

基本信息

姓名：王添毅

电话：13514685743

研究方向：目标检测、鲁棒性分析

求职意向：***

专业：控制科学与工程


微信：hillwu1998

毕业时间：2026.7

个人邮箱：zjuwty@outlook.com

个人主页：<https://hill-wu-1998.github.io/>

Github：[Hill-Wu-1998](https://github.com/Hill-Wu-1998)



教育背景

郑州大学	自动化（本科）	2016.9-2020.7
● 曾获国家励志奖学金以及三好学生、优秀团员等荣誉称号		
浙江大学	电子信息（硕士研究生）	2021.9-2023.7
● 浙江大学网络传感与控制研究组（NeSC Group）——安全组成员		
浙江大学	控制科学与工程（博士研究生）	2023.9-至今
● 浙江大学网络传感与控制研究组（NeSC Group）——安全组成员		

科研经历

2021.10-2022.1	浙江大学 NeSC 安全组-软件测试
● 师兄的工作，作为模糊测试方向的研究入门，测试对象为软件，主要负责工作中对比对象 Magma 实验部分，具体包括：使用 AFL, AFLfast, AFL++, Angora 等先进的模糊测试工具针对 libpng 等开源软件进行测试。	
● 学习很多模糊测试相关的理论和知识，充分熟悉了各种先进工具的使用和优势。	
● 相关成果：Better Pay Attention Whilst Fuzzing (TSE 六作 CCF A)	
2022.2-2023.7	浙江大学 NeSC 安全组-工控安全
● 研究方向 1:工控协议黑盒测试方法的研究，主做方向，第一个工作重点着眼于工控协议的交互过程，设计违反状态机的变异策略，发现未知的协议漏洞。	
● 相关成果: STFuzz: Stateful Fuzzing of PLC Proprietary Protocols via Violating State Transitions (ICSE 投稿中)，Reverse Engineering Industrial Protocols Driven By Control Fields 申请发明专利一项（实审中）	
● 研究方向 2:工控协议逆向分析，同门的方向，根据工控协议 control field 的特点沿用 NetPlier 的概率方法进行二进制协议黑盒逆向分析	
● 相关成果: Reverse Engineering Industrial Protocols Driven By Control Fields (INFOCOM 2024 五作 CCF A)	
2023.9-至今	浙江大学 NeSC 安全组-人工智能
● 研究方向 1: AI 模型及系统鲁棒性分析，博士主要课题，主要包含以下几个子课题	
■ CNN-based 检测模型的延迟攻击与防御：延迟攻击可以通过利用增加候选框数量来极大增加模型推理时间，影响模型可用性，核心 insights 包括 1)延迟攻击在不同算力系统上会出现瓶颈迁移，即随着算力增加从计算瓶颈迁移到带宽瓶颈；2) 图片的背景和对象对延迟攻击的鲁棒性不同，需要区别对待。基于以上两点设计了一种对抗训练方法来针对不同的算力系统自适应的训练鲁棒的目标检测模型。（CVPR 2025 一作 CCF A）	
■ Transformer-based 检测模型存在的安全问题：主要是探究 DETR 系列模型存在的独特攻击面 (ICCV 2025 在投)	
■ 多模态模型鲁棒性分析	

证书&技能

CNVD 原创漏洞十余项，英语四六级，计算机二级等