Abstract
In this article, we studied the robust security transmission design for multi-user peer-to-peer relay networks, where all users demand secure communication and the eavesdropper is passive. Although the previous researches have designed the physical-layer security schemes under perfect channel state information, this study focuses on investigating the robust transmission design in the presence of a passive eavesdropper. Our goal is to maximize the artificial noise power to confuse the passive eavesdropper and subject to the worst-case signal-to-interference-noise-ratio constraints for all users under a bounded spherical region for the norm of the channel state information error vector from the relays to the destinations and the individual power constraints of all relay nodes. Mathematically, the original robust problem is difficult to solve due to its non-linearity and non-convexity. We propose to adopt S-Procedure and rank relaxation techniques to convert it to a semidefinite programming convex problem. The numerical results show the advantage of the proposed robust method.

Keywords
Physical-layer security, multi-user peer-to-peer, robust relay beamforming

Date received: 19 May 2021; accepted: 21 May 2022
Handling Editor: Yanjiao Chen

Introduction
In order to improve the spectrum efficiency of cooperative communication, a multi-user peer-to-peer (MUP2P) relay network is proposed by Rankov and Wittneben.1 Multiple source destination pairs communicate in pairs through multiple relay nodes in the MUP2P relay network. In recent years, MUP2P relay networks have attracted more and more attention.2−4 However, the most existing researches on multi-source and multi-destination relay networks do not consider wiretap channels. Due to the broadcast nature of the MUP2P networks, private information sent by sources is more vulnerable to be eavesdropped. It is necessary to involve the security in the MUP2P networks, and the security problem in the MUP2P networks has been gradually recognized.

Physical-layer security (PLS) technology, which utilizes inherent security of wireless channels to transmit private information, can effectively improve the security performance in the wireless communication. PLS begins with Wyner’s research on wiretapping model. The achievable security rate is defined as the secret transmission rate of information from source to destination.
The maximum secrecy rate is called as security capacity. In recent years, the researches of PLS have gradually expanded to multi-users, and a large number of PLS schemes and methods have been proposed.

Recently, the PLS has been investigated for MUP2P relay networks. Wang et al. studied the PLS of MUP2P relay networks with a secure user and other unencrypted users. Gong et al. mainly studied the robust relay beamforming of MUP2P relay networks with only one secure user. Cheraghi and Darmani adopted a null space beamforming way to solve the PLS problem for an MUP2P bidirectional relay network with only a pair of secure users. We notice that only one source node sends a secrecy message to its intended destination, the eavesdropper is assumed to be active, and other unclassified users send the message without confidentiality requirements by Wang et al., Gong et al., and Cheraghi and Darmani. However, the other unclassified users may also have secrecy requirement, and the eavesdroppers are often passive in practice.

Although Gong et al. studies a more general case where multiple sources transmit confidential information to their intended destinations, the eavesdropper’s channel state information (CSI) is assumed to be known by the sender and the legitimate links’ CSI is perfect. In actual eavesdropping cases, the eavesdropper may be always passive. Sometimes, we do not even know that whether there are eavesdroppers. In the absence of eavesdropper’s CSI, we cannot optimize the secrecy capacity directly. Using artificial noise (AN) to improve the secrecy capacity of wireless communication has been received much attention in the field of PLS transmission. Goel and Negi and Khisti adopted the AN way to improve PLS in the presence of a passive eavesdropper. The transmitter generates AN using part of available power, and only the eavesdropper is degraded by AN to ensure the secrecy communication at physical layer in the AN way. AN has also been used to improve the security transmission performance for relay communications networks with single source and single destination.

In this article, we consider that all source nodes send secret messages to their intended destinations through multiple relays, while the eavesdropper is passive. All nodes are equipped with single antenna, and all relays adopt the AF protocol. First, considering perfect CSI, we maximize the transmit power of AN to interfere with the passive eavesdropper. At the same time, we consider that the receiving signal-to-interference-plus-noise ratio (SINR) constraints of all the intended destinations and individual power constraints of each relay node are subject. Second, considering imperfect CSI, we propose the robust beamforming design that maximizes the transmit power of AN under the condition of the worst-case received SINR requirement and individual power constraints at relays, which is more practical. Mathematically, the robust beamforming design is non-convex, so the solution is difficult. We propose to adopt S-Procedure and rank relaxation techniques to transform the non-convex problem into a convex problem to solve. The security performance of the proposed robust beamforming design is evaluated by simulations.

Overall, our contributions can be summarized as follows:

1. Mostly researches mainly focus on the security transmission schemes for relay networks with single source and single destination node, but this research considers the more general scenario for multi-sources and multi-destinations, and the eavesdropper is assumed to be passive.
2. The robust beamforming design is proposed for imperfect CSI, which then maximizes the transmit power of AN under the worst-case received SINR constraints and the individual relay power constraints.
3. Although the robust beamforming design for PLS transmission is non-convex, S-Procedure and rank relaxation techniques are adopted to get an efficient solution in this article.

The remainder of this article is organized as follows. In section “System model,” the system model is introduced. In section “Relay beamforming designs,” the relay beamforming schemes for security are given. In section “Simulations,” the simulation results are showed. We conclude the article in section “Conclusion.”

The notation is adopted as follows: Boldface lower (upper) case letters represent vectors (matrices); $\mathbb{C}^{m \times n}$ and $\mathbb{R}^{m \times n}$ stand for spaces of $m \times n$ complex and real matrices, respectively; $(\cdot)^T$, $(\cdot)^*$, and $(\cdot)^H$ indicate transpose, conjugate, and conjugate transpose, respectively; $\text{tr}(\cdot)$ and $E(\cdot)$ denote the trace operator and the expectation operator; $A \succ 0$ means that $A$ is positive definite; and $\log(\cdot)$ denotes the base-2 logarithm.

System model

Assume that there are $N$ source nodes, $N$ destination nodes and $L$ relay nodes in an MUP2P communication network. Multiple source-destination pairs communicate in a pairwise manner through multiple relay nodes in the MUP2P communication network. A passive eavesdropper tries to eavesdrop the messages from all the source nodes. All nodes are equipped with single antenna. We assume that the destination nodes can only receive the signals from relays due to the large path loss and strong shadow fading from source nodes.
to destination nodes (Figure 1). Each relay node only multiplies its received signal by a complex weight and retransmits it to the destination nodes. The distributed relay nodes do not solve the beamforming problem cooperatively. In this relay network, the destination nodes take the responsibility to solve the optimization problem.

The model in Figure 1 is also a two-hop relay network. In phase I, the source transmits the information to the relays, so the receiving signals of all relays, $x_r = (x_{r,1}, \ldots, x_{r,L})^T$, can be given by

$$x_r = H_s \sqrt{P_s} + n_r$$

where $s = (s_1, \ldots, s_N)^T$ is the data symbol that is transmitted by $N$ source nodes and normalized to 1. $P$ is the transmission power of each source node. $H_s = (h_{s,1}, \ldots, h_{s,N}) \in \mathbb{C}^{L \times N}$ is the CSI matrix from all sources to all relays, and its elements are i.i.d. complex Gaussian variables. $n_r \in \mathbb{C}^{L \times 1}$ is noise vector, and its elements are i.i.d. complex Gaussian with zero mean and variances $\sigma_r^2$.

In phase II, an eavesdropper tries to attack the signals from all relays. The eavesdropper is assumed to be passive, so its CSI cannot be obtained. So that the secrecy rate also cannot be optimized to get the security transmission. AN method can be used to realize PLS transmission. The decode ability of the passive eavesdropper can be tried to degrade in this scheme. The signal $y_r = (y_{r,1}, \ldots, y_{r,L})^T$ transmitted by the relays is given by

$$y_r = W x_r + n_{an}$$

where $W = \text{diag}(w_{1r}, \ldots, w_{Lr})$ is relay weights matrix in which $w_l$ is the $l$th AF relay’s weight, $\text{diag}(\cdot)$ denotes diagonal matrix, $n_{an} \in \mathbb{C}^{L \times 1}$ is the AN and the power $P_{an} = E(n_{an}^H n_{an})$ is allocated. The signal transmit power at the $l$th relay is restricted by $E(|y_{rl}|^2) \leq P_l$, $l = 1, \ldots, L$.

The total transmit power of all relays carrying information signals is expressed as

$$P_s = w^H (\mathbb{R} w + \sigma_r^2 \mathbb{1}_L) w$$

where $\mathbb{R}_l = \text{diag}(\sum_{j=1}^N |h_{ij,1}|^2, \ldots, \sum_{j=1}^N |h_{ij,L}|^2)$, $w = (w_1, \ldots, w_L)^T$.

The signal received by the $n$th destination node is given by

$$y_n = h_{dn}^T W h_{rn} \sqrt{P_{sn}} + \sum_{i \neq n} h_{dn}^T W h_{ri} \sqrt{P_{si}} + h_{dn}^T n_{an} + h_{dn}^T W n_r + n_{dn}$$

where $h_{dn}$ is CSI from the all relay nodes to the $n$th destination node, and its elements are i.i.d. complex Gaussian variables. $n_{dn} \in \mathbb{C}$ is noise vector, and its elements are i.i.d. complex Gaussian noise with zero mean and variance $\sigma_d^2$.

The SINR of the $n$th legitimate user can be expressed as

$$\Gamma_n = \frac{P_{w} w_{r,n}^H w_{r,n}^H w}{\sigma_d^2 + \sigma_r^2 P_{an} w_{r,n}^H w_{r,n}^H + \sum_{i \neq n} P_{w} w_{r,n}^H W_{r,n}^H w_{r,n}^H}$$

where $w_{r,n} = h_{dn} \odot h_{rn}$, $\odot$ denotes Hadamard product of two matrices. $R_{dn} = \text{diag}(|h_{dn,1}|^2, \ldots, |h_{dn,L}|^2)$.

The passive eavesdropper’s SINR is given by

$$\Gamma_{e,n} = \frac{P_{w} w_{e,n}^H w_{e,n}^H w}{\sigma_e^2 + \sigma_r^2 P_{an} w_{e,n}^H w_{e,n}^H + \sum_{i \neq n} P_{w} w_{e,n}^H W_{e,n}^H w_{e,n}^H}$$

where $w_{e,n} = h_{dn} \odot h_{rn}$, $R_{dn} = \text{diag}(|h_{dn,1}|^2, \ldots, |h_{dn,L}|^2)$.

The achievable secrecy rate for the $n$th legitimate destination node is given by

$$C_n = \max \left\{ \frac{1}{2} \{ \log(1 + \Gamma_n) - \log(1 + \Gamma_{e,n}) \}, 0 \right\}$$

Figure 1. System model.
Although CSI of the eavesdropper is unknown, the security transmission may be achieved by jamming the passive eavesdropper as large as possible. The transmit power of the AN is maximized to interfere with the passive eavesdropper, while satisfying the SINR constraints of the destination nodes and single relay power constraints. Under the same constraints, the optimization problem can be transformed into minimizing the total relay transmit power of the information-bearing signals. The transformed optimization problem is as follows:

$$\min_w w^H T w$$

s.t. $\Gamma_n \geq \lambda$, $1 \leq n \leq N$

$$[ww^H]_{l,l} \leq P_l, l = 1, \ldots, L$$

(9)

where $T = PR_s + \sigma_r^2 I_L$, $\lambda > 0$ is the required SINR threshold.

### Relay beamforming designs

#### Relay beamforming design with perfect CSI

If the number of relay nodes is less than the number of destination nodes, that is, $N < L$, then AN can lie in the null space of $h_{d_n}$, $n = 1, \ldots, N$, that is, $h_{d_n}^H n_{an} = 0$, $\forall n$. Assuming that $\Pi$ is orthonormal basis of the null space of $h_{d_n}^H$, $\forall n$, then $\Pi^H \Pi = \mathbf{I}$ and $n_{an} = \Pi v$, where $v$ is i.i.d. Gaussian variables. The receiving SINR of the $n$th legitimate destination node is rewritten as

$$\Gamma_n = \frac{P w^H r_{n,n} r_{n,n}^H w}{\sigma_d^2 + \sigma_r^2 w^H R_{d_w} w + \sum_{i \neq n} P w^H r_{n,i} r_{n,i}^H w}$$

(10)

The optimization problem equation (9) is converted to

$$\min_w w^H T w$$

s.t. $\Gamma_n \geq \lambda$, $1 \leq n \leq N$

$$[ww^H]_{l,l} \leq P_l, l = 1, \ldots, L$$

(11)

We can use the way of Wang et al.16 to convert the problem in equation (11) to a second-order cone program (SOCP) problem. The SOCP problem is convex and can be solved by interior methods. But if the number of users is greater than the number of relays, then AN cannot lie in the null space of $h_{d_n}$, $n = 1, \ldots, N$. Obviously, AN can also degrade to the legitimate destination node’s receiving SINR.

#### Relay beamforming design with imperfect CSI

In this section, the study focuses on the robust relay beamforming design with imperfect CSI from relays to destinations. We assume that the CSI from sources to relays can be nearly obtained perfectly due to the high training SINRs. However, CSI from relays to destinations is known imperfectly. We model CSI uncertainty as

$$h_{d_n} = \tilde{h}_{d_n} + e_{d_n}, \forall n$$

(12)

where $e_{d_n}$ is the additive error vector. If the partial knowledge of $e_{d_n}$ can be known by the transmitter, we can adjust the transmit power proportion of the information-bearing signals and AN to achieve the received SINR target at the destinations. We consider a norm-bounded CSI error model as follows:

$$S = \{e_{d_n} \in \mathbb{C}^L \times 1: \|e_{d_n}\|_2^2 \leq \rho P_n^2, \rho > 0, \forall n\}$$

(13)

Then the SINR for the $n$th destination node is given by

$$\Gamma_n = \frac{P \sum_{i=1}^L (\tilde{h}_{d_n,i} + e_{d_n,i}) h_{s_n,i} w_i}{\sigma_d^2 + \rho \sum_{i=1}^L (\tilde{h}_{d_n,i} + e_{d_n,i}) h_{s_n,i} w_i} + P \sum_{i \neq n} \frac{P \sum_{j=1}^L (\tilde{h}_{d_n,j} + e_{d_n,j}) h_{s_n,j} w_j}{\sigma_r^2 \sum_{i \neq n} P \sum_{j=1}^L (\tilde{h}_{d_n,j} + e_{d_n,j}) h_{s_n,j} w_j}$$

(14)

For imperfect CSI, we consider the robust relay beamforming problem equation (15) under the worst-case receiving SINR constraints of the legitimate destination nodes.

$$\min_w w^H T w$$

s.t. $\min_{e_{d_n}} \Gamma_n \geq \lambda$, $1 \leq n \leq N$

$$[ww^H]_{l,l} \leq P_l, l = 1, \ldots, L$$

(15)

The minimum problem equation (15) is very not easy to solve, because the first constraint is mathematically intractable.

#### An upper bound of equation (15)

We can obtain the inequalities equations (16) and (17) by utilizing the Cusky–Schwarz inequality and the triangle inequality.
We get an upper bound of the problem equation (15) by solving the following beamforming design equation (19).

\[
\begin{align*}
\min_{w} & \quad w^H Tw \\
\text{s.t.} & \quad \Gamma_{nl}^l \geq \lambda, \ 1 \leq n \leq N, \\
|w|^H [I]_{n,I} & \leq P_l, l = 1, \ldots, L
\end{align*}
\]  

(19)

Similarly, Wang et al.'s\(^{16}\) method is also used to convert the beamforming problem equation (19) to an SOCP problem.

**Robust relay beamforming design.** We can obtain the inequality equation (20) by using \(|e_{dl}|^2 \leq \lambda P^2\).

\[
\Gamma_{nl} \geq \Gamma_{low}
\]

(20)

where \(\Gamma_{low} = \frac{\rho}{\sigma_d^2 + \sigma_r^2 \sum_{j=1}^{L} \left|\hat{h}_{d,j} + e_{d,j}\right|^2 }\).

The beamforming problem equation (15) is rewritten by

\[
\begin{align}
\min_{w} & \quad w^H Tw \\
\text{s.t.} & \quad \Gamma_{nl} \geq \lambda, \ 1 \leq n \leq N, \\
|w|^H [I]_{n,I} & \leq P_l, l = 1, \ldots, L
\end{align}
\]

(21)

The first constraint in equation (21) can be rewritten as equation (22).

\[
(\hat{h}_d + e_d)^H Q (\hat{h}_d + e_d) \geq u, \forall |e_d| \leq \lambda P^2
\]

(22)

where \(Q = P R_e w w^H - \lambda \sigma_d^2 w w^H - \sum_{i \neq n} P R_i w w^H, u = \lambda \sigma_d^2, w w^H + n \lambda P^2 \left(\sum_{i=1}^{L} P_i - w w^H T w\right), R_e = \text{diag}(|h_{n,1}|^2, \ldots, |h_{n,L}|^2)\).

Then we can rewrite the first constraint of the problem equation (21) as equation (23) by using S-Procedure.\(^{18}\)

\[
F_n(Q, \beta, u) \triangleq \left(\beta I_n + Q h_{dl}^n, h_{dl}^n Q h_{dl}^n - u\right) \geq 0
\]

(23)

The beamforming problem equation (21) is rewritten as equation (24) by using \(W = w w^H\) and \(tr(AB) = tr(BA)\).

\[
\begin{align}
\min_{w \leq 0, \beta \geq 0} & \quad tr(Tw) \\
\text{s.t.} & \quad F_n(Q, \beta, u) \geq 0, \forall n, \\
|w|^H [I]_{n,I} & \leq P_l, \forall l \\
\text{rank}(W) & = 1
\end{align}
\]

(24)

The rank constraint \(\text{rank}(W) = 1\) is non-convex in equation (24). We consider to drop it as equation (25).

\[
\begin{align}
\min_{w \leq 0, \beta \geq 0} & \quad tr(Tw) \\
\text{s.t.} & \quad F_n(Q, \beta, u) \geq 0, \forall n, \\
|w|^H [I]_{n,I} & \leq P_l, \forall l
\end{align}
\]

(25)

The robust beamforming problem equation (25) can be optimally solved by adopting interior methods due to that it is a semi-definite programming (SDP) problem. The problem in equation (25) has \(N + L\) constraints and the dimension of \(W\) is \(L \times L\), so the computational complexity is at least \((N + L)^4 L^{1/2} \log 1/\varepsilon\),\(^{18}\) where \(\varepsilon\) is solution accuracy.
Assuming that the solution to the robust beamforming problem equation (25) is $W$. If the solution $W$ is rank 1, then the globally optimal solution $w_{\text{opt}}$ can be obtained by using standard matrix decomposition. If the solution $W$ is not rank 1, we can use a randomization method\(^\text{19}\) in Table 1 to convert $W$ into a feasible solution $w$. If the feasible solution $w$ does not satisfy some constraints of the beamforming design equation (21), $w$ can be mapped into a “nearby” feasible solution.

### Simulations

In this section, simulations are offered to analyze the performance of the proposed relay beamforming design for the PLS transmission. In each simulation run, we randomly generate CSI using complex zero-mean Gaussian random vectors with unit covariance, and all the noise power is same. Assuming that CSI errors are uniformly distributed and equal. We assume that the individual power constraints are equal. About 1000 independent simulations are carried out, and the average results are obtained. There are four schemes: (1) relay beamforming design with perfect CSI in section “Relay beamforming design with perfect CSI”; (2) the upper bound in section “An upper bound of equation (15)” with imperfect CSI; (3) the robust beamforming design with imperfect CSI in section “Robust relay beamforming design”; and (4) the naive scheme in which the estimated CSI is regarded as ideal CSI without utilizing the knowledge of CSI error.

Figure 2 shows the transmit power for information-bearing signals under different number of relays. We set $N = 2$, $\rho^2 = 0.01$, respectively. The results show that the robust beamforming scheme proposed by the section “Robust relay beamforming design” is superior to the upper bound in the section “An upper bound of equation (15).” We can notice that the relay transmission power decreases with the number of relays increasing. We can also notice that although the performance of the proposed beamforming methods is improved, the solution complexity of the beamforming problem for secrecy will also be increased. Therefore, there is a tradeoff between the system performance and computational complexity.

Figure 3 plots the minimum secrecy rate for destination nodes with different number of relay nodes. The simulation sets $N = 2$, $\rho^2 = 0.01$, and different SINR constraints $\lambda = 1$, $2$, respectively. We notice that the highest secrecy rate can be achieved if the perfect CSI is known. Because relay weights can be designed to make the AN not be received by the desired destination nodes when perfect CSI is known, and the potential eavesdropper is degraded by the AN. The robust relay beamforming design in section “Robust relay beamforming design”.

### Table 1. Randomization method for semidefinite relaxation.

1. Apply the eigenvalue decomposition $W = U \Sigma U^H$.
2. Choose an random vector $v \in \mathbb{C}^{L \times 1}$, where $|v_i| = e^{i\theta}$, $i = 1, \ldots, L$ is achieved, and $\theta_i$ is independent and uniformly distributed on $[0, 2\pi)$.
3. Choose $w = U \Sigma^{1/2} v$ which ensures that $w^H w = \text{tr}(W)$.

**Figure 2.** Transmit power for information-bearing signals with the different number of relays.

**Figure 3.** Minimum secrecy rate with the different number of relay nodes.
beamforming design” can achieve nonzero secrecy rate. But in naive scheme, the secrecy rate is reduced to zero because of the AN also jams the legitimate users resulting to the received SINR at the destinations decreasing. So we can know that a small part of the secrecy rate lost is recovered by using the robust relay beamforming design. It can be noted that the secrecy performance increases when the SINR constraint is small. Because the relay transmission power for information-bearing signal is reduced, which will lead to the increase of the residual power for AN. We also found that with the increase of the number of relays, the secrecy rate also increases, due to that the freedom degrees can be further adopted to increase the transmit diversity. Similarly, there is also a tradeoff between the system performance and computational complexity.

Figure 4 investigates the minimum secrecy under different individual transmit power constraints at relays. We set $\rho^2 = 0.01$, $N = 2$, and SINR constraints $\lambda = 1$, respectively. We observe that the robust beamforming design provides nonzero secrecy rate under all different relay transmitting power constraints. We also notice that the secrecy rate is the highest if CSI is perfectly known. We also note that the secrecy rate is degraded to zero in the naive scheme because channel state of the eavesdropper is better than that of the users.

In Figure 5, we study the minimum secrecy rate with different CSI error bounds. We set $\rho^2 = 0.01$, $N = 2$, and $\lambda = 1, 2$. It is observed that the secrecy rate is higher if CSI error bound is reduced in the robust beamforming design for the PLS. It is obvious that the robust beamforming design in section “Robust relay beamforming design” can obtain the desired secrecy rate. But in the naive scheme, the secrecy rate can be greatly reduced to zero. Thus, the robust relay beamforming design outperforms the naive scheme in the secrecy performance.

Figure 4. The minimum secrecy rate with different individual power constraints.

Figure 5. The minimum secrecy rate with different CSI error bounds.

Conclusion

In this article, the PLS transmission design is presented for MUP2P relay networks, where all source nodes transmit secrecy messages to their intended destinations through multiple relay nodes, and there is a passive eavesdropper in the networks. Focusing on researching the scenario in which the CSI is known imperfectly. We model the CSI error as a bounded spherical region. The robust relay beamforming scheme maximizes the transmitting power of AN to interfere with the eavesdropper and satisfies the worst-case received SINR constraints at all destinations and individual relay power constraints. Although the robust beamforming problem is non-convex, it can be transformed into a convex problem to solve by adopting S-Procedure and rank relaxation techniques. In order to show the performance gains of the robust relay beamforming design, the naive scheme is provided to compare the secrecy performance. The simulation results demonstrates the proposed robust beamforming design improves the PLS performance of the MUP2P networks due to that the CSI errors knowledge is adopted.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work is supported in part by the China Postdoctoral Science Foundation (grant no. 2020M673687), in part by the National Natural Science Foundation of China (grant no. 61971474), in part by the Beijing Nova Program (grant no. ZZ01100006820121), and in part by the Postdoctoral Science Foundation–funded project of China (grant no. 2019T120071).
References

1. Rankov B and Wittneben A. Spectral efficient protocols for half-duplex fading relay channels. *IEEE J Select Area Commun* 2007; 25(2): 379–389.
2. Li W and Dong M. Distributed Alamouti relay beamforming scheme in multiuser relay networks. *IEEE Signal Process Lett* 2017; 24(10): 1527–1531.
3. Zappone A, Atapattu S, Di Renzo M, et al. Energy-efficient relay assignment and power control in multi-user and multi-relay networks. *IEEE Wirel Commun Lett* 2018; 7(6): 1070–1073.
4. Senanayake R, Atapattu S, Evans JS, et al. Decentralized relay selection in multi-user multihop decode-and-forward relay networks. *IEEE Trans Wirel Commun* 2018; 17(5): 3313–3326.
5. Xiao L, Sheng G, Liu S, et al. Deep reinforcement learning-enabled secure visible light communication against eavesdropping. *IEEE Trans Commun* 2019; 67(10): 6994–7005.
6. Su N, Panayirci E, Koca M, et al. Spatial constellation design-based generalized space shift keying for physical layer security of multi-user MIMO communication systems. *IEEE Wirel Commun Lett* 2021; 10(8): 1785–1789.
7. Park SH and Jin X. Joint secure design of downlink and D2D cooperation strategies for multi-user systems. *IEEE Signal Process Lett* 2021; 28: 917–921.
8. Obeed M and Mesbah W. Efficient algorithms for physical layer security in one-way relay systems. *Wirel Netw* 2019; 25(8): 1327–1339.
9. Abdullah Z, Chen G and Chambers JA. A cooperative jamming scheme for physical layer security enhancement in multihop IoT networks with colluding eavesdroppers. In: *Proceedings of the 2021 IEEE statistical signal processing workshop*, Rio de Janeiro, Brazil, 11–14 July 2021, pp.506–510. New York: IEEE.
10. Wang C, Wang HM, Ng DWK, et al. Joint beamforming and power allocation for secrecy in peer-to-peer relay networks. *IEEE Trans Wirel Commun* 2015; 14(6): 3280–3293.
11. Gong X, Yin H, Dong F, et al. Robust beamforming design for secrecy in multiuser peer-to-peer wireless relay networks. *IEEE Syst J* 2018; 12(1): 682–690.
12. Cheraghi M and Darmani Y. Total transmit power minimization with physical layer security in multiuser peer-to-peer two-way relay networks. *Int J Electron Commun* 2020; 124: 153317.
13. Gong X, Long H, Dong F, et al. Secure communication design for multi-user peer-to-peer wireless relay networks. *IET Commun* 2016; 10(7): 770–777.
14. Goel S and Negi R. Guaranteeing secrecy using artificial noise. *IEEE Trans Wirel Commun* 2008; 7(6): 2180–2189.
15. Khisti A. Algorithms and architectures for multiuser, multi-terminal, and multilayer information-theoretic security. PhD Dissertation, Massachusetts Institute of Technology (MIT), Cambridge, MA, 2008.
16. Wang HM, Luo M, Xia XG, et al. Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper’s CSI. *IEEE Signal Process Lett* 2013; 20(1): 39–42.
17. Li Q and Yang L. Beamforming for cooperative secure transmission in cognitive two-way relay networks. *IEEE Trans Inform Foren Sec* 2019; 15(1): 130–143.
18. Boyd S and Vandenberghe L. *Convex optimization*. Cambridge, MA: Cambridge University Press, 2004.
19. Luo ZQ, Ma WK, So AMC, et al. Semidefinite relaxation of quadratic optimization problems: from its practical deployments and scope of applicability to key theoretical results. *IEEE Signal Process Mag* 2020; 27(3): 20–34.