

# MIMO 全双工双向安全通信系统的预编码矩阵设计

雷维嘉<sup>1,2</sup>, 周洋<sup>1,2</sup>, 谢显中<sup>3</sup>, 雷宏江<sup>1,4</sup>

(1. 重庆邮电大学通信与信息工程学院, 重庆 400065; 2. 移动通信技术重庆市重点实验室, 重庆 400065;  
3. 重庆邮电大学光电工程学院, 重庆 400065; 4. 西安邮电大学陕西省信息通信网络及安全重点实验室, 陕西 西安 710121)

**摘 要:** 研究多输入多输出全双工双向通信系统中, 合法节点在接收信息的同时向对方发送保密信息, 并协同发送人工噪声的物理层安全方案的预编码矩阵设计。针对合法信道、窃听信道的信道状态信息完美的场景, 使用 DC 规划优化信息信号与人工噪声的预编码矩阵以最大化系统保密和速率。对于信道 CSI 不完美的场景, 使用最差准则建模信道, 利用加权最小均方差算法对预编码矩阵进行稳健设计。仿真结果验证了优化算法能有效提高系统的保密和速率。

**关键词:** 物理层安全; 多输入多输出; 人工噪声; 全双工; 双向通信; 预编码矩阵

**中图分类号:** TN918

**文献标识码:** A

**doi:** 10.11959/j.issn.1000-436x.2020155

## Design of precoding matrices in MIMO full duplex two-way security communication system

LEI Weijia<sup>1,2</sup>, ZHOU Yang<sup>1,2</sup>, XIE Xianzhong<sup>3</sup>, LEI Hongjiang<sup>1,4</sup>

1. School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

2. Chongqing Key Laboratory of Mobile Communications Technology, Chongqing, 400065, China

3. School of Optoelectronic Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

4. Shaanxi Key Laboratory of Information Communication Network and Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

**Abstract:** The design of precoding matrices was studied in the multiple input multiple output (MIMO) full-duplex two-way security communication system where legitimate nodes transmit the confidential information accompanied by the artificial noise while receiving information. For the scenario where the perfect channel state information (CSI) of legitimate channels and eavesdropping channels was available, the difference of concave/convex (DC) programming was used to optimize the precoding matrices of the information signal and the artificial noise for the maximization of the secrecy sum rate. For the scenario where the CSI was imperfect, the channels were modeled by using worst-case criterion and the weighted minimum mean square error algorithm was used to get the robust precoding matrices of the information signal and the artificial noise. The simulation results prove that the proposed algorithm can effectively promote the secrecy sum rate of the system.

**Key words:** physical layer security, MIMO, artificial noise, full duplex, two-way communication, precoding matrix

收稿日期: 2020-04-19; 修回日期: 2020-06-28

基金项目: 国家自然科学基金资助项目 (No.61971080, No.61471076); 重庆市基础与前沿探索基金资助项目 (No.cstc2017jcyjAX0204, No.cstc2018jcyjAX0432); 重庆市教委科学技术研究重点基金资助项目 (No.KJZD-K201800603, No.KJZD-M201900602); 陕西省信息通信网络及安全重点实验室开放课题基金资助项目 (No.ICNS201807)

**Foundation Items:** The National Nature Science Foundation of China( No.61971080, No.61471076), Chongqing Research Program of Basic Research and Frontier Exploration( No.cstc2017jcyjAX0204, No.cstc2018jcyjAX0432), Key Project of Science and Technology Research of Chongqing Education Commission (No.KJZD-K201800603, No.KJZD-M201900602), Open Fund of the Shaanxi Key Laboratory of Information Communication Network and Security( No.ICNS201807)

## 1 引言

天线技术和信号处理技术的进步,使无线节点在同一频段同时收发信号的全双工通信成为可能。因为同时同频进行信号的收发,全双工节点处的发送信号强度远高于接收信号强度,发送信号会对信号接收通道造成强烈的自干扰,自干扰的抑制水平是决定全双工通信系统性能的关键问题。文献[1]提出通过天线选择、波束选择、零空间投影等方法进行自干扰消除,实现了 35 dB 的自干扰抑制制度。结合天线分离、模拟信号处理、数字信号处理等自干扰消除方式,构造与自干扰信号反相位的抵消信号,可控制自干扰抑制制度在 40~110 dB<sup>[2-4]</sup>。如能将残余自干扰功率控制在与信道噪声功率相近的数量级上,采用全双工传输就能有效地提高系统的频谱效率,倍增系统容量。

物理层安全以信息论为基础,利用无线信道的随机性、时变性、空间唯一性等特性实现信息的安全传输,为解决无线通信系统的安全问题提供了新的途径。在物理层安全通信系统的模型中,至少存在 3 类节点:发送节点、合法接收节点和窃听节点。系统的安全性能可用可达保密速率<sup>[5]</sup>、保密中断概率<sup>[6]</sup>等指标来衡量。当合法信道的传输质量优于窃听信道时,通过采用安全信道编码,可以实现系统的安全通信,且两者之间的质量差异越大,安全传输性能越优异。多天线波束赋形、人工噪声等技术是增大合法信道相对于窃听信道的传输质量优势、实现安全通信的重要技术手段。文献[7]指出,全双工通信系统中通信双方同时同频发送信号,窃听节点接收到的信号是合法通信双方发送信号的叠加,分离需要极大的解码复杂度,这有利于增强安全性能。目前,已有文献对在物理层利用全双工来提高系统的安全性能进行了研究。文献[8-9]研究了目的节点工作在全双工模式,在接收信息的同时发送人工噪声干扰窃听节点的物理层安全传输方案,全双工接收节点在接收信息的同时发送干扰或人工噪声,信息为单向传输,系统为单向通信系统。实际上,收发双方都工作在全双工模式进行双向通信能更有效地提高系统性能,有文献对此进行了研究。文献[10]研究了多输入单输出(MISO, multiple input single output)全双工双向通信系统中预编码矩阵设计问题,通信双方工作在天线分离式全双工模式,采用一根天线接收信号,其他天线用于信号发送,

以最大化系统保密和速率为目标,通过二维搜索迭代和半定规划算法实现最优预编码矩阵设计,同时为降低优化的复杂度,采用一维迭代搜索获取预编码矩阵的次优解。文献[11]研究了多输入多输出(MIMO, multiple input multiple output)全双工双向通信系统中仅发送方或接收方有保密需求的安全信息传输,在收发双方协作发送干扰的条件下给出了系统可达保密速率的范围,并对保密速率上界的闭式表达式进行了推导。除文献[8-11]研究的直连传输系统外,采用中继节点对信号进行转发的通信系统也是研究较多的系统模型。如文献[12]针对单天线多跳的中继系统,以系统能效最大化为优化目标,以满足特定的服务质量为约束条件,对发送节点和中继节点的功率分配进行了优化设计。全双工中继安全通信系统是受到广泛关注的系统模型,不少文献对该模型下提高安全性能的方案进行了研究。文献[13]考虑功率受限的多天线中继协作通信系统,采用两阶段中继传输协议,第一阶段全双工中继在接收信息的同时发送人工噪声干扰窃听器,文献对信号功率和人工噪声功率的分配方案进行了分析和讨论。文献[14]考虑两用户两跳非正交多址传输系统模型,多天线全双工中继采用解码转发协议,第一阶段全双工中继在接收信息的同时发送干扰,第二阶段中继在转发信息的同时基站发送干扰,推导了小区中心和边缘用户保密中断概率的解析表达式,并分析了发射功率较高情况下的渐进保密中断概率。这些文献的研究表明,采用全双工技术有利于提高系统的安全传输性能,但实际上系统的安全性能增益在很大程度上取决于各节点间信道状态信息(CSI, channel state information)的获得情况,包括文献[8-14]在内的大多数文献都假设合法信道的 CSI 是完美已知的,窃听信道的 CSI 可被完美获得或者不能获得。但是在实际的通信环境中,由于估计误差、量化误差和反馈时延等因素的影响,完美的 CSI 很难得到,因此在 CSI 存在误差情况下设计具有稳健性的物理层安全方案是一个重要的研究课题。目前,只有少量文献对不完美 CSI 条件下的全双工双向安全通信系统进行了研究。文献[15]研究了 MISO 全双工双向保密通信系统中,在信道 CSI 存在不确定性的条件下,以最大化最坏情况下的保密速率为目标的波束赋形设计。文献[16]针对全双工 MIMO 系统,假设合法信道 CSI 完美已知,在窃听信道 CSI 不完美的情况下,以保密中断

概率为约束，对发送信号的协方差矩阵进行优化。

本文在合法节点获得的合法信道、窃听信道的 CSI 完美和不完美 2 种场景下，对人工噪声辅助的多天线全双工双向通信系统中的物理层安全传输方案进行研究。其中，合法节点工作在全双工模式，在接收信息的同时不仅发送信息信号，也发送人工噪声干扰窃听节点。针对合法信道与窃听信道的 CSI 完美已知的场景，采用 DC (difference of concave/convex) 规划算法对信息信号以及人工噪声的预编码矩阵进行优化设计，以实现系统保密和速率的最大化；针对合法信道、窃听信道 CSI 不完美的场景，采用加权最小均方误差 (WMMSE, weighted minimum mean square error) 准则对信息信号以及人工噪声的预编码矩阵进行稳健设计，以最大化最坏情况下的保密和速率。与现有的对不完美 CSI 场景下全双工双向安全通信系统 [15-16] 相比，本文的研究有以下特点：1) 本文方案中，工作在全双工模式的合法节点在同时同频进行信息收发时同时发送人工噪声干扰窃听节点，可有效提高安全性能，而文献[15-16]均没有使用人工噪声；2) 文献[15]的系统模型为 MISO 模型，即仅采用一根天线接收，实际上，发送天线和接收天线数量中的较小值决定了多天线系统的容量，仅分配一根天线用于信息的接收虽然简化了系统优化的复杂度，但限制了多天线全双工系统的性能，本文的系统模型为 MIMO 模型，性能优于 MISO 系统，但系统设计和分析的复杂度要远高于后者；3) 文献[16]的系统模型虽然是 MIMO 模型，但其仅考虑窃听信道的 CSI 不完美的情况，假设合法信道 CSI 完美已知，该假设有一定的局限性，本文考虑了全双工节点获得的合法信道及窃听信道 CSI 均有误差的情况。

## 2 系统模型

考虑如图 1 所示的全双工双向通信系统模型，系统由配备多根天线的合法节点 A、B 以及窃听节点 E 组成。合法节点 A、B 工作在全双工模式，各配有  $N$  根天线，其中， $N_t$  根天线用于发送信息，其余  $N_r=N-N_t$  根天线用于接收信息。窃听节点 E 配备  $N_e$  根天线。定义  $\mathbf{H}_{AB} \in \mathbb{C}^{N_r \times N_t}$ 、 $\mathbf{H}_{BA} \in \mathbb{C}^{N_t \times N_r}$ 、 $\mathbf{G}_{AE} \in \mathbb{C}^{N_e \times N_t}$ 、 $\mathbf{G}_{BE} \in \mathbb{C}^{N_e \times N_r}$  分别为 A → B、B → A、A → E、B → E 的信道矩阵。全双工节点的收发天线之间存在自干扰，现有的自干扰消除技术并不能完全消除自干扰信号。定义 A、B 的包含自干扰消

除环节的等效自干扰信道矩阵为  $\sqrt{\rho_A} \mathbf{H}_{AA} \in \mathbb{C}^{N_r \times N_t}$ 、 $\sqrt{\rho_B} \mathbf{H}_{BB} \in \mathbb{C}^{N_t \times N_r}$ ，其中  $\rho_A$  和  $\rho_B$  表示自干扰残余因子， $0 < \rho_A \leq 1$ ， $0 < \rho_B \leq 1$ ， $\mathbf{H}_{AA} \in \mathbb{C}^{N_r \times N_t}$ 、 $\mathbf{H}_{BB} \in \mathbb{C}^{N_t \times N_r}$  为收发天线间的环衰落信道矩阵。

为了增强信息传输的保密性，合法节点 A、B 在发送信息信号的同时发送人工噪声干扰窃听节点。A、B 的发送信号分别表示为

$$\mathbf{x}_A = \mathbf{S}_A \mathbf{u}_A + \mathbf{Z}_A \mathbf{m}_A \quad (1)$$

$$\mathbf{x}_B = \mathbf{S}_B \mathbf{u}_B + \mathbf{Z}_B \mathbf{m}_B \quad (2)$$

其中， $\mathbf{u}_J \in \mathbb{C}^{N_t \times 1}$ 、 $\mathbf{m}_J \in \mathbb{C}^{N_t \times 1}$  ( $J=A$  或  $B$ ) 分别为功率归一化的信息信号、人工噪声， $\mathbf{u}_J, \mathbf{m}_J \sim \text{CN}(0, \mathbf{I}_{N_t})$ ， $\mathbf{I}_{N_t}$  为单位矩阵； $\mathbf{S}_J \in \mathbb{C}^{N_t \times N_t}$ 、 $\mathbf{Z}_J \in \mathbb{C}^{N_t \times N_t}$  分别为节点处的信息信号、人工噪声的预编码矩阵，满足  $P_{S_J} + P_{Z_J} \leq P_J$ ， $P_{S_J} = \|\mathbf{S}_J\|_F^2$  为节点  $J$  发送的信息信号功率 ( $\|\cdot\|_F$  代表矩阵的 Frobenius 范数)， $P_{Z_J} = \|\mathbf{Z}_J\|_F^2$  为人工噪声功率， $P_J$  为发送总功率。定义功率分配因子  $\alpha_J = \frac{P_{Z_J}}{P_J}$ ，表示人工噪声功率占发送总功率的比值，满足  $0 \leq \alpha_J \leq 1$ 。

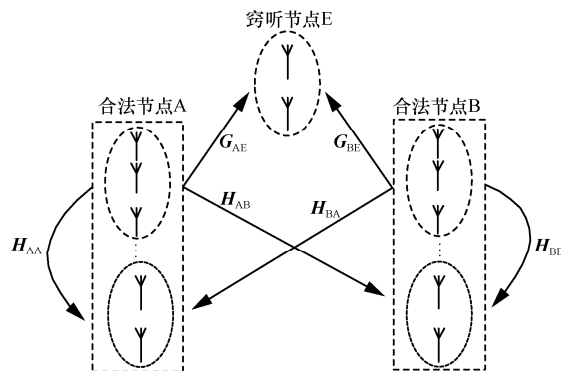


图 1 全双工双向通信系统模型

由于工作在全双工模式，合法节点在接收信息的同时会受到自干扰的影响，A、B 的接收信号  $\mathbf{y}_A$ 、 $\mathbf{y}_B$  可以表示为

$$\mathbf{y}_A = \mathbf{H}_{BA} \mathbf{x}_B + \sqrt{\rho_A} \mathbf{H}_{AA} \mathbf{x}_A + \mathbf{n}_A = \mathbf{H}_{BA} (\mathbf{S}_B \mathbf{u}_B + \mathbf{Z}_B \mathbf{m}_B) + \sqrt{\rho_A} \mathbf{H}_{AA} (\mathbf{S}_A \mathbf{u}_A + \mathbf{Z}_A \mathbf{m}_A) + \mathbf{n}_A \quad (3)$$

$$\mathbf{y}_B = \mathbf{H}_{AB} \mathbf{x}_A + \sqrt{\rho_B} \mathbf{H}_{BB} \mathbf{x}_B + \mathbf{n}_B = \mathbf{H}_{AB} (\mathbf{S}_A \mathbf{u}_A + \mathbf{Z}_A \mathbf{m}_A) + \sqrt{\rho_B} \mathbf{H}_{BB} (\mathbf{S}_B \mathbf{u}_B + \mathbf{Z}_B \mathbf{m}_B) + \mathbf{n}_B \quad (4)$$

其中， $\mathbf{n}_A \sim \text{CN}(0, \sigma_A^2 \mathbf{I}_{N_r})$ 、 $\mathbf{n}_B \sim \text{CN}(0, \sigma_B^2 \mathbf{I}_{N_t})$  分别为 A、B 处的加性复高斯白噪声。

窃听节点 E 同时接收到来自 A、B 的信号, 其接收信号为

$$\mathbf{y}_E = \mathbf{G}_{AE}\mathbf{x}_A + \mathbf{G}_{BE}\mathbf{x}_B + \mathbf{n}_E = \mathbf{G}_{AE}(\mathbf{S}_A\mathbf{u}_A + \mathbf{Z}_A\mathbf{m}_A) + \mathbf{G}_{BE}(\mathbf{S}_B\mathbf{u}_B + \mathbf{Z}_B\mathbf{m}_B) + \mathbf{n}_E \quad (5)$$

其中,  $\mathbf{n}_E \sim \text{CN}(0, \sigma_E^2 \mathbf{I}_{N_E})$  为 E 处的加性复高斯白噪声。

根据式(3), B 到 A 的信息传输速率为

$$R_{BA} = \text{lb} \left| \mathbf{I}_{N_t} + \frac{\mathbf{H}_{BA}\mathbf{S}_B\mathbf{S}_B^H\mathbf{H}_{BA}^H}{\sigma_A^2\mathbf{I}_{N_t} + \mathbf{H}_{BA}\mathbf{Z}_B\mathbf{Z}_B^H\mathbf{H}_{BA}^H + \mathbf{A}_A} \right| \quad (6)$$

其中,  $\mathbf{A}_A = \rho_A\mathbf{H}_{AA}\mathbf{S}_A\mathbf{S}_A^H\mathbf{H}_{AA}^H + \rho_A\mathbf{H}_{AA}\mathbf{Z}_A\mathbf{Z}_A^H\mathbf{H}_{AA}^H$ 。本文中, 矩阵运算  $\frac{\mathbf{E}}{\mathbf{F}}$  表示  $\mathbf{E}\mathbf{F}^{-1}$ , 上标 H 表示矩阵的共轭转置,  $|\mathbf{F}|$  表示矩阵  $\mathbf{F}$  的行列式。

同理, 根据式(4), A 到 B 的信息传输速率为

$$R_{AB} = \text{lb} \left| \mathbf{I}_{N_t} + \frac{\mathbf{H}_{AB}\mathbf{S}_A\mathbf{S}_A^H\mathbf{H}_{AB}^H}{\sigma_B^2\mathbf{I}_{N_t} + \mathbf{H}_{AB}\mathbf{Z}_A\mathbf{Z}_A^H\mathbf{H}_{AB}^H + \mathbf{A}_B} \right| \quad (7)$$

其中,  $\mathbf{A}_B = \rho_B\mathbf{H}_{BB}\mathbf{S}_B\mathbf{S}_B^H\mathbf{H}_{BB}^H + \rho_B\mathbf{H}_{BB}\mathbf{Z}_B\mathbf{Z}_B^H\mathbf{H}_{BB}^H$ 。

根据文献[17]的双向多址窃听信道容量结果, E 的窃听速率可表示为

$$R_E = \text{lb} \left| \mathbf{I}_{N_E} + \frac{\mathbf{G}_{AE}\mathbf{S}_A\mathbf{S}_A^H\mathbf{G}_{AE}^H + \mathbf{G}_{BE}\mathbf{S}_B\mathbf{S}_B^H\mathbf{G}_{BE}^H}{\sigma_E^2\mathbf{I}_{N_E} + \mathbf{G}_{AE}\mathbf{Z}_A\mathbf{Z}_A^H\mathbf{G}_{AE}^H + \mathbf{G}_{BE}\mathbf{Z}_B\mathbf{Z}_B^H\mathbf{G}_{BE}^H} \right| \quad (8)$$

系统保密和速率为

$$R_S = [R_{BA} + R_{AB} - R_E]^+ \quad (9)$$

其中,  $[x]^+$  表示  $\max\{0, x\}$ 。

### 3 预编码矩阵的设计

本节针对全双工节点获得的合法信道矩阵

$\mathbf{H}_{AB}$ 、 $\mathbf{H}_{BA}$  和窃听信道矩阵  $\mathbf{G}_{AE}$ 、 $\mathbf{G}_{BE}$  完美已知和不完美已知的 2 种场景, 分别设计信息信号与人工噪声的预编码矩阵  $\mathbf{S}_A$ 、 $\mathbf{S}_B$ 、 $\mathbf{Z}_A$ 、 $\mathbf{Z}_B$ 。

#### 3.1 信道状态信息完美时的预编码矩阵设计

当合法信道矩阵和窃听信道矩阵可完美获得时, 以最大化系统瞬时保密和速率为目标对预编码矩阵进行设计, 优化问题可以构造为

$$\begin{aligned} \max_{\mathbf{S}_A, \mathbf{S}_B, \mathbf{Z}_A, \mathbf{Z}_B} R_S &= [R_{BA} + R_{AB} - R_E]^+ \\ \text{s.t.} \quad &\|\mathbf{S}_A\|_F^2 + \|\mathbf{Z}_A\|_F^2 \leq P_A \\ &\|\mathbf{S}_B\|_F^2 + \|\mathbf{Z}_B\|_F^2 \leq P_B \end{aligned} \quad (10)$$

由于优化目标函数的非凸特性, 式(10)所示优化问题的求解非常困难。本文通过矩阵行列式的分解, 将优化目标函数近似为 2 个上凸函数之差的形式, 再利用 DC 规划求解优化问题。

定义变量  $\Sigma_A = \mathbf{S}_A\mathbf{S}_A^H$ 、 $\Sigma_B = \mathbf{S}_B\mathbf{S}_B^H$ 、 $\Phi_A = \mathbf{Z}_A\mathbf{Z}_A^H$ 、 $\Phi_B = \mathbf{Z}_B\mathbf{Z}_B^H$ , 式(10)所示的优化问题可以写为

$$\begin{aligned} \text{P1:} \quad \max_{\Sigma_A, \Sigma_B, \Phi_A, \Phi_B} R_S &= [R_{BA} + R_{AB} - R_E]^+ \\ \text{s.t.} \quad &\text{Tr}(\Sigma_A + \Phi_A) \leq P_A \\ &\text{Tr}(\Sigma_B + \Phi_B) \leq P_B \end{aligned} \quad (11)$$

其中,  $\text{Tr}$  表示矩阵的迹。

利用  $\text{lb} \left| \mathbf{I} + \frac{\mathbf{E}}{\mathbf{F}} \right| = \text{lb} |\mathbf{F} + \mathbf{E}| - \text{lb} |\mathbf{F}|$ , 式(6)可以转

换为

$$R_{BA} = f_1(\Sigma_A, \Sigma_B, \Phi_A, \Phi_B) - g_1(\Sigma_A, \Sigma_B, \Phi_A, \Phi_B) \quad (12)$$

其中,  $f_1(\Sigma_A, \Sigma_B, \Phi_A, \Phi_B)$ 、 $g_1(\Sigma_A, \Sigma_B, \Phi_A, \Phi_B)$  的定义分别如式(13)、式(14)所示。

$$\begin{aligned} f_1(\Sigma_A, \Sigma_B, \Phi_A, \Phi_B) &= \text{lb} \left| \sigma_A^2 \mathbf{I}_{N_t} + \rho_A \mathbf{H}_{AA} \Sigma_A \mathbf{H}_{AA}^H + \mathbf{H}_{BA} \Sigma_B \mathbf{H}_{BA}^H + \rho_A \mathbf{H}_{AA} \Phi_A \mathbf{H}_{AA}^H + \mathbf{H}_{BA} \Phi_B \mathbf{H}_{BA}^H \right| = \\ &\text{lb} \left| \sigma_A^2 \mathbf{I}_{N_t} + \begin{bmatrix} \sqrt{\rho_A} \mathbf{H}_{AA} & \mathbf{H}_{BA} & \sqrt{\rho_A} \mathbf{H}_{AA} & \mathbf{H}_{BA} \end{bmatrix} \begin{bmatrix} \Sigma_A & & & \\ & \Sigma_B & & \\ & & \Phi_A & \\ & & & \Phi_B \end{bmatrix} \begin{bmatrix} \sqrt{\rho_A} \mathbf{H}_{AA}^H \\ \mathbf{H}_{BA}^H \\ \sqrt{\rho_A} \mathbf{H}_{AA}^H \\ \mathbf{H}_{BA}^H \end{bmatrix} \right| \end{aligned} \quad (13)$$

$$\begin{aligned} g_1(\Sigma_A, \Sigma_B, \Phi_A, \Phi_B) &= \text{lb} \left| \sigma_A^2 \mathbf{I}_{N_t} + \rho_A \mathbf{H}_{AA} \Sigma_A \mathbf{H}_{AA}^H + \rho_A \mathbf{H}_{AA} \Phi_A \mathbf{H}_{AA}^H + \mathbf{H}_{BA} \Phi_B \mathbf{H}_{BA}^H \right| = \\ &\text{lb} \left| \sigma_A^2 \mathbf{I}_{N_t} + \begin{bmatrix} \sqrt{\rho_A} \mathbf{H}_{AA} & \mathbf{0}_{N_t \times N_t} & \sqrt{\rho_A} \mathbf{H}_{AA} & \mathbf{H}_{BA} \end{bmatrix} \begin{bmatrix} \Sigma_A & & & \\ & \Sigma_B & & \\ & & \Phi_A & \\ & & & \Phi_B \end{bmatrix} \begin{bmatrix} \sqrt{\rho_A} \mathbf{H}_{AA}^H \\ \mathbf{0}_{N_t \times N_t} \\ \sqrt{\rho_A} \mathbf{H}_{AA}^H \\ \mathbf{H}_{BA}^H \end{bmatrix} \right| \end{aligned} \quad (14)$$

定义  $\Psi \triangleq \text{diag}\{\Sigma_A, \Sigma_B, \Phi_A, \Phi_B\}$ , 并记块矩阵  $H_{A1} = \begin{bmatrix} \sqrt{\rho_A} H_{AA}, & H_{BA}, & \sqrt{\rho_A} H_{AA}, & H_{BA} \end{bmatrix}$ , 定义块矩阵  $H_{A2} = \begin{bmatrix} \sqrt{\rho_A} H_{AA}, & \mathbf{0}_{N_t \times N_t}, & \sqrt{\rho_A} H_{AA}, & H_{BA} \end{bmatrix}$ , 则式(13)、式(14)可以分别转换为

$$f_1(\Psi) = \text{lb} \left| \sigma_A^2 I_{N_t} + H_{A1} \Psi H_{A1}^H \right| \quad (15)$$

$$g_1(\Psi) = \text{lb} \left| \sigma_A^2 I_{N_t} + H_{A2} \Psi H_{A2}^H \right| \quad (16)$$

显然,  $f_1(\Psi)$ 、 $g_1(\Psi)$  为  $\Psi$  的上凸函数。

同理, 式(7)和式(8)可以分别转换为

$$R_{AB} = f_2(\Psi) - g_2(\Psi) \quad (17)$$

$$R_E = f_3(\Psi) - g_3(\Psi) \quad (18)$$

其中,

$$f_2(\Psi) = \text{lb} \left| \sigma_B^2 I_{N_t} + H_{B1} \Psi H_{B1}^H \right| \quad (19)$$

$$g_2(\Psi) = \text{lb} \left| \sigma_B^2 I_{N_t} + H_{B2} \Psi H_{B2}^H \right| \quad (20)$$

$$f_3(\Psi) = \text{lb} \left| \sigma_E^2 I_{N_E} + G_{E1} \Psi G_{E1}^H \right| \quad (21)$$

$$g_3(\Psi) = \text{lb} \left| \sigma_E^2 I_{N_E} + G_{E2} \Psi G_{E2}^H \right| \quad (22)$$

其中,  $H_{B1} = \begin{bmatrix} H_{AB}, & \sqrt{\rho_B} H_{BB}, & H_{AB}, & \sqrt{\rho_B} H_{BB} \end{bmatrix}$ ,  $H_{B2} = \begin{bmatrix} \mathbf{0}_{N_t \times N_t}, & \sqrt{\rho_B} H_{BB}, & H_{AB}, & \sqrt{\rho_B} H_{BB} \end{bmatrix}$ ,  $G_{E1} = [G_{AE}, G_{BE}, G_{AE}, G_{BE}]$ ,  $G_{E2} = \begin{bmatrix} \mathbf{0}_{N_t \times N_t}, & \mathbf{0}_{N_t \times N_t}, & G_{AE}, & G_{BE} \end{bmatrix}$ 。 $f_2(\Psi)$ 、 $g_2(\Psi)$ 、 $f_3(\Psi)$ 、 $g_3(\Psi)$  均为关于  $\Psi$  的上凸函数。

进一步地, 保密和速率  $R_S$  为

$$R_S = [y_1(\Psi) - y_2(\Psi)]^+ \quad (23)$$

其中,

$$y_1(\Psi) = f_1(\Psi) + f_2(\Psi) + g_3(\Psi) \quad (24)$$

$$y_2(\Psi) = g_1(\Psi) + g_2(\Psi) + f_3(\Psi) \quad (25)$$

由于有限个上凸函数之和依然为上凸函数, 因此  $y_1(\Psi)$ 、 $y_2(\Psi)$  为关于  $\Psi$  的上凸函数。 $R_S$  表示为 2 个上凸函数之差的形式, 可以使用 DC 规划<sup>[18]</sup>使其最大化。首先将  $y_1(\Psi)$  或  $y_2(\Psi)$  在初始迭代矩阵  $\tilde{\Psi} \triangleq \text{diag}\{\tilde{\Sigma}_A, \tilde{\Sigma}_B, \tilde{\Phi}_A, \tilde{\Phi}_B\}$  处进行一阶泰勒展开<sup>[19]</sup>, 得到其线性近似函数。本文选择对  $y_2(\Psi)$  进行线性近似, 其近似函数  $\tilde{y}_2(\Psi)$  可表示为

$$\tilde{y}_2(\Psi) = \tilde{g}_1(\Psi) + \tilde{g}_2(\Psi) + \tilde{f}_3(\Psi) = \text{lb} \left| \sigma_A^2 I_{N_t} + H_{A2} \tilde{\Psi} H_{A2}^H \right| +$$

$$\begin{aligned} & \frac{1}{\ln 2} \text{Tr} \left[ \left( \sigma_A^2 I_{N_t} + H_{A2} \tilde{\Psi} H_{A2}^H \right)^{-1} H_{A2} (\Psi - \tilde{\Psi}) H_{A2}^H \right] + \\ & \text{lb} \left| \sigma_B^2 I_{N_t} + H_{B2} \tilde{\Psi} H_{B2}^H \right| + \\ & \frac{1}{\ln 2} \text{Tr} \left[ \left( \sigma_B^2 I_{N_t} + H_{B2} \tilde{\Psi} H_{B2}^H \right)^{-1} H_{B2} (\Psi - \tilde{\Psi}) H_{B2}^H \right] + \\ & \text{lb} \left| \sigma_E^2 I_{N_E} + H_{E1} \tilde{\Psi} H_{E1}^H \right| + \\ & \frac{1}{\ln 2} \text{Tr} \left[ \left( \sigma_E^2 I_{N_E} + H_{E1} \tilde{\Psi} H_{E1}^H \right)^{-1} H_{E1} (\Psi - \tilde{\Psi}) H_{E1}^H \right] \end{aligned} \quad (26)$$

其中,  $\tilde{g}_1(\Psi)$ 、 $\tilde{g}_2(\Psi)$ 、 $\tilde{f}_3(\Psi)$  分别为  $g_1(\Psi)$ 、 $g_2(\Psi)$ 、 $f_3(\Psi)$  在  $\tilde{\Psi}$  处的线性近似函数。进一步得到  $R_S$  的近似值  $\tilde{R}_S$  为

$$\tilde{R}_S = \tilde{y}_1(\Psi) - \tilde{y}_2(\Psi) \quad (27)$$

$\tilde{R}_S$  为关于  $\Psi$  的上凸函数, 可以使用凸优化工具 (如 cvx) 获取使  $\tilde{R}_S$  最大的对角分块矩阵  $\Psi^{\text{opt}}$ , 将其作为下一次迭代的矩阵  $\tilde{\Psi}$ , 进行泰勒展开得到新的  $\tilde{y}_2(\Psi)$  以及  $\tilde{R}_S$  的表达式, 再进行凸优化获得使  $\tilde{R}_S$  最大的矩阵  $\Psi^{\text{opt}}$ 。如此进行循环迭代优化,  $\Psi^{\text{opt}}$  将逐渐逼近最优解  $\Psi^*$ , 优化矩阵  $\Psi$  的迭代算法如算法 1 所示。

**算法 1** 求解优化问题 P1 的 DC 规划算法

初始化  $j=0$ ,  $\tilde{\Sigma}_A^{(0)} = \frac{P_A}{2N_t} I_{N_t}$ ,  $\tilde{\Phi}_A^{(0)} = \frac{P_A}{2N_t} I_{N_t}$ ,

$\tilde{\Sigma}_B^{(0)} = \frac{P_B}{2N_t} I_{N_t}$ ,  $\tilde{\Phi}_B^{(0)} = \frac{P_B}{2N_t} I_{N_t}$ ,  $\tilde{\Psi}_0 = \text{diag}\{\tilde{\Sigma}_A^{(0)}, \tilde{\Sigma}_B^{(0)}, \tilde{\Phi}_A^{(0)}, \tilde{\Phi}_B^{(0)}\}$

- 1) do
- 2)  $j=j+1$
- 3)  $\Psi^{\text{opt}} = \arg \max_{\Psi} \tilde{R}_S(\tilde{\Psi}_{j-1})$
- 4)  $\tilde{\Psi}_j = \Psi^{\text{opt}}$
- 5) while  $\left\| \tilde{\Psi}_j \right\|_F - \left\| \tilde{\Psi}_{j-1} \right\|_F > \tau_1$
- 6)  $\Psi^* = \Psi^{\text{opt}}$

算法 1 中,  $j$  表示迭代的轮次, 以  $-\tau_1 \leq \left\| \tilde{\Psi}_j \right\|_F - \left\| \tilde{\Psi}_{j-1} \right\|_F \leq \tau_1$  作为 DC 规划算法的收敛条件, 其中,  $\tau_1$  为一个取值较小的正常数, 即在  $\left\| \tilde{\Psi}_j \right\|_F - \left\| \tilde{\Psi}_{j-1} \right\|_F > \tau_1$  时继续迭代。当算法收敛时, 即可得到使  $\tilde{R}_S$  最大的优化解  $\Psi^*$ , 并且根据文献[8]的定理 2,  $\Psi^*$  也是使  $R_S$  最大的一个优化解。

下面分析算法 1 的复杂度。根据文献[20], DC

规划的复杂度可以近似为  $O(\omega^{3.5} \lg(\frac{1}{\nu}))$ , 其中,  $\omega$  代表优化变量个数,  $\nu$  为给定的精度。算法 1 中, 变量个数  $\omega$  为  $4N_t^2$ , 精度  $\nu$  为  $\tau_1$ , 因此算法 1 的复杂度近似为  $O((4N_t^2)^{3.5} \lg(\frac{1}{\tau_1}))$ 。

### 3.2 信道状态信息不完美时的预编码矩阵设计

在实际通信场景中, 要想完全准确无误地获得信道的 CSI 是十分困难的, 本节考虑当获得的信道 CSI 不完美, 即获得的信道矩阵存在估计误差时, 预编码矩阵的稳健设计。

根据文献[21-22]的最差准则, 在信道状态信息不完美的情况下, 信道矩阵可以建模为

$$\begin{aligned} \mathcal{H}_1 &= \{ \mathbf{H}_{AB} \mid \mathbf{H}_{AB} = \hat{\mathbf{H}}_{AB} + \mathbf{A}_{AB}, \|\mathbf{A}_{AB}\|_F \leq \varepsilon_{AB} \} \\ \mathcal{H}_2 &= \{ \mathbf{H}_{BA} \mid \mathbf{H}_{BA} = \hat{\mathbf{H}}_{BA} + \mathbf{A}_{BA}, \|\mathbf{A}_{BA}\|_F \leq \varepsilon_{BA} \} \\ \mathcal{G}_1 &= \{ \mathbf{G}_{AE} \mid \mathbf{G}_{AE} = \hat{\mathbf{G}}_{AE} + \mathbf{A}_{AE}, \|\mathbf{A}_{AE}\|_F \leq \varepsilon_{AE} \} \\ \mathcal{G}_2 &= \{ \mathbf{G}_{BE} \mid \mathbf{G}_{BE} = \hat{\mathbf{G}}_{BE} + \mathbf{A}_{BE}, \|\mathbf{A}_{BE}\|_F \leq \varepsilon_{BE} \} \end{aligned} \quad (28)$$

其中,  $\hat{\mathbf{H}}_{AB}$ 、 $\hat{\mathbf{H}}_{BA}$ 、 $\hat{\mathbf{G}}_{AE}$ 、 $\hat{\mathbf{G}}_{BE}$  为信道估计值,  $\mathbf{A}_{AB}$ 、 $\mathbf{A}_{BA}$ 、 $\mathbf{A}_{AE}$ 、 $\mathbf{A}_{BE}$  为信道的估计误差, 其 Frobenius 范数不大于  $\varepsilon_{AB}$ 、 $\varepsilon_{BA}$ 、 $\varepsilon_{AE}$ 、 $\varepsilon_{BE}$ , 即信道误差谱半径分别为  $\varepsilon_{AB}$ 、 $\varepsilon_{BA}$ 、 $\varepsilon_{AE}$ 、 $\varepsilon_{BE}$ , 其取值范围为  $[0, +\infty)$ 。 $\mathcal{H}_1$ 、 $\mathcal{H}_2$ 、 $\mathcal{G}_1$ 、 $\mathcal{G}_2$  分别表示真实信道矩阵  $\mathbf{H}_{AB}$ 、 $\mathbf{H}_{BA}$ 、 $\mathbf{G}_{AE}$ 、 $\mathbf{G}_{BE}$  的取值集合。

基于式(28)所示的信道估计误差模型, 本文以最大化最坏情况下的保密和速率为目标对系统信息信号以及人工噪声的预编码矩阵进行稳健设计, 优化问题可以表示为

$$\begin{aligned} \max_{\mathbf{S}_A, \mathbf{S}_B, \mathbf{Z}_A, \mathbf{Z}_B} \quad & \min_{\substack{\mathbf{H}_{AB} \in \mathcal{H}_1, \mathbf{H}_{BA} \in \mathcal{H}_2 \\ \mathbf{G}_{AE} \in \mathcal{G}_1, \mathbf{G}_{BE} \in \mathcal{G}_2}} R_S = [R_{BA} + R_{AB} - R_E]^+ \\ \text{s.t.} \quad & \|\mathbf{S}_A\|_F^2 + \|\mathbf{Z}_A\|_F^2 \leq P_A, \|\mathbf{S}_B\|_F^2 + \|\mathbf{Z}_B\|_F^2 \leq P_B \end{aligned} \quad (29)$$

因为考虑了信道的估计误差, 因此式(29)所示的优化问题比式(10)所示的优化问题更具挑战性, 用于求解式(10)的 DC 规划不再适用于式(29)。根据文献[23], 采用加权最小均方误差 WMMSE 算法对预编码矩阵进行稳健设计。为此先给出定理 1<sup>[23]</sup>。

**定理 1** 定义发送节点天线数为  $N_t$ , 接收节点天线数为  $N_r$ , 包含有用信息信号、干扰信号、传输噪声的接收信号为  $\mathbf{y} \in \mathbb{C}^{N_r \times 1}$ , 其协方差矩阵  $\mathbf{V} = E\{\mathbf{y}\mathbf{y}^H\}$ 。在接收节点处, 使用检测矩阵

$\mathbf{D} \in \mathbb{C}^{N_t \times N_t}$  对接收信号  $\mathbf{y}$  进行检测, 定义接收检测信号  $\hat{\mathbf{x}} = \mathbf{D}\mathbf{y}$  与发送信号  $\mathbf{x}$  的均方误差 (MSE, mean square error) 矩阵为

$$\mathbf{M} \triangleq (\mathbf{DHT} - \mathbf{I}_{N_t})(\mathbf{DHT} - \mathbf{I}_{N_t})^H + \mathbf{DND}^H \quad (30)$$

其中,  $\mathbf{H} \in \mathbb{C}^{N_r \times N_t}$  为信道矩阵,  $\mathbf{T} \in \mathbb{C}^{N_t \times N_t}$  为有用信息信号的发送预编码矩阵,  $\mathbf{I}_{N_t} \in \mathbb{C}^{N_t \times N_t}$  为单位矩阵,  $\mathbf{N} \succeq \mathbf{0}$  为接收信号中的干扰和噪声的协方差矩阵。则有式(31)和式(32)成立。

$$-\text{lb}|\mathbf{V}| = \max_{\mathbf{W} > \mathbf{0}} \text{lb}|\mathbf{W}| - \text{Tr}(\mathbf{WV}) + \text{Tr}(\mathbf{I}_{N_t}) \quad (31)$$

$$\text{lb} \left| \mathbf{I}_{N_t} + \frac{\mathbf{HTT}^H \mathbf{H}^H}{\mathbf{N}} \right| = \max_{\mathbf{W} > \mathbf{0}, \mathbf{D}} \text{lb}|\mathbf{W}| - \text{Tr}(\mathbf{WM}) + \text{Tr}(\mathbf{I}_{N_t}) \quad (32)$$

其中, 中间变量  $\mathbf{W}$  为实矩阵, 表示接收节点的权重矩阵。

在节点 A 处使用检测矩阵  $\mathbf{D}_A$  对接收信号  $\mathbf{y}_A$  (式(3)所示) 进行处理, 可得检测信号  $\hat{\mathbf{x}}_A$  为

$$\hat{\mathbf{x}}_A = \mathbf{D}_A \mathbf{y}_A = \mathbf{D}_A \mathbf{H}_{BA} \mathbf{S}_B \mathbf{u}_B + \mathbf{D}_A \mathbf{H}_{BA} \mathbf{Z}_B \mathbf{m}_B + \sqrt{\rho_A} \mathbf{D}_A \mathbf{H}_{AA} (\mathbf{S}_A \mathbf{u}_A + \mathbf{Z}_A \mathbf{m}_A) + \mathbf{D}_A \mathbf{n}_A \quad (33)$$

节点 A 的 MSE 矩阵  $\mathbf{M}_A$  为

$$\begin{aligned} \mathbf{M}_A &= (\mathbf{D}_A \mathbf{H}_{BA} \mathbf{S}_B - \mathbf{I}_{N_t}) \cdot \\ & (\mathbf{D}_A \mathbf{H}_{BA} \mathbf{S}_B - \mathbf{I}_{N_t})^H + \mathbf{D}_A \mathbf{N}_A \mathbf{D}_A^H \end{aligned} \quad (34)$$

其中,  $\mathbf{N}_A = \sigma_A^2 \mathbf{I}_{N_t} + \mathbf{H}_{BA} \mathbf{Z}_B \mathbf{Z}_B^H \mathbf{H}_{BA}^H + \rho_A \mathbf{H}_{AA} \mathbf{S}_A \mathbf{S}_A^H \mathbf{H}_{AA}^H + \rho_A \mathbf{H}_{AA} \mathbf{Z}_A \mathbf{Z}_A^H \mathbf{H}_{AA}^H$  为节点 A 接收信号  $\mathbf{y}_A$  中的干扰与噪声的协方差矩阵。

根据式(32), 节点 B 到节点 A 的信息传输速率  $R_{BA}$  的 (即式(6)) 可进一步转换为

$$\begin{aligned} R_{BA} &= \text{lb} \left| \mathbf{I}_{N_t} + \frac{\mathbf{H}_{BA} \mathbf{S}_B \mathbf{S}_B^H \mathbf{H}_{BA}^H}{\mathbf{N}_A} \right| = \\ & \max_{\mathbf{W}_A > \mathbf{0}, \mathbf{D}_A} \text{lb}|\mathbf{W}_A| - \text{Tr}(\mathbf{W}_A \mathbf{M}_A) + \text{Tr}(\mathbf{I}_{N_t}) \end{aligned} \quad (35)$$

其中,  $\mathbf{W}_A$  为节点 A 处的权重矩阵。

同理, 节点 B 的 MSE 矩阵  $\mathbf{M}_B$  为

$$\begin{aligned} \mathbf{M}_B &= (\mathbf{D}_B \mathbf{H}_{AB} \mathbf{S}_A - \mathbf{I}_{N_t}) \cdot \\ & (\mathbf{D}_B \mathbf{H}_{AB} \mathbf{S}_A - \mathbf{I}_{N_t})^H + \mathbf{D}_B \mathbf{N}_B \mathbf{D}_B^H \end{aligned} \quad (36)$$

其中,  $\mathbf{N}_B = \sigma_B^2 \mathbf{I}_{N_t} + \mathbf{H}_{AB} \mathbf{Z}_A \mathbf{Z}_A^H \mathbf{H}_{AB}^H + \rho_B \mathbf{H}_{BB} \mathbf{S}_B \mathbf{S}_B^H \mathbf{H}_{BB}^H + \rho_B \mathbf{H}_{BB} \mathbf{Z}_B \mathbf{Z}_B^H \mathbf{H}_{BB}^H$  为节点 B 接收信号  $\mathbf{y}_B$  中的干扰与噪声的协方差矩阵,  $\mathbf{D}_B$  为节点 B 的接收检测矩阵。节点 A 到节点 B 的信息传输速率  $R_{AB}$  (即式(7)) 可转换为

$$R_{AB} = \text{lb} \left| \mathbf{I}_{N_r} + \frac{\mathbf{H}_{AB} \mathbf{S}_A \mathbf{S}_A^H \mathbf{H}_{AB}^H}{N_B} \right| = \max_{\mathbf{W}_B > \mathbf{0}, \mathbf{D}_B} \text{lb} |\mathbf{W}_B| - \text{Tr}(\mathbf{W}_B \mathbf{M}_B) + \text{Tr}(\mathbf{I}_{N_r}) \quad (37)$$

其中,  $\mathbf{W}_B$  为节点 B 处的权重矩阵。

对于窃听速率  $R_E$  (即式(8)), 首先将其转换为

$$R_E = \text{lb} \left| \underbrace{\sigma_E^2 \mathbf{I}_{N_E} + \mathbf{A}_E + \mathbf{G}_{AE} \mathbf{Z}_A \mathbf{Z}_A^H \mathbf{G}_{AE}^H + \mathbf{G}_{BE} \mathbf{Z}_B \mathbf{Z}_B^H \mathbf{G}_{BE}^H}_{=R_{E1}} \right| - \underbrace{\text{lb} \left| \sigma_E^2 \mathbf{I}_{N_E} + \mathbf{G}_{AE} \mathbf{Z}_A \mathbf{Z}_A^H \mathbf{G}_{AE}^H + \mathbf{G}_{BE} \mathbf{Z}_B \mathbf{Z}_B^H \mathbf{G}_{BE}^H \right|}_{=R_{E2}} \quad (38)$$

其中,  $\mathbf{A}_E = \mathbf{G}_{AE} \mathbf{S}_A \mathbf{S}_A^H \mathbf{G}_{AE}^H + \mathbf{G}_{BE} \mathbf{S}_B \mathbf{S}_B^H \mathbf{G}_{BE}^H$ 。令  $\mathbf{V}_E = \sigma_E^2 \mathbf{I}_{N_E} + \mathbf{A}_E + \mathbf{G}_{AE} \mathbf{Z}_A \mathbf{Z}_A^H \mathbf{G}_{AE}^H + \mathbf{G}_{BE} \mathbf{Z}_B \mathbf{Z}_B^H \mathbf{G}_{BE}^H$ ,  $\mathbf{V}_E$  为接收信号  $\mathbf{y}_E$  (式(5)) 的协方差矩阵, 根据式(31),  $R_{E1}$  可转换为

$$-R_{E1} = -\text{lb} |\mathbf{V}_E| = \max_{\mathbf{W}_{E1} > \mathbf{0}} \text{lb} |\mathbf{W}_{E1}| - \text{Tr}(\mathbf{W}_{E1} \mathbf{V}_E) + \text{Tr}(\mathbf{I}_{N_E}) \quad (39)$$

其中,  $\mathbf{W}_{E1}$  为中间变量, 表示节点 E 的权重矩阵。

$R_{E2}$  可转换为

$$R_{E2} = \text{lb} \left| \mathbf{I}_{N_E} + \frac{\mathbf{G}_{AE} \mathbf{Z}_A \mathbf{Z}_A^H \mathbf{G}_{AE}^H + \mathbf{G}_{BE} \mathbf{Z}_B \mathbf{Z}_B^H \mathbf{G}_{BE}^H}{\sigma_E^2} \right| + N_E \text{lb} \sigma_E^2 = \text{lb} \left| \mathbf{I}_{N_E} + \frac{\mathbf{X}_{E2} \mathbf{X}_{E2}^H}{\sigma_E^2} \right| + N_E \text{lb} \sigma_E^2 \quad (40)$$

其中,  $\mathbf{X}_{E2} = [\mathbf{G}_{AE} \mathbf{Z}_A, \mathbf{G}_{BE} \mathbf{Z}_B]$ 。令式(32)中的  $\mathbf{H}\mathbf{T} = \mathbf{X}_{E2}$ ,  $R_{E2}$  可转换为

$$R_{E2} = \max_{\mathbf{W}_{E2} > \mathbf{0}, \mathbf{D}_E} \text{lb} |\mathbf{W}_{E2}| - \text{Tr}(\mathbf{W}_{E2} \mathbf{M}_E) + \text{Tr}(\mathbf{I}_{N_E}) + N_E \text{lb} \sigma_E^2 \quad (41)$$

其中,  $\mathbf{D}_E$  为节点 E 处的接收检测矩阵,  $\mathbf{W}_{E2}$  为中间变量,  $\mathbf{M}_E$  为 MSE 矩阵, 其表达式为

$$\mathbf{M}_E = (\mathbf{D}_E [\mathbf{G}_{AE} \mathbf{Z}_A, \mathbf{G}_{BE} \mathbf{Z}_B] - \mathbf{I}) \cdot (\mathbf{D}_E [\mathbf{G}_{AE} \mathbf{Z}_A, \mathbf{G}_{BE} \mathbf{Z}_B] - \mathbf{I})^H + \sigma_E^2 \mathbf{D}_E \mathbf{D}_E^H \quad (42)$$

将式(35)、式(37)、式(39)、式(41)代入式(29), 并忽略常数项, 优化问题可以重写为

$$\max_{\substack{\mathbf{S}_i, \mathbf{Z}_j, \mathbf{H}_{AB} \in \mathcal{H}_4, \mathbf{H}_{BA} \in \mathcal{H}_2 \\ \mathbf{W}_j, \mathbf{D}_k, \mathbf{G}_{AE} \in \mathcal{G}_1, \mathbf{G}_{BE} \in \mathcal{G}_2}} \min \text{lb} |\mathbf{W}_A| + \text{lb} |\mathbf{W}_B| + \text{lb} |\mathbf{W}_{E1}| + \text{lb} |\mathbf{W}_{E2}| - \text{Tr}(\mathbf{W}_A \mathbf{M}_A) - \text{Tr}(\mathbf{W}_B \mathbf{M}_B) - \text{Tr}(\mathbf{W}_{E1} \mathbf{V}_E) - \text{Tr}(\mathbf{W}_{E2} \mathbf{M}_E) \quad (43)$$

其中,  $i \in \{A, B\}$ ,  $j \in \{A, B, E1, E2\}$ ,  $k \in \{A, B, E\}$ 。

通过引入松弛变量  $\{\beta_A, \beta_B, \beta_{E1}, \beta_{E2}\}$ , 式(43)可

以进一步改写为

$$\max_{\mathbf{S}_i, \mathbf{Z}_j, \mathbf{W}_j, \mathbf{D}_k} \text{lb} |\mathbf{W}_A| + \text{lb} |\mathbf{W}_B| + \text{lb} |\mathbf{W}_{E1}| + \text{lb} |\mathbf{W}_{E2}| - \beta_A - \beta_B - \beta_{E1} - \beta_{E2} \quad (44a)$$

$$\text{s.t. } \text{Tr}(\mathbf{W}_A \mathbf{M}_A) \leq \beta_A, \forall \mathbf{H}_{BA} \in \mathcal{H}_2 \quad (44b)$$

$$\text{Tr}(\mathbf{W}_B \mathbf{M}_B) \leq \beta_B, \forall \mathbf{H}_{AB} \in \mathcal{H}_1 \quad (44c)$$

$$\text{Tr}(\mathbf{W}_{E1} \mathbf{V}_E) \leq \beta_{E1}, \forall \mathbf{G}_{AE} \in \mathcal{G}_1, \forall \mathbf{G}_{BE} \in \mathcal{G}_2 \quad (44d)$$

$$\text{Tr}(\mathbf{W}_{E2} \mathbf{M}_E) \leq \beta_{E2}, \forall \mathbf{G}_{AE} \in \mathcal{G}_1, \forall \mathbf{G}_{BE} \in \mathcal{G}_2 \quad (44e)$$

$$\|\mathbf{S}_A\|_F^2 + \|\mathbf{Z}_A\|_F^2 \leq P_A, \|\mathbf{S}_B\|_F^2 + \|\mathbf{Z}_B\|_F^2 \leq P_B \quad (44f)$$

尽管式(44)所示的优化目标函数是上凸的, 但是由于真实的信道矩阵随机分布在谱半径分别为  $\varepsilon_{AB}$ 、 $\varepsilon_{BA}$ 、 $\varepsilon_{AE}$ 、 $\varepsilon_{BE}$  的空间, 因此式(44b)~式(44e)所示的约束条件并不是有限个, 对式(44)所示问题的求解依然具有很高的难度。接下来通过消除信道的估计误差项对约束条件进行转化, 再对问题进行求解。

根据  $\text{Tr}(\mathbf{X}\mathbf{X}^H) = \|\text{vec}(\mathbf{X})\|^2$ , 其中  $\text{vec}(\cdot)$  表示按列序对矩阵进行向量化,  $\|\cdot\|$  表示向量的 2 范数, 式(44b)所示约束条件中的  $\text{Tr}(\mathbf{W}_A \mathbf{M}_A)$  因  $\mathbf{M}_A$  满足  $\mathbf{X}\mathbf{X}^H$  的形式, 而  $\mathbf{W}_A$  是实矩阵, 因此,  $\text{Tr}(\mathbf{W}_A \mathbf{M}_A)$  可表示为

$$\text{Tr}(\mathbf{W}_A \mathbf{M}_A) = \left\| \begin{bmatrix} \text{vec}(\Gamma_A \mathbf{D}_A \mathbf{H}_{BA} \mathbf{S}_B - \Gamma_A) \\ \text{vec}(\Gamma_A \mathbf{D}_A \mathbf{H}_{BA} \mathbf{Z}_B) \\ \text{vec}(\Gamma_A \mathbf{D}_A \hat{\mathbf{H}}_{AA} \mathbf{S}_A) \\ \text{vec}(\Gamma_A \mathbf{D}_A \hat{\mathbf{H}}_{AA} \mathbf{Z}_A) \\ \text{vec}(\sigma_A \Gamma_A \mathbf{D}_A) \end{bmatrix} \right\|^2 \quad (45)$$

其中,  $\hat{\mathbf{H}}_{AA} = \sqrt{\rho_A} \mathbf{H}_{AA}$ ,  $\Gamma_A = \mathbf{W}_A^{\frac{1}{2}}$  (表示  $\mathbf{W}_A$  的元素开方)。进一步将式(28)代入式(45), 可得到

$$\text{Tr}(\mathbf{W}_A \mathbf{M}_A) = \|\boldsymbol{\Theta}_A\|^2 \quad (46)$$

$$\text{其中, } \boldsymbol{\Theta}_A = \begin{bmatrix} \text{vec}(\Gamma_A \mathbf{D}_A (\hat{\mathbf{H}}_{BA} + \mathbf{A}_{BA}) \mathbf{S}_B - \Gamma_A) \\ \text{vec}(\Gamma_A \mathbf{D}_A (\hat{\mathbf{H}}_{BA} + \mathbf{A}_{BA}) \mathbf{Z}_B) \\ \text{vec}(\Gamma_A \mathbf{D}_A \hat{\mathbf{H}}_{AA} \mathbf{S}_A) \\ \text{vec}(\Gamma_A \mathbf{D}_A \hat{\mathbf{H}}_{AA} \mathbf{Z}_A) \\ \text{vec}(\sigma_A \Gamma_A \mathbf{D}_A) \end{bmatrix}.$$

根据  $\text{vec}(\mathbf{X}\mathbf{Y}\mathbf{Z}) = (\mathbf{Z}^T \otimes \mathbf{X}) \text{vec}(\mathbf{Y})$  (其中,  $\otimes$  表示矩阵张量积), 可得到

$$\boldsymbol{\Theta}_A = \bar{\boldsymbol{\Theta}}_A + \boldsymbol{\Omega}_A \text{vec}(\mathbf{A}_{BA}) \quad (47)$$

$$\text{其中, } \bar{\Theta}_A = \begin{bmatrix} \text{vec}(\Gamma_A D_A \hat{H}_{BA} S_B - \Gamma_A) \\ \text{vec}(\Gamma_A D_A \hat{H}_{BA} Z_B) \\ \text{vec}(\Gamma_A D_A \hat{H}_{AA} S_A) \\ \text{vec}(\Gamma_A D_A \hat{H}_{AA} Z_A) \\ \text{vec}(\sigma_A \Gamma_A D_A) \end{bmatrix}, \Omega_A = \begin{bmatrix} S_B^T \otimes (\Gamma_A D_A) \\ Z_B^T \otimes (\Gamma_A D_A) \\ \mathbf{0}_{(2N_t^2+N_t N_r) \times (N_t N_r)} \end{bmatrix}.$$

根据式(46)和式(47), 式(44b)所示的约束条件可改写为

$$\begin{aligned} \text{Tr}(W_A M_A) \leq \beta_A &\Rightarrow \beta_A - \|\bar{\Theta}_A + \Omega_A \text{vec}(A_{BA})\|^2 \geq 0 \\ &\Rightarrow \beta_A - (\bar{\Theta}_A^H + \text{vec}(A_{BA})^H \Omega_A^H) I_{L \times L} (\bar{\Theta}_A + \Omega_A \text{vec}(A_{BA})) \geq 0 \end{aligned} \quad (48)$$

其中,  $L = 2N_t^2 + 3N_t N_r$ .

根据 Schur 引理<sup>[24]</sup>, 分块矩阵  $X = \begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix}$ ,

$K_4 \succ 0$  且  $X$  的 Schur 补  $K_1 - K_2 K_4^{-1} K_3 \succeq 0$ , 等价于  $X \succeq 0$ . 令  $K_1 = \beta_A$ ;  $K_2 = \bar{\Theta}_A^H + \text{vec}(A_{BA})^H \Omega_A^H$ ;  $K_3 = \bar{\Theta}_A + \Omega_A \text{vec}(A_{BA})$ ;  $K_4$  为单位矩阵, 即  $K_4 = I_{L \times L}$ ;  $\beta_A - (\bar{\Theta}_A^H + \text{vec}(A_{BA})^H \Omega_A^H) I_{L \times L} (\bar{\Theta}_A + \Omega_A \text{vec}(A_{BA}))$  为

$$\begin{bmatrix} \beta_A & \bar{\Theta}_A^H + \text{vec}(A_{BA})^H \Omega_A^H \\ \bar{\Theta}_A + \Omega_A \text{vec}(A_{BA}) & I_{L \times L} \end{bmatrix}$$

的 Schur 补, 且满足大于或等于 0, 因此可得

$$\begin{aligned} &\begin{bmatrix} \beta_A & \bar{\Theta}_A^H + \text{vec}(A_{BA})^H \Omega_A^H \\ \bar{\Theta}_A + \Omega_A \text{vec}(A_{BA}) & I_{L \times L} \end{bmatrix} \succeq 0 \Rightarrow \\ &\begin{bmatrix} \beta_A & \bar{\Theta}_A^H \\ \bar{\Theta}_A & I_{L \times L} \end{bmatrix} \succeq - \begin{bmatrix} 0 & \text{vec}(A_{BA})^H \Omega_A^H \\ \Omega_A \text{vec}(A_{BA}) & 0_{L \times L} \end{bmatrix} \end{aligned} \quad (49)$$

式(49)中依然包含信道估计误差项  $A_{BA}$ , 为将其移除, 需要引进 sign-definiteness 定理.

**定理 2**<sup>[22]</sup> 给定 Hermitian 矩阵  $C$  和任意矩阵  $\{P_i, Q_i\}_{i=1}^N$ , 则半无限的线性矩阵不等式  $C \succeq \sum_{i=1}^N (P_i^H Y_i Q_i + Q_i^H Y_i^H P_i)$ ,  $\forall Y_i: \|Y_i\| \leq \varepsilon_i$  成立的充要条件是当且仅当存在非负实数  $\lambda_1, \lambda_2, \dots, \lambda_N$  满足

$$\begin{bmatrix} C - \sum_{i=1}^N \lambda_i Q_i^H Q_i & -\varepsilon_1 P_1^H & \dots & -\varepsilon_N P_N^H \\ -\varepsilon_1 P_1 & \lambda_1 I & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -\varepsilon_N P_N & 0 & \dots & \lambda_N I \end{bmatrix} \succeq 0 \quad (50)$$

根据定理 2, 定义  $C_A = \begin{bmatrix} \beta_A & \bar{\Theta}_A^H \\ \bar{\Theta}_A & I \end{bmatrix}$ ,  $P_A = \begin{bmatrix} 0, \Omega_A^H \end{bmatrix}$ ,

$Q_A = [-1, 0_{1 \times L}]$ , 则式(49)可以表示为式(51)所示等价的线性矩阵不等式的形式.

$$\begin{bmatrix} \beta_A - \lambda_A & \bar{\Theta}_A^H \\ \bar{\Theta}_A & I \end{bmatrix} - \varepsilon_{BA} P_A^H \succeq 0 \quad (51)$$

类似地, 可以将式(44c)~式(44e)分别写为

$$\begin{bmatrix} \beta_B - \lambda_B & \bar{\Theta}_B^H \\ \bar{\Theta}_B & I \end{bmatrix} - \varepsilon_{AB} P_B^H \succeq 0 \quad (52)$$

$$\begin{bmatrix} \beta_{E1} - \lambda_{E1} - \lambda_{E2} & \bar{\Theta}_{E1}^H \\ \bar{\Theta}_{E1} & I \end{bmatrix} - \varepsilon_{AE} P_{E1}^H - \varepsilon_{BE} P_{E2}^H \succeq 0 \quad (53)$$

$$\begin{bmatrix} \beta_{E2} - \lambda_{E3} - \lambda_{E4} & \bar{\Theta}_{E2}^H \\ \bar{\Theta}_{E2} & I \end{bmatrix} - \varepsilon_{AE} P_{E3}^H - \varepsilon_{BE} P_{E4}^H \succeq 0 \quad (54)$$

其中, 矩阵  $P_B = \begin{bmatrix} 0, \Omega_B^H \end{bmatrix}$ ,  $P_{E1} = \begin{bmatrix} 0, \Omega_{E1}^H \end{bmatrix}$ ,  $P_{E2} = \begin{bmatrix} 0, \Omega_{E2}^H \end{bmatrix}$ ,  $P_{E3} = \begin{bmatrix} 0, \Omega_{E3}^H \end{bmatrix}$ ,  $P_{E4} = \begin{bmatrix} 0, \Omega_{E4}^H \end{bmatrix}$ ,

$$\bar{\Theta}_B = \begin{bmatrix} \text{vec}(\Gamma_B D_B \hat{H}_{AB} S_A - \Gamma_B) \\ \text{vec}(\Gamma_B D_B \hat{H}_{AB} Z_A) \\ \text{vec}(\Gamma_B D_B \hat{H}_{BB} S_B) \\ \text{vec}(\Gamma_B D_B \hat{H}_{BB} Z_B) \\ \text{vec}(\sigma_B \Gamma_B D_B) \end{bmatrix}, \bar{\Theta}_{E1} = \begin{bmatrix} \text{vec}(\Gamma_{E1} \hat{G}_{AE} S_A) \\ \text{vec}(\Gamma_{E1} \hat{G}_{AE} Z_A) \\ \text{vec}(\Gamma_{E1} \hat{G}_{BE} S_B) \\ \text{vec}(\Gamma_{E1} \hat{G}_{BE} Z_B) \\ \text{vec}(\sigma_E \Gamma_{E1}) \end{bmatrix},$$

$$\bar{\Theta}_{E2} = \begin{bmatrix} \text{vec}(\Gamma_{E2} D_E \hat{G}_{AE} Z_A - \Gamma_{E2,1}) \\ \text{vec}(\Gamma_{E2} D_E \hat{G}_{BE} Z_B - \Gamma_{E2,2}) \\ \text{vec}(\sigma_E \Gamma_{E2} D_E) \end{bmatrix}.$$

其中,  $\Gamma_B = W_B^{\frac{1}{2}}$ ,  $\Gamma_{E1} = W_{E1}^{\frac{1}{2}}$ ,  $\Gamma_{E2} = W_{E2}^{\frac{1}{2}}$ ,  $\Gamma_{E2,1}$  表示矩阵  $\Gamma_{E2}$  的前  $N_t$  列,  $\Gamma_{E2,2}$  为  $\Gamma_{E2}$  的后  $N_t$  列,

$$\Omega_B = \begin{bmatrix} S_A^T \otimes (\Gamma_B D_B) \\ Z_A^T \otimes (\Gamma_B D_B) \\ \mathbf{0}_{(2N_t^2+N_t N_r) \times N_t N_r} \end{bmatrix}, \Omega_{E1} = \begin{bmatrix} S_A^T \otimes \Gamma_{E1} \\ Z_A^T \otimes \Gamma_{E1} \\ \mathbf{0}_{(N_E(2N_t+N_r)) \times N_t N_E} \end{bmatrix},$$

$$\Omega_{E2} = \begin{bmatrix} \mathbf{0}_{2N_t N_E \times N_t N_E} \\ S_B^T \otimes \Gamma_{E1} \\ Z_B^T \otimes \Gamma_{E1} \\ \mathbf{0}_{N_E^2 \times N_t N_E} \end{bmatrix}, \Omega_{E3} = \begin{bmatrix} Z_A^T \otimes (\Gamma_{E2} D_E) \\ \mathbf{0}_{(2N_t(N_t+N_r)) \times N_t N_E} \end{bmatrix},$$

$$\boldsymbol{\Omega}_{E4} = \begin{bmatrix} \mathbf{0}_{(2N_t^2) \times (N_t N_E)} \\ \mathbf{Z}_B^T \otimes (\boldsymbol{\Gamma}_{E2} \mathbf{D}_E) \\ \mathbf{0}_{(2N_t N_E) \times (N_t N_E)} \end{bmatrix}.$$

根据式(51)~式(54), 式(44)所示优化问题可以改写为

$$\begin{aligned} \text{P2: } & \max_{\mathbf{S}_i, \mathbf{Z}_i, \boldsymbol{\Gamma}_j, \mathbf{D}_k, \beta_A, \beta_B, \beta_{E1}, \beta_{E2}} \zeta = \text{lb}|\mathbf{W}_A| + \text{lb}|\mathbf{W}_B| + \text{lb}|\mathbf{W}_{E1}| + \\ & \text{lb}|\mathbf{W}_{E2}| - \beta_A - \beta_B - \beta_{E1} - \beta_{E2} \\ \text{s.t. } & \text{式(51)~式(54), 式(44f)} \end{aligned} \quad (55)$$

其中,  $\zeta$  为优化的目标函数,  $l \in \{A, B, E1, E2, E3, E4\}$ 。

式(55)消除了不确定的信道估计误差项, 但是优化目标函数包括了多个变量, 式(55)所示优化问题依然是非凸的, 但若矩阵  $\{\mathbf{S}_i, \mathbf{Z}_i, \boldsymbol{\Gamma}_j\}$  固定, 式(55)中的优化目标函数为关于  $\mathbf{D}_k$  的上凸函数; 同理, 当  $\boldsymbol{\Gamma}_j$  (或者  $\mathbf{S}_i$ 、 $\mathbf{Z}_i$ ) 之外的其他矩阵固定时, 优化目标函数也为关于  $\boldsymbol{\Gamma}_j$  (或者  $\mathbf{S}_i$ 、 $\mathbf{Z}_i$ ) 的上凸函数。因此, 可以采用迭代优化的方法对优化问题进行求解, 在每轮迭代中首先固定矩阵  $\{\mathbf{S}_i, \mathbf{Z}_i, \boldsymbol{\Gamma}_j\}$  为上轮迭代后的值, 对  $\mathbf{D}_k$  进行优化; 然后固定  $\mathbf{D}_k$  为本轮优化值,  $\mathbf{S}_i$ 、 $\mathbf{Z}_i$  为上轮优化值, 优化  $\boldsymbol{\Gamma}_j$ ; 接着, 固定  $\mathbf{D}_k$ 、 $\boldsymbol{\Gamma}_j$  为本轮优化值,  $\mathbf{Z}_i$  为上轮优化值, 优化  $\mathbf{S}_i$ ; 最后在固定  $\mathbf{S}_i$ 、 $\mathbf{D}_k$ 、 $\boldsymbol{\Gamma}_j$  为本轮优化值的情况下, 优化  $\mathbf{Z}_i$ 。优化算法总结如算法 2 所示, 其中,  $n$  为迭代轮数;  $\tau_2$  为取值较小的正常数, 用于判断迭代过程是否收敛, 即在  $|\zeta^{(n)} - \zeta^{(n-1)}| > \tau_2$  时继续迭代,  $\zeta^{(n)}$  是第  $n$  轮迭代的目标函数值。

**算法 2** 求解 P2 的 WMMSE 算法

$$\text{初始化 } n=0, \mathbf{S}_i^{(0)} = \sqrt{\frac{P_j}{2N_t}} \mathbf{I}_{N_t}, \mathbf{Z}_i^{(0)} = \sqrt{\frac{P_j}{2N_t}} \mathbf{I}_{N_t},$$

$$\boldsymbol{\Gamma}_j^{(0)} = \mathbf{I}, \zeta^{(0)} = 0$$

1) do

2)  $n=n+1$

3) 固定  $\mathbf{S}_i = \mathbf{S}_i^{(n-1)}$ ,  $\mathbf{Z}_i = \mathbf{Z}_i^{(n-1)}$ ,  $\boldsymbol{\Gamma}_j = \boldsymbol{\Gamma}_j^{(n-1)}$ ,

使 P2 的目标函数为  $\mathbf{D}_k$  的上凸函数, 优化矩阵  $\mathbf{D}_k$ , 得优化值  $\mathbf{D}_k^{(n)}$

4) 固定  $\mathbf{S}_i = \mathbf{S}_i^{(n-1)}$ ,  $\mathbf{Z}_i = \mathbf{Z}_i^{(n-1)}$ ,  $\mathbf{D}_k = \mathbf{D}_k^{(n)}$ , 使 P2 的目标函数为  $\boldsymbol{\Gamma}_j$  的上凸函数, 优化矩阵  $\boldsymbol{\Gamma}_j$ , 得优化值  $\boldsymbol{\Gamma}_j^{(n)}$

5) 固定  $\mathbf{Z}_i = \mathbf{Z}_i^{(n-1)}$ 、 $\mathbf{D}_k = \mathbf{D}_k^{(n)}$ 、 $\boldsymbol{\Gamma}_j = \boldsymbol{\Gamma}_j^{(n)}$ ,

使 P2 的目标函数为  $\mathbf{S}_i$  的上凸函数, 优化矩阵  $\mathbf{S}_i$ , 得优化值  $\mathbf{S}_i^{(n)}$

6) 固定  $\mathbf{S}_i = \mathbf{S}_i^{(n)}$ 、 $\mathbf{D}_k = \mathbf{D}_k^{(n)}$ 、 $\boldsymbol{\Gamma}_j = \boldsymbol{\Gamma}_j^{(n)}$ ,

使 P2 的目标函数为  $\mathbf{Z}_i$  的上凸函数, 优化矩阵  $\mathbf{Z}_i$ , 得优化值  $\mathbf{Z}_i^{(n)}$

7) while  $|\zeta^{(n)} - \zeta^{(n-1)}| > \tau_2$

8)  $\mathbf{S}_i^* = \mathbf{S}_i^{(n)}$ ,  $\mathbf{Z}_i^* = \mathbf{Z}_i^{(n)}$ ,  $\boldsymbol{\Gamma}_j^* = \boldsymbol{\Gamma}_j^{(n)}$ ,  $\mathbf{D}_k^* = \mathbf{D}_k^{(n)}$

算法 2 的计算复杂度来自式(55)所示优化问题中目标函数的矩阵求解, 而矩阵求解是一个复杂度近似  $O((10N_t^2 + 2N_t N_r + 2N_t N_E + N_E^2)^{3.5} \lg(\frac{1}{\tau_2}))$  的半定优化, 因此, 算法 2 的复杂度可以表示为  $O(N_t(10N_t^2 + 2N_t N_r + 2N_t N_E + N_E^2)^{3.5} \lg(\frac{1}{\tau_2}))$ , 其中,  $N_t$  是算法 2 的迭代次数。

## 4 仿真结果与分析

本节对系统的性能进行仿真。仿真中, 所有信道为独立同分布的平坦瑞利衰落信道, 信道系数服从均值为 0、方差为 1 的复高斯分布; 噪声方差  $\sigma_A^2 = \sigma_B^2 = \sigma_E^2 = \sigma^2$ ; 自干扰残余因子  $\rho_A = \rho_B = 0.1$ ; 各信道估计误差矩阵满足复高斯分布, 设置相同的信道估计误差谱半径, 即  $\varepsilon_{AB} = \varepsilon_{BA} = \varepsilon_{AE} = \varepsilon_{BE} = \varepsilon$ ; 算法 1 和算法 2 中的参数  $\tau_1 = \tau_2 = 0.01$ 。如无特别说明, 仿真中合法节点天线数  $N=4$ , 其中  $N_t=2, N_r=2$ ; 窃听节点天线数  $N_E=2$ 。节点的功率  $P_A = P_B = P$ 。

### 4.1 信道状态信息完美场景下的仿真

首先对 DC 规划的收敛性进行仿真。图 2 给出了 CSI 完美时随机产生的 3 组信道下的保密和速率与迭代次数的关系, 仿真中节点 A、B 的发送功率与信道噪声功率的比值  $\frac{P}{\sigma^2}$  设置为 10 dB。从图 2 可知迭代开始时, 保密和速率随迭代的进行迅速提高, 大约经过 3~5 次迭代算法即收敛, 且不同信道状态下变化情况类似, 说明 DC 规划算法的收敛速率较快, 收敛性能较好。

为了评估人工噪声对系统保密性能的影响, 图 3 仿真了有人工噪声和无人工噪声 2 种情况下系统保密和速率随  $\frac{P}{\sigma^2}$  的变化情况, 保密和速率值是 1 000 组信道样本下的保密速率的平均值。从图 3 可以看

出, 虽然发送人工噪声占用了一定的功率, 使信号功率降低, 但人工噪声可以有效地对窃听者形成干扰, 提高系统的保密和速率。随着发送功率的增大, 二者保密和速率的差距由 0.08 bit/(s·Hz) ( $\frac{P}{\sigma^2}=0$ ) 增加到近 1.15 bit/(s·Hz) ( $\frac{P}{\sigma^2}=10$  dB)。这是因为在没有人工噪声的情况下, 虽然信号功率增加, 合法信道的传输速率增大, 但是由于缺少人工噪声的保护, 窃听节点对保密信息的窃听速率也在增大。而采用人工噪声的系统, 在总功率增加时, 可适当增加人工噪声的功率, 增大对窃听者的干扰, 使窃听速率的增长速度明显低于合法信道传输速率的增长速度, 因此系统的保密和速率能以更快的速度提高。

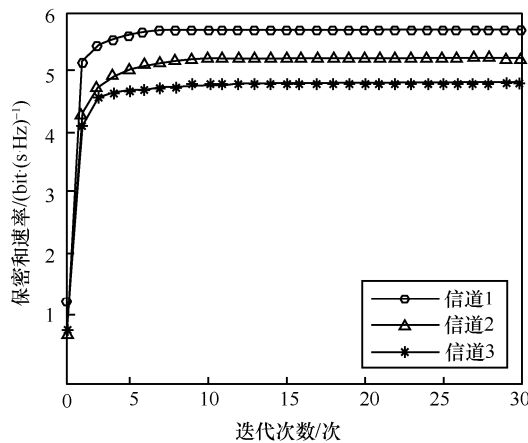


图 2 保密和速率与迭代次数的关系

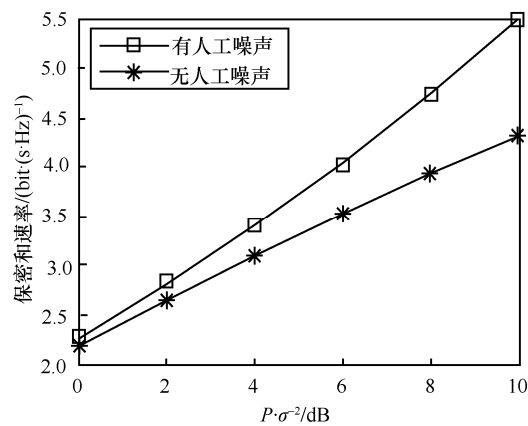


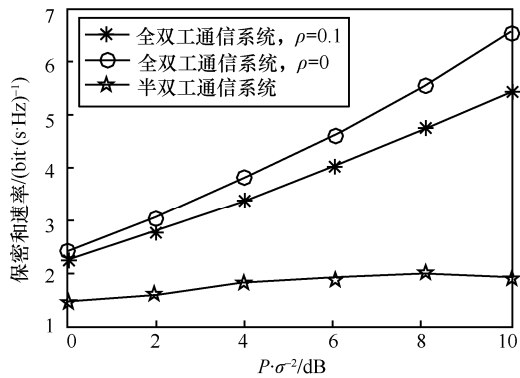
图 3 有人工噪声和无人工噪声情况下系统保密和速率比较

为了反映全双工自干扰残余因子对系统信息传输速率的影响, 图 4(a)中给出了全双工自干扰残余因子固定为 0.1 和 0 时系统保密和速率随  $\frac{P}{\sigma^2}$  变化

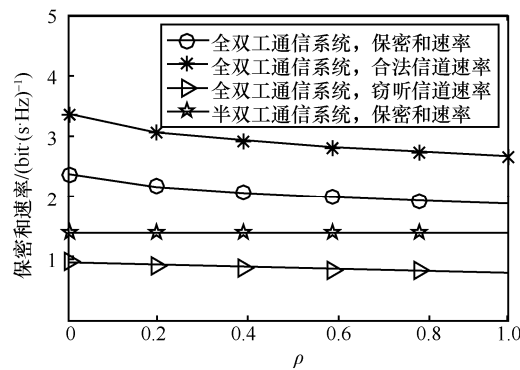
的情况, 图 4(b)中给出了  $\frac{P}{\sigma^2}=0$  时系统信息传输速率随自干扰残余因子变化的情况。同时给出了半双工通信系统的传输速率作为对比。其中, 信息传输速率值是 1 000 组信道样本下传输速率的平均值。在半双工通信系统中, 信息单向传输, 节点 A 在发送信息的同时协同发送人工噪声, 节点 B 仅进行信号的接收, 半双工发送节点的发送功率为单个全双工节点发送功率的两倍。从图 4(a)可以看出,  $\rho=0.1$  时的系统保密和速率低于  $\rho=0$  时的保密和速率。当  $\rho=0$  时, 意味着全双工节点的自干扰已完全消除, 发送的信号并不会对信号接收产生影响, 此情况较为理想, 实际较难达到。观察图 4(a)可知, 半双工通信系统的保密和速率明显低于全双工通信系统, 且两者之间的差距随着  $\frac{P}{\sigma^2}$  的增加而明显增大, 当自干扰残余因子为 0.1 时, 随着  $\frac{P}{\sigma^2}$  从 0 增加到 10 dB, 全双工系统与半双工系统的保密和速率之差从 0.83 bit/(s·Hz) 增加到 3.53 bit/(s·Hz)。这是因为与半双工通信相比, 全双工通信的频谱效率更高, 且节点 A、B 同时协同发送人工噪声, 即有 4 根天线发送人工噪声, 相较于半双工通信中仅一个节点的 2 根天线发送人工噪声, 能对窃听节点形成更有效的干扰。图 4(b)显示当  $\frac{P}{\sigma^2}$  固定时, 系统保密和速率随着全双工自干扰残余因子的增大而减小。由于本文方案在对信息信号和人工噪声的预编码矩阵进行优化的过程中考虑了全双工自干扰的影响, 即使是在自干扰残余因子达到 1 时, 全双工通信系统的保密和速率仍然显著高于半双工通信系统 (前者为后者的 1.35 倍)。

图 5 给出了合法节点配备不同收发天线数、窃听节点配备不同接收天线数下系统保密和速率随  $\frac{P}{\sigma^2}$  的变化情况。其中, 保密和速率值是 1 000 组信道样本下保密速率的平均值。从图 5 可以看出, 在合法收发天线数固定的情况下, 窃听者配备的天线越多, 系统保密和速率越低。在合法节点收发天线数为 2 的条件下, 窃听天线数为 3 时的保密和速率比窃听天线为 1 时的保密和速率小 3.82 bit/(s·Hz)。这是因为窃听者天线越多, 窃听节点拦截信息信号的能力越强, 窃听速率越高, 相应保密和速率越低。

图 5 显示在窃听天线数一样的情况下，合法节点的收发天线数越多，系统的保密和速率越大。合法节点的收发天线数越多，合法信道的传输速率越高，同时，合法节点的收发天线数越多，人工噪声的发送天线数越多，对窃听者的干扰效果越好，因此系统的保密和速率越高。



(a) 不同自干扰残余因子下的保密和速率



(b) 传输速率随自干扰残余因子变化的情况

图 4 全双工自干扰残余因子对系统安全传输性能的影响

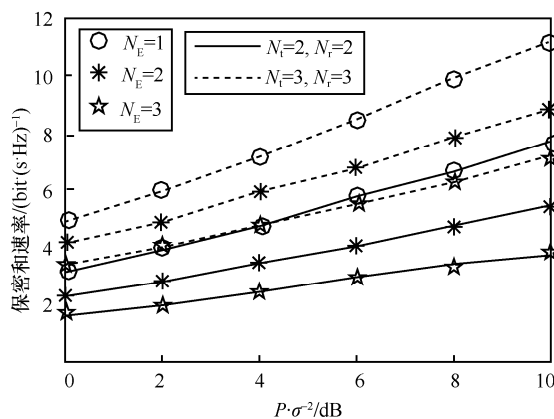
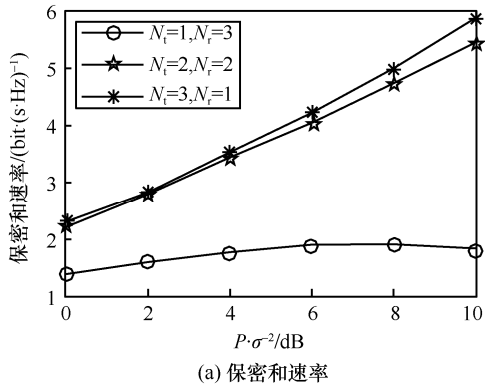


图 5 不同合法收发天线数和窃听天线数下的系统保密和速率随  $\frac{P}{\sigma^2}$  的变化

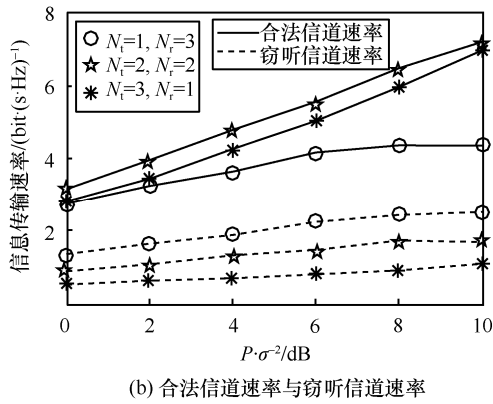
图 6 给出了窃听天线固定为  $N_E=2$  的场景下，在合法节点总天线数固定为  $N=4$ ，但分配不同数量

的收发天线时系统的信息传输速率随  $\frac{P}{\sigma^2}$  的变化情况，其中，图 6(a)为保密和速率的变化曲线，图 6(b)为合法信道速率与窃听信道速率的变化情况。信息传输速率值是 1 000 组信道样本下的平均值。从图 6(a)可以看出，当发送天线数不小于窃听天线数时，系统的平均保密和速率能随发送功率的增加而有持续增加；反之，若发送天线数小于窃听天线数，保密和速率不能随发送功率的增加而有较明显的增长。这是因为当发送人工噪声的天线数不低于窃听者的接收天线数时，窃听者的窃听能力就会被人工噪声有效地抑制。如图 6(b)所示，发送天线数越多，人工噪声对窃听者的干扰越大。图 6(b)还显示，对于合法信道而言，当收发天线数量相同时，能获得最高的传输速率，这与 MIMO 通信系统的特性是相符的；3 根发送天线一根接收天线时的传输速率高于一根发送天线 3 根接收天线时的传输速率，这是由于全双工系统中收发通道间存在自干扰，本文方案优化时考虑了该因素，当有多根发送天线时，特别是发送天线多于接收天线时，能够通过控制信号和人工噪声的预编码矩阵，有效地降低发送信号对接收通道的干扰，而在发送天线数仅为一根时则无法进行预编码设计，自干扰强度更高。综合几个方面因素的影响，分配相同数量的发送和接收天线能获得最高的合法信道传输速率，而发送天线越多，对窃听者的干扰越有效，因此应分配相近数量的发送和接收天线，同时发送天线应不少于接收天线。

图 7 给出了本文算法和迫零算法的保密和速率随  $\frac{P}{\sigma^2}$  的变化情况，仿真中  $N_t=4$ 、 $N_r=2$ 、 $N_E=2$ 。信息传输速率值是 1 000 组信道样本下的平均值。在迫零算法中，信息信号和人工噪声分布在自干扰信道的零空间，因此全双工自干扰功率为 0。此时，全双工系统可以看作是存在窃听者的 2 个 MIMO 单向传输系统，系统的预编码矩阵可以采用文献[25]提出的奇异值分解方案进行设计。为保证零空间存在，迫零算法要求发送天线数大于接收天线数。从图 7 的仿真结果可以看出，本文算法相对于迫零算法具有更高的保密和速率，这是因为本文算法在考虑全双工自干扰影响的基础上，对信息信号和人工噪声的预编码矩阵进行了联合优化。



(a) 保密和速率



(b) 合法信道速率与窃听信道速率

图 6 合法节点不同收发天线分配时传输性能的对比

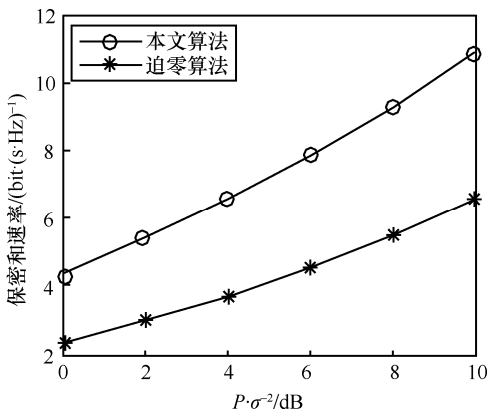
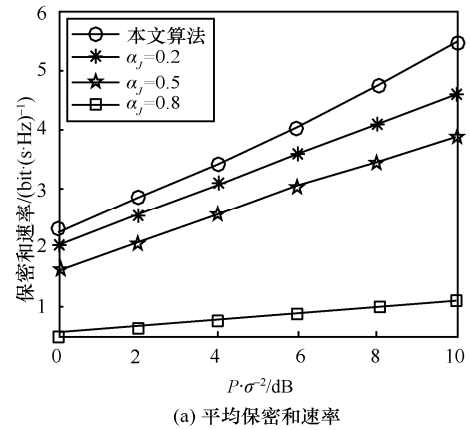


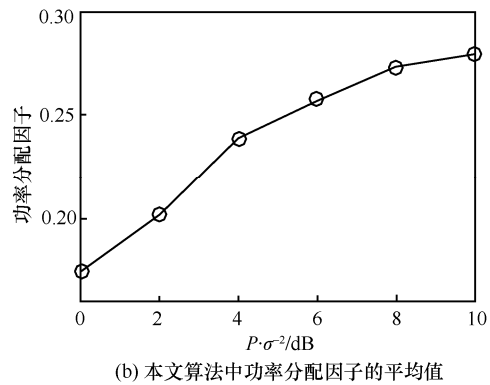
图 7 本文算法与迫零算法的保密和速率随  $\frac{P}{\sigma^2}$  的变化

为衡量功率分配因子  $\alpha_j$  对系统保密性能的影响,图 8(a)对比了本文 DC 优化算法与固定功率分配因子为 0.2、0.5、0.8 时的系统保密和速率,图 8(b)为本文优化算法中功率分配因子的平均值随  $\frac{P}{\sigma^2}$  的变化情况。在功率分配因子固定的方案中,采用 DC 规划对系统预编码矩阵进行优化。保密和速率值和功率分配因子值是 1 000 组信道样本下的平均值。从图 8(a)可以看出,本文算法根据瞬时的信道状态优化信息信号以

及人工噪声的预编码矩阵,使系统的功率分配最优,因此本文算法能达到的保密和速率优于固定功率分配因子时的保密和速率。发送总功率增大,适当增大人工噪声占发送总功率的比值,可以在提升合法信道传输速率的同时增大对窃听节点的干扰,有效提高系统的保密和速率。对比 3 个固定功率分配因子的曲线,功率分配因子为 0.8 的保密和速率最低,这是因为功率分配因子过大时,用于发送信息信号的功率过低,合法信道传输速率过低,导致系统保密和速率较低。



(a) 平均保密和速率



(b) 本文算法中功率分配因子的平均值

图 8 本文算法与固定功率分配因子时的性能对比

#### 4.2 信道状态信息不完美场景下的仿真

图 9 给出了随机产生的 3 组信道样本下,不完美 CSI 场景的保密和速率随迭代次数的变化情况。仿真中  $\varepsilon$  设置为 0.1,  $\frac{P}{\sigma^2}$  为 10 dB。图 9 显示,算法 2 大约经过 5~10 次迭代后收敛,其收敛速度稍低于 CSI 完美场景下的 DC 规划算法,但仍然具有较好的收敛性。同时因为算法 2 对 CSI 的估计误差具有稳健性,因此有较好的实用价值。

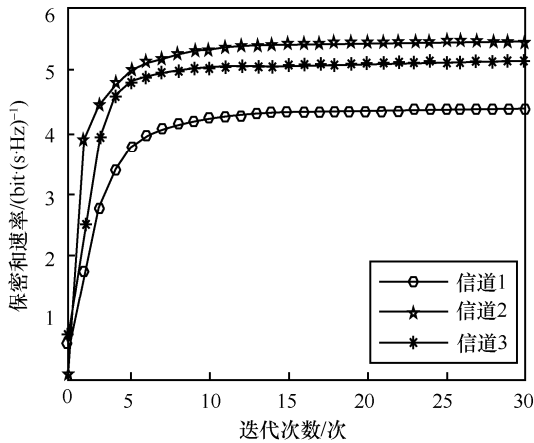
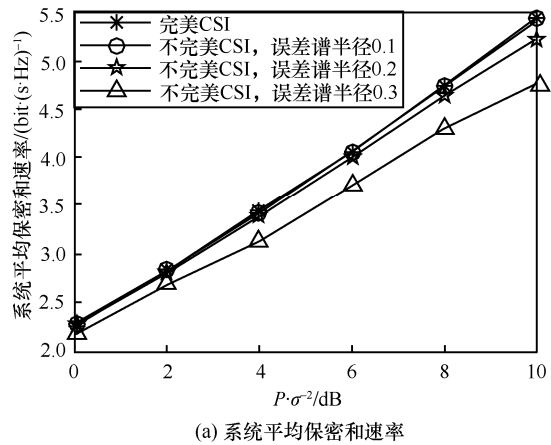


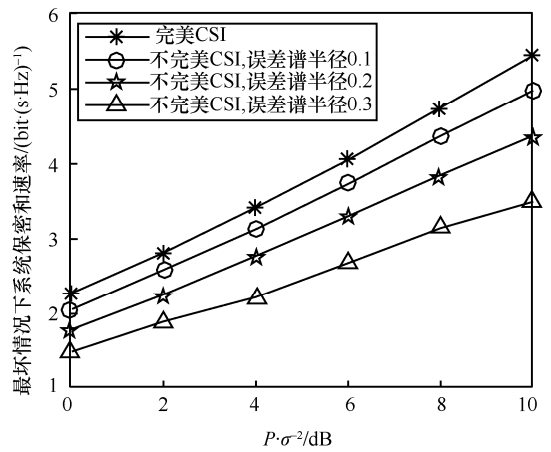
图 9 信道 CSI 不完美时系统保密和速率与迭代次数的关系

图 10 给出了当信道 CSI 完美以及信道估计误差谱半径分别为 0.1、0.2、0.3 时，系统保密和速率随  $\frac{P}{\sigma^2}$  的变化情况。在仿真中，首先产生一组元素满足均值为 0、方差为 1 的复高斯矩阵作为信道估计样本，并基于信道估计样本以及误差谱半径  $\varepsilon$  使用算法 2 进行稳健设计得到信息信号以及人工噪声的预编码矩阵  $S_A$ 、 $S_B$ 、 $Z_A$ 、 $Z_B$ ，然后在预编码矩阵固定的前提下，随机产生 40 000 组误差谱半径为  $\varepsilon$  的信道估计误差矩阵，并统计 40 000 组估计误差矩阵下系统保密和速率的平均值和最小值，分别作为系统的平均保密和速率和最坏情况下的保密和速率。随机产生 1 000 组信道估计样本，并对 1 000 组信道估计样本的平均保密和速率、最坏情况下的保密和速率进行统计平均，结果分别如图 10(a)、图 10(b)所示。从图 10(a)和图 10(b)可以看出，信道 CSI 完美时的保密和速率高于信道 CSI 不完美时的保密和速率，且信道 CSI 不完美时，信道估计误差的谱半径越大，系统保密和速率越小。图 10(a)和图 10(b)还显示，给定误差谱半径，系统保密和速率的损失（信道 CSI 完美时与信道 CSI 不完美时的保密和速率的差值）随着  $\frac{P}{\sigma^2}$  的增大而增大。这是因为当信道 CSI 完美时，可以准确地设计信息信号和人工噪声的预编码矩阵，不仅能有效地扩大合法信道和窃听信道的信号传输质量差异，还可有效降低发送信号对接收通道的干扰。而以有误差的信道估计值为依据进行优化设计的信息信号和人工噪声的预编码矩阵并不为最优，一方面合法信道与窃听信道上信号传输的质量差异有所降低，另一方面全双工节点的自干扰功率高于 CSI 完美时

的自干扰功率，且  $\frac{P}{\sigma^2}$  越大，自干扰功率在合法节点处的干扰和噪声总功率中的比重越大，导致信干噪比随发送功率增加而增加的速率越来越低，从而导致系统合法信道传输速率增长速度下降，最终导致系统保密和速率增长速度降低。因此，信道 CSI 完美与不完美场景下的系统保密和速率的差值增大。由图 10(a)可以发现， $\varepsilon = 0.1$  时的平均保密和速率非常接近信道完美时的数值， $\varepsilon = 0.2$  时只是有轻微下降， $\varepsilon = 0.3$  时的平均保密和速率与信道 CSI 完美时的数值相比，下降幅度在 3.88% ( $\frac{P}{\sigma^2} = 0 \text{ dB}$ ) ~ 12.51% ( $\frac{P}{\sigma^2} = 10 \text{ dB}$ ) 之间，表明所提算法具有很好的稳健性。



(a) 系统平均保密和速率



(b) 最坏情况下系统保密和速率

图 10 系统保密和速率与  $\frac{P}{\sigma^2}$  的关系

图 11 给出了信道 CSI 完美和不完美场景下有人工噪声对系统保密和速率的影响，其中，图 11(a)为系统的平均保密和速率随  $\varepsilon$  的变化，图 11(b)为最

差情况下系统的保密和速率随  $\varepsilon$  的变化。信道样本数量和仿真结果的获得方法与图 8 相同。 $\frac{P}{\sigma^2}$  设置为 10 dB。可以看出, 当信道 CSI 不完美时, 系统平均保密和速率与最坏情况下的保密和速率均随着  $\varepsilon$  的增大而减少, 使用人工噪声的保密和速率明显高于无人工噪声的保密和速率。对比图 11(a) 和图 11(b), 可知系统平均保密和速率随  $\varepsilon$  的增大而减少的速率小于最坏情况下系统保密和速率的减小速率。信道估计误差是分布在特定空间内的随机值, 误差值不同, 保密速率的下降度不同, 最坏情况是指使保密速率下降最大的情况; 而平均保密速率是不同估计误差下的保密速率的平均值。显然, 系统的平均保密和速率高于最坏情况下的保密和速率, 随着误差谱半径的增大, 平均保密速率的下降速度低于最坏情况下保密速率的下降速度。

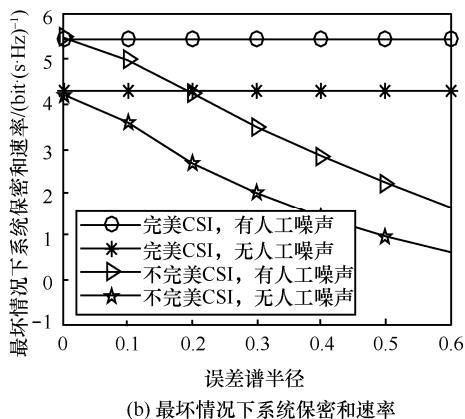
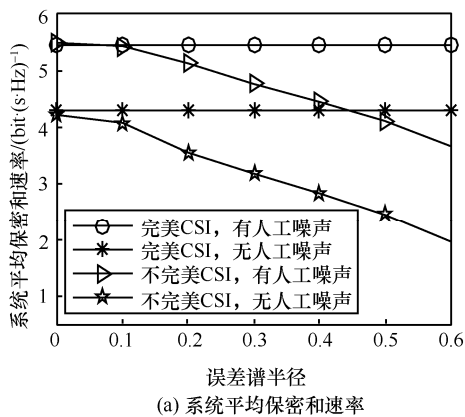
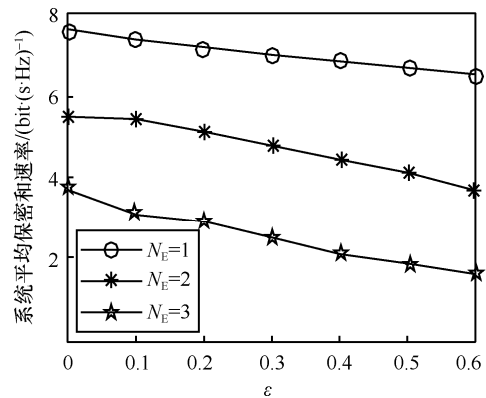


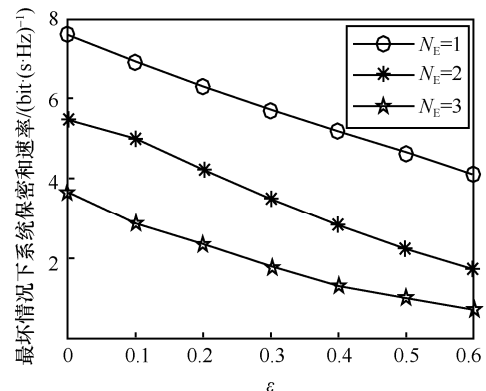
图 11 有无人工噪声对保密和速率的影响

图 12 给出了在  $N_t=2, N_r=2$  的条件下, 窃听节点 E 配备不同天线数时, 系统保密和速率随  $\varepsilon$  的变化情况, 其中图 12(a) 为平均保密和速率, 图 12(b)

为最坏情况下的保密和速率。仿真中信道样本的数量和仿真结果的获得方法与图 8 相同。设置  $\frac{P}{\sigma^2} = 10$  dB。从图 12(a) 和图 12(b) 可以看出, 在同一窃听天线数下, 系统保密和速率随信道估计误差谱半径的增大而减少。当误差谱半径相同时, 窃听天线数越多, 系统对应的保密和速率越小。



(a) 系统平均保密和速率



(b) 最坏情况下系统保密和速率

图 12 不同窃听天线数时的系统保密和速率随  $\varepsilon$  的变化

图 13 给出了  $N_E=2$  的场景下, 在  $N=4$  的条件下, 分配不同数量的收发天线时系统保密和速率随误差谱半径的变化, 其中, 图 13(a) 为系统平均保密和速率, 图 13(b) 为最坏情况下系统保密和速率。信道样本的数量和仿真结果的获得方法与图 8 相同。 $\frac{P}{\sigma^2}$  设置为 10 dB。从图 13 可以看出, 发送天线数越多, 系统保密和速率越大。这是因为发送天线数越多, 对窃听者的抑制更有效, 窃听速率更低, 同时当有多根发送天线时, 能够通过控制信号和人工噪声的预编码矩阵, 降低发送信号对接收通道的干扰, 增大合法信道速率, 从而增大保密和速率。

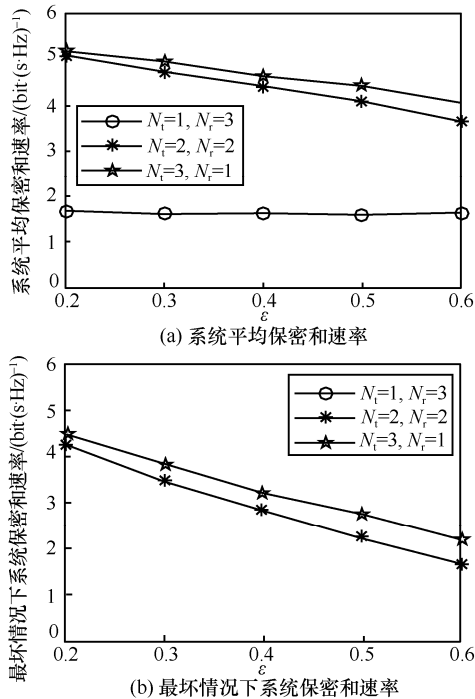


图 13 不同收发天线数时系统保密和速率随  $\epsilon$  的变化

### 5 结束语

本文考虑在合法信道、窃听信道的 CSI 完美以及不完美的 2 种场景下,设计 MIMO 全双工双向安全通信系统的预编码矩阵。系统中,合法节点工作在全双工模式,在接收信息的同时不仅向对方发送信息信号也同时发送人工噪声干扰窃听节点。针对信道 CSI 完美的场景,采用 DC 规划算法优化信息信号以及人工噪声的预编码矩阵以实现系统保密和速率的最大化;针对信道 CSI 不完美的情形,采用 WMMSE 算法对系统进行稳健设计,以最大化最坏情况下的保密和速率。在预编码的设计中,考虑了全双工残留自干扰的影响。仿真结果显示所提优化算法具有较好收敛性,且人工噪声辅助的方案比无人工噪声的方案具有更高的保密速率,显出人工噪声对于提高保密传输性能具有重要的意义。

### 参考文献:

[1] FOROOZANFARD E, FRANEK O, TATOMIRESCU A, et al. Full-duplex MIMO system based on antenna cancellation technique[J]. Electronics Letters, 2014, 50(16): 1116-1117.

[2] KIM D, LEE H, HONG D. A survey of in-band full-duplex transmission: from the perspective of PHY and MAC layers[J]. IEEE Communications Surveys & Tutorials, 2017, 17(4):2017-2046.

[3] LE A, TRAN L, HUANG X. Cyclostationary analysis of analog least mean square loop for self-interference cancellation in in-band full-duplex systems[J]. IEEE Communications Letters, 2017, 21(12):

2738-2741.

[4] SABHARWAL A, SCHNITER P, GUO D, et al. In-band full-duplex wireless: challenges and opportunities[J]. IEEE Journal on Selected Areas in Communications, 2014, 32(9):1637-1652.

[5] LEUNG Y C S K, HELLMAN M E. The Gaussian wiretap channel[J]. IEEE Transactions on Information Theory, 1978, 24(4): 451-456.

[6] LIANG Y, POOR H V, SHAMAI S. Secure communication over fading channels[J]. IEEE Transactions on Information Theory, 2008, 54(6): 2470-2492.

[7] KHANDANI A K. Two-way (true full-duplex) wireless[C]//2013 13th Canadian Workshop on Information Theory. Piscataway: IEEE Press, 2013: 33-38.

[8] ZHOU Y, ZHU Y, XUE Z. Enhanced MIMOME wiretap channel via adopting full-duplex MIMO radios[C]//2014 IEEE Global Communications Conference. Piscataway: IEEE Press, 2014: 3320-3325.

[9] KIM J, KIM J, LEE J, et al. Physical-layer security against smart eavesdroppers: exploiting full-duplex receivers[J]. IEEE Access, 2018, 6: 32945-32957.

[10] WAN Y, LI Q, ZHANG Q, et al. Optimal and suboptimal full-duplex secure beamforming designs for MISO two-way communications[J]. IEEE Wireless Communications Letters, 2015, 4(5): 493-496.

[11] QI C, CHEN Y, VINCK A J H, et al. One-sided secrecy over the two-way wiretap channel [C]//2016 International Symposium on Information Theory and Its Applications. Piscataway: IEEE Press, 2016: 626-630.

[12] 冀保峰, 杨佳, 王一丹, 等. 基于能效最优准则的双跳中继网络功率分配算法[J]. 通信学报, 2016, 37(7): 124-131.

JI B F, YANG J, WANG Y D, et al. Power allocation algorithms in two-hop relaying networks based on optimal energy efficiency[J]. Journal on Communications, 2016, 37(7): 124-131.

[13] CHEN G, GONG Y, XIAO P, et al. Physical layer network security in the full-duplex relay system[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(3): 574-583.

[14] CAO Y, ZHAO N, PAN G, et al. Secrecy analysis for cooperative NOMA networks with multi-antenna full-duplex relay[J]. IEEE Transactions on Communications, 2019, 67(8): 5574-5587.

[15] FENG R, LI Q, ZHANG Q, et al. Robust secure beamforming in MISO full-duplex two-way secure communications[J]. IEEE Transactions on Vehicular Technology, 2016, 65(1): 408-414.

[16] CHU Z, LE T A, NGUYEN H X, et al. Robust sum secrecy rate optimization for MIMO two-way full duplex systems [C]//2017 IEEE 86th Vehicular Technology Conference. Piscataway: IEEE Press, 2017: 1-5.

[17] TEKIN E, YENER A. The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming[J]. IEEE Transactions on Information Theory, 2008, 54(6): 2735-2751.

[18] LI Q, ZHANG Y, LIN J, et al. Full-duplex bidirectional secure communications under perfect and distributionally ambiguous eavesdropper's CSI[J]. IEEE Transactions on Signal Processing, 2017, 65(17): 4684-4697.

[19] CHU Z, CUMANAN K, DING Z, et al. Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer[J]. IEEE Transactions on Vehicular Technology, 2015, 64(5):1833-1847.

[20] NESTEROV Y, NEMIROVSKII A. Interior-point polynomial algorithms in convex programming[M]. Philadelphia: Society for Industrial and Applied Mathematics, 1994.

[21] VOROBYOV S A, GERSHMAN A B, LUO Z Q. Robust adaptive

beamforming using worst-case performance optimization: a solution to the signal mismatch problem[J]. IEEE Transactions on Signal Processing, 2003, 51(2): 313-324.

- [22] GHARAVOL E A, LARSSON E G. The sign-definiteness lemma and its applications to robust transceiver optimization for multiuser MIMO systems[J]. IEEE Transactions on Signal Processing, 2013, 61(2): 238-252.
- [23] LI Q, YANG L. Artificial noise aided secure precoding for MIMO untrusted two-way relay systems with perfect and imperfect channel state information[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(10): 2628-2638.
- [24] HORN R A, JOHNSON C R. Matrix analysis[M]. Cambridge: Cambridge University Press, 1985.
- [25] KHISTI A, WORNELL G W. Secure transmission with multiple antennas II: the MIMOME wiretap channel[J]. IEEE Transactions on Information Theory, 2010, 56(11): 5515-5532.

#### [作者简介]



雷维嘉 (1969- ), 男, 云南元谋人, 博士, 重庆邮电大学教授, 主要研究方向为认知无线电、物理层安全。



周洋 (1995- ), 女, 重庆合川人, 重庆邮电大学硕士生, 主要研究方向为物理层安全。



谢显中 (1966- ), 男, 四川通江人, 博士, 重庆邮电大学教授, 主要研究方向为认知无线电、干扰对齐与 MIMO 技术、绿色通信等。



雷宏江 (1975- ), 男, 陕西合阳人, 博士, 重庆邮电大学副教授, 主要研究方向为无线系统建模与分析、物理层安全。