

非正交多址系统中基于信道估计误差补偿的物理层安全方案

邱超圣^{1,2,3}, 徐大同^{1,2,3}

(1. 河南工业大学粮食信息处理与控制教育部重点实验室, 河南 郑州 450001;

2. 河南省粮情智能监测与应用工程研究中心, 河南 郑州 450001;

3. 河南工业大学信息科学与工程学院, 河南 郑州 450001)

摘要: 非正交多址接入作为6G通信的关键技术, 通过共享时频和空间资源, 有效提高了资源利用率。然而, 在基于功率域的NOMA系统中, 连续干扰消除技术的应用可能引发用户隐私信息被窃听的安全问题。为解决这一问题, 学界已提出多种方案, 但这些方案通常依赖足够准确的信道状态信息, 若信道估计精度不足, 则其性能往往难以达到预期。为此, 提出一种在信道估计存在误差的条件下基于估计误差补偿的物理层安全方案。首先通过低复杂度的额外估计实现对信道估计误差的补偿, 然后基于补偿后获得的更准确的信道状态信息重新设计收发机。仿真结果表明, 所提方案在不同信道估计误差和信噪比条件下均能显著提高系统的安全传输速率和传输可靠性。该方案为信道估计存在误差场景下的物理层安全问题提供了一种可行的解决办法。

关键词: 物理层安全; 非正交多址接入; 信道估计; 预编码; 串行干扰消除

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2026014

Physical layer security scheme based on channel estimation error compensation in non-orthogonal multiple access systems

Qiu Chaosheng^{1,2,3}, Xu Datong^{1,2,3}

1. Key Laboratory of Grain Information Processing and Control, Ministry of Education,
Henan University of Technology, Zhengzhou 450001, China

2. Henan Engineering Research Center of Grain Condition Intelligent Detection and Application,
Henan University of Technology, Zhengzhou 450001, China

3. College of Science and Engineering, Henan University of Technology, Zhengzhou 450001, China

Abstract: Non-orthogonal multiple access (NOMA) has been regarded as a key enabling technology for sixth-generation (6G) communications, since resource utilization was significantly enhanced by allowing multiple users to share the same time-frequency and spatial resources. However, in power-domain NOMA systems, user privacy information may be eavesdropped due to the application of successive interference cancellation, which introduces potential security vulnerabilities. To address this issue, various physical layer security schemes have been proposed in the literature, while their performance was highly dependent on sufficiently accurate channel state information

收稿日期: 2025-07-04; 修回日期: 2025-09-22

通信作者: 徐大同, xdtstc@163.com

基金项目: 河南省科技攻关计划项目(No.212102310296); 粮食信息处理与控制教育部重点实验室开放基金课题(No.KFJJ-2020-115)

Foundation Items: Henan Province Science and Technology Key Project (No.212102310296), Open Fund Project of Key Laboratory of Grain Information Processing and Control, Ministry of Education (No.KFJJ-2020-115)

(CSI). When channel estimation accuracy was insufficient, the achievable security performance often failed to meet expectations. To overcome this limitation, a physical layer security scheme based on channel estimation error compensation was proposed under imperfect CSI conditions. First, channel estimation errors were compensated through an additional low-complexity estimation process. Then, the transceiver was redesigned based on the more accurate CSI obtained after error compensation. Simulation results demonstrated that the proposed scheme significantly improved the secrecy rate and transmission reliability under different levels of channel estimation errors and signal-to-noise ratio. This scheme now provides a feasible solution to the physical layer security problem in scenarios where channel estimation errors exist.

Keywords: physical layer security, non-orthogonal multiple access, channel estimation, precoding, successive interference cancellation

0 引言

非正交多址接入 (non-orthogonal multiple access, NOMA) 作为 6G 通信的关键技术之一, 能够有效应对海量用户接入的挑战^[1]。它允许多个用户在相同的时间、频率和空间资源上复用通信, 从而显著提升频谱效率^[2]。根据资源复用维度的不同, NOMA 可分为功率域、码域等分支。其中, 功率域 NOMA 通过对发射功率的非正交分配来区分用户, 能够有效提高资源利用率, 从而满足 6G 网络对广域覆盖与大规模连接的需求^[3]。在 NOMA 系统中, 接收端通常采用连续干扰消除 (successive interference cancellation, SIC) 技术获取信息, 然而, SIC 过程中潜在的相互解码行为可能会泄露用户的隐私信息。虽然可以通过上层加密机制进行保护, 但是高度的非正交复用及用户间互相提取信息的行为会显著增加密钥分发与管理的复杂度。在此背景下, 物理层安全 (physical layer security, PLS) 技术作为一种补充或独立的安全增强手段, 为 NOMA 系统提供了天然的物理层防窃听能力。

1 相关工作

现有的 PLS 设计, 特别是针对 NOMA 系统的设计, 已涌现出多种方案。在中继协作方面, Guo 等^[4]考虑当存在外部窃听用户时引入具有能量收集功能的全双工协作中继, 并分析了系统的遍历保密速率的下界和用户的近似保密中断概率; 张延良等^[5]提出一种基于修改转发中继的 PLS 传输方案, 中继对解码信息进行修改后再转发, 避免合法信息泄露到窃听节点; Feng 等^[6]提出一种两级安全中继选择方案, 并基于安全中断

概率对该方案进行了评估。结果表明, 在低至中等发射功率及差异化保密需求条件下, 该方案相较于传统正交多址接入 (OMA) 方案具有显著的性能优势。在天线与用户选择方面, Yu 等^[7]在毫米波大规模多输入多输出 (multiple input multiple output, MIMO) NOMA 系统中, 联合设计波束成形和天线选择策略, 在满足基站最大发射功率和天线选择约束的同时, 最大化系统的安全和速率。在功率和载波分配方面, Thapar 等^[8]指出在不可信场景中传统 NOMA 的解码顺序无法保障每个用户的隐私安全, 并提出了一种新的功率分配与解码顺序策略, 显著提升了系统保密速率; Su 等^[9]提出由近端用户充当放大和转发中继, 协助转发远端用户信息, 从而保障远端用户的安全。在人工噪声 (artificial noise, AN) 注入方面, Jia 等^[10]为保障系统实现正向安全速率, 提出了结合 AN 的安全传输方案; Zhao 等^[11]根据不同的发射功率约束设计了两种 AN 注入方案, 均能有效保障 NOMA 网络的信息安全。在信号处理方面, Horiike 等^[12]将混沌 MIMO 原理引入 NOMA, 使多个用户的混沌调制信号在功率域叠加后通过同一子载波传输; Zhao 等^[13]针对 MIMO 双向不可信中继系统, 引入保密能效指标并建立其最大化预编码设计模型, 通过分数规划与交替优化等技术解决高维非凸优化问题, 有效提升了系统的安全能效性能; Yang 等^[14]设计了一种预编码联合优化方案, 通过人工干扰最大化多个用户的总安全速率; Abushattal 等^[15]利用信道的随机和独立特性, 设计了一种仅用户与基站可知的相位扰动规则, 使每个用户符号产生不同的相移, 从而保障用户数据的安全。

上述 PLS 方案采用了多种指标（如安全中断概率^[4-6]、安全速率^[8]、错误接收概率^[12]和安全能量效率^[13]等）评估防窃听效果，取得了丰富的研究成果。然而，这些方案大多基于一个关键假设，即收发双方拥有完全准确的信道状态信息（channel state information, CSI）。在实际通信场景中，受环境、元器件等因素制约，发射机难以获取完全准确的 CSI。基于不准确的 CSI 开展信道估计工作，估计结果的准确性将会下降。在非理想 CSI 条件下，上述方案的性能可能无法达到预期水平。

非理想 CSI 条件下的安全问题近年来受到了广泛关注，并催生了系列设计方案。Guo 等^[16]基于有界椭圆信道误差模型研究了中继能耗约束下的鲁棒波束成形设计，以便在最坏的情况下实现最大化的安全速率；Zhang 等^[17]分析了智能超表面辅助的无线电系统中非理想 CSI 对信道容量的影响；Ajayi 等^[18]在非理想 CSI 条件下推导出合法接收者的保密容量表达式，并对频率选择性瑞利衰落窃听信道模型的保密容量与误码率（bit error rate, BER）进行了数值和理论仿真；Yang 等^[19]考虑了传输和处理时延导致的过时 CSI，以及在信道估计误差情况下该系统各态历经安全容量的下界，并提出一种信道预测机制以降低不准确的 CSI 对系统可达保密容量的负面影响；Zamani 等^[20]在非理想 CSI 分量满足高斯分布的情况下，以发射功率和用户服务质量要求为限制，推导出以安全和速率最大化为目标的最优功率分配问题的闭式解；Son 等^[21]为防止 CSI 错误导致的安全性能下降，采用基于编码 MIMO 系统的信道相关交织方案，结合额外的编码机制，实现传输数据的有效保护；Cao 等^[22]基于 5G 时分双工（time division duplexing, TDD）非码本传输模式，提出通过空间自适应发射信道完成信道估计与自适应预编码矩阵辅助传输的新模型，实现密钥的高效提取。Jaiswal 等^[23]在真实车与车（V2V）通信场景中，通过分析远近用户与被动窃听用户共存时的安全速率表现，揭示了 NOMA 下行链路中潜在的泄密风险。上述方案大多基于信道估计误差统计模型，通过鲁棒波束成形、信道预测、最优功率分配及编码与交织等应对 CSI 不准确带来的挑战，致力于提升系统的安全速率、保

密容量和数据传输保护能力。

面向 6G 的空天地一体化场景，NOMA、可重构智能表面（reconfigurable intelligent surface, RIS）、无人机（unmanned aerial vehicle, UAV）和通信感知一体化（integrated sensing and communication, ISAC）等新范式为 PLS 提供了多维度的增益和更大的设计自由度。其中，空一地协同相关综述系统梳理了 RIS 在 UAV 辅助网络中的 PLS 作用机制与发展路径，涵盖被动 RIS、主动 RIS 和混合 RIS 应用场景，并探讨其与 NOMA、多接入边缘计算等技术的融合策略，以抑制窃听与干扰、提升网络安全与传输效率，为后续研究提供了框架基础^[24]。在近场通信领域，一类研究通过在 NOMA-PLS 一体化架构中显式建模波束聚焦分辨率，利用分辨率差异区分安全用户与窃听用户，显著提高平均保密速率并降低保密中断概率，缓解近场分辨率不完美导致的安全性能退化^[25]；另一类研究面向近场 ISAC，基于联合距离-角度估计优化波束成形，在满足感知需求的同时最大化保密速率，并借助半定松弛与逐步凸近似算法实现高效求解，进而强化通信安全^[26]。在加密与接入机制方面，基于混沌映射的下行功率域 NOMA 通过物理层加密与 SIC 解码协同设计，在 BER 与数据速率上均优于传统未加密 NOMA，实现“低复杂度-高保密”的性能折中^[27]。在网络体系结构层面，回程 NOMA 通过中继选择与功率分配应对不可信用户与外部窃听用户，并引入信号功率优化和人工噪声增强两种策略来强化 PLS 性能^[28]；同时，在 UAV 辅助的多点协作传输网络中，混合上下行 NOMA 结合网络编码技术，显著改善边缘用户的传输速率与抗窃听能力，且在存在窃听用户时仍能保持较高的传输效率^[29]。总体而言，上述研究从近场分辨率建模、ISAC、混沌加密、回程与协作机制等方面推动了 NOMA 驱动的 PLS 技术发展，但在复杂信道下的鲁棒设计、空一地异构协同及多目标权衡等方面仍有待深化，为后续研究提供了明确的切入点。

综上所述，现有研究围绕 NOMA 系统的 PLS 设计提出了多种抗窃听方案，但在非理想 CSI 条件下，尽管研究者基于信道估计误差统计模型已提出若干安全策略，但模型信道估计精度

不高可能影响方案的实际应用效果。因此，有必要进一步研究非理想CSI条件下的NOMA系统安全增强方法。针对这一挑战，提出一种信道误差额外估计加预编码（additional estimation plus pre-coding, AE PC）设计方案，以应对信道估计精度不高给系统内用户信息安全带来的影响。NOMA系统采用多天线技术与TDD传输模式来提升信道估计精度与系统安全性能。

AE PC方案主要包含两步核心设计：①在无法部署AN、协作中继等安全技术的场景下，设计一种低开销的参考信号，结合复杂度较低的估计算法对安全用户的信道误差进行补偿，提升用户的CSI准确度，且该额外估计过程仅针对有安全需求的用户执行；②基站获取更准确的用户CSI后，依据预编码规则，利用奇异值分解（singular value decomposition, SVD）技术对用户信道矩阵进行处理，更新收发机向量。为验证AE PC方案的有效性，仿真对比了不同信道估计误差信噪比（SNR）条件下的系统安全速率与BER。仿真结果表明，在存在信道估计误差的场景中，AE-PC方案能够较好地保障NOMA系统的可靠性。

2 系统模型

本文研究下行链路NOMA系统在信道估计信息存在误差时面临的PLS问题。系统模型如图1所示，包含一个配备 M 副天线的基站和两个单天线用户（User）。基站与 $User_k (k \in \{1, 2\})$ 之间的信道矩阵如式(1)所示。

$$\mathbf{H}_k = \sqrt{A_k} \mathbf{h}_k (\mathbf{H}_k \in \mathbb{C}^{1 \times M}, k \in \{1, 2\}) \quad (1)$$

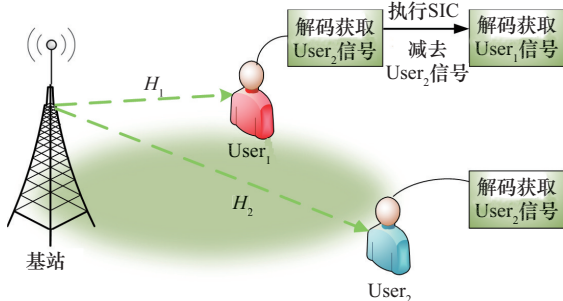


图1 系统模型

其中， $\sqrt{A_k}$ 表示基站与 $User_k$ 之间的大尺度衰落

系数， $\mathbf{h}_k$ 为满足归一化条件的准静态瑞利块衰落的小尺度信道分量。类似地，基站与窃听用户（Eve）之间的信道矩阵如式(2)所示。

$$\mathbf{H}_E = \sqrt{A_E} \mathbf{h}_E (\mathbf{H}_E \in \mathbb{C}^{1 \times M}, k \in \{1, 2\}) \quad (2)$$

其中， $\sqrt{A_E}$ 表示基站与Eve之间的大尺度衰落系数， $\mathbf{h}_E$ 为满足归一化条件的准静态瑞利块衰落信道的小尺度分量。

系统采用TDD模式进行传输，假设所有信道相互独立且在一个时隙内保持稳定，因此发射端可以通过信道互易性获取下行链路的信道矩阵信息。

在图1所示的模型中，考虑一个具体的场景：系统内的 $User_1$ 和 $User_2$ 为两个正常通信的用户，其中 $User_1$ 为近端用户、 $User_2$ 为远端用户。 $User_1$ 在执行SIC解码自身信息时存在窃听 $User_2$ 隐私信息的行为，因此 $User_1$ 兼具合法通信用户与窃听用户双重身份。这使得 $User_2$ 的信息安全面临威胁， $User_2$ 成为具有安全需求的安全用户。基于此，本文将 $User_1$ 视为窃听用户， $User_2$ 视为需要保护的安全用户。根据功率域NOMA原理，基站的发射信号可以表示为：

$$\mathbf{x} = \sqrt{P_1} \mathbf{s}_1 + \sqrt{P_2} \mathbf{s}_2 \quad (3)$$

其中， $\sqrt{P_k} (k \in \{1, 2\})$ 为 $User_k$ 的发射功率，满足总功率约束 $P_1 + P_2 = P_{\text{Total}}$ ， P_{Total} 为基站的总发射功率；传输给 $User_k$ 的数据流数量 $L_k = 1$ ， $\mathbf{s}_k (\mathbf{s}_k \in \mathbb{C}^{L_k \times G})$ 为 $User_k$ 的期望信号，满足 $E\{\|\mathbf{s}_k\|^2\} = 1$ ， G 表示数据流的长度。两个用户的接收信号可以表示为：

$$\mathbf{y}_k = \Phi_k^H \left(\mathbf{H}_k \left(\sqrt{P_1} \mathbf{w}_1 \mathbf{s}_1 + \sqrt{P_2} \mathbf{w}_2 \mathbf{s}_2 \right) + \mathbf{n}_k \right), \quad (k \in \{1, 2\}) \quad (4)$$

其中， $\mathbf{w}_k \in \mathbb{C}^{M \times 1}, (k \in \{1, 2\})$ 表示基站与 $User_k$ 之间的发射机预编码向量， $\Phi_k^H (k \in \{1, 2\})$ 为 $User_k$ 的接收机向量， $\mathbf{n}_k (k \in \{1, 2\})$ 表示 $User_k$ 处的加性复高斯白噪声，其服从分布 $\mathcal{CN}(0, \sigma_k^2)$ 。

在信号传输过程中，基站首先向用户发送导频训练序列以完成信道估计。理想情况下，用户处获取的CSI是准确的，但受无线信道噪声干扰、反馈时延等因素影响，基站通过信道互易性获取的CSI存在误差。因此，实际CSI中的信道

矩阵可以表示为:

$$\mathbf{H}_k = \sqrt{A_k} \hat{\mathbf{h}}_k + \sqrt{A_k} \boldsymbol{\Theta}_k \quad (5)$$

其中, $\hat{\mathbf{h}}_k$ 是基站与 User_k 之间估计所得的 CSI, $\boldsymbol{\Theta}_k$ 表示信道的估计误差分量。为抑制信道估计误差对安全用户安全性能的负面影响, 需要对 $\boldsymbol{\Theta}_k$ 进行额外估计, 以获取更准确的 CSI。

3 信道估计误差下的额外估计和预编码设计

图2展示了AE-PC方案的整体框架, 其核心思想是通过一种复杂度较低的额外估计算法对信道误差进行补偿。在所考虑的系统中, 所有用户均为基站的正常服务对象, 但系统在通信开始前会先对用户的安全属性进行判定, 即区分用户是否有安全需求。AE-PC方案仅在用户具有安全需求时执行。具体流程如下: 系统首先对用户的安全属性进行判定, 仅当用户被判定为安全用户时, 才允许其进入额外估计流程; 对于不具备安全需求的用户, 基站不响应其额外估计请求, 其通信过程保持不变。当用户被判定为安全用户时, 系统允许其向基站发起额外估计请求, 并发送用于额外估计的导频信号。基站借助信道互易性并利用额外估计算法对信道估计误差进行补偿, 更新信道矩阵。随后, 基站基于更新后的信道矩阵对收发机向量进行重新设计。

需要说明的是, 尽管系统已完成安全属性判定, 仍不排除部分用户(如潜在窃听用户)尝试主动发起额外估计请求的可能性。在该情况下, 由于其不满足系统的判定, 基站有权拒绝其额外估计请求。因此, 窃听用户无法执行AE-PC算法, 其窃听行为仅限于正常通信阶段。在异常行

为较严重的情况下, 系统可以终止该用户的通信过程。

3.1 对误差分量的额外估计

当安全用户的信道条件劣于窃听用户时, 若不引入额外的协作技术, 其信息安全将难以保障。因此, 具有安全需求的用户可以在实际通信前向基站请求额外估计, 以获取更准确的 CSI, 从而提升其安全性。是否执行额外估计由基站决定。

在额外估计设计中, 可以采用任何信道估计方法。考虑到最小二乘法对观测参量和被估计参量的统计信息要求较低, 且实现复杂度低, 同时不影响正常通信, 满足AE-PE方案的系统设计需求, 故选用最小二乘法进行额外估计。在发送信息前, 有安全需求的用户发送长度为 K 的专用符号向量 $\mathbf{x}'$, 基站接收到的符号可以表示为:

$$\mathbf{Y} = \sqrt{A_2} (\hat{\mathbf{h}}_2 + \boldsymbol{\Theta}_2)^H \mathbf{q} \mathbf{x}' + \mathbf{n}_2 \quad (6)$$

其中, $\mathbf{q}$ 表示映射向量。设对误差向量 $\boldsymbol{\Theta}_2$ 的额外估计结果为 $\hat{\boldsymbol{\Theta}}_2$, 求得最小二乘中的代价函数, 使式(7)所示的代价函数达到最小的 $\hat{\boldsymbol{\Theta}}_2$ 就是 $\boldsymbol{\Theta}_2$ 的最小二乘估计。则代价函数即误差平方和表示为:

$$\begin{aligned} J(\hat{\boldsymbol{\Theta}}_2) &= \mathbf{n}_2^H \mathbf{n}_2 \\ &= \left(\mathbf{Y} - \sqrt{A_2} (\hat{\mathbf{h}}_2 + \hat{\boldsymbol{\Theta}}_2)^H \mathbf{q} \mathbf{x}' \right)^H \times \\ &\quad \left(\mathbf{Y} - \sqrt{A_2} (\hat{\mathbf{h}}_2 + \hat{\boldsymbol{\Theta}}_2)^H \mathbf{q} \mathbf{x}' \right) \\ &= \left(\mathbf{A} - \hat{\boldsymbol{\Theta}}_2^H \mathbf{B} \right)^H \left(\mathbf{A} - \hat{\boldsymbol{\Theta}}_2^H \mathbf{B} \right) \end{aligned} \quad (7)$$

式中, $\mathbf{A} = \mathbf{Y} - \sqrt{A_2} \hat{\mathbf{h}}_2^H \mathbf{q} \mathbf{x}'$, $\mathbf{B} = \sqrt{A_2} \mathbf{q} \mathbf{x}'$ 。为使

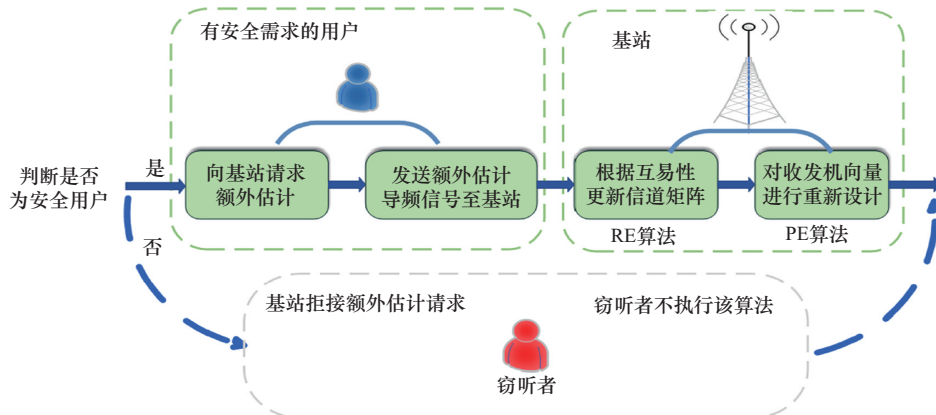


图2 AE-PC方案框架

$J(\hat{\boldsymbol{\theta}}_2)$ 最小, 对误差平方和求偏导并令其等于0。

$$\frac{\partial J(\hat{\boldsymbol{\theta}}_2)}{\partial \hat{\boldsymbol{\theta}}_2} = (\hat{\boldsymbol{\theta}}_2 \mathbf{B} - \mathbf{A}) \mathbf{B}^H = 0 \quad (8)$$

可以求得式(7)中最小二乘的估计结果为:

$$\hat{\boldsymbol{\theta}}_2 = \{(\mathbf{A} \mathbf{B}^H) \text{pinv}(\mathbf{B} \mathbf{B}^H)\} \quad (9)$$

为证明最小值存在, 对 $J(\hat{\boldsymbol{\theta}}_2)$ 求二阶导数。

$$\frac{\partial^2 J(\hat{\boldsymbol{\theta}}_2)}{\partial \hat{\boldsymbol{\theta}}_2^2} = \mathbf{B} \mathbf{B}^H \quad (10)$$

由于式(10)是代价函数的二次偏导, 且为非负定矩阵, 因此式(9)所得结果即为使 $J(\hat{\boldsymbol{\theta}}_2)$ 最小的估计向量。将 $\mathbf{A}$ 、 $\mathbf{B}$ 带入式(9)可得:

$$\hat{\boldsymbol{\theta}}_2 = \left(\left(\mathbf{Y} - \sqrt{A_2} \hat{\mathbf{h}}_2^H \mathbf{q} \mathbf{x}' \right) \left(\sqrt{A_2} \mathbf{q} \mathbf{x}' \right)^H \right) \times \text{pinv} \left(\sqrt{A_2} \mathbf{q} \mathbf{x}' \left(\sqrt{A_2} \mathbf{q} \mathbf{x}' \right)^H \right) \quad (11)$$

根据信道的互易性, 下行链路的误差向量估计结果为:

$$\hat{\boldsymbol{\theta}}_2^H = \left[\left(\left(\left(\mathbf{Y} - \sqrt{A_2} \hat{\mathbf{h}}_2^H \mathbf{q} \mathbf{x}' \right) \left(\sqrt{A_2} \mathbf{q} \mathbf{x}' \right)^H \right) \times \text{pinv} \left(\sqrt{A_2} \mathbf{q} \mathbf{x}' \left(\sqrt{A_2} \mathbf{q} \mathbf{x}' \right)^H \right) \right)^H \right] \quad (12)$$

3.2 基于SVD的收发机设计

本文提出一种基于SVD的收发机设计方法。在设计前先定义由信道矩阵进行SVD得到的相关变量。

对两个用户的信道矩阵进行SVD可得:

$$\mathbf{H}_k = \mathbf{U}_k \mathbf{A}_k \mathbf{V}_k^H \quad (13)$$

其中, $\mathbf{U}_k$ 和 $\mathbf{V}_k^H$ 分别为 $\mathbf{H}_k$ ($\mathbf{H}_k \in \mathbb{C}^{1 \times M}, k \in \{1, 2\}$)的左奇异矩阵 (为 1×1 的酉矩阵) 和右奇异矩阵 (为 $M \times M$ 的酉矩阵), 满足 $\mathbf{U}_k \mathbf{U}_k^H = \mathbf{V}_k \mathbf{V}_k^H = \mathbf{I}$ 。 $\mathbf{A}_k$ 表示大小为 $1 \times M$ 的非负对角矩阵, 其对角元素是由从大到小排列的奇异值 λ 组成的。右奇异矩阵 $\mathbf{V}_k^H$ 的形式为

$$\mathbf{V}_k^H = \{\mathbf{v}_{k(1)}, \mathbf{v}_{k(2)}, \dots, \mathbf{v}_{k(M)}\}^H, (k \in \{1, 2\}) \quad (14)$$

其中, M 为发射天线的数量, $\mathbf{v}_{k(M)}$ 为用户 k 的第 M 个奇异值对应的右奇异向量。

由上述对信道矩阵的SVD结果可以看出, 预编码向量 $\mathbf{w}_k$ 和接收机 Φ_k^H 的性能受CSI准确性的影响。只有当获取的CSI足够准确时, 才能达到理想的预编码和均衡效果。结合第3.1节额外估计获取

的准确CSI, 对安全用户的收发机进行重新设计。

具体而言, 分别对两个用户的信道矩阵进行SVD。由于窃听用户 (User₁) 未参与额外估计, 其信道矩阵保持不变, SVD结果与式(13)中 $k=1$ 时保持一致; 而安全用户 (User₂) 通过额外估计请求, 更新了其信道矩阵, 更新后的信道矩阵可以表示为:

$$\bar{\mathbf{H}}_2 = \sqrt{A_2} (\hat{\mathbf{h}}_2 + \hat{\boldsymbol{\theta}}_2^H) \quad (15)$$

对额外估计后的信道矩阵进行SVD可以得到式(16)。

$$\bar{\mathbf{H}}_2 = \mathbf{U}_2' \mathbf{A}_2' \mathbf{V}_2'^H \quad (16)$$

其中, $\mathbf{U}_2'$ 和 $\mathbf{V}_2'^H$ 分别表示 1×1 、 $M \times M$ 的酉矩阵, 满足 $\mathbf{U}_2' \mathbf{U}_2'^H = \mathbf{V}_2' \mathbf{V}_2'^H = \mathbf{I}$ 。 $\mathbf{A}_2'$ 表示大小为 $1 \times M$ 的非负对角矩阵, 其对角元素是由从大到小排列的奇异值 λ 组成的。此时安全用户的右奇异矩阵为:

$$\mathbf{V}_2'^H = \{\mathbf{v}_{2(1)}', \mathbf{v}_{2(2)}', \dots, \mathbf{v}_{2(M)}'\}^H \quad (17)$$

(1) 发射机设计

在多天系统, 合理利用分集和复用技术可以显著提高系统的容量和可靠性。根据上述分析, 结合系统模型, 酉矩阵 $\mathbf{V}_k^H$ 是 $M \times M$ 维矩阵, $\mathbf{A}_k'$ 为 $1 \times M$ 的非负对角矩阵。在图1所示的场景中, 只存在一个有效特征值 λ_1 , 因此选取 $\mathbf{V}_2^H$ 中的第一个有效奇异值对应的右奇异向量 $\mathbf{v}_{2(1)}$ 作为User₂的预编码向量 $\mathbf{w}_k$ 。由于只有安全用户的信道矩阵进行了更新, 因此式(4)中两个用户的预编码向量 $\mathbf{w}_k$ 重新设计为:

$$\begin{aligned} \mathbf{w}_1 &\rightarrow \mathbf{v}_{1(1)} \\ \mathbf{w}_2 &\rightarrow \mathbf{v}_{2(1)}' \end{aligned} \quad (18)$$

更新后的用户接收信号可以表示为:

$$\mathbf{y}_k^{\text{AE-PC}} = \Phi_k^H \times \left(\mathbf{H}_k \left(\sqrt{P_1} \mathbf{v}_{1(1)} \mathbf{s}_1 + \sqrt{P_2} \mathbf{v}_{2(1)}' \mathbf{s}_2 \right) + \mathbf{n}_k \right) (k \in \{1, 2\}) \quad (19)$$

(2) 接收机设计

在接收机设计中, 采用计算复杂度较低的迫零算法。对于安全用户 (User₂), 根据式(19)结合NOMA技术的特点, 远端用户在解码自身信息时将近端用户的信号视为噪声, 其接收机 Φ_2^H 设计为

$$\Phi_2^H = \left(\sqrt{P_2} \right)^{-1} \text{pinv}(\bar{\mathbf{H}}_2 \mathbf{v}_{2(1)}') \quad (20)$$

其中, $\text{pinv}(\cdot)$ 表示伪逆运算。对于窃听用户 (User₁), 仅考虑其对安全用户的安全威胁, 因

此仅考虑其在执行 SIC 过程中解码安全用户信息的步骤。窃听用户接收机 Φ_1^H 设计为:

$$\Phi_1^H = \left(\sqrt{P_1} \right)^{-1} \text{pinv} \left(H_1 v'_{2(1)} \right) \quad (21)$$

将更新后的接收机即式(20)和式(21)代入式(19), 此时两个用户在接收端的目标信号分别表示为

$$\begin{aligned} y_k^{\text{AE-PC}} = & \Phi_k^H \times \left(H_k \left(\sqrt{P_1} v_{1(1)} s_1 + \sqrt{P_2} v'_{2(1)} s_2 \right) + n_k \right) \\ & (k \in \{1, 2\}) \end{aligned} \quad (22)$$

4 性能分析

4.1 对信道误差分量的额外估计性能分析

本节采用安全速率作为指标, 评估算法的性能, 通过对比不同方案下用户的信干噪比 (signal to interference plus noise ratio, SINR) 和安全速率, 验证 AE-PC 算法对安全用户的安全速率的提升效果。

4.1.1 未采用 AE-PC 方案时

在图 1 所示的场景中, 近端用户充当窃听用户, 但其作为系统内的安全用户, 发送功率和解码顺序均为已知。根据 NOMA 的原理, 信道条件较好的用户分配较小的功率, 信道条件较差的用户分配较大的功率。在解码过程中, SIC 按照功率从大到小的顺序依次执行: 发射功率较大的用户优先解码自身信息, 将其他用户的信号视为干扰, 随后依次解码功率较小的用户信号。在 CSI 存在估计误差的情况下, 安全用户的信干噪比 (signal to interference plus noise ratio, SINR) 和窃听用户的 SINR 的形式化表示分别如式(23)和式(24)所示。

$$\text{SINR}_{22} = \frac{A_2 |\hat{h}_2 w_2|^2 P_2}{A_2 |(\hat{h}_2 + \Theta_2) w_1|^2 P_1 + A_2 |\Theta_2 w_2|^2 P_2 + \sigma_2^2} \quad (23)$$

$$\text{SINR}_{12} = \frac{A_1 |\hat{h}_1 w_2|^2 P_2}{A_1 |(\hat{h}_1 + \Theta_1) w_1|^2 P_1 + A_1 |\Theta_1 w_1|^2 P_2 + \sigma_1^2} \quad (24)$$

因此, 安全用户的安全速率 R_s 可以表示为:

$$\begin{aligned} R_s = & \left(\log(1 + \text{SINR}_{22}) - \log(1 + \text{SINR}_{12}) \right)^+ \\ = & \left[\log \left(1 + \frac{A_2 |\hat{h}_2 w_2|^2 P_2}{A_2 |(\hat{h}_2 + \Theta_2) w_1|^2 P_1 + A_2 |\Theta_2 w_2|^2 P_2 + \sigma_2^2} \right) \right. \\ & \left. - \log \left(1 + \frac{A_1 |\hat{h}_1 w_2|^2 P_2}{A_1 |(\hat{h}_1 + \Theta_1) w_1|^2 P_1 + A_1 |\Theta_1 w_1|^2 P_2 + \sigma_1^2} \right) \right]^+ \end{aligned} \quad (25)$$

其中, + 表示 R_s 始终为非负, 若括号内值小于 0 则安全速率 R_s 为 0。

在不进行额外估计的情况下, 受信道估计误差的影响, 无法确保安全用户始终维持正向的安全速率 R_s , 具体的仿真结果在第 5.1 节中展示。

4.1.2 采用 AE-PC 方案时

根据第 3.1 节所述, 安全用户对信道估计误差分量进行额外估计, 更新了基站到安全用户之间的信道矩阵, 而窃听用户由于未参与额外估计, 其信道矩阵保持不变。采用 AE-PC 算法对误差分量进行额外估计后, 安全用户和窃听用户的 SINR 分别更新为:

$$\begin{aligned} \text{SINR}_{22}^{\text{AE-PC}} = & \frac{A_2 |(\hat{h}_2 + \hat{\Theta}_2^H) v'_{2(1)}|^2 P_2}{A_2 |(\hat{h}_2 + \Theta_2) v_{1(1)}|^2 P_1 + A_2 |(\hat{\Theta}_2^H - \Theta_2) v'_{2(1)}|^2 P_2 + \sigma_2^2} \\ \text{SINR}_{12}^{\text{AE-PC}} = & \frac{A_1 |\hat{h}_1 v'_{2(1)}|^2 P_2}{A_1 |(\hat{h}_1 + \Theta_1) v_{1(1)}|^2 P_1 + A_1 |\Theta_1 v_{1(1)}|^2 P_2 + \sigma_1^2} \end{aligned} \quad (26)$$

$$\text{SINR}_{12}^{\text{AE-PC}} = \frac{A_1 |\hat{h}_1 v'_{2(1)}|^2 P_2}{A_1 |(\hat{h}_1 + \Theta_1) v_{1(1)}|^2 P_1 + A_1 |\Theta_1 v_{1(1)}|^2 P_2 + \sigma_1^2} \quad (27)$$

其中, $\text{SINR}_{22}^{\text{AE-PC}}$ 为采用额外估计算法 (即 AE-PC 算法) 后 User₂ 接收自己信息的 SINR, $\text{SINR}_{12}^{\text{AE-PC}}$ 表示采用 AE-PC 算法后 User₁ 窃听 User₂ 信息的 SINR。故在此情况下安全用户的安全速率可以表示为:

$$R_s^{\text{AE-PC}} = \left[\log(1 + \text{SINR}_{22}^{\text{AE-PC}}) - \log(1 + \text{SINR}_{12}^{\text{AE-PC}}) \right]^+ \quad (28)$$

由于在通信前, 系统采用复杂度较低的额外估计算法补偿了信道估计误差, 更新了安全用户的信道矩阵, 因此基站和接收端能够获取更加准确的 CSI。对比式(23)与式(26)可知, 该算法在提高信号有效功率的同时降低了干扰项功率;

对比式(24)与式(27)可知，发射机的更新有效降低了窃听用户的SINR。综上所述，所提的额外估计算法可以显著提升安全用户的安全速率，增强系统的保密性能，防止信息泄露。

4.2 收发机性能分析

本节以BER为指标，通过对比窃听用户与安全用户接收信息的差异，进一步评估AE-PC算法的性能。本节重点分析基于SVD的收发机结合额外估计算法对安全用户BER的改善效果。

4.2.1 未采用AE-PC算法时

在未对信道估计误差进行补偿的传统方案中，发射机的预编码向量 $\mathbf{w}_k$ 被设为一个随机的复高斯向量，并通过SVD信道矩阵来设计收发机。然而，传统方案未能充分利用多天线系统提供的空间自由度，且受信道估计误差的影响，波束方向可能偏离目标用户，导致性能下降。此时，安全用户和窃听用户的接收信号分别表示为：

$$\begin{cases} \Phi_1^H = (\sqrt{P_2})^{-1} \text{pinv}(\mathbf{H}_1 \mathbf{w}_2) \\ \Phi_2^H = (\sqrt{P_2})^{-1} \text{pinv}(\mathbf{H}_2 \mathbf{w}_2) \end{cases} \quad (29)$$

$$\begin{cases} \mathbf{y}_{s1} = \Phi_1^H (\mathbf{H}_1 (\sqrt{P_1} \mathbf{w}_1 s_1 + \sqrt{P_2} \mathbf{w}_2 s_2) + \mathbf{n}_1) \\ \mathbf{y}_{s2} = \Phi_2^H (\mathbf{H}_2 (\sqrt{P_1} \mathbf{w}_1 s_1 + \sqrt{P_2} \mathbf{w}_2 s_2) + \mathbf{n}_2) \end{cases} \quad (30)$$

其中， $\mathbf{y}_{s2}$ 表示安全用户接收自身信息， $\mathbf{y}_{s1}$ 表示窃听用户窃听安全用户的信息， $\Phi_k^H (k \in 1, 2)$ 表示User_k的接收机向量。受信道估计误差影响，传统方案的BER较高。

4.2.2 结合AE-PC算法的SVD方案

结合AE-PC算法后，通过SVD得到的奇异向量提升了安全用户的信道精度，设计的收发机更加精确，从而实现了更安全、更可靠的用户隐私信息传输。此时，安全用户和窃听用户的接收信号如式(31)与式(32)所示。

$$\begin{cases} \Phi_1^H = (\sqrt{P_2})^{-1} \text{pinv}(\mathbf{H}_1 \mathbf{v}'_{2(1)}) \\ \Phi_2^H = (\sqrt{P_2})^{-1} \text{pinv}(\bar{\mathbf{H}}_2 \mathbf{v}'_{2(1)}) \end{cases} \quad (31)$$

$$\begin{cases} \mathbf{y}_1^{\text{AE-PC}} = \Phi_1^H \times \\ \left(\mathbf{H}_1 (\sqrt{P_1} \mathbf{v}_{1(1)} s_1 + \sqrt{P_2} \mathbf{v}'_{2(1)} s_2) + \mathbf{n}_1 \right) \\ \mathbf{y}_2^{\text{AE-PC}} = \Phi_2^H \times \\ \left(\mathbf{H}_2 (\sqrt{P_1} \mathbf{v}_{1(1)} s_1 + \sqrt{P_2} \mathbf{v}'_{2(1)} s_2) + \mathbf{n}_2 \right) \end{cases} \quad (32)$$

其中， $\mathbf{y}_2^{\text{AE-PC}}$ 表示安全用户解码自身信息， $\mathbf{y}_1^{\text{AE-PC}}$ 表示窃听用户窃听安全用户的信息。通过额外估计和SVD优化，安全用户的BER显著降低，窃听用户的BER则因信道估计误差干扰而维持在较高水平。

4.3 AE-PC方案的额外开销和复杂度分析

为验证AE-PC方案具有低开销、低复杂度的特点，本节从额外导频开销与算法计算复杂度两个方面进行分析。

4.3.1 额外导频开销分析

为量化AE-PC方案引入的专用参考符号对系统开销的影响，本文借鉴文献[31]中式(15)使用的前置因子扣减方法，即导频占用的时频资源以比例形式从有效传输时隙中扣除。根据该思想，额外导频开销可以建模为：

$$\eta_{\text{AE-PC}} = \frac{K}{C_u} \quad (33)$$

其中， K 表示专用参考符号长度， C_u 表示用户数据符号数。

以正交相移键控 (quadrature phase shift keying, QPSK) 为例，若每个用户传输的信息长度为14 400 bit，则：

$$C_u = 14\,400/2 = 7\,200$$

$$\eta_{\text{AE-PC}} = \frac{K}{C_u} = \frac{10}{7\,200} \approx 0.139\% \quad (34)$$

因此，AE-PC的额外导频开销处于 10^{-3} 量级，对时频资源占用的影响可以忽略。

4.3.2 AE-PC算法的计算复杂度

该算法的复杂度主要由最小二乘估计和SVD决定，总复杂度可以表示为：

$$O_{\text{AE-PC}} = O_{\text{LS}} + O_{\text{SVD}} \quad (35)$$

其中， O_{LS} 表示对误差分量进行额外估计的复杂度， O_{SVD} 表示基于SVD收发机设计的复杂度。 O_{LS} 的复杂度由式(7)~式(9)中多个矩阵的乘法和求逆运算决定，其中矩阵 $\mathbf{A}$ 和 $\mathbf{B}$ 的大小与基站的发射天线数 M 、用户的接收天线数 N 及专用参考符号的长度 K 有关。 $\mathbf{A}$ 、 $\mathbf{B}$ 分别为 $M \times K$ 和 $N \times K$ 的矩阵。因此， O_{LS} 可以用式(36)表示。

$$\begin{aligned} O_{\text{LS}} = & O(M \times K \times N) + \\ & O(M \times N^2) + O(N^3) \end{aligned} \quad (36)$$

O_{SVD} 与信道矩阵的SVD有关，对式(15)中的信道矩阵进行SVD的计算复杂度为 $O(M^2 N)$ ，

故 AE-PC 算法的总复杂度:

$$O_{\text{AE-PC}} = O(M \times K \times N) + O(M \times N^2) + O(N^3) + O(M^2) + O(M^2 N) \quad (37)$$

综上所述, AE-PC 算法的计算复杂度主要来源于 LS 估计和 SVD。对于较小的 M 和 N , AE-PC 算法的计算复杂度是可以接受的。尽管存在 $O(N^3)$ 和 $O(M^2 N)$ 高阶项, 但其主要受系统规模 (如用户数和天线数) 的影响。因此 AE-PC 算法在保障用户安全性的同时, 能够保持较合理的计算开销。

5 仿真分析

为验证所提 AE-PC 算法的工程应用价值, 本文模拟了车联网下行通信场景^[32], 设定基站同时为近端用户和远端用户提供下行链路服务, 近端用户在执行 SIC 过程中可能获取远端用户的行驶轨迹等敏感信息, 构成内部窃听威胁。近端用户与基站的距离设为 100~300 m, 远端用户与基站的距离设为 200~400 m; 每个用户传输的信息长度为 14 400 bit, 调制方式采用 QPSK, 接收端采用对数似然比 (log-likelihood ratio, LLR) 软解调方法; 基站的总发射功率设为 25 W, User_2 作为远端用户在 NOMA 系统中分配了更大的功率。为简化分析, 未涉及功率分配算法, 直接设定基站发送给 User_1 的信号功率 $P_1 = (1/10^2) P_{\text{Total}}$, 发送给 User_2 的信号功率 $P_2 = (10^2/(10^2 + 1)) P_{\text{Total}}$ 。部分关键参数的配置见表 1。

表 1 部分仿真参数值

参数	数值
路径损耗 d/dB	$19.14 + 38.0 \lg(d_k)$, $k = \{1, 2\}$, d_k 为基站与用户之间的距离
对数正态阴影标准差/dB	10
发射天线数 $M/\text{副}$	4
接收天线数 $N/\text{副}$	1
基站到 User_1 的距离 d_1/m	100~300
基站到 User_2 的距离 d_2/m	200~400

5.1 用户传输速率

在实验中, 采用安全速率和用户传输速率作为评估系统安全性的主要指标。通过比较 AE-PC

方案与传统方案 (如随机预编码和人工噪声注入) 在不同信道估计误差和 SNR 条件下的表现, 发现 AE-PC 能够有效提高安全用户 (User_2) 的安全速率。

在额外误差估计仿真分析中, 设额外估计导频符号长度 $K = 10$ 。为评估该算法在不同误差下的性能, 本文引入了 CSI 估计误差系数 ρ 。 ρ 为 Θ_k 中每个元素的方差, 且 $0 \leq \rho \leq 1$ 。若无特别说明, CSI 估计误差系数 $\rho = 0.01$ 。用户的噪声功率根据传输 SNR 和发射功率设定 (即 $\sigma_k^2 = \frac{P_2}{\text{SNR}}$)。

图 3 展示了 $\rho = 0.01$ 时 AE-PC 方案与传统方案中不同用户的传输速率。其中, AE-PC Eve 表示窃听用户窃听 User_2 的速率、Trad Eve 表示未采用任何算法时 (即传统方案) 窃听用户的传输速率、Trad User_2 表示未采用任何算法时 (即传统方案) User_2 的传输速率、AE-PC User_2 表示采用 AE-PC 方案 User_2 的传输速率。仿真结果表明, 未采用 AE-PC 算法时, 随着 SNR 的提高, 噪声对传输速率的影响逐渐减小, 两个用户的传输速率均有提升, 但是 User_1 (即窃听用户) 的传输速率始终高于 User_2 , 导致安全传输无法实现; 采用 AE-PC 算法后, 由于对信道估计误差的补偿和接收机的更新, User_1 的 SINR 有效降低, 其传输速率也明显降低。从图 3 中可以观察到, 当 SNR 较小时, User_2 的传输速率较低, 这主要受额外估计噪声、基站与 User_2 的距离的影响。然而, 随着 SNR 的提高, AE-PC 的优势逐渐明显, 当 $\text{SNR} > 10 \text{ dB}$ 时, User_2 的传输速率超越了 User_1 , 并在后续 SNR 区间始终保持优势, 确保了安全用户的正常通信。

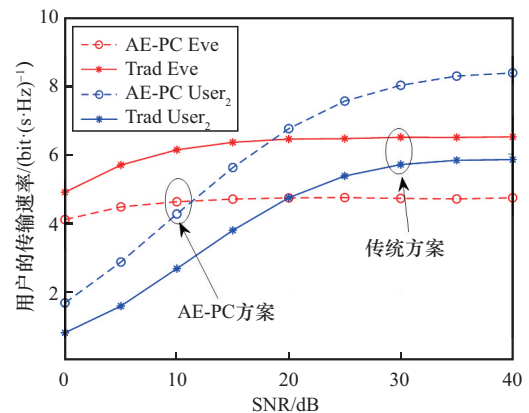


图 3 $\rho = 0.01$ 时不同方案各用户的传输速率对比

图4展示了不同SNR下 $\rho=0.01$ 时User₂的安全传输速率变化曲线。仿真结果验证了第4.1节的分析：未采用AE-PC算法时，窃听用户能够在相同时间内获取更多安全用户的有用信息，导致User₂的安全传输速率始终为0，安全用户的信息受到严重威胁；而采用AE-PC算法后，当SNR>10 dB时，User₂的安全传输速率明显大于零，表明User₂能够在存在窃听行为的情况下实现安全传输。从图4中可以看出，当SNR>40 dB时，User₂的安全传输速率采用AE-PC算法相比未采用AE-PC算法时提升了3.7 bit/(s·Hz)。

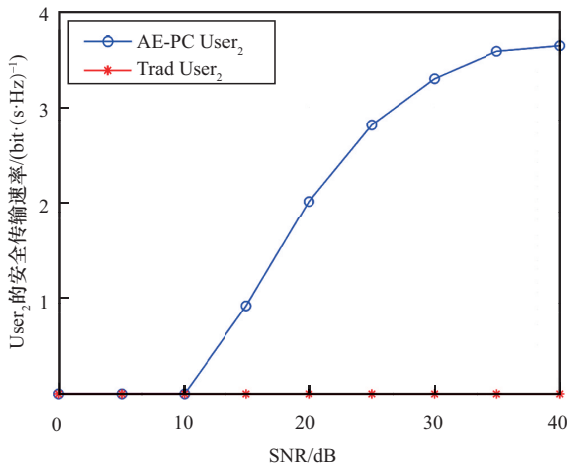


图4 $\rho = 0.01$ 时User₂的安全传输速率

图3和图4表明理论分析和仿真结果相符，验证了分析的准确性，证明AE-PC算法能够有效提高安全用户的安全传输速率。

此外，本文将AE-PC算法与传统的AN算法开展了对比实验。具体而言，将噪声信号注入信道的零空间，这样安全用户不会受到影响。

图5对比了 $\rho = 0.01$ 时不同方案的用户传输速率。仿真时，基站分配给AN的功率为5 W。AN Eve和AN User₂分别表示在发送AN时窃听用户与User₂的传输速率。在实际的NOMA场景下，基站服务多个用户，各用户信道高度相关。为便于分析，本文仅考虑两个用户，假设User₁与User₂的信道相关性为：

$$\rho_{h_1 h_2} = \frac{E[h_1 h_2^*]}{\sqrt{E[|h_1|^2]} \sqrt{E[|h_2|^2]}} = 0.9 \quad (38)$$

为满足用户的安全需求，本文在User₂的零空间注入AN，这会带来额外的功率开销。

从图5可以看出，相比传统的AN算法，AE-PC算法在不同SNR下表现出更优的传输性能。AN算法通过在User₂的零空间注入AN来抵御窃听行为，虽然能够降低窃听用户的传输速率，但也带来了额外的功率开销，并且由于两个用户的信道高度相关，安全用户的传输速率也受到影响，无法进行安全通信。相反，AE-PC算法利用额外估计补偿信道误差，结合预编码设计，在降低窃听用户传输速率的同时，有效提升了User₂的安全传输速率。在高SNR区域，AE-PC算法始终保持较大优势，确保安全用户在信道高度相关($\rho_{h_1 h_2} = 0.9$)的情况下仍能获得正向的安全传输速率。这说明AE-PC算法不仅能抑制窃听用户性能，还能改善安全用户的传输效率，整体优于AN算法。

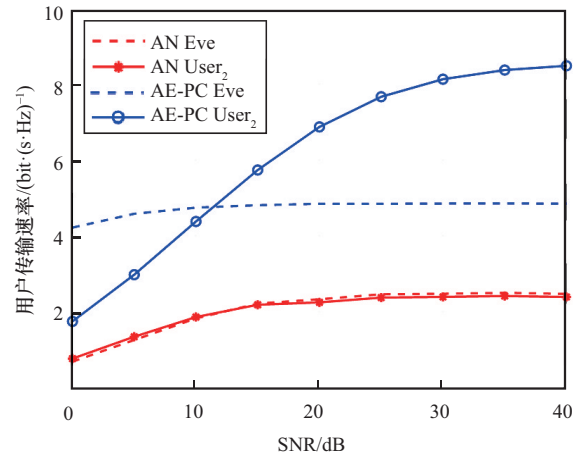
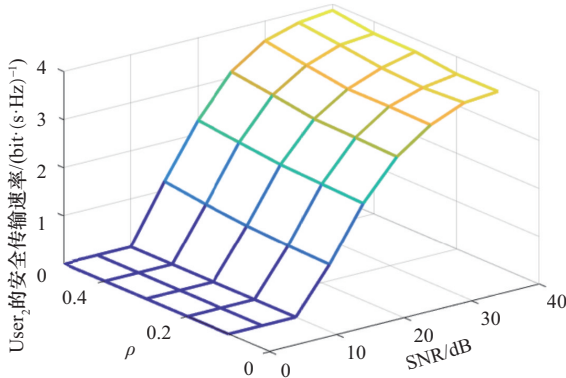


图5 $\rho=0.01$ 时不同方案的用户传输速率

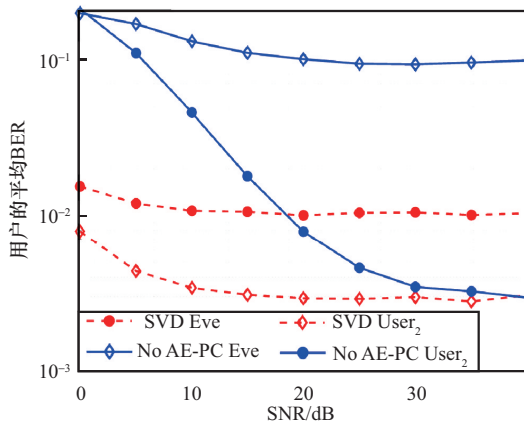
为评估AE-PC算法中安全用户的安全传输速率在不同信道估计误差系数与信噪比条件下的变化规律，本文开展了仿真实验，结果如图6所示。随着CSI估计误差系数 ρ ($0 \leq \rho \leq 0.5$)的增大，基站基于信道互易性获取的用户CSI精度呈逐步下降趋势。仿真结果表明，在此情况下，AE-PC算法的性能优势反而更加突出。尤其是当 ρ 达到0.5时，AE-PC方案的性能提升效果尤为显著。此外，随着SNR的提高，User₂的安全传输速率也呈现持续提升的态势。

图 6 不同 ρ 和SNR下User₂的安全传输速率

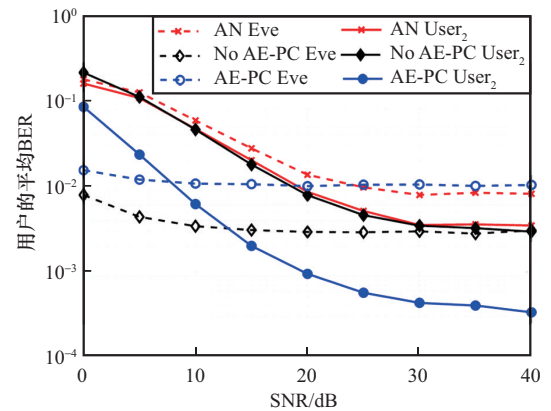
5.2 BER

BER是评估通信质量的另一项关键指标。本节分析了不同方案下安全用户和窃听用户的BER性能。对比AE-PC方案、AN方案和随机预编码方案的BER,发现AE-PC方案能够显著改善安全用户的BER,并有效抑制窃听用户的BER。

图7展示了 $\rho = 0.01$ 时两种方案的BER曲线。其中,SVD Eve和SVD User₂分别表示在CSI存在误差的条件下直接进行SVD预编码时,User₁窃听User₂的BER和User₂接收自身信息的BER。No AE-PC Eve和No AE-PC User₂分别表示采用随机预编码方案时User₁窃听User₂的BER、User₂接收自身信息的BER。仿真结果显示,在CSI存在误差的情况下,直接使用SVD设计预编码可能导致波束指向偏差,造成用户方向上的增益损失,其性能劣于随机预编码方案。为此,在后续的BER仿真评估中,以随机预编码方案作为BER对比的基准。

图 7 $\rho=0.01$ 时随机预编码与SVD预编码方案的BER曲线

为评估AE-PC方案的BER性能,本文还引入了AN方案进行对比。其实现方式与第5.1节所述一致,即向User₂的零空间注入AN。仿真中,基站分配给AN的功率为5 W。图8展示了 $\rho = 0.01$ 时不同方案的用户平均BER曲线。其中,曲线AN Eve和AN User₂分别表示采用AN方案时窃听用户的BER、User₂的BER,从中可以看出,尽管AN User₂的信息安全在一定程度上得到保障,但其BER性能明显恶化,难以满足正常通信需求。在不采用任何额外估计与预编码的情况下(即No AE-PC),由于User₂距离基站较远,其信道条件比窃听用户的信道条件更差,因此其BER在整个SNR区间始终高于窃听用户,User₂的传输性能未达到预期。相比之下,在AE-PC方案中,User₂的BER随SNR的增大呈显著下降趋势。在低SNR区域,受额外估计过程中噪声的影响,AE-PC User₂的BER略高于AN方案。当SNR为7 dB时,AE-PC User₂的BER优于AN方案;当SNR为40 dB时,AE-PC User₂的BER相比AN方案的BER降低约两个数量级。从图8可以看出,随着方案的实施,AE-PC Eve的平均BER逐渐趋向恒定。上述结果表明,AE-PC算法不仅优化了安全用户的性能,还有效恶化了窃听用户的窃听能力。

图 8 $\rho=0.01$ 时不同方案下用户的平均BER曲线

本文在仿真中将AE-PC方案与第4.2.1节中所述的未进行额外估计的收发机设计方案(即No AE-PC)进行了性能对比。图9展示了不同 ρ 下User₂的平均BER曲线,从中可以看出,随着 ρ 的增大(ρ 从0.01提升到0.5),No AE-PC User₂

的平均BER呈显著上升趋势，表明CSI估计误差会明显降低User₂获取CSI的准确度。然而，无论 ρ 如何变化，AE-PC User₂的BER性能均优于No AE-PC User₂方案。上述结果验证了对信道估计误差分量进行额外估计（即获取更准确的信道估计误差信息）是必要的（即通过获取更准确的信道估计误差信息，能够有效抑制误差带来的性能损失）。在实际的通信系统中，CSI估计误差往往难以完全避免，而AE-PC方案能够有效提高通信的可靠性。

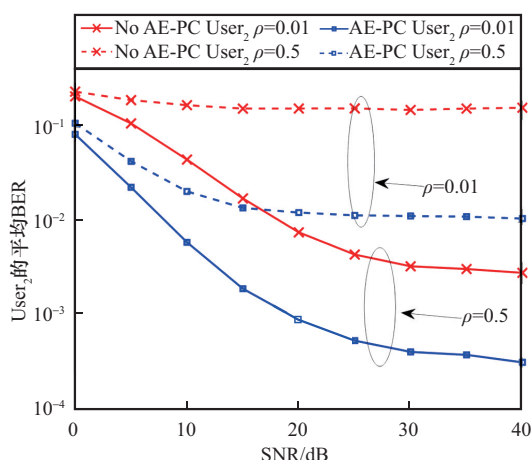


图9 不同 ρ 下User₂的平均BER曲线

5.3 恶意窃听威胁场景

在实际通信场景中，还需考虑窃听用户对安全用户发起的恶意攻击行为。攻击者可能在信道估计阶段对安全用户实施干扰式攻击，通过随机或有选择地向安全用户发送强干扰信号，从而抬高安全用户信道估计过程中的噪声功率，致使信道估计误差增大。

假设合法发射端向User₂发送导频序列 $p \in \mathbb{C}^{M \times 1}$ ，User₂的合法增益信道为 H_2 ，噪声 $n'_2 \sim \mathcal{CN}(0, \sigma_2^2)$ ，那么User₂的接收导频信号为：

$$y'_2 = H_2 p + n'_2 \quad (39)$$

窃听用户在信道估计阶段发送干扰信号 e ，于是User₂的接收导频信号变为：

$$y_2^e = H_2 p + e + n'_2 \quad (40)$$

图10给出了在恶意窃听场景下各用户的平均BER曲线。在此场景中，窃听用户通过对User₂施加干扰，致使其CSI估计误差系数增大，从而造成User₂的有效信道条件劣于窃听用户。

仿真结果表明，在未采用AE-PC算法时，基于存在误差的CSI进行随机预编码，既无法保障User₂的信息安全，也无法实现可靠传输。而在引入AE-PC算法后，系统通过额外估计补偿了恶意攻击引入的误差，并在预编码设计中予以修正，使得User₂的BER随SNR的升高而下降，同时窃听用户的BER维持在较高位。例如，当SNR=40 dB，User₂的平均BER降至 10^{-4} 量级，而窃听用户仍停留在 10^{-2} 量级左右。以上结果说明，AE-PC方案在恶意窃听场景下不仅能够保障User₂的可靠通信，还能有效抑制窃听用户的窃听能力，从而提升系统整体安全性。

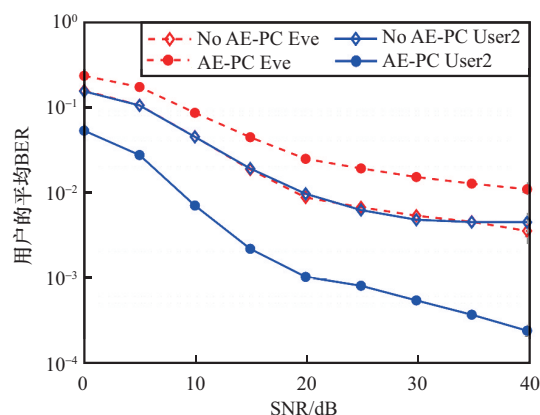


图10 恶意窃听场景下各用户的平均BER曲线

在该模型中，窃听用户也是系统内部安全用户，若其在通信过程中对其他用户实施干扰攻击，系统有权终止其接入权限。需要指出的是，本文算法建立在导频未受污染的假设之上；若攻击者发起导频污染攻击，估计信道中将叠加攻击者信道分量，导致信道估计方向出现偏差，进而引起检测及译码性能的显著劣化。这一情况已超出本文方法当前的处理能力，留待后续研究。

6 结束语

针对NOMA系统中CSI不准确及窃听威胁影响用户安全的问题，本文提出了AE-PC算法，以解决信道估计误差对安全传输造成的负面影响。该算法通过额外估计对信道误差分量进行补偿，并将修正后的信道信息用于重构收发机，从而在提升安全用户链路质量的同时抑制窃听用户性能。理论与仿真分析表明，在不同信道估计误

差条件下, AE-PC 算法均能有效增强系统的安全传输能力。

需要指出的是, 本文所提 AE-PC 方案目前针对单天线用户与单窃听用户的场景设计。未来的研究工作将围绕以下两个方面展开: 一是将该方案扩展至多天线用户及多窃听用户的复杂通信场景, 以适应更加复杂的通信环境、满足多样化的应用需求; 二是深入研究在恶意攻击(如导频污染、训练阶段干扰等)场景下的安全增强机制, 以提升算法在更加复杂攻击环境下的有效性。通过以上方向的持续探索, 有望构建更加安全、可靠且具备广泛适应性的 NOMA 通信系统。

参考文献:

- [1] Maraqa O, Rajasekaran A S, Al-Ahmadi S, et al. A survey of rate-optimal power domain NOMA with enabling technologies of future wireless networks[J]. *IEEE Communications Surveys & Tutorials*, 2020, 22(4): 2192-2235.
- [2] Ding Z G, Lei X F, Karagiannidis G K, et al. A survey on non-orthogonal multiple access for 5G networks: research challenges and future trends[J]. *IEEE Journal on Selected Areas in Communications*, 2017, 35(10): 2181-2195.
- [3] Riazul Islam S M, Avazov N, Dobre O A, et al. Power-domain non-orthogonal multiple access (NOMA) in 5G systems: potentials and challenges[J]. *IEEE Communications Surveys & Tutorials*, 2017, 19(2): 721-742.
- [4] Guo C, Zhao L Q, Feng C, et al. Secrecy performance of NOMA systems with energy harvesting and full-duplex relaying[J]. *IEEE Transactions on Vehicular Technology*, 2020, 69(10): 12301-12305.
- [5] 张延良, 田月华, 李兴旺, 等. 基于 MF 协议的协作 NOMA 系统物理层安全性能研究[J]. *电子与信息学报*, 2023, 45(4): 1211-1218.
Zhang Y L, Tian Y H, Li X W, et al. Research on physical layer security of cooperative NOMA system based on MF protocol[J]. *Journal of Electronics & Information Technology*, 2023, 45(4): 1211-1218.
- [6] Feng Y H, Yan S H, Liu C X, et al. Two-stage relay selection for enhancing physical layer security in non-orthogonal multiple access[J]. *IEEE Transactions on Information Forensics and Security*, 2019, 14(6): 1670-1683.
- [7] Yu J B, Zhao S, Tian M X, et al. Joint transmit antenna selection and beamforming design for millimeter wave massive MIMO NOMA secure networks[J]. *IEEE Communications Letters*, 2024, 28(10): 2407-2411.
- [8] Thapar S, Mishra D, Saini R. Decoding orders for securing untrusted NOMA[J]. *IEEE Networking Letters*, 2021, 3(1): 27-30.
- [9] Su B B, Yu W J, Liu H B, et al. Secure transmission design for cooperative NOMA in the presence of internal eavesdropping[J]. *IEEE Wireless Communications Letters*, 2022, 11(5): 878-882.
- [10] Jia F, Zhang C S, Jiang C J, et al. Guaranteeing positive secrecy rate for NOMA system against internal eavesdropping[J]. *IEEE Communications Letters*, 2021, 25(6): 1805-1809.
- [11] Zhao N, Wang W, Wang J J, et al. Joint beamforming and jamming optimization for secure transmission in MISO-NOMA networks[J]. *IEEE Transactions on Communications*, 2019, 67(3): 2294-2305.
- [12] Horiike N, Kitagawa H, Okamoto E, et al. Chaos MIMO-based downlink non-orthogonal multiple access scheme with physical layer security[C]//*Proceedings of the 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. Piscataway: IEEE Press, 2018: 1-7.
- [13] 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.
- [14] Yang Z T, Li D D, Zhao N, et al. Secure precoding optimization for NOMA-aided integrated sensing and communication[J]. *IEEE Transactions on Communications*, 2022, 70(12): 8370-8382.
- [15] Abushattal A, Althunibat S, Qaraqe M, et al. A secure downlink NOMA scheme against unknown internal eavesdroppers[J]. *IEEE Wireless Communications Letters*, 2021, 10(6): 1281-1285.
- [16] Guo R J, Fu C L, Jin Y, et al. Robust security beamforming for SWIPT-assisted relay system with channel uncertainty[J]. *Sensors*, 2022, 22(1): 370.
- [17] Zhang Q Q, Zhou H, Liang Y C, et al. Channel capacity of RIS-assisted symbiotic radios with imperfect knowledge of channels[J]. *IEEE Transactions on Cognitive Communications and Networking*, 2024, 10(3): 938-952.
- [18] Ajayi I, Medjahdi Y, Mroueh L, et al. Physical layer security by interleaving and diversity: impact of imperfect channel state information[C]//*Proceedings of the 2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*. Piscataway: IEEE Press, 2021: 299-304.
- [19] Yang T H, Zhang R Q, Cheng X, et al. Secure massive MIMO under imperfect CSI: performance analysis and channel prediction[J]. *IEEE Transactions on Information Forensics and Security*, 2019, 14(6): 1610-1623.
- [20] Zamani M R, Eslami M, Khorramizadeh M. Optimal sum-rate maximization in a NOMA system with channel estimation error[C]//*Proceedings of the Electrical Engineering (ICEE), Iranian Conference on*. Piscataway: IEEE Press, 2018: 720-724.
- [21] Son T, Kim S. An efficient PLS scheme for coded MIMO systems under imperfect channel estimation[C]//*Proceedings of the 2024 International Conference on Computing, Networking and Communications (ICNC)*. Piscataway: IEEE Press, 2024: 339-343.
- [22] Cao Z, Jin L, Han Q. Physical layer key generation for non-codebook transmission mode of 5G TDD system[C]//*Proceedings of the 2021 International Conference on Advanced Computing and Endogenous Security*. Piscataway: IEEE Press, 2022: 1-5.
- [23] Jaiswal N, Pandey A, Yadav S, et al. Physical layer security performance of NOMA-assisted vehicular communication systems over double-Rayleigh fading channels[J]. *Physical Communication*, 2023, 57: 101968.
- [24] Ahmed M, Amin Soofi A, Raza S, et al. A comprehensive survey on RIS-enhanced physical layer security in UAV-assisted networks[J].

- IEEE Internet of Things Journal, 2025, 12(16): 32538-32562.
- [25] Zhuo B T, Gu J P, Zhang G A, et al. Imperfect resolution of near-field beamfocusing for NOMA-aided physical-layer security[J]. IEEE Internet of Things Journal, 2025, 12(12): 18471-18483.
- [26] Zhang L, Wang Y H, Chen H, et al. Physical-layer security of the NOMA-assisted ISAC systems under near-field scenario[J]. IEEE Internet of Things Journal, 2025, 12(12): 18546-18553.
- [27] Abu Al-Atta M, Said K A, Mohamed M A, et al. Physical-layer security in power-domain NOMA based on different chaotic maps[J]. Entropy, 2023, 25(1): 140.
- [28] Le C B, Do D T, Voznak M. Secure transmission in backhaul NOMA systems: a physical layer security design with untrusted user and eavesdropper[J]. Digital Communications and Networks, 2024, 10(4): 1001-1013.
- [29] Fan X, Li G K, Li J Q, et al. A hybrid uplink-downlink secure transmission scheme for UAV-aided coordinated multi-point networks[J]. Digital Communications and Networks, 2025, 11(3): 925-936.
- [30] Xu D T, Cui M Y, Zhao P. Interference suppression and receiving performance improvement for local cooperation with channel estimation error[J]. Mobile Networks and Applications, 2022, 27(4): 1734-1745.
- [31] Kocharalakota A K, Upadhyaya K, Vorobyov S A. Impact of pilot overhead and channel estimation on the performance of massive MIMO[J]. IEEE Transactions on Communications, 2021, 69(12): 8242-8255.
- [32] Wang C, Li Z, Xia X G, et al. Physical layer security enhancement using artificial noise in cellular vehicle-to-everything (C-V2X) networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(12): 15253-15268.

[作者简介]



邱超圣（2001-），男，河南郑州人，河南工业大学硕士生，主要研究方向为物理层安全、非正交多址接入。



徐大同（1985-），男，河南郑州人，博士，河南工业大学讲师，主要研究方向为安全通信、6G通感一体化、干扰管理、资源分配。