Lu *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:259
DOI 10.1186/s13638-016-0755-5

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Successive optimization Tomlinson-Harashima precoding strategies for physical-layer security in wireless networks

Xiaotao Lu[1*], Rodrigo C. de Lamare[1,2] and Keke Zu[3]

Abstract

In this paper, we propose novel non-linear precoders for the downlink of a multi-user MIMO system in the existence of multiple eavesdroppers. The proposed non-linear precoders are designed to improve the physical-layer secrecy rate. Specifically, we combine the non-linear successive optimization Tomlinson-Harashima precoding (SO-THP) with the generalized matrix inversion (GMI) technique to maximize the physical-layer secrecy rate. For the purpose of comparison, we examine different traditional precoders with the proposed algorithm in terms of secrecy rate as well as bit error rate (BER) performance. We also investigate simplified generalized matrix inversion (S-GMI) and lattice-reduction (LR) techniques in order to efficiently compute the parameters of the precoders. We further conduct computational complexity and secrecy-rate analysis of the proposed and existing algorithms. In addition, in the scenario without knowledge of the channel state information (CSI) to the eavesdroppers, a strategy of injecting artificial noise (AN) prior to the transmission is employed to enhance the physical-layer secrecy rate. Simulation results show that the proposed non-linear precoders outperform existing precoders in terms of BER and secrecy-rate performance.

Keywords: Physical-layer security, Precoding algorithms, Successive optimization, Secrecy-rate analysis

1 Introduction

Data security in wireless systems has been traditionally dominated by encryption methods such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) [1]. However, these existing encryption algorithms suffer from high complexity and high latency. Furthermore, development in computing power also brings great challenges to existing encryption techniques. Therefore, the development of techniques that are capable of achieving secure transmission under high computing-power scenario with low complexity have become an important research topic.

From the viewpoint of information theory, Shannon established the theorem of cryptography in his seminal paper [2]. Wyner has subsequently posed the Alice-Bob-Eve problem and described the wire-tap transmission system [3]. Furthermore, the system discussed in [3] suggests that physical-layer security can be achieved in wireless networks. Later on, another study reported in [4] proved that secrecy transmission is achievable even under the situation that the eavesdropper has a better channel than the desired user in a statistical sense. Furthermore, the secrecy capacity for different kinds of channels, such as the Gaussian wire-tap channel and the multi-input multi-output (MIMO) wire-tap channel, have been studied in [5, 6]. In some later works [7, 8], it has been found that the secrecy of the transmission can be further enhanced by adding artificial noise to the system.

1.1 Prior and related work

In recent years, precoding techniques, which rely on knowledge of channel state information (CSI), have been widely studied in the downlink of multi-user MIMO (MU-MIMO) systems. Linear precoding techniques such as zero-forcing (ZF), minimum mean square error (MMSE), and block diagonalization (BD) have been introduced

*Correspondence: xtl503@york.ac.uk
[1]Communications Research Group, Department of Electronics, , University of York, YO10 5DD York, UK
Full list of author information is available at the end of the article

and studied in [9–11]. Furthermore, non-linear precoding techniques like Tomlinson-Harashima precoding (THP) [12] and vector perturbation (VP) precoding [13] have also been reported and investigated. In the previous mentioned works, the implementation of linear or non-linear precoding techniques at the transmitter are considered with perfect knowledge of CSI to the users. In the scenario without knowledge of CSI to the eavesdroppers, one technique which is effective in improving the secrecy rate of the downlink of MU-MIMO systems is the application of artificial noise (AN) at the transmitter [7]. Several criteria or strategies applying AN to wireless systems have been introduced in [14, 15]. In particular, the approaches reported in [8] have been applied to the downlink of MU-MIMO systems. Apart from the studies in precoding techniques, there are also some works that introduce lattice-reduction (LR) strategies [16, 17]. The LR strategies are also implemented prior to the transmission, and it has been proved that the LR-aided system can achieve full diversity in the downlink of MU-MIMO systems.

1.2 Motivation and contributions

Prior work on precoding for physical-layer security systems has been heavily based on [7, 8], which can effectively improve the secrecy rate of wireless systems. However, it is well known in the wireless communications literature that non-linear precoding techniques can outperform linear approaches. In particular, non-linear precoding techniques require lower transmit power than linear schemes and can achieve higher sum rates. However, work on non-linear precoding for physical-layer security in wireless systems is extremely limited even though there is potential to significantly improve the secrecy rate of wireless systems. The motivation for this work is to develop and study non-linear precoding algorithms for MU-MIMO systems that can achieve a secrecy rate higher than that obtained by linear precoders as well as a lower transmit power requirement and an improved bit error rate (BER) performance.

In our work, we develop and study successive optimization Tomlinson-Harashima precoding (SO-THP) algorithms based on the generalized matrix inversion approach reported in [11]. Specifically, the proposed non-linear precoders exploit both successive interference cancelation, lattice reduction, and block diagonalization, which can impose orthogonality between the channels of the desired users. This combined approach has not been considered previously in the literature and has the potential of achieving a higher secrecy rate than existing non-linear and linear precoding algorithms as well as an improved BER performance as compared to prior art. The major contributions in our paper are summarized as follows:

- A novel non-linear precoding technique, namely SO-THP+GMI, is proposed for the downlink of MU-MIMO networks in the presence of multiple eavesdroppers.
- The proposed SO-THP+GMI algorithm combines the SO-THP with the generalized matrix inversion (GMI) technique to achieve a higher secrecy rate.
- The proposed SO-THP+GMI precoding algorithm is extended to a simplified GMI (S-GMI) version which aims to reduce computational complexity of the SO-THP+GMI algorithm.
- An LR strategy is combined with the aforementioned S-GMI version proposed algorithm, and this so-called LR-aided-version algorithm achieves full receive diversity.
- An analysis of the secrecy rate achieved by the proposed non-linear precoding algorithms is carried out along with an assessment of their computational complexity cost.
- When different power is allocated to generate the artificial noise, an analysis of the power ratio which can achieve the optimal value in terms of secrecy rate is given

The rest of this paper is organized as follows. We begin in Section 2 by introducing the system model and the performance metrics. A brief review of the standard SO-THP algorithm is included in Section 3. In Section 4, we present the details of the proposed SO-THP+GMI, SO-THP+S-GMI, and LR-SO-THP+S-GMI precoding algorithms. Next, in Section 5, the analysis of secrecy rate and the computational complexity of the precoding algorithms are carried out. In Section 6, numerical evaluation is conducted to show the advantage of the proposed precoding algorithms. Finally, some concluding remarks are given in Section 7.

1.3 Notation

Bold uppercase letters $\boldsymbol{A} \in \mathbb{C}^{M\times N}$ denote matrices with size $M \times N$ and bold lowercase letters $\boldsymbol{a} \in \mathbb{C}^{M\times 1}$ denote column vectors with length M. Conjugate, transpose, and conjugate transpose are represented by $(\cdot)^*$, $(\cdot)^T$ and $(\cdot)^H$, respectively; $\boldsymbol{I_M}$ is the identity matrix of size $M \times M$; diag$\{\boldsymbol{a}\}$ denotes a diagonal matrix with the elements of the vector $\boldsymbol{a}$ along its diagonal; and $\mathcal{CN}(0, \sigma_n^2)$ represents complex Gaussian random variables with *i.i.d* entries with zero mean and σ_n^2 variance.

2 System model and performance metrics

In this section, we introduce the system model of the downlink of the MU-MIMO network under consideration. The performance metrics used in the assessment of the proposed and existing techniques are also described.

2.1 System model

Consider a MU-MIMO downlink wireless network consisting of one transmitter or Alice at the access point, T users or Bob, and K eavesdroppers or Eve at the receiver side as shown in Fig. 1. The transmitter is equipped with N_t antennas. Each user and each eavesdropper node are equipped with N_r and N_k receive antennas, respectively. In this system, we assume that the eavesdroppers do not jam the transmission and the channel from the transmitter to each user or eavesdropper follows a flat-fading channel model. The quantities $\boldsymbol{H}_r \in \mathbb{C}^{N_r \times N_t}$ and $\boldsymbol{H}_k \in \mathbb{C}^{N_k \times N_t}$ denote the channel matrix of the ith user and kth eavesdropper, respectively. Following [18], the number of antennas should satisfy $N_t^{\text{total}} \geqslant T \times N_r$. During the transmission, $N_t = M \times N_r$ antennas at the transmitter are activated to perform the precoding procedure. In other words, the precoding matrix is assumed here for convenience to be always a square matrix.

We use the vector $\boldsymbol{s}_r \in \mathbb{C}^{N_r \times 1}$ to represent the data symbols to be transmitted to user r. An artificial noise (AN) can be injected before the data transmission to enhance the physical-layer secrecy. We use the vector $\boldsymbol{s}'_r \in \mathbb{C}^{m \times 1}$ with $m \leqslant (N_t^{\text{total}} - T \times N_r)$ to denote the independently generated jamming signal. Assume the transmit power of user r is E_r, and $0 < \rho < 1$ is the power fraction devoted to the user. Then, the power of the user and the jamming signal can be respectively expressed as $E[\boldsymbol{s}_r^H \boldsymbol{s}_r] = \rho E_r$ and $E[\boldsymbol{s}_r'^H \boldsymbol{s}'_r] = (1-\rho)E_r$. Finally, the signal after precoding can be expressed as

$$\boldsymbol{x}_r = \boldsymbol{P}_r \boldsymbol{s}_r + \boldsymbol{P}'_r \boldsymbol{s}'_r, \tag{1}$$

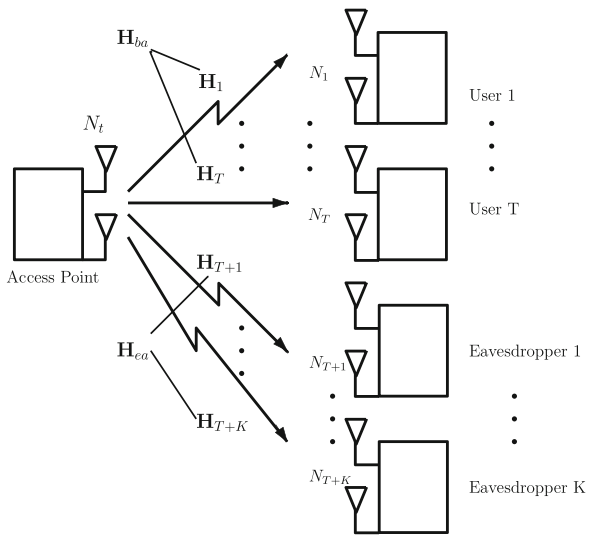


Fig. 1 System model of a MU-MIMO system with T users and K eavesdroppers

where the quantities $\boldsymbol{P}_r \in \mathbb{C}^{N_t \times N_r}$ and $\boldsymbol{P}'_r \in \mathbb{C}^{N_t \times m}$ are the corresponding precoding matrices. Here, we take zero-forcing precoding as an instance. Given the total channel matrix $\boldsymbol{H} = [\boldsymbol{H}_1^T \ \boldsymbol{H}_2^T \ \cdots \ \boldsymbol{H}_r^T \ \cdots \ \boldsymbol{H}_M^T]^T$, the total precoding matrix can be obtained as $\boldsymbol{P}^{\text{ZF}} = \boldsymbol{H}^H(\boldsymbol{H}\boldsymbol{H}^H)^{-1}$. The precoding matrix $\boldsymbol{P}^{\text{ZF}}$ can be expanded to $\boldsymbol{P}^{\text{ZF}} = [\boldsymbol{P}_1 \ \boldsymbol{P}_2 \ \cdots \ \boldsymbol{P}_r \ \cdots \ \boldsymbol{P}_M]$. Simultaneously, the precoding matrix $\boldsymbol{P}'_r$ can be generated from the null space of the rth user channel $\boldsymbol{H}_r$ by singular value decomposition (SVD) [8]. As a result, we have $\boldsymbol{H}_r \boldsymbol{P}'_r = \boldsymbol{0}$, which means the jamming signal does not interfere with the user's signal. The received data for each user or eavesdropper can be described by

$$\boldsymbol{y}_r = \beta_r^{-1} \left(\boldsymbol{H}_r \boldsymbol{P}_r \boldsymbol{s}_r + \boldsymbol{H}_r \boldsymbol{P}'_r \boldsymbol{s}'_r + \boldsymbol{H}_r \sum_{j=1, j \neq r}^{T} \boldsymbol{P}_j \boldsymbol{s}_j + \boldsymbol{n}_r \right), \tag{2}$$

where $\beta_r = \sqrt{\dfrac{E_r}{||\boldsymbol{P}_r|| + ||\boldsymbol{P}'_r||}}$ is used to ensure that the transmit power after precoding remains the same as the original transmit power E_r for user r.

2.2 Secrecy rate and other relevant metrics

In this subsection, we describe the main performance metrics used in the literature to assess the performance of precoding algorithms.

2.2.1 Secrecy rate and secrecy capacity

According to [3], the level of secrecy is measured by the uncertainty of Eve about the message R_e which is called the equivocation rate. With the total power equal to E_s, the maximum secrecy capacity C_s for the MIMO system without AN is expressed as [6]

$$\begin{aligned} C_s = \max_{\boldsymbol{Q}_s \geq 0, \text{Tr}(\boldsymbol{Q}_s) = E_s} & \log\left(\det\left(\boldsymbol{I} + \boldsymbol{H}_{ba} \boldsymbol{Q}_s \boldsymbol{H}_{ba}^H\right)\right) \\ & - \log\left(\det\left(\boldsymbol{I} + \boldsymbol{H}_{ea} \boldsymbol{Q}_s \boldsymbol{H}_{ea}^H\right)\right), \end{aligned} \tag{3}$$

where the quantity $\boldsymbol{Q}_s$ is a positive-defined covariance matrix associated with the signal after precoding. E_s is the total transmit power. $\boldsymbol{H}_{ba} \in \mathcal{CN}(0,1)$ and $\boldsymbol{H}_{ea} \in \mathcal{CN}(0, 1/m)$ represent the channel to the users and eavesdroppers, respectively. Here, $m = \frac{\sigma_{ea}^2}{\sigma_{ba}^2}$ represents the gain ratio between the main and wire-tap channels. The secrecy capacity is defined as the maximization of the difference between two mutual informations. However, the channels are usually not perfectly known in reality. This situation is known as the imperfect channel state information (CSI) case in [7], which we will address in our studies.

2.2.2 Computational complexity

According to [18], non-linear precoding techniques can approach the maximum channel capacity with high computational complexity. High complexity of the algorithm directly leads to a high cost of power consumption. In our research, however, novel non-linear precoding algorithms with reduced complexity are developed.

2.2.3 BER performance

Ideally, we would like the users to experience reliable communication and the eavesdroppers to have a very high BER (virtually no reliability when communicating). The algorithm is supposed to achieve high diversity for the MIMO system.

3 Review of the SO-THP algorithm

In this section, a brief review of the conventional successive optimization THP (SO-THP) in [9] is given. The general structure of the SO-THP algorithm is illustrated in Fig. 2, and its main implementation steps are introduced in the following.

In Fig. 2, a modulo operation $M(\cdot)$ which is defined in [19] is employed to fulfill the SO-THP algorithm. Based on [18], THP can be equivalently implemented in a successive block diagonalization manner. In particular, the precoding matrix is given by

$$\boldsymbol{P}_r^{\mathrm{BD}} = \tilde{\boldsymbol{V}}_r^{(0)} \boldsymbol{V}_{\mathrm{eff}}, \tag{4}$$

where $\tilde{\boldsymbol{V}}_r^{(0)} \in \mathbb{C}^{N_t \times N_r}$ is the nullifying matrix of the rth user's channel and $\boldsymbol{V}_{\mathrm{eff}}$ is a unitary matrix of the corresponding effective channel, and the demodulation matrix of the rth user is chosen as $\boldsymbol{D}_r = \boldsymbol{U}_{\mathrm{eff}}^H$, where $\boldsymbol{U}_{\mathrm{eff}}^H$ is also obtained from the effective channel. Given a channel matrix $\tilde{\boldsymbol{H}}_r = [\tilde{\boldsymbol{H}}_1^T \ \tilde{\boldsymbol{H}}_2^T \ \cdots \ \tilde{\boldsymbol{H}}_{r-1}^T \ \tilde{\boldsymbol{H}}_{r+1}^T \ \cdots \ \tilde{\boldsymbol{H}}_T^T]^T$, $\tilde{\boldsymbol{V}}_r^{(0)}$ can be obtained by the SVD operation $\tilde{\boldsymbol{H}}_r = \tilde{\boldsymbol{U}}_r \tilde{\boldsymbol{\Sigma}}_r [\tilde{\boldsymbol{V}}_r^{(1)} \tilde{\boldsymbol{V}}_r^{(0)}]^H$. Based on $\tilde{\boldsymbol{V}}_r^{(0)}$, an effective channel can be calculated, and with a second SVD operation $\boldsymbol{H}_{\mathrm{eff}} = \boldsymbol{H}_r \tilde{\boldsymbol{V}}_r^{(0)} = \boldsymbol{U}_{\mathrm{eff}} \boldsymbol{\Sigma}_{\mathrm{eff}} \boldsymbol{V}_{\mathrm{eff}}^H$, we are capable of getting $\boldsymbol{V}_{\mathrm{eff}}$ and $\boldsymbol{U}_{\mathrm{eff}}^H$. For each iteration, the SO-THP algorithm selects the user with maximum capacity from the remaining users and processes it first. The selection criterion is described as

$$\arg\min_r (C_{\max,r} - C_r); \tag{5}$$

where $C_{\max,r}$ denotes the maximum capacity of the rth user and C_r is the capacity considering the interference from the other users. If we assume there is no interference from other users and the capacity can be achieved by the SVD procedure, we have

$$\boldsymbol{H}_r = \boldsymbol{U}_r \boldsymbol{\Sigma}_r [\boldsymbol{V}_r^{(1)} \boldsymbol{V}_r^{(0)}]^H, \tag{6}$$

$$C_{\max,r} = \log_2 \det \left(\boldsymbol{I} + \boldsymbol{H}_r \boldsymbol{V}_r^{(1)} \boldsymbol{V}_r^{(1)H} \boldsymbol{H}_r^H \right). \tag{7}$$

In the scenario considering the interference from the other users, the BD decomposition is implemented on the channels of the remaining users in each iteration:

$$C_r = \log_2 \det \left(\boldsymbol{I} + \boldsymbol{H}_r \boldsymbol{P}_r \boldsymbol{P}_r^H \boldsymbol{H}_r^H \right); \tag{8}$$

Therefore, the filters for the SO-THP algorithm can be obtained as

$$\boldsymbol{F} = \left(\boldsymbol{P}_1^{\mathrm{BD}} \cdots \boldsymbol{P}_T^{\mathrm{BD}} \right), \tag{9}$$

$$\boldsymbol{D} = \begin{pmatrix} \boldsymbol{U}_{\mathrm{eff1}}^H & & \\ & \ddots & \\ & & \boldsymbol{U}_{\mathrm{effT}}^H \end{pmatrix}, \tag{10}$$

$$\boldsymbol{B} = \text{lower triangular} \left(\boldsymbol{DHF} \bullet \text{diag} \left([\boldsymbol{DHF}]_{ii}^{-1} \right) \right). \tag{11}$$

It is worth noting that $\boldsymbol{F}$ in (9) and $\boldsymbol{D}$ in (10) are calculated in the reordered way according to Eq. (5) and the scaling matrix $\boldsymbol{G} = \text{diag} \left([\boldsymbol{DHF}]_{ii}^{-1} \right)$.

4 Proposed precoding algorithms

In this section, we present three non-linear precoding algorithms SO-THP+GMI, SO-THP+S-GMI, and LR-SO-THP+S-GMI for the downlink of MU-MIMO systems and a selection criterion based on capacity is devised for these algorithms. We then derive filters for the three proposed precoding techniques, which are computationally simpler than SO-THP.

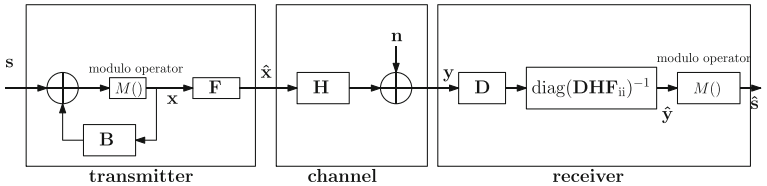


Fig. 2 Centralized SO-THP structure

According to [18], the conventional SO-THP algorithm has the advantage of improving the BER and the sum-rate performances; however, the complexity of this algorithm is high due to the successive optimization procedure and the multiple SVD operations. In [20], an approach called generalized MMSE channel inversion (GMI) is developed to overcome the noise enhancement drawback of BD caused by its focus on the suppression of multi-user interference. Later in [21], it has been shown that the complete suppression of multi-user interference is not necessary and residual interference is so small that it cannot affect the sum-rate performance. This approach is called simplified GMI (S-GMI). The proposed algorithms are inspired by dirty paper coding (DPC) [22] and other non-linear precoding techniques [18, 23, 24] which have been investigated for the downlink of MU-MIMO systems.

4.1 SO-THP+GMI algorithm

The proposed SO-THP+GMI algorithm mainly focuses on achieving high secrecy-rate performance with lower complexity than the conventional SO-THP algorithm. In the conventional SO-THP algorithm, the precoding matrix as well as the receive filters are obtained with (4) using the BD algorithm without considering noise enhancement. In [20], the GMI scheme uses the QR decomposition to decompose the MMSE channel inversion $\bar{\boldsymbol{H}} \in \mathbb{C}^{N_t \times TN_r}$ as expressed by

$$\bar{\boldsymbol{H}} = (\boldsymbol{H}^H \boldsymbol{H} + \alpha \boldsymbol{I})^{-1} \boldsymbol{H}^H, \tag{12}$$

$$\bar{\boldsymbol{H}}_r = [\,\bar{\boldsymbol{Q}}_r^{(0)} \quad \bar{\boldsymbol{Q}}_r^{(1)}]\,\bar{\boldsymbol{R}}_r \qquad \text{for} \qquad r = 1, \cdots, T, \tag{13}$$

where $\bar{\boldsymbol{H}}_r \in \mathbb{C}^{N_t \times N_r}$, $\bar{\boldsymbol{Q}}_r^{(0)} \in \mathbb{C}^{N_t \times N_t}$ is an orthogonal matrix and $\bar{\boldsymbol{R}}_r \in \mathbb{C}^{N_t \times N_r}$ is an upper triangular matrix. In (12), the noise is taken into account. As a result, the generation of the precoding matrix will mitigate the noise enhancement. When the GMI-generated precoding matrix is used to calculate the channel capacity with (8), the reduced noise contributes to the increase of secrecy rate. Also with (13), the QR decomposition reduces the computational complexity as compared with the conventional SO-THP algorithm implementing the SVD decomposition. To completely mitigate the interference, a transmit-combining matrix $\boldsymbol{T}_r$ given in [20] is applied to $\bar{\boldsymbol{Q}}_r^{(0)}$. Once we have $\bar{\boldsymbol{Q}}_r^{(0)}$ and $\boldsymbol{T}_r$, we can write the relation

$$\boldsymbol{H}_r \bar{\boldsymbol{Q}}_r^{(0)} \boldsymbol{T}_r = \bar{\boldsymbol{U}}_r \bar{\boldsymbol{\Sigma}}_r \bar{\boldsymbol{V}}_r^H, \tag{14}$$

Then, the precoding matrix and the receive filter for the GMI scheme are given by

$$\boldsymbol{P}_{\text{GMI}} = [\,\bar{\boldsymbol{Q}}_1^{(0)} \boldsymbol{T}_1 \bar{\boldsymbol{V}}_1 \quad \bar{\boldsymbol{Q}}_2^{(0)} \boldsymbol{T}_2 \bar{\boldsymbol{V}}_2 \quad \cdots \quad \bar{\boldsymbol{Q}}_T^{(0)} \boldsymbol{T}_T \bar{\boldsymbol{V}}_T], \tag{15}$$

$$\boldsymbol{M}_{\text{GMI}} = \text{diag}\left\{\bar{\boldsymbol{U}}_1^H \quad \bar{\boldsymbol{U}}_2^H \quad \cdots \quad \bar{\boldsymbol{U}}_T^H\right\}, \tag{16}$$

where $\boldsymbol{P}_{\text{GMI}} \in \mathbb{C}^{N_t \times N_t}$ and $\boldsymbol{M}_{\text{GMI}} \in \mathbb{C}^{N_t \times N_t}$. The details of the proposed SO-THP+GMI algorithm to obtain the precoding and receive filter matrices are given in the table of Algorithm 1.

Algorithm 1 Proposed SO-THP+GMI Precoding

for $r = 1 : T$ **do**
  $\boldsymbol{G}_r = \boldsymbol{H}_r$;
  $\boldsymbol{G}_r = \boldsymbol{U}_r \boldsymbol{\Sigma}_r [\,\boldsymbol{V}_r{}^{(1)} \boldsymbol{V}_r{}^{(0)}]^H$;
  $\boldsymbol{F}_r = \boldsymbol{V}_r{}^{(1)}$;
  $C_{max,r} = \log_2 \det\left(\boldsymbol{I} + \boldsymbol{R}_{k,r}^{-1} \boldsymbol{G}_r \boldsymbol{F}_r \boldsymbol{F}_r{}^H \boldsymbol{G}_r{}^H\right)$;
end for
$\boldsymbol{M} = \boldsymbol{H}$;
loop
  while $r = T : 1$ **do**
    for $n = 1 : r$ **do**
      $\boldsymbol{G} = (\boldsymbol{M}^H \boldsymbol{M} + \alpha \boldsymbol{I})^{-1} \boldsymbol{M}^H$
      $\boldsymbol{G}_n = [\,\bar{\boldsymbol{Q}}_r^{(0)} \quad \bar{\boldsymbol{Q}}_r^{(1)}]\,\bar{\boldsymbol{R}}_n$
      $\boldsymbol{M}_n \bar{\boldsymbol{Q}}_r^{(0)} \boldsymbol{T}_r = \tilde{\boldsymbol{U}}_n \tilde{\boldsymbol{\Sigma}}_n \tilde{\boldsymbol{V}}_n{}^H$
      $\boldsymbol{P}_n = \bar{\boldsymbol{Q}}_n^{(0)} \boldsymbol{T}_r \tilde{\boldsymbol{V}}_n^{(1)}$
    end for
    for $j = 1 : r$ **do**
      $C_j = \log_2 \det\left(\boldsymbol{I} + \boldsymbol{R}_{k,j}^{-1} \boldsymbol{M}_j \boldsymbol{P}_j \boldsymbol{P}_j{}^H \boldsymbol{M}_j{}^H\right)$;
    end for
    $a_r = \arg\min_j (C_{max,j} - C_j)$;
    $\boldsymbol{F}_r = \boldsymbol{P}_{a_r}$;
    $\boldsymbol{D}_r = \tilde{\boldsymbol{U}}_{a_r}{}^H$;
    $\boldsymbol{M} = [\,\boldsymbol{H}_1{}^T \cdots \boldsymbol{H}_{a_r-1}{}^T \boldsymbol{H}_{a_r+1}{}^T \cdots \boldsymbol{H}_T{}^T]^T$
  end while
end loop
$\boldsymbol{F} = (\boldsymbol{F}_1 \cdots \boldsymbol{F}_T)$;
$\boldsymbol{D} = \begin{pmatrix} \boldsymbol{D}_1 & & \\ & \ddots & \\ & & \boldsymbol{D}_T \end{pmatrix}$
$\boldsymbol{B} = \text{lower triangular}\left(\boldsymbol{DHF} \bullet \text{diag}\left([\,\boldsymbol{DHF}]_{rr}^{-1}\right)\right)$

4.2 SO-THP+S-GMI algorithm

Further development on SO-THP+GMI with complexity reduction leads to a novel SO-THP+S-GMI algorithm. A simplified GMI (S-GMI) has been developed in [21] as an improvement of the original RBD precoding in [9]. This is known as S-GMI. In (14), a transmit-combining matrix is applied to achieve complete interference cancelation between different users. In this case, the interference will not be completely mitigated, resulting in a slight decrease of the sum rate even though the complexity

will have a significant reduction [21]. Here, we incorporate the S-GMI technique into an SO-THP scheme and devise the SO-THP+S-GMI algorithm. The transmit and receive filters of the proposed SO-THP+S-GMI algorithm are described by

$$\boldsymbol{H}_r \bar{\boldsymbol{Q}}_r^{(0)} = \tilde{\boldsymbol{U}}_r \tilde{\boldsymbol{\Sigma}}_r \tilde{\boldsymbol{V}}_r^H, \tag{17}$$

$$\boldsymbol{P}_{\mathrm{S-GMI}} = [\, \bar{\boldsymbol{Q}}_1^{(0)} \tilde{\boldsymbol{V}}_1 \quad \bar{\boldsymbol{Q}}_2^{(0)} \tilde{\boldsymbol{V}}_2 \quad \cdots \quad \bar{\boldsymbol{Q}}_T^{(0)} \tilde{\boldsymbol{V}}_T \,], \tag{18}$$

$$\boldsymbol{M}_{\mathrm{S-GMI}} = \mathrm{diag}\left\{ \tilde{\boldsymbol{U}}_1^H \quad \tilde{\boldsymbol{U}}_2^H \quad \cdots \quad \tilde{\boldsymbol{U}}_T^H \right\}, \tag{19}$$

where $\boldsymbol{P}_{\mathrm{S-GMI}} \in \mathbb{C}^{N_t \times N_t}$ and $\boldsymbol{M}_{\mathrm{S\text{-}GMI}} \in \mathbb{C}^{N_t \times N_t}$.

With reduced computational complexity, the SO-THP+S-GMI algorithm is capable of achieving better secrecy-rate performance especially at lower signal-to-noise ratio (SNR). The detailed S-GMI procedure implemented in the proposed SO-THP+S-GMI algorithm is shown in Algorithm 2. Cooperated with Algorithm 1, the precoding and receive filter matrices can be obtained.

Algorithm 2 S-GMI Precoding

1: **for** $n = 1 : r$ **do**
2: $\quad \boldsymbol{G} = (\boldsymbol{M}^H \boldsymbol{M} + \alpha \boldsymbol{I})^{-1} \boldsymbol{M}^H$
3: $\quad \boldsymbol{G}_n = [\, \bar{\boldsymbol{Q}}_n^{(0)} \quad \bar{\boldsymbol{Q}}_n^{(1)} \,] \bar{\boldsymbol{R}}_n$
4: $\quad \boldsymbol{M}_n \bar{\boldsymbol{Q}}_n^{(0)} = \tilde{\boldsymbol{U}}_n \tilde{\boldsymbol{\Sigma}}_n \tilde{\boldsymbol{V}}_n^H$
5: $\quad \boldsymbol{P}_n = \bar{\boldsymbol{Q}}_n^{(0)} \tilde{\boldsymbol{V}}_n^{(1)}$
6: **end for**

4.3 LR-SO-THP+S-GMI algorithm

The development in linear algebra contribute to the lattice-reduction technique application in wireless networks. According to the study in [16], a basis change may lead to improved performance as corroborated by lattice-reduction techniques. The more correlated the columns of channel $\boldsymbol{H}$, the more significant the improvements will be. To achieve full diversity of the system, with complex lattice-reduction (CLR) algorithm [25], the LR-transformed channel for the rth user is obtained as

$$\boldsymbol{H}_{\mathrm{red}_r}^H = \boldsymbol{H}_r^H \boldsymbol{L}_r \tag{20}$$

where $\boldsymbol{H}_{\mathrm{red}_r} \in \mathbb{C}^{N_r \times N_t}$ is the transposed reduced channel matrix. The quantity $\boldsymbol{L}_r \in \mathbb{C}^{N_r \times N_r}$ is the transform matrix generated by the CLR algorithm. Note that the transmit power constraint is satisfied since $\boldsymbol{M}_r$ is a unimodular matrix.

Compared to the conventional SO-THP algorithm, the lattice-reduced channel matrix $\boldsymbol{H}_{\mathrm{red}_n}$ is employed in the conventional S-GMI algorithm. The details of the LR-aided S-GMI procedure are given in Algorithm 3. Cooperated with Algorithm 1, we can complete the calculation of the precoding and receive filter matrices.

Algorithm 3 Lattice-Reduction aided S-GMI Procedure

1: **for** $n = 1 : r$ **do**
2: $\quad \boldsymbol{G} = (\boldsymbol{H}^H \boldsymbol{H} + \alpha \boldsymbol{I})^{-1} \boldsymbol{H}^H$
3: $\quad [\, \boldsymbol{H}_{\boldsymbol{red}_n}^H \quad \bar{\boldsymbol{Q}}_n^{(0)} \,] = \mathrm{CLLL}(\boldsymbol{G}_n^H)$
4: $\quad \boldsymbol{M}_n = \boldsymbol{H}_{red_n}$
5: $\quad \boldsymbol{M}_n \bar{\boldsymbol{Q}}_n^{(0)} = \tilde{\boldsymbol{U}}_n \tilde{\boldsymbol{\Sigma}}_n \tilde{\boldsymbol{V}}_n^H$
6: $\quad \boldsymbol{P}_n = \bar{\boldsymbol{Q}}_n^{(0)} \tilde{\boldsymbol{V}}_n^{(1)}$
7: **end for**

5 Analysis of the algorithms

In this section, we develop an analysis of the secrecy rate of the proposed precoding algorithms along with a comparison of the computational complexity between the proposed and existing techniques.

5.1 Computational complexity analysis

According to [25], it can be calculated that the cost of the QR in floating-point operations per second (FLOPS) is 22.4 % lower than BD. The results shown in Table 1 indicate that the complexity is reduced by about 22.4 % by the proposed SO-THP+GMI compared with the conventional SO-THP calculated in the same way. Based on the proposed SO-THP+GMI algorithm, further complexity reduction can be achieved by SO-THP+S-GMI and the

Table 1 Computational complexity of the proposed SO-THP+GMI algorithm

Steps	Operations	FLOPS	Case
			$(2,2,2) \times 6$
1	$\boldsymbol{G}_r = \boldsymbol{U}_r \boldsymbol{\Sigma}_r [\, \boldsymbol{V}_r{}^{(1)} \boldsymbol{V}_r{}^{(0)}]^H$;	$32R(N_t N_r^2$	
		$+N_r^3)$	3072
2	$\bar{\boldsymbol{G}} =$	$(2N_t^3 - 2N_t^2$	
	$\boldsymbol{G} = (\boldsymbol{H}^H \boldsymbol{H} + \alpha \boldsymbol{I})^{-1} \boldsymbol{H}^H$	$+N_t + 16N_R N_t^2)$	3822
3	$\bar{\boldsymbol{G}}_n = \bar{\boldsymbol{Q}}_n \bar{\boldsymbol{R}}_n$	$\sum_{r=1}^{R} 16r(N_t^2 N_r$	
		$+N_t N_r^2 + \frac{1}{3} N_r^3)$	9472
4	$\boldsymbol{H}_{eff,n} = \boldsymbol{H}_n \bar{\boldsymbol{Q}}_n \boldsymbol{T}_n$	$\sum_{r=1}^{R} 16rN_R N_t^2$	20,736
5	$\boldsymbol{H}_{eff,n} = \boldsymbol{U}_n^{(4)} \boldsymbol{\Sigma}_n^{(4)} \boldsymbol{V}_n{}^{(4)H}$	$\sum_{r=1}^{R} 64r(\frac{9}{8} N_r^3 +$	
		$N_t N_r^2 + \frac{1}{2} N_t^2 N_r)$	26,496
6	$\boldsymbol{B} =$ lower triangular		
	$\left(\boldsymbol{DHF} \bullet \mathrm{diag}\left([\boldsymbol{DHF}]_{rr}^{-1} \right) \right)$	$16N_R N_t^2$	3456
			Total 67,054

complexity is about 34.4 % less than that of the conventional SO-THP algorithm.

Figure 3 shows the required FLOPS of the proposed and existing precoding algorithms. Linear precoding gives lower computational complexity, but the BER performance is worse than non-linear ones. The three proposed algorithms show an advantage over the conventional SO-THP algorithm in terms of complexity. Among all the three proposed algorithms, SO-THP+S-GMI has the lowest complexity followed by LR-SO-THP+S-GMI. SO-THP+GMI requires the highest complexity. In Fig. 3, the SO-THP+S-GMI algorithm has similar performance as the LR-SO-THP+S-GMI algorithm. Although the lattice-reduction procedure is implemented in the LR-SO-THP+S-GMI, the matrices produced in the lattice reduction can be also used in the S-GMI algorithm so that the complexity of the LR-SO-THP+S-GMI algorithm is just slightly higher than SO-THP+S-GMI.

5.2 Secrecy-rate analysis

Theorem 1 *In full-rank MU-MIMO systems with perfect knowledge of CSI, the proposed algorithms are capable of achieving a high secrecy rate, and in the high-SNR regime (i.e., $E_s \to \infty$), the secrecy rate will converge to $C_{sec}^{E_s\to\infty}$ which is given as* (21),

$$C_{sec}^{E_s\to\infty} = \log\left(\det\left(\left(\boldsymbol{H}_{ea}\boldsymbol{H}_{ea}^H\right)^{-1}\left(\boldsymbol{H}_{ba}\boldsymbol{H}_{ba}^H\right)\right)\right) \tag{21}$$

Proof Under the conditions

$$\boldsymbol{H}_{ba}^H\boldsymbol{H}_{ba} \succeq \boldsymbol{H}_{ea}^H\boldsymbol{H}_{ea} \tag{22}$$

$$\mathrm{rank}(\boldsymbol{H}_{ba}) = \mathrm{rank}(\boldsymbol{H}_{ea}) \tag{23}$$

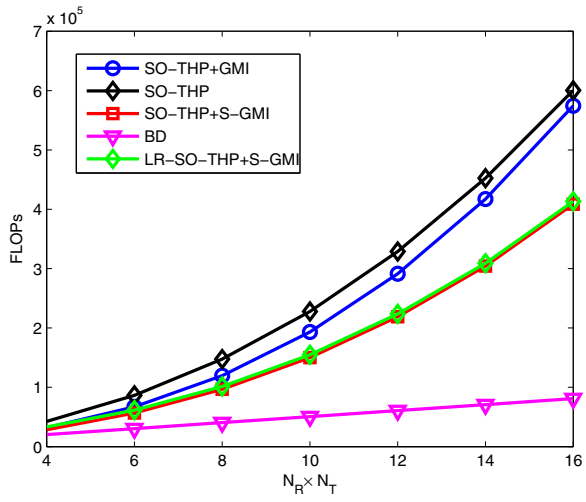


Fig. 3 Computational complexity in FLOPS for MU-MIMO systems

and based on (3), we can have the secrecy capacity expressed as (24). If $\Gamma(\boldsymbol{P}) = (\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1}(\boldsymbol{H}_{ba}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ba}^H)$, (24) can be converted to (25).

$$C_s = \max_{\boldsymbol{Q}_s\succeq 0,\mathrm{Tr}(\boldsymbol{Q}_s)=E_s} \log\left(\det\left((\boldsymbol{I}+\boldsymbol{H}_{ea}\boldsymbol{Q}_s\boldsymbol{H}_{ea}^H)^{-1}(\boldsymbol{I}+\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H)\right)\right) \tag{24}$$

$$C_s = \max_{\boldsymbol{Q}_s\succeq 0,\mathrm{Tr}(\boldsymbol{Q}_s)=E_s} \log\left(\det\left(\Gamma_{ba}(\boldsymbol{P})\Phi_1(\boldsymbol{P},\boldsymbol{Q}_s)^{-1}\Phi_2(\boldsymbol{P},\boldsymbol{Q}_s)\right)\right) \tag{25}$$

$$\Phi_1(\boldsymbol{P},\boldsymbol{Q}_s) = \left(\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H\right)^{-1}\left(\boldsymbol{I}+\boldsymbol{H}_{ea}\boldsymbol{Q}_s\boldsymbol{H}_{ea}^H\right) \tag{26}$$

$$\Phi_2(\boldsymbol{P},\boldsymbol{Q}_s) = \left(\boldsymbol{H}_{ba}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ba}^H\right)^{-1}\left(\boldsymbol{I}+\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H\right) \tag{27}$$

In (25), (26), and (27), $\boldsymbol{P}$ is the precoding matrix derived from the legitimate users' channel. With $\boldsymbol{Q}_s = E[\boldsymbol{x}_s\boldsymbol{x}_s^H] = E[\boldsymbol{P}\boldsymbol{s}\boldsymbol{s}^H\boldsymbol{P}^H]$, $E[\boldsymbol{s}\boldsymbol{s}^H] = E_s$, and $\boldsymbol{P}\boldsymbol{P}^H = \boldsymbol{I}$, we can have

$$E[(\boldsymbol{P}\boldsymbol{P}^H)^{-1}\boldsymbol{Q}_s] = E_s \tag{28}$$

Then

$$E[(\boldsymbol{H}_{ba}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ba}^H)^{-1}\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H] = E_s \tag{29}$$

$$E[(\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1}\boldsymbol{H}_{ea}\boldsymbol{Q}_s\boldsymbol{H}_{ea}^H] = E_s \tag{30}$$

In (25), the expectation value is given as (31). Substituting (29) into (31), the formula can be expressed as (33).

$$\begin{aligned} SA &= E\left[\Phi_1(\boldsymbol{P},\boldsymbol{Q}_s)^{-1}\Phi_2(\boldsymbol{P},\boldsymbol{Q}_s)\right] \\ &= E\left[\Phi_3(\boldsymbol{P},\boldsymbol{Q}_s)^{-1}\left((\boldsymbol{H}_{ba}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ba}^H)^{-1}\right.\right. \\ &\quad \left.\left.+(\boldsymbol{H}_{ba}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ba}^H)^{-1}\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H\right)\right] \end{aligned} \tag{31}$$

$$\begin{aligned} \Phi_3(\boldsymbol{P},\boldsymbol{Q}_s) &= (\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1} \\ &\quad +(\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1}\boldsymbol{H}_{ea}\boldsymbol{Q}_s\boldsymbol{H}_{ea}^H \end{aligned} \tag{32}$$

$$\begin{aligned} SA &= E\left[\left((\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1}+E_s\right)^{-1}\left((\boldsymbol{H}_{ba}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ba}^H)^{-1}+E_s\right)\right] \\ &= E\left[\left((\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1}+E_s+\boldsymbol{I}\right)^{-1}\left((\boldsymbol{H}_{ba}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ba}^H)^{-1}\right)\right] \\ &\quad -(\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1})\Big] \end{aligned} \tag{33}$$

According to (33), in the high-SNR regime and when SNR $\to \infty$, $E_s \to \infty$, $SA \to \boldsymbol{I}$. Then, the secrecy rate expressed in (25) will result in (34).

$$C_{\mathrm{sec}}^{E_s\to\infty} = \log\left(\det\left((\boldsymbol{H}_{ea}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ea}^H)^{-1}(\boldsymbol{H}_{ba}\boldsymbol{P}\boldsymbol{P}^H\boldsymbol{H}_{ba}^H)\right)\right) \tag{34}$$

To satisfy the power constraint, we always have $E[\boldsymbol{P}\boldsymbol{P}^H] = \boldsymbol{I}$, then the secrecy rate C_{sec} will converge to a constant, that is,

$$C_{\mathrm{sec}}^{E_s\to\infty} = \log\left(\det(\boldsymbol{H}_{ea}\boldsymbol{H}_{ea}^H)^{-1}(\boldsymbol{H}_{ba}\boldsymbol{H}_{ba}^H)\right) \tag{35}$$

This completes the proof. □

In the following, the percentage of the injected artificial noise power is set to 40 % of the total transmit power. The percentage of the artificial noise power is determined to achieve an optimal result in terms of the secrecy rate. The details of the derivation are expressed in the Appendix. When AN is added during the transmission, Eq. (3) can be transformed to

$$\begin{aligned}&\log\left(\det(\boldsymbol{I}+\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H)\right)\\&-\log\left(\det\left(\boldsymbol{I}+(\boldsymbol{I}+\boldsymbol{H}_{ea}\boldsymbol{Q}_s'\boldsymbol{H}_{ea}^H)^{-1}(\boldsymbol{H}_{ea}\boldsymbol{Q}_s\boldsymbol{H}_{ea}^H)\right)\right)\end{aligned} \tag{36}$$

To assess the influence of different channel gain ratios between legitimate users and the eavesdroppers, we fix the legitimate users' channel gain and change the eavesdroppers. The above Eq. (36) can be further transformed to

$$\begin{aligned}&\log(\det(\boldsymbol{I}+\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H))\\&-\log(\det(\boldsymbol{I}+((\boldsymbol{H}_{ea}\boldsymbol{H}_{ea}^H)^{-1}+\boldsymbol{Q}_s')^{-1}\boldsymbol{Q}_s)\end{aligned} \tag{37}$$

In the high-SNR regime, $E_s \to \infty$, according to (28), $Q_s, Q_s' \to \infty$, the term $(\boldsymbol{H}_{ea}\boldsymbol{H}_{ea}^H)^{-1}$ then can be omitted and the result is the following expression

$$\log(\det(\boldsymbol{I}+\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H))-\log(\det(\boldsymbol{I}+(\boldsymbol{Q}_s')^{-1}\boldsymbol{Q}_s), \tag{38}$$

Considering artificial noise, $(\boldsymbol{Q}_s')^{-1}\boldsymbol{Q}_s = \rho/(1-\rho)\boldsymbol{I}$. When ρ is fixed, $\log(\det(\boldsymbol{I}+(\boldsymbol{Q}_s')^{-1}\boldsymbol{Q}_s))$ would be a constant. From (38), the secrecy rate will increase even when the eavesdroppers have better statistical channel knowledge than the legitimate users. Although, the secrecy rate can be positive in the scenario that the eavesdroppers have better statistical channel knowledge. With more power allocated to the artificial noise $1-\rho \to 1$, less power will be available for the users $\rho \to 0$ which will lead to a fast decrease of the capacity to the intended users which is expressed as $\log(\det(\boldsymbol{I}+\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H))$. As a result, the secrecy rate will finally fall down to zero. By changing the variable ρ from 0.1 to 0.9, the secrecy rate will rise to an optimal value, then converge to zero.

6 Simulation results

A system with $N_t = 4$ transmit antennas and $T = 2$ users as well as $K = 1, 2$ eavesdroppers is considered. Each user or eavesdropper is equipped with $N_r = 2$ and $N_k = 2$ receive antennas.

6.1 Perfect channel state information

In Fig. 4, the proposed LR-SO-THP+S-GMI algorithm has the best BER performance. The SO-THP+S-GMI algorithm has the exact same secrecy-rate performance as the SO-THP+GMI algorithm. In Fig. 5, all of these non-linear proposed algorithms can achieve a much higher secrecy-rate performance especially in low-SNR scenarios. In the scenario where $T > K$, the secrecy rate of the proposed algorithms has around a 5 bits/Hz higher rate than the other precoding techniques. When $T = K$, Fig. 6a shows that the proposed algorithms achieve a higher secrecy rate than the other techniques at low SNRs. And the

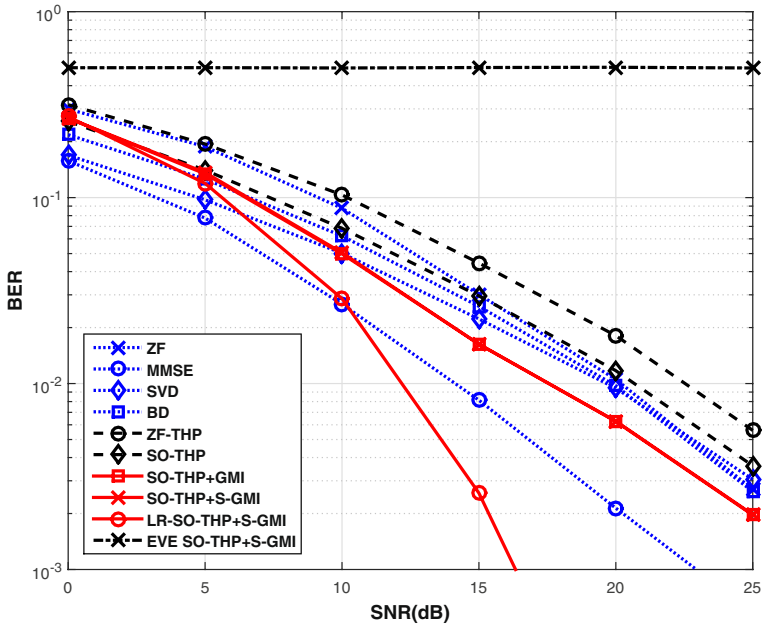


Fig. 4 BER performance with precoding techniques in 4 × 4 × 2 MU-MIMO broadcast channel, $m = 0.5$

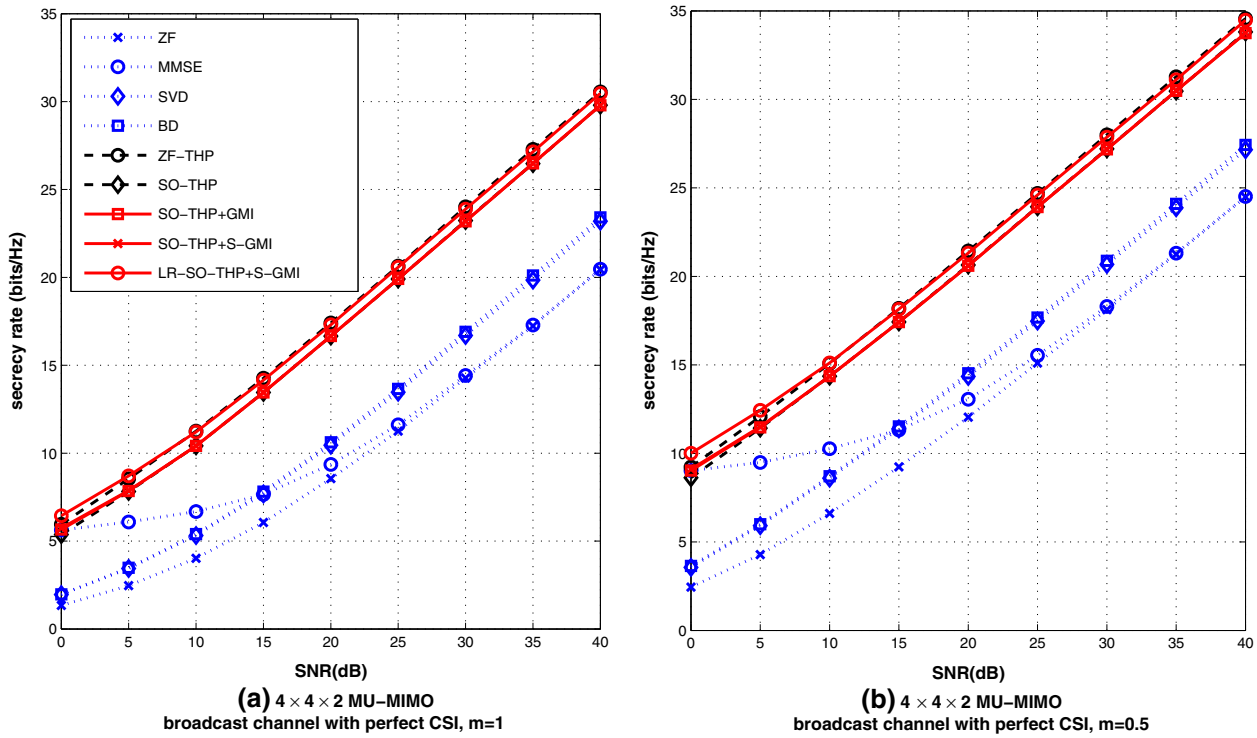


Fig. 5 Secrecy-rate performance with precoding techniques in a 4 × 4 × 2 MU-MIMO broadcast channel, $m = 0.5$ and 1

secrecy rate will converge to a constant which will depend on the gain ratio between the main and the wire-tap channels m.

6.2 Imperfect channel state information

In the simulations, the channel errors are modeled as a complex random Gaussian noise matrix $\boldsymbol{E}$ following the distribution $\mathcal{CN}(0, \sigma_e^2)$. Then, the imperfect channel matrix $\boldsymbol{H}^e$ is defined as

$$\boldsymbol{H}^e = \boldsymbol{H} + \boldsymbol{E} \tag{39}$$

We assume the channels of the legitimate users are perfect and the eavesdropper will have imperfect CSI.

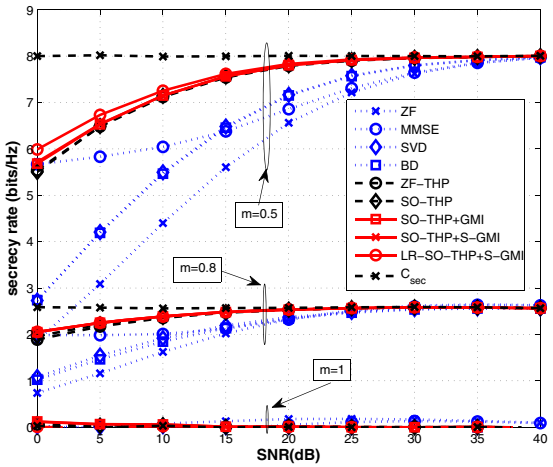
In Fig. 6b, the secrecy-rate performance is evaluated in the imperfect CSI scenario. Compared with the secrecy-rate performance in Fig. 6a, the secrecy rate will suffer a huge decrease in the imperfect CSI scenario. When $T = K$, Fig. 6b shows that the secrecy rate at low SNR is degraded and the secrecy rate requires very high SNR to converge to a constant. It is worth noting that the proposed SO-THP+S-GMI has the best secrecy-rate performance among the studied precoding techniques.

6.3 Imperfect channel state information with artificial noise

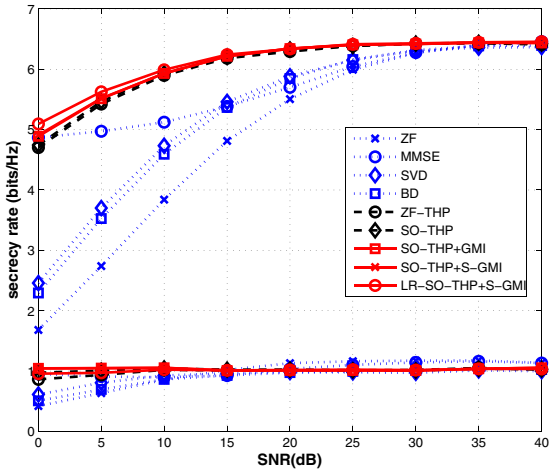
In Fig. 6c AN is added and the total transmit power E_s is the same as before. Comparing the results in Fig. 6b, c, it is clear that by injecting the artificial noise, the secrecy rate can achieve a much better performance in a high-SNR scenario. In Fig. 6c, the channel gain ratio is $m = 2$. According to the secrecy performance of Fig. 6d, 40 % of the transmit power E_s is used to generate AN. In Fig. 6d, it shows the secrecy rate with the change of the transmit signal power ratio to the artificial noise. The channel gain ratio is $m = 1$. Comparing the theoretical result and the simulation result, the optimal value can be achieved when the transmit signal power ratio to the artificial noise is 0.6.

7 Conclusions

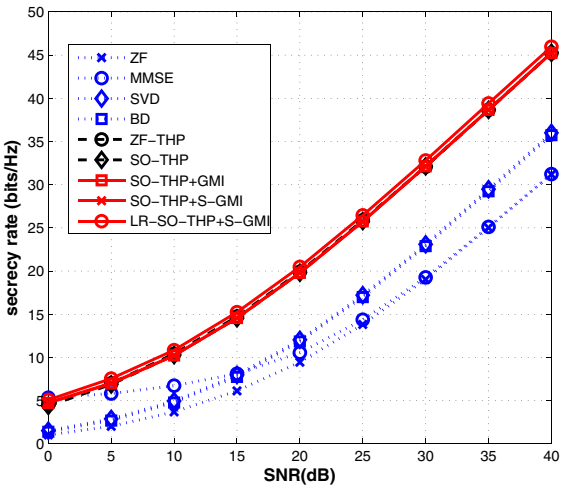
Precoding techniques are widely used in the downlink of MU-MIMO wireless networks to achieve good BER performance. They also contribute to the improvement of the secrecy rate in the physical layer. The three proposed algorithms can all achieve higher secrecy-rate performance than conventional techniques. Firstly, if we consider the complexity as the most important metric, among all the studied non-linear precoding techniques, the proposed SO-THP+S-GMI algorithm requires the lowest computational complexity which results in a



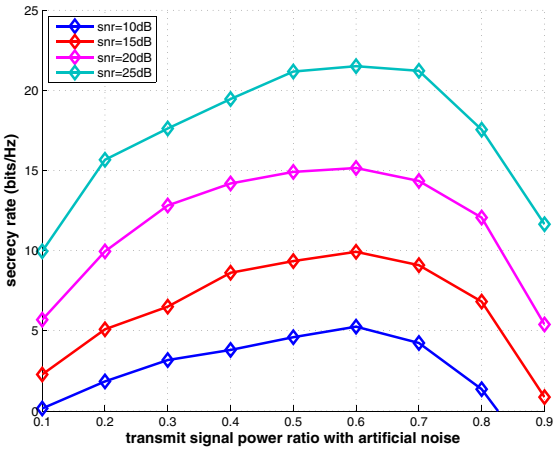
(a) Secrecy rate performance with precoding techniquesin 4×4×4 MU-MIMO broad cast channel



(b) Secrecy rate with precoding techniques 4×4×4 MU-MIMO broadcast channel with imperfect CSI



(c) Secrecy rate with precoding techniques 4×4×2 MU-MIMO broadcast channel with imperfect CSI, AN and m=2



(d) Secrecy rate change with different artificial noise power ratio

Fig. 6 Secrecy-rate performance with different CSI scenarios

significant improvement on the efficiency. Secondly, if the transmission accuracy comes first in the design, the LR-SO-THP+S-GMI algorithm is also superior to the existing linear and non-linear algorithms considered.

Appendix

Based on Eq. (38), if we consider $\rho \boldsymbol{A} = \boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H$ and $(\boldsymbol{Q}_s')^{-1}\boldsymbol{Q}_s = \rho/(1-\rho)\boldsymbol{I}$, it can be rewritten as

$$\log(\det(\boldsymbol{I}+\rho\boldsymbol{A})) - \log(\det(\boldsymbol{I}+\rho/(1-\rho)\boldsymbol{I}), \quad (40)$$

Here, we first take the derivative of $\log(\det(\boldsymbol{I}+\rho\boldsymbol{A}))$. Firstly, we assume $\boldsymbol{A}$ is an $m \times m$ matrix. The eigenvalue of matrix $\boldsymbol{I}+\rho\boldsymbol{A}$ is $1+\rho a_1, 1+\rho a_2, \cdots 1+\rho a_m$. The eigenvalue of matrix $\boldsymbol{A}(\boldsymbol{I}+\rho\boldsymbol{A})^{-1}$ is $\frac{a_1}{1+\rho a_1}$, , $\frac{a_2}{1+\rho a_2}$, $\cdots$ $\frac{a_m}{1+\rho a_m}$. With these assumptions, we can have

$$\det(\boldsymbol{I}+\rho\boldsymbol{A}) = (1+\rho a_1)(1+\rho a_2)\cdots(1+\rho a_m), \quad (41)$$

and

$$\mathrm{Tr}(\boldsymbol{A}(\boldsymbol{I}+\rho\boldsymbol{A})^{-1}) = \frac{a_1}{1+\rho a_1}+\frac{a_2}{1+\rho a_2}+\cdots+\frac{a_m}{1+\rho a_m}. \tag{42}$$

The differentiate of $\log(\det(\boldsymbol{I}+\rho\boldsymbol{A}))$ can be expressed as

$$\begin{aligned}\frac{d\{\log(\det(\boldsymbol{I}+\rho\boldsymbol{A}))\}}{d\rho} &= \frac{d\{\log((1+\rho a_1)(1+\rho a_2)\cdots(1+\rho a_m))\}}{d\rho},\\ &= \frac{d\{\log(1+\rho a_1)\}}{d\rho}\\ &\quad+\frac{d\{\log(1+\rho a_2)\}}{d\rho}+\cdots\\ &\quad+\frac{d\{\log(1+\rho a_m)\}}{d\rho},\\ &= (\frac{a_1}{1+\rho a_1}+\frac{a_2}{1+\rho a_2}+\cdots\\ &\quad+\frac{a_m}{1+\rho a_m})\ln(2),\\ &= \mathrm{Tr}(\boldsymbol{A}(\boldsymbol{I}+\rho\boldsymbol{A})^{-1})\ln(2).\end{aligned} \tag{43}$$

Similarly, the differentiate of $\log(\det(\boldsymbol{I}+\rho/(1-\rho)\boldsymbol{I})$ can be obtained as $\mathrm{Tr}(\boldsymbol{I})\ln(2)$. The optimal value can be obtained by calculating

$$\mathrm{Tr}(\boldsymbol{A}(\boldsymbol{I}+\rho\boldsymbol{A})^{-1})\ln(2)-\mathrm{Tr}(\boldsymbol{I})\ln(2)=0 \tag{44}$$

which is equivalent to

$$(1-\rho)\boldsymbol{A}=\boldsymbol{I}. \tag{45}$$

Substituting $\boldsymbol{A}$ with $\frac{1}{\rho}\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H$, (45) can be rewritten as

$$(\frac{1}{\rho}-1)\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H=\boldsymbol{I}. \tag{46}$$

Given the constraints $\mathrm{Tr}(\boldsymbol{Q}_s)=\rho E_s$ and $\boldsymbol{H}_{ba}\in\mathcal{CN}(0,1)$, in the simulation scenario, we can solve (46) as

$$4(\frac{1}{\rho}-1)\rho^2=1. \tag{47}$$

The optimal value is achieved at $\rho=0.5$. However, due to the existence of Gaussian noise, the optimal value is shifted. Based on (44), we focus on the first term $\mathrm{Tr}(\boldsymbol{A}(\boldsymbol{I}+\rho\boldsymbol{A})^{-1})\ln(2)$. It can be rewritten as $\mathrm{Tr}((\boldsymbol{A}^{-1})^{-1}(\boldsymbol{I}+\rho\boldsymbol{A})^{-1})\ln(2)$. Finally, we can have

$$\mathrm{Tr}(\boldsymbol{A}^{-1}+\rho\boldsymbol{I})\ln(2) \tag{48}$$

when considering Gaussian noise, $\boldsymbol{A}=\frac{1}{\sigma_n^2\rho}\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H$. Here, σ_n^2 represents the variance of the noise. When the signal variance is set to 1, we can have $\sigma_n^2<1$. If we use the matrix $\boldsymbol{N}_a$ to represent the effect of the noise, we can transfer $\boldsymbol{A}=\frac{1}{\rho}\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H+\boldsymbol{N}_a$ where the elements in $\boldsymbol{N}_a$ are positive. Substituting $\boldsymbol{A}$ with $\frac{1}{\rho}\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H+\boldsymbol{N}_a$, (45) can be obtained as

$$(\frac{1}{\rho}-1)(\boldsymbol{H}_{ba}\boldsymbol{Q}_s\boldsymbol{H}_{ba}^H+\boldsymbol{N}_a)=\boldsymbol{I}. \tag{49}$$

Comparing (46) with (49), the optimal value of (49) is achieved at a higher value of ρ which is 0.6 in our simulation.

Competing interests
The authors declare that they have no competing interests.

Author details
[1]Communications Research Group, Department of Electronics, , University of York, YO10 5DD York, UK. [2]CETUC, PUC-Rio, Rio de Janeiro, Brazil. [3]Ericsson Research, Kista, Sweden.

Received: 29 May 2016 Accepted: 10 October 2016
Published online: 26 October 2016

References

1. S Soni, H Agrawal, M Sharma, Analysis and comparison between AES and DES cryptographic algorithm. Int.J. Eng. Innov. Technol. (IJEIT). **2**(3) (2012)
2. C Shannon, Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949)
3. AD Wyner, The wire-tap channel. Bell Syst. Techn. J. **54**(8), 1385–1357 (1975)
4. I Csiszár, J Körner, Broadcast channels with confidential messages. IEEE Trans. Inf. Theory. **24**(3), 339–348 (1978)
5. S Leung-Yan-Cheong, M Hellman, The Gaussian wire-tap channel. IEEE Trans. Inf. Theory. **24**(4), 451–456 (1978)
6. F Oggier, B Hassibi, The secrecy capacity of the mimo wiretap channel. IEEE Trans. Inf. Theory. **57**(8), 4961–4972 (2011)
7. S Goel, R Negi, Guaranteeing secrecy using artificial noise. IEEE Trans. Wirel. Commun. **7**(6), 2180–2189 (2008)
8. A Mukherjee, A Swindlehurst, Jamming games in the MIMO wiretap channel with an active eavesdropper. IEEE Trans. Signal Process. **61**(1), 82–91 (2013)
9. V Stankovic, M Haardt, Generalized design of multi-user MIMO precoding matrices. IEEE Trans. Wirel. Commun. **7**(3), 953–961 (2008)
10. Y Cai, DL Ruyet, RC de Lamare, D Roviras, in *IEEE 12th International Workshop, Signal Processing Advances in Wireless Communications (SPAWC)*. Linear precoding based on switched relaying processing for multiuser MIMO relay systems, (2011), pp. 351–355
11. G Geraci, M Egan, J Yuan, A Razi, IB Collings, Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding. IEEE Trans. Commun. **60**(11), 3472–3482 (2012)
12. M Payaro, A Perez-Neira, M Lagunas, in *IEEE 60th Vehicular Technology Conference*. Achievable rates for generalized spatial Tomlinson-Harashima precoding in MIMO systems, vol. 4, (2004), pp. 2462–2466
13. M Mazrouei-Sebdani, W Krzymien, Vector perturbation precoding for network MIMO: sum rate, fair user scheduling, and impact of backhaul delay. IEEE Trans. Veh. Technol. **61**(9), 3946–3957 (2012)
14. P Lin, S Lai, S Lin, On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels. IEEE J.Sel. Areas Commun. **31**(9), 1728–1740 (2013)
15. A Chorti, H Poor, Achievable secrecy rates in physical layer secure systems with a helping interferer. Comput. Netw. Commun. (ICNC), 18–22 (2012)
16. H Yao, W Wornell, in *Global Telecommunications Conference*. Lattice-reduction-aided detectors for MIMO communication systems, vol. 1, (2002), pp. 424–428
17. M Taherzadeh, A Mobasher, A Khandani, Lll reduction achieves the receive diversity in MIMO decoding. IEEE Trans. Inf. Theory. **53**(12), 4801–4805 (2007)
18. V Stankovic, M Haardt, in *IEEE International Conference, Proceedings.(ICASSP '05)*. Successive optimization Tomlinson-Harashima precoding (SO THP) for multi-user MIMO systems, vol. 3, (2005), pp. 1117–1120
19. F Dietrich, P Breun, W Utschick, Robust Tomlinson–Harashima precoding for the wireless broadcast channel. IEEE Trans.Signal Process. **55**(2), 631–644 (2007)
20. S Hakjea, L Sang-Rim, L Inkyu, Generalized channel inversion methods for multiuser MIMO systems. IEEE Trans.Commun. **57**(11), 3489–3499 (2009)
21. K Zu, RC de Lamare, M Haart, Generalized design of low-complexity block diagonalization type precoding algorithms for multiuser MIMO systems. IEEE Trans.Commun. **61**(10), 4232–4242 (2013)

22. M Costa, Writing on dirty paper. IEEE Trans.Inf. Theory. **29**(3), 439–441 (1983)
23. M Huang, S Zhou, J Wang, Analysis of Tomlinson-Harashima precoding in multiuser MIMO systems with imperfect channel state information. IEEE Trans.Veh. Technol. **57**(5), 2856–2867 (2008)
24. K Zu, RC de Lamare, M Haardt, Multi-branch Tomlinson-Harashima precoding design for MU-MIMO systems: theory and algorithms. IEEE Trans.Commun. **62**(3), 939–951 (2014)
25. K Zu, RC de Lamare, Low-complexity lattice reduction-aided regularized block diagonalization for MU-MIMO systems. IEEE Commun.Lett. **16**(6), 925–928 (2012)