文章编号:1671-4598(2025)12-0286-10 DOI:10.16526/j.cnki.11-4762/tp.2025.12.037 中图分类号:TN911 文献标识码:A

未知窃听者CSI条件下的智能超表面物理层安全传输

苗睿锴，宋志群，李 勇，李行健，刘丽哲，王 斌
（中国电子科技集团公司 第五十四研究所 先进通信网全国重点实验室，石家庄 050081）

摘要：研究了基于智能超表面的安全传输，现有研究主要针对窃听者CSI已知这一理想假设，而实际中窃听者CSI通常难以获取；因此，针对窃听者CSI完全未知条件下智能超表面的安全传输进行了研究；首先通过基站波束赋形向量和智能超表面相移矩阵的主被动波束赋形在满足合法用户通信质量的约束下最小化通信信号传输功率，然后将剩余功率用于发送人工噪声以干扰潜在的窃听者；提出了一种深度学习辅助的流形优化方法来解决这一功率分配问题，该方法将黎曼梯度下降模型与深度学习方法相结合，基于神经网络的自适应学习能力动态调控黎曼梯度下降的方向和步长；实验结果表明，与现有的优化算法相比，所提出的方法在达到几乎相同的安全速率的同时，计算复杂度降低至少一个数量级。

关键词：物理层安全；智能超表面（RIS）；人工噪声；流形优化；深度学习；CSI

RIS-Based Physical Layer Secure Transmission with Unknown Eavesdropper CSI

MIAO Ruikai, SONG Zhiqun, LI Yong, LI Xingjian, LIU Lizhe, WANG Bin
(The 54th Research Institute, China Electronics Technology Group Corporation,
National Key Laboratory of Advanced Communication Networks, Shijiazhuang 050081, China)

Abstract: Research on the secure transmission based on reconfigurable intelligent surface (RIS) is conducted, where existing research mainly focuses on the ideal assumption of known eavesdropper's channel state information (CSI), while it is usually difficult for the eavesdropper's CSI to obtain in practice. Therefore, this paper studies a RIS-based secure transmission under completely unknown eavesdropper's CSI. Firstly, through the beamforming vectors in base stations and CIS phase shift matrices, the active-passive beamforming minimizes the transmission power of communication signals while meeting the constraints of legitimate users in communication quality, and then uses residual power to transmit artificial noise to jam potential eavesdroppers. A deep learning-based manifold optimization method is proposed to address the power allocation, which combines the Riemannian gradient descent model with deep learning method. The adaptive learning ability of neural networks can dynamically adjust the direction and step size of the Riemannian gradient descent. Experimental results show that compared to existing optimization algorithms, the proposed method reduces the computational complexity by at least one order of magnitude while achieving almost identical secrecy rate.

Keywords: physical layer security; RIS; artificial noise; manifold optimization; deep learning; CSI

收稿日期:2025-06-30； **修回日期**:2025-08-06。
基金项目:河北省自然科学基金(F2024523005);河北省博士后科学基金(B2023005001);先进通信网全国重点实验室基金(FFX24641X005);通信抗干扰全国重点实验室基础科研创新基金(稳定支持)项目(IFN202404)。
作者简介:苗睿锴(1999-),男,硕士研究生。
通讯作者:李 勇(1985-),男,博士,研究员。
引用格式:苗睿锴,宋志群,李 勇,等.未知窃听者CSI条件下的智能超表面物理层安全传输[J].计算机测量与控制,2025,33(12):286-295.

0　引言

无线信道的开放性和广播性质使得传输的信号面临着受到窃听和干扰等安全威胁，无线通信的安全性引起了学术界、工业界和政府机构的广泛关注[1]。传统的安全传输方法多采用基于密码学理论的加密方法[2]，通常部署于协议栈的上层，但是此类方法大量的计算开销和密钥管理成本可能会导致较高的计算复杂度和资源消耗。物理层安全技术是一种利用物理介质的随机特性以及窃听信道和合法信道之间的差异性来确保机密信息安全传输的方法。与基于密码学理论的加密方法不同，物理层安全技术基于信息论，它利用噪声、信道衰落和其他物理因素的随机性来增强系统的安全性。与基于密码学的安全传输方法相比，物理层安全技术不取决于所利用的通信设备具有的计算能力，即便窃听者具有较强大的计算能力，物理层安全技术也可以确保通信的安全性。综上所述，物理层安全技术具有较为广阔的发展前景。

智能超表面（RIS，reconfigurable intelligent surface）是一种由大量低成本可编程反射单元构成的二维电磁超表面[3]。每个反射单元都能够在智能控制器的控制下改变自身的反射系数，对入射信号引入相移达到改变入射信号相位和传播方向的作用。将 RIS 部署在环境中（如覆盖在建筑物表面或者由无人机携带），RIS 可以自适应地改变无线信道的特性，实现通信系统收发端和信道的联合优化，从而使得无线环境成为通信系统设计参量的一部分，将通信系统设计范式从“被动适应新道”转向“主动调控信道”[4]。此外，由于 RIS 没有射频链路，它的成本和功耗均较低并且不会引入额外噪声。得益于 RIS 改变电磁环境的能力以及低成本、高能效的优点，RIS 具有广阔的应用前景，被视为未来无线通信的关键技术之一[5]。

基于 RIS 的物理层安全传输的核心是将通信信号更多地集中在合法接收段，减少在窃听者处的泄漏，以提高系统的安全速率。目前，研究人员已经提出了多种基于 RIS 的安全传输方法来保障无线通信系统的安全性。文献［6］的作者首次提出了基于 RIS 的物理层安全技术，研究了环境中存在单天线窃听者场景下，基于 RIS 的无线通信系统安全传输问题，提出了基于瑞利商函数最大值闭式解和半正定松弛的主被动波束赋形技术，通过主被动波束赋形最大化安全速率。仿真结果表明，RIS 可以有效提升系统的安全速率，然而，文献［6］中所提出的算法运算复杂度较高，并且仅考虑了单天线窃听者的情况，具有一定的局限性。进一步地，文献［7］中考虑了多天线窃听者的情况，并且提出了基于瑞利商函数最大值闭式解和流形优化的主被动波束赋形技术，通过主被动波束赋形来最大化安全速率，仿真结果表明，与文献［6］所提出的算法相比，文献［7］所提出的算法在安全速率不降低的前提下，有效降低了运算复杂度；文献［8］将人工噪声引入了 RIS 辅助的无线通信系统，通过主被动波束赋形和人工噪声的联合优化来提高系统的安全速率，验证了在 RIS 辅助的无线通信系统中引入人工噪声能够获得更高的安全速率；在文献［6－8］中，RIS 均为无源 RIS，然而随着 RIS 的发展，出现了例如有源 RIS 等新型硬件架构，有源 RIS 通过在反射阵面上引入功率放大器解决无源 RIS 的双乘积路径损耗问题，围绕有源 RIS 的应用，文献［9］的作者引入了基于无源 RIS 和有源 RIS 的混合 RIS，通过引入有源 RIS 克服无源 RIS 的双乘积路径损耗，进一步提升了系统的安全速率。

在上述工作中均基于窃听者位置和信道状态信息（CSI，channel state information）准确已知，然而由于信道估计存在误差，CSI 通常是不准确的。在这种条件下，文献［10］引入了动态时变信道和窃听者 CSI 有界误差模型，提出了基于深度强化学习的鲁棒波束赋形方法，在确保合法方通信质量的前提下最大化系统安全速率，实现了比文献［6］更高的安全速率。在窃听者 CSI 有界误差模型的基础上，文献［11］进一步考虑了多 RIS 辅助无线通信中的鲁棒安全传输问题，通过多个 RIS 的联合波束赋形进一步提高系统的安全速率，首先通过 S 引理和连续凸近似处理信道不确定性问题，然后通过半正定松弛法惩罚函数和特征值分解联合优化波束赋形向量和相移矩阵；文献［12］研究了只有统计 CSI 情况下的波束赋形技术，推导出了近似遍历安全速率的表达式，并利用块坐标下降法求解联合波束赋形问题。上述工作虽然考虑了窃听者 CSI 的误差，但是仍然假设窃听者位置是已知的。因此，文献［13］考虑了更加贴近实际的情况，即窃听者的准确位置也是未知的，只有窃听者可能存在的可疑区域，在这种情况下，作者提出了两阶段优化问题，第一阶段通过最坏情况下的窃听者位置优化 RIS 的部署位置，第二阶段中进行主被动波束赋形，通过两阶段优化问题的求解有效提升了系统安全速率。

上述所有工作都基于窃听者的完美或者不完美 CSI，是已知的。然而在实际中，窃听者通常是静默的，不与通信系统交换 CSI，因此假设窃听者 CSI 是已知的这一假设过于理想。所以在实际情况下，窃听者的 CSI 是未知的。由于上述研究工作均依赖窃听者 CSI，存在一定的局限性，已有部分文献研究了窃听者 CSI 未知条件下的安全传输问题。在这种情况下，文献［14］引入

与合法信道正交的人工噪声来干扰窃听者，在满足合法用户服务质量（QoS，quality of service）的情况下增强安全性，提出了基于流形优化的主被动波束赋形方法来解决窃听者 CSI 未知时的安全传输问题。文献［15］构建了与文献［14］相同的优化问题，研究了在满足用户处 QoS 前提下的主被动波束赋形技术，提出了基于半正定松弛的主被动波束赋形方法。围绕窃听者 CSI 未知条件下的安全传输问题，文献［16］将基于 RIS 的物理层安全传输技术应用于反向散射通信系统中，研究了窃听者 CSI 未知条件下 RIS 辅助反向散射通信系统中的安全传输问题，提出了基于块坐标下降和半正定规划的主被动联合波束赋形算法。尽管上述工作研究了窃听者 CSI 未知条件下的安全传输问题，但所提出的方法需要多次迭代，计算复杂度较高，难以满足 RIS 实时调控信道环境的需要。

上述研究工作具有一定的局限性，因此研究了窃听者 CSI 未知场景下，基于 RIS 的物理层安全传输问题。主要贡献总结如下：

研究了在窃听者 CSI 未知时通过联合波束赋形和人工噪声的物理层安全传输方法。通过最小化通信信号的发射功率以满足合法用户的 QoS，剩余功率用来发送人工噪声干扰潜在的窃听者；

为了降低计算复杂度，提出了一种深度学习辅助的流形优化方法，以最小化通信信号的传输功率。与文献［14］和［15］中现有的算法不同，该方法利用深度神经网络（DNN，deep neural network）的学习能力适应地学习基于黎曼梯度的更新规则，而非手动调整规则；

实验结果显示，与现有的优化算法相比，所提出的方法在保持安全速率的同时，有效降低了计算复杂度，具有良好的实际应用前景。

1 系统模型与问题表述

如图 1 所示，考虑一个基于 RIS 的多输入单输出（MISO，multiple input single output）系统。在 RIS 的辅助下，多天线基站（以下简称 Alice）向单天线合法用户（以下简称 Bob）传输通信信号。传输过程被单天线窃听者（以下简称 Eve）窃听，窃听者的位置和 CSI 均未知。

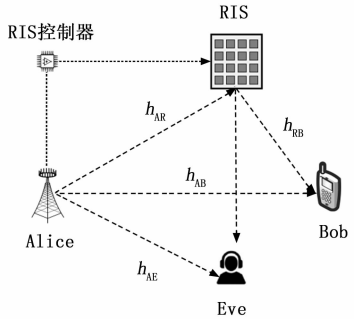

图 1 基于智能超表面的无线通信系统

假设多天线 Alice 配备了由 M 根天线组成的均匀线性阵列（ULA，uniform linear array），RIS 为配备了 N 个反射单元的均匀面阵阵列（UPA，uniform planar array）。假设系统中所有节点的位置均位于天线远场范围，所有信道都遵循准静态平坦衰落。Alice 与 RIS、Alice 与 Bob、Alice 与 Eve、RIS 与 Bob、RIS 与 Eve 之间的基带等效信道分别用 $\boldsymbol{H}_{\mathrm{AR}} \in \boldsymbol{C}^{N\times M}$，$\boldsymbol{h}_{\mathrm{AB}} \in \boldsymbol{C}^{M\times 1}$，$\boldsymbol{h}_{\mathrm{AE}} \in \boldsymbol{C}^{M\times 1}$，$\boldsymbol{h}_{\mathrm{RB}} \in \boldsymbol{C}^{N\times 1}$ 和 $\boldsymbol{h}_{\mathrm{RE}} \in \boldsymbol{C}^{N\times 1}$ 表示。系统中任意信道矩阵可以表示为：

$$\boldsymbol{H} = L\left(\sqrt{\frac{\kappa}{\kappa+1}}\boldsymbol{H}_{\mathrm{LoS}} + \sqrt{\frac{1}{\kappa+1}}\boldsymbol{H}_{\mathrm{NLoS}}\right) \tag{1}$$

信道矩阵分为视距分量和非视距分量。其中，L 是与收发端相对距离和载波频率有关的自由空间路径损耗，κ 为莱斯因子，表示莱斯信道中视距分量功率所占比例，$\boldsymbol{H}_{\mathrm{LoS}}$ 是视距分量，$\boldsymbol{H}_{\mathrm{NLoS}}$ 是非视距分量。假设 Alice 的天线阵列为 ULA 阵列，RIS 为 UPA 阵列，因此 Alice-RIS 的 $\boldsymbol{H}_{\mathrm{LoS}}$ 可以表示为 RIS 的接收响应向量和 Alice 发送响应向量的乘积：

$$\boldsymbol{H}_{\mathrm{LoS}} = \boldsymbol{a}_r(\psi)\boldsymbol{a}_t^H(\varphi) \tag{2}$$

其中：

$$\boldsymbol{a}_t(\psi) = [1,\cdots,e^{j(M-1)2\pi d/\lambda\cos(\psi)}]^H \tag{3}$$

$$\boldsymbol{a}_t(\varphi) = [1,\cdots,e^{j(M-1)2\pi d/\lambda\cos(\varphi)}]^H \tag{4}$$

ψ 为离开角（AoD，angle of departure），φ 为到达角（AoA，angle of arrival）。类似地，RIS-Bob 和 RIS-Eve 的 LoS 分量为 RIS 的阵列发送响应向量：

$$\boldsymbol{H}_{\mathrm{LoS}} = \boldsymbol{a}_I(\varphi) = [1,\cdots,e^{j(M-1)2\pi d/\lambda\cos(\varphi)}]^H \tag{5}$$

$\boldsymbol{H}_{\mathrm{NLoS}}$ 是由于环境中障碍物或散射体的存在所造成的多径衰落，建模为循环对称复高斯分布（CSCG，circularly symmetric complex gaussian），满足 $CN(0,1)$。假设直射链路中存在较多障碍物和散射体，因此 Alice-Bob 和 Alice-Eve 直射链路建模为瑞利信道，链路中仅存在由于障碍物或散射体造成的多径衰落，莱斯因子设置为 0；RIS 部署于靠近合法接收端 Bob 的附近，提供具有直射分量的视距反射链路以确保合法方的通信质量并确保传输的安全性，Alice-RIS、RIS-Bob 和 RIS-Eve 链路建模为莱斯信道。RIS 的相移矩阵定义为 $\boldsymbol{\Phi} = \mathrm{diag}(e^{j\varphi_1},e^{j\varphi_2},\cdots,e^{j\varphi_N})$，其中 φ_i 为第 i 个反射元件的相移。$s \sim CN(0,1)$ 表示 Alice 处均值为零的功率归一化的通信信号。Alice 的波束赋形向量定义为 $\boldsymbol{w} \in \boldsymbol{C}^{M\times 1}$。同时，由于 Eve 的 CSI 未知，引入人工噪声来增强通信系统的安全性。$\boldsymbol{n}_a \in \boldsymbol{C}^{M\times 1}$ 表示发送的人工噪声。根据 RIS 的级联信道模型，合法用户 Bob 和窃听者 Eve 处接收到的信号可以分别表示为：

$$y_{\mathrm{B}}=(\boldsymbol{h}_{\mathrm{AB}}^{H}+\boldsymbol{H}_{\mathrm{AR}}\boldsymbol{\Phi}\boldsymbol{h}_{\mathrm{RB}}^{H})(\boldsymbol{w}s+\boldsymbol{n}_{a})+z_{\mathrm{B}} \tag{6}$$

$$\boldsymbol{y}_{\mathrm{E}}=(\boldsymbol{h}_{\mathrm{AE}}^{H}+\boldsymbol{H}_{\mathrm{AR}}\boldsymbol{\Phi}\boldsymbol{h}_{\mathrm{RE}}^{H})(\boldsymbol{w}s+\boldsymbol{n}_{a})+z_{\mathrm{E}} \tag{7}$$

其中：$z_{\mathrm{B}}\sim CN(0,\sigma_{\mathrm{B}}^{2})$ 和 $z_{\mathrm{E}}\sim CN(0,\sigma_{\mathrm{E}}^{2})$ 分别为合法用户 Bob 和窃听者 Eve 接收机处功率为 σ_{B}^{2} 和 σ_{E}^{2} 的加性高斯白噪声。为了方便表述，进一步定义 RIS 的相移为 $\boldsymbol{q}=[q_{1},q_{2},\cdots,q_{N}]^{H}=[e^{j\varphi_{1}},e^{j\varphi_{2}},\cdots,e^{j\varphi_{N}}]^{H}$，Alice-RIS-Bob 的级联信道为 $\boldsymbol{H}_{\mathrm{B}}=\mathrm{diag}(\boldsymbol{h}_{\mathrm{RB}}^{H})\boldsymbol{H}_{\mathrm{AR}}\in\boldsymbol{C}^{N\times M}$，Alice-RIS-Eve 的级联信道为 $\boldsymbol{H}_{\mathrm{BE}}=\mathrm{diag}(\boldsymbol{h}_{\mathrm{RE}}^{H})\boldsymbol{H}_{\mathrm{AR}}\in\boldsymbol{C}^{N\times M}$。根据 RIS 的改进级联信道模型，则合法用户 Bob 和窃听者 Eve 处接收到的信号可以等效地表示为：

$$y_{\mathrm{B}}=(\boldsymbol{h}_{\mathrm{AB}}^{H}+\boldsymbol{q}^{H}\boldsymbol{H}_{\mathrm{B}})(\boldsymbol{w}s+\boldsymbol{n}_{a})+z_{\mathrm{B}} \tag{8}$$

$$y_{\mathrm{E}}=(\boldsymbol{h}_{\mathrm{AE}}^{H}+\boldsymbol{q}^{H}\boldsymbol{H}_{\mathrm{E}})(\boldsymbol{w}s+\boldsymbol{n}_{a})+z_{\mathrm{E}} \tag{9}$$

R_{B} 和 R_{E} 分别为 Bob 的通信速率和 Eve 的通信速率，可以分别表达为：

$$R_{\mathrm{B}}=\log_{2}\left(1+\frac{|\boldsymbol{h}_{\mathrm{B}}^{H}\boldsymbol{w}|^{2}}{\boldsymbol{h}_{\mathrm{B}}^{H}\boldsymbol{R}_{\mathrm{AN}}\boldsymbol{h}_{\mathrm{B}}+\sigma_{\mathrm{B}}^{2}}\right) \tag{10}$$

$$R_{\mathrm{E}}=\log_{2}\left(1+\frac{|\boldsymbol{h}_{\mathrm{E}}^{H}\boldsymbol{w}|^{2}}{\boldsymbol{h}_{\mathrm{E}}^{H}\boldsymbol{R}_{\mathrm{AN}}\boldsymbol{h}_{\mathrm{E}}+\boldsymbol{\sigma}_{\mathrm{E}}^{2}}\right) \tag{11}$$

系统安全速率可以表达为：

$$R_{\mathrm{S}}(\boldsymbol{w},\boldsymbol{q})=[\boldsymbol{R}_{\mathrm{B}}-\boldsymbol{R}_{\mathrm{E}}]^{+} \tag{12}$$

其中：$\boldsymbol{h}_{\mathrm{B}}^{H}=\boldsymbol{h}_{\mathrm{AB}}^{H}+\boldsymbol{q}^{H}\boldsymbol{H}_{\mathrm{B}}$ 为 Alice-Bob 的等效信道，$\boldsymbol{h}_{\mathrm{E}}^{H}=\boldsymbol{h}_{\mathrm{AE}}^{H}+\boldsymbol{q}^{H}\boldsymbol{H}_{\mathrm{E}}$ 为 Alice-Eve 的等效信道，$\boldsymbol{R}_{\mathrm{AN}}=E\{\boldsymbol{n}_{a}\boldsymbol{n}_{a}^{H}\}$ 表示人工噪声的协方差。其中，$[x]^{+}=max(x,0)$。由于安全速率为一个非负数，若 $R_{\mathrm{B}}-R_{\mathrm{E}}\leqslant 0$，即窃听者信道质量强于合法通信方的信道质量，系统传输的通信信号无法保证不被窃听者截获，在这种情况下，由于此时的传输是不安全的，系统将自动停止传输通信信号。给定 Alice 的总功率 $P=P_{\mathrm{T}}+P_{\mathrm{A}}$，其中，$P_{\mathrm{T}}=\|\boldsymbol{w}\|^{2}$ 为通信信号传输功率，$P_{\mathrm{A}}=tr(R_{\mathrm{AN}})$ 为人工噪声功率。

本文假设系统能够获得合法通信方的准确 CSI，合法通信方的信道估计可以通过压缩感知[17]或者张量分解[18]等方法实现。然而，在实际中，窃听者 Eve 多是被动的并且尽力避免被合法通信方发现，不参与通信系统的信道估计，窃听者的位置和 CSI 通常难以获取，因此假设 Alice 已知 Eve 的 CSI 是不现实的。这意味着 Alice-Eve 的等效信道 $\boldsymbol{h}_{\mathrm{E}}^{H}$ 未知，所以此时无法通过最大化系统安全速率 R_{S} 的方式进行主被动波束赋形。在这种情况下，为提高系统的安全性能，一种有效的方法是在保证合法用户通信质量的前提下，最大程度减小通信信号向窃听者的泄漏[19-20]。具体来说，在满足 Bob 处 QoS 的约束下，通过主被动波束赋形最小化通信信号传输功率 P_{T}，这样系统就能够分配尽可能多的功率用来发送人工噪声 $\boldsymbol{n}_{a}$ 用来干扰窃听者，减少通信信号向窃听者的泄漏。另外，为了不干扰合法通信，人工噪声 $\boldsymbol{n}_{a}$ 需要与等效合法信道正交，即 $\boldsymbol{n}_{a}\perp\boldsymbol{h}_{\mathrm{B}}^{H}$。因此，优化问题可以表述为在 RIS 相移的恒模约束、合法用户 QoS 约束和总功率约束条件下的通信信号传输功率最小化，即：

$$\begin{aligned}(\mathrm{P1}):&\min_{w,q}\quad \|w\|^{2}\\ \text{s.t.}\quad &|q_{n}|=1,\quad \forall n=1,2,\cdots,N.\\ &\frac{|\boldsymbol{h}_{\mathrm{B}}^{H}\boldsymbol{w}|^{2}}{\sigma_{B}^{2}}\geqslant\gamma\\ &0\leqslant\|\boldsymbol{w}\|^{2}\leqslant P\end{aligned} \tag{13}$$

其中：γ 为 Bob 处的 QoS 约束。在（P1）中，RIS 相移矩阵中的每个元素均位于模为 1 的复圆上，该约束是非凸的；在 QoS 不等式约束的左侧，优化变量 $\boldsymbol{w}$ 和 $\boldsymbol{q}$ 互相耦合，这一约束也是非凸的。因此，（P1）是一个非凸优化问题，难以直接求解。

2　优化算法设计

在本节中，采用主被动波束赋形和人工噪声来增强基于 RIS 的无线通信系统的传输安全性能[19]。这一方法的核心是通信信号传输功率最小化（P1）。目前，问题（P1）通常采用半正定松弛算法求解，这一算法计算复杂度较高。为解决这一缺陷，提出了深度学习辅助的黎曼流形优化算法来解决问题（P1）。该方法受到黎曼流形梯度下降方法的启发，为了加速收敛，不同于经典的黎曼流形优化采用的基于人工设计的更新规则，采用深度神经网络在迭代过程中自适应地学习变量的更新规则，根据通用近似定理，DNN 的非线性特性可以发现新的更新规则[20-21]。所提方法的整体如图 2 所示。

2.1　通信信号功率最小化

对于问题（P1）中任何给定的相移 $\boldsymbol{q}$，波束赋形向量的最优解可以通过最大比传输（MRT，maximum ratio transmission）[14]获得。因此，对于任意给定的相移 $\boldsymbol{q}$，波束赋形向量的最优解可以表示为：

$$w^{*}=\sqrt{P_{\mathrm{T}}}\frac{(\boldsymbol{h}_{\mathrm{AB}}^{H}+\boldsymbol{q}^{H}\boldsymbol{H}_{\mathrm{B}})^{H}}{\|\boldsymbol{h}_{\mathrm{AB}}^{H}+\boldsymbol{q}^{H}\boldsymbol{H}_{\mathrm{B}}\|} \tag{14}$$

然后，将最优波束赋形向量 w^{*} 带入问题（P1），通信信号传输功率可以表达为：

$$P_{\mathrm{T}}^{*}=\frac{\gamma\sigma_{\mathrm{B}}^{2}}{\|\boldsymbol{h}_{\mathrm{AB}}^{H}+\boldsymbol{q}^{H}\boldsymbol{H}_{\mathrm{B}}\|^{2}} \tag{15}$$

因此，通信信号传输功率 P_{T} 最小化等效为 Alice-Bob 的等效信道增益 $\|\boldsymbol{h}_{\mathrm{AB}}^{H}+\boldsymbol{q}^{H}\boldsymbol{H}_{\mathrm{B}}\|^{2}$ 最大化。因此，问题（P1）可以等价地转化为，在满足 RIS 相移恒模约束的条件下最大化 Alice-Bob 的等效信道增益：

$$\begin{aligned}(\mathrm{P2}):&\max_{q}\|\boldsymbol{h}_{\mathrm{AB}}^{H}+\boldsymbol{q}^{H}\boldsymbol{H}_{\mathrm{B}}\|^{2}\\ \text{s.t.}\quad &|q_{n}|=1,\quad \forall n=1,2,\cdots,N.\end{aligned} \tag{16}$$

定义问题（P2）的目标函数为 $f(\boldsymbol{q})=\|\boldsymbol{h}_{\mathrm{AB}}^{H}+\boldsymbol{q}^{H}\boldsymbol{H}_{\mathrm{B}}\|^{2}$，提出深度学习辅助的黎曼流形优化算法来处理问题（P2）。对于问题（P2），恒模约束难以

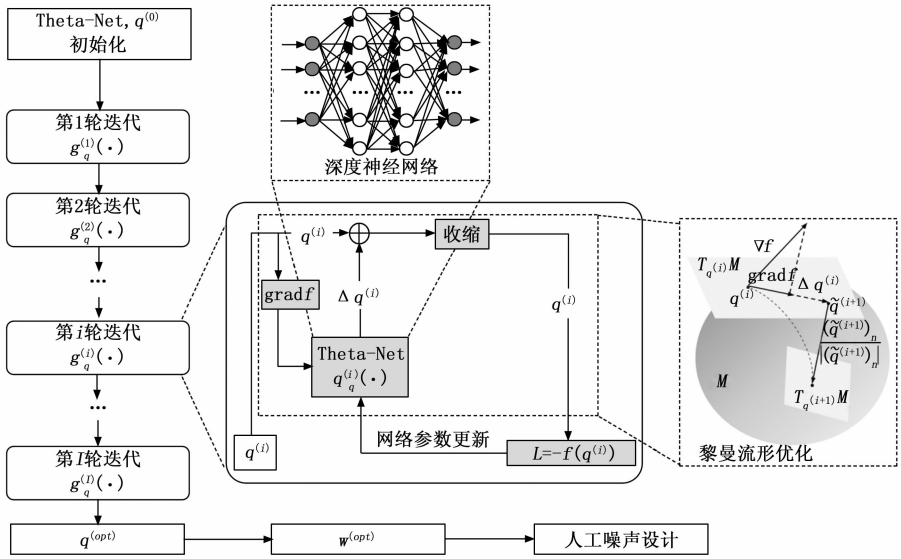

图 2 深度学习辅助的黎曼流形优化算法框图

处理，而黎曼流形优化是处理此类问题的一种非常有效的解法。其中，RIS 每个单元的反射系数 q_n 都可以视为是一个复圆流形，则问题（P2）可以视为 N 维黎曼复圆流形上的无约束优化，即 $CCM=\{\boldsymbol{q}\in\boldsymbol{C}^{N\times 1}:|q_1|=|q_1|=\cdots=|q_N|=1\}$。对目标函数进行求导，可以得到目标函数 f 在点 $\boldsymbol{q}^{(i)}$ 的欧几里得梯度为：

$$\nabla_{\boldsymbol{q}^{(i)}} f=2\boldsymbol{H}_{\mathrm{B}}(\boldsymbol{h}_{\mathrm{AB}}+\boldsymbol{H}_{\mathrm{B}}^{H}\boldsymbol{q}^{(i)}) \tag{17}$$

黎曼梯度定义为欧几里得梯度在切空间上的正交投影。则目标函数 f 在点 $\boldsymbol{q}^{(i)}$ 的黎曼梯度可以表示为：

$$\mathrm{grad}_{\boldsymbol{q}^{(i)}} f=\nabla_{\boldsymbol{q}^{(i)}} f-\mathrm{Re}\{\nabla_{\boldsymbol{q}^{(i)}} f\circ\boldsymbol{q}^{(i)}\}\circ\boldsymbol{q}^{(i)} \tag{18}$$

其中：$\mathrm{Re}\{\cdot\}$ 表示为取实部操作，$\circ$ 为 Hadamard 乘积，即 $(\boldsymbol{A}\circ\boldsymbol{B})_{ij}=\boldsymbol{A}_{ij}*\boldsymbol{B}_{ij}$。在传统的流形优化算法[14]中，更新步长和方向由人工设计的规则确定（例如：Polak-Ribiere 准则）。与此不同的是，所提出的算法利用神经网络 Theta-Net 自适应地学习黎曼梯度更新步长。Theta-Net 为轻量级 DNN，具有 3 个隐藏层，每个隐藏层包含 32 个神经元，神经元的激活函数采用线性整流函数（ReLU，rectified linear unit），表达式为：

$$\mathrm{ReLU}(x)=max(0,x) \tag{19}$$

ReLU 函数的非线性性质使得网络能够学习和表示复杂的非线性映射，从而提高模型的表达能力，进而更好地通过数据驱动的方式自适应地学习黎曼梯度的更新步长。此外，相对于 Sigmoid 或 Tanh 激活函数，ReLU 激活函数在输入大于 1 时，梯度恒为 1，能够更好地缓解梯度消失和梯度爆炸问题。由于黎曼梯度 $\mathrm{grad}_{\boldsymbol{q}^{(i)}} f$ 是一个 N 维复数向量，而神经网络无法处理复数数据。因此，在输入神经网络之前，需要对黎曼梯度 $\mathrm{grad}_{\boldsymbol{q}^{(i)}} f$ 进行实部与虚部分离：

$$\mathrm{grad}_{\boldsymbol{q}^{(i)}} f=\{\mathrm{Re}[\mathrm{grad}_{\boldsymbol{q}^{(i)}} f]\quad \mathrm{Im}[\mathrm{grad}_{\boldsymbol{q}^{(i)}} f]\} \tag{20}$$

完成实部与虚部分离后，黎曼梯度转换为神经网络可以处理的维度为 $2N$ 的实数向量，将此 $2N$ 维实数向量输入 Theta-Net，Theta-Net 的输出在进行实部与虚部合并后生成基于该黎曼梯度的更新步长，该过程如图 3 所示。Theta-Net 的输入和输出维度均为 $2N$。将 $\boldsymbol{q}^{(i)}$ 与神经网络的输出相加得到这一轮的 RIS 相移的更新，这一过程可以表示为：

$$\tilde{\boldsymbol{q}}^{(i+1)}=\boldsymbol{q}^{(i)}+\boldsymbol{g}_q^{(i)}[\mathrm{grad}_{\boldsymbol{q}^{(i)}} f;\theta_{\boldsymbol{q}^{(i)}}^{(i)}] \tag{21}$$

其中：$\theta_{\boldsymbol{q}^{(i)}}^{(i)}$ 为 Theta-Net 的网络参数，$g_q^{(i)}$ 为 Theta-Net 对应的隐函数，该函数就是基于神经网络的变量更新规则。

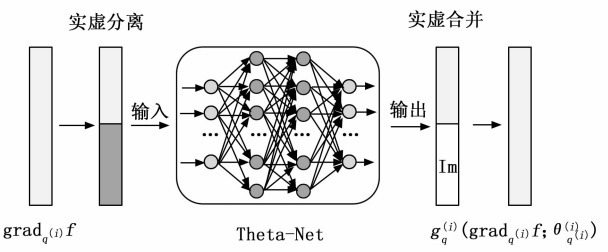

图 3 基于神经网络 Theta-Net 的变量更新

在完成变量更新后，$\tilde{\boldsymbol{q}}^{(i+1)}$ 未必满足恒模约束，需要将不在复圆流形上的点收缩至复圆流形上：

$$\tilde{\boldsymbol{q}}^{(i+1)}=\frac{[\tilde{\boldsymbol{q}}^{(i+1)}]_n}{|[\tilde{\boldsymbol{q}}^{(i+1)}]_n|} \tag{22}$$

最后，利用无监督学习来定义损失函数，（P2）的优化目标是信道增益 f 最大化，因此定义损失函数为目标函数 f 的相反数：

$$L=-f(\boldsymbol{q}) \tag{23}$$

在第 i 次更新完成之后，损失函数进行反向传播求

出损失函数关于网络参数的导数，然后根据自适应矩估计（Adam，adaptive moment estimation）优化器[22]对网络参数进行更新：

$$\theta_q^{(i+1)} = \theta_q^{(i)} + \alpha_q \cdot \mathrm{Adam}[\nabla_{q^{(i)}} L, \boldsymbol{\theta}_q^{(i)}] \tag{24}$$

其中：α_q 是 Adam 优化器的学习率。传统深度学习方法直接将迭代求解过程完全用神经网络替代，通过数据驱动的方法训练网络使之能够完成从信道矩阵到波束赋形向量或者 RIS 相移矩阵的非线性映射，此类方法需要大量数据进行预训练。所提出的算法保留了传统黎曼流形优化的迭代结构，神经网络并不是完成从信道矩阵到相移矩阵的映射，而是完成从黎曼梯度到更新量的映射，网络本身可以视为隐式更新规则，输出为基于此更新规则的变量更新量。此外，Theta-Net 并不是预先基于数据集离线训练的，而是随着迭代的过程动态更新，DNN 的训练过程即是优化问题的求解过程，优化问题的求解过程可以看作为每一个优化问题的样本训练一个专用 DNN。该算法是一种具有可解释性的即插即用方法，避免了传统深度学习方法依赖大量数据的缺点。

目标函数在复圆流形上可能存在多个局部最优解。传统黎曼梯度下降方法（如文献［14］）依赖人工设计的更新规则，易因更新方向选择不当而陷入局部最优。为克服这一局限，本文所提出的算法融合深度学习的自适应学习能力，Theta-Net 通过数据驱动方式学习更新规则，并通过损失函数动态更新网络参数以达到在迭代中动态调整搜索路径的效果，相对于传统黎曼梯度算法，这种方式能够有效降低陷入局部最优解的概率。所提算法如下所示：

算法 1：深度学习辅助的黎曼流形优化算法

输入：$M, N, \gamma, \boldsymbol{h}_{\mathrm{AB}}$ 和 $\boldsymbol{H}_{\mathrm{B}}$

初始化：$\boldsymbol{q}^{(0)}$ 和网络参数

for $i=1:I$

根据式(17)～(18)计算黎曼梯度

实部虚部分离(20)

根据式(20)～(21)计算更新步长

根据式(22)计算更新后的相移

根据式(23)计算损失函数

根据式(24)更新网络参数

end for

根据式(14)计算波束赋形向量

输出：w 和 q

下面给出算法的计算复杂度分析。由于基于 MRT 传输得到最优波束赋形向量只在最后执行一次，因此这部分运算对整体计算复杂度无明显贡献。算法复杂度主要由网络 Theta-Net 的前向传播和网络参数更新产生。对于不同规模的 N，Theta-Net 的输入和输出层神经元个数均为 $2N$，隐藏层的神经元个数不变，因此对于不同的 N，网络参数量与 N 呈线性增长，由于神经网络的前向传播和参数更新均只涉及矩阵运算，不涉及复杂的矩阵求逆等操作，所以每一次迭代网络前向传播和参数更新这两部分的复杂度均与 N 呈线性关系，假设总迭代次数为 I，则算法的总体复杂度为 $O[I(kN+c)]$，其中，c 是常量，k 是斜率，由于深度学习硬件高效的并行运算机制，k 是一个很小的常量，可以被忽略，c 是一个固定的常量，该常量与系统硬件性能有关，无法忽略。因此，实际上，该算法的复杂度可以视为 $O(I)$。即算法复杂度只与迭代次数有关。

2.2　人工噪声设计

通过上述方法得到最小化的通信信号传输功率后，剩余功率 P_{A} 被用来发送人工噪声。因为窃听者 CSI 完全未知，所以无法通过优化人工噪声协方差 $\boldsymbol{R}_{\mathrm{AN}}$ 的方式来最大化安全速率。

为便于计算，定义 $\boldsymbol{H}_{\mathrm{b}} = \boldsymbol{h}_{\mathrm{B}}\boldsymbol{h}_{\mathrm{B}}^H$，$\boldsymbol{H}_{\mathrm{b}}$ 的秩 $rank(\boldsymbol{H}_{\mathrm{b}}) = 1$，由于 Alice 配备了多天线，根据秩－零化度定理，$\boldsymbol{H}_{\mathrm{b}}$ 零空间的维度为 $M-1$，下面对 $\boldsymbol{H}_{\mathrm{b}}$ 进行特征值分解：

$$\boldsymbol{H}_{\mathrm{b}} = \boldsymbol{U}\boldsymbol{\Lambda}\boldsymbol{U}^H \tag{25}$$

其中：$\boldsymbol{\Lambda}$ 为对角矩阵，对角阵的每个元素为 $\boldsymbol{H}_{\mathrm{b}}$ 的特征值。由于 $\mathrm{rank}(\boldsymbol{H}_{\mathrm{b}}) = 1$，因此只含有一个非零特征值；$\boldsymbol{U}$ 为酉矩阵，其列向量为 $\boldsymbol{H}_{\mathrm{b}}$ 的特征向量，包括一个非零特征值对应的一个特征向量和 $M-1$ 个零特征值对应的特征向量，这 $M-1$ 个零特征值对应的特征向量构成了 $\boldsymbol{H}_{\mathrm{b}}$ 的零空间。记 $\boldsymbol{U}_{\mathrm{AN}}$ 为零空间对应的特征向量矩阵，满足 $\boldsymbol{H}_{\mathrm{b}}\boldsymbol{U}_{\mathrm{AN}} = 0$，人工噪声 $\boldsymbol{n}_a = \boldsymbol{U}_{\mathrm{AN}}z$，这确保了人工噪声与合法信道正交，其中，$z \sim CN(0, \sum)$，$\sum = E\{zz^H\}$ 为复高斯变量 z 的协方差矩阵。由于采用等功率分配策略在零空间的每个维度上传输人工噪声，因此 $\sum$ 可以表达为：

$$\sum = \frac{P_A}{\boldsymbol{M}-1}\boldsymbol{I}_{M-1} \tag{26}$$

因此人工噪声的协方差矩阵可以表达为：

$$\boldsymbol{R}_{\mathrm{AN}} = E\{\boldsymbol{U}_{\mathrm{AN}}z(\boldsymbol{U}_{\mathrm{AN}}^H\boldsymbol{z})^H\} = \boldsymbol{U}_{\mathrm{AN}}E\{zz^H\}\boldsymbol{U}_{\mathrm{AN}}^H = \frac{P_A}{M-1}\boldsymbol{U}_{\mathrm{AN}}\boldsymbol{U}_{\mathrm{AN}}^H \tag{27}$$

3　实验结果

3.1　仿真参数

本节中对提出的算法进行仿真实验验证。Alice 的天线数 $M = 16$，如图 4 所示，Alice、Bob 和 RIS 的坐标分别为（0 m，0 m）、（165 m，20 m）和（200 m，0 m）。假设系统中合法用户的 CSI 均是已知的，窃听者 Eve 位于（160 m，30 m），Eve 的 CSI 不用于主被动波束赋形和人工噪声设计，仅用于评估所提出方案对于系统安全性能提升的有效性。

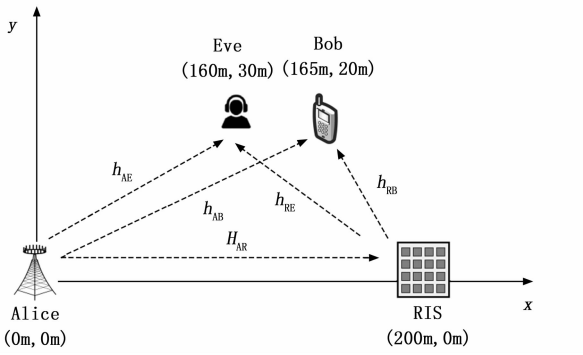

图 4 基于 RIS 的物理层安全传输仿真环境

L 是与收发端相对距离和载波频率有关的自由空间路径损耗，为确保模型更接近与真实环境，自由空间路径损耗采用 3 GPP TR 36.814 v9.2.0 标准中的 Umi (Urban Micro) 场景模型，该模型能够准确反映实际环境的传播特性。

Alice-Bob 和 Alice-Eve 直射链路建模为瑞利信道，莱斯因子设置为 0；Alice-RIS、RIS-Bob 和 RIS-Eve 链路建模为莱斯信道，设定莱斯因子 $\kappa = 10$，信道矩阵由阵列响应向量建模的视距分量和多径衰落分量组成。系统仿真参数总结如表 2 所示。

表 2 仿真参数设置

参数配置	参数数值
载波频率 f_C	2.4 GHz
天线间距	0.5 λ
传输带宽	180 kHz
噪声功率谱密度	−170 dBm/Hz
$\boldsymbol{h}_{AB}$ 和 $\boldsymbol{h}_{AE}$ 的路径损耗/dB	$36.7\lg d + 22.7 + 26\lg f_C$
$\boldsymbol{H}_{AR}$、$\mathbf{h}_{RB}$ 和 $\boldsymbol{h}_{RE}$ 的路径损耗/dB	$22.0\lg d + 28.0 + 20\lg f_C$

仿真环境的软件配置如下：编程语言为 Python 3.7，深度学习开源库为 Pytorch 1.8；仿真环境的硬件配置如下：CPU 为 Intel® Core™ i9-10980XE CPU @ 3.00 GHz，运行内存 256 GB，GPU 为 NVIDIA GeForce RTX 3 090。Theta-Net 的是输入和输出层的维数均为 $2N$，具有 3 个隐藏层，每个隐藏层均有 32 个神经元，激活函数均为 ReLU 函数。更新网络参数所采用的 Adam 优化器的学习率设置为 0.1。为避免信道小尺度衰落对算法性能评估的影响，每一条仿真曲线均为 100 个独立信道衰落的平均值。选取了两个现有的优化算法作为对比算法，这两个算法的基本原理如下：

流形优化算法[14]：采用典型的流形优化算法来解决 (P1)，其中相移的优化通过典型的斜流形算法来解决，采用基于 Polak-Ribiere 参数的变量更新准则。

半正定松弛算法[15]：通过半正定松弛技术解决相移的非凸约束，将问题转化为半正定规划问题，并通过内点法解决，之后通过高斯随机化生成满足恒模约束的解来解决。

所提出的算法和两种对比算法的计算复杂度总结如表 3 所示。

表 3 计算复杂度比较

算法	复杂度
所提出的算法	$O(I)$
半正定松弛算法	$O(N^6)$
流形优化算法	$O(N^2)$

3.2 仿真实验

首先给出所提出的算法的收敛性能比较，如图 5 所示。Alice 的天线数量均设定为 16，从图中可以看到，所提出的算法不到 5 轮迭代即可收敛，并且 N 越大时需要收敛的迭代次数越多，这是因为随着 N 的增大，优化问题的维数变大，算法的搜索空间变大，需要更多的迭代次数收敛。与此同时，给出了算法的运行时间比较，如图 6 所示。从图中可以看出，半正定松弛算法在求解过程中由于采用相对耗时的内点法来求解半正定规划问题，并且需要高斯随机化将生成的解满足非凸约束，因此它的耗时是最高的，运行时间不低于 1 s，该算法的实时性较差，无法满足 RIS 实时调控的需求；而所提出的算法由于采用了深度学习方法，并且能够利用硬件的并行计算性能，因此它的用时相对较低，具体来说，运行时间维持在 0.06 s 左右，能够达到与流形优化算法相当的运行耗时，在 RIS 元件个数为 128 时，运行时间仅为半正定松弛算法的 5%，计算复杂度降低至少一个数量级。此外，随着 RIS 元件规模的增大，运行时间的增长极为缓慢，运行时间的增长与前述计算复杂度分析相吻合，验证了计算复杂度分析的合理性。

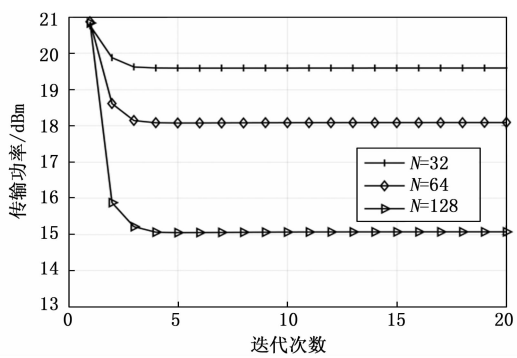

图 5 算法收敛性

下面验证了人工噪声信号与合法信道的正交性，根据 3.1 节所述仿真参数生成了 100 个合法信道的信道实现样本，通过计算人工噪声信号与合法信道的内积来验证人工噪声与合法信道的正交性。如图 7 所示，人工噪声信号与合法信道的内积几乎为 0，均处于 10^{-9} 数量级

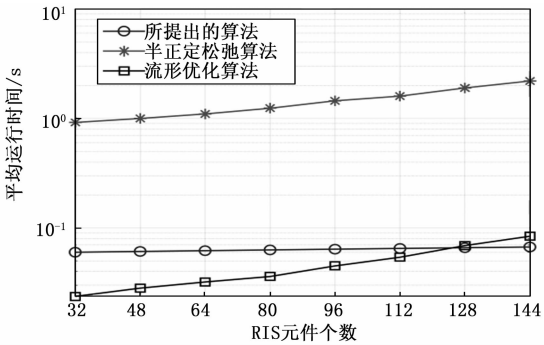

图 6　不同算法平均运行时间

内，这表明所生成的人工噪声信号与合法信道具有良好的正交性。

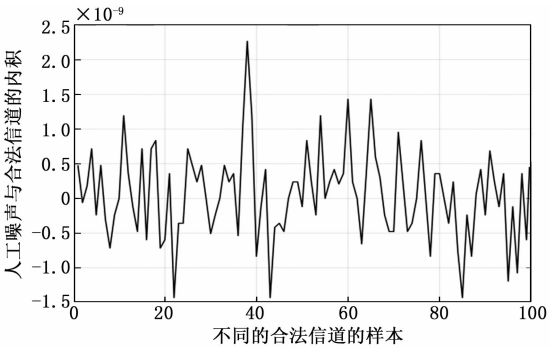

图 7　人工噪声与合法信道的正交性验证

在 Bob 处 QoS 约束不同的情况下所提出的方法达到的系统安全性能的分析，如图 8 所示。其中，Alice 的天线数 $M = 16$，总功率为 $P = 10$ dBm。从图中可以看出，随着 QoS 的增长，3 种算法所得出的系统安全速率均呈现先上升后下降的趋势，在 QoS 为 21 dB 时，所提出的算法达到的系统速率达到最高值 6.24 bps/Hz，这一数值与半正定松弛算法达到了几乎相同的性能，而传统的流形优化算法在 QoS 为 18 dB 时达到最高点，最高安全速率为 5.25 bps/Hz。安全速率先上升后下降是因为，当 QoS 较低时，通信信号的传输功率也较低，系统可以分配足够的剩余功率用来干扰窃听者，而随着 QoS 的增长，系统需要分配更多的通信信号传输功率来满足 Bob 处的 QoS 约束，分配给人工噪声的功率也随之降低，系统通信信号与人工噪声功率分配如图 9 所示。从图中可以看出，当 QoS 为 24 dB 时，分配给人工噪声的功率比例超过了通信信号传输功率，此时，系统无法分配足够的人工噪声功率来干扰窃听者，因此当 QoS 大于 21 之后，系统安全速率开始下降。当 QoS 为 27 时，通信信号传输功率占比达到几乎 100%，分配给人工噪声的功率几乎为零，当 QoS 再增长时，系统便无法满足合法通信方的通信质量。此外，从图 8 中可以看出，所提出的算法能够达到与半正定松弛算法几乎一样的安全速率，并且能够获得比流形优化更高的安全速率，并且保持了相对较低的运算复杂度。这是因为，一方面，相对于传统的基于人工设计的变量更新规则，神经网络的自适应学习能力能够找到更高质量的局部最优解；另一方面，与半正定松弛算法相比，神经网络的低复杂度特性和 GPU 硬件的并行计算机制能够带来更低的运算时间开销，具有广阔的应用前景。

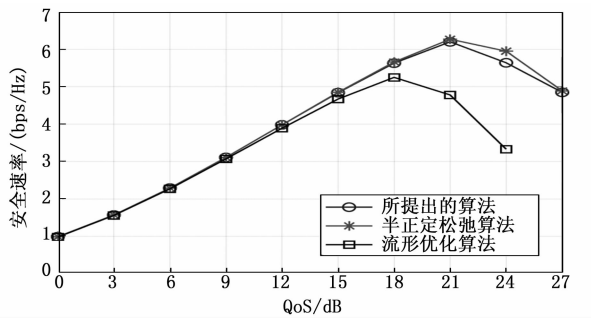

图 8　安全速率与 QoS 的关系曲线

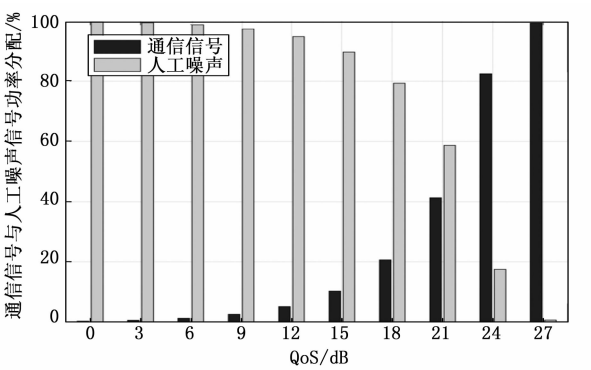

图 9　所提出的方法的通信信号传输功率/人工噪声功率分配与 QoS 的关系比较

进一步地，分别给出了所提出的方法的 Bob 和 Eve 的通信速率随 QoS 的变化情况，如图 10 所示。从图中可以看出，随着 QoS 的提高，Bob 的通信速率逐渐提升；在 QoS 小于等于 18 dB 时，由于系统能够分配足够的功率来压制窃听者对通信信号的截获，因此在这一范围内，Eve 的通信速率是极低的；当 QoS 大于 18 dB 时，Eve 处的通信速率开始明显变大，这意味着由于人工噪声功率的降低，人工噪声不足以遏制通信信号向窃听者方向的泄漏；当 QoS 为 21 dB 时，Bob 的通信速率与 Eve 的通信速率的差值达到最大，也就是安全速率达到最大值，当 QoS 继续变大时，Bob 的通信速率与 Eve 的通信速率差值变小，安全速率逐渐降低，与图 8 所展示的趋势一致。

不同功率分配策略下系统安全速率的变化情况如图 11 所示。其中，“随机功率分配策略”将人工噪声功率随机地分配在合法信道零空间的所有维度中；“人

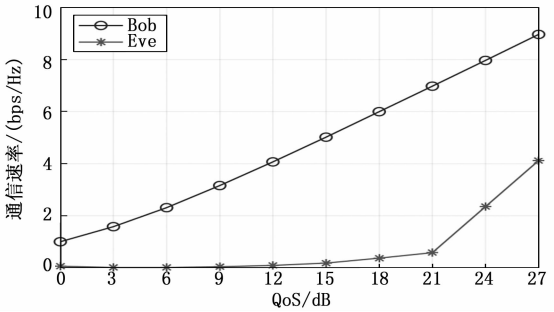

图 10 Bob 和 Eve 的通信速率与 QoS 的关系曲线

工噪声不满足零空间约束”中，人工噪声处于信道空间和零空间中，不严格处于信道的零空间中。从图 11 中可以看出，等功率分配策略在 QoS 较低的时候略微优于随机功率分配策略，而人工噪声不严格处于信道零空间约束时，人工噪声在干扰窃听者的同时也会对合法通信产生干扰，因此这种条件下的系统安全速率是最低的。

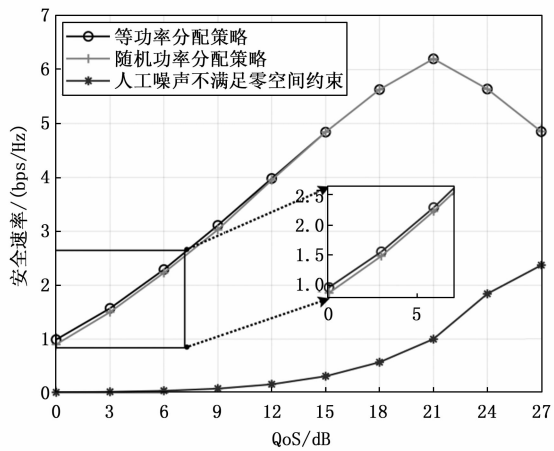

图 11 不同人工噪声功率分配策略对比

系统安全速率随 RIS 元件个数的变化曲线如图 12 所示。从图中可以看出，随着 RIS 元件个数的增加，系统安全速率也增加。这是因为，随着 RIS 元件个数的增加，RIS 具有更强的信道调控能力，RIS 反射链路的波束赋形增益变大，为达到相同的 QoS 所需要的通信信号传输功率减小，用于干扰窃听者的人工噪声功率增大，系统安全速率因此增大。

最后，分析了 Eve 位于不同位置时系统的安全速率。如图 13 所示，Alice、Bob 和 RIS 的坐标分别为（0 m，0 m）、（200 m，10 m）和（100 m，20 m），Eve 的位置为（x，10 m）。Eve 位于不同位置时系统的安全速率如图 14 所示，从图中可以看出，相对于没有采用人工噪声的方案，所提出的方案无论 Eve 的位置在哪里，系统的安全速率均可以达到 8.70 bps/Hz 左右，而没有人工噪声的方案在 x 处于［0 m，25 m］范围内时，系统安全速率为零，随着 x 的增长，系统安全速率开始缓慢增加，但仍然小于所提出的方案。这是因为，当 x 位于［0 m，25 m］范围内时，Eve 位于 Alice 的主波束范围内，Eve 的信道质量强于 Bob 的信道质量，系统通信信号向 Eve 有大量泄漏，此时系统安全速率为零，随着 Eve 的移动逐渐避开了 Alice 的主波束范围，Eve 能截获的信号逐渐降低。而所提出的方案由于在发送信号内引入了人工噪声，减小了信号向窃听者的泄漏。

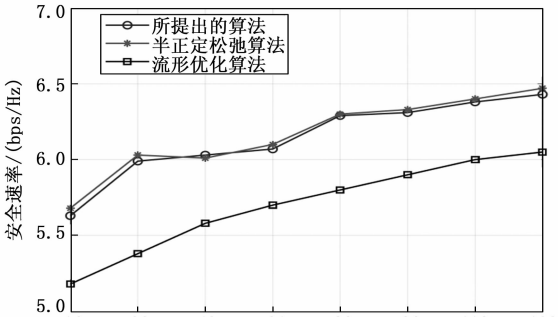

图 12 安全速率与 RIS 元件个数的关系曲线

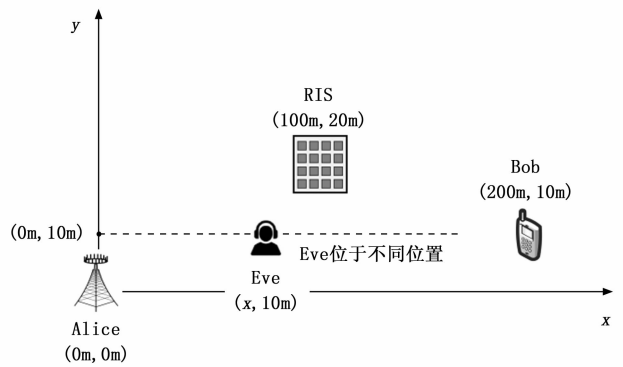

图 13 Eve 位于不同位置

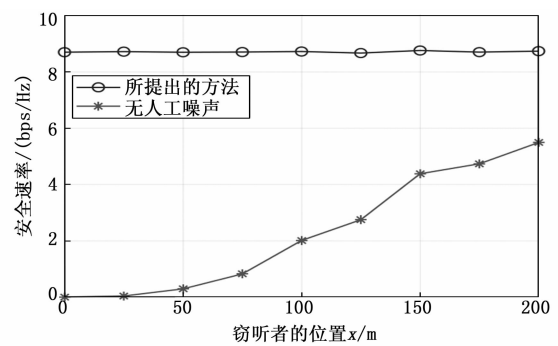

图 14 安全速率与窃听者位置的关系曲线

4 结束语

本文对基于智能超表面的物理层安全传输技术进行了研究。不同于现有研究通常认为窃听者 CSI 已知的假设，本文研究了窃听者 CSI 完全未知条件下智能超表面

的安全传输。首先通过主被动波束赋形在满足合法用户通信质量的约束下最小化通信信号传输功率，然后将剩余功率用于发送人工噪声以干扰潜在的窃听者；提出了一种深度学习辅助流形优化方法来解决这一功率分配问题。实验结果表明，所提出的方法在达到几乎相同的安全速率的前提下，计算复杂度降低不小于一个数量级。未来将进一步研究合法用户 CSI 存在误差情况下的鲁棒波束赋形技术，提升算法对 CSI 误差的鲁棒性；另外，将进一步开展基于多个智能超表面的安全传输技术。

参考文献：

[1] HONG Y，LAN P，KUO C. Enhancing physical-layer secrecy in multiantenna wireless systems：an overview of signal processing approaches [J]. IEEE Signal Processing Magazine，2013，30 (5)：29－40.

[2] SHANNON C. Communication theory of secrecy systems [J]. The Bell System Technical Journal，1949，28 (4)：656－715.

[3] CUI T，QI M，WAN X，et al. Coding metamaterials，digital metamaterials and programmable metamaterials [J]. Light：Science & Applications，2014，3 (10)：e218.

[4] DI R，ZAPPONE A，DEBBAB M，et al. Smart radio environments empowered by reconfigurable intelligent surfaces：How it works，state of research，and the road ahead [J]. IEEE Journal on Selected Areas in Communications，2020，38 (11)：2450－2525.

[5] WU Q，ZHENG B，YOU C，et al. Intelligent surfaces empowered wireless network：Recent advances and the road to 6G [J]. Proceedings of the IEEE，2024，112 (7)：724－763.

[6] CUI M，ZHANG G，ZHANG R. Secure wireless communication via intelligent reflecting surface [J]. IEEE Wireless Communications Letters，2019，8 (5)：1410－1414.

[7] FENG K，LI X，HAN Y，et al. Physical layer security enhancement exploiting intelligent reflecting surface [J]. IEEE Communications Letters，2020，25 (3)：734－738.

[8] GUAN X，WU Q，ZHANG R. Intelligent reflecting surface assisted secrecy communication：Is artificial noise helpful or not? [J]. IEEE Wireless Communications Letters，2020，9 (6)：778－782.

[9] CHEN Z，GUO Y，ZHANG P，et al. Physical layer security improvement for hybrid RIS-assisted MIMO communications [J]. IEEE Communications Letters，2024，28 (11)：2493－2497.

[10] YANG H，XIONG Z，ZHAO J，et al. Deep reinforcement learning-based intelligent reflecting surface for secure wireless communications [J]. IEEE Transactions on Wireless Communications，2020，20 (1)：375－388.

[11] YU X，XU D，SUN Y，et al. Robust and secure wireless communications via intelligent reflecting surfaces [J]. IEEE Journal on Selected Areas in Communications，2020，38 (11)：2637－2652.

[12] CHEN T，LI N，TAO X. Statistical CSI based robust and secure transmission via reconfigurable intelligent surfaces with eavesdropper location uncertainty [C] //2024 IEEE 35th International Symposium on Personal，Indoor and Mobile Radio Communications (PIMRC). IEEE，2024：1－6.

[13] BAI J，WANG H，LIU P. Robust RIS-aided secrecy transmission with location optimization [J]. IEEE Transactions on Communications，2022，70 (9)：6149－6163.

[14] WANG H，BAI J，DONG L. Intelligent reflecting surfaces assisted secure transmission without eavesdropper′s CSI [J]. IEEE Signal Processing Letters，2020，27：1300－1304.

[15] WU Q，ZHANG R. Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming [J]. IEEE Transactions on Wireless Communications，2019，18 (11)：5394－5409.

[16] WANG J，WANG S，HAN S，LI C. Intelligent reflecting surface secure backscatter communication without Eavesdropping CSI [J]. IEEE Communications Letters，2023，27 (6)：1496－1500.

[17] ABDALLAH A，CELIK A，MANSOUR M，et al. RIS-aided mmwave MIMO channel estimation using deep learning and compressive sensing [J]. IEEE Transactions on Wireless Communications，2023，22 (5)：3503－3521.

[18] WEI L，HUANG C，ALEXANDROPOULOS C，et al. Channel estimation for RIS-empowered multi-user MISO wireless communications [J] IEEE Transactions on Communications，2021，69 (6)：4144－4157.

[19] BOYD S P，VANDENBERGHE L. Convex optimization [M]. Cambridge University Press，2004.

[20] YANG Z，XIA J，LUO J，et al. A learning-aided flexible gradient descent approach to MISO beamforming [J]. IEEE Wireless Communications Letters，2022，11 (9)：1895－1899.

[21] CHEN T，CHEN X，CHEN W，et al. Learning to optimize：A primer and a benchmark [J]. Journal of Machine Learning Research，2022，23 (189)：1－59.

[22] KINGMA D，BA J. Adam：a method for stochastic optimization [J]. Arxiv Preprint Arxiv：1412.6980，2014.