东北石油大学

毕业设计（论文）存档资料

|  |  |
| --- | --- |
| 题目： | 基于EMS的FDIA |
|  | 电力CPS检测系统设计 |
| 学生专业： | 电气工程及其自动化 |
| 学生姓名： | 徐浩洋 |
| 指导教师： | 高新成 |
| 辅助教师： |  |

2024年5月24日

东北石油大学学生开题报告表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 课题名称 | 基于EMS的针对FDIA的电力CPS检测系统设计 | | | | |
| 课题来源 | 自拟  题目 | 课题  类型 | 软件开发 | 指导教师姓名 | 高新成 |
| 学生姓名 | 徐浩洋 | 学 号 | 200603140111 | 专 业 | 电气工程及其自动化 |
| **调研资料的准备：**  通过中国知网等学术网站查找相关期刊文献，了解基于EMS的针对FDIA的电力CPS检测系统设计的基本概念和相关的防御算法以及模型搭建。  **设计目的：**  使用Matlab对电力系统进行建模，模拟电网在遭受FDIA时的行为，以评估攻击对系统的影响。结合卡方算法与卡尔曼滤波器设计一种新的检测算法，并通过Matlab仿真验证其在FDIA前后的性能。建立数据库以存储和管理电力系统数据，利用Python编程语言，结合Web技术，开发一个实时监控和检测FDIA的在线系统，该系统将集成EMS，实现对电力系统安全的实时监控，为推动智能电网的发展提高电力系统的韧性和可恢复性提高电力系统的安全性和可靠性提供参考和指导。  **设计要求：**  设计Matlab电网FDIA影响与其检测算法仿真模拟；能完成MySQL数据库对电力系统数据的保存，搭建与处理；建立基于Python语言与Power BI开发的EMS系统实现FDIA的检测。  **设计思路：**  本设计拟采用Matlab仿真程序与Python开发语言与MySQL数据库，仿真模拟检测算法电网CPS遭受FDIA前后的性能，并基于此算法开发出一套功能完整的检测系统。  **预期成果：**  针对智能电表所采集的消耗功率等数据集进行检测并实现根据此数据集的算法分析以实现对FDIA的判断，以及基于EMS的检测系统的可用性。  **时间安排：**  1-4周完成Matlab仿真平台与Python的编程学习工作；  5-8周完成Matlab中FDIA与检测算法的各部分的模型建立；  9-12周完成算法研究分析与数据库的建立与其数据处理；  12-13周开发具有FDIA检测功能的EMS搭建与运行并进行真实测试；  14-15周撰写论文并准备答辩。  **完成设计所具备的条件：**  学过电力系统相关课程智能电网相关知识，会使用Matlab搭建模型与Python程序开发。  指导教师签名： 日期：2023.12.18 | | | | | |

1. 课题来源：课题来源分为结合实际课题和自拟课题两种，结合实际课题中来源于科研课题的要填写确切基金项目、企事业单位项目，不能写横向、纵向课题等。

2、课题类型：A—工程设计；B—科学实验；C—软件开发；D—理论研究；E—应用研究。

**东北石油大学**毕业设计（论文）学生自查表

（中期教学检查用）

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 学生姓名 | 徐浩洋 | 专业 | | | 电气工程及其自动化 | | | | | | 班级 | | | 电气20-1班 | | |
| 指导教师  姓 名 | 高新成 | | | | | | 职称 | | | | | 教授 | | | | |
| 课题名称 | 基于EMS的FDIA电力CPS检测系统设计 | | | | | | | | | | | | | | | |
| 个人作息  时间 | 上午 | | 自 8时  至 10 时 | | | 下午 | | | 自 13时  至 15时 | | | | 晚间 | | 自 18时  至 19 时 | |
| 个人精力  实际投入 | 日平均工作时间 | | 5 | 周平均工作时间 | | | | 35 | | 迄今缺席天数 | | | 0 | 出勤率% | | 100% |
| 指导教师每周指导次数 | 2 | | 每周指导时间（小时） | | | | | 4 | | 备注 | | | | 每周二、四上午指导 | | |
| 毕业设计（论文）工作进度（完成）内容及  比重 | 已完成主要内容 | | | | | | | % | | 待完成主要内容 | | | | | | % |
| 1.收集查阅相关文献资料  2.完成仿真模型程序的搭建和基于EMS的检测系统的搭建  3.完成文献翻译、开题报告和任务书以及每周日志 | | | | | | | 60% | | 1.对程序调试运行  2.对程序进行分析和验证以及验证  3.总结分析完善，写每周日志，攥写论文 | | | | | | 40% |
| 存在问题 | 1.对于Matlab软件掌握不是很熟练；  2.对算法的运用还存有疑惑；  3.对整体思路论文攥写等还需认真把握。 | | | | | | | | | | | | | | | |

指导教师签字： 2024年4月19日



**东北石油大学电气信息工程学院毕业设计（论文）学生申请答辩表**

|  |  |  |  |
| --- | --- | --- | --- |
| 课 题 名 称 | 基于EMS的FDIA电力CPS检测系统设计 | | |
| 申 请 理 由 | 顺利完成毕业设计（论文）任务，申请答辩 | | |
| 学 生 签 名 |  | 日期 | 2024年5月24日 |

**东北石油大学电气信息工程学院毕业设计（论文）评审表（指导教师）**

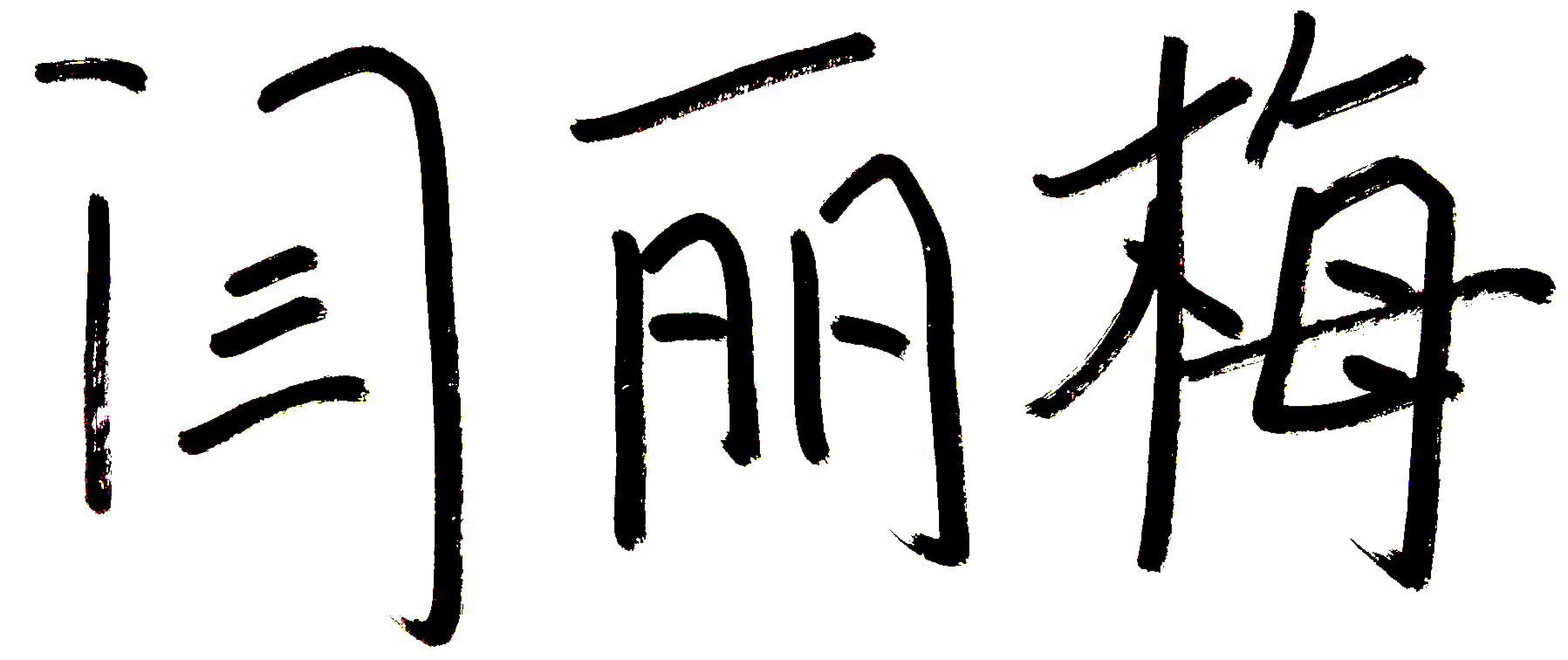
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 课题名称 | 基于EMS的FDIA电力CPS检测系统设计 | | | | | 课题类型 | 软件开发 | |
| 教师姓名 | 高新成 | 职 称 | 教授 | | 课题来源 | 自拟题目 | | |
| 学生姓名 | 徐浩洋 | 学 号 | 200603140111 | | 专 业 | 电气工程及其自动化 | | |
| 评审  项目 | 评分标准 | | | | | | 满分 | 得分 |
| A | | | C | | |
| 分析解决问题能力  （20分） | 能够通过文献研究，对复杂工程问题进行有效分析，开题论证充分。 | | | 文献检索达到要求，开题论证基本合理。 | | | 10 | 9 |
| 合理利用科学原理、设计实验，分析与解释数据，通过信息综合得到有效结论。 | | | 初步具备设计实验，分析与解释数据以及信息综合能力。 | | | 10 | 9 |
| 沟通  （10分） | 毕业设计过程中定期与指导教师沟通交流，能按期圆满完成毕业设计工作；具有探索精神和自主学习意识。 | | | 能与指导教师沟通交流，能按期基本完成任务书规定的任务，工作较努力，能遵守纪律。 | | | 10 | 9 |
| 设计（论文）与专业文献翻译质量  （40分） | 论文内容符合撰写要求、规范，图纸标准整洁。理论与分析正确、论述条理清晰、文理通顺、数据详实，结论严谨。 | | | 内容70％以上符合撰写要求。理论与分析基本正确、论述基本清晰、通顺。 | | | 20 | 18 |
| 译文翻译准确且内容贴近课题，译文字数3000字以上。 | | | 译文基本准确，字数2000字以上。 | | | 10 | 9 |
| 论文字数≥1.5万字，摘要300字左右；摘要、结论能确切地体现主要内容及成果。 | | | 论文字数≥1.2万字，摘要、结论能基本体现主要工作内容及成果。 | | | 10 | 8 |
| 使用现代工具  （10分） | 根据毕业设计需要能够开发或选用所需的现代工程和信息技术工具，仿真、设计和辨识电力能源及石油工业(为油保电)中的复杂工程问题，并能够分析其优缺点，理解其局限性。 | | | 具有一定的现代工程和信息技术工具应用能力。 | | | 10 | 9 |
| 环境和可持续发展  （10分） | 毕业设计兼顾环境和可持续发展思想，能清楚认识该设计对社会、健康、安全、法律、文化及环境的影响与责任。能合理评估毕业设计成果对人类和环境是否存在潜在的损害或隐患。 | | | 技术因素认识较为充分，社会、健康、安全、法律、文化及环境因素考虑不充分，方案设计基本合理。 | | | 10 | 9 |
| 成本核算  （10分） | 工程设计类毕业设计能核算该设计成果所需成本，并与市场上同类商品做比较。 应用研究类毕业设计能评估该研究的社会或经济价值，以及后续产生的社会经济影响。 | | | 工程设计类毕业设计能基本完成毕业设计成果所需成本核算；  应用研究类毕业设计能对该研究的社会或经济价值有初步认识。 | | | 10 | 6 |
| 是否同意参加答辩：同意 | | | | | | | 总分 | 86 |
| 评语：该生围绕FDIA导致电力CPS存在工控安全威胁问题，通过研究结合卡方算法与卡尔曼滤波器设计一种新的检测算法，并通过Matlab仿真验证其在FDIA前后的性能。建立数据库以存储和管理电力系统数据，利用Python编程语言，结合Web技术，开发一个实时监控和检测FDIA的在线系统，该系统将集成EMS，实现对电力系统安全的实时监控，为推动智能电网的发展提高电力系统的韧性和可恢复性提高电力系统的安全性和可靠性提供参考和指导。  该学生较好的完成了毕业设计工作，研究内容具有一定创新性，同意该生参加答辩。 | | | | | | | | |

 指导教师签字： 2024 年 5 月 27 日

**注：1、课题类型包括：A—工程设计；B—科学实验；C—软件开发；D—理论研究；E—应用研究 2、课题来源包括：X—结合实际课题；Y—自拟课题。**

**东北石油大学电气信息工程学院毕业设计（论文）评审表（评阅人）**

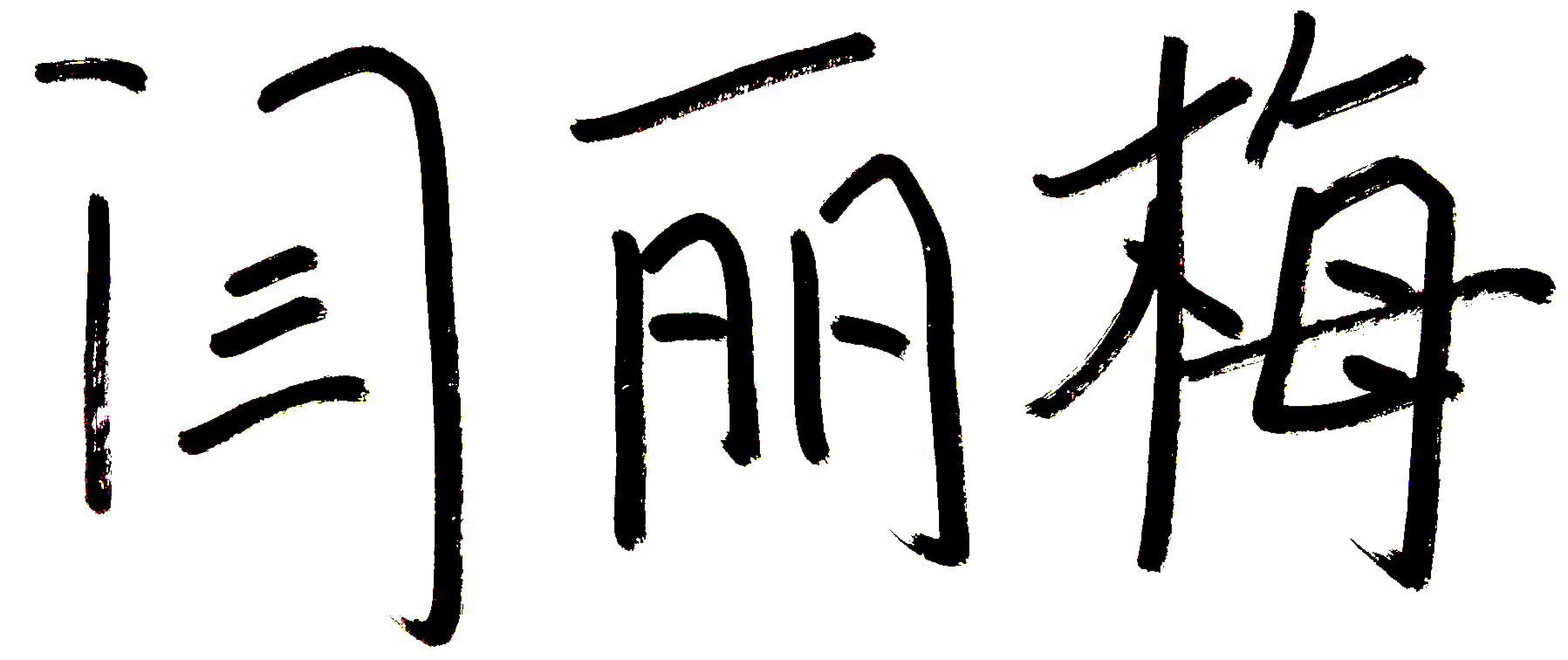
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 课题名称 | 基于EMS的FDIA电力CPS检测系统设计 | | | | | 课题类型 | 软件开发 | |
| 教师姓名 | 高新成 | 职 称 | 教授 | | 课题来源 | 自拟题目 | | |
| 学生姓名 | 徐浩洋 | 学 号 | 200603140111 | | 专 业 | 电气工程及其自动化 | | |
| 评审  项目 | 评分标准 | | | | | | 满分 | 得分 |
| A | | | C | | |
| 分析解决问题能力  （20分） | 能够通过文献研究，对复杂工程问题进行有效分析，开题论证充分。 | | | 文献检索达到要求，开题论证基本合理。 | | | 10 | 9 |
| 合理利用科学原理、设计实验，分析与解释数据，通过信息综合得到有效结论。 | | | 初步具备设计实验，分析与解释数据以及信息综合能力。 | | | 10 | 9 |
| 沟通  （10分） | 成果检查过程中能与评阅教师有效沟通交流，能效回应评阅教师指令，清晰阐述自己观点。 | | | 能与评阅教师沟通交流，能基本阐述自己观点。 | | | 10 | 9 |
| 设计（论文）与专业文献翻译质量  （40分） | 论文内容符合撰写要求、规范，图纸标准整洁。理论与分析正确、论述条理清晰、文理通顺、数据详实，结论严谨。 | | | 内容70％以上符合撰写要求。理论与分析基本正确、论述基本清晰、通顺。 | | | 20 | 15 |
| 译文翻译准确且内容贴近课题，译文字数3000字以上。 | | | 译文基本准确，字数2000字以上。 | | | 10 | 9 |
| 论文字数≥1.5万字，摘要300字左右；摘要、结论能确切地体现主要内容及成果。 | | | 论文字数≥1.2万字，摘要、结论能基本体现主要工作内容及成果。 | | | 10 | 9 |
| 使用现代工具  （10分） | 根据毕业设计需要能够开发或选用所需的现代工程和信息技术工具，仿真、设计和辨识电力能源及石油工业(为油保电)中的复杂工程问题，并能够分析其优缺点，理解其局限性。 | | | 具有一定的现代工程和信息技术工具应用能力。 | | | 10 | 9 |
| 环境和可持续发展  （10分） | 毕业设计兼顾环境和可持续发展思想，能清楚认识该设计对社会、健康、安全、法律、文化及环境的影响与责任。能合理评估毕业设计成果对人类和环境是否存在潜在的损害或隐患。 | | | 技术因素认识较为充分，社会、健康、安全、法律、文化及环境因素考虑不充分，方案设计基本合理。 | | | 10 | 8 |
| 成本核算  （10分） | 工程设计类毕业设计能核算该设计成果所需成本，并与市场上同类商品做比较。  应用研究类毕业设计能评估该研究的社会或经济价值，以及后续产生的社会经济影响。 | | | 工程设计类毕业设计能基本完成毕业设计成果所需成本核算；  应用研究类毕业设计能对该研究的社会或经济价值有初步认识。 | | | 10 | 8 |
| 是否同意参加答辩：同意 | | | | | | | 总分 | 85 |
| 评语：该生基于EMS的FDIA对电力CPS检测系统进行了设计。论文章节题目过于简单，表达不了章节研究的主要内容。部分撰写不符合规范要求。具有很强的计算机应用能力。摘要、结论能确切地体现主要内容及成果。译文翻译准确且内容贴近课题。修改后答辩。 | | | | | | | | |

评阅人签字: 2024年 5 月 30 日

**注：1、课题类型包括：A—工程设计；B—科学实验；C—软件开发；D—理论研究；E—应用研究 2、课题来源包括：X—结合实际课题；Y—自拟课题。**

**东北石油大学电气信息工程学院毕业设计（论文）评审表（答辩组）**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 课题名称 | 基于EMS的FDIA电力CPS检测系统设计 | | | | | 课题类型 | 软件开发 | |
| 教师姓名 | 高新成 | 职 称 | 教授 | | 课题来源 | 自拟题目 | | |
| 学生姓名 | 徐浩洋 | 学 号 | 200603140111 | | 专 业 | 电气工程及其自动化 | | |
| 评审  项目 | 评分标准 | | | | | | 满分 | 得分 |
| A | | | C | | |
| 分析解决问题能力  （20分） | 能够通过文献研究，对复杂工程问题进行有效分析，开题论证充分。 | | | 文献检索达到要求，开题论证基本合理。 | | | 10 | 7 |
| 合理利用科学原理、设计实验，分析与解释数据，通过信息综合得到有效结论。 | | | 初步具备设计实验，分析与解释数据以及信息综合能力。 | | | 10 | 8 |
| 答辩  （30分） | 能够与同行进行有效沟通和交流，答辩提纲整洁清楚，时间安排得当，条理清晰、技术用语准确、概念正确。 | | | 提纲、时间安排及报告内容基本符合要求，技术用语和概念基本正确。 | | | 15 | 10 |
| 能有效回应教师提问，回答准确，逻辑清晰。 | | | 基本上能回答主要问题。 | | | 15 | 11 |
| 设计（论文）与专业文献翻译质量  （35分） | 论文内容符合撰写要求、规范，图纸标准整洁。理论与分析正确、论述条理清晰、文理通顺、数据详实，结论严谨。 | | | 内容70％以上符合撰写要求。理论与分析基本正确、论述基本清晰、通顺。 | | | 15 | 12 |
| 译文翻译准确且内容贴近课题，译文字数3000字以上。 | | | 译文基本准确，字数2000字以上。 | | | 10 | 8 |
| 论文字数≥1.5万字，摘要300字左右；摘要、结论能确切地体现主要内容及成果。 | | | 论文字数≥1.2万字，摘要、结论能基本体现主要工作内容及成果。 | | | 10 | 7 |
| 使用现代工具  （5分） | 根据毕业设计需要能够开发或选用所需的现代工程和信息技术工具，仿真、设计和辨识电力能源及石油工业(为油保电)中的复杂工程问题，并能够分析其优缺点，理解其局限性。 | | | 具有一定的现代工程和信息技术工具应用能力。 | | | 5 | 4 |
| 环境和可持续发展  （5分） | 毕业设计兼顾环境和可持续发展思想，能清楚认识该设计对社会、健康、安全、法律、文化及环境的影响与责任。能合理评估毕业设计成果对人类和环境是否存在潜在的损害或隐患。 | | | 技术因素认识较为充分，社会、健康、安全、法律、文化及环境因素考虑不充分，方案设计基本合理。 | | | 5 | 4 |
| 成本核算  （5分） | 工程设计类毕业设计能核算该设计成果所需成本，并与市场上同类商品做比较。  应用研究类毕业设计能评估该研究的社会或经济价值，以及后续产生的社会经济影响。 | | | 工程设计类毕业设计能基本完成毕业设计成果所需成本核算；  应用研究类毕业设计能对该研究的社会或经济价值有初步认识。 | | | 5 | 4 |
| 答辩成绩 | 75 | | | | | | | |
| 毕业设计（论文）成绩及评语 | 毕业设计成绩（结构分）：=90×10%+86×30%+ 85×20%+ 75×40%  评语：该生基于EMS的FDIA对电力CPS检测系统进行了设计。论文内容符合撰写要求、规范，具有一定的现代工程和信息技术工具应用能力。毕业设计兼顾环境和可持续发展思想，论文字数≥1.2万字，摘要、结论能基本体现主要工作内容及成果。但是答辩幻灯片和答辩时间安排得不好。成绩为中等。 | | | | | | | |

注：结构分=中期检查×10%+指导教师评分×30%+评阅教师评分×20%+答辩总分×40%答辩小组负责人签字：  2024年6月1 日

答辩委员会负责人签字： 徐建军签名 2024年6月1 日

东北石油大学本科生毕业设计（论文）

英文主要参考文献及中文译文

Detection and Localization of Load Redistribution Attacks on Large-scale Systems

电网的大规模系统中负载再分配攻击的检测与定位

——原文摘自Journal of Modern Power Systems and Clean Energy (2022)

361-370

|  |  |
| --- | --- |
| 专业： | 电气工程及其自动化 |
| 班级： | 电气20-1班 |
| 姓名： | 徐浩洋 |
| 学号： | 200603140111 |

2024年5月24日

**Abstract**

A nearest neighbor-based detection scheme against load redistribution attacks is presented. The detector is designed to scale from small to very large systems while guaranteeing consistent detection performance. Extensive testing is performed on a realistic, large scale system to evaluate the performance of the proposed detector against a wide range of attacks, from simple random noise attacks to sophisticated load redistribution attacks. The detection capability is analyzed against different attack parameters to evaluate its sensitivity. Finally, a statistical test that leverages the proposed detection algorithm is introduced to identify which loads are likely to have been maliciously modified, thus, localizing the attack subgraph. This test is based on ascribing to each load a risk measure (probability of being attacked) and then computing the best posterior likelihood that minimizes log-loss.

**Key words:** attack detection; cybersecurity; false data injection (FDI) attack; load redistribution attack; machine learning; nearest neighbor

摘 要

提出了一种基于最近邻的检测方案，用于抵抗负载重分配攻击。该检测器旨在从小型到非常大型的系统中扩展，同时保证一致的检测性能。在现实的大型系统上进行了广泛的测试，以评估所提出检测器针对从简单的随机噪声攻击到复杂的负载重分配攻击的各种攻击的性能。分析了针对不同攻击参数的检测能力，以评估其敏感性。最后，引入了一种利用所提出检测算法的统计测试，以识别可能被恶意修改的负载，从而定位攻击子图。该测试基于为每个负载分配一个风险度量（被攻击的概率），然后计算最小化对数损失的最好后验概率。

关键词：攻击检测；网络安全；错误数据注入（FDI）攻击；负载重分配攻击；机器学习；最近邻

第1章 INTRODUCTION引言

The electrical grid is a constantly evolving cyber-physical system and, as such, it is increasingly reliant on information and communication technology. A vast research effort undertaken in the past decade in the field of cybersecurity of power systems has identified some crucial vulnerabilities of the cyber layer which can be exploited to disrupt the physical system. In this context, [1] shows that state estimation (SE) and the traditional bad data detector (BDD) used in energy management systems (EMSs) can be easily spoofed and bypassed via false data injection (FDI) attacks. This finding represents the basis for the design of a wide class of attacks called load redistribution (LR) attacks. Load redistribution attacks can be performed by injecting intelligently designed false measurements that lead to a wrong estimate of the system state. From the operator’s perspective the attack makes it appear as if the system loads have changed from their actual values, without changing the net load. In [2] and [3], the concept of load redistribution attacks is formalized by developing a bi-level attacker-defender problem for targeted attacks. In this setting, the attacker can design false measurements which can cause physical consequences on the system; specifically, [3] attempts to find an attack, unobservable to the EMS, to cause a power overload on a target line. In a similar fashion, [4], [5] present examples of LR attacks on the electricity market: the authors show that it is possible to launch load redistribution attacks that create system congestion, thus manipulating locational marginal prices. We propose a new bad data detector that can identify LR attacks based on the analysis of load estimates, thus overcoming the limitations of SE and the traditional BDD. In [6], we developed three anomaly detectors, each based on a different machine learning technique: replicator neural network, support vector machine, and nearest neighbor. These detectors can effectively determine if the observed loads represent a normative system state or if they have been maliciously modified. The nearest neighbor-based detector works by finding in the historical data the closest load vector to the real time loads and, based on the measured Euclidean distance, a thresholding technique is used to decide if the loads are normative or anomalous. From our tests, nearest neighbor demonstrated the best performance out of the three proposed. In this paper, we build on this preliminary work to design an improved detector and an attack localization scheme. The novel contributions of this paper are as follows:

• The basic detector is modified so that it scales to much larger power system models while preserving the good detection performance shown in [6]. This is achieved by devising a grouping strategy to organize the system loads into clusters that can be analyzed independently.

• Extensive testing and sensitivity analysis is performed to evaluate the performance of the detector against intelligently designed LR attacks as well as random anomalous load changes. This allows for the characterization of the strengths and limitations of the detector. Furthermore, the proposed algorithm is integrated within a complete EMS platform to showcase its detection performance and computational efficiency.

• Building on the improved detector, a statistical approach is presented to localize the attacks and determine the likelihood of each load of being attacked. The deviation in loads is captured via a Z-score and log-loss is used as a measure to find the likelihood function that minimizes the error. This represents a crucial step towards the development of decision tools that can help operators to securely manage power systems when targeted by cyber attacks work, the method there proposed is designed for distribution systems and, as we will explain later, the attacks tested are not realistic as they simulate changes in loads of up to 100%. Other work focuses on using deep neural networks to learn the temporal correlation which exists between the real-time measurements and previous samples [8], or verifying the statistical behavior of the estimated states over time [9]. The assumption on which these detectors are built is that when an attack is injected, the false measurements are not compatible with the dynamics observed from the previous measurements thus making it possible to flag them as attacked. Based on this, a slow ramping attack which only slightly changes the system’s state at each sampling time will likely not be detected. Moreover, these detectors are tested on limited attack scenarios and their performance is not verified against multiple classes of attacks. Finally, while many attack detectors have been proposed, to the best of the authors’ knowledge, the idea of detecting FDI attacks by identifying patterns in the observed loads has not been explored before. The rest of the paper is organized as follows: in Section II a description of load redistribution attacks and how to design them is presented. In Section III we summarize the basic detection algorithm we have presented in [6] and show its performance limitations when used on large scale systems. The required improvements are described in Section IV and the detection results on a wide range of load redistribution attacks are presented in Section V. Section VI illustrates the statistical analysis that leverages the improved nearest neighbor-based detector to determine the buses that have been attacked

控制安全电力网格是一个不断发展的网络物理系统，因此，它越来越依赖于信息和通信技术。在电力系统网络安全领域，过去十年进行了大量的研究工作，发现了一些可以利用来破坏物理系统的网络层的关键漏洞。在这方面，文献[1]表明，状态估计（SE）和能量管理系统（EMS）中使用的传统不良数据检测器（BDD）可以通过虚假数据注入（FDI）攻击轻易地被欺骗和绕过。这一发现代表了设计一类广泛的攻击——负载重分配（LR）攻击的基础。负载重分配攻击可以通过注入智能设计的虚假测量来实现，这些测量导致系统状态的错误估计。从运营商的角度来看，这种攻击使得系统负载看起来好像从其实际值发生了变化，而实际上并没有改变净负载。在文献[2]和[3]中，通过为有针对性的攻击开发一个双层攻击者-防御者问题，对负载重分配攻击的概念进行了形式化。在这种设置中，攻击者可以设计虚假测量，这些测量可以对系统产生物理后果；特别是，文献[3]试图找到一个对EMS不可见的攻击，以对目标线路造成过载。类似地，文献[4]和[5]展示了在电力市场上的LR攻击示例：作者们表明，可以发起负载重分配攻击，创建系统拥塞，从而操纵位置边际价格。我们提出了一种新的不良数据检测器，它可以根据对负载估计的分析来识别LR攻击，从而克服了SE和传统BDD的限制。在文献[6]中，我们开发了三种异常检测器，每种检测器基于不同的机器学习技术：复制器神经网络、支持向量机和最近邻。这些检测器可以有效地确定观察到的负载是否代表规范系统状态，或者它们是否被恶意修改。基于最近邻的检测器通过在历史数据中找到与实时负载最接近的负载向量，然后基于测量的欧几里得距离，使用阈值技术来决定负载是否规范或异常。从我们的测试中，最近邻在所提出的三个中表现最佳。在本文中，我们基于这项初步工作来设计一个改进的检测器和攻击定位方案。本文的新颖贡献如下：

•基本检测器经过修改，可以扩展到更大的电力系统模型，同时保留了文献[6]中显示的良好检测性能。这是通过设计一个分组策略来实现的，该策略将系统负载组织成可以独立分析的集群。

•进行了广泛测试和敏感性分析，以评估检测器针对智能设计的LR攻击以及随机异常负载变化的性能。这允许表征检测器的优势和局限性。此外，所提出的算法被集成到一个完整的EMS平台中，以展示其检测性能和计算效率。

•在改进的检测器的基础上，提出了一种统计方法来定位攻击并确定每个负载被攻击的可能性。负载偏差通过Z分数捕获，log-loss用作度量来确定最小化误差的可能性函数。这代表了向开发决策工具迈出的关键一步，这些工具可以帮助运营商在遭受网络攻击时安全地管理电力系统。

在其他工作中，文献[7]中提出的方法是为配电网设计的，正如我们稍后将解释的，所测试的攻击并不现实，因为它们模拟了负载高达100%的变化。其他工作集中在使用深度神经网络学习实时测量和先前样本之间的时间相关性[8]，或验证估计状态随时间的统计行为[9]。这些检测器构建的假设是，当注入攻击时，虚假测量与从先前测量观察到的动态不兼容，因此可以将其标记为被攻击。基于此，一个仅在每次采样时间稍微改变系统状态的缓慢爬坡攻击可能不会被检测到。此外，这些检测器只在有限的攻击场景上进行测试，它们的性能没有针对多类攻击进行验证。最后，尽管提出了许多攻击检测器，但据作者所知，通过识别观察到的负载中的模式来检测FDI攻击的想法尚未被探索。本文的其余部分组织如下：在第II节中，介绍了负载重分配攻击以及如何设计它们。在第III节中，我们总结了我们在文献[6]中提出的基本检测算法，并展示了在大型系统上使用时的性能限制。所需改进在第IV节中描述，广泛的负载重分配攻击的检测结果在第V节中呈现。第VI节说明了利用改进的基于最近邻的检测器进行的统计分析，以确定被攻击的母线。

第2章 ATTACK MODEL AND DESIGN攻击模型与设计

For a power system, the relationship between the vector of measurements and the state vector can be written as

(1)

where h is the non-linear relationship between measurements and states (usually, complex bus voltages), while vector e represents the random measurement noise. As shown in [1], an unobservable attack can be constructed by replacing the original measurements with a corrupted set of measurements such that.

(2)

where is the state attack vector. Based on this fundamental result, the authors in [3] present a bi-level optimization problem to compute an attack vector that will maximize the power flow on a specific target line. To cause such physical consequences on the system, the false measurements must be designed in such a way that they will initiate a system response in the form of generation redispatch. This can be done by creating an unobservable attack that will lead state estimation to wrongly estimate the system loads, thus causing a wrong dispatch solution. The bi-level optimization problem proposed in [3] is improved in [10] to make it more efficient and scalable to large scale systems. The first level models the attacker’s choice of attack to maximize the overload on a target line; the second level models the system’s response to the attack via a DCOPF to observe the resulting physical consequences. In designing the false measurements, the attacker is limited on how much the false loads can deviate from the real loads: the load shift factor represents the maximum percentage by which any load can be modified. This constraint comes from the fact that an operator would easily identify a large change in load over a short period of time as an anomaly; in the existing literature, load shifts ranging from 10% [3], [10] to 50% [2] are considered as the maximum allowable for an attack to remain unobservable. The attack detector presented in this paper aims at identifying in real time if the set of measured loads is genuine or if it is the result of an attack on state estimation. As we will show, the proposed detector is effective in identifying attacks with relatively low load shifts and it reaches perfect detection for attacks with 15% load shifts or higher.

对于一个电力系统，测量向量和状态向量之间的关系可以写成如下形式：

(1)

其中是测量和状态（通常是复杂的母线电压）之间的非线性关系，而向量表示随机的测量噪声。如文献[1]所示，可以通过用一组被污染的测量值替换原始测量值来构建一个不可观测的攻击，使得

(2)

其中是状态攻击向量。基于这个基本结果，文献[3]中的作者们提出了一个双层优化问题，用以计算一个攻击向量c，该向量将最大化特定目标线路上的电力流。为了在系统上造成这样的物理后果，虚假测量必须以这样的方式设计：它们将引发系统响应，形式为发电重新调度。这可以通过创建一个不可观测的攻击来实现，该攻击将导致状态估计错误地估计系统负载，从而造成错误的调度解决方案。文献[10]对文献[3]中提出的双层优化问题进行了改进，使其更加高效，并能够扩展到大型系统。第一层模型描述了攻击者选择攻击以最大化目标线路上的过载；第二层模型通过直流最优潮流（DCOPF）来模拟系统对攻击的响应，以观察由此产生的物理后果。在设计虚假测量时，攻击者对于虚假负载偏离真实负载的程度是有限制的：负载转移因子代表了任何负载可以被修改的最大百分比。这个约束来自于这样一个事实：运营商很容易将短时间内负载的大幅变化识别为异常；在现有文献中，将 10%[3]、[10] 到 50%[2]的负载转移视为攻击可以保持不可观测的最大允许范围。本文提出的攻击检测器的目标是在实时识别测量的负载集是否真实，还是状态估计攻击的结果。正如我们将展示的，所提出的检测器在识别相对较低的负载转移攻击方面是有效的，并且在攻击具有15%或更高负载转移时达到完美检测。

第3章 BASIC DETECTION ALGORITHM

## 3.1 Small systems小系统

The proposed attack detection mechanism works by analyzing the correlation structure within the currently observed load values and comparing it to attack-free historical load data. The measured load configuration to be tested is given as input to the detector which generates a scalar value. This value is then compared against a thresholdto label the loads as normative or attacked. To evaluate the detection performance, two metrics are used: detection probability, which is the ratio between the number of cases correctly labelled as attacked and the total number of attacked cases tested, and false alarm rate, which is the number of normative cases that are labelled as attacked divided by the total number of normative cases tested. The specific value of the threshold is chosen as a tradeoff between detection probability and false alarm rate. Our approach can be considered a semi-supervised learning problem since the detectors are trained only on normative data which is already widely available to operators. Because no attacked data is needed in the training phase, the detectors will not be biased towards specific types of attacks. Given the almost identical detection capability of the three detectors tested in [6], in the following work, the nearest neighbor detector is chosen for its computational and explanatory simplicity.

Nearest neighbor algorithms are based on the assumption that data labelled as normative lies in limited, dense regions of space while anomalies are located further from these neighborhoods [11], [12]. Let us define as the vector of observed load values to be tested, where is the number of loads in the system. The normative data is represented by the set of historical load vectors that have been observed in the past, where is the total number of historical vectors. The classification is done by measuring the Euclidean distance between the current load profile p and every vector in the historical dataset (assumed to be attack free). The closest distance for sample is defined as

(3)

To labelas normative or attacked, d is compared against a predetermined threshold . In [6], we tested this approach on the IEEE 30 bus system. Publicly available zonal historical load data from the PJM system [13] was mapped to the loads of the 30 bus system to create hourly load profiles for 5 consecutive years. The proposed detector showed very high detection capability with low false alarm rates. Figure 1 is taken from [6] and it shows some of the results obtained on this small system. The blue points represent the minimum distance for the normative load vectors (not attacked) while in green and red are the distances corresponding to attacked cases with 10% and 15% load shift, respectively. This illustrates how loads resulting from attacks lead to much higher nearest neighbor distances compared to normative load profiles; thus, suggesting that the minimum distance is an effective metric for attack detection.

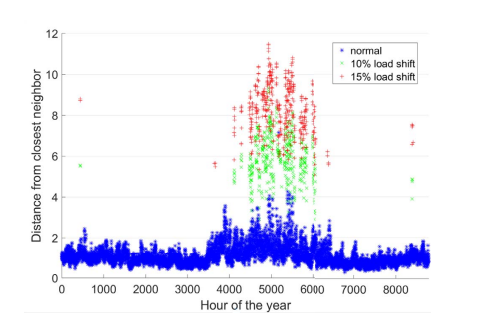


图1 IEEE 30 bus system: distribution of nearest neighbor distance for normative and attacked cases.IEEE 30 总线系统：规范和攻击案例的最近邻距离分布

所提出的攻击检测机制通过分析当前观察到的负载值内的相关性结构，并将其与无攻击的历史负载数据进行比较来工作。待测试的测量负载配置作为输入提供给检测器，检测器生成一个标量值。然后将这个值与阈值进行比较，以将负载标记为规范或被攻击。为了评估检测性能，使用了两个指标：检测概率，即正确标记为被攻击的案例数与测试的总被攻击案例数之间的比率，以及误报率，即被标记为被攻击的正常案例数除以测试的总正常案例数。阈值的特定值是检测概率和误报率之间的权衡。我们的方法可以被视为一个半监督学习问题，因为检测器只在规范数据上进行训练，而这些数据已经广泛地提供给运营商。由于训练阶段不需要攻击数据，因此检测器不会偏向于特定类型的攻击。鉴于[6]中测试的三种检测器几乎相同的检测能力，在后续工作中，选择最近邻检测器是因为其计算和解释的简单性。最近邻算法基于这样一个假设：标记为规范的 数据位于空间的有限密集区域，而异常值则位于这些邻域之外[11],[12]。让我们定义为待测试的观察负载值向量，其中 n 是系统中的负载数量。规范数据由历史负载向量集 表示，这些历史负载向量 过去曾经观察到，其中是历史向量的总数。分类是通过测量当前负载轮廓与历史数据集中每个向量之间的欧几里得距离来完成的。样本的最短距离定义为

(3)

为了将 标记为规范或被攻击，将 与预定的阈值 进行比较。在[6] 中，我们对 IEEE 30 总线系统测试了这种方法。从 PJM 系统[13] 公开的区域历史负载数据被映射到 30 总线系统的负载上，以创建连续 5 年的每小时负载配置文件。所提出的检测器展示了非常高的检测能力，同时误报率很低。图 1 取自[6]，它展示了在这个小系统上获得的一些结果。蓝色点代表规范负载向量（未受攻击）的最小距离，而绿色和红色点分别对应于 10% 和 15% 负载转移的攻击案例的距离。这说明了与规范负载配置文件相比，攻击导致的负载会使最近邻距离大大增加；因此，表明最小距离是攻击检测的有效指标。

## 3.2 Large systems大系统

While the results obtained on the 30 bus system are promising, the detector needs to be tested on large scale systems to verify its performance in a more realistic setting and to guarantee its suitability for implementation in real system operations. To this end, the same analysis presented in [6] and summarized in the previous section is performed on the synthetic Texas system [14], [15]. This model, developed at Texas A&M, is a synthetic grid of the state of Texas. It has 2000 buses, 3206 branches, and 1125 loads and it includes bus-level hourly load data for the year 2016. Using the attack model described in Section II, around 280 attacks with load shift of 15% have been designed on the most congested cases. We randomly selected 90% of the 8784 normative load vectors to represent the historical data, and the remaining 10% for testing. The nearest neighbor algorithm is used to compute the minimum distance for the test and the attacked load vectors against the historical load data. Figure 2 shows the minimum distance for each normative load vector (blue points) and for the attacked cases (red points). It is easy to see that the detector does not perform well, and that the attacked cases are indistinguishable from the normative ones. This can be explained by the fact that when measuring the Euclidean distance between two high-dimensional vectors, the contribution of a limited subset of dimensions is small. That is, if only a few tens of loads are attacked, the total distance measured over hundreds of loads will deviate only slightly from the distance computed on the load vector where no loads are modified. In this case, each load vector has dimension 1125 and the attacks modify only about 100 to 200 loads; the effect of the attacked loads is not large enough to result in distance values significantly higher than those of the normative data.

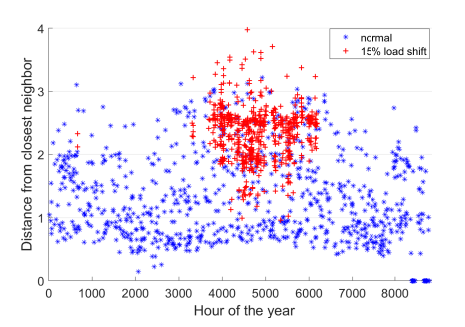


图2 Synthetic Texas system: distribution of nearest neighbor distance for normative and attacked cases.合成德克萨斯系统：规范和攻击案例的最近邻距离分布。

尽管在 30 总线系统上获得的结果是令人鼓舞的，但检测器需要在大规模系统上进行测试，以在更现实的设置中验证其性能，并确保其适合在实际系统操作中实施。为此，我们在 [6] 中呈现的相同分析和对前一部分的总结在合成德克萨斯系统 [14], [15] 上进行了。这个模型是在德克萨斯 A&M 开发的，是德克萨斯州的合成电网。它有 2000 个总线、3206 个分支和 1125 个负载，并包括了 2016 年的总线级别每小时负载数据。使用在第 II 节中描述的攻击模型，针对最拥堵的情况设计了约 280 次负载转移为 15% 的攻击。我们从 8784 个规范负载向量中随机选择了 90% 来代表历史数据，其余 10% 用于测试。最近邻算法用于计算测试和攻击负载向量与历史负载数据的最小距离。图 2 显示了每个规范负载向量（蓝色点）和攻击案例（红色点）的最小距离。很容易看出，检测器表现不佳，攻击案例与规范案例难以区分。这可以解释为，当测量两个高维向量之间的欧几里得距离时，有限子集维度的贡献很小。也就是说，如果只攻击了几十个负载，在数百个负载上测量的总距离与在没有任何负载被修改的负载向量上计算的距离只会略有偏差。在这种情况下，每个负载向量都有 1125 个维度，攻击只修改了大约 100 到 200 个负载；攻击负载的效果不足以导致距离值显著高于规范数据。

第4章 DETECTION ON LARGE SCALE SYSTEMS大规模系统的检测

The simple test presented in the previous section shows that the basic nearest neighbor detector introduced in [6] does not perform as well when applied to large scale systems (hundreds or thousands of buses). For this reason we need a new approach to improve the detection mechanism to be effective for any system, regardless of its size. The method we propose aims to leverage the capability of the nearest neighbor algorithm to identify anomalous loads even when only a small fraction of the total system loads are being attacked

Previous work has shown that in a large transmission-level system, load redistribution attacks tend to target only some portions of the network. As a consequence, the loads which are modified represent a subset of the total system loads and they are restricted to a subgraph of limited size. Based on these observations, the detection algorithm is modified so that it analyzes multiple predefined subsets of the system loads. In this work we propose a grouping strategy that can be used to divide the loads into relatively small groups such that they can be analyzed independently and in parallel by the attack detector. It is important to notice that the strategy presented in the next section is just one example of grouping which empirically worked well for the systems tested. Different grouping techniques, perhaps leveraging specific knowledge and insights regarding the power system to be secured, can be easily implemented within the framework of the proposed detection algorithm.

前一部分中简单测试显示，在[6]中引入的基本最近邻检测器在应用于大规模系统（数百或数千个总线）时性能并不理想。因此，我们需要一种新方法来改进检测机制，使其对任何系统都有效，无论其大小。我们提出的方法旨在利用最近邻算法识别异常负载的能力，即使只有系统总负载的一小部分受到攻击。

先前的研究表明，在大型输电系统中，负载重分配攻击倾向于只针对网络的某些部分。因此，被修改的负载代表了整个系统负载的一个子集，并且它们被限制在一个有限大小的子图中。基于这些观察结果，检测算法被修改，以便它分析系统负载的多个预定义子集。在这项工作中，我们提出了一种分组策略，可以将负载划分为相对较小的组，以便攻击检测器可以独立并行地分析这些组。重要的是要注意，接下来部分中提出的策略只是一个分组示例，它在测试的系统中经验上表现良好。不同的分组技术，可能利用了关于需要保护的电力系统的特定知识和洞察，可以轻松地在所提出的检测算法的框架内实现。

## 4.1 Grouping strategy分组策略

The first step required to define the load groups is to sort the loads based on their MW rating, from largest to smallest. Starting from the largest load, the first group is created by including the load itself and all its neighboring loads within a certain radius , where the radius is measured as the smallest number of branches connecting two loads. At this point, the next largest load is selected and if it is not contained in any of the previous groups, a new group is created. This process is repeated until groups are defined. Note that it is possible for a bus to be contained in multiple groups, or no groups. The parameters and have a direct effect on the detection performance and their selection will be discussed in the next sections. As our results show, this grouping strategy proves to be very effective in the detection of LR attacks because it ensures that the largest loads in a system are monitored. Prior work on FDI attacks on SE shows that, to cause significant consequences, an attacker is required to target large loads in order to create large power flow changes [2]–[5].

定义负载组的第一步是根据负载的兆瓦（MW）等级进行排序，从大到小排序。从最大的负载开始，第一个组是通过包括负载本身及其在一定半径内的所有相邻负载来创建的，其中半径是通过连接两个负载的最小分支数量来测量的。在这一点上，选择下一个最大的负载，如果它没有被包含在前面的任何组中，就会创建一个新的组。这个过程一直重复，直到定义了个组。需要注意的是，一个总线可能包含在多个组中，或者没有组。参数和对检测性能有直接影响，它们的选取将在下一部分讨论。正如我们的结果所示，这种分组策略在检测 LR 攻击方面非常有效，因为它确保了对系统中的最大负载进行监控。关于 SE 的 FDI 攻击的先前的研究表明，为了造成重大后果，攻击者需要针对大负载以创建大的电力流变化[2]–[5]。

## 4.2 Detection algorithm检测算法

Dividing the system loads into groups allows us to overcome the dimensionality issue observed in Section III-B. The basic nearest neighbor detector can be used on large systems by running the algorithm individually on each load group. In this case, a threshold must be defined for each individual group ,for. The vector containing the estimated loads computed by SE is divided into groups according to the procedure described in the previous subsection. Let us define as the vector containing the real-time values of the loads in group. For each group, the minimum distance between the load vector and the corresponding loads in the historical dataset is calculated as

(4)

where is the subset of loads belonging to group from the rth historical load vector. The minimum distance is then compared to the threshold to determine if the loads in group are normative or anomalous. Specifically, if , an alarm is raised, while if the loads are considered attack-free. This process is repeated for every group and if one or more alarms are raised, the load vector is labelled as anomalous.

将系统中的个负载分成组可以让我们克服在第 III-B 节观察到的维度问题。基本最近邻检测器可以通过对每个负载组分别运行算法来用于大型系统。在这种情况下，必须为每个单独的组 定义一个阈值 ，其中 。由 SE 计算的负载估计值组成的向量 根据前一小节中描述的程序分为个组。让我们定义 为包含组中实时负载值的向量。对于每个组，计算负载向量 与历史数据集中相应负载之间的最小距离，如

(4)

其中 是来自第 r 个历史负载向量的组的负载子集。然后将最小距离与阈值 进行比较，以确定组中的负载是规范的还是异常的。具体来说，如果 ，则发出警报，而如果，则认为负载是攻击自由的。这个过程对每个组重复进行，如果有一个或多个警报被触发，负载向量 被标记为异常。

第5章 TESTING THE IMPROVED DETECTOR测试改进的检测器

## 5.1 Experimental procedure实验程序

The performance of the nearest neighbor-based detector in conjunction with the grouping strategy is tested in depth in the following sections. The detection capability is measured both on intelligently designed attacks as well as random load redistribution attacks; moreover, we study its sensitivity to different parameters, such as the load shift of the attack and the number of attacked buses.

The goal of the following experiments is to analyze the quality of the detector at understanding if a load vector is normative or attacked. The primary test system used is the synthetic Texas system described in Section III-B; all numerical results discussed below are based on this system. Additional testing performed on the 2383 bus Polish test case [16], for which we generated historical load profiles based on real data from a major US ISO [17], showed comparable results and it is here omitted due to space constraints. First, the 1125 system loads in the Texas system are divided into groups following the procedure from Section IV-A. For the tests described below, the parameters chosen for the creation of the groups are: radius = 7 and number of groups = 35. These values ensure that more than 60% of the loads in the system are included in one or more groups and the ones that are outside of the groups have at least one monitored neighboring load. Moreover, these load groups are equally spread across the system; as a result, the system is effectively monitored in its entirety. Preliminary testing has shown that increasing the number of groups (and, thus, of the loads considered) did not improve detection performance.

In each experiment, two datasets are needed: the normative load data and the anomalous load data, where varies for the different type of attacks. The normative data represents one load vector for each hour of 2016 (2016 was a leap year). The set contains attacked load vectors which are designed starting from the normative load vectors in ; depending on the type of attack, some of the loads are modified either intelligently or randomly, as described below. To compute detection probability and false alarm, the load vectors of dataset are first divided into three subsets: historical, training, and testing. The historical dataset includes 70% of the total hours of 2016 and it represents the past loads known to the system operator and used in its nearest neighbor algorithms. The training dataset represents another 20% of and it is needed to determine the thresholdsfor each load group. The remaining 10% of normative load vectors is used as the testing dataset to determine the false alarm rate. To determine the threshold τj for group , the minimum distance between each load vector for in and the historical dataset is computed using (4). The threshold is defined as a fixed fraction of the maximum closest distance, defined for each group as

(5)

For each load vector in , the minimum distance from is computed and compared with the threshold: the false alarm rate is the ratio between the number of times a load vector is labelled as attacked (e.g. at least one load group has minimum distance greater than its corresponding threshold) and the total number of load vectors in . Similarly, the minimum distance is calculated for every attacked case and the detection probability is computed. As we will explain in more detail in the next sections, varying the threshold about the value allows to span different detection probabilities and false alarm rates in order to determine the receiver operating characteristic (ROC). The proposed algorithm is extremely efficient and testing a load vector only takes a fraction of a second on a normal laptop; thus, even on large power systems, the detector can easily run in real-time. Because the normative load dataset is limited to one year, to have a more complete assessment of the performance of the detector, a k-folding technique is used to test every hour of the year by rotating through multiple sets of historical, training, and testing datasets. The hours of 2016 are randomly divided into ten equally sized partitions as illustrated in Fig. 3; the partitions are fixed throughout the testing process. For the first fold, the load vectors corresponding to the hours in the first partition are assigned to , the second and third partitions to and the remaining seven represent the historical data . Given these partitions, the number of false alarms and the number of attacks detected are calculated on the normative and attacked load vectors in the testing partition. The subsequent folds are created by shifting the partitions assigned to the three datasets by one: for example, in the second fold will coincide with the second partition, with the third and fourth partitions, and . with the remaining ones. The final detection probability is then calculated by adding up the correctly identified attacks across all folds and dividing by the total number of attacks; the false alarm rate is the total number of false alarms divided by 8784.

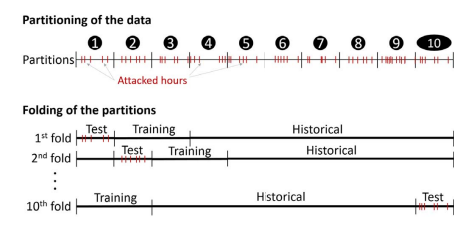


图3 Description of the 10-folding technique and definition of the datasets十折交叉验证技术描述和数据集定义

在接下来的章节中，我们将深入测试基于最近邻的检测器与分组策略的性能。检测能力将在智能设计的攻击以及随机负载重分配攻击上进行测量；此外，我们还研究了它对不同参数的敏感性，例如攻击的负载转移和受攻击的母线数量。

以下实验的目的是分析检测器在理解负载向量是否规范或被攻击方面的质量。主要测试系统是第三部分B节中描述的合成德克萨斯系统；下面讨论的所有数值结果都是基于这个系统。此外，对拥有2383个总线的波兰测试案例进行了额外测试，我们基于主要美国ISO的真实数据生成了历史负载配置文件，结果相当，但由于空间限制，此处省略。首先，德克萨斯系统中的1125个系统负载按照第四部分A节的程序进行分组。对于下面描述的测试，用于创建组的参数选择为：半径 = 7 和组数 = 35。这些值确保系统中有超过60%的负载包含在一个或多个组中，而那些不在组中的负载至少有一个被监控的相邻负载。此外，这些负载组在系统上均匀分布；因此，系统可以得到有效的监控。初步测试表明，增加组数（从而增加被考虑的负载数量）并未提高检测性能。

在每个实验中，需要两个数据集：规范负载数据 和异常负载数据，其中 H 因不同类型的攻击而异。规范数据代表2016年每小时的一个负载向量（2016年是闰年）。集合 包含从 中的规范负载向量设计的攻击负载向量；根据攻击类型，一些负载被智能地或随机地修改，如下所述。为了计算检测概率和误报率，负载向量数据集 首先分为三个子集：历史、训练和测试。历史数据集包括2016年总小时数的70%，它代表系统运营商已知的历史负载，并用于其最近邻算法。训练数据集 代表 的另一20%，用于确定每个负载组的阈值 。剩余的10%规范负载向量用作测试数据集 以确定误报率。为了确定组 的阈值 ，使用公式（4）计算 中每个负载向量 与历史数据集之间的最小距离 。阈值 定义为每个组的最大最近距离的固定比例，定义为

(5)

对于中的每个负载向量，计算与 的最小距离，并与阈值进行比较：误报率是负载向量被标记为攻击的次数（例如，至少有一个负载组的最小距离大于其对应的阈值）与 中负载向量总数之比。类似地，为每个攻击案例计算最小距离，并计算检测概率。正如我们在下一部分更详细地解释的那样，调整阈值相对于 的值可以跨越不同的检测概率和误报率，以确定接收者操作特征（ROC）。所提出的算法极其高效，测试一个负载向量只需要普通笔记本电脑的一小部分时间；因此，即使在大型电力系统中，检测器也可以轻松地在实时运行。由于规范负载数据集仅限于一年，为了更全面地评估检测器的性能，使用 k-折技术测试一年的每个小时，通过旋转多个历史、训练和测试数据集。2016年的小时被随机分为十个等大小的分区，如图3所示；这些分区在整个测试过程中固定不变。对于第一折，第一分区的负载向量被分配到 ，第二和第三分区到 ，剩余的七个代表历史数据 。根据这些分区，计算测试分区中规范和攻击负载向量的误报次数和检测到的攻击次数。后续的折是通过将分区分配给三个数据集进行移动创建的：例如，在第二折中， 将与第二分区重合， 与第三和第四分区重合， 与剩余的几个分区重合。最终的检测概率是通过将所有折叠中正确识别的攻击次数相加，然后除以总攻击次数计算出来的；误报率是总误报次数除以8784。

## 5.2 Detection of intelligently designed attacks智能设计的攻击检测

We use the bi-level problem in [3] to design attacks that simulate specific changes in loads to cause physical overflows on a target line, while being unobservable to the system operators (and SE). The testing procedure described in the previous sections is employed here to verify the ability of the proposed detector and grouping strategy in correctly identifying malicious loads resulting from these intelligent attacks. The bi-level problem in [3] is structured so that any one branch can be selected as a target, and an attack will be designed to maximize the flow on it. Depending on the specific system conditions, a successful attack (that is, one causing the resulting power flow to go above the branch rating) may not exist; generally, the higher the pre-attack flow, the more likely the attack will lead to overflow. For this reason, the first step in designing the attacks is to run an AC optimal power flow (ACOPF) for every load vector in to identify any congested branch. For the purpose of this study, a congested branch is any line or transformer that has a base case power flow loading of 90% of its rating or more. Attacks are designed on each hour of 2016 for which one or more branches are congested. These branches are individually selected as targets of the attacks; thus, an hour will have as many different attacks as the number of branches with base case flow above 90% in that hour. Moreover, for each target branch, attacks are designed with a load shift factor ranging from 1% to 15% in steps of 1%. This allows us to study how the detection performance varies in relation to the attack magnitude. As a result of this process, 8861 successful attacks are computed, across every hour, target line, and load shifts. The resulting attacked load vectors have been tested following the k-folding procedure in Section V-A, where the threshold for each group was varied from 0.9 to 1.1 timesFigure 4 shows the detection probability (colored scale) as a function of the load shift (x-axis) and the false alarm rate (y-axis). It can be seen that the detector does not perform well on attacks with very low load shifts, while for load shift between 10 and 15% the detection probability goes from 80 to 100% with false alarm rates ranging from 0 to 3%. While the load shift factor is an important metric in the design phase of the attacks, from an operator’s perspective it is more meaningful to evaluate the physical consequences of the attacks. Figure 5 shows the detection probability as a function of the line overload resulting from the attacks. From this figure we can easily see that the detector has extremely high probability of detecting any attack that would cause important physical damage: considering the safety margins built into the operational tools, an overload of 2 or 3% is not likely to cause any system disruption.

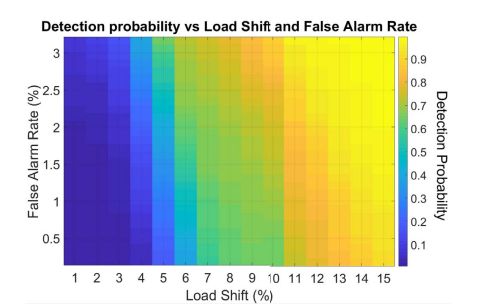


图4 Intelligent attacks: detection probability as a function of load shift and false alarm rate智能攻击：检测概率作为负载转移的函数和误报率

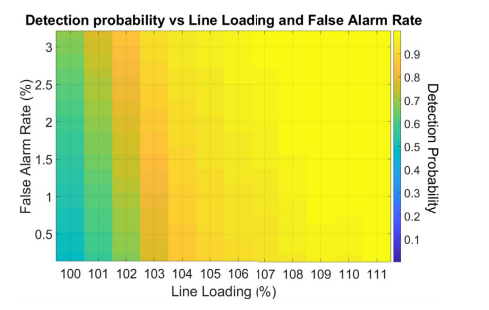


图5 Intelligent attacks: detection probability as a function of line overload and false alarm rate. 智能攻击：检测概率作为线路过载的函数和误报率

我们使用文献 [3] 中的双层问题来设计攻击，这些攻击模拟特定的负载变化以在目标线路上引起物理过载，同时对系统操作员（和状态估计器）不可见。这里采用了前述章节中描述的测试程序来验证所提出的检测器和分组策略在正确识别这些智能攻击产生的恶意负载方面的能力。文献 [3] 中的双层问题结构允许选择任何一条分支作为目标，并设计攻击以最大化其上的电力流。根据具体的系统条件，可能不存在成功的攻击（即导致电力流超过分支额定值）；通常，预攻击流越高，攻击导致过载的可能性越大。因此，设计攻击的第一步是对 中的每个负载向量运行交流最优功率流（ACOPF），以识别任何拥堵的分支。在本研究中，任何负载向量在 中的负载超过其额定值的 90% 或更多的线路或变压器都被视为拥堵的分支。对 2016 年的每个小时设计攻击，该小时至少有一个分支的基准流量超过 90%。这些分支被单独选为目标进行攻击；因此，一个小时将会有与该小时中基准流量超过 90% 的分支数量相同的不同攻击。此外，对于每个目标分支，攻击的负载转移因子从 1% 到 15%，以 1% 的步长变化。这允许我们研究检测性能如何随着攻击大小的变化而变化。由于这一过程，我们计算出了 8861 次成功的攻击，覆盖了每个小时、目标线和负载转移。这些攻击后的负载向量按照第五部分 A 节中的 k-折程序进行了测试，其中每个组的阈值 从 0.9 到 1.1 倍的。图 4 显示了检测概率（彩色刻度）作为负载转移（x 轴）和误报率（y 轴）的函数。可以看出，检测器在负载转移非常低的攻击上的表现不佳，而对于 10% 到 15% 的负载转移，检测概率从 80% 到 100% 变化，误报率从 0% 到 3%。虽然负载转移因子在攻击设计阶段是一个重要的度量，但从运营商的角度来看，评估攻击的物理后果更有意义。图 5 显示了攻击导致的线路过载作为检测概率的函数。从这个图中我们可以清楚地看到，检测器具有极高概率检测任何可能造成重要物理损害的攻击：考虑到操作工具中建立的安全裕度，2% 或 3% 的过载不太可能引起任何系统中断。

## 5.3 Detection of random load redistribution attacks随机负载重分配攻击的检测

The experiments in the previous section have shown that the proposed detector is very effective in identifying attacked load vectors designed to create significant overflows on specific target lines. In this section we study the sensitivity of this algorithm to anomalous loads which have not necessarily been intelligently designed. To do so, many false load vectors will be created starting from the historical data; the detection performance is then computed as the number of modified loads and the amount of load change are varied across a broad spectrum. The false load vectors are created by randomly selecting a subset of the loads in each vector of and modifying them by either increasing or decreasing their value by a given load shift factor. For this study, the same load shifts as in the previous section are used, while the footprint size of the attack as a percentage of the total number of system loads is varied between 10% and 100% in steps of 10% for every hour. The resulting anomalous load dataset has dimensions 1125×, where = 8784×15×10 = 1,317, 600. Similarly to what done in the previous section, all these false load vectors are fed to the proposed detector and the detection probability computed. In this case, the detection probability is a function of three parameters: the false alarm rate, the load shift, and the footprint size. Figure 6 shows the detection probability (colored scale) as a function of the footprint size (x-axis) and the load shift (y-axis), when a high false alarm rate of 5.5% is allowed (top) and for a very low false alarm rate of 0.4% (bottom). Clearly, for a given load shift and footprint size, the detection probability is higher when the false alarm rate is higher. Overall, the detector performs well, having perfect detection capability for a wide range of different attacks. Compared to the detection performance on intelligently designed attacks, the detector is not as good at identifying the random attacks with small load shift and small percentages of attacked loads. This can be explained by the fact that the intelligent attacks are designed in such a way that the modified loads belong to a spatially concentrated subgraph, thus it is likely that some of the load groups will include a large number of attacked loads. In the random attacks, the loads are modified across the whole network and, hence, distributed across a higher number of groups; because of this, each group will experience a smaller deviation from the normative data, resulting in worse detection capability. On the other hand, because of this fact, the random attacks are less likely to cause line overloads. Figure 7 shows the detection probability versus line overload and false alarm rate. From these results it can be seen that any random attack that would result in line overloads is easily detected, demonstrating the high effectiveness of the proposed algorithm in detecting anomalous and dangerous load vectors.

前一部分的实验表明，所提出的检测器在识别旨在在特定目标线路上造成显著过载的攻击负载向量方面非常有效。在本节中，我们研究了该算法对可能没有经过智能设计的异常负载的敏感性。为此，我们将从历史数据中随机选择大量的虚假负载向量；然后，在负载修改的数量和负载变化量在整个广泛的范围内变化时，计算检测性能。虚假负载向量是通过随机选择 中的每个向量中的负载子集并修改它们的值来创建的，增加或减少给定的负载转移因子。在本研究中，与前一部分相同的使用负载转移因子，而攻击的足迹大小作为系统负载总数的百分比在每小时之间变化，范围从 10% 到 100%，步长为 10%。因此，产生的异常负载数据集 具有 1125× 的维度，其中 = 8784×15×10 = 1,317,600。与前一部分类似，所有这些虚假负载向量都输入到所提出的检测器中，并计算检测概率。在这种情况下，检测概率是三个参数的函数：误报率、负载转移和足迹大小。图 6 显示了检测概率（彩色刻度）作为足迹大小（x 轴）和负载转移（y 轴）的函数，当允许高误报率 5.5% 时（顶部）和非常低的误报率 0.4% 时（底部）。显然，对于给定的负载转移和足迹大小，当误报率较高时，检测概率也较高。总体而言，检测器表现良好，对于各种不同的攻击具有完美的检测能力。与智能设计的攻击的检测性能相比，检测器在识别具有小负载转移和小受攻击负载百分比的随机攻击方面并不那么好。这可以解释为智能攻击被设计成使得修改后的负载属于空间上集中的子图，因此很可能有一些负载组包含大量受攻击的负载。在随机攻击中，负载在整个网络上被修改，因此分布在更多的组中；因此，每个组都会从规范数据中经历较小的偏差，导致检测能力下降。另一方面，由于这一点，随机攻击不太可能导致线路过载。图 7 显示了检测概率与线路过载和误报率的关系。从这些结果可以看出，任何可能导致线路过载的随机攻击都很容易被检测到，这证明了所提出的算法在检测异常和危险的负载向量方面的极高有效性。

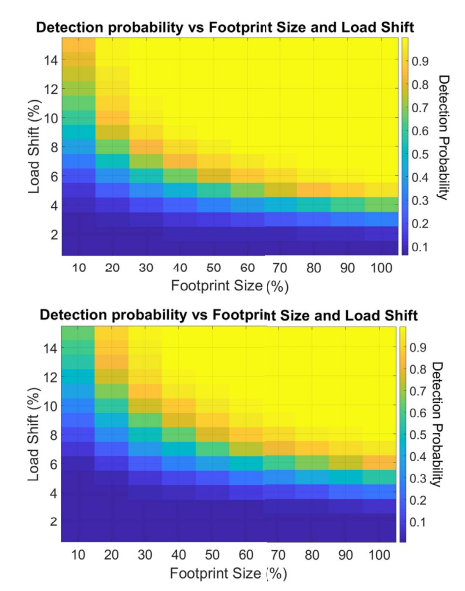


图6 . Random attacks: detection probability as a function of load shift and footprint size for false alarm rate of 5.5% (top) and 0.4% (bottom). 随机攻击：检测概率作为负载转移的函数和误报率为 5.5% 的（顶部）和 0.4% 的（底部）足迹大小。

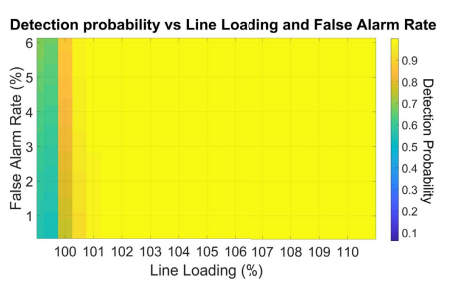


图7 Random attacks: detection probability as a function of line overload and false alarm rate. 随机攻击：检测概率作为线路过载的函数和误报率。

## 5.4 Integration within EMS集成EMS

The proposed detector has been fully implemented in a state-of-the-art EMS platform developed at Arizona State University [18]. This software was created as part of NSF Grant 1449080, by an ASU team lead by Dr. Lalitha Sankar, Dr. Kory Hedman, and Dr. Oliver Kosut and in collaboration with Dr. Robin Podmore from IncSys, Inc., leader in power system simulation tools and operator training [19], [20]. Figure 8 shows the interface of the platform: on the left is the network graph of the Texas system, while, on the right, the simulation page with the main blocks of the EMS is displayed. In the example shown, the traditional residue based BDD has easily been bypassed, while the proposed anomalous load detector identifies the attack and gives information on the extent of the attack based on the number of groups that raised a flag. Overall, this platform allows for the testing of the detector in a realistic power system operations environment while show casing its effectiveness in terms of computational efficiency and integration within energy managements systems. Details on the design of the software platform and its building blocks can be found in [21], while the code for the attack detection algorithm is freely available on Github [22].

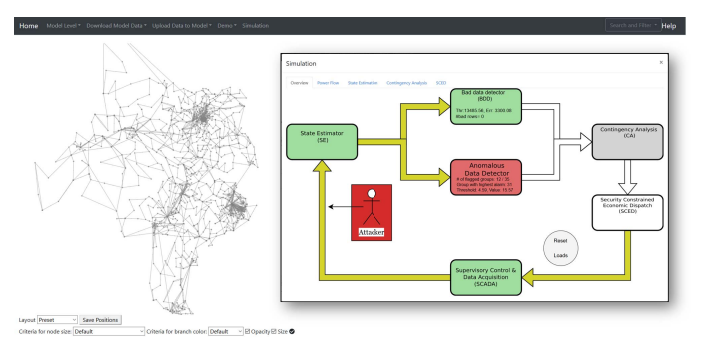


图8 Implementation of the improved bad data detector within an EMS在能量管理系统中实施改进的不良数据检测器

该检测器已完全集成到一个由亚利桑那州立大学开发的前沿能量管理系统平台中 [18]。该软件是在国家科学基金会拨款 1449080 的支持下创建的，由亚利桑那州立大学的 Lalitha Sankar 博士、Kory Hedman 博士和 Oliver Kosut 博士领导，并与 IncSys, Inc. 的 Robin Podmore 博士合作，IncSys, Inc. 是电力系统仿真工具和操作员培训的领导者 [19], [20]。图 8 显示了该平台的界面：左侧是德克萨斯系统的网络图，而右侧是显示 EMS 主要块的仿真页面。在所示的示例中，传统的基于残差的 BDD 轻易被绕过，而提出的异常负载检测器识别了攻击，并基于触发了警报的组数提供了攻击范围的信息。总体而言，这个平台允许在现实的电力系统操作环境中测试检测器，并展示了其在计算效率和集成到能量管理系统方面的有效性。关于软件平台及其构建块的设计细节可以在 [21] 中找到，而攻击检测算法的代码在 Github 上免费提供 [22]。

第6章 ATTACK LOCALIZATION测试改进的检测

In the previous sections, we have introduced a load anomaly detector based on nearest neighbor and a grouping strategy which was shown to have excellent performance against both intelligently designed attacks and random load changes. This algorithm can be extended beyond simply determining whether a load vector contains anomalous data or not; it can be leveraged to determine which buses have been modified or are deviating from their usual behavior. Localizing the subgraph affected by an attack or load anomaly represents a step forward in terms of system operations security. Knowing which loads are likely to have caused the detector to raise an alarm is an important step in the implementation of secure EMS functionalities. For example, the load values which are determined to be unreliable could be replaced by forecasted values or an uncertainty margin assigned to them so that the system could be operated in a secure state. A similar approach for secure operations against cyberattacks is studied in [23], where the authors present an optimal dispatch problem to find a secure and cost-effective dispatch solution considering variable bus loads and, thus, protecting the system from unexpected load changes. Also, in [24], a secure unit commitment (UC) problem is formulated such that in case of a cyber-attack the system operator can switch from the normal UC solution to a secure one while following all network constraints. The issue with these approaches is that it would cause the system to be operated in a too conservative and, thus, less efficient state for most of the time. The advantage of being able to detect and localize an attack is that the system operator can make a better-informed decision on when and how to secure the system, without impacting normal operations.

在前面几节中，我们介绍了一种基于最近邻和分组策略的负载异常检测器，该检测器在智能设计的攻击和随机负载变化方面都表现出卓越的性能。该算法不仅可以简单地确定负载向量是否包含异常数据；它还可以用于确定哪些母线已被修改或偏离其通常的行为。定位攻击或负载异常影响的子图在系统操作安全性方面是一个进步。知道哪些负载可能导致检测器发出警报对于实施安全的EMS功能至关重要。例如，被确定为不可靠的负载值可以被替换为预测值，或者给它们分配一个不确定性区间，以便系统可以在安全状态下运行。类似地，在[23]中，作者研究了一种针对网络攻击的安全操作方法，其中提出了一种最优调度问题，以找到一个考虑可变母线负载的安全和成本效益的调度解决方案，从而保护系统免受意外负载变化的影响。在[24]中，制定了一个安全的有功单元承诺（UC）问题，这样在网络攻击的情况下，系统运营商可以从正常的UC解决方案切换到安全的解决方案，同时遵守所有网络约束。这些方法的问题是，它将导致系统在大多数时间以过于保守的方式运行，从而效率较低。能够检测和定位攻击的优势在于，系统运营商可以根据何时以及如何安全地运行系统做出更好的决策，而不会影响正常运行。

## 6.1 Likelihood determination似然度确定

The grouping strategy provides an approximate way of localizing the attacks by identifying groups of loads that deviate from their normative behavior. In this section, we describe a statistical approach to further analyze the values of the individual loads to identify which ones are more likely to have triggered the detector. Because of the many attack subgraphs that are possible, determining exactly which are the attacked loads would be extremely hard. For this reason, our goal is to assign to each load a probability that represents the likelihood of that load being attacked. In this sense, the likelihood is a risk measure, and it can be quantified using an empirical metric that relies on estimated likelihoods, namely average log-loss (also known as cross-entropy) [25]. Average log-loss is defined as

(6)

where represents the total number of samples (e.g. loads tested), is the probability associated with each load, and is 1 if the load was indeed attacked and 0 if it was not modified. We define the values of the loads in group at time as , where is the number of loads in group j. The minimum distance between the load vector and the historical data is computed using (4); as explained in Section IV-B, if is greater than threshold , group j is said to raise a violation at time i. Moreover, define the loads in the nearest neighbor of as , where hr is the rth historical load vector in. For each load in group j, the normalized difference between load l at time i and its corresponding value in the nearest neighbor is computed as

(7)

We cannot directly look at this normalized difference to know if a load is attacked because different loads could have different amounts of deviation. In order to account for this variability, we determine the normative behavior of each load by computing the first and second order statistics of its normalized difference:

(8)

(9)

Given a specific load vector and its corresponding for all l and j, we determine how far each load deviates from the normative behavior using a Z-score which is defined as follows:

(10)

Intuitively, the Z-score indicates the number of standard deviations by which is above (or below) the mean for load l in group j observed in the attack-free data. Based on this setup, there exists a joint distribution between whether a load was attacked (a = 1) or not (a = 0), if it belongs to a group that raised a violation (v = 1) or not (v = 0), and its Z-score z. While is not known, we can empirically estimate the conditional probability of a load being attacked given its Z-score and whether it raised a violation or not. In other words, our goal is to define a likelihood function that takes as inputs a load’s Z-score and whether it raised a violation to determine the probability that the load is attacked. First, we compute the Z-score (10) for all intelligently designed attacks in PA that result in an overload of 3% or more. As discussed in Section V-B, those are the attacks that can cause significant damage and they are almost always detected by the nearest neighbor algorithm. The histogram of the Z-score for the loads that belonged to groups that raised a violation is shown in Fig. 9. In particular, the solid black line represents the histogram of Z-scores for loads that were attacked and we indicate as , while the black dotted line represents the histogram for loads that were not attacked . From these two curves, we notice that overall if a load belongs to a group that raised a violation it is very likely that the load is indeed being attacked. Moreover, the higher the Z-score, the more likely it is that a load is attacked. Based on these observations we can now define a function that maps the Z-score of a load to the likelihood of the load being attacked. The estimated conditional likelihood for loads that are in groups that raise a violation is computed as

(11)

and it is shown by the solid red line in Fig. 9. For the set of data points, we obtain using (11), we fitted a smooth curve of the form to avoid overfitting as shown by the dotted red line. This curve is defined as the conditional likelihood which can be used to assign to each load a probability of being attacked based on its Z-score. The same procedure is performed on the loads in groups that do not raise a violation and the corresponding likelihood is estimated; the results are shown in Fig. 10. Comparing the two conditional likelihood functions we notice that, for low Z-score values, reaches a minimum likelihood value of around 0.5 while reaches zero.

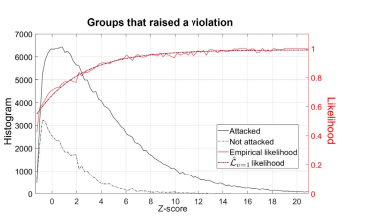


图9 Distribution of Z-scores (in black) and likelihood function (in red) for loads in groups that raise a violation. 违反组的负载的Z分数分布（黑色）和似然函数（红色）分布。

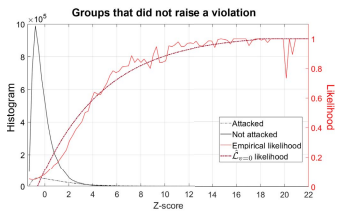


图10 . Distribution of Z-scores (in black) and likelihood function (in red) for loads in groups that do not raise a violation. 未违反组的负载的Z分数分布（黑色）和似然函数（红色）分布。

分组策略提供了一种近似的方法来定位攻击，通过识别与规范行为偏离的负载组。在本节中，我们描述了一种统计方法，进一步分析单个负载值，以确定哪些负载更有可能触发了检测器。由于可能的攻击子图数量众多，确定确切哪些负载被攻击将极为困难。因此，我们的目标是为每个负载分配一个概率，代表该负载被攻击的可能性。在这种情况下，似然度是一种风险度量，可以使用依赖于估计似然度的经验指标来量化，即平均对数损失（也称为交叉熵）[25]。平均对数损失定义为

(6)

其中 代表样本总数（例如，被测试的负载），q\_l 是与每个负载相关的概率，而 是负载确实被攻击时的值（ = 1），否则（= 0）。我们定义负载组 j 在时间 i 的负载值为 ，其中 是组 j 中的负载数。使用公式（4）计算负载向量 与历史数据之间的最小距离 ；正如在第四部分 B 节中所解释的，如果 大于阈值 ，则称组 j 在时间 i 触发了违规。此外，定义负载 的最近邻为 ，其中 是 中的第 r 个历史负载向量。对于组 j 中的每个负载，计算负载 l 在时间 i 与其在最近邻 中的对应值之间的归一化差异，定义为

(7)

我们无法直接通过这个归一化差异来判断负载是否被攻击，因为不同的负载可能有不同的偏差量。为了考虑到这种变异性，我们通过计算归一化差异的一阶和二阶统计量来确定每个负载的规范行为：

(8)

(9)

对于特定的负载向量 及其对应的所有 l 和 j 的 ，我们使用 Z-score 来确定每个负载偏离规范行为的程度，Z-score 定义如下：

(10)

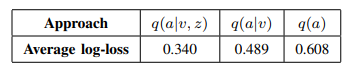
直观上，Z-score 表示 相对于攻击前数据中负载 l 在组 j 中的平均值超出了（或低于）标准差的数量。基于这种设置，存在一个联合分布 表示负载是否被攻击（a = 1）或未受攻击（a = 0），它是否属于触发了违规的组（v = 1）或未触发违规的组（v = 0），以及它的 Z-score z。虽然 未知，但我们可以通过经验估计条件概率 来估计给定负载的 Z-score 和是否触发了违规的情况下，该负载被攻击的可能性。换句话说，我们的目标是定义一个似然函数 ，它接受负载的 Z-score 和是否触发了违规作为输入，以确定负载被攻击的概率。首先，我们为所有导致超过 3% 过载的智能设计攻击计算 Z-score（10）。正如在第五部分 B 节中所讨论的，那些攻击是可能造成重大损害的攻击，几乎总是被最近邻算法检测到。负载的 Z-score 分布图中，黑色实线表示被攻击的负载的 Z-score 分布，我们将其标记为，而黑色虚线表示未被攻击的负载的 Z-score 分布 。从这两条曲线中，我们注意到，如果一个负载属于触发了违规的组，那么这个负载被攻击的可能性非常大。此外，Z-score 越高，负载被攻击的可能性也越大。基于这些观察，我们现在可以定义一个函数，将负载的 Z-score 映射到该负载被攻击的可能性。对于触发了违规的负载集，估计的条件似然为

(11)

在图 9 中，这个估计的条件似然由实线表示。对于数据点集，我们使用公式（11）得到了一个平滑的曲线 ，以避免过拟合，如图 9 中虚线所示。这个曲线定义为条件似然，可以根据负载的 Z-score 为其分配被攻击的概率。对没有触发违规的负载组也进行了相同的处理，并估计了相应的条件似然 ；结果如图 10 所示。比较这两个条件似然函数，我们注意到，对于低 Z-score 值， 达到约 0.5 的最小似然值，而 达到零。

## 6.2 Numerical results随机负载重分配攻击的检测

The performance of this approach is tested on the intelligently designed attacks from Section V-B, with =The performance of this approach is tested on the in telligently designed attacks from Section V-B, with =TABLE I PERFORMANCE COMPARISON OF THE THREE LIKELIHOOD APPROACHES.



这种方法在第五部分 B 节的智能设计攻击上进行了测试，其中 = TABLE I 三种似然度方法的性能比较。

结论

In this paper we presented an improved data-driven algorithm for the detection of load redistribution attacks and a statistical approach for the localization of the attacked buses. The detector, based on nearest neighbor and a grouping strategy, was tested on a large number of attacks belonging to two different classes: intelligent attacks and random load changing attacks. The results obtained on the synthetic Texas system show excellent detection capability, especially against the attacks that have the worst consequences on the system. The attack localization scheme assigns a likelihood value to each load indicating the probability of that load being attacked; this approach offers operators a greater insight in case of cyber-attacks allowing for more secure system operation. As part of our future work, we intend to extend the detection algorithm to the analysis of different anomalies; the model can be trained to not only detect an anomaly, but also determine the type of event that caused it (cyber-attack, natural event, fault, etc.). Moreover, the algorithm can be enhanced by taking into consideration additional information about rare and sporadic events, such as forecasts of extreme weather events or temporary changes in load patterns due to known causes (e.g. sporting events, holidays, etc.). This could result in both improved detection probability and lower false alarm rate.

在本文中，我们提出了一种改进的数据驱动算法，用于检测负载重分配攻击，并提出了一种统计方法用于定位被攻击的母线。基于最近邻和分组策略的检测器在大量属于两类不同攻击的攻击上进行了测试：智能攻击和随机负载变化攻击。在合成德克萨斯系统上获得的结果显示，特别是针对对系统产生最严重后果的攻击，检测能力非常出色。攻击定位方案为每个负载分配一个似然值，指示该负载被攻击的概率；这种方法在发生网络攻击时为运营商提供了更大的洞察力，从而允许更安全的系统运行。

作为我们未来工作的一部分，我们打算将检测算法扩展到分析不同的异常；该模型不仅可以被训练来检测异常，还可以确定引起异常的事件类型（网络攻击、自然事件、故障等）。此外，通过考虑关于罕见和偶发事件的额外信息，可以增强算法，例如极端天气事件的预测或由于已知原因（例如体育赛事、假日等）导致的负载模式的临时变化。这可能导致检测概率的提高和误报率的降低。

参考文献

1. Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” Ccs, vol. 14, no. 1, pp. 1–33, 2009.
2. Y. Yuan, Z. Li, and K. Ren, “Modeling load redistribution attacks in power systems,” IEEE Transactions on Smart Grid, 2011
3. J. Zhang and L. Sankar, “Physical system consequences of unobservable state-and-topology cyber-physical attacks,” IEEE Transactions on Smart Grid, vol. 7, no. 4, pp. 2016–2025, 2016.
4. A. Sanjab and W. Saad, “Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective,” IEEE Transactions on Smart Grid, vol. 7, no. 4, pp. 2038–2049, jul 2016.
5. L. Xie, Y. Mo, and B. Sinopoli, “Integrity data attacks in power market operations,” IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 659– 666, dec 2011.
6. A. Pinceti, L. Sankar, and O. Kosut, “Load redistribution attack detection using machine learning: A data-driven approach,” in IEEE Power and Energy Society General Meeting, 2018.
7. V. Joshi, J. Solanki, and S. K. Solanki, “Statistical methods for detection and mitigation of the effect of different types of cyber-attacks and parameter inconsistencies in a real world distribution system,” in 2017 North American Power Symposium, NAPS 2017, 2017.
8. J. J. Yu, Y. Hou, and V. O. Li, “Online false data injection attack detection with wavelet transform and deep neural networks,” IEEE Transactions on Industrial Informatics, 2018.
9. Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, “Real time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis,” IEEE Systems Journal, 2016.
10. Z. Chu, J. Zhang, O. Kosut, and L. Sankar, “Evaluating power system vulnerability to false data injection attacks via scalable optimization,” Smart Grid Communications (Smart Grid Comm), 2016 IEEE International Conference, Nov. 2016.
11. T. Cover and P. Hart, “Nearest neighbor pattern classification,” IEEE Transactions on Information Theory, vol. 13, no. 1, January 1967.
12. V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection : A survey,” ACM Computing Surveys, vol. 41(3), no. 15, July 2009.
13. PJM, “PJM metered load data.” [Online]. Available: https://dataminer2. pjm.com/feed/hrlloadmetered/definition.
14. A. B. Birchfield, T. Xu, K. M. Gegner, K. S. Shetye, and T. J. Overbye, “Grid structural characteristics as validation criteria for synthetic networks,” IEEE Transactions on Power Systems, vol. 32, no. 4, pp. 3258–3265, Jul 2017.
15. H. Li, A. L. Bornsheuer, T. Xu, A. B. Birchfield, and T. J. Overbye, “Load modeling in synthetic electric grids,” in 2018 IEEE Texas Power and Energy Conference, TPEC 2018, 2018.
16. R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, “Mat- ´ power: Steady-state operations, planning, and analysis tools for power systems research and education,” IEEE Transactions on Power Systems, vol. 26, no. 1, pp. 12–19, Feb 2011.
17. A. Pinceti, L. Sankar, and O. Kosut, “Data-driven generation of synthetic load datasets preserving spatial-temporal features,” in IEEE Power and Energy Society General Meeting, 2019.
18. L. Sankar, O. Kosut, and K. Hedman, “A verifiable framework for cyber-physical attacks and countermeasures in a resilient electric power grid.” [Online]. Available: https://sankar.engineering.asu.edu/ nfs-dhs-cps-framework/
19. R. Podmore, “Digital computer analysis of power system networks,” PhD Thesis, University of Canterbury, Christchurch, New Zealand, 1972.
20. IncSys, Inc., “IncSys - power system simulation software.” [Online]. Available: [www.incsys.com](http://www.incsys.com)
21. R. Khodadadeh, “Designing a software platform for evaluating cyberattacks on the electric power grid,” Master’s Thesis, 2019. [Online]. Available: http://search.proquest.com/docview/2228212793/
22. A. Pinceti, “Nearest neighbor attack detection,” https://github.com/apince/EMS FDI Nearest Neighbor Attack Detection, 2019.
23. A. Abusorrah, A. Alabdulwahab, Z. Li, and M. Shahidehpour, “Minimax-regret robust defensive strategy against false data injection attacks,” 2017.
24. H. Shayan and T. Amraee, “Network constrained unit commitment under cyber attacks driven overloads,” IEEE Transactions on Smart Grid, p. 1, 2019.
25. T. M. Cover and J. A. Thomas, Elements of information theory. Wiley Intercedence, 1991, ch. 13.