IET Communications

Research Article

IET Journals
The Institution of Engineering and Technology

Non-linear transceiver design for secure communications with artificial noise-assisted MIMO relay

ISSN 1751-8628
Received on 27th May 2016
Revised 1st December 2016
Accepted on 3rd January 2017
E-First on 27th March 2017
doi: 10.1049/iet-com.2016.0617
www.ietdl.org

Lei Zhang[1], *Yunlong Cai*[1] ✉, *Benoit Champagne*[2], *Minjian Zhao*[1]

[1]*College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, People's Republic of China*
[2]*Department of Electrical and Computer Engineering, McGill University, Montreal, Canada*
✉ *E-mail: ylcai@zju.edu.cn.*

Abstract: This study investigates the problem of physical layer security for amplify-and-forward (AF) multiple-input multiple-output (MIMO) relay systems operating in the presence of a passive eavesdropper. Specifically, the authors consider the robust design of an artificial noise (AN)-assisted non-linear transceiver employing Tomlinson–Harashima precoding (THP), with imperfect knowledge of the legitimate channel states. The design problem can be reformulated as a two-level optimisation, where the outer problem aims to optimise the source precoder as a function of the relay precoder, while the inner problem at the relay aims to jointly optimise the relay precoder as well as the power allocation between the AN and the information-bearing signals. To solve the inner problem, the authors adopt a bisection method which attempts to maximise the AN power level, to confuse the eavesdropper, while satisfying the mean-squared-error requirement for the intended user. Some relaxation for the objective function is applied to transform the problem into a standard convex optimisation one. Regarding the outer problem, closed-form solutions for the precoders can be derived by an iterative method based on the Karush–Kuhn–Tucker conditions. Simulation results illustrate the superior secrecy performance provided by the proposed non-linear transceiver design with AN and THP.

1 Introduction

With the rapid development of wireless communications, service providers nowadays can no longer just focus on the transmission rate and reliability. Indeed, privacy and security have also become critical issues due to the broadcast nature of the communication medium and the confidential nature of the information being exchanged. Recently, relay transmission has attracted considerable attention, because it can not only enhance coverage and throughout but also greatly improve the wireless security against malicious eavesdroppers. To guarantee secure relay communications, the physical layer security problem based on quality of service (QoS) criteria has been studied [1–8]. In [1], Wang *et al.* proposed a QoS-based linear relay precoding scheme to improve security with perfect channel state information (CSI), where the QoS refers to the signal-to-interference-plus-noise ratio. A generalised singular value decomposition (SVD)-based joint source and relay linear precoding and power allocation scheme has been investigated in [2]. Taking channel uncertainty into account, some robust linear processing techniques were proposed in [3–8]. In [3], a joint source and relay precoding design algorithm was proposed to minimise the overall power consumption while satisfying the intended user's preset QoS requirements and maintaining the eavesdropper's signal-to-noise ratio below a given threshold.

When the eavesdropper is passive, the legitimate transmitter and relay can hardly acquire the CSI of the former. To overcome this difficulty, the use of artificial noise (AN) has emerged as a means to confuse the eavesdropper without knowing its CSI [9]. Joint design of the relay precoders and the AN covariance matrices for secrecy rate maximisation in multi-antenna multi-relay sub-networks were investigated in [4–7]. In these works, robustness against imperfect CSI of the eavesdroppers was approached via a worst-case robust formulation. In [8], the authors considered the uncertainty of all the available CSI and adopted the minimum-mean-squared-error (MMSE) as the QoS metric for the precoder design. As an alternative to the linear transceiver designs, non-linear transceivers based on Tomlinson–Harashima precoding (THP) have recently generated great interest. The non-linear transceiver design algorithms in multiple-input multiple-output (MIMO) relay systems employing THP at the source node were proposed in [10–13]. While the linear precoding algorithms have been applied to improve physical layer security, the study of the non-linear precoder designs for secure communications remain largely unexplored.

In this paper, we consider the secrecy of amplify-and-forward (AF) MIMO relay systems operating in the presence of a passive eavesdropper. We propose a robust AN-assisted non-linear transceiver design scheme that takes into account imperfect CSI of legitimate links, where the Kronecker model is used for the CSI mismatch. We concentrate on optimising the non-linear transceiver to guarantee the QoS satisfaction for the intended user in terms of mean-squared error (MSE), while creating maximum confusion through AN at the eavesdropper under a total transmission power constraint. The transceiver design can be reformulated as a two-level optimisation, where the outer problem aims to optimise the source precoder, while the inner problem aims to jointly optimise the relay precoder as well as the power allocation between the AN and the information-bearing signals. For the inner problem, a bisection method is adopted to maximise the AN power level while achieving the MSE requirement for the information-bearing signal. We also employ some relaxation for the objective function to transform the problem into a standard convex optimisation one. Regarding the outer problem, the closed-form solutions for precoders can be derived by an iterative method through the Karush–Kuhn–Tucker (KKT) conditions. Simulation results are provided to demonstrate the effectiveness of our proposed non-linear transceiver design in providing improved physical layer security.

The rest of this paper is organised as follows. The proposed system model is described in Section 2. In Section 3, we formulate the joint optimisation problem and present the proposed solution for the robust non-linear transceiver design of an AN-assisted AF MIMO relay system. Simulation results and comparisons with alternative approaches are presented in Section 4. Finally, we give the conclusions in Section 5.

Notation: Boldface lowercase letters represent vectors, while boldface uppercase letters represent matrices. $E[\cdot]$ denotes the statistical expectation. The operators $(\cdot)^{\mathrm{T}}$, $(\cdot)^{*}$, $(\cdot)^{\mathrm{H}}$, $\mathrm{tr}(\cdot)$ and $|\cdot|$

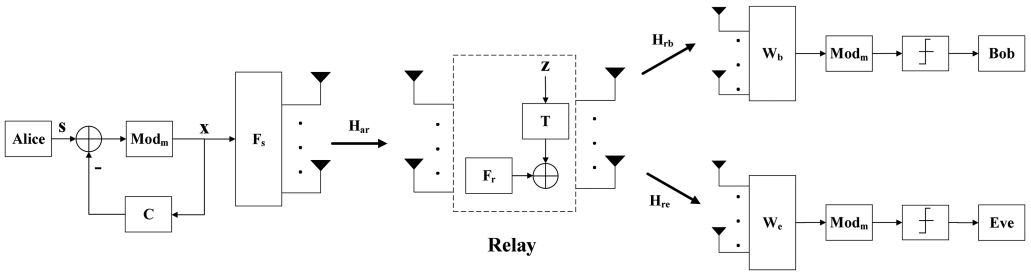

Fig. 1 *MIMO relay wiretap channel with THP-based transceiver*

denote the matrix transpose, conjugate, Hermitian transpose, trace and determinant, respectively. The operation of the Kronecker product is denoted by $\otimes$. $\lfloor \cdot \rfloor$ represents the floor function, which returns the largest integer not exceeding the argument. $Q(\cdot)$ is the quantisation operation. $\mathcal{CN}(\boldsymbol{m}, \boldsymbol{C})$ denotes a multi-variate complex circular Gaussian distribution with mean $\boldsymbol{m}$ and covariance matrix $\boldsymbol{C}$.

2 System model

We consider a three-node MIMO relay system as shown in Fig. 1, where a source (Alice) sends confidential information to a legitimate destination (Bob) through an AF relay in the presence of a passive eavesdropper (Eve). We consider a system where the source, relay and destination nodes are equipped with N_s, N_r and N_d antennas, respectively. It is assumed that there is no direct link from Alice to either Bob or Eve, due to the limited transmission power and the large-scale fading over the long distance between them. To ensure that N_s independent data streams can be transmitted across the network, we assume that $N_s \le N_r$ and $N_s \le N_d$. Moreover, the condition $N_r > N_d$ needs to be met for the AN design at the relay [14]. All the channels between the different nodes of the systems are assumed to be flat fading and quasi-static.

At the source, an M-ary square quadrature amplitude modulation (QAM) modulated signal $\boldsymbol{s} = [s_1, \ldots, s_{N_s}]^{\mathrm{T}}$ is transmitted, with zero mean and covariance $E[\boldsymbol{s}\boldsymbol{s}^{\mathrm{H}}] = \sigma_s^2 \boldsymbol{I}$. It is assumed that the real and imaginary parts of s_k belong to the set $\{\pm 1, \pm 3, \ldots, \pm(\sqrt{M}-1)\}$. To calculate the THP precoded signal, a modulo operator is first defined as

$$\mathrm{MOD}_M(x) = x - 2\sqrt{M}\left\lfloor \frac{x+\sqrt{M}}{2\sqrt{M}} \right\rfloor = x + e, \tag{1}$$

where e is the residual error, such that $\mathrm{MOD}_M(x)$ is constrained to the range $[-\sqrt{M}, \sqrt{M})$. Then the information-bearing signal $\boldsymbol{x}$ for Bob can be recursively calculated by

$$\begin{aligned} x_k &= \mathrm{MOD}_M\left(s_k - \sum_{l=1}^{k-1} \boldsymbol{U}_{k,l} x_l\right) \\ &= s_k - \sum_{l=1}^{k-1} \boldsymbol{U}_{k,l} x_l + e_k, \quad k = 1, 2, \ldots, N_s, \end{aligned} \tag{2}$$

where $\boldsymbol{U}$ is a strictly lower triangular matrix with entries $\boldsymbol{U}_{k,l}$, and e_k is the residual error after applying the modulo operator. Equation (2) can be rewritten in matrix form as $\boldsymbol{x} = \boldsymbol{B}^{-1}\boldsymbol{v}$, where $\boldsymbol{B} = \boldsymbol{U} + \boldsymbol{I}$ is a unit diagonal lower triangular matrix and $\boldsymbol{v} = \boldsymbol{s} + \boldsymbol{e}$ is the effective signal vector. Note that for moderate-to-high M, $\boldsymbol{x}$ can be assumed to have a covariance of the form $E[\boldsymbol{x}\boldsymbol{x}^{\mathrm{H}}] = \sigma_s^2 \boldsymbol{I}$ [11]. Following THP, the resulting vector $\boldsymbol{x}$ is passed through a linear precoding matrix $\boldsymbol{F}_s \in \mathbb{C}^{N_s \times N_s}$ prior to its transmission. The maximum transmit power available for Alice is assumed to be constrained by P_s.

The signal transmission is carried out in two time slots. In the first time slot, Alice transmits the private message to the relay. During the second time slot, the relay adopts the linear AF and AN strategies together to forward the source message to Bob while aiming to keep the eavesdropper from overhearing the message. Consequently, the signals received at Bob and Eve are, respectively, given by

$$\boldsymbol{y}_b = \boldsymbol{H}_{rb}\boldsymbol{F}_r(\boldsymbol{H}_{ar}\boldsymbol{F}_s\boldsymbol{x} + \boldsymbol{n}_r) + \boldsymbol{H}_{rb}\boldsymbol{T}\boldsymbol{z} + \boldsymbol{n}_b, \tag{3}$$

$$\boldsymbol{y}_e = \boldsymbol{H}_{re}\boldsymbol{F}_r(\boldsymbol{H}_{ar}\boldsymbol{F}_s\boldsymbol{x} + \boldsymbol{n}_r) + \boldsymbol{H}_{re}\boldsymbol{T}\boldsymbol{z} + \boldsymbol{n}_e, \tag{4}$$

where $\boldsymbol{H}_{ar} \in \mathbb{C}^{N_r \times N_s}$, $\boldsymbol{H}_{rb} \in \mathbb{C}^{N_d \times N_r}$ and $\boldsymbol{H}_{re} \in \mathbb{C}^{N_d \times N_r}$ denote the Alice-to-relay, relay-to-Bob and relay-to-Eve channel matrices, respectively. Matrix $\boldsymbol{F}_r \in \mathbb{C}^{N_r \times N_r}$ is used to implement the AF transformation at the relay. Matrix $\boldsymbol{T} \in \mathbb{C}^{N_r \times (N_r - N_d)}$ is used to properly shape the AN in terms of its power level and spatial correlation, while vector $\boldsymbol{z} \in \mathbb{C}^{(N_r - N_d)}$ serves as the excitation. The latter is independent of the confidential signal $\boldsymbol{s}$, and its entries are independent and identically distributed (i.i.d.) Gaussian random variables with zero-mean and unit variance. The terms $\boldsymbol{n}_r$, $\boldsymbol{n}_b$ and $\boldsymbol{n}_e$ represent zero-mean complex circular Gaussian noise vectors with covariance matrices $\sigma_{n_r}^2 \boldsymbol{I}$, $\sigma_{n_b}^2 \boldsymbol{I}$ and $\sigma_{n_e}^2 \boldsymbol{I}$, respectively. Note that the maximum transmit power at the relay is given by $P_r = P_f + \mathrm{E}[\mathrm{tr}(\boldsymbol{T}\boldsymbol{T}^{\mathrm{H}})]$, where P_f represents the transmit power for the signal received at the relay (i.e. information-bearing component $\boldsymbol{H}_{ar}\boldsymbol{F}_s\boldsymbol{x}$ plus antenna noise $\boldsymbol{n}_r$), which can be expressed as $P_f = E[\mathrm{tr}(\boldsymbol{F}_r(\sigma_s^2 \boldsymbol{H}_{ar}\boldsymbol{F}_s\boldsymbol{F}_s^{\mathrm{H}}\boldsymbol{H}_{ar}^{\mathrm{H}} + \sigma_{n_r}^2 \boldsymbol{I})\boldsymbol{F}_r^{\mathrm{H}})]$. The optimum Wiener filter is employed at Bob to detect the received signal, that is,

$$\hat{s}_b = Q(\mathrm{MOD}_M(\boldsymbol{W}_b \boldsymbol{y}_b)), \tag{5}$$

where $\boldsymbol{W}_b \in \mathbb{C}^{N_s \times N_d}$ is the corresponding spatial filter and $Q(\,)$ is the QAM threshold detector. Similarly, it is assumed in this work that Eves employs a linear receiver with spatial filter $\boldsymbol{W}_e \in \mathbb{C}^{N_s \times N_d}$.

Since channel estimation errors are inevitable in practical systems, we use the Kronecker model [15] to describe the CSI mismatch for the legitimate links

$$\boldsymbol{H}_{ar} = \bar{\boldsymbol{H}}_{ar} + \Delta\boldsymbol{H}_{ar}, \tag{6}$$

$$\boldsymbol{H}_{rb} = \bar{\boldsymbol{H}}_{rb} + \Delta\boldsymbol{H}_{rb}, \tag{7}$$

where $\bar{\boldsymbol{H}}_{ar}$ and $\bar{\boldsymbol{H}}_{rb}$ represent the estimated CSI of the Alice-to-relay and relay-to-Bob channels, while $\Delta\boldsymbol{H}_{ar}$ and $\Delta\boldsymbol{H}_{rb}$ are the corresponding channel estimation error matrices. $\Delta\boldsymbol{H}_{ar}$ can be written as $\Delta\boldsymbol{H}_{ar} = \boldsymbol{\Sigma}_{ar}^{1/2}\boldsymbol{H}_0\boldsymbol{\Psi}_{ar}^{\mathrm{T}/2}$, where the entries of $\boldsymbol{H}_0$ are i.i.d. with zero-mean and unit-variance circular complex Gaussian distribution [16], that is $\Delta\boldsymbol{H}_{ar} \sim \mathcal{CN}(0_{N_r \times N_s}, \boldsymbol{\Psi}_{ar} \otimes \boldsymbol{\Sigma}_{ar})$. $\boldsymbol{\Psi}_{ar}$ and $\boldsymbol{\Sigma}_{ar}$ denote the covariance matrices of the Alice-to-relay channel as seen from the transmitter and receiver, respectively. Similar definitions can be applied to $\Delta\boldsymbol{H}_{rb}$, with $\boldsymbol{\Psi}_{rb}$ and $\boldsymbol{\Sigma}_{rb}$ now characterising the relay-to-Bob channel.

3 Problem formulation and proposed algorithm

In this section, we first formulate the optimisation problem for the non-linear transceiver design and then introduce the proposed two-level solution algorithm. Before proceeding however, we state the following lemma which will be used in our developments:

Lemma 1: For a random matrix $\boldsymbol{A} \in \mathbb{C}^{M\times N}$ with a multi-variate Gaussian distribution $\boldsymbol{A} \sim \mathscr{CN}(\bar{\boldsymbol{A}}, \boldsymbol{C} \otimes \boldsymbol{D})$, we have for any deterministic matrix $\boldsymbol{F} \in \mathbb{C}^{N\times N}$ that $\mathrm{E}[\boldsymbol{AFA}^{\mathrm{H}}] = \bar{\boldsymbol{A}}\boldsymbol{F}\bar{\boldsymbol{A}}^{\mathrm{H}} + \mathrm{tr}(\boldsymbol{FC}^{\mathrm{T}})\boldsymbol{D}$.

Proof: Please refer to [16]. □

3.1 Problem formulation

The system MSE at Bob is calculated as

$$\begin{aligned}
&\mathrm{MSE}(\boldsymbol{B}, \boldsymbol{F}_{\mathrm{s}}, \boldsymbol{F}_{\mathrm{r}}, \boldsymbol{T}, \boldsymbol{W}_{\mathrm{b}}) \\
&= E\left[\| \boldsymbol{W}_{\mathrm{b}}\boldsymbol{y}_{\mathrm{b}} - \boldsymbol{v} \|^2\right] \\
&= E\left[\mathrm{tr}\left(\sigma_{\mathrm{s}}^2(\boldsymbol{W}_{\mathrm{b}}\boldsymbol{H}_{\mathrm{rb}}\boldsymbol{F}_{\mathrm{r}}\boldsymbol{H}_{\mathrm{ar}}\boldsymbol{F}_{\mathrm{s}} - \boldsymbol{B})(\boldsymbol{W}_{\mathrm{b}}\boldsymbol{H}_{\mathrm{rb}}\boldsymbol{F}_{\mathrm{r}}\boldsymbol{H}_{\mathrm{ar}}\boldsymbol{F}_{\mathrm{s}} - \boldsymbol{B})^{\mathrm{H}}\right)\right] \\
&\quad + E\left[\mathrm{tr}\left(\sigma_{n_{\mathrm{b}}}^2 \boldsymbol{W}_{\mathrm{b}}\boldsymbol{W}_{\mathrm{b}}^{\mathrm{H}}\right)\right] \\
&\quad + E\left[\mathrm{tr}\left(\sigma_{n_{\mathrm{r}}}^2(\boldsymbol{W}_{\mathrm{b}}\boldsymbol{H}_{\mathrm{rb}}\boldsymbol{F}_{\mathrm{r}})(\boldsymbol{W}_{\mathrm{b}}\boldsymbol{H}_{\mathrm{rb}}\boldsymbol{F}_{\mathrm{r}})^{\mathrm{H}}\right)\right] \\
&\quad + E\left[\mathrm{tr}\left((\boldsymbol{W}_{\mathrm{b}}\boldsymbol{H}_{\mathrm{rb}}\boldsymbol{T})(\boldsymbol{W}_{\mathrm{b}}\boldsymbol{H}_{\mathrm{rb}}\boldsymbol{T})^{\mathrm{H}}\right)\right],
\end{aligned} \tag{8}$$

where the expectation is taken over the joint distribution of $\Delta\boldsymbol{H}_{\mathrm{ar}}, \Delta\boldsymbol{H}_{\mathrm{rb}}, \boldsymbol{n}_{\mathrm{r}}, \boldsymbol{n}_{\mathrm{b}}$. With the use of *Lemma 1*, the MSE expression can be rewritten as

$$\begin{aligned}
&\mathrm{MSE}(\boldsymbol{B}, \boldsymbol{F}_{\mathrm{s}}, \boldsymbol{F}_{\mathrm{r}}, \boldsymbol{T}, \boldsymbol{W}_{\mathrm{b}}) \\
&= \mathrm{tr}\left(\boldsymbol{W}_{\mathrm{b}}\boldsymbol{A}\boldsymbol{W}_{\mathrm{b}}^{\mathrm{H}}\right) - \sigma_{\mathrm{s}}^2\mathrm{tr}\left(\boldsymbol{B}\boldsymbol{F}_{\mathrm{s}}^{\mathrm{H}}\bar{\boldsymbol{H}}_{\mathrm{ar}}^{\mathrm{H}}\boldsymbol{F}_{\mathrm{r}}^{\mathrm{H}}\bar{\boldsymbol{H}}_{\mathrm{rb}}^{\mathrm{H}}\boldsymbol{W}_{\mathrm{b}}^{\mathrm{H}}\right) \\
&\quad + \sigma_{\mathrm{s}}^2\mathrm{tr}\left(\boldsymbol{B}\boldsymbol{B}^{\mathrm{H}}\right) - \sigma_{\mathrm{s}}^2\mathrm{tr}\left(\boldsymbol{W}_{\mathrm{b}}\bar{\boldsymbol{H}}_{\mathrm{rb}}\boldsymbol{F}_{\mathrm{r}}\bar{\boldsymbol{H}}_{\mathrm{ar}}\boldsymbol{F}_{\mathrm{s}}\boldsymbol{B}^{\mathrm{H}}\right),
\end{aligned} \tag{9}$$

where we introduce

$$\begin{aligned}
\boldsymbol{A} \triangleq\ & \bar{\boldsymbol{H}}_{\mathrm{rb}}\boldsymbol{F}_{\mathrm{r}}\left(\sigma_{\mathrm{s}}^2\bar{\boldsymbol{H}}_{\mathrm{ar}}\boldsymbol{F}_{\mathrm{s}}\boldsymbol{F}_{\mathrm{s}}^{\mathrm{H}}\bar{\boldsymbol{H}}_{\mathrm{ar}}^{\mathrm{H}} + \sigma_{\mathrm{s}}^2\alpha_1\boldsymbol{\Sigma}_{\mathrm{ar}} + \sigma_{n_{\mathrm{r}}}^2\boldsymbol{I}\right)\boldsymbol{F}_{\mathrm{r}}^{\mathrm{H}}\bar{\boldsymbol{H}}_{\mathrm{rb}}^{\mathrm{H}} \\
&+ \alpha_2\boldsymbol{\Sigma}_{\mathrm{rb}} + \alpha_3\boldsymbol{\Sigma}_{\mathrm{rb}} + \sigma_{n_{\mathrm{b}}}^2\boldsymbol{I},
\end{aligned} \tag{10}$$

$\alpha_1 \triangleq \mathrm{tr}\left(\boldsymbol{F}_{\mathrm{s}}\boldsymbol{F}_{\mathrm{s}}^{\mathrm{H}}\boldsymbol{\Psi}_{\mathrm{ar}}^{\mathrm{T}}\right)$,
$\alpha_2 \triangleq \mathrm{tr}(\boldsymbol{F}_{\mathrm{r}}(\sigma_{\mathrm{s}}^2\bar{\boldsymbol{H}}_{\mathrm{ar}}\boldsymbol{F}_{\mathrm{s}}\boldsymbol{F}_{\mathrm{s}}^{\mathrm{H}}\bar{\boldsymbol{H}}_{\mathrm{ar}}^{\mathrm{H}} + \sigma_{\mathrm{s}}^2\alpha_1\boldsymbol{\Sigma}_{\mathrm{ar}} + \sigma_{n_{\mathrm{r}}}^2\boldsymbol{I})\boldsymbol{F}_{\mathrm{r}}^{\mathrm{H}}\boldsymbol{\Psi}_{\mathrm{rb}}^{\mathrm{T}})$ and
$\alpha_3 \triangleq \mathrm{tr}\left(\boldsymbol{T}\boldsymbol{T}^{\mathrm{H}}\boldsymbol{\Psi}_{\mathrm{rb}}^{\mathrm{T}}\right)$. Here, to ensure that the AN does not interfere with the intended signal for Bob [9], we require $\bar{\boldsymbol{H}}_{\mathrm{rb}}\boldsymbol{T} = 0$. Hence, the AN spatial shaping matrix is designed as

$$\boldsymbol{T} = \sqrt{\frac{P_{\mathrm{r}} - P_f}{N_{\mathrm{r}} - N_{\mathrm{d}}}}\boldsymbol{F}_{\perp}, \tag{11}$$

where $\boldsymbol{F}_{\perp}$ is chosen to be an orthonormal basis of the null space of $\bar{\boldsymbol{H}}_{\mathrm{rb}}$.

The optimal MMSE receiver $\boldsymbol{W}_{\mathrm{b}}$ at Bob can be derived by solving $(\partial/\partial\boldsymbol{W}_{\mathrm{b}}^{*})\mathrm{MSE}(\boldsymbol{B}, \boldsymbol{F}_{\mathrm{s}}, \boldsymbol{F}_{\mathrm{r}}, \boldsymbol{T}, \boldsymbol{W}_{\mathrm{b}}) = 0$, and it is given by

$$\boldsymbol{W}_{\mathrm{b}} = \sigma_{\mathrm{s}}^2\boldsymbol{B}\boldsymbol{F}_{\mathrm{s}}^{\mathrm{H}}\bar{\boldsymbol{H}}_{\mathrm{ar}}^{\mathrm{H}}\boldsymbol{F}_{\mathrm{r}}^{\mathrm{H}}\bar{\boldsymbol{H}}_{\mathrm{rb}}^{\mathrm{H}}\boldsymbol{A}^{-1}. \tag{12}$$

By substituting (12) into (9) and making use of the matrix inversion lemma [17], the MSE expression can be represented as

$$\mathrm{MSE}(\boldsymbol{B}, \boldsymbol{F}_{\mathrm{s}}, \boldsymbol{F}_{\mathrm{r}}) = \mathrm{tr}\left(\boldsymbol{B}\boldsymbol{E}\boldsymbol{B}^{\mathrm{H}}\right), \tag{13}$$

where

$$\boldsymbol{E} \triangleq \left(\sigma_{\mathrm{s}}^{-2}\boldsymbol{I} + \boldsymbol{F}_{\mathrm{s}}^{\mathrm{H}}\bar{\boldsymbol{H}}_{\mathrm{ar}}^{\mathrm{H}}\boldsymbol{F}_{\mathrm{r}}^{\mathrm{H}}\bar{\boldsymbol{H}}_{\mathrm{rb}}^{\mathrm{H}}\boldsymbol{R}_n^{-1}\bar{\boldsymbol{H}}_{\mathrm{rb}}\boldsymbol{F}_{\mathrm{r}}\bar{\boldsymbol{H}}_{\mathrm{ar}}\boldsymbol{F}_{\mathrm{s}}\right)^{-1}, \tag{14}$$

$$\boldsymbol{R}_n \triangleq \bar{\boldsymbol{H}}_{\mathrm{rb}}\boldsymbol{F}_{\mathrm{r}}\left(\sigma_{\mathrm{s}}^2\alpha_1\boldsymbol{\Sigma}_{\mathrm{ar}} + \sigma_{n_{\mathrm{r}}}^2\boldsymbol{I}\right)\boldsymbol{F}_{\mathrm{r}}^{\mathrm{H}}\bar{\boldsymbol{H}}_{\mathrm{rb}}^{\mathrm{H}} + \alpha_2\boldsymbol{\Sigma}_{\mathrm{rb}} + \alpha_3\boldsymbol{\Sigma}_{\mathrm{rb}} + \sigma_{n_{\mathrm{b}}}^2\boldsymbol{I}. \tag{15}$$

Since the eavesdropper is passive, the legitimate transmitter and relay can hardly acquire the CSI of relay-to-eavesdropper channel. Here, we choose the MSE at Bob as the objective function and try to save more power for AN. By taking the power constraints at the source and relay into consideration, the optimisation problem of interest can be formulated as

$$\begin{aligned}
\min_{\boldsymbol{B}, \boldsymbol{F}_{\mathrm{s}}, \boldsymbol{F}_{\mathrm{r}}, P_f}\ & \mathrm{tr}\left(\boldsymbol{B}\boldsymbol{E}\boldsymbol{B}^{\mathrm{H}}\right) \\
\mathrm{s.t.}\ & \mathrm{tr}\left(\sigma_{\mathrm{s}}^2\boldsymbol{F}_{\mathrm{s}}\boldsymbol{F}_{\mathrm{s}}^{\mathrm{H}}\right) \le P_{\mathrm{s}} \\
& \mathrm{tr}(\boldsymbol{F}_{\mathrm{r}}(\sigma_{\mathrm{s}}^2\bar{\boldsymbol{H}}_{\mathrm{ar}}\boldsymbol{F}_{\mathrm{s}}\boldsymbol{F}_{\mathrm{s}}^{\mathrm{H}}\bar{\boldsymbol{H}}_{\mathrm{ar}}^{\mathrm{H}} + \sigma_{\mathrm{s}}^2\alpha_1\boldsymbol{\Sigma}_{\mathrm{ar}} + \sigma_{n_{\mathrm{r}}}^2\boldsymbol{I})\boldsymbol{F}_{\mathrm{r}}^{\mathrm{H}}) \le P_f \le P_{\mathrm{r}},
\end{aligned} \tag{16}$$

note that the value of P_f also needs to be optimised for the power allocation problem at the relay.

3.2 Proposed robust transceiver design

In general, it is difficult to achieve the globally optimal solution of optimisation problem (16) due to its non-convexity. To simplify this problem, we adopt the prime decomposition method to convert it into a two-level optimisation, where the outer problem aims to optimise the source precoder $\boldsymbol{F}_{\mathrm{s}}$ and the feedback matrix $\boldsymbol{B}$ while the inner problem at the relay aims to jointly optimise the AF matrix $\boldsymbol{F}_{\mathrm{r}}$ and the power P_f allocated for the information-bearing signal.

We first focus on the outer problem, where $\boldsymbol{F}_{\mathrm{r}}$ and P_f are assumed to be known here. Then, according to (16), the optimum $\boldsymbol{F}_{\mathrm{s}}$ and $\boldsymbol{B}$ can be derived as a function of $\boldsymbol{F}_{\mathrm{r}}$. Let us define $\bar{\boldsymbol{H}} = \bar{\boldsymbol{H}}_{\mathrm{rb}}\boldsymbol{F}_{\mathrm{r}}\bar{\boldsymbol{H}}_{\mathrm{ar}}$ and introduce $\tilde{\boldsymbol{H}} = \boldsymbol{R}_n^{-1/2}\bar{\boldsymbol{H}}$. Invoking the eigenvalue decomposition, we have

$$\tilde{\boldsymbol{H}}^{\mathrm{H}}\tilde{\boldsymbol{H}} = \boldsymbol{V}_h\boldsymbol{\Lambda}_h\boldsymbol{V}_h^{\mathrm{H}}, \tag{17}$$

where $\boldsymbol{V}_h$ is a unitary matrix and $\boldsymbol{\Lambda}_h$ is a diagonal matrix with ith diagonal entry denoted as $\lambda_{h,i}$. As proved in Appendix A in [10], the optimum precoder at Alice has the following structure (We use the maximum power property provided in [10] to obtain the optimum structure of $\boldsymbol{F}_{\mathrm{s}}$. The main focus of the proposed algorithm is on the solution to the relay AF matrix and the power allocation problem between the information-bearing signal and the AN.)

$$\boldsymbol{F}_{\mathrm{s}} = \sqrt{\frac{P_{\mathrm{s}}}{N_{\mathrm{s}}\sigma_{\mathrm{s}}^2}}\boldsymbol{V}_h\boldsymbol{U}_{\mathrm{s}}, \tag{18}$$

where $\boldsymbol{U}_{\mathrm{s}}$ is a unitary matrix yet to be defined.

Substituting (18) into (14), a lower triangular matrix $\boldsymbol{L}$ is obtained via the Cholesky factorization of $\boldsymbol{E}$, as expressed by

$$\begin{aligned}
\boldsymbol{E} = \boldsymbol{L}\boldsymbol{L}^{\mathrm{H}} &= \left(\sigma_{\mathrm{s}}^{-2}\boldsymbol{I} + \frac{P_{\mathrm{s}}}{N_{\mathrm{s}}\sigma_{\mathrm{s}}^2}(\boldsymbol{V}_h\boldsymbol{U}_{\mathrm{s}})^{\mathrm{H}}\tilde{\boldsymbol{H}}^{\mathrm{H}}\tilde{\boldsymbol{H}}\boldsymbol{V}_h\boldsymbol{U}_{\mathrm{s}}\right)^{-1} \\
&= \boldsymbol{U}_{\mathrm{s}}^{\mathrm{H}}\left(\sigma_{\mathrm{s}}^{-2}\boldsymbol{I} + \frac{P_{\mathrm{s}}}{N_{\mathrm{s}}\sigma_{\mathrm{s}}^2}\boldsymbol{\Lambda}_h\right)^{-1}\boldsymbol{U}_{\mathrm{s}}.
\end{aligned} \tag{19}$$

Note that for a positive semi-definite matrix $\boldsymbol{M} \in \mathbb{C}^{N\times N}$, we have $|\boldsymbol{M}|^{1/N} \le \mathrm{tr}(\boldsymbol{M})/N$, which is the arithmetic–geometric mean inequality; the equality can be achieved only when $\boldsymbol{M}$ is a diagonal matrix with equal diagonal elements [11]. Thus, the minimum value in (13) can be achieved when $\boldsymbol{B}\boldsymbol{E}\boldsymbol{B}^{\mathrm{H}}$ is a diagonal matrix with equal diagonal elements.

Thus, the optimum value of matrix $\boldsymbol{B}$ takes the form

$$\boldsymbol{B} = \boldsymbol{D}\boldsymbol{L}^{-1}, \tag{20}$$

where $\boldsymbol{D} = \mathrm{diag}\{\boldsymbol{L}\}$ is used to make the diagonal elements of $\boldsymbol{B}$ unity. Substituting (18) and (20) into (13), we see that the value of the MSE can be written as

$$\mathrm{tr}\left(\boldsymbol{B}\boldsymbol{E}\boldsymbol{B}^{\mathrm{H}}\right) = \sum_{k=1}^{N_\mathrm{s}} \boldsymbol{L}(k,k)^2. \tag{21}$$

It is simple to see that the expression of the MSE in (13) can achieve the lower bound when the diagonal elements of $\boldsymbol{L}$ are equal. Therefore, to find $\boldsymbol{L}$, we apply the geometric mean decomposition [18], namely $\left(\sigma_\mathrm{s}^{-2}\boldsymbol{I} + (P_\mathrm{s}/N_\mathrm{s}\sigma_\mathrm{s}^2)\boldsymbol{\Lambda}_h\right)^{-1/2} = \boldsymbol{Q}\boldsymbol{R}\boldsymbol{P}^{\mathrm{H}}$, where $\boldsymbol{Q}$ and $\boldsymbol{P}$ are unitary and $\boldsymbol{R}$ is an upper triangular matrix with equal diagonal elements. From there, we let $\boldsymbol{U}_\mathrm{s} = \boldsymbol{P}$, so that we can obtain $\boldsymbol{L} = \boldsymbol{R}^{\mathrm{H}}$.

As a result, the optimisation problem can be reduced to solve for unknown $\boldsymbol{F}_\mathrm{r}$ and P_f. Substituting (18) into (16), it is clear that the source power constraint is satisfied while the source and relay power constraints are decoupled. We can then formulate the inner problem as

$$\min_{\boldsymbol{F}_\mathrm{r}, P_f} \left| \left(\frac{N_\mathrm{s}}{P_\mathrm{s}}\boldsymbol{I} + \tilde{\boldsymbol{H}}^{\mathrm{H}}\tilde{\boldsymbol{H}} \right)^{-1} \right| \tag{22}$$

$$\mathrm{s.t.} \quad \mathrm{tr}\left(\boldsymbol{F}_\mathrm{r}\left(\sigma_\mathrm{s}^2\tilde{\boldsymbol{H}}_\mathrm{ar}\boldsymbol{F}_\mathrm{s}\boldsymbol{F}_\mathrm{s}^{\mathrm{H}}\tilde{\boldsymbol{H}}_\mathrm{ar}^{\mathrm{H}} + \sigma_\mathrm{s}^2\alpha_1\boldsymbol{\Sigma}_\mathrm{ar} + \sigma_{n_\mathrm{r}}^2\boldsymbol{I}\right)\boldsymbol{F}_\mathrm{r}^{\mathrm{H}}\right) \le P_f. \tag{23}$$

To obtain a closed-form solution for $\boldsymbol{F}_\mathrm{r}$, the problem is relaxed by proceeding as in [11]. Specifically, we employ the following approximations:

$$\begin{aligned} \alpha_1\boldsymbol{\Sigma}_\mathrm{ar} &= \mathrm{tr}\left(\boldsymbol{F}_\mathrm{s}\boldsymbol{F}_\mathrm{s}^{\mathrm{H}}\boldsymbol{\Psi}_\mathrm{ar}^{\mathrm{T}}\right)\boldsymbol{\Sigma}_\mathrm{ar} \\ &\simeq P_\mathrm{s}\lambda_{\max}\left(\boldsymbol{\Psi}_\mathrm{ar}^{\mathrm{T}}\right)\boldsymbol{\Sigma}_\mathrm{ar}, \end{aligned} \tag{24}$$

$$\begin{aligned} &\alpha_2\boldsymbol{\Sigma}_\mathrm{rb} + \alpha_3\boldsymbol{\Sigma}_\mathrm{rb} \\ &= \mathrm{tr}\left(\boldsymbol{F}_\mathrm{r}\left(\sigma_\mathrm{s}^2\tilde{\boldsymbol{H}}_\mathrm{ar}\boldsymbol{F}_\mathrm{s}\boldsymbol{F}_\mathrm{s}^{\mathrm{H}}\tilde{\boldsymbol{H}}_\mathrm{ar}^{\mathrm{H}} + \sigma_\mathrm{s}^2\alpha_1\boldsymbol{\Sigma}_\mathrm{ar} + \sigma_{n_\mathrm{r}}^2\boldsymbol{I}\right)\boldsymbol{F}_\mathrm{r}^{\mathrm{H}}\boldsymbol{\Psi}_\mathrm{rb}^{\mathrm{T}}\right)\boldsymbol{\Sigma}_\mathrm{rb} \\ &\quad + \mathrm{tr}\left(\boldsymbol{T}\boldsymbol{T}^{\mathrm{H}}\boldsymbol{\Psi}_\mathrm{rb}^{\mathrm{T}}\right)\boldsymbol{\Sigma}_\mathrm{rb} \\ &\simeq P_\mathrm{r}\lambda_{\max}\left(\boldsymbol{\Psi}_\mathrm{rb}^{\mathrm{T}}\right)\boldsymbol{\Sigma}_\mathrm{rb}. \end{aligned} \tag{25}$$

By introducing the matrix variables

$$\tilde{\boldsymbol{\Sigma}}_\mathrm{ar} = \alpha_1\boldsymbol{\Sigma}_\mathrm{ar} + \sigma_{n_\mathrm{r}}^2\boldsymbol{I}, \tag{26}$$

$$\tilde{\boldsymbol{\Sigma}}_\mathrm{rb} = \alpha_2\boldsymbol{\Sigma}_\mathrm{rb} + \alpha_3\boldsymbol{\Sigma}_\mathrm{rb} + \sigma_{n_\mathrm{b}}^2\boldsymbol{I}, \tag{27}$$

$$\tilde{\boldsymbol{H}}_\mathrm{ar} = \sqrt{\frac{P_\mathrm{s}}{N_\mathrm{s}}}\tilde{\boldsymbol{\Sigma}}_\mathrm{ar}^{-1/2}\tilde{\boldsymbol{H}}_\mathrm{ar}, \tag{28}$$

$$\tilde{\boldsymbol{H}}_\mathrm{rb} = \tilde{\boldsymbol{\Sigma}}_\mathrm{rb}^{-1/2}\tilde{\boldsymbol{H}}_\mathrm{rb}, \tag{29}$$

and considering the following SVD:

$$\tilde{\boldsymbol{H}}_\mathrm{ar} = \boldsymbol{U}_\mathrm{ar}\boldsymbol{\Lambda}_\mathrm{ar}\boldsymbol{V}_\mathrm{ar}^{\mathrm{H}}, \tag{30}$$

$$\tilde{\boldsymbol{H}}_\mathrm{rb} = \boldsymbol{U}_\mathrm{rb}\boldsymbol{\Lambda}_\mathrm{rb}\boldsymbol{V}_\mathrm{rb}^{\mathrm{H}}, \tag{31}$$

the relay AF matrix can be structured as follows:

$$\boldsymbol{F}_\mathrm{r} = \boldsymbol{V}_\mathrm{rb}\boldsymbol{\Lambda}_\mathrm{r}\boldsymbol{U}_\mathrm{ar}^{\mathrm{H}}\tilde{\boldsymbol{\Sigma}}_\mathrm{ar}^{-1/2}, \tag{32}$$

$$\tilde{\boldsymbol{F}}_\mathrm{r} = \boldsymbol{F}_\mathrm{r}\tilde{\boldsymbol{\Sigma}}_\mathrm{ar}^{1/2}, \tag{33}$$

where $\boldsymbol{\Lambda}_\mathrm{r}$ is a diagonal matrix with ith diagonal entry denoted as $\lambda_{\mathrm{r},i}$. By substituting expression (33) into (14) and (15), we obtain

$$\tilde{\boldsymbol{E}} = \boldsymbol{I} + \tilde{\boldsymbol{H}}_\mathrm{ar}^{\mathrm{H}}\tilde{\boldsymbol{F}}_\mathrm{r}^{\mathrm{H}}\tilde{\boldsymbol{H}}_\mathrm{rb}^{\mathrm{H}}\tilde{\boldsymbol{R}}_n^{-1}\tilde{\boldsymbol{H}}_\mathrm{rb}\tilde{\boldsymbol{F}}_\mathrm{r}\tilde{\boldsymbol{H}}_\mathrm{ar}, \tag{34}$$

$$\tilde{\boldsymbol{R}}_n = \tilde{\boldsymbol{H}}_\mathrm{rb}\tilde{\boldsymbol{F}}_\mathrm{r}\tilde{\boldsymbol{F}}_\mathrm{r}^{\mathrm{H}}\tilde{\boldsymbol{H}}_\mathrm{rb}^{\mathrm{H}} + \boldsymbol{I}. \tag{35}$$

Note that for a positive semi-definite matrix $\boldsymbol{M} \in \mathbb{C}^{N\times N}$, we have [17]

$$\det(\boldsymbol{M}) \le \prod_{i=1}^{N} \boldsymbol{M}(i,i), \tag{36}$$

where the equality holds when $\boldsymbol{M}$ is a diagonal matrix [19]. Denoting the ith diagonal element of $\boldsymbol{\Lambda}_\mathrm{ar}$ and $\boldsymbol{\Lambda}_\mathrm{rb}$ as $\lambda_{1,i}$ and $\lambda_{2,i}$, respectively, where $i = 1,\ldots,N_\mathrm{s}$, the optimisation problem can be rewritten as

$$\min_{\lambda_{\mathrm{r},i}, P_f} \prod_{i=1}^{N_\mathrm{s}} \left(1 + \frac{\lambda_{1,i}^2\lambda_{2,i}^2\lambda_{\mathrm{r},i}^2}{\lambda_{2,i}^2\lambda_{\mathrm{r},i}^2 + 1}\right)^{-1} \tag{37}$$

$$\mathrm{s.t.} \quad \sum_{i=1}^{N_\mathrm{s}} \lambda_{\mathrm{r},i}^2\left(\sigma_\mathrm{s}^2\lambda_{1,i}^2 + 1\right) \le P_f, \tag{38}$$

$$\lambda_{\mathrm{r},i} \ge 0, \quad i = 1,\ldots,N_\mathrm{s}. \tag{39}$$

By introducing $y_i = \lambda_{\mathrm{r},i}^2\left(\sigma_\mathrm{s}^2\lambda_{1,i}^2 + 1\right)$ and using the logarithm function (which is monotonically increasing), (37) can be turned into the following equivalent maximization problem:

$$\max_{y_i, P_f} \sum_{i=1}^{N_\mathrm{s}} \ln\left(\frac{y_i\lambda_{2,i}^2\lambda_{1,i}^2 + y_i\lambda_{2,i}^2 + \lambda_{1,i}^2 + 1}{y_i\lambda_{2,i}^2 + \lambda_{1,i}^2 + 1}\right) \tag{40}$$

$$\mathrm{s.t.} \quad \sum_{i=1}^{N_\mathrm{s}} y_i \le P_f, \tag{41}$$

$$y_i \ge 0, \quad i = 1,\ldots,N_\mathrm{s}. \tag{42}$$

Due to the monotonicity of the problem, an iterative method can be used to solve it with guaranteed convergence. The optimum y_i can be obtained by means of KKT conditions [20] as follows:

$$y_i = \frac{1}{2\lambda_{2,i}^2}\left[\sqrt{\lambda_{1,i}^4 + 4\lambda_{1,i}^2\lambda_{2,i}^2\mu_\mathrm{r}} - \lambda_{1,i}^2 - 2\right]^+, \tag{43}$$

where $[y]^+ = \max[0, y]$, and μ_r is the Lagrange multiplier such that $\sum_{i=1}^{N_\mathrm{s}} y_i = P_f$ holds.

Nevertheless, for the purpose of calculating the relay AF matrix, we require the value of P_f. To confuse the passive eavesdropper, we need to allocate more power to maximise the AN power level, while a proper MSE requirement for Bob should be satisfied to maintain a desired performance level for the intended user. To this end, the power allocation procedure is developed as follows. For each P_f in the interval $[0, P_\mathrm{r}]$, we employ the proposed algorithm to calculate the related variables to minimise the MSE. If the achieved minimum MSE satisfies the required target, the search terminates; otherwise the iterative procedure is continued to find the appropriate value of P_f. A bisection method is adopted to effectively search over the interval for the iterative procedure. The solution to the inner problem is summarised in Table 1, while the overall procedure of the proposed algorithm with the outer problem is shown in Table 2.

As we can see from (2), the proposed THP non-linear scheme involves an additional $N_\mathrm{s} \times N_\mathrm{s}$ triangular matrix multiplication

Table 1 Solution to the inner problem at the relay

Input	MSE target ε_b for Bob, and the desired resolution γ
0	Initialisation: Set $P_{min}=0$, $P_{max}=P_r$
1	Set $P_f=(P_{min}+P_{max})/2$. Solve for the unknown $y_i=(1/2\lambda_{2,i}^2)\left[\sqrt{\lambda_{1,i}^4+4\lambda_{1,i}^2\lambda_{2,i}^2\mu_r}-\lambda_{1,i}^2-2\right]^+$ by means of the KKT conditions. Note that the variable μ_r is chosen to satisfy $\sum_{i=1}^{N_s}y_i=P_f$, which can be solved by the bisection method in [10]. Compute $\boldsymbol{F}_r$ from (32)
2	If the objective function $f(P_f)<\varepsilon_b$, then set $P_{max}=P_f$; otherwise set $P_{min}=P_f$.
3	If $(P_{max}-P_{min})>\gamma$, then go back to step 1.
Output:	Minimum required power P_f and $\boldsymbol{F}_r$.

Table 2 Proposed algorithm with solution to the outer problem

1 Compute $\boldsymbol{F}_r$ and P_f by solving the inner problem, as described in Table 1
2 Derive the AN spatial shaping matrix $\boldsymbol{T}$ by using (11)
3 Solve for the outer problem: compute $\boldsymbol{F}_s$ and $\boldsymbol{B}$ based on (18) and (20), respectively
4 Compute the optimal MMSE receiver $\boldsymbol{W}_b$ by using the obtained $\boldsymbol{F}_s$, $\boldsymbol{F}_r$, $\boldsymbol{T}$ and $\boldsymbol{B}$

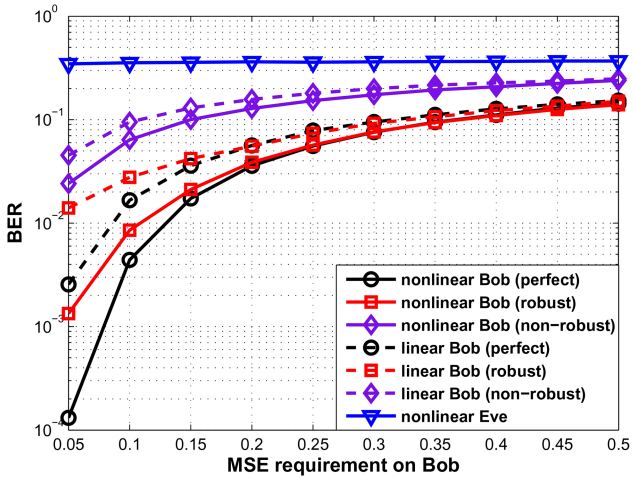

Fig. 2 *BER versus the MSE target with* $P_r=30$ dB

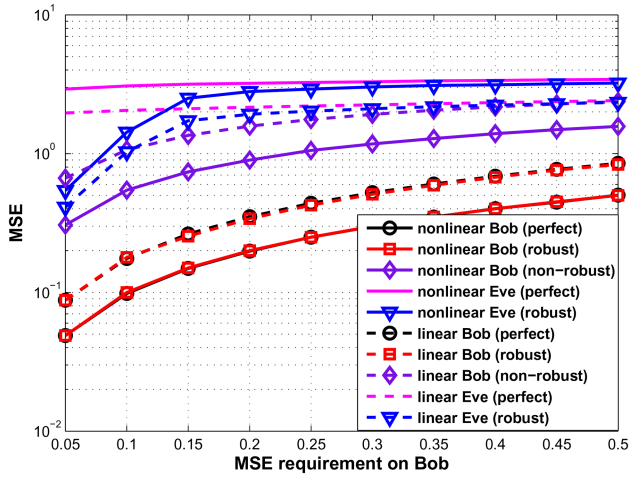

Fig. 3 *Achieved MSE versus the MSE target with* $P_r=30$ dB

compared with linear precoding (The corresponding SVD-based linear transceiver is also considered for the purpose of comparison in our simulations.). The overall computational complexity of the proposed non-linear transceiver is $O(N_s^3+N_rN_s^2+N_dN_r^2+N_r^3+N_dN_s^2+I_rN_s)$, where parameter I_r denotes the iteration number in solving for the relay AF matrix. Hence, we advocate an affordable increase in complexity in exchange for a significant improvement in performance, as will be demonstrated in Section 4.

4 Simulation results

In this section, we assess the performance of the proposed non-linear transceiver design algorithm numerically. We consider an AF MIMO relay system in the presence of a passive eavesdropper with $N_r=6$, $N_s=N_d=4$. By using the exponential model [21], the channel estimation error covariance matrices have elements given by $[\boldsymbol{\Psi}_{ar}]_{i,j}=[\boldsymbol{\Psi}_{rb}]_{i,j}=\alpha^{|i-j|}$, $[\boldsymbol{\Sigma}_{ar}]_{i,j}=[\boldsymbol{\Sigma}_{rb}]_{i,j}=\sigma_e^2\beta^{|i-j|}$. Here, α and β denote the correlation coefficients and σ_e^2 is the estimation error variance. The estimated channels, $\bar{\boldsymbol{H}}_{ar}$ and $\bar{\boldsymbol{H}}_{rb}$, are generated as follows:

$$\bar{\boldsymbol{H}}_{ar}\sim\mathcal{CN}\left(0_{N_r\times N_s},\frac{(1-\sigma_e^2)}{\sigma_e^2}\boldsymbol{\Psi}_{ar}\otimes\boldsymbol{\Sigma}_{ar}\right),\tag{44}$$

$$\bar{\boldsymbol{H}}_{rb}\sim\mathcal{CN}\left(0_{N_d\times N_r},\frac{(1-\sigma_e^2)}{\sigma_e^2}\boldsymbol{\Psi}_{rb}\otimes\boldsymbol{\Sigma}_{rb}\right),\tag{45}$$

such that channel realisations have unit variance. In the simulations, we consider data transmission with 16-QAM modulation scheme. The SNR at the relay is defined as $\text{SNR}_{ar}=P_s/\sigma_{n_r}^2$, and the SNR at the destination is defined as $\text{SNR}_{rb}=P_r/\sigma_{n_b}^2$. We also assume that the noise variance $\sigma_{n_r}^2=\sigma_{n_b}^2=\sigma_{n_e}^2=1$. All the results are averaged over 10^4 independent channel realisations.

Fig. 2 displays the bit error rate performance comparison for Bob and Eve versus the desired MSE requirement ε_b for Bob. The maximum transmit power at the relay is assumed to be $P_r=30$ dB. The MSE target ε_b is varied from 0.05 to 0.5. Here, we set $\text{SNR}_{ar}=\text{SNR}_{rb}=30$ dB, $\alpha=\beta=0$ and $\sigma_e^2=0.005$. As shown in Fig. 2, the BER performance of Eve is always inferior to Bob. The proposed algorithm with perfect CSI achieves the best performance, while the performance of the proposed robust algorithm considering the channel estimation errors is better than that of the non-robust algorithm based on the estimated channels only. This shows the ability of the proposed algorithm to deal with CSI uncertainties. Also, when compared with the corresponding linear scheme, the proposed non-linear design achieves a significant performance improvement as expected.

Fig. 3 illustrates the comparative MSE performance of the various algorithms under study. It is observed that the MSE target for Bob is always achieved when using the proposed design, while the MSE of Eve is degraded because of the jamming effect of AN. As expected, the MSE for Bob is greatly degraded in the non-robust scheme. We also note that the MSE of Eve in the robust scheme is lower than that in the perfect case. This is reasonable because the transmit power allocated at the relay for the information-bearing signal increases due to the imperfect CSI, which leads to a reduction in the AN power.

In Fig. 4, we plot the normalised transmit power ratio for the information-bearing signal versus the MSE requirement for Bob. The ratio P_f/P_r decreases as the MSE target ε_b varies from 0.05 to 0.5. Furthermore, it is observed that higher SNR leads to smaller ratio P_f/P_r, as the relay tends to allocate a smaller portion of power for the information-bearing signal to satisfy the MSE requirement for Bob. The dashed lines display the corresponding normalised transmit power ratio for the robust design with $\sigma_e^2=0.005$. Note

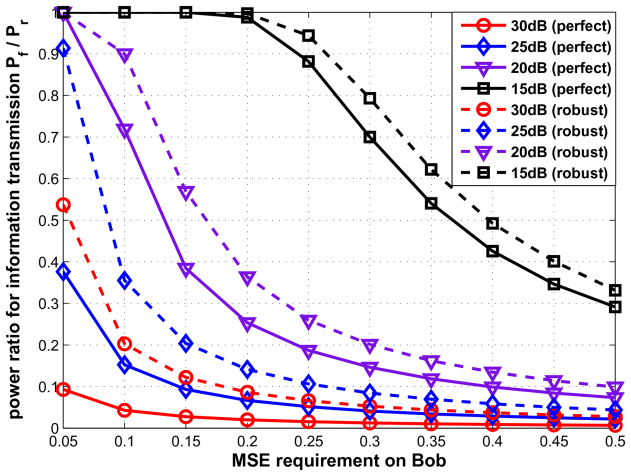

Fig. 4 *Normalised transmit power ratio for information-bearing signal versus the MSE target*

that the perfect scheme has a smaller ratio compared with the robust design for the same SNR. This is because the relay needs to allocate more power for the information-bearing signal to counteract the effects of channel estimation errors.

5 Conclusion

In this paper, a QoS-based robust non-linear transceiver design for secure communications in AF MIMO relay systems has been proposed. We focused on optimising the transceiver to achieve predefined QoS requirement at the intended user in terms of MSE. The transceiver design was reformulated as a two-level optimisation, where the outer problem considers the source precoder design and the inner problem aims to jointly optimise the relay precoder and the AN covariance matrices. We proposed to tackle the power allocation problem at the relay by means of the bisection method while achieving the MSE requirement for the intended user. With the aid of a lower bound on the objective function, closed-form solutions for the AF relaying matrix were derived by an iterative method based on the KKT conditions. The effectiveness of the proposed non-linear transceiver design over other benchmark approaches has been verified by numerical simulations.

6 References

[1] Wang, H.-M., Liu, F., Yang, M.: 'Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems', *IEEE Trans. Veh. Technol.*, 2015, **64**, (10), pp. 4893–4898

[2] Wang, H.-M., Liu, F., Xia, X.-G.: 'Joint source-relay precoding and power allocation for secure amplify-and-forward MIMO relay networks', *IEEE Trans. Inf. Forensics Security*, 2014, **9**, (8), pp. 1240–1250

[3] Zhang, M., Huang, J., Yu, H., *et al.*: 'QoS-based source and relay secure optimization design with presence of channel uncertainty', *IEEE Commun. Lett.*, 2013, **17**, (8), pp. 1544–1547

[4] Wang, C., Wang, H.-M.: 'Robust joint beamforming and jamming for secure AF networks: low-complexity design', *IEEE Trans. Veh. Technol.*, 2015, **64**, (5), pp. 2192–2198

[5] Wang, H.-M., Luo, M., Xia, X.-G., *et al.*: 'Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI', *IEEE Signal Process. Lett.*, 2013, **20**, (1), pp. 39–42

[6] Li, Q., Yang, Y., Ma, W.-K., *et al.*: 'Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks', *IEEE Trans. Signal Process.*, 2015, **63**, (1), pp. 206–220

[7] Shen, H., Xu, W., Zhao, C.: 'QoS constrained optimization for multi-antenna AF relaying with multiple eavesdroppers', *IEEE Signal Process. Lett.*, 2015, **22**, (12), pp. 2224–2228

[8] Gong, X., Long, H., Yin, H., *et al.*: 'Robust amplify-and-forward relay beamforming for security with mean square error constraint', *IET Commun.*., 2015, **9**, (8), pp. 1081–1087

[9] Goel, S., Negi, R.: 'Guaranteeing secrecy using artificial noise', *IEEE Trans. Wirel. Commun.*, 2008, **7**, (6), pp. 2180–2189

[10] Tseng, F., Chang, M., Wu, W.: 'Joint Tomlinson–Harashima source and linear relay precoder design in amplify-and-forward MIMO relay systems via MMSE criterion', *IEEE Trans. Veh. Technol.*, 2011, **60**, (4), pp. 1687–1698

[11] Millar, A., Weiss, S., Stewart, R.: 'Robust transceiver design for MIMO relay systems with Tomlinson Harashima precoding'. Proc. IEEE EUSIPCO, August 2012, pp. 1374–1378

[12] Xing, C., Ma, S., Gao, F., *et al.*: 'Robust transceiver with Tomlinson-Harashima precoding for amplify-and-forward MIMO relaying systems', *IEEE J. Sel. Areas Commun.*, 2012, **30**, (8), pp. 1370–1382

[13] Zhang, L., Cai, Y., de Lamare, R., *et al.*: 'Robust multibranch Tomlinson-Harashima precoding design in amplify-and-forward MIMO relay systems', *IEEE Trans. Commun.*, 2014, **62**, (10), pp. 3476–3490

[14] Jin, L., Zhang, L., Huang, K., *et al.*: 'Robust artificial noise assisted secure transceiver optimization in af relay networks with multiple source-destination pairs'. Proc. IEEE ICSPCS, Gold Coast, AUS, December 2014, pp. 1–6

[15] Xing, C., Ma, S., Wu, Y.: 'Robust joint design of linear relay precoder and destination equalizer for dual-hop amplify-and-forward MIMO relay systems', *IEEE Trans. Signal Process.*, 2010, **58**, (4), pp. 2273–2283

[16] Gupta, A., Nagar, D.: '*Matrix variate distributions*' (Chapman & Hall/CRC, London, UK, 2000)

[17] Bernstein, D.: '*Matrix mathematics: theory, facts, and formulas*' (Princeton University Press, Princeton, USA, 2011)

[18] Jiang, Y., Li, J., Hager, W.: 'Joint transceiver design for MIMO communications using geometric mean decomposition', *IEEE Trans. Signal Process.*, 2005, **53**, (10), pp. 3791–3803

[19] Palomar, D., Cioffi, J., Lagunas, M.: 'Joint Tx-Rx beamforming design for multicarrier MIMO channels: A unified framework for convex optimization', *IEEE Trans. Signal Process.*, 2003, **51**, (9), pp. 2381–2401

[20] Rong, Y., Tang, X., Hua, Y.: 'A unified framework for optimizing linear nonregenerative multicarrier MIMO relay communication systems', *IEEE Trans. Signal Process.*, 2009, **57**, (12), pp. 4837–4851

[21] Ding, M., Blostein, S.: 'MIMO minimum total MSE transceiver design with imperfect CSI at both ends', *IEEE Trans. Signal Process.*, 2009, **57**, (3), pp. 1141–1150