Algorithms for Secrecy Guarantee With Null Space Beamforming in Two-Way Relay Networks

Reported by Yaping Wan

This paper appeared in:
IEEE transactions on Signal Processing, Vol. 62,No. 8
Date of publication: April 15,2014
Authors: Yunchuan Yang, Cong Sun, Hui Zhao, Hang Long, Wenbo Wang

Outline

- Background knowledge
- Abstract
- Introduction
- System model
- Simulation results
- Conclusions
- Future work

Outline

- Background knowledge
- Abstract
- Introduction
- System model
- Simulation results
- Conclusions
- Future work

Active-set method

The original problem is

$$\min_{p_i \in R^{2(N-2)\times 1}} \frac{1}{2}\mathbf{p}_i^T \mathbf{W}_i \mathbf{p}_i + g_i^T \mathbf{p}_i$$

$$s.t. \quad \left(\widetilde{\mathbf{A}}_1 \mathbf{x}_i\right)^T \mathbf{p}_i + \frac{1}{2}\mathbf{x}_i^T \widetilde{\mathbf{A}}_1 \mathbf{x}_i - t_1 \sigma_1^2 \geq 0,$$

$$\left(\widetilde{\mathbf{A}}_2 \mathbf{x}_i\right)^T \mathbf{p}_i + \frac{1}{2}\mathbf{x}_i^T \widetilde{\mathbf{A}}_2 \mathbf{x}_i - t_2 \sigma_2^2 \geq 0$$

Based on the remark 1, for simplicity, we assume that the first inequality satisfies with equality at the ith iteration, where the first constraint is regarded as active set.

Thus, the problem can be reduced as following problem

$$\min_{\mathbf{p}_i \in R^{2(N-2)\times 1}} \quad \frac{1}{2}\mathbf{p}_i^T \mathbf{W}_i \mathbf{p}_i + \mathbf{g}_i^T \mathbf{p}_i \tag{50a}$$

$$s.t. \quad (\tilde{\mathbf{A}}_1 \mathbf{x}_i)^T \mathbf{p}_i + c_1 = 0 \tag{50b}$$

where $c_1 = \frac{1}{2}\mathbf{x}_i^T \tilde{\mathbf{A}}_1 \mathbf{x}_i - t_1 \sigma_1^2$.

Next, we focus on finding the local optimal solution of problem (19). Define

$$\tilde{\mathbf{A}}_1\mathbf{x}_i = [\,\mathbf{Q}_1 \quad \mathbf{Q}_2\,]\begin{bmatrix} R_1 \\ \mathbf{R}_2 \end{bmatrix} \in C^{2(N-2)\times 1} \tag{51}$$

as its QR factorization, the unitary space can be divided into two subspaces, where $\mathbf{Q}_1 \in C^{2(N-2)\times 1}$ and $\mathbf{Q}_2 \in C^{2(N-2)\times(2(N-2)-1)}$ are orthogonal matrix. Here, $R \in C$ is a scalar and $\mathbf{R}_2 \in C^{(2(N-2)-1)\times 1}$ is a vector. Then, the solution of (50) can be expressed as:

$$\mathbf{p}_i = \mathbf{Q}_1 a + \mathbf{Q}_2\mathbf{b} \tag{52}$$

where $a \in R$ and $\mathbf{b} \in R^{(2(N-2)-1)\times 1}$ are the optimization variables. Substitute (52) in to (50b), we have $a = -c_1 R_1^{-1}$. At the same time, the solution $\mathbf{p}_i$ should satisfy with the inequality constraint of problem (19), i.e.,

$$(\tilde{\mathbf{A}}_2\mathbf{x}_i)^T(\mathbf{Q}_1 a + \mathbf{Q}_2\mathbf{b}) + c_2 \geq 0 \tag{53}$$

where $c_2 = \frac{1}{2}\mathbf{x}_i^T\tilde{\mathbf{A}}_2\mathbf{x}_i - t_2\sigma_2^2$.

Without loss of generality, in our paper, $\mathbf{b}$ is chosen as:

$$\mathbf{b} = \frac{(-c_2 - (\mathbf{A}_2\mathbf{x}_i)^T\mathbf{Q}_1 a + 1)((\tilde{\mathbf{A}}_2\mathbf{x}_i)^T\mathbf{Q}_2)^T}{\left\|(\tilde{\mathbf{A}}_2\mathbf{x}_i)^T\mathbf{Q}_2\right\|_2}. \tag{54}$$

Obviously, the search direction $\mathbf{p}_i$ is a feasible solution of problem. Define $\tilde{\mathbf{p}}_i = \mathbf{p}_i + \delta$, and substitute it into (50), the subproblem can be equivalently expressed as

$$\min_{\delta \in R^{2(N-2)\times 1}} \quad \frac{1}{2}\delta^T\mathbf{W}_i\delta + \nabla f(\mathbf{p}_i)^T\delta + f(\mathbf{p}_i) \tag{55a}$$

$$s.t. \quad (\tilde{\mathbf{A}}_1\mathbf{x}_i)^T\delta = 0. \tag{55b}$$

Here

$$f(\mathbf{p}_i) = \frac{1}{2}\mathbf{p}_i^T\mathbf{W}_i\mathbf{p}_i + \mathbf{g}_i^T\mathbf{p}_i, \nabla f(\mathbf{p}_i) = \mathbf{W}_i\mathbf{p}_i + \mathbf{g}_i. \tag{56}$$

Outline

- Background knowledge
- Abstract
- Introduction
- System model
- Simulation results
- Conclusions
- Future work

Abstract

- Problem： A joint optimization whose goal is to obtain the optimal two sources' transmit power as well as the beamforming vector at relay subject to various criteria.
- Method： semi-definite programming(SDP), sequential quadratic programming(SQP), alternative iterative optimize(AO).

Outline

- Background knowledge
- Abstract
- Introduction
- System model
- Simulation results
- Conclusions
- Future work

Introduction

- Two-hop secure communication using an untrusted relay[28].
- Securing multi-antenna two-way relay channels with analog network coding against eavesdropper[30].
- Distributed beamforming for physical-layer security of two way relay networks[32].

Outline

- Background knowledge
- Abstract
- Introduction
- System model
- Simulation results
- Conclusions
- Future work

System model

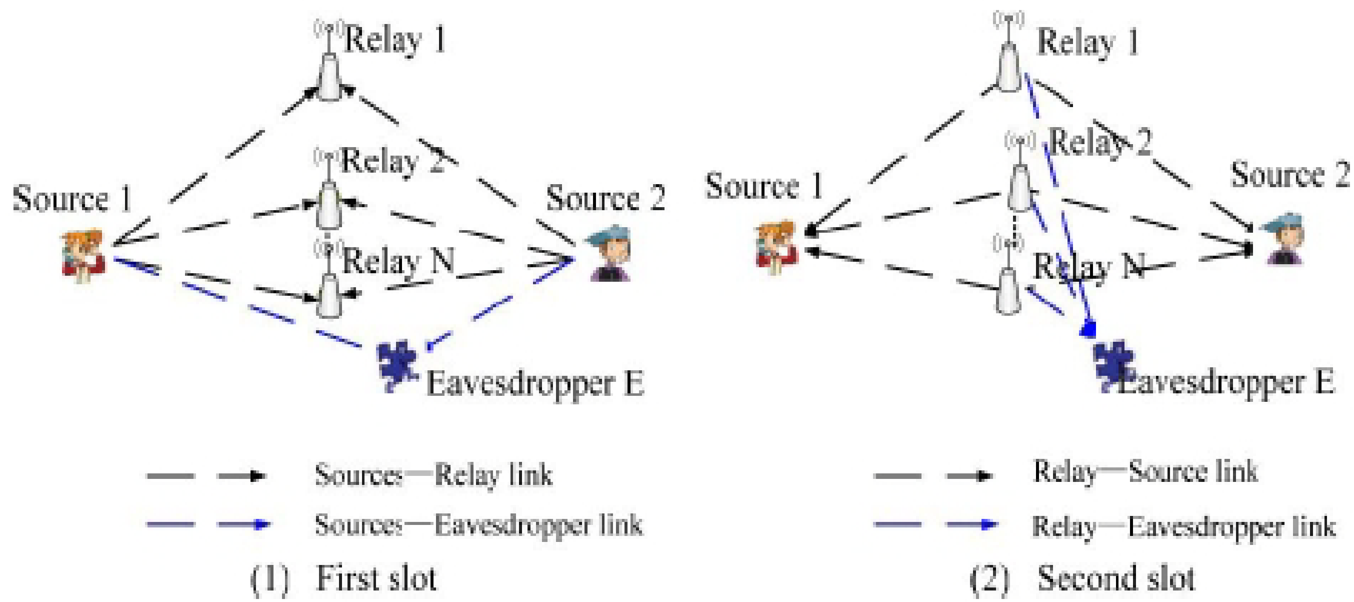


Fig. 1. The secure communication model in two-way relay networks.

Two sources, an eavesdropper and N relays. Each node equips with signal antenna and operates in a half-duplex way.

System model

- Multiple access channel(MAC): S_1,S_2 transmit their messages to the relays simultaneously.
- Broadcast channel(BC): the i th relay multiplies its received signal r_i by w_i^* , where w_i^* is the complex beam forming weight at the i th relay.

The received signal at S1,S2:

$$y_1 = \mathbf{f}_1^T \mathbf{s} + n_1$$
$$= \mathbf{w}^H \mathbf{F}_1 \left(\mathbf{f}_1 x_1 + \mathbf{f}_2 x_2 + \mathbf{n}_R \right) + n_1 \qquad (1)$$
$$y_2 = \mathbf{f}_2^T \mathbf{s} + n_2$$
$$= \mathbf{w}^H \mathbf{F}_2 \left(\mathbf{f}_1 x_1 + \mathbf{f}_2 x_2 + \mathbf{n}_R \right) + n_2 \qquad (2)$$

Where $\mathbf{s} = \mathbf{Wr}$, $\mathbf{W} = diag\left(\left[w_1^*, w_2^*, \cdots, w_N^*\right]\right)$, $\mathbf{w} = diag\left(\mathbf{W}^H\right)$

$\mathbf{F}_k = diag\left(\mathbf{f}_k\right), k = 1, 2.$

n1,n2 are additive zero-mean noises with variances σ_1^2 and σ_2^2 at two sources.

- The received signal at the eavesdropper:

$$\underbrace{\begin{bmatrix} y_E^1 \\ y_E^2 \end{bmatrix}}_{y_E} = \underbrace{\begin{bmatrix} g_1 & g_2 \\ \mathbf{w}^H\mathbf{L}\mathbf{f}_1 & \mathbf{w}^H\mathbf{L}\mathbf{f}_2 \end{bmatrix}}_{H_E} \underbrace{\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}}_{\mathbf{x}} + \underbrace{\begin{bmatrix} n_E^1 \\ \mathbf{w}^H\mathbf{L}\mathbf{n}_R + n_E^2 \end{bmatrix}}_{N_E} \quad (3)$$

where $\mathbf{L} = diag(l), l = [l_1, l_2, \cdots, l_N]$

n_E^1 and n_E^2 are additive zero-mean noises with variances $\sigma_{E,1}^2$ and $\sigma_{E,2}^2$.

- Using Gaussian inputs and stochastic encoders, the achievable secrecy rate:

$$R_1 \le [I(x_2; y_1) - I(x_2; \mathbf{y}_E)]^+ \quad (4a)$$

$$R_2 \le [I(x_1; y_2) - I(x_1; \mathbf{y}_E)]^+ \quad (4b)$$

$$R_1 + R_2 \le [I(x_1; y_2) + I(x_1; y_2) - I(x_1, x_2; \mathbf{y}_E)]^+ \quad (4c)$$

- The maximum achievable rates for S2 to S1 and S1 to S2:

$$I(x_2; y_1) = \frac{1}{2}\log_2(1+\gamma_1) = \frac{1}{2}\log_2\left(1+\frac{P_2\left|\mathbf{w}^H\mathbf{F}_1\mathbf{f}_2\right|^2}{\sigma_R^2\left\|\mathbf{w}^H\mathbf{F}_1\right\|_2^2+\sigma_1^2}\right) \quad (5)$$

$$I(x_1; y_2) = \frac{1}{2}\log_2(1+\gamma_2) = \frac{1}{2}\log_2\left(1+\frac{P_1\left|\mathbf{w}^H\mathbf{F}_2\mathbf{f}_1\right|^2}{\sigma_R^2\left\|\mathbf{w}^H\mathbf{F}_2\right\|_2^2+\sigma_2^2}\right) \quad (6)$$

- The information rate achieved at the eavesdropper:

$$I(x_2;\mathbf{y}_E)=\frac{1}{2}\log_2\left(1+\frac{P_2(|g_2|^2+|\mathbf{w}^H\mathbf{L}\mathbf{f}_1|^2)}{P_1(|g_1|^2+|\mathbf{w}^H\mathbf{L}\mathbf{f}_2|^2)+\sigma_{E,1}^2+\sigma_{E,2}^2+\sigma_R^2\|\mathbf{w}^H\mathbf{L}\|_2^2}\right), \quad (7a)$$

$$I(x_1;\mathbf{y}_E)=\frac{1}{2}\log_2\left(1+\frac{P_1(|g_1|^2+|\mathbf{w}^H\mathbf{L}\mathbf{f}_2|^2)}{P_2(|g_2|^2+|\mathbf{w}^H\mathbf{L}\mathbf{f}_1|^2)+\sigma_{E,1}^2+\sigma_{E,2}^2+\sigma_R^2\|\mathbf{w}^H\mathbf{L}\|_2^2}\right), \quad (7b)$$

$$I(x_1,x_2;\mathbf{y}_E)=\frac{1}{2}\log_2\det\left(\mathbf{I}_2+\frac{\mathbf{H}_E\mathbf{Q}_E\mathbf{H}_E^H}{\mathbf{K}_E}\right). \quad (7c)$$

Equation (7c) is obtained from the equivalent MIMO system. $\mathbf{Q}=\mathrm{diag}(P_1,P_2)$ is the diagonal power allocation matrix of two sources, and $\mathbf{K}_E=\mathrm{diag}(\sigma_{E,1}^2,\sigma_{E,2}^2+\sigma_R^2\mathbf{w}^H\mathbf{L}\mathbf{L}\mathbf{w})$ is the equivalent noise covariance matrix at the eavesdropper.

- Using zero-forcing method to eliminate some jamming terms: $\mathbf{w}^H\mathbf{Z}=0, \mathbf{Z}=\mathbf{L}[\mathbf{f}_1,\mathbf{f}_2]$ is the $N\times 2$ equivalent channel matrix.
- After ZF, the achievable secrecy rate:

$$R^1 \le C_s^1 = \left[I(x_2;y_1) - \frac{1}{2}\log_2\left(1+\frac{P_2|g_2|^2}{P_1|g_1|^2+\sigma_{E,1}^2}\right)\right]^+ \quad (8a)$$

$$R^2 \le C_s^2 = \left[I(x_1;y_2) - \frac{1}{2}\log_2\left(1+\frac{P_1|g_1|^2}{P_2|g_2|^2+\sigma_{E,1}^2}\right)\right]^+ \quad (8b)$$

$$R^1+R^2 \le C_s^{sum} = \left[I(x_2;y_1) + I(x_1;y_2) - \frac{1}{2}\log_2\left(1+\frac{P_1|g_1|^2+P_2|g_2|^2}{\sigma_{E,1}^2}\right)\right]^+ \quad (8c)$$

Total transmit power minimization(TTPM):

$$\min_{\substack{P_1>0, P_2>0 \\ \mathbf{w}\in C^{N\times 1}}} \quad P_T = P_1 + P_2 + P_R \tag{9a}$$

$$s.t. \quad C_s^1 \geq r_1, C_s^2 \geq r_2. \tag{9b}$$

r_1 and r_2 are the given secrecy rate thresholds for two sources, P_R is total relay transmit power,

$$\begin{aligned} P_R &= E\left(s^H s\right) = Tr\left(E\left(\left(\mathbf{W}r\right)\left(\mathbf{W}r\right)^H\right)\right) \\ &= P_1 \mathbf{w}^H \mathbf{D}_1 \mathbf{w} + P_2 \mathbf{w}^H \mathbf{D}_2 \mathbf{w} + \sigma_R^2 \mathbf{w}^H \mathbf{w} \end{aligned} \tag{10}$$

where $\mathbf{D}_1 = \mathbf{F}_1 \mathbf{F}_1^H, \mathbf{D}_2 = \mathbf{F}_2 \mathbf{F}_2^H$.

Optimization of Relay Beamforming Vector(TTPM)

- When P1 and P2 is fixed, the equivalent problem:

$$\min_{\mathbf{c}\in C^{(N-2)\times 1}} \quad \mathbf{c}^H \mathbf{A}_0 \mathbf{c} \qquad (11a)$$

$$s.t. \quad \mathbf{c}^H \mathbf{A}_k \mathbf{c} - t_k \sigma_k^2 \geq 0, k = 1, 2 \qquad (11b)$$

where $\mathbf{w} = \mathbf{G}\mathbf{c}$, $\mathbf{G}$ is the column-orthogonal matrix corresponding to zero singular value of matrix $\mathbf{Z}^H$ and $\mathbf{c}$ is the combination vector with dimension $(N-2)\times 1$.

$$\left.\begin{aligned} \mathbf{A}_0 &= \mathbf{G}^H \left(P_1 \mathbf{D}_1 + P_2 \mathbf{D}_2 + \sigma_R^2 \mathbf{I}_N \right) \mathbf{G} \\ \mathbf{A}_1 &= \mathbf{G}^H \left(P_2 \mathbf{R}_1 - t_1 \sigma_R^2 \mathbf{D}_1 \right) \mathbf{G} \\ \mathbf{A}_2 &= \mathbf{G}^H \left(P_1 \mathbf{R}_2 - t_2 \sigma_R^2 \mathbf{D}_2 \right) \mathbf{G} \end{aligned}\right\} \quad (12)$$

$$\left.\begin{aligned} \mathbf{R}_1 &= \mathbf{R}_2 = \mathbf{F}_1 \mathbf{f}_2 \mathbf{f}_2^H \mathbf{F}_1^H \\ t_1 &= 2^{2r_1} - 1 + 2^{2r_1} \frac{P_2 |g_2|^2}{P_1 |g_1|^2 + \sigma_{E,1}^2} \\ t_2 &= 2^{2r_2} - 1 + 2^{2r_2} \frac{P_1 |g_1|^2}{P_2 |g_2|^2 + \sigma_{E,1}^2} \end{aligned}\right\} \quad (13)$$

SDP method

- Let $\mathbf{C} = \mathbf{c}\mathbf{c}^H$, then

$$\min_{\mathbf{C}\in C^{(N-2)\times(N-2)}} \quad Tr\left(\mathbf{A}_0\mathbf{C}\right) \tag{14a}$$

$$s.t. \quad Tr\left(\mathbf{A}_k\mathbf{C}\right) - t_k\sigma_k^2 \geq 0, k = 1, 2 \tag{14b}$$

$$rank\left(\mathbf{C}\right) = 1, \quad \mathbf{C} \succ 0 \tag{14c}$$

- Using SDR technique, the above problem can be relaxed as a standard SDP problem.

- Remark 1: a complex valued homogeneous QCQP problem with n constraints is guaranteed to have a global optimum solution with rank $r \leq \sqrt{n}$. [43].
- Since the number of constraints n in (14) is equal 2, $\mathbf{C}_{opt}$ is always the rank-one solution.
- At least one inequality constraint is satisfied with equality at the optimum $\mathbf{C}_{opt}$.

SQP method

- We apply SQP algorithm to solve subproblem (14) to reduce the high complexity of SDP. The QCQP problem in real domain as:

$$\min_{\mathbf{x}\in R^{2(N-2)\times 1}} \quad \frac{1}{2}\mathbf{x}^T\widetilde{\mathbf{A}}_0\mathbf{x} \tag{15a}$$

$$s.t. \quad \frac{1}{2}\mathbf{x}^T\widetilde{\mathbf{A}}_1\mathbf{x}-t_1\sigma_1^2\geq 0 \tag{15b}$$

$$\frac{1}{2}\mathbf{x}^T\widetilde{\mathbf{A}}_2\mathbf{x}-t_2\sigma_2^2\geq 0 \tag{15c}$$

- Where $\mathbf{x}=\left[\mathrm{Re}\left(\mathbf{c}^T\right) \quad \mathrm{Im}\left(\mathbf{c}^T\right)\right]^T$ and $\widetilde{\mathbf{A}}_k=\begin{pmatrix} 2\,\mathrm{Re}\left(\mathbf{A}_k\right) & -2\,\mathrm{Im}\left(\mathbf{A}_k\right) \\ 2\,\mathrm{Im}\left(\mathbf{A}_k\right) & 2\,\mathrm{Re}\left(\mathbf{A}_k\right)\end{pmatrix}, \quad k=0,1,2$

(16)

➢ The Lagrangian function:

$$L(\mathbf{x};\lambda_k)=\frac{1}{2}\mathbf{x}^T\widetilde{\mathbf{A}}_0\mathbf{x}+\sum_{k=1}^{2}\lambda_k\left(t_k\sigma_k^2-\frac{1}{2}\mathbf{x}^T\widetilde{\mathbf{A}}_k\mathbf{x}\right) \qquad (17)$$

where $\lambda_k \geq 0$ and $\left(\widetilde{\mathbf{A}}_0-\sum_{k=1}^{2}\lambda_k^i\widetilde{\mathbf{A}}_k\right)\succeq 0.$

- At each iterative point x_i with Lagrange multipliers λ_k^i , the basic SQP defines an appropriate search direction p_i as a solution of the QP subproblem:

$$\min_{\mathbf{p}_i\in R^{2(N-2)\times 1}} \quad \frac{1}{2}\mathbf{p}_i^T\mathbf{W}_i\mathbf{p}_i+g_i^T\mathbf{p}_i \qquad (18a)$$

$$s.t. \quad \left(\widetilde{\mathbf{A}}_1\mathbf{x}_i\right)^T\mathbf{p}_i+\frac{1}{2}\mathbf{x}_i^T\widetilde{\mathbf{A}}_1\mathbf{x}_i-t_1\sigma_1^2\geq 0 \qquad (18b)$$

$$\left(\widetilde{\mathbf{A}}_2\mathbf{x}_i\right)^T\mathbf{p}_i+\frac{1}{2}\mathbf{x}_i^T\widetilde{\mathbf{A}}_2\mathbf{x}_i-t_2\sigma_2^2\geq 0 \qquad (18c)$$

- Where $g_i=\widetilde{\mathbf{A}}_0\mathbf{x}_i$ and $\mathbf{W}_i=\left(\widetilde{\mathbf{A}}_0-\sum_{k=1}^{2}\lambda_k^i\widetilde{\mathbf{A}}_k\right)$

SQP Algorithm with inequality constraints

1) Set the initial value of $\mathbf{x}_1$ and Lagrange multipliers $\lambda_k^1 \geq 0$, $k = 1, 2$, the algorithm terminated threshold δ_1 as $\delta_1 = 1E - 4$, the maximum inner iteration number T^{inner}, and $i = 1$.
2) Begin iteration:
   2.1) Solve (18) with active-set method, and obtain the optimal search direction $\mathbf{p}_i$ as well as Lagrange multipliers estimation λ_1^i, λ_2^i.
   2.2) Update $\mathbf{x}_i = \mathbf{x}_i + \mathbf{p}_i$, Lagrange multiplier λ_1^i and λ_2^i, and set $i = i + 1$.
   2.3) Calculate the value of objective function with $\mathbf{x}_i$, λ_1^i and λ_2^i, at the ith iteration, denoted as $f^i(\mathbf{x}, \lambda_1^i, \lambda_2^i)$.
   2.4) If $|f^i(\mathbf{x}, \lambda_1, \lambda_2) - f^{i+1}(\mathbf{x}, \lambda_1, \lambda_2)| < \delta$, stop and output $\mathbf{x}$. If $i > T^{inner}$, stop and no feasible solution is found, else continue the iteration.

Optimization of Transmit Powers

- When w is fixed, the corresponding problem:

$$\min_{\substack{P_1>0\\P_2>0}} \quad f(P_1,P_2)=P_1s_1+P_2s_2 \tag{19a}$$

$$\text{s.t.} \quad \frac{2^{2r_1}|g_2|^2}{(P_1|g_1|^2+\sigma_{e,1}^2)d_1}+\frac{2^{2r_1}-1}{P_2d_1}=1, \tag{19b}$$

$$\frac{2^{2r_2}|g_1|^2}{(P_2|g_2|^2+\sigma_{e,1}^2)d_2}+\frac{2^{2r_2}-1}{P_1d_2}\leq 1, \tag{19c}$$

where $s_k=(1+\mathbf{w}^H\mathbf{D}_k\mathbf{w})$ and $d_k=\frac{\mathbf{w}^H\mathbf{R}_k\mathbf{w}}{\sigma_k^2+\sigma_r^2\mathbf{w}^H\mathbf{D}_k\mathbf{w}}$, $k=1,2$.

- Substitute the equality constraint (19b) into (19a) and (19c), then

$$\min_{P_1>0} \quad f(P_1) = P_1 s_1 + b_1 s_2 + \frac{b_1 a_1 s_2}{P_1 |g_1|^2 + \sigma_{E,1}^2 - a_1} \tag{20a}$$

$$s.t. \quad c_2 P_1^2 + c_1 P_1 + c_0 \geq 0 \tag{20b}$$

$$P_1 > P_1^B = \max\left(\frac{a_1 - \sigma_{E,1}^2}{|g_1|^2}, 0 \right) \tag{20c}$$

where

$$\left. \begin{aligned} c_2 &= |g_1|^2 |g_2|^2 b_1 + \sigma_{E,1}^2 |g_1|^2 - a_2 |g_1|^2 \\ c_1 &= |g_2| b_1 \sigma_{E,1}^2 + \sigma_{E,1}^2 \left(\sigma_{E,1}^2 - a_1 \right) \end{aligned} \right\} \tag{21}$$

$$\left. \begin{aligned} c_0 &= -b_2 b_1 |g_2|^2 \sigma_{E,1}^2 - b_2 \sigma_{E,1}^2 \left(\sigma_{E,1}^2 - a_1 \right) \\ a_1 &= \frac{2^{2r_1} |g_2|^2}{d_1}, a_2 = \frac{2^{2r_2} |g_1|^2}{d_2} \\ b_1 &= \frac{\left(2^{2r_1} - 1\right)}{d_1}, b_2 = \frac{\left(2^{2r_2} - 1\right)}{d_2} \end{aligned} \right\} \tag{22}$$

Secrecy sum rate maximization(SSRM)

- The SSRM problem:

$$\max_{\substack{P_1>0,P_2>0\\ \mathbf{w}\in C^{N\times 1}}} \frac{(1+\gamma_1)(1+\gamma_2)}{1+\frac{P_1|g_1|^2+P_2|g_2|^2}{\sigma_{E,1}^2}} \qquad (27a)$$

$$s.t. \quad P_1+P_2+P_R \le P_T \qquad (27b)$$

- Utilizing $\mathbf{w}=\mathbf{G}\mathbf{c}$, the problem to optimize vector $\mathbf{w}$ with P1 and P2 fixed:

$$\max_{\mathbf{c}\in C^{(N-2)\times 1}} \frac{\mathbf{c}^H\mathbf{P}_1\mathbf{c}+\sigma_1^2}{\mathbf{c}^H\mathbf{Q}_1\mathbf{c}+\sigma_1^2}\cdot\frac{\mathbf{c}^H\mathbf{P}_2\mathbf{c}+\sigma_2^2}{\mathbf{c}^H\mathbf{Q}_2\mathbf{c}+\sigma_2^2} \qquad (28a)$$

$$s.t. \quad \mathbf{c}^H\mathbf{A}_0\mathbf{c} \le P_T-P_1-P_2 \qquad (28b)$$

where $\mathbf{P}_1=\mathbf{G}^H\left(\sigma_R^2\mathbf{D}_1+P_2\mathbf{R}_1\right)\mathbf{G}$, $\mathbf{P}_2=\mathbf{G}^H\left(\sigma_R^2\mathbf{D}_2+P_1\mathbf{R}_2\right)\mathbf{G}$,

$\mathbf{Q}_1=\sigma_R^2\mathbf{G}^H\mathbf{D}_1\mathbf{G}$, $\mathbf{Q}_2=\sigma_R^2\mathbf{G}^H\mathbf{D}_2\mathbf{G}$

- Define $\mathbf{c} = \mathbf{A}_0^{-\frac{1}{2}} \tilde{\mathbf{c}}$, then

$$\max_{\tilde{\mathbf{c}} \in C^{(N-2)\times 1}} \quad \frac{\tilde{\mathbf{c}}^H \tilde{\mathbf{P}}_1 \tilde{\mathbf{c}} + \sigma_1^2}{\tilde{\mathbf{c}}^H \tilde{\mathbf{Q}}_1 \tilde{\mathbf{c}} + \sigma_1^2} \cdot \frac{\tilde{\mathbf{c}}^H \tilde{\mathbf{P}}_2 \tilde{\mathbf{c}} + \sigma_2^2}{\tilde{\mathbf{c}}^H \tilde{\mathbf{Q}}_2 \tilde{\mathbf{c}} + \sigma_2^2} \qquad (29a)$$

$$s.t. \quad \tilde{\mathbf{c}}^H \tilde{\mathbf{c}} \le P_T - P_1 - P_2 \qquad (29b)$$

Here,

$$\tilde{\mathbf{P}}_k = \left(\mathbf{A}_0^{-\frac{1}{2}}\right)^H \mathbf{P}_k \mathbf{A}_0^{-\frac{1}{2}}, \ \tilde{\mathbf{Q}}_k = \left(\mathbf{A}_0^{-\frac{1}{2}}\right)^H \mathbf{Q}_k \mathbf{A}_0^{-\frac{1}{2}}, k = 1, 2.$$

Substituting the equality $\tilde{\mathbf{c}}^H \tilde{\mathbf{c}} = P_T - P_1 - P$ into (29a),here, we introduce an new variable $\tilde{\mathbf{C}} = \tilde{\mathbf{c}}\tilde{\mathbf{c}}^H$ then

$$\frac{\tilde{\mathbf{c}}^H \hat{\mathbf{P}}_1 \tilde{\mathbf{c}}}{\tilde{\mathbf{c}}^H \hat{\mathbf{Q}}_1 \tilde{\mathbf{c}}} \cdot \frac{\tilde{\mathbf{c}}^H \hat{\mathbf{P}}_2 \tilde{\mathbf{c}}}{\tilde{\mathbf{c}}^H \hat{\mathbf{Q}}_2 \tilde{\mathbf{c}}} \overset{(a)}{=} \frac{Tr\left(\tilde{\mathbf{C}}\hat{\mathbf{P}}_1\tilde{\mathbf{C}}^H\hat{\mathbf{P}}_2\right)}{Tr\left(\tilde{\mathbf{C}}\hat{\mathbf{Q}}_1\tilde{\mathbf{C}}^H\hat{\mathbf{Q}}_2\right)}$$

Step (b) follows from

$Tr\left(\mathbf{ABA}^H\mathbf{C}\right) = \left(vec\left(\mathbf{A}\right)\right)^H \left(\mathbf{B}^T \otimes \mathbf{C}\right) vec\left(\mathbf{A}\right)$

for any matrix A,B and C.

$$\overset{(b)}{=} \frac{\left(vec\left(\tilde{\mathbf{C}}\right)\right)^H \left(\hat{\mathbf{P}}_1^T \otimes \hat{\mathbf{P}}_2\right) vec\left(\tilde{\mathbf{C}}\right)}{\left(vec\left(\tilde{\mathbf{C}}\right)\right)^H \left(\hat{\mathbf{Q}}_1^T \otimes \hat{\mathbf{Q}}_2\right) vec\left(\tilde{\mathbf{C}}\right)} \qquad (30)$$

where

$$\hat{\mathbf{P}}_k = \tilde{\mathbf{P}}_k + \frac{\sigma_k^2}{P_T - P_1 - P_2}\mathbf{I}_{(N-2)} \qquad (31)$$

$$\hat{\mathbf{Q}}_k = \tilde{\mathbf{Q}}_k + \frac{\sigma_k^2}{P_T - P_1 - P_2}\mathbf{I}_{(N-2)}, k = 1,2 \qquad (32)$$

Define $\mathbf{x} = vec\left(\widetilde{\mathbf{C}}\right)$, we can get the following problem as:

$$\max_{\tilde{\mathbf{c}} \in C^{(N-2)\times 1}} \quad f\left(\mathbf{x}\right) = \frac{\mathbf{x}^H \left(\widehat{\mathbf{P}}_1^T \otimes \widehat{\mathbf{P}}_2\right)\mathbf{x}}{\mathbf{x}^H \left(\widehat{\mathbf{Q}}_1^T \otimes \widehat{\mathbf{Q}}_2\right)\mathbf{x}} \qquad (33a)$$

$$s.t. \quad \mathbf{x}^H \mathbf{x} = 1 \qquad (33b)$$

$$vec^{-1}\left(\mathbf{x}\right) \succ 0, rank\left(vec^{-1}\left(\mathbf{x}\right)\right) = 1 \qquad (33c)$$

If the solution is Hermitian matrix, then the solution is exactly the optimal point:

$$\mathbf{x}_{opt} = V_{\max}\left(\left(\widehat{\mathbf{Q}}_1^T \otimes \widehat{\mathbf{Q}}_2\right)^{-1}\left(\widehat{\mathbf{P}}_1^T \otimes \widehat{\mathbf{P}}_2\right)\right) \qquad (34)$$

$$\mathbf{w} = \sqrt{P_T - P_1 - P_2}\,\mathbf{G}\mathbf{A}_0^{-\frac{1}{2}}\hat{\mathbf{c}} \qquad (35)$$

If the solution is not Hermitian matrix with rank one, then choose $\mathbf{X}_l = vec^{-1}\left(\mathbf{x}_{opt}\right)\Phi_l$, where Φ_l is i.i.d zero-mean complex Gaussian random matrix with covariance matrix $\mathbf{I}_{(N-2)}$.

Subalgorithm B: Construction Algorithm Around $\mathbf{x}_{opt}$

1) Calculate the eigen-decomposition of $\mathbf{X}_l = \mathbf{U}\Sigma\mathbf{U}^{-1}$, and choose $\tilde{\mathbf{x}}_l = \mathrm{V}_{max}(\mathbf{X}_l)$.
2) Define $\tilde{\mathbf{X}}_l = \tilde{\mathbf{x}}_l\tilde{\mathbf{x}}_l^H$, and $\hat{\mathbf{x}}_l = \mathrm{vec}(\tilde{\mathbf{X}}_l) \in C^{(N-2)^2\times 1}$.

Optimization of Transmit Power

- When w is fixed, the equivalent problem:

$$\max_{\substack{P_1>0\\P_2>0}} \quad \log_2\left(\left(1+P_2 d_1\right)\left(1+P_1 d_2\right)\right)-\log_2\left(1+\frac{P_1\left|g_1\right|^2+P_2\left|g_2\right|^2}{\sigma_{E,1}^2}\right) \qquad (36a)$$

$$s.t. \quad P_1 s_1+P_2 s_2 \le P_T-\sigma_R^2 \mathbf{w}^H \mathbf{w} \qquad (36b)$$

where $s_k=\left(1+\mathbf{w}^H \mathbf{D}_k \mathbf{w}\right)$ and $d_k=\dfrac{\mathbf{w}^H \mathbf{R}_k \mathbf{w}}{\sigma_k^2+\sigma_r^2 \mathbf{w}^H \mathbf{D}_k \mathbf{w}}, k=1,2$

- Substituting $P_2 = \left(P_T - \sigma_R^2 \mathbf{w}^H \mathbf{w} - P_1 s_1\right) / s_2$ into (36a),thus

$$\max_{P_1} \quad f\left(P_1\right) = \frac{e_2 P_1^2 + e_1 P_1 + e_0}{a_1 P_1 + a_0} \qquad (40a)$$

$$s.t. \quad P_1^L < P_1 < P_1^U \qquad (40b)$$

where $P_1^L = \max\left(0, \frac{\left|g_2\right|^2 - d_1 \sigma_{E,1}^2}{\left|g_1\right|^2 d_1}\right)$ (41)

$$P_1^U = \frac{P_T - \sigma_R^2 \mathbf{w}^H \mathbf{w}}{s_1} - \max\left(0, \frac{s_2\left(\left|g_1\right|^2 - d_2 \sigma_{E,1}^2\right)}{s_1 \left|g_2\right|^2 d_2}\right) \qquad (42)$$

$$\left.\begin{array}{c} e_2 = -\sigma_{E,1}^2 s_1 d_1 d_2 \\ e_1 = \sigma_{E,1}^2\left(s_2 d_2 - s_1 d_1\right) + \left(P_T - \sigma_R^2 \mathbf{w}^H \mathbf{w}\right) d_1 d_2 \sigma_{E,1}^2 \\ e_0 = \sigma_{E,1}^2\left(s_2 + \left(P_T - \sigma_R^2 \mathbf{w}^H \mathbf{w}\right)\right) \end{array}\right\} (38) \qquad \left.\begin{array}{c} a_1 = s_2 \left|g_1\right|^2 - s_1 \left|g_2\right|^2 \\ a_0 = s_2 \sigma_{E,1}^2 + \left(P_T - \sigma_R^2 \mathbf{w}^H \mathbf{w}\right) \end{array}\right\} (39)$$

Minimum per-user secrecy rate maximization(MPSRM)

- The MPSRM problem:

$$\max_{\substack{P_1>0,P_2>0\\ \mathbf{w}\in C^{N\times 1}}} \min\left(\frac{1+\gamma_1}{1+\frac{P_2|g_2|^2}{P_1|g_1|^2+\sigma_{E,1}^2}},\frac{1+\gamma_2}{1+\frac{P_1|g_1|^2}{P_2|g_2|^2+\sigma_{E,1}^2}}\right) \quad (43a)$$

$$s.t. \quad P_1+P_2+P_R\le P_T \quad (43b)$$

Optimization of relay beamforming vector

- Let $$t=\min\left(\frac{1+\gamma_1}{1+\frac{P_2|g_2|^2}{P_1|g_1|^2+\sigma_{E,1}^2}},\frac{1+\gamma_2}{1+\frac{P_1|g_1|^2}{P_2|g_2|^2+\sigma_{E,1}^2}}\right) \qquad (44)$$
- The problem (43) with P1,P2 fixed:

$$\max_{\mathbf{c}\in C^{(N-2)\times 1}} \quad t \qquad (45a)$$
$$s.t. \quad Tr(\mathbf{G}_1\mathbf{C})\ge\sigma_1^2(t_3-1) \qquad (45b)$$
$$Tr(\mathbf{G}_2\mathbf{C})\ge\sigma_2^2(t_4-1) \qquad (45c)$$
$$Tr(\mathbf{A}_0\mathbf{C})\le P_T-P_1-P_2 \qquad (45d)$$

- Here, $t_3=t\left(1+\frac{P_2|g_2|^2}{P_1|g_1|^2+\sigma_{E,1}^2}\right)$, $t_4=t\left(1+\frac{P_1|g_1|^2}{P_2|g_2|^2+\sigma_{E,1}^2}\right)$,

$\mathbf{G}_1=\mathbf{G}^H\left(P_2\mathbf{R}_1+(1-t_3)\sigma_R^2\mathbf{D}_1\right)\mathbf{G}$, $\mathbf{G}_2=\mathbf{G}^H\left(P_1\mathbf{R}_2+(1-t_4)\sigma_R^2\mathbf{D}_2\right)\mathbf{G}$

Actually, for any fixed t, the set of feasible $\mathbf{C}$ in (45) is convex [45]. Let t^* be the maximum value obtained by solving problem (45). For a given value of t, we need to solve the following feasibility problem as:

$$
\begin{aligned}
\text{Find} \quad & \mathbf{C} && \text{(46a)} \\
s.t. \quad & \mathrm{Tr}(\mathbf{G}_1\mathbf{C}) \geq \sigma_1^2(t_3 - 1), && \text{(46b)} \\
& \mathrm{Tr}(\mathbf{G}_2\mathbf{C}) \geq \sigma_2^2(t_4 - 1), && \text{(46c)} \\
& \mathrm{Tr}(\mathbf{A}_0\mathbf{C}) \leq P_T - P_1 - P_2. && \text{(46d)}
\end{aligned}
$$

If it is feasible, we have $t \leq t^*$. Otherwise, we have $t > t^*$. We apply the bisection search algorithm over t to solve (46) at each step with SDP method

Subalgorithm C: Bisection Search Algorithm

Define an interval $[1, \bar{t}]$ known to contain the optimal value t^*, and the algorithm terminated threshold δ_3 as $\delta_3 = 1E - 4$.

1) Initial $t_{min} = 1$, $t_{max} = \bar{t}$.
2) Set $t = \frac{1}{2}(t_{min} + t_{max})$.
3) Solve the problem (46) with given t.
4) Update t by the bisection search algorithm
    4.1) If problem (46) is feasible: $t_{min} = t$.
    4.2) If problem (46) is infeasible: $t_{max} = t$.
5) Until $t_{max} - t_{min} < \delta_3$. Then the converged t_{min} is the optimal solution of problem (45), and obtain the corresponding beamforming vector $\mathbf{w}$.

Optimization of transmit power

- While w is fixed, the MPSRM problem with respect to two sources power P1 and P2:

$$\max_{\substack{P_1>0\\P_2>0}} \quad \min\left(\frac{1+P_2 d_1}{1+\dfrac{P_2\left|g_2\right|^2}{P_1\left|g_1\right|^2+\sigma_{E,1}^2}},\frac{1+P_1 d_2}{1+\dfrac{P_1\left|g_1\right|^2}{P_2\left|g_2\right|^2+\sigma_{E,1}^2}}\right) \qquad (47a)$$

$$s.t. \quad P_1 s_1 + P_2 s_2 \le P_T - \sigma_R^2 \mathbf{w}^H \mathbf{w} \qquad (47b)$$

Convergence discussion

Theorem 1: The proposed iterative algorithm based on SDP method for TTPM is convergent.

Proof: Let $s_k(\mathbf{w}(n-1))$ and $d_k(\mathbf{w}(n-1))$, $k=1,2$, denote s_k and d_k defined as based on $\mathbf{w}(n-1)$ in (14), respectively, where $\mathbf{w}(n-1)$ is the solution obtained from (14). Then, $\hat{P}_1(n)$ and $\hat{P}_2(n)$ at the nth iteration are obtained by $\arg\min_{(P_1,P_2)} f(P_1,P_2)$ under the constraint. Then

$$\begin{aligned} I(n) &= \hat{P}_1(n) + \hat{P}_2(n) + P_R(\mathbf{w}(n-1)) \\ &\geq \hat{P}_1(n) + \hat{P}_2(n) + P_R(\mathbf{w}(n)). \end{aligned} \tag{48}$$

The inequality (48) holds on because $\mathbf{w}(n)$ is the rank-one solution of (14), which is optimal for the given $\hat{P}_1(n)$ and $\hat{P}_2(n)$. Since $(\hat{P}_1(n+1), \hat{P}_2(n+1)) = \arg\min_{(P_1,P_2)} f(P_1,P_2)$, then,

$$\begin{aligned} I(n+1) &= \hat{P}_1(n+1) + \hat{P}_2(n+1) + P_R(\mathbf{w}(n)) \\ &\leq \hat{P}_1(n) + \hat{P}_2(n) + P_R(\mathbf{w}(n)). \end{aligned} \tag{49}$$

Outline

- Background knowledge
- Abstract
- Introduction
- System model
- Simulation results
- Conclusions
- Future work

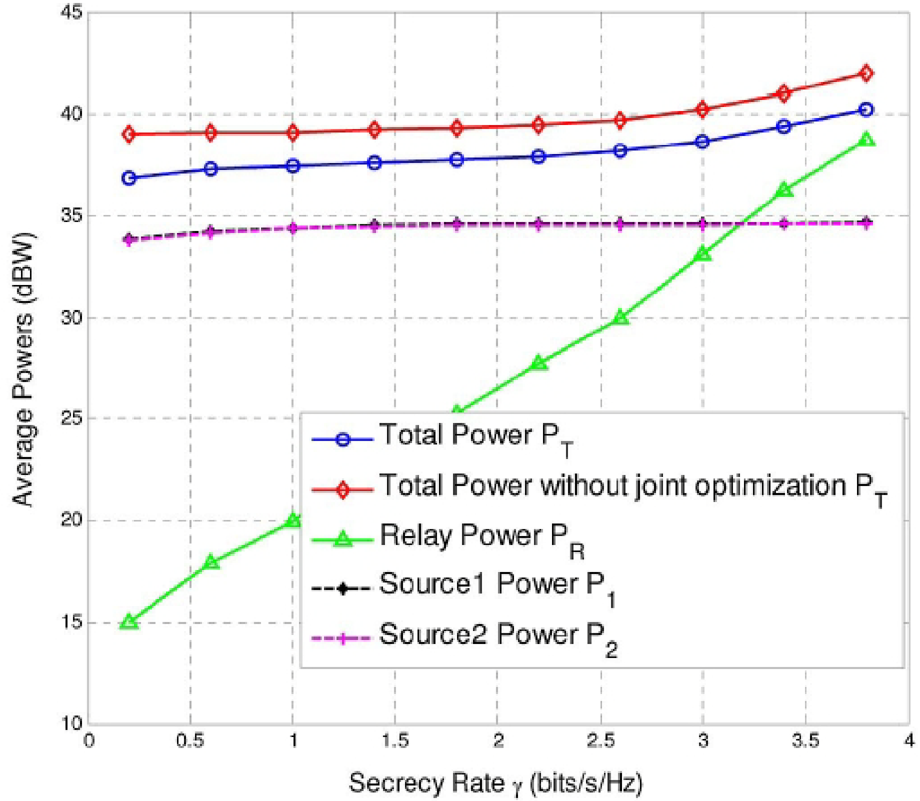


Fig. 2. The average minimum power for relay, two sources achieved by iterative algorithm with SDP method versus secrecy rate r, $N = 4$, $\sigma_{f_1}^2 = \sigma_{f_2}^2 = 0$ dB, $\sigma_{g_1}^2 = \sigma_{g_2}^2 = 0$ dB.

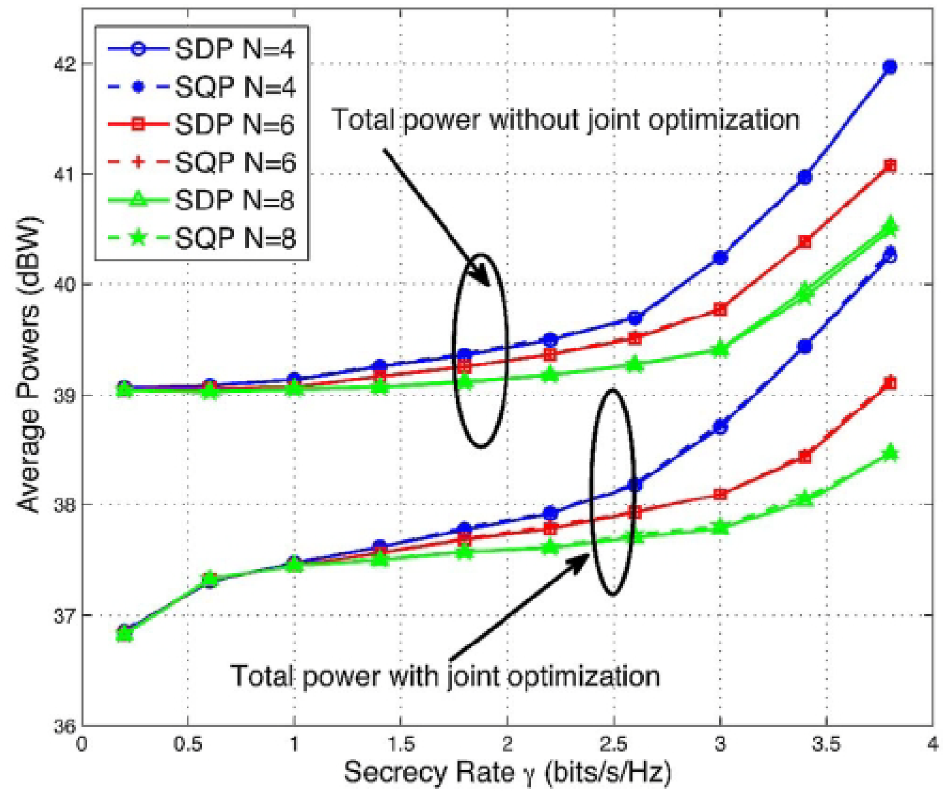


Fig. 3. Total power with or without joint optimization achieved by SDP and SQP methods versus secrecy rate r, $N = 4$, 6 and 8, $\sigma_{f_1}^2 = \sigma_{f_2}^2 = 0$ dB, $\sigma_{g_1}^2 = \sigma_{g_2}^2 = 0$ dB.

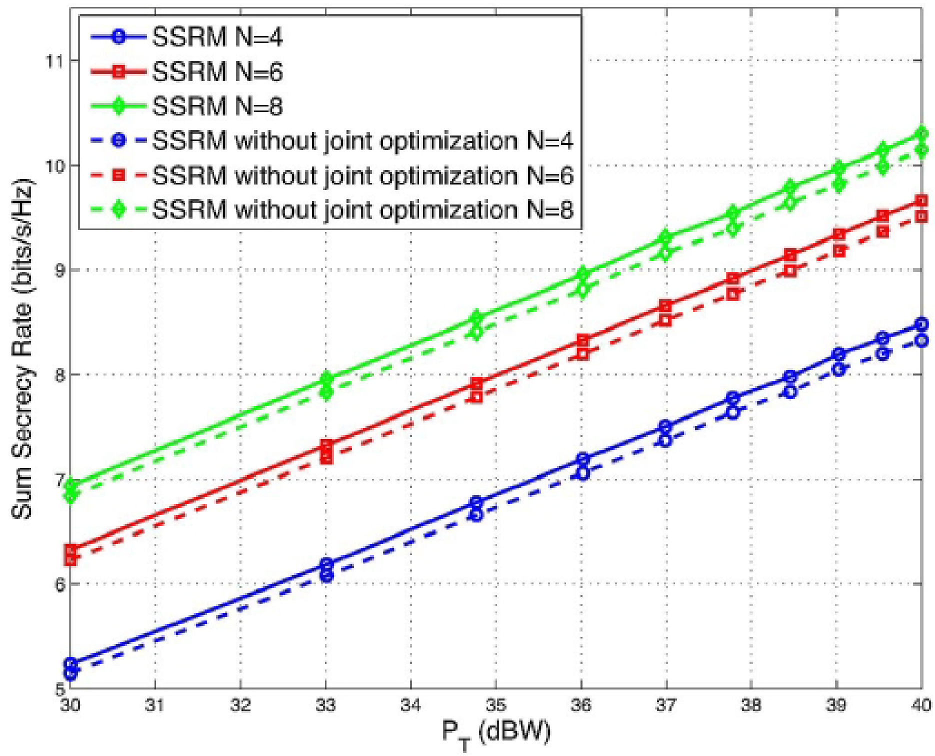
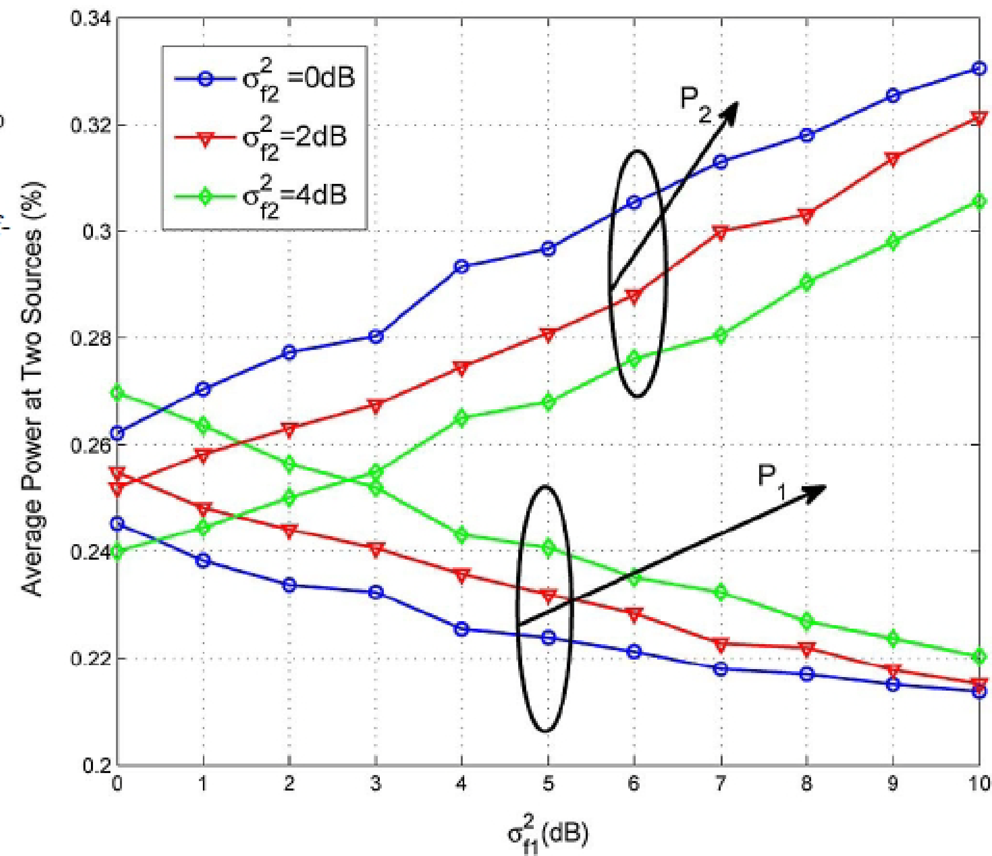


Fig. 6. The secrecy sum rate achieved by SSRM approach versus P_T for different number of relay, $\sigma_{f_1}^2 = \sigma_{f_2}^2 = 0$ dB, $\sigma_{g_1}^2 = \sigma_{g_2}^2 = 0$ dB.



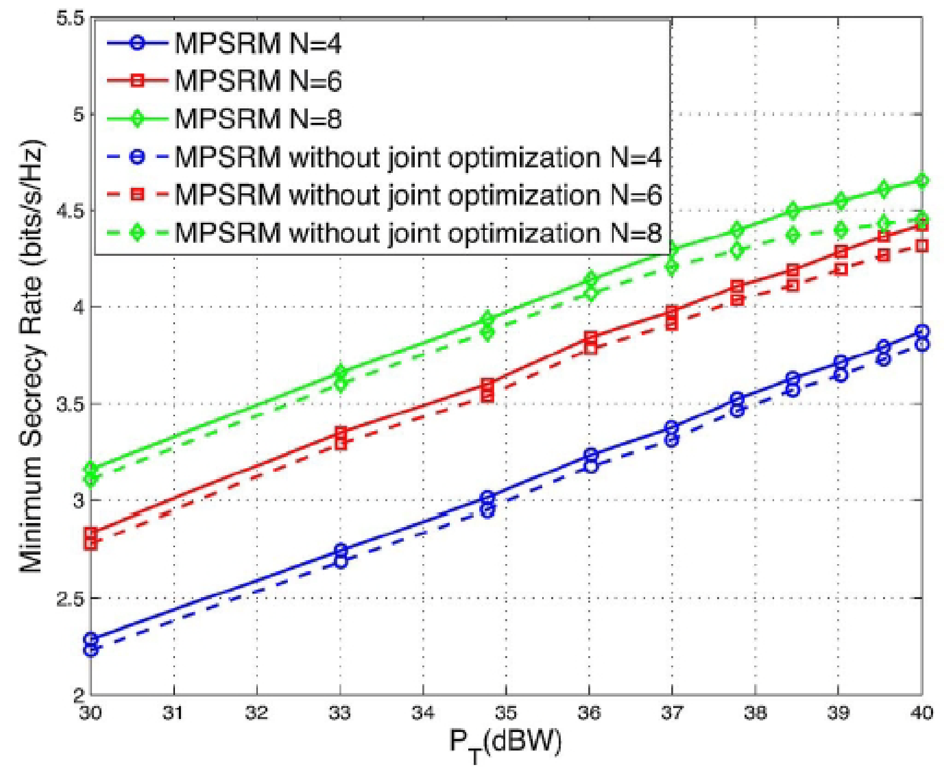


Fig. 9. The secrecy sum rate achieved by MPSRM approach versus P_T for different number of relay, $\sigma_{f_1}^2 = \sigma_{f_2}^2 = 0$ dB.

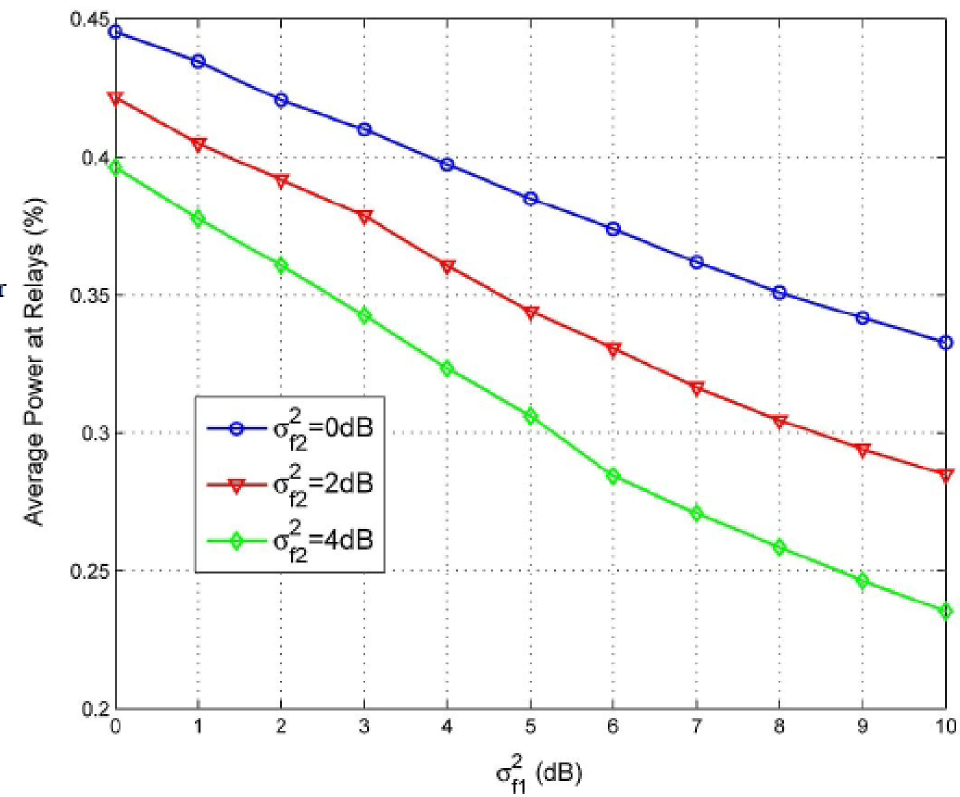


Fig. 10. The power allocation P_R at all relays achieved by MPSRM approach versus $\sigma_{f_1}^2$ with $\sigma_{f_2}^2 = 0, 2$ and 4 dB, $N = 6$ and $P_T = 40$ dBW.

Outline

- Background knowledge
- Abstract
- Introduction
- System model
- Simulation results
- Conclusions
- Future work

Conclusions

Three approaches are proposed to optimize null space beamforming vector and two sources' transmit power in an alternating iterative way. All these approaches, two subproblem are formulated to solve beamforming vector and sources' power in each iteration.

Outline

- Background knowledge
- Abstract
- Introduction
- System model
- Simulation results
- Conclusions
- Future work

Future work

- MIMO full-duplex +two way relay+ eavesdropper

其中，$\mathbf{h}_A = \mathbf{H}_A \mathbf{t}, \mathbf{h}_B = \mathbf{H}_B^H \mathbf{r}, \mathbf{W} = \mathbf{w}_t \mathbf{w}_r^H$

$$\begin{cases} \mathbf{y}_R(n) = \mathbf{H}_A \mathbf{t} x_A(n) + \mathbf{H}_R x_R(n) + \mathbf{n}_R(n) \\ x_R(n) = \mathbf{W}\mathbf{y}_R(n-\tau) \end{cases}$$

$$\Downarrow$$

$$x_R(n) = \mathbf{W}\mathbf{h}_A x_A(n-\tau) + \mathbf{W}\mathbf{H}_R x_R(n-\tau) + \mathbf{W}\mathbf{n}_R(n)$$

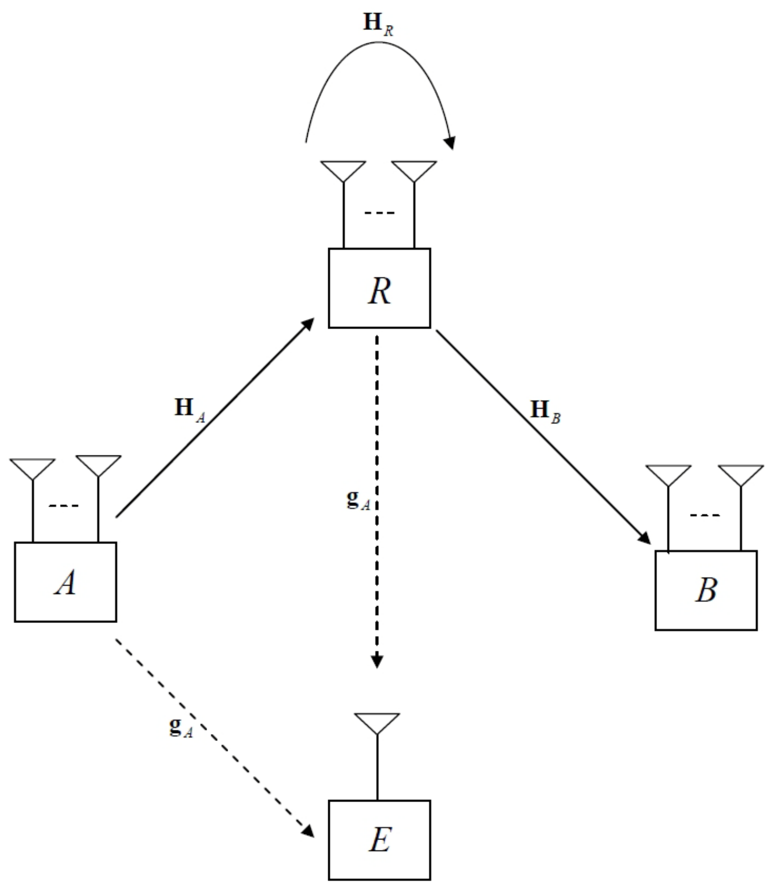
$$I_B = \log_2\left(1 + \frac{P_x \left\|\mathbf{h}_B^H \mathbf{W}\mathbf{h}_A\right\|^2}{1 + \left\|\mathbf{h}_B^H \mathbf{W}\right\|^2}\right)$$

$$I(x_A; y_E) = \log_2\left(1 + \frac{P_s\left(\left\|\mathbf{g}_A \mathbf{t}\right\|^2 + \left\|\mathbf{g}_R \mathbf{W}\mathbf{h}_A\right\|^2\right)}{2 + \left\|\mathbf{g}_R \mathbf{W}\right\|^2}\right)$$

$$\max_{\mathbf{W},\mathbf{t},\mathbf{r}} C_S = \left[I_B - I(x_A; y_E)\right]^+$$

$$s.t.\ \mathbf{W}\mathbf{H}_R\mathbf{W} = 0,$$

$$P_S\left\|\mathbf{W}\mathbf{h}_A\right\|^2 + \left\|\mathbf{W}\right\|^2 \le P_R$$



Future work

- MIMO + two way + eavesdropper

$$phase\,1:\ \mathbf{y}_R = \mathbf{H}_A\mathbf{q}_A s_A + \mathbf{H}_B\mathbf{q}_B s_B + \mathbf{n}_R$$

$$y_E^1 = \mathbf{g}_A\mathbf{q}_A s_A + \mathbf{g}_B\mathbf{q}_B s_B + n_1$$

$$phase\,2:\ \mathbf{y}_A = \mathbf{H}_A^T\mathbf{F}\mathbf{y}_R + \mathbf{n}_A$$

$$\mathbf{y}_B = \mathbf{H}_B^T\mathbf{F}\mathbf{y}_R + \mathbf{n}_B$$

$$y_E^2 = \mathbf{g}_R\mathbf{F}\mathbf{y}_R + n_2$$

$assume\ perfect\ self-interference:$

$$\mathbf{y}_A = \mathbf{H}_A^T\mathbf{F}\mathbf{H}_B\mathbf{q}_B s_B + \mathbf{H}_A^T\mathbf{F}\mathbf{n}_R + \mathbf{n}_A$$

$$\mathbf{y}_B = \mathbf{H}_B^T\mathbf{F}\mathbf{H}_A\mathbf{q}_A s_A + \mathbf{H}_B^T\mathbf{F}\mathbf{n}_R + \mathbf{n}_B$$

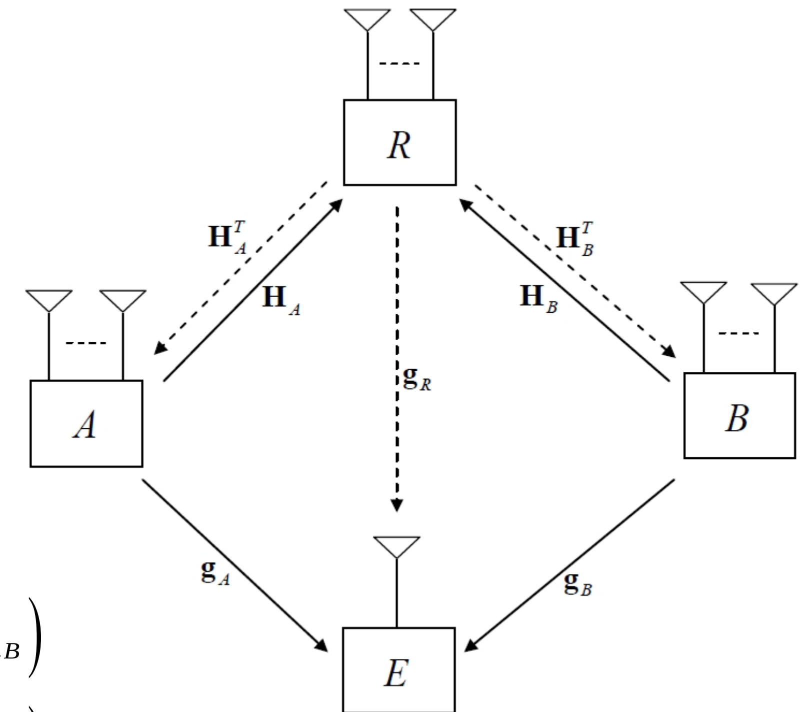
$$\begin{pmatrix} y_E^1 \\ y_E^2 \end{pmatrix} = \begin{pmatrix} \mathbf{g}_A\mathbf{q}_A & \mathbf{g}_B\mathbf{q}_B \\ \mathbf{g}_R\mathbf{F}\mathbf{H}_A\mathbf{q}_A & \mathbf{g}_R\mathbf{F}\mathbf{H}_B\mathbf{q}_B \end{pmatrix}\begin{pmatrix} s_A \\ s_B \end{pmatrix} + \begin{pmatrix} n_1 \\ \mathbf{g}_R\mathbf{F}\mathbf{n}_R + n_2 \end{pmatrix}$$

$$R_A = \frac{1}{2}\log_2\left(1 + \mathbf{q}_B^H\mathbf{H}_B^H\mathbf{F}^H\mathbf{H}_A^*\left(\mathbf{I} + \mathbf{H}_A^T\mathbf{F}\mathbf{F}^H\mathbf{H}_A^*\right)^{-1}\mathbf{H}_A^T\mathbf{F}\mathbf{H}_B\mathbf{q}_B\right)$$

$$R_B = \frac{1}{2}\log_2\left(1 + \mathbf{q}_A^H\mathbf{H}_A^H\mathbf{F}^H\mathbf{H}_B^*\left(\mathbf{I} + \mathbf{H}_B^T\mathbf{F}\mathbf{F}^H\mathbf{H}_B^*\right)^{-1}\mathbf{H}_B^T\mathbf{F}\mathbf{H}_A\mathbf{q}_A\right)$$

$utilize\ ZF, then$

$$R_E = \frac{1}{2}\log_2\left(1 + \mathbf{q}_A^H\mathbf{g}_A^H\mathbf{g}_A\mathbf{q}_A + \mathbf{q}_B^H\mathbf{g}_B^H\mathbf{g}_B\mathbf{q}_B\right)$$



$$\therefore \max_{F,q_A,q_B} R_S = \left[R_A + R_B - R_E\right]^+$$

$$s.t.\ \mathbf{F}\left(\mathbf{H}_A\mathbf{q}_A, \mathbf{H}_B\mathbf{q}_B\right) = 0, \|\mathbf{q}_A\|^2 \le P_A, \|\mathbf{q}_B\|^2 \le P_B,$$

$$Tr\left(\mathbf{F}\mathbf{H}_A\mathbf{q}_A\mathbf{q}_A^H\mathbf{H}_A^H\mathbf{F}^H + \mathbf{F}\mathbf{H}_B\mathbf{q}_B\mathbf{q}_B^H\mathbf{H}_B^H\mathbf{F}^H + \mathbf{F}\mathbf{F}^H\right) \le P_R$$

Thank you!