A Cooperative Jamming Based Joint Transceiver Design for Secure Communications in MIMO Interference Channels

Boyang Huang[1,2], Zhengmin Kong[2],Yanjun Fang[2] and Xin Jin[1]
[1] Electric of Power Research Institute, China Southern Power Grid Co Ltd.,
Guangzhou, Guangdong 510663, China,
[e-mail: byhuang_whu@whu.edu.cn, jinxin1@csg.cn]
[2] School of Electrical Engineering and Automation, Wuhan University,
Wuhan, Hubei 430072, China,
[e-mail: zmkong@whu.edu.cn, yjfang@whu.edu.cn]
*Corresponding author: Zhengmin Kong

Received April 18, 2018; revised September 23, 2018; accepted November 7, 2018; published April 30, 2019

Abstract

In this paper, we investigate the problem of secure communications in multiple-input-multiple-output interference networks from the perspective of physical layer security. Specifically, the legitimate transmitter-receiver pairs are divided into different categories of active and inactive. To enhance the security performances of active pairs, inactive pairs serve as cooperative jammers and broadcast artificial noises to interfere with the eavesdropper. Besides, active pairs improve their own security by using joint transceivers. The encoding of active pairs and inactive pairs are designed by maximizing the difference of mean-squared errors between active pairs and the eavesdropper. In detail, the transmit precoder matrices of active pairs and inactive pairs are solved according to game theory and linear programming respectively. Experimental results show that the proposed algorithm has fast convergence speed, and the security performances in different scenarios are effectively improved.

Keywords: interference channel, physical layer security, secure communications, Nash equilibrium, cooperative jamming

http://doi.org/10.3837/tiis.2019.04.009 **ISSN : 1976-7277**

1. Introduction

Interference channels are usually used to model multi-user scenarios, such as cognitive radio systems, ad-hoc wireless networks, and various forms of broadcast channels [1]. Due to the broadcast nature, signals from any transmitter are shared by all access receivers, which means interference channels are exposed to security risks of eavesdropping attacks. Traditionally, secure communications are achieved by using encryption algorithms [2-3]. However, with the rapid development of computing speed, once quantum computers are put into practice, traditional cryptography will be greatly challenged by brute force of quantum computing. Therefore, the physical layer security (PLS) technology, which is defined from the perspective of the information theory, has been proposed in the physical layer to complement and enhance the confidentiality provided at upper layers [4-5]. By PLS encoding, the qualities of legitimate channels are improved while the eavesdropping channels are degraded. As a benefit, even if the encoding leaked, security can still be guaranteed because of the advantage in channel qualities [6].

Recently, the multiple-input and multiple-output (MIMO) techniques have been proposed to improve the spectral efficiency as well as the multiplexing gain in wireless communication systems. With multi-antennas at both transmitters and receivers, communication resources in physical layer are highly increased, which significantly facilitates the PLS encoding [7]. In last decade, several PLS methods have been proposed. Without the aid of external communication nodes, beam-forming is the main method for improving the PLS in MIMO wireless interference networks [8-12]. Specifically, confidential signals are precoded at the transmitter and decoded at the receiver according to the channel state information (CSI), which is known as the joint transceiver [13-14]. Besides, the quality of the eavesdropping channel can be degraded by transmitting artificial noises (AN) together with confidential signals. To eliminate influences on the legitimate channel, AN must occupy part of antennas which are initially used to transmit confidential signals. As a result, the data rate will reduce remarkably. On the contrary, if there are excess communication nodes in the network, redundant transmitters can serve as cooperative jammers and send AN to interfere with the eavesdropper [15-16]. By this means, it is no need to allocate data streams to send AN, so the data rate can remain at a high level.

On the other hand, although cooperative jamming has been widely recognized as an effective approach for improving the PLS, its application in MIMO Interference networks remains a significant challenge. The main difficulty lies in reducing the interferences from cooperative jammers to legitimate users. In multiple-input-single-output (MISO) systems and MIMO systems with redundant antennas, the authors in [17-18] force the AN to be zero by sending it in the null space of channel transfer matrices. However, in MIMO system, if the transmitters and receivers use the same number of antennas to transmit data symbols, the null space is not existent and the zero-forcing is infeasible. Except for zero-forcing, although some AN designs in MIMO interference networks have been proposed to ensure PLS while reducing the impact on legitimate receivers by as much as possible [19-20], but the optimization problem of the secrecy rate is non-convex and the complexity remains fairly high. Therefore, how to design cooperative jamming considering both security performance and computing efficiency is still an unsolved problem.

Motivated by this challenge, we aim for providing an algorithm with low complexity and well security performance in order to jointly design the PLS encoding of transmitters, receivers and jammers. Specifically, we consider a MIMO interference network consisting of

a plurality of legitimate transmitter-receiver pairs and one eavesdropper (Eve). The transmitter-receiver pairs are divided into active pairs (AP) and inactive pairs (IP) according to if they are active or not. The security performances of APs are our main concern, hence IPs play supporting roles and broadcast AN to interfere with Eve. To this end, we did the following contributions: 1) we use mean-squared errors (MSE) to denote the security performance, and the security problem in MIMO interference wiretap channel is formulated as an optimization problem for the purpose of maximizing the MSE difference between APs and Eve. 2) We propose an asynchronous algorithm to obtain the Nash equilibrium (NE) solution of joint transceivers. Specifically, the non-convex MSE expressions of APs are transformed into convex forms, and the closed-form solutions are obtained at each iteration. Benefit from that, the computational time is saved greatly, and the proposed algorithm has fast convergence speed. 3) We design the ANs from cooperative jammers for the purpose of maximizing the MSE difference between APs and Eve while reducing the impacts on APs as much as possible. The MSE variation of APs and Eve with the active of IPs is derived and the TPCs of IPs are solved based on the linear programming.

The rest of this paper is organized as follows: Section 2 analyses the MIMO interference network and build the wiretap channel model. In section 3, the security strategies of APs and IPs are designed respectively. And an asynchronous algorithm is put forth to solve the joint transmitters and receivers. In Section 4, the performance of our design is tested by simulation experiments, and a detailed analysis is also conducted. Finally, this paper is concluded in Section 5.

2. System Model

Here we consider an interference network of $M+N$ legitimate transmitter-receiver pairs, in which each receiver could be the potential Eve. For each legitimate transmitter-receiver pair, a pair of transceivers consisting of a TPC and a receive decoder (RDC) is adopted to achieve secure communications, and Eve only has a RDC for eavesdropping. We assume that an alliance is formed by all the legitimate transmitter-receiver pairs, the aim of which is to enhance the security performance of the whole network. In fact, transmitter-receiver pairs can be divided into two types: M APs and N IPs. APs are engaged with transmitting and receiving data while IPs are idle. For the benefit of the whole network, APs share their CSIs and TPC matrices. We assume that Eve is an active eavesdropper who may register in the network. Since Eve is not recognized as a hostile node, but as one existing receiver who tries to wiretap data signals from non-paired transmitter, so the perfect CSIs of APs are available to Eve as well. On the contrary, IPs serve as cooperative jammers and broadcast ANs without publishing their TPC matrices. Moreover, it takes a very short time to transmit a data frame, so each channel is assumed to change sufficiently slowly to be considered fixed during this period.

As shown in **Fig. 1**, the mth transmitter, the mth receiver, and Eve are equipped with $N_{t,m}$, $N_{r,m}$ and N_e antennas, respectively. Because of the broadcast nature, the mth receiver will receive the signals not only from the mth transmitter but also other transmitters including transmitters of IPs, which causes mutual interferences. We assume that Eve is trying to wiretap data signals from the mth transmitter, and the wiretap model can be built from the perspective of the mth receiver and Eve as:

$$y_m = \mathbf{H}_{mm}\mathbf{T}_m s_m + \sum_{i\neq m}^{M}\mathbf{H}_{im}\mathbf{T}_i s_i + \sum_{n=1}^{N}\mathbf{H}_{nm}\mathbf{\Gamma}_n z_n + n_m \tag{1}$$

$$y_{e,m} = \mathbf{H}_{me}\mathbf{T}_m s_m + \sum_{i\neq m}^{M} \mathbf{H}_{ie}\mathbf{T}_i s_i + \sum_{n=1}^{N} \mathbf{H}_{ne}\mathbf{\Gamma}_n z_n + n_e \tag{2}$$

where $y_m \in \mathbb{C}^{N_{r,m}\times 1}$, $y_e \in \mathbb{C}^{N_e\times 1}$ are the vectors of signals at the *m*th receiver and Eve, respectively, and $\mathbb{C}$ denotes the complex field; $s_m \in \mathbb{C}^{d\times 1}$ and $z_n \in \mathbb{C}^{d\times 1}$ are the vectors of data symbols from the *m*th transmitter and AN from the *n*th IP, where d is the number of data streams; $\mathbf{T}_m \in \mathbb{C}^{N_{t,m}\times d}$ and .. are the TPC matrices of the *m*th AP and the *n*th IP, respectively; $\mathbf{H}_{im} \in \mathbb{C}^{N_{r,m}\times N_{t,i}}$ and $\mathbf{H}_{ie} \in \mathbb{C}^{N_e\times N_{t,i}}$ are the channel matrices of the *i*th transmitter to the *m*th receiver link and the *i*th transmitter to Eve link, respectively; $n_m \in \mathbb{C}^{N_{r,m}\times 1}$ and $n_e \in \mathbb{C}^{N_e\times 1}$ are the complex additive white Gaussian noise (AWGN) vectors received by the *m*th receiver and Eve, respectively. And we have $n_m \sim \mathcal{CN}\left(0, \delta_m^2\mathbf{I}\right)$ and $n_e \sim \mathcal{CN}\left(0, \delta_e^2\mathbf{I}\right)$, where δ_m^2 and δ_e^2 are the variances of noises.

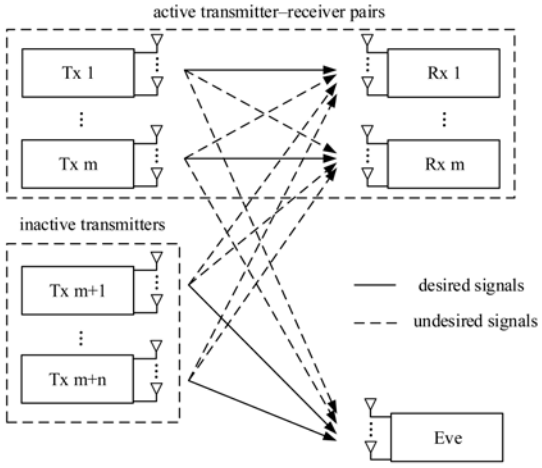


Fig. 1. a MIMO interference network with *M* APs, *N* IPs and an Eve

Let $\mathbf{R}_m \in \mathbb{C}^{d\times N_{r,m}}$ and $\mathbf{R}_{e,m} \in \mathbb{C}^{d\times N_e}$ denote the RDC matrices of the *m*th AP and Eve respectively, the estimated data symbol vectors of the *m*th receiver and Eve are given by:

$$\hat{s}_m = \mathbf{R}_m^H y_m = \mathbf{R}_m^H \mathbf{H}_{mm}\mathbf{T}_m s_m + \mathbf{R}_m^H \sum_{i\neq m}^{M} \mathbf{H}_{im}\mathbf{T}_i s_i + \mathbf{R}_m^H \sum_{n=1}^{N} \mathbf{H}_{nm}\mathbf{\Gamma}_n z_n + \mathbf{R}_m^H n_m \tag{3}$$

$$\hat{s}_{e,m} = \mathbf{R}_{e,m}^H y_m = \mathbf{R}_{e,m}^H \mathbf{H}_{me}\mathbf{T}_m s_m + \mathbf{R}_{e,m}^H \sum_{i\neq m}^{M} \mathbf{H}_{ie}\mathbf{T}_i s_i + \mathbf{R}_{e,m}^H \sum_{n=1}^{N} \mathbf{H}_{ne}\mathbf{\Gamma}_n z_n + \mathbf{R}_{e,m}^H n_e \tag{4}$$

where $(\cdot)^H$ is the Hermitian operator.

Based on the fact that the bit-error-rate is closed related to the MSE, we use the MSE of the transmitted data symbols to measure the security performance. Secure communications can be realized if the MSE of the *m*th transmitter to *m*th receiver link is smaller than that of the mth transmitter to Eve link. By assuming that $\mathbb{E}\{s_m s_m{}^H\} = \mathbf{I}$, $\forall m \in \{1,2,...,M\}$, MSE matrices of both links are as follows:

$$\begin{aligned}\mathbf{MSE}_{\mathrm{Tx}_m,\mathrm{Rx}_m} &= \mathbb{E}\left\{\left(\hat{s}_m - s_m\right)\left(\hat{s}_m - s_m\right)^H\right\} \\ &= \mathbf{R}_m^H \sum_{i=1}^{M} \mathbf{H}_{im}\mathbf{T}_i\mathbf{T}_i^H\mathbf{H}_{im}^H\mathbf{R}_m + \mathbf{R}_m^H \sum_{n=1}^{N} \mathbf{H}_{nm}\boldsymbol{\Gamma}_n\boldsymbol{\Gamma}_n^H\mathbf{H}_{nm}^H\mathbf{R}_m - \mathbf{R}_m^H\mathbf{H}_{mm}\mathbf{T}_m \\ &\quad - \mathbf{T}_m^H\mathbf{H}_{mm}^H\mathbf{R}_m + \sigma_m^2\mathbf{R}_m^H\mathbf{R}_m + \mathbf{I}\end{aligned} \tag{5}$$

$$\begin{aligned}\mathbf{MSE}_{\mathrm{Tx}_m,\mathrm{Eve}} &= \mathbb{E}\left\{\left(\hat{s}_{e,m} - s_m\right)\left(\hat{s}_{e,m} - s_m\right)^H\right\} \\ &= \mathbf{R}_{e,m}^H \sum_{i=1}^{M} \mathbf{H}_{ie}\mathbf{T}_i\mathbf{T}_i^H\mathbf{H}_{ie}^H\mathbf{R}_{e,m} + \mathbf{R}_{e,m}^H \sum_{n=1}^{N} \mathbf{H}_{ne}\boldsymbol{\Gamma}_n\boldsymbol{\Gamma}_n^H\mathbf{H}_{ne}^H\mathbf{R}_{e,m} - \mathbf{R}_{e,m}^H\mathbf{H}_{me}\mathbf{T}_m \\ &\quad - \mathbf{T}_m^H\mathbf{H}_{me}^H\mathbf{R}_{e,m} + \sigma_{e,m}^2\mathbf{R}_{e,m}^H\mathbf{R}_{e,m} + \mathbf{I}\end{aligned} \tag{6}$$

where $\mathbb{E}(\cdot)$ is the expectation operator; $\mathbf{I}$ is the identity matrix.

For the sake of communication quality, we expect the MSE of the evaluations of confidential signals to be as small as possible. Thus, in this paper, the linear MMSE receiver is selected as the RDC matrix [21-22], which can be calculated by taking a derivative with respect to the MSE expression:

$$\frac{d\mathbf{MSE}_{RX_m,TX_m}\left(\{\mathbf{T}\},\{\boldsymbol{\Gamma}\}\right)}{d\mathbf{R}_m^H} = 0 \tag{7}$$

As shown in (7), the RDC matrix depends on the set of TPC matrices. Therefore, in what follows, the main focus of our work is solving for the optimal TPC matrices.

3. TPC Design Method

For the purpose of maximizing the MSE difference between APs and Eve, we design the TPC matrices of APs and IPs separately. Firstly, to simplify the analysis, the TPC matrices of APs are solved while ignoring the interferences from IPs. Secondly, the TPC matrices of IPs are generated with the smallest possible impact on APs.

3.1 TPC Design Method of APs

In this section, we design the TPC matrices of APs by using the game theory, the main reasons are as follows. Firstly, the security performances of all the APs are assumed to be of equal importance, which is satisfied the conditions of a non-cooperative game. Secondly, as shown in (5), the MSE of each AP is determined by not only its TPC matrix but also TPC matrices of all other pairs. Thus, it is difficult to obtain the closed-form solution of the global optimal solution, which tries to minimize the sum-MSE of all APs, because of the high complexity of solving all TPC matrices synchronously. Conversely, after using game theory and asynchronous algorithm to simplify the expression, the closed-form solution of NE can be obtained at each iteration. Therefore, we formulate the problem as a non-cooperative game, in which all APs are regarded as competing players. Each player acts independently and simultaneously according to their own interests with no apriori knowledge of other players' strategies. Specifically, we formulate the problem as follow:

Definition 1: Given a strategic form game $\mathcal{G} = \left(\mathcal{M}, \{\mathcal{Q}_m\}_{m\in\mathcal{M}}, \{\mathcal{U}_m\}_{m\in\mathcal{M}}\right)$, an action profile $\mathbf{T}^* \in \mathcal{Q}$ is a pure-strategy NE of $\mathcal{G}$ if the following condition holds for all $m \in \mathcal{M}$:

$$\mathcal{U}_m\left(\mathbf{T}_m^*, \mathbf{T}_{-m}^*\right) \geq \mathcal{U}_m\left(\mathbf{T}_m, \mathbf{T}_{-m}^*\right), \ \forall \mathbf{T}_m \in \mathcal{Q}_m \tag{8}$$

where $\mathcal{M} = \{1, 2, ..., M\}$ is the set of players; $\mathcal{Q}_m$ is a nonempty set of the available pure

strategies for the mth player; $\mathcal{U}_m$ is the utility function of the *m*th player. The existence of NE is proved in Appendix A.

According to the non-cooperative game, we define the utility function as (9). An asynchronous algorithm, which is formally presented in **Table 1**, is proposed to obtain the NE solution.

$$\mathcal{U}_m\left(\mathbf{T}_m^*, \mathbf{T}_{-m}^*\right) = \mathbf{MSE}_{\mathrm{Tx}_m,\mathrm{Eve}} - \mathbf{MSE}_{\mathrm{Tx}_m,\mathrm{Rx}_m} \tag{9}$$

Table 1. Asynchronous Algorithm

1. Initialization: set the iteration counter $n=0$, and start with arbitrary TPC matrices $\left\{\mathbf{T}^{(n)}\right\}=\left\{\mathbf{T}^{(0)}\right\}$.

2. Begin the iteration: calculate and update $\left\{\mathbf{R}^{(n+1)}\right\}$ and $\left\{\mathbf{R}_e^{(n+1)}\right\}$ according to (7).

3. Update TPC matrices $\left\{\mathbf{T}_i^{(n+1)}\right\}$:

for $i=1$ to M **do**

$$\mathbf{T}_i^{(n+1)} = \arg\max\ \mathcal{U}_i\left(\mathbf{T}_i^*, \mathbf{T}_{-i}^{(n)}\right) \tag{10}$$

end

4. $n=n+1$; Repeat Step 2 through 3 until $\{\mathcal{U}_i\}$ is converged.

To obtain the optimal solution of the utility function, the influences from IPs are ignored, then (5) and (6) can be transformed as:

$$\mathbf{MSE}_{\mathrm{Tx}_m,\mathrm{Rx}_m} = \mathbf{R}_m^H \sum_{i=1}^{M} \mathbf{H}_{im}\mathbf{T}_i\mathbf{T}_i^H\mathbf{H}_{im}^H\mathbf{R}_m - \mathbf{R}_m^H\mathbf{H}_{mm}\mathbf{T}_m - \mathbf{T}_m^H\mathbf{H}_{mm}^H\mathbf{R}_m + \sigma_m^2\mathbf{R}_m^H\mathbf{R}_m + \mathbf{I} \tag{11}$$

$$\mathbf{MSE}_{\mathrm{Tx}_m,\mathrm{Eve}} = \mathbf{R}_{e,m}^H \sum_{i=1}^{M} \mathbf{H}_{ie}\mathbf{T}_i\mathbf{T}_i^H\mathbf{H}_{ie}^H\mathbf{R}_{e,m} - \mathbf{R}_{e,m}^H\mathbf{H}_{me}\mathbf{T}_m - \mathbf{T}_m^H\mathbf{H}_{me}^H\mathbf{R}_{e,m} + \sigma_{e,m}^2\mathbf{R}_{e,m}^H\mathbf{R}_{e,m} + \mathbf{I} \tag{12}$$

For secure communications, we ensure that the MSE of the signals from each AP decoded by Eve remains higher than a certain threshold. In detail, we set the minimum threshold of the MSE to an acceptable constant, any value greater than it will be considered as a representation of poor communication quality. Then, the optimization problem of utility function can be formulated as:

$$\begin{aligned} &\mathbf{T}_m^* = \arg\min_{\mathbf{T}_m}\ tr\left(\mathbf{MSE}_{\mathrm{Tx}_m,\mathrm{Rx}_m}\right),\ \forall m\in\{1,2,...,M\} \\ \text{s.t. }\ &tr\left(\mathbf{MSE}_{\mathrm{Tx}_m,\mathrm{Eve}}\right)\ge\varepsilon_m,\ \forall m\in\{1,2,...,M\} \\ &\left\|\mathbf{T}_m\right\|_F^2 \le p_m,\ \forall m\in\{1,2,...,M\} \end{aligned} \tag{13}$$

where $\mathbf{T}_m^*$ is the optimal solution obtained; $\|\cdot\|_F$ denotes the Frobenius norm of a matrix; $tr(\cdot)$ denotes the trace operator; ε_m is the minimum threshold of MSE of the *m*th transmitter to Eve link; P_m is the maximum power constraint imposed on the *m*th transmitter. In fact, the increase of P_m will grow the signal-to-noise-ratio, which will finally decrease ε_m. Thus, P_m and ε_m are in inverse proportion, the mathematical proof of which is shown in Appendix B. As a result, once ε_m is fixed, the minimum of P_m is determined, and the optimization problem can be simplified by ignoring the transmitted power constraint.

To start with, according to (7) and (11), we calculate the RDC matrix of the *m*th AP as follow:

$$\begin{aligned}\mathbf{R}_m &= \left(\mathbf{H}_{mm}\mathbf{T}_m\mathbf{T}_m^H\mathbf{H}_{mm}^H + \sum_{i\neq m}^{M}\mathbf{H}_{im}\mathbf{T}_i\mathbf{T}_i^H\mathbf{H}_{im}^H + \sigma_m^2\mathbf{I}\right)^{-1}\mathbf{H}_{mm}\mathbf{T}_m \\ &= \left(\mathbf{H}_{mm}\mathbf{T}_m\mathbf{T}_m^H\mathbf{H}_{mm}^H + \mathbf{\Phi}_m\right)^{-1}\mathbf{H}_{mm}\mathbf{T}_m\end{aligned} \tag{14}$$

where $\mathbf{\Phi}_m = \sum_{i\neq m}^{M}\mathbf{H}_{im}\mathbf{T}_i\mathbf{T}_i^H\mathbf{H}_{im}^H + \sigma_m^2\mathbf{I}$.

By substituting (14) into (11) and using the matrix inversion lemma, the MSE matrix is simplified as:

$$\mathbf{MSE}_{\mathrm{Tx}_m,\mathrm{Rx}_m} = \mathbf{I} - \mathbf{T}_m^H\mathbf{H}_{mm}^H\left(\mathbf{H}_{mm}\mathbf{T}_m\mathbf{T}_m^H\mathbf{H}_{mm}^H + \mathbf{\Phi}_m\right)^{-1}\mathbf{H}_{mm}\mathbf{T}_m = \left(\mathbf{I}+\mathbf{T}_m^H\mathbf{H}_{mm}^H\mathbf{\Phi}_m^{-1}\mathbf{H}_{mm}\mathbf{T}_m\right)^{-1} \tag{15}$$

Similarly, the MSE matrix of the *m*th transmitter to Eve link is as follow:

$$\mathbf{MSE}_{\mathrm{Tx}_m,\mathrm{Eve}} = \left(\mathbf{I}+\mathbf{T}_m^H\mathbf{H}_{me}^H\mathbf{\Phi}_{e,m}^{-1}\mathbf{H}_{me}\mathbf{T}_m\right)^{-1} \tag{16}$$

where $\mathbf{\Phi}_{e,m} = \sum_{i\neq m}^{M}\mathbf{H}_{ie}\mathbf{T}_i\mathbf{T}_i^H\mathbf{H}_{ie}^H + \sigma_{e,m}^2\mathbf{I}$.

Then, the optimization problem in (13) can be transformed as:

$$\begin{aligned}&\mathbf{T}_m^* = \arg\min_{\mathbf{T}_m} tr\left(\mathbf{I}+\mathbf{T}_m^H\mathbf{H}_{mm}^H\mathbf{\Phi}_m^{-1}\mathbf{H}_{mm}\mathbf{T}_m\right)^{-1} \\ &\text{s.t. } tr\left(\mathbf{I}+\mathbf{T}_m^H\mathbf{H}_{me}^H\mathbf{\Phi}_{e,m}^{-1}\mathbf{H}_{me}\mathbf{T}_m\right)^{-1} \geq \varepsilon_m,\ \forall m\in\{1,2,...,M\}\end{aligned} \tag{17}$$

To simplify analysis, we note that $\mathbf{H}_{mm}^H\mathbf{\Phi}_m^{-1}\mathbf{H}_{mm}$ and $\mathbf{H}_{me}^H\mathbf{\Phi}_{e,m}^{-1}\mathbf{H}_{me}$ are two Hermite matrices, which can be diagonalized by a non-singular matrix $\mathbf{C}$ at the same time [23].

$$\begin{cases}\mathbf{C}^H\mathbf{H}_{mm}^H\mathbf{\Phi}_m^{-1}\mathbf{H}_{mm}\mathbf{C} = \mathbf{\Lambda}_m = \mathrm{diag}(\gamma_{m,i}) \\ \mathbf{C}^H\mathbf{H}_{me}^H\mathbf{\Phi}_{e,m}^{-1}\mathbf{H}_{me}\mathbf{C} = \mathbf{\Lambda}_{em} = \mathrm{diag}(\gamma_{em,i})\end{cases} \tag{18}$$

where $\gamma_{m,i}\geq 0,\ \gamma_{e,i}\geq 0,\ \forall i\in\{1,2,...,d\}$; $\mathrm{diag}(\gamma_{m,i})$ and $\mathrm{diag}(\gamma_{em,i})$ are diagonal matrices, the coefficients of which are $\gamma_{m,i}$ and $\gamma_{em,i}$.

In [24], the optimal TPC matrix in MIMO wiretap channel with secrecy constraints is proved to follow the diagonal structure as follow:

$$\mathbf{T}_m = \mathbf{C}\mathrm{diag}\left(\sqrt{\varphi_{m,i}}\right) \tag{19}$$

where $\varphi_{m,i}\geq 0,\ \forall i\in\{1,2,...,d_m\}$, the problem in (17) can be simplified as:

$$\begin{aligned}&\mathbf{T}_m^* = \arg\min_{\mathbf{T}_m} \sum_{i=1}^{d_m}\left(1+\gamma_{m,i}\varphi_{m,i}\right)^{-1} \\ &\text{s.t. } \sum_{i=1}^{d_m}\left(1+\gamma_{me,i}\varphi_{m,i}\right)^{-1} \geq \varepsilon_m,\ \forall m\in\{1,2,...,M\}\end{aligned} \tag{20}$$

However, the utility function in (20) is non-convex. Thus, we use a one-to-one mapping $\varphi'_{m,i} = \left(1+\gamma_{me,i}\varphi_{m,i}\right)^{-1}$ to transform it into a standard convex form. By substituting $\varphi_{m,i} = \left(1/\varphi'_{m,i}-1\right)/\gamma_{me,i}$ into (20), we have:

$$\mathbf{T}_m^* = \arg\min_{\mathbf{T}_m} \sum_{i=1}^{d_m} \frac{\varphi'_{m,i}}{\varphi'_{m,i}\left(1-\frac{\gamma_{m,i}}{\gamma_{em,i}}\right)+\frac{\gamma_{m,i}}{\gamma_{em,i}}}$$

$$\text{s.t.} \quad \sum_{i=1}^{d_m} \varphi'_{m,i} \geq \varepsilon_m, \quad \forall m \in \{1,2,...,M\} \tag{21}$$

$$0 \leq \varphi'_{m,i} \leq 1, \quad \forall m \in \{1,2,...,M\}$$

The Lagrangian function of (21) is as follow:

$$\begin{aligned} L(\mathbf{T}_m, \mathbf{R}_m, \mu_m, \lambda_m) = & \sum_{i=1}^{d_m} \frac{\varphi'_{m,i}}{\varphi'_{m,i}\left(1-\frac{\gamma_{m,i}}{\gamma_{em,i}}\right)+\frac{\gamma_{m,i}}{\gamma_{em,i}}} + \lambda_m\left[\varepsilon_m - \varphi'_{m,i}\right] \\ & + \mu_m\left(0-\varphi'_{m,i}\right) + \mu'_m\left(\varphi'_{m,i}-1\right) \end{aligned} \tag{22}$$

where λ_m, μ_m and μ'_m are the Lagrange multipliers. Since it is convex, at the optimal point, the Karush-Kuhn-Tucker (KKT) conditions must be satisfied, which are given by:

Stationarity:

$$\frac{\partial L(\mathbf{T}_m, \mathbf{R}_m, \mu_m, \lambda_m)}{\partial \varphi'_{m,i}} = 0 \Rightarrow \frac{\frac{\gamma_{m,i}}{\gamma_{em,i}}}{\left[\varphi'_{m,i}\left(1-\frac{\gamma_{m,i}}{\gamma_{em,i}}\right)+\frac{\gamma_{m,i}}{\gamma_{em,i}}\right]^2} = \lambda_m + \mu_m - \mu'_m \tag{23}$$

Primal Feasibility:

$$\varepsilon_m - \varphi'_{m,i} \leq 0 \tag{24}$$

$$0 - \varphi'_{m,i} \leq 0 \tag{25}$$

$$\varphi'_{m,i} - 1 \leq 0 \tag{26}$$

Dual Feasibility:

$$\lambda_m \geq 0 \tag{27}$$

$$\mu_m \geq 0 \tag{28}$$

$$\mu'_m \geq 0 \tag{29}$$

Complementary Slackness:

$$\lambda_m\left[\varepsilon_m - \varphi'_{m,i}\right] = 0 \tag{30}$$

$$\mu_m\left(0-\varphi'_{m,i}\right) = 0 \tag{31}$$

$$\mu'_m\left(\varphi'_{m,i}-1\right) = 0 \tag{32}$$

Combining (23)-(32), the optimal solution is given by:

$$\begin{cases} \varphi'_{m,i} = 1, & \frac{\gamma_{m,i}}{\gamma_{em,i}} \leq \lambda_m \\ \varphi'_{m,i} = \left(\sqrt{\frac{\gamma_{m,i}\gamma_{em,i}}{\lambda_m}} - \gamma_{m,i}\right) \Big/ \left(\gamma_{em,i} - \gamma_{m,i}\right), & \frac{\gamma_{m,i}}{\gamma_{em,i}} < \lambda_m < \frac{\gamma_{em,i}}{\gamma_{m,i}} \\ \varphi'_{m,i} = 0, & \frac{\gamma_{em,i}}{\gamma_{m,i}} \geq \lambda_m \end{cases} \tag{33}$$

Consequently, the allocation of $\varphi_{m,i}$ can be derivable from (33):

$$\begin{cases} \varphi_{m,i}=0, & \dfrac{\gamma_{m,i}}{\gamma_{em,i}} \le \lambda_m \\ \varphi_{m,i}=\left(\sqrt{\dfrac{\gamma_{m,i}}{\lambda_m\gamma_{em,i}}}-1\right)\Bigg/\left(\gamma_{m,i}-\gamma_{em,i}\sqrt{\dfrac{\gamma_{m,i}}{\lambda_m\gamma_{em,i}}}\right), & \dfrac{\gamma_{em,i}}{\gamma_{m,i}} < \lambda_m < \dfrac{\gamma_{m,i}}{\gamma_{em,i}} \\ \varphi_{m,i}=\infty, & \dfrac{\gamma_{em,i}}{\gamma_{m,i}} \ge \lambda_m \end{cases} \tag{34}$$

Obviously, (34) is a piecewise function which is segmented by λ_m. And λ_m can be derived by substituting (33) into (30):

$$\sqrt{\lambda_m}=\left(\sum_{i=1}^{n_{act}}\frac{\sqrt{\gamma_{m,i}\gamma_{em,i}}}{\gamma_{em,i}-\gamma_{m,i}}\right)\Bigg/\left(\sum_{i=1}^{n_{act}}\frac{\gamma_{m,i}}{\gamma_{em,i}-\gamma_{m,i}}+\varepsilon_m-n_{inact}\right) \tag{35}$$

where n_{act} and n_{inact} are the number of active data streams (where $0<\varphi_{m,i}<\infty$) and inactive data streams (where $\varphi_{m,i}=0$), respectively.

By substituting (34) into (35), we can obtain the solution of $\varphi_{m,i}$. But the expression of λ_m consists of n_{inact}, which is related to $\varphi_{m,i}$. So, $\varphi_{m,i}$ and λ_m depend on each other. To solve them, value of n_{inact} must by obtained firstly. Therefore, we propose a searching algorithm to search n_{inact} by comparing λ_m to boundary conditions in (34). Specifically, we rearrange the values of $\frac{\gamma_{m,i}}{\gamma_{em,i}}$ in a decreasing order, i.e. $\frac{\gamma_{m,1}}{\gamma_{em,1}}>\frac{\gamma_{m,2}}{\gamma_{em,2}}>\ldots>\frac{\gamma_{m,d_m}}{\gamma_{em,d_m}}$. After that, λ_m is compared to $\frac{\gamma_{m,d_m}}{\gamma_{em,d_m}}$, and if $\frac{\gamma_{em,d_m}}{\gamma_{m,d_m}}<\lambda_m<\frac{\gamma_{m,d_m}}{\gamma_{em,d_m}}$ is satisfied, $\frac{\gamma_{em,1}}{\gamma_{m,1}}<\lambda_m<\frac{\gamma_{m,1}}{\gamma_{em,1}}$ is also satisfied. If it is not, we will continue to compare the λ_m to $\frac{\gamma_{m,d_m-1}}{\gamma_{em,d_m-1}}$ until the right n_{inact} is obtained. The searching algorithm is summarized in **Table 2**. To ensure the existence of the solution of this algorithm, two conditions should be satisfied. Firstly, $\frac{\gamma_{em,i}}{\gamma_{m,i}}\le\frac{\gamma_{m,i}}{\gamma_{em,i}}$ should be satisfied to ensure the interval $\left(\frac{\gamma_{em,i}}{\gamma_{m,i}},\frac{\gamma_{m,i}}{\gamma_{em,i}}\right)$ non-empty. Secondly, the right-hand side in (35) must be positive. To sum up the discussion, following condition should be satisfied:

$$\begin{aligned}\sqrt{\frac{\gamma_{m,i}}{\gamma_{em,i}}}\sum_{i=1}^{n_{act}}\frac{\sqrt{\gamma_{m,i}\gamma_{em,i}}}{\gamma_{em,i}-\gamma_{m,i}}-\sum_{i=1}^{n_{act}}\frac{\gamma_{m,i}}{\gamma_{em,i}-\gamma_{m,i}}+n_{inact}<\varepsilon_m \\ <\sqrt{\frac{\gamma_{em,i}}{\gamma_{m,i}}}\sum_{i=1}^{n_{act}}\frac{\sqrt{\gamma_{m,i}\gamma_{em,i}}}{\gamma_{em,i}-\gamma_{m,i}}-\sum_{i=1}^{n_{act}}\frac{\gamma_{m,i}}{\gamma_{em,i}-\gamma_{m,i}}+n_{inact}\end{aligned} \tag{36}$$

Table 2. TPC Generation Algorithm of APs

1. Initialization: set $n=0$, and start with an arbitrary TPC matrix $\left\{\mathbf{T}^{(n)}\right\}=\left\{\mathbf{T}^{(0)}\right\}$.

2. Begin the iteration: update $\left\{\mathbf{R}^{(n+1)}\right\}$ and $\left\{\mathbf{R}_e^{(n+1)}\right\}$ according to (14).

3. Update TPC matrix $\left\{\mathbf{T}^{(n+1)}\right\}$:

for $i=1$ to M **do**

1) Initialization: set $n'=2$, $n_{act}=0$

2) Begin the iteration: set $\lambda_m=\gamma_{m,i}/\gamma_{em,i}$

3) if $\sqrt{1/\lambda_m}\sum_{i=1}^{n_{act}}\frac{\sqrt{\gamma_{m,i}\gamma_{em,i}}}{\gamma_{em,i}-\gamma_{m,i}}-\sum_{i=1}^{n_{act}}\frac{\gamma_{m,i}}{\gamma_{em,i}-\gamma_{m,i}}\le\varepsilon_m-n_{inact}$ **then**

set $\varphi_{n'}=0$, $n'=n'-1$, $n_{inact}=n_{inact}+1$; go to step 2).

else

calculate λ_m according to (35).

if $\lambda_m\le\gamma_{em,i}/\gamma_{m,i}$ **then**

set $\varphi_{n'}=\infty$, $n'=n'-1$; go to step 2).

else

set $n_{act}=n'$

end

end

4) **set** $\varphi_{n'}=\left(\sqrt{\frac{\gamma_{m,i}}{\lambda_m\gamma_{em,i}}}-1\right)\Bigg/\left(\gamma_{m,i}-\gamma_{em,i}\sqrt{\frac{\gamma_{m,i}}{\lambda_m\gamma_{em,i}}}\right),\ \forall i\in\{1,2,...,n_{act}\}$

end

4. $n=n+1$; Repeat step 2 through 3 until $\left\{tr\left(\mathbf{MSE}_{\mathrm{Tx}_i,\mathrm{Rx}_i}\right)\right\}$ is converged.

3.2 TPC Design Method of IPs

In this section, TPC matrices of IPs are designed to improve the security performance of APs, which is reflected by the MSE difference between APs and Eve. According to (5), ANs from IPs will increase the MSE of the mth AP by $\mathbf{R}_m^H\sum_{n=1}^{N}\mathbf{H}_{nm}\mathbf{\Gamma}_n\mathbf{\Gamma}_n^H\mathbf{H}_{nm}^H\mathbf{R}_m$. In traditional zero-forcing method, this term is completely eliminated by setting the TPC matrix $\mathbf{\Gamma}_n$ in the null space of $\mathbf{H}_{nm}$. However, if the transmitters and receivers make use of the same number of antennas, the null space is not existent. Thus, we can only reduce the impact from AN as much as possible by design $\mathbf{\Gamma}_n$ reasonably. Specifically, we expect that ANs from each IP will maximize the difference between the sum-MSE of signals from all APs decoded by Eve and the sum-MSE of APs, which can be formulated as an optimization problem as follow:

$$\begin{aligned}\mathbf{\Gamma}_n^*=&\arg\max_{\mathbf{\Gamma}_n}\ tr\left(\sum_{m=1}^{M}\mathbf{R}_{e,m}^H\mathbf{H}_{ne}\mathbf{\Gamma}_n\mathbf{\Gamma}_n^H\mathbf{H}_{ne}^H\mathbf{R}_{e,m}-\sum_{m=1}^{M}\mathbf{R}_m^H\mathbf{H}_{nm}\mathbf{\Gamma}_n\mathbf{\Gamma}_n^H\mathbf{H}_{nm}^H\mathbf{R}_m\right)\\ \text{s.t.}\quad&\left\|\mathbf{\Gamma}_n\right\|_F^2\le P_n\end{aligned}\tag{37}$$

where P_n is the maximum power of the transmitter of nth IP.

Using the properties of trace $tr\left(\mathbf{A}\mathbf{A}^H\right)=tr\left(\mathbf{A}^H\mathbf{A}\right)$, we rewrite the MSE expressions as:

$$\begin{cases} tr\left(\sum_{m=1}^{M}\mathbf{R}_m^H\mathbf{H}_{nm}\boldsymbol{\Gamma}_n\boldsymbol{\Gamma}_n^H\mathbf{H}_{nm}^H\mathbf{R}_m\right)= tr\left(\sum_{m=1}^{M}\boldsymbol{\Gamma}_n^H\mathbf{H}_{nm}^H\mathbf{R}_m\mathbf{R}_m^H\mathbf{H}_{nm}\boldsymbol{\Gamma}_n\right) \\ tr\left(\sum_{m=1}^{M}\mathbf{R}_{e,m}^H\mathbf{H}_{ne}\boldsymbol{\Gamma}_n\boldsymbol{\Gamma}_n^H\mathbf{H}_{ne}^H\mathbf{R}_{e,m}\right)=tr\left(\sum_{m=1}^{M}\boldsymbol{\Gamma}_n^H\mathbf{H}_{ne}^H\mathbf{R}_{e,m}\mathbf{R}_{e,m}^H\mathbf{H}_{ne}\boldsymbol{\Gamma}_n\right) \end{cases} \tag{38}$$

Similar to the mathematical manipulation in section 3.1, $\mathbf{H}_{nm}^H\mathbf{R}_m\mathbf{R}_m^H\mathbf{H}_{nm}$ and $\mathbf{H}_{ne}^H\mathbf{R}_{e,m}\mathbf{R}_{e,m}^H\mathbf{H}_{ne}$ are diagonalized synchronously by a non-singular matrix $\mathbf{U}$, and The TPC matrix of the *n*th IP can be formulated according to (39) and (40).

$$\begin{cases} \mathbf{U}^H\mathbf{H}_{nm}^H\mathbf{R}_m\mathbf{R}_m^H\mathbf{H}_{nm}\mathbf{U}=\boldsymbol{\Lambda}_n=\text{diag}(\delta_{n,i}) \\ \mathbf{U}^H\mathbf{H}_{ne}^H\mathbf{R}_{e,m}\mathbf{R}_{e,m}^H\mathbf{H}_{ne}\mathbf{U}=\boldsymbol{\Lambda}_{en}=\text{diag}(\delta_{en,i}) \end{cases} \tag{39}$$

$$\boldsymbol{\Gamma}_n=\mathbf{U}\text{diag}\left(\sqrt{\omega_{n,i}}\right) \tag{40}$$

where $\delta_{n,i}\ge 0,\delta_{en,i}\ge 0,\omega_i\ge 0,\ \forall i\in\{1,2,...,d\}$.

Then, the optimization problem in (37) is simplified as:

$$\begin{aligned} &\boldsymbol{\Gamma}_n^*=\arg\max_{\boldsymbol{\Gamma}_n}\ \sum_{i=1}^{d}\left(\delta_{en,i}-\delta_{n,i}\right)\omega_{n,i},\ \forall n\in\{1,2,...,N\} \\ &\text{s.t.}\ \ \sum_{i=1}^{d}\omega_{n,i}\le P_n,\ \forall n\in\{1,2,...,N\} \\ &\omega_{n,i}\ge 0,\ \forall i\in\{1,2,...,d\} \end{aligned} \tag{41}$$

where $\omega_{n,i}$ is the power of the *i*th data stream.

Obviously, it is a linear programming problem, and among $\left\{\left(\delta_{en,i}-\delta_{n,i}\right)\omega_{n,i}\right\}$, the one with the largest coefficient will be allocated with all the transmitted power. If coefficients of all data streams are negative, the equivalent channels between the *n*th IP and APs are worse than that between the *n*th IP and Eve, and $\{\omega_{n,i}\}$ will be set to zero. The pseudo-codes are summarized in **Table 3**.

Table 3. TPC Generation Algorithm of IPs

for $j=1$ to N do
  if $\max\left\{\delta_{en,i}-\delta_{n,i}\right\}\ge 0,\ \forall i\in\{1,2,...,d\}$ **then**
    $i^*=\arg\max_{\{i\}}\left\{\delta_{en,i}-\delta_{n,i}\right\};\ \omega_{j,i^*}=p_n;\ \omega_{j,i}=0,\ \forall i\in\left\{1,...,i^*-1,i^*+1,...,d\right\}$
  else
    $\omega_{j,i}=0,\quad \forall i\in\{1,2,...,d\}$
  end
end

4. Simulation Analysis

In this section, we provide numerical results to examine the effectiveness of the proposed algorithm. Specifically, we consider a MIMO interference network with five legitimate transmitter-receiver pairs and an Eve. Each legitimate transmitter-receiver pairs may be active or inactive. In the network, all the transmitters and receivers are equipped with 3 antennas, and the channels are 3×3 dimension. The elements of all channel matrices are assumed to be i.i.d. zero-mean unit-variance complex-valued Gaussian random variables, i.e. $\mathcal{CN}(0,1)$. The power of background noise is assumed to be the same for all APs and Eve, i.e. $\delta_m^2 = \delta_e^2 = 1$. For each scenario below, we randomly generate 500 channel realizations, and any conclusion is the arithmetic mean of 500 trials. The simulation runs on a computer equipped with a 2.30GHz dual-core CPU and 8 gigabytes of memory.

4.1 Convergence performance

In the network we considered, there is no difference among the APs statistically. Therefore, without any loss of generality, we use the performance of the 1st AP to reflect other APs. For secure communications, we ensure the MSE between every AP and Eve is bigger than 2, i.e. $\varepsilon_1 = \varepsilon_2 = ... = \varepsilon_M = 2,\ \forall m \in \{1,2,...,M\}$. Then the joint transceivers of APs are solved according to section 3.1. And we select the Minimum Total MSE (MT-MSE) algorithm in [13] which pursues global optimality as a comparison. **Fig. 2**. Shows the MSE performance of two algorithms with increasing iteration number in networks with different number of APs. We observe that MSE values of two algorithms are convergent over iterations, and the final MSE values are very close. This can be explained by that the channels of all APs are independent identically distributed, and the NE solution and global optimality solution are similar. However, MSE of the NE algorithm is falling faster. As shown in **Table 4**, MT-MSE algorithm takes more CPU time at each iteration, and it is sharply increased with the number of APs increasing. Conversely, for NE algorithm, average CPU time at each iteration is increased slightly. This mainly because that the closed-form solution can be obtained at each iteration by using NE algorithm. Conversely, MT-MSE leads to approximately solution at each iteration. So NE algorithm has lower complexity and faster convergence speed.

Table 4. Iteration and CPU time of NE and MT-MSE algorithm

	number of transmitter-receiver pairs	2	3	4
NE	**iteration**	7	12	19
	CPU time (s)	16.17	38.88	82.08
	average CPU time (s)	2.31	3.24	4.32
MT-MSE	**iteration**	8	18	26
	CPU time (s)	26.16	92.88	218.66
	average CPU time (s)	3.27	5.16	8.41

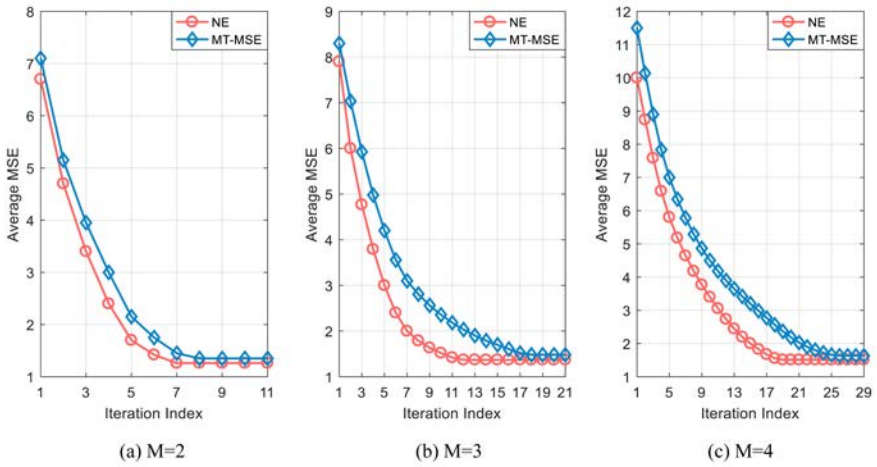


Fig. 2. MSE performance of the 1st transmitter to the 1st receiver link

4.2 Security Performance

Without the help of IPs, the MSE performance in networks of the number from 2 to 4 APs are simulated. As shown in **Fig. 3**, the MSE of the 1st AP decreases with the transmitted power increasing. We note that the final MSE of the 1st AP is in proportion to the total number of APs. This can be explained by that the mutual interferences are more serious in the networks of more APs. Furthermore, the final MSE is smaller than the MSE of the 1st transmitter to Eve link, the minimum threshold of which is set to 2. Therefore, the secure communications of the1st AP is achieved. Moreover, we note that the MSE of the 1st AP is larger than 2 when transmitted power is insufficient. In such case, since the transmitted power is small, the MSE of both legitimate receivers and Eve is higher than 2, and the secrecy constraint in (24) is failed to achieve. Therefore, enough transmitted power should be provided in practical application.

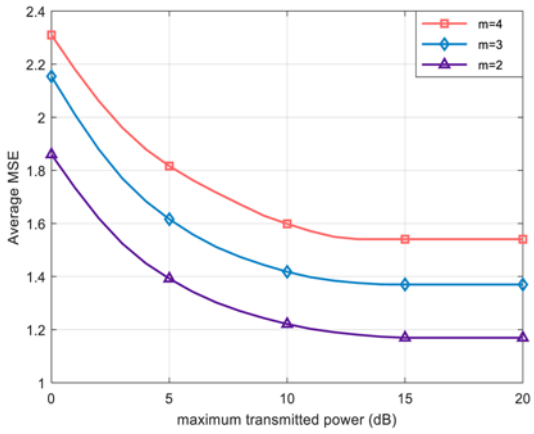
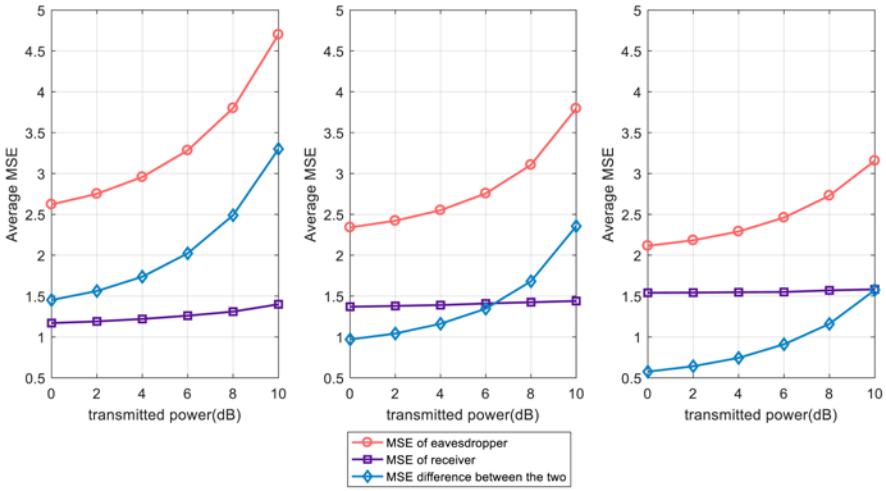


Fig. 3. MSE performance of the 1st transmitter to the 1st receiver link

Next, we enable the IPs in the network and **Fig. 4** show the MSE performance of the 1st AP in different scenarios. As expected, the MSE of the 1st transmitter to Eve link is remarkably increased with the increase of transmitted power of IPs while MSE of the 1st transmitter to the 1st receiver link is scarcely increased. Moreover, the MSE of the 1st transmitter to Eve link grows faster when the proportion of IPs in the network increases. This can be explained by two primary reasons. Firstly, with the number of cooperative jammers increasing, the total power of AN is increased, which will interfere Eve more effectively. Secondly, each IP allocates the power of AN for the benefit of all APs according to (41). The data stream selected may not be the optimal choice for some APs. If IPs are sufficient, this defect can be remedied efficiently.



(a) M=2, N=3 (b) M=3, N=2 (c) M=4, N=1

Fig. 4. MSE performance of the 1st transmitter to the 1st receiver link with cooperative jammers

5. Conclusion

In this paper, we investigated the joint transceiver design for secure communications in MIMO interference networks. In order to make full use of communication nodes, legitimate transmitter-receiver pairs have been divided into different categories of active and inactive. IPs served as cooperative jammers and sent ANs to enhance the security performance of APs. Specifically, we designed the security strategies of APs and IPs based on maximizing the MSE difference between APs and Eve. Firstly, the optimization problem of TPC matrices of APs has been formulated as a non-cooperative game, and the NE solution has been solved by an asynchronous algorithm. Then, the TPC matrices of IPs were designed following the principle minimizing the impact on APs. The simulation results demonstrated that our security strategies can effectively increase the MSE difference between APs and Eve. The proposed asynchronous algorithm was also confirmed to have faster convergence speed compared to an iterative algorithm pursuing global optimality.

Appendix A. Proof of the Existence and uniqueness of Nash Equilibrium

In [25], Nash demonstrated the existence of equilibrium points in n-person games by Kakutani's fixed-point theorem.

Theorem 1 Kakutani's fixed-point theorem: Given $\mathrm{X} \subseteq \mathbb{R}^n$, let $\mathrm{S}(x): \mathrm{X} \ni x \to \mathrm{S}(x) \subseteq \mathrm{X}$ be a multifunction. Suppose that the following hold:

(a) X is a nonempty, compact and convex set;

(b) $\mathrm{S}(x)$ is a convex-valued correspondence and has a closed graph.

Then, there exists a fixed point of $\mathrm{S}(x)$.

For classical n-person games, assumption (b) of Theorem 1 can be simplified into two sufficient conditions [26-27].

Theorem 2 Existence of NE: Consider a strategic form $\mathcal{G} = \left(\mathcal{M}, \{\mathcal{Q}_m\}_{m\in\mathcal{M}}, \{\mathcal{U}_m\}_{m\in\mathcal{M}}\right)$, where $\mathcal{M}$ is a finite set. Suppose that:

(a) Each $\mathcal{Q}_m$ is a non-empty, compact and convex subset of a finite-dimensional Euclidean space;

(b) One of the two following conditions holds

(1) Each utility function $\mathcal{U}_m(\mathbf{T}_m, \mathbf{T}_{-m})$ is continuous on $\mathcal{Q}$, and for any given $\mathbf{T}_{-m} \in \mathcal{Q}_{-m}$, it is quasi-concave on $\mathcal{Q}_m$;

(2) Each utility function $\mathcal{U}_m(\mathbf{T}_m, \mathbf{T}_{-m})$ is continuous on $\mathcal{Q}$, and for any given $\mathbf{T}_{-m} \in \mathcal{Q}_{-m}$, the following optimization problem

$$\max_{\mathbf{T}_m \in \mathcal{Q}_m} \mathcal{U}_m(\mathbf{T}_m, \mathbf{T}_{-m}) \tag{42}$$

admits a unique optimal solution.

Then, game $\mathcal{G}$ admits a pure-strategy NE.

Here, the proof of existence of NE algorithm we proposed is given as follow:

Proof:

According to (19), the TPC matrix of the *m*th transmitter is transformed into the product of a constant matrix and a diagonal matrix. Due to the power constraint, coefficients of the diagonal matrix are follow $\varphi_i \in [0, p_i]$, $\forall i \in \{1, 2, ..., N\}$, which means $\mathcal{Q}_m$ is bounded. Moreover, $\mathcal{Q}_m$ is a nonempty, compact and convex subset of a *N*-dimensional Euclidean space. Thus, Theorem 2 (a) is satisfied.

According to (21), the utility function $\mathcal{U}_m(\mathbf{T}_m, \mathbf{T}_{-m})$ is continuous and convex. And the closed-form solution of the optimization problem (21) is given by (34), which means the solution is unique and optimal. Therefore, Theorem 2 (b.2) is satisfied. And the existence of NE is proved

Appendix B. Proof of the Inverse Correlation between MSE and Transmitted Power

Proposition 1: the minimum threshold of power constraint $p_{m,\min}$ is inversely proportional to the MSE constraint ε_m.

Proof: According to (35), we have $\varepsilon_m = \sqrt{\frac{1}{\lambda_m}}\alpha - \beta + n_{inact}$, where $\alpha = \sum_{i=1}^{n_{act}} \frac{\sqrt{\gamma_{m,i}\gamma_{em,i}}}{\gamma_{em,i} - \gamma_{m,i}} < 0$, $\beta = \sum_{i=1}^{n_{act}} \frac{\gamma_{m,i}}{\gamma_{em,i} - \gamma_{m,i}} < 0$, and $\lambda_m > 0$.

Take the derivative of it with respect to λ_m, we have $\frac{d\varepsilon_m(\lambda_m)}{d\lambda_m} = -\frac{1}{2}\alpha\lambda_m^{-\frac{3}{2}} > 0$, which means that ε_m is in direct proportion to λ_m.

Take the derivative of (34) with respect to λ_m, we have $\frac{d\varphi_{m,i}}{d\lambda_m} = \frac{-\frac{1}{2}\sqrt{\frac{\gamma_{m,i}}{\lambda_m\lambda_{ei}}}\left(\gamma_{m,i} - \gamma_{em,i}\right)}{\left(\gamma_{m,i} - \gamma_{em,i}\sqrt{\frac{\gamma_{m,i}}{\lambda_m\gamma_{em,i}}}\right)^2} < 0$,

which means that $\varphi_{m,i}$ is in direct proportion to λ_m.

In conclusion, $\varphi_{m,i}$ is in inversely proportion to ε_m and $p_{m,\min} = \sum_{i}^{n_{act}} \varphi_{m,i}$, thus $p_{m,\min}$ is in inversely proportional to the security constraint ε_m.

References

[1] D. Maamari, D. Tuninetti, N. Devroye, "Multi-user Cognitive Interference Channels: A Survey and New Capacity Results," *IEEE Transactions on Cognitive Communication & Networking*, vol. 1, no. 1, pp. 29-44, 2017. Article (CrossRef Link).

[2] F. Liu and H. Koenig, "A survey of video encryption algorithms," *Computers & Security*, vol. 29, no. 1, pp. 3-15, 2010. Article (CrossRef Link).

[3] Z. Wang, X. Pang, Y. Chen, et al, "Privacy-preserving Crowd-sourced Statistical Data Publishing with An Untrusted Server," in *Proc. of IEEE Transactions on Mobile Computing*, pp. 1-1, 2018. Article (CrossRef Link).

[4] W. Harrison, J. Almeida, M. Bloch, et al, "Coding for Secrecy :An overview of error-control coding techniques for physical-layer security," *IEEE Signal Processing Magazine*, vol. 30. no. 5, pp. 41-50, 2013. Article (CrossRef Link).

[5] M. Bloch, M. Hayashi, A. Thangaraj, "Error-Control Coding for Physical-Layer Secrecy," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1725-1746, 2015. Article (CrossRef Link).

[6] A. Mukherjee, S. Fakoorian, J. Huang, et al, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550-1573, 2014. Article (CrossRef Link).

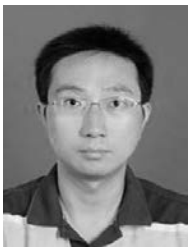
[7] V. Singh, A. Chaturvedi, "Statistically Robust Transceiver Design Algorithms for Relay aided MIMO Interference Systems," *IET Signal Processing*, vol. 12, no. 1, pp. 51-63, 2018. Article (CrossRef Link).

[8] X. Chen, D. Ng, W. Gerstacker, et al, "A Survey on Multiple-Antenna Techniques for Physical Layer Security," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, 1027-1053, 2017. Article (CrossRef Link).

[9] Q. Li , W. Ma , D. Han. "Sum Secrecy Rate Maximization for Full-Duplex Two-Way Relay Networks Using Alamouti-Based Rank-Two Beamforming," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1359-1374, 2016. Article (CrossRef Link).

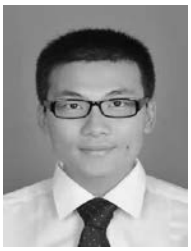
[10] Q. Shi, W. Xu, J. Wu, et al, "Secure Beamforming for MIMO Broadcasting With Wireless Information and Power Transfer," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2841-2853, 2014. Article (CrossRef Link).
[11] X. Gong, H. Long, H. Yin, et al, "Robust amplify-and-forward relay beamforming for security with mean square error constraint," *IET Communications*, vol. 9, no. 8, pp. 1081-1087, 2015. Article (CrossRef Link).
[12] L. Jiang， H. Tian， C. Qin, et al, "Secure Beamforming in Wireless-Powered Cooperative Cognitive Radio Networks," *IEEE Communications Letters*, vol. 20, no. 3, pp. 522-525, 2016. Article (CrossRef Link).
[13] Z. Kong, S. Yang, F. Wu, et al, "Iterative Distributed Minimum Total MSE Approach for Secure Communications in MIMO Interference Channels," *IEEE Transactions on Information Forensics & Security*, vol. 11, no. 3, pp. 594-608, 2017. Article (CrossRef Link).
[14] H. Shen, B. Li, M. Tao, et al, "MSE-Based Transceiver Designs for the MIMO Interference Channel," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3480-3489, 2010. Article (CrossRef Link).
[15] S. Huang, L. Zhu, S. Liu, "Based on virtual beamforming cooperative jamming with Stackelberg game for physical layer security in the heterogeneous wireless network," *Eurasip Journal on Wireless Communications & Networking*. 2018. Article (CrossRef Link).
[16] I. Stanojev, A. Yener, "Improving Secrecy Rate via Spectrum Leasing for Friendly Jamming," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 134-145, 2013. Article (CrossRef Link).
[17] J. Yang, I. Kim, I. Dong, "Power-Constrained Optimal Cooperative Jamming for Multiuser Broadcast Channel," *IEEE Wireless Communications Letters*, vol. 2, no. 4, pp. 411-414, 2013. Article (CrossRef Link).
[18] P. Siyari, M. Krunz, D. Nguyen, "Price-based Friendly Jamming in a MISO Interference Wiretap Channel," in *Proc. of The 35th Ann. IEEE Conf. on 35th Computer Communications*, pp. 1-9, 2016. Article (CrossRef Link).
[19] P. Siyari, M. Krunz, D. Nguyen, "Joint transmitter- and receiver-based friendly jamming in a MIMO wiretap interference network," in *Proc. of 2017 IEEE Int. Conf. on Communications Workshops*. pp. 1323-1328, 2017. Article (CrossRef Link).
[20] P. Siyari, M. Krunz, D. Nguyen, "Friendly Jamming in a MIMO Wiretap Interference Network: A Nonconvex Game Approach," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 3, pp. 601- 614, 2017. Article (CrossRef Link).
[21] C. Zhong, T. Ratnarajah, Z. Zhang, et al, "Performance of Rayleigh-Product MIMO Channels with Linear Receivers," *IEEE Transactions on Wireless Communications*, vol. 13, no. 4, pp. 2270-2281, 2014. Article (CrossRef Link).
[22] M. Razaviyayn, M. Sanjabi, Z. Luo, "Linear Transceiver Design for Interference Alignment: Complexity and Computation," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 2896-2910, 2012. Article (CrossRef Link).
[23] M. Pei, L. Wang, D. Ma, "Linear MMSE Transceiver Optimization for General MIMO Wiretap Channels with QoS Constraints," in *Proc. of 2013 IEEE/CIC Int. Conf. Communications in China*, pp. 259-263, 2013. Article (CrossRef Link).
[24] M. Rodrigues, P. Almeida, "Filter Design with Secrecy Constraints: The Degraded Parallel Gaussian Wiretap Channel," in *Proc. of 2008 IEEE Global Telecommunications Conf.*, pp. 1-5, 2008. Article (CrossRef Link).
[25] J. Nash, "Equilibrium Points in n-Person Games," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 36, no. 1, pp. 48-49, 1950. Article (CrossRef Link).
[26] J. Rosen, "Existence and Uniqueness of Equilibrium Points for Concave N-Person Games," *Econometrica*, vol. 33, no. 3, pp. 520-534, 1965. Article (CrossRef Link).
[27] G. Scutari, D. Palomar, S. Barbarossa, "Competitive optimization of cognitive radio MIMO systems via game theory," in *Proc. of 2009 Int. Conf. on Game Theory for Networks*, vol. 23, no.3, pp. 13-15, 2009. Article (CrossRef Link).

Boyang Huang is currently pursuing the PhD degree from School of Electrical Engineering and Automation, Wuhan University, China. His current research interests include physical layer security and interference management techniques. (e-mail: byhuang_whu@whu.edu.cn)



Zhengmin Kong is with the Automation Department, Wuhan University, China, and also with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. His current research interests include wireless communications and signal processing (e-mail: zmkong@whu.edu.cn)

Yanjun Fang received the PhD degree in automation of electronic power system from Wuhan University, China, in1987. His research interests include industrial automation, control theory and intelligent algorithms. (e-mail: yjfang@whu.edu.cn)



Xin jin is a research fellow of electric of Power Research Institute of China Southern Power Grid. He received the master degree in School of Comunication &Information Engineering from University of Electronic Science and Technology of China. His research interests include communication theory and electrical system. (e-mail: jinxin1@csg.cn)