

薛世喆

◎ 南京市栖霞区文苑路九号(210023)



教育经历

南京邮电大学(双一流) 理工科强化班(计算机科学与技术) 2022.09-2026.07

GPA: 4.17 / 5.00 排名: 20 / 298 (前7%)

主要课程:操作系统(96) 数据结构(94) 汇编语言程序设计(98) C语言程序设计(90)

JAVA程序设计(**94**) 算法设计与分析(92)

项目经历

神经元可解释性引导的迁移黑盒攻击(对抗攻击、目标检测)

2024.09-2025.04

- 针对解释性引导的黑盒攻击效果差的问题,提出了一种基于神经网络逐层增量分解(LID)的中间 层攻击方法,并与SoftMax gradient-LRP(SG-LRP)和集成梯度(IG)进一步结合,利用 SoftMax函数增加类区分度的同时,使用IG减缓梯度饱和的问题,改进动量优化方法,使用预攻击 提前稳定动量方向,用步长放大器替换Sign函数降低动量和梯度方向的偏差,提高攻击成功率。
- 《Explanation-inspired Transferable Adversarial Attacks with Layer-wise Increment Decomposition》**第一作者**,负责代码编写,论文撰写,**已发表**ICIC2025(**CCF-C**)。

基于重要神经元的神经网络对抗攻击方法(对抗攻击)

2024.04-2024.08

- 针对黑盒攻击的攻击耗时和迁移效果的平衡问题,公开了一种基于神经元决策归因的迁移攻击方法,利用输入图片在源模型和其中重要神经元生成的掩膜模型的耦合梯度信息实施攻击,平衡了攻击耗时和攻击效果的关系。
- 参与专利《一种基于重要神经元的深度神经网络对抗攻击方法》第三作者,专利**已受理**,负责实验验证、专利撰写。

数学、编程、英语

• **数学**: 工科数学分析(上)(92)、 工科数学分析(下)(91)、 概率统计和随机过程(92)

• 编程: 熟练掌握C语言、C++、熟悉Java、Python。

• 英语: 四级: 564; 六级: 531

荣誉奖项

- 一等奖学金(2023)
- 优秀学生干部(2023)、南京邮电大学"优秀青年志愿者"称号(2022、2023)
- 全国大学生英语竞赛C类三等奖(2024)、创新杯大学生课外学术科技作品竞赛特等奖(校级)

学生工作

曾任班级副班长,贝尔英才学院学生会主席、青协宣传部部长负责学院新媒体宣传工作

自我评价与规划

本人性格乐观开朗、坚韧不拔、自驱力强; 热爱编程,喜欢团队合作; 热爱生活,喜欢摄影、健身; 殷切期盼度过一个充实的研究生生活!