Optimization of pre-equalized time reversal security transmission systems assisted with artificial noise

Weijia Lei
Chongqing University of Posts and Telecommunications
Mengting Zou
Chongqing University of Posts and Telecommunications
Weihan Zhang (2321760356@qq.com)
Chongqing University of Posts and Telecommunications https://orcid.org/0000-0002-5856-4816
Yue Zhang
Chongqing University of Posts and Telecommunications
Hongjiang Lei
Chongqing University of Posts and Telecommunications

Research Article

Keywords: Physical layer security, Time reversal, Pre-equalization, Artificial noise

Posted Date: May 26th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1623887/v1

Optimization of pre-equalized time reversal security transmission systems assisted with artificial noise

Weijia Lei[1,2], Mengting Zou[1,2], Weihan Zhang [1,2], Yue Zhang[1,2], Hongjiang Lei[1,2]

Abstract

Time reversal (TR) transmission technology can focus the power of a signal in both time and space domains and reduce signal energy leakage to unintended receivers, making it suitable for physical layer security systems. By adding a pre-equalizer to the transmitter and optimizing it, the performance of multi-antenna TR transmission system can be improved obviously with an acceptable optimization complexity. In this paper, the pre-equalizer and artificial noise (AN) are jointly optimized to enhance the security performance of pre-equalized TR (ETR) systems when eavesdropping channel state information (ECSI) is unknown or known. When ECSI is unknown, null-space AN is adopted, and the pre-equalizer is optimized to minimize the signal power under the constraint of the minimum signal-to-interference-plus-noise ratio (SINR) of the legitimate receiver. When ECSI is known, under the minimum SINR constraint of the legitimate receiver, the pre-equalizer and AN's covariance matrix are jointly optimized to minimize the SINR of the eavesdropper. The optimization problem is non-convex and is transformed into a convex problem, which can be solved using the CVX toolbox. Simulation results demonstrate that compared with TR systems, by optimizing the pre-equalizer, the security performance of ETR multi-antenna systems can be significantly improved, and the optimization complexity is acceptable.

Keywords Physical layer security · Time reversal · Pre-equalization · Artificial noise

1 Introduction

In wireless communication systems, signals travel along different paths between the transmitter and the receiver. The propagation time of signals on each path is different, resulting in the extension of the symbol period and inter-symbol interference (ISI). RAKE receive and equalization are two leading technologies applied by receivers to eliminate or reduce ISI and gather the signal energy from multiple paths to enhance the signal strength. However, a complex equalizer or RAKE receiver is seldom available for the receivers with limited processing capacity. Time reversal (TR) is a signal processing technology employed at the transmitter to reduce ISI and enhance the signal strength at the intended receiver. A TR transmission consists of two steps. In the first step, the receiver sends an impulse signal to the transmitter. The transmitter estimates the multipath channel's channel impulse response (CIR) based on the received signal. The TR pre-filter's impulse response (IR) is time-reversed and conjugated with CIR. In the second step, the signal is filtered by the TR pre-filter and transmitted. Therefore, the multipath channel is the matched filter of the pre-filtered signal at a particular moment. The signals from the different paths are coherently superposed to the intended receiver. So, there is an obvious signal peak while the delay spread is reduced and ISI is alleviated. Conversely, the channel between the transmitter and any unintended receiver is not the matched filter of the pre-filtered signal, and the power of the signal received at unintended receivers is significantly lower than that of the intended receiver. This feature is called spatial-temporal focusing of TR transmission. Since the transmitter is mainly used for signal processing in TR systems, the processing complexity of the receiver is very low.

Early research on TR transmission mainly focused on underwater acoustic communications 1. In recent years, TR transmission technology in wireless communications has been studied. Ref. 2 verified the spatial-temporal focusing of TR and proved that the leakage of radiofrequency energy interference to unintended receivers is low in TR wireless communication systems. Although TR pre-filtering alleviates ISI, ISI still exists and has a severe impact on the received signal when the delay spread of the channel is larger than the symbol period. ISI can be reduced by up-sampling the transmitted signal, but the spectrum efficiency will decline 3. Some research works studied the design of the TR pre-filter to reduce ISI or maximize the signal-to-interference-plus-noise ratio (SINR). In 4, a method to reduce ISI by aligning interference is studied. Predistortion waveform is designed for each symbol to align the ISI of the signal at the intended receiver, so the signal energy is promoted while ISI is suppressed. In 5, the optimization of the TR pre-filter for cloud access networks is studied, and a content-aware waveform design and an optimal receiving algorithm are proposed. The simulation results show that the performance of the proposed scheme is better than that of the conventional TR pre-filter scheme.

Information security is a crucial issue in communications. Compared with wired communications, wireless communications meet more severe security threats. Physical layer security (PLS) exploits the characteristics of wireless channels and guarantees the security of information by using physical layer technologies. Multi-antenna beamforming and artificial noise (AN) are commonly used in PLS. By beamforming, the radiation direction of signals towards the legitimate receiver and the signal energy leaked to the eavesdropper can be suppressed 6. AN is often employed in multi-antenna systems. By controlling AN's radiation direction, the latter can significantly deteriorate the signal quality at the eavesdropper without interfering with the legitimate receiver. However, the number of antennas is limited at small-size and low-cost nodes, which greatly restricts the effect of

✉ Weihan Zhang
2321760356@qq.com

[1] School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
[2] Chongqing Key Laboratory of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

beamforming and AN. The spatial-temporal focusing feature of TR transmission focuses the signal energy on the target receiver, so it is very suitable for PLS. The signal-to-noise ratio of the target receiver and the unintended receiver in a distributed TR system is studied by 7. It demonstrates that TR pre-filter can improve security performance. In 8, the ergodic achievable secrecy rate of TR systems is derived, and the bit error rates (BERs) at the target receiver and the unintended receiver for binary phase-shift keying (BPSK) are deduced too. The results show that the target receiver can achieve a higher transmission rate and a lower BER than the unintended receiver. In 9, the security performance of multiple-input multiple-output (MIMO) TR systems is studied. The results show that TR pre-processing can significantly improve the security performance of the system. However, the conventional TR pre-processing, whose pre-filter is matched with the channel of the target receiver, can improve the signal power of the target receiver. Still, from the perspective of secure transmission, it is not optimal. In 10, for a multi-input single-output (MISO) TR transmission system, the optimal design scheme of TR pre-filter to maximize the secrecy rate is studied. The simulation results show that the achievable secrecy rate of the proposed method is better than that of the conventional TR scheme. In 11, for a multi-user secure transmission system, two optimization schemes to the TR system assisted with AN are proposed, respectively, based on or not based on the eavesdropping channel state information (ECSI). When ECSI is unknown, null-space AN is adopted, and the TR pre-filter is optimized to minimize the signal's transmission power, so AN power is maximized. When ECSI is known, AN and the TR pre-filter are jointly optimized to maximize the sum secrecy rate. The simulation results show that the sum secrecy rate of the proposed scheme is higher than that of the conventional TR system. In 12, a secure transmission scheme combining AN and TR pre-processing is proposed, and the power allocation scheme between the signal and AN is optimized. The simulation shows that AN can effectively improve the secure transmission performance of the system.

In multi-antenna TR systems, each antenna assigns a TR pre-filter. In order to obtain a good performance, all TR pre-filters need to be optimized jointly. When the number of paths of the channel or the number of antennas is large, the complexity of optimization is very high. A pre-equalized time reversal (ETR) transmission scheme is proposed to reduce the optimization complexity of multi-antenna TR systems. In ETR systems, a pre-equalizer is added ahead of the conventionally TR matched pre-filters. The pre-equalizer is designed according to a specific criterion, such as zero-forcing (ZF), minimum mean square error (MMSE), etc. The pre-equalizer can also be optimized to improve a certain performance index. Because only one pre-equalizer is optimized, the optimization complexity of ETR systems is much lower than that of TR systems. Refs. 13 and 14 respectively studied the design of the pre-equalizer according to the ZF criterion and MMSE criterion for ETR-MIMO systems. In 15, for a MISO TR transmission system, the pre-equalizer is optimized to minimize ISI under the constraint of the minimum peak power of the received signal. In PLS systems, because the security performance is related to both the legitimate channel and the eavesdropping channel, the optimization of the TR pre-filter is more complicated than in conventional TR systems, especially in multi-antenna TR systems. The optimization complexity will be reduced significantly if a pre-equalizer is introduced into a multi-antenna TR PLS system.

To the best of our knowledge, there are few works on applying ETR in PLS systems. For an ETR-MISO secure transmission system, this paper designs an AN scheme and optimizes AN and pre-equalizer when ECSI is known or unknown. When ECSI is unknown, null-space AN is adopted. The pre-equalizer is optimized to minimize the signal's power under the constraint of the minimum SINR of the legitimate receiver to maximize AN's power. When ECSI is known, under the constraint of the minimum SINR of the legitimate receiver, the AN's covariance matrix and the pre-equalizer are optimized to minimize the SINR of the eavesdropper.

2 System model

The model of the system studied by this paper is shown in Fig. 1, which is an ETR-MISO system consisting of a multi-antenna transmitter, a single-antenna legitimate receiver, and a single-antenna eavesdropper. The number of antennas of the transmitter is N. It is assumed that both the legitimate channel and the eavesdropping channel are frequency selective. CIRs from the i-th antenna of the transmitter to the legitimate receiver and to the eavesdropper is expressed as $h_{\mathrm{B},i}[l]$ and $h_{\mathrm{E},i}[l]$, respectively, where $l = 0,\ldots,L-1$, and L is the channel response length, that is, the number of the paths of the channels. The IR of the TR pre-filter is the time-reversed and conjugated CIR of the legitimate channel, that is, the IR of the TR pre-filter of the i-th antenna is $g_i[l] = h^*_{\mathrm{B},i}[L-1-l]$, where $(\cdot)^*$ represents the conjugate operation. Before the TR pre-filter, there is a pre-equalizer. The IR of the pre-equalizer is denoted as $g_{\mathrm{pre}}[l]$, where $l = 0,1,\ldots,2L-2$. The number of taps of the pre-equalizer is $2L-1$. The CIRs and the IRs of the pre-filters and the pre-equalizer can be expressed in vector form, respectively as

$$
\begin{aligned}
\mathbf{h}_{\mathrm{B},i} &= \left[h_{\mathrm{B},i}[0], h_{\mathrm{B},i}[1], \cdots, h_{\mathrm{B},i}[L-1]\right]^T \\
\mathbf{h}_{\mathrm{E},i} &= \left[h_{\mathrm{E},i}[0], h_{\mathrm{E},i}[1], \cdots, h_{\mathrm{E},i}[L-1]\right]^T \\
\mathbf{g}_i &= \left[h^*_{\mathrm{B},i}[L-1], h^*_{\mathrm{B},i}[L-2], \cdots, h^*_{\mathrm{B},i}[0]\right]^T \\
\mathbf{g}_{\mathrm{pre}} &= \left[g_{\mathrm{pre}}[0], g_{\mathrm{pre}}[1], \cdots, g_{\mathrm{pre}}[2L-2]\right]^T
\end{aligned}
\tag{1}
$$

where the superscript T denotes transpose operation.

The symbol sequence to be transmitted is denoted as $\{x[n]\}_{n=0}^{M-1}$, where M is the length of the symbol sequence and $E\left\{\left|x[n]\right|^2\right\} = 1$. After going through the pre-equalizer and the TR pre-filters, the antennas send out $x[n]$, and the transmitter also transmits AN with power P_{AN} to prevent the information from being wiretapped. The AN sequence transmitted by each antenna is denoted as $\frac{z_{\mathrm{AN}}[n]}{\sqrt{N}}$, where $E\left\{\left|z[n]\right|^2\right\} = P_{\mathrm{AN}}$. The signal sent by the i-th antenna is expressed as

$$
s_i[n] = x[n] \otimes g_{\mathrm{pre}}[n] \otimes g_i[n] + \frac{z_{\mathrm{AN}}[n]}{\sqrt{N}} \tag{2}
$$

where $\otimes$ represents discrete convolution. The first part on

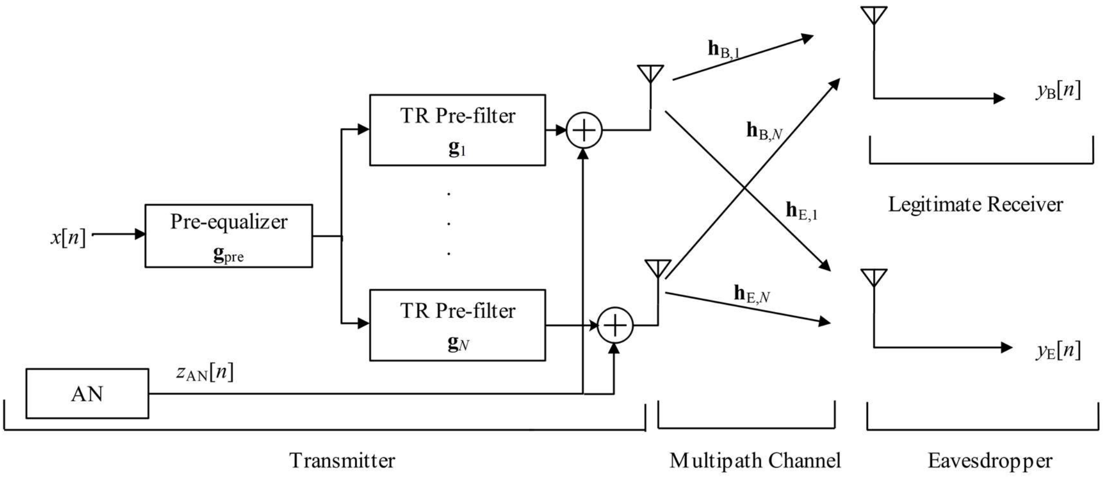


Fig.1 System model

the right side of (2) is the signal carrying information, and the second part is AN. The sequence length of the information signal is $L_{\mathrm{s}} = M + 3L - 3$, and the sequence length of AN is also L_{s}.

The received signal of the legitimate receiver is

$$\tilde{y}_{\mathrm{B}}[n] = \sum_{i=1}^{N} s_i[n] \otimes h_{\mathrm{B},i}[n] + \tilde{z}_{\mathrm{B}}[n] \tag{3}$$

where $\tilde{z}_{\mathrm{B}}[n]$ is the complex Gaussian channel noise with variance σ_{B}^2. By substituting (2) into (3), we get

$$\begin{aligned}\tilde{y}_{\mathrm{B}}[n] &= \sum_{i=1}^{N} x[n] \otimes g_{\mathrm{pre}}[n] \otimes g_i[n] \otimes h_{\mathrm{B},i}[n] \\ &\quad + \sum_{i=1}^{N} \frac{z_{\mathrm{AN}}[n]}{\sqrt{N}} \otimes h_{\mathrm{B},i}[n] + \tilde{z}_{\mathrm{B}}[n] \\ &= x[n] \otimes g_{\mathrm{pre}}[n] \otimes \sum_{i=1}^{N} \left(g_i[n] \otimes h_{\mathrm{B},i}[n]\right) \\ &\quad + z_{\mathrm{AN}}[n] \otimes \sum_{i=1}^{N} \frac{h_{\mathrm{B},i}[n]}{\sqrt{N}} + \tilde{z}_{\mathrm{B}}[n]\end{aligned} \tag{4}$$

Letting $h_{\mathrm{B,TR}}[n] = \sum_{i=1}^{N} g_i[n] \otimes h_{\mathrm{B},i}[n]$, $h_{\mathrm{B,AN}}[n] = \sum_{i=1}^{N} \frac{h_{\mathrm{B},i}[n]}{\sqrt{N}}$, the above formula can be rewritten as

$$\tilde{y}_{\mathrm{B}}[n] = x[n] \otimes g_{\mathrm{pre}}[n] \otimes h_{\mathrm{B,TR}}[n] + z_{\mathrm{AN}}[n] \otimes h_{\mathrm{B,AN}}[n] + \tilde{z}_{\mathrm{B}}[n] \tag{5}$$

After the symbol is sent, the symbol peak at the legitimate receiver appears at the (2L−2)-th sample. So the received sequence for detection is expressed as

$$\begin{aligned}y_{\mathrm{B}}[n] &= \tilde{y}_{\mathrm{B}}[n + 2L - 2] \\ &= \sum_{l=0}^{4L-4} \left(g_{\mathrm{pre}} \otimes h_{\mathrm{B,TR}}\right)[l] \times x[n + 2L - 2 - l] \\ &\quad + \left(z_{\mathrm{AN}} \otimes h_{\mathrm{B,AN}}\right)[n + 2L - 2] + z_{\mathrm{B}}[n] \\ &= \left(g_{\mathrm{pre}} \otimes h_{\mathrm{B,TR}}\right)[2L-2] \times x[n] \\ &\quad + \sum_{k=-(2L-2),k\neq 0}^{2L-2} \left(g_{\mathrm{pre}} \otimes h_{\mathrm{B,TR}}\right)[2L - 2 - k] \times x[n+k] \\ &\quad + \left(z_{\mathrm{AN}} \otimes h_{\mathrm{B,AN}}\right)[n + 2L - 2] + z_{\mathrm{B}}[n]\end{aligned} \tag{6}$$

where $z_{\mathrm{B}}[n] = \tilde{z}_{\mathrm{B}}[n + 2L - 2]$. The first part on the right side of the last equal sign is the expected signal, the second part is ISI, and the third part is AN.

We replace the convolution operation in (6) with matrix multiplication for the convenience of description. Firstly, we define a $(4L-3)\times(2L-1)$ -dimensional Toeplitz matrix $\mathbf{H}_{\mathrm{B,TR}}$ composed of $h_{\mathrm{B,TR}}[n]$, which is

$$\mathbf{H}_{\mathrm{B,TR}} = \begin{bmatrix} h_{\mathrm{B,tr}}[0] & 0 & & 0 \\ h_{\mathrm{B,tr}}[1] & h_{\mathrm{B,tr}}[0] & \ddots & \vdots \\ \vdots & h_{\mathrm{B,tr}}[1] & \ddots & \vdots \\ h_{\mathrm{B,tr}}[2L-2] & \vdots & \ddots & h_{\mathrm{B,tr}}[0] \\ \vdots & h_{\mathrm{B,tr}}[2L-2] & \ddots & \vdots \\ \vdots & \vdots & & h_{\mathrm{B,tr}}[2L-3] \\ 0 & 0 & & h_{\mathrm{B,tr}}[2L-2] \end{bmatrix} \tag{7}$$

Furthermore, we denote $\mathbf{h}_{\mathrm{B},l}$ as the transpose of the l-th row of $\mathbf{H}_{\mathrm{B,TR}}$. Then we define a $(L_{\mathrm{s}} + L - 1)\times L_{\mathrm{s}}$ -dimensional Toeplitz matrix $\mathbf{H}_{\mathrm{B,AN}}$ which is composed of $h_{\mathrm{B,AN}}[n]$, which is expressed as

$$\mathbf{H}_{\mathrm{B,AN}} = \begin{bmatrix} h_{\mathrm{B,AN}}[0] & 0 & & 0 \\ h_{\mathrm{B,AN}}[1] & h_{\mathrm{B,AN}}[0] & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ h_{\mathrm{B,AN}}[L-1] & \vdots & \ddots & h_{\mathrm{B,AN}}[0] \\ \vdots & h_{\mathrm{B,AN}}[L-1] & \ddots & \vdots \\ \vdots & \vdots & & h_{\mathrm{B,AN}}[L-2] \\ 0 & 0 & & h_{\mathrm{B,AN}}[L-1] \end{bmatrix} \tag{8}$$

Letting $\mathbf{q}_{\mathrm{B},n}^T = \hat{\mathbf{e}}_{n+2L-1}^T \mathbf{H}_{\mathrm{B,AN}}$, where $\hat{\mathbf{e}}_{n+2L-1}^T$ is the $(n + 2L - 1)$ -th row of the identity matrix $\mathbf{I}_{(L_{\mathrm{s}}+L-1)\times(L_{\mathrm{s}}+L-1)}$, (6) can be rewritten as

$$\begin{aligned}y_{\mathrm{B}}[n] &= \mathbf{h}_{\mathrm{B},(2L-1)}^T \mathbf{g}_{\mathrm{pre}} x[n] + \sum_{l=-(2L-2),l\neq 0}^{(2L-2)} \mathbf{h}_{\mathrm{B},(2L-1)+l}^T \mathbf{g}_{\mathrm{pre}} x[n+l] \\ &\quad + \mathbf{z}_{\mathrm{AN}}^T \mathbf{q}_{\mathrm{B},n} + z_{\mathrm{B}}[n]\end{aligned} \tag{9}$$

where $\mathbf{z}_{\mathrm{AN}} = \left[z_{\mathrm{AN}}[0], z_{\mathrm{AN}}[1], \cdots, z_{\mathrm{AN}}[L_{\mathrm{s}} - 1]\right]^T$ is the vector form of the AN sequence. The SINR of the symbol $y_{\mathrm{B}}[n]$ is

$$\gamma_{\mathrm{B},n} = \frac{\mathbf{h}_{\mathrm{B},(2L-1)}^H \mathbf{g}_{\mathrm{pre}} \mathbf{g}_{\mathrm{pre}}^H \mathbf{h}_{\mathrm{B},(2L-1)}}{\sum_{l=1,l\neq(2L-1)}^{(4L-3)} \mathbf{h}_{\mathrm{B},l}^H \mathbf{g}_{\mathrm{pre}} \mathbf{g}_{\mathrm{pre}}^H \mathbf{h}_{\mathrm{B},l} + \mathbf{q}_{\mathrm{B},n}^H \mathbf{\Phi}_{\mathrm{AN}} \mathbf{q}_{\mathrm{B},n} + \sigma_{\mathrm{B}}^2} \tag{10}$$

where $\mathbf{\Phi}_{\mathrm{AN}} = E\left\{\mathbf{z}_{\mathrm{AN}}^H \mathbf{z}_{\mathrm{AN}}\right\}$ is the covariance matrix of AN, and $(\mathbf{X})^H$ represents the conjugate transpose of matrix or vector **X**.

Similarly, a $(4L-3)\times(2L-1)$-dimensional Toeplitz matrix $\mathbf{H}_{\mathrm{E,TR}}$ is defined as

$$\mathbf{H}_{\mathrm{E,TR}} = \begin{bmatrix} h_{\mathrm{E,TR}}[0] & 0 & & 0 \\ h_{\mathrm{E,TR}}[1] & h_{\mathrm{E,TR}}[0] & \ddots & \vdots \\ \vdots & h_{\mathrm{E,TR}}[1] & \ddots & \vdots \\ h_{\mathrm{E,TR}}[2L-2] & \vdots & \ddots & h_{\mathrm{E,TR}}[0] \\ \vdots & h_{\mathrm{E,TR}}[2L-2] & \ddots & \vdots \\ \vdots & \vdots & & h_{\mathrm{E,TR}}[2L-3] \\ 0 & 0 & & h_{\mathrm{E,TR}}[2L-2] \end{bmatrix} \tag{11}$$

where $h_{\mathrm{E,TR}}[n] = \sum_{i=1}^{N} g_i[n] \otimes h_{\mathrm{E},i}[n]$. We also denote $\mathbf{h}_{\mathrm{E},l}$ as the transpose of the l-th row of $\mathbf{H}_{\mathrm{E,TR}}$. Then we define a $(L_{\mathrm{s}}+L-1)\times L_{\mathrm{s}}$ -dimensional Toeplitz matrix $\mathbf{H}_{\mathrm{E,AN}}$ as follows:

$$\mathbf{H}_{\mathrm{E,AN}} = \begin{bmatrix} h_{\mathrm{E,AN}}[0] & 0 & & 0 \\ h_{\mathrm{E,AN}}[1] & h_{\mathrm{E,AN}}[0] & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ h_{\mathrm{E,AN}}[L-1] & \vdots & \ddots & h_{\mathrm{E,AN}}[0] \\ \vdots & h_{\mathrm{E,AN}}[L-1] & \ddots & \vdots \\ \vdots & \vdots & & h_{\mathrm{E,AN}}[L-2] \\ 0 & 0 & & h_{\mathrm{E,AN}}[L-1] \end{bmatrix} \tag{12}$$

where $h_{\mathrm{E,AN}}[n] = \sum_{i=1}^{N} \frac{h_{\mathrm{E},i}[n]}{\sqrt{N}}$. Letting $\mathbf{q}_{\mathrm{E},n}^T = \hat{\mathbf{e}}_{n+2L-1}^T \mathbf{H}_{\mathrm{E,AN}}$, the received sequence of the eavesdropper is expressed as

$$\begin{aligned} y_{\mathrm{E}}[n] = {} & \mathbf{h}_{\mathrm{E},(2L-1)}^T \mathbf{g}_{\mathrm{pre}} x[n] + \sum_{l=-(2L-2),l\neq 0}^{(2L-2)} \mathbf{h}_{\mathrm{E},(2L-1)+l}^T \mathbf{g}_{\mathrm{pre}} x[n+l] \\ & + \mathbf{z}_{\mathrm{AN}}^T \mathbf{q}_{\mathrm{E},n} + z_{\mathrm{E}}[n] \end{aligned} \tag{13}$$

where $z_{\mathrm{E}}[n]$ is the complex Gaussian channel noise with variance σ_{E}^2. The SINR of the symbol $y_{\mathrm{E}}[n]$ is

$$\gamma_{\mathrm{E},n} = \frac{\mathbf{h}_{\mathrm{E},(2L-1)}^H \mathbf{g}_{\mathrm{pre}} \mathbf{g}_{\mathrm{pre}}^H \mathbf{h}_{\mathrm{E},(2L-1)}}{\mathbf{q}_{\mathrm{E},n}^H \mathbf{\Phi}_{\mathrm{AN}} \mathbf{q}_{\mathrm{E},n} + \sigma_{\mathrm{E}}^2} \tag{14}$$

In this paper, we consider the worst-case that the eavesdropper has a strong signal processing ability and can eliminate all ISI, so there is no ISI power in (14).

The achievable secrecy rate is one of the indexes to measure the PLS performance, which is the difference between the legitimate channel capacity and the eavesdropping channel capacity:

$$R_s = \left[B\log_2(1+\gamma_{\mathrm{B}}) - B\log_2(1+\gamma_{\mathrm{E}})\right]^+ \tag{15}$$

where $[x]^+ \triangleq \max\{0,x\}$, γ_{B} and γ_{E} represent the SINR of the legitimate receiver and that of the eavesdropper, respectively. The secrecy rate can be improved by increasing the SINR of the legitimate receiver or by reducing the SINR of the eavesdropper. From (10) and (14), we can find that the IR of the pre-equalizer and the AN's covariance matrix need to be optimized to promote the secrecy rate. We will discuss this in the next section.

3 A scheme and optimization algorithm

3.1 Scheme and optimization when ECSI is unknown

When the transmitter does not know ECSI, null-space AN is commonly adopted. In this way, AN is radiated in all directions without interfering with the legitimate receiver. The expression of the received AN at the legitimate receiver in Eq. (6) can be rewritten as

$$\boldsymbol{y}_{\mathrm{AN}} = \mathbf{Q}_{\mathrm{AN}} \mathbf{H}_{\mathrm{B,AN}} \mathbf{z}_{\mathrm{AN}} \tag{16}$$

where $\mathbf{Q}_{\mathrm{AN}}$ is an $M\times(L_{\mathrm{s}}+L-1)$-dimensional sparse matrix, and only the elements of $\mathbf{Q}_{\mathrm{AN}}$ in the row $m+1$ and column $m+2L-1$, $\forall m\in\{0,1,\ldots,M-1\}$, are 1, and the others are 0. Obviously, it will not interfere with the legitimate receiver when it is in the null-space. Therefore, AN should be $\mathbf{z}_{\mathrm{AN}} = \mathbf{W}\mathbf{v}$, where **W** is the base of the null-space of $\mathbf{Q}_{\mathrm{AN}}\mathbf{H}_{\mathrm{B,AN}}$ with dimension $N_{\mathrm{AN}} = L_{\mathrm{s}} - M$, and **v** is a Gaussian random vector with the covariance matrix $\mathbf{\Phi}_v^{\text{N-AN}} = E\left\{\mathbf{v}\mathbf{v}^H\right\} = \frac{P_{\mathrm{AN}}}{N_{\mathrm{AN}}} \mathbf{I}_{(N_{\mathrm{AN}}\times N_{\mathrm{AN}})}$. The covariance matrix of AN is expressed as

$$\mathbf{\Phi}_{\mathrm{AN}} = \mathbf{W}\mathbf{\Phi}_v^{\text{N-AN}}\mathbf{W}^H = \frac{P_{\mathrm{AN}}}{N_{\mathrm{AN}}}\mathbf{W}\mathbf{W}^H \tag{17}$$

In this case, the SINR of the legitimate receiver is

$$\gamma_{\mathrm{B}}^{\text{N-AN}} = \frac{\mathbf{h}_{\mathrm{B},(2L-1)}^H \mathbf{g}_{\mathrm{pre}} \mathbf{g}_{\mathrm{pre}}^H \mathbf{h}_{\mathrm{B},(2L-1)}}{\sum_{l=1,l\neq(2L-1)}^{(4L-3)} \mathbf{h}_{\mathrm{B},l}^H \mathbf{g}_{\mathrm{pre}} \mathbf{g}_{\mathrm{pre}}^H \mathbf{h}_{\mathrm{B},l} + \sigma_{\mathrm{B}}^2} \tag{18}$$

Because ECSI is unknown, the expression of the secrecy rate cannot be obtained, and the secrecy rate cannot be the objective of the optimization. As an alternative, we optimize the tap coefficients of the pre-equalizer to minimize the signal power under the constraints of the total transmission power limit and the minimum SINR requirement of the legitimate receiver. In this way, the power of AN will be maximized. The optimization problem can be expressed as

$$\begin{aligned} \min_{\mathbf{g}_{\mathrm{pre}}} \quad & P_s \\ \text{s.t.} \quad & \gamma_{\mathrm{B}}^{\text{N-AN}} \geq \gamma_0 \\ & P_s \leq P_{\max} \end{aligned} \tag{19}$$

where γ_0 is the SINR threshold of the legitimate receiver, $P_{\max}$ is the maximum transmission power, $P_s = \sum_{i=1}^{N}\sum_{n=0}^{3L-2}\left|g_{\mathrm{pre}}[n]\otimes g_i[n]\right|^2$ is the signal power, and $P_s + P_{\mathrm{AN}} \leq P_{\max}$. The expression of P_s can be rewritten in matrix form as

$$P_s = \sum_{i=1}^{N} \mathbf{g}_{\text{pre}}^H \mathbf{G}_i^H \mathbf{G}_i \mathbf{g}_{\text{pre}} \tag{20}$$

where $\mathbf{G}_i$ is a $(3L-2)\times(2L-1)$ -dimensional Toeplitz matrix:

$$\mathbf{G}_i = \begin{bmatrix} g_i[0] & 0 & & 0 \\ g_i[1] & g_i[0] & \ddots & \vdots \\ \vdots & g_i[1] & \ddots & \vdots \\ g_i[L-1] & \vdots & \ddots & g_i[0] \\ \vdots & g_i[L-1] & \ddots & \vdots \\ \vdots & \vdots & & g_i[L-2] \\ 0 & 0 & & g_i[L-1] \end{bmatrix} \tag{21}$$

Letting $\mathbf{A} = \sum_{i=1}^{N} \mathbf{G}_i^H \mathbf{G}_i$, we get $P_s = \mathbf{g}_{\text{pre}}^H \mathbf{A} \mathbf{g}_{\text{pre}}$. It is easy to know that $\mathbf{A}$ is a symmetric positive definite matrix. The optimization problem (19) can be re-expressed as

$$\begin{aligned} \min_{\mathbf{g}_{\text{pre}}} \quad & \mathbf{g}_{\text{pre}}^H \mathbf{A} \mathbf{g}_{\text{pre}} \\ \text{s.t.} \quad & \gamma_{\text{B}}^{\text{N-AN}} \geq \gamma_0 \\ & \mathbf{g}_{\text{pre}}^H \mathbf{A} \mathbf{g}_{\text{pre}} \leq P_{\max} \end{aligned} \tag{22}$$

It is challenging to solve the optimization problem (22) directly, so we transform the problem. Matrix $\mathbf{A}$ can be decomposed into $\mathbf{A} = \tilde{\mathbf{A}}^H \tilde{\mathbf{A}}$, where $\tilde{\mathbf{A}} = \mathbf{\Sigma}^{\frac{1}{2}} \mathbf{U}$, $\mathbf{U}$ is the matrix composed of the eigenvectors of $\mathbf{A}$, $\mathbf{\Sigma}^{\frac{1}{2}} \triangleq \text{diag}(\sqrt{\lambda_1}, \sqrt{\lambda_2}, \ldots, \sqrt{\lambda_i}, \ldots, \sqrt{\lambda_{2L-1}})$, and $\lambda_1, \lambda_2, \cdots, \lambda_{2L-1}$ are the eigenvalues of $\mathbf{A}$. Letting $\tilde{\mathbf{A}} \mathbf{g}_{\text{pre}} = \sqrt{P_s} \boldsymbol{\alpha}$, where $\boldsymbol{\alpha}$ is a column vector with 2-norm 1, we can get $P_s = \mathbf{g}_{\text{pre}}^H \mathbf{A} \mathbf{g}_{\text{pre}} = P_s \boldsymbol{\alpha}^H \boldsymbol{\alpha}$ and $\mathbf{g}_{\text{pre}} = \sqrt{P_s} \tilde{\mathbf{A}}^{-1} \boldsymbol{\alpha}$. Substituting $\sqrt{P_s} \tilde{\mathbf{A}}^{-1} \boldsymbol{\alpha}$ in (18) for $\mathbf{g}_{\text{pre}}$, the SINR of the legitimate receiver can be rewritten as

$$\gamma_{\text{B}}^{\text{N-AN}}(\boldsymbol{\alpha}, P_s) = \frac{\boldsymbol{\alpha}^H (\tilde{\mathbf{A}}^{-1})^H \mathbf{h}_{\text{B},(2L-1)} \mathbf{h}_{\text{B},(2L-1)}^H \tilde{\mathbf{A}}^{-1} \boldsymbol{\alpha}}{\boldsymbol{\alpha}^H \left(\frac{\sigma_{\text{B}}^2}{P_s} \mathbf{I} + (\tilde{\mathbf{A}}^{-1})^H \left(\sum_{l=1, l\neq(2L-1)}^{(4L-3)} \mathbf{h}_{\text{B},l} \mathbf{h}_{\text{B},l}^H \right) \tilde{\mathbf{A}}^{-1} \right) \boldsymbol{\alpha}} \tag{23}$$

Then, substituting (23) into (22) and adding a 2-norm constraint about $\boldsymbol{\alpha}$, that is, $\boldsymbol{\alpha}^H \boldsymbol{\alpha} = 1$, we can get a new form of the optimization problem as

$$\begin{aligned} \min_{\boldsymbol{\alpha}, P_s} \quad & P_s \\ \text{s.t.} \quad & \frac{\boldsymbol{\alpha}^H (\tilde{\mathbf{A}}^{-1})^H \mathbf{h}_{\text{B},(2L-1)} \mathbf{h}_{\text{B},(2L-1)}^H \tilde{\mathbf{A}}^{-1} \boldsymbol{\alpha}}{\boldsymbol{\alpha}^H \left(\frac{\sigma_{\text{B}}^2}{P_s} \mathbf{I} + (\tilde{\mathbf{A}}^{-1})^H \left(\sum_{l=1, l\neq(2L-1)}^{(4L-3)} \mathbf{h}_{\text{B},l} \mathbf{h}_{\text{B},l}^H \right) \tilde{\mathbf{A}}^{-1} \right) \boldsymbol{\alpha}} \geq \gamma_0 \\ & \boldsymbol{\alpha}^H \boldsymbol{\alpha} = 1 \\ & 0 < P_s \leq P_{\max} \end{aligned} \tag{24}$$

It can be seen that $\gamma_{\text{B}}^{\text{N-AN}}(\boldsymbol{\alpha}, P_s)$ is a generalized Rayleigh quotient, and its maximum value is the maximum generalized eigenvalue of matrix pencil $(\mathbf{\Gamma}_1, \mathbf{\Gamma}_2)$, is a monotone increasing function of P_s, where

$$\begin{aligned} \mathbf{\Gamma}_1 &= (\tilde{\mathbf{A}}^{-1})^H \mathbf{h}_{\text{B},(2L-1)} \mathbf{h}_{\text{B},(2L-1)}^H \tilde{\mathbf{A}}^{-1} \\ \mathbf{\Gamma}_2 &= \frac{\sigma_{\text{B}}^2}{P_s} \mathbf{I} + (\tilde{\mathbf{A}}^{-1})^H \left(\sum_{l=1, l\neq(2L-1)}^{(4L-3)} \mathbf{h}_{\text{B},l} \mathbf{h}_{\text{B},l}^H \right) \tilde{\mathbf{A}}^{-1} \end{aligned} \tag{25}$$

We denote the maximum value of $\gamma_{\text{B}}^{\text{N-AN}}(\boldsymbol{\alpha}, P_s)$ as $\gamma_{\text{B,max}}^{\text{N-AN}}(\boldsymbol{\alpha}\ , P_s)$. So, the minimum signal power P_s^{opt} under the SINR constraint must meet $\gamma_{\text{B,max}}^{\text{N-AN}}(\boldsymbol{\alpha}^{\text{opt}}, P_s^{\text{opt}}) = \gamma_0$, where $\boldsymbol{\alpha}^{\text{opt}}$ is the generalized eigenvector corresponding to the maximum generalized eigenvalue of the matrix pencil when $P_s = P_s^{\text{opt}}$. The binary search can be applied to find the minimum signal power efficiently. Each search is carried out in two steps. In the first step, P_s in matrix pencil $(\mathbf{\Gamma}_1, \mathbf{\Gamma}_2)$ is substituted with the middle point of the search section, and the generalized eigenvalue decomposition of the matrix pencil is done. In the second step, find the maximum generalized eigenvalue of matrix pencil and compare it with γ_0. If the eigenvalue is larger than γ_0, the upper boundary of the search section is updated with the middle point; otherwise, the lower boundary is updated with the middle point. The above two steps are repeated until the range of the search section is less than ε, which is a small positive number and determines the precision of the search. After the binary search is completed, the optimal solution of the signal power (P_s^{opt}) is the middle point of the search section. The optimal solution $\boldsymbol{\alpha}$ is the generalized eigenvector corresponding to the maximum generalized eigenvalue of the matrix pencil when $P_s = P_s^{\text{opt}}$. The optimal solution to the IR of the pre-equalizer is $\mathbf{g}_{\text{pre}}^{\text{opt}} = \sqrt{P_s^{\text{opt}}} \tilde{\mathbf{A}}^{-1} \boldsymbol{\alpha}^{\text{opt}}$, and the power of AN is $P_{\text{AN}} = P_{\max} - P_s^{\text{opt}}$. Algorithm 1 summarizes The algorithm. In Algorithm 1, u and v are the binary search's lower and upper bound, respectively. The search round of the binary search is $\log_2\left(\frac{P_{\max}}{\varepsilon}\right)$.

Algorithm 1 Search algorithm for solving the problem (24)

1) Set $u = 0$, $v = P_{\max}$.
2) **Repeat**
3) $\quad P_s = (u+v)/2$
4) $\quad$ Calculate the eigenvalues of matrix pencil (Γ_1, Γ_2).
5) $\quad$ Get $\gamma_{\text{B,max}}^{\text{N-AN}}(\boldsymbol{\alpha}\ , P_s)$ by finding the maximum generalized eigenvalue of the matrix pencil.
6) $\quad$ **If** $\gamma_{\text{B,max}}^{\text{N-AN}}(\boldsymbol{\alpha}\ , P_s) \geq \gamma_0$
   $\quad\quad v = P_s$
   $\quad$ **else**
   $\quad\quad u = P_s$
   $\quad$ **end**.
7) **Until** $v - u \leq \varepsilon$.
8) $P_s^{\text{opt}} = P_s$.
9) Get $\boldsymbol{\alpha}^{\text{opt}}$ by finding the generalized eigenvector corresponding to the maximum generalized eigenvalue of the matrix pencil (Γ_1, Γ_2).
10) $\mathbf{g}_{\text{pre}}^{\text{opt}} = \sqrt{P_s^{\text{opt}}} \tilde{\mathbf{A}}^{-1} \boldsymbol{\alpha}^{\text{opt}}$.

In Algorithm 1, $\gamma_{\text{B,max}}^{\text{N-AN}}(\boldsymbol{\alpha}\ , P_s)$ is calculated for each search, that is, to find the largest eigenvalue and the corresponding eigenvector of $\mathbf{\Gamma}$, and the complexity of this step is $O(L^3)$. After completing the search, the final solution can be obtained by substituting the result into $\mathbf{g}_{\text{pre}}^{\text{opt}} = \sqrt{P_s^{\text{opt}}} \tilde{\mathbf{A}}^{-1} \boldsymbol{\alpha}^{\text{opt}}$. Therefore, the complexity of the optimization algorithm is

$O\left(\log_2\left(\frac{P_{\max}}{\varepsilon}\right)L^3\right)$.

3.2 Scheme and optimization when ECSI is known

If the eavesdropper is one network user, ECSI can be obtained. In this case, jointly optimizing the AN's covariance matrix and the pre-equalizer's IR is the optimal scheme. However, the complexity of the optimization is very high. As a sub-optimal scheme, we adopt null-space AN and jointly optimize the covariance matrix of AN and the IR of the pre-equalizer to minimize the eavesdropper's SINR under the constraints of the minimum requirement of the legitimate receiver's SINR. Like that in Section 3.1, AN is $\mathbf{z}_{\text{AN}} = \mathbf{W}\mathbf{v}$. AN's covariance matrix is expressed as

$$\mathbf{\Phi}_{\text{AN}} = \mathbf{W}\mathbf{\Phi}_v\mathbf{W}^H \tag{26}$$

where $\mathbf{\Phi}_v = E\left\{\mathbf{v}\mathbf{v}^H\right\}$. Unlike that in Section 3.1, $\mathbf{\Phi}_v$ needs to be optimized. The optimization problem is expressed as

$$\begin{aligned}
&\min_{\mathbf{g}_{\text{pre}},\mathbf{\Phi}_v}\ \max_{n\in\{0,\ldots,M-1\}}\ \frac{\mathbf{h}_{\text{E},(2L-1)}^H\mathbf{g}_{\text{pre}}\mathbf{g}_{\text{pre}}^H\mathbf{h}_{\text{E},(2L-1)}}{\mathbf{q}_{\text{E},n}^H\mathbf{W}\mathbf{\Phi}_v\mathbf{W}^H\mathbf{q}_{\text{E},n}+\sigma_{\text{E}}^2}\\
&\text{s.t.}\ \frac{\mathbf{h}_{\text{B},(2L-1)}^H\mathbf{g}_{\text{pre}}\mathbf{g}_{\text{pre}}^H\mathbf{h}_{\text{B},(2L-1)}}{\sum_{l=1,l\neq(2L-1)}^{(4L-3)}\mathbf{h}_{\text{B},l}^H\mathbf{g}_{\text{pre}}\mathbf{g}_{\text{pre}}^H\mathbf{h}_{\text{B},l}+\sigma_{\text{B}}^2}\geq\gamma_0\\
&\quad\ \mathbf{g}_{\text{pre}}^H\mathbf{A}\mathbf{g}_{\text{pre}}+\text{Tr}\left(\mathbf{W}\mathbf{\Phi}_v\mathbf{W}^H\right)\leq P_{\max}\\
&\quad\ \mathbf{\Phi}_v\geq 0
\end{aligned}\tag{27}$$

Constraint $\mathbf{\Phi}_v \geq 0$ means that $\mathbf{\Phi}_v$ must be a positive semidefinite matrix.

Problem (27) is non-convex and is difficult to be solved. By introducing a relaxation variable t, problem (27) is transformed into

$$\begin{aligned}
&\min_{\mathbf{g}_{\text{pre}},\mathbf{\Phi}_v,t\geq 0}\ t\\
&\text{s.t.}\ \frac{\mathbf{h}_{\text{E},(2L-1)}^H\mathbf{g}_{\text{pre}}\mathbf{g}_{\text{pre}}^H\mathbf{h}_{\text{E},(2L-1)}}{\mathbf{q}_{\text{E},n}^H\mathbf{W}\mathbf{\Phi}_v\mathbf{W}^H\mathbf{q}_{\text{E},n}+\sigma_{\text{E}}^2}\leq t,\forall n\in\{0,\ldots,M-1\}\\
&\quad\ \frac{\mathbf{h}_{\text{B},(2L-1)}^H\mathbf{g}_{\text{pre}}\mathbf{g}_{\text{pre}}^H\mathbf{h}_{\text{B},(2L-1)}}{\sum_{l=1,l\neq(2L-1)}^{(4L-3)}\mathbf{h}_{\text{B},l}^H\mathbf{g}_{\text{pre}}\mathbf{g}_{\text{pre}}^H\mathbf{h}_{\text{B},l}+\sigma_{\text{B}}^2}\geq\gamma_0\\
&\quad\ \mathbf{g}_{\text{pre}}^H\mathbf{A}\mathbf{g}_{\text{pre}}+\text{Tr}\left(\mathbf{W}\mathbf{\Phi}_v\mathbf{W}^H\right)\leq P_{\max}\\
&\quad\ \mathbf{\Phi}_v\geq 0
\end{aligned}\tag{28}$$

Eq. (28) can be further rewritten as

$$\begin{aligned}
&\min_{\mathbf{g}_{\text{pre}},\mathbf{\Phi}_v,t\geq 0}\ t\\
&\text{s.t.}\ \sigma_{\text{E}}^2+\mathbf{q}_{\text{E},n}^H\mathbf{W}\mathbf{\Phi}_v\mathbf{W}^H\mathbf{q}_{\text{E},n}-\frac{1}{t}\mathbf{h}_{\text{E},(2L-1)}^H\mathbf{g}_{\text{pre}}\mathbf{g}_{\text{pre}}^H\mathbf{h}_{\text{E},(2L-1)}\geq 0\\
&\quad\ \forall n\in\{0,\ldots,M-1\}\\
&\quad\ \gamma_0\sigma_{\text{B}}^2+\gamma_0\sum_{l=1,l\neq(2L-1)}^{(4L-3)}\mathbf{h}_{\text{B},l}^H\mathbf{g}_{\text{pre}}\mathbf{g}_{\text{pre}}^H\mathbf{h}_{\text{B},l}\leq\mathbf{h}_{\text{B},(2L-1)}^H\mathbf{g}_{\text{pre}}\mathbf{g}_{\text{pre}}^H\mathbf{h}_{\text{B},(2L-1)}\\
&\quad\ \mathbf{g}_{\text{pre}}^H\mathbf{A}\mathbf{g}_{\text{pre}}+\text{Tr}\left(\mathbf{W}\mathbf{\Phi}_v\mathbf{W}^H\right)\leq P_{\max}\\
&\quad\ \mathbf{\Phi}_v\geq 0
\end{aligned}\tag{29}$$

The first and second constraints are non-convex, so the problem (29) is still non-convex. The left part of the first constraint can be regarded as the Schur complement of t in $\mathbf{T}=\begin{bmatrix} t & \mathbf{g}_{\text{pre}}^H\mathbf{h}_{\text{E},(2L-1)}\\ \mathbf{h}_{\text{E},(2L-1)}^H\mathbf{g}_{\text{pre}} & \sigma_{\text{E}}^2+\mathbf{q}_{\text{E},n}^H\mathbf{W}\mathbf{\Phi}_v\mathbf{W}^H\mathbf{q}_{\text{E},n}\end{bmatrix}$ [16]. It is easy to know that $\mathbf{T}\geq 0$ is equivalent to $t\geq 0$ and $\sigma_{\text{E}}^2+\mathbf{q}_{\text{E},n}^H\mathbf{W}\mathbf{\Phi}_v\mathbf{W}^H\mathbf{q}_{\text{E},n}-\frac{1}{t}\mathbf{h}_{\text{E},(2L-1)}^H\mathbf{g}_{\text{pre}}\mathbf{g}_{\text{pre}}^H\mathbf{h}_{\text{E},(2L-1)}\geq 0$, so the first constraint can be transformed into

$$\begin{bmatrix} t & \mathbf{g}_{\text{pre}}^H\mathbf{h}_{\text{E},(2L-1)}\\ \mathbf{h}_{\text{E},(2L-1)}^H\mathbf{g}_{\text{pre}} & \sigma_{\text{E}}^2+\mathbf{q}_{\text{E},n}^H\mathbf{W}\mathbf{\Phi}_v\mathbf{W}^H\mathbf{q}_{\text{E},n}\end{bmatrix}\geq 0 \tag{30}$$

Then, by introducing a phase constraint that represents the imaginary part of complex x, the second constraint can be changed to another form, and problem (30) is transformed into

$$\begin{aligned}
&\min_{\mathbf{g}_{\text{pre}},\mathbf{\Phi}_v,t\geq 0}\ t\\
&\text{s.t.}\ \begin{bmatrix} t & \mathbf{g}_{\text{pre}}^H\mathbf{h}_{\text{E},(2L-1)}\\ \mathbf{h}_{\text{E},(2L-1)}^H & \sigma_{\text{E}}^2+\mathbf{q}_{\text{E},n}^H\mathbf{W}\mathbf{\Phi}_v\mathbf{W}^H\mathbf{q}_{\text{E},n}\end{bmatrix}\geq 0,\forall n\in\{0,\ldots,M-1\}\\
&\quad\ \sqrt{\gamma_0\sigma_{\text{B}}^2+\gamma_0\sum_{l=1,l\neq(2L-1)}^{(4L-3)}\mathbf{h}_{\text{B},l}^H\mathbf{g}_{\text{pre}}\mathbf{g}_{\text{pre}}^H\mathbf{h}_{\text{B},l}}\leq\mathbf{h}_{\text{B},(2L-1)}^H\mathbf{g}_{\text{pre}}\\
&\quad\ \mathbf{g}_{\text{pre}}^H\mathbf{A}\mathbf{g}_{\text{pre}}+\text{Tr}\left(\mathbf{W}\mathbf{\Phi}_v\mathbf{W}^H\right)\leq P_{\max}\\
&\quad\ \text{Im}(\mathbf{h}_{\text{E},(2L-1)}^H\mathbf{g}_{\text{pre}})=0\\
&\quad\ \mathbf{\Phi}_v\geq 0.
\end{aligned}\tag{31}$$

Since any phase rotation of $\mathbf{g}_{\text{pre}}$ does not change the value of the objective function and the constraints in problem (27), problem (31) is equivalent to the problem (27). Problem (31) is a convex optimization problem that can be solved using the CVX optimization tool. The complexity of this convex optimization problem is $\sqrt{L_s+M}\cdot n\cdot\left[\left(L_s^3-M^3+8M\right)+n\cdot\left(L_s^2-M^2+4M\right)+5n^2\right]$, where $n=O\left(\left(L_s-M\right)^2+2L\right)$ [17].

4 Simulation results

In this section, the proposed scheme is evaluated by MATLAB simulation. In the simulation, all channels are Rayleigh fading channels, and specifical parameters of the channels are: the number of paths is L=10; the channel bandwidth is B=1MHz; the coefficient of each path follows the complex Gaussian random distribution with zero mean, and the variance of the path coefficients of the legitimate channel and eavesdropping channel are $E\left[\left|h_{\text{B},i}[l]\right|^2\right]=\eta_{\text{B}}\mathrm{e}^{-\frac{lT_{\text{S}}}{\sigma_{\text{T}}}}$ and $E\left[\left|h_{\text{E},i}[l]\right|^2\right]=\eta_{\text{E}}\mathrm{e}^{-\frac{lT_{\text{S}}}{\sigma_{\text{T}}}}$ respectively, where $\sigma_{\text{T}}=10/B$ is the root mean square delay of the channel, and $T_{\text{s}}=1/B$ is the sampling period. $\eta_{\text{B}}=\eta_0\left(d_{\text{B}}/d_0\right)^{-c}$ and $\eta_{\text{E}}=\eta_0\left(d_{\text{E}}/d_0\right)^{-c}$ are the large-scale fading coefficients of the legitimate channel and that of the eavesdropping channel, where c=4 is the path loss exponent, $\eta_0=10^{-5}$ is the loss at the reference distance d_0=10 m, and d_{B} and d_{E} are the distances from the transmitter to the legitimate receiver and to the eavesdropper respectively. In the simulation, we set $d_{\text{E}}=d_{\text{B}}=100\text{m}$. The legitimate receiver's SINR threshold is $\gamma_0=6\text{dB}$, the number of transmitted symbols is M=3, and the noise power of the channels is 1×10^{-11} W . The search precision in Algorithm 1 is $\varepsilon = 1\times10^{-6}$. The data given in this section are the average values under 10000 channel realizations.

Fig. 2 shows the simulation results of the average SINR at the legitimate receiver and the eavesdropper. Fig. 3 gives the simulation results of the ergodic capacities of the legitimate channel and that of the eavesdropping channel and the ergodic achievable secrecy rate. The number of transmitting antennas N is 2. It can be seen from Fig. 2 that the legitimate receiver's SINR remains unchanged and keeps at 6 dB with the increase of the total transmission power whether the ECSI is known or unknown, which indicates that the solution to the optimization problem meets the constraint of minimum SINR of the legitimate receiver. Because the legitimate receiver's SINR does not change, the capacity of the legitimate channel remains constant, as is shown in Fig. 3. Whether ECSI is known or unknown, the optimization objective is to minimize the signal power under the constraint of minimum SINR of the legitimate receiver. The signal power does not change significantly when the total transmission power increases. Still, the AN power increases synchronously, so both the eavesdropper's SINR and the capacity of the eavesdropping channel decrease. AN is radiated in all directions when ECSI is unknown, while it is radiated directly to the eavesdropper by optimizing AN's covariance matrix when ECSI is known. So, AN interferes with the eavesdropper more effectively, and its SINR is lower when ECSI is known, and a higher secrecy rate can be achieved, as is shown in Fig. 3.

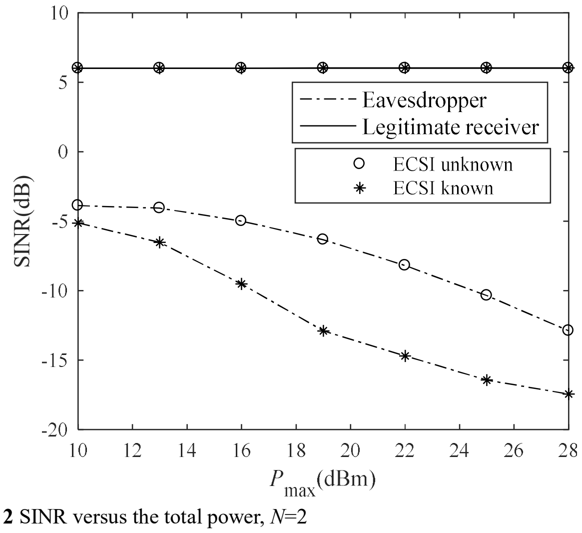


Fig. 2 SINR versus the total power, N=2

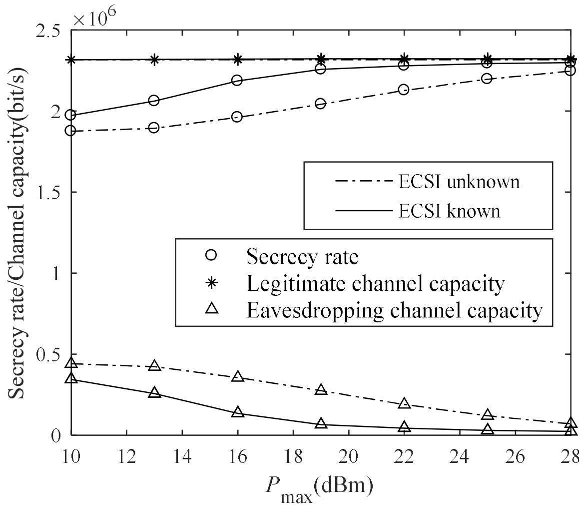


Fig. 3 Secrecy rate and channel capacity versus the total power, N=2

Fig. 4 compares the achievable secrecy rate of the proposed scheme with that of the conventional TR transmission scheme. The number of the transmitting antennas is N=4. In the traditional TR scheme, there is no pre-equalizer, and the TR pre-filters for each antenna are the matched filter of the channel from the antenna to the legitimate receiver, that is, $g_i^{\mathrm{TR}}[l] = \frac{h_{\mathrm{B},i}^*[L-1-l]}{\sqrt{N\mathbf{h}_{\mathrm{B},i}^H \mathbf{h}_{\mathrm{B},i}}}, i=1,\cdots,N$. The null-space AN is employed too, and AN's covariance matrix is obtained in the same way as the proposed scheme in this paper. The signal power meets the legitimate receiver's SINR requirement, and the remaining power is used to transmit AN. It can be seen from Fig. 4 that the secrecy rate of our proposed scheme is higher than that of the conventional TR scheme. The reason is that the pre-equalizer is optimized to minimize the signal power in the proposed scheme under the constraint of the minimum legitimate receiver's SINR, while there is no pre-equalizer and the TR pre-filters are not optimized in the conventional TR scheme, so the signal power in the proposed scheme is lower than conventional TR scheme. As a result, AN's power in the proposed scheme is higher, so the secrecy rate is higher.

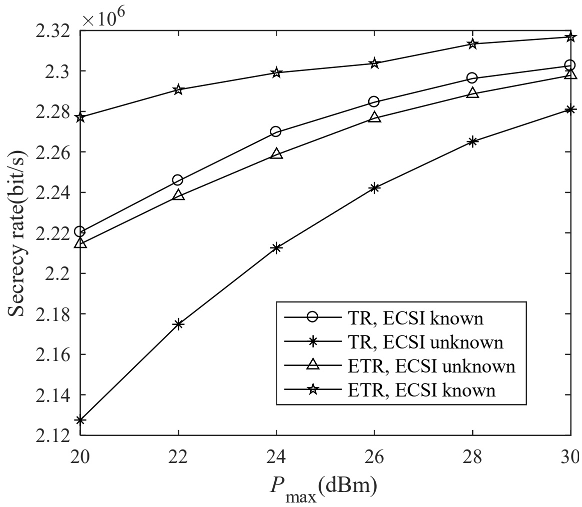
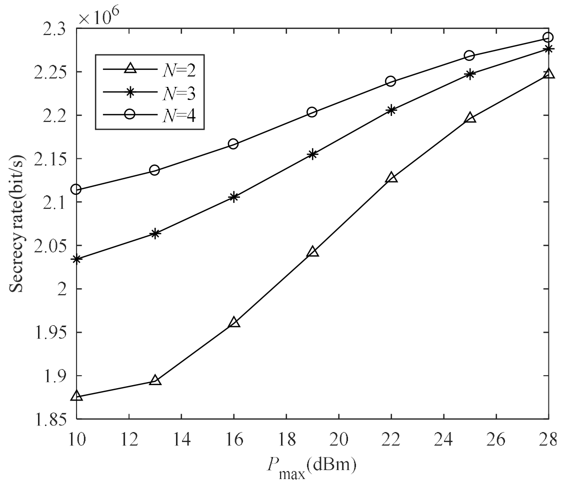
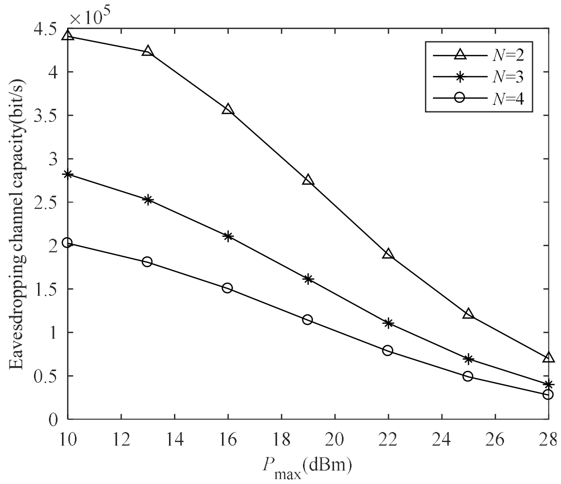


Fig. 4 Secrecy rate comparison with the conventional TR scheme, N=4

Fig. 5 and Fig. 6 are the simulation results when the transmitter is equipped with different numbers of antennas. Because the SINR of the legitimate receiver is constrained at 6 dB in the optimization, the legitimate channel capacity will not change and is the same as that in Fig. 3 even when the total transmission power and the number of the transmitting antenna are changing, so we do not show it in Figs. 5 and 6. Fig. 5(b) and 6(b) show that the more transmitting antennas there are, the lower the eavesdropping channel capacity is. This is because the more antennas there are, the larger the gain of the transmitting antenna array is, and the smaller the signal power is required to meet the SINR requirement of the legitimate receiver. As a result, AN's power increases, the SINR of the eavesdropper decreases, and so does the eavesdropping channel capacity. Since the legitimate channel capacity remains unchanged, the achievable secrecy rate increases with the number of antennas, as shown in Fig. 5(a) and 6(a).

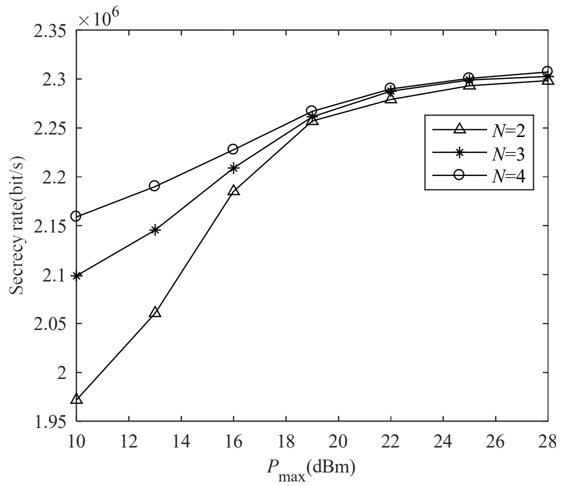


(a)

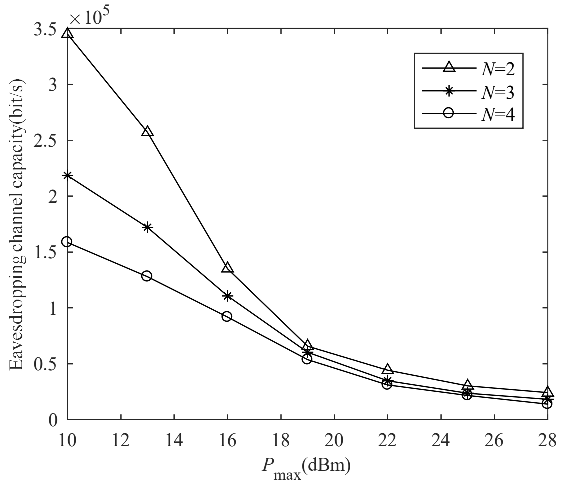


(b)

Fig. 5 Security performance with different numbers of antennas when ECSI is unknown. (a) Achievable secrecy rate. (b) Eavesdropping channel capacity.



(a)



(b)

Fig. 6 Security performance with different numbers of antennas when ECSI is known. (a) Achievable secrecy rate. (b) Eavesdropping channel capacity

5 Conclusion

In this paper, an ETR-MISO system assisted with AN is optimized to improve the secrecy rate when ECSI is known or unknown. When ECSI is unknown, the omnidirectional null-space AN is employed, and the pre-equalizer is optimized to minimize the signal power under the minimum SINR constraint of the legitimate receiver. The optimization problem is non-convex. The original optimization problem is transformed into an issue of finding the maximum generalized eigenvalue, the eigenvector corresponding to the eigenvalue, and the minimum signal power meeting the SINR constraint. When ECSI is known, the covariance matrix of null-space AN and the pre-equalizer are jointly optimized to minimize the SINR of the eavesdropper under the minimum SINR constraint of the legitimate receiver. The non-convex optimization problem is transformed by introducing a relaxation variable and changing the non-convex constraints into convex constraints; thereby, the original non-convex optimization problem is transformed into a convex optimization problem, which can be solved by using the CVX optimization tool. The proposed scheme is evaluated by simulation, and the results demonstrate that the achievable secrecy rate can be improved obviously by optimizing the pre-equalizer and AN.

Acknowledgments

This work was supported by The National Natural Science Foundation of China (No.61971080).

References

1. Rouseff D, Jackson DR, Fox WLJ, et al. Underwater acoustic c ommunication by passive-phase conjugation: theory and experime ntal results. *IEEE J Ocean Eng*. 2001; 26(4): 821-831. https://doi.org/10.1109/48.972122.
2. Wang B, Wu Y, Han F, et al. Green wireless communications: a time-reversal paradigm. *IEEE J Sel Areas Commun*. 2011; 29(8): 1698-1710. https://doi.org/10.1109/JSAC.2011.110918.
3. Lei W, Yao L. Performance analysis of time reversal communication systems. *IEEE Commun Lett*. 2019; 23(4): 680-683. https://doi.org/10.1109/LCOMM.2019.2901484.
4. Yoon E, Kim SY, Yun U. A time-reversal-based transmission using predistortion for intersymbol interference alignment. *IEEE Trans Commun*. 2015; 63(2): 455-465. https://doi.org/10.1109/TCOMM.2014.2371462.
5. Ma H, Wang B, Chen Y, et al. Waveforming optimizations for time-reversal cloud radio access networks. *IEEE Trans Commun*. 2018; 66(1): 382-393. https://doi.org/10.1109/TCOMM.2017.2753253.
6. Chen X, Ng DWK, Gerstacher WH, et al. A survey on multiple-antenna techniques for physical layer security. *IEEE Commun Surv Tutor*. 2017; 19(2): 1027-1053. https://doi.org/10.1109/COMST.2016.2633387.
7. Wang L, Li R, Cao C, et al. SNR analysis of time reversal signaling on target and unintended receivers in distributed transmission. *IEEE Trans Commun*. 2016; 64(5): 2176-2191. https://doi.org/10.1109/TCOMM.2016.2547425.
8. Lei W, Yang M, Yao L, et al. Physical layer security performance analysis of the time reversal transmission system. *IET Commun*. 2020; 14(3): 635-645. https://doi.org/10.1049/iet-com.2019.0872.
9. Tan VT, Ha DB, Tran DD. Evaluation of physical layer secrecy in MIMO ultra-wideband system using time-reversal techniques. In: 2014 IEEE Int. Conf. on Computing, Management and Telecommunications (ComManTel) IEEE; 2014: 70-74. https://doi.org/10.1109/ComManTel.2014.6825581.
10. Cao W, Lei J, Hu W, et al. Secrecy capacity achievable time reversal pre-filter in MISO communication system and the unequal secrecy protection application. *Wirel Pers Commun*. 2017; 97(4): 5427-5437.

https://doi.org/10.1007/s11277-017-4787-x.
11. Lei W, Zhang W, Yang M, et al. Optimization of pre-processing filter for time-reversal multi-user secure transmission systems based on artificial noise. *Digit Signal Prog*. 2020; 109: 1-15. https://doi.org/10.1016/j.dsp.2020.102933.
12. Li S, Li N, Tao XF, et al. Artificial noise inserted secure communication in time-reversal systems. In: 2018 IEEE Wireless Commun. Networking Conf (WCNC) IEEE; 2018: 1-6. https://doi.org/10.1109/WCNC.2018.8377356.
13. Viteri-Mera CA, Teixeira FL. Equalized time reversal beamforming for frequency-selective indoor miso channels. *IEEE Access*. 2017; 5: 3944-3957. https://doi.org/10.1109/ACCESS.2017.2682160.
14. Nguyen H, Zhao Z, Zheng F, et al. Preequalizer design for spatial multiplexing SIMO-UWB TR systems. *IEEE Trans Veh Technol*. 2010; 59(8): 3798-3805. https://doi.org/10.1109/TVT.2010.2064345.
15. Yoon M, Lee C. A TR-MISI serial pre-filter for robustness to ISI and noise in indoor wireless communication system. *IEEE Signal Process Lett*. 2014; 21(4): 386-389. https://doi.org/10.1109/LSP.2014.2303814.
16. Horn RA, Johnson CR (2013). *Matrix analysis*. Cambridge University Press.
17. Wang K, Chang T, Ma W, et al. Outage constrained robust transmit optimization for multiuser MISO downlinks: tractable approximations by conic optimization. *IEEE Transactions on Signal Processing*. 2014; 62(21): 5690-5705. https://doi.org/10.1109/TSP.2014.2354312

Statements & Declarations

Funding: This work was supported by The National Natural Science Foundation of China (No.61971080).

Competing Interests: The authors have no relevant financial or non-financial interests to disclose.

Author Contributions: All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by [Weijia Lei], [Mengting Zou], [Yue Zhang] and [Hongjiang Lei]. The first draft of the manuscript was written by [Weihan Zhang] and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.