

密言 Yan Mi

✉ miyan26@mails.ucas.ac.cn

☎ 155-8818-6051

📍 北京

🌐 Academic Homepage

📝 Personal Blog

🐙 GitHub: M1YAN

👤 Google Scholar

研究兴趣: Agent · LLM4Rec · User Simulation · Agentic RL

🎓 教育背景



中国科学院计算技术研究所

2026.09 - 至今

智能算法安全全国重点实验室 人工智能 硕士研究生 导师: 曹婧



北京邮电大学

2022.09 - 2026.06

未来学院 (元班) 计算机科学与技术 本科

💼 实习经历



阿里巴巴·淘天集团

2025.12 - 2026.08

推荐算法研究型实习生 淘宝首页信息流

RecVerse: 面向电商推荐的真实用户行为仿真

WWW 在投 / 共同一作

Agentic RL · User Simulation · Benchmark · GUI Agent · Hierarchical Memory

- **核心实现:** 负责项目核心代码实现, 围绕电商首页推荐场景的 **User Simulation**, 打通 GUI 交互环境、用户仿真 Agent、训练与评测链路, 生成连续浏览、点击、加购与购买轨迹。
- **Benchmark 构建:** 实现 USB 交互环境, 重建曝光商品、页面布局与界面状态, 支持偏离真实日志动作后的多轮探索; 涵盖 **5,274 条轨迹**、**69,842 次动作**、**8 类行为**。
- **Agent 记忆设计:** 实现工作 / 情景 / 偏好三级记忆, 分别保留近期视觉上下文、会话行为与长期购物意图; 将记忆更新作为可学习动作, 与浏览决策联合优化, 保持跨页面偏好一致性。
- **SFT 数据与训练:** 使用教师模型补全用户心态与记忆更新, 构建结构化 SFT 数据; 以幂律平滑重采样缓解行为长尾, 完成 **Qwen3.5-2B** 冷启动。
- **Agentic RL:** 实现多轮 rollout 与轨迹级 **GRPO**, 联合优化行为分布、意图一致性与输出格式, 使用 **Megatron-LM + vLLM** 完成训练与采样。
- **论文结果:** 相较 GUI 基线 STA, 商品级 F1 从 **4.27% 提升至 7.19%**, 品类一致性 HCO 从 **23.11% 提升至 32.64%**; 匿名轨迹对比中获得 **92%** 的人工偏好。

🔬 科研项目

ARGUS: 多智能体错误信息识别与纠偏

ICLR 2026 / 第二作者

Multi-Agent System · Dataset · Goal-Aware Reasoning

- **Dataset 构建与威胁建模:** 参与构建 **MisinfoTask** 数据集, 覆盖 **108 个复杂任务**、注入点与参考流程, 评估 Prompt Injection、RAG Poisoning、Tool Injection 对多智能体协作的影响。
- **两阶段防御:** 参与提出免训练 ARGUS 框架, 将智能体通信建模为有向图, 结合拓扑重要性、语义相关性与通信频率定位关键传播信道, 以目标感知推理进行多轮纠偏。
- **论文结果:** 在 GPT-4o-mini 的三类攻击平均结果中, 错误信息毒性 MT 从 **5.22 降至 3.43**, 任务成功率从 **67.43% 提升至 78.43%**。

📄 代表论文

Towards Faithful Simulation of Human Shopping Behavior

Jiakai Tang*, Yan Mi*, Jing Yu*, et al. WWW 在投 * 共同一作

Goal-Aware Identification and Rectification of Misinformation in Multi-Agent Systems

Zherui Li, Yan Mi, et al. ICLR 2026 第二作者

Omni-Safety under Cross-Modality Conflict: Vulnerabilities, Dynamics Mechanisms and Efficient Alignment

Kun Wang, Zherui Li, Zhenhong Zhou, Yitong Zhang, Yan Mi, et al. NeurIPS 2026

💻 技术能力

训练与推理 SFT、GRPO、Agentic RL、Megatron-LM、vLLM

Agent 与评测 GUI Agent、分层记忆、用户仿真、Benchmark 构建、多智能体安全

工程基础 Python、PyTorch、Linux、Git、Shell、 $\LaTeX$

🏆 荣誉奖励

全国一等奖·全球校园人工智能算法精英大赛 (2024) 北京市一等奖·RAICOM 机器人开发者大赛 (2024)

北京邮电大学学业奖学金 (2025) 三好学生 (2022 - 2023 学年)