

能量采集多天线中继网络中基于人工噪声辅助的安全传输方案

任清华^{1,2}, 张广大^{1†}, 樊志凯¹

(1. 空军工程大学信息与导航学院, 陕西 西安 710077;

2. 中国电子科技集团公司 航天信息应用技术重点实验室, 河北 石家庄 050081)

摘要:针对多天线中继系统中继节点面临的可用能量受限问题和存在的严重信息泄露隐患,提出了一种基于能量采集技术的联合中继波束成形和多天线友好干扰机协作干扰的物理层安全传输方案.首先,构建基于放大转发(Amplify-and-Forward, AF)模式的多天线协作中继网络,其次,中继节点和友好干扰机在时隙切换(Time Switch, TS)策略下进行能量采集和保密信号传输.接着,以系统保密速率最大化(Secrecy Rate Maximization, SRM)为目标,在满足中继节点和友好干扰机采集能量约束条件下,联合设计出最优中继信号传输波束成形矩阵、人工噪声(Artificial Noise, AN)协方差矩阵和时隙切换系数.然而,由于条件约束,导致该SRM问题为非凸问题,故通过结合半定松弛(Semi-Definite Relaxation, SDR)技术以及拉格朗日对偶理论,设计出一种双层优化算法求得最优解,并且,为了降低复杂度和对比方案性能,给出了一种基于迫零预编码的次优传输方案.最后,仿真结果表明,所提方案能够显著提高系统保密性能,具备一定抗窃听攻击能力.

关键词:物理层安全;能量采集;波束成形;协作干扰;保密速率;半定松弛

中图分类号:TN918.82 **文献标志码:**A

Secure Transmission Scheme Based on Artificial Noise-aided for Energy Harvesting Multi-antenna Relay Networks

REN Qinghua^{1,2}, ZHANG Guangda^{1†}, FAN Zhikai¹

(1. Information and Navigation College, Air Force Engineering University, Xi'an 710077, China;

2. Key Laboratory of Aerospace Information Applications, China Electronics Technology Group, Shijiazhuang 050081, China)

Abstract: Aiming at the problem of limited available energy and serious information leakage risks faced by the relay nodes in the multi-antenna relay system, a physical layer secure transmission scheme of joint relay beamforming and multi-antenna friendly jammer cooperative jamming based on energy harvesting technology is proposed. Firstly, a multi-antenna cooperative relay network based on the amplify-and-forward (AF) mode is constructed. Secondly, the relay nodes and friendly jammers perform energy harvesting and confidentiality signal transmission based on the time switching (TS) strategy. Then, with the goal of the system secrecy rate maximization (SRM), the optimal

* 收稿日期:2021-11-04

基金项目:国家重点实验室发展项目(KX162600022),The State Key Laboratories Development Program of China (KX162600022)

作者简介:任清华(1967—),男,浙江三门人,空军工程大学教授,硕士生导师

† 通信联系人, E-mail: 18782117541@163.com

relay signal transmission beamforming matrix, artificial noise (AN) covariance and time switching coefficient are jointly designed under the condition of meeting the energy harvesting constraints of the relay and the friendly jammers. However, due to conditional constraints, the SRM problem is a non-convex. Therefore, a Bi-level optimization algorithm is designed to obtain the optimal solution by combining semi-definite relaxation (SDR) technology and Lagrange duality theory, and in order to reduce the complexity and compare the performance of the proposed scheme, a suboptimal transmission scheme based on zero-forcing precoding is given. Finally, the simulation results show that the proposed scheme can significantly improve the security performance of the system and has a certain anti-eavesdropping attack capability.

Key words: physical-layer security; energy harvesting; beamforming; cooperative jamming; secrecy rate; semi-definite relaxation

随着第五代移动通信技术的迅猛发展和移动终端的广泛普及,无线通信网络的业务量呈现爆炸式增长,诸多问题也随之而来.如:海量设备的接入使得无线通信网络结构日益复杂化;各类通信终端标准化协议不完善;更为重要的是,无线通信网络的信道的开放特性引起了广大用户对隐私信息泄露的担忧^[1].而传统无线通信网络的安全机制主要依赖基于密码体制的加密技术,其原理是通过提高计算复杂度和代价确保安全.近年来,由于计算科学领域不断取得突破性进展,故寻求更为安全的传输技术和机制成为网络安全的一个重要研究内容.物理层安全作为传统上层加密方案的补充,利用无线信道的内在特性实现安全传输,为解决无线通信系统中安全传输问题,提供了新的思路^[2].

协作中继作为物理层安全技术的重要组成部分,被证明能够在扩大通信网络覆盖范围的同时,也可提升网络的保密性能^[3-4].因此,学者将各种增强物理层安全的有关技术引入协作中继网络,比如协作波束成形技术^[5]、中继选择技术^[6]和协作干扰技术^[7]等.其中,协作干扰技术因其实现复杂度低而成为研究的热点内容.根据协作干扰节点的不同,一般可划分为内部节点协作和外部节点协作.针对协作中继网络下的安全方案,内部节点协作主要是利用源节点^[8]或者目的节点^[9]等系统内在通信节点进行协作干扰.文献[8]研究了不可信全双工中继网络存在的信息安全问题,提出了基于源节点协作干扰的安全传输方案,推导了保密中断概率闭合表达式和可达保密速率的渐近表达式.文献[9]针对存在多天线目的节点的协作中继网络,提出一种利用天线切换和最优功率分配策略联合优化方案.外部节点协作则主要通过借助友好干扰机对窃听节点进行干

扰^[10].文献[10]考虑协作非正交多址网络下存在单窃听者的通信场景,提出一种利用友好干扰机协作干扰的安全传输方案,并分别推导了系统的保密中断概率、截获概率和可达保密速率的闭合表达式.

多天线中继网络不仅能够充分利用天线带来的空间资源,而且能够在不增加频谱资源和发射功率的前提下,提升系统容量.这为设计物理层安全方案提供了更为丰富的资源.因此,许多学者针对多天线中继网络的安全传输展开深入研究.文献[11-13]利用波束成形技术从不同侧面对多天线协作中继网络的安全方案展开设计.可以看到:单一的安全波束成形方案对系统保密性能的提升具有一定局限性.在此基础上,文献[14-15]通过在中继节点处引入AN进行协作干扰以提高系统安全性,其实现方式是在中继节点处构造联合波束成形和AN矩阵.联合构造和优化矩阵将大大提高中继节点处计算代价,但也给中继节点有限的能量和资源带来巨大挑战.

文献[16-17]通过设计不同的能量优化方案在保证系统保密性能的同时,提高系统的能量利用效率,但这并未从根本上解决问题.在多天线中继网络中,随着中继处能量的减少,最优化波束成形方案效果将减弱,系统保密性能将减弱.因此,能量受限问题严重制约了多天线中继网络的安全性能.

针对以上问题,本文考虑能量受限的多天线中继网络下存在非法窃听者时的信息安全传输问题,提出了一种AN辅助的安全传输方案.首先,利用多天线波束成形结合能量采集技术向中继节点传输信息和能量;接着,引入友好干扰机进行AN协作干扰.多天线中继在放大转发信息的同时,友好干扰机发射AN对窃听者进行干扰.所提方案在中继和友好干扰机采集能量的约束下,通过联合设计中继波束成

形矩阵、AN协方差矩阵和时隙切换系数,最大化系统保密速率.数值仿真实验表明,本文所提方案相较于传统方案,对提升系统保密性能具有明显优势.

1 系统模型与问题描述

1.1 系统模型

本文针对图1所示的多天线中继网络展开研究.其中,包含一个基站S、一个合法用户D、一个中继节点R和一个非法窃听者E.另外,本文引入 K 个友好干扰机J辅助完成安全传输.除中继节点和友好干扰机均配有 N 根天线外,其他节点均配备单天线用于信息传输.中继节点R和友好干扰机J均具备能量采集能力,能够从射频信号中提取能量用于自身对信息的处理.不失一般性,本文假设由于深度衰落或障碍物的影响,基站S和合法用户D间不存在直连链路,故需要借助R完成信息交互.

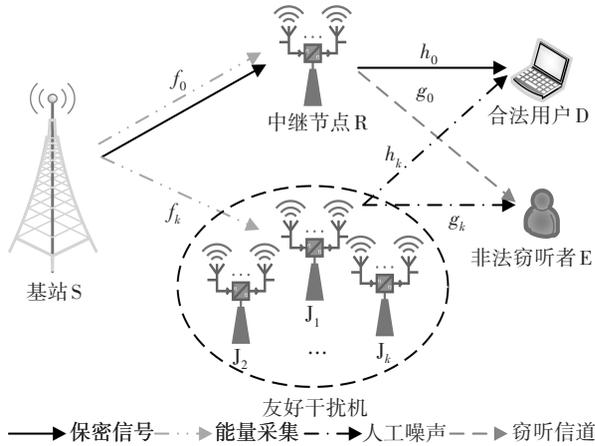


图1 多天线中继系统模型

Fig.1 Model for multi-antenna relay system

本文通信系统信道模型同时考虑大尺度衰落和小尺度衰落模型.其中,大尺度衰落采用标准路径衰落模型即 $L(d_{ij}) = d_{ij}^{-\kappa}$, d_{ij} 表示节点 i 和节点 j 间距离, κ 表示路径损耗系数.小尺度衰落采用准静态莱斯衰落模型.以 \mathbf{h}_i 为例,信道增益矩阵表示为:

$$\mathbf{h}_i = \sqrt{\frac{K_R}{K_R + 1}} \bar{\mathbf{h}}_i^{\text{LOS}} + \sqrt{\frac{1}{K_R + 1}} \tilde{\mathbf{h}}_i^{\text{NLOS}} \quad (1)$$

式中: K_R 表示莱斯 K 因子, $\bar{\mathbf{h}}_i^{\text{LOS}}$ 表示相应节点的视距直达分量, $\tilde{\mathbf{h}}_i^{\text{NLOS}}$ 表示瑞利衰落分量,并且为服从均值为0,方差为 $\sigma_i^2 \mathbf{I}$ 的循环对称复高斯随机变量.

图2为基于TS策略的协作中继网络的信息与能量传输过程.在整个过程中,利用时隙分配系数 α 将每个传输块周期 T 划分为3个阶段.

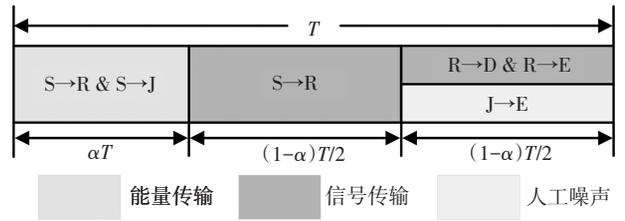


图2 多天线中继网络中信息与能量传输过程

Fig.2 Information and energy transmission process of multi-antenna relay network

具体描述为:在第1时隙中,基站S向中继节点R和友好干扰机J发送射频信号,R和J利用射频信号完成能量采集.则二者接收到的信号可表示为:

$$\mathbf{y}_{\text{IR}} = \sqrt{P_s} \mathbf{f}_0 x_0 + \mathbf{n}_R \quad (2)$$

$$\mathbf{y}_{\text{Jk}} = \sqrt{P_s} \mathbf{f}_k x_0 + \mathbf{n}_{\text{Jk}} \quad (3)$$

式中: P_s 为发射功率; $\mathbf{f}_0 \in \mathbb{C}^{N \times 1}$, $\mathbf{f}_k \in \mathbb{C}^{N \times 1}$ 分别为S到R、 J_k 处天线间的信道系数向量; \mathbf{n}_R 和 \mathbf{n}_{Jk} 为R和 J_k 处加性高斯白噪声(Additive White Gaussian Noise, AWGN), $\mathbf{n}_R \sim \text{CN}(0, \sigma_R^2 \mathbf{I}_N)$, $\mathbf{n}_{\text{Jk}} \sim \text{CN}(0, \sigma_{\text{Jk}}^2 \mathbf{I}_N)$. \mathbf{I}_N 表示 $N \times N$ 单位矩阵.

基于TS策略,R以及任意友好干扰机 J_k 在规定时间内能够采集到的能量为:

$$E_R = \eta \alpha T (P_s \|\mathbf{f}_0\|^2 + \sigma_R^2) \quad (4)$$

$$E_{\text{Jk}} = \eta \alpha T (P_s \|\mathbf{f}_k\|^2 + \sigma_{\text{Jk}}^2) \quad (5)$$

式中: $\eta \in (0, 1)$ 表示能量转换效率.

在第2时隙中,S以相同的功率 P_s 向R发送保密信号 x_s ,则R接收到的保密信号为:

$$\mathbf{y}_{2R} = \sqrt{P_s} \mathbf{f}_0 x_s + \mathbf{n}_R \quad (6)$$

在第3时隙中,R基于AF模式将保密信号 \mathbf{y}_{2R} 转发至D处,则转发信号可表示为:

$$\mathbf{x}_R = \mathbf{W} \mathbf{y}_{2R} \quad (7)$$

式中: $\mathbf{W} \in \mathbb{C}^{N \times N}$ 为R处的波束成形矩阵.

该时隙中,友好干扰机 J_k 利用第1时隙中采集的能量发送AN向量 \mathbf{z}_k ,因此,D接收到的信号为:

$$\mathbf{y}_D = \sqrt{P_s} \mathbf{x}_R + \mathbf{n}_D \quad (8)$$

将式(6)和式(7)代入后,可得:

$$\mathbf{y}_D = \sqrt{P_s} \mathbf{h}_0^H \mathbf{W} \mathbf{f}_0 x_s + \mathbf{h}_0^H \mathbf{W} \mathbf{n}_R + \sum_{k=1}^K \mathbf{h}_k^H \mathbf{z}_k + \mathbf{n}_D \quad (9)$$

式中: \mathbf{z}_k 中元素为循环对称复高斯随机变量,且服从 $\mathbf{z}_k \sim \text{CN}(0, \boldsymbol{\Sigma}_k)$, $\boldsymbol{\Sigma}_k$ 为AN协方差矩阵. $\mathbf{h}_0 \in \mathbb{C}^{N \times 1}$ 表示R处天线与D处天线间的信道系数向量,

$\mathbf{n}_D \sim \text{CN}(0, \sigma_D^2 \mathbf{I}_N)$, 表示合法用户处 AWGN.

此时, 窃听者 E 能够接收到的信号可表示为:

$$\mathbf{y}_E = \sqrt{P_S} \mathbf{g}_0^H \mathbf{W} \mathbf{f}_0 x_S + \mathbf{g}_0^H \mathbf{W} \mathbf{n}_R + \sum_{k=1}^K \mathbf{g}_k^H \mathbf{z}_k + \mathbf{n}_E \quad (10)$$

式中: $\mathbf{g}_0 \in \mathbb{C}^{N \times 1}$ 表示 R 处天线与 E 处天线间的信道系数向量. $\mathbf{n}_E \sim \text{CN}(0, \sigma_E^2 \mathbf{I}_N)$, 表示窃听者处 AWGN.

根据式(9)和式(10), 可得 D 和 E 处的信干噪比 (Signal-to-Interference-plus-Noise Ratio, SINR) 为:

$$\gamma_D = P_S \left| \mathbf{h}_0^H \mathbf{W} \mathbf{f}_0 \right|^2 / \left(\sigma_R^2 \left| \mathbf{h}_0^H \mathbf{W} \right|^2 + \sum_{k=1}^K \left| \mathbf{h}_k^H \mathbf{z}_k \right|^2 + \sigma_D^2 \right) \quad (11)$$

$$\gamma_E = P_S \left| \mathbf{g}_0^H \mathbf{W} \mathbf{f}_0 \right|^2 / \left(\sigma_R^2 \left| \mathbf{g}_0^H \mathbf{W} \right|^2 + \sum_{k=1}^K \left| \mathbf{g}_k^H \mathbf{z}_k \right|^2 + \sigma_E^2 \right) \quad (12)$$

由上述信号模型可知, R 转发信号的功率为:

$$P_R = \text{Tr}(\mathbb{E}\{x_R x_R^H\}) = \text{Tr}(\mathbf{W} (P_S \mathbf{f}_0 \mathbf{f}_0^H + \sigma_R^2 \mathbf{I}_N) \mathbf{W}^H) \quad (13)$$

式中: $\text{Tr}(\cdot)$ 表示矩阵的迹.

结合式(4), 考虑到 R 中原有能量, 因此, R 处在功率约束可表示为:

$$P_R \leq \frac{2E_R}{(1-\alpha)T} + P_0 = P_{\max} \quad (14)$$

式中: P_0 为中继节点初始功率.

对任意友好干扰机 J_k , 存在 AN 发射功率应小于所能采集的能量, 故存在以下约束:

$$\text{Tr}(\boldsymbol{\Sigma}_k) \leq E_{J_k}, \forall k, \quad (15)$$

1.2 问题描述

根据文献[18]可知, 当合法信道的信道条件优于窃听信道时, 系统将能够获得正的保密速率, 此时, 表明系统能够进行安全通信. 具体描述为:

$$R_S = [C_D - C_E]^+ \quad (16)$$

上式中有: $[x]^+ = \max\{0, x\}$; $C_D = \frac{1-\alpha}{2} \log_2(1 + \gamma_D)$ 和 $C_E = \frac{1-\alpha}{2} \log_2(1 + \gamma_E)$ 分别表示合法信道容量和窃听信道容量.

本文根据全局信道状态信息 (Channel State Information, CSI), 在 R 处总功率以及任意 J_k 功率受限时, 通过联合优化波束成形矩阵以及 AN 协方差矩阵, 从而实现 SRM 的目标. 具体表示为:

$$(P1): R_S^* = \max_{\boldsymbol{\Sigma}_k, \mathbf{W}, \alpha} \frac{1-\alpha}{2} \left[\log_2(1 + \gamma_D) - \log_2(1 + \gamma_E) \right]^+ \quad (17a)$$

$$\text{s. t. } P_R \leq P_{\max} \quad (17b)$$

$$\text{Tr}(\boldsymbol{\Sigma}_k) \leq E_{J_k}, \forall k \quad (17c)$$

$$\boldsymbol{\Sigma}_k \geq \mathbf{0}, \forall k \quad (17d)$$

$$0 < \alpha < 1 \quad (17e)$$

由于在以上约束中, 存在目标函数, 对于保密速率最大化的求解问题为非凸的优化问题, 故无法直接求解. 因此, 本文采用分布优化方案对该问题求解.

2 人工噪声辅助下波束成形设计

2.1 最优波束成形设计

为了对 SRM 问题求解, 首先引入辅助变量 χ , 将问题(P1)重写为问题(P1.1).

$$R_S^* = \max_{\boldsymbol{\Sigma}_k, \mathbf{W}, \alpha} \frac{1-\alpha}{2} \left(\log_2(1 + \gamma_D) - \log_2\left(\frac{1}{\chi}\right) \right) \quad (18a)$$

$$\text{s. t. } 1 + \frac{P_S \left| \mathbf{g}_0^H \mathbf{W} \mathbf{f}_0 \right|^2}{\sigma_R^2 \left\| \mathbf{g}_0^H \mathbf{W} \right\|^2 + \sum_{k=1}^K \left\| \mathbf{g}_k^H \mathbf{z}_k \right\|^2 + \sigma_E^2} \leq \frac{1}{\chi} \quad (18b)$$

$$\text{式(17b) ~ 式(17e)} \quad (18c)$$

因为上式为非凸优化问题, 无法对其直接求解, 故根据文献[19]的思想, 将问题(P1)转化为两个子问题进行求解. 对第一个子问题求解, 将问题(P1.1)转化为双层优化问题, 其中, 外层优化问题作为一个单变量优化问题, 可以采用一维搜索方法求解, 内层作为一个半定规划问题, 能够利用半定松弛技术对子问题展开求解; 而后, 通过一维搜索得到第二个子问题的最优解. 首先, 固定时隙切换系数 α 以优化波束成形向量 \mathbf{W} 和 AN 协方差矩阵 $\boldsymbol{\Sigma}_k$, 其次, 根据得到的 \mathbf{W} 和 $\boldsymbol{\Sigma}_k$ 优化 α . 对于问题(P1.1), 能够将外层单变量优化问题转化为:

$$(P1.1): R_S^* = \max_{\boldsymbol{\Sigma}_k, \mathbf{W}, \alpha} \frac{1-\alpha}{2} \left(\log_2(1 + H(\chi)) - \log_2\left(\frac{1}{\chi}\right) \right) \quad (19)$$

$$\text{s. t. } \chi_{\min} \leq \chi \leq \chi_{\max}$$

式中: χ_{\min} 和 χ_{\max} 分别为单变量 χ 的下界与上界. 当给定 χ 时, 内层优化问题最优目标值表示为:

$$(P2): H(\chi) = \max_{\Sigma, \mathbf{W}} \frac{P_s |\mathbf{h}_0^H \mathbf{W} \mathbf{f}_0|^2}{\sigma_R^2 \|\mathbf{h}_0^H \mathbf{W}\|^2 + \sum_{k=1}^K \|\mathbf{h}_k^H \mathbf{z}_k\|^2 + \sigma_D^2}$$

$$\text{s. t. } 1 + \frac{P_s |\mathbf{g}_0^H \mathbf{W} \mathbf{f}_0|^2}{\sigma_R^2 \|\mathbf{g}_0^H \mathbf{W}\|^2 + \sum_{k=1}^K \|\mathbf{g}_k^H \mathbf{z}_k\|^2 + \sigma_E^2} \leq \frac{1}{\chi}, \forall k \in K$$

式(17b)~式(17e)

(20)

对于外层优化问题式(19)中的一维变量的变化范围,由式(18b)可知, $\chi \leq 1$, 即 $\chi_{\max} = 1$. 而 χ_{\min} 则可通过保密传输速率 $R_s^* \geq 0$ 得到, 即当 $R_s^* \geq 0$, 必须满足 $1 + H(\chi) \geq 1/\chi$, 解得:

$$\chi \geq \left(1 + \frac{\mathbf{w}^H \mathbf{D}_1 \mathbf{w}}{\sigma_R^2 \mathbf{w}^H \mathbf{D}_2 \mathbf{w} + \sum_{k=1}^K \mathbf{h}_k^H \Sigma_k \mathbf{h}_k + \sigma_D^2} \right)^{-1} \quad (21)$$

式中: $\mathbf{w} = \text{vec}(\mathbf{W})$. $\text{vec}(\cdot)$ 表示矩阵的列向量化操作. $\mathbf{D}_1 = (\mathbf{h}_0 \mathbf{h}_0^H) \otimes \mathbf{I}_N$, $\mathbf{D}_2 = P_s (\mathbf{f}_0^* \mathbf{f}_0^T) \otimes (\mathbf{h}_0 \mathbf{h}_0^H)$. 定义新变量 ψ :

$$\psi = \frac{\mathbf{w}^H \mathbf{D}_1 \mathbf{w}}{\sigma_R^2 \mathbf{w}^H \mathbf{D}_2 \mathbf{w} + \sigma_D^2} \quad (22)$$

故只需要求出 ψ_{\max} , 即可得到变量下界 χ_{\min} . 因此, 可通过优化下列问题, 得式(22)对应最大值:

$$\psi^* = \max_{\mathbf{w}} \frac{\mathbf{w}^H \mathbf{D}_1 \mathbf{w}}{\sigma_R^2 \mathbf{w}^H \mathbf{D}_2 \mathbf{w} + \sigma_D^2} \quad (23)$$

s. t. $\mathbf{w}^H \mathbf{D}_3 \mathbf{w} \leq P_{\max}$

式中: $\mathbf{D}_3 = (P_s \mathbf{f}_0^* \mathbf{f}_0^T + \sigma_R^2 \mathbf{I}_N) \otimes \mathbf{I}_N$, 故式(21)和下面的广义 Rayleigh 熵问题等价.

$$\psi^* = \max_{\mathbf{w}} \frac{\mathbf{w}^H \mathbf{D}_1 \mathbf{w}}{\mathbf{w}^H (\sigma_D^2 \mathbf{D}_3 / P_{\max} + \sigma_R^2 \mathbf{D}_2) \mathbf{w}} \quad (24)$$

根据文献[20]知, 式(24)最优目标值大小为 $\psi_{\max} = P_s \mathbf{u}^H (\sigma_D^2 \mathbf{D}_3 / P_{\max} + \sigma_R^2 \mathbf{D}_2)^{-1} \mathbf{u}$, $\mathbf{u} = (\mathbf{f}_0^* \otimes \mathbf{h}_0)$, 可知一维变量下界为:

$$\chi_{\min} = \left(1 + P_s \mathbf{u}^H (\sigma_D^2 \mathbf{D}_3 / P_{\max} + \sigma_R^2 \mathbf{D}_2)^{-1} \mathbf{u} \right)^{-1} \quad (25)$$

观察式(19)和式(20)可知, 式(19)可以通过一维搜索寻找最优的 χ 以及对应的最优目标值. 但在此之前, 需要得到式(20)的最优目标值. 故双层优化问题的关键在于对内层优化问题式(20)的求解.

为便于后续分析, 利用矩阵论知识对式(20)进行处理, 有以下等式成立.

$$\begin{cases} |\mathbf{h}_0^H \mathbf{W} \mathbf{f}_0|^2 = (\mathbf{f}_0^* \otimes \mathbf{h}_0)(\mathbf{f}_0^* \otimes \mathbf{h}_0)^H \mathbf{W} \mathbf{W}^H = \text{Tr}(\mathbf{A}_1 \mathbf{X}) \\ \|\mathbf{h}_0^H \mathbf{W}\|^2 = \mathbf{h}_0^H \mathbf{W} \mathbf{W}^H \mathbf{h}_0 = \mathbf{W}^H (\mathbf{I}_N \otimes \mathbf{h}_0 \mathbf{h}_0^H) \mathbf{W} = \text{Tr}(\mathbf{Y}_1 \mathbf{X}) \\ |\mathbf{g}_0^H \mathbf{W} \mathbf{f}_0|^2 = (\mathbf{f}_0^* \otimes \mathbf{g}_0)(\mathbf{f}_0^* \otimes \mathbf{g}_0)^H \mathbf{W} \mathbf{W}^H = \text{Tr}(\mathbf{A}_2 \mathbf{X}) \\ \|\mathbf{g}_0^H \mathbf{W}\|^2 = \mathbf{g}_0^H \mathbf{W} \mathbf{W}^H \mathbf{g}_0 = \mathbf{W}^H (\mathbf{I}_N \otimes \mathbf{g}_0 \mathbf{g}_0^H) \mathbf{W} = \text{Tr}(\mathbf{Y}_2 \mathbf{X}) \end{cases} \quad (26)$$

对约束条件处理后有:

$$\begin{cases} \text{Tr}(\mathbf{W} (P_s \mathbf{f}_0 \mathbf{f}_0^H + \sigma_R^2 \mathbf{I}_N) \mathbf{W}^H) = \|\Phi \mathbf{W}\|^2 \\ \Phi = (\mathbf{I}_N \otimes \Theta)^{1/2} \end{cases} \quad (27)$$

式中: $\Theta = P_s \mathbf{f}_0 \mathbf{f}_0^H + \sigma_R^2 \mathbf{I}_N$.

定义 $\mathbf{X} = \mathbf{w} \mathbf{w}^H$, $\bar{\Phi} = \Phi^H \Phi$. 将等式代入式(20)后, 由于式(20)中仍存在限制 $\text{rank}(\mathbf{X}) = 1$ 是非凸的, 且约束项中变量相互耦合的情况, 使得求解困难, 故利用 SDR 技术, 去掉非凸限制条件 $\text{rank}(\mathbf{X}) = 1$, 得到式(20)的松弛问题表示如下:

$$H(\chi) = \max_{\Sigma, \mathbf{X}} \frac{P_s \text{Tr}(\mathbf{A}_1 \mathbf{X})}{\sigma_R^2 \text{Tr}(\mathbf{Y}_1 \mathbf{X}) + \sum_{k=1}^K \mathbf{h}_k^H \Sigma_k \mathbf{h}_k + \sigma_D^2} \quad (28a)$$

$$\text{s. t. } P_s \text{Tr}(\mathbf{A}_2 \mathbf{X}) \leq \varepsilon \left(\sigma_R^2 \text{Tr}(\mathbf{Y}_2 \mathbf{X}) + \sum_{k=1}^K \mathbf{g}_k^H \Sigma_k \mathbf{g}_k + \sigma_E^2 \right) \quad (28b)$$

$$\text{Tr}(\bar{\Phi} \mathbf{X}) \leq P_{\max} \quad (28c)$$

$$\text{Tr}(\Sigma_k) \leq \eta \alpha T \left(P_s \|\mathbf{f}_k\|^2 + \sigma_J^2 \right), \forall k \quad (28d)$$

$$\mathbf{X} \geq \mathbf{0}, \Sigma_k \geq \mathbf{0}, \forall k \quad (28e)$$

式中: $\varepsilon = 1/\chi - 1$. 利用 Charnes-Cooper 变换, 把上式转化为一个凸的 SDP 问题. 所以, 引入松弛变量 $\tau \geq 0$, 式(28)可重写为问题(P2.1):

$$(P2.1): \max_{\Sigma, \mathbf{X}, \tau} P_s \text{Tr}(\mathbf{A}_1 \mathbf{X})$$

$$\text{s. t. } \sigma_R^2 \text{Tr}(\mathbf{Y}_1 \mathbf{X}) + \sum_{k=1}^K \mathbf{h}_k^H \Sigma_k \mathbf{h}_k + \tau \sigma_D^2 \leq 1$$

$$P_s \text{Tr}(\mathbf{A}_2 \mathbf{X}) \leq \varepsilon \left(\sigma_R^2 \text{Tr}(\mathbf{Y}_2 \mathbf{X}) + \sum_{k=1}^K \mathbf{g}_k^H \Sigma_k \mathbf{g}_k + \tau \sigma_E^2 \right)$$

式(28c)~式(28e)

(29)

此时, 式(29)转化为标准形式凸优化问题, 接着, 利用 Slater 条件^[21]进行验证, 可知其存在严格可行点. 因此, 原始问题与对偶问题间强对偶成立, 所以式(29)最优解可以通过求解其对偶问题等价得到. 对应拉格朗日对偶函数为:

$$L(\Omega) = \text{Tr}(\mathbf{M}\mathbf{X}) + \sum_{k=1}^K \text{Tr}(\mathbf{N}_k \boldsymbol{\Sigma}_k) + \mu\tau + \lambda \quad (30)$$

其中, Ω 为包含式(29)原始问题和对偶问题变量的集合. 经过计算合并后, 相关变量表达式为:

$$\mathbf{M} = P_s \mathbf{A}_1 - \lambda \sigma_R^2 \mathbf{Y}_1 - \delta P_s \mathbf{A}_2 + \delta \varepsilon \sigma_R^2 \mathbf{Y}_2 - \beta_0 \bar{\Phi} \quad (31)$$

$$\mathbf{N}_k = -\lambda \mathbf{h}_k \mathbf{h}_k^H + \delta \varepsilon \mathbf{g}_k \mathbf{g}_k^H - \beta_k \mathbf{I}, \forall k \quad (32)$$

$$\mu = -\lambda \sigma_D^2 + \delta \varepsilon \sigma_E^2 + \beta_0 P_{\max} + \sum_{k=1}^K \eta \alpha T \left(P_s \|f_k\|^2 + \sigma_j^2 \right) \quad (33)$$

其中, $\lambda, \delta, \beta_0, \beta_k, \mu$ 分别对应于式(29)中约束项的拉格朗日乘子. 式(30)作为一个非线性规划问题, 最优解应当满足 Karush-Kuhn-Tucker 条件. 故式(30)有关的 KKT 条件表示为:

$$\mathbf{M}^* \mathbf{X}^* = 0, \quad (34)$$

$$\mathbf{N}_k^* \boldsymbol{\Sigma}_k^* = 0, \forall k \quad (35)$$

$$\beta_k^* \left(\text{Tr}(\boldsymbol{\Sigma}_k^*) - \tau^* \eta \alpha T \left(P_s \|f_k\|^2 + \sigma_j^2 \right) \right) = 0, \forall k \quad (36)$$

定理 1 内层问题(P2.1)最优解 $(\mathbf{X}^*, \{\boldsymbol{\Sigma}_k^*\}, \tau^*)$ 必满足下列条件:

$$1) \text{rank}(\boldsymbol{\Sigma}_k^*) \begin{cases} \geq N - 2, & \text{if } \beta_k^* = 0, \\ = 1, & \text{if } \beta_k^* > 0, \end{cases} \quad \forall k.$$

$$2) \text{最优解 } \mathbf{X}^* \text{ 满足: } \mathbf{X}^* = \sum_{n=1}^{N^2 - r_c} a_n \boldsymbol{\pi}_n \boldsymbol{\pi}_n^H + b \xi \xi^H, \text{ 其}$$

中, $a_n \geq 0, b > 0, r_c = \text{rank}(\mathbf{C}^*)$.

3) 根据条件2), 若 \mathbf{X}^* 满足条件: $\text{rank}(\mathbf{X}^*) > 1$, 可以通过以下充分条件构建一个新的秩为1的解 $(\hat{\mathbf{X}}^*, \{\hat{\boldsymbol{\Sigma}}_k^*\}, \hat{\tau}^*)$:

$$\hat{\mathbf{X}}^* = b \xi \xi^H = \mathbf{X}^* - \sum_{n=1}^{N^2 - r_c} a_n \boldsymbol{\pi}_n \boldsymbol{\pi}_n^H \quad (37)$$

$$\hat{\boldsymbol{\Sigma}}_k^* = \boldsymbol{\Sigma}_k^*, \forall k$$

$$\hat{\tau}^* = \tau^* + \Delta\tau$$

其中, 存在 $\Delta\tau \geq 0$, 且满足下式:

$$\left[\sum_{n=1}^{N^2 - r_c} a_n \text{Tr} \left(\boldsymbol{\pi}_n^H \left(\frac{\sigma_R^2 \mathbf{Y}_2}{\sigma_E^2} - \frac{P_s \mathbf{A}_2}{\gamma_E \sigma_E^2} \right) \boldsymbol{\pi}_n \right) \right]^+ \leq \Delta\tau \leq \frac{\sigma_R^2}{\sigma_D^2} \sum_{n=1}^{N^2 - r_c} a_n \text{Tr}(\boldsymbol{\pi}_n^H \mathbf{Y}_1 \boldsymbol{\pi}_n) \quad (38)$$

证 充分条件1).

由式(32)知, 对任意确定的 k :

(a) 若 $\beta_k^* = 0$, 则 $\mathbf{N}_k^* = -\lambda^* \mathbf{h}_k \mathbf{h}_k^H + \delta^* \varepsilon \mathbf{g}_k \mathbf{g}_k^H$. 根据矩阵秩的性质有:

$$\text{rank}(\mathbf{N}_k^*) \leq \text{rank}(\mathbf{h}_k \mathbf{h}_k^H) + \text{rank}(\mathbf{g}_k \mathbf{g}_k^H) = 2 \quad (39)$$

根据式(35), 有 $\text{rank}(\boldsymbol{\Sigma}_k^*) \geq N - 2$.

(b) 若 $\beta_k^* > 0$, 同理可得, 对 $\forall k$:

$$\text{rank}(\mathbf{N}_k^*) \geq \text{rank}(-\beta_k^* \mathbf{I}_N - \lambda \mathbf{h}_k \mathbf{h}_k^H) - \delta \varepsilon \mathbf{g}_k \mathbf{g}_k^H = N - 1 \quad (40)$$

依据式(35), 则有 $\text{rank}(\boldsymbol{\Sigma}_k^*) \leq 1$. 若

$\text{rank}(\boldsymbol{\Sigma}_k^*) = 0$, 则有 $\text{Tr}(\boldsymbol{\Sigma}_k^*) - \tau^* \eta \alpha T \left(P_s \|f_k\|^2 + \sigma_j^2 \right) < 0$, 此时在式(36)中必有 $\beta_k^* = 0$. 这与假设矛盾.

故当 $\beta_k^* > 0$ 时, 有等式 $\text{rank}(\boldsymbol{\Sigma}_k^*) = 1$ 成立.

充分条件2)和3).

定义新变量 \mathbf{C}^* , 具体为:

$$\mathbf{C}^* = -\lambda^* \sigma_R^2 \mathbf{Y}_1 - \delta^* P_s \mathbf{A}_2 + \delta^* \varepsilon \sigma_R^2 \mathbf{Y}_2 - \beta_0^* \bar{\Phi} \quad (41)$$

依据式(31), 计算后, 知下式成立: $\mathbf{M}^* = P_s \mathbf{A}_1 + \mathbf{C}^*$.

令 Ψ 表示 \mathbf{M}^* 的零空间, $\boldsymbol{\pi}_n$ 表示 Ψ 第 n 列, $n=1, 2, \dots, N^2 - r_c$, 即 $\Psi = \left\{ \boldsymbol{\pi}_n \right\}_{n=1}^{N^2 - r_c}$.

(a) 当 $r_c = N^2$ 时, 此时矩阵 \mathbf{C}^* 满秩, 可得:

$$\text{rank}(\mathbf{M}^*) \geq r_c - 1 = N^2 - 1 \quad (42)$$

因此, $N^2 - 1 \leq \text{rank}(\mathbf{M}^*) \leq N^2$, 当 \mathbf{M}^* 的秩取 $N^2 - 1$ 时, 则有 $\text{rank}(\text{null}(\mathbf{M}^*)) = 1$, 令 ξ 为 \mathbf{M}^* 对应的唯一基础解系, 则对应问题的最优解可表示为 $\mathbf{X}^* = b \xi \xi^H$. 当 \mathbf{M}^* 的秩取 N^2 时, 由式(34)知, 最优解 $\mathbf{X}^* = \mathbf{0}$, 表示波束成形矩阵为 $\mathbf{0}$, 故此时不为式(29)的最优解.

(b) 当 $r_c < N^2$, 知 \mathbf{C}^* 非满秩, 有 $\text{rank}(\mathbf{M}^*) \geq r_c - 1$.

将 $\mathbf{M}^* = P_s \mathbf{A}_1 + \mathbf{C}^*$ 两端左乘 $\boldsymbol{\pi}_n^H$, 同时右乘 $\boldsymbol{\pi}_n$, 有:

$$\boldsymbol{\pi}_n^H \mathbf{M}^* \boldsymbol{\pi}_n = P_s \boldsymbol{\pi}_n^H \mathbf{A}_1 \boldsymbol{\pi}_n + \boldsymbol{\pi}_n^H \mathbf{C}^* \boldsymbol{\pi}_n = P_s \boldsymbol{\pi}_n^H \mathbf{A}_1 \boldsymbol{\pi}_n, \forall n \quad (43)$$

根据式(30)可知, 当且仅当 $\mathbf{M}^* \leq \mathbf{0}$, 可得最优值, 使得 $\boldsymbol{\pi}_n^H \mathbf{M}^* \boldsymbol{\pi}_n \leq 0$ 成立. 又因为 $P_s \boldsymbol{\pi}_n^H \mathbf{A}_1 \boldsymbol{\pi}_n \geq 0$, 故当且仅当 $\mathbf{M}^* \boldsymbol{\pi}_n = \mathbf{0}, \mathbf{A}_1 \boldsymbol{\pi}_n = \mathbf{0}$ 同时成立时, 满足上述条件. 故有 $\Psi \subseteq \text{null}(\mathbf{M}^*)$, 即

$$N^2 - \text{rank}(\mathbf{M}^*) \geq N^2 - r_c \Rightarrow \text{rank}(\mathbf{M}^*) \leq r_c \quad (44)$$

同理, 对 \mathbf{M}^* 的秩分别讨论: 当 $\text{rank}(\mathbf{M}^*) = r_c$ 时,

等式 $\Psi = \text{null}(\mathbf{M}^*)$ 和 $\mathbf{X}^* = \sum_{n=1}^{N^2 - r_c} a_n \boldsymbol{\pi}_n \boldsymbol{\pi}_n^H$ 将成立, 而因

为 $\mathbf{A}_1 \boldsymbol{\pi}_n = \mathbf{0}$, 代入得 $P_s \text{Tr}(\mathbf{A}_1 \mathbf{X}^*) = 0$, 表示 D 处接收保密信号的 SINR 为 0, 故 \mathbf{X}^* 非最优解. \mathbf{M}^* 的秩将满足 $\text{rank}(\mathbf{M}^*) = r_c - 1$, 则 \mathbf{M}^* 的零空间的秩大小为

$\text{rank}(\text{null}(\mathbf{M}^*)) = N^2 - r_c + 1$. 表明 \mathbf{M}^* 的零空间除 Ψ 外, 还存在一个额外维度的基向量, 令其为 ξ , 则此时最优解可表示为:

$$\mathbf{X}^* = \sum_{n=1}^{N^2-r_c} a_n \boldsymbol{\pi}_n \boldsymbol{\pi}_n^H + b \xi \xi^H \quad (45)$$

假设 $\{\mathbf{X}^*, \{\boldsymbol{\Sigma}_k^*\}, \tau^*\}$ 为问题 (P2.1) 的一个最优解. 当 $\text{rank}(\mathbf{X}^*) \geq 2$ 时, 可以根据式 (37) 条件构建新的秩-1 解 $\{\hat{\mathbf{X}}^*, \{\hat{\boldsymbol{\Sigma}}_k^*\}, \hat{\tau}^*\}$.

已知最优解满足式 (38), 下面验证最优解是否满足式 (29), 分别代入不同约束项进行验证:

$$\begin{aligned} & \sigma_R^2 \text{Tr}(\mathbf{Y}_1 \hat{\mathbf{X}}^*) + \sum_{k=1}^K \mathbf{h}_k^H \hat{\boldsymbol{\Sigma}}_k^* \mathbf{h}_k + \hat{\tau}^* \sigma_D^2 \\ & \leq \sigma_R^2 \text{Tr} \left(\mathbf{Y}_1 \left(\mathbf{X}^* - \sum_{n=1}^{N^2-r_c} a_n \boldsymbol{\pi}_n \boldsymbol{\pi}_n^H \right) \right) \\ & + \sum_{k=1}^K \mathbf{h}_k^H \boldsymbol{\Sigma}_k^* \mathbf{h}_k + \left(\tau^* + \frac{\sigma_R^2}{\sigma_D^2} \sum_{n=1}^{N^2-r_c} a_n \text{Tr}(\mathbf{Y}_1 \boldsymbol{\pi}_n \boldsymbol{\pi}_n^H) \right) \sigma_D^2 \quad (46) \\ & = \sigma_R^2 \text{Tr}(\mathbf{Y}_1 \mathbf{X}^*) + \sum_{k=1}^K \mathbf{h}_k^H \boldsymbol{\Sigma}_k^* \mathbf{h}_k + \tau^* \sigma_D^2 \leq 1 \end{aligned}$$

$$\begin{aligned} P_S \text{Tr}(\mathbf{A}_2 \hat{\mathbf{X}}^*) &= P_S \text{Tr} \left(\mathbf{A}_2 \left(\mathbf{X}^* - \sum_{n=1}^{N^2-r_c} a_n \boldsymbol{\pi}_n \boldsymbol{\pi}_n^H \right) \right) \\ & \leq \varepsilon \left(\sigma_R^2 \text{Tr}(\mathbf{Y}_2 \mathbf{X}^*) + \sum_{k=1}^K \mathbf{g}_k^H \boldsymbol{\Sigma}_k^* \mathbf{g}_k + \tau^* \sigma_E^2 \right) \\ & + \varepsilon \left(\sigma_E^2 \Delta \tau - \sigma_R^2 \text{Tr} \left(\mathbf{Y}_2 \sum_{n=1}^{N^2-r_c} a_n \boldsymbol{\pi}_n \boldsymbol{\pi}_n^H \right) \right) \\ & = \varepsilon \left(\sigma_R^2 \text{Tr}(\mathbf{Y}_2 \hat{\mathbf{X}}^*) + \sum_{k=1}^K \mathbf{g}_k^H \hat{\boldsymbol{\Sigma}}_k^* \mathbf{g}_k + \hat{\tau}^* \sigma_E^2 \right) \end{aligned} \quad (47)$$

同理, 易验证所求得最优解将满足式 (29) 中其他约束项. 由于 $P_S \text{Tr}(\mathbf{A}_2 \mathbf{X}^*) = P_S \text{Tr}(\mathbf{A}_2 \hat{\mathbf{X}}^*)$, 表明重构的最优解能够实现相同最优目标值. 因此, 总可以找到一组最优解 \mathbf{X}^* , 满足条件 $\text{rank}(\mathbf{X}^*) = 1$. 证毕.

2.2 求解算法描述

根据以上分析, 回到双层优化问题式 (19) 和式 (20), 给定 χ , 通过求解式 (29) 得到内层优化式 (28) 的最优目标值, 进而可求得外层优化式 (19) 的最优目标值, 该双层优化问题的求解算法详细步骤见表 1.

表 1 双层优化求解算法

Tab.1 Bi-level optimization algorithm

初始化参数, $a = \left(1 + P_S \mathbf{u}^H \left(\sigma_D^2 \mathbf{D}_3 / P_{\max} + \sigma_R^2 \mathbf{D}_2 \right)^{-1} \mathbf{u} \right)^{-1}$, $b = 1$, 设置一维搜索精度 ζ .

步骤 1 令 $l = a + 0.382(b - a)$, $u = a + 0.618(b - a)$, 对优化式 (29) 进行求解, 得到 $\phi_l = \phi(1/l - 1)$, $\phi_u = \phi(1/u - 1)$, 用 ϕ_l 和 ϕ_u 分别代替 $H(\chi)$, 计算式 (19) 的目标函数值, 分别得到 $R(l)$ 和 $R(u)$.

步骤 2 While $(b - a) > \zeta$

步骤 3 if $(R(l) < R(u))$ then

步骤 4 令 $a = l$, $l = u$, $\phi_l = \phi_u$, $u = a + 0.618(b - a)$, 求解式 (29), 得到 $\phi_u = \phi(1/u - 1)$, 然后用 ϕ_u 代替 $H(\chi)$, 最后, 计算式 (19) 的最优目标值, 得到 R_u .

步骤 5 else

步骤 6 令 $b = u$, $u = l$, $\phi_u = \phi_l$, $l = a + 0.382(b - a)$, 求解式 (29), 得到 $\phi_l = \phi(1/l - 1)$, 然后用 ϕ_l 代替 $H(\chi)$. 最后, 计算式 (19) 的最优目标值, 得到 R_l .

步骤 7 end if

步骤 8 end while

步骤 9 $\chi = (a + b)/2$, 将 $\varepsilon = 1/\chi - 1$ 代入式 (29) 求解后得最优目标值 $H(\varepsilon)$ 和最优解 $(\mathbf{X}^*, \{\boldsymbol{\Sigma}_k^*\})$, 然后, 用 $H(\varepsilon)$ 代替 $H(\chi)$, 最后, 计算式 (19) 得到最优目标函数值 R_S^* .

步骤 10 if $\text{rank}(\mathbf{X}) \geq 2$

步骤 11 while 满足式 (38) 中给出的充分条件时

步骤 12 根据式 (37) 中条件构造新的可行解 $\{\hat{\mathbf{X}}^*, \{\hat{\boldsymbol{\Sigma}}_k^*\}, \hat{\tau}^*\}$, 同时令 $\mathbf{w}^* = \sqrt{b} \xi$.

步骤 13 end while

步骤 14 else if 不满足式 (38) 给出的充分条件时:

步骤 15 利用文献 [22] 中算法 1 对任意秩的解进行降秩和重构后. 根据本文所提算法求解, 得到最优解 $(\mathbf{X}^*, \{\boldsymbol{\Sigma}_k^*\})$.

步骤 16 end if

步骤 17 利用奇异值分解理论, 分解矩阵 $\mathbf{X} = \mathbf{w}\mathbf{w}^H$ 后, 得到 $\mathbf{X}^* = \text{vec}^{-1}(\mathbf{w})$;

步骤 18 输出最优解 $(\mathbf{X}^*, \{\boldsymbol{\Sigma}_k^*\})$ 和最优目标函数值 R_S^* .

2.3 时隙切换系数优化

经过上述算法得到最优解 $(\mathbf{X}^*, \{\Sigma_k^*\})$ 后,代入并重写式(19),将最优解代入式(28)后,采用一维搜索方法即可得最优的 α^* .

3 基于迫零预编码次优传输方案设计

迫零预编码的基本思想是通过限制每个发送波束矢量,使其位于接收者信道组成的复合信道的零空间中^[23].由上文可知,AN辅助下的保密传输方案实现较为复杂.因此,为降低复杂度,并对比所提方案性能,提出一种基于迫零预编码次优传输方案.该方案主要思想是将噪声波束垂直于合法用户信道,同时最大化AN对窃听者的干扰效果.即

$$\mathbf{h}_k \mathbf{z}_k = 0 \quad (48)$$

为实现上述目的,令AN信号结构为 $\mathbf{z}_k = \tilde{\mathbf{V}}_k \tilde{\mathbf{z}}_k$,有 $\tilde{\mathbf{z}}_k \in \mathbb{C}^{(N-1) \times 1}, \forall k, \tilde{\mathbf{z}}_k \sim \text{CN}(\mathbf{0}, \tilde{\Sigma}_k)$,则 \mathbf{h}_k 的零空间可表示为:

$$\tilde{\mathbf{V}}_k \tilde{\mathbf{V}}_k^H = \mathbf{I} - \mathbf{h}_k \mathbf{h}_k^H / \|\mathbf{h}_k\|^2 \quad (49)$$

上式中, \mathbf{I} 表示单位矩阵.将式(49)代入式(29)中约束项,当等式成立时,有 $\tilde{\Sigma}_k^* = \mathbf{s}_k^2 \tilde{\mathbf{g}}_k \tilde{\mathbf{g}}_k^H$.其中, $\tilde{\mathbf{g}}_k = \tilde{\mathbf{V}}_k^T \mathbf{g}_k$,且 $\mathbf{s}_k = \sqrt{\eta \alpha T (P_s \|\mathbf{f}_k\|^2 + \sigma_j^2)} / \|\tilde{\mathbf{g}}_k\|$.可知,当给定任意波束成形矩阵 \mathbf{W} ,能够优化AN信号 $\tilde{\mathbf{z}}_k$,从而最大限度地提高其在窃听者处的影响,可表示为:

$$q = \max_{\tilde{\Sigma}_k} \sum_{k=1}^K \mathbf{g}_k^H \mathbf{V}_k \Sigma_k \tilde{\mathbf{V}}_k^H \mathbf{g}_k \quad (50)$$

结合式(48),则式(29)可重写为:

$$\begin{aligned} & \max_{\mathbf{X}, \tau} P_s \text{Tr}(\mathbf{A}_1 \mathbf{X}) \\ & \text{s. t. } \sigma_R^2 \text{Tr}(\mathbf{Y}_1 \mathbf{X}) + \tau \sigma_D^2 \leq 1 \\ & P_s \text{Tr}(\mathbf{A}_2 \mathbf{X}) \leq \varepsilon (\sigma_R^2 \text{Tr}(\mathbf{Y}_2 \mathbf{X}) + \tau q + \tau \sigma_E^2) \\ & \text{Tr}(\bar{\Phi} \mathbf{X}) \leq \tau P_{\max}, \mathbf{X} \geq \mathbf{0}, \tau \geq 0 \end{aligned} \quad (51)$$

因此,可通过求解式(51)找出最优解和最优值.

定理2 优化问题式(51)总存在一个最优解 \mathbf{X}^* ,满足 $\text{rank}(\mathbf{X}^*) = 1$,以及下列条件:

$$\begin{cases} \mathbf{w}^* = \mu \mathbf{v}_{\max}(\mathbf{Z}^*) \\ \mathbf{Z}^* = P_s \mathbf{A}_1 - \lambda^* \sigma_R^2 \mathbf{Y}_1 - \boldsymbol{\omega}^* P_s \mathbf{A}_2 + \boldsymbol{\omega}^* \sigma_R^2 \mathbf{Y}_2 - \beta_0^* \bar{\Phi} \end{cases} \quad (52)$$

式中: $\lambda^*, \boldsymbol{\omega}^*, \beta_0^*$ 表示式中约束项对偶变量的最优解,即拉格朗日乘子. $\mathbf{v}_{\max}(\cdot)$ 表示伴随矩阵的最大特征值所对应的特征向量,并且

$$\mu = \sqrt{\frac{P_{\max}}{\text{Tr}(\bar{\Phi}) \mathbf{v}_{\max}(\mathbf{Z}^*) \mathbf{v}_{\max}^H(\mathbf{Z}^*)}} \quad (53)$$

证 优化问题式(51)对应的拉格朗日函数为:

$$\begin{aligned} L(\Lambda) = & \text{Tr}((P_s \mathbf{A}_1 - \lambda \sigma_R^2 \mathbf{Y}_1 - \alpha P_s \mathbf{A}_2 + \alpha \varepsilon \sigma_R^2 \mathbf{Y}_2 - \beta_0 \bar{\Phi}) \mathbf{X}) \\ & + (-\lambda \sigma_D^2 + \alpha \varepsilon (q + \sigma_E^2) + \beta_0 P_{\max}) \tau + \lambda \end{aligned}$$

式中: $\Lambda = \{\mathbf{X}, \tau, \lambda, \boldsymbol{\omega}, \beta_0\}$ 表示由原始变量和对偶变量组成的集合.由于式(51)对应的优化问题是凸的,且满足Slater约束条件,故该优化问题与其对偶问题的对偶间隙为0.设优化问题式(51)与其对偶问题的最优解为 $\lambda^*, \boldsymbol{\omega}^*$ 和 β_0^* .为保证拉格朗日函数有界,以下约束必须成立:

$$\mathbf{Z} = P_s \mathbf{A}_1 - \lambda \sigma_R^2 \mathbf{Y}_1 - \alpha P_s \mathbf{A}_2 + \alpha \varepsilon \sigma_R^2 \mathbf{Y}_2 - \beta_0 \bar{\Phi} \leq \mathbf{0} \quad (54)$$

$$-\lambda \sigma_D^2 + \alpha \varepsilon (q + \sigma_E^2) + \beta_0 P_{\max} \leq 0 \quad (55)$$

可以看到 $\mathbf{Z} \leq \mathbf{0}$,表明式(51)中半定松弛是紧的,所以该情况下采用半定松弛的方法可以获得全局最优解.即存在 \mathbf{w}^* ,有 $\mathbf{X}^* = \mathbf{w}^* \mathbf{w}^{*H}$.又因为最优解满足KKT条件,有 $\mathbf{Z}^* \mathbf{X}^* = \mathbf{0}$.所以结合矩阵论知识和式(51)中约束,求解后有:

$$\mathbf{w}^* = \mu \mathbf{v}_{\max}(\mathbf{Z}^*) \quad (56)$$

式中: \mathbf{w}^* 是矩阵 \mathbf{Z}^* 的零特征值对应的特征向量. μ 的大小见式(53).证毕.

4 仿真结果与分析

本节针对所提传输方案的性能采用蒙特卡洛方法进行数值分析与仿真验证.所有的仿真结果均是 10^6 次信道实现后取平均值得到的.

4.1 仿真参数设置

为验证本文所提联合AN的最优协作波束成形方案保密性能,与以下3种方案进行对比:1)基于迫零预编码次优传输方案.2)全向人工噪声方案:该方案通过将AN均匀分散在合法用户信道的零空间里,确保在对窃听者造成干扰的同时,使得合法用户对保密信号的接收过程不受影响.3)最优安全波束成形方案:该方案中中继节点在转发数据时,友好干扰机不发送AN,即AN协方差矩阵设为 $\mathbf{0}$.

为了更好地说明本文中的特定参数设置对系统保密性能的影响,并考虑到通信节点间的距离引起的衰落^[24],本文仿真位置参数按图3所示位置拓扑结构进行设置.其中,存在两个同心圆,并且满足 $r_2 = 2r_1$.S、D与E的方向角分别为 $\pi, \pi/6$ 和 $11\pi/6$,其中,R位于圆心.友好干扰机均匀分布在半径为 r_1 的圆周

上,则第 k 个节点的方向角为 $\theta_k = 2\pi(k - 1)/K$.

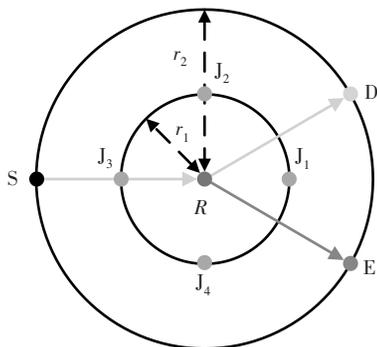


图3 通信节点位置变化拓扑结构

Fig.3 Topology structure of communication node location change

具体的仿真参数如表2所示,后文中如无特殊说明,仿真中均使用表2中所给参数值.

表2 仿真参数

Tab.2 Simulation parameters

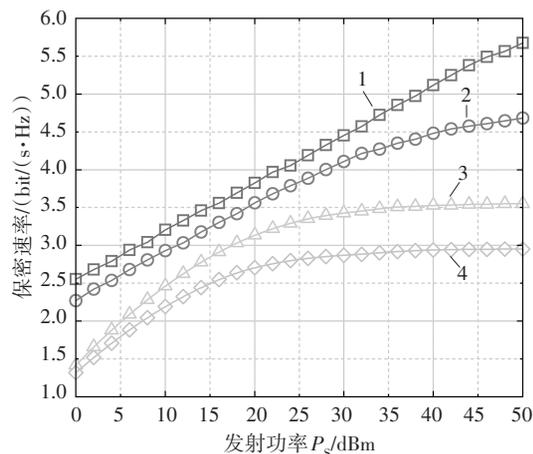
| 参数 | 仿真值 |
|---|---------|
| 发射功率 P_s | 25 dBm |
| 莱斯因子 K_R | 3 dB |
| 路径损耗系数 κ | 2.7 |
| 初始功率 P_0 | 20 dBm |
| 大圆半径 r_2 | 10 m |
| 小圆半径 r_1 | 5 m |
| 能量转化效率 η | 0.7 |
| 时隙切换系数 α | 0.4 |
| 传输时隙 T | 1 s |
| 友好干扰机数目 K | 8 |
| 天线数目 N | 8 |
| 噪声功率 $\sigma_R^2, \sigma_D^2, \sigma_E^2$ | -50 dBm |
| σ_0^2, σ_i^2 | -30 dBm |

4.2 结果与分析

图4为不同安全传输方案下,系统保密速率随着基站S发射功率增大时的变化情况.

如图4所示,从中可以得出,随着基站S发射功率的增加,4种方案的保密速率均随之提升.当 $P_s = 50$ dBm时,所提方案能够实现的保密速率相比另外3种方案分别高出约 0.989 8 bit/(s·Hz)、2.123 3 bit/(s·Hz)和 2.722 bit/(s·Hz).并且,在S发射功率较小时,全向人工噪声方案略微优于最优安全波束成形方案,表明在保密信号对应信噪比较低时,人工噪声方案对信息保密传输十分重要.另外,对比4种方案曲线,可以发现,全向人工噪声方案和最优安全波束成形方案随着发射功率的增大,系统保密速率的提升将逐渐减弱后收敛.这是因为,最优安全波束成形

方案没有对窃听者进行约束,因而,系统保密速率不能从发射功率的增大而得到相应提升.全向人工噪声方案虽然对D不造成干扰,但由于R和 J_k 能够收集的能量随发射功率增加而增加,故D和E处的信噪比都随之增大,因此,系统的保密速率将逐渐收敛.而基于迫零预编码的方案之所以要优于全向人工噪声方案,是因为迫零预编码方案通过利用窃听信道CSI,进行了相应设计,因此,保密性能更好,这表明CSI对系统保密传输意义重大.但总体来看,所提方案保密性能更好,具备一定的抗窃听攻击的能力.

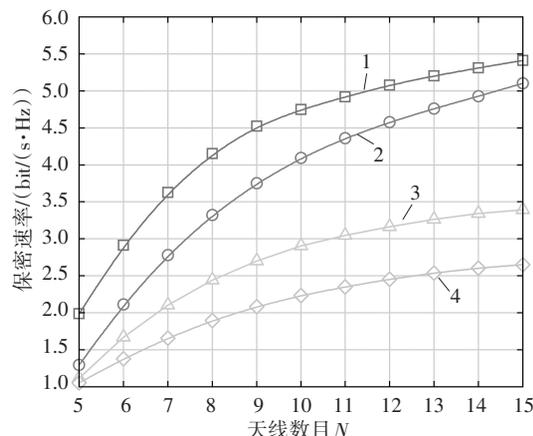


1-本文所提方案;2-基于迫零预编码次优传输方案;3-全向人工噪声方案;4-最优安全波束成形传输方案

图4 系统保密速率随基站S发射功率的变化图

Fig.4 System secrecy rate achieved by different schemes versus emission power P_s

图5为不同安全传输方案下,系统保密速率随中继节点配备天线数目N的变化情况.



1-本文所提方案;2-基于迫零预编码次优传输方案;3-全向人工噪声方案;4-最优安全波束成形传输方案

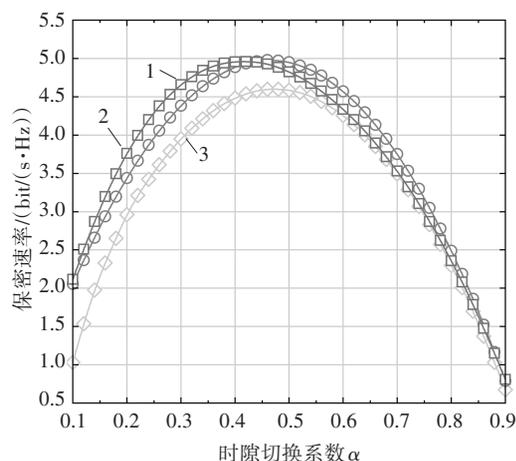
图5 系统保密速率随中继节点配备天线数目N变化图

Fig.5 System secrecy rate achieved by different schemes versus the number of antenna N

从图5可以看出,随着天线数目 N 逐渐增加,4种安全传输方案的保密速率均得到提升.当 N 为15时,本文所提方案相较于其他3种方案对应的保密速率要分别高出约 $0.3079 \text{ bit}/(\text{s}\cdot\text{Hz})$ 、 $2.0158 \text{ bit}/(\text{s}\cdot\text{Hz})$ 和 $2.7585 \text{ bit}/(\text{s}\cdot\text{Hz})$.这是因为,当天线数目较多时,在上述几种方案中, R 和 J_k 都具备足够的空间自由度,能够根据窃听者的CSI,更加有针对性地设计波束成形向量和AN协方差矩阵进行安全传输.同时,大规模阵列天线也更有利于中继节点收集能量,使得能量采集节点的传输功率增大,进一步增强了系统保密性能.另外,当 N 不断增大后,所提方案与基于迫零预编码次优传输方案的系统保密速率差距逐渐缩小.这是因为,随着 N 的增加,本文提到的两种方案的最优解空间逐渐趋于相同,因此,在发射功率不变时,天线数目的增加会提供更多的自由度用于安全传输设计,以提升系统保密性能.

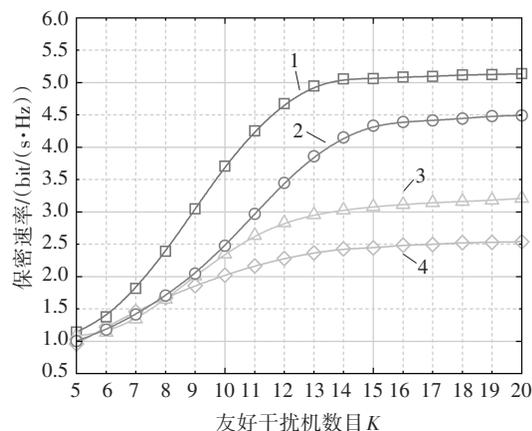
图6为在本文所提传输方案下,系统保密速率随时隙切换系数 α 的变化情况.从图6可以看出,对应方案在不同参数下能够达到的最大保密速率分别约为 $4.9780 \text{ bit}/(\text{s}\cdot\text{Hz})$ 、 $4.9692 \text{ bit}/(\text{s}\cdot\text{Hz})$ 和 $4.6002 \text{ bit}/(\text{s}\cdot\text{Hz})$.本文所提方案和基于迫零预编码次优传输方案对应的系统保密速率均随着 α 的增大,呈现先增大后减小的变化趋势.这是因为,在取得最优 α 时,系统将能够采集到足够的能量,分别用于AN和保密信号的传输.并且,从保密信号的传输角度来看,此时,系统的合法信道容量达到最大,能量的利用效率最高.因此,最优 α 能够实现能量采集与保密信号传输的平衡,有助于增强系统保密性能.另外,可以发现,对于两种方案来说,相较于基于迫零预编码次优传输方案,本文所提方案的保密性能优势在整个 α 的变化过程中十分明显.能量转化效率的提升有助于对能量采集过程因发射功率的不足进行补偿,但随着 α 的增大,两种方案的保密速率趋于一致.这是因为在该阶段中,两种方案中的中继传输保密信号吞吐量较小,故保密速率相差不大,AN对系统的影响变得有限.所以,当 α 较大时,采用基于迫零预编码次优传输方案来完成信号的传输,既能够做到降低系统复杂度,又能够使系统达到不错的保密性能.

图7为在本文所提安全传输方案下,系统保密速率随友好干扰机数目 K 的变化情况.从图7可以看出,两种方案的保密速率均随着 K 的增加而增大,但曲线将趋于平缓.这是因为,友好干扰机对D以及E均有影响,当达到一定数目后,D和E处的SINR都将收敛到一个阈值,故系统保密速率的变化率逐渐减小.虽然基于迫零预编码次优传输方案对D不产



1-本文所提方案, $P_s = 30 \text{ dBm}$, $\eta = 0.8$; 2-本文所提方案, $P_s = 35 \text{ dBm}$; 3-基于迫零预编码次优传输方案, $P_s = 35 \text{ dBm}$

图6 系统保密速率随时隙切换系数 α 变化图
Fig.6 System secrecy rate achieved by different schemes versus time switching coefficient α



1-本文所提方案, $N=6$; 2-本文所提方案, $N=3$; 3-基于迫零预编码次优传输方案, $N=6$; 4-基于迫零预编码次优传输方案, $N=3$

图7 系统保密速率随友好干扰机数目 K 变化图
Fig.7 System secrecy rate achieved by proposed schemes versus the numbers of friendly jammer K

生影响,但随着 K 数目的增多,射频信号的能量利用效率将降低,AN的干扰效果将减弱,因此,基于迫零预编码次优传输方案对提高保密速率不再显著.另外,在 N 从3增加到6时,当 K 为12时,本文所提方案对系统保密速率的提高约为 $1.2225 \text{ bit}/(\text{s}\cdot\text{Hz})$,基于迫零预编码的方案对保密速率的提升约为 $0.5516 \text{ bit}/(\text{s}\cdot\text{Hz})$,所以,本文所提方案对硬件设备的利用效率更高.因此,为提升系统保密速率,既可以通过增加天线的策略;若受制于硬件天线时,也可利用空闲中继节点临时充当友好干扰机来增强系统保密性能.

5 结论

本文研究能量受限的基于AF模式的多天线中继通信网络中,面临窃听攻击所存在的保密传输问题.借助外部的友好干扰机,提出了一种AN辅助的保密波束成形设计方案.基于能量采集技术,中继节点和友好干扰机利用射频信号采集能量,在采集能量的约束下,联合优化波束成形矩阵、AN协方差矩阵和时隙切换系数,从而最大化系统保密速率.采用双层优化方法和半定松弛技术求解非凸优化问题,并证明了形成的松弛问题总是存在秩-1的最优解.与传统的迫零波束成形方案相比,仿真结果和性能分析表明,所提方案具有明显的性能优势.

参考文献

- [1] 任品毅,唐晓.面向5G的物理层安全技术综述[J].北京邮电大学学报,2018,41(5):69-77.
REN P Y, TANG X. A review on physical layer security techniques for 5G[J]. Journal of Beijing University of Posts and Telecommunications, 2018, 41(5):69-77. (In Chinese)
- [2] VAISHNAVI K N, KHORVI S D, KISHORE R, *et al.* A survey on jamming techniques in physical layer security and anti-jamming strategies for 6G[C]//2021 28th International Conference on Telecommunications (ICT). London: IEEE, 2021:174-179.
- [3] KRIKIDIS I. Opportunistic relay selection for cooperative networks with secrecy constraints[J]. IET Communications, 2010, 4(15):1787.
- [4] 江虹,辜馨月,杨浩.全双工多中继网络的中断分析与中继决策[J].湖南大学学报(自然科学版),2021,48(6):67-73.
JIANG H, GU X Y, YANG H. Outage analysis and relay selection in full duplex multi-relay networks[J]. Journal of Hunan University (Natural Sciences), 2021, 48(6):67-73. (In Chinese)
- [5] HUANG P M, HAO Y Q, LV T, *et al.* Secure beamforming design in relay-assisted Internet of Things[J]. IEEE Internet of Things Journal, 2019, 6(4):6453-6464.
- [6] YANG L, CHEN J, JIANG H, *et al.* Optimal relay selection for secure cooperative communications with an adaptive eavesdropper[J]. IEEE Transactions on Wireless Communications, 2017, 16(1):26-42.
- [7] JAMEEL F, WYNE S, KADDOUM G, *et al.* A comprehensive survey on cooperative relaying and jamming strategies for physical layer security[J]. IEEE Communications Surveys & Tutorials, 2019, 21(3):2734-2771.
- [8] ATAPATTU S, ROSS N, JING Y D, *et al.* Source-based jamming for physical-layer security on untrusted full-duplex relay[J]. IEEE Communications Letters, 2019, 23(5):842-846.
- [9] 李元健,赵睿,谭星,等.全双工目的端加扰安全传输系统中的天线模式切换[J].信号处理,2018,34(4):457-464.
LI Y J, ZHAO R, TAN X, *et al.* Antenna mode switching for full-duplex at a destination of a jamming secure transmission system[J]. Journal of Signal Processing, 2018, 34(4):457-464. (In Chinese)
- [10] MOBINI Z. Secrecy performance of non-orthogonal multiple access cognitive untrusted relaying with friendly jamming[J]. AEU - International Journal of Electronics and Communications, 2020, 118:153-156.
- [11] BOZORGI S F, AKHLAGHI S. Secrecy sum rate maximisation in multi-antenna two-way relay networks[J]. IET Communications, 2020, 14(4):541-548.
- [12] HU Z T, JIN Y, LIU H J. A stochastic beamforming algorithm for wireless sensor network with multiple relays and multiple eavesdroppers[J]. Wireless Personal Communications, 2021, 116(3):2035-2048.
- [13] SHARIFI F, AKHLAGHI S. Maximizing the minimum secrecy rate of two-way relay networks[J]. Computer Communications, 2021, 178:259-270.
- [14] 张立健,金梁,刘璐,等.多天线中继系统中人工噪声辅助的安全波束成形[J].通信学报,2014,35(11):81-88.
ZHANG L J, JIN L, LIU L, *et al.* Artificial noise aided secure beamforming for multi-antenna relay systems[J]. Journal on Communications, 2014, 35(11):81-88. (In Chinese)
- [15] LI Q Z, YANG L. Beamforming for cooperative secure transmission in cognitive two-way relay networks[J]. IEEE Transactions on Information Forensics and Security, 2020, 15:130-143.
- [16] OBEED M, MESBAH W. Efficient algorithms for physical layer security in one-way relay systems[J]. Wireless Networks, 2019, 25(3):1327-1339.
- [17] ZHAO S R, LIU J, SHEN Y L, *et al.* Secure and energy-efficient precoding for MIMO two-way untrusted relay systems[J]. IEEE Transactions on Information Forensics and Security, 2021, 16:3371-3386.
- [18] WYNER A D. The wire-tap channel[J]. Bell System Technical Journal, 1975, 54(8):1355-1387.
- [19] 方冰,韩冰. MISO无线携能通信系统保密波束成形方法[J].系统工程与电子技术,2021,43(6):1692-1698.
FANG B, HAN B. Secure beamforming method for the MISO SWIPT system[J]. Systems Engineering and Electronics, 2021, 43(6):1692-1698. (In Chinese)
- [20] CHEN H H, GERSHMAN A B, SHAHBAZPANAHI S. Filter-and-forward distributed beamforming in relay networks with frequency selective fading[J]. IEEE Transactions on Signal Processing, 2010, 58(3):1251-1262.
- [21] 冯立,邝育军,代泽洋,等.异构认知网中基于能效的协作技术研究[J].电子科技大学学报,2017,46(5):666-672.
FENG L, KUANG Y J, DAI Z Y, *et al.* Network cooperation for energy-efficient communication in multi-RAT heterogeneous cognitive radio networks[J]. Journal of University of Electronic Science and Technology of China, 2017, 46(5):666-672. (In Chinese)
- [22] HUANG Y W, PALOMAR D P. Rank-constrained separable semi-definite programming with applications to optimal beamforming[J]. IEEE Transactions on Signal Processing, 2010, 58(2):664-678.
- [23] 叶夏,朱丰超,高飞飞.一种全双工物理层安全通信波束成形的低功耗方法[J].西安交通大学学报,2015,49(8):31-37.
YE X, ZHU F C, GAO F F. A beam forming method for secure communications of full duplex physical layer[J]. Journal of Xi'an Jiaotong University, 2015, 49(8):31-37. (In Chinese)
- [24] 赵睿,谭星,李元健,等.全双工加扰的非可信中继系统的渐近性能分析[J].通信学报,2018,39(9):20-30.
ZHAO R, TAN X, LI Y J, *et al.* Asymptotic performance analysis of untrusted relay system with full-duplex jamming destination[J]. Journal on Communications, 2018, 39(9):20-30. (In Chinese)