

# 刘子正

邮箱: lzz@purdue.edu

电话/微信: (+86) 135-0403-9426

个人主页: <https://cangjie103.github.io>

## 教育背景

2021.08-目前	普渡大学, 美国	计算机科学	博士在读
2018.08-2019.12	哥伦比亚大学, 美国	计算机科学	理学硕士
2017.08-2018.05	伊利诺伊大学芝加哥分校, 美国	电气与计算机工程	留基委公派交换生
2014.09-2018.06	东北大学, 中国	计算机科学与技术	工程学士

## 科研经历

2021.08-目前	分布式系统隐私与安全	普渡大学
项目1 (隐私计算 / 人工智能安全): 利用多方安全计算设计一种具备隐私保护和拜占安全的联邦学习聚合方案. (合作: 罗格斯大学, 苏黎世联邦理工学院)		
项目2 (卫星通信 / 人工智能安全): 基于星地网络特有的威胁模型, 为其设计通信信道感知的联邦学习投毒攻击的防御方案. (合作: 弗吉尼亚理工大学)		
项目3 (形式验证 / 协同攻击): 在分布式系统中, 使用形式验证的手段为基于机器学习的入侵检测系统提供关于潜在的协同攻击的证据, 以提高检测系统对协同攻击检测的准确率. (合作: 弗吉尼亚理工大学)		
项目4 (车联网安全): 在车联网基于地理位置的路由协议GeoNetworking (ETSI EN 302 636 / IEEE 1609.3)中发现安全漏洞. 设计实验评估隐患危害并提出解决方案.		
2019.01-2019.12	基于家用路由器的物联网设备信息保护系统	哥伦比亚大学
• 通过机器学习方法检测来自家用物联网设备的潜在信息泄漏或流量异常, 实时更新路由器端防火墙以保护用户信息及设备的隐私与安全.		
2017.08-2018.05	基于数据融合的室内导航系统	伊利诺伊大学芝加哥分校
• 基于 Raspberry Pi 开发手持室内导航系统, 解决 GPS 或其他卫星定位系统在室内信号较弱的问题.		
• 手持导航仪收集来自陀螺仪、WiFi 接口等信号源的信号数据. 通过数据融合和校正算法判断用户在室内所在位置. 用 Dijkstra 算法为用户提供当前位置到目的地的最短路径.		

## 学术成果

- **Liu, Zizheng**, Bharat K. Bhargava, and Nagender Aneja. "STARFed: Link-Aware Defense Against Poisoning Attacks in Satellite-Terrestrial Federated Learning." *IEEE Transactions on Network Science and Engineering* (2025). (IF:7.9, JCR1区)
- **Liu, Zizheng**, Shaan Shekhar, and Chunyi Peng. "Breaking Geographic Routing Among Connected Vehicles." In 2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 42-54. IEEE, 2023. (CCF B, 录用率: 47/235 = 20%)
- Zhang, Zhehui, Yanbing Liu, Qianru Li, **Zizheng Liu**, Chunyi Peng, and Songwu Lu. "Dependent Misconfigurations in 5G/4.5 G Radio Resource Control." ACM CoNext 2023 (Proceedings of the ACM on Networking (PACMNET)) (2023). (CCF B, 录用率: 4/41 = 9.8%)
- **Liu, Zizheng**, and Chunyi Peng. "Poster: Security Analysis for Emerging Cellular Network Technologies." NSF AI Institute for Future Edge Networks and Distributed Intelligence (AI-EDGE Institute) Annual Meeting (2022).
- **Liu, Zizheng**, and Chunyi Peng. "Quality Measurement over Quality Data Reuse in Cellular Networks." 2nd NSF Workshop on Overcoming Measurement Barriers to Internet Research (WOMBIR-2) (2021).

## 学术兼职

期刊评审: IEEE-Transactions on Information Forensics and Security, Computer Networks, Computer Communications

## 荣誉奖励

- DSN'23 Student Travel Grant (2023)
- 本科期间两次获得国家奖学金 (2015, 2017), 多次获得校一或二等奖学金 (2015, 2016, 2017)
- 本科获国家留学基金委资助去美国伊利诺伊大学芝加哥分校交流学习, 期间完成的本科毕业设计获得优秀毕业设计奖.

## 教学经历

- 普渡大学, 助教: CS536 数据通信与计算机网络, CS448 关系数据库系统导论, CS176 Python数据工程
- 哥伦比亚大学, 助教: COMS4701 人工智能

## 技能特长

- 编程语言及开源框架: Python, C++, PyTorch, MP-SPDZ, ns3
- TOEFL: 108/120; GRE: 325/340 + 5/6