2}+\frac{2k+1}{2}}$ when N is even. Above all, the asymptotic expression of P_{LB}^{GUS} can be given as follows

$$P_{\mathrm{LB}}^{GUS}\simeq\begin{cases}\frac{\Lambda_2}{2\varpi_1!}(\frac{1}{P})^{\frac{N}{2}}, & N\text{ is odd},\\ \frac{\Lambda_2\Lambda_3}{\sqrt{\pi}}(\frac{1}{P})^{\frac{N}{2}}, & N\text{ is even},\end{cases} \tag{58}$$

where $\Lambda_2=\frac{\sqrt{N\pi\psi\sigma_1}(N-1)!}{(\sigma_2)^N}(\frac{\psi\sigma_1}{4N})^{\frac{N-1}{2}}$, $\varpi_1=\frac{N-1}{2}$ and $\Lambda_3=\sum_{k=0}^{\varpi_2}\frac{(-1)^k}{(\varpi_2-k)!k!(2k+1)}$, $\varpi_2=\frac{N-2}{2}$. It can be easily obtained that the upper bound of outage probability is at the order of $\frac{N}{2}$. Thus, the diversity order of GUS scheme is equal to $\frac{N}{2}$. It completes the proof.

APPENDIX G
PROOF OF PROPOSITION 4

From the expression of ASR in (28), we have

$$\begin{aligned} R_{\text{ASR}}^{GUS} &\geq \frac{1}{2\ln 2}\left[E\left\{\max_{i\in\{1,\ldots,N\}}\ln(\tfrac{\alpha_i\nu}{\alpha_i+2\nu})-\ln(1+\tfrac{\alpha_i}{\nu})\right\}\right]^+ \\ &\geq \left[\frac{E\left\{\max\limits_{i\in\{1,\ldots,N\}}\ln(\frac{\alpha_i\nu}{\alpha_i+2\nu})-\max\limits_{j\in\{1,\ldots,N\}}\ln(1+\frac{\alpha_j}{\nu})\right\}}{2\ln 2}\right]^+ \\ &= \frac{1}{2\ln 2}\left[E\left\{\ln(\tfrac{\bar{\alpha}\nu}{\bar{\alpha}+2\nu})-\ln(1+\tfrac{\bar{\alpha}}{\nu})\right\}\right]^+ \\ &= \frac{1}{2\ln 2}\left[E\left\{\ln(\bar{\alpha})\right\}+E\left\{\ln(\nu)\right\}\right. \\ &\qquad \left.-E\left\{\ln(\bar{\alpha}+2\nu)\right\}-E\left\{\ln(1+\tfrac{\bar{\alpha}}{\nu})\right\}\right]^+, \end{aligned} \tag{59}$$

where $\bar{\alpha}=\max\limits_{i\in\{1,\ldots,N\}}\alpha_i$. To obtain the expectation in (59), the PDF of the related random variables are also required. The PDF of ν is given in (24), and it is easy to obtain $f_{\bar{\alpha}}$ owing to symmetry. Then the PDF of $\bar{\alpha}+2\nu$ and $\frac{\bar{\alpha}}{\nu}$ are given as follows

$$\begin{aligned} f_{\bar{\alpha}+2\nu}(x) = &\sum_{n=0}^{N-1}\tbinom{N-1}{n}(-1)^n\tfrac{N\lambda_2}{2}e^{-\frac{\xi_5}{2}x}+\sum_{n_1=1}^{N}\sum_{n_2=0}^{N-1}\tbinom{N}{n_1} \\ &\tbinom{N-1}{n_2}(-1)^{n_1+n_2+1}N\lambda_2\left\{\underset{\xi_5=2\xi_4}{\Delta}\left\{\tfrac{1}{2}e^{-\xi_4 x}(\xi_4 x-1)\right\}\right. \\ &\left.+\underset{\xi_5\neq 2\xi_4}{\Delta}\left\{\frac{\xi_4 e^{-\xi_4 x}-\frac{\xi_5}{2}e^{-\frac{\xi_5}{2}x}}{\xi_5-2\xi_4}\right\}\right\}, \end{aligned} \tag{60}$$

$$f_{\frac{\bar{\alpha}}{\nu}}(x)=\sum_{n_1=1}^{N}\sum_{n_2=0}^{N-1}\frac{\binom{N}{n_1}\binom{N-1}{n_2}(-1)^{n_1+n_2+1}N\lambda_2}{(\xi_4 x+\xi_5)^2/\xi_4}. \tag{61}$$

By using [42, eq.(4.331.1)], [42, eq.(4.352.2)] and [42, eq.(4.291.15)], we can derive the four expectations respectively. After some reorganizations, we can get (32). It completes the proof.

REFERENCES

[1] T. X. Zheng, H. M. Wang, J. Yuan, Z. Han and M. H. Lee, "Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3827-3839, Jun. 2017.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Commun. Surv. Tutor.*, vol. 16, no. 3, pp. 1550-1573, Aug. 2014.

[3] L. Lv, Z. Ding, Q. Ni and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6700-6705, Jul. 2018.

[4] G. Pan, C. Tang, X. Zhang, T. Li, Y. Weng and Y. Chen, "Physical-layer security over non-small-scale fading channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1326-1339, Mar. 2016.

[5] 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.

[6] L. Yang, H. Jiang, S. A. Vorobyov, J. Chen and H. Zhang, "Secure communications in underlay cognitive radio networks: user scheduling and performance analysis," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1191-1194, Jun. 2016.

[7] Y. Zou, X. Wang and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103-5113, Dec. 2013.

[8] H. Deng, H. M. Wang, J. Yuan, W. Wang and Q. Yin, "Secure communication in uplink transmissions: user selection and multiuser secrecy gain," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3492-3506, Aug. 2016.

[9] X. Ge, H. Jin, J. Zhu, J. Cheng and V. C. M. Leung, "Exploiting opportunistic scheduling in uplink wiretap networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 4886-4897, Jun. 2017.

[10] L. Fan, N. Yang, T. Q. Duong, M. Elkashlan and G. K. Karagiannidis, "Exploiting direct links for physical layer security in multiuser multirelay networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3856-3867, Jun. 2016.

[11] T. M. Hoang, T. Q. Duong, H. A. Suraweera, C. Tellambura and H. V. Poor, "Cooperative beamforming and user selection for improving the security of relay-aided systems," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5039-5051, Dec. 2015.

[12] H. Deng, H. Wang, W. Guo and W. Wang, "Secrecy transmission with a helper: To relay or to jam," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 293-307, Feb. 2015.

[13] S. I. Kim, I. M. Kim and J. Heo,"Secure transmission for multiuser relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3724-3737, Jul. 2015.

[14] C. Wang, H. M. Wang, D. W. K. Ng, X. G. Xia and C. Liu, "Joint beamforming and power allocation for secrecy in peer-to-peer relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 6, pp. 3280-3293, Jun. 2015.

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

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

[17] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. Inf. Theory Workshop (ITW)*, Cairns, QLD, Australia, Sep. 2001, pp. 87-89.

[18] 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.

[19] 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.

[20] J. Huang, A. Mukherjee, and A. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536-2550, May 2013.

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

[22] D. A. Karpuk and A. Chorti, "Perfect secrecy in physical-layer network coding systems from structured interference," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1875-1887, Aug. 2016.

[23] Y. Huo, Y. Tian, L. Ma, X. Cheng and T. Jing, "Jamming strategies for physical layer decurity," *IEEE Wireless Commun.*, vol. PP, no. 99, pp. 1-6.

[24] L. Lv, J. Chen, L. Yang and Y. Kuo, "Improving physical layer security in untrusted relay networks: cooperative jamming and power allocation," *IET Commun.*, vol. 11, no. 3, pp. 393-399, Feb. 2017.

[25] R. Zhang, L. Song, Z. Han and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693-3704, Oct. 2012.

[26] A. El Shafie, A. Mabrouk, K. Tourki, N. Al-Dhahir and R. Hamila, "Securing untrusted RF-EH relay networks using cooperative jamming signals," *IEEE Access*, vol. 5, pp. 24353-24367, Nov. 2017.

[27] A. Kuhestani, A. Mohammadi and M. Mohammadi, "Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 341-355, Feb. 2018.

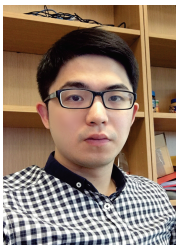
[28] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *Proc. IEEE Global Telecommunications Conference (Globecom)*, New Orleans, LA, Dec. 2008, pp. 1-5.

[29] 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.

[30] 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.

[31] B. He, J. Chen, Y. Kuo and L. Yang, "Cooperative jamming for energy harvesting multicast networks with an untrusted relay," *IET Commun.*, vol. 11, no. 13, pp. 2058-2065, Oct. 2017.

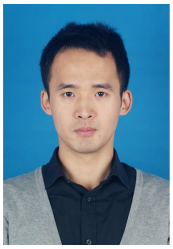
[32] L. Sun, T. Zhang, Y. Li and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801-3807, Oct. 2012.
[33] J. B. Kim, J. Lim and J. M. Cioffi, "Capacity scaling and diversity order for secure cooperative relaying with untrustworthy relays," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3866-3876, Jul. 2015.
[34] Q. Cao, Y. Jing and H. V. Zhao, "Power allocation in multi-user wireless relay networks through bargaining," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2870-2882, Jun. 2013.
[35] Z. Ding and H. V. Poor, "Multi-user SWIPT cooperative networks: Is the max-min criterion still diversity-optimal?," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 553-567, Jan. 2016.
[36] X. Ding, T. Song, Y. Zou and X. Chen, "Security-reliability tradeoff for friendly jammer assisted user-pair selection in the face of multiple eavesdroppers," *IEEE Access*, vol. 4, pp. 8386-8393, Sep. 2016.
[37] M. Zhang, M. Ding, L. Gui, H. Luo and M. Bennis,"Sum secrecy rate maximization for relay-aided multiple-source multiple-destination networks," *IEEE Trans. Veh Technol.*, vol. 66, no. 5, pp. 4098-4109, May 2017.
[38] S. Atapattu, Y. Jing, H. Jiang and C. Tellambura, "Relay selection schemes and performance analysis approximations for two-way networks," *IEEE Trans. Commun.*, vol. 61, no. 3, pp. 987-998, Mar. 2013.
[39] Q. Li, H. Li, P. Russell, Z. Chen and C. Wang, "CA-P2P: context-aware proximity-based peer-to-peer wireless communications," *IEEE Commun. Mag.*, vol. 52, no. 6, pp. 32-41, Jun. 2014.
[40] C. Xu, S. Jia, L. Zhong and G. M. Muntean, "Socially aware mobile peer-to-peer communications for community multimedia streaming services," *IEEE Commun. Mag.*, vol. 53, no. 10, pp. 150-156, Oct. 2015.
[41] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. New York, NY, USA: Dover, 1972.
[42] A. Jeffrey and D. Zwillinger, *Table of Integrals, Series, and Products*. New York, NY, USA: Academic, 2007.
[43] 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.
[44] D. S. Michalopoulos, H. A. Suraweera, G. K. Karagiannidis and R. Schober, "Amplify-and-forward relay selection with outdated channel estimates," *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1278-1290, May 2012.



Bingtao He received the B.Sc. and M.Sc. degrees from Xidian University, Xi'an, China, in 2013 and 2016 respectively, and is currently pursuing the Ph.D. degree in telecommunications engineering with Xidian University. Since 2017, he has been with Lancaster University, U.K., as a joint Ph.D. student sponsored by the China Scholarship Council. His current research interests include cooperative communications, physical layer security and wireless multicast.

Qiang Ni (M'04-SM'08) received the B.Sc., M.Sc., and Ph.D. degrees from the Huazhong University of Science and Technology, China, all in engineering. He is currently a Professor and the Head of the Communication Systems Group, School of Computing and Communications, Lancaster University, Lancaster, U.K. His research interests include the area of future generation communications and networking, including green communications and networking, millimeter-wave wireless communications, cognitive radio network systems, non-orthogonal multiple access (NOMA), heterogeneous networks, 5G and 6G, SDN, cloud networks, energy harvesting, wireless information and power transfer, IoTs, cyber physical systems, machine learning, big data analytics, and vehicular networks. He has authored or co-authored over 200 papers in these areas. He was an IEEE 802.11 Wireless Standard Working Group Voting Member and a contributor to the IEEE Wireless Standards.

Jian Chen received the B.S. from Xi'an Jiaotong University, China, in 1989, the M.S. degree from Xi'an Institute of Optics and Precision Mechanics of Chinese Academy of Sciences in 1992, and the Ph.D. in Telecommunications Engineering in Xidian University, China, in 2005. He is a professor in the school of Telecommunications Engineering in Xidian University. He was a visitor scholar in the University of Manchester from 2007 to 2008. His research interests include cognitive radio, OFDM and wireless sensor networks.



Long Yang (M'18) received the B.Sc. and Ph.D. degrees from Xidian University, Xi'an, China, in 2010 and 2015, respectively. Since December 2015, he has been a faculty member with Xidian University, Xi'an, China, where he is currently an Lecturer at the School of Telecommunications Engineering. Since November 2017, he has also been a Post-Doctoral Fellow with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, Alberta, Canada. His current research interests include cooperative communications, non-orthogonal multiple access (NOMA), wireless multicast, and wireless physical-layer security.

Lu Lv received his Ph.D degree in Communication and Information Systems from Xidian University, China, in 2018. In 2016, he was a visiting Ph.D. student at the School of Computing and Communications, Lancaster University, U.K. From 2016 to 2018, he was a visiting Ph.D student at the Department of Electrical and Computer Engineering, University of Alberta, Canada. He is currently a research fellow at the School of Telecommunications Engineering, Xidian University, China. His research interests include cooperative communications, non-orthogonal multiple access, and physical layer security.