王绎鸣

Email: YimingWang0619@gmail.com

Tel: 18350472267

个人博客主页：https://areswang0619.github.io/

个人介绍

北方工业大学，信息学院，人工智能专业 2021.9 - 至今

- **均分绩点：** 92.50 • **专业排名：** 1/25
- **核心课程：**知识工程（97）、模式识别与计算机视觉（93）、机器学习（91）、数据结构（98）、计算机网络（91）、概率论与数理统计（96）、线性代数（96）
- **英语成绩：**CET4: **632** CET6: **572** 具备扎实的英语基础，可无障碍阅读英文文献且写作能力好。
- **荣誉奖项：**共获校级各类奖学金十次、体育类奖项若干，身体素质好，性格开朗，善于沟通。

科研经历

大规模流数据集成与分析北京市重点实验室 | 客座学生

■ **学生三作/《Attack based on data: A novel perspective to attack sensitive points directly》**
CCF-C，已出版，信工所期刊《Cybersecurity》

➤ **研究内容:** 对抗攻击可以是不针对模型的，而是从对抗样本出发。通过深度学习去学习对抗样本中的敏感点。通过这种方式训练出的深度学习模型可以在面对一个全新的数据集的时候快速找到样本中的敏感点并对其进行篡改，只需要微小的修改就可以使服务端的深度学习模型产生误判。相比于基于进化算法的 One-pixel attack 的 ASR 为 68.8%，而我们的方法的 ASR 达到 89.1%，提高了 20.3%。

■ **学生三作/《基于数据特征的无监督对抗攻击》**
CCF T2 类，中文核心，在投

➤**研究内容:** 该论文以上一篇论文为基础，同样是聚焦于对抗攻击，但是查找敏感点的手段不再是使用深度学习模型而是使用无监督的机器学习算法。同时，在数据上不再局限于时序数据，而是可以迁移到图像数据。在 Fashion-MNIST 数据集上，由本文方法生成的对抗样本相较于 One-pixel attack 方法生成的对抗样本在同一深度学习模型上准确率低约 25%。

■ **第一作者/《Reasoning with Large Language Models on Graph Tasks: The Influence of Temperature》**
EI 会议，已检索

➤**研究内容:** 探究 LLM 在图形数据上的推理能力，以 NLGraph 为 benchmark 特别关注了温度参数对模型性能的影响。温度敏感性在不同的任务和水平下各不相同。调整温度参数可以提高某些图推理任务的准确性，特别是对于模型的复杂性与其能力相匹配的任务，由于生成答案的确定性和一致性较高，温度越低，准确率越高。随着温度的升高，创造性和无组织性也随之提高，导致准确率下降。

智能助老服务机器人的研究与实现 | 国家级大创，第二负责人

➤ **研究内容:** 设计基于 RNN 的中文大数据系统数据置信度评估模型，爬取相关数据集，将文本中的事件向量化，通过循环神经网络的学习训练来挖掘表示文本深层的特征。设计人体姿态识别模型，运用空间-时间图卷积网络（GCN），用于分析人体骨架数据，以识别和分类不同的动作。实现了基于 LLM 的智能药箱，通过 OCR 技术识别处方信息，推荐适合的药品，提供风险评估报告和用药指南。

获奖经历

- 中国智能机器人大赛**全国一等奖**
- 中国机器人及人工智能大赛**全国二等奖**
- 全国大学生英语竞赛**全国二等奖**
- 中国智能机器人大赛**全国二等奖**
- 全国大学生翻译大赛**全国三等奖**
- 中国机器人及人工智能大赛**北京市一等奖**
- 蓝桥杯 C/C++ 组**北京市二等奖**
- 蓝桥杯 Python 组**北京市三等奖**