曾行健

联系方式：(+86)13829651972 个人邮箱：zengxingjian@seu.edu.cn

教育经历

东南大学，网络空间安全学院，(学术学位)硕士在读 2023.09 至今

- **学习专业**：网络空间安全
- **规格化成绩**：81.71(前25%)

东南大学，网络空间安全学院，本科毕业 2019.09 - 2023.06

- **学习专业**：网络空间安全

研究内容

Boosting open-world website fingerprinting attacks via outlier exposure and cross-domain adversarial training

- 加密流量分析工作(进行中)；预计投递至ACM Conference on Computer and Communications Security(CCS'25第二轮，截稿日期4.15)
- 研究动机：
  - 在开放世界场景中，现有网站指纹攻击方法存在两方面局限：**A.缺乏对监控外网站流量进行合理建模**，**B.易受对抗流量防御措施干扰**；
  - 相关工作缺乏使用现实合理的开放世界设置对攻击方法进行评估；先进攻击方法对流量防御措施的抵抗能力来自人为设计的鲁棒特征表示。
- 主要贡献：
  - 监控外网站流量本质上是相对于监控内网站流量的分布外数据。因此我们通过引入**分布外损失**来最大化分类模型对分布外样本的不确定性，以提升现有网站指纹攻击方法在现实开放世界场景中的表现；
  - 为了避免与流量防御措施陷入**对抗性博弈循环**，我们不再局限于设计更加复杂的人工流量特征表示，而是通过引入基于对比学习的跨域对抗训练策略，以增强现有攻击方法对流量防御策略的鲁棒性。

AHE:Adaptive hybrid-sampling ensemble for large-scale highly imbalanced data classification PDF

- 数据挖掘方向工作；已投递至*Knowledge-Based Systems* (中科院1区，CCF-C) 状态：Under Review
- 主要贡献：
  - 提出一种新颖的基于集成学习与混合采样的不平衡分类方法。通过在boosting集成架构中引入恰当的混合采样策略，克服了已有基于采样与集成的不平衡学习方法固有的缺陷；
  - 在24个异质不平衡数据集上与4种常见的机器学习分类器搭配时，取得了比其他17种方法更好的表现。

M3S-UPD: Efficient Multi-Stage Self-Supervised Learning for Fine-Grained Encrypted Traffic Classification with Unknown Pattern Discovery

- 非一作/学生一作，负责文章部分内容(abstract,introduction与method)撰写。

项目工作

协助组内"面向暗网抑制的普适性安全理论研究"项目申报，负责项目书多个章节撰写

获奖情况

"华为杯"第二十一届中国研究生数学建模竞赛三等奖

个人简介

- 具备初步独立、持续开展研究的能力；较善于寻找研究问题空间与创新方向；
-