刘 小垒 | 个人简历

电子科技大学 – 高新区（西区）西源大道 2006 号, 成都市 611731

(+86) 17713401296 • luxaole@gmail.com • https://xiaolei.tech

教育背景

电子科技大学 **博士**

软件理论与分析, 导师：张小松 教授、长江学者 & 朱清新教授 *2014.09–至今*

研究方向：对抗生成模型 (Adversarial Samples)、机器学习及应用、群体进化优化算法、网络安全

电子科技大学 **本科**

软件工程, 导师：张小松 教授、长江学者 *2010.09–2014.06*

研究方向：网络安全

项目经历

机器学习算法本身的安全性研究 - 3 项

一种针对图像数据 + 流量数据 + Android App 的黑盒对抗样本生成方法 **横向课题**

伊利诺伊香槟分校合作项目，主研 *2017—至今*

- 任意性：以很低的相对误差扰动原始数据，使攻击者可以将检测结果扰动成任意的类别标签。
- 通用性：该方法能够攻击常见的机器学习算法。
- 黑盒性：无需目标网络的内部参数，只需结果输出的各类标签的概率就可以生成所需的对抗样本。
- 随机性：每次生成的对抗样本是不同的，能够更好的抵御防御蒸馏等手段。

决策优化类算法的研究 - 3 项

无线传感器网络布局优化算法 **横向课题**

中电集团某研究所合作项目，主研 *2016—2017*

- 将传统的基于概率学的覆盖率计算方法改进为基于几何学来计算，提高了计算速度与精度。
- 结合基于改进 t 分布的进化优化算法，实现无限传感器网络布局自动化调整的功能。

无人飞行器智能协同控制系统 **横向课题**

中电集团某研究所合作项目，主研 *2015—2016*

- 针对无人飞行器航迹规划算法在复杂环境下飞行时存在的无法动态规划航迹、收敛速度慢和容易陷入局部最优等问题，提出一种群体智能进化优化算法。通过建模随机生成等效于复杂环境下的数字地图，结合最小航迹段长度、最大拐弯角、最大爬升/下滑角、航迹距离约束、最低飞行高度等实际情况等限制，运用该改进算法进行动态航迹规划。
- 提出一种协同控制优化算法，解决多架无人飞行器之间无法有效协同完成指定任务的问题。

智能处理与效能评估系统 **横向课题**

中电集团某研究所合作项目，主研 *2014—2015*

- 利用分布式爬虫工具对主流新闻网站、社交网站上的内容进行爬取。
- 利用中文分词工具对爬取到的数据进行关键词提取、词性及情感分析，然后再利用模糊聚类算法进行聚类，为用户进行评估提供可视化依据；并对之后的舆论发展趋势进行预测。

大数据安全 - 4 项

数盾 - 数字水印系统关键技术研究 **自主创业**

团队自主创业项目，主研 *2016—2017*

- 支持多样化数据类型，跟踪数据流通轨迹，数字化标记，具备数据源可追溯性。
- 实现文件加密保护；在安全流通基础上，实现权限细分、权限可控（授予、回收等特性）。

电子商务网站钓鱼页面检测的研究 + 僵尸网络检测的研究 + 匿名网络检测技术研究 **省部级**

四川省科技厅项目、中电集团某研究所合作项目，主研 *2014—2017*

- 将 Web 页面转换为灰度图，结合图像识别的方法对网站进行分类。
- 结合黑白名单、布隆过滤器、URL 检测等其他维度的评价，实现电子商务网站钓鱼页面的识别。
- 通过抓取、解析 DNS 流量，结合模糊聚类算法来检测具有 Fast Flux 特征的僵尸网络。
- 利用特征选择算法选出和加密流量最相关的特征，建立机器学习模型分析识别加密流量。

传统网络攻防、检测 - 3 项

远程侦控工具 + 隐蔽传输技术 + 复杂攻击网络建模和行为分析研究 **国家级**

国家重点研发计划课题、国家自然科学基金项目，技术负责人 *2016—2019*

- 场景策略设置：包括组合策略、修改策略参数、更新策略、激活策略等能力。
- 反侦查/反取证：解决检测防御、差异化样本、反逆向分析、自毁不留痕的问题。
- 多平台支持：支持对市面上常见的 Android 智能终端及 iOS 终端（已越狱）进行远程监控。
- 多形态呈现：底层驱动、软件、硬件。
- 基于 Tor 、蓝牙、无线传感器网络的隐蔽传输。
- 结合疾病传播模型对木马传播过程进行建模，并研究其传播特性。

独立开发作品 - 2 项

清水河畔 - 电子科技大学官方论坛 iOS 客户端 **个人作品**

独立开发者作品 *2017—至今*

- 从设计、实现到宣传、营销，全部独立完成，涉及到 Sketch、PS、Swift、Web 开发、海报制作等。
- App Store 社交类付费排行榜前三（最佳排名）。

Insert-Img - Atom 插件 **个人作品**

独立开发者作品 *2016—2017*

- 为 Atom 编辑器开发的开源插件。方便用户将图片插入到 Markdown 文件中，并自动上传到图床。

学术成果

期刊论文（第一作者）

- **The Deployment Optimization of Wireless Sensor Network Based on Parallelized Cuckoo Search Algorithm.** *Application Research of Computers, 2017.*
- **The Deployment Optimization of Wireless Sensor Network Base on Parallelized Fireworks Algorithm.** *Application Research of Computers, 2016.*
- **Modified t-distribution Evolutionary Algorithm for Dynamic Deployment of Wireless Sensor Networks.** *IEICE TRANSACTIONS on Information and Systems, 2016.*

会议论文（第一作者）

- **A Black-box Attack to Neural Networks Based on Swarm Evolutionary Algorithm** [Submitted] *International Joint Conferences on Artificial Intelligence Organization(IJCAI), 2018*

- **Enhanced Fireworks Algorithm for Dynamic Deployment of Wireless Sensor Networks.**
  International Conference on Frontiers of Sensors Technologies(ICFST), 2017.
- **An Improvement of Chinese Text Hierarchical Clustering Algorithm.**
  International Conference on Computer, Intelligent and Education Technology(CICET), 2015

专利

第一发明人 3 项: 一种数值型关系数据库水印的嵌入及提取验证方法、一种基于 Sunday 算法的字符搜索方法、基于模拟栈和线程注入的一种 ROP 攻击栈溢出防护方法

第二发明人 2 项: 一种基于浏览器标签属性的入侵检测方法及装置、一种基于浏览器脚本行为的入侵检测方法及装置

第三发明人及之后共 11 项: 一种预测强降雨及洪涝灾害的方法、一个基于主权区块链的记账系统及方法、一种基于区块链的货运物流应用方法、一种基于收敛加密的数据块动态操作方法、一种基于区块链的用户多形态身份的安全融合认证方法、一种抗量子计算攻击的无人机区块链管控策略、一种基于区块链的漫游话费记录和结算方法、一种基于区块链的云数据管理方法、基于主权区块链的供应链金融区块链应用方法, 基于主权区块链的供应链管理方法、一种基于区块链技术的数字版权管理方法

荣誉奖励

2017.11: 唐立新教育发展基金“唐立新奖学金”（奖励全校综合测评排名前 3‰）

2016.10: 国家网络安全奖学金（奖励全国在网络安全领域突出贡献的 100 名学生）

2016.10: 电子科技大学学业一等奖学金（年级唯一名额）

2015.10: 荣获电子科技大学优秀研究生称号

2014.09: 荣获电子科技大学优秀毕业生称号

2013.07: 全国大学生信息安全大赛二等奖（团队组长）

2012.12: “东软睿道杯”APP 创新大赛优秀奖

2012.11: “Sybase 杯”软件设计大赛三等奖

2012.07: 全国大学生信息安全大赛二等奖（团队组长）

社会实践

2017.02-至今: 电子科技大学网络空间安全研究中心，助理研究员

2016.08-2017.02: 网空中心团队创业公司——成都网域复兴科技有限公司，技术总监

2015.12-2016.08: 网空中心团队创业公司——迅鳐成都科技有限公司，技术总监

2012.09-2013.09: 电子科技大学腾讯俱乐部，主席

其他

- **English:** CET-4, CET-6.
- **Skills:** Python, Java, Swift, JavaScript, CSS, PHP, Shell Scripts, MATLAB, LATEX, Adobe Photoshop, Microsoft Word, Microsoft Excel, Microsoft PowerPoint.
- **Activities:** 伊利诺伊大学-香槟分校 (UIUC) 联合培养.