闫金柱

2000.01 | 198-0301-3687 | yanjz22@mails.tsinghua.edu.cn

Inspiring Group Homepage: https://liuzhuotao.github.io/

教育经历

清华大学 **网络科学与网络空间研究院 – 博士** **2022.09～2027.06**

- **研究方向**：AI 驱动的流量分析系统 | **导师**：刘卓涛 | **学术成果**：网络系统与安全顶会论文 2 篇，国内外专利 7 项

北京航空航天大学 **高等理工学院 – 计算机科学学士** **2018.09～2022.06**

- **GPA**：3.93/4.0（前1%）| **荣誉奖项**：宝钢奖学金（全校仅四名）、国家奖学金等数十项奖学金及竞赛奖项

项目经历

基于大语言模型的流量分析智能体技术 **清华大学-华为研究项目，技术负责人** **2025.12～2027.06**

- 在 Agentic Reasoning for Traffic Analysis 方向开展研究，聚焦于**为大语言模型提供网络流量分析领域的专家知识和操作工具链**，进而构建真正具备专家级推理能力的通用流量分析智能体；例如，基于 Agentic RAG 工具链为智能体提供流量样本数据库知识，基于知识图谱检索工具链为智能体提供流量交互上下文知识，基于渐进式披露机制为智能体提供威胁情报等辅助语料知识

基于 Transformer 模型的加密流量识别系统 **字节跳动实习项目，技术负责人** **2025.02～2025.12**

- 提出了基于多模态流量表征与模态融合的 Transformer 流量分析模型，并针对工业环境中海量背景流量所带来的假阳性问题提出了基于训练噪声清洗与假阳性结果召回的优化技术；研发成果在恶意流量识别与应用流量识别两类关键加密流量检测场景下落地应用，实现了**千万分之一级假阳性率下对主流攻击工具与移动应用的稳定检出**

大语言模型的移动端部署应用 **腾讯实习项目，技术负责人** **2024.07～2024.09**

- 在 QQ 浏览器的移动端应用程序中集成大语言模型的推理能力，进而对用户的本地文档、浏览痕迹进行本地分析，以优化搜索结果、广告投放；基于模型量化与 KV Cache 优化技术使**端侧推理开销降低 60%**

代表论文

CertTA: Certified Robustness Made Practical for Learning-based Traffic Analysis **网络安全顶级会议 USENIX Security，第一作者** **2025.08**

- **AI 模型的对抗安全认证**：针对流量数据中的多模态对抗扰动构建了通用的鲁棒性认证范式，显著提升人工智能模型面对流量分析对抗攻击时的鲁棒性表现，**多类 AI 模型的可认证准确率平均提升超 80%**
- **异常检测的联合防御机制**：提出了将异常检测与随机平滑范式结合以应对不同强度对抗攻击的联合防御机制，为对抗攻击创造了进退两难的攻击困境，较单一系统**攻击防御成功率平均提升超 30%**
- **Code:** https://github.com/InspiringGroup-NeoLab/CertTA

Brain-on-Switch: Towards Advanced Intelligent Network Dataplane via NN-Driven Traffic Analysis at Line-Speed **网络系统顶级会议 USENIX NSDI，第一作者** **2024.04**

- **硬件感知的神经网络架构设计**：提出针对可编程交换机硬件限制的二值循环神经网络架构，于网络数据平面实现神经网络驱动的线速流量分析，单交换机流量**推理吞吐达 100Gbps 至 1.6Tbps**
- **准确高效的模型协作分析机制**：提出网络控制平面 Transformer 模型与数据平面二值 RNN 模型的协作流量分析机制，构建了兼具高准确率、高速、高吞吐的智能流量分析系统，较最先进方案**准确率平均提升超 13%**
- **Code:** https://github.com/InspiringGroup-NeoLab/Brain-on-Switch

竞赛奖项

基于大语言模型的网络流量捕获与处理助手 **华为GDE&AskO3全球开发者大赛优秀智能助手奖** **2024**

- 基于华为 AskO3 AI 引擎构建可以快速编写自定义网络流量嗅探与分析处理程序的智能体助手工具，作为高校组唯一获奖代表参会进行作品分享

高效协作的互联网动态行为安全可信技术与应用 **中国电子学会科技进步一等奖** **2024**

- 贡献加密恶意网络流量检测关键技术成果，通过中国电子学会组织的科技成果鉴定并授予科技进步一等奖

基于循环神经网络的线速流量分析系统 **中国高校计算机大赛网络技术挑战赛三等奖** **2023**

- 在可编程交换机中部署专门为处理序列数据而设计的循环神经网络模型