周展霆

电子科技大学 · 国家示范性软件学院
ztzhou@std.uestc.edu.cn | +86 18981788896

教育背景

电子科技大学，软件工程（学术型），*硕士* 2023.9 - 2026.7

- 2023-2025 三等学业奖学金、2024-2025 电子科技大学学术青苗

西南民族大学，通信工程，*本科* 2019.9 - 2023.7

- 2022-2023 三等学业奖学金、英语六级、参与自适应滤波 LMS 算法研究

过往经历

澳门大学 · 智慧城市物联网全国重点实验室（实习），研究助理 2025.01 - 2025.12

- 参与论文《FU-DWS: Effective Federated Unlearning via Domain-aware Weight Surgery》。NIPS 2025 在投（得分 5/4/3/3，满分 6 分），**共同一作**。主要负责算法设计、实验验证、论文写作。**关键词：**联邦学习、域差异自适应、机器遗忘学习、隐私保护。
- 参与论文《Towards Federated Domain Unlearning: Verification Methodologies and Challenges》。Special Issue of IEEE Transactions on Dependable and Secure Computing [J] 在投，**共同一作**。主要负责实验验证、论文写作。**关键词：**联邦学习、域差异自适应、指标评测、机器遗忘学习、隐私保护。
- 进行中论文《Inference Acceleration for multi-task Vision Language Models on Mobile Device for certain Human-Computer Interaction》。MobiSys 2026，**共同一作**。主要负责算法设计、实验验证、论文写作。**关键词：**视觉语言模型、移动端推理加速、多模态量化、Token 压缩、多任务切换、人机交互。
- 参与论文《FedRD: Towards Memory-efficient Federated Learning via Adaptive Recomputation and Defragmentation》。SenSys 2026 在投，**三作**。主要负责实验验证。**关键词：**联邦学习、移动端部署、分布式内存受限场景。

中国民用航空第二研究所（实习），算法实习生 2024.10 - 2024.12

- 依托国家重点研发项目《多模式机场群跨域协同运行机制与运行品质评价技术研究》，实现机场传播时延相关算法优化，设计机场运行品质评价指标。
- 完成航空业内算法 Python 复现代码 1 份、算法优化方案 1 份、清理适配数据 1 份，并参与运行品质评价指标设计。

参与校内项目

国家重点研发：订单驱动的制造产业链完整性评估和风险预警理论 2023.06 - 2024.03

- 构建产业链供应分层图数据集一份。图数据挖掘专利 1 份。
- 设计图神经网络域自适应算法一份，以**一作**身份发表论文《HKTGNN: Hierarchical Knowledge Transferable Graph Neural Network-based Supply Chain Risk Assessment》在 IEEE ISPA 2023。**关键词：**图学习，域差异自适应，数据挖掘。**核心洞见：**构建了一个产业链供应图，并通过域差异自适应算法实现数据挖掘。

国家自然基金：民航复杂运行系统的安全风险监测与辅助决策技术研究及验证 2024.04 - 2026.07

- 主要负责子课题“安全-经济”综合平衡与“模型-数据”混合驱动的安全风险预测方法”的问题解决。
- **一作**在投 AAAI 2026 论文《FedIA: A Plug-and-Play Importance-Aware Gradient Pruning Aggregation Method for Domain-Robust Federated Graph Learning on Node Classification》. **关键词：**联邦学习、图学习、域差异自适应。**核心洞见：**联邦学习的分布式数据结构加深了跨域图学习的复杂性和有效性。现在的主流方法通过原型学习（需要额外上传，增加通信量，加大隐私泄露风险）或公平性聚合（服务器需要保存所有客户端的模型参数，不现实）来解决这一困难。文章提出的 FedIA 算法通过不需要额外开销的安全聚合方法提高精度，并通过剪枝降低开销和隐私泄露风险。
- **一作**在投 ICASSP 2026 2026 论文《FedSSG: Federated Learning with Non-iid Data via Stochastic Sampling-Guided Local Drift》。**关键词：**联邦学习、数据异质性。**核心洞见：**通过递归思想优化本地漂移项，感知历史梯度，并进一步解决客户端漂移带来的问题。
- **一作**在投 ICASSP 2026 2026 论文《MAGIA: Sensing Per-Image Signals from Single-Round Averaged Gradients for Label-Inference-Free Gradient Inversion》. **关键词：**联邦学习、梯度反转攻击、理论证明、隐私泄露。**核心洞见：**通过理论证明实现了让攻击者从平均梯度中感知理想场景下才能得到的具体样本梯度，并提高了梯度反转攻击的性能。

其他学术成果

《Diagnosis-driven and Modality-aware Unlearning: A Hierarchical Gradient Surgery for Multimodal Recommendation》 **一作**，ICLR 2026 在投

- **关键词：**多模态推荐系统、机器遗忘学习、隐私保护。
- **核心洞见：**多模态推荐系统遗忘主要存在三大问题：**（1）数据稀疏性与长尾分布。**多模态交互图之间连接较少，导致图数据异常稀疏，召回率较低；**（2）模态不耦合。**文本和图像在交互图连接下模态区分度更强烈，造成现有模型难以耦合；**（3）推荐系统冷启动。**协同过滤文献表明，互动稀少时相似性估计会变得不可靠，从而加剧冷启动效应和流行度偏差。文章提出的 DAMU 算法尝试从图神经网络模型和模态感知出发，解决上述问题带来的遗忘困难问题，保护用户隐私。