Journal of Parallel and Distributed Computing 144 (2020) 260–267

Contents lists available at ScienceDirect

J. Parallel Distrib. Comput.

journal homepage: www.elsevier.com/locate/jpdc

Securing transmissions by friendly jamming scheme in wireless networks

Guangshun Li [a,b], Xiaofei Sheng [a], Junhua Wu [a,*], Haili Yu [a]

[a] School of Information Science and Engineering, Qufu Normal University, Rizhao, Shandong, China
[b] Department of computer, the Hong Kong Polytechnic University, HongKong, China

ARTICLE INFO

Article history:
Received 25 November 2019
Received in revised form 25 April 2020
Accepted 27 April 2020
Available online 27 May 2020

Keywords:
Physical layer security
CSI of illegitimate nodes
Computation complexity
Secrecy outage probability

ABSTRACT

In this paper, we focus on the design of optimal relay and jammer selection strategy in relay-aided wireless networks. Different from previous works, assuming that the channel state information (CSI) of illegitimate nodes was available and only an eavesdropper existed, we first analyze disadvantages of joint relay and jammer selection (JRJS), average optimal relay selection (AORS), traditional maximum relay selection (TMRS) schemes. Then, we design an optimal relay and jammer selection strategy where the ratio of received SNRs at the destination generated by any two relays is maximized. By applying proposed strategy, computation complexity can be reduced. Moreover, we derive the lower and upper bounds of the secrecy outage probability based on the assumptions of existence of only illegitimate node and symmetric case for mathematical convenience. Finally, simulation shows that the proposed strategy operating with no CSI of illegitimate nodes can work efficiently compared with JRJS, TMRS and AORS strategies.

1. Introduction

The broadcast nature of the transmission medium makes wireless communication systems vulnerable to security attacks. Traditionally, the security of wireless communications depends on cryptography-based techniques on the higher layers of the protocol stack. However, these techniques rely heavily on the assumption of limited computing power for illegitimate nodes, and have a high computational complexity consuming a significant energy. In recent years, the physical layer security (PLS) has emerged as a promising technique to improve the confidentiality of wireless communications, which exploits the time-varying properties of fading channels [38], such as fading, noise and interference.

To measure the performance of PLS-enhancement methods, the concept of secrecy outage probability (SOP) is introduced. That is, SOP refers to the probability that the secrecy capacity is less than a target secure rate R_s, where secrecy capacity is computed by max (C_s, 0), C_s denotes the capacity difference between the primary channel, from the source to the destination, and the eavesdropping channel, from the source to the illegitimate nodes [40,45].

Information of illegitimate nodes has a great effect on design and analysis of PLS-enhancement based strategies. In the past few years, several PLS-enhancement approaches have been proposed in the literature with unavailability or availability of illegitimate nodes' channel state information (CSI). Specifically, assuming that illegitimate nodes' CSI does not be unavailable, adding artificial noise can hold back illegitimate nodes from intercepting the data (e.g. [4,10,16,17,25,32,33,35,42,47]), but this behavior also poses a negative effect on transmission reliability. Assume that legitimate nodes can detect the existence of illegitimate nodes in their vicinity, setting protected zones (e.g. [4,26,50]) and guard zones (e.g. [9,41,44]) are additional effective schemes to ensure the PLS. Applying the availability assumption of illegitimate node's CSI, relay-based cooperative communications, usually combining with cooperative jamming schemes, (e.g., [14,19,23,28,34,36,38,46]) are designed to achieve both transmission reliability and security simultaneously, which is emerging as a promising research topic.

Given that the global CSI of both the legitimate and eavesdropping links was available, in [48,49], *Zou et al.* investigated both amplify-and-forward (AF) and decode-and-forward (DF) based optimal relay selection conceived for enhancing PLS in cooperative wireless networks. To prevent the data from being intercepted by illegitimate nodes, jamming techniques, which impose artificial interference on the illegitimate nodes, have also attracted significant attention (e.g., [5,7,22]). More specifically, several sophisticated joint relay and jammer selection (JRJS) schemes were proposed in [22], where the first relay increases the reliability of primary channel, whereas the carefully selected jammer creates intentional interference on the illegitimate nodes. In detail, let γ_{kd} and γ_{ke} denote the received SNR from relay k at the destination and illegitimate node e, respectively. With regard

* Corresponding author.
E-mail address: shdwjh@163.com (J. Wu).

https://doi.org/10.1016/j.jpdc.2020.04.013

to the relay and the illegitimate nodes, the relay selection tries to maximize the ratio γ_{kd}/γ_{ke} with $k = 1, \ldots, n$, while the jammer tries to minimize the same function, consequently the selection policy is independent of the selection order and will always select different relay terminals, where n is the number of relays. As far as the complexity, the simplified optimal selection with jamming policy has a complexity $O(n)$ and does not require algebraic computations [22]. Subsequently, most optimal relay and jammer selections were proposed based on this idea with using the assumption of global or average of illegitimate node's CSI.

In addition, because of the time variance of the channel and the processing delay, CSIs for legitimate and eavesdropping links used to make the relay and jammer selections may not be these ones during data transmission, i.e., the former is outdated [24,30,31,37]. Furthermore, more effective relaying and jamming schemes, when taking the effect of the outdated CSIs, have been presented lately in [6,38,39].

Considering multiple illegitimate nodes, in [1], *Alnahari et al.* presented two-phase cooperative protocol. In the first phase of the adopted DF relaying protocol, a jammer is selected from the set of relays to send an intentional interference to the illegitimate nodes. In the second phase, two relaying nodes are selected: one relay is selected to assist the source to deliver its information to its legitimate destination using the DF protocol, while the second relay behaves as a jamming node to confuse the illegitimate nodes. The proposed selection schemes were analyzed in terms of the achievable secrecy rate and SOP. To further increase the achievable secrecy rate, in [12], *Han et al.* exploited the JRJS technique and proposed a smart jamming algorithm to interfere the eavesdropping channels. Instead of maximizing the achievable secrecy rate, in [21], *Kolokotronis et al.* proposed a signal-to-noise ratio based approach, as this can be proved to be more practical.

In the above-mentioned literatures, all relays are friendly trusted, but the eavesdroppers are external illegitimate nodes. Even so, such untrusted relays are still valuable in cooperative transmission with AF or DF protocols, such as [13,29].

Based on the idea assumption of perfect CSI among legitimate and illegitimate nodes, most prior studies focused on the selection of optimal relay and jammer. However, it is not realistic in real scenarios, since practical channel estimation imposes CSI imperfections, which are aggravated by the feedback delay, limited-rate feedback, and channel estimation errors [15]. Moreover, a special case where only one illegitimate node exists is analyzed, such as [38,48,49]. Therefore, it is a challenging problem to choose optimal relay and jammer without the use of CSI between legitimate nodes and illegitimate nodes.

Our work assumes relaying and jamming at both stages of DF protocol, but unlike [18] and [27] they assume the existence of a direct link between the source and the destination; another difference with all the aforementioned works is that, with the unavailability of the global CSI of illegitimate nodes, we propose a new jammer selection scheme, and simulated results show that this scheme is more effective than JRJS in some special cases. Even when illegitimate nodes cooperatively intercept the data, obtained SOP is lower than that of JRJS. Moreover, the closed-form expression of SOP can be established even if no CSI of illegitimate nodes is used.

Explicitly, in this paper, we focus our attention on the design of transmission schemes for ensuring PLS with one relay and one jammer in cooperative relays-assisted networks. Assume that global illegitimate nodes' CSI does not be available, we propose a max-ratio relay selection scheme (MRRSS), which maximizes the difference between ratio of γ_{id}/γ_{jd}. Specifically, the main contributions of this paper can be summarized as follows.

- Based on traditional selection scheme in [48], we regard the legitimate relay which can generate the maximum SNR at the destination as the optimal relay. In this way, transmission reliability can be ensured as much as possible. Then, the legitimate relay which can generate the minimum SNR at the destination is selected to be as the optimal jammer. Note that MRRSS strategy has only a complexity of $O(n)$.
- Applying the probability density function and the cumulative distribution function of random variable, we derive the lower and upper bounds of SOP for designed strategies.
- Simulated results show that MRRSS strategy can present a higher secure communication compared to [22] and [1] (considering the global CSI of illegitimate nodes) and [38] (considering the average CSI of illegitimate nodes).

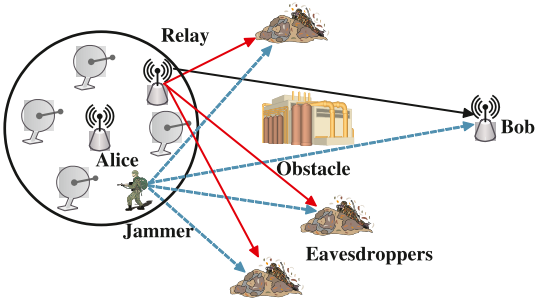

Fig. 1. Two phase cooperative protocol.

The remainder of this paper is organized as follows. In Section 2, we present the network model, performance metrics based on the PLS and analysis of previous PLS-enhancement methods. In Section 3, we derive mathematical expressions on the SOP for symmetric case. Simulated results are shown in Section 4. Finally, conclusion is given in Section 5.

2. Network model and preliminaries

2.1. Network model

Considering a cooperative wireless network consisting of a source s, a destination d, a set of n relays $\mathcal{R} = \{r_1, r_2, \ldots, r_n\}$ and a set of n_e illegitimate nodes $E = \{e_1, e_2, \ldots, e_{n_e}\}$. The direct communication between s and d is assumed to be unavailable due to the presence of obstructions and low transmission power, as well as the illegitimate nodes [38]. This assumption has been routinely exploited in previous literature, where the source and relays are located in the same cluster, the destination and illegitimate nodes are located outside the cluster, as shown in Fig. 1, and is particularly valid in networks with broadcast and unicast transmissions [22,38]. Moreover, the distances among the relays are assumed to be much smaller than the distances between relays and source/destination/illegitimate nodes; hence, the corresponding path losses among the different relays are approximately the same [1,38].

A slow flat block Rayleigh fading channel is assumed. That is, the channel fading gain remains static for one coherence interval (i.e., one slot) and changes independently in different coherence intervals, denoted by $h_{ij} \sim \mathcal{CN}(0, \sigma_{ij}^2)$, where $\sigma_{ij}^2 = l_{ij}^{-\alpha}$, l_{ij} is the Euclidean distance between nodes i and j, and α is the path-loss exponent [22,38]. Furthermore, additive white Gaussian noise (AWGN) is assumed with zero mean and unit variance σ_n^2 [20,43]. Let P denote the uniform transmission power of all nodes, then the instantaneous signal-noise ratio (SNR) from node i to node j is given by $\gamma_{ij} = \frac{P|h_{ij}|^2}{\sigma_n^2}$.

Table 1 shows some important notations.

Table 1
Notation.

Term	Description	Page
n	The number of relays	5
R	The set of relays	5
n_e	The number of illegitimate nodes	5
E	The set of eavesdroppers	5
h_{ij}	Channel fading gain between i and j	6
l_{ij}	Distance between i and j	6
σ_n^2	The noise power	6
γ_{ij}	The SNR from i to j	6
C_{id}^{DF}	The capacity from r_i to destination	6
R_s	Target secrecy rate	7

2.2. Secure and cooperative communication

The communication from source s to destination d applies two-phase cooperative protocol. Considering the DF protocol, the source first broadcasts the signal to trusted relays. Next, the optimal relay is selected to re-encode and forward its decoded signal to the destination. Furthermore, another kind of relays is selected to generate intended interference to illegitimate nodes for high reliability. In this way, when selected relay r_i transmits data to destination d, the instantaneous SNRs measured by destination d and illegitimate node e are $\gamma_{id} = \frac{P|h_{id}|^2}{\sigma_n^2}$ and $\gamma_{ie} = \frac{P|h_{ie}|^2}{\sigma_n^2}$, respectively.

Hence, considering r_i as the best relay, we can obtain the capacity of DF relaying transmission from r_i to destination by

$$C_{id}^{DF} = \frac{1}{2}\log_2\left(1+\frac{|h_{id}|^2 P}{\sigma_n^2}\right), \tag{1}$$

where the scalar factor is $\frac{1}{2}$ due to the fact that two time units are required in the two-phase cooperative scheme.

Meanwhile, the illegitimate nodes can overhear the transmission from r_i to destination. Hence, the channel capacity from r_i to illegitimate nodes can be easily represented as

$$C_{ie}^{DF} = \frac{1}{2}\log_2\left[1+\max_{e\in E}\left(\frac{|h_{ie}|^2 P}{\sigma_n^2}\right)\right]. \tag{2}$$

To measure the performance of designed cooperative communication scheme, we introduce two measurement indexes to evaluate the performance of selected relay and jammer as follows.

The Capacity of DF Relaying Transmission (CDFT) [48]: CDFT refers to the difference between transmitting rate and eavesdropping rate which are given by Eqs. (1) and (2). That is Eq. (3).

$$C_i^{DF} = \begin{cases} \left[C_{id}^{DF} - C_{ie}^{DF}\right]^+ = \left[\frac{1}{2}\log_2\left(1+\frac{|h_{id}|^2 P}{\sigma_n^2}\right) \right. \\ \quad \left. - \frac{1}{2}\log_2\left(1+\max_{e\in E}\left(\frac{|h_{ie}|^2 P}{\sigma_n^2}\right)\right)\right]^+, & |\mathcal{R}|>0; \\ 0, & |\mathcal{R}|=0 \end{cases} \tag{3}$$

where $|\mathcal{R}|$ denotes the size of set $\mathcal{R}$.

Note that no instantaneous non-zero secrecy rate can ensure to be achieved under fading channels. When CDFT is negative, the illegitimate nodes can intercept the signal. Thus, the probability that the illegitimate nodes wiretap source signal successfully, called ***secrecy outage probability (SOP)***, is a key measuring index in evaluating the performance of PLS. In this paper, we mainly focus on how to decrease the SOP by exploiting the optimal relay and jammer selections.

The secrecy outage probability (SOP): The SOP is defined as the probability that the CDFT is less than a given target secrecy rate $R_s > 0$ [2,3,22]:

$$\begin{aligned} p_{so} &= \Pr[C_i^{DF} < R_s] \\ &= \Pr\left[\left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{RD}}{\max_{E_{m\in S_{eav}}}\{1+\gamma_{RE_m}\}}\right)\right]^+ < R_s\right], \end{aligned} \tag{4}$$

where C_s is given in Eq. (3).

2.3. Analysis of previous methods

In this subsection, we give a brief summary for methods of cooperation communication with or without illegitimate node(s).

(1) *Traditional Max–min Relay Selection Scheme (TMRS)* [3]: Let us first present the traditional max–min relay selection scheme for the purpose of comparison. In the traditional relay selection scheme, the relay that maximizes the capacity of DF relaying transmission is viewed as the best relay. Thus, the traditional relay selection criterion is obtained from Eq. (1) as

$$r_{i^*} = \arg\max_{r_i\in\mathcal{R}} \min\left(|h_{si}|^2, |h_{id}|^2\right). \tag{5}$$

As shown in Eq. (5), only the main links' CSI $|h_{si}|^2$ and $|h_{id}|^2$ is considered in the max–min relay selection scheme without considering the illegitimate node's CSI $|h_{ie}|^2$ for $e \in E$.

(2) *Proposed Best Relay Selection Scheme (PBRSS)* [48]: Considering the CSI of both main and wiretap links, in PBRSS, the relay that maximizes the secrecy capacity of DF relaying transmission is selected as the best relay. Thus, the best relay selection criterion is obtained from Eq. (3) as

$$\begin{aligned} r_{i^*} &= \arg\max_{r_i\in\mathcal{R}} C_i^{DF} \\ &= \arg\max_{r_i\in\mathcal{R}} \frac{\min\left(|h_{si}|^2, |h_{id}|^2\right)P + \sigma_n^2}{|h_{ie}|^2 P + \sigma_n^2}. \end{aligned} \tag{6}$$

One can observe from Eq. (6) that the proposed best relay selection scheme takes into account not only the main links' CSI, but also the wiretap link's CSI. This differs from the traditional max–min relay selection criterion in Eq. (5) where only the main links' CSI is considered.

(3) *The average optimal relay selection (AORS)* [22]: Only average CSI of illegitimate nodes is obtained, AORS selects the optimal relay. It is a solution which efficiently makes a trade-off between TMRS and PBRSS with a low complexity overhead. The AORS is expressed as

$$r_{i^*} = \arg\max_{r_i\in\mathcal{R}}\left\{\frac{\gamma_{id}}{E[\gamma_{ie}]}\right\}. \tag{7}$$

(4) *The joint relay and jammer selection (JRJS)* [38]: To increase transmission security in schemes of TMRS, PBRSS and AORS, the JRJS is expressed as

$$r_{i^*} = \arg\max_{r_i\in\mathcal{R}}\left\{\frac{\gamma_{id}}{\min_{e\in E}\{\gamma_{ie}\}}\right\}, \tag{8a}$$

$$r_{j^*} = \arg\min_{r_i\in\mathcal{R}\setminus\{r_{i^*}\}}\left\{\frac{\gamma_{jd}}{\max_{e\in E}\{\gamma_{je}\}}\right\}, \tag{8b}$$

where r_{j^*} is the selected optimal jammer.

Note that PBRSS and JRJS schemes need the global CSI of illegitimate nodes, whereas AORS scheme needs their average CSI. From [22], we observe that with regard to the relaying and the eavesdropping nodes, the relay selection tries to maximize the ratio γ_{id}/γ_{ie}, while the jammer tries to minimize the same function, consequently the selection policy is independent of the selection order and will always select different relays.

However, illegitimate nodes intercept the data once the optimal relay is selected by Eq. (8a). Without considering cooperation among illegitimate nodes, a special illegitimate node, denoted by e^*, whose received SNR γ_{i^*e} is maximum has the greatest possibility of wiretapping the data successfully. Based on this fact, we should choose another relay to generate intended interference to above illegitimate node rather than to illegitimate node e which means that the ratio of received SNRs γ_{jd}/γ_{je} is minimum among for all illegitimate nodes. In fact, the optimal jammer selected by Eq. (8b) may not generate larger enough interference to e^*, then resulting in a higher SOP.

Next, we design two PLS-based strategies as follows.

(4) *The Max Relay Selection Scheme (MRSS):* In MRSS, the relay that maximizes CDFT C_{id}^{DF} is viewed as the best relay. That is,

$$\begin{aligned} r_{i^*} &= \arg\max_{r_i\in\mathcal{R}} C_{id}^{DF} \\ &= \arg\max_{r_i\in\mathcal{R}} |h_{id}|^2. \end{aligned} \tag{9}$$

Without considering the CSI of illegitimate nodes, the idea of MRSS is only maximizing received SNR at the destination for high level of reliability. Then, to achieve high level of transmission security, we give following scheme consisting of optimal relaying and jamming nodes. The computation complexity of MRSS is at most n.

(5) *The Max-Ratio Relay Selection Scheme (MRRSS):* We now propose the best relay selection criterion without considering the CSI of wiretap links, in which the relay that maximizes CDFT C_{id}^{DF} is selected as the best relay, and the jammer that minimizes CDFT C_{jd}^{DF} is selected as the best jammer. Thus, the best relay and jammer selection criterions are given by

$$(r_{i^*}, r_{j^*}) = \arg\max_{r_i\in\mathcal{R}} \frac{|h_{id}|^2}{\arg\min_{r_j\in\mathcal{R}\setminus\{r_{i^*}\}} |h_{jd}|^2}. \tag{10}$$

Additionally, for mathematical convenience of the SOP, as shown in [22,38,49] and [8], assume that $n_e = 1$ and $E[\sigma_{id}^2] = E[\sigma_{ie}^2] = E[\sigma_{je}^2] = \sigma^2$. This configuration simplifies the analysis and gives a guideline for the general asymmetric case. But in simulation, those assumptions are removed and we evaluate performance difference of cooperative communication schemes mentioned in this paper.

3. The expression of SOP with proposed selection

We apply the following proposition and corollary to derive SOP.

Proposition 1. *If X_k and Y_k are two independent and identically distributed (i.i.d.) exponential random variables with mean λ and $k = 1, \ldots, n$, the probability density function (PDF) and the cumulative distribution function (CDF) of new random variable $Z_k = \frac{X_k}{Y_k}$ are given by*

$$P_Z(z) = \begin{cases} \frac{z}{1+z}, & z \geq 0 \\ 0, & otherwise, \end{cases} \tag{11}$$

$$p_Z(z) = \begin{cases} \frac{1}{(1+z)^2}, & z \geq 0 \\ 0, & otherwise. \end{cases} \tag{12}$$

Corollary 1. *The CDF and the PDF of new random variable $\mathcal{Z}_{max} = \max\{Z_k\}$ with $k = 1, \ldots, n$ are expressed as*

$$P_{\mathcal{Z}_{max}}(z) = \begin{cases} \left(\frac{z}{1+z}\right)^n, & z \geq 0 \\ 0, & otherwise, \end{cases} \tag{13}$$

$$p_{\mathcal{Z}_{max}}(z) = \begin{cases} n\left(\frac{z}{1+z}\right)^{n-1} \frac{1}{(1+z)^2}, & z \geq 0 \\ 0, & otherwise. \end{cases} \tag{14}$$

Under the MRSS, only optimal relaying node is selected. Thus, we get with high SNR

$$\begin{aligned} p_{so} &= \Pr\left[C_i^{DF} < R_s\right] \\ &= \Pr\left[\log_2\left(\frac{1+\frac{|h_{id}|^2 P}{\sigma_n^2}}{1+\frac{|h_{ie}|^2 P}{\sigma_n^2}}\right) < R_s\right] \\ &\simeq \Pr\left[\frac{\max_{r_i\in\mathcal{R}} |h_{id}|^2}{|h_{ie}|^2} < \epsilon\right] \\ &= P_{\hat{\mathcal{X}}_{max}}(\epsilon), \end{aligned} \tag{15}$$

where $\epsilon = 2^{2R_s}$, $\mathcal{X}_{max} = \max\{X_k\}$, and $P_{\hat{\mathcal{X}}_{max}}(\cdot)$ denotes the CDF of $\frac{\mathcal{X}_{max}}{X_k}$ with $k = 1, \ldots, n$ which is given by

$$\begin{aligned} P_{\hat{\mathcal{X}}_{max}}(\epsilon) &= \int_0^{+\infty} P_{\mathcal{X}_{max}}(x\epsilon) p_X(x) dx \\ &= \int_0^{+\infty} \left(1 - e^{-\lambda\epsilon x}\right)^n \lambda e^{-\lambda x} dx \\ &\overset{(*)}{=} \frac{1}{\epsilon} \mathbf{B}\left(\frac{1}{\epsilon}, n+1\right), \end{aligned} \tag{16}$$

where $\mathbf{B}(x, y) = \int_0^1 t^{x-1}(1-t)^{y-1} dt$ is the Beta function, and $(*)$ holds due to $\int_0^{+\infty} (1 - e^{-\frac{x}{\beta}})^{\nu-1} e^{-\mu x} dx = \beta \mathbf{B}(\beta\mu, \nu)$ [11].

Furthermore, we show that the SOP obtained by MRSS strategy cannot be reduced to 0 due to unavailability of illegitimate nodes' CSI. That is, the lower bound of SOP can be derived by

$$\begin{aligned} p_{so} &\simeq \Pr\left[\frac{\max_{r_i\in\mathcal{R}} |h_{id}|^2}{|h_{ie}|^2} < \epsilon\right] \\ &= 1 - \Pr\left[\frac{\max_{r_i\in\mathcal{R}} |h_{id}|^2}{|h_{ie}|^2} \geq \epsilon\right] \\ &\geq 1 - \Pr\left[\max_{r_i\in\mathcal{R}} \frac{|h_{id}|^2}{|h_{ie}|^2} \geq \epsilon\right] \\ &= 1 - \int_\epsilon^\infty n\left(\frac{z}{1+z}\right)^{n-1} \frac{1}{(1+z)^2} dz \\ &= \left(\frac{\epsilon}{1+\epsilon}\right)^n. \end{aligned} \tag{17}$$

From results in Eqs. (16) and (17), increasing the number of relays is an effective way to ensure high level of security.

Corollary 2. *The CDF and the PDF of new random variable $\mathcal{Z}'_{min} = \min\{Z_k\}$ with $k = 1, \ldots, n-1$ are expressed as*

$$P_{\mathcal{Z}'_{min}}(z) = \begin{cases} 1 - \left(\frac{1}{1+z}\right)^{n-1}, & z \geq 0 \\ 0, & otherwise, \end{cases} \tag{18}$$

$$p_{\mathcal{Z}'_{min}}(z) = \begin{cases} (n-1)\frac{1}{(1+z)^n}, & z \geq 0 \\ 0, & otherwise. \end{cases} \tag{19}$$

Under the MRRSS, both optimal relaying node and jamming node are selected, based on conclusions of Corollaries 1 and 2, we get with high SNR

$$\begin{aligned} p_{so} &= \Pr\left[C_i^{DF} < R_s\right] \\ &= \Pr\left[\log_2\left(\frac{1+\frac{|h_{id}|^2 P}{|h_{jd}|^2 P+\sigma_n^2}}{1+\frac{|h_{ie}|^2 P}{|h_{je}|^2 P+\sigma_n^2}}\right) < R_s\right] \\ &\simeq \Pr\left[\frac{\frac{|h_{id}|^2}{|h_{ie}|^2}}{\frac{|h_{jd}|^2}{|h_{je}|^2}} < \epsilon\right] \end{aligned}$$

$$\geq \Pr\left[\frac{\mathcal{Z}_{\max}}{\mathcal{Z}'_{\min}} < \epsilon\right]$$
$$= P_{\hat{\mathcal{Z}}}(\epsilon) \tag{20}$$

where $P_{\hat{\mathcal{Z}}}(\cdot)$ denotes the CDF of $\hat{\mathcal{Z}} = \frac{\mathcal{Z}_{\max}}{\mathcal{Z}'_{\min}}$ which is given by

$$\begin{aligned} P_{\hat{\mathcal{Z}}}(\epsilon) &= \Pr\left[\frac{\mathcal{Z}_{\max}}{\mathcal{Z}_{\min}} < \epsilon\right] = \Pr\left[\mathcal{Z}_{\max} < \mathcal{Z}_{\min}\epsilon\right] \\ &= \int_0^{+\infty} P_{\mathcal{Z}_{\max}}(z\epsilon) p_{\mathcal{Z}_{\min}}(z) dz \\ &= \int_0^{+\infty} \left(\frac{z\epsilon}{1+z\epsilon}\right)^n (n-1)\frac{1}{(1+z)^n} dz \\ &= (n-1)\epsilon^n \int_0^{+\infty} \left[\frac{z}{(1+z\epsilon)(1+z)}\right]^n dz \\ &= \frac{\epsilon^n}{2^n - (1+\epsilon)^n}\left(\frac{1}{\epsilon} - 1\right). \end{aligned} \tag{21}$$

Additionally, we get

$$\begin{aligned} p_{\text{so}} &\leq \Pr\left[\frac{\mathcal{Z}_{\min}}{\mathcal{Z}'_{\max}} < \epsilon\right] \\ &= P_{\hat{\mathcal{Z}}}(\epsilon) = \Pr\left[\mathcal{Z}_{\min} < \mathcal{Z}'_{\max}\epsilon\right] \\ &= \int_0^{+\infty} P_{\mathcal{Z}_{\min}}(z\epsilon) p_{\mathcal{Z}'_{\max}}(z) dz \\ &= \int_0^{+\infty} \left[1 - \left(\frac{1}{1+z\epsilon}\right)^n\right](n-1)\frac{z^{n-2}}{(1+z)^n} dz \\ &= n\epsilon \int_0^{+\infty} \left(\frac{z}{1+z}\right)^{n-1} \left(\frac{1}{1+z\epsilon}\right)^{n+1} dz. \end{aligned} \tag{22}$$

To sum up, MRRSS scheme is completely independent of the global CSI of illegitimate node, and we derive the close-form expression of SOP. In the following section, we evaluate the performance of PLS-based schemes in realistic environment.

4. Evaluations

In this section, we validate the performance of TMRS [3], PBRSS [48], AORS [22], JRJS [1,22,38], MRSS and MRRSS strategies by simulator MATLAB. Furthermore, simulations are carried out on a 1000 × 1000 m^2 plane constructed by randomly placing legitimate relays and illegitimate nodes, the source is located in [300, 300], and the results averaged over 5000 runs. Additionally, we set the transmission power $P = 1$ mW, the decoding threshold $\beta_t = 0.5$ dB, the path-loss exponent $\alpha = 5$, the radius of cluster is 10 m, the distance between the source and the destination is 50 m, and a fraction of transmission power in broadcasting phase P is 0.1 mW.

The radius of cluster is 10 m, the distance between the source and the destination is 50 m, the number of relays $n = 10$, the target rate $R_s = 0.01$ and the noise power is $\sigma_n^2 = 10^{-9}$, in Fig. 2, we evaluate the performance of TMRS, PBRSS, AORS, JRJS and MRRSS (considering illegitimate node cooperation or not) strategies for different number of eavesdroppers. As expected, although MRRSS scheme does not obtain the eavesdroppers's CSI, the corresponding SOP is strictly lower than those of TMRS, PBRSS, AORS and JRJS schemes. The reason is that although the difference between strengths of two different signals is maximized, interference suffered from jamming node has little difference compared with strength of expected signal transmitted by optimal relay due to small radius of cluster, namely $\gamma_{i^*e}/\gamma_{j^*e}$ is more or less the same. This confirms that the PRRSS scheme is effective by modifying selecting process of optimal relaying and jamming nodes from Eqs. (8a) and (8b) to Eq. (10).

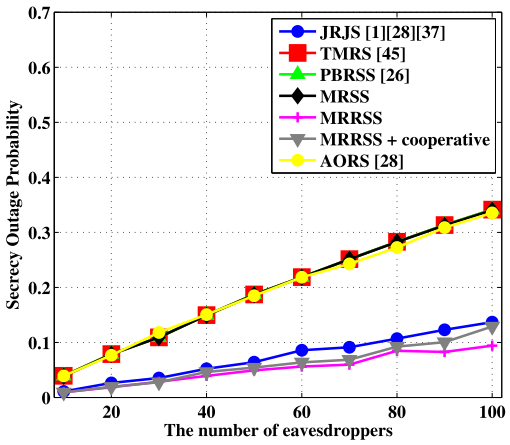

Fig. 2. The SOP vs. n_e with $R_s = 0.01$.

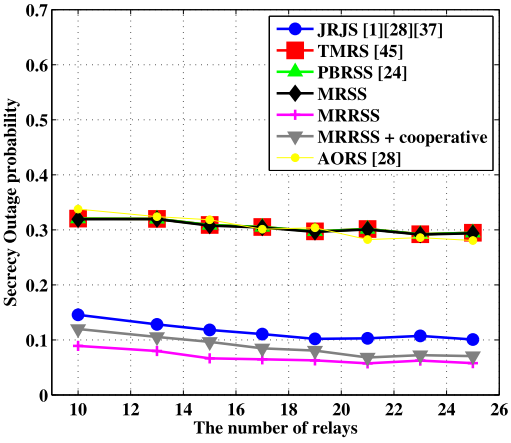

Fig. 3. The SOP vs. n with $R_s = 0.01$.

Generally speaking, cooperation among illegitimate nodes can decrease the transmission security. MRRSS with cooperative illegitimate nodes can obtain a lower SOP than those of PBRSS, AORS, JRJS operating with illegitimate nodes' CSI, which further evaluates the effectiveness of MRRSS scheme. MRSS operating no jamming cannot provide a secure transmission, in other words, applying jamming scheme can improve transmission security to some extent, even if illegitimate nodes eavesdrop the data cooperatively, as shown in MRRSS with cooperative eavesdropping. Similarly, AORS scheme only knows average CSI of eavesdroppers and does not consider cooperative jamming scheme, the SOP of AORS scheme is almost same to those of TMRS, MRSS operating with no eavesdroppers' CSI.

The radius of cluster is 10 m, the distance between the source and the destination is 50 m, the number of relays $n_e = 100$, the target rate $R_s = 0.01$ and the noise power is $\sigma_n^2 = 10^{-9}$, in Fig. 3, we can see that MRRSS strategy outperforms TMRS, PBRSS, JRJS, AORS and MRSS for different number of relays, which validates the effectiveness of our conclusion for MRRSS. Furthermore, as expected, increasing the number of relays will be able to improve the performance of transmission security. Generally, cooperation among illegitimate nodes can decrease the transmission security, even if jamming scheme is adopted. Specifically, MRRSS with eavesdropping cooperatively shows a higher level of security than other schemes. This is because that the selected optimal jammer is more optimal than those of JRJS, which demonstrates the effectiveness of Eq. (10).

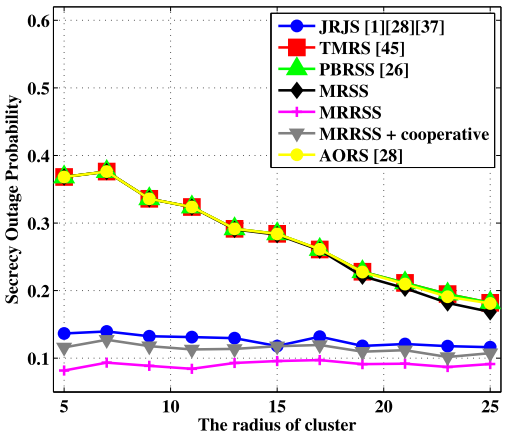

Fig. 4. The SOP vs. the radius of cluster with $R_s = 0.01$.

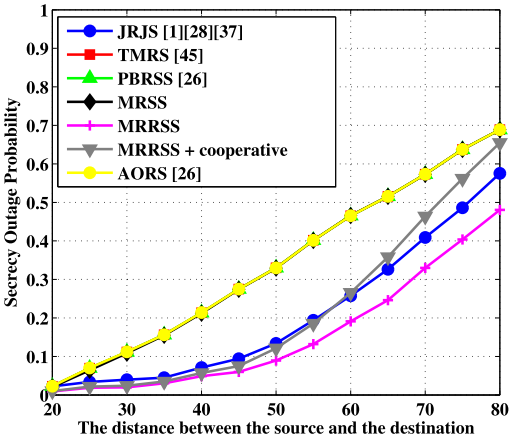

Fig. 5. The SOP vs. the distance with $R_s = 0.01$.

The number of illegitimate nodes is $n_e = 100$, the distance between the source and the destination is 50 m, the number of relays $n = 10$, the target rate $R_s = 0.01$ and the noise power is $\sigma_n^2 = 10^{-9}$, in Fig. 4, we compare MRRSS scheme with other schemes for different radius of cluster. Similar to Figs. 3 and 4, MRRSS strategy shows the best performance of security; and the level of security for MRRSS with cooperative illegitimate nodes is higher than those of JRJS, PBRSS and AORS operating with the illegitimate nodes' CSI. The reason is also similar to those in Figs. 3 and 4.

The number of illegitimate nodes is $n_e = 100$, the number of relays $n = 10$, the target rate $R_s = 0.01$ and the noise power is $\sigma_n^2 = 10^{-9}$, in Fig. 5, we validate the performance difference between MRRSS strategy and other strategies for different settings of communication distance. As expected, on the one hand, MRRSS shows the best secure performance; on the other hand, although illegitimate nodes cooperatively intercept the data by using MRRSS strategy, the induced SOP is lower than that of JRJS when transmission distance from the source to the destination 60 m, which further confirms the effectiveness of MRRSS strategy.

The number of illegitimate nodes is $n_e = 100$, the number of relays $n = 10$, the distance between the source and the destination is 50 m and the target rate $R_s = 0.01$, to further explore the impact of noise power on the SOP, we show in Fig. 6 how MRRSS outperforms TMRS, PBRSS, JRJS, AORS and MRSS for different settings of noise power. It can be observed from Fig. 6 that the SOPs achieved by those strategies increase with σ_n^2. It is noticed that the overall impact of noise on the strength of

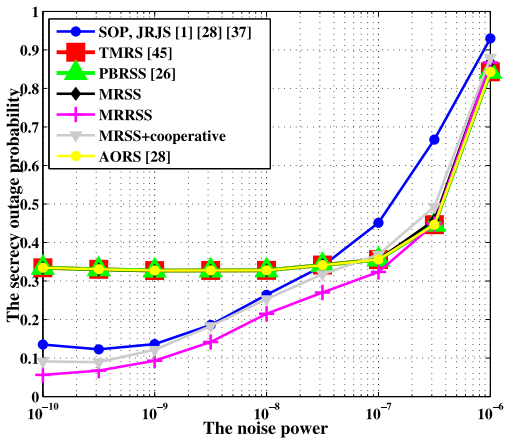

Fig. 6. The SOP vs. σ_n^2 with $R_s = 0.01$.

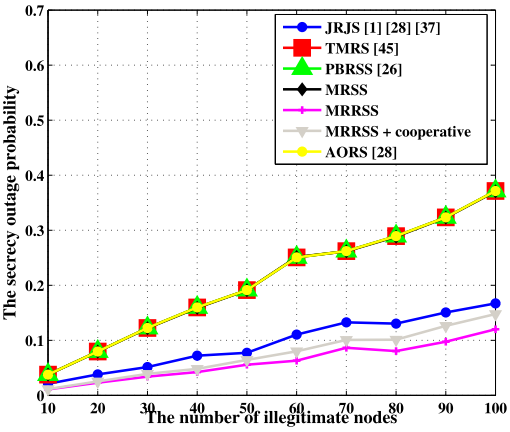

Fig. 7. The SOP vs. n_e with $R_s = 0.1$.

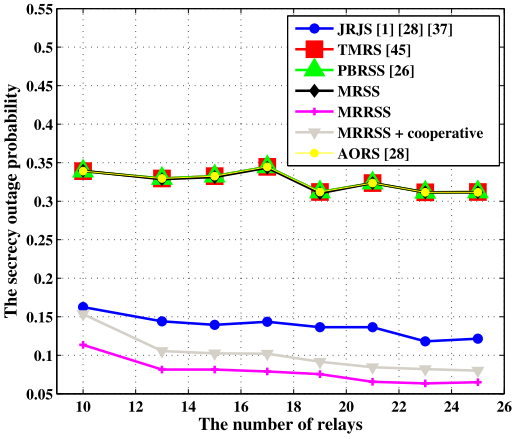

Fig. 8. The SOP vs. n with $R_s = 0.1$.

received signal from the relay to the destination is larger than the impact of noise power on the strength of eavesdropping signal from the relay to the illegitimate nodes. Although adding artificial noise may lower the transmission from the relay to the illegitimate nodes, it also makes the transmission from the relay to the destination bad. Therefore, it is suggested to not add some artificial noise to achieve a lower SOP for some occasions.

With settings of $R_s = 0.1$, the impacts of n, n_e, σ_n^2 and the distance from the source to the destination on the SOP are shown in Figs. 7–11.

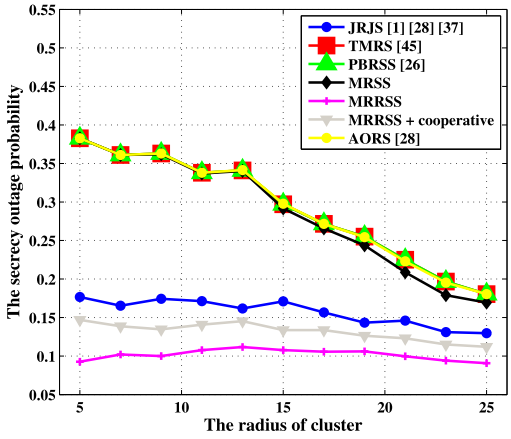

Fig. 9. The SOP vs. the radius of cluster with $R_s = 0.1$.

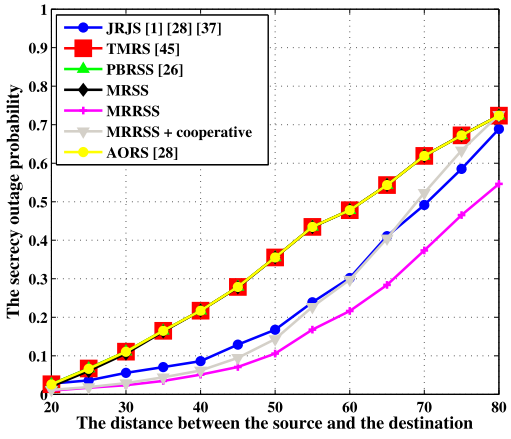

Fig. 10. The SOP vs. the distance with $R_s = 0.1$.

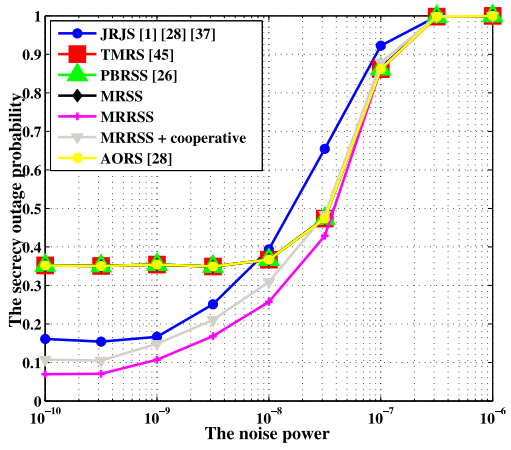

Fig. 11. The SOP vs. σ_n^2 with $R_s = 0.1$.

To sum up, MRRSS strategy not only achieves the highest level of transmission security without available CSI of illegitimate nodes, but also needs more lower computation complexity.

5. Conclusion

In this paper, we investigated how to improve the physical layer security in cooperative wireless networks with multiple trusted relays and no CSI of illegitimate nodes. We analyzed three popular PLS-enhancement methods and derived the lower and upper bounds of the SOP of MRRSS scheme. Theoretical analysis and simulated results demonstrated that MRRSS scheme is more effective than JRJS scheme. However, all relays are friendly trusted in this paper, in some situations, the relays act as illegitimate nodes to decode the message besides forwarding the confidential message. Therefore, how to enhance PLS for untrusted relays will be studied in future work.

CRediT authorship contribution statement

Guangshun Li: Conceptualization, Methodology. **Xiaofei Sheng:** Writing - original draft. **Junhua Wu:** Writing - review & editing. **Haili Yu:** Writing - review & editing.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Acknowledgments

This work is supported by the Major Basic Research of Natural Science Foundation of Shandong Province, China (ZR2019ZD10), Key Research and Development Plan of Shandong Province, China (2019GGX101050).

References

[1] A. Al-nahari, I. Krikidis, A. Ibrahim, M. Dessouky, F. Abd El-Samie, Relaying techniques for enhancing the physical layer secrecy in cooperative networks with multiple eavesdroppers, Trans. Emerg. Telecommun. Technol. 25 (2014) 445–460.
[2] J. Barros, M.R.D. Rodrigues, Secrecy capacity of wireless channels, in: Proceedings of IEEE ISIT, 2006, pp. 356–360.
[3] A. Bletsas, H. Shin, M.Z. Win, A. Lippman, A simple cooperative diversity method based on network path selection, IEEE J. Sel. Areas Commun. 24 (3) (2006) 659–672.
[4] S. Chae, W. Choi, J. Lee, T. Quek, Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone, IEEE Trans. Inf. Forensics Secur. 9 (10) (2014) 1617–1628.
[5] J. Chen, R. Zhang, L. Song, Z. Han, B. Jiao, Joint relay and jammer selection for secure two-way relay networks, IEEE Trans. Inf. Forensic Secur. 7 (1) (2012) 310–320.
[6] H. Deng, H. Wang, W. Guo, W. Wang, Secrecy transmission with a helper: To relay or to jam, IEEE Trans. Inf. Forensics Secur. 10 (2) (2015) 293–307.
[7] Z. Ding, M. Xu, J. Lu, F. Liu, Improving wireless security for bidirectional communication scenarios, IEEE Trans. Veh. Technol. 61 (6) (2012) 2842–2848.
[8] L. Dong, Z. Han, A. Petropulu, H. Poor, Improving wireless physical layer security via cooperating relays, IEEE Trans. Signal Process. 58 (3) (2010) 1875–1888.
[9] M. Ghogho, A. Swami, Physical-layer secrecy of MIMO communications in the presence of a Poisson random field of eavesdroppers, in: Proceedings of IEEE ICC, 2011, pp. 1–5.
[10] S. Goel, R. Negi, Guaranteeing secrecy using artificial noise, IEEE Trans. Wireless Commun. 7 (6) (2008) 2180–2189.
[11] I.S. Gradshteyn, I.M. Ryzhik, Table of Integrals, Series and Products, 2000.
[12] B. Han, J. Li, J. Su, M. Guo, B. Zhao, Secrecy capacity optimization via cooperative relaying and jamming for WANETs, IEEE Trans. Parallel Distrib. Syst. 26 (4) (2015) 1117–1128.
[13] B. He, Q. Ni, J. Chen, L. Yang, L. Lv, User-pair selection in multiuser cooperative networks with an untrusted relay, IEEE Trans. Veh. Technol. 68 (1) (2019) 869–882.
[14] F. He, A. Yener, Cooperative jamming: The tale of friendly interference for secrecy, in: Proceedings of Annual Allerton Conference on Communication, Control, and Computing 2010, 2010, pp. 65–88.
[15] B. He, X. Zhou, T.D. Abhayapala, Wireless physical layer security with imperfect channel state information: A survey, ZTE Commun. 11 (3) (2013) 11–19.
[16] L. Hu, H. Wen, B. Wu, F. Pan, R. Liao, H. Song, J. Tang, X. Wang, Cooperative jamming for physical layer security enhancement in internet of things, IEEE Internet Things J. 5 (1) (2018) 219–228.

[17] L. Hu, H. Wen, B. Wu, J. Tang, F. Pan, R. Liao, Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers, IEEE Trans. Veh. Technol. 67 (3) (2018) 2025–2034.
[18] J. Huang, A.L. Swindlehurst, Secure communications via cooperative jamming in two–hop relay systems, in: Proceedings of IEEE GLOBECOM, 2010, pp. 1–5.
[19] M. Kang, Y. Kim, J. Lee, J. Lee, W. Choi, Secrecy capacity scaling by jamming-aided hierarchical cooperation in ad hoc networks, IEEE J. Sel. Top. Sign. Proces. 10 (8) (2016) 1390–1403.
[20] D.S. Karas, A.A. Boulogeorgos, G.K. Karagiannidis, Physical layer security with uncertainty on the location of the eavesdropper, IEEE Wirel. Commun. Lett. 5 (5) (2016) 540—543.
[21] N. Kolokotronis, M. Athanasakos, Improving physical layer security in DF relay networks via two-stage cooperative jamming, in: Proceedings of EUSIPCO, 2016, pp. 1173–1177.
[22] I. Krikidis, J. Thompson, S. McLaughlin, Relay selection for secure cooperative networks with jamming, IEEE Trans. Wireless Commun. 8 (10) (2009) 5003–5011.
[23] L. Lai, H. Gamal, The relay-eavesdropper channel: cooperation for secrecy, IEEE Trans. Inform. Theory 54 (9) (2008) 4005–4019.
[24] Y. Li, Q. Yin, W. Xu, H.-M. Wang, On the design of relay selection strategies in regenerative cooperative networks with outdated CSI, IEEE Trans. Wireless Commun. 10 (9) (2011) 3086–3097.
[25] W. Liao, T. Chang, W. Ma, C. Chi, QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach, IEEE Trans. Inform. Theory 59 (3) (2011) 1202–1216.
[26] W. Liu, Z. Ding, T. Ratnarajah, J. Xue, On ergodic secrecy capacity of random wireless networks with protected zones, IEEE Trans. Veh. Technol. 65 (8) (2016) 6146–6158.
[27] Y. Liu, J. Li, A. Petropulu, Destination assisted cooperative jamming for wireless physical–layer security, IEEE Trans. Inf. Forensics Secur. 8 (4) (2013) 682–694.
[28] D. Lun, H. Zhu, A. Petropulu, H. Poor, Secure wireless communications via cooperation, in: Proceedings of Annual Allerton Conference on Communication, Control, and Computing, 2008, pp. 1132–1138.
[29] L. Lv, F. Zhou, J. Chen, N. Al-Dhahir, Secure cooperative communications with an untrusted relay: a NOMA-inspired jamming and relaying approach, IEEE Trans. Inf. Forensics Secur. 14 (12) (2019) 3191–3205.
[30] D.S. Michalopoulos, N.D. Chatzidiamantis, R. Schober, G.K. Karagiannidis, The diversity potential of relay selection with practical channel estimation, IEEE Trans. Wireless Commun. 12 (2) (2013) 481–493.
[31] D.S. Michalopoulos, H.A. Suraweera, G.K. Karagiannidis, R. Schober, Amplify-and-forward relay selection with outdated channel estimates, IEEE Trans. Wireless Commun. 60 (5) (2012) 1278–1289.
[32] H. Qin, X. Chen, Y. Sun, M. Zhao, J. Wang, Optimal power allocation for joint beamforming and artificial noise design in secure wireless communications, in: Proceedings of IEEE ICC, 2011, pp. 1–5.
[33] Z. Romero, M. Ghogho, D. McLernon, Outage probability based power distribution between data and artificial noise for physical layer security, IEEE Signal Process. Lett. 19 (2) (2012) 71–74.
[34] W. Shi, J. Ritcey, Distributed jamming for secure communication in Poisson fields of legitimate nodes and eavesdroppers, in: Proceedings of ASILOMAR, 2012, pp. 1881–1885.
[35] A. Swindlehurst, Fixed SINR solutions for the MIMO wiretap channel, in: Proceedings of IEEE ICASSP, 2009, pp. 2437–2440.
[36] E. Tekin, A. Yener, The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming, IEEE Trans. Inform. Theory 54 (6) (2008) 2735–2751.
[37] J.L. Vicario, A. Bel, J.A. Lopez-Salcedo, G. Seco, Opportunistic relay selection with outdated CSI: Outage probability and diversity analysis, IEEE Trans. Wireless Commun. 8 (6) (2009) 2872–2876.
[38] L. Wang, Y. Cai, Y. Zou, W. Yang, L. Hanzo, Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays, IEEE Trans. Veh. Technol. 65 (8) (2016) 6259–6274.
[39] C. Wang, H.M. Wang, X.G. Xia, Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks, IEEE Trans. Wireless Commun. 14 (2) (2015) 589–605.
[40] A. Wyner, The wire-tap channel, Bell Syst. Tech. J. 54 (8) (1975) 1355–1387.
[41] J. Zhang, L. Fu, X. Wang, Asymptotic analysis on secrecy capacity in large-scale wireless networks, IEEE/ACM Trans. Netw. 22 (1) (2014) 66–79.
[42] X. Zhang, M. McKay, X. Zhou, R. Heath, Artificial-noise-aided secure multi-antenna transmission with limited feedback, IEEE Trans. Wireless Commun. 14 (5) (2015) 2742–2754.
[43] T. Zhang, H. Wen, J. Tang, H. Song, R. Liao, Y. Chen, Y. Jiang, Analysis of the physical layer security enhancing of wireless communication system under the random mobile, IET Commun. 13 (2019) 1164—1170.
[44] X. Zhou, R. Ganti, J. Andrews, A. Hjorungnes, On the throughput cost of physical layer security in decentralized wireless networks, IEEE Trans. Wireless Commun. 10 (8) (2011) 2764–2775.
[45] X. Zhou, M. McKay, B. Maham, A. Hjørungnes, Rethinking the secrecy outage formulation: A secure transmission design perspective, IEEE Commun. Lett. 15 (3) (2011) 302–304.
[46] X. Zhou, M. Tao, R. Kennedy, Cooperative jamming for secrecy in decentralized wireless networks, in: Proceedings of IEEE ICC, 2012, pp. 2339–2344.
[47] J. Zhu, Y. Chen, Y. Shen, O. Takahashi, X. Jiang, N. Shiratori, Secrecy transmission capacity in noisy wireless ad hoc networks, Ad Hoc Netw. 21 (2014) 123–133.
[48] Y. Zou, X. Wang, W. Shen, Optimal relay selection for physical-layer security in cooperative wireless networks, IEEE J. Sel. Areas Commun. 31 (10) (2013) 2099–2111.
[49] Y. Zou, X. Wang, W. Shen, L. Hanzo, Security versus reliability analysis of opportunistic relaying, IEEE Trans. Veh. Technol. 63 (6) (2014) 2653–2661.
[50] N. Zurita, D. McLernon, M. Ghogho, A. Swami, PHY layer security based on protected zone and artificial noise, IEEE Signal Process. Lett. 20 (5) (2013) 487–490.

Guangshun Li received the PH.D. degree from Harbin Engineering University, China, in 2008. He is currently an associate professor of the School of Information Science and Engineering, Qufu Normal University, China. He is a Visiting scholar of the Hong Kong polytechnic university in the second half year of 2019. He has already published more than 50 papers. His research interests include wireless networks, IoT, and Big data.

Xiaofei Sheng received the bachelor's degree in computer science and technology from Qufu Normal University, China, in 2017. She is currently working toward the MSc degree at Qufu Normal University, China. Her current research interests include mobile edge computing, privacy protection, and access control.

Junhua Wu received the PH.D. degree from Harbin Engineering University, China, in 2009. She is currently an associate professor of the School of Information Science and Engineering, Qufu Normal University, China. She has already published more than 40 papers. His research interests include wireless networks, edge computing and IoT.

Haili Yu received her bachelor's degree in computer science and technology from Qufu Normal University in 2018. She is currently studying for a master's degree at Qufu Normal University in China. Her current research interests include mobile edge computing, privacy protection and blockchain.