doi:10.3969/j.issn.1003-3114.2025.05.004
引用格式:王毅,杨少川,赵飞,等.硬件损伤情况下 IRS 辅助密钥生成系统鲁棒波束赋形设计[J].无线电通信技术,2025,51(5):911-918.[WANG Yi, YANG Shaochuan, ZHAO Fei, et al. Joint Robust Beamforming Design for IRS-assisted Physical Layer Key Generation Under Hardware Impairments[J]. Radio Communications Technology, 2025, 51(5): 911-918.]

硬件损伤情况下 IRS 辅助密钥生成系统鲁棒波束赋形设计

王　毅[1,2,3],杨少川[1,2,3*],赵　飞[1,2,3],冀保峰[4],楚　征[5],李春国[6]
(1.郑州航空工业管理学院 电子信息学院,河南 郑州 450046;
2.河南省通用航空技术重点实验室,河南 郑州 450046;
3.航空航天电子信息技术河南省协同创新中心,河南 郑州 450046;
4.河南科技大学 信息工程学院,河南 洛阳 471023;
5.宁波诺丁汉大学 电器与电子工程学院,浙江 宁波 315100;
6.东南大学 信息科学与工程学院,江苏 南京 210096)

摘　要:研究了存在残余收发信机硬件损伤(Transceiver Hardware Impairments,THI)情况下的智能反射面(Intelligent Reflecting Surface,IRS)辅助的物理层密钥生成(Physical-layer Key Generation,PKG)系统,推导了密钥生成速率(Key Generation Rate,KGR)的闭合表达式,并在基站发射功率约束和 IRS 相位偏移单位模约束下,构建了 KGR 最大化问题。为求解该问题,提出了一种鲁棒优化算法,该算法结合了交替优化(Alternating Optimization,AO)、逐次凸逼近(Successive Convex Approximation,SCA)、半定松弛(Semi-Definite Relaxation,SDR)和惩罚方法,迭代优化发射波束成形和 IRS 相移。仿真结果表明,所提鲁棒算法能够有效对抗硬件损伤、提升 KGR。

关键词:硬件损伤;密钥生成;智能反射面;交替优化

中图分类号:TN919.23　　**文献标志码**:A　　**开放科学(资源服务)标识码(OSID)**:

文章编号:1003-3114(2025)05-0911-08

Joint Robust Beamforming Design for IRS-assisted Physical Layer Key Generation Under Hardware Impairments

WANG Yi[1,2,3], YANG Shaochuan[1,2,3*], ZHAO Fei[1,2,3], JI Baofeng[4], CHU Zheng[5], LI Chunguo[6]
(1. School of Electronics and Information, Zhengzhou University of Aeronautics, Zhengzhou 450046, China;
2. Henan Key Laboratory of General Aviation Technology, Zhengzhou 450046 China;
3. Collaborative Innovation Center of Aeronautics and Astronautics Electronic Information Technology Zhengzhou 450046, China;
4. College of Information Engineering, Henan University of Science and Technology, Luoyang 471023, China;
5. Department of Electrical and Electronic Engineering, University of Nottingham Ningbo China, Ningbo 315100, China;
6. School of Information Science and Engineering, Southeast University, Nanjing 210096, China)

Abstract: This paper investigates an Intelligent Reflecting Surface (IRS)-assisted Physical-layer Key Generation (PKG) system under residual Transceiver Hardware Impairments(THI). A closed-form expression for the Key Generation Rate(KGR) is derived, and

收稿日期:2025-04-27

基金项目:河南省自然科学基金(252300421516);河南省科技研发计划联合基金重点项目(225200810033);郑州航空工业管理学院科研团队支持计划专项(23ZHTD01005);郑州航空工业管理学院教育教学改革研究与实践项目(zhjy24-09);郑州航空工业管理学院研究生教育改革与发展研究项目(2025YJSJG31);河南省高等学校重点科研项目(26A510017);宁波市自然科学基金(2024J233);河南省杰出外籍科学家工作室(GZS2022011)

Foundation Item:Henan Natural Science Foundation (252300421516);Key Project of the Joint Fund of Henan Province Science and Technology R&D Program (225200810033);Research Team Support Program of Zhengzhou University of Aeronautics (23ZHTD01005);Teaching Reform and Practice Project of Zhengzhou University of Aeronautics (zhjy24-09);Graduate Education Reform and Development Project of Zhengzhou University of Aeronautics (2025YJSJG31);Scientific Research Foundation of the Higher Education Institutions of Henan Province (26A510017);Ningbo Natural Science Foundation (2024J233);Henan Distinguished Foreign Scientist Studio (GZS2022011)

a KGR maximization problem is formulated under the base station transmit power constraint and the unit-modulus constraint on the IRS phase shifts. To solve this problem, a robust optimization algorithm is proposed, which integrates Alternating Optimization(AO), Successive Convex Approximation (SCA), Semi-Definite Relaxation(SDR), and penalty methods to iteratively optimize the transmit beamforming and IRS phase shifts. Numerical simulation results demonstrate that the proposed robust algorithm can effectively mitigate the impact of hardware impairments and improve the KGR.

Keywords: hardware impairments; key generation; IRS; AO

0 引言

现今,无线通信网络已成为人们日常生活密不可分的重要组成部分,其安全问题也受到广泛关注。由于无线信道的开放特性,通信系统极易遭受各种攻击,因此无线空口安全作为保障无线通信系统安全性的关键环节之一,具有重要的研究意义[1]。尤其值得注意的是,未来 6G 网络将提供全域覆盖、高密度连接、低时延高可靠通信等服务,展现出“泛在链接、多域融合”的特征,而现有的高层加密方案普遍存在计算复杂度高、密钥管理繁琐等问题[2]。作为一种轻量级加密技术, PKG 利用无线信道固有的随机性与互易性等特性,在合法用户之间建立对称密钥,可以作为上层加密机制的有效补充[3]。PKG 无需进行传统的密钥分发与管理,且借助无线信道的空间多样性,只要窃听者位置与合法用户间距超过半个波长,就无法窃取与密钥相关的任何信息[4]。此外,PKG 具有实时更新、动态变化的特点,有望实现“一次一密”的完美加密机制,从而有效抵御量子计算技术所带来的安全挑战。

为了实现“一次一密”的安全通信愿景,KGR 必须与通信速率相匹配。然而,KGR 受限于无线信道的时变性,特别是在传感器网络、智能家居网络等准静态环境中,由于无线信道在较长时间内保持相对稳定,连续生成的密钥之间存在较强相关性,导致 KGR 降低并引发安全性问题。值得庆幸的是,IRS 为提升密钥生成性能提供了全新的解决思路。IRS 由大量近乎无源的反射单元构成,每个单元能够独立调整反射信号的幅度、相位及极化方向等参数,同时具备低成本、易部署、兼容性强等优势,在无线携能通信、隐蔽通信和通感一体化等通信场景中有非常广泛的应用[5-8]。通过随机改变 IRS 单元的相位偏移,可以有效增加复合信道的熵值,从而提升 KGR[9]。进一步,通过对 IRS 单元的优化设计,不仅可以增强合法通信双方信道观测值的相关性、减少信息泄露,还能显著提升密钥生成性能。现有研究针对不同应用场景提出了多种 IRS 辅助密钥生成的方法,文献[10]通过调整 IRS 单元开关状态提升 KGR,推导了 IRS 辅助下的 KGR 表达式,并通过仿真验证了所提鲁棒算法相较于随机切换策略具有更优的性能表现。文献[11]面向多用户单输入单输出(Single Input Single Output, SISO)网络,结合 SCA 与 SDR 技术,提出了一种 IRS 相位偏移优化方法。文献[12]进一步扩展至多输入单输出(Multiple Input Single Output, MISO)系统,分析了 IRS 单元间空间相关性对密钥生成性能的不利影响。文献[13]则研究了 IRS 辅助下的多小区 PKG 系统,分别采用拉格朗日对偶方法与投影梯度上升算法,联合优化基站波束赋形矩阵与 IRS 相位偏移,以最大化加权和密钥速率。

在实际通信系统中,由于相位噪声、I/Q 失衡、频率偏移及功放非线性增益等因素引起的 THI 将对通信性能产生严重影响[14]。尽管硬件校准技术在一定程度上能够削弱硬件损伤带来的影响,但仍存在残余噪声。而且此类噪声的功率与有用信号功率成正比,无法通过简单地提高发射功率来抵消。文献[15]首次分析了 THI 对 PKG 系统性能的影响,推导出了 THI 条件下 SISO 系统的 KGR 闭合表达式,揭示了硬件损伤噪声会导致 KGR 下降的现象。文献[16]则研究了 IRS 辅助 MISO 密钥生成系统在硬件损伤条件下的性能,提出了一种鲁棒波束赋形算法,通过联合优化基站波束赋形向量与 IRS 相位偏移向量以提升 KGR;但其假设硬件损伤噪声在所有天线上均匀分布,该假设较为理想化,未能充分反映实际硬件环境中硬件损伤噪声功率与天线发射/接收功率成正比的特性。

针对上述问题,本文引入了更加贴近实际的硬件损伤建模方法,假设硬件损伤噪声功率与各天线发射/接收功率成正比,在此基础上设计了更为精细的鲁棒波束赋形算法,以进一步提升硬件损伤条件下的 KGR。

本文的主要贡献如下:① 推导了在 THI 条件下 IRS 辅助 PKG 系统的 KGR 闭式表达式,并在此基础上提出了在基站发射功率和 IRS 单位模相位偏移约束下的 KGR 最大化问题。② 提出了一种 AO 算法,通过结合 SCA、SDR 和惩罚方法,迭代优化发射

波束成形和 IRS 相位偏移,解决了高度耦合的非凸优化问题。③ 通过仿真验证了所提波束成形方案的优越性,结果表明该方案在硬件损伤条件下比传统的非鲁棒方案更具鲁棒性,同时揭示了 IRS 在提高 KGR 方面的优势以及硬件损伤对 KGR 的影响。

本文的研究为 IRS 辅助的 PKG 系统在硬件损伤条件下的实际应用提供了理论支持和算法指导,为未来无线通信系统的安全性设计提供了新的思路。

1 系统模型

IRS 辅助的密钥生成系统如图 1 所示,该系统包含一个基站、一个 IRS、一个合法用户 Bob 和一个窃听者 Eve。基站和 IRS 分别装配 N 个天线和 M 个反射单元,Bob 和 Eve 均为单天线节点。为了保证上下行信道的互易性,假设基站和 Bob 之间在时分双工(Time Division Duplexing,TDD)模式下利用无线信道生成密钥。一个智能控制器被用于协调基站的波束赋形和 IRS 的相移以提高 KGR。基站与 IRS、基站与 Bob/Eve、IRS 与 Bob/Eve 间的基带等效信道因子分别表示为:$\boldsymbol{F}\in\mathbb{C}^{N\times M}$;$\boldsymbol{h}_{\mathrm{d}}\in\mathbb{C}^{N\times 1}$、$\boldsymbol{g}_{\mathrm{d}}\in\mathbb{C}^{N\times 1}$;$\boldsymbol{h}_{\mathrm{r}}\in\mathbb{C}^{M\times 1}$、$\boldsymbol{g}_{\mathrm{r}}\in\mathbb{C}^{M\times 1}$。

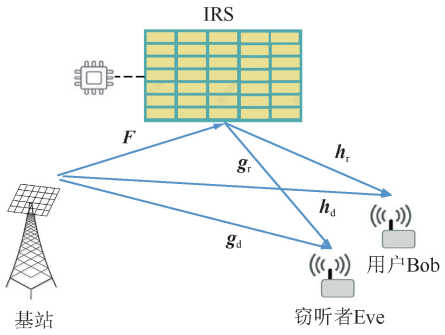

图 1 硬件损伤情况下 IRS 辅助的密钥生成系统

Fig. 1 IRS-assisted key generation system under hardware impairments

1.1 密钥生成流程

本文涉及的 IRS 辅助密钥生成方案包含以下 3 个步骤:

① 参数配置:Bob 发送信道探测信号,基站估计信道的统计信道状态信息并利用后文提出的鲁棒算法设计基站的发送波束赋形向量和 IRS 的相移向量。

② 信道探测:基站和 Bob 互发公开导频并进行信道估计。假设合法通信双方存在硬件损伤。为了分析方便,将基站和 Bob 的发送天线与接收天线的残余硬件损伤程度分别用 $1-\eta_v^{\mathrm{t}}$ 和 $1-\eta_v^{\mathrm{r}}$ 表示。其中,$v\in\{a,b\}$,角标 a 和 b 分别表示基站和 Bob。基站先发送下行导频,则 Bob 和 Eve 的接收信号分别为[17]:

$$y_b=\sqrt{\eta_b^{\mathrm{r}}}(\boldsymbol{h}_{\mathrm{d}}^{\mathrm{H}}+\boldsymbol{h}_{\mathrm{r}}^{\mathrm{H}}\boldsymbol{\Theta}^{\mathrm{H}}\boldsymbol{F}^{\mathrm{H}})(\sqrt{\eta_a^{\mathrm{t}}}\boldsymbol{w}s_a+\boldsymbol{\xi}_a^{\mathrm{t}})+\boldsymbol{\xi}_b^{\mathrm{r}}+n_b,\tag{1}$$

$$y_e=(\boldsymbol{g}_{\mathrm{d}}^{\mathrm{H}}+\boldsymbol{g}_{\mathrm{r}}^{\mathrm{H}}\boldsymbol{\Theta}^{\mathrm{H}}\boldsymbol{F}^{\mathrm{H}})\left(\sqrt{\eta_a^{\mathrm{t}}}\boldsymbol{w}s_a+\boldsymbol{\xi}_a^{\mathrm{t}}\right)+n_e,\tag{2}$$

式中:$\boldsymbol{\Theta}=\mathrm{diag}(\mathrm{e}^{\mathrm{j}\varphi_1},\mathrm{e}^{\mathrm{j}\varphi_2},\cdots,\mathrm{e}^{\mathrm{j}\varphi_m},\cdots,\mathrm{e}^{\mathrm{j}\varphi_M})$,$\varphi_m\in[0,2\pi)$,$\forall m$ 表示 IRS 的相移矩阵,$\boldsymbol{w}\in\mathbb{C}^{N\times 1}$ 和 $s_a\in\mathbb{C}$($|s_a|^2=1$)分别表示发送波束赋形向量和基站发送的导频信号,$\boldsymbol{\xi}_b^{\mathrm{r}}\in\mathbb{C}$ 和 $\boldsymbol{\xi}_a^{\mathrm{t}}\in\mathbb{C}^{N\times 1}$ 分别表示由 Bob 的接收机和基站发射机的残余硬件损伤产生的干扰噪声。根据文献[18],$\boldsymbol{\xi}_b^{\mathrm{r}}$ 和 $\boldsymbol{\xi}_a^{\mathrm{t}}$ 表示方差与有用信号功率成正比的 0 均值复高斯随机向量,即 $\boldsymbol{\xi}_b^{\mathrm{r}}\sim\mathcal{CN}(0,(1-\eta_b^{\mathrm{r}})|\boldsymbol{h}_{\mathrm{d}}^{\mathrm{H}}\boldsymbol{w}+\boldsymbol{h}_{\mathrm{r}}^{\mathrm{H}}\boldsymbol{\Theta}^{\mathrm{H}}\boldsymbol{F}^{\mathrm{H}}\boldsymbol{w}|^2)$,$\boldsymbol{\xi}_a^{\mathrm{t}}\sim\mathcal{CN}(0,(1-\eta_a^{\mathrm{t}})\widetilde{\mathrm{diag}}(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}))$,其中 $\widetilde{\mathrm{diag}}\{\boldsymbol{A}\}$ 表示以矩阵 $\boldsymbol{A}$ 的对角元素构成的对角矩阵。$n_v\in\mathbb{C}$ 表示 Bob 和 Eve 端的高斯白噪声(Adaptive White Gaussian Noise,AWGN),即 $n_v\sim\mathcal{CN}(0,\sigma_v^2)$,$v\in\{b,e\}$。Bob 和 Eve 利用最小二乘(Least Square,LS)法对复合信道进行估计,获得信道估计值 h_b 和 h_e:

$$h_b\triangleq\sqrt{\eta_b^{\mathrm{r}}}(\boldsymbol{h}_{\mathrm{d}}^{\mathrm{H}}+\boldsymbol{h}_{\mathrm{r}}^{\mathrm{H}}\boldsymbol{\Theta}^{\mathrm{H}}\boldsymbol{F}^{\mathrm{H}})(\sqrt{\eta_a^{\mathrm{t}}}\boldsymbol{w}+\boldsymbol{\xi}_a^{\mathrm{t}}conj(s_a))+\boldsymbol{\xi}_b^{\mathrm{r}}conj(s_a)+z_b,\tag{3}$$

$$h_e\triangleq(\boldsymbol{g}_{\mathrm{d}}^{\mathrm{H}}+\boldsymbol{g}_{\mathrm{r}}^{\mathrm{H}}\boldsymbol{\Theta}^{\mathrm{H}}\boldsymbol{F}^{\mathrm{H}})(\sqrt{\eta_a^{\mathrm{t}}}\boldsymbol{w}+\boldsymbol{\xi}_a^{\mathrm{t}}conj(s_a))+z_e,\tag{4}$$

式中:$z_v=n_v conj(s_a)$,$v\in\{b,e\}$。随后 Bob 发送上行导频,基站的接收信号为:

$$y_a=\sqrt{\eta_a^{\mathrm{r}}}(\boldsymbol{h}_{\mathrm{d}}+\boldsymbol{F}\boldsymbol{\Theta}\boldsymbol{h}_{\mathrm{r}})(\sqrt{\eta_b^{\mathrm{t}}}s_b+\boldsymbol{\xi}_b^{\mathrm{t}})+\boldsymbol{\xi}_a^{\mathrm{r}}+\boldsymbol{n}_a,\tag{5}$$

式中:$s_b\in\mathbb{C}$,$|s_b|^2=1$ 表示 Bob 发送的公开导频。同样地,假设 $\boldsymbol{\xi}_b^{\mathrm{t}}\sim\mathcal{CN}(0,(1-\eta_b^{\mathrm{t}}))$,$\boldsymbol{\xi}_a^{\mathrm{r}}\sim\mathcal{CN}(0,(1-\eta_a^{\mathrm{r}})\widetilde{\mathrm{diag}}(\boldsymbol{h}_{\mathrm{d}}+\boldsymbol{F}\boldsymbol{\Theta}\boldsymbol{h}_{\mathrm{r}}))$。$\boldsymbol{n}_a\in\mathbb{C}^{N\times 1}$ 为基站的接收噪声,且 $\boldsymbol{n}_a\sim\mathcal{CN}(0,\sigma_a^2\boldsymbol{I}_N)$。经过 LS 信道估计后,基站获得复合信道的估计值 $\boldsymbol{h}_a$:

$$\boldsymbol{h}_a\triangleq\sqrt{\eta_a^{\mathrm{r}}}(\boldsymbol{h}_{\mathrm{d}}+\boldsymbol{F}\boldsymbol{\Theta}\boldsymbol{h}_r)(\sqrt{\eta_b^{\mathrm{t}}}+\boldsymbol{\xi}_b^{\mathrm{t}}conj(s_b))+\boldsymbol{\xi}_a^{\mathrm{r}}conj(s_b)+\boldsymbol{n}_a conj(s_b)。\tag{6}$$

为了得到共享随机源,基站需要将 $\boldsymbol{h}_a$ 和 $\boldsymbol{w}^{\mathrm{H}}$ 相乘得到 $\hat{h}_a$:

$$\hat{h}_a=\sqrt{\eta_a^{\mathrm{r}}}(\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{d}}+\boldsymbol{w}^{\mathrm{H}}\boldsymbol{F}\boldsymbol{\Theta}\boldsymbol{h}_{\mathrm{r}})(\sqrt{\eta_b^{\mathrm{t}}}+\boldsymbol{\xi}_b^{\mathrm{t}}conj(s_b))+\boldsymbol{w}^{\mathrm{H}}\boldsymbol{\xi}_a^{\mathrm{r}}conj(s_b)+z_a,\tag{7}$$

式中:$z_a=\boldsymbol{w}^{\mathrm{H}}\boldsymbol{n}_a conj(s_b)$。为了分析方便,假设收发双方的噪声方差相等,即 $\sigma_{z_a}^2=\sigma_{z_b}^2=\sigma^2$。基站和 Bob 获得的复合信道特征信息 $\hat{h}_a$ 和 $\hat{h}_b$ 中含有共享

随机项、残余硬件损伤噪声和 AWGN,因此 $\hat{h}_a$ 和 $\hat{h}_b$ 可以当作共享随机源提取密钥。

③ 密钥生成:在信道探测之后,基站和 Bob 首先将收集到的信道特征信息 h_a 和 h_b 量化为原始比特序列;再通过信息协商来消除不一致的比特;最后,基站和 Bob 利用隐私放大技术降低信息协商过程中的信息泄露,并提高密钥的随机性。由于这一步骤与现有的密钥生成方案类似[4,11,13],因此本文只关注前 2 个步骤。

1.2 KGR 闭合表达式

本文推导硬件损伤存在时 KGR 的闭合表达式,首先,定义 $\hat{h} \triangleq \boldsymbol{w}^{\mathrm{H}}\boldsymbol{h} = \boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_d + \boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}\boldsymbol{\theta}$,其中 $\boldsymbol{H} = \boldsymbol{F}\mathrm{diag}(\boldsymbol{h}_{\mathrm{r}})$,$\boldsymbol{\theta} = [\mathrm{e}^{\mathrm{j}\varphi_1}, \mathrm{e}^{\mathrm{j}\varphi_2}, \cdots, \mathrm{e}^{\mathrm{j}\varphi_M}]^{\mathrm{T}}$。则 $\hat{h}_a$ 和 $\hat{h}_b$ 可以分别改写为:

$$\hat{h}_a = \sqrt{\eta_a^{\mathrm{r}}\eta_b^{\mathrm{t}}}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h} + \sqrt{\eta_a^{\mathrm{r}}}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}\boldsymbol{\xi}_b^{\mathrm{t}}conj(s_b) + \boldsymbol{w}^{\mathrm{H}}\boldsymbol{\xi}_a^{\mathrm{r}}conj(s_b) + z_a, \tag{8}$$

$$\hat{h}_b = \sqrt{\eta_b^{\mathrm{r}}\eta_a^{\mathrm{t}}}\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w} + \sqrt{\eta_b^{\mathrm{r}}}\boldsymbol{h}^{\mathrm{H}}\boldsymbol{\xi}_a^{\mathrm{t}}conj(s_a) + \boldsymbol{\xi}_b^{\mathrm{r}}conj(s_a) + z_b。 \tag{9}$$

然后,推导出 $\hat{h}$ 的协方差矩阵 $\boldsymbol{R}_{\hat{h}} \triangleq \mathbb{E}\{\hat{h}conj(\hat{h})\}$ 为:

$$\begin{aligned} R_{\hat{h}} &= \mathbb{E}\{(\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{d}} + \boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}\boldsymbol{\theta})conj(\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{d}} + \boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}\boldsymbol{\theta})\} = \\ &\boldsymbol{w}^{\mathrm{H}}\mathbb{E}\{\boldsymbol{h}_{\mathrm{d}}\boldsymbol{h}_{\mathrm{d}}^{\mathrm{H}}\}\boldsymbol{w} + \boldsymbol{w}^{\mathrm{H}}\mathbb{E}\{\boldsymbol{H}\boldsymbol{\theta}\boldsymbol{\theta}^{\mathrm{H}}\boldsymbol{H}^{\mathrm{H}}\}\boldsymbol{w} \overset{(a)}{=} \\ &\boldsymbol{w}^{\mathrm{H}}[\mathbb{E}\{\boldsymbol{h}_{\mathrm{d}}\boldsymbol{h}_{\mathrm{d}}^{\mathrm{H}}\} + (\boldsymbol{\theta}^{\mathrm{T}} \otimes \boldsymbol{I}_N)\mathbb{E}\{vec(\boldsymbol{H})(vec(\boldsymbol{H}))^{\mathrm{H}}\} \cdot \\ &(conj(\boldsymbol{\theta}) \otimes \boldsymbol{I}_N)]\boldsymbol{w} \triangleq \boldsymbol{w}^{\mathrm{H}}\boldsymbol{E}\boldsymbol{w}, \end{aligned} \tag{10}$$

式中:$\boldsymbol{E} = \mathbb{E}\{\boldsymbol{h}_{\mathrm{d}}\boldsymbol{h}_{\mathrm{d}}^{\mathrm{H}}\} + (\boldsymbol{\theta}^{\mathrm{T}} \otimes \boldsymbol{I}_N)\mathbb{E}\{vec(\boldsymbol{H}) \cdot (vec(\boldsymbol{H}))^{\mathrm{H}}\}(conj(\boldsymbol{\theta}) \otimes \boldsymbol{I}_N)$,等式(a)用到了式 $vec(\boldsymbol{A}\boldsymbol{C}) = (\boldsymbol{C}^{\mathrm{T}} \otimes \boldsymbol{I})vec(\boldsymbol{A})$。考虑到不同设备残留硬件损伤产生的干扰噪声相互独立,可以推导出信道协方差如下:

$$\mathbb{E}\{\hat{h}_v conj(\hat{h}_v)\} = \boldsymbol{w}^{\mathrm{H}}\boldsymbol{E}_v\boldsymbol{w} + \sigma^2 \triangleq R_{\hat{h}_v}, v \in \{a,b\}, \tag{11}$$

$$\mathbb{E}\{\hat{h}_a conj(\hat{h}_b)\} = \mathbb{E}\{\hat{h}_b conj(\hat{h}_a)\} = \sqrt{\eta_a^{\mathrm{t}}\eta_a^{\mathrm{r}}\eta_b^{\mathrm{t}}\eta_b^{\mathrm{r}}}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{E}\boldsymbol{w}。 \tag{12}$$

其中:

$$\boldsymbol{E}_a = \eta_a^{\mathrm{r}}\boldsymbol{E} + (1-\eta_a^{\mathrm{r}})\widetilde{\mathrm{diag}}(\boldsymbol{E}), \tag{13}$$

$$\boldsymbol{E}_b = \eta_b^{\mathrm{r}}\eta_a^{\mathrm{t}}\boldsymbol{E} + \eta_b^{\mathrm{r}}(1-\eta_a^{t})\widetilde{\mathrm{diag}}(\boldsymbol{E}) + (1-\eta_b^{\mathrm{r}})\boldsymbol{E}。 \tag{14}$$

根据文献[12],KGR 为基站与 Bob 提取的信道特征信息 $\hat{h}_a$ 和 $\hat{h}_b$ 在 $\hat{h}_e$ 下的条件互信息:

$$I_s = I(\hat{h}_a;\hat{h}_b \mid \hat{h}_e) \overset{(b)}{=} I(\hat{h}_a;\hat{h}_b) = \mathrm{lb}\left(\frac{R_{\hat{h}_a}R_{\hat{h}_b}}{\det(\boldsymbol{R}_{\hat{h}_a\hat{h}_b})}\right), \tag{15}$$

式中:等式(b)成立是由于当 Eve 距离合法通信双方超过半个波长时,窃听信道与合法信道不相关[19]。协方差矩阵 $\boldsymbol{R}_{\hat{h}_a\hat{h}_b}$ 由下式给出:

$$\boldsymbol{R}_{\hat{h}_a\hat{h}_b} = \mathbb{E}\left\{\begin{pmatrix}\hat{h}_a\\ \hat{h}_b\end{pmatrix}(conj(\hat{h}_a) \quad conj(\hat{h}_b))\right\}。 \tag{16}$$

将式(11)和式(12)代入式(16)可以得到 $\det(\boldsymbol{R}_{\hat{h}_a\hat{h}_b})$ 的表达式如下:

$$\begin{aligned} \det(\boldsymbol{R}_{\hat{h}_a\hat{h}_b}) &= \boldsymbol{w}^{\mathrm{H}}\boldsymbol{E}_a\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{E}_b\boldsymbol{w} - \eta_a^{\mathrm{t}}\eta_a^{\mathrm{r}}\eta_b^{\mathrm{t}}\eta_b^{\mathrm{r}}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{E}\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{E}\boldsymbol{w} + \\ &\sigma^2\boldsymbol{w}^{\mathrm{H}}\boldsymbol{E}_c\boldsymbol{w} + \sigma^4, \end{aligned} \tag{17}$$

式中:$\boldsymbol{E}_c = \boldsymbol{E}_a + \boldsymbol{E}_b$。将式(11)代入式(15)可推导出 KGR 的闭合表达式如下:

$$\begin{aligned} I_s = &\sum_{v\in\{a,b\}}\mathrm{lb}(\boldsymbol{w}^{\mathrm{H}}\boldsymbol{E}_a\boldsymbol{w} + \sigma^2) - \\ &\mathrm{lb}(\boldsymbol{w}^{\mathrm{H}}\boldsymbol{E}_a\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{E}_b\boldsymbol{w} - \eta_a^{\mathrm{t}}\eta_a^{\mathrm{r}}\eta_b^{\mathrm{t}}\eta_b^{\mathrm{r}}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{E}\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{E}\boldsymbol{w} + \\ &\sigma^2\boldsymbol{w}^{\mathrm{H}}\boldsymbol{E}_c\boldsymbol{w} + \sigma^4)。 \end{aligned} \tag{18}$$

2 波束赋形设计

提出一种联合波束赋形算法,通过优化基站发送波束赋形和 IRS 相移,以最大化系统的 KGR。建立 KGR 最大化问题如下:

$$\begin{aligned} &\max_{\boldsymbol{w},\boldsymbol{\theta}} I_s \\ &\text{s.t. } \mathrm{C1}: \|\boldsymbol{w}\|^2 \leqslant P_{\mathrm{t}} \\ &\quad \mathrm{C2}: |[\boldsymbol{\theta}]_m| = 1, m = 1,2,\cdots,M, \end{aligned} \tag{19}$$

式中:P_{t} 表示基站的最大发送功率,$[\boldsymbol{\theta}]_m$ 表示 $\boldsymbol{\theta}$ 的第 m 个元素。约束条件 C1 和 C2 分别表示发送功率约束与 IRS 相移单位模值约束。式(19)的目标函数是非凹的,优化变量深度耦合且约束条件 C2 是非凸的,因此难以直接求解。为此,本文利用 AO 技术将其解耦为 2 个子问题,分别交替优化 $\boldsymbol{w}$ 和 $\boldsymbol{\theta}$。

2.1 基站波束赋形设计

在任意给定 IRS 相移向量 $\boldsymbol{\theta}$ 的情况下优化基站发送波束赋形向量 $\boldsymbol{w}$。定义 $\boldsymbol{W} \triangleq \boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}$ 满足 $\boldsymbol{W} >= 0$ 和 $Rank(\boldsymbol{W}) = 1$。考虑到 $\boldsymbol{w}^{\mathrm{H}}\boldsymbol{E}\boldsymbol{w} = \mathrm{tr}(\boldsymbol{E}\boldsymbol{W})$,因此对于给定 $\boldsymbol{\theta}$,式(19)可被改写为关于 $\boldsymbol{W}$ 的优化问题:

$$\begin{aligned} &\min_{\boldsymbol{W}} \mathrm{lb}(f(\boldsymbol{W})) - \sum_{v\in\{a,b\}}\mathrm{lb}(\mathrm{tr}(\boldsymbol{E}_v\boldsymbol{W}) + \sigma^2) \\ &\text{s.t. } \mathrm{C1}: \mathrm{tr}(\boldsymbol{W}) \leqslant P_{\mathrm{t}} \\ &\quad \mathrm{C2}: \boldsymbol{W} >= 0 \\ &\quad \mathrm{C3}: Rank(\boldsymbol{W}) = 1 \end{aligned} \tag{20}$$

式中:$f(\boldsymbol{W}) \triangleq \mathrm{tr}(\boldsymbol{E}_a\boldsymbol{W}\boldsymbol{E}_b^{\mathrm{H}}\boldsymbol{W}) - \eta_a^{\mathrm{t}}\eta_a^{\mathrm{r}}\eta_b^{\mathrm{t}}\eta_b^{\mathrm{r}}\mathrm{tr}(\boldsymbol{E}\boldsymbol{W}\boldsymbol{E}^{\mathrm{H}}\boldsymbol{W}) + \sigma^2\mathrm{tr}(\boldsymbol{E}_c\boldsymbol{W}) + \sigma^4$。式(20)的目标函数仍是非凸的且含有 $\boldsymbol{W}$ 的高次方。利用 SCA 方法将目标函数线性化,引入松弛变量 α 和 β 并将式(20)改写:

$$\begin{aligned} &\min_{\boldsymbol{W},\alpha,\beta} \mathrm{lb}(\hat{f}(\boldsymbol{W},\alpha,\beta)) - \sum_{v\in\{a,b\}}\mathrm{lb}(\mathrm{tr}(\boldsymbol{E}_v\boldsymbol{W}) + \sigma^2) \\ &\text{s.t. } \mathrm{C1} \sim \mathrm{C3} \\ &\quad \mathrm{C4}: \alpha - \mathrm{tr}(\boldsymbol{E}_a\boldsymbol{W}\boldsymbol{E}_b^{\mathrm{H}}\boldsymbol{W}) \geqslant 0 \\ &\quad \mathrm{C5}: \beta - \mathrm{tr}(\boldsymbol{E}\boldsymbol{W}\boldsymbol{E}^{\mathrm{H}}\boldsymbol{W}) \leqslant 0, \end{aligned} \tag{21}$$

式中:

$$\hat{f}(\boldsymbol{W},\alpha,\beta) \triangleq \alpha - \eta_a^{\mathrm{t}}\eta_a^{\mathrm{r}}\eta_b^{\mathrm{t}}\eta_b^{\mathrm{r}}\beta + \sigma^2\mathrm{tr}(\boldsymbol{E}_c\boldsymbol{W}) + \sigma^4 。(22)$$

为分析方便,按照以下形式定义 $\tilde{f}(\boldsymbol{W},\alpha,\beta)$ 和 $q(\boldsymbol{W})$:

$$\tilde{f}(\boldsymbol{W},\alpha,\beta) \triangleq \mathrm{lb}(\hat{f}(\boldsymbol{W},\alpha,\beta)), \quad (23)$$

$$q(\boldsymbol{W}) \triangleq \mathrm{tr}(\boldsymbol{E}\boldsymbol{W}\boldsymbol{E}^{\mathrm{H}}\boldsymbol{W}) 。 \quad (24)$$

利用一阶泰勒展开公式分别推导出 $\tilde{f}(\boldsymbol{W},\alpha,\beta)$ 和 $q(\boldsymbol{W})$ 的线性估计值:

$$\begin{aligned}\tilde{f}(\boldsymbol{W},\alpha,\beta) \approx\ & \mathrm{tr}(\nabla_{\boldsymbol{W}}\tilde{f}(\boldsymbol{W}^{(t)},\alpha^{(t)},\beta^{(t)})^{\mathrm{H}}(\boldsymbol{W}-\boldsymbol{W}^{(t)})) + \\ & \mathrm{tr}(\nabla_{\alpha}\tilde{f}(\boldsymbol{W}^{(t)},\alpha^{(t)},\beta^{(t)})^{\mathrm{H}}(\alpha-\alpha^{(t)})) + \\ & \mathrm{tr}(\nabla_{\beta}\tilde{f}(\boldsymbol{W}^{(t)},\alpha^{(t)},\beta^{(t)})^{\mathrm{H}}(\beta-\beta^{(t)})) + \\ & \tilde{f}(\boldsymbol{W}^{(t)},\alpha^{(t)},\beta^{(t)}) \triangleq \widehat{f}(\boldsymbol{W},\alpha,\beta), \end{aligned} \quad (25)$$

$$\begin{aligned}q(\boldsymbol{W}) \approx\ & \mathrm{tr}((\boldsymbol{E}\boldsymbol{W}^{(t)}\boldsymbol{E}^{\mathrm{H}} + \boldsymbol{E}^{\mathrm{H}}\boldsymbol{W}^{(t)}\boldsymbol{E})^{\mathrm{H}}(\boldsymbol{W}-\boldsymbol{W}^{(t)})) + \\ & q(\boldsymbol{W}^{(t)}) \triangleq \tilde{q}(\boldsymbol{W}), \end{aligned} \quad (26)$$

式中:$\{\boldsymbol{W}^{(t)},\alpha^{(t)},\beta^{(t)}\}$ 表示第 t 次迭代中的一个可行点。$\tilde{f}(\boldsymbol{W}^{(t)},\alpha^{(t)},\beta^{(t)})$ 在 $\{\boldsymbol{W}^{(t)},\alpha^{(t)},\beta^{(t)}\}$ 的梯度由下式给出:

$$\begin{cases}\nabla_{\boldsymbol{W}}\tilde{f}(\boldsymbol{W}^{(t)},\alpha^{(t)},\beta^{(t)}) = \dfrac{\sigma^2\boldsymbol{E}_c^{\mathrm{T}}\mathrm{lb}(e)}{\hat{f}(\boldsymbol{W}^{(t)},\alpha^{(t)},\beta^{(t)})} \\ \nabla_{\alpha}\tilde{f}(\boldsymbol{W}^{(t)},\alpha^{(t)},\beta^{(t)}) = \dfrac{\mathrm{lb}(e)}{\hat{f}(\boldsymbol{W}^{(t)},\alpha^{(t)},\beta^{(t)})} \\ \nabla_{\beta}\tilde{f}(\boldsymbol{W}^{(t)},\alpha^{(t)},\beta^{(t)}) = \dfrac{-\eta_a^{\mathrm{t}}\eta_a^{\mathrm{r}}\eta_b^{\mathrm{t}}\eta_b^{\mathrm{r}}\mathrm{lb}(e)}{\hat{f}(\boldsymbol{W}^{(t)},\alpha^{(t)},\beta^{(t)})}\end{cases} 。 \quad (27)$$

接下来利用 SDR 将非凸的秩一约束 C3 直接省略,得到关于 $\boldsymbol{W}$ 的优化问题如下:

$$\begin{aligned}&\min_{\boldsymbol{W},\alpha,\beta} \widehat{f}(\boldsymbol{W},\alpha,\beta) - \sum_{v\in\{a,b\}}\mathrm{lb}(\mathrm{tr}(\boldsymbol{E}_v\boldsymbol{W}) + \sigma^2) \\ &\text{s.t. C6: } \beta - \tilde{q}(\boldsymbol{W}) \leqslant 0 \\ &\quad \text{C1,C2,C4} 。\end{aligned} \quad (28)$$

式(28)是一个半正定松弛问题,可以利用优化问题求解器 CVX 直接求解。最优发送波束赋形向量 $\boldsymbol{w}^*$ 可以通过特征根分解 $\boldsymbol{W}^*$ 得到。

2.2 IRS 相移偏移设计

在任意给定发送波束赋形向量 $\boldsymbol{w}$ 的情况下设计 IRS 相移向量 $\boldsymbol{\theta}$。将 R_h 改写为 $R_h = \hat{\boldsymbol{\theta}}^{\mathrm{H}}\hat{\boldsymbol{E}}\hat{\boldsymbol{\theta}}$,定义 $\hat{\boldsymbol{\theta}} = (\boldsymbol{\theta}^{\mathrm{T}},1)^{\mathrm{T}}$,利用 $\boldsymbol{a}^{\mathrm{H}}\widetilde{\mathrm{diag}}(\boldsymbol{b}\boldsymbol{b}^{\mathrm{H}})\boldsymbol{a} = \boldsymbol{b}^{\mathrm{H}}\widetilde{\mathrm{diag}}(\boldsymbol{a}\boldsymbol{a}^{\mathrm{H}})\boldsymbol{b}$ 结合式(3)和式(7)可以推导出:

$$\mathbb{E}\{h_v conj(h_v)\} = \hat{\boldsymbol{\theta}}^{\mathrm{H}}\hat{\boldsymbol{E}}_v\hat{\boldsymbol{\theta}} + \sigma^2 \triangleq \hat{R}_{h_v}, v \in \{a,b\}, \quad (29)$$

$$\mathbb{E}\{h_a conj(h_b)\} = \mathbb{E}\{h_b conj(h_a)\} = \sqrt{\eta_a^{\mathrm{t}}\eta_a^{\mathrm{r}}\eta_b^{\mathrm{t}}\eta_b^{\mathrm{r}}}\boldsymbol{\theta}^{\mathrm{H}}\hat{\boldsymbol{E}}_c\boldsymbol{\theta}, \quad (30)$$

式中:$\hat{\boldsymbol{E}}_a = \begin{pmatrix}\boldsymbol{A}_1 & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{A}_2\end{pmatrix}$,$\hat{\boldsymbol{E}}_b = \begin{pmatrix}\boldsymbol{B}_1 & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{B}_2\end{pmatrix}$,$\hat{\boldsymbol{E}}_c = \begin{pmatrix}\boldsymbol{E}_\theta & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{w}^{\mathrm{H}}\mathbb{E}\{\boldsymbol{h}_d\boldsymbol{h}_d^{\mathrm{H}}\}\boldsymbol{w}\end{pmatrix}$。

$$\begin{cases}\boldsymbol{A}_1 = \eta_a^{\mathrm{r}}\boldsymbol{E}_\theta + (1-\eta_a^{\mathrm{r}})\mathbb{E}\{\boldsymbol{H}^{\mathrm{H}}\widetilde{\mathrm{diag}}(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}})\boldsymbol{H}\} \\ \boldsymbol{A}_2 = \eta_a^{\mathrm{r}}\boldsymbol{w}^{\mathrm{H}}\mathbb{E}\{\boldsymbol{h}_d\boldsymbol{h}_{\mathrm{d}}^{\mathrm{H}}\}\boldsymbol{w} + (1-\eta_a^{\mathrm{r}})\boldsymbol{w}^{\mathrm{H}}\mathbb{E}\{\widetilde{\mathrm{diag}}(\boldsymbol{h}_d\boldsymbol{h}_d^{\mathrm{H}})\}\boldsymbol{w} \\ \boldsymbol{B}_1 = (1-\eta_b^{\mathrm{r}}+\eta_b^{\mathrm{r}}\eta_a^{\mathrm{t}})\boldsymbol{E}_\theta + \eta_b^{\mathrm{r}}(1-\eta_a^{\mathrm{t}})\mathbb{E}\{\boldsymbol{H}^{\mathrm{H}}\widetilde{\mathrm{diag}}(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}})\boldsymbol{H}\} \\ \boldsymbol{B}_2 = (1-\eta_b^{\mathrm{r}}+\eta_b^{\mathrm{r}}\eta_a^{\mathrm{t}})\boldsymbol{w}^{\mathrm{H}}\mathbb{E}\{\boldsymbol{h}_d\boldsymbol{h}_d^{\mathrm{H}}\}\boldsymbol{w} + \eta_b^{\mathrm{r}}(1-\eta_a^{\mathrm{t}})\cdot \\ \qquad \boldsymbol{w}^{\mathrm{H}}\mathbb{E}\{\widetilde{\mathrm{diag}}(\boldsymbol{h}_d\boldsymbol{h}_d^{\mathrm{H}})\}\boldsymbol{w} \\ \boldsymbol{E}_\theta = (\boldsymbol{w}^{\mathrm{T}}\otimes\boldsymbol{I}_M)\mathbb{E}\{vec(\boldsymbol{H}^{\mathrm{H}})(vec(\boldsymbol{H}^{\mathrm{H}}))^{\mathrm{H}}\}\cdot \\ \qquad (conj(\boldsymbol{w})\otimes\boldsymbol{I}_M)\end{cases} 。 \quad (31)$$

将式(29)和式(30)与式(16)和式(15)相结合,可以推导出:

$$\begin{aligned}I_s = & \sum_{v\in\{a,b\}}\mathrm{lb}(\hat{\boldsymbol{\theta}}^{\mathrm{H}}\hat{\boldsymbol{E}}_a\hat{\boldsymbol{\theta}} + \sigma^2) - \mathrm{lb}(\hat{\boldsymbol{\theta}}^{\mathrm{H}}\hat{\boldsymbol{E}}_a\hat{\boldsymbol{\theta}}\hat{\boldsymbol{\theta}}^{\mathrm{H}}\hat{\boldsymbol{E}}_b\hat{\boldsymbol{\theta}} - \eta_a^{\mathrm{t}}\eta_a^{\mathrm{r}}\eta_b^{\mathrm{t}}\cdot \\ & \eta_b^{\mathrm{r}}\hat{\boldsymbol{\theta}}^{\mathrm{H}}\hat{\boldsymbol{E}}_c\hat{\boldsymbol{\theta}}\hat{\boldsymbol{\theta}}^{\mathrm{H}}\hat{\boldsymbol{E}}_c\hat{\boldsymbol{\theta}} + \sigma^2\hat{\boldsymbol{\theta}}^{\mathrm{H}}\hat{\boldsymbol{E}}_d\hat{\boldsymbol{\theta}} + \sigma^4), \end{aligned} \quad (32)$$

式中:$\hat{\boldsymbol{E}}_d = \hat{\boldsymbol{E}}_a + \hat{\boldsymbol{E}}_b$。定义 $\boldsymbol{Q} = \hat{\boldsymbol{\theta}}\hat{\boldsymbol{\theta}}^{\mathrm{H}}$ 满足 $\boldsymbol{Q} \succ = 0$。与前文类似,将关于 $\boldsymbol{Q}$ 的优化问题表示为:

$$\begin{aligned}&\min_{\boldsymbol{Q}} \mathrm{lb}(g(\boldsymbol{Q})) - \sum_{v\in\{a,b\}}\mathrm{lb}(\mathrm{tr}(\hat{\boldsymbol{E}}_v\boldsymbol{Q}) + \sigma^2), \\ &\text{s.t. C8:}[\boldsymbol{Q}]_{m,m} = 1, m = 1,2,\cdots,M+1 \\ &\quad \text{C9:}\boldsymbol{Q} \succ = 0 \\ &\quad \text{C10:}Rank(\boldsymbol{Q}) = 1, \end{aligned} \quad (33)$$

式中:

$$\begin{aligned}g(\boldsymbol{Q}) \triangleq\ & \mathrm{tr}(\hat{\boldsymbol{E}}_a\boldsymbol{Q}\hat{\boldsymbol{E}}_b^{\mathrm{H}}\boldsymbol{Q}) - \eta_a^{\mathrm{t}}\eta_a^{\mathrm{r}}\eta_b^{\mathrm{t}}\eta_b^{\mathrm{r}}\mathrm{tr}(\hat{\boldsymbol{E}}_c\boldsymbol{Q}\hat{\boldsymbol{E}}_c^{\mathrm{H}}\boldsymbol{Q}) + \\ & \sigma^2\mathrm{tr}(\hat{\boldsymbol{E}}_d\boldsymbol{Q}) + \sigma^4。\end{aligned} \quad (34)$$

约束条件 C8 表示 $\boldsymbol{Q}$ 的所有对角线元素均等于 1,对应于 IRS 相移的单位模值约束。式(33)的目标函数和约束条件 C10 均是非凸的,导致难以直接求解。利用罚函数法处理秩一约束 C10。将式(33)改写为[19]:

$$\begin{aligned}&\max_{\boldsymbol{Q}} \mathrm{lb}(g(\boldsymbol{Q})) - \sum_{v\in\{a,b\}}\mathrm{lb}(\mathrm{tr}(\hat{\boldsymbol{E}}_v\boldsymbol{Q}) + \sigma^2) + \\ &\quad \kappa(\|\boldsymbol{Q}\|_* - \|\boldsymbol{Q}\|_2) \\ &\quad \text{s.t. C8,C9}, \end{aligned} \quad (35)$$

式中:$\|\boldsymbol{Q}\|_* = \sum_{i=1}^{M}\delta_i$ 表示核范数,其中 δ_i 为矩阵 $\boldsymbol{Q}$ 的第 i 大的奇异值。$\|\boldsymbol{Q}\|_2 = \delta_1$ 为谱范数,$\kappa > 0$ 为惩罚因子。对于任意的半正定矩阵 $\boldsymbol{Q}$,不等式 $\|\boldsymbol{Q}\|_* - \|\boldsymbol{Q}\|_2 \geqslant 0$ 均成立,当且仅当矩阵 $\boldsymbol{Q}$ 的秩为 1 时,等号成立。因此,惩罚项可以保证式(35)的最优解满足秩一约束 C10。惩罚项属于凸差形式,可以利用一阶泰勒展开公式推导出 $\|\boldsymbol{Q}\|_2$ 的凸下界:

$$\begin{aligned}\|\boldsymbol{Q}\|_2 \geqslant\ & \mathrm{tr}(\lambda_{\max}(\boldsymbol{Q}^{(t)})\boldsymbol{\lambda}_{\max}^{\mathrm{H}}(\boldsymbol{Q}^{(t)})(\boldsymbol{Q}-\boldsymbol{Q}^{(t)})) + \\ & \boldsymbol{Q}^{(t)}{}_2 \triangleq \tilde{\boldsymbol{Q}}^{(t)}, \end{aligned} \quad (36)$$

式中:$\boldsymbol{\lambda}(\boldsymbol{Q})_{\max}$ 表示矩阵 $\boldsymbol{Q}$ 的最大特征根对应的特征向量,$\boldsymbol{Q}^{(t)}$ 为第 t 次迭代中的一个固定值。式(35)可以改写为:

$$\max_{\boldsymbol{Q}} \operatorname{lb}(g(\boldsymbol{Q})) - \sum_{v\in\{a,b\}} \operatorname{lb}(\operatorname{tr}(\hat{\boldsymbol{E}}_v\boldsymbol{Q}) + \sigma^2) + \kappa(\|\boldsymbol{Q}\|_* - \tilde{\boldsymbol{Q}}^{(t)})$$
$$\text{s.t. C8, C9。} \tag{37}$$

式(37)的目标函数可以利用前文提出的 SCA 方法线性化,再利用 CVX 求解出最优解 $\boldsymbol{Q}^*$。最优的 IRS 相移向量 $\boldsymbol{\theta}^*$ 可以通过 $\boldsymbol{Q}^*$ 的特征值分解得到。所提 KGR 最大化算法的详细步骤总结在算法 1 中。

算法 1　求解式(19)的 KGR 最大化鲁棒联合优化算法

参数初始化:设置初始值 $\{\boldsymbol{W}^{(t)} = \boldsymbol{w}^{(t)}(\boldsymbol{w}^{(t)})^{\mathrm{H}}, \boldsymbol{Q}^{(t)} = \hat{\boldsymbol{\theta}}^{(t)}\cdot(\hat{\boldsymbol{\theta}}^{(t)})^{\mathrm{H}}\}$,$t = i = 0$;
1:外循环 t:
2:给定 $\{\boldsymbol{W}^t, \boldsymbol{Q}^t\}$,通过求解式(28)更新 $\boldsymbol{W}^{t+1}$;
3:设置 $\hat{\boldsymbol{Q}}^i = \boldsymbol{Q}^t$ 和惩罚因子 κ;
4:内循环 i;
5:给定 $\{\boldsymbol{W}^{t+1}, \hat{\boldsymbol{Q}}^i\}$,通过求解式(37)获得 $\hat{\boldsymbol{Q}}^{i+1}$;
6:更新 $\kappa = \tau\kappa$,$i = i + 1$;
7:直到 $\|\hat{\boldsymbol{Q}}\|_* - \|\hat{\boldsymbol{Q}}\|_2 \leqslant \varepsilon_2$,退出内循环;
8:更新 $\boldsymbol{Q}^{t+1} = \boldsymbol{Q}^i$,$t = t + 1$ 计算 I_s^{t+1};
9:直到 $|I_s^t - I_s^{t-1}| \leqslant \varepsilon_1$,停止外循环;
10:利用特征值分解由 $\boldsymbol{W}^*$ 和 $\boldsymbol{Q}^*$ 得到 $\boldsymbol{w}^*$ 和 $\boldsymbol{\theta}^*$。

2.3　计算复杂度分析

所提 KGR 最大化鲁棒算法的计算复杂度主要来自于步骤 2 和步骤 5,涉及 2 个 SDP 问题。如果利用内点法求解,相应的计算复杂度分别为 $\mathcal{O}(N^{3.5})$ 和 $\mathcal{O}((M+1)^{3.5})$。因此,所提鲁棒算法的计算复杂度可以表示为 $\mathcal{O}(T_{\mathrm{AO}}(N^{3.5} + T_{\mathrm{PM}}(M+1)^{3.5}))$,其中 T_{AO} 和 T_{PM} 分别表示 AO 和罚函数法的迭代次数。

3　仿真结果

通过 Matlab 仿真验证所提鲁棒算法的性能,并分析硬件损伤对 KGR 的影响。在仿真设置中,基站、IRS 和 Bob 的坐标分别为 (0,0,20) m、(0,20,20) m 和 (40,0,1.5) m。参考距离 1 m 处的路径损耗设定为 −30 dB。直射链路(基站至 Bob)的路径损耗指数设置为 4,IRS 相关链路(基站至 IRS 和 IRS 至用户)的路径损耗指数设置为 2.2。小尺度衰落方面,直射链路建模为瑞利分布,IRS 相关链路建模为莱斯分布,莱斯因子为 3 dB。除非特别说明,其他仿真参数设置为:$N = M = 10$,$P_{\mathrm{t}} = 10$ dBm,$\sigma_{b,k}^2 = \sigma_{e,k}^2 = -90$ dBm,$\eta_v^{\mathrm{t}} = \eta_v^{\mathrm{r}} = 0.95$,$v \in \{a,b\}$。

为评估所提鲁棒算法的性能,采用以下对比方案:① 理想情况。不存在硬件损伤的理想情况。② 非鲁棒算法。存在硬件损伤,但是设计基站发送波束赋形和 IRS 相移时不考虑硬件损伤。③ 鲁棒随机相移。存在硬件损伤,利用所提鲁棒算法设计基站发送波束赋形向量,随机生成 IRS 相移向量。④ 鲁棒无 IRS。存在硬件损伤,并且没有 IRS 辅助,利用所提鲁棒算法设计基站发送波束赋形向量。

图 2 展示了不同基站天线数和 IRS 单元数配置下所提鲁棒算法的收敛性能。可以看出,所有配置下 KGR 均随着交替优化迭代次数的增加不断升高,而且能够很快收敛,说明所提鲁棒算法具有良好的收敛特性。同时,基站天线数和 IRS 单元数量越多,收敛所需的迭代次数就越多,这是由于更多的优化变量导致收敛速度变慢。

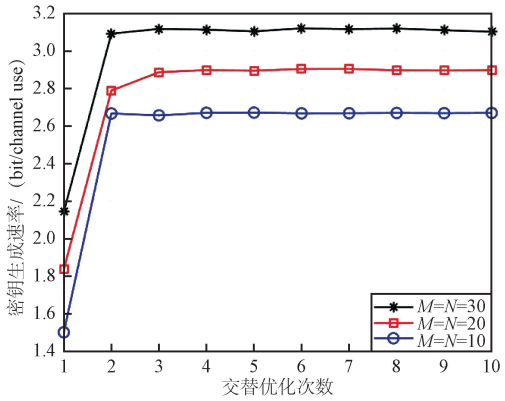

图 2　所提鲁棒算法的收敛性

Fig. 2　Convergence behavior of the proposed robust algorithm

图 3 展示了基站最大发射功率与 KGR 之间的关系。可以看出,所提鲁棒算法的性能优于非鲁棒方案,表明所提鲁棒算法在抵抗硬件损伤噪声方面的良好性能。同时,与未使用 IRS 的情形相比,引入 IRS 的方案表现更佳,这是因为在直射路径之外,IRS 增加了额外的反射路径,从而带来了更多优化自由度。随机相移方案的 KGR 远小于所提鲁棒算法的 KGR,说明通过合理设计 IRS 的反射相移,能够有效提高密钥生成性能,凸显了 IRS 在增强 KGR 方面的作用。此外,随着基站发射功率的增加,理想条件与非理想条件下系统性能差异逐渐扩大,原因在于残余硬件损伤引入的干扰噪声功率会随信号功率同步增长,因此在高功率场景下硬件损伤的负面影响更加突出。

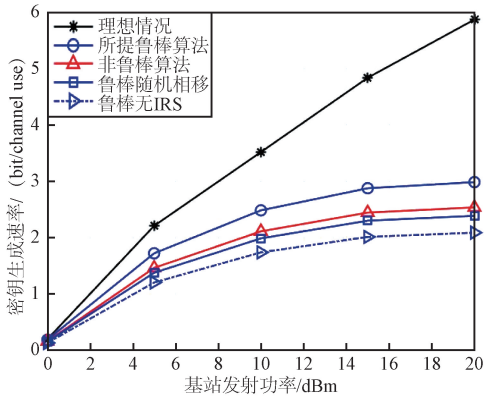

图 3　KGR 与基站最大发射功率的关系

Fig. 3　Relationship between KGR and the maximum transmit power of the base station

图 4 给出了 KGR 随 IRS 反射单元数量变化的趋势。可以看出,在存在硬件损伤时,所提鲁棒算法表现出最优性能。除“鲁棒无 IRS”的情形外,其余各方案的 KGR 随着 IRS 反射单元数量的增加而上升,这是因为反射单元数量越多,系统可调控的自由度越大,进而增强了对信道的优化能力,提高了整体性能。

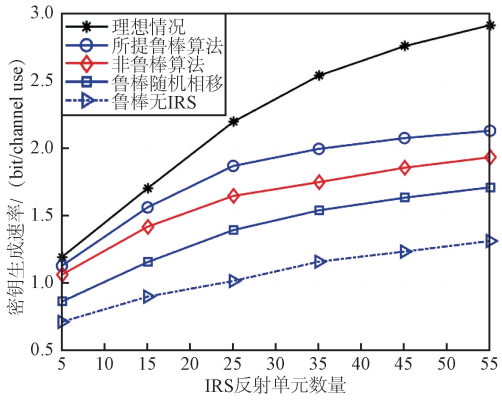

图 4　KGR 与 IRS 反射单元数量的关系

Fig. 4　Relationship between KGR and the number of IRS reflecting elements

采用高质量的收发信机可以降低硬件损伤、提升系统性能,但同时会增加硬件成本。因此,在给定硬件成本的情况下,在收发信机链路中设计最优的硬件损伤组合以实现性能最大化具有重要的现实意义[15]。图 5 展示了硬件成本固定时 KGR 与硬件损伤程度的关系,假设 $\eta_a^{\mathrm{t}}=\eta_b^{\mathrm{r}}=\eta_{ab}$, $\eta_b^{\mathrm{t}}=\eta_a^{\mathrm{r}}=\eta_{ba}$,当硬件成本固定时,可以认为 $\eta_{ab}+\eta_{ba}=1$。可以看出,当 η_{ab} 与 η_{ba} 相等时 KGR 出现最大值,即当上行链路与下行链路的硬件损伤程度相同时,系统性能最好,当上行链路的硬件损伤程度大于或小于下行链路的硬件损伤程度时,都会造成系统性能下降。

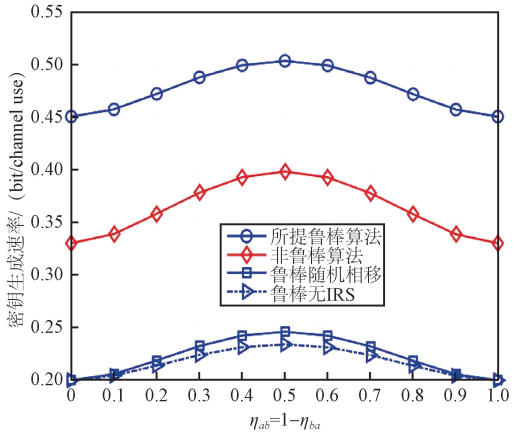

图 5　硬件成本固定时 KGR 与硬件损伤程度的关系

Fig. 5　Relationship between KGR and hardware impairment level under fixed hardware cost

图 6 展示了 KGR 与 IRS 相关信道的莱斯因子之间的关系。可以看出,除了“无 IRS”的情形外,其余方案的 KGR 都会随莱斯因子的增加而下降。这是因为只有随机的非视距分量才能用于生成密钥,而莱斯因子越大,非视距分量的功率越低,导致 KGR 变小。

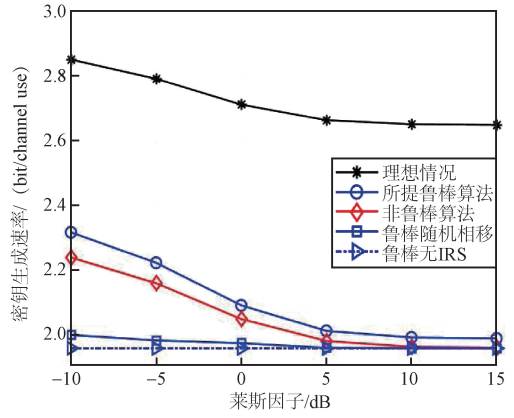

图 6　KGR 与莱斯因子的关系

Fig. 6　Relationship between KGR and the Rician factor

4　结束语

本文针对 IRS 辅助的 PKG 系统,提出了一种对抗残余硬件损伤的鲁棒波束赋形算法。推导出了 KGR 的闭合表达式,在基站最大发送功率约束与 IRS 单位模值约束下构造了 KGR 最大化问题。利用 SCA 技术、泰勒展开公式、SDR 和罚函数法设计了一种基于 AO 的鲁棒波束赋形算法用以提升 KGR,仿真结果验证了所提鲁棒算法的有效性。未来的研究可以考虑 IRS 的非理想硬件特性,包括幅

值与相位耦合、反射单元互耦和相位噪声等对密钥生成性能的影响以及相应的鲁棒方案设计。

参 考 文 献

[1] 黄开枝,金梁,钟州 .5G 物理层安全技术——以通信促安全[J]. 中兴通讯技术,2019,25(4):43-49.

[2] PRADHAN A, DAS S, PIRAN M J, et al. A Survey on Physical Layer Security of Ultra/Hyper Reliable Low Latency Communication in 5G and 6G Networks: Recent Advancements, Challenges, and Future Directions[J]. IEEE Access, 2024, 12: 112320-112353.

[3] 唐燕群,李为,张立健,等. 基于无线信道特征的内生安全通信技术及应用[J]. 无线电通信技术,2020,46(2):159-167.

[4] HU X Y, JIN L, HUANG K Z, et al. Intelligent Reflecting Surface-assisted Secret Key Generation with Discrete Phase Shifts in Static Environment[J]. IEEE Wireless Communications Letters, 2021, 10(9): 1867-1870.

[5] WU Q Q, ZHANG S W, ZHENG B X, et al. Intelligent Reflecting Surface-aided Wireless Communications: A Tutorial[J]. IEEE Transactions on Communications, 2021, 69(5): 3313-3351.

[6] 李兴旺,田志发,张建华,等. IRS 辅助 NOMA 网络下隐蔽通信性能研究[J]. 中国科学:信息科学,2024,54(6):1502-1515.

[7] 李兴旺,王新莹,田心记,等. 基于非理想条件 RIS 辅助 SWIPT-NOMA 系统通感性能研究[J]. 电子与信息学报,2024,46(6):2434-2442.

[8] LI X W, GAO X S, LIU Y T, et al. Overlay Cognitive Radio-assisted NOMA Intelligent Transportation Systems with Imperfect SIC and CEEs[J]. Chinese Journal of Electronics, 2023, 32(6): 1258-1270.

[9] JI Z J, YEOH P L, ZHANG D Y, et al. Secret Key Generation for Intelligent Reflecting Surface Assisted Wireless Communication Networks[J]. IEEE Transactions on Vehicular Technology, 2021, 70(1): 1030-1034.

[10] LU X J, LEI J, SHI Y X, et al. Intelligent Reflecting Surface Assisted Secret Key Generation[J]. IEEE Signal Processing Letters, 2021, 28: 1036-1040.

[11] LI G Y, SUN C, XU W, et al. On Maximizing the Sum Secret Key Rate for Reconfigurable Intelligent Surface-assisted Multiuser Systems[J]. IEEE Transactions on Information Forensics and Security, 2022, 17(5): 211-225.

[12] HU L, LI G Y, QIAN X W, et al. Reconfigurable Intelligent Surface-assisted Secret Key Generation in Spatially Correlated Channels[J]. IEEE Transactions on Wireless Communications, 2024, 23(3): 2153-2166.

[13] HU L, SUN C, LI G Y, et al. Reconfigurable Intelligent Surface-aided Secret Key Generation in Multi-cell Systems[J]. IEEE Transactions on Communications, 2023, 71(11): 6499-6513.

[14] CHU Z, ZHONG J, XIAO P, et al. RIS Assisted Wireless Powered IoT Networks with Phase Shift Error and Transceiver Hardware Impairment[J]. IEEE Transactions on Communications, 2022, 70(7): 4910-4924.

[15] LETAFATI M, BEHROOZI H, KHALAJ B H, et al. Hardware-impaired PHY Secret Key Generation with Man-in-the-Middle Adversaries[J]. IEEE Wireless Communications Letters, 2022, 11(4): 856-860.

[16] YANG S C, HUANG K Z, NIU H H, et al. IRS-assisted Secret Key Generation with Transceiver Hardware Impairments[J]. IEEE Transactions on Vehicular Technology, 2024, 73(8): 12154-12159.

[17] SAEIDI M A, EMADI M J, MASOUMI H, et al. Weighted Sum-rate Maximization for Multi-IRS-assisted Full-duplex Systems with Hardware Impairments[J]. IEEE Transactions on Cognitive Communications and Networking, 2021, 7(2): 466-481.

[18] ZHOU G, PAN C H, REN H, et al. Secure Wireless Communication in RIS-aided MISO System with Hardware Impairments[J]. IEEE Wireless Communications Letters, 2021, 10(6): 1309-1313.

[19] MU X D, LIU Y W, GUO L, et al. Simultaneously Transmitting and Reflecting (STAR) RIS Aided Wireless Communications[J]. IEEE Transactions on Wireless Communications, 2022, 21(5): 3083-3098.

作者简介:

王 毅 男,(1984—),博士,副教授。主要研究方向:大规模 MIMO、能效通信、无人机辅助通信、IRS 辅助无线通信、物理层安全等。

(*通信作者)**杨少川** 男,(1989—),博士,讲师。主要研究方向:IRS 辅助无线通信、物理层安全、能效通信等。

赵 飞 男,(1985—),博士,讲师。主要研究方向:IRS 辅助无线通信、NOMA、能效通信等。

冀保峰 男,(1985—),博士,教授,博士生导师。主要研究方向:智能系统、移动通信、通感算控一体化。

楚 征 男,(1986—),博士,助理教授。主要研究方向:移动通信、通感一体化、IRS 辅助无线通信、物理层安全、SWIPT 等。

李春国 男,(1983—),博士,教授,博士生导师。主要研究方向:6G 蜂窝通信、网络空间安全、人工智能、计算机视觉等。