同行专家业内评价意见书编号：20250858228

附件1

浙江工程师学院（浙江大学工程师学院）
同行专家业内评价意见书

姓名：张泽邦

学号：22260497

申报工程师职称专业类别（领域）：能源动力

浙江工程师学院（浙江大学工程师学院）制

2025年03月18日

填表说明

一、本报告中相关的技术或数据如涉及知识产权保护、军工项目保密等内容，请作脱密处理。

二、请用宋体小四字号撰写本报告，可另行附页或增加页数，A4纸双面打印。

三、表中所涉及的签名都必须用蓝、黑色墨水笔，亲笔签名或签字章，不可以打印代替。

四、同行专家业内评价意见书编号由工程师学院填写，编号规则为：年份4位＋申报工程师职称专业类别(领域)4位+流水号3位，共11位。

一、个人申报

（一）基本情况【围绕《浙江工程师学院（浙江大学工程师学院）工程类专业学位研究生工程师职称评审参考指标》，结合该专业类别(领域)工程师职称评审相关标准，举例说明】

1.对本专业基础理论知识和专业技术知识掌握情况(不少于200字)

在电气工程领域，我系统掌握了电路理论、电子技术、电磁场理论、自动控制原理、信号与系统、电力电子技术等基础理论知识，并在此基础上深入研究了智能电网、电力信息安全等关键技术。特别是在电力信息网络安全领域，我结合自身研究方向，重点掌握了电力信息网络流量特征、入侵检测系统、网络攻击防御技术及安全态势分析方法。在工程实践和科研过程中，我熟练运用Python、Matlab等编程语言和工具进行数据分析、算法开发及仿真建模。在硕士期间，共发表期刊、会议论文5篇，申请发明专利2项。

2.工程实践的经历(不少于200字)

在工程实践方面，我积极参与多项国家级和省级重点研发项目，积累了丰富的工程经验，并在电力信息安全、智能监测和深度学习应用等方向形成了系统性的实践能力。
参与的项目包括：
[1] 2023.10-
2026.12，支撑海量终端接入与跨安全域协同的云安全防御关键技术研究，国家重点研发计划。
[2] 2022.01-
2024.12，基于深度学习的恶意软件行为检测与分类系统研究与应用，浙江省重点研发计划。
[3] 2024.09-
2025.06，面向智慧电厂安全的网络智能监测和安全态势分析研究与应用，国家能源集团科技项目。
这些工程实践经历不仅提升了我的技术能力，也增强了我在复杂工程环境中的团队协作与项目管理能力。
此外，作为首届工程硕博士培养改革专项的学生，我进入国能浙江北仑第一发电有限公司进行实践学习。实习实践内容主要分四个阶段：以公司各职能部门对企业战略文化、规章制度以及科技创新等内容宣讲的综合素质培训阶段，以劳模工匠为主导的火电厂生产见习阶段，以企业导师和高级专家为主导的智慧企业实践实习阶段，以及最后实习总结和鉴定考核。

3.在实际工作中综合运用所学知识解决复杂工程问题的案例（不少于1000字)

随着信息技术的快速发展和智能电网的建设，电力系统正逐渐向高度信息化、自动化的方向发展。智慧电厂借助信息化技术，实现了电力系统的集成化、智能化和可持续发展。然而，随之而来的是电厂网络系统面临日益复杂严峻的安全威胁。智慧电厂的网络系统涉及多个关键领域，如监控与控制系统、通信网络、数据中心等，这些系统的连通性和依赖性加剧了网络安全风险。电厂网络面临的威胁包括网络攻击、数据泄露、恶意软件等，这些威胁可能导致电力系统的瘫痪、信息泄露以及其他严重后果。通过引入先进的网络终端智能监测技术和防御方法，可以有效监测、识别、预警网络安全威胁，提升北仑电厂的安全性和稳定性，满足信息系统对网络空间安全防护的严格要求。
浙江公司北仑电厂积极拥抱数字经济新时代，以集团智慧电厂示范企业建设为契机，以达到集团卓越级水平为目标，坚持统筹推进、需求主导、数据驱动、集成创新的原则,将智慧企业建设工作重心由核心经营管理业务的数字化与在线化，向以数据资源为驱动力、全面提升核心竞争力转变，致力推进生产作业现场的智能化与无人化，积极实行生产和管理的体制机

构变革，为构建清洁低碳、安全高效的世界一流电厂提供有力支撑。曾荣获“国际一流火电厂”、全国文明单位、全国五一劳动奖状、全国优质工程金质奖、中央企业先进基层党组织、全国创先争优先进基层党组织等多项荣誉。经过多年的持续投入，现已发展至以1000M 网络为主干 100M 网络到桌面，拥有数十台服务器，数百台
PC机，业务覆盖全厂各个部门生产和管理业务流程的近三十套应用系统。因此，为了保障智慧电厂的运行安全和数据安全,有必要开展面向智慧电厂安全的网络智能监测和安全态势分析研究与应用。
结合北仑电厂网络安全防护系统建设需要，提供一种创新的智慧电厂安全解决方案，支撑面向智慧电厂安全的网络终端数据智能分析、入侵智能检测和积极防御等。
围绕计算机高级网络威胁智能检测与响应原型系统的主要流程环节：高级网络威胁通用表征模型与智能分析框架→大规模系统数据的采集与数据管理融合方法→基于原型聚类的APT智能检测与分类方法→原型系统自主研制与第三方机构测试验证→原型系统在北仑第一发电公司实际场景的应用示范开展以下研究工作：
智慧电厂安全解决方案结合北仑电厂的实际情况，提出一套从底层数据采集、数据处理、数据分析、动态恶意行为审计到恶意行为阻断的网络终端安全防护方案，阻断方式不少于3种。能够实现从应用层和内核层对命令执行、文件访问、网络通信、用户等多个维度的行为进行监控分析，对威胁事件一键黑名单隔离处理，并生成事件关联分析报告。研究内容主要包括：研究高级网络威胁通用表征模型与智能分析框架、研究大规模系统数据的采集与数据管理融合方法、研究基于原型聚类算法和联邦学习的APT智能检测与分类方法，研制“面向智慧电厂安全的网络智能监测和安全态势分析原型系统”。

（二）取得的业绩（代表作）【限填3项，须提交证明原件（包括发表的论文、出版的著作、专利证书、获奖证书、科技项目立项文件或合同、企业证明等）供核实，并提供复印件一份】

1.
公开成果代表作【论文发表、专利成果、软件著作权、标准规范与行业工法制定、著作编写、科技成果获奖、学位论文等】

成果名称	成果类别 [含论文、授权专利（含发明专利申请）、软件著作权、标准、工法、著作、获奖、学位论文等]	发表时间/授权或申请时间等	刊物名称/专利授权或申请号等	本人排名/总人数	备注
FedStackRF: A Network Intrusion Detection Framework Based on Federated and Ensemble Learning	会议论文	2024年12月15日	Energy Conversion and Economics Annual Forum	1/3	EI会议收录
Defect detection and classification of photovoltaic modules based on image fusion analysis	会议论文	2023年05月10日	IEEE Conference on Energy Internet and Energy System Integration	1/3	EI会议收录
Statistical Knowledge and Game-Theoretic Integrated Model for Cross-Layer Impact Assessment in Industrial Cyber-Physical Systems	TOP期刊	2024年01月01日	Advanced Engineering Informatics	3/6	SCI期刊收录

2.其他代表作【主持或参与的课题研究项目、科技成果应用转化推广、企业技术难题解决方案、自主研发设计的产品或样机、技术报告、设计图纸、软课题研究报告、可行性研究报告、规划设计方案、施工或调试报告、工程实验、技术培训教材、推动行业发展中发挥的作用及取得的经济社会效益等】

（三）在校期间课程、专业实践训练及学位论文相关情况	
课程成绩情况	按课程学分核算的平均成绩： 89 分
专业实践训练时间及考核情况(具有三年及以上工作经历的不作要求)	累计时间： 1.3 年（要求1年及以上） 考核成绩： 83 分
本人承诺	
个人声明：本人上述所填资料均为真实有效，如有虚假，愿承担一切责任，特此声明！ **申报人签名：** 张泽邦	

2226049

二、日常表现考核评价及申报材料审核公示结果

日常表现考核评价	非定向生由德育导师考核评价、定向生由所在工作单位考核评价： ✓优秀 ☐良好 ☐合格 ☐不合格 德育导师/定向生所在工作单位分管领导签字（公章）：2025年3月19日
申报材料审核公示	根据评审条件，工程师学院已对申报人员进行材料审核（学位课程成绩、专业实践训练时间及考核、学位论文、代表作等情况），并将符合要求的申报材料在学院网站公示不少于5个工作日，具体公示结果如下： ☐通过 ☐不通过（具体原因：　　） 工程师学院教学管理办公室审核签字（公章）：　　年　月　日

浙 江 大 学 研 究 生 院

攻读硕士学位研究生成绩表

学号：22260497	姓名：张泽邦	性别：男	学院：工程师学院	专业：电气工程	学制：2.5年
毕业时最低应获：24.0学分		已获得：30.0学分		入学年月：2022-09	毕业年月：
学位证书号：			毕业证书号：		授予学位：

学习时间	课程名称	备注	学分	成绩	课程性质	学习时间	课程名称	备注	学分	成绩	课程性质
2022-2023学年秋季学期	新时代中国特色社会主义理论与实践		2.0	94	专业学位课	2022-2023学年春夏学期	智能装备与创新设计实践		4.0	96	专业学位课
2022-2023学年秋季学期	工程技术创新前沿		1.5	88	专业学位课	2022-2023学年夏季学期	研究生英语基础技能		1.0	免修	公共学位课
2022-2023学年秋冬学期	工程管理		2.0	85	跨专业课	2022-2023学年夏季学期	自然辩证法概论		1.0	89	公共学位课
2022-2023学年秋冬学期	研究生论文写作指导		1.0	90	专业选修课	2022-2023学年夏季学期	物联网信息安全技术与应用基础		2.0	94	跨专业课
2022-2023学年冬季学期	工程中的有限元方法		2.0	100	专业选修课	2022-2023学年夏季学期	智能装备创新设计案例分析		2.0	91	专业学位课
2022-2023学年冬季学期	产业技术发展前沿		1.5	85	专业学位课	2022-2023学年春夏学期	高阶工程认知实践		3.0	89	专业学位课
2022-2023学年秋冬学期	工程伦理		2.0	95	专业学位课	2023-2024学年秋季学期	深度科技国际创业前沿		1.0	84	跨专业课
2022-2023学年夏季学期	研究生英语		2.0	免修	专业学位课		硕士生读书报告		2.0	通过	

说明：1.研究生课程按三种方法计分：百分制，两级制（通过、不通过），五级制（优、良、中、及格、不及格）。

2.备注中“*”表示重修课程。

学院成绩校核章：

成绩校核人：张梦依

打印日期：2025-03-20

FedStackRF: A Network Intrusion Detection Framework Based on Federated and Ensemble Learning

Zebang Zhang[1], Xuan Wang[1], Qiang Yang[2,]*

[1] *Polytechnic Institute, Zhejiang University, Hangzhou 310027, China*
[2] *College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China*
**qyang@zju.edu.cn*

Keywords: Federated Learning, Random Forest, Stacking Architecture, Network Intrusion Detection, Non-IID Data

Abstract

With the rapid digitalization of society, network intrusion detection has become a critical defense for safeguarding information systems against evolving cyber threats. However, traditional detection methods face significant challenges in handling sophisticated attacks and ensuring data privacy. This paper proposes FedStackRF, a novel framework that combines federated learning with ensemble learning techniques, specifically stacking and Random Forest, to address these challenges. FedStackRF employs a stacking architecture where Random Forest acts as the base model and logistic regression serves as the meta-model. Federated learning is utilized during meta-model training to ensure privacy preservation while effectively handling non-IID data across distributed clients. Experimental results validate the effectiveness of FedStackRF, demonstrating a near-centralized performance with only a marginal AUC difference of 0.0051% compared to the centralized Random Forest model. The framework significantly improves anomaly detection capabilities, achieving an average AUC improvement of 1.53% over local models and a 0.19% improvement over Ensemble Random Forest. Moreover, the framework's interpretability and low computational cost make it suitable for deployment in resource-constrained edge environments. These findings highlight FedStackRF as a robust and scalable solution for advancing network intrusion detection in privacy-sensitive and distributed scenarios.

1 Introduction

With the pervasive digitalization of society, network intrusion detection has become a foundational component in protecting information systems against evolving cyber threats. Traditional intrusion detection methods primarily depend on rule-based or signature-based mechanisms, which, although effective for known threats, struggle to counter sophisticated and stealthy attacks such as advanced persistent threats (APTs) and newly emerging attack vectors. Additionally, the widespread adoption of IoT devices, mobile platforms, and other connected endpoints has led to unprecedented growth in network traffic, intensifying concerns around data privacy. This raises an urgent need for network security solutions that can effectively safeguard user data privacy in distributed environments.

Random Forest (RF), as an ensemble learning technique, is widely adopted for its high classification accuracy, robustness, and interpretability. However, traditional machine learning models like Random Forest rely heavily on access to sufficient and diverse data to perform effectively. As privacy and security concerns grow, centralized machine learning approaches face increasing limitations when collecting and processing large-scale user data. This is particularly critical for network intrusion detection, where data associated with attack characteristics is highly sensitive, and centralized storage and processing of such data carry considerable security risks. In this context, Federated Learning (FL) has emerged as an effective distributed learning framework that allows models to be trained locally on each client while only transmitting model parameters, thereby preserving data privacy.

Most existing FL frameworks are primarily designed for neural networks. Although neural networks excel at handling unstructured data such as images and audio, their decision-making process is often opaque and lacks transparency. In contrast, Random Forest models are highly effective with structured tabular data, including complex categorical variables and feature interactions, and they provide clear insights into the decision-making process through feature importance scores and decision paths. This transparency is particularly valuable in network security, where interpretability is essential. Additionally, Random Forest models are computationally efficient, with relatively low training costs, making them ideal for deployment on edge nodes with limited storage and processing capacity.

However, applying Random Forest models within a federated learning context presents unique challenges. Conventional FL methods, such as those based on the FedAvg algorithm, rely on averaging gradients across clients to optimize a global model, which is well-suited for parameterized models like neural networks. In contrast, tree-based models such as Random Forest lack this parameterized structure, rendering such approaches ineffective. Consequently, specialized FL techniques tailored to Random Forest are necessary, capable of handling the non-IID (non-independent and identically distributed) nature of data across clients while maintaining model interpretability during inference.

To address these challenges, we propose FedStackRF, a novel network intrusion detection framework that combines

Defect Detection and Classification of Photovoltaic Modules Based on Image Fusion Analysis

2022 IEEE 6th Conference on Energy Internet and Energy System Integration (EI2) | 979-8-3503-4715-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/EI256261.2022.10116597

Zebang Zhang
Polytechnic Institute
Zhejiang University
Hangzhou, 310027 China
22260497@zju.edu.cn

Yuan Cao
College of Electrical Engineering
Zhejiang University
Hangzhou, 310027 China
cy1998@zju.edu.cn

Qiang Yang
College of Electrical Engineering
Zhejiang University
Hangzhou, 310027 China
qyang@zju.edu.cn

***Abstract*—The operation and maintenance challenges of photovoltaic (PV) plants are becoming increasingly prominent due to their long service life and environmental factors. Considering the high cost of manual maintenance, intelligent operation and maintenance technology represented by unmanned aerial vehicle (UAV) inspection has received great attention. The UAV carrying dual-light cameras can collect visible and infrared images of PV modules simultaneously. In this paper, we propose to use the Faster-RCNN model to complete the defect detection and classification of PV modules. The experimental results show that the trained Faster-RCNN model has high recognition accuracy for defects in both types of images. The models trained by the two types of images are combined to jointly complete the task of defect identification and classification of photovoltaic modules, realizing the complementary and fusion analysis of information, which is conducive to the better judgment of defects.**

Keywords—photovoltaic plants, visible light image, infrared image, defect detection, fusion analysis

I. INTRODUCTION

Solar energy performs well among renewable energy sources known to human beings. It is widely distributed, clean, safe, and renewable, making it an ideal energy choice for the future of mankind. At present, the utilization rate of solar energy by human beings is still low, the production cost is still high, and the photovoltaic industry has great development potential. To build a smarter, greener, safer and more efficient energy intelligent operation and inspection system, the construction scale of photovoltaic (PV) plants is getting larger and larger, and the O&M challenges of PV plants are becoming more and more prominent. The maintenance of photovoltaic modules is the top priority in operation and maintenance. High-frequency problems such as shelter and hotspots of PV modules are the main causes of power plant equipment failures, and the overall power generation efficiency of the power plant will be greatly improved by timely detection and treatment of these problems.

Defect detection by visible and infrared images of PV modules is a less labor-intensive method. An unmanned aerial vehicle (UAV) can be used to collect images of PV modules directly. This technology is very economical and practical for the operation and maintenance of photovoltaic plants. The flexibility of UAVs can greatly improve the efficiency of operation and maintenance as PV plants usually have complex terrain conditions. UAVs equipped with dual-light cameras can obtain both visible and infrared images of PV modules at the same moment. The visible image has high resolution and contains a lot of details and color information. In contrast, infrared images, although it is not as high resolution and not as capable of capturing module details, can detect the surface temperature of the PV module, introducing a new dimension of information for fault detection that can react to faults located inside the PV module [1]. Therefore, maximizing the information within both images allows for more accurate detection and classification of PV module surface faults. The authors in [2] have completed the detection and classification of some surface defects and intrinsic defects of PV modules by extracting the features of the electroluminescent images of PV modules through deep networks. However, the electroluminescence images of PV modules require special instruments and a specific environment to complete the capture, which cannot be done by UAVs. The authors in [3] used a convolutional neural network model to accomplish the detection and classification of defects in visible light images taken by UAVs. The authors in [4] used two approaches to accomplish the detection of hot spot defects in PV modules. One approach is the classical digital image processing methods using surface features for classification and the other approach uses convolutional neural networks for classification. Experimental results show that the conventional image processing algorithms are not very robust and require a lot of adjustment of the model parameters when the detection environment changes. Convolutional neural networks have more powerful and efficient feature extraction capability in image processing and have more robustness and generality. The Faster-RCNN algorithm is widely adopted in the field of target detection, and it has been continuously improved to achieve high recognition accuracy [5]-[7]. Therefore, this algorithm is intended to be used in this experiment to complete the construction of the detection model.

The main technical contributions made in this work are summarized as follows: (1) The raw visible and infrared images collected by the UAV are processed. The characteristics of the PV components with defects on the images are clarified, and the images containing defective components are screened to produce the dataset. (2) The produced dataset is used to train the built Faster-RCNN model. The experimental results show that the trained model can well perform the detection and classification tasks of PV module defects, and the detection results are fused after the visible image based detection model

Advanced Engineering Informatics 59 (2024) 102338

Contents lists available at ScienceDirect

Advanced Engineering Informatics

journal homepage: www.elsevier.com/locate/aei

Statistical knowledge and game-theoretic integrated model for cross-layer impact assessment in industrial cyber-physical systems

Pengchao Yao [a], Xuan Wang [c], Zebang Zhang [c], Bingjing Yan [b], Qiang Yang [b,*], Wenhai Wang [a]

[a] College of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China
[b] College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China
[c] Polytechnic Institute, Zhejiang University, Hangzhou 310027, China

ARTICLE INFO

Keywords:
Industrial cyber-physical system (ICPS)
Statistical knowledge
Game theory
Intrusion-defense interaction
Impact assessment

ABSTRACT

Cyberspace intrusions targeting modern industrial cyber-physical systems (ICPSs) are considered highly persistent and stealthy penetration processes that can result in catastrophic consequences for industrial infrastructures. Existing studies predominantly concentrated on detection and defense strategies for specific stages of intrusions without much knowledge of underlying system operational mechanisms, characteristics and evolutionary patterns. In this paper, we present a novel approach that integrates statistical knowledge and game theory to establish a comprehensive security model covering various aspects, including anomaly detection, behavioral analysis, strategy generation and impact assessment. Specifically, a statistical model, i.e. Poisson intrusion model (PIM), is developed to characterize the probabilistic properties of intrusions by leveraging knowledge of their occurrence patterns and frequencies. A Bayesian inference-based model is proposed to analyze the intrusion behaviors for anomaly detection. Then, by integrating statistical knowledge of intrusions and detections, a Markov game model is formulated to characterize the interactive actions and strategies between attackers and defenders throughout the intrusion process. Further, the cross-layer impact is assessed by quantifying the potential consequences under corresponding cyber security conditions in terms of production performance degradation and unintended incident losses. Finally, the proposed approach is validated through extensive experiments for power plant operational scenarios.

1. Introduction

The rapid progress and extensive adoption of state-of-the-art information and communication technologies (ICTs) have brought about a significant revolution in conventional industrial control systems (ICSs) [1]. These systems have transformed into interconnected and networked industrial cyber-physical systems (ICPSs), seamlessly merging cyberspace technologies with physical systems. This intelligent digital transformation has brought about a substantial enhancement in production efficiency and manufacturing capabilities across a wide range of industrial sectors (e.g., power grids, water distribution systems, chemical factories) [2]. However, the increasing interconnectedness of the Internet also exposes ICPSs to potential cyber intrusions from external networks, that can cause seriously destructive effects on the critical physical infrastructure [3,4]. For instance, the Stuxnet attack on Iran's nuclear facilities in 2010 and the BlackEnergy on Ukraine's power grid in 2015 both resulted in catastrophic consequences for industrial infrastructures [5–7]. Consequently, there is a pressing need for the implementation of robust and comprehensive security measures to protect ICPSs against such threats.

As highlighted in [8], advanced cyber intrusions targeting ICPSs exhibit the characteristics of a high level of specificity and persistence. The cyber intrusions can be carefully designed and tailored to exploit specific vulnerabilities and maintain a persistent presence within the compromised systems [9,10]. However, existing security methods predominantly focus on proposing detection technologies and defense strategies for specific stages of cyber intrusions, while lacking a profound understanding of their underlying mechanisms, characteristics, and evolutionary patterns [11]. For instance, intrusion detection systems (IDS) and intrusion prevention systems (IPS) can only operate up to the initial stage of intrusion detection [12,13]. While they can effectively identify potential intrusions and apply preventive measures, their scope is limited to the early stages of an attack [14]. Therefore, it is of utmost importance to develop comprehensive defense mechanisms that can anticipate and counter attacks at every stage of the intrusion process

* Corresponding author.
E-mail address: qyang@zju.edu.cn (Q. Yang).

https://doi.org/10.1016/j.aei.2023.102338
Received 16 July 2023; Received in revised form 18 November 2023; Accepted 23 December 2023
Available online 27 December 2023