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

Weijia Lei · Mengting Zou · Weihan Zhang · Yue Zhang · Hongjiang Lei

Accepted: 10 September 2022 / Published online: 16 October 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

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 improve 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, so the AN power and the interference with the eavesdropper are maximized. The optimization problem is transformed into the problem of finding the maximum generalized eigenvalue of a matrix pencil. 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. The optimization complexity is independent of the number of transmit antennas. 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 receiving and equalization are two technologies applied by receivers to eliminate or reduce ISI and gather the signal energy from multiple paths to enhance the signal strength. However, the 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 power 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 the time-reversed and conjugated 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. The signals from the different paths are coherently superposed at a specific moment in the intended receiver. So, there is an obvious signal peak while the delay spread is reduced and ISI is alleviated. The channel between the transmitter and any unintended receiver is not the matched filter of the pre-filtered signal, so 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 signal processing is
executed at the transmitter in TR systems, the complexity of the receiver is low.

The early research of TR transmission technology mainly focused on its application in underwater acoustic communications [1]. In recent years, TR transmission technology in wireless communications has been studied by scholars. The spatial–temporal focusing effect of TR has been verified by [2], and the experiment results proved that the leakage of radio frequency energy to unintended receivers is low in TR wireless communication systems. Although ISI is alleviated by TR pre-filtering, 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 (SNIR). In [4], a method to reduce ISI by aligning interference is studied. Pre-distortion 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. Because of the openness of wireless channels, wireless communications meet more severe security threats than wired communications. The security threats include eavesdropping, jamming, fake information, disguising, etc. [6–8]. Physical layer security (PLS) exploits the characteristics of wireless channels such as randomness, time-varying, and reciprocity to guarantee the security of information transmission by using physical layer technologies [9, 10]. The PLS technologies can be used for anti-eavesdropping, anti-jamming, key generation, identification, etc. Anti-eavesdropping is the most in-depth research field in PLS. Secrecy capacity is an important metric to evaluate the anti-eavesdropping performance of PLS. To increase the secrecy capacity, it is necessary to increase the quality advantage of the legitimate channel over the eavesdropping channel. The technologies to increase the secrecy capacity include multiple antenna pre-coding and beamforming [11], artificial noise (AN) [12], cooperative forwarding [13], etc. By beamforming, the signal is radiated to the legitimate receiver and the signal energy leaked to the eavesdropper is suppressed. AN is often employed in multi-antenna systems. By controlling AN’s radiation direction, AN 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 beamforming and AN. When the channels are multipath channels, the spatial–temporal focusing feature of TR transmission makes the signal energy focus on the target receiver. The received signal power and AN power at the legitimate receiver and the eavesdropper can be controlled by TR pre-filtering, even when there is only one antenna installed at the transmitter. Whether it is a multi-antenna or a single-antenna system, its security performance can be improved by using TR technology. The signal-to-noise ratio (SNR) of the target receiver and the unintended receiver in a distributed TR system is studied by [14]. It demonstrates that TR pre-filtering can improve security performance of the system. In [15], 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 [16], 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. [17] studies the security performance of a TR multi-user MIMO downlink system. It finds that TR beamforming can promote the secrecy capacity and is an attractive and cost-effective solution for security. It also finds that the inter-user correlation may cause a significant loss of achievable secrecy sum-rate. The conventional TR pre-processing, whose pre-filter is matched to the channel of the target receiver, can improve the signal power of the target receiver. However, from the perspective of secure transmission, it is not optimal. In [18], 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 [19], for a multi-user TR secure transmission system, two optimization schemes for the TR filters and AN are proposed respectively for the scenarios when the eavesdropping channel state information (ECSI) is known and unknown. When ECSI is unknown, null-space AN is adopted, and the TR pre-filter is optimized to minimize the signal power and AN power is maximized. When ECSI is known, TR pre-filter and AN are jointly optimized to maximize the sum secrecy rate. In [20], a secure transmission scheme combining AN with TR pre-processing is proposed, and the power allocation scheme between the signal and AN is optimized. A frequency domain TR security precoding and AN injection scheme for orthogonal frequency-division multiplexing (OFDM) systems is proposed by [21]. The TR precoder and the AN power are optimized. The simulation results of [19–21] show that AN can effectively improve the secure transmission performance of TR systems.
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. Pre-equalized time reversal (ETR) transmission scheme is proposed to reduce the optimization complexity of multi-antenna TR systems [22–25]. In ETR systems, a pre-equalizer is added ahead of the conventionally TR 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 specific performance of the system. Because only one pre-equalizer is optimized, the optimization complexity of ETR systems is much lower than that of TR systems. [22] compares the performances of the conventional TR system combined with a ZF pre-equalizer, the pure ZF system and the pure TR system, and demonstrates that the TR system combined with the pre-equalizer has the best BER performance. A theoretical bound on the BER of ZF-ETR systems has been derived in [23]. The numeric results based on the bound show that the ETR system has a better BER performance than the conventional TR system under any SNR. [24] studied the design of the pre-equalizer to mitigate ISI and the multi-stream interference for a spatial multiplexing single-input-multiple-output ETR system, according to the ZF criterion and MMSE criterion respectively. Simulation results show that the pre-equalization can considerably improve BER performance of the system. In [25], 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 multi-antenna PLS transmission systems, adopting TR pre-processing and optimizing each pre-filter can significantly improve the security performance. However, because the security performance is related to both the legitimate channel and the eavesdropping channel, the optimization of the TR pre-filters is more complicated than in non-secure 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.

For an ETR-MISO system with eavesdroppers, this paper designs an anti-eavesdropping scheme employing AN and TR pre-processing technologies. AN and the pre-equalizer are optimized to enhance the anti-eavesdropping performance when ECSI is known or unknown respectively. When ECSI is unknown, null-space AN is adopted. To maximize AN power, the pre-equalizer is optimized to minimize the signal power under the constraint of the minimum SINR of the legitimate receiver. When ECSI is known, under the constraint of the minimum SINR of the legitimate receiver, the AN covariance matrix and the pre-equalizer are optimized to minimize the SINR of the eavesdropper. To the best of our knowledge, there are not working researching the optimization of ETR PLS systems.

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. For frequency selective fading channels, CIR is a basic function to describe the channels’ characteristic. In this paper, CSI is identical to CIR. CIRs from the \( i \)-th antenna of the transmitter to the legitimate receiver and to the eavesdropper are expressed as \( h_{\text{E},i}[l] \) and \( h_{\text{E},i}[l] \), respectively, where \( l = 0, 1, \ldots, L - 1 \), and \( L \) is the CIR’s length, that is, the number of the paths of the channels. The IR of the 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 \( g_{i} = h_{\text{E},i}[L - 1 - l] \), 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 \( g_{\text{pre},i} \), where \( i = 0, 1, \ldots, 2L - 2 \). 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

\[
\mathbf{h}_{\text{E},i} = \begin{bmatrix} h_{\text{E},i}[0], & h_{\text{E},i}[1], & \ldots, & h_{\text{E},i}[L - 1] \end{bmatrix}^T \\
\mathbf{h}_{\text{B},i} = \begin{bmatrix} h_{\text{B},i}[0], & h_{\text{B},i}[1], & \ldots, & h_{\text{B},i}[L - 1] \end{bmatrix}^T \\
\mathbf{g}_{i} = \begin{bmatrix} h_{\text{B},i}[L - 1], & h_{\text{B},i}[L - 2], & \ldots, & h_{\text{B},i}[0] \end{bmatrix}^T \\
\mathbf{g}_{\text{pre},i} = \begin{bmatrix} g_{\text{pre},i}[0], & g_{\text{pre},i}[1], & \ldots, & g_{\text{pre},i}[2L - 2] \end{bmatrix}^T
\]

(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 \( E\{|x[n]|^2\} = 1 \). After filtered by the pre-equalizer and the TR pre-filters, the signals are transmitted by all antennas. The transmitter also emits AN with power \( P_{\text{AN}} \) to prevent the information from being wiretapped. The AN sequence emitted by each antenna is denoted as \( \frac{z_{\text{AN},i}[n]}{\sqrt{N}} \), where \( E\{|z[n]|^2\} = P_{\text{AN}} \). The signal sent by the \( i \)-th antenna is expressed as

\[
s_i[n] = x[n] \otimes g_{\text{pre},i}[n] \otimes g_{i}[n] + \frac{z_{\text{AN},i}[n]}{\sqrt{N}}
\]

(2)

where \( \otimes \) represents discrete convolution. The first part on the right side of (2) is the signal carrying information, and the second part is AN. The sequence length of the signal is \( L_s = M + 3L - 3 \), and the sequence length of AN is also \( L_s \). The received signal of the legitimate receiver is
Fig. 1 System model

\[ \hat{y}_B[n] = \sum_{i=1}^{N} s_i[n] \otimes h_{B,i}[n] + \tilde{z}_B[n] \]  

(3)

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

\[ \hat{y}_B[n] = \sum_{i=1}^{N} x[n] \otimes g_{pre}[n] \otimes g_i[n] \otimes h_{B,i}[n] 
+ \sum_{i=1}^{N} \frac{z_{AN}[n]}{\sqrt{N}} \otimes h_{B,i}[n] 
+ \tilde{z}_B[n] = x[n] \otimes g_{pre}[n] \otimes \sum_{i=1}^{N} \left( g_i[n] \otimes h_{B,i}[n] \right) 
+ z_{AN}[n] \otimes \sum_{i=1}^{N} \frac{h_{B,i}[n]}{\sqrt{N}} + \tilde{z}_B[n] \]  

(4)

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

\[ \hat{y}_B[n] = x[n] \otimes g_{pre}[n] \otimes h_{B,TR}[n] 
+ z_{AN}[n] \otimes h_{B,AN}[n] + \tilde{z}_B[n] \]  

(5)

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

\[ y_B[n] = \hat{y}_B[n + 2L - 2] = \sum_{l=0}^{4L-4} (g_{pre} \otimes h_{B,TR})[l] \times x[n + 2L - 2 - l] + (z_{AN} \otimes h_{B,AN})[n + 2L - 2] 
+ \tilde{z}_B[n] = (g_{pre} \otimes h_{B,TR})[2L - 2] \times x[n] 
+ \sum_{k=-(2L-2), k\neq0}^{2L-2} (g_{pre} \otimes h_{B,TR})[2L - 2 - k] \times x[n + k] + (z_{AN} \otimes h_{B,AN})[n + 2L - 2] + z_{B}[n] \]  

(6)

where \( z_B[n] = \tilde{z}_B[n + 2L - 2] \). 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 \( H_{B,TR} \) composed of \( h_{B,TR}[n] \), which is

\[ H_{B,TR} = \begin{bmatrix} 
    h_{B,TR}[0] & 0 & 0 \\
    h_{B,TR}[1] & h_{B,TR}[0] & \ddots & \vdots \\
    \vdots & h_{B,TR}[1] & \ddots & \vdots \\
    h_{B,TR}[2L-2] & \vdots & \ddots & h_{B,TR}[0] \\
    \vdots & \vdots & \ddots & h_{B,TR}[2L-2] \\
    h_{B,TR}[2L-3] & \vdots & \ddots & \vdots \\
    0 & 0 & \ddots & h_{B,TR}[2L-2] 
\end{bmatrix} \]  

(7)

Furthermore, we denote \( h_{B,i} \) as the transpose of the \( l \)-th row of \( H_{B,TR} \). We also define a \((L_x + L - 1) \times L_x\)-dimensional Toeplitz matrix \( H_{B,AN} \) which is composed of \( h_{B,AN}[n] \), which is expressed as

\[ H_{B,AN} = \begin{bmatrix} 
    h_{B,AN}[0] & 0 & 0 \\
    h_{B,AN}[1] & h_{B,AN}[0] & \ddots & \vdots \\
    \vdots & h_{B,AN}[1] & \ddots & \vdots \\
    h_{B,AN}[L-1] & \vdots & \ddots & h_{B,AN}[0] \\
    \vdots & \vdots & \ddots & h_{B,AN}[L-1] \\
    \vdots & \vdots & \ddots & \vdots \\
    0 & 0 & \ddots & h_{B,AN}[L-1] 
\end{bmatrix} \]  

(8)

Letting \( q_{B,n}^T = \hat{e}_{n+2L-1}^T H_{B,AN} \), where \( \hat{e}_{n+2L-1}^T \) is the \((n + 2L - 1)\)-th row of the identity matrix \( I_{(L_x+L-1) \times (L_x+L-1)} \), (6) can be rewritten as
\[ y_B[n] = h_{B,(2L-1)}^T g_{pre} x[n] \]
\[ + \sum_{l=-(2L-2), l \neq 0}^{(2L-2)} h_{B,(2L-1)+l}^T g_{pre} x[n+l] \]
\[ + z_{AN}^T q_{B,n} + z_B[n] \]  \hspace{1cm} (9)

where \( z_{AN} = [z_{AN}[0], z_{AN}[1], \ldots, z_{AN}[L_s - 1]]^T \) is the vector form of the AN sequence. The SINR of the symbol \( y_B[n] \) is

\[ \gamma_B[n] = \frac{h_{B,(2L-1)}^H g_{pre} H B,(2L-1)}{\sum_{l=1, l \neq (2L-1)}^{(4L-3)} h_{B,l}^H g_{pre} H B,l + q_{B,n}^T \Phi_{AN} q_{B,n} + \sigma_B^2} \]  \hspace{1cm} (10)

where \( \Phi_{AN} = E\{z_{AN} z_{AN}^H\} \) is the covariance matrix of AN, and \( (X)^H \) represents the conjugate transpose of matrix or vector \( X \).

Similarly, a \((4L-3) \times (2L-1)\)-dimensional Toeplitz matrix \( H_{E,TR} \) is defined as

\[
H_{E,TR} = \begin{bmatrix}
    h_{E,TR}[0] & 0 & 0 \\
    h_{E,TR}[1] & h_{E,TR}[0] & \cdot & \cdot & \cdot \\
    \vdots & \vdots & \ddots & \vdots & \vdots \\
    h_{E,TR}[2L-2] & \cdot & \cdot & h_{E,TR}[0] \\
    \vdots & \vdots & \vdots & \vdots & \vdots \\
    0 & 0 & \cdots & h_{E,TR}[2L-1] \\
\end{bmatrix}
\]  \hspace{1cm} (11)

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

\[
H_{E,AN} = \begin{bmatrix}
    h_{E,AN}[0] & 0 & 0 \\
    h_{E,AN}[1] & h_{E,AN}[0] & \cdot & \cdot & \cdot \\
    \vdots & \vdots & \ddots & \vdots & \vdots \\
    h_{E,AN}[L-1] & \cdot & \cdot & h_{E,AN}[0] \\
    \vdots & \vdots & \vdots & \vdots & \vdots \\
    0 & 0 & \cdots & h_{E,AN}[L-2] \\
\end{bmatrix}
\]  \hspace{1cm} (12)

where \( h_{E,AN}[n] = \sum_{i=1}^{N} h_{E,i}[n] \). Letting \( q_{E,n}^T = e_{n+2L-1}^T H_{E,AN} \), the sampled sequence of the eavesdropper is expressed as

\[ y_E[n] = h_{E,(2L-1)}^T g_{pre} x[n] \]
\[ + \sum_{l=-(2L-2), l \neq 0}^{(2L-2)} h_{E,(2L-1)+l}^T g_{pre} x[n+l] \]
\[ + z_{AN}^T q_{E,n} + z_E[n] \]  \hspace{1cm} (13)

where \( z_E[n] \) is the complex Gaussian channel noise with variance \( \sigma_E^2 \). The SINR of the symbol \( y_E[n] \) is

\[ \gamma_E[n] = \frac{h_{E,(2L-1)}^H g_{pre} H E,(2L-1)}{q_{E,n}^H \Phi_{AN} q_{E,n} + \sigma_E^2} \]  \hspace{1cm} (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 metrics to measure the performance of PLS systems and is widely adopted in the research of PLS, which is the difference between the legitimate channel’s capacity and the eavesdropping channel’s capacity:

\[ R_s = \left[ B \log_2(1 + \gamma_B) - B \log_2(1 + \gamma_E) \right]^+ \]  \hspace{1cm} (15)

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

### 3 Scheme and optimization algorithm

In this paper, it is assumed that the CSI of the legitimate channel, that is, \( h_{B,i}, i \in \{1, \ldots, N\} \) is known, and the CSI of the eavesdropping channel–EC2s, that is, \( h_{E,i}, i \in \{1, \ldots, N\} \) is either known or unknown. The security schemes are designed and optimized for the two scenarios respectively.

#### 3.1 Scheme and optimization when EC2s is unknown

AN is widely used in PLS systems. When EC2s is unknown, AN should be radiated in all directions. In order not to interfere with the legitimate receiver, AN is arranged in the null space of the legitimate channel. The expression of the...
received AN at the legitimate receiver in (6) can be rewritten as

\[ y_{AN} = Q_{AN} H_{B,AN} z_{AN} \]  

(16)

where \( Q_{AN} \) is an \( M \times (L_s + L - 1) \)-dimensional sparse matrix, and only the elements of \( Q_{AN} \) 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, to not interfere with the legitimate receiver, AN should be \( z_{AN} = Wv \), where \( W \) is the base of the null-space of \( Q_{AN} H_{B,AN} \) with dimension \( N_{AN} = L_s - M \), and \( v \) is a Gaussian random vector with the covariance matrix \( \Phi_{N\cdot AN} = E\{vv^H\} = \frac{P_{AN}}{N_{AN}} I_{(N_{AN} \times N_{AN})} \). The covariance matrix of AN is expressed as

\[ \Phi_{AN} = W \Phi_{N\cdot AN} W^H = \frac{P_{AN}}{N_{AN}} W W^H \]  

(17)

In this case, the SINR of the legitimate receiver is

\[ \gamma_{B}^{N\cdot AN} = \frac{h_{B, (2L-1)}^H g_{pre} \Phi_{B, (2L-1)} h_{B, (2L-1)} \sigma_B^2}{(4L-3) \sum_{l=1,l\neq(2L-1)} h_{B, l}^H g_{pre} \Phi_{B, l} h_{B, l} + \sigma_B^2} \]  

(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 transmit power limit and the minimum SINR requirement of the legitimate receiver. In this way, the power of AN will be maximized and the eavesdropper is disturbed in the most degree. The optimization problem can be expressed as

\[
\begin{align*}
\min_{g_{pre}} P_{s} \\
\text{s.t. } \gamma_{B}^{N\cdot AN} \geq \gamma_0 \\
\end{align*}
\]  

(19)

where \( \gamma_0 \) is the SINR threshold of the legitimate receiver, \( P_{\text{max}} \) is the maximum transmit power, \( P_s = \sum_{i=1}^{N} \sum_{n=0}^{3L-2} |g_{\text{pre}}[n] \otimes g_{i}[n]|^2 \) is the signal power, and \( P_{AN} \leq P_{\text{max}} \). The expression of \( P_s \) can be rewritten in matrix form as

\[ P_s = \sum_{i=1}^{N} g_{pre}^H G_i g_{pre} \]  

(20)

where \( G_i \) is a \((3L-2) \times (2L-1)\)-dimensional Toeplitz matrix:

\[
G_i = \begin{bmatrix}
g_{i}[0] & 0 & 0 \\
g_{i}[1] & g_{i}[0] & \ddots & \vdots \\
\vdots & g_{i}[1] & \ddots & \vdots \\
g_{i}[L-1] & \ddots & \ddots & g_{i}[0] \\
0 & \ddots & \ddots & g_{i}[L-2] \\
0 & 0 & g_{i}[L-1] & \end{bmatrix}
\]  

(21)

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

\[
\begin{align*}
\min_{g_{\text{pre}}} P_{s} \\
\text{s.t. } \gamma_{B}^{N\cdot AN} \geq \gamma_0 \\
P_{\text{pre}} g_{\text{pre}}^H g_{\text{pre}} \leq P_{\text{max}}
\end{align*}
\]  

(22)

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

\[
\gamma_{B}^{N\cdot AN}(\alpha, P_s) = \frac{\alpha^H (\tilde{A}^{-1})^H h_{B, (2L-1)}^H h_{B, (2L-1)}^H \tilde{A}^{-1} \alpha}{\alpha^H \left( \frac{\sigma_B^2}{P_{\text{pre}}} I + (\tilde{A}^{-1})^H \left( \sum_{l=1,l\neq(2L-1)} h_{B, l}^H h_{B, l}^H \right) \tilde{A}^{-1} \right) \alpha}
\]  

(23)

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

\[
\begin{align*}
\min_{\alpha, P_s} P_s \\
\text{s.t. } \alpha^H (\tilde{A}^{-1})^H h_{B, (2L-1)}^H h_{B, (2L-1)}^H \tilde{A}^{-1} \alpha \geq \gamma_0 \\
\alpha^H \left( \frac{\sigma_B^2}{P_{\text{pre}}} I + (\tilde{A}^{-1})^H \left( \sum_{l=1,l\neq(2L-1)} h_{B, l}^H h_{B, l}^H \right) \tilde{A}^{-1} \right) \alpha \geq \gamma_0 \\
\alpha^H \alpha = 1 \\
0 < P_s \leq P_{\text{max}}
\end{align*}
\]  

(24)
It can be found that $γ_B^{N-AN}(α, P_s)$ is a generalized Rayleigh quotient, and its maximum value is the maximum generalized eigenvalue of matrix pencil $(Γ_1, Γ_2)$ and is a monotone increasing function of $P_s$, where

$$Γ_1 = (\tilde{A}^{-1})^Hh_B(2L-1)h_B^H(2L-1)\tilde{A}^{-1},$$

$$Γ_2 = \frac{γ^2}{P_s}I + (\tilde{A}^{-1})^H\left(\sum_{i=1,i\neq(2L-1)}^{(4L-3)}h_B_i h_B_i^H\right)\tilde{A}^{-1}$$

(25)

We denote the maximum value of $γ_B^{N-AN}(α, P_s)$ as $γ_B^{N-AN}(α, P_s)$. So, the minimum signal power $P_s^{opt}$ under the SINR constraint must meet $γ_B^{N-AN}(α^{opt}, P_s^{opt}) = γ_0$, where $α^{opt}$ is the generalized eigenvector corresponding to the maximum generalized eigenvalue of the matrix pencil when $P_s = P_s^{opt}$. 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 $(Γ_1, Γ_2)$ 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, we 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 $α$ is the eigenvalue eigenvector corresponding to the maximum generalized eigenvalue of the matrix pencil when $P_s = P_s^{opt}$. The optimal solution to the IR of the pre-equalizer is $γ_0^{opt} = \sqrt{P_s^{opt}A^{-1}α^{opt}}$, and the power of AN is $P_{AN} = P^{max} - P_s^{opt}$. Algorithm is summarized in Table 1 as Algorithm 1. In Algorithm 1, $u$ and $v$ are the lower and upper bound of binary searching, respectively.

In Algorithm 1, $γ_B^{N-AN}(α, P_s)$ is calculated for each search round, and the complexity of one round is $O(L^3)$. The search round of binary searching is $\log_2\left(\frac{P_{max}}{ε}\right)$. After the search, the final solution is obtained by substituting $α^{opt}$ into $γ_0^{opt} = \sqrt{P_s^{opt}A^{-1}α^{opt}}$. Therefore, the complexity of the optimization algorithm is $O\left(\log_2\left(\frac{P_{max}}{ε}\right)\right)$. [27]

### 3.2 Scheme and optimization when ECSI is known

If the eavesdropper a user of the network, ECSI can be obtained. In this case, it is optimal that the AN’s covariance matrix and the pre-equalizer’s IR are jointly optimized to maximize the secrecy rate. 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. As that in Sect. 3.1, AN is $z_{AN} = Wv$. AN’s covariance matrix is expressed as

$$Φ_{AN} = WvW^H$$

(26)

where $Φ_v = E\{vv^H\}$. Unlike that in Sect. 3.1, $Φ_v$ needs to be optimized. The optimization problem is expressed as

$$\min_{γ_{pre}, Φ_v, n \in \{0, \ldots, M-1\}} \frac{h_{E,n}^Hg_{pre,n}h_{E,(2L-1)}}{Q_{E,n}W_{E,v}W_{E,v}^Hq_{E,n} + \sigma_v^2}$$

s.t.

$$\frac{h_{B,n}^Hg_{pre,n}h_{B,(2L-1)}}{(4L-3)^{\sum_{l=1,i\neq(2L-1)}(4L-3)}} \geq γ_0$$

$$γ_{pre}^Hg_{pre}^H + Tr(WvW^H) \leq P_{max}$$

$$Φ_v \succeq 0$$

Constraint $Φ_v \succeq 0$ means that $Φ_v$ 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

\[
\begin{align*}
\min_{g_{\text{rec}}, \Phi_v, t \geq 0} & & t \\
\text{s.t.} & & h_{E, (L-1)}^H g_{\text{pre}}^H h_{E, (L-1)} + \sigma_E^2 + q_{E,n}^H W_8 W^H q_{E,n} \\ & & \leq t, \forall n \in \{0, \ldots, M - 1\} \\
& & h_{B, (L-1)}^H g_{\text{pre}}^H h_{B, (L-1)} + \sigma_B^2 \\ & & \geq \gamma_0 \\
& & \sum_{l=1, l \neq (L-1)} h_{B,l}^H g_{\text{pre}}^H h_{B,l} \\ & & \leq h_{B, (L-1)}^H g_{\text{pre}}^H h_{B, (L-1)} + \sigma_B^2 \\ & & \mu_{\text{pre}} Ag_{\text{pre}} + \text{Tr}(W_8 W^H) \leq P_{\text{max}} \\
& & \Phi_v \geq 0
\end{align*}
\]

(28)

(28) can be further rewritten as

\[
\begin{align*}
\min_{g_{\text{pre}}, \Phi_v, t \geq 0} & & t \sigma_E^2 + q_{E,n}^H W_8 W^H q_{E,n} \\
& & - \frac{1}{l} h_{E, (L-1)}^H g_{\text{pre}}^H h_{E, (L-1)} \\ & & \geq 0, \forall n \in \{0, \ldots, M - 1\} \\
& & \gamma_0 \\
& & \sum_{l=1, l \neq (L-1)} h_{B,l}^H g_{\text{pre}}^H h_{B,l} \\ & & \leq h_{B, (L-1)}^H g_{\text{pre}}^H h_{B, (L-1)} + \sigma_B^2 \\ & & \mu_{\text{pre}} Ag_{\text{pre}} + \text{Tr}(W_8 W^H) \leq P_{\text{max}} \\
& & \Phi_v \geq 0
\end{align*}
\]

(29)

The first and second constraints are non-convex, so the problem (29) is still non-convex. The left side of the first constraint can be regarded as the Schur complement of \( t \) in [26]

\[
T = \begin{bmatrix}
t \\
h_{E, (L-1)}^H g_{\text{pre}}^H h_{E, (L-1)} + \sigma_E^2 + q_{E,n}^H W_8 W^H q_{E,n}
\end{bmatrix}
\]

(30)

It is easy to know that \( T \geq 0 \) is equivalent to \( t \geq 0 \) and \( \sigma_E^2 + q_{E,n}^H W_8 W^H q_{E,n} - \frac{1}{l} h_{E, (L-1)}^H g_{\text{pre}}^H h_{E, (L-1)} \geq 0 \), so the first constraint can be transformed into

\[
\begin{bmatrix}
t \\
h_{E, (L-1)}^H g_{\text{pre}}^H h_{E, (L-1)} + \sigma_E^2 + q_{E,n}^H W_8 W^H q_{E,n}
\end{bmatrix} \geq 0
\]

(31)

Then, by introducing a phase constraint, the second constraint can be changed to another form, and problem (30) is transformed into

\[
\begin{align*}
\min_{g_{\text{rec}}, \Phi_v, t \geq 0} & & t \\
\text{s.t.} & & h_{E, (L-1)}^H g_{\text{pre}}^H h_{E, (L-1)} + \sigma_E^2 + q_{E,n}^H W_8 W^H q_{E,n} \\ & & \geq 0, \forall n \in \{0, \ldots, M - 1\} \\
& & \gamma_0 (\sigma_B^2 + \gamma_0) \\
& & \sum_{l=1, l \neq (L-1)} h_{B,l}^H g_{\text{pre}}^H h_{B,l} \leq h_{B, (L-1)}^H g_{\text{pre}}^H h_{B, (L-1)} + \sigma_B^2 \\
& & \mu_{\text{pre}} Ag_{\text{pre}} + \text{Tr}(W_8 W^H) \leq P_{\text{max}} \\
& & \Phi_v \geq 0
\end{align*}
\]

(32)

Since any phase rotation of \( g_{\text{pre}} \) does not change the value of the objective function and the constraints in problem (27), problem (32) is equivalent to the problem (27). Problem (32) is a convex optimization problem that can be solved using the CVX optimization tool.

The complexity of this convex optimization problem is listed in Table 2. For comparison, the complexities of the algorithms proposed by [19] and [20] are also given. [19] and [20] optimize the TR filters and AN to improve the PLS performance. It can be found that the complexity of our proposed scheme is independent of the number of antennas \( N \), while the complexities of the schemes of [19] and [20] are proportional to \( N^3 \). The more the antennas are, the larger complexity advantage of our scheme is.

### 4 Simulation results

In this section, the proposed scheme is evaluated by MATLAB simulation. In the simulation, all channels are Rayleigh fading channels, and the parameters of the channels are: the number of paths is \( L = 10 \); the channel bandwidth is \( B = 1 \text{ MHz} \); 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 \( E\left[ \left| h_{B,l}[i]\right|^2 \right] = \eta_B e^{-j\theta_B} \) and \( E\left[ \left| h_{E,l}[i]\right|^2 \right] = \eta_E e^{-j\theta_E} \) respectively, where \( f \sigma_T = 10/B \) is the root mean square delay of the channel, and \( T_s = 1/B \) is the sampling period. \( \eta_B = \eta_0 (d_B/d_0)^{-c} \) and \( \eta_E = \eta_0 (d_E/d_0)^{-c} \) 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 \( d_0 = 10 \text{ m} \), 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
Table 2 Complexity of different schemes

| Scheme               | Complexity                                                                 |
|----------------------|-----------------------------------------------------------------------------|
|                      | ESI is known                                                               |
|                      | $O\left(n_0 \sqrt{n_0} \left[N^3 L^3 + n_0^3\right] + n_0 \left(N^2 L^2 + n_0^2\right)\right)$ |
|                      | $\text{ESI is unknown}$                                                    |
|                      | $O\left(N L^3 \sqrt{L} \left(N^2 + NL\right)\right)$                     |
|                     | $n_0 = M + NL$                                                               |
| [20]                | $O\left(c_0 c_1 \left[\left(ML^2 + L_0^2 + N^3 L^3\right) + c_1^1\right]\right)$ |
|                      | $c_0 = \log_2 \left(\frac{P_{\max}}{\epsilon}\right) \sqrt{ML + NL + L_0}$ |
|                      | $c_1 = L_0^2 + L_0$                                                        |
| This work           | $O\left(L^2 \sqrt{L + M}\right)$                                         |
|                      | $\text{ESI is unknown}$                                                    |
|                      | $O\left(\log_2 \left(\frac{P_{\max}}{\epsilon}\right) L^3\right)$       |

$d_E = d_B = 100m$. 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 $1 \times 10^{-11} \text{W}$. The search precision in Algorithm 1 is $\epsilon = 1 \times 10^{-6}$. The data given in this section are the average values under 10,000 channel realizations.

Figure 2 shows the simulation results of the average SINR at the legitimate receiver and the eavesdropper. Figure 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 transmit 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 transmit 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 constraint of the optimization is the minimum SINR of the legitimate receiver. Because AN is in the null space of the legitimate channel and the AN power is zero in the legitimate receiver, so the signal power does not change as the total transmit power increases. When ECSI is known, the SINR of the eavesdropper is minimized. When ECSI is unknown, the AN power is maximized. So, in both scenarios, the AN power increases and the SINR of the eavesdropper decreases as the total transmit power increases. 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, when ECSI is known, AN interferes with the eavesdropper more effectively and its SINR is lower and a higher secrecy rate can be achieved, as is shown in Figs. 2 and 3.

Figure 4 compares the achievable secrecy rate of the proposed scheme with that of the conventional TR transmission scheme. The number of the transmit 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, $g_i^{\text{TR}}[l] = \frac{h_{B,i}[L-l]}{\sqrt{|h_{B,i}|^2 + h_{B,j}}}, i = 1, \ldots, N$. 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, the AN power in the proposed scheme is higher, so the secrecy rate is higher. The comparison indicates that the optimization of the pre-equalizer can improve security performance significantly.

Figure 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 transmits power and the number of the transmit antenna are changing, so we do not show it in Figs. 5 and 6. Figures 5b and 6b show that the more transmit antennas there are, the lower the eavesdropping channel capacity is. This is because the more antennas there are, the larger the gain of the transmit antenna array is, and the smaller the signal power is required to meet the SINR requirement of the legitimate receiver. As a result, the AN power increases and the SINR of the eavesdropper decreases, so the eavesdropping channel capacity decreases. Since the legitimate channel capacity remains unchanged, the achievable secrecy rate increases with the number of antennas, as shown in Figs. 5a and 6a. The performance gain brought by installing more transmit antennas decreases as the transmit power increases. The higher

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

Fig. 5 Security performance with different numbers of antennas when ECSI is unknown. a Achievable secrecy rate. b Eavesdropping channel capacity.
channel, so it does not interfere with the legitimate receiver. When ECSI is unknown, the pre-equalizer is optimized to minimize the transmit power under the constraint of the minimum SINR of the legitimate receiver and the AN power is maximized. The optimization problem is transformed into the problem of finding the maximum generalized eigenvalue of a matrix pencil and the minimum signal power. When ECSI is known, the covariance matrix of the 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 optimization problem is non-convex. By introducing a relaxation variable and transforming the non-convex constraints into convex constraints, the original 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. The simulation results show that the secrecy rate of the system can be significantly promoted by optimizing the pre-equalizer and the power allocation of the signal and AN, and the more the transmit antennas, the higher the secrecy rate. In the proposed scheme, only one pre-equalizer needs to be optimized, so the optimization complexity is significantly lower than those of the schemes in which all TR pre-filters need to be jointly optimized. The optimization complexity of the proposed scheme is independent of the number of the transmit antennas, so the configuration of the transmit antennas is not limited by the optimization complexity.

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

Author’s contribution All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by [WL], [MZ], [YZ] and [HL]. The first draft of the manuscript was written by [WZ] and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

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

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose.

References

1. Rouseff, D., Jackson, D. R., Fox, W., Jones, C., Ritcey, J., & Dowling, D. (2001). Underwater acoustic communication by passive-phase conjugation: Theory and experimental results. IEEE Journal of Oceanic Engineering, 26(4), 821–831. https://doi.org/10.1109/48.972122
2. Wang, B., Wu, Y., Han, F., Yang, Y. H., & Liu, K. J. (2011). Green wireless communications: A time-reversal paradigm. IEEE Journal
on Selected Areas in Communications, 29(8), 1698–1710. https://doi.org/10.1109/JSAC.2011.110918
3. Lei, W., & Yao, L. (2019). Performance analysis of time reversal communication systems. *IEEE Communication Letters*, 23(4), 680–683. https://doi.org/10.1109/LCOMM.2019.2901484
4. Yoon, E., Kim, S. Y., & Yun, U. (2015). A time-reversal-based transmission using predistortion for intersymbol interference alignment. *IEEE Transactions on Communications*, 63(2), 455–465. https://doi.org/10.1109/TCOMM.2014.2371462
5. Ma, H., Wang, B., Chen, Y., Liu, K. J., & Ray. (2017). Waveforming optimizations for time-reversal radio access networks. *IEEE Transactions on Communications*, 66(1), 382–393. https://doi.org/10.1109/TCOMM.2017.2753253
6. Rajkumar, P. V., & Ravi, S. (2016). Poster: security enhanced administrative role based access control models. The 2016 ACM SIGSAC Conference, 1802–1804. doi: https://doi.org/10.1145/2976749.2989068.
7. Rajkumar, P. V., & Ravi, S. (2016). Safety decidability for pre-authorization usage control with finite attribute domains. *IEEE Transactions on Dependable and Secure Computing*, 13(5), 582–590. https://doi.org/10.1109/TDSC.2015.2427834
8. Rajkumar, P. V., & Ravi, S. (2020). Safety decidability for pre-authorization usage control with identifier attribute domains. *IEEE Transactions on Dependable and Secure Computing*, 17(3), 465–478. https://doi.org/10.1109/TDSC.2018.2839745
9. Ajayi, I., Medjahdi, Y., Kaddour, F., & Mroueh, L. (2021). Impact of imperfect channel state information on physical layer security by precoding and diversity. 2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (pp.322–327). doi: https://doi.org/10.23919/ECECSI53397.2021.9624230
10. Djordjevic, I. (2022). Physical-layer security for wireless and optical channels. *Advanced Optical and Wireless Communications Systems*, 45, 713–760. https://doi.org/10.1007/978-3-030-98491-5_11
11. Chen, X., Ng, D., Gerstacher, W. H., & Hsiao, H. (2017). A survey on multiple-antenna techniques for physical layer security. *IEEE Communication Survey & Tutorials*, 19(2), 1027–1053. https://doi.org/10.1109/COMST.2016.2633387
12. Li, D., Ma, X., & Han, W. (2021). A point-to-point security communication system: artificial noise jamming insertion. 14. 2021 IEEE 9th International Conference on Information Communication and Networks, 139–143. doi: https://doi.org/10.1109/ICICN52636.2021.9673871.
13. Zhang, C., Ge, J., Gong, F., Ji, Y., & Li, J. (2019). Improving physical-layer security for wireless communication systems using duality-aware two-way relay cooperation. *IEEE Systems Journal*, 13(2), 1241–1249. https://doi.org/10.1109/JSYST.2018.2864778
14. Wang, L., Li, R., Cao, C., & Stubber, G. (2016). SNR analysis of time reversal signaling on target and unintended receivers in distributed transmission. *IEEE Transactions on Communications*, 64(5), 2176–2191. https://doi.org/10.1109/TCOMM.2016.2547425
15. Lei, W., Yang, M., Yao, L., & Lei, H. (2020). Physical layer security performance analysis of the time reversal transmission system. *IET Communications*, 14(4), 635–645. https://doi.org/10.1049/iet-com.2019.0872
16. Tan, Y. T., Ha, D. B., & Tran, D.D. (2014). Evaluation of physical layer secrecy in MIMO ultra-wideband system using time-reversal techniques. 2014 International Conference on Computing, Management and Telecommunications, ComManTel 2014 (pp.70–74). doi: https://doi.org/10.1109/ComManTel.2014.6825581.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.
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.

Mengting Zou received the B.Sc. degree in communication engineering from the Henan Normal University, Xinxiang, China, in 2020. She is currently working toward the M.Sc. degree in electronics and communications engineering from the Chongqing University of Posts and Telecommunications, Chongqing, China. Her research focuses on physical layer security.

Weihan Zhang received the B.Sc. degree in communication engineering from the Chongqing University of Posts and Telecommunications, Chongqing, China, in 2019, the M.Sc. degree in information and communication engineering from the Chongqing University of Posts and Telecommunications, Chongqing, China, in 2022. His research focuses on physical layer security.

Hongjiang Lei received the B.Sc. degree in mechanical and electrical engineering from the Shenyang Institute of Aeronautical Engineering, Shenyang, China, in 1998, the M.Sc. degree in computer application technology from Southwest Jiaotong University, Chengdu, China, in 2004, and the Ph.D. degree in instrument science and technology from Chongqing University, Chongqing, China, in 2015. In 2004, he joined the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, where he is currently an Associate Professor.

Yue Zhang received the B.Sc. degree in internet of things engineering from Jiangxi Science and Technology Normal University, Jiangxi, China, in 2019, the M.Sc. degree in information and communication engineering from the Chongqing University of Posts and Telecommunications, Chongqing, China, in 2022. Her research focuses on non-orthogonal multiple access.