SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

June 2016, Vol. 59 062304:1–062304:14
doi: 10.1007/s11432-015-5401-z

Cooperative beamforming design for physical-layer security of multi-hop MIMO communications

Shiqi GONG, Chengwen XING*, Zesong FEI & Jingming KUANG

School of Information and Electronics, Beijing Institute of Technology, Beijing 100081*, China*

Received May 26, 2015; accepted June 30, 2015; published online September 7, 2015

Abstract The security issue is critically important for wireless communications, especially for multi-hop communications. In this paper, we propose a cooperative secrecy beamforming scheme for a multi-hop MIMO communication network, in which there is a single-antenna source, multiple multi-antenna relays and a single-antenna destination. Moreover, two types of eavesdroppers exist in the network, one of which has known channel state information (CSI), while the other not. To achieve security communications, in our work null-space beamforming and artificial noise beamforming are jointly optimized to improve the secrecy rate of the multi-hop network. In nature, the joint optimization is nonconvex and challenging. Exploiting its structure, the considered optimization problem is decoupled into a series of subproblems that can be efficiently solved based on convex optimization theory. Finally, some numerical experiment results are provided to assess the performance of the proposed secrecy beamforming design.

Keywords MIMO, physical layer security, multi-hop network, null-space beamforming, artificial noise

Citation Gong S Q, Xing C W, Fei Z S, et al. Cooperative beamforming design for physical-layer security of multi-hop MIMO communications. Sci China Inf Sci, 2016, 59(6): 062304, doi: 10.1007/s11432-015-5401-z

1 Introduction

Multi-hop relaying is an effective technique to realize reliable and efficient communications in a flexible network topology such as military vehicle to vehicle communications and ad-hoc networks [1–3]. In order to achieve high frequency efficiency and system capacity of wireless networks, the multiple-input multiple-output (MIMO) technology is widely accepted as an effective way to exploit spatial freedom. With this technology, multiple antennas are deployed at transmitters and receivers to transmit multiple data streams simultaneously [4]. Furthermore, considering the openness of wireless links and the multiple signals transmitted by multiple antennas, almost all receivers located in the communication range of a transmitter are able to obtain quite an amount of information about the transmitted signals, which may lead to the confidential or private information leakage. Overall, wireless communications are susceptible to security threatening [5, 6]. Hence, in order to realize the high information transmission rate as much as possible without being wiretapped by any eavesdropper of current wireless networks, the design of security transmission strategy for multi-hop MIMO communications is important and meaningful [7].

* Corresponding author (email: chengwenxing@ieee.org)

There are also plenty of research publications about the optimal transmission strategy for the multi-hop network [8–10]. For example, Ref. [8] proposed a low-complexity beamforming scheme for multi-hop networks using aggregate information about the neighborhood of each node. In [9], a three-hop channel model is constructed and then a collaborative beamforming design utilizing the subspace average concept is conducted. Similar to [9], the [10] also designed a collaborative beamforming scheme for three-hop multi-relay network. Nevertheless, it is different from [9] in the sense that this scheme optimizes the two relay beamformings alternatively under different optimization objectives. However, it is obvious that all these studies do not consider the information security issues in multi-hop network.

On the other hand, there also exists abundant literature work considering the security communication for wireless network. From signal processing perspective, it is well-known that physical layer security technology has become a promising technology to realize the security communication in the future communication systems. The fundamental information theory for physical layer security was firstly introduced by Shannon [11]. Then Wyner investigated the famous wiretap channel model in [12] from the point of view of the information theory, in which the channel secrecy capacity is defined as the maximum achievable rate between transmitter and receiver when the eavesdropper is completely unknown about the transmitted signal. Following [11], a more general wiretap channel model is proposed in [13] and it is demonstrated that the security communication can be realized by utilizing the physical security techniques only instead of secret key encryption. Furthermore, Ref. [14] proposed a widely used Gaussian degraded wiretap channel.

After these pioneering theoretical studies, a lot of related literature focusing on the design of security transmission strategy has been published [15–22]. These studies mainly concentrate on the various multiple-antenna systems because of the flexible spatial degrees of freedom provided by multiple antennas. Generally, there are various types of multi-antenna networks, e.g., multiple-input single-output (MISO) networks [15, 16], single-input multiple-output (SIMO) networks [17] and MIMO networks [18–22]. For example, in [15] the optimal secrecy beamforming is designed for MISO system and the Pareto boundary is obtained. In [17], a security transmission scheme utilizing the encryption technique at source is proposed for SIMO network, which is based on the random message transmitted by destination. As for the more complicated security communication issue, a collaborative physical-layer security transmission scheme based on the game theory is proposed for MIMO network in [18]. This scheme can effectively balance the security performance among different links. Besides, in [20], a distributed secrecy beamforming scheme for two-way relay channel (TWRC) is proposed, which contains both the null-space beamforming and the artificial noise beamforming. Further, considering introducing jammer to the TWRC to decrease the wiretap information rate in MAC phase, a novel cooperative beamforming and jamming scheme is proposed in [21].

To the best of the authors' knowledge, most of the existing studies focus on physical layer security of single-hop or dual-hop communications as above. It is worth noting that multi-hop communications are more general and also important for practical communication systems such as device-to-device communications and vehicle-to-vehicle communications. In this paper, we take a further step to investigate beamforming designs for physical layer security of multi-hop MIMO communications. In particular, two different types of eavesdroppers are considered, one of which has perfect CSI, while the other not. Then both null-space beamforming and artificial noise are adopted to improve the system security. Specifically, for a K-hop network with total $K-1$ relays, it is observed that once any $K-2$ relay beamformings are determined, the original optimization problem can be transformed into a generalized Rayleigh quotient problem or a quasi-convex problem, which both can be effectively solved by the existing methods. In a word, by formulating the original optimization problem into $K-1$ independent subproblems and solving them iteratively, the security transmission can finally be achieved.

The rest of this paper is organized as follows. The system model and problem formulated are firstly given in Section 2. In Section 3, to realize security communication, the proposed collaborative beamforming design is presented. The simulation results are shown in Section 4 and the conclusions are drawn in Section 5.

Notation: The light-faced lowercase letters denote scalars, such as a. The bold-faced lowercase letters

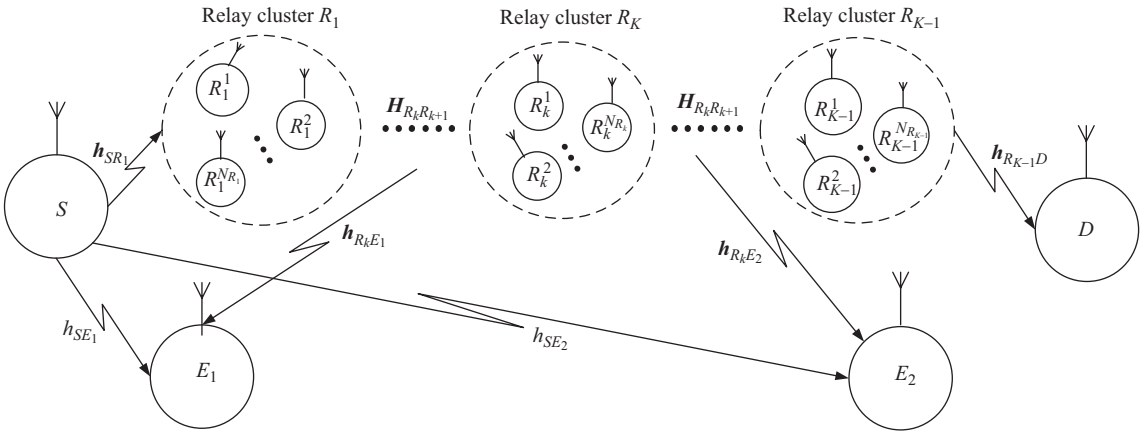

Figure 1 A K-hop cooperative communication network with two eavesdroppers.

denote vectors, such as $\boldsymbol{a}$. Matrices are denoted by the bold-faced uppercase letters, e.g., $\boldsymbol{A}$. For matrices, the expression $\boldsymbol{A}^{-1}$, $\boldsymbol{A}^{\mathrm{T}}$, $\boldsymbol{A}^{\mathrm{H}}$, $\boldsymbol{A}^{*}$ denote the inverse, transpose, Hermitian (conjugate transpose), conjugate of $\boldsymbol{A}$, respectively. The symbol $\mathrm{Tr}(\boldsymbol{A})$ denotes the trace of $\boldsymbol{A}$ and $\mathrm{rank}(\boldsymbol{A})$ is the rank of $\boldsymbol{A}$. Besides, $\boldsymbol{A}[k,m]$ denotes the kth row and mth column element of matrix $\boldsymbol{A}$ and the symbol $\boldsymbol{A}^{(n)}$ is the n-th row of matrix $\boldsymbol{A}$. $\boldsymbol{A} \succeq 0$ means that $\mathbf{A}$ is a positive semidefinite matrix. $|a|$ means the absolute value of scalar a and $\|\boldsymbol{a}\|$ denotes the Euclidean norm of vector $\boldsymbol{a}$. $\mathcal{CN}(0,1)$ represents the zero-mean and unit variance Complex Gaussian random variable.

2 System model

In this paper, we focus our attention on a multi-hop cooperative network, in which as shown in Figure 1, a single antenna source node S communicates with a single antenna destination node D via multiple multi-antenna relay nodes $R_k, k = 1, \ldots, K-1$. Without loss of generality, the kth relay R_k is assumed to be equipped with N_{R_k} antennas. In addition, there are two potential single-antenna eavesdroppers E_1 and E_2. To model a more practical and general scenario, in our considered system only one eavesdropper E_1 has the perfect channel state information (CSI). In other words, E_1 is a legitimate but not the intended receiver. Whereas, the CSI of the other eavesdropper E_2 is completely unknown. The channel matrices from S to R_1, R_k to $R_{k+1}, \forall k = 1, \ldots, K-2$ and R_{K-1} to D are denoted by $\boldsymbol{h}_{SR_1} \in \mathbb{C}^{N_{R_1} \times 1}$, $\boldsymbol{H}_{R_kR_{k+1}} \in \mathbb{C}^{N_{R_{k+1}} \times N_{R_k}}$ and $\boldsymbol{h}_{R_{K-1}D} \in \mathbb{C}^{1 \times N_{R_{K-1}}}$, respectively. Moreover, the channels from source S to E_1 and E_2 are denoted by h_{SE_1} and h_{SE_2}, respectively. Similarly, $\boldsymbol{h}_{R_kE_1}$ and $\boldsymbol{h}_{R_kE_2}$ are channels from relay R_k to E_1 and E_2, respectively.

At each relay, the received signals is multiplied by a forwarding matrix $\boldsymbol{W}_{R_k}$ and then forwarded to the next hop, where $\boldsymbol{W}_{R_k} = \mathrm{diag}([\boldsymbol{\omega}_{k,1}^*, \boldsymbol{\omega}_{k,2}^*, \ldots, \boldsymbol{\omega}_{k,N_{R_k}}^*])$. As the CSI of eavesdropper E_2 is unavailable, artificial noise $\boldsymbol{n}_a$ is further transmitted to improve the security. As signals are forwarded hop by hop, for simplicity we only need the first relay R_1 to transmit artificial noise $\boldsymbol{n}_a$. As a result, the received signal at the kth relay R_k equals (In this paper, we mainly concentrate on the $K \geqslant 3$ hops system)

$$\begin{aligned}\boldsymbol{y}_{R_k} = &\left(\prod_{m=1}^{k-1} \boldsymbol{H}_{R_mR_{m+1}}\boldsymbol{W}_{R_m}\right)\boldsymbol{h}_{SR_1}\sqrt{P_1}s_1 + \sum_{i=1}^{k-1}\left(\prod_{m=i}^{k-1} \boldsymbol{H}_{R_mR_{m+1}}\boldsymbol{W}_{R_m}\right)\boldsymbol{n}_{R_i} + \boldsymbol{n}_{R_k}\\ &+ \left(\prod_{m=2}^{k-1} \boldsymbol{H}_{R_mR_{m+1}}\boldsymbol{W}_{R_m}\right)\boldsymbol{H}_{R_1R_2}\boldsymbol{n}_a, \end{aligned} \tag{1}$$

where s_1 and P_1 are the transmit signal and power of source S, respectively. $\boldsymbol{n}_{R_i}$ is the received noise at relay R_i. Generally, we often set $\mathrm{E}|s_1|^2 = 1$. It is emphasized that the artificial noise $\boldsymbol{n}_a$ firstly appears at the relay R_2. Further, the received signal at the destination D is

$$y_D^K = \boldsymbol{h}_{R_{K-1}D}\boldsymbol{W}_{R_{K-1}}\boldsymbol{y}_{R_{K-1}} + n_D^K. \tag{2}$$

The symbol n_D^K denotes the received noise at destination D. Then based on the quality $\boldsymbol{a}^{\mathbf{T}}\mathrm{diag}[\boldsymbol{b}] = \boldsymbol{b}^{\mathbf{T}}\mathrm{diag}[\boldsymbol{a}]$ and (1), the received signal at D in (2) can be rewritten as

$$y_D^K = \boldsymbol{\omega}_{R_{K-1}}^{\mathrm{H}} \boldsymbol{F}_{R_{K-1}D} \left(\prod_{m=1}^{k-1} \boldsymbol{H}_{R_m R_{m+1}} \boldsymbol{W}_{R_m} \right) \boldsymbol{h}_{SR_1} \sqrt{P_1} s_1 + \tilde{n}_D^K, \tag{3}$$

where

$$\begin{aligned} \boldsymbol{\omega}_{R_{K-1}} &= \mathrm{diag}(\boldsymbol{W}_{R_{K-1}})^*, \quad \boldsymbol{F}_{R_{K-1}D} = \mathrm{diag}(\boldsymbol{h}_{R_{K-1}D}), \\ \tilde{n}_D^K &= n_D^K + \boldsymbol{\omega}_{R_{K-1}}^{\mathrm{H}} \boldsymbol{F}_{R_{K-1}D} \sum_{i=1}^{K-2} \left(\prod_{m=i}^{K-2} \boldsymbol{H}_{R_m R_{m+1}} \boldsymbol{W}_{R_m} \right) \boldsymbol{n}_{R_i} \\ &\quad + \boldsymbol{\omega}_{R_{K-1}}^{\mathrm{H}} \boldsymbol{F}_{R_{K-1}D} \prod_{m=2}^{K-2} \boldsymbol{H}_{R_m R_{m+1}} \boldsymbol{W}_{R_m} \boldsymbol{H}_{R_1 R_2} \boldsymbol{n}_a + \boldsymbol{\omega}_{R_{K-1}}^{\mathrm{H}} \boldsymbol{F}_{R_{K-1}D} \boldsymbol{n}_{R_{K-1}}. \end{aligned} \tag{4}$$

Further, the wiretapped signals at E_1 and E_2 in the kth phase from the relay R_{k-1} are denoted by $y_{E_u}^{(k)}$ with $u = 1, 2$, respectively.

$$y_{E_u}^{(k)} = \boldsymbol{h}_{R_{k-1}E_u} \boldsymbol{W}_{R_{k-1}} \boldsymbol{y}_{R_{k-1}} + n_{E_u}^{(k)}, \qquad u = 1, 2, \quad k = 2, \ldots, K. \tag{5}$$

Particularly, the first phase wiretapped signal $y_{E_u}^{(1)}$ (from source S) has the following formula

$$y_{E_u}^{(1)} = h_{SE_u} \sqrt{P_1} s_u + n_{E_u}^{(1)}, \qquad u = 1, 2. \tag{6}$$

For above formulations, $n_{E_u}^{(k)}$ denotes the received noise at eavesdropper E_u in the kth phase. To make the derivations more readable, the total wiretapped signal is further reformulated as a compact SIMO signal model

$$\boldsymbol{y}_{E_u} = \boldsymbol{H}_{E_u} \sqrt{P_1} s_1 + \boldsymbol{n}_{E_u}, \quad u = 1, 2, \tag{7}$$

where

$$\boldsymbol{y}_{E_1} = \begin{bmatrix} y_{E_1}^{(1)} \\ y_{E_u}^{(2)} \\ \ldots \\ y_{E_u}^{(n)} \\ \ldots \\ y_{E_u}^{(K)} \end{bmatrix}, \quad \boldsymbol{H}_{E_u} = \begin{bmatrix} h_{SE_u} \\ \boldsymbol{h}_{R_1 E_1} \boldsymbol{W}_{R_1} \boldsymbol{h}_{SR_1} \\ \ldots \\ \boldsymbol{h}_{R_{n-1}E_1} \boldsymbol{W}_{R_{n-1}} \prod_{m=1}^{n-2} \boldsymbol{H}_{R_m R_{m+1}} \boldsymbol{W}_{R_m} \boldsymbol{h}_{SR_1} \\ \ldots \\ \boldsymbol{h}_{R_{K-1}E_1} \boldsymbol{W}_{R_{K-1}} \prod_{m=1}^{K-2} \boldsymbol{H}_{R_m R_{m+1}} \boldsymbol{W}_{R_m} \boldsymbol{h}_{SR_1} \end{bmatrix},$$

$$\boldsymbol{n}_{E_u} = \begin{bmatrix} n_{E_u}^{(1)} \\ \boldsymbol{h}_{R_1 E_1} \boldsymbol{W}_{R_1} \boldsymbol{n}_{R_1} + \boldsymbol{h}_{R_1 E_1} \boldsymbol{n}_a + n_{E_u}^{(2)} \\ \ldots \\ \boldsymbol{h}_{R_{n-1}E_1} \boldsymbol{W}_{R_{n-1}} \sum_{i=1}^{n-2} \left(\prod_{m=i}^{n-2} \boldsymbol{H}_{R_m R_{m+1}} \boldsymbol{W}_{R_m} \right) \boldsymbol{n}_{R_i} + \boldsymbol{h}_{R_{n-1}E_1} \boldsymbol{W}_{R_{n-1}} \prod_{m=2}^{n-2} \boldsymbol{H}_{R_m R_{m+1}} \boldsymbol{W}_{R_m} \boldsymbol{H}_{R_1 R_2} \boldsymbol{n}_a \\ + \boldsymbol{h}_{R_{n-1}E_1} \boldsymbol{W}_{R_{n-1}} \boldsymbol{n}_{R_{n-1}} + n_{E_u}^{(n)} \\ \ldots \\ \boldsymbol{h}_{R_{K-1}E_1} \boldsymbol{W}_{R_{K-1}} \sum_{i=1}^{K-2} \left(\prod_{m=i}^{K-2} \boldsymbol{H}_{R_m R_{m+1}} \boldsymbol{W}_{R_m} \right) \boldsymbol{n}_{R_i} + \boldsymbol{h}_{R_{K-1}E_1} \boldsymbol{W}_{R_{K-1}} \prod_{m=2}^{K-2} \boldsymbol{H}_{R_m R_{m+1}} \boldsymbol{W}_{R_m} \boldsymbol{H}_{R_1 R_2} \boldsymbol{n}_a \\ + \boldsymbol{h}_{R_{K-1}E_1} \boldsymbol{W}_{R_{K-1}} \boldsymbol{n}_{R_{K-1}} + n_{E_u}^{(K)} \end{bmatrix}. \tag{8}$$

As that all elements of the actually received noise terms at each node of K-hop network are Gaussian distributed, the elements of artificial noise $\boldsymbol{n}_a$ are assumed to be distributed as $\mathcal{CN}(0,\sigma_a^2)$ and σ_a^2 is an optimization variable. Further, the covariance matrices θ_D and $\boldsymbol{\theta}_{E_u}$ of the equivalent noise terms $\tilde{n}_D^K$ and $\boldsymbol{n}_{E_u}$ are expressed respectively as

$$\theta_D = \boldsymbol{\omega}_{R_{K-1}}^{\mathrm{H}} \boldsymbol{F}_{R_{K-1}D} \left(\sigma^2 \boldsymbol{I} + \sigma_a^2 \left(\prod_{m=2}^{K-2} \boldsymbol{H}_{R_m R_{m+1}} \boldsymbol{W}_{R_m} \right) \boldsymbol{R}_{H_1 H_2} \left(\prod_{m=2}^{K-2} \boldsymbol{W}_{R_{K-m}}^{\mathrm{H}} \boldsymbol{H}_{R_{K-m} R_{K-m+1}}^{\mathrm{H}} \right) + \sigma^2 \sum_{i=1}^{K-2} \left(\prod_{m=i}^{K-2} \boldsymbol{H}_{R_m R_{m+1}} \boldsymbol{W}_{R_m} \right) \left(\prod_{m=i}^{K-2} \boldsymbol{W}_{R_{K+i-m-2}}^{\mathrm{H}} \boldsymbol{H}_{R_{K+i-m-2} R_{K+i-m-1}}^{\mathrm{H}} \right) \right) \boldsymbol{F}_{R_{K-1}D}^{\mathrm{H}} \boldsymbol{\omega}_{R_{K-1}} + \sigma^2, \quad (9)$$

where $\boldsymbol{R}_{H_1H_2} = \boldsymbol{H}_{H_1H_2} \boldsymbol{H}_{H_1H_2}^{\mathrm{H}}$ and $\boldsymbol{I}$ is an identity matrix with proper dimensions. On the other hand, the elements of the Hermitian matrix $\boldsymbol{\theta}_{E_u}$ are equivalent to (for general situation where $k \geqslant 4$, $l = k+1, k+2, ..., K$)

$$\boldsymbol{\theta}_{E_u}[k,k] = \boldsymbol{\omega}_{R_{k-1}}^{\mathrm{H}} \boldsymbol{F}_{R_{k-1}E_u} \left(\sigma^2 \sum_{i=1}^{k-2} \left(\prod_{m=i}^{k-2} \boldsymbol{H}_{R_m R_{m+1}} \boldsymbol{W}_{R_m} \right) \left(\prod_{m=i}^{k-2} \boldsymbol{W}_{R_{k+i-m-2}}^{\mathrm{H}} \boldsymbol{H}_{R_{k+i-m-2} R_{k+i-m-1}}^{\mathrm{H}} \right) + \sigma^2 \boldsymbol{I} + \sigma_a^2 \left(\prod_{m=2}^{k-2} \boldsymbol{H}_{R_m R_{m+1}} \boldsymbol{W}_{R_m} \right) \boldsymbol{R}_{H_1 H_2} \left(\prod_{m=2}^{k-2} \boldsymbol{W}_{R_{k-m}}^{\mathrm{H}} \boldsymbol{H}_{R_{k-m} R_{k-m+1}}^{\mathrm{H}} \right) \right) \boldsymbol{F}_{R_{k-1}E_u}^{\mathrm{H}} \boldsymbol{\omega}_{R_{k-1}} + \sigma^2, \quad (10)$$

$$\boldsymbol{\theta}_{E_u}[k,l] = \boldsymbol{\omega}_{R_{k-1}}^{\mathrm{H}} \boldsymbol{F}_{R_{k-1}E_u} \left(\sigma^2 \sum_{i=1}^{k-2} \left(\prod_{m=i}^{k-2} \boldsymbol{H}_{R_m R_{m+1}} \boldsymbol{W}_{R_m} \right) \left(\prod_{m=i}^{l-2} \boldsymbol{W}_{R_{l+i-m-2}}^{\mathrm{H}} \boldsymbol{H}_{R_{l+i-m-2} R_{l+i-m-1}}^{\mathrm{H}} \right) + \sigma_a^2 \left(\prod_{m=2}^{k-2} \boldsymbol{H}_{R_m R_{m+1}} \boldsymbol{W}_{R_m} \right) \boldsymbol{R}_{H_1 H_2} \left(\prod_{m=2}^{l-2} \boldsymbol{W}_{R_{l-m}}^{\mathrm{H}} \boldsymbol{H}_{R_{l-m} R_{l-m+1}}^{\mathrm{H}} \right) + \sigma^2 \left(\prod_{m=k-1}^{l-2} \boldsymbol{W}_{R_{k+l-m-3}}^{\mathrm{H}} \boldsymbol{H}_{R_{k+l-m-3} R_{k+l-m-2}}^{\mathrm{H}} \right) \right) \boldsymbol{F}_{R_{l-1}E_u}^{\mathrm{H}} \boldsymbol{\omega}_{R_{l-1}}, \quad (11)$$

where $\boldsymbol{F}_{R_{k-1}E_u} = \mathrm{diag}(\boldsymbol{h}_{R_{k-1}E_u})$, $u = 1, 2$. And particularly, for $k = 1$ we have

$$\boldsymbol{\theta}_{E_u}[1,1] = \sigma^2, \quad \boldsymbol{\theta}_{E_u}[1,l] = 0, \quad l = 2, ..., K, \quad u = 1, 2. \quad (12)$$

As for the other special cases, they all can be calculated easily, which only have the slight difference to (10) and (11).

In order to realize security multi-hop communications, the performance metric namely achievable secrecy rate [23] is adopted as the objective of the optimization of beamforming matrices and artificial noise. It is worth noting that as there is more than one eavesdropper independently intercepting the signal, the overall wiretap rate of the communication network should be the maximum individual rate among the involved multiple eavesdroppers. Hence, the achievable secrecy rate region is finally defined as

$$R \leqslant \left[\sum_{n \in D} I(y_n, s) - \max_{n \in N_e} \left(I(y_{E_n}, s) \right) \right]^+, \quad (13)$$

where D and N_e denote the collection of legitimate receivers and eavesdroppers, respectively, and $[a]^+ = \max(0, a)$. Specifically, for the K-hop network in this paper, the achievable secrecy rate is derived as

$$R_{\mathrm{sec}} \leqslant \left[I(y_D, s) - \max \left(I(y_{E_1}, s), I(y_{E_2}, s) \right) \right]^+, \quad (14)$$

where

$$I(y_D, s) = \log \left(1 + \frac{P_1 \boldsymbol{\omega}_{R_{K-1}}^{\mathrm{H}} \boldsymbol{R}_{SD} \boldsymbol{\omega}_{R_{K-1}}}{\theta_D} \right),$$

$$I(y_{E_u}, s) = \log\det\left(I + \boldsymbol{H}_{E_u}\boldsymbol{H}_{E_u}^{\mathrm{H}}\boldsymbol{\theta}_{E_u}^{-1}\right), \qquad u = 1, 2, \tag{15}$$

with $\boldsymbol{R}_{SD} = \boldsymbol{a}_{sd}\boldsymbol{a}_{sd}^{\mathrm{H}}$, $\boldsymbol{a}_{sd} = \boldsymbol{F}_{R_{K-1}D}(\prod_{m=1}^{K-2}\boldsymbol{H}_{R_mR_{m+1}}\boldsymbol{W}_{R_m})\boldsymbol{h}_{SR_1}$. Finally, the optimization problem is formulated as follows

$$\begin{aligned} \underset{\boldsymbol{\omega}_{R_1},\ldots,\boldsymbol{\omega}_{R_{K-1}}}{\text{maximize}} \quad & \log\left(\frac{1+\frac{P_1\boldsymbol{\omega}_{R_{K-1}}^{\mathrm{H}}\boldsymbol{R}_{SD}\boldsymbol{\omega}_{R_{K-1}}}{\theta_D}}{\det(I+\boldsymbol{H}_{E_u}\boldsymbol{H}_{E_u}^{\mathrm{H}}\boldsymbol{\theta}_{E_u}^{-1})}\right) \\ \text{s.t.} \quad & P_{R_k}^n \leqslant P_{R_k}^{n,\max}, \quad k = 1, ..., K-1, \quad n = 1, 2..., N_{R_k}, \end{aligned} \tag{16}$$

where $P_{R_k}^n$ denotes the nth antenna transmit power of relay R_k, $P_{R_k} = \sum_{n=1}^{N_{R_k}} P_{R_k}^n$ is the total transmit power of relay R_k. It is obvious that for the above optimization problem its objective is a product of two interdependent generalized Rayleigh quotients [21], which makes the optimization problem nonconvex and difficult to solve. In general, some advanced optimization tools will be used to solve complicated mathematic problems [24,25]. In our work, to reveal the physical meaning of the considered optimization problem, an iterative optimization algorithm is proposed.

3 Proposed secrecy relay beamforming designs

Because the CSI of eavesdropper E_1 is available, each relay beamforming $\boldsymbol{\omega}_{R_k}$ can be chosen in the null space of $\boldsymbol{H}_k$,

$$\boldsymbol{H}_k = \left[\boldsymbol{F}_{R_kE_1}\prod_{m=1}^{k-1}\boldsymbol{H}_{R_mR_{m+1}}\boldsymbol{W}_{R_m}\boldsymbol{h}_{SR_1}\right], \quad \forall k = 1, 2, ..., K-1. \tag{17}$$

Thus the information leakage to E_1 can be completely eliminated. However, for the CSI unavailable eavesdropper E_2, we utilize the artificial noise $\boldsymbol{n}_a$ generated by relay R_1 to make the information leakage as little as possible. In order to avoid the interference to destination D, the $\boldsymbol{n}_a$ should be in the null space of the following matrix

$$\boldsymbol{H}_a^K = \left[\boldsymbol{F}_{R_{K-1}D}\prod_{m=2}^{K-2}\boldsymbol{H}_{R_mR_{m+1}}\boldsymbol{W}_{R_m}\boldsymbol{H}_{R_1R_2}\right]. \tag{18}$$

Furthermore, for notational simplicity it is defined that $\boldsymbol{n}_a = \boldsymbol{H}_{a,\perp}^K\boldsymbol{\mu}$, where $\boldsymbol{H}_{a,\perp}^K$ is the projection matrix onto the null space of $\boldsymbol{H}_a^K$ and $\boldsymbol{\mu}$ is a random vector. Owing to the constraint for $\boldsymbol{n}_a$, $\boldsymbol{\mu}$ becomes the actual Gaussian random artificial noise, whose elements should be distributed as $\mathcal{CN}(0, \sigma_a^2)$. Hence, we need to replace the term $\prod_{m=2}^{k-1}\boldsymbol{H}_{R_mR_{m+1}}\boldsymbol{W}_{R_m}\boldsymbol{H}_{R_1R_2}$ by

$$\boldsymbol{B}_{R_1R_k}^{'} = \prod_{m=2}^{k-1}\boldsymbol{H}_{R_mR_{m+1}}\boldsymbol{W}_{R_m}\boldsymbol{H}_{R_1R_2}\boldsymbol{H}_{a,\perp}^K, \quad \forall k = 1, ..., K-1. \tag{19}$$

It is also observed that the value of σ_a^2 should be as large as possible to reduce the information leakage to E_2, which however may greatly decrease the transmit power of the effective signal s_1. Hence, the trade off between the transmit power of s_1 and that of $\boldsymbol{n}_a$ should be researched to achieve the security communication. Overall, our optimization problem can be finally formulated into maximizing the received SNR at destination D with above constraints and transmit power constraints of each relay. Mathematically, that is

$$\begin{aligned} \underset{\boldsymbol{\omega}_{R_1},\ldots,\boldsymbol{\omega}_{R_{K-1}},\sigma_a^2}{\text{maximize}} \quad & \frac{P_1\boldsymbol{\omega}_{R_{K-1}}^{\mathrm{H}}\boldsymbol{R}_{SD}\boldsymbol{\omega}_{R_{K-1}}}{\theta_D} \\ \text{s.t.} \quad & \left(\boldsymbol{\omega}_{R_k}\boldsymbol{\omega}_{R_k}^{\mathrm{H}}\right)[n,n]\boldsymbol{D}_{R_k}[n,n] \leqslant P_{R_k}^n, \quad \forall k = 1, ..., K-1, \quad \forall n = 1, ..., N_{R_k}, \\ & \boldsymbol{\omega}_{R_1}^{\mathrm{H}}\boldsymbol{D}_{R_1}\boldsymbol{\omega}_{R_1} \leqslant P_{R_1} - \sigma_a^2\mathrm{rank}(\boldsymbol{H}_{a,\perp}^K), \end{aligned}$$

$$\boldsymbol{\omega}_{R_k} = \boldsymbol{H}_{k,\perp}\boldsymbol{\nu}_k, \quad \forall k = 1, ..., K-1, \tag{20}$$

where $\boldsymbol{D}_{R_k},\ k = 1, ..., K-1$ all are diagonal matrices, whose diagonal elements are

$$\begin{aligned}\boldsymbol{D}_{R_k}[m,m] = P_1 \left| \left(\prod_{l=1}^{k-1} \boldsymbol{H}_{R_l R_{l+1}} \boldsymbol{W}_{R_l} \boldsymbol{h}_{SR_1} \right)[m,1] \right|^2 \\ + \sigma^2(a_m^k + 1) + \sigma_a^2 b_m^k, \quad \forall m = 1, ..., N_{r_k}, \quad \forall k = 1, ..., K-1,\end{aligned} \tag{21}$$

$$a_m^k = \begin{cases} \sum\limits_{i=1}^{k-1} \left\| \left(\prod\limits_{l=i}^{k-1} \boldsymbol{H}_{R_l R_{l+1}} \boldsymbol{W}_{R_l} \right)^{(m)} \right\|^2, & k = 2, ..., K-1; \\ 0, & k = 1, \end{cases} \quad b_m^k = \begin{cases} \sum\limits_{l=1}^{L} |\boldsymbol{B}'_{R_1 R_k}[m,l]|^2, & k = 2, ..., K-1; \\ 0, & k = 1. \end{cases} \tag{22}$$

$\boldsymbol{H}_{k,\perp}$ denotes the projection matrix onto the null space of $\boldsymbol{H}_k$. L is the rank of matrix $\boldsymbol{H}_{a,\perp}^K$. Generally speaking, the joint optimization for $[\boldsymbol{\omega}_{R_1}, \boldsymbol{\omega}_{R_2}, ..., \boldsymbol{\omega}_{R_{K-1}}]$ is difficult owing to the mutual dependence between them. Fortunately, it is discovered that once the previous $K-2$ relay beamformings $[\boldsymbol{\omega}_{R_1}, \boldsymbol{\omega}_{R_2}, ..., \boldsymbol{\omega}_{R_{K-2}}]$ are determined, the corresponding relay power constraints of problem (20) can be satisfied. Based on this, we substitute the constraint $\boldsymbol{\omega}_{R_{K-1}} = \boldsymbol{H}_{K-1,\perp}\boldsymbol{\nu}_{K-1}$ into the relay R_{K-1} power constraint and the objective function, thus the optimization problem is transformed into the following optimization problem

$$\begin{aligned} \underset{\boldsymbol{\nu}_{K-1}}{\text{maximize}} \quad & P_1 \frac{\boldsymbol{\nu}_{K-1}^{\mathrm{H}} \boldsymbol{R}'_{SD} \boldsymbol{\nu}_{K-1}}{\sigma^2(1 + \boldsymbol{\nu}_{K-1}^{\mathrm{H}} \boldsymbol{Q}_{\nu_{K-1}} \boldsymbol{\nu}_{K-1})} \\ \text{s.t.} \quad & \boldsymbol{\nu}_{K-1}^{\mathrm{H}} \boldsymbol{D}'_{R_{K-1}} \boldsymbol{\nu}_{K-1} \leqslant P_{R_{K-1}}, \end{aligned} \tag{23}$$

where $\boldsymbol{R}'_{SD}$, $\boldsymbol{D}'_{R_{K-1}}$ and $\boldsymbol{Q}_{\nu_{K-1}}$ are defined as follows

$$\begin{aligned} &\boldsymbol{R}'_{SD} = \boldsymbol{H}_{K-1,\perp}^{\mathrm{H}} \boldsymbol{R}_{SD} \boldsymbol{H}_{K-1,\perp}, \quad \boldsymbol{D}'_{R_{K-1}} = \boldsymbol{H}_{K-1,\perp}^{\mathrm{H}} \boldsymbol{D}_{R_{K-1}} \boldsymbol{H}_{K-1,\perp}, \\ &\boldsymbol{Q}_{\nu_{K-1}} = \boldsymbol{H}_{K-1,\perp}^{\mathrm{H}} \boldsymbol{F}_{R_{K-1},D} \left(\sum_{i=1}^{K-2} \left(\prod_{m=i}^{K-2} \boldsymbol{H}_{R_m R_{m+1}} \boldsymbol{W}_{R_m} \right) \left(\prod_{m=i}^{K-2} \boldsymbol{W}_{R_{K+i-m-2}}^{\mathrm{H}} \boldsymbol{H}_{R_{K+i-m-2} R_{K+i-m-1}}^{\mathrm{H}} \right) \right. \\ &\qquad \left. + \boldsymbol{I} \right) \boldsymbol{F}_{R_{K-1},D}^{\mathrm{H}} \boldsymbol{H}_{K-1,\perp}. \end{aligned} \tag{24}$$

In order to obtain the closed-form solution of $\boldsymbol{\omega}_{R_{K-1}}$ to greatly simplify the optimization problem, we relax the individual antenna power constraints of relay R_{K-1} to the total power constraint of problem (23). It is also noticed that $\boldsymbol{D}'_{R_{K-1}}$ is a positive definite matrix and has a Cholesky factorization, i.e.,

$$\boldsymbol{D}'_{R_{K-1}} = \boldsymbol{D}'^{\frac{1}{2}\mathrm{H}}_{R_{K-1}} \boldsymbol{D}'^{\frac{1}{2}}_{R_{K-1}}.$$

Based on this fact, it is obvious that the above problem is a generalized Rayleigh quotient problem [23], which has the following closed-form optimal solution

$$\tilde{\boldsymbol{\nu}}_{K-1} = \sqrt{P_{R_{K-1}}}\, a(\boldsymbol{\omega}_{R_1}, ..., \boldsymbol{\omega}_{R_{K-2}}) \boldsymbol{D}'^{-\frac{1}{2}}_{R_{K-1}} (\boldsymbol{I} + P_{R_{K-1}} \boldsymbol{D}'^{-\frac{1}{2}\mathrm{H}}_{R_{K-1}} \boldsymbol{Q}_{\nu_{K-1}} \boldsymbol{D}'^{-\frac{1}{2}}_{R_{K-1}})^{-1} \boldsymbol{D}'^{-\frac{1}{2}\mathrm{H}}_{R_{K-1}} \boldsymbol{H}_{K-1,\perp}^{\mathrm{H}} \boldsymbol{a}_{sd}, \tag{25}$$

where the normalizing factor equals

$$a(\boldsymbol{\omega}_{R_1}, ..., \boldsymbol{\omega}_{R_{K-2}}) = \left(\boldsymbol{a}_{sd}^{\mathrm{H}} \boldsymbol{H}_{K-1,\perp} \boldsymbol{D}'^{-\frac{1}{2}}_{R_{K-1}} (\boldsymbol{I} + P_{R_{K-1}} \boldsymbol{D}'^{-\frac{1}{2}\mathrm{H}}_{R_{K-1}} \boldsymbol{Q}_{\nu_{K-1}} \boldsymbol{D}'^{-\frac{1}{2}}_{R_{K-1}})^{-2} \boldsymbol{D}'^{-\frac{1}{2}\mathrm{H}}_{R_{K-1}} \boldsymbol{H}_{K-1,\perp}^{\mathrm{H}} \boldsymbol{a}_{sd} \right)^{-\frac{1}{2}}. \tag{26}$$

Furthermore, the $\tilde{\boldsymbol{\omega}}_{R_{K-1}}$ satisfies $\tilde{\boldsymbol{\omega}}_{R_{K-1}} = \boldsymbol{H}_{K-1,\perp}\tilde{\boldsymbol{\nu}}_{K-1}$. Once the closed-form suboptimal $\tilde{\boldsymbol{\omega}}_{R_{K-1}}$ is derived, it can be utilized to find the value of $\boldsymbol{\omega}_{R_k}, \quad \forall k = 1, ..., K-2$ in a one by one way. In addition,

considering the artificial noise $\boldsymbol{n}_a$ transmitted with effective signal s_1 together, a natural problem is to determine the power allocation between information transmission and artificial noise transmission, which has great influence on the optimization of $\boldsymbol{\omega}_{R_k}$, $\forall k = 1, ..., K-2$.

In view of the artificial noise only generated by R_1, the artificial noise is only a function of $\boldsymbol{\omega}_{R_1}$. Similar to formulate (23), $\boldsymbol{\omega}_{R_1}^{\text{ini}} = \boldsymbol{H}_{1,\perp}\boldsymbol{\nu}_{1,\text{ini}}$ is substituted into the objective function and all other constraints and then the optimization problem is formulated as

$$\begin{aligned}
\underset{\boldsymbol{\nu}_{1,\text{ini}},\sigma_a^2}{\text{minimize}} \quad & \boldsymbol{\nu}_{1,\text{ini}}^{\text{H}}\boldsymbol{D}_{R_1}^{'}\boldsymbol{\nu}_{1,\text{ini}} \\
\text{s.t.} \quad & \left(\boldsymbol{H}_{1,\perp}\boldsymbol{\nu}_{1,\text{ini}}\boldsymbol{\nu}_{1,\text{ini}}^{\text{H}}\boldsymbol{H}_{1,\perp}^{\text{H}}\right)[n,n]\boldsymbol{D}_{R_1}[n,n] \leqslant P_{R_1}^n, \quad \forall n = 1, ..., N_{R_1}, \\
& \boldsymbol{\nu}_{1,\text{ini}}^{\text{H}}\boldsymbol{D}_{R_1}^{'}\boldsymbol{\nu}_{1,\text{ini}} \leqslant P_{R_1} - \sigma_a^2\text{rank}(\boldsymbol{H}_{a,\perp}^K), \\
& \frac{P_1\boldsymbol{\nu}_{1,\text{ini}}^{\text{H}}\boldsymbol{D}_{R_2}^{n'}\boldsymbol{\nu}_{1,\text{ini}}}{\boldsymbol{\nu}_{1,\text{ini}}^{\text{H}}\boldsymbol{G}_{R_2}^n\boldsymbol{\nu}_{1,\text{ini}} + \sigma_a^2\|\boldsymbol{G}_a^{(n)}\|^2 + \sigma^2} \geqslant \gamma_{R_2}, \quad \forall n = 1, ..., N_{R_2},
\end{aligned} \tag{27}$$

where

$$\begin{aligned}
&\boldsymbol{D}_{R_1}^{'} = \boldsymbol{d}_{R_1}\boldsymbol{d}_{R_1}^{\text{H}}, \quad \boldsymbol{d}_{R_1} = \boldsymbol{H}_{1,\perp}{}^{\text{H}}\boldsymbol{D}_{R_1}^{\frac{1}{2}}, \\
&\boldsymbol{D}_{R_2}^{n'} = \boldsymbol{\beta}_n\boldsymbol{\beta}_n^{\text{H}}, \quad \boldsymbol{\beta}_n = \boldsymbol{H}_{1,\perp}^{\text{H}}\text{diag}(\boldsymbol{H}_{R_1R_2}^{(n)})\boldsymbol{h}_{SR_1}, \\
&\boldsymbol{G}_{R_2}^n = \boldsymbol{g}_n\boldsymbol{g}_n^{\text{H}}, \quad \boldsymbol{g}_n = \boldsymbol{H}_{1,\perp}^{\text{H}}\boldsymbol{H}_{R_1R_2}^{(n)^{\text{T}}}, \quad \boldsymbol{G}_a = \boldsymbol{H}_{R_1R_2}\boldsymbol{H}_{a,\perp}^K.
\end{aligned} \tag{28}$$

It is clear that the initial $\boldsymbol{W}_{R_1}$ and determined σ_a^2 can be obtained simultaneously by solving the above problem. Besides, we find that the objective function of (27) is to minimize the allocated power for information transmission, thus more remaining power can be used to transmit artificial noise $\boldsymbol{n}_a$ to confuse the eavesdropper E_2. And the third constraint of (27) denotes the received SNR at each antenna of R_2, which is set to be higher than the threshold γ_{R_2}. With this constraint, the power allocation between information transmission and artificial noise transmission can be determined. Then, the problem (27) can be further transformed as

$$\begin{aligned}
\underset{\boldsymbol{\nu}_{1,\text{ini}},\sigma_a^2}{\text{minimize}} \quad & \boldsymbol{\nu}_{1,\text{ini}}^{\text{H}}\boldsymbol{D}_{R_1}^{'}\boldsymbol{\nu}_{1,\text{ini}} \\
\text{s.t.} \quad & |\boldsymbol{H}_{1,\perp}^{(n)}\boldsymbol{\nu}_{1,\text{ini}}|^2 \leqslant \frac{P_{R_1}^n}{\boldsymbol{D}_{R_1}[n,n]}, \quad \forall n = 1, ..., N_{R_1}, \\
& \|\boldsymbol{d}_{R_1}^{\text{H}}\boldsymbol{\nu}_{1,\text{ini}}\|^2 \leqslant P_{R_1} - \sigma_a^2\text{rank}(\boldsymbol{H}_{a,\perp}^K), \\
& |\boldsymbol{\nu}_{1,\text{ini}}^{\text{H}}\boldsymbol{\beta}_n|^2 \geqslant \frac{\gamma_{R_2}}{P_1}\left\|\frac{\boldsymbol{g}_n^{\text{H}}\boldsymbol{\nu}_{1,\text{ini}}}{\sqrt{\sigma_a^2\|\boldsymbol{G}_a^{(n)}\|^2+\sigma^2}}\right\|^2, \quad \forall n = 1, ..., N_{R_2}.
\end{aligned} \tag{29}$$

It is observed that the objective function and the constraints of (29) both are not affected by multiplying the obtained $\tilde{\boldsymbol{\nu}}_{1,\text{ini}}$ by an arbitrary phase constant $\text{e}^{\text{j}\phi}$. Hence, without loss of generality it is assumed that the term $\boldsymbol{\nu}_{1,\text{ini}}^{\text{H}}\boldsymbol{\beta}_n$ is a real number. Based on this simplification, the problem (29) is further rewritten as follows

$$\begin{aligned}
\underset{\hat{\boldsymbol{\nu}}_{1,\text{ini}},\sigma_a^2}{\text{minimize}} \quad & t \\
\text{s.t.} \quad & \|\hat{\boldsymbol{d}}_{R_1}^{\text{H}}\hat{\boldsymbol{\nu}}_{1,\text{ini}}\| \leqslant t, \\
& |\boldsymbol{h}_n\hat{\boldsymbol{\nu}}_{1,\text{ini}}|^2 \leqslant \frac{P_{R_1}^n}{\boldsymbol{D}_{R_1}[n,n]}, \quad \forall n = 1, ..., N_{R_1}, \\
& \|\hat{\boldsymbol{d}}_{R_1}^{\text{H}}\hat{\boldsymbol{\nu}}_{1,\text{ini}}\| \leqslant \sqrt{P_{R_1} - \sigma_a^2\text{rank}(\boldsymbol{H}_{a,\perp}^K)}, \\
& \|\hat{\boldsymbol{g}}_n^{\text{H}}\hat{\boldsymbol{\nu}}_{1,\text{ini}}\| \leqslant \sqrt{\frac{P_1}{\gamma_{R_2}}}\hat{\boldsymbol{\beta}}_n^{\text{H}}\hat{\boldsymbol{\nu}}_{1,\text{ini}}, \quad \forall n = 1, ..., N_{R_2},
\end{aligned} \tag{30}$$

where

$$\hat{\boldsymbol{\nu}}_{1,\mathrm{ini}}=\begin{bmatrix}\boldsymbol{\nu}_{1,\mathrm{ini}}\\1\end{bmatrix},\quad \boldsymbol{h}_n=[\boldsymbol{H}_{1,\perp}^{(n)},0],\quad \hat{\boldsymbol{\beta}}_n=\begin{bmatrix}\boldsymbol{\beta}_n\\0\end{bmatrix},\quad \hat{\boldsymbol{d}}_{R_1}^{\mathrm{H}}=[\boldsymbol{d}_{R_1}^{\mathrm{H}}\mathbf{0}],\quad \hat{\boldsymbol{g}}_n^{\mathrm{H}}=\begin{bmatrix}\boldsymbol{g}_n^{\mathrm{H}} & 0\\ \mathbf{0} & \sqrt{\sigma_a^2\|\boldsymbol{G}_a^{(n)}\|^2+\sigma^2}\end{bmatrix}. \tag{31}$$

It is obvious that the problem (30) is a second-order cone programming (SOCP) problem [19] and can be solved efficiently by interior point methods. After solving (30), the initial value of $\boldsymbol{\omega}_{R_1}^{\mathrm{ini}}=\boldsymbol{H}_{1,\perp}\tilde{\boldsymbol{\nu}}_{1,\mathrm{ini}}$ can be obtained. Furthermore, the initial $\boldsymbol{W}_{R_k}^{\mathrm{ini}},\ \ \forall k=2,...,K-2$ can also be obtained successively by simply satisfying the power constraint of each relay

$$\left(\boldsymbol{\omega}_{R_k}\boldsymbol{\omega}_{R_k}^{\mathrm{H}}\right)[n,n]\boldsymbol{D}_{R_k}[n,n]\leqslant P_{R_k}^n,\quad \forall k=2,...,K-2,\qquad \forall n=1,...,N_{R_k}. \tag{32}$$

With the computed initial $\boldsymbol{W}_{R_k}^{\mathrm{ini}},\ \ \forall k=1,...,K-2$, we can calculate the suboptimal relay beamforming $\boldsymbol{\omega}_{R_{K-1}}$ by (25). And in turn, we will utilize it to optimize the $\boldsymbol{\omega}_{R_k}$, $k=1,...,K-2$ successively. Note that only $\boldsymbol{\omega}_{R_k}\ \forall k=1,...,K-2$ related optimization problem can be derived from the original optimization problem (20), which is expressed as

$$\begin{aligned}\underset{\boldsymbol{\omega}_{R_k}}{\text{maximize}}\quad & \frac{P_1\boldsymbol{\omega}_{R_k}^{\mathrm{H}}\boldsymbol{Q}_{k,K-1}^{K,1}\boldsymbol{\omega}_{R_k}}{\boldsymbol{\omega}_{R_k}^{\mathrm{H}}\boldsymbol{P}_{k,K-1}^{K,1}\boldsymbol{\omega}_{R_k}+\sigma^2(a_{k,K-1}^K+\|\boldsymbol{h}_{R_{K-1}D}\boldsymbol{W}_{R_{K-1}}\|^2+1)}\\ \text{s.t.}\quad & \left(\boldsymbol{\omega}_{R_k}\boldsymbol{\omega}_{R_k}^{\mathrm{H}}\right)[m,m]\boldsymbol{D}_{R_k}[m,m]\leqslant P_{R_k}^m,\quad \forall m=1,...,N_{R_k},\\ & \boldsymbol{\omega}_{R_k}^{\mathrm{H}}\boldsymbol{P}_{k,n}^{l,m}\boldsymbol{\omega}_{R_k}+\sigma^2a_{k,n}^{l,m}+\sigma_a^2\|\boldsymbol{Q}_B^{k,n}\|_F^2+\sigma^2|\boldsymbol{\omega}_{R_n}[m]|^2\leqslant P_{R_n}^m,\\ & \forall n=l=k+1,...,K-1,\quad \forall m=1,...,N_{R_n},\\ & \boldsymbol{\omega}_{R_k}=H_{k,\perp}\boldsymbol{\nu}_{\boldsymbol{k}}.\end{aligned} \tag{33}$$

In order to solve the above optimization problem, some necessary transformations are needed. First the following auxiliary symbols are defined.

$$\boldsymbol{Q}_{k,n}^{l,m}=\boldsymbol{S}_{k,n}^{l(m)^{\mathrm{H}}}\boldsymbol{S}_{k,n}^{l(m)},\quad \boldsymbol{S}_{k,n}^{l(m)}=\boldsymbol{C}_{k,n}^{l}\mathrm{diag}\left(\prod_{m=1}^{k-1}\boldsymbol{H}_{R_mR_{m+1}}\boldsymbol{W}_{R_m}\boldsymbol{h}_{SR_1}\right),$$

$$\boldsymbol{C}_{k,n}^{l}=\begin{cases}\boldsymbol{W}_{R_n}\left(\prod_{m=k+1}^{n-1}\boldsymbol{H}_{R_mR_{m+1}}\boldsymbol{W}_{R_m}\right)\boldsymbol{H}_{R_kR_{k+1}}, & n=l=k+1,...,K-1,\\ \boldsymbol{h}_{R_{K-1}D}\boldsymbol{W}_{R_{K-1}}\left(\prod_{m=k+1}^{K-2}\boldsymbol{H}_{R_mR_{m+1}}\boldsymbol{W}_{R_m}\right)\boldsymbol{H}_{R_kR_{k+1}}, & n=K-1,\ \ l=K.\end{cases} \tag{34}$$

In addition, the term of $\boldsymbol{P}_{k,n}^{l,m}$ in (33) is defined based on the following equations

$$\begin{aligned}&\boldsymbol{P}_{k,n}^{l,m}=P_1\boldsymbol{Q}_{k,n}^{l,m}+\sigma^2\boldsymbol{G}_{k,n}^{l,m}+\sigma_a^2\boldsymbol{B}_{k,n}^{l,m},\quad \boldsymbol{G}_{k,n}^{l,m}=\sum_{i=1}^{k}\boldsymbol{R}_{k,i}\odot\boldsymbol{R}_{k,n}^{l,m},\\ &\boldsymbol{R}_{k,i}=\left(\prod_{m=i}^{k-1}\boldsymbol{H}_{R_mR_{m+1}}\boldsymbol{W}_{R_m}\right)\left(\prod_{m=i}^{k-1}\boldsymbol{W}_{R_{K+i-m-2}}^{\mathrm{H}}\boldsymbol{H}_{R_{K+i-m-2}R_{K+i-m-1}}^{\mathrm{H}}\right),\\ &\boldsymbol{R}_{k,n}^{l,m}=\boldsymbol{C}_{k,n}^{l(m)^{\mathrm{H}}}\boldsymbol{C}_{k,n}^{l(m)},\\ &\boldsymbol{B}_{k,n}^{l,m}=\boldsymbol{J}_k\ \odot\boldsymbol{R}_{k,n}^{l,m},\quad \boldsymbol{J}_k=\boldsymbol{B}_{R_1R_k}^{'}\boldsymbol{B}_{R_1R_k}^{'H}.\end{aligned} \tag{35}$$

The terms of $\boldsymbol{Q}_B^{k,n}$ and $a_{k,n}^l$ in (33) are defined as

$$\boldsymbol{Q}_B^{k,n}=\begin{cases}\mathbf{0}, & k\neq 1;\\ \boldsymbol{W}_{R_n}\boldsymbol{B}_{R_1R_n}^{'}, & k=1,\end{cases}\quad a_{k,n}^{l,m}=\begin{cases}\sum_{i=k+1}^{n-1}\|\boldsymbol{N}_{i,n}^{l(m)}\|^2, & n\geqslant k+2;\\ 0,\end{cases}$$

$$\boldsymbol{N}_{i,n}^{l}=\begin{cases}\boldsymbol{W}_{R_n}(\prod\limits_{m=i}^{n-1}\boldsymbol{H}_{R_mR_{m+1}}\boldsymbol{W}_{R_m}), & n=l;\\ \boldsymbol{h}_{R_{K-1}D}\boldsymbol{W}_{R_{K-1}}(\prod\limits_{m=i}^{K-2}\boldsymbol{H}_{R_mR_{m+1}}\boldsymbol{W}_{R_m}), & n=K-1,\ l=K.\end{cases}\tag{36}$$

$\boldsymbol{A}\odot\boldsymbol{B}$ denotes the Hadamard product between matrices $\boldsymbol{A}$ and $\boldsymbol{B}$. Particularly, for relay R_1, an modified constraint $\boldsymbol{\omega}_{R_1}^{\mathrm{H}}\boldsymbol{D}_{R_1}\boldsymbol{\omega}_{R_1}\leqslant t$, in which the value of t can be derived from (30), should be satisfied. Further, in order to solve the above problem effectively, we define an extra auxiliary matrix $\boldsymbol{X}_k=\boldsymbol{\omega}_{R_k}\boldsymbol{\omega}_{R_k}^{\mathrm{H}}$ to transform (33) into

$$\begin{aligned}\underset{\boldsymbol{X}_k}{\text{maximize}}\quad & \frac{P_1\mathrm{Tr}(\boldsymbol{Q}_{k,K-1}^{K,1}\boldsymbol{X}_k)}{\mathrm{Tr}(\boldsymbol{P}_{k,K-1}^{K,1}\boldsymbol{X}_k)+\sigma^2(a_{k,K-1}^{K}+\|\boldsymbol{h}_{R_{K-1}D}\boldsymbol{W}_{R_{K-1}}\|^2+1)}\\ \text{s.t.}\quad & \mathrm{Tr}\left(\boldsymbol{I}_k^{(m)}\boldsymbol{X}_k{\boldsymbol{I}_k^{(m)}}^{\mathrm{H}}\right)\leqslant\frac{P_{R_k}^{m}}{\boldsymbol{D}_{R_k}[m,m]},\quad\forall m=1,...,N_{R_k},\\ & \mathrm{Tr}(\boldsymbol{P}_{k,n}^{l,m}\boldsymbol{X}_k)\leqslant P_{R_n}^{m}-\sigma^2(a_{k,n}^{l,m}+|\boldsymbol{\omega}_{R_n}[m]|^2)-\sigma_a^2\|\boldsymbol{Q}_B^{k,n}\|_F^2,\\ & \forall n=l=k+1,...,K-1,\quad\forall m=1,...,N_{R_n},\\ & \mathrm{Tr}(\boldsymbol{Q}_H^{k}\boldsymbol{X}_k)=0,\quad\mathrm{rank}(\boldsymbol{X}_k)=1,\quad\boldsymbol{X}_k\succeq 0,\end{aligned}\tag{37}$$

where $\boldsymbol{Q}_H^k=\boldsymbol{H}_k\boldsymbol{H}_k^{\mathrm{H}}$, and $\boldsymbol{I}_k$ is an $N_{R_k}\times N_{R_k}$ identity matrix. Generally, the bisection method mentioned in [26] is always used to solve this problem. With this method, the upper bound of the objective function is defined as $\gamma_{\boldsymbol{\omega}_{R_k}}^{\max}=P_1\lambda_{\max}((\boldsymbol{P}_{k,K-1}^{K,1})^{-1}\hat{\boldsymbol{Q}}_{k,K-1}^{K,1})$, where $\lambda_{\max}(\boldsymbol{A})$ denotes the maximum eigenvalue of matrix $\boldsymbol{A}$, and the lower bound is zero. Because of the non-convexity of the above optimization problem, a relaxed semidefinite (SDR) technique is further performed by neglecting the rank-one constraint temporarily. Then, the SDR problem is formula in (38), which can also be solved by the interior point methods

$$\begin{aligned}\underset{\boldsymbol{X}_k}{\text{maximize}}\quad & \gamma_{\boldsymbol{\omega}_{R_k}}\\ \text{s.t.}\quad & \frac{P_1\mathrm{Tr}(\boldsymbol{Q}_{k,K-1}^{K,1}\boldsymbol{X}_k)}{\mathrm{Tr}(\boldsymbol{P}_{k,K-1}^{K,1}\boldsymbol{X}_k)+\sigma^2(a_{k,K-1}^{K}+\|\boldsymbol{h}_{R_{K-1}D}\boldsymbol{W}_{R_{K-1}}\|^2+1)}\geqslant\gamma_{\boldsymbol{\omega}_{R_k}},\\ & \mathrm{Tr}\left(\boldsymbol{X}_k\boldsymbol{I}_k^{m'}\right)\leqslant\frac{P_{R_k}^{m}}{\boldsymbol{D}_{R_k}[m,m]},\quad\forall m=1,...,N_{R_k},\\ & \mathrm{Tr}(\boldsymbol{P}_{k,n}^{l,m}\boldsymbol{X}_k)\leqslant P_{R_n}^{m}-\sigma^2(a_{k,n}^{l}+|\boldsymbol{\omega}_{R_n[m]}|^2)-\sigma_a^2\|\boldsymbol{Q}_B^{k,n}\|^2,\\ & \forall n=l=k+1,...,K-1,\quad\forall m=1,...,N_{R_n},\\ & \mathrm{Tr}(\boldsymbol{Q}_H^{k}\boldsymbol{X}_k)=0,\quad\boldsymbol{X}_k\succeq 0,\end{aligned}\tag{38}$$

where $\boldsymbol{I}_k^{m'}={\boldsymbol{I}_k^{(m)}}^{\mathrm{H}}\boldsymbol{I}_k^{(m)}$, and $\gamma_{\boldsymbol{\omega}_{R_k}}$ is the objective function of (37). Then, a penalty function method [21] considering the rank-one constraint again is applied to obtain the $\boldsymbol{\omega}_{R_k}$, which satisfies all constraints in (37). Specifically, by combining the SDR technique with the penalty function method simultaneously, the ultimate optimization problem is given by

$$\begin{aligned}{\boldsymbol{X}_k}^{t+1}\triangleq\arg\min_{\boldsymbol{X}_k}\ & \mathrm{Tr}(\boldsymbol{X}_k)-\lambda_{\max}(\boldsymbol{X}_k^t)\\ & -\mathrm{Tr}\left(\boldsymbol{v}_{k,\max}^{t}{\boldsymbol{v}_{k,\max}^{t}}^{\mathrm{H}}(\boldsymbol{X}_k-\boldsymbol{X}_k^t)\right)\\ \text{s.t.}\quad & (38),\end{aligned}\tag{39}$$

where t denotes the iteration index. $\lambda_{\max}(\boldsymbol{X}_k^t)$ is the maximum eigenvalue of $\boldsymbol{X}_k^t$ and $\boldsymbol{v}_{k,\max}^t$ is the corresponding eigenvector of $\lambda_{\max}(\boldsymbol{X}_k^t)$. By solving (39) iteratively with the initial point $\boldsymbol{X}_k^0$ (which is the optimal solution of the SDR problem (38)), we can get a sequence of $\boldsymbol{X}_k^t, t=1,2,\ldots$, whose rank approaches 1. The convergence of this method is illustrated in [21]. Hence, the final optimal $\tilde{\boldsymbol{X}}_k$ satisfies $\tilde{\boldsymbol{X}}_k=\boldsymbol{X}_k^{t+1}=\boldsymbol{X}_k^t$. Further, the suboptimal $\tilde{\boldsymbol{\omega}}_{R_k}$ can be obtained by decomposing the optimal $\tilde{\boldsymbol{X}}_k$.

In a nutshell, for a K-hop network, we can obtain the closed-form suboptimal $\boldsymbol{W}_{R_{K-1}}$ solution through (25) with the initial value $\boldsymbol{W}_{R_1}^{\text{ini}}$ and $\boldsymbol{W}_{R_k}^{\text{ini}}, ...k = 2, ..., K-2$, which are derived from (30) and (32), respectively. Next, in order to update the value of $\boldsymbol{W}_{R_k}$, $k = 1, ..., K-2$ successively, we solve the SDP problem (39) correspondingly. Owing to the convergence of the problem (39), we can obtain the final suboptimal $\boldsymbol{W}_{R_k}, k = 1, ..., K-1$, which achieves the security communication of the K-hop network. The detailed process is summarized in Algorithm 1.

Algorithm 1 The proposed suboptimal collaborative algorithm for achieving security communication

Initialize: Set the received SNR threshold γ_2 and the initial iteration index $t = 0$. Solving problem (30) for initial $\boldsymbol{\omega}_{R_1}^{(t)}$, and then $\boldsymbol{\omega}_{R_k}^{(t)}, ..., k = 2, ..., K-2$ can also be calculated successively through (32).

1: **repeat**
2: Substituting $\boldsymbol{\omega}_{R_k}^{(t)}, ..., k = 1, ..., K-2$ into (25), thus the suboptimal $\boldsymbol{\omega}_{R_{K-1}}^{(t)}$ is obtained.
3: Set the initial relay index $k = 1$
4: **repeat**
5: With the obtained $[\boldsymbol{\omega}_{R_1}^{(t)}, ..., \boldsymbol{\omega}_{R_{k-1}}^{(t)}, ..., \boldsymbol{\omega}_{R_{k+1}}^{(t)}, ..., \boldsymbol{\omega}_{R_{K-1}}^{(t)}]$, we solve problem (38) to get the initial point $\boldsymbol{X}_k$ for (39).
6: Solving problem (39) iteratively with the initial point $\boldsymbol{X}_k$ until the optimal point $\tilde{\boldsymbol{X}}_k$ is obtained (the iteration symbol of solving (39) is neglected). Further the suboptimal $\boldsymbol{\omega}_{R_k}^{(t+1)}$ can be derived by decomposing $\tilde{\boldsymbol{X}}_k$.
7: Set $k = k + 1$
8: **until** $k = K - 1$
9: Set $t = t + 1$
10: **until** $\tilde{\boldsymbol{\omega}}_{R_k} = \boldsymbol{\omega}_{R_k}^{(t+1)} = \boldsymbol{\omega}_{R_k}^{(t)}$, $\forall k = 1, ..., K-1$
11: Stop and output the obtained parameters $\tilde{\boldsymbol{\omega}}_{R_k}$, $\forall k = 1, ..., K-1$. Further, the achievable secrecy sum rate of the K-hop network can be calculated.

4 Simulation results

In this section, simulation results are given to assess the performance of the proposed cooperative beamforming designs for security communication. In specific, a three-hop cooperative network is simulated, in which all the channel coefficients are generated independently according to $\mathcal{CN}(0, 1)$. Without loss of generality, in our simulation the variance of noise σ^2 is always set to be unit, and the maximum transmit power of source S is fixed as $P_1 = 15$ dB. In addition, the transmit power at each antenna of the relay R_k is denoted as $P_{R_k}^1 = P_{R_k}^2 = P_{R_k}^n = P_{R_k}/(N_{R_k})$, $n = 1, 2, ..., N_{R_k}$. In order to solve standard convex optimization problems, e.g., SOCP (30) and SDP (39) efficiently, the famous software toolbox CVX [27] is used. In the following figures, each point for the secrecy sum rate (SSR) of the three-hop network is an average of 500 Monte Carlo tests.

In Figure 2, the SSR of this three-hop network is shown, with different total transmit powers P_{R_1} of relay R_1 ranging from 8 dB to 28 dB. The initial threshold γ_{R_2} is 15 dB, which determines the power allocation between the information transmission and the artificial noise transmission. In addition, the number of antennas of relay R_2 also varies to assess the security performance of the proposed designs. From this figure, it can be obvious that our proposed algorithm can achieve higher SSR compared with the existing method in [2]. The method in [2] can demonstrate the optimal diagonalization of relay structure of multi-hop MIMO system without considering the secrecy constraints. Further, for maximizing the system capacity, the optimal solution of relay matrix can be obtained by a water-filling algorithm [28]. Hence, utilizing [2] as a comparison, we can clearly observe the security performance improvement of our proposed algorithm. From Figure 2, it can also be observed that the achievable SSR tends to be saturated as P_{R_1} increases, which is due to the arising of the artificial noise and the actually received noise at relay R_2 and destination D, respectively. Similarly, as is shown in Figure 3, we also research the achievable SSR versus the total transmit power P_{R_2} of relay R_2 and the similar results can be achieved. Hence, it can be concluded that our proposed algorithm outperforms the method in [2] in terms of SSR.

As discussed previously, the power allocation between information transmission and the artificial noise transmission has great influence on the network security performance. Therefore, it is necessary to evaluate the achievable SSR versus the initial SNR threshold γ_{R_2} under different total transmit powers

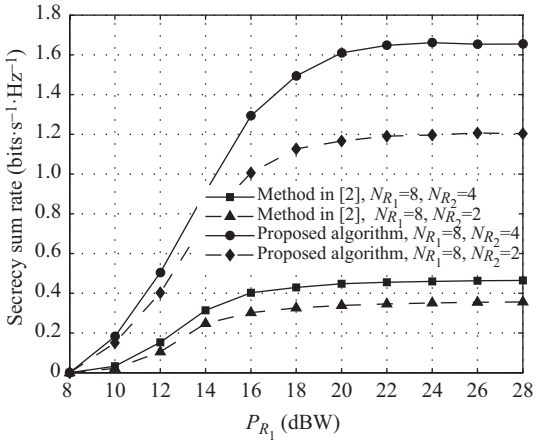

Figure 2 The achievable SSR versus the total transmit power P_{R_1} with different antenna numbers of relay R_2 when $\gamma_{R_2} = 15$ dB and $P_{R_2} = 20$ dB.

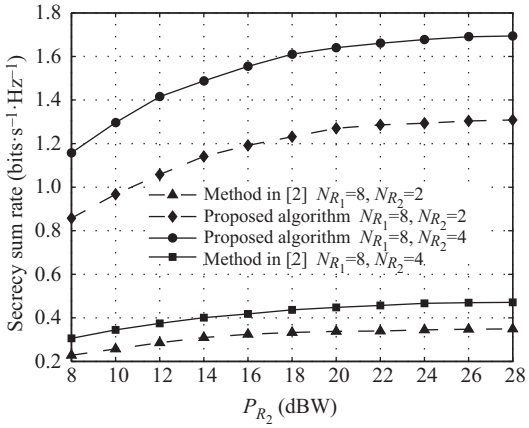

Figure 3 The achievable SSR versus the total transmit power P_{R_2} with different antenna numbers of relay R_2 when $\gamma_{R_2} = 15$ dB and $P_{R_1} = 20$ dB.

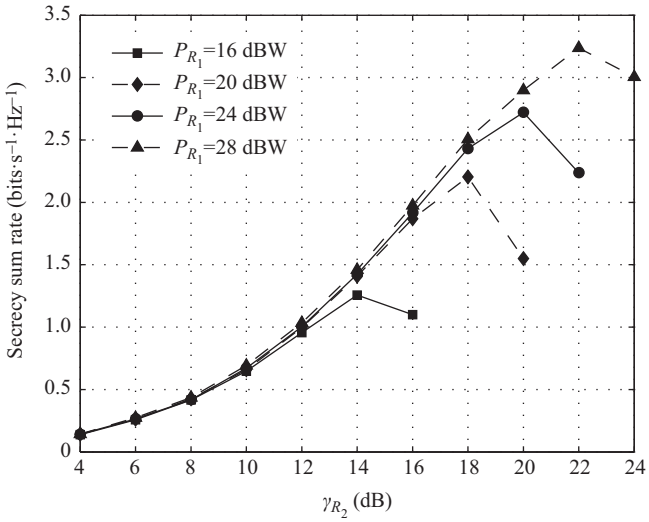

Figure 4 The achievable SSR versus the SNR threshold γ_{R_2} with different total transmit power of relay R_1 when $N_{r1} = 8$ and $N_{r2} = 4$.

P_{R_1} of relay R_1. From Figure 4, it can be seen that for any given P_{R_1}, the SSR increases firstly as threshold γ_{R_2} increases. This is because as the allocated power for information transmission arises, the received SNR at the destination will be improved. However, as the γ_{R_2} increases further, the value of achievable SSR goes down. This is because the AF relay strategy also amplifies the forward noise of relay R_1, which further makes the received SNR at relay R_2 not arbitrarily high. Under the circumstances, problem (27) may be infeasible and the SSR is generally set to be 0. It can also be found that the larger P_{R_1} can support the higher SNR threshold γ_{R_2}, and finally result in larger SSR of the three-hop network.

5 Conclusion

In this paper, we investigated cooperative beamforming design for physical layer security of multi-hop communications. Both the eavesdroppers with available and unavailable CSI are taken into account. To realize security multi-hop communications with such kinds of eavesdroppers, null-space beamforming and artificial noise are adopted together. The joint optimization of beamforming and artificial noise is in nature non-convex and difficult to solve. Hence, by means of the iterative optimization procedure, the

original optimization problem can be decoupled into a series of subproblems. Furthermore, by exploiting convex optimization theory the resulting subproblems can be solved efficiently. Finally, the simulation results demonstrate that our proposed cooperative relay beamforming design achieves better security performance compared with the pre-existing schemes.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61371075, 61421001) and 111 Project of China (Grant No. B14010).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Xing C W, Ma S D, Wu Y C. Robust joint design of linear relay precoder and destination equalizer for dual-hop amplify-and-forward MIMO relay systems. IEEE Trans Signal Process, 2010, 58: 2273–2283
2 Rong Y, Hua Y. Optimality of diagonalization of multi-hop MIMO relays. IEEE Trans Wirel Commun, 2009, 8: 6068–6077
3 Xing C W, Xia M, Gao F, et al. Robust transceiver with Tomlinson-Harashima precoding for amplify-and-forward MIMO relaying systems. IEEE J Sele Area Commun, 2012, 30: 1370–1382
4 Telatar I E. Capacity of multi-antenna gaussian channels. Eur Trans Telecommun, 1999, 10: 585–595
5 Zhu F, Gao F, Yao M, et al. Joint information and jamming beamforming for physical layer security with full duplex base station. IEEE Trans Signal Process, 2014, 62: 6391–6401
6 Li Z, Trappe W, Yates R. Secret communication via multi-antenna transmission. In: Proceedings of 41st Conf Inf Sci Syst, Baltimore, 2007. 905–910
7 Ni J Q, Fei Z S, Xing C W, et al. Secrecy balancing over two-user MISO interference channels with rician fading. Int J Antenn Propag, 2013, 2013: 546260
8 Lindblom J, Karipidis E. Closed-form parameterization of the pareto boundary for the two-user MISO interference channel. In: Proceedings of IEEE Int Conf Acoustics, Speech, and Signal Processing, Prague, 2011. 3372–3375
9 Chen L, Wong K K, Chen H. Optimizing transmitter-receiver collaborative-relay beamforming with perfect CSI. IEEE Commun Lett, 2011, 15: 314–316
10 Wang C, Liu J, Dong Z. Multi-hop collaborative relay beamforming. In: Proceedings of IEEE Vehicular Technology Conference, Las Vegas, 2013. 1–5
11 Shannon C E. Communication theory of secrecy systems. Bell Syst Tech J, 1949, 28: 656–715
12 Wyner A D. The wire-tap channel. Bell Sys Tech J, 1975, 54: 1355–1387
13 Dai B, Ma Z. Achievable rate-equivocation regions for relay broadcast channels with confidential messages. In: Proceedings of ISITA, Melbourne, 2014. 393–397
14 Leung-Yan-Cheong S, Hellman M E. The Gaussian wire-tap channel. IEEE Trans Inf Theory, 1978, 24: 451–456
15 Jorswieck A E, Mochaourab R. Secrecy rate region of MISO interference channel: pareto boundary and non-cooperative games. In: Proceedings of international ITG workshop on smart Antennas, Berlin, 2009. 1–8
16 Fei Z S, Ni J Q, Zhao D, et al. Ergodic secrecy rate of two-user MISO interference channels with statistical CSI. Sci China Inf Sci, 2014, 57: 102302
17 Mu P C, Wang H M, Yin Q Y. Improving the secrecy rate of wireless SIMO systems via two-step transmission. In: Proceedings of Globecom Workshops, Atlanta, 2013. 1280–1285
18 Wang Y W, Yu F R, Tang H, et al. A mean field game theoretic approach for security enhancements in mobile ad hoc networks. IEEE Trans Wirel Commun, 2014, 13: 1616–1627
19 Luan T, Gao F, Zhang X. Joint resource scheduling for relay-assisted broadband cognitive radio networks. IEEE Trans Wirel Commun, 2012, 11: 3090–3100
20 Wang H M, Yin Q Y. Improving the physical-layer security of wireless two-way relaying via analog network coding. In: Proceedings of Global Telecommunications Conference, Houston, 2011. 5–9
21 Wang H M, Luo M, Yin Q Y. Hybrid cooperative beamforming and jamming for physical-layer security of two-way

relay networks. IEEE Trans Inf Foren Secur, 2013, 8: 2007–2020

22 Khisti A, Wornell G. Secure transmission with multiple antennas II: the MIMOME wiretap channel. IEEE Trans Inf Theory, 2010, 56: 5515–5532

23 Tekin E, Yener A. The general gaussian multiple access and two-way wire-tap channels: achievable rates and cooperative jamming. IEEE Trans Inf Theory, 2008, 54: 2735–2751

24 Zhang Z, Long K, Wang J, et al. On swarm intelligence inspired self-organized networking: its bionic mechanisms, designing principles and optimization approaches. IEEE Commun Surv Tut, 2014, 16: 513–537

25 Zhang Z, Long K, Wang J. Self-organization paradigms and optimization approaches for cognitive radio technologies: a survey. IEEE Wirel Commun, 2013, 20: 36–42

26 Vaikundam G, Sudha G F. Distributed beamforming for randomly distributed sensors using bisection method and dynamic programming technique. In: Proceedings of IEEE Int Conf CONECCT, Bangalore, 2013. 1–6

27 Michael G, Stephen B. CVX Users' Guide for CVX version 1.21, 1996

28 Ekrem E, Ulukus S. Secure broadcasting using multiple antennas. J Commun Netw, 2010, 12: 411–432