R1 Reviewer 2: comparer ma technique avec cet article

Digital Signal Processing 109 (2021) 102933

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Optimization of pre-processing filter for time-reversal multi-user secure transmission systems based on artificial noise

Weijia Lei [a,b], Weihan Zhang [a,b], Miaomiao Yang [a,b,*], Hongjiang Lei [a,b], Xianzhong Xie [c]

[a] School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
[b] Chongqing Key Laboratory of Mobile Communications Technology, Chongqing, 400065, China
[c] School of Optoelectronic Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

ARTICLE INFO

Article history:
Available online 3 December 2020

Keywords:
Physical layer security
Time reversal
Pre-processing filter
Artificial noise

ABSTRACT

Physical layer security is a way to realize the secure transmission of information by employing the characteristics of wireless channels. Thanks to its spatial and temporal focusing property, the time-reversal (TR) transmission can achieve effective secure communications even when the transmitter is only equipped with one antenna. This paper studies the design and optimization of the security scheme based on artificial noise (AN) with or without the eavesdropper's channel state information (ECSI) in a TR multi-user downlink multiple access system. The null-space AN is adopted when ECSI is unavailable, and the corresponding optimization problem is to minimize the signal power under each user's signal-to-interference-plus-noise ratio (SINR) target constraint, so that the power used to send AN is maximized and the interception rate of the eavesdropper is minimized. The problem is solved by transforming it into a semidefinite program (SDP) with semidefinite relaxation (SDR). The pre-processing filter and AN are jointly optimized to maximize the sum secrecy rate when ECSI is available. The problem is solved by transforming it into a convex program by using SDR and the first-order Taylor approximation. Simulation results show that the sum secrecy rate of the proposed scheme is significantly higher than that of the conventional TR transmission system with or without AN.

1. Introduction

The broadcast nature of wireless channels makes the information transmitted in wireless communication systems easy to be wire-tapped. The traditional secrecy method is encrypting information with a security code on the upper layer, and the security of the information is guaranteed by the high computational complexity in the process of decrypting the encrypted data without the secret key. With the development of computer technology, the traditional encryption technology is facing the risk of failure. Secure communication can also be achieved by using physical layer technology [1]. The physical layer security (PLS) applies appropriate channel coding and signal processing methods to keep information confidential to the eavesdropper while ensuring that the information can be correctly decoded by the intended receiver [2]. One hot topic in the research of PLS is to maximize the quality difference between the legitimate channel and the eavesdropping channel, which can be achieved by promoting the received signal's quality of the legitimate receiver or degrading that of the eavesdropper or by both.

Multi-antenna technology is a key technology in PLS. The security beamforming and artificial noise (AN) which are most commonly used in PLS are both based on the spatial freedom provided by multiple transmitting antennas. Beamforming is a signal preprocessing technology based on antenna array, which can control the radiation direction of the signal. By beamforming, the beam is pointed to the legitimate receiver and promotes its received signal's strength, while the null is pointed to the eavesdropper, so the security performance can be improved [3,4]. Beamforming can be regarded as a spatial filter, which weighs signals sent by different transmitting antennas so that the signals at the intended receiver coherently superimpose. Embedding AN in the transmitted signal to degrade the signal quality of the eavesdropper is another effective method to enhance the security performance [5], especially when the channel state information (CSI) of the eavesdropping channel cannot be obtained. AN is generally adopted on the basis of beamforming to achieve a more serious

* Corresponding author at: School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China.
E-mail address: yangmiao1004@163.com (M. Yang).

https://doi.org/10.1016/j.dsp.2020.102933
1051-2004/

interference with the eavesdropper than with the legitimate receiver. In general, beamforming is used to control the directions of both AN and the signal.

Time reversal (TR) transmission is a signal processing technique that exploits the multiple paths in the wireless channel and focuses the signal energy at a specific temporal and spatial point [6]. In the conventional TR communication system, the signal is filtered by a pre-processing filter before being sent, and the impulse response (IR) of the pre-processing filter is the time-reversed and conjugate version of the channel impulse response (CIR). The multipath channel is the matched filter of the pre-filtered signal, and the signal transmitted through the multiple paths will coherently superimpose at the receiver at a specific time point. In [7], TR's spatial and temporal focusing property was verified. [8] proved that the spatial and temporal focusing property of TR transmission can improve system performance and save transmission energy, so TR transmission is a green communication technology. The performance of the single-antenna TR transmission system under Rayleigh fading channel was analyzed in [9]. The probability density function and cumulative distribution function of the signal-to-noise ratio (SNR) at the receiver were derived, and the capacity, outage probability, and bit error rate (BER) when using BPSK were analyzed, too. In [10], the performance of the time-reversal division multiple access (TRDMA) system was analyzed. The results show that the CIRs of the channels from the base station to the users can be used to identify different users, and the downlink multi-user transmission can be realized by using TR pre-processing. TRDMA and orthogonal frequency division multiplexing (OFDM) are compared in terms of computational complexity and the system's achievable rate in [11]. The results show that when the bandwidth is large enough, the TRDMA system can obtain a higher achievable rate and lower complexity than the OFDM system. The TRDMA system was further researched in [12], and it is proved that TR transmission can achieve a system performance similar to that of multiple-input multiple-output (MIMO) transmission even when only a single antenna is equipped at the transmitter. In [13], the waveform was optimized based on CIRs and the content information to suppress the inter-user interference (IUI) for a TR-based cloud radio access network.

In the PLS system, most techniques to improve the secrecy performance, such as beamforming and AN, are based on the spatial freedom provided by multiple antennas. However, only a single antenna or a small number of antennas can be installed in size-limited or cost-limited devices, so it is not easy to achieve good PLS performance. The spatial and temporal focusing property of TR transmission not only improves the signal-to-interference-noise ratio (SINR) at the target receiver, but also suppresses energy leakage to the unintended receiver. So TR transmission has a natural anti-eavesdropping capability. The SNRs of the target and unintended receivers in the distributed time-reversal (DTR) transmission system were analyzed in [14], and the results show that TR transmission has a better security performance than direct transmission. The PLS performance of the TR transmission system was analyzed in [15]. The theoretical expressions of the achievable secrecy rate and BERs at the target receiver and the eavesdropper were deduced. The results show that the legitimate receiver can achieve a higher rate and a lower BER than the eavesdropper. However, the IR of the pre-processing filter in a conventional TR system is the time-reversed and conjugate CIR of the channel between the transmitter and the target receiver, which is not optimal for security transmission. Optimizing the pre-processing filter for secure transmission can further improve the security performance of the TR system. In [16], the design of the pre-processing filter in a TR multiple-input single-output (MISO) single user system, with the goal of maximizing achievable secrecy capacity, was studied, and a better security performance than the conventional TR was obtained. The TR pre-processing filter technique can also be combined with the AN technique to further degrade the received signal's quality of the eavesdropper. In [17], three TR pre-processing filters of the signal and AN were designed for the cases with or without eavesdropper's channel state information (ECSI). In [18], the security performance of the TR system assisted by AN was analyzed, and the influence of channel correlation was considered in the analysis.

However, the above-mentioned publications about the PLS issue in the TR transmission system are for the single user scenario. To the best of our knowledge, there is no paper studying the pre-processing filter design for the multi-user PLS TR transmission system so far. This paper studies the scheme for enhancing the security performance of the multi-user TR downlink transmission system when ECSI is known or unknown, and designs pre-processing filters and AN to promote the secrecy rate.

- We adopt the null-space AN for the scenario without ECSI, and optimize pre-processing filters to minimize the signal power under the constraint of the legitimate users' SINR target. In this approach, the power used to send AN is maximized and the interception rate of the eavesdropper is minimized. We transform the original optimization problem into a semidefinite program (SDP) by using semidefinite relaxation (SDR) and obtain the optimal IRs of the pre-processing filters.
- We jointly design pre-processing filters and AN to maximize the sum secrecy rate under the total power constraint for the scenario with ECSI. We transform the original optimization problem into a convex program by using SDR and the first-order Taylor approximation, and we propose an iterative algorithm to solve the program and obtain the optimal solution to IRs of the pre-processing filters and AN.
- Both transmission schemes are compared with the conventional TR scheme with or without AN. Simulation results demonstrate that the proposed scheme can achieve a higher secrecy rate.

The remainder of this paper is organized as follows. Section 2 presents the system model. In section 3, the security transmission schemes are designed for the scenarios with or without ECSI, and the optimization problems are formulated and solved. Section 4 simulates and verifies the performance of the proposed schemes, followed by concluding remarks in Section 5.

2. System model

The single-input single-output (SISO) multi-user downlink multiple-access system model studied in this paper is shown in Fig. 1. There are K legitimate receivers and one eavesdropper in the system. The transmitter, the legitimate receivers and the eavesdropper are each equipped with one antenna. The transmitter uses TR filters to pre-process the transmitted signals. At the same time, AN is introduced to interfere with the eavesdropper to further suppress the quality of its received signal. We jointly design the pre-processing filters and AN to maximize the sum secrecy rate of the system. Denote the CIR from the transmitter to user k $(k = 1, 2, \ldots, K)$ as $h_k[n]$, and that to the eavesdropper as $h_e[n]$. For the convenience of analysis, it is assumed that the length of all CIRs is L, that is, when $n < 0$ or $n \geq L$, $h_k[n] = 0$ and $h_e[n] = 0$. The vector form of the CIRs are $\boldsymbol{h}_k = [h_k[0], h_k[1], \cdots, h_k[L-1]]^{\mathrm{T}}$ and $\boldsymbol{h}_e = [h_e[0], h_e[1], \cdots, h_e[L-1]]^{\mathrm{T}}$, where the superscript T means transpose. The vector form of the IR of the pre-processing filter for user k is $\boldsymbol{g}_k = [g_k[0], g_k[1], \cdots, g_k[L-1]]^{\mathrm{T}}$.

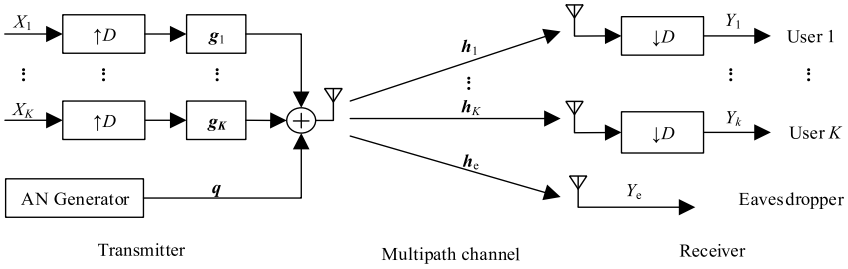

Fig. 1. AN assisted TR multi-user downlink multiple access system.

In transmission, the transmitter simultaneously sends K sequences $\{X_k[m]\}_{m=0}^{M-1}$ $(k = 1, 2, \ldots, K)$ with length M to K users respectively. The sequences are up-sampled before entering the pre-processing filters to increase the sampling rate, which can reduce inter-symbol interference (ISI). The rate back-off factor, or up-sampling factor, D is defined as the ratio of the sampling rate to the baud rate (that is, the symbol rate). The up-sampled sequence can be expressed as

$$X_k^{[D]}[n] = \begin{cases} X_k[m], & \text{if } n = mD \\ 0, & \text{else.} \end{cases} \tag{1}$$

The output sequence $\{S[n]\}_{n=0}^{L_M-1}$ of the pre-processing filters is

$$S[n] = \sum_{k=1}^{K} \left(X_k^{[D]} * g_k \right)[n] \tag{2}$$

where $L_M = (M-1)D + L$ is the length of the output sequence, "$*$" denotes the convolution operation. We assume that $X_k^{[D]}[n]$ is the unit power, so the transmission power is $P_s = \sum_{k=1}^{K} \boldsymbol{g}_k^{\mathrm{H}} \boldsymbol{g}_k$.

Denote the AN sequence as $\{q[n]\}_{n=0}^{L_M-1}$ and the power of AN as P_z. The transmitted sequence is $\{S[n] + q[n]\}_{n=0}^{L_M-1}$. The received signal at user k is the convolution of the transmitted sequence and CIR $h_k[n]$:

$$Y_k^{[D]}[n] = ((S+q) * h_k)[n] + \tilde{z}_k[n] = \left(\left(\sum_{i=1}^{K} \left(X_i^{[D]} * g_i \right) + q \right) * h_k \right)[n] + \tilde{z}_k[n] \tag{3}$$

where $\tilde{z}_k[n]$ is the additive white Gaussian noise (AWGN) sequence with mean zero and variance σ^2.

User k down-samples the received signal, that is, strips the Dth sample from each segment of length D as the sample of the symbol. The down-sampled sequence of user k can be expressed as

$$Y_k[m] = \sum_{i=1}^{K} \sum_{l=-L_D+1}^{L_D-1} \sum_{n=0}^{L-1} h_k[n] g_i[L-1-Dl-n] X_i[m+l] + \sum_{n=0}^{L-1} h_k[n] q[mD+L-1-n] + z_k[m] \tag{4}$$

where $L_D = \left\lfloor \dfrac{L-1}{D} \right\rfloor + 1$, $\lfloor \cdot \rfloor$ represents floor operation, $z_k[m] = \tilde{z}_k[Dm]$ is AWGN with mean zero and variance σ^2. Splitting $Y_k[m]$ into five parts, that is, signal, ISI, IUI, AN and noise, (4) can be re-expressed as

$$\begin{aligned} Y_k[m] = & \underbrace{\sum_{n=0}^{L-1} h_k[n] g_k[L-1-n] X_k[m]}_{\text{signal}} + \underbrace{\sum_{l=-L_D+1, l\neq 0}^{L_D-1} \sum_{n=0}^{L-1} h_k[n] g_k[L-1-Dl-n] X_k[m+l]}_{\text{ISI}} \\ & + \underbrace{\sum_{i=1, i\neq k}^{K} \sum_{l=-L_D+1}^{L_D-1} \sum_{n=0}^{L-1} h_k[n] g_i[L-1-Dl-n] X_i[m+l]}_{\text{IUI}} + \underbrace{\sum_{n=0}^{L-1} h_k[n] q[mD+L-1-n]}_{\text{AN}} + \underbrace{z_k[m]}_{\text{noise}} \end{aligned} \tag{5}$$

Define a $(2L-1) \times L$ Toeplitz matrix $\tilde{\boldsymbol{H}}_k$ as

$$\tilde{\boldsymbol{H}}_k = \begin{bmatrix} h_k[0] & 0 & 0 & \cdots & \cdots & 0 \\ h_k[1] & h_k[0] & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \cdots & \vdots \\ h_k[L-1] & h_k[L-2] & h_k[L-3] & \cdots & \cdots & h_k[0] \\ 0 & h_k[L-1] & h_k[L-2] & \cdots & \cdots & h_k[1] \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \cdots & h_k[L-1] \end{bmatrix} \tag{6}$$

Define the equivalent channel matrix $\boldsymbol{H}_k$ with dimension $(2L_D-1)\times L$ as

$$\begin{aligned}\boldsymbol{H}_k &= \sum_{l=-L_D+1}^{L_D-1} \tilde{\boldsymbol{e}}_{L_D+l}\boldsymbol{e}_{L+lD}^{\mathrm{T}}\tilde{\boldsymbol{H}}_k \\ &= \begin{bmatrix} h_k[D-1] & h_k[D-2] & \cdots & h_k[0] & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ h_k[2D-1] & h_k[2D-2] & \cdots & \cdots & \cdots & \cdots & h_k[0] & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ h_k[(L_D-1)D-1] & h_k[(L_D-1)D-2] & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & h_k[0] & 0 & \cdots & 0 \\ h_k[L-1] & h_k[L-2] & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & h_k[0] \\ 0 & h_k[L-1] & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & h_k[L-(L_D-1)D] \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & h_k[L-1] & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & h_k[L-2D] \\ 0 & 0 & \cdots & \cdots & 0 & h_k[L-1] & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & h_k[L-D] \end{bmatrix}\end{aligned} \tag{7}$$

where $\tilde{\boldsymbol{e}}_{L_D+l}$ is the (L_D+l)-th column of a $(2L_D-1)\times(2L_D-1)$ identity matrix, and $\boldsymbol{e}_{L+lD}$ is the $(L+lD)$-th column of a $(2L-1)\times(2L-1)$ identity matrix. The r-th row of $\boldsymbol{H}_k$ is actually the $(r\times D)$-th row of $\tilde{\boldsymbol{H}}_k$. In other words, $\boldsymbol{H}_k$ is obtained by extracting the first row of every D rows from matrix $\tilde{\boldsymbol{H}}_k$, starting from the L-th row. The $(2L_D-1)$ extracted rows form matrix $\boldsymbol{H}_k$.

By defining the equivalent channel matrix, and describing the input sequence of the channel as a vector, the convolution operation between the input sequence and the impulse response of the channel can be described as the multiplication of the equivalent channel matrix by the input sequence vector. So (5) can be rewritten in a matrix (vector) form, that is

$$\begin{aligned}Y_k[m] = &\underbrace{\left(\boldsymbol{h}_k^{(L_D)}\right)^{\mathrm{T}}\boldsymbol{g}_k X_k[m]}_{\text{signal}} + \underbrace{\sum_{l=-L_D+1,\, l\neq 0}^{L_D-1}\left(\boldsymbol{h}_k^{(L_D+l)}\right)^{\mathrm{T}}\boldsymbol{g}_k X_k[m+l]}_{\text{ISI}} \\ &+ \underbrace{\sum_{i=1,i\neq k}^{K}\sum_{l=-L_D+1}^{L_D-1}\left(\boldsymbol{h}_k^{(L_D+l)}\right)^{\mathrm{T}}\boldsymbol{g}_i X_i[m+l]}_{\text{IUI}} + \underbrace{\left(\boldsymbol{h}_{\mathrm{AN},k}^{(mD+L)}\right)^{\mathrm{T}}\boldsymbol{q}}_{\text{AN}} + \underbrace{z_k[m]}_{\text{noise}}\end{aligned} \tag{8}$$

where $\boldsymbol{h}_k^{(L_D)}$ and $\boldsymbol{h}_k^{(L_D+l)}$ are the transpose of the L_D-th and (L_D+l)-th rows of $\boldsymbol{H}_k$, respectively. $\boldsymbol{h}_{\mathrm{AN},k}^{(mD+L)}$ is the transpose of the $(mD+L)$-th row of $\tilde{\boldsymbol{H}}_{\mathrm{AN},k}$, where $\tilde{\boldsymbol{H}}_{\mathrm{AN},k}$ is an $(L_M+L-1)\times L_M$ Toeplitz matrix and its first column is $\left[\boldsymbol{h}_k^{\mathrm{T}}\ \boldsymbol{0}_{1\times(L_M-1)}^{\mathrm{T}}\right]^{\mathrm{T}}$, where $\boldsymbol{0}_{m\times n}$ is an $m\times n$ zero matrix. The expression of $\tilde{\boldsymbol{H}}_{\mathrm{AN},k}$ is

$$\tilde{\boldsymbol{H}}_{\mathrm{AN},k} = \begin{bmatrix} h_k[0] & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ h_k[1] & h_k[0] & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ h_k[L-1] & h_k[L-2] & h_k[L-3] & \cdots & h_k[0] & 0 & \cdots & \cdots & 0 \\ 0 & h_k[L-1] & \cdots & \cdots & h_k[1] & h_k[0] & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & \cdots & h_k[L-1] & h_k[L-2] & \cdots & \cdots & h_k[0] \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 & 0 & \cdots & \cdots & h_k[L-1] \end{bmatrix} \tag{9}$$

The SINR of the received signal of user k is

$$\gamma_k = \frac{\boldsymbol{g}_k^{\mathrm{H}}\boldsymbol{R}_k^{(1)}\boldsymbol{g}_k}{\boldsymbol{g}_k^{\mathrm{H}}\boldsymbol{R}_k^{(0)}\boldsymbol{g}_k + \sum_{i=1,i\neq k}^{K}\boldsymbol{g}_i^{\mathrm{H}}\boldsymbol{R}_k\boldsymbol{g}_i + \left(\boldsymbol{h}_{\mathrm{AN},k}^{(mD+L)}\right)^{\mathrm{H}}\boldsymbol{Q}\,\boldsymbol{h}_{\mathrm{AN},k}^{(mD+L)} + \sigma^2} \tag{10}$$

where $\boldsymbol{R}_k = \boldsymbol{H}_k^{\mathrm{H}}\boldsymbol{H}_k$, $\boldsymbol{R}_k^{(1)} = \boldsymbol{h}_k^{(L_D)}(\boldsymbol{h}_k^{(L_D)})^{\mathrm{H}}$, $\boldsymbol{R}_k^{(0)} = \boldsymbol{R}_k - \boldsymbol{R}_k^{(1)}$, $\boldsymbol{Q} = E\{\boldsymbol{q}\boldsymbol{q}^{\mathrm{H}}\}$. The first and second terms of the denominator in (10) represent the ISI power and the IUI power respectively, and the third term is the AN power.

When the channel bandwidth is B, the channel capacity from the transmitter to the legitimate user k is

$$C_k = \frac{B}{D}\log_2(1+\gamma_k) = \frac{B}{D}\log_2\left(1+\frac{\boldsymbol{g}_k^{\mathrm{H}}\boldsymbol{R}_k^{(1)}\boldsymbol{g}_k}{\boldsymbol{g}_k^{\mathrm{H}}\boldsymbol{R}_k^{(0)}\boldsymbol{g}_k + \sum_{i=1,i\neq k}^{K}\boldsymbol{g}_i^{\mathrm{H}}\boldsymbol{R}_k\boldsymbol{g}_i + \left(\boldsymbol{h}_{\mathrm{AN},k}^{(mD+L)}\right)^{\mathrm{H}}\boldsymbol{Q}\,\boldsymbol{h}_{\mathrm{AN},k}^{(mD+L)} + \sigma^2}\right) \tag{11}$$

Similar to the definition of the equivalent channel matrix of legitimate channels, we define the equivalent channel matrix of the eavesdropping channel transmitting the signal as

$$\boldsymbol{H}_{\mathrm{e}}=\begin{bmatrix} h_{\mathrm{e}}[0] & 0 & 0 & \cdots & \cdots & 0 \\ h_{\mathrm{e}}[1] & h_{\mathrm{e}}[0] & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \cdots & \vdots \\ h_{\mathrm{e}}[L-1] & h_{\mathrm{e}}[L-2] & h_{\mathrm{e}}[L-3] & \cdots & \cdots & h_{\mathrm{e}}[0] \\ 0 & h_{\mathrm{e}}[L-1] & h_{\mathrm{e}}[L-2] & \cdots & \cdots & h_{\mathrm{e}}[1] \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \cdots & h_{\mathrm{e}}[L-1] \end{bmatrix} \tag{12}$$

$\boldsymbol{H}_{\mathrm{e}}$ is a $(2L-1)\times L$ Toeplitz matrix, and its first column $\left[\boldsymbol{h}_{\mathrm{e}}^{\mathrm{T}}\ \boldsymbol{0}_{1\times(L-1)}^{\mathrm{T}}\right]^{\mathrm{T}}$. The equivalent channel matrix of the eavesdropping channel transmitting AN is

$$\boldsymbol{H}_{\mathrm{e},m}=[\boldsymbol{0}_{(2L-1)\times mD}\ \boldsymbol{I}_{(2L-1)}\ \boldsymbol{0}_{(2L-1)\times(M-m-1)D}]\tilde{\boldsymbol{H}}_{\mathrm{e}} \tag{13}$$

where $\boldsymbol{I}_{(N)}$ is an $N\times N$ identity matrix. $\tilde{\boldsymbol{H}}_{\mathrm{e}}$ is an $(L_M+L-1)\times L_M$ Toeplitz matrix and its first column is $[\boldsymbol{h}_{\mathrm{e}}^{\mathrm{T}}\ \boldsymbol{0}_{1\times(L_M-1)}^{\mathrm{T}}]^{\mathrm{T}}$, which has a form similar to $\boldsymbol{H}_{\mathrm{e}}$.

When evaluating the security performance of TR transmission, we consider the most detrimental case for security transmission. Similar to [17], we assume that the eavesdropper has an ideal processing capability: (1) the eavesdropper has a perfect equalizer and ISI can be completely eliminated; (2) the eavesdropper can utilize all the signal samples coming from all paths to obtain the information; (3) the eavesdropper can separate the signals sent to all users and there is no IUI. With these assumptions about the processing capability of the eavesdropper, the received signal of the eavesdropper can be expressed as

$$\boldsymbol{Y}_{\mathrm{e},m}=\boldsymbol{H}_{\mathrm{e}}\sum_{k=1}^{K}\boldsymbol{g}_k X_k[m]+\boldsymbol{H}_{\mathrm{e},m}\boldsymbol{q}+\boldsymbol{z}_{\mathrm{e}} \tag{14}$$

where $\boldsymbol{z}_{\mathrm{e}}=[z_{\mathrm{e}}[0],z_{\mathrm{e}}[1],\cdots,z_{\mathrm{e}}[2L-1]]^{\mathrm{T}}$, $z_{\mathrm{e}}[n]$ is an AWGN sequence with mean zero and variance σ^2. The first term in (14) is the desired signal without ISI or IUI, the second term is AN, and the third term is the channel noise.

When the channel bandwidth is B, the capacity of the eavesdropping channel is

$$C_{\mathrm{e}}=\frac{B}{D}\log_2(1+\gamma_{\mathrm{e}})=\frac{B}{D}\log_2\left(1+\sum_{k=1}^{K}(\boldsymbol{H}_{\mathrm{e}}\boldsymbol{g}_k)^H\left(\boldsymbol{H}_{\mathrm{e},m}\boldsymbol{Q}\,\boldsymbol{H}_{\mathrm{e},m}^{\mathrm{H}}+\sigma^2\boldsymbol{I}_{(2L-1)}\right)^{-1}\boldsymbol{H}_{\mathrm{e}}\boldsymbol{g}_k\right) \tag{15}$$

In this paper, achievable secrecy rate is used to evaluate the performance of the scheme. Achievable secrecy rate is a popular performance measure of PLS, which is defined as the difference between the rate of the legitimate receiver and that of the eavesdropper [19]. Based on (11) and (15), we can obtain the sum secrecy rate of the system when the channel bandwidth is B as

$$R_{\mathrm{s}}=\left[\sum_{k=1}^{K}C_k-C_{\mathrm{e}}\right]^{+} \tag{16}$$

where $[x]^{+}\triangleq\max\{0,x\}$.

3. Transmission scheme and optimization algorithm

3.1. Transmission scheme and optimization when ECSI is unavailable

When ECSI is unavailable, omnidirectional radiated AN is a rational choice. In order not to interfere with the legitimate users, AN is assigned in the null-space of the legitimate channels. Let $\boldsymbol{q}=\boldsymbol{W}\boldsymbol{v}$, where $\boldsymbol{v}$ is an independent and identically distributed Gaussian random vector, and the columns of $\boldsymbol{W}$ are the orthonormal bases of the null-space of the legitimate channel matrix $\boldsymbol{H}_{\mathrm{AN}}$. $\boldsymbol{H}_{\mathrm{AN}}$ is a $KM\times L_M$ matrix, defined as

$$\boldsymbol{H}_{\mathrm{AN}}=\begin{bmatrix}\boldsymbol{H}_{\mathrm{AN},1}^{\mathrm{T}} & \boldsymbol{H}_{\mathrm{AN},2}^{\mathrm{T}} & \cdots & \boldsymbol{H}_{\mathrm{AN},K}^{\mathrm{T}}\end{bmatrix}^{\mathrm{T}} \tag{17}$$

where

$$\boldsymbol{H}_{\mathrm{AN},k}=\begin{bmatrix}\boldsymbol{h}_{\mathrm{AN},k}^{(L)} & \boldsymbol{h}_{\mathrm{AN},k}^{(D+L)} & \cdots & \boldsymbol{h}_{\mathrm{AN},k}^{(mD+L)} & \cdots & \boldsymbol{h}_{\mathrm{AN},k}^{((M-1)D+L)}\end{bmatrix}^{\mathrm{T}} \tag{18}$$

In (18), $\boldsymbol{h}_{\mathrm{AN},k}^{(l)}$ is the transpose of the l-th row of $\tilde{\boldsymbol{H}}_{\mathrm{AN},k}$. It should be noted that the null-space of $\boldsymbol{H}_{\mathrm{AN}}$ exists when $L_M>KM$, which can be satisfied by setting the length of the information symbol sequence to an appropriate value. The auto-correlation matrix of $\boldsymbol{q}$ is

$$\boldsymbol{Q}=E\{\boldsymbol{q}\boldsymbol{q}^{\mathrm{H}}\}=\boldsymbol{W}\boldsymbol{v}\boldsymbol{v}\boldsymbol{W}^{\mathrm{H}}=\boldsymbol{W}\boldsymbol{V}\boldsymbol{W}^{\mathrm{H}} \tag{19}$$

where $\boldsymbol{V} = E\{\boldsymbol{v}\boldsymbol{v}^{\mathrm{H}}\} = \frac{P_z}{N_z}\boldsymbol{I}_{(N_z)}$, $N_z = L_M - M$. The total power is $P_{\max} = P_s + P_z$.

Since AN is located in the null-space of the legitimate channel $\boldsymbol{H}_{\mathrm{AN}}$, the AN term can be removed from (5), then the SINR of user k can be rewritten as

$$\gamma_k^{\mathrm{NS}} = \frac{\boldsymbol{g}_k^{\mathrm{H}}\boldsymbol{R}_k^{(1)}\boldsymbol{g}_k}{\boldsymbol{g}_k^{\mathrm{H}}\boldsymbol{R}_k^{(0)}\boldsymbol{g}_i + \sum_{i=1,i\neq k}^{K}\boldsymbol{g}_i^{\mathrm{H}}\boldsymbol{R}_k\boldsymbol{g}_i + \sigma^2} \tag{20}$$

Since the eavesdropping channel vector $\boldsymbol{h}_{\mathrm{e}}$ is unavailable for the transmitter, the capacity of the eavesdropping channel cannot be obtained, neither can the secrecy rate. Therefore, the secrecy rate maximization cannot be taken as the optimization goal. As an alternative, we choose a scheme similar to [17], which optimizes the IR of the pre-processing filter $\boldsymbol{g}_k$ ($k = 1, 2, \ldots, K$) to minimize the signal power P_{s} under the constraint that SINR at each user reaches its pre-defined target value. In this way, the power used for transmitting AN is maximized and the SINR of the eavesdropper is minimized with the limitation of the total power. The optimization problem can be expressed as

$$\begin{aligned} \min_{\substack{\boldsymbol{g}_k \\ k\in\{1,\cdots,K\}}} \quad & P_{\mathrm{s}} \\ \text{s.t.} \quad & \gamma_k^{\mathrm{NS}} \geq \tilde{\gamma}_k \\ & P_s \leq P_{\max} \end{aligned} \tag{21}$$

where $\tilde{\gamma}_k$ is the SINR target of user k.

Using the SINR expression (20), optimization problem (21) can be rewritten as

$$\begin{aligned} \min_{\substack{\boldsymbol{g}_k \\ k\in\{1,\cdots,K\}}} \quad & \sum_{k=1}^{K}\boldsymbol{g}_k^{\mathrm{H}}\boldsymbol{g}_k \\ \text{s.t.} \quad & \boldsymbol{g}_k^{\mathrm{H}}\boldsymbol{R}_k^{(1)}\boldsymbol{g}_k \geq \tilde{\gamma}_k\left(\boldsymbol{g}_k^{\mathrm{H}}\boldsymbol{R}_k^{(0)}\boldsymbol{g}_k + \sum_{i=1,i\neq k}^{K}\boldsymbol{g}_i^{\mathrm{H}}\boldsymbol{R}_k\boldsymbol{g}_i + \sigma^2\right) \\ & \sum_{k=1}^{K}\boldsymbol{g}_k^{\mathrm{H}}\boldsymbol{g}_k \leq P_{\max} \end{aligned} \tag{22}$$

Problem (22) is a non-convex problem. Letting $\boldsymbol{G}_k = \boldsymbol{g}_k\boldsymbol{g}_k^{\mathrm{H}}$, we rewrite (22) as

$$\begin{aligned} \min_{\substack{\boldsymbol{G}_k \\ k\in\{1,\cdots,K\}}} \quad & \sum_{k=1}^{K}\mathrm{Tr}(\boldsymbol{G}_k) \\ \text{s.t.} \quad & \mathrm{Tr}(\boldsymbol{R}_k^{(1)}\boldsymbol{G}_k) - \tilde{\gamma}_k(\mathrm{Tr}(\boldsymbol{R}_k^{(0)}\boldsymbol{G}_k) + \sum_{i=1,i\neq k}^{K}\mathrm{Tr}(\boldsymbol{R}_k\boldsymbol{G}_i)) \geq \tilde{\gamma}_k\sigma^2 \\ & \sum_{k=1}^{K}\mathrm{Tr}(\boldsymbol{G}_k) \leq P_{\max} \\ & \boldsymbol{G}_k \succeq 0 \\ & \mathrm{rank}(\boldsymbol{G}_k) = 1 \end{aligned} \tag{23}$$

where $\boldsymbol{G}_k \succeq 0$ means that $\boldsymbol{G}_k$ is a positive semidefinite matrix, $\mathrm{Tr}(\boldsymbol{A})$ denotes the trace of matrix $\boldsymbol{A}$, and $\mathrm{rank}(\boldsymbol{A})$ denotes the rank of matrix $\boldsymbol{A}$. Due to the rank 1 constraint of $\boldsymbol{G}_k$, optimization problem (23) is still a non-convex problem. We adopt semidefinite relaxation (SDR) to remove the rank 1 constraint in the problem and convert it to a semidefinite program (SDP) problem. After removing the constraint of rank 1, (23) can be rewritten as

$$\begin{aligned} \min_{\substack{\boldsymbol{G}_k \\ k\in\{1,\cdots,K\}}} \quad & \sum_{k=1}^{K}\mathrm{Tr}(\boldsymbol{G}_k) \\ \text{s.t.} \quad & \mathrm{Tr}(\boldsymbol{R}_k^{(1)}\boldsymbol{G}_k) - \tilde{\gamma}_k(\mathrm{Tr}(\boldsymbol{R}_k^{(0)}\boldsymbol{G}_k) + \sum_{i=1,i\neq k}^{K}\mathrm{Tr}(\boldsymbol{R}_k\boldsymbol{G}_i)) \geq \tilde{\gamma}_k\sigma^2 \\ & \sum_{k=1}^{K}\mathrm{Tr}(\boldsymbol{G}_k) \leq P_{\max} \\ & \boldsymbol{G}_k \succeq 0 \end{aligned} \tag{24}$$

Problem (24) is now a convex optimization problem, which can be solved by using the CVX optimization toolbox. Although problem (24) ignores the rank 1 constraint of $\boldsymbol{G}_k$, by examining the Karush-Kuhn-Tucker (KKT) condition of optimization problem (24), it can be proved that the optimal solution $\boldsymbol{G}_k^{\mathrm{o}}$ to the above optimization problem must satisfy the condition that the number of its non-zero

eigenvalues is 1, so the rank 1 constraint of $\boldsymbol{G}_k$ is met. The solution to (22) $\boldsymbol{g}_k^o$ is the principal eigenvector of $\boldsymbol{G}_k^o$ multiplied by the square root of its principal eigenvalue.

Theorem 1. *The optimal solution $\boldsymbol{G}_k^o$ to problem (24) satisfies rank$(\boldsymbol{G}_k^o) = 1$, $\forall k$.*

For the proof of Theorem 1, please refer to Appendix.

3.2. Transmission scheme and optimization when ECSI is available

When ECSI is available, that is, $\boldsymbol{h}_e$ is known, we can optimize the IR of the pre-processing filter $\boldsymbol{g}_k$ $(k = 1, 2, \ldots, K)$ and AN covariance $\boldsymbol{Q} = E\{\boldsymbol{q}\boldsymbol{q}^H\}$ to maximize the sum secrecy rate, which enables the system to achieve a better security transmission performance than the null-space AN scheme. The optimization problem can be expressed as

$$\begin{aligned} \max_{\substack{\boldsymbol{g}_k, \boldsymbol{Q} \\ k\in\{1,\cdots,K\}}} \quad & R_s \\ \text{s.t.} \quad & P_s + P_z \le P_{\max} \end{aligned} \tag{25}$$

where R_s is the achievable sum secrecy rate and is defined in (16). Substituting (11), (15) and (16) into (25), optimization problem (25) can be rewritten as

$$\begin{aligned} \max_{\substack{\boldsymbol{g}_k, \boldsymbol{Q} \\ k\in\{1,\cdots,K\}}} \quad & \sum_{k=1}^{K} \log_2 \left(1 + \frac{\boldsymbol{g}_k^H \boldsymbol{R}_k^{(1)} \boldsymbol{g}_k}{\boldsymbol{g}_k^H \boldsymbol{R}_k^{(0)} \boldsymbol{g}_k + \sum\limits_{i=1, i\neq k}^{K} \boldsymbol{g}_i^H \boldsymbol{R}_k \boldsymbol{g}_i + \left(\boldsymbol{h}_{\mathrm{AN},k}^{(mD+L)}\right)^H \boldsymbol{Q}\, \boldsymbol{h}_{\mathrm{AN},k}^{(mD+L)} + \sigma^2} \right) \\ & - \log_2 \left(1 + \sum_{k=1}^{K} (\boldsymbol{H}_e \boldsymbol{g}_k)^H \left(\boldsymbol{H}_{e,m} \boldsymbol{Q}\, \boldsymbol{H}_{e,m}^H + \sigma^2 \boldsymbol{I}_{(2L-1)} \right)^{-1} \boldsymbol{H}_e \boldsymbol{g}_k \right) \\ \text{s.t.} \quad & \sum_{k=1}^{K} \mathrm{Tr}(\boldsymbol{g}_k \boldsymbol{g}_k^H) + \mathrm{Tr}(\boldsymbol{Q}) \le P_{\max} \end{aligned} \tag{26}$$

(26) can be further rewritten as

$$\begin{aligned} \max_{\substack{\boldsymbol{G}_k, \boldsymbol{Q} \\ k\in\{1,\cdots,K\}}} \quad & \log_2 \left(\prod_{k=1}^{K} \frac{\sum\limits_{i=1}^{K} \mathrm{Tr}(\boldsymbol{R}_k \boldsymbol{G}_i) + \mathrm{Tr}(\boldsymbol{R}_{\mathrm{AN},k} \boldsymbol{Q}) + \sigma^2}{\mathrm{Tr}(\boldsymbol{R}_k^{(0)} \boldsymbol{G}_k) + \sum\limits_{i=1, i\neq k}^{K} \mathrm{Tr}(\boldsymbol{R}_k \boldsymbol{G}_i) + \mathrm{Tr}(\boldsymbol{R}_{\mathrm{AN},k} \boldsymbol{Q}) + \sigma^2} \right) \\ & - \log_2 \left(\frac{\sum\limits_{k=1}^{K} \mathrm{Tr}(\boldsymbol{R}_e \boldsymbol{G}_k) + \mathrm{Tr}(\boldsymbol{R}_{e,m} \boldsymbol{Q}) + \mathrm{Tr}\left(\sigma^2 \boldsymbol{I}_{(2L-1)}\right)}{\mathrm{Tr}(\boldsymbol{R}_{e,m} \boldsymbol{Q}) + \mathrm{Tr}\left(\sigma^2 \boldsymbol{I}_{(2L-1)}\right)} \right) \\ \text{s.t.} \quad & \sum_{k=1}^{K} \mathrm{Tr}(\boldsymbol{G}_k) + \mathrm{Tr}(\boldsymbol{Q}) \le P_{\max} \\ & \boldsymbol{G}_k \succeq 0 \\ & \boldsymbol{Q} \succeq 0 \\ & \mathrm{rank}(\boldsymbol{G}_k) = 1 \end{aligned} \tag{27}$$

where $\boldsymbol{R}_{\mathrm{AN},k} = \boldsymbol{h}_{\mathrm{AN},k}^{(mD+L)} \left(\boldsymbol{h}_{\mathrm{AN},k}^{(mD+L)}\right)^H$, $\boldsymbol{R}_e = (\boldsymbol{H}_e)^H \boldsymbol{H}_e$, $\boldsymbol{R}_{e,m} = \left(\boldsymbol{H}_{e,m}\right)^H \boldsymbol{H}_{e,m}$.

To solve the optimization problem, we first replace the items of the objective function in (27) by exponential variables as follows

$$e^{u_k} = \sum_{i=1}^{K} \mathrm{Tr}(\boldsymbol{R}_k \boldsymbol{G}_i) + \mathrm{Tr}(\boldsymbol{R}_{\mathrm{AN},k} \boldsymbol{Q}) + \sigma^2 \tag{28}$$

$$e^{s_k} = \mathrm{Tr}(\boldsymbol{R}_k^{(0)} \boldsymbol{G}_k) + \sum_{i=1, i\neq k}^{K} \mathrm{Tr}(\boldsymbol{R}_k \boldsymbol{G}_i) + \mathrm{Tr}(\boldsymbol{R}_{\mathrm{AN},k} \boldsymbol{Q}) + \sigma^2 \tag{29}$$

$$e^{v} = \sum_{k=1}^{K} \mathrm{Tr}(\boldsymbol{R}_e \boldsymbol{G}_k) + \mathrm{Tr}(\boldsymbol{R}_{e,m} \boldsymbol{Q}) + \mathrm{Tr}\left(\sigma^2 \boldsymbol{I}_{(2L-1)}\right) \tag{30}$$

$$\mathrm{e}^{t} = \mathrm{Tr}(\boldsymbol{R}_{\mathrm{e},m}\boldsymbol{Q}) + \mathrm{Tr}\left(\sigma^2 \boldsymbol{I}_{(2L-1)}\right) \tag{31}$$

for $k = 1, \ldots, K$. Note that $\mathrm{Tr}(\boldsymbol{R}_k \boldsymbol{G}_i) \geq 0$, $\mathrm{Tr}(\boldsymbol{R}_k^{(0)} \boldsymbol{G}_k) \geq 0$, $\mathrm{Tr}(\boldsymbol{R}_{\mathrm{e}} \boldsymbol{G}_k) \geq 0$, $\mathrm{Tr}(\boldsymbol{R}_{\mathrm{AN},k}\boldsymbol{Q}) \geq 0$, $\mathrm{Tr}(\boldsymbol{R}_{\mathrm{e},m}\boldsymbol{Q}) \geq 0$, so $\mathrm{e}^{u_k} \geq \sigma^2$, $\mathrm{e}^{s_k} \geq \sigma^2$, $\mathrm{e}^{v} \geq \mathrm{Tr}(\sigma^2 \boldsymbol{I})$, $\mathrm{e}^{t} \geq \mathrm{Tr}(\sigma^2 \boldsymbol{I})$. Due to the total power constraint, e^{u_k}, e^{s_k}, e^{v} and e^{t} are finite. So are u_k, s_k, v and t.

Substituting (28)–(31) into (27), based on the properties of exponential function and logarithmic function, the objective function in (27) can be written as

$$\sum_{k=1}^{K} \log_2 \mathrm{e}^{(u_k - s_k)} - \log_2 \mathrm{e}^{(v-t)} = \left(\sum_{k=1}^{K}(u_k - s_k) - (v-t)\right)\log_2 \mathrm{e} \tag{32}$$

Since $\log_2 \mathrm{e}$ is a positive constant number, it can be neglected in the optimization process, the objective function can be rewritten as $\zeta(u_k, s_k, v, t) = \sum_{k=1}^{K}(u_k - s_k) - (v-t)$. The maximization of the sum secrecy rate can be realized by maximizing e^{u_k} and e^{t}, which are the lower bound of the numerator of the legitimate channel capacity and the denominator of the eavesdropping channel capacity respectively, while minimizing e^{s_k} and e^{v}, which are the upper bound of the denominator of the legitimate channel capacity and the numerator of the eavesdropping channel capacity respectively. So we construct unequal constraint for u_k, s_k, v and t according to (28)–(31), respectively. Furthermore, by utilizing SDR technique through defining relaxation variables $\boldsymbol{u} = [u_1, \ldots, u_K]^{\mathrm{T}}$ and $\boldsymbol{s} = [s_1, \ldots, s_K]^{\mathrm{T}}$, and optimizing variable set $\{\boldsymbol{G}_k, \boldsymbol{Q}, \boldsymbol{u}, \boldsymbol{s}, v, t\}$, the rank 1 constraint of $\boldsymbol{G}_k$ is removed, so optimization problem (27) can be rewritten as

$$\begin{aligned}
\max_{\substack{u_k, s_k, v, t, \boldsymbol{G}_k, \boldsymbol{Q} \\ k\in\{1,\cdots,K\}}} \quad & \zeta(u_k, s_k, v, t) \\
\text{s.t.} \quad & \sum_{i=1}^{K} \mathrm{Tr}(\boldsymbol{R}_k \boldsymbol{G}_i) + \mathrm{Tr}(\boldsymbol{R}_{\mathrm{AN},k}\boldsymbol{Q}) + \sigma^2 \geq \mathrm{e}^{u_k} && \text{(a)} \\
& \mathrm{Tr}(\boldsymbol{R}_k^{(0)} \boldsymbol{G}_k) + \sum_{i=1, i\neq k}^{K} \mathrm{Tr}(\boldsymbol{R}_k \boldsymbol{G}_i) + \mathrm{Tr}(\boldsymbol{R}_{\mathrm{AN},k}\boldsymbol{Q}) + \sigma^2 \leq \mathrm{e}^{s_k} && \text{(b)} \\
& \sum_{k=1}^{K} \mathrm{Tr}(\boldsymbol{R}_{\mathrm{e}} \boldsymbol{G}_k) + \mathrm{Tr}(\boldsymbol{R}_{\mathrm{e},m}\boldsymbol{Q}) + \mathrm{Tr}\left(\sigma^2 \boldsymbol{I}_{(2L-1)}\right) \leq \mathrm{e}^{v} && \text{(c)} \\
& \mathrm{Tr}(\boldsymbol{R}_{\mathrm{e},m}\boldsymbol{Q}) + \mathrm{Tr}\left(\sigma^2 \boldsymbol{I}_{(2L-1)}\right) \geq \mathrm{e}^{t} && \text{(d)} \\
& \sum_{k=1}^{K} \mathrm{Tr}(\boldsymbol{G}_k) + \mathrm{Tr}(\boldsymbol{Q}) \leq P_{\max} && \text{(e)} \\
& \boldsymbol{G}_k \succeq 0,\ \boldsymbol{Q} \succeq 0 && \text{(f)}
\end{aligned} \tag{33}$$

The objective function in (33) is now convex. The constraints (33-b) and (33)-c) in problem (33) are non-convex, so optimization problem (33) is still difficult to solve. Assuming that $\bar{\boldsymbol{G}}_k$ $(k = 1, 2, \ldots, K)$ and $\bar{\boldsymbol{Q}}$ are the possible solutions to problem (33) and taking a simple transform, we get

$$\bar{s}_k = \ln\left(\mathrm{Tr}(\boldsymbol{R}_k^{(0)}\bar{\boldsymbol{G}}_k) + \sum_{i=1, i\neq k}^{K} \mathrm{Tr}(\boldsymbol{R}_k \bar{\boldsymbol{G}}_k) + \mathrm{Tr}(\boldsymbol{R}_{\mathrm{AN},k}\bar{\boldsymbol{Q}}) + \sigma^2\right) \tag{34}$$

$$\bar{v} = \ln\left(\sum_{k=1}^{K} \mathrm{Tr}(\boldsymbol{R}_{\mathrm{e}}\bar{\boldsymbol{G}}_k) + \mathrm{Tr}(\boldsymbol{R}_{\mathrm{e},m}\bar{\boldsymbol{Q}}) + \mathrm{Tr}\left(\sigma^2 \boldsymbol{I}_{(2L-1)}\right)\right) \tag{35}$$

$\bar{s}_k$ and $\bar{v}$ are possible optimization point for problem (33). Then we adopt a method similar to that used in [20] and [21] to convert (33-b) and (33-c) into convex constraints. The basic idea is to approximate the exponent function on the right-hand side of (33-b) and (33-c) with its first-order Taylor expansion, which is the affine function of optimization variables, so that (33-b) and (33-c) are converted into convex constraints. The Taylor series of function $f(x)$ at point x_0 is $\sum_{n=0}^{\infty} \frac{f^{(n)}(x_0)}{n!}(x - x_0)^n$, so the first-order Taylor expansions of e^{s_k} and e^{v} at points $\bar{s}_k$ and $\bar{v}$ are

$$\mathrm{e}^{s_k} = \mathrm{e}^{\bar{s}_k}(s_k - \bar{s}_k + 1) \tag{36}$$

$$\mathrm{e}^{v} = \mathrm{e}^{\bar{v}}(v - \bar{v} + 1) \tag{37}$$

By approximating the exponent function on the right-hand side of constraints (33-b) and (33-c) with their first-order Taylor expansions, (33) can be transformed into

$$
\begin{aligned}
\max_{\substack{u_k,s_k,v,t,\boldsymbol{G}_k,\boldsymbol{Q}\\ k\in\{1,\cdots,K\}}} \quad & \zeta(u_k,s_k,v,t) \\
\text{s.t.} \quad & \sum_{i=1}^{K}\mathrm{Tr}(\boldsymbol{R}_k\boldsymbol{G}_i)+\mathrm{Tr}(\boldsymbol{R}_{\mathrm{AN},k}\boldsymbol{Q})+\sigma^2\geq \mathrm{e}^{u_k} && \text{(a)} \\
& \mathrm{Tr}(\boldsymbol{R}_k^{(0)}\boldsymbol{G}_k)+\sum_{i=1,i\neq k}^{K}\mathrm{Tr}(\boldsymbol{R}_k\boldsymbol{G}_i)+\mathrm{Tr}(\boldsymbol{R}_{\mathrm{AN},k}\boldsymbol{Q})+\sigma^2\leq \mathrm{e}^{\bar{s}_k}(s_k-\bar{s}_k+1) && \text{(b)} \\
& \sum_{k=1}^{K}\mathrm{Tr}(\boldsymbol{R}_{\mathrm{e}}\boldsymbol{G}_k)+\mathrm{Tr}(\boldsymbol{R}_{e,m}\boldsymbol{Q})+\mathrm{Tr}\left(\sigma^2\boldsymbol{I}_{(2L-1)}\right)\leq \mathrm{e}^{\bar{v}}(v-\bar{v}+1) && \text{(c)} \\
& \mathrm{Tr}(\boldsymbol{R}_{\mathrm{e},m}\boldsymbol{Q})+\mathrm{Tr}\left(\sigma^2\boldsymbol{I}_{(2L-1)}\right)\geq \mathrm{e}^{t} && \text{(d)} \\
& \sum_{k=1}^{K}\mathrm{Tr}(\boldsymbol{G}_k)+\mathrm{Tr}(\boldsymbol{Q})\leq P_{\max} && \text{(e)} \\
& \boldsymbol{G}_k\succeq 0,\ \boldsymbol{Q}\succeq 0 && \text{(f)}
\end{aligned}
\tag{38}
$$

Problem (38) is a convex optimization problem which can be efficiently solved by using the CVX optimization toolbox. If the optimal $\boldsymbol{G}_k$ $(k=1,2,\ldots,K)$ satisfies the rank 1 constraint, we can take the eigenvalue decomposition for $\boldsymbol{G}_k$ $(k=1,2,\ldots,K)$ to obtain the optimal solution $\boldsymbol{g}_k$ $(k=1,2,\ldots,K)$ to the original problem (26). If the optimal $\boldsymbol{G}_k$ $(k=1,2,\ldots,K)$ does not satisfy the rank 1 constraint, we can use a randomization method to obtain the optimal solution to the original problem (26) [22]. The goal of the randomization method here is to get vector $\boldsymbol{g}_k$ which satisfies $E[\boldsymbol{g}_k\boldsymbol{g}_k^{\mathrm{H}}]=\boldsymbol{G}_k$ when the rank of matrix $\boldsymbol{G}_k$ is not 1. The specific steps are as follows. First, we take the eigenvalues decomposition for $\boldsymbol{G}_k$ and get $\boldsymbol{G}_k=\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{U}^{\mathrm{H}}$, where $\boldsymbol{U}$ is a unitary matrix and $\boldsymbol{\Sigma}$ is a diagonal matrix composed of the eigenvalues of $\boldsymbol{G}_k$. Then let $\boldsymbol{g}_k=\boldsymbol{U}\boldsymbol{\Sigma}^{1/2}\boldsymbol{v}_k$, where $\boldsymbol{v}_k$ is a vector composed of circular symmetric complex Gaussian (CSCG) random variables with zero mean and unit variance (Here $\boldsymbol{g}_k$ is a random vector, so we call the method randomization method). It is easy to verify that $E[\boldsymbol{g}_k\boldsymbol{g}_k^{\mathrm{H}}]=\boldsymbol{G}_k$. Finally, $\boldsymbol{g}_k$ is scaled to satisfy the constraint of the power.

The solution to (38) is based on the Taylor expansions of e^{s_k} and e^{v} at points $\bar{s}_k$ and $\bar{v}$, which is an approximate optimal solution. $\bar{s}_k$ and $\bar{v}$ are the possible optimization points and are defined in (34) and (35) respectively. To further improve the accuracy of the approximation, an iteration process is required. The optimal solution to problem (38) in the j-th iteration is denoted by $\{\boldsymbol{G}_k^{(j)},\boldsymbol{Q}^{(j)},u_k^{(j)},s_k^{(j)},v^{(j)},t^{(j)},k=1,\ldots,K\}$. First, we give a set of feasible initial vectors $\{\boldsymbol{g}_k^{(0)}\}_{k=1}^{K}$ and $\boldsymbol{q}^{(0)}$ to obtain $\{\bar{\boldsymbol{G}}_k\}_{k=1}^{K}$ and $\bar{\boldsymbol{Q}}$, and bring them into (34) and (35) to obtain $\{\bar{s}_k^{(1)}\}_{k=1}^{K}$ and $\bar{v}^{(1)}$. Then we substitute $\{\bar{s}_k^{(1)}\}_{k=1}^{K}$ and $\bar{v}^{(1)}$ into (38-b) and (38-c) and use the CVX toolbox to solve problem (38), obtaining solution $\{\boldsymbol{G}_k^{(1)}\}_{k=1}^{K}$, $\boldsymbol{Q}^{(1)}$, $\{s_k^{(1)}\}_{k=1}^{K}$ and $v^{(1)}$. Now the first round of the iteration is completed. In the second round, we update $\{\bar{s}_k^{(2)}\}_{k=1}^{K}$ and $\bar{v}^{(2)}$ with the solution to the first round $\{s_k^{(1)}\}_{k=1}^{K}$ and $v^{(1)}$ respectively, that is, $\{\bar{s}_k^{(2)}\}_{k=1}^{K}=\{s_k^{(1)}\}_{k=1}^{K}$, $\bar{v}^{(2)}=v^{(1)}$. Then the CVX toolbox is used to solve problem (38) to obtain $\{\boldsymbol{G}_k^{(2)}\}_{k=1}^{K}$, $\boldsymbol{Q}^{(2)}$, $\{s_k^{(2)}\}_{k=1}^{K}$ and $v^{(2)}$. In the third round, let $\{\bar{s}_k^{(3)}\}_{k=1}^{K}=\{s_k^{(2)}\}_{k=1}^{K}$ and $\bar{v}^{(3)}=v^{(2)}$, and the optimization problem can be solved. Repeat the above iteration process until the difference between the values of the objective function of (38) in two successive iterations is smaller than a predetermined positive value ε (we call it convergence factor), that is, $\left|\zeta^{(j)}-\zeta^{(j-1)}\right|<\varepsilon$, where $\zeta^{(j)}=\sum_{k=1}^{K}\left(u_k^{(j)}-s_k^{(j)}\right)-\left(v^{(j)}-t^{(j)}\right)$ is the value of the objective function in the j-th round of the iteration. The iterative algorithm is summarized in Algorithm 1.

It needs to be noted that the randomly generated initial vectors $\{\boldsymbol{g}_k^{(0)}\}_{k=1}^{K}$ and $\boldsymbol{q}^{(0)}$ at the beginning of the iteration should be checked to see whether they are suitable for starting the iteration process. The requirement is that the solution to the first round of the iteration $u_k^{(1)}$, $s_k^{(1)}$, $v^{(1)}$ and $t^{(1)}$ should be larger than zero. If one of $u_k^{(1)}$, $s_k^{(1)}$, $v^{(1)}$ and $t^{(1)}$ is negative or zero, the random generation process of $\{\boldsymbol{g}_k^{(0)}\}_{k=1}^{K}$ and $\boldsymbol{q}^{(0)}$ needs to be repeated.

Algorithm 1 Iterative algorithm for solving problem (38).

1) Generate feasible initial vector $\{\boldsymbol{g}_k^{(0)}\}_{k=1}^{K}$ and $\boldsymbol{q}^{(0)}$.
2) Calculate $\bar{\boldsymbol{G}}_k=\boldsymbol{g}_k^{(0)}(\boldsymbol{g}_k^{(0)})^{\mathrm{H}}$ and $\bar{\boldsymbol{Q}}=\boldsymbol{q}^{(0)}(\boldsymbol{q}^{(0)})^{\mathrm{H}}$; calculate $\bar{s}_k^{(1)}$ and $\bar{v}^{(1)}$ according to (34) and (35).
3) **Loop:**
4) Solve problem (38) to obtain $\{\boldsymbol{G}_k^{(j)}\}_{k=1}^{K}$, $\boldsymbol{Q}^{(j)}$, $s_k^{(j)}$ and $\boldsymbol{v}^{(j)}$.
5) $j:=j+1$
6) Update the initial value $\bar{s}_k^{(j)}=s_k^{(j-1)}$ and $\bar{v}^{(j)}=v^{(j-1)}$;
7) Calculate the objective function value $\zeta^{(j)}=\sum_{k=1}^{K}\left(u_k^{(j)}-s_k^{(j)}\right)-(v^{(j)}-t^{(j)})$
8) **If** $\left|\zeta^{(j)}-\zeta^{(j-1)}\right|\leq\varepsilon$ **then** break
else go to step 4 to continue the iteration.
9) Output the optimal solution $\{\boldsymbol{G}_k\}_{k=1}^{K}$ and $\boldsymbol{Q}$.
10) When rank($\boldsymbol{G}_k$)=1, obtain $\boldsymbol{g}_k$ by utilizing eigenvalue decomposition;
Otherwise, obtain $\boldsymbol{g}_k$ by utilizing the randomization method.

4. Simulation results

This section verifies the performance of the proposed scheme by simulations. The data of the secrecy rate given in the simulation diagram is the average value of the secrecy rates under 1×10^5 channel realizations. In the simulation, we set the number of paths

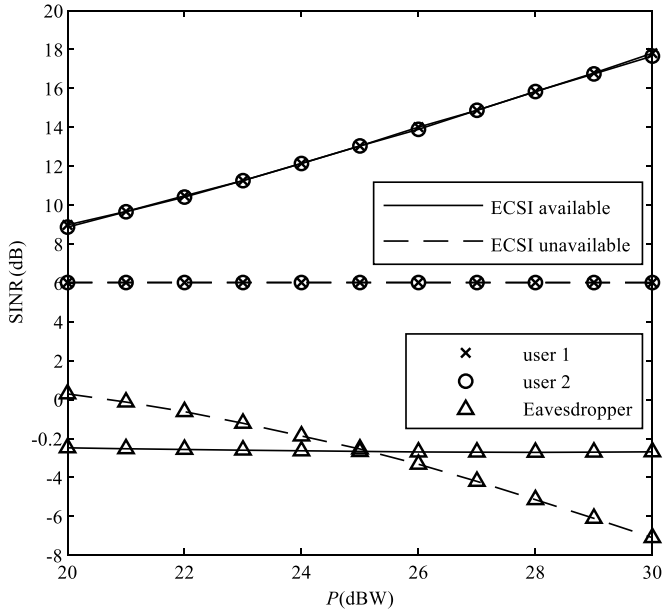

Fig. 2. SINR versus the total power, $D = 4$.

$L = 10$, the number of users $K = 2$, and the channel bandwidth $B = 1$ MHz. The channels are Rayleigh fading channel, the coefficient of CIR is a complex Gaussian random variable with zero mean, and the variance is

$$E\left[|h_k[n]|^2\right] = e^{-\frac{nT_S}{\sigma_T}} \tag{39}$$

where $\sigma_T = 10/B = 10^{-5}$ s is the root mean square delay of the path, and $T_s = 1/B$ is the sampling period. Channel AWGN power σ^2 is normalized to 1 W. When ECSI is unavailable, the legitimate user's SINR target threshold is $\tilde{\gamma}_k = 6$ dB, $k = 1, \ldots, K$. When ECSI is available, the convergence factor in the iterative algorithm is $\varepsilon = 1 \times 10^{-4}$.

Fig. 2 is the simulation results of the average SINR of the received signal at the legitimate users and that at the eavesdropper with or without ECSI. The up-sampled factor D is 4 in the simulation. The algorithm aims to minimize the signal transmission power under the constraint that the SINR of the two users is not less than the target threshold when ECSI is unavailable. The values of the legitimate users' SINR remains 6 dB when the total available power changes from 20 dBW to 30 dBW, which are just the target threshold. The results show that the SINR constraint is satisfied. The eavesdropper's SINR decreases with the increase of the total power. This is because when the total power increases, the signal power does not increase significantly because the SINR target threshold of the legitimate users is fixed, and almost all increased power is used in the transmission of AN. Therefore, the SINR of the eavesdropper decreases as the power increases. When ECSI is available, the SINR of the legitimate users increases rapidly with the increase of the total power, while the SINR of the eavesdropper almost remains unchanged. This means that when the total power increases, the increased power is allocated to both the signal and AN, so the power of the received signal and AN at the eavesdropper increase synchronously and SINR is almost unchanged. The legitimate users' SINRs increase because the pre-processing filters and AN have been optimized and the received signal's power increases at a higher speed than the AN power.

Fig. 3 compares the sum secrecy rate between the proposed scheme with the traditional TR scheme with or without AN. The up-sampled factor D is 4 in the simulation. "Traditional TR" adopts the traditional TR pre-processing filter, that is, $\boldsymbol{g}_k^{\mathrm{TR}} = \boldsymbol{h}_k^{(L_D)}/\|\boldsymbol{h}_k^{(L_D)}\|$, and "Traditional TR-AN" adopts the same traditional TR pre-processing filter accompanied by the null-space AN, where the signal power and the AN power are the same as those in our algorithm when ECSI is unavailable. It can be seen that the sum secrecy rate of the proposed scheme, even when ECSI is unavailable, is significantly better than that of the two traditional TR schemes, which proves that the optimization of TR pre-processing filters can greatly improve the security performance of the system, even when the eavesdropper has a super capability to completely eliminate ISI and IUI. The secrecy rate when ESCI is available is higher and increases faster with the increase of the transmission power than when ESCI is unavailable, which means that the joint optimization of the TR pre-processing filters and AN can improve the security performance more significantly. Comparing the secrecy rates of the two traditional TR schemes, we can find that the secrecy rate can increase as the transmission power increases when AN is adopted. Otherwise, the secrecy rate decreases. The reason is explained as follows. There are ISI and IUI in the received signal of the legitimate users in traditional TR schemes. When the transmission power is large, the interference power (including the ISI power and IUI power) is relatively larger than the channel noise power. With the increase of the transmission power, both the signal power and the interference power increase synchronously, so SINR almost remains unchanged when the transmission power increases, and the capacity of the legitimate channel does not increase significantly. On the other hand, it is assumed that all ISIs and IUIs in the received signal of the eavesdropper can be eliminated, so the SINR of the eavesdropper can continue to increase as the transmission power increases if AN does not exist, and the capacity of the eavesdropping channel increases too. So, the secrecy rate will decrease with the increase of the transmission power. The results also prove that the use of AN can significantly improve the security performance.

Fig. 4 and Fig. 5 show the simulation results of the channel capacity of the legitimate channel and that of the eavesdropping channel, and the sum secrecy rate with different up-sampled factor D when ECSI is unavailable respectively. It can be seen from Fig. 4 that the D times of the legitimate channel capacity does not change under different D values, nor does it change with the change of the transmission

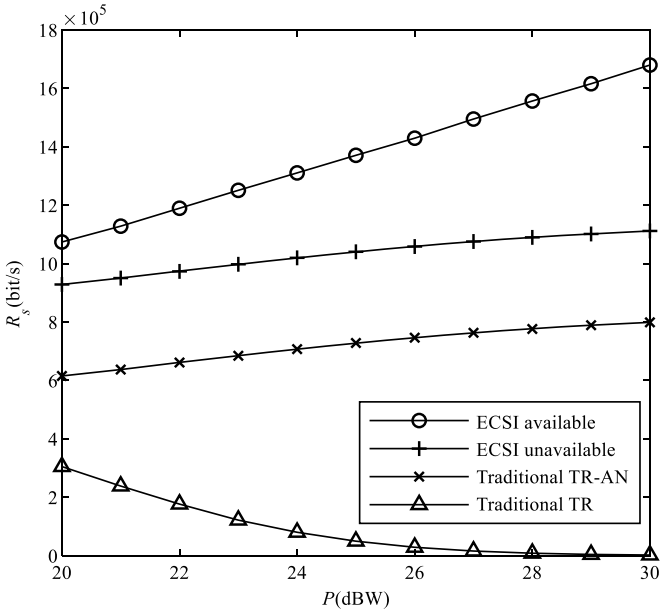

Fig. 3. Sum secrecy rate versus the total transmission power, $D = 4$.

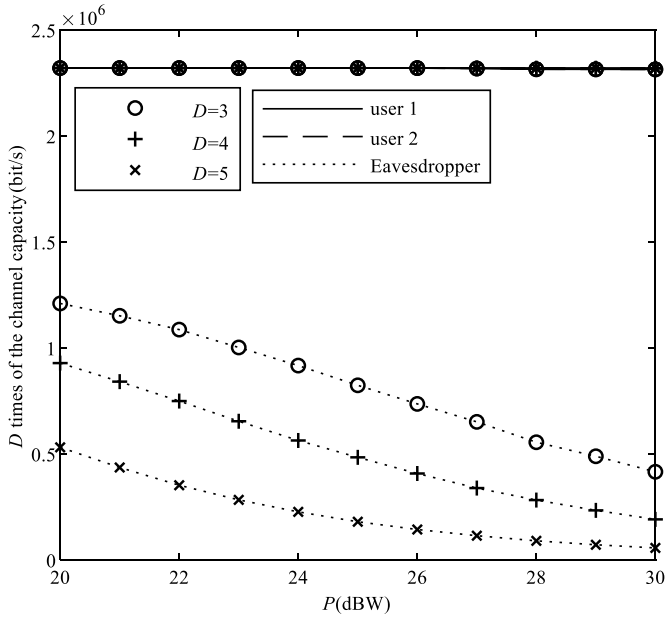

Fig. 4. Channel capacity with different up-sampled factors when ECSI is unavailable.

power. The constraint in the optimization in this case is that the SINR of each user is not less than the target threshold, so the SINR of all users remains on the threshold value even when the transmission power or the up-sampled factor is changing. As a result, the mutual information obtained from each received symbol by the legitimate users remains a constant.[1] So the D times of the legitimate channel capacity does not change with the D value or the transmission power. Since increasing D can reduce ISI, so the signal power can be reduced under the same SINR requirement, and there is more power to send AN. As a result, the received signal's SINR at the eavesdropper is reduced, and the mutual information of each output symbol of the eavesdropping channel decreases, so the D times of the eavesdropping channel capacity decreases as D increases. So, the amount of the confidential information carried by each symbol, which is the difference between the mutual information obtained by the legitimate receiver and that obtained by the eavesdropper, increases with the increase of the up-sampled factor. Therefore, without taking into account the reduction in channel utilization efficiency by increasing the up-sampled factor, the secrecy performance (i.e. the D times of the secrecy rare) of the system will increase as the up-sampled factor increases, as is shown in Fig. 5(a). However, when the up-sampled factor increases to D, the symbol rate decreases to $1/D$ of the un-up-sampled system under the same bandwidth, as is illustrated in (11) and (15). The increase in the amount of the information carried by each symbol brought about by the alleviation of ISI and IUI cannot compensate for the decrease in the symbol rate,

[1] The formula of the mutual information is $I(X;Y) = \frac{1}{2}\log_2(1+\gamma)$, where X and Y are input symbol and output symbol of the channel respectively, and γ is SINR.

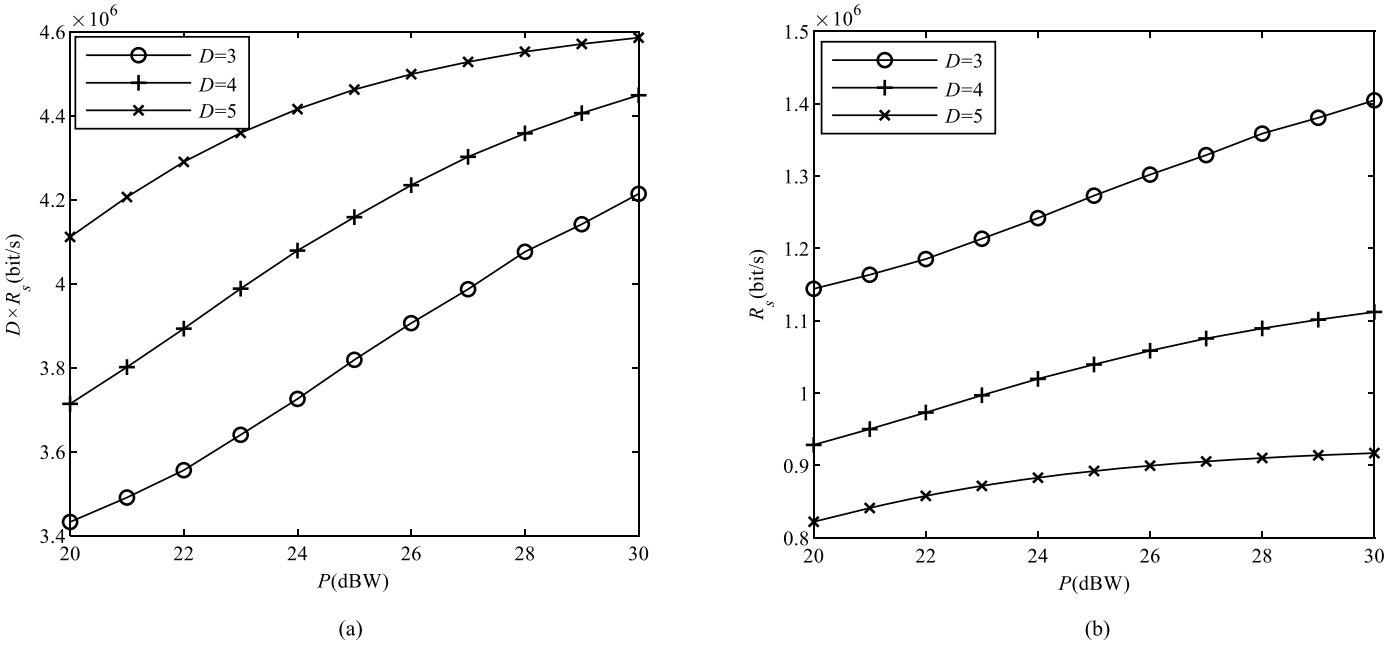

Fig. 5. Sum secrecy rate with different up-sampled factors when ECSI is unavailable. (a) D times of the sum secrecy rate. (b) Sum secrecy rate.

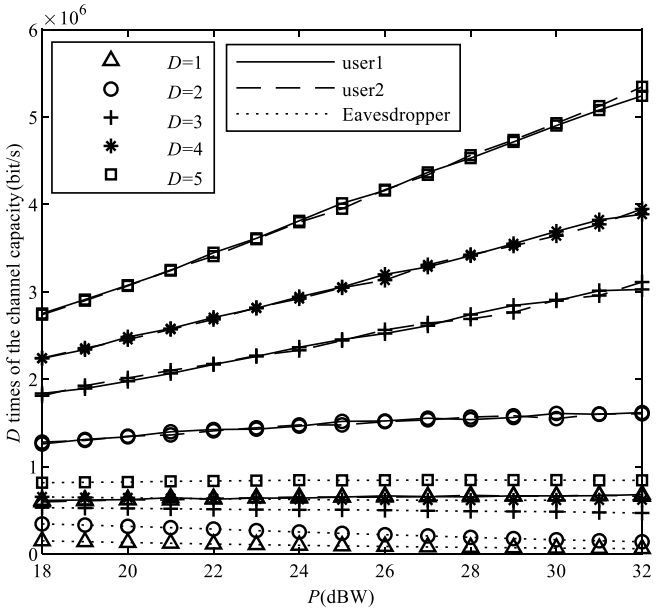

Fig. 6. Channel capacities of the legitimate channel and the eavesdropping channel with different up-sampled factors when ECSI is available.

and the secrecy rate will decrease as D increases. However, it does not follow that the smaller D is, the better the security is. If D is too small, ISI and IUI will become too high, and the target SINR of the legitimate users cannot be achieved. For example, if D is less than 3 in the simulation, the target SINR 6 dB cannot be achieved for any amount of transmission power.

Fig. 6 and Fig. 7 show the simulation results of the capacity of the legitimate channel and that of the eavesdropping channel, and the sum secrecy rate with different up-sampled factor D when ECSI is available respectively. In this case, the SINR of the legitimate users is not required to remain a constant in the optimization, and the ISI power at the legitimate user decreases and the SINR increases as the value of D increases, therefore, the D times of the capacity of the legitimate channel capacity will increase. On the other hand, due to the decrease of ISI power, SINR can increase fast with the increase of the transmission power. The larger the value of D is, the higher the growth rate of the D times of the legitimate channel capacity is with the increase of the transmission power. It can be seen that as the value of D increases, the capacity of the eavesdropping channel increases too. The reason is explained as follows. The optimization object in this case is the sum secrecy rate. The larger D is, the smaller is the ISI in the received signal at the legitimate receiver. The mutual information per symbol of the legitimate channel can be effectively promoted by increasing the signal power. Therefore, more power will be allocated for the transmission of the signal and the AN power will decrease when D increases. So the D times of the capacity of the eavesdropping channel will increase slightly. However, the SINRs of the legitimate users have a more significant improvement, so the D times of the sum secrecy rate increases, as is shown in Fig. 7(a). Furthermore, the larger D is, the smaller ISI is, so the legitimate channel capacity increases fast with the increase of the total power. For eavesdropping channels, because AN power will increase with the increase

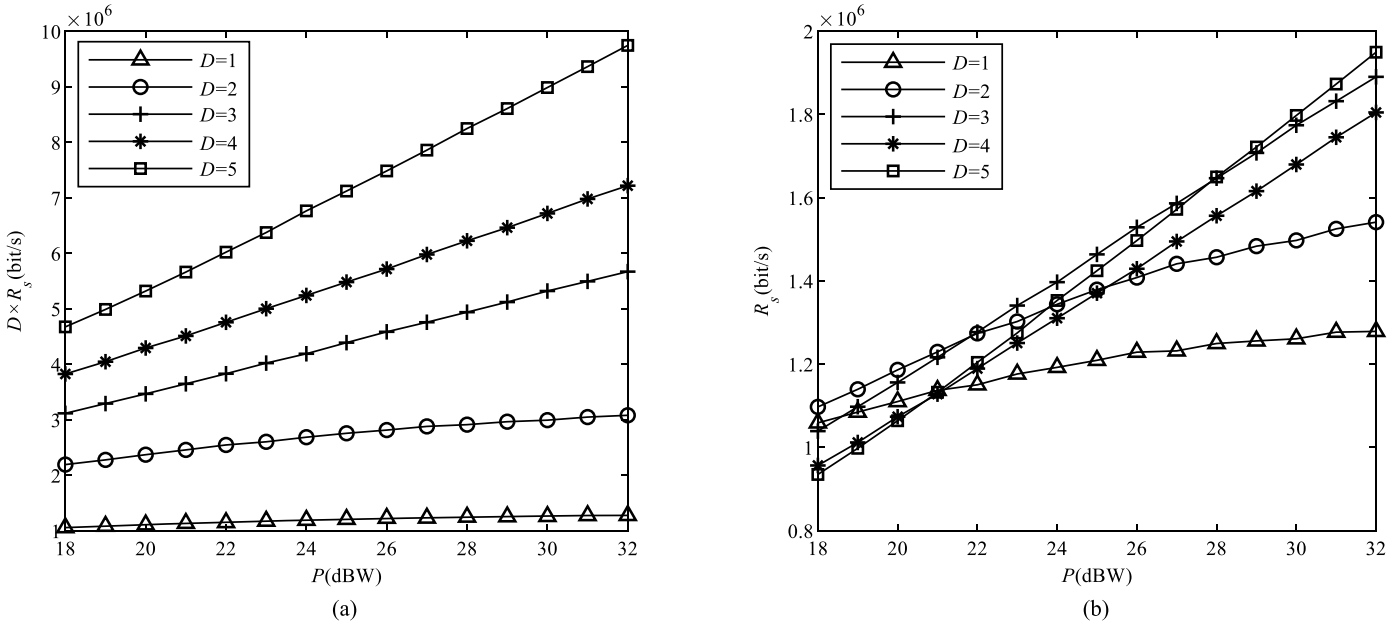

Fig. 7. Sum secrecy rate with different up-sampled factors when ECSI is available. (a) D times of the sum secrecy rate. (b) Sum secrecy rate.

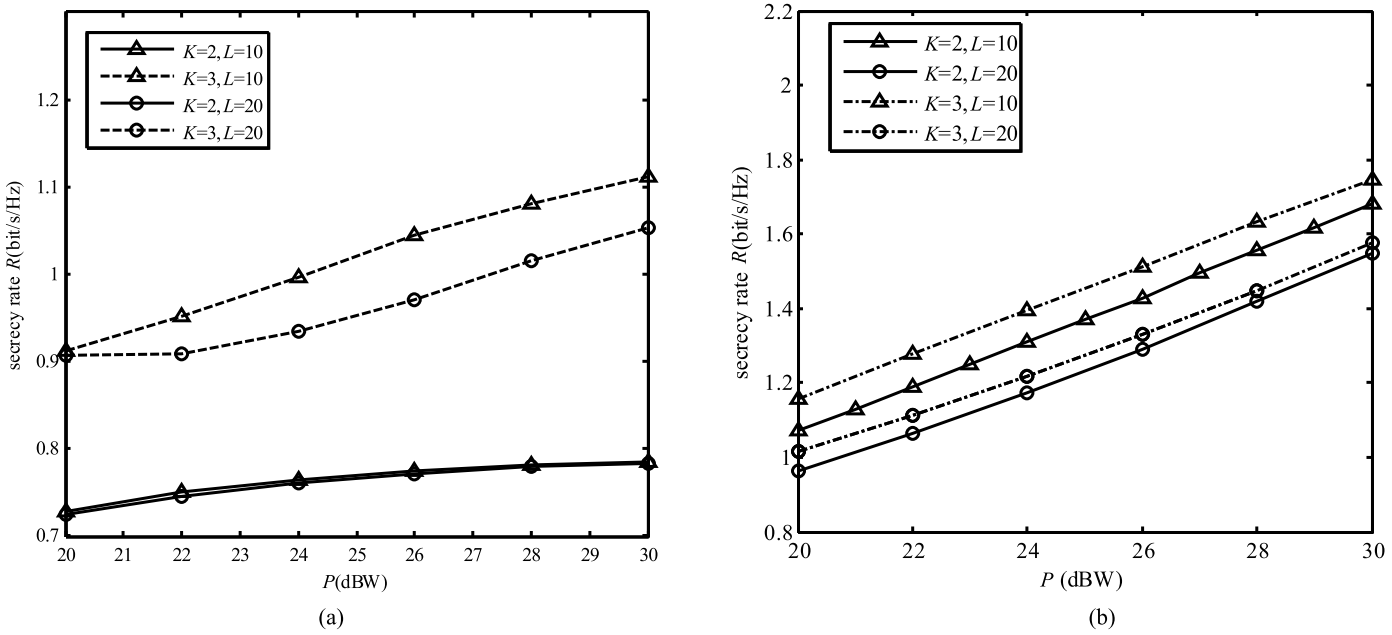

Fig. 8. Sum secrecy rate with different number of users and length of CIR. (a) ECSI is unavailable. (b) ECSI is available.

of the total power, the capacity of the eavesdropping channel is almost unchanged with the increase of the transmission power. However, it should be noted that although the increase of the D value improves the SINRs of the legitimate receivers, and the growth rate of the legitimate channel capacity with the increase of the transmission power is also higher, but the symbol rate drops, so the sum secrecy rate of the system does not increase monotonically with the increase of D, as is shown in Fig. 7(b).

Fig. 8 shows the simulation results of the sum secrecy rate when the number of users $K = 2$ and 3, the length of CIR $L = 10$ and 20. When $L = 10$, $B = 1$ MHz, and $L = 20$, $B = 2$ MHz. The root mean square delay of the path is fixed to $\sigma_{\mathrm{T}} = 10^{-5}$ s, and other parameters of the channels remain unchanged. In order to compare the performance of different L, the sum secrecy rate is divided by B, so its unit is bits/s/Hz. The simulation results with or without ECSI are given in Fig. 8(a) and Fig. 8(b) respectively. It can be seen from Fig. 8 that the sum secrecy rate when the number of users is 3 is higher than that when the number is 2. When the number of channel paths is larger than that of users, the more users there are, the higher is the sum secrecy rate of the users, so the higher is the sum secrecy rate of the system. It can also be seen that the sum secrecy rate decreases with the increase of the length of CIR. In the analysis and simulation, we assume that the eavesdropper has a super capability to completely eliminate ISI and IUI and utilize all signals coming from all paths, so the rate of the eavesdropper will increase greatly with the increase of the number of CIR. In contrast, although the power of the received signal of the legitimate users increases with the increase of the number of CIR, the power of ISI and IUI increases too. Therefore, the SINR of the legitimate users does not increase obviously, neither does their sum rate. As a result, the sum secrecy rate decreases when the

number of CIR increases. It needs to noted that if the eavesdropper does not have the ideal processing capability as is assumed, the sum secrecy rate may increase when the number of CIR increases.

5. Conclusion

This paper proposes a physical-layer security scheme and its optimization in a TR multi-user downlink multiple access system. We have designed two mechanisms for the two different scenarios in terms of ECSI's availability, and the pre-processing filters and AN are jointly optimized to improve the security performance of the system. When ECSI is unavailable, we adopt the null-space AN mechanism to minimize the power to transmit the signal under the minimum SINR constraint of the legitimate users, so the power to transmit AN is maximized under the total transmission power limit. The optimization problem is converted into a SDP problem through SDR, and then the optimal solution is obtained by using the CVX tool. Because the optimization process only relies on the CSI of the legitimate channels, the scheme can be directly applied to the case with multiple eavesdroppers. When ECSI is available, we jointly optimize the TR pre-processing filters and the AN waveform to maximize the sum secrecy rate of the system. The optimization problem is converted into a convex optimization problem through SDR and the first-order Taylor approximation, and solved by using an iterative algorithm. If there are multiple eavesdroppers wiretapping independently, we can optimize the TR filters and the covariance matrix of AN based on the ECSI of the eavesdropper which has the best channel to the transmitter among the eavesdroppers. If the eavesdroppers collude to wiretap, the multiple eavesdroppers can be regarded as one eavesdropper with multiple antennas. In this case, by extending the equivalent channel matrix of the eavesdropping channel ($\boldsymbol{H}_{\mathrm{e}}$) to the form of multiple receiving antennas, the capacity of the eavesdropping channel will have a similar expression as (15). Then the proposed optimization method can be used. Finally, the performance of the proposed scheme has been evaluated by computer simulation. The simulation results show that the sum secrecy rate of the system when ECSI is available is better than that when ECSI is unavailable, and the secrecy rates of both mechanisms are significantly higher than those of traditional TR systems with or without the null-space AN.

CRediT authorship contribution statement

Weijia Lei: Conceptualization, Methodology, Supervision. **Weihan Zhang:** Data curation, Formal analysis, Investigation, Validation. **Miaomiao Yang:** Formal analysis, Software, Visualization, Writing – original draft. **Hongjiang Lei:** Writing – review & editing. **Xianzhong Xie:** Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by The National Natural Science Foundation of China under grant nos. 61971080 and 61471076, the Chongqing Research Program of Basic Research and Frontier Exploration under grant no. cstc2018jcyjAX0432, and The Key Project of Science and Technology Research of Chongqing Education Commission under grant nos. KJZD-K201800603 and KJZD-M201900602.

Appendix A. Proof of Theorem 1

The proof process is similar to that in [17]. The Lagrangian function of problem (24) can be expressed as

$$L(\Xi)=\sum_{k=1}^{K}\mathrm{Tr}(\boldsymbol{G}_k)+\sum_{k=1}^{K}\lambda_k\left(\tilde{\gamma}_k\sigma^2+\tilde{\gamma}_k(\mathrm{Tr}(\boldsymbol{R}_k^{(0)}\boldsymbol{G}_k)+\sum_{i=1,i\neq k}^{K}\mathrm{Tr}(\boldsymbol{R}_k\boldsymbol{G}_i))-\mathrm{Tr}(\boldsymbol{R}_k^{(1)}\boldsymbol{G}_k)\right)-\sum_{k=1}^{K}\mathrm{Tr}(\boldsymbol{W}_k\boldsymbol{G}_k) \tag{40}$$

where $\boldsymbol{W}_k\succeq 0$ and $\lambda_k\geq 0$ are dual variables associated with the constraints. Ξ is the collection of all the primal and dual variables of problem (24).

Let $\boldsymbol{G}_k^{\mathrm{o}}$ be the optimal solution to (24). $\boldsymbol{W}_k^{\mathrm{o}}$ and λ_k^{o} are the corresponding optimal solutions to the dual problem of (24). The KKT conditions corresponding to $\boldsymbol{G}_k^{\mathrm{o}}$ can be expressed as

$$\begin{cases}\nabla L(\Xi)=\boldsymbol{I}_{(L)}+\lambda_k^{\mathrm{o}}\tilde{\gamma}_k\boldsymbol{R}_k^{(0)}+\sum\limits_{i=1,i\neq k}^{K}\lambda_i^{\mathrm{o}}\tilde{\gamma}_i\boldsymbol{R}_i-\lambda_k^{\mathrm{o}}\boldsymbol{R}_k^{(1)}-\boldsymbol{W}_k^{\mathrm{o}}=0 & \text{(a)}\\ \boldsymbol{W}_k^{\mathrm{o}}\boldsymbol{G}_k^{\mathrm{o}}=0 & \text{(b)}\\ \boldsymbol{W}_k^{\mathrm{o}}\succeq 0,\boldsymbol{G}_k^{\mathrm{o}}\succeq 0,\lambda_k^{\mathrm{o}}\geq 0,\forall k & \text{(c)}\end{cases} \tag{41}$$

We multiply both sides of (41-a) by $\boldsymbol{G}_k^{\mathrm{o}}$. According to (41-b), we have

$$\left(\boldsymbol{I}_{(L)}+\lambda_k^{\mathrm{o}}\tilde{\gamma}_k\boldsymbol{R}_k^{(0)}+\sum_{i=1,i\neq k}^{K}\lambda_i^{\mathrm{o}}\tilde{\gamma}_i\boldsymbol{R}_i\right)\boldsymbol{G}_k^{\mathrm{o}}=\left(\lambda_k^{\mathrm{o}}\boldsymbol{R}_k^{(1)}\right)\boldsymbol{G}_k^{\mathrm{o}} \tag{42}$$

Based on the basic rank inequality property, that is, $\mathrm{rank}(\boldsymbol{AB})\leq\min\{\mathrm{rank}(\boldsymbol{A}),\mathrm{rank}(\boldsymbol{B})\}$ for any matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ with appropriate dimension, we have

$$\operatorname{rank}\left(\left(\boldsymbol{I}_{(L)}+\lambda_k^{o}\tilde{\gamma}_k\boldsymbol{R}_k^{(0)}+\sum_{i=1,i\neq k}^{K}\lambda_i^{o}\tilde{\gamma}_i\boldsymbol{R}_i\right)\boldsymbol{G}_k^{o}\right)=\operatorname{rank}\left(\lambda_k^{o}\boldsymbol{R}_k^{(1)}\boldsymbol{G}_k^{o}\right)\leq\operatorname{rank}\left(\boldsymbol{R}_k^{(1)}\right)\leq 1 \tag{43}$$

Because $\boldsymbol{I}_{(L)}+\lambda_k^{o}\tilde{\gamma}_k\boldsymbol{R}_k^{(0)}+\sum_{i=1,i\neq k}^{K}\lambda_i^{o}\tilde{\gamma}_i\boldsymbol{R}_i$ is positive definite, and the rank of a matrix does not change when the matrix is multiplied by a nonsingular matrix, we have

$$\operatorname{rank}(\boldsymbol{G}_k^{o})=\operatorname{rank}\left(\left(\boldsymbol{I}_{(L)}+\lambda_k^{o}\tilde{\gamma}_k\boldsymbol{R}_k^{(0)}+\sum_{i=1,i\neq k}^{K}\lambda_i^{o}\tilde{\gamma}_i\boldsymbol{R}_i\right)\boldsymbol{G}_k^{o}\right)\leq 1 \tag{44}$$

Based on (44) and $\operatorname{rank}(\boldsymbol{G}_k^{o})\neq 0$, $\operatorname{rank}(\boldsymbol{G}_k^{o})=1$ always holds.

Appendix B. Supplementary material

Supplementary material related to this article can be found online at https://doi.org/10.1016/j.dsp.2020.102933.

References

[1] H.V. Poor, R.F. Schaefer, Wireless physical layer security, Proc. Natl. Acad. Sci. USA 114 (1) (Jan. 2017) 19–26.
[2] A.D. Wyner, The wire-tap channel, Bell Syst. Tech. J. 54 (8) (Oct. 1975) 1355–1387.
[3] X. Chen, D.W.K. Ng, W.H. Gerstacker, H.-H. Chen, A survey on multiple-antenna techniques for physical layer security, IEEE Commun. Surv. Tutor. 19 (2) (2017) 1027–1053.
[4] Y.-W.P. Hong, P.-C. Lan, C.-C.J. Kuo, Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches, IEEE Signal Process. Mag. 30 (5) (Sept. 2013) 29–40.
[5] Y. Huo, Y. Tian, L. Ma, X. Cheng, T. Jing, Jamming strategies for physical layer security, IEEE Wirel. Commun. 25 (1) (Feb. 2018) 148–153.
[6] H.C. Song, W.A. Kuperman, W.S. Hodgkiss, et al., Iterative time reversal in the ocean, J. Acoust. Soc. Am. 105 (6) (1997) 3176–3184.
[7] B. Wang, Y. Wu, F. Han, Y.-H. Yang, K.J.R. Liu, Green wireless communications: a time-reversal paradigm, IEEE J. Sel. Areas Commun. 29 (8) (Sept. 2011) 1698–1710.
[8] M.A. Bouzigues, I. Siaud, M. Helard, A.-M. Ulmer-Moll, Turn back the clock: time reversal for green radio communications, IEEE Veh. Technol. Mag. 8 (1) (Mar. 2013) 49–56.
[9] W. Lei, L. Yao, Performance analysis of time reversal communication systems, IEEE Commun. Lett. 23 (4) (Apr. 2019) 680–683.
[10] F. Han, Y.-H. Yang, B. Wang, Y. Wu, K.J.R. Liu, Time-reversal division multiple access over multi-path channels, IEEE Trans. Commun. 60 (7) (July 2012) 1953–1965.
[11] Y. Chen, Y.-H. Yang, F. Han, K.J.R. Liu, Time-reversal wideband communications, IEEE Signal Process. Lett. 20 (12) (Dec. 2013) 1219–1222.
[12] Y. Han, Y. Chen, B. Wang, K.J.R. Liu, Time-reversal massive multipath effect: a single-antenna “massive MIMO” solution, IEEE Trans. Commun. 64 (8) (Aug. 2016) 3382–3394.
[13] H. Ma, B. Wang, Y. Chen, K.J.R. Liu, Waveforming optimizations for time-reversal cloud radio access networks, IEEE Trans. Commun. 66 (1) (Jan. 2018) 382–393.
[14] L. Wang, R. Li, C. Cao, G.L. Stüber, SNR analysis of time reversal signaling on target and unintended receivers in distributed transmission, IEEE Trans. Commun. 64 (5) (May 2016) 2176–2191.
[15] W. Lei, M. Yang, L. Yao, H. Lei, Physical layer security performance analysis of the time reversal transmission system, IET Commun. 14 (4) (2020) 635–645.
[16] W. Cao, J. Lei, W. Hu, W. Li, Secrecy capacity achievable time reversal pre-filter in MISO communication system and the unequal secrecy protection application, Wirel. Pers. Commun. 97 (4) (Aug. 2017) 5427–5437.
[17] Q. Xu, P. Ren, Q. Du, L. Sun, Security-aware waveform and artificial noise design for time-reversal-based transmission, IEEE Trans. Veh. Technol. 67 (6) (June 2018) 5486–5490.
[18] J. Zhu, Y. Wang, T. Yang, F. Li, Time-reversal based secure transmission scheme for 5G networks over correlated wireless multi-path channels, Wirel. Pers. Commun. 101 (2) (April 2018) 979–1001.
[19] S. Leung-Yan-Cheong, M. Hellman, The Gaussian wire-tap channel, IEEE Trans. Inf. Theory 24 (4) (1978) 451–456.
[20] P. Zhao, M. Zhang, H. Yu, H. Luo, W. Chen, Robust beamforming design for sum secrecy rate optimization in MU-MISO networks, IEEE Trans. Inf. Forensics Secur. 10 (9) (Sept. 2015) 1812–1823.
[21] M. Alageli, A. Ikhlef, J. Chambers, Optimization for maximizing sum secrecy rate in MU-MISO SWIPT systems, IEEE Trans. Veh. Technol. 67 (1) (Jan. 2018) 537–553.
[22] Y. Huang, D.P. Palomar, Rank-constrained separable semidefinite programming with applications to optimal beamforming, IEEE Trans. Signal Process. 58 (2) (Feb. 2010) 664–678.

Weijia Lei received the B.Sc. degree in communication engineering from the Chongqing University of Posts and Telecommunications (CQUPT), Chongqing, China, in 1992, the M.Sc. degree in communication and electronic system from the Beijing University of Posts and Telecommunications, Beijing, China, in 1999, and the Ph.D. degree in signal and information processing from the University of Electronic Science and Technology of China, Chengdu, China, in 2010. He is currently a Professor with the School of Communication and Information Engineering, CQUPT. His research focuses on wireless communications technology, including channel coding and modulation, cooperation relay, and physical layer security.

Weihan Zhang received the B.Sc. degree in communication engineering from the Chongqing University of Posts and Telecommunications (CQUPT), Chongqing, China, in 2018. He is currently pursuing the M.Sc. degree in CQUPT. His main research interests include physical layer security and time reversal technology.

Miaomiao Yang received the B.Sc. degree in communication engineering from the Xi’an Shiyou University, Xi’an, China, in 2017, the M.Sc. degree from the Chongqing University of Posts and Telecommunications, Chongqing, China, in 2020. Her main research interests include time reversal technology, multiple antenna technology and physical layer security.

Hongjiang Lei received the Ph.D. degree in instrument science and technology from Chongqing University, Chongqing, China, in 2015. He is currently Professor with the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing. His current research interests include physical layer security, cooperative relaying systems, and so on.

Xianzhong Xie received the Ph.D. degree in communication and information systems from Xidian University, Xi’an, China, in 2000. He is currently a Professor with the School of Optoelectronic Engineering and the Director of Chongqing Key Laboratory of Computer Network and Communication Technology, Chongqing University of Posts and Telecommunications, Chongqing, China. His research interests include MIMO precoding, cognitive radio networks, and cooperative communications.