Tomlinson-Harashima Precoding Design in MIMO Wiretap Channels Based on the MMSE Criterion

Lei Zhang*, Yunlong Cai*, Benoit Champagne†, Minjian Zhao*
*Department of Information Science and Electronic Engineering, Zhejiang University, Hangzhou, China, 310027
†Department of Electrical and Computer Engineering, McGill University, Montreal, QC, Canada, H3A 0E9
Emails: {bestleileisara, ylcai, mjzhao}@zju.edu.cn and benoit.champagne@mcgill.ca

***Abstract*—This paper investigates the Tomlinson-Harashima precoding (THP) design for secure communications in broadcast multiple-input multiple-output (MIMO) systems in the presence of a passive eavesdropper. We focus on optimizing the nonlinear transceiver to guarantee a certain Quality-of-Service (QoS) level for the intended receiver in terms of mean-squared-error (MSE). The scheme allocates the transmit power in order to achieve the target MSE for the intended receiver, and then uses the remaining available power to transmit artificial noise (AN) to degrade the eavesdropper's channel. With the geometric mean decomposition (GMD) based THP, the lower MSE bound can be achieved. We convert the nonlinear transmit power minimization problem to a standard convex optimization problem. The solution for the problem is obtained by the waterfilling method via the Karush-Kuhn-Tucker (KKT) conditions. Simulation results demonstrate that the proposed nonlinear scheme outperforms existing linear transceiver designs.** [1]

***Index Terms*—Artificial noise, physical layer secure communications, multiple-input multiple-output (MIMO), Tomlinson-Harashima precoding (THP), convex optimization**

I. Introduction

Nowadays, with the continuous increase in transmission rate and reliability of wireless communications, service providers are shifting more attention toward the privacy and security. Traditionally, communication secrecy is achieved by using cryptographic encryption algorithms at the network layer [1]. However, these algorithms suffer from high complexity and inherent vulnerabilities associated with secret key distribution and management. As a result, research on new physical layer techniques to guarantee secure communications has drawn considerable interest lately. The physical layer security problem was first introduced by Wyner [2], who proposed the concept of wiretap channel and established the so-called Alice-Bob-Eve transmission model. Many recent studies on the Gaussian wiretap channel have focused on information theoretic aspects such as the secrecy capacity issue [3], [4]. The secrecy capacity achievable in multiple-input multiple-output (MIMO) systems has also been studied in [5]–[9] due to the great advantages of MIMO techniques. In parallel to these works, the authors in [10]–[13] optimized the transmission design based on quality of service (QoS) criteria. Recently, authors in [13] considered the joint transmit and receive filters design which minimizes the mean-squared-error (MSE) between the legitimate parties, whilst guaranteeing that the MSE of the eavesdropper remains above a certain threshold subject to a power constraint. Compared with designs derived from an information-theoretic viewpoint, the filter designs based on the MSE criterion to characterize security lead to realizable processing structures which can be easily implemented in practical systems.

An important aspect for MIMO secure communications is the availability of channel state information (CSI). When the eavesdropper is passive, it is difficult for the transmitter to obtain the CSI of the former. To overcome this problem, the injection of artificial noise (AN) emerged as a promising technique to guarantee secrecy without the knowledge of the eavesdropper's channel [14]. The transmission of AN along with the precoded information-bearing signal can be employed to deteriorate quality of reception at the eavesdropper. To this end, the transmitter aligns the AN within the null space of the legitimate receiver's channel; consequently, only the eavesdropper's channel is degraded. Since the use of AN will decrease the available power for data transmission, the power allocation between the information-bearing signal and the AN is of great importance to ensure good performance under secrecy constraints. Some power allocation strategies were proposed in [11], [12], which aim to meet a target signal-to-interference-and-noise ratio (SINR) at the desired receiver to satisfy the QoS requirement.

In recent years, precoding techniques have been widely applied to MIMO systems. Compared with the conventional linear precoding design, nonlinear precoding provides an alternative algorithm that offers the potential for performance improvements over the linear approaches. A capacity achieving nonlinear dirty paper coding (DPC) technique [15] was first proposed for pre-subtracting interference at the source prior to transmission. However, the complexity of DPC is prohibitively high, which motivates various suboptimal approaches. For this reason, the Tomlinson-Harashima precoding (THP) algorithm [16] which employs a transmit feedback filter and a modulo operation to limit the transmitted power was presented as a low complexity alternative. While the linear precoding techniques have been applied to physical layer security as in e.g., [7]–[10], the study of the nonlinear precoding design in secure communications remains largely unexplored.

In this paper, we propose a QoS-based THP scheme for secure transmission, where two legitimate parties (Alice and Bob) communicate in the presence of an eavesdropper (Eve) over a Gaussian MIMO wiretap channel. We focus on minimizing the transmit power to guarantee a certain QoS criterion for the intended receiver in terms of MSE. Then the transmitter utilizes the remaining available power to emit the AN

[1] This work was supported in part by the National Natural Science Foundation of China under Grants 61471319, Zhejiang Provincial Natural Science Foundation of China under Grant LY14F010013, the Fundamental Research Funds for the Central Universities, and the National High Technology Research and Development Program (863 Program) of China under Grant 2014AA01A707.

to degrade the eavesdropper's channel. The transmit power minimization problem can be solved by using the bisection method while satisfying the MSE requirement for the intended receiver. We apply the geometric mean decomposition (GMD) [17] to design the THP and show that the resulting GMD-THP achieves the MSE lower bound. We finally convert the nonlinear problem to a standard convex optimization problem. The solution for the precoder is obtained by the waterfilling method via the Karush-Kuhn-Tucker (KKT) conditions. Simulation results are provided to illustrate the secrecy performance and advantages of the proposed nonlinear algorithm.

The rest of the paper is organized as follows. The system model is introduced in Section II. In Section III, we present the proposed THP-based transceiver design for the MIMO wiretap channel. Simulation results and comparisons are given in Section IV. Finally, conclusions are drawn in Section V.

Notation: Throughout the paper, we denote vectors and matrices by lower and upper case bold letters, respectively. The operators $(\cdot)^T$, $(\cdot)^H$, $\mathrm{tr}(\cdot)$ and $|\cdot|$ denote the matrix transpose, Hermitian transpose, trace and determinant, respectively. $\lfloor\cdot\rfloor$ represents the floor operator which returns the largest integer smaller than or equal to the argument. $\mathrm{E}[\cdot]$ stands for the statistical expectation. $\mathbf{A}^{-\frac{1}{2}}$ represents the inverse square root of positive definite matrix $\mathbf{A}$. $\mathrm{diag}(\mathbf{A})$ denotes the diagonal matrix whose elements are the elements of $\mathbf{A}$.

II. System Model

We consider a scenario with two nodes, Alice and Bob, and a passive eavesdropper, Eve. They are equipped with N_a, N_b and N_e antennas, respectively. It is further assumed that only the CSI of the legitimate channel between Alice and Bob is known at the transmitter. The secrecy network consists of a source THP for Alice and a linear minimum-mean-squared-error (MMSE) receiver for Bob, as shown in Fig. 1. The source signal vector $\mathbf{s} = [s_1, ..., s_N]^T$ is obtained from m-ary square quadrature amplitude modulation (QAM) where the real and imaginary parts of s_k belong to the set $\{\pm 1, ..., \pm(\sqrt{m}-1)\}$. The transmit vector $\mathbf{x} = [x_1, ..., x_N]^T$ is recursively computed through the application of a backward squared matrix $\mathbf{U}$ and a nonlinear modulo operation, which in effect amounts to a successive cancellation operation.

In Fig. 1, $\mathrm{MOD}_m(\cdot)$ stands for the modulo operator which is used to constrain its input argument to the interval $(-\sqrt{m}, \sqrt{m}]$. In fact, the modulo operator acts independently on the real and imaginary parts of its input according to the following rule ($x \in \mathbb{R}$ is assumed):

$$\mathrm{MOD}_m(x) = x - 2\sqrt{m}\left\lfloor \frac{x+\sqrt{m}}{2\sqrt{m}} \right\rfloor. \tag{1}$$

With the help of the modulo operation in (1) and the matrix $\mathbf{U}$, which is a strictly lower triangular, the entries of vector $\mathbf{x}$ are successively generated as

$$x_k = s_k - \sum_{n=1}^{k-1} \mathbf{U}(k,n)s_n + e_k, \tag{2}$$

where $\mathbf{e} = [e_1, ..., e_N]^T$ is the vector selected by the modulo operation to ensure that the real and imaginary parts of the elements in $\mathbf{x}$ are bounded by the square region. The previous equation can be rewritten into a compact form as

$$\mathbf{x} = \mathbf{B}^{-1}\mathbf{v}, \tag{3}$$

where $\mathbf{B} = \mathbf{U} + \mathbf{I}$ is a lower triangular matrix with ones on the main diagonal, $\mathbf{v}$ is given by $\mathbf{v} = \mathbf{s} + \mathbf{e}$. The vector $\mathbf{x}$ is the information-bearing signal intended for Bob. Also, an AN vector $\mathbf{z} \in \mathbb{C}^{(N_a - N)\times 1}$ is designed to interfere with Eve. The entries of $\mathbf{z}$ are chosen as independent and identically distributed (i.i.d.) Gaussian random variables with zero-mean and unit-variance.

Hence, the precoded signal $\mathbf{x}_a$ transmitted by Alice has the following structure:

$$\mathbf{x}_a = \mathbf{F}\mathbf{x} + \mathbf{T}\mathbf{z}, \tag{4}$$

where $\mathbf{F} \in \mathbb{C}^{N_a \times N}$ and $\mathbf{T} \in \mathbb{C}^{N_a \times (N_a - N)}$ represent the precoding matrices corresponding to $\mathbf{x}$ and $\mathbf{z}$, respectively.

The maximum transmit power available for Alice is assumed to be constrained by P, i.e., we have

$$\mathrm{E}\left[\mathbf{x}_a \mathbf{x}_a^H\right] = \mathbf{Q}_a \tag{5}$$

$$\mathrm{tr}(\mathbf{Q}_a) = P. \tag{6}$$

The signals received by the legitimate receiver Bob and the eavesdropper Eve can be respectively represented as

$$\mathbf{y}_b = \mathbf{H}_{ba}\mathbf{x}_a + \mathbf{n}_b \tag{7}$$

$$\mathbf{y}_e = \mathbf{H}_{ea}\mathbf{x}_a + \mathbf{n}_e, \tag{8}$$

where $\mathbf{H}_{ba} \in \mathbb{C}^{N_b \times N_a}$ denotes the legitimate channel matrix between Alice and Bob, $\mathbf{H}_{ea} \in \mathbb{C}^{N_e \times N_a}$ stands for the channel matrix between Alice and Eve. $\mathbf{n}_b \in \mathbb{C}^{N_b \times 1}$ and $\mathbf{n}_e \in \mathbb{C}^{N_e \times 1}$ are the zero-mean complex Gaussian noise vectors with the covariance of $\sigma_b^2\mathbf{I}$ and $\sigma_e^2\mathbf{I}$, respectively.

At the receiver Bob, a linear receiver $\mathbf{R_b}$ is then employed to detect the received signal:

$$\hat{\mathbf{v}}_b = \mathbf{R}_b^H \mathbf{y}_b = \mathbf{R}_b^H \mathbf{H}_{ba}\mathbf{F}\mathbf{x} + \mathbf{R}_b^H \mathbf{H}_{ba}\mathbf{T}\mathbf{z} + \mathbf{R}_b^H \mathbf{n}_b. \tag{9}$$

Finally, the receiver has to be equipped with another modulo operator to recover the transmit signal.

$$\hat{\mathbf{s}}_b = \mathrm{Q}\left(\mathrm{MOD}_m\left(\hat{\mathbf{v}}_b\right)\right), \tag{10}$$

where $\mathrm{Q}(\cdot)$ denotes the quantization operation.

III. Proposed Nonlinear Transceiver Design

In this work, we aim to maximize the transmit power of the AN subject to the MSE constraint on Bob and the total power constraint of Alice. This is equivalent to minimizing the transmit power of the information-bearing signal to achieve the MSE target ε_b for Bob, and to use the remaining resources to transmit AN to impair the reception by Eve.

For the design of precoder $\mathbf{T}$, we require that

$$\mathbf{H}_{ba}\mathbf{F}\mathbf{x} \perp \mathbf{H}_{ba}\mathbf{T}\mathbf{z} \tag{11}$$

for all $\mathbf{z}$, which means $\mathbf{F}^H\mathbf{H}_{ba}^H\mathbf{H}_{ba}\mathbf{T} = \mathbf{0}$.

Here we use the optimal Wiener filter for Bob:

$$\mathbf{R}_b^H = \mathbf{B}\mathbf{F}^H\mathbf{H}_{ba}^H\left(\mathbf{H}_{ba}\mathbf{F}\mathbf{F}^H\mathbf{H}_{ba}^H + \mathbf{H}_{ba}\mathbf{T}\mathbf{T}^H\mathbf{H}_{ba}^H + \sigma_b^2\mathbf{I}\right)^{-1}. \tag{12}$$

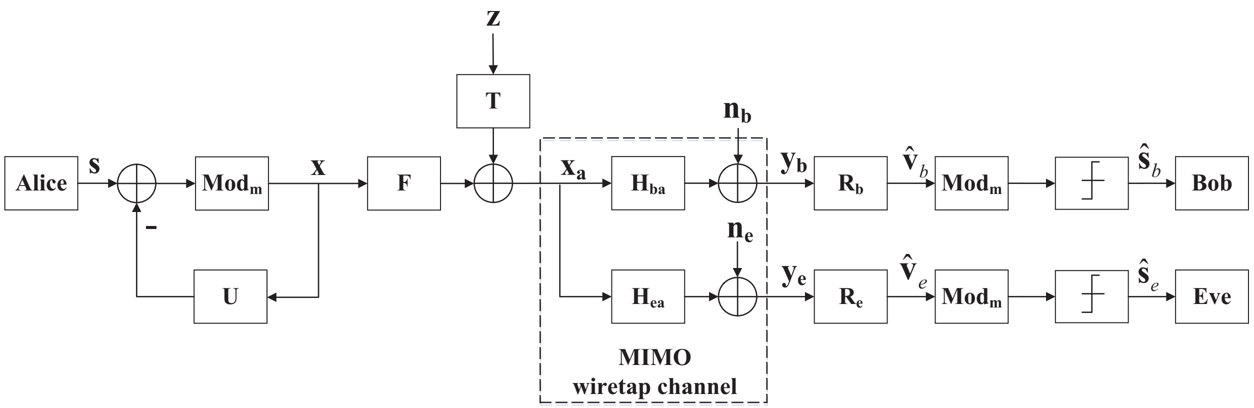

Fig. 1: MIMO wiretap channel with THP-based transmitter and MMSE receiver

By substituting the receiver matrix $\mathbf{R}_b$ and making use of the matrix inversion lemma [18], the MSE matrix of Bob is calculated as

$$\begin{aligned}
&\mathrm{MSE}_b\left(\mathbf{F},\mathbf{T},\mathbf{R}_b,\mathbf{B}\right)=\mathrm{E}\left[\left\|\mathbf{R}_b^H\mathbf{y}_b-\mathbf{v}\right\|^2\right]\\
&=\mathrm{E}\left[\mathrm{tr}\left(\left(\mathbf{R}_b^H\mathbf{H}_{ba}\mathbf{F}-\mathbf{B}\right)\left(\mathbf{R}_b^H\mathbf{H}_{ba}\mathbf{F}-\mathbf{B}\right)^H\right)\right]\\
&\quad+\mathrm{E}\left[\mathrm{tr}\left(\left(\mathbf{R}_b^H\mathbf{H}_{ba}\mathbf{T}\right)\left(\mathbf{R}_b^H\mathbf{H}_{ba}\mathbf{T}\right)^H\right)\right]+\mathrm{tr}\left(\sigma_b^2\mathbf{R}_b^H\mathbf{R}_b\right)\\
&=\mathrm{tr}\left(\mathbf{B}\left(\mathbf{I}+\mathbf{F}^H\mathbf{H}_{ba}^H\left(\mathbf{H}_{ba}\mathbf{T}\mathbf{T}^H\mathbf{H}_{ba}^H+\sigma_b^2\mathbf{I}\right)^{-1}\mathbf{H}_{ba}\mathbf{F}\right)^{-1}\mathbf{B}^H\right)\\
&=\mathrm{tr}\left(\mathbf{B}\left(\mathbf{I}+\sigma_b^{-2}\mathbf{F}^H\mathbf{H}_{ba}^H\mathbf{H}_{ba}\mathbf{F}\right)^{-1}\mathbf{B}^H\right). \qquad (13)
\end{aligned}$$

We then focus on the power minimization design, which we formulate as follows:

$$\begin{aligned}
\min_{\mathbf{B},\mathbf{F}}\ &\mathrm{tr}\left(\mathbf{B}\left(\mathbf{I}+\sigma_b^{-2}\mathbf{F}^H\mathbf{H}_{ba}^H\mathbf{H}_{ba}\mathbf{F}\right)^{-1}\mathbf{B}^H\right)\\
\text{s.t.}\quad &\mathrm{tr}\left(\mathbf{F}\mathbf{F}^H\right)\le P_f, \qquad (14)
\end{aligned}$$

where P_f is the power devoted to the transmission of the information-bearing signal.

By using the property of the positive semi-definite matrix $|\mathbf{M}|^{1/N}\le\mathrm{tr}\left(\mathbf{M}\right)/N$, we obtain the following bound on the $\mathrm{MSE}\left(\mathbf{B},\mathbf{F}\right)$:

$$\begin{aligned}
&\left|\left(\mathbf{I}+\sigma_b^{-2}\mathbf{F}^H\mathbf{H}_{ba}^H\mathbf{H}_{ba}\mathbf{F}\right)\right|^{-1/N}\\
\le&\mathrm{tr}\left(\mathbf{B}\left(\mathbf{I}+\sigma_b^{-2}\mathbf{F}^H\mathbf{H}_{ba}^H\mathbf{H}_{ba}\mathbf{F}\right)^{-1}\mathbf{B}^H\right)/N, \qquad (15)
\end{aligned}$$

We note that the expression of the MSE in (13) can achieve the lower bound when $\mathbf{B}\left(\mathbf{I}+\sigma_b^{-2}\mathbf{F}^H\mathbf{H}_{ba}^H\mathbf{H}_{ba}\mathbf{F}\right)^{-1}\mathbf{B}^H=\xi\mathbf{I}$, where ξ is a scaling parameter. In the following we propose to minimise the lower bound (15) on the MSE and then find the appropriate precoder such that the bound holds with equality. The constrained optimization problem can be written as

$$\begin{aligned}
&\min\left|\left(\mathbf{I}+\sigma_b^{-2}\mathbf{F}^H\mathbf{H}_{ba}^H\mathbf{H}_{ba}\mathbf{F}\right)\right|^{-1}\\
&\text{s.t.}\quad\mathrm{tr}\left(\mathbf{F}\mathbf{F}^H\right)\le P_f. \qquad (16)
\end{aligned}$$

Based on the eigenvalue decomposition (EVD), we have

$$\mathbf{H}_{ba}^H\mathbf{H}_{ba}=\mathbf{V}_{ba}\mathbf{\Lambda}_{ba}\mathbf{V}_{ba}^H. \qquad (17)$$

where $\mathbf{V}_{ba}$ is unitary and $\mathbf{\Lambda}_{ba}$ is a diagonal matrix with i-th diagonal entry denoted as $\lambda_{H_{ba},i}$. In turn, the precoder for Bob has the following structure

$$\mathbf{F}=\mathbf{V}_{ba}\mathbf{\Lambda}_f^{1/2}\mathbf{\Phi}, \qquad (18)$$

where $\mathbf{\Lambda}_f$ is a diagonal matrix with the i-th diagonal element $\lambda_{F,i}$. $\mathbf{\Phi}$ is an unitary matrix yet to be determined.

Note that for a positive semi-definite matrix $\mathbf{M}\in\mathbb{C}^{N\times N}$, we have [18]

$$\det\left(\mathbf{M}\right)\le\prod_{i=1}^{N}\mathbf{M}\left(i,i\right), \qquad (19)$$

the equality holds when $\mathbf{M}$ is a diagonal matrix [19]. Hence, we can rewrite the objective function as:

$$\begin{aligned}
&\min\prod_{i=1}^{N}\left(1+\sigma_b^{-2}\lambda_{F,i}\lambda_{H_{ba},i}\right)^{-1}\\
&\text{s.t.}\quad\sum_{i=1}^{N}\lambda_{F,i}\le P_f. \qquad (20)
\end{aligned}$$

Taking the natural logarithm of the objective function, the problem can be further simplified as:

$$\begin{aligned}
&\max\sum_{i=1}^{N}\ln\left(1+\sigma_b^{-2}\lambda_{F,i}\lambda_{H_{ba},i}\right)\\
&\text{s.t.}\quad\sum_{i=1}^{N}\lambda_{F,i}\le P_f. \qquad (21)
\end{aligned}$$

This latter problem (21) can be solved by means of the KKT optimality conditions. The optimal diagonal element $\lambda_{F,i}$ is obtained as

$$\lambda_{F,i}=\mu-\sigma_b^2/\lambda_{H_{ba},i}, \qquad (22)$$

where μ (water level) is chosen to satisfy the power constraint with equality, yielding

$$\mu=\frac{1}{N}\left(P_f+\sum_{i=1}^{N}\frac{\sigma_b^2}{\lambda_{H_{ba},i}}\right). \qquad (23)$$

The solution for P_f can be obtained by using a bisection method, which is summarized in Table I. We then have the following expression:

$$\left(\mathbf{I}+\sigma_b^{-2}\mathbf{F}^H\mathbf{H}_{ba}^H\mathbf{H}_{ba}\mathbf{F}\right)^{-1}=\mathbf{\Phi}^H\left(\mathbf{I}+\sigma_b^{-2}\mathbf{\Lambda}_f^{H/2}\mathbf{\Lambda}_{ba}\mathbf{\Lambda}_f^{1/2}\right)^{-1}\mathbf{\Phi} \tag{24}$$

We know that the lower bound of MSE is achieved when the MSE expression is a scaled identity matrix. To complete the design of $\mathbf{F}$, we need to select the unitary matrix $\mathbf{\Phi}$ so that the minimized lower bound is attained. Here we define $\mathbf{D}=\left(\mathbf{I}+\sigma_b^{-2}\mathbf{\Lambda}_f^{H/2}\mathbf{\Lambda}_{ba}\mathbf{\Lambda}_f^{1/2}\right)^{-1}$ and apply the GMD to $\mathbf{D}^{1/2}$, i.e., $\mathbf{D}^{1/2}=\mathbf{QRP}^H$. The unitary matrix $\mathbf{\Phi}$ is chosen as $\mathbf{\Phi}=\mathbf{P}$. The feedback matrix $\mathbf{B}$ is calculated as $\mathbf{B}=\mathbf{LR}^{-H}$, where $\mathbf{L}=\mathrm{diag}\left\{\mathbf{R}\right\}$ is used to make the diagonal elements of $\mathbf{B}$ unity. It can be verified that the equality is achieved.

TABLE I: Procedure of the Proposed Scheme

Input:	MSE target ε_b for Bob, and the desired resolution γ
0	Initialization: Set $P_{\min}=0$, $P_{\max}=P$, such that $f\left(P_{\min}\right)>\varepsilon_b$, $f\left(P_{\max}\right)<\varepsilon_b$;
1	Set $P_f=\left(P_{\min}+P_{\max}\right)/2$, compute $f\left(P_f\right)=N\prod_{i=1}^{N}\left(1+\sigma_b^{-2}\lambda_{F,i}\lambda_{H_{ba},i}\right)^{-1/N}$;
2	If $f\left(P_f\right)<\varepsilon_b$, then set $P_{\max}=P_f$. Otherwise, set $P_{\min}=P_f$;
3	If $\left(P_{\max}-P_{\min}\right)>\gamma$, then go back to step 1.
Output:	Minimum required power P_f

Subsequently, we focus on the precoder design for the AN. We need to allocate the interference power so that it does not degrade Bob's signal. By satisfying the expression in equation (11), the precoder for the AN can be designed as

$$\mathbf{T}=\sqrt{\frac{P-P_f}{N_a-N}}\mathbf{F}_{\perp}, \tag{25}$$

where $\mathbf{F}_{\perp}$ is chosen to be the remaining $\left(N_a-N\right)$ eigenvectors of $\mathbf{H}_{ba}^H\mathbf{H}_{ba}$.

Finally, the MMSE receiver $\mathbf{R}_b$ can be derived by substituting (18) and (25) into (12).

As we can see, the proposed nonlinear scheme mainly involves singular value decomposition (SVD), matrix multiplications, matrix inversions, and the GMD. Compared with the conventional linear SVD-based precoding algorithm, the proposed THP nonlinear scheme has an additional $N\times N$ triangular matrix multiplication and a GMD operation. The additional complexity of GMD is $O(N^3)$. We advocate an affordable increase in complexity in exchange for the improvement in performance, as discussed below.

IV. Simulation Results

In this section, we investigate the performance of the proposed scheme. We consider a MIMO secrecy channel in the presence of a passive eavesdropper with $N_a=N_b=N_e=6$, $N=4$. All the results are averaged over 10^4 independent channel realizations. The elements of the channel matrices are i.i.d. zero-mean unit-variance complex Gaussian random variables. For all simulations, we set the background noise power $\sigma_b^2=\sigma_e^2=1$. Also, we use 4-QAM modulation as the modulation scheme.

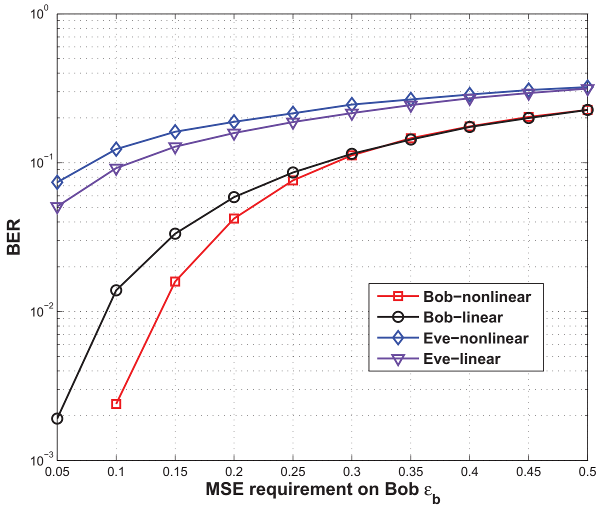

Fig. 2: BER versus the MSE target with $P=20dB$

Fig. 2 illustrates the bit error rate (BER) performance comparison for the intended receiver (Bob) and the eavesdropper (Eve) versus the desired MSE target ε_b for Bob. The maximum transmit power is assumed to be $P=100$ or 20 dB. The MSE requirement ε_b is varied from 0.05 to 0.5. As shown in Fig. 2, the BER performance of Bob is always superior to Eve's. As expected, a degree of performance improvement is achieved compared to the linear scheme. Compared to the conventional linear SVD-based scheme, the proposed nonlinear algorithm improves Bob's BER and degrades Eve's one.

Fig. 3 displays the corresponding MSE performance comparison, which is consistent with the BER performance. The intended user Bob always achieves the target MSE and the MSE in the Eve's channel is higher than that in the desired channel. The MSE of the proposed nonlinear scheme for the eavesdropper is significantly degraded compared with the linear scheme.

V. Conclusion

In this paper, we proposed a GMD-THP transceiver design for secure communications in broadcast MIMO systems in the presence of a passive eavesdropper. The scheme allocates the transmit power in order to achieve a target MSE for the desired user, and uses the remaining available power to transmit the AN to degrade the eavesdropper's channel. The transmit power minimization problem can be solved by using the bisection method while satisfying the MSE requirement for the desired user. With the aid of the GMD-THP, the lower MSE bound can be achieved. We convert the nonlinear problem to a standard convex optimization problem. The solution for the precoder is obtained by using the waterfilling method via the KKT conditions. Simulation results have verified the effectiveness of the proposed nonlinear scheme.

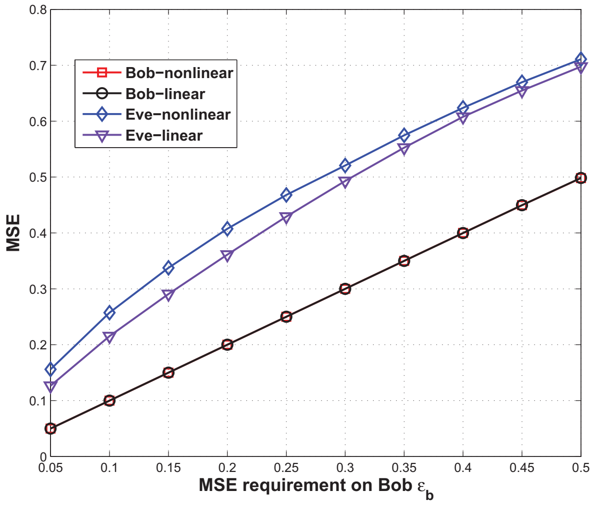

Fig. 3: Achieved MSE versus the MSE target with $P = 20dB$

References

[1] B. Schneier, "Cryptographic design vulnerabilities," *IEEE Comput.*, vol. 31, no. 9, pp. 29–33, Sep. 2008.

[2] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[3] S. L. Y. Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[4] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. M. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[5] A. Khisti and G. Wornell, "Secure transmission with multiple antennas–II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[7] S. A. A. Fakoorian and A. L. Swindlehurst, "Optimal power allocation for GSVD-based beamforming in the MIMO Gaussian wiretap channel," in *Proc. IEEE ISIT, Boston, MA, USA*, Jul. 2012, pp. 2321–2325.

[8] Y. Wu, C. Xiao, and Z. Ding, "Linear precoding for finite-alphabet signaling over MIMOME wiretap channel," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2599–2612, Jul. 2012.

[9] C.-H. Lin, S.-H. Tsai, and Y.-P. Lin, "Secure transmission using MIMO precoding," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 801–813, May 2014.

[10] M. Pei, J. Wei, K.-K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544–549, Feb. 2012.

[11] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE ICASSP, Taipei, Taiwan*, Apr. 2009, pp. 2437–2440.

[12] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noiseaided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[13] J. X. Hugo Reboredo and M. R. D. Rodrigues, "Filter design with secrecy constraints: the MIMO gaussian wiretap channel," *IEEE Trans. Signal Process.*, vol. 61, no. 15, pp. 3799–3814, Aug. 2013.

[14] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[15] M. Costa, "Writing on dirty paper (corresp.)," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 439–441, May 1983.

[16] M. B. Shenouda and T. N. Davidson, "A framework for designing MIMO systems with decision feedback equalization or Tomlinson-Harashima precoding," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 4, pp. 401–411, Feb. 2008.

[17] Y. Jiang, J. Li, and W. Hager, "Joint transceiver design for MIMO communications using geometric mean decomposition," *IEEE Trans. Signal Process*, vol. 53, no. 10, pp. 3791–3803, Oct. 2005.

[18] D. Bernstein, *Matrix Mathematics: Theory, Facts, and Formulas*. Princeton University Press, 2011.

[19] D. Palomar, J. Cioffi, and M. Lagunas, "Joint Tx-Rx beamforming design for multicarrier MIMO channels: A unified framework for convex optimization," *IEEE Trans. Signal Process.*, vol. 51, no. 9, pp. 2381–2401, Sep. 2003.