王硕

男 | shuo.wang@studenti.unipd.it | 15621048621 | GitHub/wshuo97

教育经历

帕多瓦大学，计算机科学，在读博士生，**导师：Prof. Mauro Conti** 2022.10 –至今
研究方向：计算机网络安全，无线通信安全。
利物浦大学，计算机科学，访问学生，**导师：Prof. Junqing Zhang** 2025.04 –2025.08
华东师范大学，计算机技术，硕士，**导师：Prof. Xiangfeng Wang** 2019.09 –2022.03
研究方向：图神经网络应用，强化学习算法。
中科院计算技术研究所，SSD 驱动工程师，访问学生，**导师：Prof. Dejun Jiang** 2021.06 –2021.08
山东科技大学，物联网工程，学士。 2015.09 –2019.06

作品列表

- **DOA-CGAN：基于 GAN 的雷达信号到达角度估计增强应用** 2024.09
- **项目描述：**本研究中提出了一种生成方法，即“通过条件生成对抗网络进行到达方向 (DOA) 估计 (DOA-CGAN)”，以解决干扰攻击下雷达系统 DOA 估计不可靠的问题。当前的 DOA 估计方法在来自不同方向的随机干扰信号下并不总是能取得良好的效果，并且通常需要事先了解预期信号。DOA-CGAN 模型由一个无监督生成器和一个有监督鉴别器组成。生成器学习如何从接收信号协方差矩阵中消除干扰，并生成一个新的矩阵，鉴别器可以识别该矩阵是否有效。鉴别器使用条件标签（真实信号协方差矩阵）来区分真实数据和生成数据。在这个框架中，生成器不直接使用这些标签，从而在测试阶段保持灵活性。
- **相关产出：**相关论文”Evaporative Angle: A Machine Learning Approach-Assisted DOA Estimation under Jamming，” 已发表在 IEEE Wireless Communication Letters（10.1109/LWC.2024.3454108）。

- **GANSec: 通过定制条件 GAN 增强增强监督无线异常检测的鲁棒性** 2025.06
- **项目描述：**该项目与法国国家信息与自动化研究所 (INRIA) 研究人员合作完成。本文提出的 GANSec 方法，一个特殊的条件生成对抗网络 (GAN) 框架，旨在提高监督无线异常检测的鲁棒性。我们调研发现，无线异常检测面临诸多问题，例如数据不足、类别不平衡、环境变化以及数据收集成本高昂。这些问题使得训练和推广更优的模型变得困难，尤其是在模型可能遇到新的网络情况时。GANSec 使用生成器 (G) 和鉴别器 (D)：G 使用随机噪声和条件信息（例如目标标签和上下文）来生成类似于真实无线信号的虚假时间序列数据，而 D 用于区分虚假数据和真实数据。GANSec 专为无线数据设计，采用适用于序列数据的 LSTM 和 2D CNN 等骨干网络，力求保留统计特征并运用领域知识。我们使用 5G 网络干扰异常场景测试了 GANSec 框架；使用 GANSec 生成的数据训练的分类器模型在新的网络条件下的表现远优于使用原始数据或其他基线方法训练的分类器模型，展现出更好的泛化能力和鲁棒性。
- **相关产出：**论文”GANSec: Enhancing Supervised Wireless Anomaly Detection Robustness through Tailored Conditional GAN Augmentation，” 已被会议 ESORICS 2025 接收。

- **Capodoglio: Tackling Multi-Armed Bandit Jamming Attacks** under review

- **Catch-All GNN: A Graph Neural Network Approach for Anomaly Detection in WiFi Networks** under review

- **ADFed: Asynchronous Decentralized Federated Learning with Efficient Cluster-Based Aggregation and Privacy Assurance** under review

- **Step into Balance: A Consistency-Aware and Loose Homophily Guided Generative Method for Class Imbalanced Graphs** under review

- **Confundus: Mitigating Hostile Wireless Source Localization** Accepted by IEEE CNS 2025

- **PreyLoop: Reconciliation of Privacy Protection and Security Defense in Collaborative Deep Learning** under review

实习经历

SSD 主控程序开发, 中科院计算技术研究所 2021.06 –2021.08

- **背景介绍：**固态硬盘 SSD 的出现与应用将代表着计算机的存储速度与容量得到了巨大的提升，然而在之前的计算机设备中大量应用的是机械硬盘等类似结构的存储设备，由于固态硬盘与机械硬盘在原理与结构上存在着巨大的差别，因此在应用 SSD 时需要通过主控程序将 SSD 硬盘按照计算机系统的读取规则进行适配，从而将 SSD 应用到计算机中。
- 学习固态硬盘的存在原理与基本结构，更加深入的理解计算机工作的原理。
- 阅读开源项目 openSSD 的代码，理解垃圾回收机制在 SSD 中的应用原理。
- 设计对应的垃圾回收机制，同时使用 C 语言将其实现并进行实际 SSD 测试。

项目经历

基于 GAN 的 RFFI 多接收机影响解决方案（利物浦大学） 2025.04 - 至今

- **背景介绍：**射频指纹识别 (RFFI) 是一种无线设备身份验证方法，它利用硬件差异导致的独特信号特征。然而，传统的 RFFI 模型通常无法在不同接收机之间有效工作，因为设备指纹可能会与接收机特有的效应混淆。
- 为了解决这个问题，在本次研究期间，我们正在研究如何在多接收机场景中使用生成对抗网络 (GAN)，以发挥 GAN 的数据生成与增强在信号领域里的潜在性能。在我们的研究中，特征提取器（生成器）学习生成仅与发射域相关的特征，同时使用域鉴别器进行对抗训练，域鉴别器尝试查找特定于接收机域的信息。这种对抗性训练引导模型从特征中消除接收器特定的差异，从而使设备识别更加稳健，并且不受接收器域的影响。此外，还会联合训练一个分类器，以确保学习到的特征仍然保留重要的设备身份信息。
- **相关产出：**论文已完成并投稿到 AAAI 2026。

基于 Town-Crier 的去中心化分布式数据系统（代尔夫特理工大学） 2024.06 - 2024.10

- **项目介绍：**本项目基于区块链技术，构建一套安全可信的数据共享框架；通过设备状态审计与入站 Oracle、信任证据自动监控及去中心化 Town-Crier 机制，实现数据在生成、传输和存储全流程的不可篡改与可追溯。
- 对 Town-Crier 进行适配，实现去中心化的本地系统与区块链的交互过程。
- 使用 Intel SGX 的 Enclave 技术实现高可信的数据本地处理功能。
- 开发可用的共识算法以应用在系统中，提高单个结点及整体系统的威胁应对能力。

获得奖项

- 第 42 届 ACM-ICPC 亚洲区域赛（新疆） 铜奖
- 第 42 届 ACM-ICPC 亚洲区域赛（青岛） 铜奖
- 2016 ACM-ICPC China Final（上海） 铜奖
- 第 41 届 ACM-ICPC 亚洲区域赛（青岛） 铜奖
- “浪潮杯”第八届山东省 ACM 大学生程序设计竞赛 银奖
- 第八届蓝桥杯大赛（国赛） 二等奖
- 2017 中国高校计算机大赛团体程序设计天梯赛（决赛） 一等奖
- 2017 第一届百度之星开发者大赛 优秀应用作品奖
- CCF 大学生程序设计竞赛（华东赛区） 银奖

个人介绍

- 熟悉 C/C++、Python 等编程语言，熟悉常用的编程相关工具，有良好的代码习惯；参加过 ACM 及各类比赛，并获得 ACM-ICPC 区域赛铜奖等奖项，CCF 计算机软件能力认证 400 分 (前 0.3%)，具有扎实的数据结构和算法基础；熟悉 Linux 操作系统，常年使用 Ubuntu 作为个人工作环境；
- 在多年的求学生活中，多次与不同方向和国家的研究人员进行合作，在合作过程中了解了不同领域的相关技术也曾参与过相关项目，如 SSD 驱动开发、区块链与分布式算法及 RFFI 信号系统及处理等；熟练掌握英文学术阅读、写作与口语技能。