



(12) 发明专利申请

(10) 申请公布号 CN 103856299 A

(43) 申请公布日 2014. 06. 11

(21) 申请号 201410025414. X

(22) 申请日 2014. 01. 20

(71) 申请人 西安交通大学

地址 710049 陕西省西安市碑林区咸宁西路
28号

(72) 发明人 王慧明 刘峰 殷勤业

(74) 专利代理机构 西安通大专利代理有限责任
公司 61200

代理人 陆万寿

(51) Int. Cl.

H04L 1/06(2006. 01)

H04B 7/15(2006. 01)

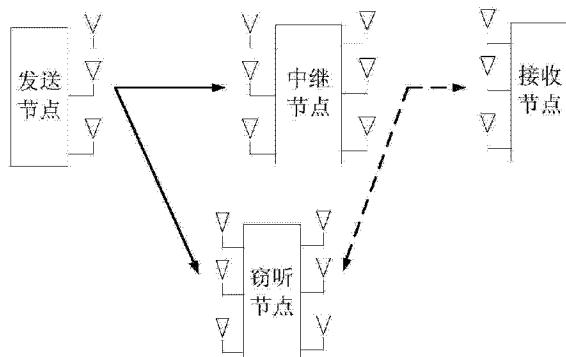
权利要求书4页 说明书9页 附图3页

(54) 发明名称

一种 MIMO 放大转发中继网络的信号安全传
输方法

(57) 摘要

本发明提出了一种 MIMO 放大转发中继网络的信号安全传输方法，在设计预编码矩阵时，采用了 GSVD-ZF-SVD 的联合策略，使得系统并行化，简化了系统安全速率的表达形式，在功率约束的条件下求解一个最优化问题。在进行功率分配的时候，原问题的非凸性使得直接求解很难进行，采用交替迭代优化的方式，每一个子问题都能得到唯一的最优解，并且最终交替迭代能够得到一个收敛点。本发明考虑了发送节点端和中继节点的联合预编码，利用 GSVD-ZF-SVD 方法，将信道并行化，简化了问题的分析难度；并对功率分配进行了优化；计算复杂度较低。



1. 一种MIMO放大转发中继网络的信号安全传输方法,其特征在于,所述MIMO放大转发中继网络包括一个发送节点,一个中继节点,一个窃听节点以及一个接收节点,各个节点都配备有多天线,天线数目分别为 N_A, N_R, N_E, N_B ;

所述信号安全传输方法包括以下步骤:

1) 第一阶段,发送节点对发送信息进行线性预编码,中继节点和窃听节点接收到发送节点发射的信息分别为: $y_R = H_{AR}Fs + n_R$, $\mathbf{y}_E^{(1)} = \mathbf{H}_{AE}\mathbf{F}s + \mathbf{n}_E^{(1)}$,其中 H_{AR}, H_{AE} 是发送节点到中继节点和窃听节点的信道矩阵, F 是发送节点线性预编码矩阵, s 是发送节点发射信息矢量,协方差矩阵为 $\sigma_s^2\mathbf{I}$, $n_R, \mathbf{n}_E^{(1)}$ 是加性高斯噪声矢量,协方差矩阵为 $\sigma_n^2\mathbf{I}$, $y_R, \mathbf{y}_E^{(1)}$ 是接收矢量;

2) 第二阶段,中继节点将接收到的信号,进行放大转发,预编码矩阵为 W ,接收节点和窃听节点接收到的信息分别为:

$$y_B = H_{RB}WH_{AR}Fs + H_{RB}Wn_R + n_B, \quad \mathbf{y}_E^{(2)} = \mathbf{H}_{RE}\mathbf{W}\mathbf{H}_{AR}\mathbf{F}s + \mathbf{H}_{RE}\mathbf{W}\mathbf{n}_R + \mathbf{n}_E^{(2)}.$$

其中 H_{RB}, H_{RE} 是中继节点到接收节点和窃听节点的信道矩阵, $n_B, \mathbf{n}_E^{(2)}$ 是加性高斯白噪声,协方差矩阵为 $\sigma_n^2\mathbf{I}$, $y_B, \mathbf{y}_E^{(2)}$ 是接收矢量;

等效的窃听节点接收信息为:

$$\mathbf{y}_E = \begin{bmatrix} \mathbf{y}_E^{(1)} \\ \mathbf{y}_E^{(2)} \end{bmatrix} = \mathbf{H}_E\mathbf{s} + \mathbf{n}_E, \quad \mathbf{H}_E = \begin{bmatrix} \mathbf{H}_{AE}\mathbf{F} \\ \mathbf{H}_{RE}\mathbf{W}\mathbf{H}_{AR}\mathbf{F} \end{bmatrix}, \quad \mathbf{n}_E = \begin{bmatrix} \mathbf{n}_E^{(1)} \\ \mathbf{H}_{RE}\mathbf{W}\mathbf{n}_R + \mathbf{n}_E^{(2)} \end{bmatrix}$$

3) 在功率约束下,最大化安全传输的速率,即最优化功率分配,实现最大的安全速率:

$$R_s = \max(I(y_B; s) - I(y_E; s))^+$$

$$\text{s.t. } \sigma_s^2 \text{tr}(\mathbf{FF}^H) \leq P_1$$

$$\text{tr}(\sigma_s^2 \mathbf{W}\mathbf{H}_{AR}\mathbf{F}\mathbf{F}^H \mathbf{H}_{AR}^H \mathbf{W}^H + \sigma_n^2 \mathbf{W}\mathbf{W}^H) \leq P_2.$$

2. 根据权利要求1所述的一种MIMO放大转发中继网络的信号安全传输方法,其特征在于,得到发送节点和中继节点的预编码矩阵的步骤包括:

首先对信道矩阵 H_{AR}, H_{AE} 进行广义奇异值分解得到:

$$H_{AR} = U \Lambda_{AR} \Phi$$

$$H_{AE} = V \Lambda_{AE} \Phi$$

其中 $\Phi = R\Psi^H$ 是一个 $N_A \times N_A$ 的非奇异矩阵, U, V 是酉矩阵, Λ_{AR} 和 Λ_{AE} 为:

$$\Lambda_{AR} = \begin{pmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{D}_{AR} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{q \times q} \end{pmatrix}_{N_R \times M}$$

$$\mathbf{A}_{AE} = \begin{pmatrix} \mathbf{D}_{AE} & \mathbf{0} \\ \mathbf{0} & \mathbf{0}_{(N_E-s) \times q} \end{pmatrix}_{N_E \times M}$$

其中 $q+s=N_A$, $K=N_A=M$,

$D_{AR}=\text{diag}(d_{AR,1}, d_{AR,2}, \dots, d_{AR,s})$, $D_{AE}=\text{diag}(d_{AE,1}, d_{AE,2}, \dots, d_{AE,s})$, 其中 $d_{AR,i}$ 升序排列, $d_{AE,i}$ 降序排列 ; 设计发端预编码矩阵为 :

$$\mathbf{F} = \frac{\mathbf{\Psi}\mathbf{R}^{-1}}{\|\mathbf{R}^{-1}\|} \sqrt{\mathbf{P}_a}$$

其中 $\mathbf{P}_a = \text{diag}(\sqrt{p_{a,1}}, \sqrt{p_{a,2}}, \dots, \sqrt{p_{a,K}})$;

设中继节点到合法用户信道矩阵的奇异值分解为 $\mathbf{H}_{RB} = \bar{\mathbf{U}}\Sigma_{RB}\bar{\mathbf{V}}$,

$\Sigma_{RB} = (\mathbf{0} \quad \bar{\Sigma}_{RB})$, $\bar{\Sigma}_{RB} = \text{diag}(\lambda_{RB,1}, \lambda_{RB,2}, \dots, \lambda_{RB,K})$, 设计预编码矩阵 \mathbf{W} 使得窃听节点在第二阶段接收不到任何信息, 即令 $\mathbf{W} = \mathbf{H}_{RE}^\perp \bar{\mathbf{W}}$, \mathbf{H}_{RE}^\perp 是 \mathbf{H}_{RE} 零空间的投影矩阵, 使得 $\mathbf{H}_{RE}\mathbf{W}=0$; 然后利用奇异值分解, 设计中继预编码矩阵为

$$\bar{\mathbf{W}} = \bar{\mathbf{V}} \sqrt{\mathbf{P}_r} \mathbf{U}^H$$

$$\mathbf{W} = \mathbf{H}_{RE}^\perp \bar{\mathbf{V}} \sqrt{\mathbf{P}_r} \mathbf{U}^H$$

其中, $\mathbf{P}_r = \text{diag}(\sqrt{p_{r,1}}, \sqrt{p_{r,2}}, \dots, \sqrt{p_{r,K}})$; 这样就完成了发送节点和中继节点的预编码矩阵的设计。

3. 根据权利要求 1 所述的一种 MIMO 放大转发中继网络的信号安全传输方法, 其特征在于, 步骤 3) 中得到安全速率及其功率约束为 :

$$\begin{aligned} \max_{p_{a,k}, p_{r,k}} \quad R_s &= \frac{1}{2} \sum_{k=1}^K \left[\log \left(1 + \frac{\bar{\rho} p_{r,k} p_{a,k} \lambda_{RB,k}^2 \bar{d}_{AR,k}^2}{1 + p_{r,k} \lambda_{RB,k}^2} \right) - \log \left(1 + \bar{\rho} p_{a,k} \bar{d}_{AE,k}^2 \right) \right] \\ \text{s.t.} \quad P_A &= \sigma_s^2 \sum_{k=1}^K p_{a,k} \leq P_1 \\ P_R &= \sigma_n^2 \sum_{k=1}^K \left(\bar{\rho} p_{r,k} p_{a,k} \bar{d}_{AR,k}^2 + p_{r,k} \right) \leq P_2 \end{aligned}$$

其中 P_1, P_2 分别是发送节点和中继节点的总功率,

$$\bar{\rho} = \sigma_s^2 / \sigma_n^2 \|\mathbf{R}^{-1}\|^2, \quad \bar{\mathbf{D}}_{AR} = \text{diag}(d_{AR,1}, d_{AR,2}, \dots, d_{AR,s}, 1, \dots, 1),$$

$\bar{\mathbf{D}}_{AE} = \text{diag}(d_{AE,1}, d_{AE,2}, \dots, d_{AE,s}, 0, \dots, 0)$ $\bar{d}_{AR,k}, \bar{d}_{AE,k}$ 分别是 $\bar{\mathbf{D}}_{AR}, \bar{\mathbf{D}}_{AE}$ 的第 k 个对角元素。

4. 根据权利要求 3 所述的一种 MIMO 放大转发中继网络的信号安全传输方法，其特征在于，对安全速率及其功率约束采用交替迭代求解的方法；首先进行变量代换 $z_k = p_{a,k}$, $r_k = \bar{\rho} p_{r,k} p_{a,k} \bar{d}_{AR,k}^2 + p_{r,k}$, $\bar{P}_1 = P_1 / \sigma_s^2$, $\bar{P}_2 = P_2 / \sigma_n^2$ ，对上述优化问题进行变形，当给定 z_k ，优化 r_k 得到优化问题为：

$$\begin{aligned} \max_{r_k} \quad & \sum_{k=1}^K \log \left(\frac{1 + \lambda_{RB,k}^2 r_k}{1 + \lambda_{RB,k}^2 r_k + \bar{\rho} \bar{d}_{AR,k}^2 z_k} \right) \\ \text{s.t.} \quad & \sum_{k=1}^K r_k \leq \bar{P}_2, \quad r_k \geq 0, \quad k = 1, 2, \dots, K. \end{aligned}$$

其解为

$$r_k^*(v) = \frac{1}{2\lambda_{RB,k}^2} \left[\sqrt{\left(\bar{\rho} \bar{d}_{AR,k}^2 z_k \right)^2 + 4\bar{\rho} \bar{d}_{AR,k}^2 z_k \lambda_{RB,k}^2 v} - \bar{\rho} \bar{d}_{AR,k}^2 z_k - 2 \right]^+$$

其中 $[x]^+$ 表示取 x 和 0 之间的较大者，变量 v 需要满足下式

$$\sum_{k=1}^K r_k^*(v) = \bar{P}_2$$

当固定 r_k ，优化 z_k ，得到优化问题为

$$\begin{aligned} \max_{z_k} \quad & \sum_{k=1}^K \left[\log \left(\frac{1 + a_k z_k}{1 + b_k + c_k z_k} \right) - \log(1 + c_k z_k) \right] \\ \text{s.t.} \quad & \sum_{k=1}^K z_k \leq \bar{P}_1, \quad z_k \geq 0, \quad k = 1, 2, \dots, K. \end{aligned}$$

5. 根据权利要求 4 所述的一种 MIMO 放大转发中继网络的信号安全传输方法，其特征在于，

当发送节点比窃听节点天线少或相同的情况，解为：

(1) 当 $\sum_{k \in \Omega} \bar{P}_{c,k} \leq \bar{P}_1$ 时，解为 $z_k^* = \begin{cases} \bar{P}_{c,k}, & k \in \Omega \\ 0, & \text{其他} \end{cases}$ ，其中集合 Ω 是所有满足

$$d_k = a_k b_k - b_k c_k - c_k > 0 \text{ 的 } k \text{ 组成的, } \bar{P}_{c,k} = \frac{-2a_k c_k + \sqrt{4a_k^2 c_k^2 + 4a_k^2 c_k d_k}}{2a_k^2 c_k}$$

(2) 当 $\sum_{k \in \Omega} \bar{P}_{c,k} > \bar{P}_1$ 时, 解为 $z_k^* = \begin{cases} \left[\max_i (\gamma_k^{(i)}(\mu)) \right]^+, & k \in \Omega_+ \\ 0, & \text{其他} \end{cases}$, 其中 $\gamma_k^{(i)}(\mu)$ 是 $\ln 2 (1 + a_k z_k) (1 + b_k + a_k z_k) (1 + c_k z_k) \mu + a_k^2 c_k z_k^2 + 2 a_k c_k z_k - d_k = 0$ 的三个解, 并且满足 $\sum_{k=1}^K z_k^* = \bar{P}_1$;

当发送节点比窃听节点天线有更多天线的情况, 解为 :

$$z_k^* = \begin{cases} \left[\max_i (\gamma_k^{(i)}(\mu)) \right]^+, & k \in \Omega_+ \\ \left[\frac{1}{2a_k} \sqrt{(2+b_k) - 4 \left(1+b_k - \frac{a_k b_k}{\mu \ln 2} \right)} - \frac{2+b_k}{2a_k} \right], & k \in \Omega_0 \\ 0, & \text{其他} \end{cases}$$

其中集合 $\Omega_0 = \{k : k \in \Omega, c_k = 0\}$, $\Omega_+ = \{k : k \in \Omega, c_k > 0\}$;

通过交替迭代, 最后结果收敛到一个点处, 即得到功率分配。

一种 MIMO 放大转发中继网络的信号安全传输方法

技术领域

[0001] 本发明属于无线传输技术领域，特别涉及一种 MIMO 放大转发中继网络的信号安全传输方法。

背景技术

[0002] 安全问题是无线通信中的一个基本问题。无线介质的开放性，给安全性带来了更大的挑战。无线通信的物理层安全技术是一项新的无线信号安全传输技术。它不依赖于利用密钥加密来实现数据安全传输，而是通过合理设计信号、分配功率以及调制编码方式，来提高信号传输的安全速率，防止信息被窃听者窃听，从而提升了信息传输的安全。近年来，无线物理层安全得到了学术界的极大关注。

[0003] 多输入多输出(MIMO)技术和中继通信技术是两项提升无线通信的物理层安全的手段。它们都可以通过利用空间自由度，使得信号的设计更加灵活，都能够提升无线传输的安全速率。将两者结合能够进一步提升无线通信的物理层传输安全。但是，对一个 MIMO 中继网络的物理层安全传输信号直接进行最优设计非常困难，无法得到一个有效的结果，因此目前这方面的研究结果较少。

[0004] J. Huang, A. L. Swindlehurst 在 文 献“Cooperative jamming for secure communications in MIMO relay network,”IEEE Trans. Signal Processing, vol. 59, no. 1 0, pp. 4871–4884, Oct. 2011 中考虑了利用中继发射干扰信号实现信号安全传输。但是考虑的是中继采用解码转发的中继方案。解码转发方案要求中继节点对信息进行解码，这使得系统的复杂度增大，同时系统的延时增加，并且在中继节点还必须保证正确解码。

[0005] 刘洋,宋梅,张勇等人在发明专利“基于分层调制的无线中继安全转发方法”中提到了中继安全的问题，但是没有考虑利用 MIMO 技术，另外，发明人考虑的也是在中继节点进行解码。

发明内容

[0006] 本发明的目的在于提供一种 MIMO 放大转发中继网络的信号安全传输方法，以提高通信的安全性；本发明是对 MIMO 中继网络下的无线物理层安全提出一个算法复杂度较低并能够实现较高速率的方法。

[0007] 为了实现上述目的，本发明采用如下技术方案：

[0008] 一种 MIMO 放大转发中继网络的信号安全传输方法，所述 MIMO 放大转发中继网络包括一个发送节点，一个中继节点，一个窃听节点以及一个接收节点，各个节点都配备有多天线，天线数目分别为 N_A, N_R, N_E, N_B ；

[0009] 所述信号安全传输方法包括以下步骤：

[0010] 1) 第一阶段，发送节点对发送信息进行线性预编码，中继节点和窃听节点接收到发送节点发射的信息分别为： $y_R = H_{AR}Fs + n_R$, $\mathbf{y}_E^{(1)} = \mathbf{H}_{AE}\mathbf{F}\mathbf{s} + \mathbf{n}_E^{(1)}$ ，其中 H_{AR}, H_{AE} 是发送节点到中继节点和窃听节点的信道矩阵， F 是发送节点线性预编码矩阵， s 是发送节点发射信息矢

量, 协方差矩阵为 $\sigma_s^2 \mathbf{I}$, \mathbf{n}_R , $\mathbf{n}_E^{(1)}$ 是加性高斯噪声矢量, 协方差矩阵为 $\sigma_n^2 \mathbf{I}$, \mathbf{y}_R , $\mathbf{y}_E^{(1)}$ 是接收矢量;

[0011] 2) 第二阶段, 中继节点将接收到的信号, 进行放大转发, 预编码矩阵为 \mathbf{W} , 接收节点和窃听节点接收到的信息分别为:

$$[0012] \quad \mathbf{y}_B = \mathbf{H}_{RB} \mathbf{W} \mathbf{H}_{AR} \mathbf{F} \mathbf{s} + \mathbf{H}_{RB} \mathbf{W} \mathbf{n}_R + \mathbf{n}_B, \quad \mathbf{y}_E^{(2)} = \mathbf{H}_{RE} \mathbf{W} \mathbf{H}_{AR} \mathbf{F} \mathbf{s} + \mathbf{H}_{RE} \mathbf{W} \mathbf{n}_R + \mathbf{n}_E^{(2)}.$$

[0013] 其中 $\mathbf{H}_{RB}, \mathbf{H}_{RE}$ 是中继节点到接收节点和窃听节点的信道矩阵, \mathbf{n}_B , $\mathbf{n}_E^{(2)}$ 是加性高斯白噪声, 协方差矩阵为 $\sigma_n^2 \mathbf{I}$, \mathbf{y}_B , $\mathbf{y}_E^{(2)}$ 是接收矢量;

[0014] 等效的窃听节点接收信息为:

$$[0015] \quad \mathbf{y}_E = \begin{bmatrix} \mathbf{y}_E^{(1)} \\ \mathbf{y}_E^{(2)} \end{bmatrix} = \mathbf{H}_E \mathbf{s} + \mathbf{n}_E, \quad \mathbf{H}_E = \begin{bmatrix} \mathbf{H}_{AE} \mathbf{F} \\ \mathbf{H}_{RE} \mathbf{W} \mathbf{H}_{AR} \mathbf{F} \end{bmatrix}, \quad \mathbf{n}_E = \begin{bmatrix} \mathbf{n}_E^{(1)} \\ \mathbf{H}_{RE} \mathbf{W} \mathbf{n}_R + \mathbf{n}_E^{(2)} \end{bmatrix}$$

[0016] 3) 在功率约束下, 最大化安全传输的速率, 即最优化功率分配, 实现最大的安全速率:

$$[0017] \quad R_s = \max(I(\mathbf{y}_B; \mathbf{s}) - I(\mathbf{y}_E; \mathbf{s}))^+$$

$$[0018] \quad \text{s.t. } \sigma_s^2 \text{tr}(\mathbf{F} \mathbf{F}^H) \leq P_1$$

$$[0019] \quad \text{tr}(\sigma_s^2 \mathbf{W} \mathbf{H}_{AR} \mathbf{F} \mathbf{F}^H \mathbf{H}_{AR}^H \mathbf{W}^H + \sigma_n^2 \mathbf{W} \mathbf{W}^H) \leq P_2$$

[0020] 本发明进一步的改进在于: 得到发送节点和中继节点的预编码矩阵的步骤包括:

[0021] 首先对信道矩阵 $\mathbf{H}_{AR}, \mathbf{H}_{AE}$ 进行广义奇异值分解得到:

$$[0022] \quad \mathbf{H}_{AR} = \mathbf{U} \Lambda_{AR} \mathbf{\Phi}$$

$$[0023] \quad \mathbf{H}_{AE} = \mathbf{V} \Lambda_{AE} \mathbf{\Phi}$$

[0024] 其中 $\Phi = \mathbf{R} \Psi^H$ 是一个 $N_A \times N_A$ 的非奇异矩阵, \mathbf{U}, \mathbf{V} 是酉矩阵 Λ_{AR} 和 Λ_{AE} 为:

$$[0025] \quad \mathbf{\Lambda}_{AR} = \begin{pmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{D}_{AR} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{q \times q} \end{pmatrix}_{N_R \times M}$$

$$[0026] \quad \mathbf{\Lambda}_{AE} = \begin{pmatrix} \mathbf{D}_{AE} & \mathbf{0} \\ \mathbf{0} & \mathbf{0}_{(N_E-s) \times q} \end{pmatrix}_{N_E \times M}$$

[0027] 其中 $q+s=N_A, K=N_A=M$,

[0028] $\mathbf{D}_{AR}=\text{diag}(d_{AR,1}, d_{AR,2}, \dots, d_{AR,s})$, $\mathbf{D}_{AE}=\text{diag}(d_{AE,1}, d_{AE,2}, \dots, d_{AE,s})$, 其中 $d_{AR,i}$ 升序排列, $d_{AE,i}$ 降序排列; 设计发端预编码矩阵为:

$$[0029] \quad \mathbf{F} = \frac{\mathbf{\Psi} \mathbf{R}^{-1}}{\|\mathbf{R}^{-1}\|} \sqrt{\mathbf{P}_a}$$

[0030] 其中 $\mathbf{P}_a = \text{diag}(\sqrt{p_{a,1}}, \sqrt{p_{a,2}}, \dots, \sqrt{p_{a,K}})$;

[0031] 设中继节点到合法用户信道矩阵的奇异值分解为 $\mathbf{H}_{RB} = \bar{\mathbf{U}} \Sigma_{RB} \bar{\mathbf{V}}$,

[0032] $\Sigma_{RB} = (\mathbf{0} \quad \bar{\Sigma}_{RB})$, $\bar{\Sigma}_{RB} = \text{diag}(\lambda_{RB,1}, \lambda_{RB,2}, \dots, \lambda_{RB,K})$, 设计预编码矩阵 \mathbf{W} 使得窃听节点在第二阶段接收不到任何信息, 即令 $\mathbf{W} = \mathbf{H}_{RE}^\perp \bar{\mathbf{V}}$, \mathbf{H}_{RE}^\perp 是 \mathbf{H}_{RE} 零空间的投影矩阵, 使得 $\mathbf{H}_{RE} \mathbf{W} = 0$; 然后利用奇异值分解, 设计中继预编码矩阵为

$$[0033] \quad \bar{\mathbf{W}} = \bar{\mathbf{V}} \sqrt{\mathbf{P}_r} \mathbf{U}^H$$

$$[0034] \quad \mathbf{W} = \mathbf{H}_{RE}^\perp \bar{\mathbf{V}} \sqrt{\mathbf{P}_r} \mathbf{U}^H$$

[0035] 其中, $\mathbf{P}_r = \text{diag}(\sqrt{p_{r,1}}, \sqrt{p_{r,2}}, \dots, \sqrt{p_{r,K}})$; 这样就完成了发送节点和中继节点的预编码矩阵的设计;

[0036] 本发明进一步的改进在于: 步骤 3) 中得到安全速率及其功率约束为:

$$[0037] \quad \max_{p_{a,k}, p_{r,k}} \quad R_s = \frac{1}{2} \sum_{k=1}^K \left[\log \left(1 + \frac{\bar{\rho} p_{r,k} p_{a,k} \lambda_{RB,k}^2 \bar{d}_{AR,k}^2}{1 + p_{r,k} \lambda_{RB,k}^2} \right) - \log \left(1 + \bar{\rho} p_{a,k} \bar{d}_{AE,k}^2 \right) \right]$$

$$[0038] \quad \text{s.t.} \quad P_A = \sigma_s^2 \sum_{k=1}^K p_{a,k} \leq P_1$$

$$[0039] \quad P_R = \sigma_n^2 \sum_{k=1}^K \left(\bar{\rho} p_{r,k} p_{a,k} \bar{d}_{AR,k}^2 + p_{r,k} \right) \leq P_2$$

[0040] 其中 P_1, P_2 分别是发送节点和中继节点的总功率,

$$\bar{\rho} = \sigma_s^2 / \sigma_n^2 \left\| \mathbf{R}^{-1} \right\|^2, \quad \bar{\mathbf{D}}_{AR} = \text{diag}(d_{AR,1}, d_{AR,2}, \dots, d_{AR,s}, 1, \dots, 1),$$

$\bar{\mathbf{D}}_{AE} = \text{diag}(d_{AE,1}, d_{AE,2}, \dots, d_{AE,s}, 0, \dots, 0)$ $\bar{d}_{AR,k}, \bar{d}_{AE,k}$ 分别是 $\bar{\mathbf{D}}_{AR}, \bar{\mathbf{D}}_{AE}$ 的第 k 个对角元素。

[0041] 本发明进一步的改进在于: 对安全速率及其功率约束采用交替迭代求解的方法; 首先进行变量代换 $z_k = p_{a,k}$, $r_k = \bar{\rho} p_{r,k} p_{a,k} \bar{d}_{AR,k}^2 + p_{r,k}$, $\bar{P}_1 = P_1 / \sigma_s^2$, $\bar{P}_2 = P_2 / \sigma_n^2$, 对上述优化问题进行变形, 当给定 z_k , 优化 r_k 得到优化问题为:

$$[0042] \quad \max_{r_k} \quad \sum_{k=1}^K \log \left(\frac{1 + \lambda_{RB,k}^2 r_k}{1 + \lambda_{RB,k}^2 r_k + \bar{\rho} \bar{d}_{AR,k}^2 z_k} \right)$$

[0043] s.t. $\sum_{k=1}^K r_k \leq \bar{P}_2, \quad r_k \geq 0, \quad k = 1, 2, \dots, K.$

[0044] 其解为

[0045] $r_k^*(v) = \frac{1}{2\lambda_{RB,k}^2} \left[\sqrt{\left(\bar{\rho}\bar{d}_{AR,k}^2 z_k\right)^2 + 4\bar{\rho}\bar{d}_{AR,k}^2 z_k \lambda_{RB,k}^2 v} - \bar{\rho}\bar{d}_{AR,k}^2 z_k - 2 \right]^+$

[0046] 其中 $[x]^+$ 表示取 x 和 0 之间的较大者, 变量 v 需要满足下式

[0047] $\sum_{k=1}^K r_k^*(v) = \bar{P}_2$

[0048] 当固定 r_k , 优化 z_k , 得到优化问题为

[0049] $\max_{z_k} \sum_{k=1}^K \left[\log\left(\frac{1+a_k z_k}{1+b_k + c_k z_k}\right) - \log(1+c_k z_k) \right]$

[0050] s.t. $\sum_{k=1}^K z_k \leq \bar{P}_1, \quad z_k \geq 0, \quad k = 1, 2, \dots, K.$

[0051] 本发明进一步的改进在于:当发送节点比窃听节点天线少或相同的情况,解为:

[0052] (1) 当 $\sum_{k \in \Omega} \bar{P}_{c,k} \leq \bar{P}_1$ 时, 解为 $z_k^* = \begin{cases} \bar{P}_{c,k}, & k \in \Omega \\ 0, & \text{其他} \end{cases}$, 其中集合 Ω 是所有满足

$d_k = a_k b_k - b_k c_k - c_k > 0$ 的 k 组成的, $\bar{P}_{c,k} = \frac{-2a_k c_k + \sqrt{4a_k^2 c_k^2 + 4a_k^2 c_k d_k}}{2a_k^2 c_k}$

[0053] (2) 当 $\sum_{k \in \Omega} \bar{P}_{c,k} > \bar{P}_1$ 时, 解为 $z_k^* = \begin{cases} \left[\max_i (\gamma_k^{(i)}(\mu)) \right]^+, & k \in \Omega \\ 0, & \text{其他} \end{cases}$, 其中

$\gamma_k^{(i)}(\mu)$ 是 $\ln 2(1+a_k z_k)(1+b_k + a_k z_k)(1+c_k z_k) \mu + a_k^2 c_k z_k^2 + 2a_k c_k z_k - d_k = 0$

的三个解, 并且满足 $\sum_{k=1}^K z_k^* = \bar{P}_1$;

[0054] 当发送节点比窃听节点天线有更多天线的情况,解为:

[0055]

$$z_k^* = \begin{cases} \left[\max_i (\gamma_k^{(t)}(\mu)) \right]^+, & k \in \Omega_+ \\ \frac{1}{2a_k} \sqrt{(2+b_k) - 4 \left(1 + b_k - \frac{a_k b_k}{\mu \ln 2} \right) - \frac{2+b_k}{2a_k}}, & k \in \Omega_0 \\ 0, & \text{其他} \end{cases}$$

[0056] 其中集合 $\Omega_0 = \{k : k \in \Omega, c_k = 0\}$, $\Omega_+ = \{k : k \in \Omega, c_k > 0\}$;

[0057] 通过交替迭代, 最后结果收敛到一个点处, 即得到功率分配。

[0058] 与现有的方法相比, 本发明的有益效果是 :

[0059] 1、考虑了发送节点端和中继节点的联合预编码, 利用 GSVD-ZF-SVD 方法, 将信道并行化, 简化了问题的分析难度; 并进行了最优的功率分配。在安全传输的前提下实现最高速率传输。

[0060] 2、计算复杂度较低: 交替迭代优化的结果有两个, 一个是得到闭式解, 一个是得到一个类似注水的结果, 计算复杂度低。

附图说明

[0061] 图 1 是本发明方法所涉及的系统模型。

[0062] 图 2 是本发明中等效的并行信道图。

[0063] 图 3a 和图 3b 是现有方法的仿真结果, 其中: 图 3a 给出了安全速率和中继节点功率约束的变化曲线图, 图 3b 给出了安全速率和发送节点端功率约束的变化曲线图。

具体实施方式

[0064] 下面结合附图与具体实施例对本发明做进一步的详细说明。

[0065] 本发明涉及系统模型如图 1 所示, 有一个发送节点(Alice), 一个中继节点(Relay), 一个接收节点(Bob) 以及一个窃听节点(Eve), 每个节点都配置有多个天线, 天线数目分别为 N_A, N_R, N_E, N_B 。中继节点采用 AF(放大转发) 的中继策略对接收信号进行放大转发。通过对(发送节点 - 中继信道矩阵, 发送节点 - 窃听信道矩阵) 利用广义奇异值分解(GSVD), 在发送节点端设计预编码矩阵与之匹配, 得到发送节点预编码矩阵为

$$\mathbf{F} = \frac{\Psi \mathbf{R}^{-1}}{\|\mathbf{R}^{-1}\|} \sqrt{\mathbf{P}_a} \circ \text{在中继节点, 中继节点对接收到的信息利用 ZF-SVD 方法设计预编码矩}$$

阵, 得到中继预编码矩阵为 $\mathbf{W} = \mathbf{H}_{RE}^\perp \bar{\mathbf{V}} \sqrt{\mathbf{P}_r} \mathbf{U}^H$, 从而实现了信道的并行化, 如附图 2 所示。

[0066] A、当发送节点端天线数目不如窃听节点多的时候, 得到的功率分配为 :

[0067] (1) 当 $\sum_{k \in \Omega} \bar{P}_{c,k} \leq \bar{P}_1$ 时, 解为 $z_k^* = \begin{cases} \bar{P}_{c,k}, & k \in \Omega \\ 0, & \text{其他} \end{cases}$, 其中集合 Ω 是所有满足

$$d_k = a_k b_k - b_k c_k - c_k > 0 \text{ 的 } k \text{ 组成的}, \bar{P}_{c,k} = \frac{-2a_k c_k + \sqrt{4a_k^2 c_k^2 + 4a_k^2 c_k d_k}}{2a_k^2 c_k}$$

[0068] (2) 当 $\sum_{k \in \Omega} \bar{P}_{c,k} > \bar{P}_1$ 时, 解为 $z_k^* = \begin{cases} \left[\max_i (\gamma_k^{(i)}(\mu)) \right]^+, & k \in \Omega \\ 0, & \text{其他} \end{cases}$, 其中

$\gamma_k^{(i)}(\mu)$ 是 $\ln 2(1+a_k z_k)(1+b_k + a_k z_k)(1+c_k z_k)\mu + a_k^2 c_k z_k^2 + 2a_k c_k z_k - d_k = 0$

的三个解, 并且满足 $\sum_{k=1}^K z_k^* = \bar{P}_1$ 。

[0069] B、而当发送节点端天线数目更多的时候, 得到功率分配为:

[0070]

$$z_k^* = \begin{cases} \left[\max_i (\gamma_k^{(i)}(\mu)) \right]^+, & k \in \Omega_+ \\ \left[\frac{1}{2a_k} \sqrt{(2+b_k) - 4\left(1+b_k - \frac{a_k b_k}{\mu \ln 2}\right)} - \frac{2+b_k}{2a_k} \right], & k \in \Omega_0 \\ 0, & \text{其他} \end{cases}$$

[0071] 可以看到, 当发送节点天线数目较少时, 发送节点端功率不是越多越好的, 它存在一个最优值, 这个从图 3b 可以反映出来。在这种情况下, 发送节点端功率如果全部使用, 使得第一阶段泄漏量增多, 而第二阶段的信息传输速率受到中继节点功率的约束, 使得系统的安全速率反而降低了。而当发送节点天线数目更多时, 会出现 $c_k=0$ 的情况, 这个时候, 窃听节点实际上是收不到信息的, 因而全部分配发送节点功率不会出现速率反降的情形。这些讨论从图 3 中都可以看出来。无论哪种情形, 最终的安全速率都会趋于平稳, 这是发送节点或者中继节点功率有限的原因。

[0072] 本发明一种 MIMO 放大转发中继网络的信号安全传输方法, 包括以下步骤:

[0073] 1) 第一阶段, 发送节点对发送信息进行线性预编码, 中继节点和窃听节点分别接收到发送节点发射的信息 $y_R = H_{AR}Fs + n_R$, $\mathbf{y}_E^{(1)} = \mathbf{H}_{AE}F\mathbf{s} + \mathbf{n}_E^{(1)}$, 其中 H_{AR}, H_{AE} 是信道矩阵, F 是发送节点线性预编码矩阵, s 是发送节点发射信息矢量, $n_R, \mathbf{n}_E^{(1)}$ 是加性高斯噪声矢量, $y_R, \mathbf{y}_E^{(1)}$ 是接收矢量。

[0074] 2) 第二阶段, 中继节点将接收到的信号, 进行放大

转发，预编码矩阵为 \mathbf{W} ，接收节点和窃听节点接收到的信息为 $\mathbf{y}_B = \mathbf{H}_{RB} \mathbf{W} \mathbf{H}_{AR} \mathbf{F} \mathbf{s} + \mathbf{H}_{RB} \mathbf{W} \mathbf{n}_R + \mathbf{n}_B$, $\mathbf{y}_E^{(2)} = \mathbf{H}_{RE} \mathbf{W} \mathbf{H}_{AR} \mathbf{F} \mathbf{s} + \mathbf{H}_{RE} \mathbf{W} \mathbf{n}_R + \mathbf{n}_E^{(2)}$. 这样就可以得到等效的窃听节点接收信息为

$$[0075] \quad \mathbf{y}_E = \begin{bmatrix} \mathbf{y}_E^{(1)} \\ \mathbf{y}_E^{(2)} \end{bmatrix} = \mathbf{H}_E \mathbf{s} + \mathbf{n}_E, \quad \mathbf{H}_E = \begin{bmatrix} \mathbf{H}_{AE} \mathbf{F} \\ \mathbf{H}_{RE} \mathbf{W} \mathbf{H}_{AR} \mathbf{F} \end{bmatrix}, \quad \mathbf{n}_E = \begin{bmatrix} \mathbf{n}_E^{(1)} \\ \mathbf{H}_{RE} \mathbf{W} \mathbf{n}_R + \mathbf{n}_E^{(2)} \end{bmatrix}$$

[0076] 3) 在功率约束下, 最大化安全传输的速率, 即最优化功率分配, 实现最大的安全速率 :

$$[0077] \quad R_s = \max(I(y_B; s) - I(y_E; s))^+$$

$$[0078] \quad \text{s.t. } \sigma_s^2 \text{tr}(\mathbf{F} \mathbf{F}^H) \leq P_1$$

$$[0079] \quad \text{tr}(\sigma_s^2 \mathbf{W} \mathbf{H}_{AR} \mathbf{F} \mathbf{F}^H \mathbf{H}_{AR}^H \mathbf{W}^H + \sigma_n^2 \mathbf{W} \mathbf{W}^H) \leq P_2$$

[0080] 按照上述的方法, 首先需要得到发送节点和中继节点的预编码矩阵, 然后进行最优的功率分配。

[0081] 采用 GSVD-ZF-SVD 的方法 :

[0082] 1、首先对信道矩阵 $\mathbf{H}_{AR}, \mathbf{H}_{AE}$ 进行广义奇异值分解得到 :

$$[0083] \quad \mathbf{H}_{AR} = \mathbf{U} \Lambda_{AR} \Phi$$

$$[0084] \quad \mathbf{H}_{AE} = \mathbf{V} \Lambda_{AE} \Phi$$

[0085] 其中 $\Phi = \mathbf{R} \Psi^H$ 是一个 $N_A \times N_A$ 的非奇异矩阵, Λ_{AR} 和 Λ_{AE} 具有如下形式

$$[0086] \quad \mathbf{\Lambda}_{AR} = \begin{pmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{D}_{AR} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{q \times q} \end{pmatrix}_{N_R \times M}$$

$$[0087] \quad \mathbf{\Lambda}_{AE} = \begin{pmatrix} \mathbf{D}_{AE} & \mathbf{0} \\ \mathbf{0} & \mathbf{0}_{(N_E-s) \times q} \end{pmatrix}_{N_E \times M}$$

[0088] 其中 $q+s=N_A, K=N_A=M$,

[0089] $D_{AR} = \text{diag}(d_{AR,1}, d_{AR,2}, \dots, d_{AR,s})$, $D_{AE} = \text{diag}(d_{AE,1}, d_{AE,2}, \dots, d_{AE,s})$, 其中 $d_{AR,i}$ 升序排列, $d_{AE,i}$ 降序排列。

[0090] 设计发送节点预编码矩阵为 :

$$[0091] \quad \mathbf{F} = \frac{\mathbf{\Psi} \mathbf{R}^{-1}}{\|\mathbf{R}^{-1}\|} \sqrt{\mathbf{P}_a}$$

[0092] 其中 $\mathbf{P}_a = \text{diag}(\sqrt{p_{a,1}}, \sqrt{p_{a,2}}, \dots, \sqrt{p_{a,K}})$ 。

[0093] 2、设中继节点到接收节点信道矩阵的奇异值分解为 $\mathbf{H}_{RB} = \bar{\mathbf{U}} \Sigma_{RB} \bar{\mathbf{V}}$, 设计预编

码矩阵 \mathbf{W} 使得窃听节点在第二阶段接收不到任何信息, 即令 $\mathbf{W} = \mathbf{H}_{RE}^\perp \bar{\mathbf{W}}$, \mathbf{H}_{RE}^\perp 是 \mathbf{H}_{RE} 零空间的投影矩阵, 使得 $\mathbf{H}_{RE}\mathbf{W}=0$ 。然后利用奇异值分解, 设计中继预编码矩阵为

$$[0094] \quad \bar{\mathbf{W}} = \bar{\mathbf{V}} \sqrt{\mathbf{P}_r} \mathbf{U}^H$$

[0095] 这样就完成了发送节点和中继节点的预编码矩阵的设计。

[0096] 3、为了实现最优的功率分配, 在上面设计的预编码矩阵的情况下, 得到安全速率及其功率约束为

$$[0097] \quad \max_{p_{a,k}, p_{r,k}} R_s = \frac{1}{2} \sum_{k=1}^K \left[\log \left(1 + \frac{\bar{\rho} p_{r,k} p_{a,k} \lambda_{RB,k}^2 \bar{d}_{AR,k}^2}{1 + p_{r,k} \lambda_{RB,k}^2} \right) - \log \left(1 + \bar{\rho} p_{a,k} \bar{d}_{AE,k}^2 \right) \right]$$

$$[0098] \quad \text{s.t.} \quad P_A = \sigma_s^2 \sum_{k=1}^K p_{a,k} \leq P_1$$

$$[0099] \quad P_R = \sigma_n^2 \sum_{k=1}^K \left(\bar{\rho} p_{r,k} p_{a,k} \bar{d}_{AR,k}^2 + p_{r,k} \right) \leq P_2$$

[0100] 直接求解上面优化问题难度较大, 采用交替迭代求解的方法。做变量代换 $z_k = p_{a,k}$, $r_k = \bar{\rho} p_{r,k} p_{a,k} \bar{d}_{AR,k}^2 + p_{r,k}$, $\bar{P}_1 = P_1 / \sigma_s^2$, $\bar{P}_2 = P_2 / \sigma_n^2$, 对上述优化问题进行变形, 当给定 z_k , 优化 r_k 得到优化问题为:

$$[0101] \quad \max_{r_k} \quad \sum_{k=1}^K \log \left(\frac{1 + \lambda_{RB,k}^2 r_k}{1 + \lambda_{RB,k}^2 r_k + \bar{\rho} \bar{d}_{AR,k}^2 z_k} \right)$$

$$[0102] \quad \text{s.t.} \quad \sum_{k=1}^K r_k \leq \bar{P}_2, \quad r_k \geq 0, \quad k = 1, 2, \dots, K.$$

[0103] 其解为

$$[0104] \quad r_k^*(v) = \frac{1}{2\lambda_{RB,k}^2} \left[\sqrt{\left(\bar{\rho} \bar{d}_{AR,k}^2 z_k \right)^2 + 4\bar{\rho} \bar{d}_{AR,k}^2 z_k \lambda_{RB,k}^2 v} - \bar{\rho} \bar{d}_{AR,k}^2 z_k - 2 \right]^+$$

[0105] 其中 $[x]^+$ 表示取 x 和 0 之间的较大者, 变量 v 需要满足下式

$$[0106] \quad \sum_{k=1}^K r_k^*(v) = \bar{P}_2$$

[0107] 当固定 r_k , 优化 z_k , 得到优化问题为

$$[0108] \quad \max_{z_k} \quad \sum_{k=1}^K \left[\log \left(\frac{1 + a_k z_k}{1 + b_k + c_k z_k} \right) - \log \left(1 + c_k z_k \right) \right]$$

[0109] s.t. $\sum_{k=1}^K z_k \leq \bar{P}_1, \quad z_k \geq 0, \quad k = 1, 2, \dots, K.$

[0110] 当发送节点比窃听节点天线少或相同的情况,解为

[0111] (1) 当 $\sum_{k \in \Omega} \bar{P}_{c,k} \leq \bar{P}_1$ 时,解为 $z_k^* = \begin{cases} \bar{P}_{c,k}, & k \in \Omega \\ 0, & \text{其他} \end{cases}$, 其中集合 Ω 是所有满足

$$d_k = a_k b_k - b_k c_k - c_k > 0 \text{ 的 } k \text{ 组成的}, \quad \bar{P}_{c,k} = \frac{-2a_k c_k + \sqrt{4a_k^2 c_k^2 + 4a_k^2 c_k d_k}}{2a_k^2 c_k}$$

[0112] (2) 当 $\sum_{k \in \Omega} \bar{P}_{c,k} > \bar{P}_1$ 时,解为 $z_k^* = \begin{cases} \left[\max_i (\gamma_k^{(i)}(\mu)) \right]^+, & k \in \Omega \\ 0, & \text{其他} \end{cases}$, 其中

$\gamma_k^{(i)}(\mu)$ 是 $\ln 2(1+a_k z_k)(1+b_k + a_k z_k)(1+c_k z_k) \mu + a_k^2 c_k z_k^2 + 2a_k c_k z_k - d_k = 0$

的三个解,并且满足 $\sum_{k=1}^K z_k^* = \bar{P}_1$ 。

[0113] 当发送节点比窃听节点天线有更多天线的情况,解为

[0114]

$$z_k^* = \begin{cases} \left[\max_i (\gamma_k^{(i)}(\mu)) \right]^+, & k \in \Omega_+ \\ \left[\frac{1}{2a_k} \sqrt{(2+b_k) - 4 \left(1+b_k - \frac{a_k b_k}{\mu \ln 2} \right)} - \frac{2+b_k}{2a_k} \right], & k \in \Omega_0 \\ 0, & \text{其他} \end{cases}$$

[0115] 其中集合 $\Omega_0 = \{k : k \in \Omega, c_k = 0\}$, $\Omega_+ = \{k : k \in \Omega, c_k > 0\}$ 。

[0116] 通过交替迭代,最后结果收敛到一个点处,得到功率分配。

[0117] 本发明提出了一种 MIMO 放大转发中继网络的信号安全传输方法,在设计预编码矩阵时,采用了 GSVD-ZF-SVD 的联合策略,使得系统并行化,简化了系统安全速率的表达形式,在功率约束的条件下求解一个最优化问题。在进行功率分配的时候,原问题的非凸性使得直接求解很难进行,采用交替迭代优化的方式,每一个子问题都能得到唯一的最优解,并且最终交替迭代能够得到一个收敛点,而这个收敛点肯定是一个临界点。当窃听节点天线数目不少于发送节点端,中继节点功率固定的时候,发端功率存在一个最优值。

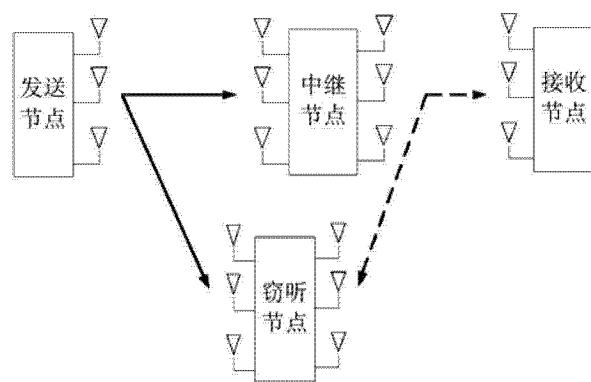


图 1

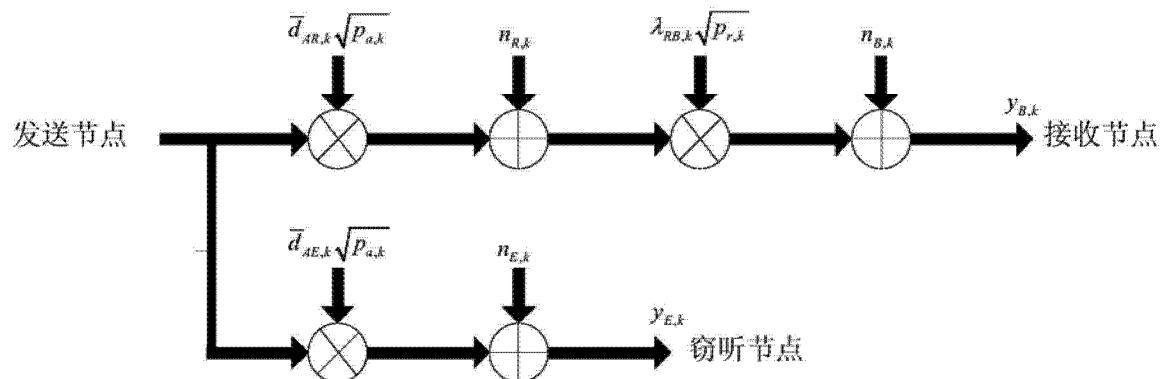


图 2

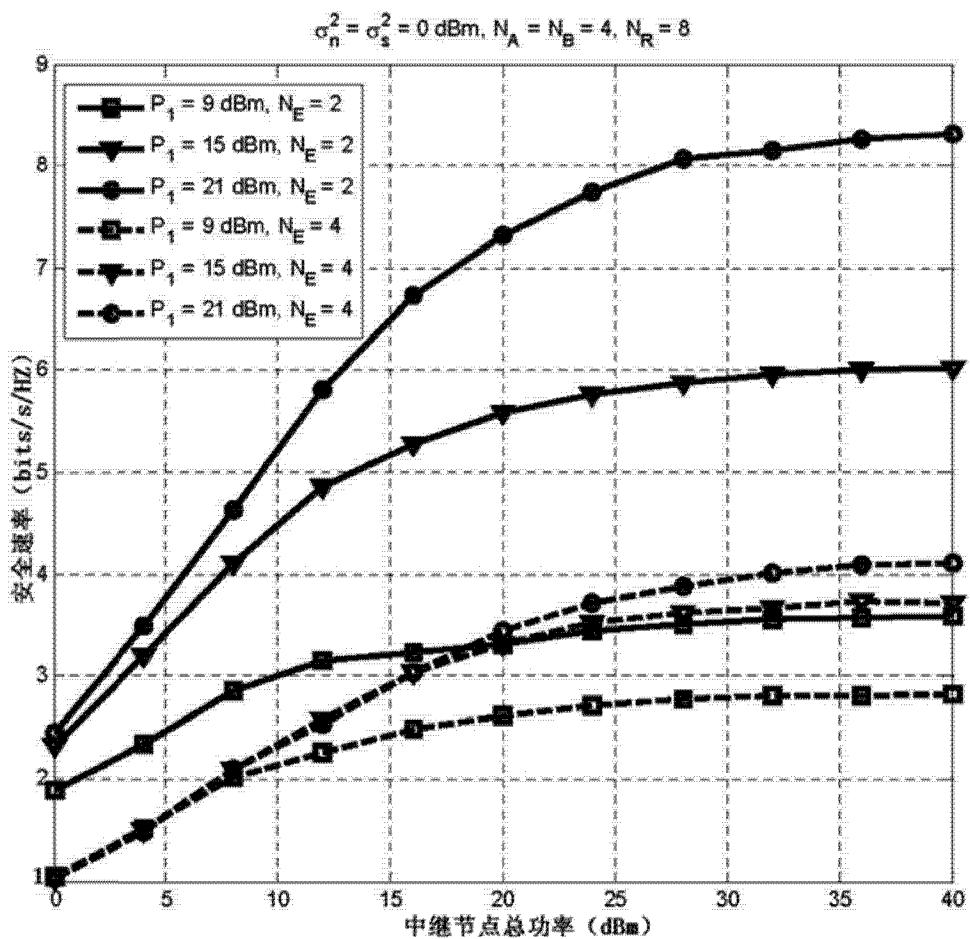


图 3a

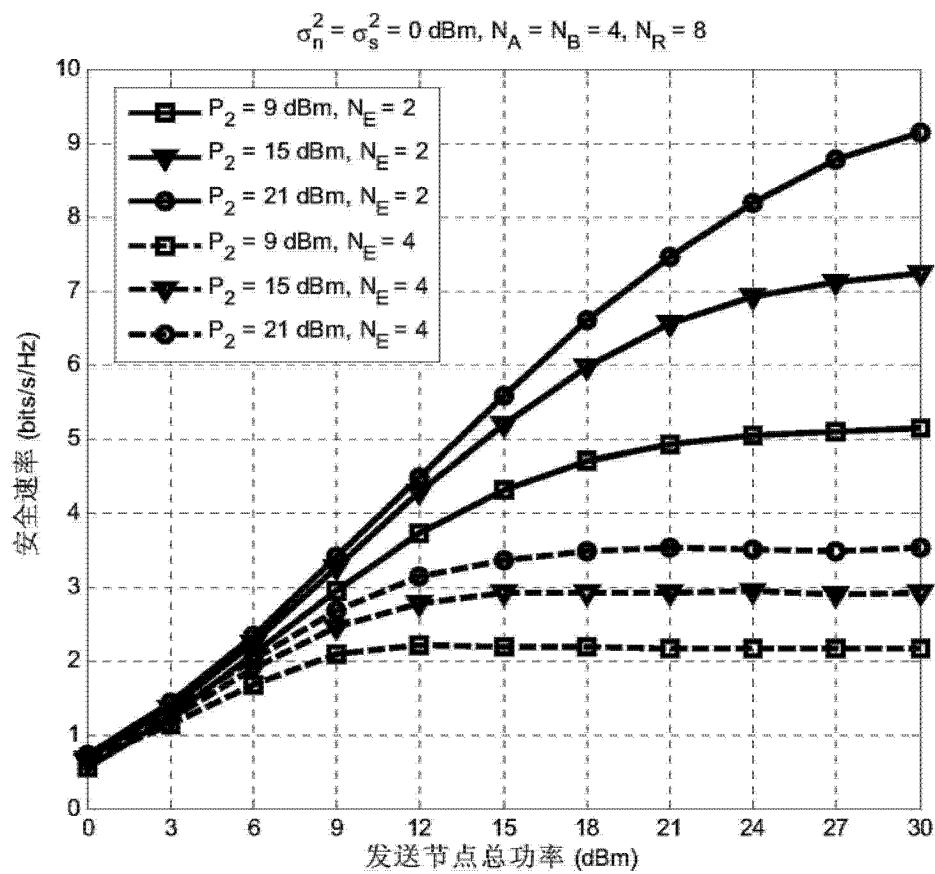


图 3b