

多载波 NOMA 安全通信系统稳健性资源分配算法

张钰^{1,2}, 赵雄文^{1,2}, 王晓晴^{1,2}, 耿绥燕^{1,2}, 秦鹏^{1,2}, 周振宇^{1,2}

(1. 华北电力大学新能源电力系统国家重点实验室, 北京 102206;

2. 华北电力大学河北省电力物联网技术重点实验室, 河北 保定 071003)

摘要: 为提升无线网络频谱利用率和增强信息传输的安全性, 针对下行多载波非正交多址接入安全通信系统, 提出了一种基于安全和速率最大化的稳健性资源分配算法。首先, 设计人工噪声 (AN) 预编码矢量与合法用户信道正交, 消除人工噪声对合法传输的影响。然后, 考虑每个用户最小速率约束、基站最大功率约束, 基于窃听信道不确定性建立 AN 预编码、下行数据预编码和子载波分配联合优化问题模型。为求解该非凸问题, 将其分解为预编码优化和子载波分配 2 个子问题进行联合优化, 基于 S-procedure 和块坐标下降算法对预编码优化问题进行求解, 基于动态匹配理论进行子载波分配。研究结果表明, 所提算法具有很好的稳健性, 能够有效提高系统安全和速率。

关键词: 多载波; 非正交多址接入; 物理层安全; 人工噪声; 预编码; 子载波分配

中图分类号: TN92

文献标志码: A

DOI: 10.11959/j.issn.1000-436x.2022044

Robust resource allocation algorithm for multicarrier NOMA security communication system

ZHANG Yu^{1,2}, ZHAO Xiongwen^{1,2}, WANG Xiaoqing^{1,2}, GENG Suiyan^{1,2}, QIN Peng^{1,2}, ZHOU Zhenyu^{1,2}

1. State Key Laboratory of Alternate Electrical Power System with Renewable Energy Sources, North China Electric Power University, Beijing 102206, China

2. Hebei Key Laboratory of Power Internet of Things Technology, North China Electric Power University, Baoding 071003, China

Abstract: To improve the spectrum efficiency and enhance the information security of wireless network, a sum secrecy rate maximization-based robust resource allocation algorithm was proposed for a downlink multicarrier NOMA security communication system. Firstly, the artificial noise (AN) precoding vector was designed to be orthogonal to the legitimate channel, so that the legitimate transmission would not be affected by the AN. Then, considering the constraints of rate requirement of each user and the maximum transmit power of base station, a joint AN precoding, downlink data precoding and subcarrier allocation optimization problem was formulated under eavesdropping channel uncertainties. To solve that non-convex problem, it was decomposed into two joint optimization subproblems: precoding optimization and subcarrier allocation. The former was solved based on S-procedure and block coordinate descent (BCD) algorithm, the latter was solved by dynamic matching theory. Simulation results demonstrate that the proposed algorithm has good robustness and can effectively improve the sum secrecy rate.

Keywords: multicarrier, NOMA, physical layer security, artificial noise, precoding, subcarrier allocation

0 引言

随着 5G 通信技术的发展和网络的建设, 面向

海量终端业务接入的 5G 物联网将应用到工业和人们的日常生活中^[1-2]。在该背景下, 如何充分利用有限频谱资源扩大网络连接以及如何提升网络信息

收稿日期: 2021-10-31; 修回日期: 2022-01-22

通信作者: 赵雄文, zhaowx@ncepu.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61931001)

Foundation Item: The National Natural Science Foundation of China (No.61931001)

传输的安全性和隐私性是无线通信系统需要考虑的关键问题。近年来,非正交多址接入(NOMA, non-orthogonal multiple access)^[3-4]允许在同一时频资源块上服务多个用户,成倍提升系统容量,受到人们广泛关注。基于人工噪声(AN, artificial noise)的物理层安全(PLS, physical layer security)技术^[5-6]提供了一种轻量级安全通信手段,以信息论为基础,利用无线信道的物理层特性实现信息安全传输,不需要依赖复杂的加密解密算法。因此,基于物理层安全的NOMA系统可实现提升信息安全性、提高频谱效率和扩大网络连接的目标,成为工业界和学术界关注的热点。

NOMA通过在发送端进行功率叠加编码,在接收机利用连续干扰消除(SIC, successive interference cancellation)技术来避免同道干扰,从而获取期望信号^[7]。关于单载波NOMA系统中资源配置与优化的研究已取得较大进展,而针对多载波NOMA系统的研究相对较少。文献[8-9]分别针对存在2个用户的下行和上行单载波NOMA系统,以最大化系统可达和速率为目标提出了功率分配和预编码矢量联合优化算法。文献[4,10]针对存在多用户(2个以上)的单载波NOMA系统,分别以最大化频效和能效为目标,对基站预编码和用户功率分配方案进行了研究。单载波NOMA系统中,所有用户占用同一信道,彼此之间同频干扰严重,多载波NOMA系统中用户被分配到不同的信道,不同信道上的用户彼此间不会产生同频干扰,但子载波分配策略会对系统性能产生显著的影响。文献[11]研究发现将信道增益差别较大的2个用户分配到同一子载波上有助于改善系统性能。文献[12-13]假设基站和用户都是单天线,对子载波和功率分配算法进行了优化设计。实际无线通信系统都是多载波系统,且多载波NOMA技术具备更高的资源配置灵活性,因此研究多载波NOMA系统更有意义。

PLS技术在NOMA系统中的应用尚处于初步研究阶段。近年来,文献[14]考虑存在一个单天线窃听者(Eve, eavesdropper)的下行NOMA网络,假设基站能够获取完美的合法和窃听信道状态信息(CSI, channel state information),建立了以最大化安全能效为目标的功率优化问题,同时满足基站最大发射功率和用户数据传输速率限制,并采用一阶泰勒展开和连续凸逼近算法求解。文献[15]考虑基站发射AN对Eve进行干扰,假设窃听信道CSI

未知,提出了下行数据及AN预编码矢量优化算法,以最大化AN发射功率的同时满足基站最大发射功率和用户数据传输速率约束。文献[16]假设窃听信道非完美CSI,分析了多天线下行NOMA系统安全中断概率。与单载波系统不同,多载波NOMA网络中子载波分配与预编码矩阵和人工噪声等优化变量紧密耦合,导致资源分配问题中待优化变量增多,求解难度增大,因此文献[14-16]所提资源分配算法不能直接应用于多载波系统。目前针对PLS在多载波NOMA系统中的应用研究较少,文献[17]以最大化安全和速率为目标对上行NOMA系统中功率和子载波分配进行联合优化,文献[18]以最大化安全能效为目标,对放大转发的双向中继NOMA网络中功率和子载波分配进行联合优化。上述工作都是针对单天线系统,不涉及预编码矢量的优化,所提算法不能直接用于求解多天线系统的资源分配问题。

针对上述问题,本文研究多载波下行多天线NOMA安全传输系统AN预编码矢量、数据预编码矢量以及子载波分配的联合优化,主要的研究工作如下。

1) 建立下行多载波NOMA安全通信网络资源分配模型。首先,设计AN预编码矢量与合法用户信道正交,消除AN对合法用户信号的干扰。随后,以最大化合法用户的安全和速率为目标,对下行数据信号和AN的预编码矢量以及子载波分配策略进行优化,满足最小速率和最大发射功率约束。考虑窃听信道不确定性的影响,建立非理想CSI情况下的稳健性资源分配问题。本文所建立的优化模型是一个非凸、非线性、多变量耦合的优化问题,很难直接获得解析解。与单载波系统优化问题相比,本文模型增加了子载波分配,不同分配方案将导致优化问题的目标函数及限制条件的表达式发生变化,求解难度更大。

2) 提出了稳健性资源分配算法。将原始问题分解为预编码优化和子载波分配2个子优化问题,利用S-procedure算法^[19]将预编码矢量优化问题中含不确定性参数的目标函数转换为确定性形式,再利用块坐标下降(BCD, block coordinate descent)算法求解;利用动态匹配理论^[20]将子载波分配问题重新定义为双边匹配问题,并采用延迟接受(DA, deferred acceptance)算法^[21]求解;同时给出了本文的算法步骤、计算复杂度分析。多载波系统资源分配算法^[12-13]没有考虑信息传输的安全性,文献[17-18]

算法只适用于单天线系统，且只能对功率和子载波 2 种资源进行优化配置，本文所提算法适用于多天系统，且能够实现 AN、数据预编码矢量（包含功率）、子载波多种资源的联合优化。

3) 研究表明，本文所提方案具有很好的稳健性，与传统 OMA 传输以及其他文献中先进方案相比，能有效提高系统安全和速率。所提子载波分配算法性能与穷尽搜索算法性能非常接近，但计算复杂度显著降低。

1 系统模型

1.1 信号分析

存在窃听者的下行多载波 NOMA 系统模型如图 1 所示，下行多载波 NOMA 通信系统中存在一个多天线基站、 K 个合法用户和一个多天线 Eve。基站为合法用户提供数据服务的同时需要额外发送一个 AN 信号，以降低窃听信道的质量，提高信息传输的安全性。假设所有合法用户配置单根天线，基站和 Eve 分别配置 M 和 N 根天线，且 $M > N$ [22]。为避免用户之间过强的共道干扰并降低接收机 SIC 复杂度，网络中可用带宽 B 被均分为 I 个带宽为 $B_c = \frac{B}{I}$ 的子载波，每个子载波上只允许存在 2 个用户同时工作。定义 $\mathcal{I} = \{C_i\}_{i=1}^I$ 和 $\mathcal{S}^{(i)} = \{U_1^{(i)}, U_2^{(i)}\}$, $\forall i \in \{1, 2, \dots, I\}$ 分别表示子载波集合和分配在子载波 C_i 上的用户集合。基站的发射信号可表示为

$$\mathbf{x} = \sum_{i=1}^I \left(\sum_{j=1}^2 \mathbf{v}_j^{(i)} s_j^{(i)} + \mathbf{v}_A^{(i)} z^{(i)} \right) \quad (1)$$

其中， $\mathbf{v}_A^{(i)} \in \mathbb{C}^{M \times 1}$ 和 $\mathbf{v}_j^{(i)} \in \mathbb{C}^{M \times 1}$ 分别表示子载波 C_i 上 AN 预编码矢量和第 j 个用户的数据预编码矢量； $\|\mathbf{v}_A^{(i)}\|^2 = p_A^{(i)}$ 和 $\|\mathbf{v}_j^{(i)}\|^2 = p_j^{(i)}$ 分别表示对应的基站发射功率； $s_j^{(i)} \sim \mathcal{CN}(0, 1)$ 和 $z^{(i)} \sim \mathcal{CN}(0, 1)$ 为独立同分布的高斯随机变量，分别表示基站在 C_i 上发送的数据信号和 AN 信号。假设子载波 C_i 上基站到 Eve 和基站到用户的信道分别为 $\mathbf{H}_E^{(i)} \in \mathbb{C}^{N \times M}$ 和 $\mathbf{h}_j^{(i)} \in \mathbb{C}^{1 \times M}$ ， $i \in \{1, 2, \dots, I\}$ ， $j \in \{1, 2\}$ ，则子载波 C_i 上第 j 个用户 $U_j^{(i)}$ 的接收信号为

$$y_j^{(i)} = \sum_{l=1}^2 \mathbf{h}_j^{(i)} \mathbf{v}_l^{(i)} s_l^{(i)} + \mathbf{h}_j^{(i)} \mathbf{v}_A^{(i)} z^{(i)} + n_j^{(i)} \quad (2)$$

子载波 C_i 上 Eve 的接收信号为

$$y_E^{(i)} = \sum_{l=1}^2 \mathbf{H}_E^{(i)} \mathbf{v}_l^{(i)} s_l^{(i)} + \mathbf{H}_E^{(i)} \mathbf{v}_A^{(i)} z^{(i)} + \mathbf{n}_E^{(i)} \quad (3)$$

其中， $n_j^{(i)} \sim \mathcal{CN}(0, \sigma^2)$ 和 $\mathbf{n}_E^{(i)} \sim \mathcal{CN}(0, \sigma_E^2 \mathbf{I}_N)$ 表示用户和 Eve 接收机处复加性白高斯噪声，噪声功率分别为 σ^2 和 σ_E^2 。

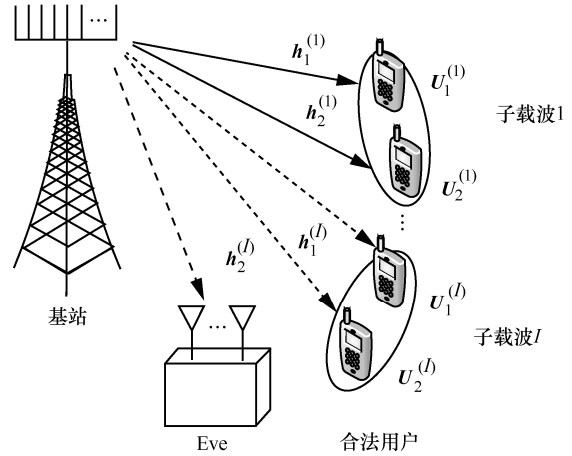


图 1 存在窃听者的下行多载波 NOMA 系统模型

1.2 数据速率

本节基于图 1 所示系统模型，推导网络整体安全和速率表达式，作为第 2 节数学优化问题中的目标函数。以子载波 C_i 为例，根据 NOMA 原理，信道增益较强的用户能解码出信道增益较弱用户的信号，并将其从接收信号中剔除，假设 $\|\mathbf{h}_1^{(i)}\|_2 \leq \|\mathbf{h}_2^{(i)}\|_2$ ，则强用户 $U_2^{(i)}$ 接收机处 SIC 的解码顺序遵循

$$|\mathbf{h}_2^{(i)} \mathbf{v}_2^{(i)}|^2 \leq |\mathbf{h}_2^{(i)} \mathbf{v}_1^{(i)}|^2 \quad (4)$$

合法用户数据传输速率为

$$R_1^{(i)} = B_c \text{lb} \left(1 + \frac{|\mathbf{h}_1^{(i)} \mathbf{v}_1^{(i)}|^2}{|\mathbf{h}_1^{(i)} \mathbf{v}_2^{(i)}|^2 + |\mathbf{h}_1^{(i)} \mathbf{v}_A^{(i)}|^2 + \sigma^2} \right) \quad (5)$$

$$R_2^{(i)} = B_c \text{lb} \left(1 + \frac{|\mathbf{h}_2^{(i)} \mathbf{v}_2^{(i)}|^2}{|\mathbf{h}_2^{(i)} \mathbf{v}_A^{(i)}|^2 + \sigma^2} \right) \quad (6)$$

为确保安全传输，本文考虑最坏的情况，假设 Eve 具有 $\mathbf{H}_E^{(i)}$ 的完美 CSI，并且能够完全消除同一子载波上的用户间信号干扰，则 Eve 窃听合法用户数据速率的上限为

$$E_1^{(i)} = B_c \text{lb} \det \left(\mathbf{I}_{N_E} + \mathbf{H}_E^{(i)} \mathbf{v}_1^{(i)} \mathbf{v}_1^{(i)H} \mathbf{H}_E^{(i)H} \mathbf{Y}^{-1} \right) \quad (7)$$

$$E_2^{(i)} = B_c \text{lb} \det \left(\mathbf{I}_{N_E} + \mathbf{H}_E^{(i)} \mathbf{v}_2^{(i)} \mathbf{v}_2^{(i)H} \mathbf{H}_E^{(i)H} \mathbf{Y}^{-1} \right) \quad (8)$$

其中, $\mathbf{Y} = \mathbf{H}_E^{(i)} \mathbf{v}_A^{(i)} \mathbf{v}_A^{(i)H} \mathbf{H}_E^{(i)H} + \sigma^2 \mathbf{I}_N$ 。因此, 子载波 C_i 上合法用户 $U_j^{(i)}$ 可达安全速率的下界可表示为

$$S_j^{(i)} = [R_j^{(i)} - E_j^{(i)}]^+ \quad (9)$$

其中, $[x]^+$ 表示 $\max\{x, 0\}$ 。网络整体安全和速率为

$$S_{\text{sum}} = \sum_{i=1}^I (S_1^{(i)} + S_2^{(i)}) \quad (10)$$

1.3 信道状态信息

本节给出的信道模型将直接应用于第2节所建立的数学优化问题。本文假设基站能够获取所有合法链路的完美 CSI。对于窃听链路 $\mathbf{H}_E^{(i)}$, 基站可以通过 Eve 的本振泄露进行信道估计, 但由于泄露功率很小, 难以获取完美 CSI。因此, 采用以下信道模型^[23]表征窃听链路 CSI 的不确定性

$$\mathbf{H}_E^{(i)} = \hat{\mathbf{H}}_E^{(i)} + \Delta \mathbf{H}_E^{(i)}, \forall i \in \{1, 2, \dots, I\} \quad (11)$$

其中, $\hat{\mathbf{H}}_E^{(i)}$ 表示估计信道, $\Delta \mathbf{H}_E^{(i)} \in \mathcal{Y}^{(i)}$ 表示信道估计误差, 且 $\mathcal{Y}^{(i)} = \{\Delta \mathbf{H}_E^{(i)} : \|\Delta \mathbf{H}_E^{(i)}\|_F \leq \delta^{(i)}\}, \forall i$ 。

2 算法设计

2.1 AN 预编码矢量设计与问题建模

观察式(5)和式(6), 可以发现基站发射的 AN 信号对合法用户的信号也造成了干扰, 为提升合法用户数据速率, 设计迫零 AN 预编码矢量为

$$\mathbf{h}_1^{(i)} \mathbf{v}_A^{(i)} = \mathbf{h}_2^{(i)} \mathbf{v}_A^{(i)} = 0, \forall i \in \{1, 2, \dots, I\} \quad (12)$$

此时, 子载波 C_i 上合法用户数据速率可重写为

$$R_1^{(i)} = B_c \text{lb} \left(1 + \frac{|\mathbf{h}_1^{(i)} \mathbf{v}_1^{(i)}|^2}{|\mathbf{h}_1^{(i)} \mathbf{v}_2^{(i)}|^2 + \sigma^2} \right) \quad (13)$$

$$R_2^{(i)} = B_c \text{lb} \left(1 + \frac{|\mathbf{h}_2^{(i)} \mathbf{v}_2^{(i)}|^2}{\sigma^2} \right) \quad (14)$$

在此基础上, 建立最大化安全和速率的资源分配模型为

$$\begin{aligned} & \max_{\mathbf{v}_j^{(i)}, \mathbf{Q}_A^{(i)}} \min_{\mathcal{S}^{(i)} \Delta \mathbf{H}_E^{(i)} \in \mathcal{Y}^{(i)}} S_{\text{sum}} \\ \text{s.t. } & \text{C1: } \|\mathbf{v}_1^{(i)}\|^2 + \|\mathbf{v}_2^{(i)}\|^2 + \text{Tr}(\mathbf{Q}_A^{(i)}) \leq P_{\text{max}}^{\text{DL}(i)}, \forall i \\ & \text{C2: } \text{Tr}(\mathbf{h}_j^{(i)} \mathbf{Q}_A^{(i)} \mathbf{h}_j^{(i)H}) = 0, \forall i, \forall j \in \{1, 2\} \\ & \text{C3: } |\mathbf{h}_2^{(i)} \mathbf{v}_2^{(i)}|^2 \leq |\mathbf{h}_2^{(i)} \mathbf{v}_1^{(i)}|^2, \forall i \\ & \text{C4: } R_j^{(i)} \geq B_c r_j^{(i)}, \forall i, j \\ & \text{C5: } \mathbf{Q}_A^{(i)} \succeq \mathbf{0}, \forall i \\ & \text{C6: } \text{card}(\mathcal{S}^{(i)}) \leq 2, \forall i \end{aligned} \quad (15)$$

其中, $\mathbf{Q}_A^{(i)} = \mathbf{v}_A^{(i)} \mathbf{v}_A^{(i)H}$ 表示人工噪声协方差矩阵, 约束条件 C1 决定子载波 C_i 上基站发射功率的上限; 本文考虑所有子载波上的发射功率都均匀分配; C2 是式(12)的等效形式; C3 代表 SIC 解码顺序限制; C4 决定了每个用户的最低数据速率门限, $r_j^{(i)}$ 为预先设定的阈值; C5 约束 $\mathbf{Q}_A^{(i)}$ 是一个半正定矩阵; C6 确保同一子载波上同时工作的用户数不超过 2 个。式(15)描述的优化问题能够在信道估计误差 $\Delta \mathbf{H}_E^{(i)} \in \mathcal{Y}^{(i)}, \forall i$ 的情况下确保优化结果的可行性, 因此通过求解该问题得到的资源分配方案具备稳健性。显然, 式(15)是一个多变量耦合、非凸优化问题, 难以直接求解。相较于一般非凸优化问题, 求解式(15)的难度如下: 1) 不确定性信道 $\mathbf{H}_E^{(i)}$ 导致式(15)是一个含参数摄动的无穷维非确定性问题, 必须先将其转化成确定性优化问题; 2) 不同子载波分配方案会导致集合 $\mathcal{S}^{(i)}$ 中元素的变化, 从而使目标函数和限制条件的表达式发生改变。通常可采用穷尽搜索法寻找最优 $\mathcal{S}^{(i)}$, 得到固定的优化问题表达式再进行求解, 但这种方法计算复杂度极高, 难以实现。

为求解问题式(15), 首先在 2.2 节中假定任一子载波分配方案, 提出 AN 及下行数据预编码矢量优化算法; 其次, 在 2.3 节利用匹配理论为所有合法用户分配子载波, 在每轮匹配过程中, 采用 2.2 节提出的算法计算安全和速率作为匹配合适程度的衡量标准, 通过多次迭代, 最终输出一个稳定的匹配结果。

2.2 稳健性预编码矢量优化算法

假设网络中用户已分配好子载波, 问题式(15)可等效为 I 个子问题, 即

$$\begin{aligned} & \max_{\mathbf{v}_j^{(i)}, \mathbf{Q}_A^{(i)}} \min_{\Delta \mathbf{H}_E^{(i)} \in \mathcal{Y}^{(i)}} S_1^{(i)} + S_2^{(i)} \\ \text{s.t. } & \text{C1: } \|\mathbf{v}_1^{(i)}\|^2 + \|\mathbf{v}_2^{(i)}\|^2 + \text{Tr}(\mathbf{Q}_A^{(i)}) \leq P_{\text{max}}^{\text{DL}(i)} \\ & \text{C2: } \text{Tr}(\mathbf{h}_j^{(i)} \mathbf{Q}_A^{(i)} \mathbf{h}_j^{(i)H}) = 0, \forall j \\ & \text{C3: } |\mathbf{h}_2^{(i)} \mathbf{v}_2^{(i)}|^2 \leq |\mathbf{h}_2^{(i)} \mathbf{v}_1^{(i)}|^2 \\ & \text{C4: } R_j^{(i)} \geq B_c r_j^{(i)}, \forall j \\ & \text{C5: } \mathbf{Q}_A^{(i)} \succeq \mathbf{0} \end{aligned} \quad (16)$$

式(16)仍是一个含不确定性参数的无穷维、非凸优化问题。引入新变量 $\mathbf{W}_j^{(i)} = \mathbf{v}_j^{(i)} \mathbf{v}_j^{(i)H}, \forall i, j$, 其中 $\mathbf{W}_j^{(i)}$ 是一个秩为 1 的对称半正定矩阵, 式(16)可进一步转化为

$$\begin{aligned}
 & \max_{\mathbf{w}_j^{(i)}, \mathbf{Q}_A^{(i)}} \min_{\Delta \mathbf{H}_E^{(i)} \in \mathcal{Y}^{(i)}} S_1^{(i)} + S_2^{(i)} \\
 \text{s.t. C1: } & \text{Tr}(\mathbf{W}_1^{(i)} + \mathbf{W}_2^{(i)} + \mathbf{Q}_A^{(i)}) \leq P_{\max}^{\text{DL}(i)} \\
 \text{C2: } & \text{Tr}(\mathbf{h}_j^{(i)} \mathbf{Q}_A^{(i)} \mathbf{h}_j^{(i)\text{H}}) = 0 \\
 \text{C3: } & \text{Tr}(\mathbf{h}_2^{(i)} \mathbf{W}_2^{(i)} \mathbf{h}_2^{(i)\text{H}}) \leq \text{Tr}(\mathbf{h}_2^{(i)} \mathbf{W}_1^{(i)} \mathbf{h}_2^{(i)\text{H}}) \\
 \text{C4: } & R_j^{(i)} \geq B_c r_j^{(i)}, \forall j \\
 \text{C5: } & \mathbf{Q}_A^{(i)} \succeq \mathbf{0} \\
 \text{C6: } & \mathbf{W}_j^{(i)} \succeq \mathbf{0}, \forall j \\
 \text{C7: } & \text{Rank}(\mathbf{W}_j^{(i)}) = 1, \forall j
 \end{aligned} \tag{17}$$

将式(17)中的目标函数转换为凸函数，根据文献[24-25]可得

$$\begin{aligned}
 & -\ln(\sigma^{-2} \text{Tr}(\mathbf{h}_1^{(i)} \mathbf{W}_2^{(i)} \mathbf{h}_1^{(i)\text{H}}) + 1) = \\
 & \max_{a^{(i)} \geq 0} \ln(a^{(i)}) + 1 - a^{(i)} (\sigma^{-2} \text{Tr}(\mathbf{h}_1^{(i)} \mathbf{W}_2^{(i)} \mathbf{h}_1^{(i)\text{H}}) + 1)
 \end{aligned} \tag{18}$$

$$\begin{aligned}
 & -\ln \det(\sigma_E^{-2} \mathbf{H}_E^{(i)} (\mathbf{Q}_A^{(i)} + \mathbf{W}_1^{(i)}) \mathbf{H}_E^{(i)\text{H}} + \mathbf{I}_N) = \\
 & \max_{\mathbf{Q}_1^{(i)} \succeq \mathbf{0}} \ln \det(\mathbf{Q}_1^{(i)}) + N - \\
 & \text{Tr}(\mathbf{Q}_1^{(i)} (\sigma_E^{-2} \mathbf{H}_E^{(i)} (\mathbf{Q}_A^{(i)} + \mathbf{W}_1^{(i)}) \mathbf{H}_E^{(i)\text{H}} + \mathbf{I}_N))
 \end{aligned} \tag{19}$$

$$\begin{aligned}
 & -\ln \det(\sigma_E^{-2} \mathbf{H}_E^{(i)} (\mathbf{Q}_A^{(i)} + \mathbf{W}_2^{(i)}) \mathbf{H}_E^{(i)\text{H}} + \mathbf{I}_N) \\
 & = \max_{\mathbf{Q}_2^{(i)} \succeq \mathbf{0}} \ln \det(\mathbf{Q}_2^{(i)}) + N - \\
 & \text{Tr}(\mathbf{Q}_2^{(i)} (\sigma_E^{-2} \mathbf{H}_E^{(i)} (\mathbf{Q}_A^{(i)} + \mathbf{W}_2^{(i)}) \mathbf{H}_E^{(i)\text{H}} + \mathbf{I}_N))
 \end{aligned} \tag{20}$$

其中， $a^{(i)} \in \mathbb{C}$ 、 $\mathbf{Q}_1^{(i)} \in \mathbb{C}^{N \times N}$ 、 $\mathbf{Q}_2^{(i)} \in \mathbb{C}^{N \times N}$ 是辅助变量，将式(18)~式(20)代入问题式(17)的目标函数可得

$$\begin{aligned}
 S_1^{(i)} + S_2^{(i)} = & B_c \left[\text{lb}(\text{Tr}(\mathbf{h}_1^{(i)} (\mathbf{W}_1^{(i)} + \mathbf{W}_2^{(i)}) \mathbf{h}_1^{(i)\text{H}}) + \sigma^2) + \right. \\
 & \text{lb}(\text{Tr}(\mathbf{h}_2^{(i)} \mathbf{W}_2^{(i)} \mathbf{h}_2^{(i)\text{H}}) + \sigma^2) + \frac{1+2N}{\ln 2} - \frac{\text{Tr}(\mathbf{Q}_1^{(i)} + \mathbf{Q}_2^{(i)})}{\ln 2} - \text{lb}(\sigma^4) + \\
 & \text{lb}(a^{(i)}) - \frac{a^{(i)} (\sigma^{-2} \text{Tr}(\mathbf{h}_1^{(i)} \mathbf{W}_2^{(i)} \mathbf{h}_1^{(i)\text{H}}) + 1)}{\ln 2} + \\
 & 2 \text{lb} \det(\sigma_E^{-2} \mathbf{H}_E^{(i)} \mathbf{Q}_A^{(i)} \mathbf{H}_E^{(i)\text{H}} + \mathbf{I}_N) + \\
 & \left. \text{lb} \det(\mathbf{Q}_1^{(i)}) - \frac{\text{Tr}(\sigma_E^{-2} \mathbf{Q}_1^{(i)} \mathbf{H}_E^{(i)} (\mathbf{Q}_A^{(i)} + \mathbf{W}_1^{(i)}) \mathbf{H}_E^{(i)\text{H}})}{\ln 2} + \right. \\
 & \left. \text{lb} \det(\mathbf{Q}_2^{(i)}) - \frac{\text{Tr}(\sigma_E^{-2} \mathbf{Q}_2^{(i)} \mathbf{H}_E^{(i)} (\mathbf{Q}_A^{(i)} + \mathbf{W}_2^{(i)}) \mathbf{H}_E^{(i)\text{H}})}{\ln 2} \right]
 \end{aligned} \tag{21}$$

由于变量 $\mathbf{H}_E^{(i)}$ 的不确定性，式(21)的表达式有无穷多个，问题式(17)仍难以求解。需要将含信道不确定

性的优化问题转换为确定性优化问题。通过引入辅助变量 $\mathbf{T}^{(i)} \succeq \mathbf{0}$ ， $b_1^{(i)} \geq 0$ ， $b_2^{(i)} \geq 0$ ，可将式(17)转化为

$$\begin{aligned}
 & \max_{\mathbf{w}_j^{(i)}, \mathbf{Q}_A^{(i)}, a^{(i)}, b_1^{(i)}, b_2^{(i)}, \mathbf{Q}_1^{(i)}, \mathbf{Q}_2^{(i)}, \mathbf{T}^{(i)}} S_1^{(i)} + S_2^{(i)} \\
 \text{s.t. C1~C7} \\
 \text{C8: } & \mathbf{T}^{(i)} \preceq \mathbf{H}_E^{(i)} \mathbf{Q}_A^{(i)} \mathbf{H}_E^{(i)\text{H}}, \Delta \mathbf{H}_E^{(i)} \in \mathcal{Y}^{(i)} \\
 \text{C9: } & b_1^{(i)} \geq \text{Tr}(\mathbf{Q}_1^{(i)} \mathbf{H}_E^{(i)} (\mathbf{Q}_A^{(i)} + \mathbf{W}_1^{(i)}) \mathbf{H}_E^{(i)\text{H}}), \\
 & \Delta \mathbf{H}_E^{(i)} \in \mathcal{Y}^{(i)} \\
 \text{C10: } & b_2^{(i)} \geq \text{Tr}(\mathbf{Q}_2^{(i)} \mathbf{H}_E^{(i)} (\mathbf{Q}_A^{(i)} + \mathbf{W}_2^{(i)}) \mathbf{H}_E^{(i)\text{H}}), \\
 & \Delta \mathbf{H}_E^{(i)} \in \mathcal{Y}^{(i)}
 \end{aligned} \tag{22}$$

其中，目标函数表达式为

$$\begin{aligned}
 S_1^{(i)} + S_2^{(i)} = & B_c \left[\text{lb}(\text{Tr}(\mathbf{h}_1^{(i)} (\mathbf{W}_1^{(i)} + \mathbf{W}_2^{(i)}) \mathbf{h}_1^{(i)\text{H}}) + \sigma^2) + \right. \\
 & \text{lb}(\text{Tr}(\mathbf{h}_2^{(i)} \mathbf{W}_2^{(i)} \mathbf{h}_2^{(i)\text{H}}) + \sigma^2) + \frac{1+2N}{\ln 2} - \\
 & \frac{\text{Tr}(\mathbf{Q}_1^{(i)} + \mathbf{Q}_2^{(i)})}{\ln 2} - \text{lb}(\sigma^4) + \text{lb}(a^{(i)}) - \\
 & \frac{a^{(i)} (\sigma^{-2} \text{Tr}(\mathbf{h}_1^{(i)} \mathbf{W}_2^{(i)} \mathbf{h}_1^{(i)\text{H}}) + 1)}{\ln 2} + 2 \text{lb} \det(\sigma_E^{-2} \mathbf{T}^{(i)} + \mathbf{I}_N) + \\
 & \left. \text{lb} \det(\mathbf{Q}_1^{(i)}) + \text{lb} \det(\mathbf{Q}_2^{(i)}) - \frac{b_1^{(i)} + b_2^{(i)}}{\sigma_E^2 \ln 2} \right]
 \end{aligned} \tag{23}$$

根据 S-procedure 引理^[19]，存在 $\lambda_1^{(i)}, \lambda_2^{(i)} \geq 0$ ，使约束条件 C8、C9、C10 等价为

$$\begin{aligned}
 & \begin{bmatrix} \hat{\mathbf{H}}_E^{(i)} \mathbf{Q}_A^{(i)} \hat{\mathbf{H}}_E^{(i)\text{H}} - \mathbf{T}^{(i)} & \hat{\mathbf{H}}_E^{(i)} \mathbf{Q}_A^{(i)} \\ \mathbf{Q}_A^{(i)} \hat{\mathbf{H}}_E^{(i)\text{H}} & \mathbf{Q}_A^{(i)} \end{bmatrix} - \\
 & \lambda_T^{(i)} \begin{bmatrix} \mathbf{I}_N & \mathbf{0} \\ \mathbf{0} & -\frac{1}{(\delta^{(i)})^2} \mathbf{I}_M \end{bmatrix} \succeq \mathbf{0}
 \end{aligned} \tag{24}$$

$$\begin{aligned}
 & \lambda_1^{(i)} \begin{bmatrix} \mathbf{I}_{M \times N} & \mathbf{0} \\ \mathbf{0} & (\delta^{(i)})^2 \end{bmatrix} - \\
 & \begin{bmatrix} \mathbf{Q}_1^{(i)} & \mathbf{Q}_1^{(i)} \text{vec}(\hat{\mathbf{H}}_E^{(i)}) \\ \text{vec}(\hat{\mathbf{H}}_E^{(i)})^{\text{H}} \mathbf{Q}_1^{(i)} & \text{vec}(\hat{\mathbf{H}}_E^{(i)})^{\text{H}} \mathbf{Q}_1^{(i)} \text{vec}(\hat{\mathbf{H}}_E^{(i)}) - b_1^{(i)} \end{bmatrix} \succeq \mathbf{0}
 \end{aligned} \tag{25}$$

$$\begin{aligned}
 & \lambda_2^{(i)} \begin{bmatrix} \mathbf{I}_{M \times N} & \mathbf{0} \\ \mathbf{0} & (\delta^{(i)})^2 \end{bmatrix} - \\
 & \begin{bmatrix} \mathbf{Q}_2^{(i)} & \mathbf{Q}_2^{(i)} \text{vec}(\hat{\mathbf{H}}_E^{(i)}) \\ \text{vec}(\hat{\mathbf{H}}_E^{(i)})^{\text{H}} \mathbf{Q}_2^{(i)} & \text{vec}(\hat{\mathbf{H}}_E^{(i)})^{\text{H}} \mathbf{Q}_2^{(i)} \text{vec}(\hat{\mathbf{H}}_E^{(i)}) - b_2^{(i)} \end{bmatrix} \succeq \mathbf{0}
 \end{aligned} \tag{26}$$

其中, $\boldsymbol{\theta}_j^{(i)} = (\boldsymbol{\Omega}_A^{(i)} + \boldsymbol{W}_j^{(i)})^T \otimes \boldsymbol{Q}_j^{(i)}$ 。将问题式(22)中约束条件 C8~C10 替换为式(24)~式(26), 根据半定松弛方法^[26], 去掉秩 1 约束 C7 可得

$$\begin{aligned} & \max_{\boldsymbol{W}_j^{(i)}, \boldsymbol{\Omega}_A^{(i)}, a^{(i)}, b_1^{(i)}, b_2^{(i)}, \boldsymbol{Q}_1^{(i)}, \boldsymbol{Q}_2^{(i)}, \boldsymbol{T}^{(i)}} S_1^{(i)} + S_2^{(i)} \\ & \text{s.t. C1~C6, 式(24)~式(26)} \end{aligned} \quad (27)$$

当优化变量 $\{a^{(i)}, \boldsymbol{Q}_1^{(i)}, \boldsymbol{Q}_2^{(i)}\}$ 给定时, 式(27)是关于变量 $\{\boldsymbol{W}_j^{(i)}, \boldsymbol{\Omega}_A^{(i)}, b_1^{(i)}, b_2^{(i)}, \boldsymbol{T}^{(i)}\}$ 的凸优化问题; 反之, 当优化变量 $\{\boldsymbol{W}_j^{(i)}, \boldsymbol{\Omega}_A^{(i)}, b_1^{(i)}, b_2^{(i)}, \boldsymbol{T}^{(i)}\}$ 给定时, 式(27)是关于 $\{a^{(i)}, \boldsymbol{Q}_1^{(i)}, \boldsymbol{Q}_2^{(i)}\}$ 的凸优化问题。因此可采用 BCD 算法对式(27)进行迭代求解。

通过求解式(27)得到的 $\boldsymbol{W}_j^{(i)}$ 可能不满足秩 1 约束, 此时, 采用式(28)计算出一个可行解^[27]。

$$\boldsymbol{W}_j^{(i)*} = \frac{\boldsymbol{W}_j^{(i)} \boldsymbol{h}_j^{(i)} \boldsymbol{h}_j^{(i)H} \boldsymbol{W}_j^{(i)}}{\boldsymbol{h}_j^{(i)H} \boldsymbol{W}_j^{(i)} \boldsymbol{h}_j^{(i)}} \quad (28)$$

$\boldsymbol{W}_j^{(i)*}$ 满足下列线性矩阵不等式关系

$$\begin{aligned} & \boldsymbol{W}_j^{(i)} - \boldsymbol{W}_j^{(i)*} = \\ & \left(\boldsymbol{I} - \frac{\boldsymbol{W}_j^{(i)\frac{1}{2}} \boldsymbol{h}_j^{(i)} \boldsymbol{h}_j^{(i)H} \boldsymbol{W}_j^{(i)\frac{1}{2}}}{\boldsymbol{h}_j^{(i)H} \boldsymbol{W}_j^{(i)} \boldsymbol{h}_j^{(i)}} \right) \boldsymbol{W}_j^{(i)\frac{1}{2}} \succeq \mathbf{0} \end{aligned} \quad (29)$$

由于 $\text{Tr}(\boldsymbol{W}_j^{(i)}) - \text{Tr}(\boldsymbol{W}_j^{(i)*}) \geq 0$, 因此可行解 $\boldsymbol{W}_j^{(i)*}$ 依然满足约束条件 C1 中的功率限制。与经典方法高斯随机化 (GRP, Gaussian randomization procedure)^[28] 相比, 通过式(28)所求得的秩 1 可行解并不次于原解^[27]。证明在附录 1 中给出。本文所提出的稳健性预编码矢量设计具体步骤如算法 1 所示。

算法 1 稳健性预编码矢量优化算法

初始化 设迭代次数 $n=1$, 迭代阈值 $\zeta=0.005$, 初始 $a^{(i)}(0)=1$, $\boldsymbol{Q}_1^{(i)}(0)=\boldsymbol{I}_N$, $\boldsymbol{Q}_2^{(i)}(0)=\boldsymbol{I}_N$, $S_1^{(i)}(0)=S_2^{(i)}(0)=0$

1) 利用 CVX 凸优化工具求解式(27), 得出最优解 $\{\boldsymbol{W}_j^{(i)}, \boldsymbol{\Omega}_A^{(i)}, b_1^{(i)}, b_2^{(i)}, \boldsymbol{T}^{(i)}\}$, 并更新

$$\begin{aligned} \boldsymbol{W}_j^{(i)}(n) &= \boldsymbol{W}_j^{(i)}, \quad \boldsymbol{\Omega}_A^{(i)}(n) = \boldsymbol{\Omega}_A^{(i)}, \quad b_1^{(i)}(n) = b_2^{(i)}, \\ b_2^{(i)}(n) &= b_2^{(i)}, \quad \boldsymbol{T}^{(i)}(n) = \boldsymbol{T}^{(i)} \end{aligned}$$

2) 利用 CVX 凸优化工具求解式(27), 得出最优解 $\{a^{(i)}, \boldsymbol{Q}_1^{(i)}, \boldsymbol{Q}_2^{(i)}\}$, 并更新 $a^{(i)}(n)=a^{(i)}$,

$$\boldsymbol{Q}_1^{(i)}(n) = \boldsymbol{Q}_1^{(i)}, \quad \boldsymbol{Q}_2^{(i)}(n) = \boldsymbol{Q}_2^{(i)}$$

3) 计算

$$\zeta^* = S_1^{(i)}(n) + S_2^{(i)}(n) - S_1^{(i)}(n-1) - S_2^{(i)}(n-1)$$

4) 更新迭代次数 $n = n + 1$

5) 若 $\zeta^* \leq \zeta$, 跳出迭代进入步骤 6); 否则返回步骤 1) 继续迭代

6) 根据式(28)计算 $\boldsymbol{W}_j^{(i)*}$

2.3 子载波分配算法

本文利用动态匹配理论处理子载波分配问题。定义网络中所有合法用户的集合为 $\mathcal{K} = \{U_k\}_{k=1}^K$, 考虑集合 \mathcal{K} 与 \mathcal{I} 之间进行二对一双边匹配。如果子载波 C_i 被分配给用户 U_k , 则认为 C_i 与 U_k 匹配成功。定义 $\text{PF}(U_k)$ 和 $\text{PF}(C_i)$ 分别为 U_k 与 C_i 的偏好表, 对于子载波 $C_i, C_r \in \mathcal{I}$, 如果基站到 U_k 的信道增益在子载波 C_i 上较大, 则认定 U_k 更偏好 C_i , 记为 $U_k : (C_i \succ C_r)$ 。对于用户集合 $\chi, \chi' \subset \mathcal{K}$, 满足 $\text{card}(\chi) = \text{card}(\chi') = 2$, 如果式(30)成立, 则认定 C_i 更偏好 χ , 记为 $C_i : (\chi \succ \chi')$ 。

$$\Xi_i(\chi) > \Xi_i(\chi') \quad (30)$$

其中, $\Xi_i(\chi)$ 表示子载波 C_i 被分配给用户集合 χ 时该子载波上的可达安全速率。

定义 1 定义二对一双边匹配 Ψ 由若干个从集合 \mathcal{K} 到集合 \mathcal{I} 的映射构成, Ψ 需满足以下 4 个特性。

1) $\Psi(U_k) \in \mathcal{I}$ 。

2) $\Psi^{-1}(C_i) \subset \mathcal{K}$ 。

3) $\text{card}(\Psi(U_k)) = 1$, $\text{card}(\Psi^{-1}(C_i)) = 2$ 。

4) $C_i \in \Psi(U_k) \Leftrightarrow U_k \in \Psi^{-1}(C_i)$ 。

定义 1 中, 特性 1) 表示每个用户可以匹配集合 \mathcal{I} 中的子载波; 特性 2) 表示每个子载波可以匹配集合 \mathcal{K} 中的用户子集; 特性 3) 限制每个用户能且只能匹配一个子载波, 每个子载波能且只能匹配 2 个用户; 特性 4) 表示 C_i 与 U_k 相互匹配。为最大化系统安全和速率, 可采用穷尽搜索算法寻找全局最优匹配结果, 但这种方法复杂度过高。本文利用 DA 算法构造稳定的双边匹配, 该算法的具体步骤如算法 2 所示。

算法 2 基于匹配理论子载波分配算法

初始化 根据信道增益初始化偏好表 $\text{PF}(U_k)$, 设 $S^{(i)} = \emptyset$ 表示分配到子载波 C_i 的用户集合, 设 $\bar{S} = \mathcal{K}$ 表示尚未分配到子载波的用户集合

1) while $\bar{S} \neq \emptyset$ do

2) for $k=1: \text{card}(\mathcal{K})$

3) 用户 U_k 向最偏好的子载波 C_{i^*} 发送匹配请求

- 4) if 子载波 C_{i^*} 没有被 2 个用户占用
- 5) C_{i^*} 接受 U_k 的匹配请求, C_{i^*} 与 U_k 匹配成功, 并更新 $\mathcal{S}^{(i^*)}$ 和 $\bar{\mathcal{S}}$
- 6) else if 子载波 C_{i^*} 已被 2 个用户占用
- 7) 从包含 3 个用户的集合 $\{\mathcal{S}^{(i^*)}, U_k\}$ 中任意选取双元素集合 χ , 利用算法 1 计算相应的 $\Xi_{i^*}(\chi)$ 值。 C_{i^*} 与最大 $\Xi_{i^*}(\chi)$ 值对应的集合 χ 匹配, 更新 $\mathcal{S}^{(i^*)}$ 和 $\bar{\mathcal{S}}$
- 8) 被拒绝的用户从其偏好列表中删除子载波 C_{i^*}
- 9) end if
- 10) end for
- 11) end while

定理 1 算法 2 必定能在集合 \mathcal{K} 与 \mathcal{I} 之间构成一个稳定匹配 Ψ 。

证明 采用反证法证明定理 1。假设 Ψ 不是一个稳定匹配, 则存在一个子载波-用户对 (C_i, U_k) , 满足 $C_i \notin \Psi(U_k)$, $U_k \notin \Psi^{-1}(C_i)$, 且 $U_k : (C_i \succ C_{i'})$, $C_{i'} \in \Psi(U_k)$ (即用户 U_k 与子载波 $C_{i'}$ 匹配, 但更偏好子载波 C_i), $C_i : (\chi \succ \Psi^{-1}(C_i))$, $\chi \subseteq U_k \cup \Psi^{-1}(C_i)$, $U_k \in \chi$ (即子载波 C_i 与用户子集 $\Psi^{-1}(C_i)$ 匹配, 但更偏好包含 U_k 在内的用户子集 χ)。

由算法 2 可知, U_k 在第 t 次迭代中向偏好列表中优先级更高的子载波 C_i 发送匹配请求信息, 但被拒绝。此时子载波 C_i 匹配用户集合 χ_t , 满足 $C_i : (\chi_t \succ \chi)$, $U_k \notin \chi_t$ 。由于算法 2 迭代结束后, 子载波 C_i 与用户集合 $\Psi^{-1}(C_i)$ 匹配, 因此 $C_i : (\Psi^{-1}(C_i) \succ \chi_t \succ \chi)$ 与假设矛盾。所以算法 2 必定能构成稳定匹配 Ψ 。证毕。

2.4 计算复杂度分析

根据文献[28], 半定规划 (SDP, semi-definite programming) 问题求解复杂度可表示为 $\mathcal{O}\left\{\max\{m, n\}^4 n^{\frac{1}{2}} \log\left(\frac{1}{\varepsilon}\right)\right\}$, 其中 m 是不等式的个数, n 是优化变量的维度, ε 是求解精度。算法 1 中步骤 1) 所求解的 SDP 问题不等式限制条件数量为 9, 优化变量维度为 M , 步骤 2) 所求解的 SDP 问题不等式限制条件数量为 2, 优化变量维度是 N 。定义 $X = \max\{M, 9\}$, $Y = \max\{N, 2\}$, 则步骤 1) 和步骤

2) 的计算复杂度分别为 $\mathcal{O}\left\{X^4 M^{\frac{1}{2}} \log\left(\frac{1}{\varepsilon}\right)\right\}$ 和 $\mathcal{O}\left\{Y^4 N^{\frac{1}{2}} \log\left(\frac{1}{\varepsilon}\right)\right\}$ 。假设 BCD 算法最大迭代次数为 N_{\max} , 又由于算法 2 中 DA 方法的最大迭代次数为 $KI - 2K + 2$, 因此本文所提资源分配算法总计算复杂度为 $\mathcal{O}\left\{2I^2 N_{\max} \left(X^4 M^{\frac{1}{2}} + Y^4 N^{\frac{1}{2}}\right) \log\left(\frac{1}{\varepsilon}\right)\right\}$ 。若采用穷尽搜索算法进行子载波分配, 总搜索次数为 $C_{2I}^2 C_{2(I-1)}^2 \cdots C_2^2 A_I'$, 资源分配算法总计算复杂度为 $\mathcal{O}\left\{\frac{(2I)! I!}{2^I} N_{\max} \left(X^4 M^{\frac{1}{2}} + Y^4 N^{\frac{1}{2}}\right) \log\left(\frac{1}{\varepsilon}\right)\right\}$, 远高于本文算法。如将算法 1 替换为文献[15]算法, 根据文献 [15], 资源分配算法总计算复杂度为 $\mathcal{O}\left\{6I^2 N'_{\max} (7 + 6M)^2 (16 + 4M)\right\}$, 其中 N'_{\max} 表示文献[15]算法的最大迭代次数。表 1 总结了上述 3 种算法的复杂度。

表 1 算法复杂度对比

算法	复杂度
本文算法	$\mathcal{O}\left\{2I^2 N_{\max} \left(X^4 M^{\frac{1}{2}} + Y^4 N^{\frac{1}{2}}\right) \log\left(\frac{1}{\varepsilon}\right)\right\}$
穷尽搜索算法	$\mathcal{O}\left\{\frac{(2I)! I!}{2^I} N_{\max} \left(X^4 M^{\frac{1}{2}} + Y^4 N^{\frac{1}{2}}\right) \log\left(\frac{1}{\varepsilon}\right)\right\}$
文献[15]算法	$\mathcal{O}\left\{6I^2 N'_{\max} (7 + 6M)^2 (16 + 4M)\right\}$

3 仿真分析

为了验证本文所提算法性能的优越性, 本节利用以下 6 种基准方案进行了对比研究: 方案 1, 本文算法采用穷尽搜索子载波分配; 方案 2, 本文算法采用随机子载波分配; 方案 3, OMA 传输方案; 方案 4, 基于连续凸逼近的安全和速率最大化算法^[14]; 方案 5, 基于连续凸逼近的 AN 发射功率最大化算法^[15]; 方案 6, 窃听信道信息完全已知情况下信道安全容量理论值。本文方案与方案 1 和方案 2 对比可验证所提子载波分配算法的优越性; 与方案 3 对比可验证 NOMA 系统相较于 OMA 系统的优势; 与方案 4 和方案 5 对比可验证本文所提预编码矢量优化算法的优越性, 为实现公平对比, 本文将文献[14-15]中的算法扩展到多载波系统, 并采用本文所提的子载波分配方

案；与方案 6 对比可反映出本文算法的安全和速率与理想安全和速率上限的差距。仿真中假设基站位于小区中心，用户均匀分布在半径为 500 m 的圆形区域内，归一化信道估计误差的上界定义为 $\xi^{(i)} = \frac{\delta^{(i)}}{\|H_{E}^{(i)}\|_F}, \forall i$ ，并假设 $\xi^{(1)} = \xi^{(2)} = \dots = \xi^{(l)} = \xi$ ，

为充分利用频谱资源，考虑网络中子载波被全部占用，用户数为子载波数的 2 倍，并假设所有子载波上发射功率均匀分配。系统仿真参数如表 2 所示。

参数	取值
子载波数	16
小区半径/m	500
系统带宽/MHz	5
噪声功率谱密度/(dBm·Hz ⁻¹)	-174
路径损失/km	128.1+37.6lgd
基站发射天线数	4
窃听天线数	{1, 2}
归一化信道估计误差	0.02
用户最小传输速率需求门限/(bit·(s·Hz) ⁻¹)	1
基站最大传输功率/dBm	30

BCD 算法收敛情况如图 2 所示。从图 2 可以看出，在不同参数取值下，算法均收敛，且迭代次数少于 10 次。当窃听天线数量变少时，系统安全和速率增大，原因在于 Eve 窃听能力下降，基站能够分配更多的功率进行数据传输，提升了用户数据速率。

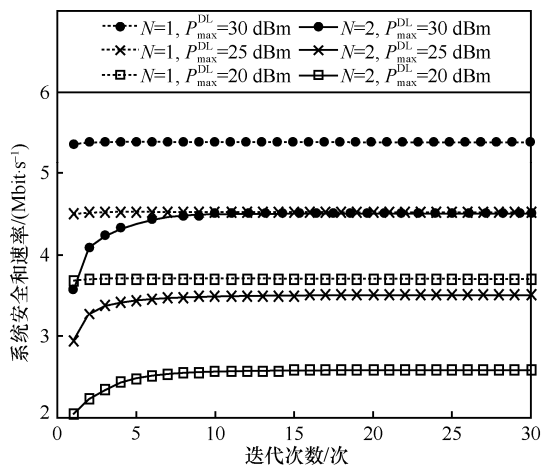


图 2 BCD 算法收敛情况

图 3 给出了本文算法的稳健性分析，其中归一化信道估计误差 ξ 取值从 0.02 变化到 0.30。从图 3

可以看出，在 ξ 取值范围内，系统安全和速率始终大于 20 Mbit/s，说明算法具有良好的稳健性。随着 ξ 增大，系统安全和速率降低，这是因为信道误差越大，基站能够获取的 CSI 质量越差。

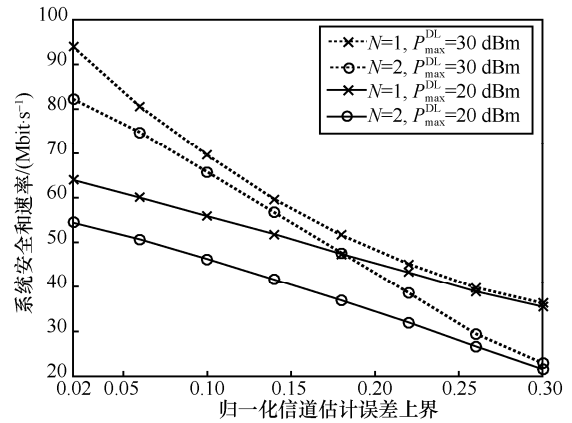


图 3 本文算法的稳健性分析

不同窃听天线数目下系统安全和速率随基站最大传输功率的变化如图 4 所示，其中图 4(a)和图 4(b)中窃听天线数分别设置为 1 和 2。由于文献[14]算法只适用于单窃听天线场景，因此仅在图 4(a)中给出。

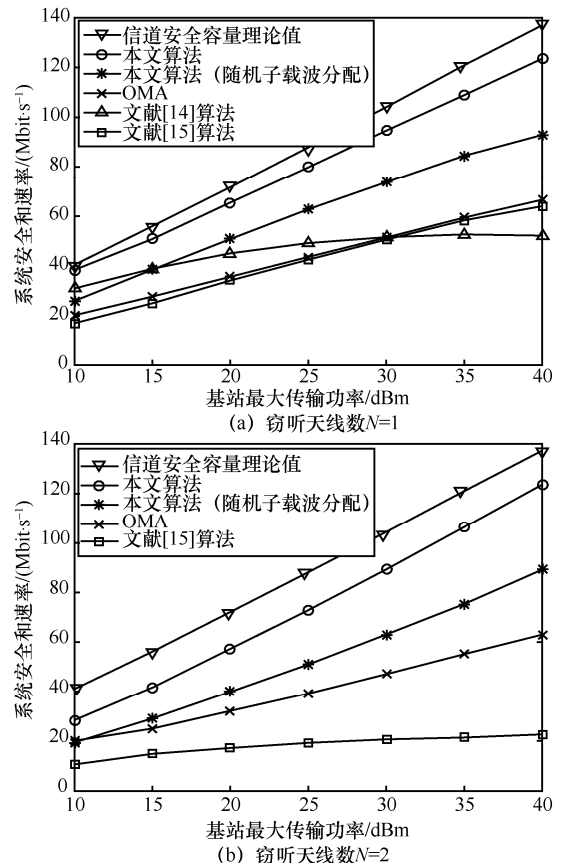


图 4 不同窃听天线数目下系统安全和速率随基站最大传输功率的变化

从图 4 中可以看出,随着基站最大传输功率的增加,系统安全和速率随之增大。在基站功率相同的情况下,本文算法显著优于文献[14-15]算法,且安全和速率约为传统 OMA 方案的 2 倍。对比分析可知,本文算法性能最接近信道安全容量,且所提低复杂度子载波分配算法明显优于随机子载波分配算法。另外,文献[15]算法在窃听天线数为 1 时性能增长较快,在窃听天线数为 2 时性能增长缓慢,原因在于随着天线数增大 Eve 窃听能力增强,文献[15]算法会分配更多的发射功率发送 AN 以干扰窃听信道,分配给用户数据传输的发射功率相应减少,导致数据速率下降。

不同窃听天线数目下系统安全和速率随用户数量的变化如图 5 所示,其中图 5(a)和图 5(b)中窃听天线数分别设置为 1 和 2。由于文献[14]算法只适用于单窃听天线场景,因此仅在图 5(a)中给出。从图 5 中可以看出,所有方案的安全和速率均随着用户数量的增大而增大。在用户数相同的情况下,本文方案显著优于 OMA 方案和文献[14-15]方案,所提低复杂度子载波分配算法性能明显优于随机子载波分配算法。

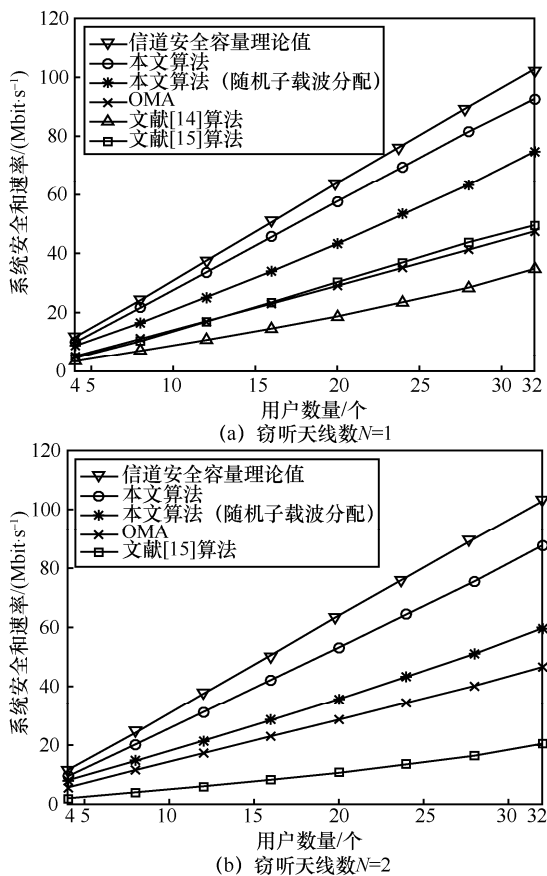


图 5 不同窃听天线数目下系统安全和速率随用户数量的变化

本文子载波分配算法与穷尽搜索子载波分配算法(以下简称穷尽搜索法)的性能对比如图 6 所示。由于穷尽搜索法程序在子载波数量较多的情况下运行非常耗时,因此在图 6 中子载波数量设置为 3。从图 6 中可以看出,本文算法的安全和速率略低于穷尽搜索法。这是因为通过穷尽搜索能够找到使系统安全和速率最大的子载波分配方案,而所提基于匹配的算法是寻找彼此最偏好的用户与子载波组合,并不能保证达到系统最大安全和速率。当基站最大传输功率 $P_{max}^{DL} = 40$ dBm、窃听天线数 $N = 1$ 时,二者性能差距约为 3 Mbit/s;当 $P_{max}^{DL} = 40$ dBm、 $N = 2$ 时,二者性能差距约为 2.5 Mbit/s,相较于系统总安全和速率所占比重较小。

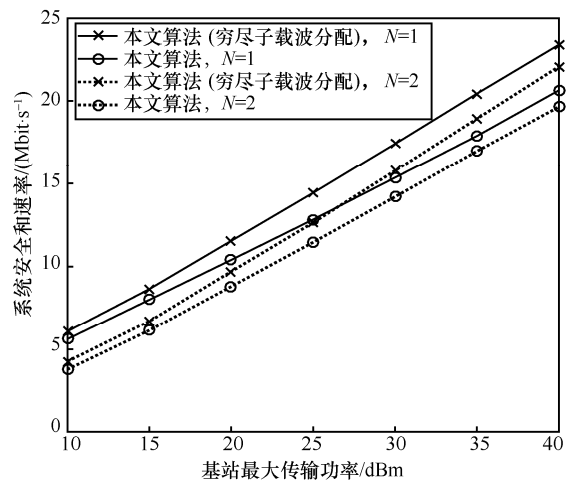


图 6 本文子载波分配算法与穷尽搜索子载波分配算法的性能对比

4 结束语

本文针对下行多载波 NOMA 安全传输系统稳健性资源分配算法进行了深入研究。考虑用户最小速率约束和基站最大传输功率约束,建立基于窃听信道不确定性的安全和速率最大化资源分配模型。为求解该非凸问题,将其分解为 AN、数据预编码矢量优化子问题和子载波分配子问题,并对这两部分进行联合优化。基于 S-procedure 算法将含不确定性参数的预编码优化子问题转化为确定性问题,利用 BCD 算法求解;基于动态匹配理论将子载波分配问题重新定义为双边匹配问题,采用 DA 算法求解;同时给出了算法的计算复杂度分析。仿真结果表明,本文算法具有较好的稳健性和安全性,所提子载波分配算法性能与穷尽搜索法性能非常接近,但能显著降低计算的复杂度。

本文研究工作为海量终端业务接入的 5G 物联网提供了一种高频效、高安全性的信息传输手段。为更符合实际应用, 后续工作将考虑同一子载波上存在 2 个以上用户, 非完美合法信道 CSI 估计以及存在多个 Eve 的场景, 进一步扩展本文所提方案。

附录 1 秩 1 解性能证明

证明 优化问题式(27)的目标函数可写为

$$\begin{aligned} S_1^{(i)} + S_2^{(i)} = & B_c \text{lb} \left(1 + \frac{\text{Tr}(\mathbf{h}_1^{(i)} \mathbf{W}_1^{(i)} \mathbf{h}_1^{(i)H})}{\text{Tr}(\mathbf{h}_1^{(i)} \mathbf{W}_2^{(i)} \mathbf{h}_1^{(i)H}) + \sigma^2} \right) + \\ & B_c \text{lb} \left(1 + \frac{\text{Tr}(\mathbf{h}_2^{(i)} \mathbf{W}_2^{(i)} \mathbf{h}_2^{(i)H})}{\sigma^2} \right) - \\ & B_c \text{lb} \det(\mathbf{I}_N + \mathbf{H}_E^{(i)} \mathbf{W}_1^{(i)} \mathbf{H}_E^{(i)H} \mathbf{Y}^{-1}) - \\ & B_c \text{lb} \det(\mathbf{I}_N + \mathbf{H}_E^{(i)} \mathbf{W}_2^{(i)} \mathbf{H}_E^{(i)H} \mathbf{Y}^{-1}) \end{aligned} \quad (31)$$

因此, 只要满足式(32)~式(34), 就可以保证用秩 1 解求得的目标函数不小于原解求得的目标函数。

$$\text{Tr}(\mathbf{h}_j^{(i)} \mathbf{W}_j^{(i)*} \mathbf{h}_j^{(i)H}) \geq \text{Tr}(\mathbf{h}_j^{(i)} \mathbf{W}_j^{(i)} \mathbf{h}_j^{(i)H}), j \in \{1, 2\} \quad (32)$$

$$\mathbf{H}_E^{(i)} \mathbf{W}_j^{(i)*} \mathbf{H}_E^{(i)H} \leq \mathbf{H}_E^{(i)} \mathbf{W}_j^{(i)} \mathbf{H}_E^{(i)H}, j \in \{1, 2\} \quad (33)$$

$$\text{Tr}(\mathbf{h}_1^{(i)} \mathbf{W}_2^{(i)*} \mathbf{h}_1^{(i)H}) \leq \text{Tr}(\mathbf{h}_1^{(i)} \mathbf{W}_2^{(i)} \mathbf{h}_1^{(i)H}) \quad (34)$$

通过式(29)可得到 $\mathbf{W}_j^{(i)} \geq \mathbf{W}_j^{(i)*}$, 因此式(33)和式(34)必然成立。又由于

$$\begin{aligned} \text{Tr}(\mathbf{h}_j^{(i)} \mathbf{W}_j^{(i)*} \mathbf{h}_j^{(i)H}) &= \\ \text{Tr} \left(\mathbf{h}_j^{(i)} \frac{\mathbf{W}_j^{(i)} \mathbf{h}_j^{(i)} \mathbf{h}_j^{(i)H} \mathbf{W}_j^{(i)}}{\mathbf{h}_j^{(i)} \mathbf{W}_j^{(i)} \mathbf{h}_j^{(i)H}} \mathbf{h}_j^{(i)H} \right) &= \\ \text{Tr}(\mathbf{h}_j^{(i)} \mathbf{W}_j^{(i)} \mathbf{h}_j^{(i)H}) \end{aligned} \quad (35)$$

因此, 式(32)成立。综上, 可得出结论, 通过式(28)所求得的秩 1 可行解 $\mathbf{W}_j^{(i)*}$ 并不次于原解 $\mathbf{W}_j^{(i)}$ 。证毕。

参考文献:

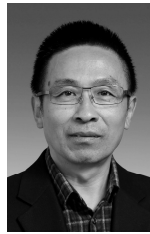
- [1] CHETTRI L, BERA R. A comprehensive survey on Internet of things (IoT) toward 5G wireless systems[J]. *IEEE Internet of Things Journal*, 2020, 7(1): 16-32.
- [2] WANG N, WANG P, ALIPOUR-FANID A, et al. Physical-layer security of 5G wireless networks for IoT: challenges and opportunities[J]. *IEEE Internet of Things Journal*, 2019, 6(5): 8169-8181.
- [3] DING Z G, LEI X F, KARAGIANNIDIS G K, et al. A survey on non-orthogonal multiple access for 5G networks: research challenges and future trends[J]. *IEEE Journal on Selected Areas in Communications*, 2017, 35(10): 2181-2195.
- [4] ZHU L P, ZHANG J, XIAO Z Y, et al. Millimeter-wave NOMA with user grouping, power allocation and hybrid beamforming[J]. *IEEE Transactions on Wireless Communications*, 2019, 18(11): 5065-5079.
- [5] 张波, 黄开枝, 钟州, 等. 异构携能通信网络中人工噪声辅助的稳健能量与信息安全传输方案[J]. *通信学报*, 2019, 40(3): 60-72. ZHANG B, HUANG K Z, ZHONG Z, et al. Artificial noise-aided robust secure information and power transmission scheme in heterogeneous networks with simultaneous wireless information and power transfer[J]. *Journal on Communications*, 2019, 40(3): 60-72.
- [6] 雷维嘉, 周洋, 谢显中, 等. MIMO 全双工双向安全通信系统的预编码矩阵设计[J]. *通信学报*, 2020, 41(10): 156-171. LEI W J, ZHOU Y, XIE X Z, et al. Design of precoding matrices in MIMO full duplex two-way security communication system[J]. *Journal on Communications*, 2020, 41(10): 156-171.
- [7] ZHANG Y, ZHAO X W, GENG S Y, et al. Power allocation algorithms for stable successive interference cancellation in millimeter wave NOMA systems[J]. *IEEE Transactions on Vehicular Technology*, 2021, 70(6): 5833-5847.
- [8] XIAO Z Y, ZHU L P, CHOI J, et al. Joint power allocation and beamforming for non-orthogonal multiple access (NOMA) in 5G millimeter wave communications[J]. *IEEE Transactions on Wireless Communications*, 2018, 17(5): 2961-2974.
- [9] ZHU L P, ZHANG J, XIAO Z Y, et al. Joint power control and beamforming for uplink non-orthogonal multiple access in 5G millimeter-wave communications[J]. *IEEE Transactions on Wireless Communications*, 2018, 17(9): 6177-6189.
- [10] HAO W M, ZENG M, CHU Z, et al. Energy-efficient power allocation in millimeter wave massive MIMO with non-orthogonal multiple access[J]. *IEEE Wireless Communications Letters*, 2017, 6(6): 782-785.
- [11] DING Z G, FAN P Z, POOR H V. Impact of user pairing on 5G non-orthogonal multiple-access downlink transmissions[J]. *IEEE Transactions on Vehicular Technology*, 2016, 65(8): 6010-6023.
- [12] LEI L, YUAN D, HO C K, et al. Power and channel allocation for non-orthogonal multiple access in 5G systems: tractability and computation[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(12): 8580-8594.
- [13] ZENG M, YADAV A, DOBRE O A, et al. Energy-efficient joint user-RB association and power allocation for uplink hybrid NOMA-OMA[J]. *IEEE Internet of Things Journal*, 2019, 6(3): 5119-5131.
- [14] ZHAO F, HAO W M, SHEN L F, et al. Secure energy efficiency transmission for mmWave-NOMA system[J]. *IEEE Systems Journal*, 2021, 15(2): 2226-2229.
- [15] ZHAO N, WANG W, WANG J J, et al. Joint beamforming and jamming optimization for secure transmission in MISO-NOMA networks[J]. *IEEE Transactions on Communications*, 2019, 67(3): 2294-2305.
- [16] LIU Y W, QIN Z J, ELKASHLAN M, et al. Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks[J]. *IEEE Transactions on Wireless Communications*, 2017, 16(3): 1656-1672.
- [17] HAN S J, XU X D, TAO X F, et al. Joint power and sub-channel allocation for secure transmission in NOMA-based mMTC networks[J]. *IEEE Systems Journal*, 2019, 13(3): 2476-2487.

- [18] ZHANG H J, YANG N, LONG K P, et al. Secure communications in NOMA system: subcarrier assignment and power allocation[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(7): 1441-1452.
- [19] LUO Z Q, STURM J F, ZHANG S Z. Multivariate nonnegative quadratic mappings[J]. SIAM Journal on Optimization, 2004, 14(4): 1140-1162.
- [20] HUA G, GOH J, THING V L L. A dynamic matching algorithm for audio timestamp identification using the ENF criterion[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(7): 1045-1055.
- [21] ZHU J, WANG J, HUANG Y, et al. On optimal power allocation for downlink non-orthogonal multiple access systems[J]. IEEE Journal on Selected Areas in Communications, 2017, 35(12): 2744-2757.
- [22] ZHOU X Y, MCKAY M R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation[J]. IEEE Transactions on Vehicular Technology, 2010, 59(8): 3831-3842.
- [23] HUANG J, SWINDLEHURST A L. Robust secure transmission in MISO channels based on worst-case optimization[J]. IEEE Transactions on Signal Processing, 2012, 60(4): 1696-1707.
- [24] FENG R H, LI Q Z, 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.
- [25] SHI Q J, XU W Q, WU J S, et al. Secure beamforming for MIMO broadcasting with wireless information and power transfer[J]. IEEE Transactions on Wireless Communications, 2015, 14(5): 2841-2853.
- [26] ZHAO X W, ZHANG Y, GENG S Y, et al. Hybrid precoding for an adaptive interference decoding SWIPT system with full-duplex IoT devices[J]. IEEE Internet of Things Journal, 2020, 7(2): 1164-1177.
- [27] KONG Z M, YANG S S, WANG D, et al. Robust beamforming and jamming for enhancing the physical layer security of full duplex radios[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(12): 3151-3159.
- [28] LUO Z Q, MA W K, SO A M C, et al. Semidefinite relaxation of quadratic optimization problems[J]. IEEE Signal Processing Magazine, 2010, 27(3): 20-34.

[作者简介]



张钰 (1995-), 女, 安徽六安人, 华北电力大学博士生, 主要研究方向为 5G 毫米波通信中的预编码技术、非正交多址接入技术、无线通信网络资源优化等。



赵雄文 (1964-), 男, 陕西清涧人, 博士, 华北电力大学教授、博士生导师, 主要研究方向为无线通信与电力系统通信等。



王晓晴 (1998-), 女, 青海西宁人, 华北电力大学硕士生, 主要研究方向为智能超表面、无线通信网络资源优化等。



耿绥燕 (1966-), 女, 陕西绥德人, 博士, 华北电力大学副教授, 主要研究方向为短距离无线通信技术。



秦鹏 (1987-), 男, 河南商丘人, 博士, 华北电力大学副教授, 主要研究方向为网络通信技术等。



周振宇 (1983-), 男, 河北张家口人, 博士, 华北电力大学教授、博士生导师, 主要研究方向为无线通信网络与新技术、物联网与现代传感技术、能源互联网信息通信技术等。