张禹喆

15611511983 | 22072125@emails.bjut.edu.cn

教育经历

学　　校：**北京工业大学**　　专　　业：信息安全（实验班）

加权平均分：**91.93/100**　　专业排名：**1/60**　　CET4 / CET6： 614 / 534

核心课程成绩：

网络协议分析与设计：100　　网络攻击与防护：100　　数据结构课设：98　　数据结构与算法：96

密码学：96　　安全协议：94　　操作系统原理及安全：93　　计算机网络（双语）：92　　信息安全数学基础：92

项目经历

1. 项目：《The Eye of Sherlock Holmes: Uncovering User Private Attribute Profiling via Vision-Language Model Agentic Framework》　　2024.12 – 2025.4

动机：

随着 VLM 的快速发展，我们发现了一个新的隐私风险：这些模型能够从个人日常照片中推断出敏感特征，甚至能分析出抽象的个性和社交特质。考虑到现代应用程序可轻易访问用户相册，且从多张照片中的推断比单一照片更具威胁性，我们亟需深入研究此类隐私攻击的潜力与防御机制。

内容：

构我们构建了 PAPI——首个专门用于研究个人照片中隐私属性分析的大型数据集，包含 251 位志愿者的 2,510 张图像和 3,012 个隐私属性标注。同时，我们提出了 HolmesEye 框架，结合视觉语言模型和大语言模型，提取图像内部和图像间的信息。实验表明，HolmesEye 在隐私属性推断准确率上比现有方法平均提高 10.8%，在抽象属性预测上超过人类 15.0%，且分析速度比人类快 3.45 倍，凸显了这一技术带来的严峻隐私挑战。

贡献：

作为**第二作者**参与设计模型架构，独立完成代码的撰写，参与完成消融实验与性能验证、论文撰写等工作。

阶段成果：

ACM MM 2025（CCFA）会议在投。

---

2. 项目：《WaveConvX: Multi-Level Wavelet Enhancement for Histopathology Image Classification》　　2024.12 – 2025.4

动机：

传统卷积神经网络虽在病理图像分类上取得进展，但难以同时捕捉组织的多尺度特征和丰富的高频细节。这些特征对癌症诊断至关重要，因此我们提出了一种结合多级小波分解和卷积网络的创新方法——WaveConvX，以增强模型对病理组织的理解能力。

内容：

WaveConvX 将双阶段离散小波变换与 ConvNeXt 骨干网络相结合，对特征图进行多频带分解。我们设计了自适应幂 Gabor 卷积（APGConv）处理高频成分，为中频使用注意力机制，有效融合全局和局部形态学特征。在三个公开数据集上，WaveConvX 超越 10 种 SOTA 基线，乳腺癌二分类准确率 99.6%（40×），胃癌分类 F1 提升 2.2%，肺结肠癌准确率达 99.3%

贡献：

作为**第一作者**设计模型架构，完成消融实验与性能验证，论文撰写等工作。

阶段成果：

IEEE SMC 2025（CCFC）会议在投。

---

3. 项目：《GECAT: A Graph-Enhanced Causality-Aware Transformer for Industrial Control System Intrusion Detection》

2024.9 – 2025.3

动机：

现代工业控制系统因连接性不断增强而面临越来越复杂的攻击，传统入侵检测方法无法有效捕捉复杂时序动态和传感器间关联，忽略物理因果关系，难以抵御高级持续性威胁。

内容：

我们提出了 GECAT 框架，创新性地结合了三方面优势：物理拓扑知识（邻接矩阵）、数据驱动的图表示学习和多头注意力机制。关键贡献包括因果感知机制、三重融合邻接矩阵、动态因果层和 Transformer 序列建模与因果正则化的协同。实验证明 GECAT 在 SWaT 和 WADI 测试平台上显著优于十个基准方法，F1 分数分别达到 98.6%和 98.7%，误报率仅为 0.16%和 0.04%，多类攻击分类任务上也表现卓越。

贡献：

作为**第一作者**设计模型架构，完成消融实验与性能验证，论文撰写等工作。

阶段成果：

IEEE SMC 2025 （CCFC）会议在投。

---

4. 项目：《DynaFlow Logic Transformer: A Neuro-Symbolic Approach to Industrial Control System Intrusion Detection》

2024.9 – 2025.3

动机：

工业控制系统（ICS）面临复杂攻击，传统的入侵检测缺乏动态传感器关系建模、可解释决策机制和数据不平衡处理能力，亟需创新解决方案提升关键基础设施安全性。

内容：

提出 DynaFlow Logic Transformer，融合 Transformer 动态邻接估计、阈值逻辑规则和 WGAN-GP 数据增强，在 SWaT 和 WADI 数据集上实现 97.9%和 96.8%异常检测 F1 分数，93.9%和 96.7%攻击分类 F1 分数，显著超越现有方法，同时提供可视化邻接矩阵和逻辑规则增强系统透明度。

贡献：

作为**第一作者**设计模型架构，完成消融实验与性能验证，论文撰写等工作。

阶段成果：

已被 ICIC 2025 （CCFC）会录用为 **oral** 。

竞赛经历

2023 美国大学生数学建模竞赛（队长）	国际一等奖（M 奖）
2025 全国大学生软件创新大赛（项目负责人）	区域赛三等奖

荣誉奖励

北京工业大学 学习优秀奖	2023.11、2024.11
北京工业大学 创新创业奖	2023.11
北京工业大学 三好学生	2023.11