

# Mixed secure autoprecoder design for MIMO broadcast channel with confidential messages

Che Jiaqi, Wang Qiang (✉), Luo Hongtao

School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

## Abstract

Deep learning (DL) exhibits great potential in addressing the nonconvex optimization challenges for secure precoding in multiple-input multiple-output (MIMO) communication systems. However, existing studies rarely consider the internal eavesdropping threat where legitimate users may intercept confidential messages intended for other users. To fill this gap, a mixed secure autoprecoder (MSAP) approach is proposed for two-user MIMO broadcast channels with confidential messages. The MSAP jointly designs a data-driven autoencoder (AE) and a model-driven zero-forcing (ZF) constraint to optimize the transmitter and receivers simultaneously, ensuring that each user's signal is nulled at the unintended receiver to guarantee confidentiality. Extensive simulation results demonstrate that the MSAP achieves stronger security against legitimate eavesdroppers and lower symbol error rate (SER) for reliable transmission, and outperforms existing schemes.

**Keywords** multiple-input multiple-output (MIMO) broadcast channel, physical layer security, autoencoder (AE), zero-forcing (ZF), confidential messages

## 1 Introduction

MIMO is a multi-antenna technology that employs multiple antennas at both the transmitter and the receiver. Compared with single-input single-output (SISO) systems, MIMO transmits multiple independent data streams<sup>[1]</sup>. In MIMO communication systems, optimization problems associated with precoding often exhibit nonconvexity<sup>[2]</sup>. The computational complexity of traditional iterative methods increases with the number of antennas and users significantly. This increase limits their practical

applicability. Introducing DL can significantly improve the latency introduced by high-dimensional spatial calculation with offline pretraining<sup>[3–4]</sup>.

Recently, a DL-based transmission architecture named AE has shown great potential for end-to-end encoding and decoding. This architecture avoids complex optimization procedures<sup>[5]</sup>. Its main advantage is independence from specific input distributions and channel models. It also enables joint optimization of the transmitter and receiver in a data-driven manner<sup>[6–8]</sup>. In Ref. [6], AE is first applied to the design of a MIMO spatial multiplexing communication system. In Ref. [7], an AE architecture incorporating singular value decomposition (SVD) is proposed to improve AE performance in MIMO systems. Moreover, an AE for the MIMO broadcast channel (AE-BC) is proposed in Ref. [8]. The results verify that AE-BC

provides a low-complexity solution with satisfactory performance.

Although AE simplifies the design of communication systems, it also faces security challenges inherent in traditional wireless communication. Wireless communications are inherently open. As a result, sensitive information may be eavesdropped during transmission<sup>[9–10]</sup>. To resist eavesdropping risk, secure transceivers based on AE are studied in Refs. [11–12]. For the SISO Gaussian wiretap channel, an AE-based method is proposed in Ref. [11]. This method enhances security by clustering the transmitter constellation and misleading symbol detection at external eavesdroppers. In Ref. [12], an adversarial learning (AL)-enhanced AE is proposed. This approach protects information security against attacks from external eavesdroppers. However, the above studies only consider external eavesdroppers and cannot deal with the threats of legitimate receiver eavesdropping. Specifically, eavesdroppers are not always illegal entities outside the communication system. Instead, a legitimate receiver of a message may act as an eavesdropper for other messages<sup>[13]</sup>. MIMO broadcast channel with confidential messages is studied as a special secure scenario without external eavesdroppers<sup>[14]</sup>. Due to competition among legitimate users, the precoder design faces additional constraints and challenges.

In this paper, MSAP approach was proposed for two-user MIMO broadcast channels. The goal is to protect confidential messages from legitimate receiver eavesdropping. Simulation results demonstrate that MSAP outperforms existing AE-based methods in terms of security. This improvement is reflected by a lower eavesdropping success rate at unintended receivers. In addition, MSAP effectively reduces inter-user interference, which further decreases the SERs of intended receivers. Contributions are summarized as follows.

1) Sequential integration of neural networks (NNs) and ZF techniques is performed to develop secure precoders. The strong nonlinear fitting capability and trainable nature of NNs are exploited for adaptive precoding optimization, while ZF is employed to

eliminate information leakage and avoid competitive interference between users.

2) Independent power constraints are set for each user's confidential message to avoid information leakage.

3) Considering the coupling between modulation and precoding in multi-antenna transceivers, an end-to-end learning approach is adopted to jointly optimize both transmitter and receivers, thereby reducing the SERs at the intended receivers.

## 2 System model

Consider a two-user MIMO broadcast channel with confidential messages<sup>[13–14]</sup>, where a single transmitter simultaneously serves two receivers, as shown in Fig. 1.

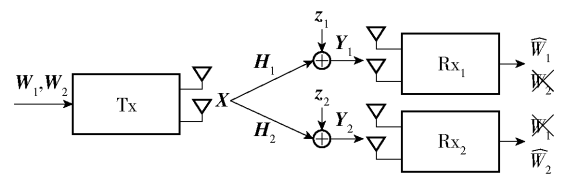


**Fig. 1** System model of the two-user MIMO broadcast channel with confidential messages

The transmitter, receiver 1, and receiver 2 are represented by Tx, Rx<sub>1</sub>, and Rx<sub>2</sub>, respectively, and are equipped with  $n_t$ ,  $n_1$ , and  $n_2$  antennas, where  $n_t \geq n_1 + n_2$ . The Tx sends two confidential messages  $\mathbf{W}_1$  and  $\mathbf{W}_2$  to Rx<sub>1</sub> and Rx<sub>2</sub>, respectively. Message  $\mathbf{W}_i = (w_{i1}, w_{i2}, \dots, w_{ij})$ ,  $i \in \{1, 2\}$  consists of  $J$  elements, where the  $j$ th element  $w_{ij}$  is chosen from the set  $\mathcal{W}_i = \{1, 2, \dots, 2^{R_i}\}$ , where  $R_i$  denotes the length of the message  $\mathbf{W}_i$ . Each receiver Rx<sub>i</sub> can only decode the corresponding confidential message  $\mathbf{W}_i$ , but cannot decode other messages. To prevent the risk of message eavesdropping between receivers, the Tx maps the confidential message  $\mathbf{W}_i$  into the transmission signal  $\mathbf{X} \in \mathbb{C}^{n_t \times 1}$  by the method of physical layer security. And  $\mathbf{X} \in \mathbb{C}^{n_t \times 1}$  is subject to a total transmit power constraint  $P_t$ , where  $P_t$  is the maximum transmit power. To truly reflect the channel scattering characteristics and be close to the actual propagation environment, the Saleh-Valenzuela channel model is utilized<sup>[15]</sup>. Let define  $\mathbf{H}_1 \in \mathbb{C}^{n_1 \times n_t}$  and  $\mathbf{H}_2 \in \mathbb{C}^{n_2 \times n_t}$  as the complex channel

matrices from Tx to Rx<sub>1</sub> and Rx<sub>2</sub>, respectively, which can be written as

$$\mathbf{H}_i = \sqrt{\frac{n_i n_i}{N_{pi}}} \sum_{l=1}^{N_{pi}} \alpha_{i,l} \mathbf{a}_i(\varphi_{i,l}) \mathbf{a}_t^H(\theta_{i,l}); \quad i=1,2 \quad (1)$$

where  $N_{pi}$  is the number of propagation path from Tx to the Rx<sub>i</sub>.  $\alpha_{i,l}$ ,  $\varphi_{i,l}$ , and  $\theta_{i,l}$  are the channel gain, angle-of-arrival (AoA), and angle-of-departure (AoD) of the  $l$ th path, respectively. When configured as the uniform linear array (ULA), the response vector  $\mathbf{a}_t(\theta_{i,l})$  and  $\mathbf{a}_i(\varphi_{i,l})$  of the antenna array at the receivers and transmitter can be expressed as<sup>[15]</sup>

$$\mathbf{a}_t(\theta_{i,l}) = \sqrt{\frac{1}{n_i}} \left[ 1, e^{j\frac{2\pi}{\lambda} \tilde{d} \sin \theta_{i,l}}, \dots, e^{j\frac{2\pi}{\lambda} \tilde{d} (n_i-1) \sin \theta_{i,l}} \right]^T; \quad i=1,2 \quad (2)$$

$$\mathbf{a}_i(\varphi_{i,l}) = \sqrt{\frac{1}{n_i}} \left[ 1, e^{j\frac{2\pi}{\lambda} \tilde{d} \sin \varphi_{i,l}}, \dots, e^{j\frac{2\pi}{\lambda} \tilde{d} (n_i-1) \sin \varphi_{i,l}} \right]^T; \quad i=1,2 \quad (3)$$

where  $\lambda$  is the wavelength and  $\tilde{d}$  is the space between adjacent antennas.

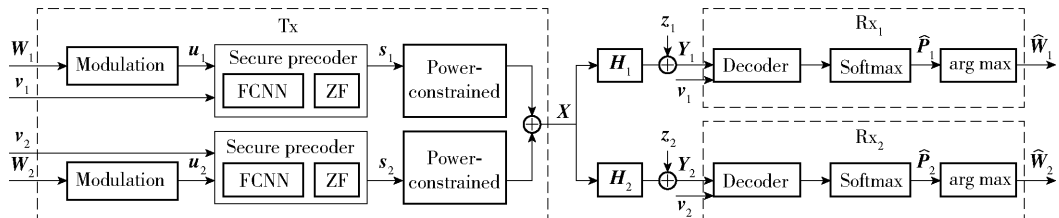


Fig. 2 MSAP architecture under the two-user MIMO broadcast channels

### 1) Network input

The Tx sends a message  $\mathbf{W}_1$  of  $R_1$  bits and a message  $\mathbf{W}_2$  of  $R_2$  bits to Rx<sub>1</sub> and Rx<sub>2</sub>, respectively. In addition to the messages to be transmitted, channel characteristic sequences  $\mathbf{v}_1$  and  $\mathbf{v}_2$  are added to the inputs of the transmitter and receivers to facilitate the networks to efficiently precode and decode. The channel characteristic sequences are defined as

$$\mathbf{v}_1 = V([\mathbf{H}_1 \mathbf{H}_2^\perp]) \quad \mathbf{v}_2 = V([\mathbf{H}_2 \mathbf{H}_1^\perp]) \quad (5)$$

where  $V(\cdot)$  denotes the vectorization of the matrix,  $\mathbf{H}_1^\perp \in \mathbb{C}^{n_i \times (n_i - n_1)}$  and  $\mathbf{H}_2^\perp \in \mathbb{C}^{n_i \times (n_i - n_2)}$  are the null spaces of  $\mathbf{H}_1$  and  $\mathbf{H}_2$ , respectively.

### 2) Transmitter design

Two modulation modules are constructed using fully connected neural networks (FCNNs). The modulated

The confidential messages of two users are transmitted in the same time slot, and both the transmitter and the receivers have instantaneous channel state information (CSI). The received signals  $\mathbf{Y}_1 \in \mathbb{C}^{n_1 \times 1}$  and  $\mathbf{Y}_2 \in \mathbb{C}^{n_2 \times 1}$  at Rx<sub>1</sub> and Rx<sub>2</sub> are denoted as

$$\begin{cases} \mathbf{Y}_1 = \mathbf{H}_1 \mathbf{X} + \mathbf{z}_1 \\ \mathbf{Y}_2 = \mathbf{H}_2 \mathbf{X} + \mathbf{z}_2 \end{cases} \quad (4)$$

where  $\mathbf{z}_i \sim N(0, \sigma_i^2)$ ,  $i=1,2$  is additive white Gaussian noise (AWGN),  $\sigma_i^2$  is the power of noise.

## 3 MSAP design

### 3.1 Architecture of the MSAP

In this section, secure precoders are designed, and the end-to-end learning framework is adopted to optimize the whole system. The architecture of the MSAP is shown in Fig. 2.

signal  $\mathbf{u}_i \in \mathbb{C}^{J \times 1}$  can be expressed as a function of the confidential message.

$$\mathbf{u}_i = M_i(\mathbf{W}_i) \quad (6)$$

where  $M_i(\cdot)$  represents the  $i$ th modulation function, which is composed of an  $E$ -layer NN.

$$\mathbf{u}_i = F_{M_i}^E(F_{M_i}^{E-1}(\dots F_{M_i}^1(\mathbf{W}_i))) \quad (7)$$

where  $F_{M_i}^e(x) = \sigma_{M_i}^e(\mathbf{K}_{M_i}^e x + \mathbf{b}_{M_i}^e)$  represents the NN calculation process at the  $e$ th layer of  $M_i(\cdot)$ .  $\sigma_{M_i}^e(\cdot)$ ,  $\mathbf{K}_{M_i}^e$ , and  $\mathbf{b}_{M_i}^e$  are the activation function, the weights, and the bias of each layer of  $M_i(\cdot)$ , respectively.

To ensure that the messages received by intended receivers remain confidential and are indecipherable to unintended receivers, two secure precoders are developed using FCNNs and ZF. Precoded signals  $\mathbf{s}_1 \in \mathbb{C}^{n_1 \times 1}$  and  $\mathbf{s}_2 \in \mathbb{C}^{n_2 \times 1}$  can be denoted as

$$\begin{cases} \mathbf{s}_1 = \mathbf{H}_2^\perp P_1(\mathbf{u}_1, \mathbf{v}_1) \\ \mathbf{s}_2 = \mathbf{H}_1^\perp P_2(\mathbf{u}_2, \mathbf{v}_2) \end{cases} \quad (8)$$

where  $P_1(\cdot)$  and  $P_2(\cdot)$  are  $G$ -layer precoding NNs.  $\mathbf{u}_i$  and  $\mathbf{v}_i$  are input to the precoding NNs in concatenated form.

The FCNNs have the characteristic of unbounded output, they cannot directly control the power output of the transmitter. Therefore, power constraint layers are designed to ensure that the signal power output by the transmitter meets the constraint conditions. To achieve the independent transmission of messages, a power split factor  $\gamma \in [0, 1]$  is introduced to independently allocate  $\gamma P_t$  and  $(1 - \gamma)P_t$  to the confidential messages of the two receivers. And the precoded signals  $\mathbf{s}_1$  and  $\mathbf{s}_2$  are adjusted through power limiting factors  $\beta_1$  and  $\beta_2$  to achieve power control. The power limiting factors  $\beta_1$  and  $\beta_2$  are defined as

$$\begin{cases} \beta_1 = \frac{\min(\sqrt{\gamma P_t}, |\mathbf{s}_1|)}{|\mathbf{s}_1|} \\ \beta_2 = \frac{\min(\sqrt{(1 - \gamma)P_t}, |\mathbf{s}_2|)}{|\mathbf{s}_2|} \end{cases} \quad (9)$$

The final output of the transmitter is given by

$$\mathbf{X} = \beta_1 \mathbf{s}_1 + \beta_2 \mathbf{s}_2 = \frac{\min(\sqrt{\gamma P_t}, |\mathbf{s}_1|)}{|\mathbf{s}_1|} \mathbf{s}_1 + \frac{\min(\sqrt{(1 - \gamma)P_t}, |\mathbf{s}_2|)}{|\mathbf{s}_2|} \mathbf{s}_2 \quad (10)$$

where the power of signals  $\beta_1 \mathbf{s}_1$  and  $\beta_2 \mathbf{s}_2$  are limited to  $\gamma P_t$  and  $(1 - \gamma)P_t$ , respectively, while the output  $\mathbf{X}$  satisfies the constraint of  $P_t$ .

Applying Eq. (9) to Eq. (3), the signals at the two receivers  $\mathbf{Y}_1$  and  $\mathbf{Y}_2$  can be expressed as

$$\begin{cases} \mathbf{Y}_1 = \mathbf{H}_1 \mathbf{X} + \mathbf{z}_1 = \mathbf{H}_1 (\beta_1 \mathbf{H}_2^\perp P_1(\mathbf{u}_1, \mathbf{v}_1) + \beta_2 \mathbf{H}_1^\perp \cdot \\ \quad P_2(\mathbf{u}_2, \mathbf{v}_2)) + \mathbf{z}_1 = \beta_1 \mathbf{H}_1 \mathbf{H}_2^\perp P_1(M_1(\mathbf{W}_1), \mathbf{v}_1) + \mathbf{z}_1 \\ \mathbf{Y}_2 = \mathbf{H}_2 \mathbf{X} + \mathbf{z}_2 = \mathbf{H}_2 (\beta_2 \mathbf{H}_1^\perp P_2(\mathbf{u}_2, \mathbf{v}_2) + \beta_1 \mathbf{H}_2^\perp \cdot \\ \quad P_1(\mathbf{u}_1, \mathbf{v}_1)) + \mathbf{z}_2 = \beta_2 \mathbf{H}_2 \mathbf{H}_1^\perp P_2(M_2(\mathbf{W}_2), \mathbf{v}_2) + \mathbf{z}_2 \end{cases} \quad (11)$$

where the received signals  $\mathbf{Y}_1$  and  $\mathbf{Y}_2$  do not contain any unintended message components. The transmitter design satisfies the strict requirements of confidential transmission.

### 3) Receiver design

Decoders  $D_1$  and  $D_2$  are responsible for decoding the

received signals  $\mathbf{Y}_1$  and  $\mathbf{Y}_2$ , respectively.  $D_1$  and  $D_2$  are constructed by  $Q$ -layer, which take the received signals  $\mathbf{Y}_1$  and  $\mathbf{Y}_2$  and the channel feature sequences  $\mathbf{v}_1$  and  $\mathbf{v}_2$  as inputs. They are fed into the decoders in a concatenated form. The decoded signal  $\mathbf{d}_i$  can be expressed as

$$\mathbf{d}_i = F_{D_i}^Q(F_{D_i}^{Q-1}(\dots F_{D_i}^1(\mathbf{Y}_i, \mathbf{v}_i))) \quad (12)$$

where  $F_{D_i}^q(x) = \sigma_{D_i}^q(K_{D_i}^q x + \mathbf{b}_{D_i}^q)$ ,  $q = 1, 2, \dots, Q$ , represents the NN calculation process at the  $q$ th layer of  $D_i$ .  $K_{D_i}^q$  and  $\mathbf{b}_{D_i}^q$  are the weights and the bias at each layer of  $D_i$ , respectively.  $\sigma_{D_i}^q(\cdot)$  represents the activation function. Next, the softmax activation function maps the outputs of the decoders to probability matrices  $\hat{\mathbf{P}}_1 \in \mathbb{R}^{J \times 2^{R_1}}$  and  $\hat{\mathbf{P}}_2 \in \mathbb{R}^{J \times 2^{R_2}}$ , set  $k$  as the index of a symbol in set  $w_i$ , the element in the  $j$ th row and  $k$ th column of the probability matrix represents the probability that the  $j$ th transmitted symbol is received as the  $k$ th symbol.

#### 4) Loss function

In MSAP, each receiver needs to decode and estimate the transmitted messages. The whole loss function is  $L = L_1 + L_2$ , where  $L_1$  and  $L_2$  are the loss functions at  $Rx_1$  and  $Rx_2$ , respectively. In order to correctly decode the corresponding message, cross-entropy (CE) is adopted to train the networks.

$$L_i = -\frac{1}{J} \sum_{j=1}^J \sum_{k=1}^{2^{R_i}} P_{i,j,k} \ln \hat{P}_{i,j,k} \quad (13)$$

where  $i \in \{1, 2\}$  represents the  $i$ th receiver,  $P_{i,j,k} \in \{0, 1\}$  is the element located at the  $j$ th row and the  $k$ th column of the one-hot encoding matrix  $\mathbf{P}_i^m \in \mathbb{R}^{J \times 2^{R_i}}$  for the confidential message  $\mathbf{W}_i$ . For example,  $P_{i,j,k} = 1$  when  $k = w_{ij} \in w_i$ , and  $P_{i,j,k} = 0$  otherwise. Similarly,  $\hat{P}_{i,j,k}$  is the element located at the  $j$ th row and  $k$ th column of the received probability matrices  $\hat{\mathbf{P}}_i \in \mathbb{R}^{J \times 2^{R_i}}$  at the  $Rx_i$ . The loss is minimized through end-to-end training, which reduces the SERs of message transmission.

### 3.2 Training procedure of the MSAP

First, channel matrices are randomly generated using Eq. (1). In the training process, the channel layers are the non-trainable layers between the Tx and the  $Rx_i$ . The channel matrices  $\mathbf{H}_1$  and  $\mathbf{H}_2$  serve as the weights of the channel layers of  $Rx_1$  and  $Rx_2$ , respectively. The transmitter is responsible for mapping

the confidential messages  $\mathbf{W}_i$  and channel characteristic sequences  $\mathbf{v}_i$  into the transmitted signal  $\mathbf{X}$ . After the signal passes through the channel layers, Gaussian white noises with power of  $\sigma_1^2$  and  $\sigma_2^2$  are added at the two receivers. The sub-networks of the transmitter and receivers are trained simultaneously. Each training epoch covers all possible channel matrices, allowing MSAP to adapt to any channel. Finally, when the SERs for both receivers stabilize and stop decreasing, it indicates that convergence of the NNs has been achieved.

### 3.3 Computational complexity comparison

The online computational complexity of MSAP is analyzed and compared with that of AE-BC<sup>[8]</sup>. The computational complexity of the MSAP transmitter comes from the modulator and precoder. For the modulator and precoder of  $\mathbf{W}_i$ , let  $T_{M_{i,e}}$  and  $T_{P_{i,g}}$  represent the number of neurons in the  $e$ th layer and  $g$ th layer, respectively. As for the modulator, the computational complexity of the  $\mathbf{W}_i$  modulator can be expressed as  $C_{M_i} = O \left( JT_{M_{i,1}} + \sum_{e=1}^{E-1} T_{M_{i,e}} T_{M_{i,e+1}} \right)$ . Computing the null space of a matrix of size  $n_i \times n_t$  requires  $4n_i^2(3n_t - n_i)$  flops<sup>[16]</sup>. As for the precoder, the computational complexity of the  $\mathbf{W}_i$  precoder can be expressed as  $C_{P_i} = O \left( (2n_i(n_t - n_{3-i}) + 2J)T_{P_{i,1}} + \sum_{g=1}^{G-2} T_{P_{i,g}} T_{P_{i,g+1}} + 2(n_t - n_{3-i})T_{P_{i,G-1}} + 4n_{3-i}^2(3n_t - n_{3-i}) + n_t(n_t - n_{3-i}) \right)$ . Then, the computational complexity of the transmitter can be expressed as  $C_T = \sum_{i=1}^2 (C_{M_i} + C_{P_i})$ . Let  $T_{D_{i,q}}$  be the number of neurons in the  $q$ th layer of the  $i$ th receiver. The computational complexity of the  $i$ th receiver is  $C_{D_i} = O \left( (2n_i(n_t - n_{3-i}) + 2n_i)T_{D_{i,1}} + \sum_{q=1}^{Q-2} T_{D_{i,q}} T_{D_{i,q+1}} + 2^{R_i} JT_{D_{i,Q-1}} \right)$ . From the analysis above, it can be seen that increasing the number of neurons will bring significant overhead. The MSAP approach eliminates user interference using the ZF, which in turn decreases the NN scale requirement. Since the number of neurons is quadratic to the computation, MSAP using small-scale NNs

requires much less computation than AE-BC using large-scale NNs. When the number of antennas is relatively small, the computation increase from the ZF is negligible. It can be concluded that the MSAP approach has computational advantages.

## 4 Simulation result

### 4.1 Simulation parameters of the system

To simulate and evaluate the MSAP approach, a MIMO broadcast system with  $n_1 = n_2 = n_r$  is constructed. To avoid overly large training datasets, one symbol is transmitted from Tx to each receiver, i. e.,  $J = 1$ . Each symbol contains 3 bit of data, i. e.,  $R_1 = R_2 = 3$ . The maximum transmit power is set to  $P_t = 2$  W. Assume that the space between antenna units in ULA is equivalent to half of the wavelength. The channel gain distribution for the  $l$ th propagation path at  $Rx_i$  is defined as  $\alpha_{i,l} \in N(0.5 + 0.5j, 1)$ . For each propagation path, the AoD and AoA at  $Rx_i$  are uniformly distributed as  $\theta_{i,l} \in U(-40^\circ, 40^\circ)$ ,  $\varphi_{i,l} \in U(-40^\circ, 40^\circ)$ , where  $i \in \{1, 2\}$ . And assume that  $\mathbf{H}_1$  and  $\mathbf{H}_2$  are not significantly correlated with each other. Each modulation consists of a four-layer NN,  $E = 4$ . Each precoder consists of a five-layer NN,  $G = 5$ . Each decoder consists of a five-layer NN,  $Q = 5$ . The NN parameters used in each module of MSAP are shown in Table 1. The rectified linear unit (ReLU) is adopted as the activation function of the hidden layers. Furthermore, intelligent eavesdroppers mentioned in Ref. [12] are deployed at the  $Rx_1$  and  $Rx_2$  to simulate potential eavesdropping behaviors in real-world scenarios.

**Table 1** NN parameters in MSAP

| NN           | Hidden layer      | Output layer   |
|--------------|-------------------|----------------|
| $M_1(\cdot)$ | 128, 128, 64      | $2J$           |
| $M_2(\cdot)$ | 128, 128, 64      | $2J$           |
| $P_1(\cdot)$ | 256, 256, 128, 64 | $2(n_t - n_2)$ |
| $P_2(\cdot)$ | 256, 256, 128, 64 | $2(n_t - n_1)$ |
| $D_1$        | 256, 256, 128, 64 | $2^{R_1} J$    |
| $D_2$        | 256, 256, 128, 64 | $2^{R_2} J$    |

The security of confidential message transmission is measured by evaluating the SERs of these eavesdroppers. During both the training and testing

phases, over 10 000 pairs of distinct channels are generated.

#### 4.2 Evaluation of security and reliability

Fig. 3 shows the SER of the intended and unintended receivers using different methods and two antenna configurations with the power split factor  $\gamma = 0.5$  and the propagation path number  $N_{p1} = N_{p2} = 1$ .

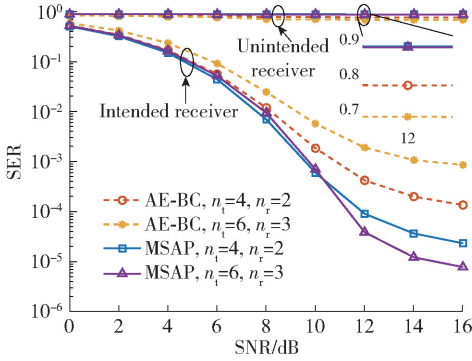


**Fig.3** SER vs. SNR for MSAP and AE-BC with  $N_{p1} = N_{p2} = 1$

Fig. 4 shows the SER of the intended and unintended receivers with different propagation path numbers.

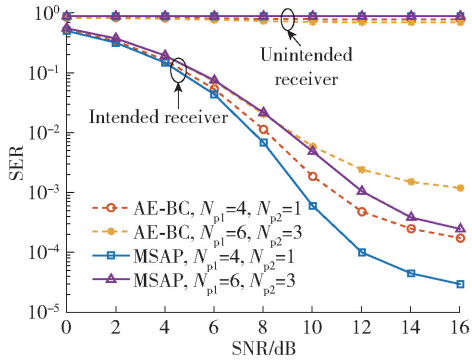


**Fig.4** SER vs. SNR for MSAP and AE-BC with  $n_t = 4$  and  $n_r = 2$

From Figs. 3 – 4, the results indicate that the MSAP performs better than the AE-BC across various system conditions, with performance improvements increasing as the signal-to-noise ratio (SNR) rises. Specifically, when  $n_t = 4$ ,  $n_r = 2$ , and SNR is 12 dB, message transmission SER reduces by 78% for intended receivers, while the eavesdropping success rate drops by 11% relative to the benchmark results. This improvement is because the MSAP eliminates information leakage and reduces mutual interference

between users. With the expansion of channel matrices, the processing capability of the AE-BC NN is insufficient to cope with increasingly complex channel environments, resulting in its performance in terms of security and reliability being inferior to when  $n_t = 4$  and  $n_r = 2$ . In addition, due to the greater computational complexity of multi-path channels, the performance of both methods declines, the MSAP is still better than the AE-BC benchmark. The MSAP uses ZF to eliminate interference, enabling the NNs to avoid dealing with user interference. Thus, it still maintains high security and reliability.

Fig. 5 shows the SER of the confidential messages  $W_1$  and  $W_2$  decoded at the intended and unintended receivers versus the power split factor  $\gamma$  when  $n_t = 4$ ,  $n_r = 2$ , and SNR is 8 dB. It is obvious that the SER of the intended receiver of  $W_1$  decreases monotonically as  $\gamma$  increases. The SER of the intended receiver of  $W_2$  increases monotonically as  $\gamma$  increases. As expected, allocating more power to the confidential message increases its relative SNR, which in turn enhances transmission accuracy.

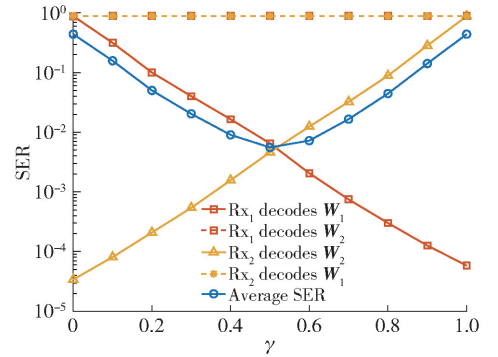


**Fig.5** SER vs.  $\gamma$  for MSAP

To further explore the reasons behind the performance improvements of the MSAP, Fig. 6 shows the constellations of the confidential message received by the intended and unintended receivers. The results show that the MSAP makes the signals received by the unintended receivers contain only noise without any information, which renders the confidential messages indecipherable. As Figs. 6 (a) and 6 (c) show, MSAP makes more efficient use of the limited constellation space than the benchmark, further improving communication reliability. As a result, after end-to-end joint optimization, the performance of the

MSAP is better than the benchmark.

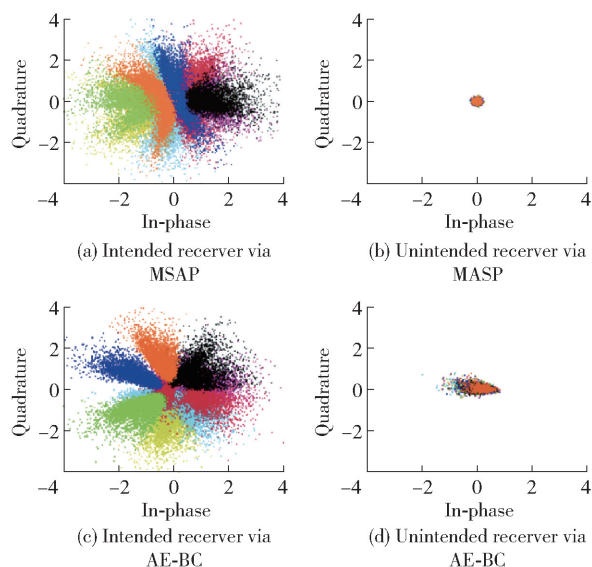


**Fig. 6** Constellations of confidential messages with  $n_t = 4$  and  $n_r = 2$

## 5 Conclusions

To protect confidential messages from legitimate receiver eavesdropping, a secure autoprecoder approach called MSAP is proposed for two-user MIMO broadcast channels with confidential messages. Specifically, MSAP uses NNs and ZF to build secure precoders, which significantly improves the security of confidential message transmission. End-to-end learning is used to jointly optimize the NNs of the transmitter and receivers to ensure the reliability of message transmission. Simulation results show that, when there are 4 transmitting antennas, 2 receiving antennas and SNR of 12 dB, MSAP outperforms the AE-BC method. It cuts the SER of normal message transmission by 78%. Meanwhile, the eavesdropping success rate falls by 11%.

## Acknowledgements

This work was supported by the National Key Research and Development Program of China (2020YFB1806602), the National Natural Science Foundation of China (62071066).

## References

[1] ZHANG Z Q, XIAO Y, MA Z, et al. 6G wireless networks: vision, requirements, architecture, and key technologies. *IEEE*

*Vehicular Technology Magazine*, 2019, 14(3): 28–41.

[2] YU W, SOHRABI F, JIANG T. Role of deep learning in wireless communications. *IEEE Information Theory Magazine*, 2022, 2(2): 56–72.

[3] PAULS J, VAEZI M. Secure precoding in MIMO-NOMA: a deep learning approach. *IEEE Wireless Communications Letters*, 2022, 11(1): 77–80.

[4] ZHANG S, LIU Y S, GAO F F, et al. Deep learning based channel extrapolation for large-scale antenna systems: opportunities, challenges and solutions. *IEEE Wireless Communications*, 2021, 28(6): 160–167.

[5] O'SHEA T, HOYDIS J. An introduction to deep learning for the physical layer. *IEEE Transactions on Cognitive Communications and Networking*, 2017, 3(4): 563–575.

[6] O'SHEA T J, ERPEK T, CLANCY T C. Deep learning-based MIMO communications. *arXiv Preprint*, arXiv:1707.07980, 2017.

[7] ZHANG X L, VAEZI M, O'SHEA T J. SVD-embedded deep autoencoder for MIMO communications. *Proceedings of the 2022 IEEE International Conference on Communications (ICC'22)*, 2022, May 16–20, Seoul, Republic of Korea. Piscataway, NJ, USA: IEEE, 2022: 5190–5195.

[8] SONG J X, HÄGER C, SCHRÖDER J, et al. Benchmarking and interpreting end-to-end learning of MIMO and multi-user communication. *IEEE Transactions on Wireless Communications*, 2022, 21(9): 7287–7298.

[9] QI Y, VAEZI M. Secure transmission in MIMO-NOMA networks. *IEEE Communications Letters*, 2020, 24(12): 2696–2700.

[10] LI B, FEI Z S, ZHOU C Q, et al. Physical-layer security in space information networks: a survey. *IEEE Internet of Things Journal*, 2020, 7(1): 33–52.

[11] FRITSCHKE R, SCHAEFER R F, WUNDER G. Deep learning for the Gaussian wiretap channel. *Proceedings of the 2019 IEEE International Conference on Communications (ICC'19)*, 2019, May 20–24, Shanghai, China. Piscataway, NJ, USA: IEEE, 2019: 6p.

[12] WANG X Y, ZHENG Z, FEI Z S. ASAP: adversarial learning based secure autoprecoder design for MIMO wiretap channels. *IEEE Wireless Communications Letters*, 2022, 11(9): 1915–1919.

[13] GOLDFELD Z, PERMUTER H H. MIMO Gaussian broadcast channels with common, private, and confidential messages. *IEEE Transactions on Information Theory*, 2019, 65(4): 2525–2544.

[14] WANG Q, ZHANG T J, DONG D L, et al. Secure degrees of freedom of rank-deficient BCCM and rank-deficient ICCM. *IEEE Transactions on Vehicular Technology*, 2020, 69(4): 4033–4041.

[15] SOHRABI F, YU W. Hybrid digital and analog beamforming design for large-scale antenna arrays. *IEEE Journal of Selected Topics in Signal Processing*, 2016, 10(3): 501–513.

[16] TRAN L N, JUNTTI M, BENGTTSSON M, et al. Successive zero-forcing DPC with sum power constraint: low-complexity optimal designs. *Proceedings of the 2012 IEEE International Conference on Communications (ICC'12)*, 2012, Jun 10–15, Ottawa, Canada. Piscataway, NJ, USA: IEEE, 2012: 4857–4861.

(Editor: Wang Xuying)