分类号：TM73　　学校代码：10363
密　级：公开　　学　　号：2210310106

安徽工程大学
Anhui Polytechnic University

硕士学位论文

题目　面向虚假数据注入攻击的智能电网状态估计研究

论 文 作 者　胡朋飞
指 导 教 师　高文根
学科（专业）　电气工程
研 究 方 向　电力系统及其自动化

论文提交日期：2024 年 5 月 31 日

安徽工程大学学位论文原创性声明

本人郑重声明：我恪守学术道德，崇尚严谨学风。所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已明确注明和引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的作品及成果的内容。论文为本人亲自撰写，我对所写的内容负责，并完全意识到本声明的法律后果由本人承担。

学位论文作者签名：胡明飞

日期：　　2024 年　5 月　28 日

安徽工程大学学位论文版权使用授权书

学位论文作者完全了解学校有关保留、使用学位论文的规定，同意学校保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅或借阅。本人授权安徽工程大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

保密 □，在 ____ 年解密后适用本版权书。

本学位论文属于

不保密 ☑。

学位论文作者签名：胡明飞　　指导教师签名：高振根

日期： 2024 年 5 月 28 日　　日期： 2024 年 5 月 28 日

面向虚假数据注入攻击的智能电网状态估计研究

摘 要

网络物理电力系统(Cyber-Physical Power Systems, CPPS)将物理电力系统与信息和通信网络融合，利用现代信息和通信技术连接网络和集成各种电力设备，以实现电力系统的实时监控、控制和优化。状态估计对电力系统的量测数据进行处理和分析，从而推断出电力系统各组件的实际运行状态，为电力系统监控、分析和优化决策提供准确的基础数据，是实现电力系统可靠运行的重要支撑。然而，在物理电力系统与信息技术系统紧密耦合的背景下，状态估计的过程容易受到虚假数据注入攻击(False Data Injection Attacks, FDIAs)等各种网络攻击的影响。攻击者通过篡改传感器数据、量测数据或控制信号向系统注入虚假数据，导致状态估计器错误的估计系统状态，从而采取错误的控制策略或决策，影响电力系统的安全和稳定运行。目前，大多数研究主要聚焦于 FDIA 的检测，而针对 FDIA 的定位以及被其篡改的测量值和状态估计值的校正方面的研究则相对较少。因此，研究 FDIA 的检测和定位，以及状态估计的校正对电力系统的安全稳定运行具有重要意义。本文对 FDIA 影响下的电力系统状态估计方法进行了深入研究，主要研究内容概述如下：

（1）根据电力系统量测模型，详细研究了在直流潮流和交流潮流情况下的传统状态估计方法，以及目前基于加权最小二乘(Weighted Least Squares, WLS)估计的不良数据检测系统的漏洞问题。同时，研

究了在两种潮流下的虚假数据构造原理，并分析了虚假数据绕过传统不良数据检测方法的过程。

（2）鉴于 FDIAs 导致传统扩展卡尔曼滤波(Extended Kalman Filter, EKF)的状态估计性能下降，提出了一种改进的鲁棒状态估计方法，通过在估计过程中引入指数加权函数，自适应地调整卡尔曼滤波增益，以降低虚假数据在状态估计过程中的权重，从而提高 EKF 在 FDIA 场景中的状态估计性能。

（3）考虑 EKF 和 WLS 的状态估计特性差异，提出一种联合动态和静态状态估计的 FDIAs 检测方法，通过把两种估计方法在面对 FDIAs 时产生的估计偏差与相应误报率的检测阈值进行比较，实现对 FDIAs 的精准检测。在检测到 FDIAs 的基础上，进一步提出了基于电力网划分的 FDIAs 定位方法，通过电力网等冗余分区和子系统内部攻击检测，实现对 FDIAs 的定位。

（4）为了及时校正 FDIAs 篡改的量测值和状态估计值，提出了一种基于滑动窗口的数据补偿和状态校正策略，通过补偿后的测量结果重建系统的状态方程和量测方程，进一步对重建后的方程进行状态估计，实现快速校正系统状态。其中，改进了传统的 Holt 双参数指数平滑法，通过预测误差自适应地调整平滑参数，提高状态预测准确性，优化状态估计过程。

关键词：智能电网，网络安全，卡尔曼滤波，虚假数据注入，状态估计，攻击检测

Research on Smart Grid State Estimation for False Data Injection Attacks

ABSTRACT

Cyber-physical power systems (CPPS) integrates physical power systems with information and communication networks, using modern information and communication technologies to connect networks and integrate various power devices to achieve real-time monitoring, control and optimization of power systems. State estimation processes and analyzes the measurement data of the power system, so as to infer the actual operating state of each component of the power system, and provide accurate basic data for power system monitoring, analysis and optimization decision-making, which is an important support for the reliable operation of the power system. However, in the context of the close coupling of physical power system and information technology system, the process of state estimation is susceptible to various cyber-attacks such as false data injection attacks (FDIAs). Attackers inject false data into the system by tampering with sensor data, measurement data, or control signals, which causes the state estimator to incorrectly estimate the system state, and thus take wrong control strategies or decisions, affecting the safe and stable operation of the power system. Currently, most of the researches mainly focus on the detection of FDIA, while there are relatively few researches

on the localization of FDIA and the correction of the measurements and state estimation values tampered by it. Therefore, it is important to study the detection and localization of FDIA and the correction of state estimates for the safe and stable operation of power systems. In this paper, an in-depth study of power system state estimation methods under the influence of FDIA is carried out, and the main research content is summarized as follows:

(1) Based on the power system measurement model, a detailed study was conducted on traditional state estimation methods under both DC and AC flow conditions, as well as the vulnerabilities of current systems based on weighted least squares (WLS) estimation for bad data detection. Additionally, the principles of false data construction under both types of flows were researched, and the process by which false data circumvents traditional bad data detection methods was analyzed.

(2) In view of the performance degradation of the extended Kalman filter (EKF) for state estimation caused by FDIAs, an improved robust state estimation method is proposed. This method introduces an exponential weighting function into the estimation process to adaptively adjust the Kalman filter gain, reducing the weight of false data in the state estimation process, thereby enhancing the state estimation performance of EKF in FDIA scenarios.

(3) Considering the difference in state estimation characteristics

between EKF and WLS, a joint dynamic and static state estimation method for FDIAs detection is proposed. By comparing the estimation biases generated by the two estimation approaches when facing FDIAs with their respective detection thresholds for false alarm rates, precise detection of FDIAs is achieved. Building upon the detection of FDIAs, a further method for FDIA localization based on power grid partitioning is proposed. This method achieves FDIA localization through redundant partitioning of the power grid and internal attack detection within subsystems.

(4) To promptly correct the measurement values and state estimates manipulated by FDIAs, a sliding window-based data compensation and state correction strategy is proposed. This strategy involves reconstructing the system's state and measurement equations using the compensated measurement results and further performing state estimation on the reconstructed equations to achieve rapid correction of the system state. Notably, an improved version of the traditional Holt double exponential smoothing method is introduced, which adaptively adjusts smoothing parameters based on prediction errors to enhance prediction accuracy and optimize the state estimation process.

KEY WORDS: smart grid, network security, Kalman filtering, false data injection, state estimation, attack detection

目录

摘 要.....I
ABSTRACT.....III
第 1 章 绪论.....1
1.1 课题研究背景及意义.....1
1.2 国内外研究现状.....3
1.2.1 状态估计研究现状.....3
1.2.2 虚假数据注入攻击检测和状态恢复研究现状.....7
1.2.3 研究现状分析.....9
1.3 主要研究内容及创新点.....11
第 2 章 电力系统状态估计和虚假数据注入攻击原理.....13
2.1 引言.....13
2.2 电力系统状态估计.....13
2.2.1 交流状态估计.....13
2.2.2 直流状态估计.....16
2.3 不良数据检测原理.....17
2.4 虚假数据注入攻击原理.....19
2.4.1 直流模型中的 FDIAs.....19
2.4.2 交流模型中的 FDIAs.....20
2.5 本章小结.....21
第 3 章 基于动静态联合估计的 FDIAs 检测方法.....22
3.1 引言.....22
3.2 状态估计模型.....22
3.3 改进的扩展卡尔曼滤波.....24
3.3.1 扩展卡尔曼滤波原理.....24
3.3.2 基于指数加权函数的扩展卡尔曼滤波.....24
3.4 基于动静态联合估计和电力网划分的 FDIA 检测和定位.....26
3.4.1 基于动静态联合估计的 FDIA 检测.....26
3.4.2 基于电力网划分的 FDIA 定位.....29

3.5 仿真实验与结果分析.....31
3.5.1 仿真系统.....31
3.5.2 仿真数值分析.....35
3.6 本章小结.....44
第 4 章 基于 EKF 和数据补偿的智能电网异常值检测和状态校正策略.....45
4.1 引言.....45
4.2 基于自适应调节平滑参数的指数平滑法.....45
4.3 异常值检测和状态校正.....48
4.3.1 基于状态偏差指数的异常值检测.....48
4.3.2 量测补偿和状态校正.....50
4.4 仿真实验和结果分析.....53
4.4.1 仿真系统.....53
4.4.2 仿真数值分析.....54
4.5 本章小结.....67
第 5 章 总结与展望.....68
5.1 总结.....68
5.2 展望.....69
参考文献.....70
攻读硕士期间取得的学术成果.....76
致谢.....77

第 1 章 绪论

1.1 课题研究背景及意义

随着信息通信技术(Information and Communication Technologies, ICT)的快速进步，电力系统中已经广泛部署了众多具备通信能力的仪器和设备，以增强系统在应对不断上升的可再生能源渗透率方面的状态可观测性、控制响应性和运行灵活性。在所有电压等级的发电领域，以及众多最终用户场景中，电气化计划正在大规模实施。这一趋势促成了电力系统向网络化物理电力系统(Cyber-Physical Power Systems, CPPS)的转型，实现了物理基础设施、信息感知与挖掘，以及网络空间中系统运行和控制资产之间的无缝集成与互动[1]。此举有助于优化电流计算和分布式可再生能源的有效整合[2][3]，同时支持交通运输等其他行业的碳中和[4][5]。CPPS 的最终目标是智能地整合能源供应链中所有利益相关方的行为，以提供经济高效、安全可靠的电力供应，促进环境与经济的可持续发展[6][7]。

显然，CPPS 将深刻变革传统电力系统的运作模式。然而，通信与计算技术的融合为 CPPS 带来了新的网络安全挑战。首先，传统电力系统中的控制设备在设计时往往未充分考虑网络安全问题，因为它们在很长一段历史时期内都是在孤立的物理环境中运作。其次，当通信和计算设备与传统控制系统发生耦合时，现有的安全技术难以直接适用于几乎不设防的控制设备，从而产生固有的网络安全漏洞[8][9]。此外，鉴于 CPPS 的多点、多类型和多层特征，攻击者可以较容易地识别这些漏洞，从而实施恶意网络攻击。因此，随着电力系统的数字化和 CPPS 的发展，新的网络安全问题可能时有发生。

近几十年来出现了多起网络攻击事件，对不同国家的人民工作、生活、安全带来了不同程度的影响。例如，乌克兰电网攻击(2015 年)：这是历史上最为知名的电力系统网络攻击之一。在 2015 年 12 月，乌克兰的电力系统遭受到广泛的网络攻击，导致数十万人在寒冷的冬季断电。攻击者采取了恶意软件入侵电力公司的控制系统，使得能源分布受到干扰，导致大范围停电。这次事件被认为是首次导致大规模电力中断的网络攻击事件[10]。在 2016 年，乔治亚的电力系统遭受了一次网络攻击，导致部分地区的电力中断。攻击者使用了恶意软件来干扰电力系

统的运行。虽然这次攻击规模较小，但引起了对电力系统网络安全的更多关注。在 2016 年，乌克兰的电力系统再次成为网络攻击的目标。虽然这次攻击未造成大规模停电，但它仍然凸显了电力系统的脆弱性。2019 年，委内瑞拉电网连续遭遇两次大面积停电。据国内外媒体报道，委内瑞拉电网接连遭受五轮攻击，水电站、变电站、变压器和输电线路都成为攻击目标。由于停电，委内瑞拉部分地区的供水、通信和公共交通受到严重影响。因此，民众无法进行正常的生活和生产。2021 年，美国的一家电力公司遭受了网络攻击，导致部分系统被禁用。虽然这次攻击未导致大范围停电，但它引发了对美国电力系统安全性的担忧。这些事件强调了电力系统网络安全的紧迫性，并促使电力公司和政府采取更多措施来保护电力系统免受网络攻击的威胁。这些事件也强调了网络攻击对社会和经济稳定的潜在影响，因此加强电力系统的网络安全至关重要[11][12]。

电力系统状态估计是电力系统运行和监控的重要组成部分，它涉及到对电力系统各个组件和参数的准确估计，以确保电力系统的稳定、安全和可靠运行[13]。电力系统是一个庞大而复杂的网络，包括发电厂、输电线路、变电站、配电系统等多个组成部分。这些组件之间的相互作用和电能流动使得电力系统的状态监测和管理变得非常复杂。电力系统是现代社会的基础设施之一，它为工业、商业和家庭提供了必要的电能供应。因此，电力系统的可靠性和稳定性对社会经济的发展至关重要。数据采集与监视控制(Supervisory Control and Data Acquisition, SCADA)系统通常用于监测和控制电力系统以及其他工业过程。SCADA 系统通过传感器和测量设备来实时采集电力系统中的数据，包括电压、电流、频率、相位角等关键参数。这些数据通常以模拟信号或数字信号的形式传输到 SCADA 系统中。采集到的数据被传输到 SCADA 系统的数据中心或服务器，同时存储在数据库中，以供后续分析和处理使用[14]。状态估计是指利用各种测量数据和模型，来估计电力系统中各个组件(例如发电机、变压器、线路等)的状态变量，如电压、电流、相角等[15]。这些状态变量的准确估计对于系统操作、控制和故障检测至关重要。电力系统状态估计的输入数据通常来自各种传感器和测量装置，如电流传感器、电压传感器、相角测量装置等。这些数据以实时或间歇性的方式采集，用于监测系统的运行情况。状态估计通常依赖于电力系统的数学模型，这些模型描述了电力系统各个组件之间的物理关系和电力流动规律。这些模型用于将测量数

据与系统状态变量关联起来。状态估计的结果被广泛用于电力系统的操作和控制，包括电压控制、电流控制、故障检测、负荷预测等[16][17]。它还用于实时监测电力系统的稳定性，以便在出现问题时采取必要的措施。电力系统状态估计面临着测量误差、模型不确定性、数据通信延迟、网络攻击等多种挑战[18]。因此，研究和开发高效、准确的状态估计算法和工具是电力系统运营和管理的重要任务之一。综上所述，电力系统状态估计在维护电力系统的稳定性和可靠性方面发挥着关键作用。通过准确估计电力系统的状态变量，运营人员可以及时采取措施来应对各种运行问题，确保电力系统能够满足不断增长的电能需求，同时保障供电的可靠性和安全性。因此，电力系统状态估计是电力行业不可或缺的技术和工具之一。

虚假数据注入攻击(False Data Injection Attacks, FDIAs)是一种针对电力系统状态估计的安全威胁，涉及向电力系统中注入虚假或恶意数据以干扰状态估计过程，从而导致系统操作错误或产生安全风险[19]。攻击者试图通过篡改电力系统的测量数据，向状态估计过程中注入虚假信息，从而导致状态估计结果错误或误导操作员。例如，降低电压估计、误导负荷预测或隐藏潜在故障。这可以对电力系统的操作、控制和安全性构成威胁[20]。这种攻击可能对电力系统的稳定性和可靠性造成严重影响，甚至可能导致电力系统的崩溃。

为了保护电力系统免受虚假数据注入攻击，需要采取安全措施。检测和定位这些攻击，以及补偿和校正被篡改的量测值和状态估计值有助于确保电力系统的稳定性和可靠性，电力系统操作员可以更快地采取应急措施，如隔离受感染的部分、修复受损的设备等，以减小攻击的影响，避免潜在的系统崩溃和故障[21][22]。同时还有助于提供准确的系统状态信息，帮助操作员做出正确的决策，维护系统的正常运行。因此，投入资源来开发并实施有效的虚假数据注入攻击检测与定位技术，以及对量测值和状态估计值进行补偿与校正的技术是至关重要的。

1.2 国内外研究现状

1.2.1 状态估计研究现状

电力系统状态估计(Power System State Estimation, PSSE)是电力系统运行和控制的关键技术之一。它主要涉及利用可用的测量数据(如电压、电流、功率等)

来估计电网的整体状态，以便于实时监控和优化电网运行[23][24]。同时，电力系统状态估计，作为能源管理系统(Energy Management System, EMS)的核心组成部分，亦称为实时潮流分析，指在已知的网络拓扑结构、支路参数及测量系统配置的前提下，对电网状态进行的估计以及对不良数据的检测与识别过程。电力系统状态估计和不良数据辨识过程如图 1-1 所示。此过程充分利用量测系统的冗余特性，以增强电力系统的操作性和可靠性。这些状态估计结果常被用于电力调度、系统保护、故障分析和能源管理系统。截至到目前，电力系统状态估计的研究和发展趋势主要包括以下几个方面：算法创新和优化、数据处理和数据质量、分布式和去中心化状态估计、动态状态估计、集成先进的测量技术、应对大规模电力系统的挑战和面向未来电网的状态估计等。

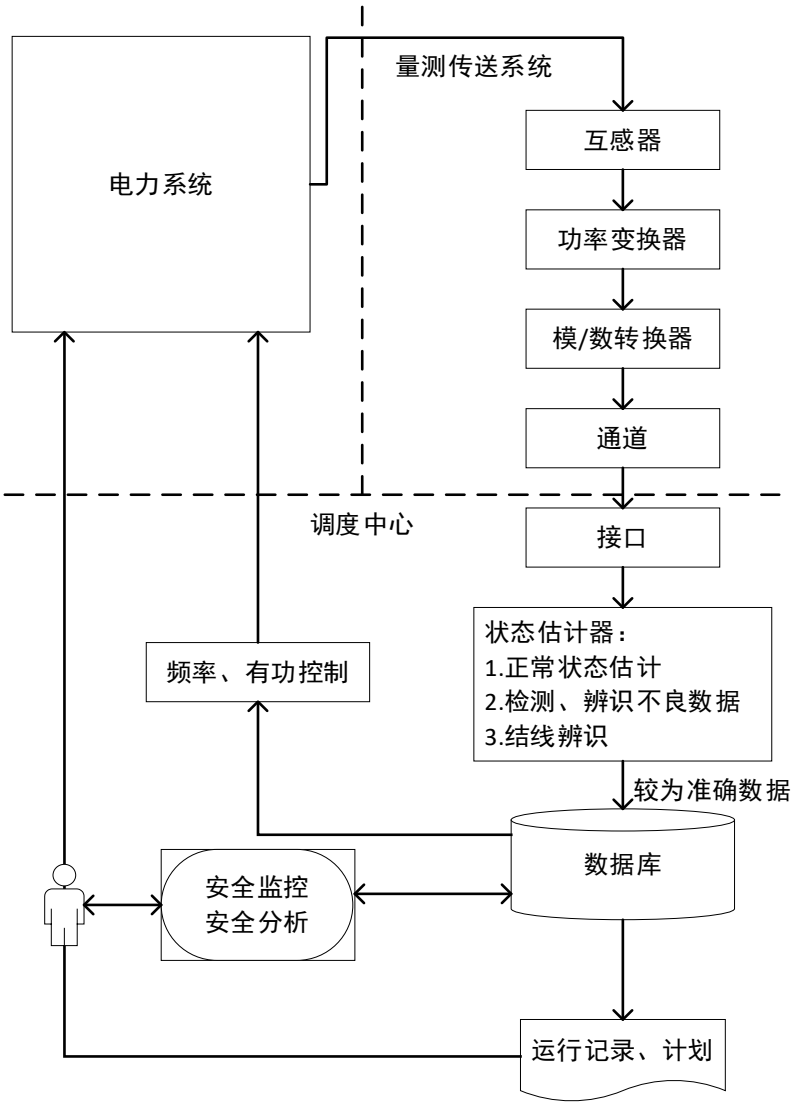


图 1-1 电力系统中数据量测、传送和处理工作示意图

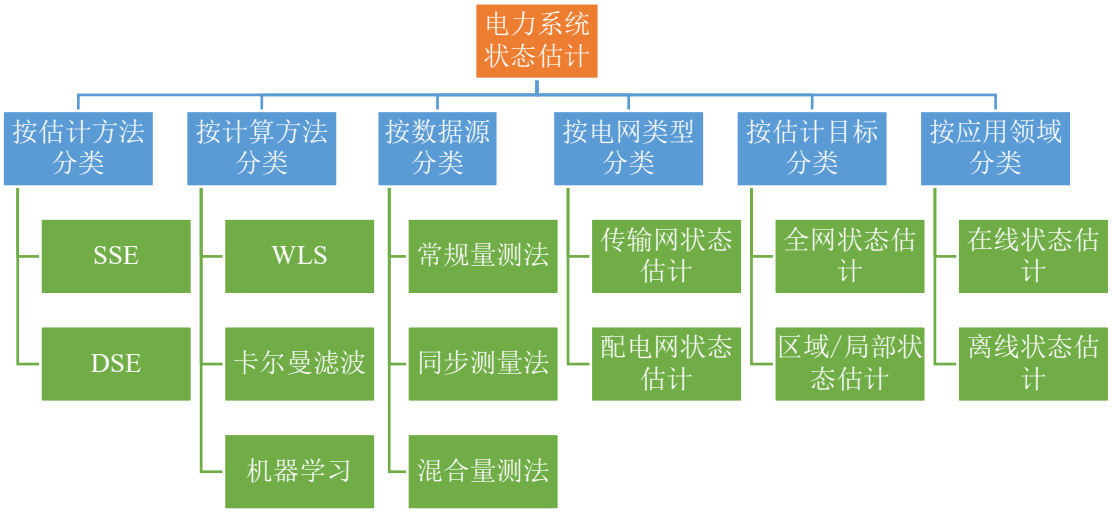


图 1-2 电力系统状态估计分类

电力系统状态估计可以根据不同的标准和特性进行分类。主要的分类方式如图 1-2 所示。按照估计方法分类，状态估计分为静态状态估计(Static State Estimation, SSE)和动态状态估计(Dynamic State Estimation, DSE)。SSE 是电力系统状态估计的一种基本形式，主要用于估计电力系统在某一特定时刻的稳态工作条件。它的核心目标是提供一个快照，展示电网在静态条件下的电压幅值和相角分布。SSE 主要处理的是静态数据，如电压、电流、有功和无功功率等，在某一特定时刻的测量值。虽然处理的是静态数据，但这些数据通常实时或近实时收集，用于监控电网的当前状态[25][26]。最常用的 SSE 是加权最小二乘法(Weighted Least Squares, WLS)，该方法通过最小化预测值和实际测量值之间的误差平方和来估计电网状态[27]。在电力系统控制中心的众多监控和控制应用中，大量应用依赖于系统的稳态模型。然而，由于电力系统需求和发电量的随机波动，系统实际上从未处于完全的稳态条件下。特别是，发电端的分布式能源资源(Distributed Energy Resources, DER)的广泛融合，以及需求侧复杂负荷的增加和新兴需求响应技术的应用(如电动汽车和物联网设备)，进一步强化了系统的非稳态特性。这些变化导致电力系统动态特性的不确定性显著增加。因此，传统的稳态假设变得不再适用，传统的静态状态估计方法无法更好地捕捉运行环境中的这些动态变化。鉴于电力系统的动态特性和不断增长的复杂性，目前在 EMS 中广泛采用的 SSE 方法需进行重新评估，并通过引入新型监测工具，例如 DSE 来进行增强。DSE 能够有效地捕捉电力系统状态的时变特性，这对于电力系统控制和保护至关重要，尤其是

在新技术的不断部署加剧了系统不确定性的当下环境中。DSE 的应用将为适应电力系统运行中日益增加的复杂性提供关键的技术支持[28]。

DSE 通常使用基于卡尔曼滤波器(Kalman Filter, KF)的算法，特别是扩展卡尔曼滤波器(Extended Kalman Filter，EKF)或其变种，这些方法在电力系统中被广泛应用[29]。EKF 算法作为最常见的基于 KF 的非线性算法之一，其基础是泰勒级数展开。文献[30]讨论了在使用同步相量测量单元(Phasor Measurement Units, PMUs)获得的数据时，将 EKF 应用于电力系统的可行性。此外，在 3 台发电机和 9 台母线电力系统模型的背景下，对 EKF 的估计性能进行了详细探讨。值得注意的是，估计性能在采样频率、测量误差、故障和负载波动方面保持稳健，不受其影响。UKF 采用一种称为“无迹变换”的技术，以选择一组称为“sigma 点”的状态样本。这些 sigma 点是从状态分布中采样的，以捕获非线性性质。通常，选择的 sigma 点是均匀分布在状态的均值周围的点。总的来说，UKF 通过无迹变换和非线性状态转移函数来处理非线性系统的状态估计问题，避免了 EKF 中的线性化误差，从而提高了估计的准确性和鲁棒性[31]。文献[32]针对配电网和分布式发电在不同运行场景下的特征，提出了一种基于 EKF 和 UKF 的交互多模型动态状态估计方法。在自适应估计阶段，对两种经典状态估计器进行了改进，以适应不同的操作模式，并将它们嵌入到交互式多模型算法框架中。交互式多模型算法根据运行模式的识别结果赋予相应的估计器更高的权重，从而最终产生联合状态估计结果。鉴于非高斯噪声的存在会降低滤波的精度和鲁棒性，因此可用的观测结果不够准确。为应对这一挑战，一些非线性卡尔曼滤波器采用鲁棒的最优性标准或近似后验密度来校正状态估计。文献[33]提出了一种新颖的方法，即修改测量的平方根无迹卡尔曼滤波器(Square Root Unscented Kalman Filter with Modified Measurement, SRUKF-MM)，该方法能够直接对测量进行加权，以校正误差协方差和噪声方差。这一创新方法基于平方根无迹卡尔曼滤波器，旨在提高滤波过程的数值稳定性。鉴于非高斯噪声和网络攻击可能会对标准卡尔曼滤波器的性能产生显著不利影响，文献[34]提出了一种新型弹性容积卡尔曼滤波器(Cubature Kalman Filter, CKF)，其基于柯西核最大相关熵(Cauchy Kernel Maximum Correntropy, CKMC)的最优准则方法。该方法通过采用统计线性化技术将状态误差和测量误差的成本函数统一起来，并使用定点迭代方法来获得最优状态估计。

这一创新性方法的引入旨在提高滤波器对非高斯噪声和网络攻击等外部干扰因素的鲁棒性。

由于 SCADA 测量的低采样率和测量与状态变量之间的非线性特性，因此限制了 SE 的实时状态跟踪性能[35]。PMU 数据通常包含高精度的时间戳和电气量测量(如电压、电流、频率)，这使得 PMU 非常适合于快速变化的电力系统动态分析[36]。SCADA 虽然也能提供电气量测量，但其数据精度和更新速度通常低于 PMU。SCADA 系统的数据更新频率通常在几秒到几分钟不等，然而 PMU 可以达到毫秒级的时间精度。仅使用 PMU 测量来跟踪系统状态可以得到更可靠、更准确的状态估计结果。但是，实际电力系统中安装的 PMU 数量通常受到限制。因此，通过 PMU 测量仍然无法保证整个电力系统的可观测性。鉴于上述问题，同时利用 SCADA 和 PMU 测量的混合状态估计(Hybrid State Estimation, HSE)对于实现整个电力系统状态及时、准确更新的需求将变得前所未有的迫切。文献[37]通过引入混合线性鲁棒状态估计器来提高电力系统状态估计的准确性。为此，通过 M 估计器(即具有 Huber 损失函数的 Schweppe 型估计器)完成自动不良数据剔除。迭代重加权最小二乘(Iterative Reweighted Least Squares, IRLS)方法用于最大化 M 估计器中的似然函数。实验结果表明与基于单一量测的状态估计器相比，所提出的鲁棒 HSE 具有更高的估计精度。

在电力系统状态估计的研究领域，为了平衡估计性能和计算效率，众多学者开始融合人工智能技术[38-40]。文献[38]探讨了利用深度神经网络结合相关性分析的策略，通过提取高度相关的量测数据来实施分布式状态估计，这不仅提高了模型的鲁棒性，还增强了计算效率。另外，文献[39][40]分别将长短期记忆(Long Short-Term Memory, LSTM)网络和卷积神经网络(Convolutional Neural Networks, CNN)引入到状态估计领域。这些方法通过深入挖掘和利用量测数据中的关键信息，有效提升了状态估计的准确性和实时性。与传统的纯数据驱动方法相比，这种结合物理知识的方法展现了更好的可解释性，为电力系统状态估计的研究提供了一个新的视角。

1.2.2 虚假数据注入攻击检测和状态恢复研究现状

目前对于电力系统中 FDIA 的研究主要集中在攻击检测与识别、安全性与鲁

棒性评估、防御方法与机制、网络安全架构与策略、攻击模型构建与威胁分析等方面。这些研究的目的是提高电力系统的安全性和可靠性，保障其正常运行[41]。

经典的卡方检验和最大归一化残差检验是根据 WLS 的估计结果实现的。然而，这两种不良数据检测(Bad Data Detection, BDD)方法无法准确检测出系统中的 FDIA。为了可靠地检测 FDIA，最近提出了几种有效的检测方案。在现实中，攻击者很难捕捉到电网的实时状态估计、网络拓扑和参数等准确信息。因此，有缺陷的 FDIA 会导致测量残差的概率分布发生变化。文献[42]利用这一特点提出了基于测量残差一致性的检测方案。同时，詹森-香农距离(Jensen Shannon Distance, JSD)被用来测量残差分布的相似性，以检测系统中是否存在 FDIA。这种方法虽然能可靠地检测出 FDIA，但却无法找到 FDIA 的确切位置，也无法在攻击发生后修正状态。由于静态状态估计和动态状态估计具有不同的估计特性，文献[43]提出了一种基于估计测量值偏差的检测方法。该方法利用 WLS 和 KF 获得的状态估计偏差与相应的阈值进行比较，以确定是否存在 FDIA。但是，该方法没有考虑负载突变(Sudden Load Changes, SLC)的影响以及检测到 FDIA 后如何恢复系统状态。文献[44]提出了一种使用 KF 和递归神经网络(Kalman Filter and Recurrent Neural Network, KFRNN)两级学习器的 FDIA 检测方法。在第一级学习器中，KF 用于状态预测以拟合线性数据，KFRNN 用于拟合非线性数据特征。在第二层学习器中，全连接层和反向传播模块用于整合 KF 和 KFRNN 的结果，然后将结果与动态检测阈值进行比较，以检测 FDIA。

大多数研究都集中在如何检测系统中的 FDIA，然而及时恢复攻击后的测量和状态对于 CPPS 至关重要。文献[45]提出了一种在电力系统受到攻击时恢复测量和状态估计的方法。利用测量数据的惯性效应推导出攻击前的测量数据，以接近攻击前的值。文献[46]针对受到网络攻击的 PMU 提出了一种基于密度的空间聚类方案。该方案可在线检测网络攻击并对其进行分类，还能在受到攻击后恢复 PMU 数据。然而，这种方法仅适用于 PMU 数据恢复，因此缺乏通用性。文献[47]提出了一种抵御 FDIA 的物理模型。该模型将捕捉理想测量值的物理模型与生成对抗网络整合在一起，生成对抗网络捕捉理想测量值的偏差，生成非干扰数据来替代被攻击数据。然而，这种方法需要大量正常数据集和攻击数据集作为训练样本，但在实际电力系统中却没有足够的攻击数据集用于训练模型。文献[48]提出

了一种使用粒子滤波的状态预测算法，用于评估被攻击后状态的原始运行水平。然后，使用快速双线性状态恢复方案来降低网络攻击对状态的影响。然而，潮流方程的非线性特性可能会降低状态恢复的准确性。

1.2.3 研究现状分析

在电力系统的动态状态估计领域，已有的研究采用了多种先进的方法，包括卡尔曼滤波、深度学习、粒子滤波等技术的应用。尽管这些方法各自在处理系统的非线性、提高估计的准确性和鲁棒性等方面取得了一定的进展，但仍存在一些共同的研究局限和可以改进的方向：

（1）处理非线性问题的能力：许多方法在处理电力系统中的强非线性问题时，特别是在极端和复杂的操作条件下，仍然面临挑战。即使是那些特别为非线性设计的方法，如无迹卡尔曼滤波或粒子滤波，也可能在高度非线性或不确定性条件下遇到性能瓶颈。

（2）计算效率：尽管一些方法如基于深度学习的状态估计能够提供良好的估计精度，但这往往以增加计算负担为代价，尤其是在需要大量历史数据进行训练的情况下。对于大规模和实时的电力系统应用，如何平衡计算效率和估计精度仍是一个重要考虑因素。

（3）模型的适应性和泛化能力：许多方法在特定条件下表现良好，但可能缺乏足够的泛化能力来应对电网拓扑、操作条件或数据质量的变化。特别是基于深度学习的方法，可能需要频繁地重新训练来适应新的系统状态，这在实际应用中可能是不可行的。

（4）数据融合和处理：虽然一些方法尝试融合来自不同源的数据，如 SCADA 和 PMU 数据，以提高状态估计的准确性，但在数据融合、处理冗余度以及处理不一致性和异常值方面仍有改进空间。

（5）实时性和动态适应性：在电力系统的实时监测和控制中，确保状态估计算法能够快速响应系统变化，同时保持高准确性和稳定性是一项挑战。此外，随着电网条件和操作模式的不断变化，算法需要具有良好的动态适应性。

综上所述，未来的研究可以聚焦于增强算法处理非线性问题的能力，优化计算效率以适应大规模系统的需求，提升模型的适应性和泛化能力，改进数据融合

和处理技术，以及增强算法的实时性和动态适应性。通过解决这些挑战，可以进一步提高电力系统状态估计的准确性、鲁棒性和实用性，更好地满足现代电力系统的需求。

在智能电网中针对虚假数据注入攻击的检测与防御方面，尽管已有研究提出了基于卡尔曼滤波器、递归神经网络、统计一致性检验等多种方法，但这些方法在实际应用中仍面临一系列挑战和局限性。这些挑战主要包括对攻击行为的假设可能不全面、计算复杂度高、对网络拓扑变化的适应性不足、误报和漏报问题、以及实时操作的限制等。多数研究基于特定的模型假设来设计防御机制，这可能限制了方法对新型或复杂攻击模式的适应性。一些方法如基于粒子滤波和卡尔曼滤波的方案，虽然在提高检测精度方面表现出色，但同时也增加了计算负担，尤其是在需要实时响应的大规模系统中。依赖于历史数据和状态估计的方法可能在面对电网动态变化和新颖攻击策略时，准确性和鲁棒性受到挑战。统计一致性检测可能在高动态电网环境中遇到误报或漏报的问题，尤其是当假数据与历史趋势不显著偏离时。针对这些局限性，未来的研究可以从以下几个方向进行改进和优化：

（1）适应性与泛化能力：加强方法的适应性，以便能够处理更广泛的攻击模式和电网条件变化，可以通过引入更先进的机器学习和数据分析技术来实现。

（2）计算效率优化：探索算法优化或利用并行计算和近似方法来减少计算负担，从而提高方法在实时和大规模系统中的可行性。

（3）动态阈值与参数调整：实现动态阈值调整和自动参数优化机制，以适应电网实时状态和操作条件的变化，从而减少误报和提高检测准确性。

（4）综合多种检测手段：将现有方法与其他检测机制结合，如基于模式识别和异常检测的机器学习方法，可以提供更全面和鲁棒的防御体系。通过以上改进方向的探索和实践，可以期待未来智能电网的虚假数据注入攻击检测与防御技术将更加成熟和有效，为智能电网的安全稳定运行提供更加坚实的保障。

综上所述，虽然当前的研究已经在智能电网安全防护方面取得了一定的进展，但仍然存在着对新型攻击策略适应性不足、计算效率低下以及检测准确性有待提高等问题。未来的研究需要在增强方法的适应性、优化计算效率以及提高检测精度和鲁棒性等方面进行更深入的探索和改进。

1.3 主要研究内容及创新点

综上所述，本文对电力系统中的 FDIA 检测和定位，以及状态恢复问题进行了深度研究，以降低 FDIA 对于状态估计性能的影响。全文主要分为以下几部分内容：FDIA 检测和状态恢复的研究背景和意义、状态估计和 FDIA 检测的国内外研究现状、状态估计和 FDIA 原理、FDIA 检测和定位，以及 FDIA 下的状态估计恢复。本文的主要研究内容如下：

第 1 章：详细讨论了电力系统向网络物理电力系统(Cyber-Physical Power Systems, CPPS)的转型及其挑战。CPPS 通过集成信息通信技术提高了电力系统的状态可观测性和灵活性，尤其在可再生能源和电气化方面。然而，这种融合也带来了网络安全风险，特别是针对电力系统状态估计的 FDIA。进一步介绍了状态估计、FDIA 检测和状态恢复的研究现状。

第 2 章：详细介绍了电力系统的量测模型，包括直流线性模型和交流非线性模型。深入分析了电力系统状态估计的过程和方法，并对基于 WLS 估计结果的不良数据检测方法进行详细分析。最后对 FDIA 的原理和构建方法进行深入研究，并且讨论了 FDIA 在两种模型中的构建方法，包括：直流模型中的 FDIA 和交流模型中的 FDIA。

第 3 章：深入分析了传统 EKF 在电力系统状态估计中的应用原理。考虑到 FDIA 可能导致传统 EKF 在状态估计性能方面的下降，引入了一种具有指数加权函数的扩展卡尔曼滤波器，通过自适应地调整卡尔曼滤波增益，提高系统在 FDIA 环境下的状态估计鲁棒性。利用 WLS 和 EKF 在状态估计方面的差异性，提出一种基于状态估计偏差的 FDIA 检测策略。同时，还提出了一种基于电力网划分的 FDIA 定位技术，以更精确地识别和定位网络中受攻击的区域。

第 4 章：提出一种基于滑动窗口的量测值补偿和状态校正方案。所提出的异常值检测和状态校正算法具体分为三个阶段。第一阶段采用 WLS 对测量数据进行状态估计，随后利用基于 WLS 估计结果的不良数据检测算法，如卡方检验，初步确定系统中是否存在坏数据。第二阶段利用 WLS 和 EKF 的估计结果之间的差异来检测其他异常情况。具体方法是将估计值的差异与预设的检测阈值进行比较，以识别经典不良数据检测算法无法检测到的异常情况。此外，引入了参数可

自适应调节的指数平滑法来预测系统状态，该方法能够根据预测误差动态调整平滑参数，以提升 EKF 状态估计的准确性。第三阶段利用基于滑动窗口的数据补偿策略对测量数据进行修正，并利用这些修正后的数据来重建系统的状态方程和测量方程。最后，对受异常现象影响的状态估计值进行相应的校正。

第 5 章：综合概述了研究内容及其成果，并分析了当前研究的局限性。此外，还对未来的研究方向提出了前瞻性的展望，并就相关课题进行了深入探讨。

本文主要创新点如下：

（1）提高了 EKF 在 FDIA 场景中的状态估计性能。通过在 EKF 中引入指数加权函数，增强状态估计的鲁棒性。具有指数加权函数的 EKF 能够在面对 FDIA 时，自适应地降低当前虚假测量数据的权重，同时增加预测估计测量值的权重，以维持良好的估计性能。

（2）提出了基于状态偏差指数和电力网划分的 FDIA 检测和定位方法。利用 EKF 和 WLS 之间的状态偏差指数与特定误报率的检测阈值进行比较来检测异常值，并通过电力系统量测方程识别被篡改量测向量中的具体条目。提出一种保持子系统冗余度近似相等的系统分区方法，通过在每个子系统中单独检测 FDIA，实现对 FDIA 的定位。

（3）提出了基于 EKF 和数据补偿的状态校正策略。采用基于滑动窗口的数据补偿策略来补偿量测向量中被篡改的特定条目，利用补偿后的量测值重建系统的状态和量测方程，进一步对重建后的方程进行状态估计，实现快速校正系统状态。其中，在状态估计的过程中改进了传统 Holt 双参数指数平滑法，通过预测误差自适应地调节平滑参数，提高状态预测和状态估计的准确性。

第 2 章 电力系统状态估计和虚假数据注入攻击原理

2.1 引言

FDIA 是针对电力系统状态估计的一种安全威胁。在这种攻击模式中，攻击者通过修改存储或传输的数据，并且可以针对数据通信基础设施、控制中心的数据存储，甚至针对 SCADA 远程终端单元(Remote Terminal Units, RTUs)来操纵状态估计的结果，这导致错误的系统分析和决策，甚至可能引发电力系统不稳定或故障。因此，通过对状态估计和虚假数据注入攻击原理进行深入分析，可以发现可能存在的漏洞和攻击手段，从而及时采取措施加以应对，提高系统的安全性和可靠性。

2.2 电力系统状态估计

2.2.1 交流状态估计

在电力系统中，根据不同的求解模型，通常把潮流计算分为直流潮流和交流潮流。电力系统状态估计实质上是量测类型和数量上扩大了的广义潮流。电力系统的状态估计可以分为交流(Alternating Current, AC)状态估计和直流(Direct Current, DC)状态估计两种。在全交流潮流状态估计中，潮流与电压幅值和角度非线性相关，假设电力系统在每次数据采样中具有 m 个测量值和 n 个状态变量，通常 $m > n$ 。交流电力系统的分支等效电路如图 2-1 所示。

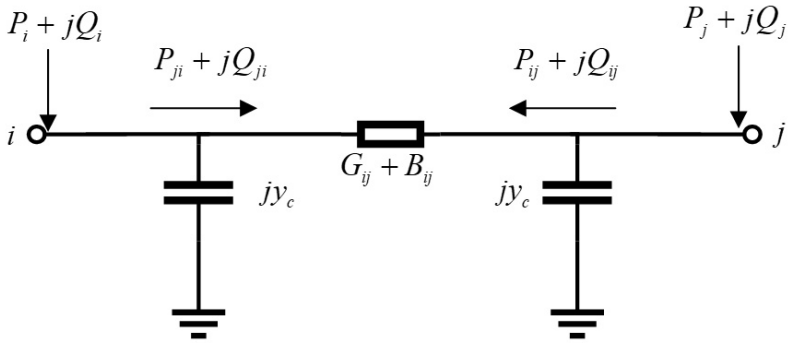


图 2-1 电力系统交流支路等值电路

在交流状态估计中采用交流潮流模型来描述电力系统，产生的非线性量测方

程如式(2.1)所示[13]。

$$\boldsymbol{z}=\boldsymbol{h}(\boldsymbol{x})+\boldsymbol{e} \tag{2.1}$$

式中，$\boldsymbol{z}=\mathbb{R}^{m\times 1}$ 为原始测量向量(有功潮流和无功潮流、有功和无功功率注入、电压幅值和角度)；$\boldsymbol{x}=\mathbb{R}^{n\times 1}$ 为状态向量(电压幅值和电压相角)；$\boldsymbol{e}=\mathbb{R}^{m\times 1}$ 为传感器测量和数据传输误差向量，一般假设其服从均值为 0，协方差矩阵为 $\boldsymbol{R}$ 的高斯分布，即 $\boldsymbol{R}=diag(\sigma_1^2,\ldots,\sigma_m^2)$；$\boldsymbol{h}(\cdot)$ 表示测量向量 $\boldsymbol{z}$ 和状态向量 $\boldsymbol{x}$ 之间的非线性关系。

根据基尔霍夫定律，状态向量与测量向量之间的非线性关系 $\boldsymbol{h}(\cdot)$ 为[13]

$$P_i=V_i\sum_{j\in\Omega_i}V_j(G_{ij}\cos\theta_{ij}+B_{ij}\sin\theta_{ij}) \tag{2.2}$$

$$Q_i=V_i\sum_{j\in\Omega_i}V_j(G_{ij}\sin\theta_{ij}-B_{ij}\cos\theta_{ij}) \tag{2.3}$$

$$P_{ij}=V_i^2(g_{si}+g_{ij})-V_iV_j(g_{ij}\cos\theta_{ij}+b_{ij}\sin\theta_{ij}) \tag{2.4}$$

$$Q_{ij}=-V_i^2(b_{si}+b_{ij})-V_iV_j(g_{ij}\sin\theta_{ij}-b_{ij}\cos\theta_{ij}) \tag{2.5}$$

式中，P_i 和 Q_i 分别是节点 i 的有功功率注入和无功功率注入；P_{ij} 和 Q_{ij} 分别是从节点 i 到节点 j 的有功功率和无功功率；V_i 是节点 i 上的电压；θ_i 是节点 i 的相位角；θ_{ij} 为节点 i 与 j 之间的相位角差；$G_{ij}+jB_{ij}$ 是节点 i 和 j 之间的线路导纳矩阵；$g_{ij}+jb_{ij}$ 是节点 i 处的分流支路导纳；Ω_i 是与节点 i 相关的节点集合。

加权最小二乘(Weighted Least Squares, WLS)状态估计是电力系统分析中一种常用的状态估计方法[27]。它的目的是估计电网的状态变量，如节点电压的幅度和相角，以便更好地监控和控制电网的运行。在电力系统状态估计中，WLS 通过最小化观测值和理论值之间的加权残差平方和来求解状态变量，进而提供电力系统的实时运行状态。这个过程通常包括以下几个步骤：

（1）模型设定：根据电力系统的网络拓扑和线路参数，建立节点功率方程和测量方程。

（2）观测值获取：收集电力系统中的测量数据，如电压、电流、功率等。

（3）权值分配：根据不同测量设备的精确度给予不同的权值，精度高的测量设备具有更大的权重。

（4）求解过程：利用加权最小二乘法，通过迭代计算逼近真实的系统状态。

（5）结果评估：对估计结果进行评估，检查是否满足收敛条件，必要时进行修正或重新估计。

状态估计的目标就是求解出式(2.1)中的状态向量，一般状态估计变量为节点的电压幅值和相角。为了在 WLS 算法的状态估计中找到状态变量的最小无偏估计，引入测量向量误差的目标函数为

$$\begin{aligned} J(\boldsymbol{x}) &= \sum_{i=1}^{m}[z_i - h_i(x)]^2 / \sigma_i^2 \\ &= [\boldsymbol{z} - h(\boldsymbol{x})]^T \boldsymbol{R}^{-1}[\boldsymbol{z} - h(\boldsymbol{x})] \end{aligned} \tag{2.6}$$

式中，$\boldsymbol{x}$ 代表状态向量；m 表示测量值数量；σ_i^2 表示测量向量中第 i 个测量条目的误差；z_i 代表测量向量中的第 i 个测量条目；$\boldsymbol{R}$ 是以 σ_i^2 为对角元素的量测误差方差阵，起权重调整的作用。

WLS 的状态估计结果可以通过最小化目标函数(2.6)来获得[27]。

$$\hat{\boldsymbol{x}} = \arg\min_{x}[\boldsymbol{z} - h(\boldsymbol{x})]^T \boldsymbol{R}^{-1}[\boldsymbol{z} - h(\boldsymbol{x})] \tag{2.7}$$

式中，$\hat{\boldsymbol{x}}$ 是最佳拟合测量向量 $\boldsymbol{z}$ 的状态估计向量。牛顿法可用于求解 WLS 估计问题[13]。

因此，若要计算 $J(\boldsymbol{x})$ 的极值，需要将目标函数 $J(\boldsymbol{x})$ 对状态向量 $\boldsymbol{x}$ 求偏导，然后令其为零，即可计算出状态估计向量 $\hat{\boldsymbol{x}}$。具体计算方法为

$$\frac{\partial J(\boldsymbol{x})}{\partial \boldsymbol{x}^T} = -2\boldsymbol{H}^T(x)\boldsymbol{R}^{-1}[\boldsymbol{z} - h(\boldsymbol{x})] = 0 \tag{2.8}$$

式中，$\boldsymbol{H}(\boldsymbol{x})$ 为雅可比矩阵，即 $\boldsymbol{H}(\boldsymbol{x}) = \dfrac{\partial \boldsymbol{h}(\boldsymbol{x})}{\partial \boldsymbol{x}^T}$。具体的计算过程如下：

先假定状态初值为 $\boldsymbol{x}^{(0)}$，使 $h(\boldsymbol{x})$ 在 $\boldsymbol{x}^{(0)}$ 处线性化，在 $\boldsymbol{x}^{(0)}$ 附近展开 $h(\boldsymbol{x})$ 并略去 $\Delta\boldsymbol{x}$ 的高阶项得

$$h(\boldsymbol{x}) \approx h(\boldsymbol{x}^{(0)}) + \boldsymbol{H}(\boldsymbol{x}^{(0)})\Delta\boldsymbol{x} \tag{2.9}$$

则目标函数 $J(\boldsymbol{x})$ 可以进一步表示为

$$J(\boldsymbol{x}) = [\boldsymbol{z} - h(\boldsymbol{x}^{(0)}) - H(\boldsymbol{x}^{(0)})\Delta\boldsymbol{x}]^T \boldsymbol{R}^{-1}[\boldsymbol{z} - h(\boldsymbol{x}^{(0)}) - \boldsymbol{H}(\boldsymbol{x}^{(0)})\Delta\boldsymbol{x}] \tag{2.10}$$

令 $\Delta \boldsymbol{z}=\boldsymbol{z}-h(\boldsymbol{x}^{(0)})$，把式(2.10)展开为

$$\begin{aligned} J(\boldsymbol{x})=&\Delta \boldsymbol{z}^{T}[\boldsymbol{R}^{-1}-\boldsymbol{R}^{-1}\boldsymbol{H}(\boldsymbol{x}^{(0)})d(\boldsymbol{x}^{(0)})\boldsymbol{H}^{T}(\boldsymbol{x}^{(0)})\boldsymbol{R}^{-1}]\Delta \boldsymbol{z} \\ &+[\Delta \boldsymbol{x}-d(\boldsymbol{x}^{(0)})\boldsymbol{H}^{T}(\boldsymbol{x}^{(0)})\boldsymbol{R}^{-1}\Delta \boldsymbol{z}]^{T}d^{-1}(\boldsymbol{x}^{(0)}) \\ &\cdot[\Delta \boldsymbol{x}-d(\boldsymbol{x}^{(0)})\boldsymbol{H}^{T}(\boldsymbol{x}^{(0)})\boldsymbol{R}^{-1}\Delta \boldsymbol{z}] \end{aligned} \tag{2.11}$$

式中，$d(\boldsymbol{x}^{(0)})=[\boldsymbol{H}^{T}(\boldsymbol{x}^{(0)})\boldsymbol{R}^{-1}\boldsymbol{H}(\boldsymbol{x}^{(0)})]^{-1}$。

在式(2.11)中，右边第一项与 $\Delta \boldsymbol{x}$ 无关，因此要使 $J(\boldsymbol{x})$ 最小，令第二项为零即可，从而有

$$\Delta \boldsymbol{x}=d(\boldsymbol{x}^{(0)})\boldsymbol{H}^{T}(\boldsymbol{x}^{(0)})\boldsymbol{R}^{-1}\Delta \boldsymbol{z} \tag{2.12}$$

由此得到

$$\hat{\boldsymbol{x}}=\boldsymbol{x}^{(0)}+\Delta \hat{\boldsymbol{x}}=\boldsymbol{x}^{(0)}+d(\boldsymbol{x}^{(0)})\boldsymbol{H}^{T}(\boldsymbol{x}^{(0)})\boldsymbol{R}^{-1}[\boldsymbol{z}-h(\boldsymbol{x}^{(0)})] \tag{2.13}$$

利用式(2.13)逐次迭代，可以计算得到 $\hat{\boldsymbol{x}}$。以 l 作为迭代次数，式(2.12)和(2.13)可以表示为

$$\Delta \hat{\boldsymbol{x}}^{(l)}=[\boldsymbol{H}^{T}(\hat{\boldsymbol{x}}^{(l)})\boldsymbol{R}^{-1}\boldsymbol{H}(\hat{\boldsymbol{x}}^{(l)})]^{-1}\boldsymbol{H}^{T}(\hat{\boldsymbol{x}}^{(l)})\boldsymbol{R}^{-1}[\boldsymbol{z}-h(\hat{\boldsymbol{x}}^{(l)})] \tag{2.14}$$

$$\hat{\boldsymbol{x}}^{(l+1)}=\hat{\boldsymbol{x}}^{(l)}+\Delta \hat{\boldsymbol{x}}^{(l)} \tag{2.15}$$

利用式(2.14)和(2.15)反复迭代修正，直到达到收敛条件时迭代停止，判断收敛的三种方法为

$$\max_{i}\left|\Delta \hat{\boldsymbol{x}}_{i}^{(l)}\right|\le \varepsilon_{a} \tag{2.16}$$

$$\left|J(\hat{\boldsymbol{x}}^{(l)})-J(\hat{\boldsymbol{x}}^{(l-1)})\right|<\varepsilon_{b} \tag{2.17}$$

$$\left\|\Delta \hat{\boldsymbol{x}}^{(l)}\right\|\le \varepsilon_{c} \tag{2.18}$$

式中，i 为状态向量 $\boldsymbol{x}$ 中分量的序号；ε_{a}、ε_{b} 和 ε_{c} 分别为三种不同的收敛标准。

2.2.2 直流状态估计

在直流潮流模型中，假定所有节点上的电压幅值的标幺值恒定且等于 1 p.u.，忽略线路中的并联电纳和串联电阻，并且节点之间的角度差很小。因此，$\cos\theta_{ij}\approx 1$，$\sin\theta\approx\theta_{ij}$，此时可以计算出无功功率近似为 0。基于直流潮流模型，流入线路 i 和

j 的有功潮流可以表示为

$$P_{ij}=\frac{\theta_i-\theta_j}{x_{ij}} \tag{2.19}$$

式中，θ_i 和 θ_j 分别表示为节点 i 和 j 的电压相位角；x_{ij} 表示为节点 i 和 j 之间的电抗。

直流状态估计采用直流潮流模型描述电力系统，量测值和状态变量之间的线性方程可以表示为

$$\boldsymbol{z}=\boldsymbol{H}\boldsymbol{x}+\boldsymbol{e} \tag{2.20}$$

式中，$\boldsymbol{H}$ 为 $m\times n$ 的常数雅可比矩阵，其矩阵中的元素仅取决于电网拓扑和线路导纳。

根据加权最小二乘准则建立的目标函数为

$$J(\boldsymbol{x})=[\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x}]^T\boldsymbol{R}^{-1}[\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x}] \tag{2.21}$$

令目标函数 $J(\boldsymbol{x})$ 最小即可得到状态估计向量 $\hat{\boldsymbol{x}}$，使目标函数最小的条件为

$$\frac{\partial J(\boldsymbol{x})}{\partial \boldsymbol{x}}=-2\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{z}+2\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H}\boldsymbol{x}=0 \tag{2.22}$$

通过求解式(2.22)得到状态估计向量 $\hat{\boldsymbol{x}}$ 为

$$\hat{\boldsymbol{x}}=(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{z} \tag{2.23}$$

2.3 不良数据检测原理

在电力系统中，不良数据检测(也称为异常或坏数据检测)是确保系统状态估计准确性的重要步骤。SCADA 系统是电力系统(以及其他许多工业系统)的关键组成部分，负责收集现场传感器和控制设备的数据，并为操作员提供监控与控制界面。然而由于传感器或其连接设备可能因为老化、损坏或其他故障导致读数不准确、数据在传输过程中可能因为电磁干扰以及采集数据不同步等原因，造成获得的实时数据精度低、不完整，有时甚至有错误数据。因此需要不良数据检测和辨识方法来识别和处理测量数据中的错误或异常值，对实时数据进行筛选加工、并剔除错误数据。状态估计器利用处理后的数据进行状态估计得出系统较为准确

的实时数据后，再利用这些数据进行系统的潮流计算、最优潮流和经济调度等工作。目前商用状态估计器中使用的不良数据检测方法主要为卡方检验(Chi-Square, χ^2)和最大归一化残差(Largest Normalized Residual, LNR)检验[49]。这些方法利用统计学原理，例如基于残差的假设检验，来判断测量残差是否符合正态分布或其他已知的分布特性。如果残差不符合预期的分布特性，表明系统中可能存在异常或不良数据。

利用 WLS 估计出状态向量 $\hat{\boldsymbol{x}}$ 后可以得到测量值和估计测量值的差，即残差 $\boldsymbol{r}$ 为

$$\boldsymbol{r} = \boldsymbol{z} - \hat{\boldsymbol{z}} = \boldsymbol{z} - h(\hat{\boldsymbol{x}}) \tag{2.24}$$

把利用 WLS 估计得到的状态估计向量 $\hat{\boldsymbol{x}}$ 带入式(2.6)中得到状态估计后的目标函数为

$$J(\hat{\boldsymbol{x}}) = [\boldsymbol{z} - h(\hat{\boldsymbol{x}})]^T \boldsymbol{R}^{-1} [\boldsymbol{z} - h(\hat{\boldsymbol{x}})] \tag{2.25}$$

使用目标函数 $J(\hat{\boldsymbol{x}})$ 检测不良数据可以通过假设检验来实现，具体检测方法为

$$\begin{cases} H_0\text{：}\ J(\hat{x}) \le \chi^2_{(m-n),p}\text{，则}H_0\text{属真，接受}H_0 \\ H_1\text{：}\ J(\hat{x}) > \chi^2_{(m-n),p}\text{，则}H_0\text{不真，接受}H_1 \end{cases} \tag{2.26}$$

式中，H_0 称为原始假设，即不存在不良数据；H_1 称为备择假设，即存在不良数据。$\chi^2_{(m-n),p}$ 是置信水平为 p 和自由度为 $(m-n)$ 的卡方检验阈值。

LNR 测试是另一种广泛使用的不良数据检测方法。核心是对测量残差进行归一化，即

$$r_i^N = \frac{|z_i - h_i(\hat{\boldsymbol{x}})|}{\sqrt{\Omega_{ii}}} \tag{2.27}$$

$$\boldsymbol{\Omega} = [\boldsymbol{I} - \boldsymbol{H}(\boldsymbol{H}^T \boldsymbol{R}^{-1} \boldsymbol{H})^{-1} \boldsymbol{H}^T \boldsymbol{R}^{-1}] \boldsymbol{R} \tag{2.28}$$

式中，z_i 代表第 i 个测量值；$h_i(\cdot)$ 是将状态向量与第 i 个测量相关联的非线性函数；r_i^N 是第 i 个归一化残差；Ω_{ii} 是 $\boldsymbol{\Omega}$ 的第 i 个对角线条目；$\boldsymbol{I} \in \mathbb{R}^{m \times m}$ 是单位矩阵。如果最大归一化残差大于阈值 ε，则相应的测量将被怀疑为不良数据。

2.4 虚假数据注入攻击原理

针对电力系统状态估计的 FDIA 是一种特殊而复杂的攻击方式，旨在篡改电力系统的状态估计过程，这个过程是电力调度和管理的核心部分。攻击者需要获取或估计电力系统的拓扑结构、线路参数以及系统的运行状态。基于电力系统的数学模型，攻击者设计一个虚假数据向量，这个向量当加到真实的测量数据上时，会导致误导性的状态估计结果。这个攻击向量通常需要细心设计，使得它在数学上与正常的测量误差难以区分，从而绕过不良数据检测机制。

2.4.1 直流模型中的 FDIAs

不良数据辨识模块基于状态估计后的残差进行分析，如果攻击者可以保证攻击前后残差不变或变化程度很小(总残差小于3σ)，虚假数据就可以绕过不良数据辨识模块。直流状态估计的残差为

$$\begin{aligned} \boldsymbol{r} &= \boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}} = \boldsymbol{z} - \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{z} \\ &= [\boldsymbol{I} - \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}]\boldsymbol{z} \end{aligned} \tag{2.29}$$

攻击者的目标是向真实测量向量 $\boldsymbol{z}$ 中叠加一个攻击向量 $\boldsymbol{a}$ 得到虚假测量向量 $\boldsymbol{z}_f$，但保持攻击前后的残差不变，即

$$[\boldsymbol{I} - \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}]\boldsymbol{z} = [\boldsymbol{I} - \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}](\boldsymbol{z}+\boldsymbol{a}) \tag{2.30}$$

进一步化简，得

$$\begin{aligned} \boldsymbol{a} &= \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{a} \\ &= \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}(\boldsymbol{z}_f - \boldsymbol{z}) \\ &= \boldsymbol{H}(\hat{\boldsymbol{x}}_f - \hat{\boldsymbol{x}}) \\ &= \boldsymbol{H}\boldsymbol{c} \end{aligned} \tag{2.31}$$

式中，$\boldsymbol{c}$ 为 FDIA 对状态估计造成的偏移；$\hat{\boldsymbol{x}}_f$ 为攻击者期望的状态估计结果；$\boldsymbol{a}$ 为攻击者注入的攻击向量；$\boldsymbol{z}_f$ 为被篡改后的测量向量。

假设攻击者在正常测量向量 $\boldsymbol{z}$ 中叠加了一个攻击向量 $\boldsymbol{a}$，则被攻击后的状态估计残差为

$$\begin{aligned} \boldsymbol{r}_f &= \boldsymbol{z}_f - \boldsymbol{H}(\hat{\boldsymbol{x}} + \boldsymbol{c}) \\ &= \boldsymbol{z} + \boldsymbol{a} - \boldsymbol{H}\hat{\boldsymbol{x}} - \boldsymbol{H}\boldsymbol{c} \\ &= \boldsymbol{z} + \boldsymbol{H}\boldsymbol{c} - \boldsymbol{H}\hat{\boldsymbol{x}} - \boldsymbol{H}\boldsymbol{c} \\ &= \boldsymbol{r} \end{aligned} \tag{2.32}$$

式中，$\boldsymbol{r}_f$ 为攻击后的状态估计残差。如果攻击者注入的攻击向量为 $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$，则从式(2.32)可以推导出攻击后的状态估计残差 $\boldsymbol{r}_f$ 和正常的状态估计残差 $\boldsymbol{r}$ 相等。因此，攻击者注入的虚假数据可以绕过不良数据检测模块，从而对电力系统的状态估计过程造成破坏。

上述详细介绍了 FDIA 绕过传统不良数据检测的原理。那么，为了针对某个状态变量 $\boldsymbol{x}_i$ 发起虚假数据注入攻击，需要篡改哪些量测值才能实现目标并且不被检测到。从攻击向量 $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$ 中就可以找到其中的隐藏信息，实际上，量测雅可比矩阵 $\boldsymbol{H}$ 建立了量测和状态变量之间的电气联系。假设攻击者对状态变量 $\boldsymbol{x}_i$ 发起 FDIA，那么量测雅可比矩阵 $\boldsymbol{H}$ 的第 i 列所有非零元素所在的行均对应于与状态变量 $\boldsymbol{x}_i$ 有电气联系的量测量，这些量测都需要同时按规律地被篡改。

如果向一个特定的状态变量注入虚假数据，需要篡改的量测值个数与以下因素有关：(1) 网络拓扑结构直接影响量测雅可比矩阵 $\boldsymbol{H}$，$\boldsymbol{H}$ 建立了量测值与状态变量之间的电气联系；(2) 目标状态变量对应的母线是否有功率注入；(3) 系统内量测装置的安装位置；(4) 攻击者注入的攻击分量 $\boldsymbol{a}$ 的值等因素密切相关，通常要篡改的量测值要大于一个。

2.4.2 交流模型中的 FDIAs

直流/线性状态估计只是更一般的交流/非线性状态估计的简化版本。线性和非线性状态估计之间存在一些差异。首先，与以封闭形式获得解的线性情况不同，在非线性状态估计中，解是通过迭代获得的。其次，线性状态估计基于有功潮流分析，而非线性状态估计基于有功潮流分析和无功潮流分析。第三，线性状态估计中的状态变量只是电压相位角，而非线性状态估计将电压相位角和幅值都视为状态。这些差异使得非线性状态估计变得更加复杂。这种复杂性是导致针对非线性状态估计的 FDIA 难以实现的主要原因。

针对直流状态估计的 FDIA 模型中，攻击者只需要一些有关电网拓扑的离线数据。然而，针对交流状态估计的 FDIA 模型更加复杂，要求攻击者在实施攻击时从网格中收集一些在线数据。

令 $\boldsymbol{a} \in \mathbb{R}^{m\times 1}$ 表示攻击者试图注入电表的攻击向量。那么正常测量向量 $\boldsymbol{z}$ 受到攻击后就变成 $\boldsymbol{z}_f = \boldsymbol{z} + \boldsymbol{a}$。设 $\hat{\boldsymbol{x}}_f = \hat{\boldsymbol{x}} + \boldsymbol{c}$ 表示受到攻击后的状态估计向量，其中 $\boldsymbol{c}$ 是 FDIA 引起的状态估计偏差，即 $\boldsymbol{c} = [c_1, \ldots c_n]^T$。如果攻击者构造一个精心设计的攻击向量为

$$\boldsymbol{a} = h(\hat{\boldsymbol{x}} + \boldsymbol{c}) - h(\hat{\boldsymbol{x}}) \tag{2.33}$$

则受攻击后的残差向量为

$$\begin{aligned} \boldsymbol{r}_f &= \boldsymbol{z}_f - h(\hat{\boldsymbol{x}}_f) \\ &= \boldsymbol{z} + h(\hat{\boldsymbol{x}} + \boldsymbol{c}) - h(\hat{\boldsymbol{x}}) - h(\hat{\boldsymbol{x}} + \boldsymbol{c}) \\ &= \boldsymbol{z} - h(\hat{\boldsymbol{x}}) \\ &= \boldsymbol{r} \end{aligned} \tag{2.34}$$

式中，$\boldsymbol{r}_f$ 和 $\boldsymbol{r}$ 分别是攻击和正常的测量残差向量。式(2.34)表明，攻击和正常的测量残差相等。因此，传统的不良数据检测方法无法检测上述构造的虚假数据注入攻击。

2.5 本章小结

本章主要介绍了电力系统状态估计和虚假数据注入攻击原理。首先介绍了交流潮流和直流潮流的不同之处；其次给出了交流和直流状态估计的详细推导过程，并在状态估计的基础上详细介绍了传统不良数据检测方法和对应的原理；最后详细阐述了传统不良数据检测的漏洞，并详细介绍了直流模型和交流模型中的 FDIA 原理与构建方式。为后续研究虚假数据注入攻击检测和定位以及状态估计校正夯实基础。

第 3 章 基于动静态联合估计的 FDIAs 检测方法

3.1 引言

在电力系统安全领域，虚假数据注入攻击已经成为电网安全运行的严重威胁。第二章详细介绍了电力系统状态估计和虚假数据注入攻击原理。由于虚假数据注入攻击变得日益复杂和隐蔽，因此传统的 WLS 方法已经不足以有效检测和应对虚假数据注入攻击。此外，WLS 方法所获得的状态估计仅基于当前测量数据，缺乏历史信息，这限制了其对系统运行状态的准确预测能力。

为解决上述问题，本章提出了一种改进的 EKF 方法，以提高状态估计的鲁棒性。EKF 方法不仅考虑了当前测量数据，还融合了历史信息，能够更准确地预测系统的运行状态。此外，考虑到 WLS 和改进 EKF 的状态估计特性，通过一致性检验和残差检验的方式，实现对虚假数据注入攻击的检测。此外，为了更精确地定位虚假数据注入攻击，本章还提出了一种基于子系统近似等冗余的电力网划分方法。该方法能够帮助系统管理员迅速定位潜在的攻击点，进一步加强了电网安全性的保障。

3.2 状态估计模型

电力信息物理系统是一个高度多维非线性系统，电力系统交流潮流方程呈现非线性关系。状态估计的状态方程和测量方程分别为[50]

$$\boldsymbol{x}_{k+1} = \boldsymbol{f}(\boldsymbol{x}_k) + \boldsymbol{w}_k \tag{3.1}$$

$$\boldsymbol{z}_k = \boldsymbol{h}(\boldsymbol{x}_k) + \boldsymbol{v}_k \tag{3.2}$$

式中，$\boldsymbol{x}_k$ 和 $\boldsymbol{x}_{k+1}$ 分别表示 k 时刻和 $k+1$ 时刻的状态向量；$\boldsymbol{f}(\cdot)$ 为状态向量 $\boldsymbol{x}_k$ 到 $\boldsymbol{x}_{k+1}$ 的状态转移方程；$\boldsymbol{w}_k$ 是 k 时刻的过程误差；$\boldsymbol{z}_k$ 和 $\boldsymbol{v}_k$ 分别表示 k 时刻的测量向量和测量误差向量；$\boldsymbol{h}(\cdot)$ 表示状态向量 $\boldsymbol{x}$ 和测量向量 $\boldsymbol{z}$ 之间的非线性关系。假设 $\boldsymbol{w}_k$ 和 $\boldsymbol{v}_k$ 不相关并且服从零均值的高斯白噪声，它们的误差协方差矩阵分别为 $\boldsymbol{Q}$ 和 $\boldsymbol{R}$。

卡尔曼滤波器(Kalman Filter, KF)是一种线性最优估计器。然而，CPPS 是一

个高度多维、非线性的系统。因此，本章考虑使用 EKF 进行状态估计[29]。EKF 的线性化模型为

$$\boldsymbol{x}_{k+1} = \boldsymbol{F}_k \boldsymbol{x}_k + \boldsymbol{G}_k + \boldsymbol{w}_k \tag{3.3}$$

$$\boldsymbol{z}_k = \boldsymbol{H}_k \boldsymbol{x}_k + \boldsymbol{v}_k \tag{3.4}$$

式中，$\boldsymbol{F}_k = \partial \boldsymbol{f} / \partial \boldsymbol{x}|_{\boldsymbol{x}=\hat{\boldsymbol{x}}_k}$ 是 k 时刻状态方程的雅可比矩阵；$\boldsymbol{G}_k$ 表示为 k 时刻的输入矩阵；$\boldsymbol{H}_k = \partial \boldsymbol{h} / \partial \boldsymbol{x}|_{\boldsymbol{x}=\hat{\boldsymbol{x}}_k}$ 是 k 时刻测量方程的雅可比矩阵。

CPPS 是一个复杂性、多维性、负载变化性的网络。每个时刻的状态转移矩阵很难确定，采用对状态方程进行线性化的方法会引入误差。因此，本章采用 Holt 双参数指数平滑法来预测下一时刻的状态值[51]。该方法具有存储变量少、计算速度快的优点，适合短期负荷预测。它是一种在线识别方法。利用 Holt 双参数指数平滑技术，式(3.1)中的状态转移函数 $\boldsymbol{f}(\cdot)$ 可表示为

$$\hat{\boldsymbol{x}}_{k+1|k} = \boldsymbol{a}_k + \boldsymbol{b}_k \tag{3.5}$$

其中，式(3.5)中的 $\boldsymbol{a}_k$ 和 $\boldsymbol{b}_k$ 可以表示为

$$\begin{cases} \boldsymbol{a}_k = \alpha \hat{\boldsymbol{x}}_k + (1-\alpha)\hat{\boldsymbol{x}}_{k|k-1} \\ \boldsymbol{b}_k = \beta(\boldsymbol{a}_k - \boldsymbol{a}_{k-1}) + (1-\beta)\boldsymbol{b}_{k-1} \end{cases} \tag{3.6}$$

式中，$\hat{\boldsymbol{x}}_k$ 和 $\hat{\boldsymbol{x}}_{k+1|k}$ 分别表示 k 时刻的状态估计向量和预测状态向量；$\boldsymbol{a}_k$ 和 $\boldsymbol{b}_k$ 分别表示为水平值和趋势值；α 和 β 分别表示为平滑水平和平滑趋势的参数。这些参数控制了水平和趋势的平滑程度。

从式(3.5)和(3.6)可以得到式(3.3)中的 $\boldsymbol{F}_k$ 和 $\boldsymbol{G}_k$ 为

$$\begin{cases} \boldsymbol{F}_k = \alpha(1+\beta)\boldsymbol{I} \\ \boldsymbol{G}_k = (1+\beta)(1-\alpha)\hat{\boldsymbol{x}}_{k|k-1} - \beta\boldsymbol{a}_{k-1} + (1-\beta)\boldsymbol{b}_{k-1} \end{cases} \tag{3.7}$$

因此，利用式(3.7)计算状态转移矩阵 $\boldsymbol{F}_k$ 和输入矩阵 $\boldsymbol{G}_k$，避免了 $\boldsymbol{F}_k$ 和 $\boldsymbol{G}_k$ 难以获得的困难。利用 Holt 双参数指数平滑法得到的状态预测值将进一步应用于基于 EKF 的状态估计过程中，解决状态估计预测步骤中的状态预测问题，提高状态估计的计算效率。

3.3 改进的扩展卡尔曼滤波

3.3.1 扩展卡尔曼滤波原理

KF 是一种用于估计动态系统状态的递归滤波器，它结合了系统模型和测量数据，通过递归地更新状态估计来提高估计的精度。EKF 是 KF 的一种扩展，特别适用于非线性系统。KF 的基本思想是通过结合先验信息(由系统模型提供)和测量信息来估计系统的当前状态。EKF 通过使用泰勒级数展开并忽略二次项和更高阶项来处理非线性系统模型和测量方程。EKF 算法的基本流程为

（1）预测步

$$\hat{\boldsymbol{x}}_{k|k-1}=\boldsymbol{F}_{k-1}\hat{\boldsymbol{x}}_{k-1} \tag{3.8}$$

$$\boldsymbol{P}_{k|k-1}=\boldsymbol{F}_{k-1}\boldsymbol{P}_{k-1}\boldsymbol{F}_{k-1}^{T}+\boldsymbol{Q}_{k-1} \tag{3.9}$$

（2）更新步

$$\hat{\boldsymbol{x}}_{k}=\hat{\boldsymbol{x}}_{k|k-1}+\boldsymbol{K}_{k}\left[\boldsymbol{z}_{k}-\boldsymbol{h}\left(\hat{\boldsymbol{x}}_{k|k-1}\right)\right] \tag{3.10}$$

$$\boldsymbol{K}_{k}=\boldsymbol{P}_{k|k-1}\boldsymbol{H}_{k}^{T}(\boldsymbol{H}_{k}\boldsymbol{P}_{k|k-1}\boldsymbol{H}_{k}^{T}+\boldsymbol{R}_{k})^{-1} \tag{3.11}$$

$$\boldsymbol{P}_{k}=\left(\boldsymbol{I}-\boldsymbol{K}_{k}\boldsymbol{H}_{k}\right)\boldsymbol{P}_{k|k-1} \tag{3.12}$$

式中，$\boldsymbol{P}_{k|k-1}$和$\boldsymbol{P}_{k}$分别表示为k时刻的先验估计误差的协方差矩阵和后验估计误差的协方差矩阵；$\boldsymbol{K}_{k}$表示k时刻的卡尔曼增益。状态和估计误差协方差矩阵的初始值分别设置为$\hat{\boldsymbol{x}}_{0}=\boldsymbol{0}$和$\boldsymbol{P}_{0}=\boldsymbol{I}$。

3.3.2 基于指数加权函数的扩展卡尔曼滤波

将k时刻的预测估计残差定义为$\tilde{\boldsymbol{r}}=\boldsymbol{z}_{k}-\boldsymbol{h}(\hat{\boldsymbol{x}}_{k|k-1})$。攻击者在$k$时刻向电力系统发起虚假数据注入攻击。此外，攻击者只能向仪表量测值中注入偏差来篡改量测值，篡改后的量测值从$\boldsymbol{z}_{k}$变为$\boldsymbol{z}_{k}^{a}$。因此，k时刻状态估计的计算公式可由式(3.10)重写为

$$\begin{aligned}\hat{\boldsymbol{x}}_k^a &= \boldsymbol{F}\hat{\boldsymbol{x}}_{k-1} + \boldsymbol{K}_k[\boldsymbol{z}_k^a - \boldsymbol{h}(\hat{\boldsymbol{x}}_{k|k-1})] \\ &= \boldsymbol{F}\hat{\boldsymbol{x}}_{k-1} + \boldsymbol{K}_k[\boldsymbol{z}_k + \boldsymbol{a}_k - \boldsymbol{h}(\hat{\boldsymbol{x}}_{k|k-1})] \\ &= \hat{\boldsymbol{x}}_k + \boldsymbol{K}_k\boldsymbol{a}_k\end{aligned} \tag{3.13}$$

式中，$\hat{\boldsymbol{x}}_k^a$ 表示在 k 时刻受到攻击后的状态估计向量；$\boldsymbol{a}_k$ 表示在 k 时刻注入的攻击向量。

假设在 k 时刻虚假数据注入攻击造成的状态估计偏差为 $\Delta\hat{\boldsymbol{x}}_k^a = \hat{\boldsymbol{x}}_k^a - \hat{\boldsymbol{x}}_k$。因此，在 $k+1$ 时刻受到攻击后得到的状态估计向量为

$$\begin{aligned}\hat{\boldsymbol{x}}_{k+1}^a &= \boldsymbol{F}\hat{\boldsymbol{x}}_k^a + \boldsymbol{K}_{k+1}[\boldsymbol{z}_{k+1}^a - \boldsymbol{h}(\hat{\boldsymbol{x}}_{k+1|k}^a)] \\ &= \boldsymbol{F}\hat{\boldsymbol{x}}_k^a + \boldsymbol{K}_{k+1}[\boldsymbol{z}_{k+1} + \boldsymbol{a}_{k+1} - \boldsymbol{h}(\hat{\boldsymbol{x}}_{k+1|k}^a)] \\ &= \boldsymbol{F}\Delta\hat{\boldsymbol{x}}_k^a + \boldsymbol{K}_{k+1}[\Delta\boldsymbol{h}^a(\hat{\boldsymbol{x}}_{k+1|k}) + \boldsymbol{a}_{k+1}] + \hat{\boldsymbol{x}}_{k+1}\end{aligned} \tag{3.14}$$

将 k 时刻预测的估计测量值的注入偏差定义为 $\Delta\boldsymbol{h}^a(\hat{\boldsymbol{x}}_{k+1|k}) = \boldsymbol{h}(\hat{\boldsymbol{x}}_{k+1|k}) - \boldsymbol{h}(\hat{\boldsymbol{x}}_{k+1|k}^a)$。因此，在 $k+1$ 时刻虚假数据注入攻击造成的状态估计偏差为

$$\hat{\boldsymbol{x}}_{k+1}^a - \hat{\boldsymbol{x}}_{k+1} = \boldsymbol{F}\Delta\hat{\boldsymbol{x}}_k^a + \boldsymbol{K}_{k+1}\Delta\boldsymbol{h}^a(\hat{\boldsymbol{x}}_{k+1|k}) + \boldsymbol{K}_{k+1}\boldsymbol{a}_{k+1} \tag{3.15}$$

从式(3.15)可以得出，当前时刻的状态估计偏差不仅受到前一时刻状态估计偏差的影响，还受到当前时刻注入攻击的影响。当使用 EKF 进行状态估计时，状态转移方程和过程噪声会对状态估计产生一定的影响，因此 EKF 中存在一个收敛的过渡过程。

在 k 时刻注入 FDIA 时，预测估计残差 $\tilde{\boldsymbol{r}} = \boldsymbol{z}_k - \boldsymbol{h}(\hat{\boldsymbol{x}}_{k|k-1})$ 增加。此外，利用具有虚假数据的测量值进行状态估计，导致传统 EKF 的状态估计结果出现偏差，破坏了状态估计的有效性。为了使 EKF 在 FDIA 存在的情况下仍具有良好的状态估计性能，本节利用预测残差自适应地降低 EKF 的滤波器增益，从而允许受攻击的测量值在状态估计过程中具有较低的权重。同时，增加预测估计测量值的权重。测量的加权矩阵 $\boldsymbol{W}_k$ 和测量噪声的协方差矩阵 $\boldsymbol{R}$ 之间的关系为 $\boldsymbol{W}_k = \boldsymbol{R}^{-1}$。因此，测量的加权矩阵可以更新为

$$(\boldsymbol{W}_k^{new})^{-1} = \boldsymbol{W}_k^{-1} * e^{|z_k - h(\hat{x}_{k|k-1})|} \tag{3.16}$$

上述方法能够有效抑制由于攻击强度的增加而导致的状态估计性能下降。当测量值 $\boldsymbol{z}_k$ 显著偏离预测估计测量值 $\boldsymbol{h}(\hat{\boldsymbol{x}}_{k|k-1})$ 时，预测残差向量模的增加使得测量

噪声增加，最终降低卡尔曼增益。相反，预测估计测量值和当前测量值之间的微小偏差会导致测量噪声的微小变化，这进一步导致卡尔曼增益的微小变化，并最终导致估计值的微小变化。当 FDIA 存在时，具有指数加权函数的扩展卡尔曼滤波(Extended Kalman Filtering with Exponential Weighting Function, WEKF)可以更好地抑制虚假数据对状态估计的影响，从而使得 WEKF 具有更好的估计鲁棒性。

根据上节对于 Holt 双参数指数平滑法和改进 EKF 的原理分析，WEKF 的状态估计算法流程如表 3-1 所示。

表 3-1 基于 WEKF 的状态估计算法流程

算法：基于 WEKF 的状态估计算法
输入：$\boldsymbol{a}_0$，$\boldsymbol{b}_0$，$\boldsymbol{Q}$，$\boldsymbol{R}$，$\hat{\boldsymbol{x}}_0$ 和 $\boldsymbol{P}_0$
输出：$\hat{\boldsymbol{x}}_k$ 和 $\boldsymbol{P}_k$
1：　获取量测向量和量测雅可比矩阵：$\boldsymbol{z}_k$ 和 $\boldsymbol{H}_k = \partial \boldsymbol{h} / \partial \boldsymbol{x} \mid_{\boldsymbol{x}=\hat{\boldsymbol{x}}_{k\mid k-1}}$
2：　状态变量预测：$\hat{\boldsymbol{x}}_{k\mid k-1} = \alpha(1+\beta)\hat{\boldsymbol{x}}_k + (1+\beta)(1-\alpha)\hat{\boldsymbol{x}}_{k\mid k-1} - \beta \boldsymbol{a}_{k-1} + (1-\beta)\boldsymbol{b}_{k-1}$
3：　预测误差协方差矩阵：$\boldsymbol{P}_{k\mid k-1} = \boldsymbol{F}_{k-1}\boldsymbol{P}_{k-1}\boldsymbol{F}_{k-1}^T + \boldsymbol{Q}_{k-1}$
4：　预测估计残差：$\tilde{\boldsymbol{r}} = \boldsymbol{z}_k - h(\hat{\boldsymbol{x}}_{k\mid k-1})$
5：　更新权重矩阵：$(\boldsymbol{W}_k^{new})^{-1} = \boldsymbol{W}_k^{-1} * e^{\lvert z_k - h(\hat{x}_{k\mid k-1})\rvert} = \boldsymbol{W}_k^{-1} * e^{\lvert \tilde{r} \rvert}$
6：　获取更新的卡尔曼增益：$\boldsymbol{K}_k = \boldsymbol{P}_{k\mid k-1}\boldsymbol{H}_k^T(\boldsymbol{H}_k\boldsymbol{P}_{k\mid k-1}\boldsymbol{H}_k^T + \boldsymbol{R}_k)^{-1}$
7：　获取更新的状态：$\hat{\boldsymbol{x}}_k = \hat{\boldsymbol{x}}_{k\mid k-1} + \boldsymbol{K}_k\left[\boldsymbol{z}_k - \boldsymbol{h}\left(\hat{\boldsymbol{x}}_{k\mid k-1}\right)\right]$
8：　更新估计误差协方差矩阵：$\boldsymbol{P}_k = \left(\boldsymbol{I} - \boldsymbol{K}_k\boldsymbol{H}_k\right)\boldsymbol{P}_{k\mid k-1}$

3.4 基于动静态联合估计和电力网划分的 FDIA 检测和定位

3.4.1 基于动静态联合估计的 FDIA 检测

SCADA 系统通过 RTUs 采集系统的量测数据，然后将这些数据传输到中央控制主站，以实现实时监控、控制和数据分析，从而确保工业过程的安全性和效

率。然而量测工具的偶然故障、数据传输的干扰以及采集数据不同步等因素，造成获得的实时数据精度低，这些量测情况下的较大误差和干扰一般会被不良数据辨识模块发现和剔除。通过第二章对于 FDIA 的详细介绍可知，攻击者通过分析和模仿真实数据的特征，使得注入的虚假数据具有与正常数据相似的估计残差、统计特征、趋势和分布。这减少了虚假数据和真实数据之间的差异，从而使其具有高度隐蔽性。因此，传统的不良数据检测方法无法检测出具有高度隐蔽性的 FDIA。

由前面章节详细介绍的基于 WLS 和 EKF 的状态估计原理可知，WLS 利用当前时刻的量测数据和模型，进行加权最小二乘估计，以计算状态变量的估计值。这个估计值代表了系统在当前时刻的状态。然而 EKF 的状态估计结果集成了历史信息和当前信息。EKF 是一种递归的状态估计方法，用于估计系统的状态变量。它通过融合历史信息(先前的状态估计结果)和当前信息(最新的观测或量测数据)来更新和改进状态估计，并使用系统模型来预测和估计电力系统的状态。因此，当测量中存在虚假数据时，WLS 的估计结果会由于当前量测值的改变导致估计结果的跳变，然而 EKF 是一种递归状态估计方法，导致状态估计的结果存在状态转移的变化过程。这使得 WLS 和 EKF 的估计结果将会出现差异。同时，利用上节提出的 WEKF 可以更好地抑制 FDIA 对状态估计结果的影响，使得 WEKF 和 WLS 的状态估计偏差更大，从而更容易检测到 FDIA。将两种估计器的状态估计偏差与相应的阈值比较可以有效地检测系统中的异常情况。详细的检测过程如下：

首先，在 k 时刻对电力系统进行潮流计算，将计算结果加上符合高斯分布的扰动误差作为当前系统的量测数据。然后，分别使用 WLS 和 WEKF 两种状态估计方法来估计系统的当前状态。进一步使用一致性检验来比较两个估计结果之间的偏差。具体的一致性检验公式为

$$\left\| \hat{\boldsymbol{x}}_k^s - \hat{\boldsymbol{x}}_k^d \right\|_2 \le \tau_a \tag{3.17}$$

式中，$\hat{\boldsymbol{x}}_k^s$ 和 $\hat{\boldsymbol{x}}_k^d$ 分别表示 WEKF 和 WLS 的状态估计结果。τ_a 为一致性检验阈值，其值由测量误差和状态估计结果的准确性决定。

由于状态预测值是使用 Holt 双参数指数平滑法计算的，导致发电机和负载

突然变化的系统不再适用。因此，即使系统没有受到攻击，也可能无法满足一致性测试。为了消除由发电机突变和负荷突变引起的错误检测，可以进一步检验估计量测值和实际量测值之间的残差来解决这一问题。具体的残差检验公式为

$$\left\| \boldsymbol{z}_k - \boldsymbol{h}(\hat{\boldsymbol{x}}_k^s) \right\|_2 \le \tau_b \tag{3.18}$$

式中，$\boldsymbol{h}(\hat{\boldsymbol{x}}_k^s)$ 是使用 WEKF 获得的估计量测值；τ_b 是残差检测阈值，其值由卡方分布的误差容限决定。

基于动静态联合估计的 FDIA 检测流程如图 3-1 所示。

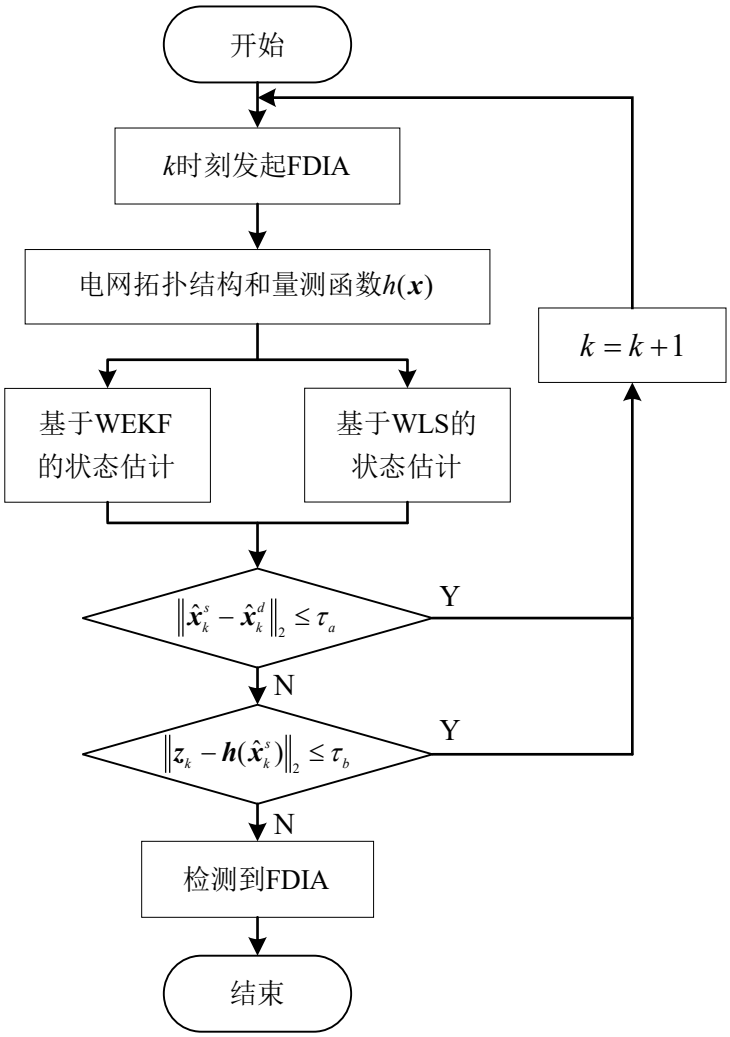


图 3-1 基于状态偏差的 FDIA 检测流程图

如图 3-1 所示，检测 FDIA 和判断不良数据干扰的过程可以总结如下：当 FDIA 确实存在时，正常量测值被虚假数据篡改，由于基于 WLS 的状态估计过程利用当前时刻的量测值，所以 WLS 的状态估计结果会以迅速响应的方式受到影响。与之相对应，WEKF 考虑了状态转移的变化以及前一时刻的状态估计结果，

因此其下一时刻的状态估计结果不会出现较大的变化。在这种情况下，WLS 和 WEKF 的估计值之间存在显著差异，导致一致性检验的结果大幅超过检验阈值。从而可以及时检测到系统中存在的异常情况。接下来，需要进一步判断这一情况是由于突变干扰还是FDIA确实存在引起的。为了进行这一判断，进一步对WEKF的残差进行检验。如果残差检验的结果也超过了预定的阈值，那么可以得出 FDIA 确实存在的结论。反之，如果残差检验结果未超过阈值，那么可以认为存在干扰情况。

3.4.2 基于电力网划分的 FDIA 定位

电力系统的稳定性是保证社会正常运行的基础。FDIA 可能会导致错误的状态估计，引起错误的调度决策，甚至引发电网失稳或大规模停电，对社会造成巨大影响。在上一节中详细介绍了基于状态偏差的 FDIA 检测方法，然而检测到系统中存在 FDIA 后对其定位具有重要意义。通过对攻击的有效定位，可以了解攻击的特点和模式，进一步加强系统的安全性设计和防御措施，提高电力系统对未来攻击的抵抗力。

当系统中存在 FDIA 时，进行一致性检验和残差检验使得式(3.17)和式(3.18)均大于相应的检测阈值。在检测到整个系统中存在 FDIA 后，为了进一步确定其位置，可以对整个电力网进行更细致的划分，然后分别在每个子网络中进行卡方检验来确定 FDIA 可能存在的位置。系统的划分是按照量测冗余度近似相等的原则，其原因是可以保证在每个子系统量测冗余度相等的情况下检测阈值相等。系统的量测冗余度可以表示为

$$K = m/n \tag{3.19}$$

式中，m 为量测值个数或者量测方程个数；n 为状态变量个数或者未知数的个数。

系统的划分是根据量测冗余度近似相等以及总线编号建立的，划分后的系统可以表示为

$$\begin{aligned} & S_i = \{S \to Bus_{number}, K_i\} \\ \text{subject to } & K_i \approx K,\ \forall i = 1,2,\ldots,N \\ & \bigcup_{i=1}^{N} S_i = S \end{aligned} \tag{3.20}$$

式中，S 代表整个电力系统；S_i 代表第 i 个子系统；Bus_{number} 代表总线对应的编号；K_i 代表第 i 个子系统的量测冗余度；K 代表所需的冗余度；N 代表子系统的数量。

当使用本章介绍的基于状态偏差的 FDIA 检测方法检测到系统中存在 FDIA 后触发系统划分，系统划分是根据量测冗余度近似相等以及总线编号建立的，然后分别在每个子系统中进行卡方检验来确定 FDIA 的位置。其中，卡方检验的阈值由卡方分布的置信水平 p 和自由度 $c=m-n$ 决定[49]。此外，一旦状态偏差超过预设阈值，本节提出的方法就会触发系统划分，将电力网划分为更小的子系统，然后在每个子系统内应用卡方检验。在这些子系统的范围内，测试变得更加有效，因为冗余测量的数量减少，从而减少了 χ^2 和 $J(\boldsymbol{x})$。

综上所述，基于动静态联合估计和电力网划分的 FDIA 检测和定位的具体执行过程如表 3-2 所示。

表 3-2 基于动静态联合估计和电力网划分的 FDIA 检测和定位流程

算法：基于动静态联合估计和电力网划分的 FDIA 检测和定位
输入：平滑参数 α 和 β；噪声误差协方差矩阵 $\boldsymbol{Q}$ 和 $\boldsymbol{R}$；初始状态 $\boldsymbol{x}_0$ 和状态误差协方差矩阵 $\boldsymbol{P}_0$；一致性测试阈值 τ_a 和残差测试阈值 τ_b
输出：FDIA 的位置
1：**for** $k=1:N$，其中 N 代表时间断面数 **do**
2：　获取测量向量 $\boldsymbol{z}_k$ 并确定雅可比矩阵 $\boldsymbol{H}_k$
3：　采用式(3.5)和(3.6)的 Holt 指数平滑方法来预测下一时刻的状态 $\hat{\boldsymbol{x}}_{k\|k-1}$
4：　采用式(2.7)计算加权最小二乘法的状态估计向量 $\hat{\boldsymbol{x}}_k^d$
5：　由式(3.9)获得预测估计误差协方差矩阵 $\boldsymbol{P}_{k\|k-1}$
6：　使用式(3.16)更新测量噪声协方差矩阵，其中 $\boldsymbol{W}_k=\boldsymbol{R}^{-1}$
7：　使用式(3.11)更新卡尔曼增益 $\boldsymbol{K}_k$
8：　由式(3.10)获取 WEKF 的状态估计值 $\hat{\boldsymbol{x}}_k^s$

续表 3-2 基于动静态联合估计和电力网划分的 FDIA 检测和定位流程

9：	**if** $\left\|\hat{\boldsymbol{x}}_k^s - \hat{\boldsymbol{x}}_k^d\right\|_2 \geq \tau_a$ **then**
10：	FDIA 和不良数据可能同时存在
11：	**else if** $\left\|\boldsymbol{z}_k - \boldsymbol{h}(\hat{\boldsymbol{x}}_k^s)\right\|_2 \geq \tau_b$ **then**
12：	检测到 FDIA 存在并触发警报和划分系统
13：	使用式(2.26)对划分后的子系统分别进行卡方检验
14：	如果利用式(2.25)得到的子系统的目标函数仍然大于阈值
15：	将子系统划分为更小的子系统，直至定位到 FDIA 攻击位置
16：	**else**
17：	FDIA 不存在，状态估计过程继续执行
18：	**end if**
19：	**end for**

3.5 仿真实验与结果分析

3.5.1 仿真系统

Matpower 是一款开源的 Matlab 工具包，专门用于电力系统稳态分析[52]。这个软件主要用于解决电力系统稳态操作问题，包括潮流计算、最优潮流(Optimal Power Flow, OPF)、可行性研究和市场分析等。在 Matpower 中，预定义了一系列的标准节点电力系统，每个标准测试系统包含的数据通常包括节点(母线)信息、支路信息、发电机参数、负荷需求等。这些数据为 Matpower 提供了必要的输入，以执行各种电力系统分析任务。这些标准系统提供了不同规模和复杂性的电网模型，从而使研究人员和工程师能够在一个受控且一致的环境中测试他们的方法和算法。

本文利用 Matpower 7.1 工具箱执行连续最优潮流，以获得系统中状态和测量的真实值。同时，通过在真实测量值中添加平均值为 0、标准差为 0.015 的高斯噪声来获得实时量测值。大多数针对 FDIA 的研究都是在 IEEE 标准节点系统中进行仿真验证的，IEEE-14 标准节点系统如图 3-2 所示。

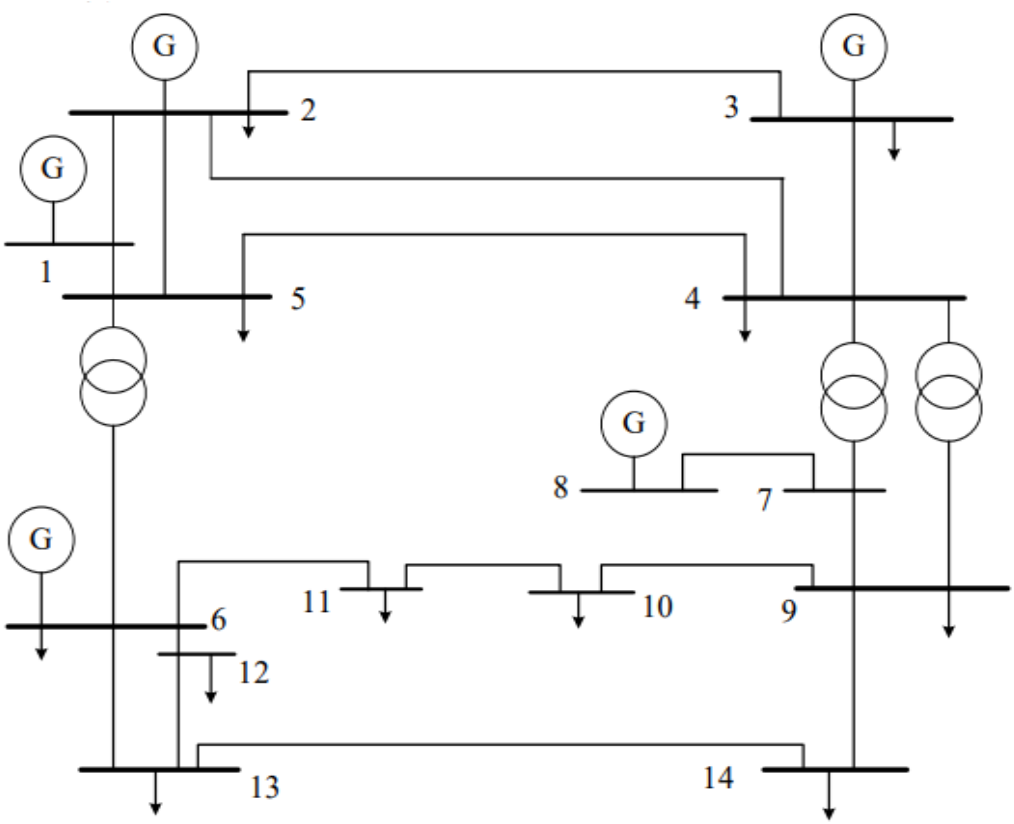


图 3-2 IEEE-14 标准节点系统图

在 IEEE-14 标准节点系统中，共 14 个节点，其中 1 号节点为平衡节点，20 条支路，5 台发电机和 11 个负载。在本章中，采用了系统中的 41 个量测值，分别为 1 个节点电压，8 个节点有功功率注入，8 个节点无功功率注入，12 个支路有功功率，12 个支路无功功率。IEEE-14 标准节点系统中的节点和支路功率如表 3-3 和表 3-4 所示。

表 3-3 IEEE-14 节点系统注入功率

量测数	节点i	有功功率P_i	无功功率Q_i
1	2	0.1830	0.3086
2	3	-0.9420	0.0608
3	7	0.00	0.00
4	8	0.00	0.1762
5	10	-0.0900	-0.0580
6	11	-0.0350	-0.0180
7	12	-0.0610	-0.0160
8	14	-0.1490	-0.0500

表 3-4 IEEE-14 节点系统支路功率

量测数	起始节点i	终止节点j	有功功率P_{ij}	无功功率Q_{ij}
1	1	2	1.5688	-0.2040
2	2	3	0.7324	0.0356
3	4	2	-0.5445	0.0302
4	4	7	0.2807	-0.2107
5	4	9	0.1608	-0.0658
6	5	2	-0.4061	-0.0210
7	5	4	0.6167	-0.1420
8	5	6	0.4409	-0.1982
9	6	13	0.1775	0.0722
10	7	9	0.2807	0.0578
11	11	6	-0.0730	-0.0344
12	12	13	0.0161	0.0075

IEEE-30 标准节点系统如图 3-3 所示。

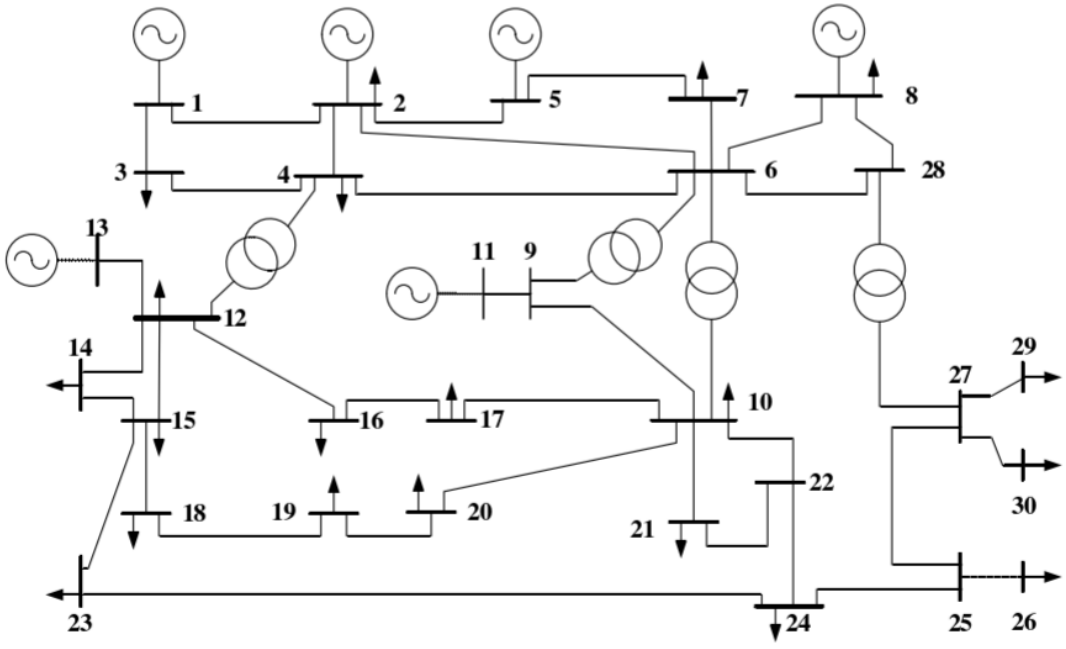


图 3-3 IEEE-30 标准节点系统图

在 IEEE-30 标准节点系统中，共 30 个节点，其中 1 号节点为平衡节点，41 条支路，6 台发电机和 20 个负载。在本章中，采用了系统中的 93 个量测值，分别为 1 个节点电压，18 个节点有功功率注入，18 个节点无功功率注入，28 个支路有功功率，28 个支路无功功率。IEEE-30 标准节点系统中的节点和支路功率如

表 3-5 和表 3-6 所示。

表 3-5 IEEE-30 节点系统注入功率

量测数	节点i	有功功率P_i	无功功率Q_i
1	4	-0.0760	-0.0160
2	5	-0.9420	0.1538
3	6	0.00	0.00
4	8	-0.3000	0.2096
5	10	-0.0580	-0.0200
6	11	0.00	0.2066
7	13	0.00	0.1483
8	14	-0.0621	-0.0160
9	15	-0.0819	-0.0250
10	16	-0.0350	-0.0180
11	18	-0.0320	-0.0090
12	20	-0.0220	-0.0070
13	21	-0.1750	-0.1120
14	24	-0.0870	-0.0670
15	25	0.00	0.00
16	26	-0.0350	-0.0230
17	28	0.00	0.00
18	29	-0.0240	-0.0090

表 3-6 IEEE-30 节点系统支路功率

量测数	起始节点i	终止节点j	有功功率P_{ij}	无功功率Q_{ij}
1	2	4	0.4377	0.0451
2	2	5	0.8213	0.0402
3	3	1	-0.8487	0.0577
4	4	3	-0.8160	0.0687
5	4	6	0.7161	-0.2202
6	5	7	-0.1475	0.1027
7	6	2	-0.5836	0.0624
8	7	6	-0.3772	0.0089
9	9	6	-0.2705	0.1463
10	10	6	-0.1539	0.0244

续表 3-6 IEEE-30 节点系统支路功率

11	10	9	-0.2705	-0.1599
12	12	14	0.0810	0.0327
13	15	12	-0.1786	-0.0977
14	15	18	0.0623	0.0310
15	16	17	0.0423	0.0420
16	17	10	-0.0480	-0.0167
17	19	20	-0.0623	-0.0133
18	20	10	-0.0844	-0.0205
19	21	10	-0.1760	-0.0973
20	21	22	0.00	0.00
21	22	10	-0.0554	-0.0361
22	23	24	0.0177	0.0248
23	24	22	-0.0549	-0.0353
24	25	27	-0.0500	-0.0309
25	27	28	-0.1832	-0.0219
26	28	6	-0.1883	0.0399
27	29	30	0.0370	0.0061
28	30	27	-0.0693	-0.0136

3.5.2 仿真数值分析

为了比较 WEKF 和 EKF 在系统受到 FDIA 影响时的状态估计性能，本节使用均方根误差(Root Mean Square Error, RMSE)来量化两个估计器的估计性能。RMSE 通过使用预测估计值与实际值之间的差异来计算两个估计器的估计误差。将节点估计的电压值与电网受到攻击时的实际电压值进行比较。RMSE 的公式定义为

$$\mathrm{RMSE}=\sqrt{\frac{1}{N}\sum_{j=1}^{N}(\hat{\boldsymbol{x}}_j-\boldsymbol{x}_j)^2} \tag{3.21}$$

式中，N 代表节点的数量；$\hat{\boldsymbol{x}}_j$ 是第 j 个节点的电压估计值；$\boldsymbol{x}_j$ 表示第 j 个节点的实际电压值。

根据第二章关于虚假数据注入攻击原理的详细介绍，本节针对 IEEE-14 节点

系统注入的虚假数据攻击向量为[53]

$$\boldsymbol{a}=\left[\Delta P_3,\Delta Q_3,\Delta P_{1-2},\Delta P_{2-3},\Delta P_{4-2},\Delta Q_{1-2},\Delta Q_{2-3},\Delta Q_{4-2}\right]^{\mathrm{T}} \tag{3.22}$$

在电网受到攻击后，运用不同的状态估计算法得到的各节点电压估计误差如表 3-7 中所示。表 3-7 表明，当电网遭受虚假数据注入攻击时，WEKF 表现出最小的估计误差，而采用 WLS 进行状态估计时的误差最大。综合来看，系统遭受攻击时，WEKF 在估计性能方面优于 WLS 和 EKF。

表 3-7 每个节点的电压幅值估计误差

节点	WLS	EKF	WEKF
1	8.23×10^{-2}	1.71×10^{-2}	-3.1×10^{-3}
2	10.20×10^{-2}	2.80×10^{-2}	5.3×10^{-3}
3	9.94×10^{-2}	2.23×10^{-2}	4.2×10^{-3}
4	12.14×10^{-2}	2.2×10^{-2}	5.1×10^{-3}
5	12.16×10^{-2}	2.50×10^{-2}	6.2×10^{-3}
6	11.47×10^{-2}	1.75×10^{-2}	7.5×10^{-3}
7	10.90×10^{-2}	2.50×10^{-2}	5.5×10^{-3}
8	11.44×10^{-2}	2.64×10^{-2}	5.8×10^{-3}
9	10.96×10^{-2}	1.87×10^{-2}	3.9×10^{-3}
10	10.94×10^{-2}	2.42×10^{-2}	6.1×10^{-3}
11	11.75×10^{-2}	2.37×10^{-2}	5.2×10^{-3}
12	11.64×10^{-2}	2.41×10^{-2}	3.7×10^{-3}
13	11.71×10^{-2}	1.97×10^{-2}	4.1×10^{-3}
14	12.05×10^{-2}	3.31×10^{-2}	7.2×10^{-3}

根据每个节点的电压幅值估计误差，状态估计的 RMSE 如表 3-8 所示。

表 3-8 电压幅值估计的 RMSE

算法	RMSE
WLS	0.1116
EKF	0.0575
WEKF	0.0054

表 3-8 表明，WEKF 计算出的 RMSE 明显低于 WLS 和 EKF。因此，在存在虚假数据注入攻击的情况下，WEKF 在估计性能上明显优于 WLS 和 EKF。

本节采用误差平方和法(The Sum of Squared Errors, SSE)来确定参数 τ_a 的数值。该误差是在没有 FDIA 的情况下，通过比较 WLS 和 WEKF 所估计的状态偏差而产生的。具体而言，确定 τ_a 的步骤如下：

（1）在没有 FDIA 的情况下，首先分别使用 WLS 和 WEKF 获取电网状态的估计值。然后计算这两个估计值之间的偏差，最终得到误差的二范数;

（2）其次，采用 Weibull 分布来拟合误差二范数的样本值[54];

（3）最后，利用误报率(False Positive Rate，FPR)来确定相应的阈值。

如图 3-4 所示，该图描述了在 IEEE-14 节点系统中确定检测阈值 τ_a 的方法。其中，绿色线为 WLS 和 WEKF 估计偏差的累计概率分布曲线，红色线为利用 Weibull 分布对绿色线进行拟合后得到的分布曲线。首先，需要确定误报率。然后，将(1−FPR)的值，即 0.95，作为垂直坐标的数值，以对应 Weibull 分布。最终，从 Weibull 分布曲线上获取对应的横坐标值，作为检测阈值，即 $\tau_a = 2.172$ 。

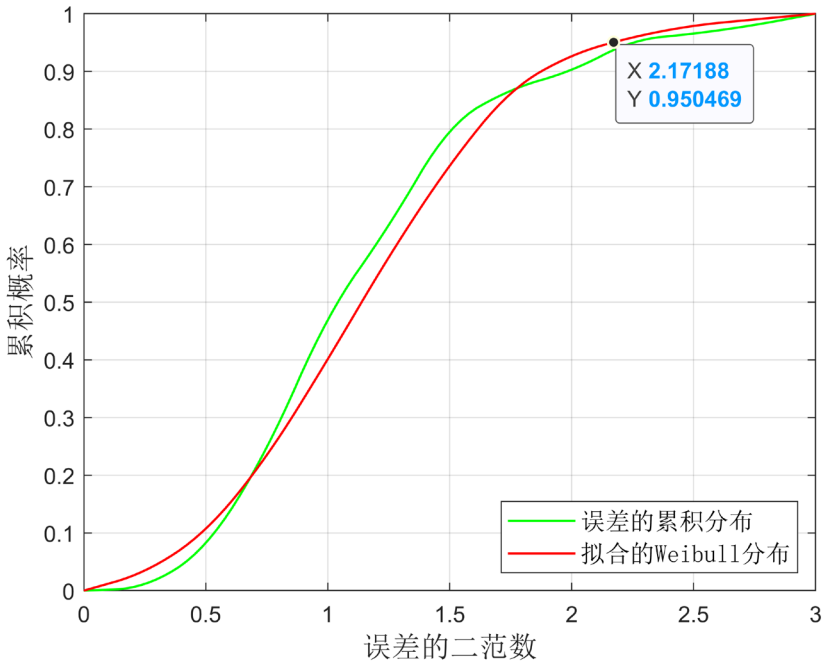


图 3-4 估计偏差二范数的拟合累积分布函数

本节通过向本地子网的测量数据中注入式(3.22)中的攻击向量来发起攻击。

以此，保持攻击向量的隐蔽性。

假定电力系统在前两个小时内未受到任何虚假数据注入攻击，而在第三小时开始受到攻击，此攻击持续影响。同时，能源管理系统每隔 30 秒进行一次量测值采样。IEEE-14 节点系统的各节点电压幅值和相位角在攻击前后的变化如图 3-5 和图 3-6 所示。

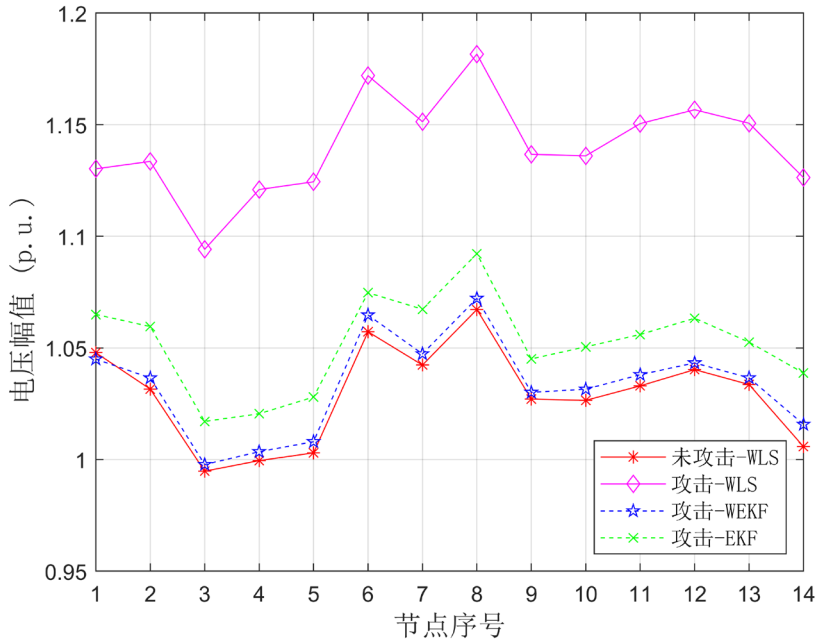


图 3-5 攻击前后每个节点的电压幅值估计值

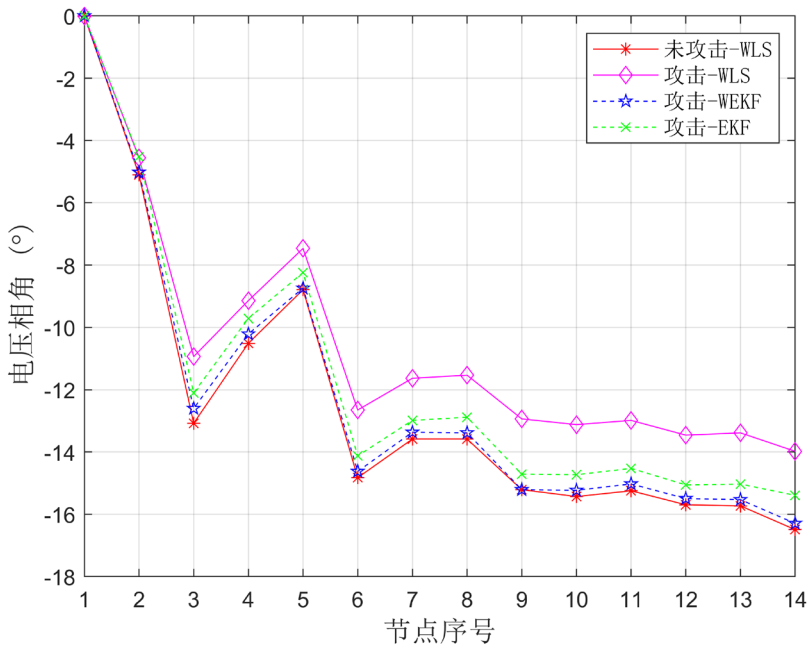


图 3-6 攻击前后每个节点的电压相角估计值

图 3-5 和图 3-6 表明了不同的估计算法在不同场景下的估计结果。在电力系统受到攻击后，WLS 算法的估计结果表现出明显的偏差，各节点的电压幅值相较于未受攻击时都有不同程度的增加。传统的 EKF 算法在受到攻击时的状态估计值也出现了轻微的偏差，这是由于 EKF 的递归特性所导致的。然而，值得注意的是，在系统受到攻击后，本章提出的 WEKF 算法的估计值偏差相对于其他两种估计方法最小。其估计结果与未受攻击时的估计值非常接近，这得益于 WEKF 能够根据攻击强度的大小自适应调整卡尔曼增益。这一事实证明了在面对 FDIA 时，WEKF 能够维持良好的状态估计性能。

在系统受到攻击前后使用 WLS 进行状态估计的残差结果如图 3-7 所示。根据计算，在未受到攻击时，WLS 的估计残差为 4.1572。然而，当系统受到攻击后，估计残差升高至 5.5671。因此，攻击前后的估计残差变化较为微小。IEEE-14 节点系统具有 41 个测量值和 27 个状态变量。因此，自由度可计算为 $c=m-n=14$。在设定了 0.95 的置信度水平下，通过查询卡方分布表，得到的不良数据检测阈值为 23.685。攻击后的残差值小于此阈值。此外，电压幅值和相位角在攻击后发生变化，因此基于 WLS 的不良数据检测方法无法检测到 FDIA 的存在。

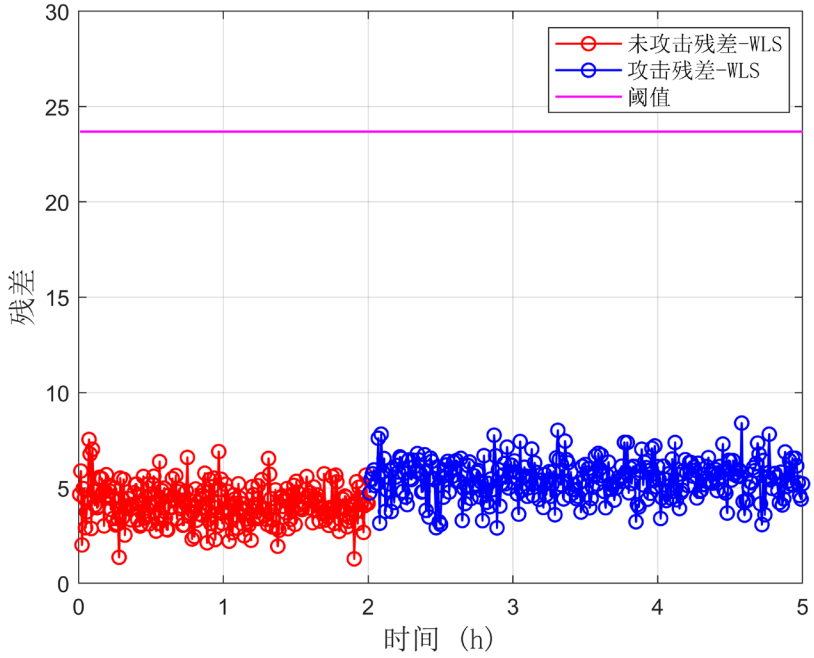


图 3-7 系统受到攻击前后 WLS 的估计残差

假设电力系统在前两个小时内正常运行，然后从第三个小时开始持续受到虚

假数据注入攻击。基于 WLS 和 WEKF 这两种状态估计方法，在攻击前后 5 号节点的电压幅值和相位角的状态估计变化过程如图 3-8 和图 3-9 所示。

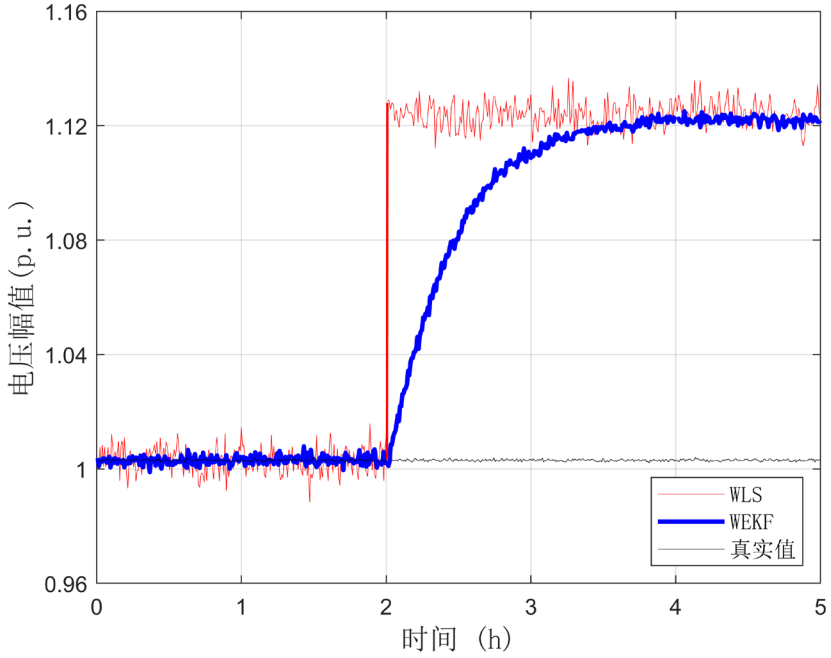


图 3-8 攻击前后 5 号节点电压幅值变化过程

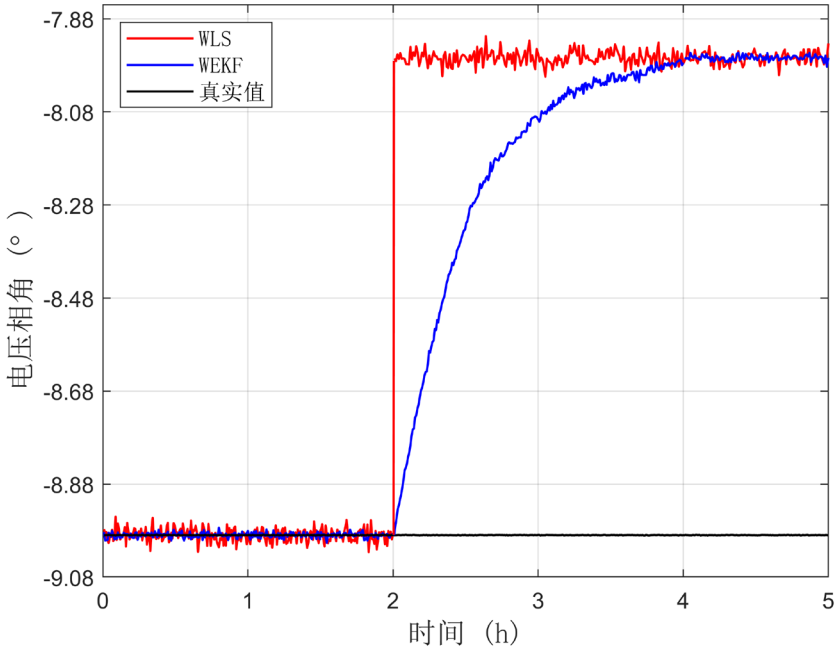


图 3-9 攻击前后 5 号节点电压相角变化过程

由于传统的 WLS 是一种基于当前测量值的静态状态估计方法，因此当 FDIA 在第三个小时发生时，WLS 会快速做出响应。然而，WEKF 则采用了一种递归的方法，能够根据预测估计的残差自适应地调整卡尔曼增益。此外，WEKF 的当前状态估计值是通过历史数据和当前测量值的联合计算而得出的。当 FDIA 事件

发生时，WEKF 中涉及一个状态调整的过程。因此，可以通过比较两种方法获得的状态估计值偏差来检测 FDIA 事件的发生。

在电力系统运行过程中，当不存在 FDIA 时，利用式(3.17)进行一致性检验的结果为 0.7426。然而，当 FDIA 确实存在时，一致性检验的结果升高至 19.361。值得注意的是，一致性检验的阈值 τ_a 已事先设定为 2.172。由此可见，经过攻击后，一致性检验的结果明显超过了事先设定的阈值。为了排除由于发电机或负载突然变化引起的误检测，进一步使用式(3.18)对 WEKF 的状态估计结果进行残差检验。WEKF 估计的残差检验结果为 31.614，明显高于预先设定的阈值 23.685。这一结果进一步证明了 FDIA 的存在，并排除了突变干扰的可能性。总结而言，当电力系统中存在 FDIA 事件时，无论是一致性检验还是残差检验的结果都明显高于相应的预设阈值，因此可以确定 FDIA 事件的存在。

为了深入验证所提出的方法在 IEEE-30 节点系统中的有效性和适用性，本节进一步进行了仿真实验。图 3-10 和图 3-11 表明了在受到攻击前后，使用不同估计算法获得的各个节点的状态估计值。

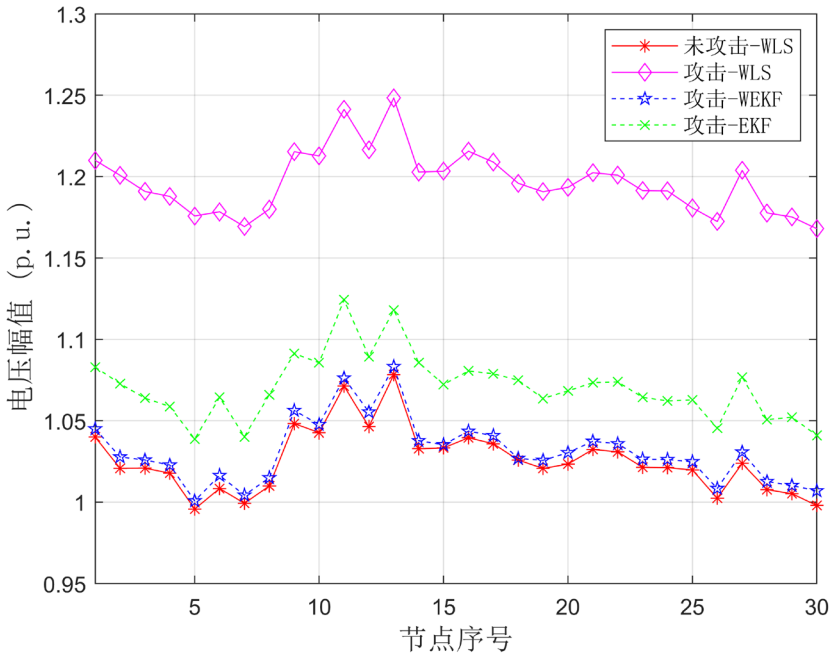


图 3-10 攻击前后每个节点的电压幅值估计值

仿真结果显示，尽管系统遭受攻击，WEKF 仍然能够保持良好的估计性能，但传统的基于 WLS 的状态估计值偏离了正常值。在进行仿真时，IEEE-30 节点系统具有 93 个测量值和 59 个状态变量。因此，自由度可计算为 $c = m - n = 34$。

在设定了 0.95 的置信度水平下，通过查询卡方分布表，确定了检测阈值为 48.602。此外，在受到攻击后，WLS 的估计残差从 4.624 增加到 5.867，仍然低于阈值。这表明传统的不良数据检测算法无法有效检测到此类攻击。为了检测 FDIA 事件，首先使用公式(3.17)进行一致性检验。在没有 FDIA 事件发生时，一致性检验的结果为 1.844。然而在攻击注入时，一致性检验结果却显著增加至 20.961。鉴于一致性检验的阈值为 3.216，因此攻击后的一致性检验结果明显高于该阈值。为了排除外部条件的干扰，进一步使用公式(3.18)进行残差检验。WEKF 估计值的残差检验结果为 54.622，远高于阈值 48.602，不符合等式(3.18)的条件。因此，可以确定 FDIA 事件确实存在，而不是由于突变干扰所引起的。

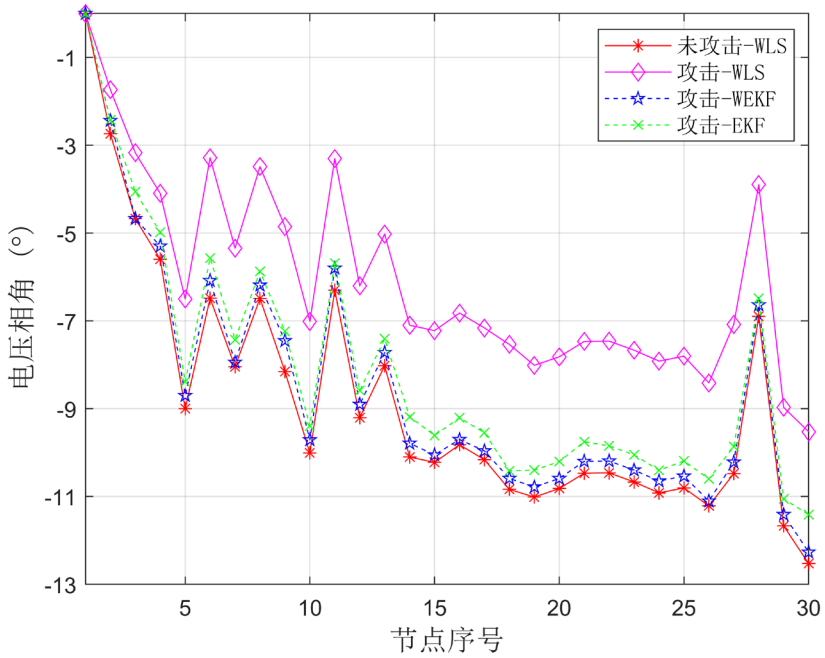


图 3-11 攻击前后每个节点的电压相角估计值

综上所述，通过使用公式(3.17)和公式(3.18)，可以有效地检测到 FDIA 事件，这进一步验证了所提出方法的有效性和适用性。

为了定位 FDIA 的位置，本节在 IEEE-14 节点系统中进行了仿真实验。在没有 FDIA 事件的情况下，目标函数 $J(\hat{\boldsymbol{x}})$ 的值小于 IEEE-14 节点系统的检测阈值。在这种情况下，使用 WLS 和 WEKF 进行状态估计，它们的估计偏差非常小，不足以触发系统的区域划分。

首先，采用公式(3.17)和公式(3.18)来确认 FDIA 的存在。随后，系统触发分区操作，将整个系统划分为三个子系统。这种分区方法旨在更好地维护每个子系

统中几乎相同的冗余度。系统被划分为三个部分，如图 3-12 所示。

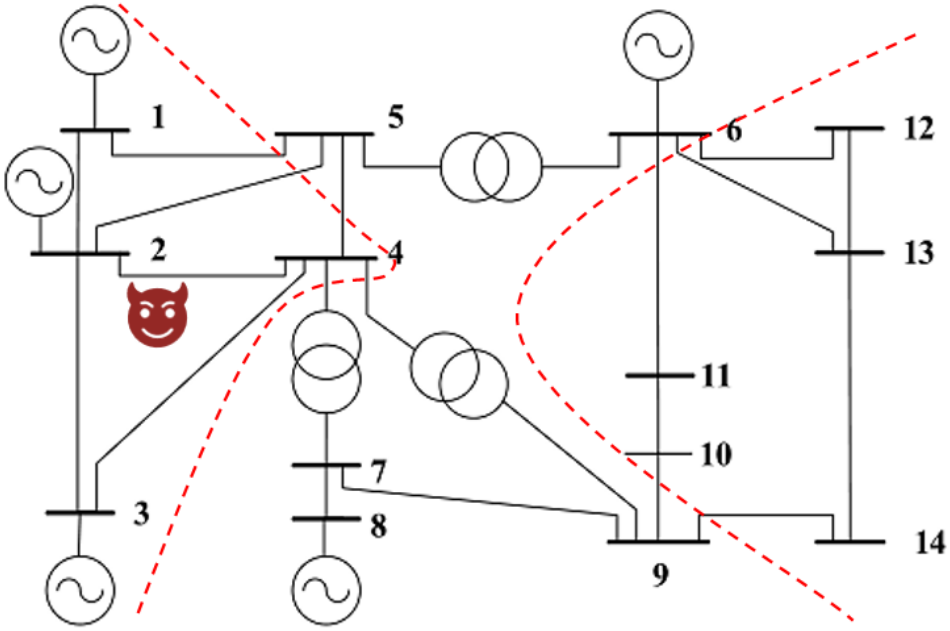


图 3-12 IEEE-14 节点系统划分图

最后，对每个子系统分别进行卡方检验，各子系统的目标函数值 $J(\hat{x})$ 和检测阈值 χ^2 如表 3-9 所示。由于子系统 2 和 3 未受到攻击，因此它们的目标函数值 $J(\hat{x})$ 均小于卡方检验阈值 χ^2 。

表 3-9 子系统卡方检测

子系统	$J(\hat{x})$	阈值 χ^2
1	20.145	12.592
2	6.473	9.488
3	7.811	9.488

具体来说，子系统 2 和 3 的目标函数值分别为 6.473 和 7.811，都小于卡方检验阈值 9.488。然而，子系统 1 的目标函数值 20.145 大于卡方检测阈值 12.592，这表明在该子系统中存在 FDIA 事件。通过仿真实验的结果表明，本章提出的方法能够有效地检测和定位攻击所在的区域。

当式(3.17)和式(3.18)的计算结果均超过相应的阈值时，将触发警报并报告检测到 FDIA 事件的存在。为了验证在不同攻击强度下 WEKF 和传统 EKF 的检测性能，定义了启动和停止警报之间的时间间隔来评估其性能。不同攻击强度下的

时间间隔如图 3-13 所示。

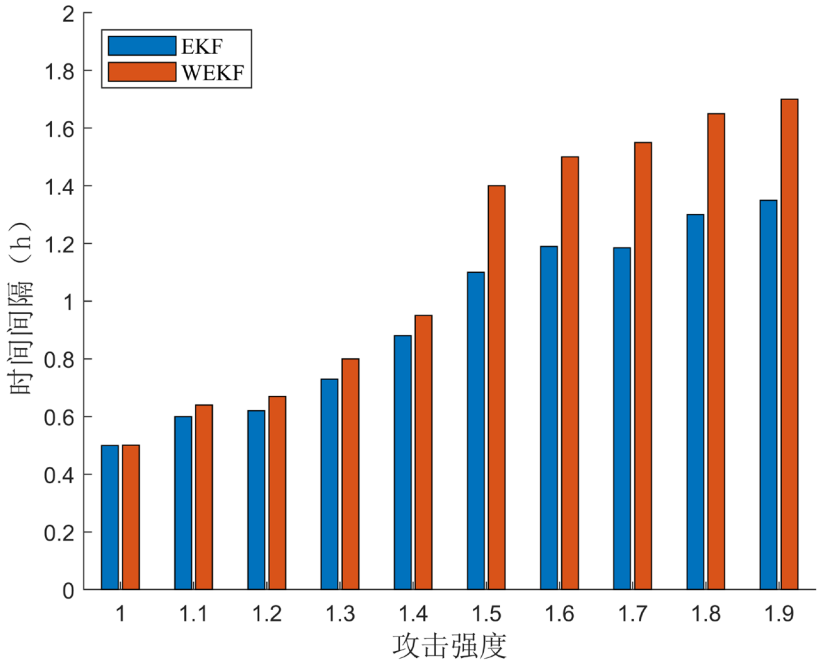


图 3-13 不同攻击强度时的检测性能比较

随着攻击强度的增加，本章提出的 WEKF 检测方法相对于传统的 EKF 检测方法表现出更佳的检测性能。这一结果的主要原因在于，随着攻击强度的提高，WEKF 能够自适应地抑制 FDIA，从而导致两种估计方法的估计值差异增大。这使得 WLS 和 WEKF 的状态估计值之间的差异不断增加，进一步提高了对 FDIA 事件的检测概率。

3.6 本章小结

本章讨论了一种在电力系统中检测和定位 FDIA 的方法，该方法采用了联合动态和静态估计，以及电力网划分的方法。首先强调了 FDIA 在电网运行中的破坏性。接着提出了一种改进的 EKF 方法，该方法可以自适应调节卡尔曼滤波增益以实现更为稳健的状态估计。随后，介绍了一种基于 WLS 和 WEKF 的 FDIA 检测技术，该技术利用一致性检验和卡方检验。此外，为了定位 FDIA，还引入了一种系统划分方法，并通过模拟实验来验证所提方法的有效性。

第 4 章 基于 EKF 和数据补偿的智能电网异常值检测和状态校正策略

4.1 引言

目前大多数研究主要集中在如何检测 CPPS 中的 FDIA，这是理解和确保系统的安全性的关键方面。然而，与检测攻击相比，更加关键的是及时恢复受到攻击的测量值和状态估计值，尤其是对于 CPPS 这类关键基础设施而言。攻击后的恢复过程在 CPPS 中至关重要，因为它直接涉及到电力系统的运行和控制。如果不及时采取校正措施，攻击可能导致电力系统出现严重的问题，包括电力质量下降、设备损坏甚至系统崩溃。因此，及时识别受到攻击的测量值和状态估计，并采取有效的恢复措施，对于确保电力系统的连续可靠运行至关重要。

本章将研究利用状态偏差指数和相应的阈值来检测异常值。同时，为了及时恢复测量值和校正状态估计值，提出了一种基于滑动窗口的数据补偿和状态校正策略，通过补偿后的测量结果重建系统的状态方程和测量方程，进一步利用重建后的方程进行状态估计，实现量测值补偿和状态校正的目的。

4.2 基于自适应调节平滑参数的指数平滑法

在状态转移方程中，采用广泛应用于短期负荷预测的 Holt 双参数指数平滑法。这种方法利用两个常数系数以及前一时刻状态量的预测值和估计值的组合，对两个状态值赋予不同的权重，从而得到当前时刻状态量的预测值。借助霍尔特双参数指数平滑技术，可以将式(3.1)中的状态转移函数 $f(\cdot)$ 表示为

$$\begin{cases} f(\boldsymbol{x}_k)=\tilde{\boldsymbol{x}}_{k+1}=\boldsymbol{a}_k+\boldsymbol{b}_k \\ \boldsymbol{a}_k=\alpha\hat{\boldsymbol{x}}_k+(1-\alpha)\tilde{\boldsymbol{x}}_k \\ \boldsymbol{b}_k=\beta(\boldsymbol{a}_k-\boldsymbol{a}_{k-1})+(1-\beta)\boldsymbol{b}_{k-1} \end{cases} \tag{4.1}$$

式中，$\boldsymbol{a}_k$ 和 $\boldsymbol{b}_k$ 分别表示水平和垂直分量；$\tilde{\boldsymbol{x}}_k$ 和 $\hat{\boldsymbol{x}}_k$ 分别表示 k 时刻的预测状态向量和状态估计向量；α 和 β 分别表示预设的平滑参数。

由于式(4.1)中的平滑参数α和β是固定的，因此当系统模式发生变化时，其预测估计值的误差会发生较大的变化。为了根据预测误差的大小自适应地调整平滑参数，本文采用式(4.2)中的时变参数模型。

$$\begin{cases} f(\boldsymbol{x}_k)=\tilde{\boldsymbol{x}}_{k+1}=\boldsymbol{a}_k+\boldsymbol{b}_k \\ \boldsymbol{a}_k=\alpha_k\hat{\boldsymbol{x}}_k+(1-\alpha_k)\tilde{\boldsymbol{x}}_k \\ \boldsymbol{b}_k=\beta_k(\boldsymbol{a}_k-\boldsymbol{a}_{k-1})+(1-\beta_k)\boldsymbol{b}_{k-1} \end{cases} \tag{4.2}$$

式中，α_k和β_k是时变参数。这两个时变参数的具体确定方法如下所述。

首先，在步骤k中选择三组值：中心值是α_0和β_0，低值是α_L和β_L，高值是α_H和β_H。这些值之间的关系可以表示为

$$\begin{cases} \alpha_L=\alpha_0-\Delta\alpha,\alpha_H=\alpha_0+\Delta\alpha \\ \beta_L=\beta_0-\Delta\beta,\beta_H=\beta_0+\Delta\beta \end{cases} \tag{4.3}$$

式中，$\Delta\alpha$和$\Delta\beta$是预定义的值。利用式(4.3)可以得到五种组合，对应于式(4.4)中的N^1-N^5。

$$\begin{aligned} &N^1=(\alpha_0,\beta_0)\quad N^2=(\alpha_L,\beta_L) \\ &N^3=(\alpha_H,\beta_H)\ N^4=(\alpha_H,\beta_L) \\ &N^5=(\alpha_L,\beta_H) \end{aligned} \tag{4.4}$$

其次，利用式(4.4)中的五种平滑参数组合N^j，生成五种与之对应的预测状态值$\tilde{\boldsymbol{x}}_{k+1}^j$。每个预测状态值和状态估计值之间的误差和均方误差可由式(4.5)和式(4.6)计算得到。

$$e_{k+1}^j(i)=\hat{x}_{k+1}^j(i)-\tilde{x}_{k+1}^j(i),i=1,\ldots,n;j=1,\ldots,5 \tag{4.5}$$

$$S_j=\frac{1}{n}\sum_{i=1}^{n}(e_{k+1}^j(i))^2,j=1,\ldots,5 \tag{4.6}$$

最后，可以通过最小化S_j得到预测估计误差最小的组合N^j，并进一步确定其对应的α和β值。具体的实现方法为

$$S_p=\min\left\{S_j\right\},j=1,\ldots,5 \tag{4.7}$$

该方法通过根据预测误差的大小实时调整平滑参数，维持预测估计值的准确

性，最终进一步提高状态估计的精度。自适应调整平滑参数的具体实现流程如图4-1 所示。

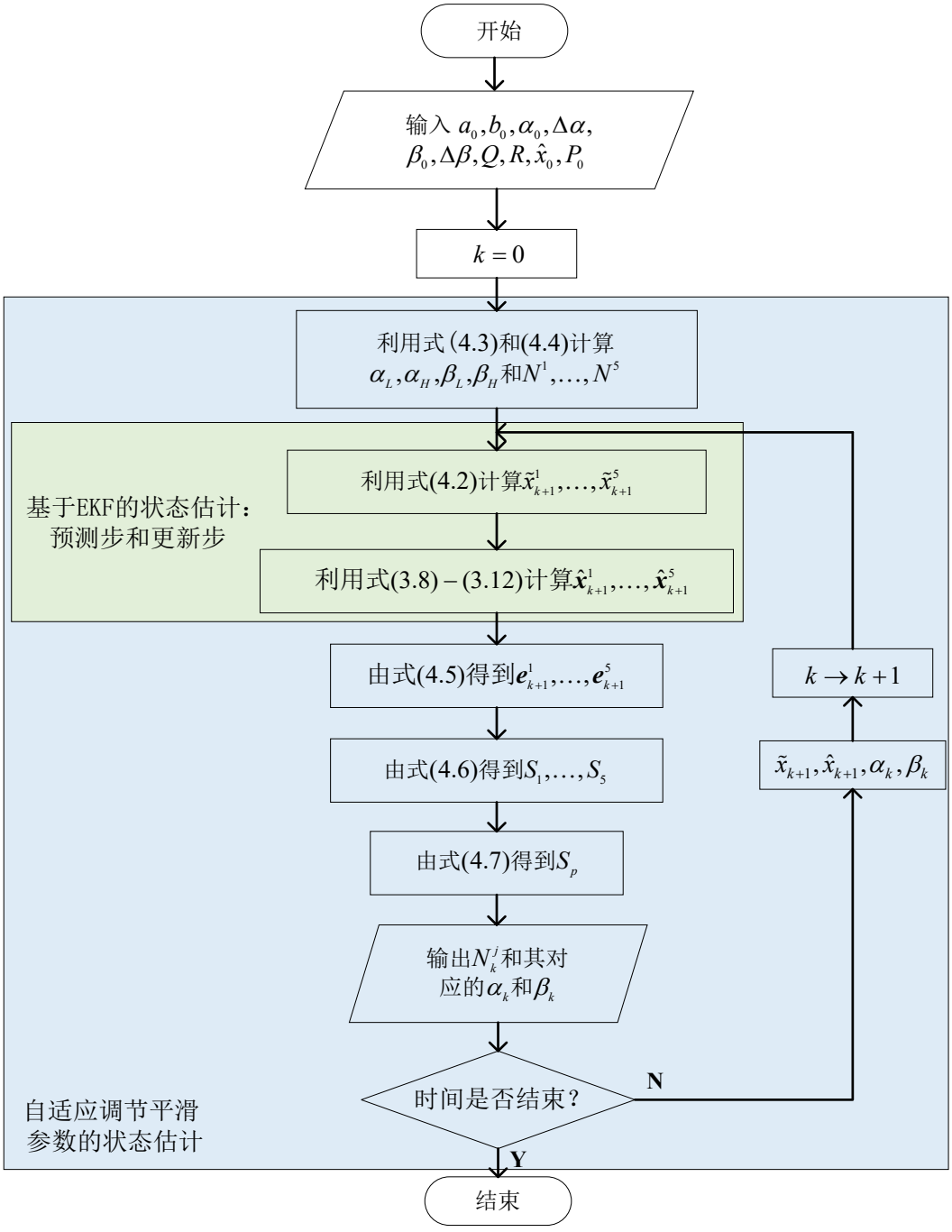


图 4-1 具有自适应调整平滑参数的辅助预测状态估计流程图

考虑系统噪声，状态转移模型的一般形式可以导出为

$$\boldsymbol{x}_{k+1}=\boldsymbol{F}_k\boldsymbol{x}_k+\boldsymbol{U}_k+\boldsymbol{w}_k \tag{4.8}$$

从式(4.2)到式(4.8)可以得到式(4.9)

$$\begin{cases} \boldsymbol{F}_k = \alpha_k(1+\beta_k)\boldsymbol{I} \\ \boldsymbol{U}_k = (1+\beta_k)(1-\alpha_k)\tilde{\boldsymbol{x}}_k - \beta_k \boldsymbol{a}_{k-1} + (1-\beta_k)\boldsymbol{b}_{k-1} \end{cases} \tag{4.9}$$

因此，利用式(4.9)计算状态转移矩阵 $\boldsymbol{F}_k$ 和参数向量 $\boldsymbol{U}_k$，避免了 $\boldsymbol{F}_k$ 和 $\boldsymbol{U}_k$ 难以获得的困难[55]。这将进一步应用于基于 EKF 的状态估计中，以解决状态估计预测步中的状态预测问题。

在 EKF 算法过程中，采用自适应调整参数的霍尔特指数平滑方法获得的预测估计值作为预测步骤。然后将 EKF 算法获得的状态估计和先前的预测估计值用于式(4.5)、(4.6)和(4.7)中，以获得最适合当前系统运行模式的平滑参数。通过执行上述步骤来提高状态估计的准确性，具体实现步骤如图 4-1 所示。

4.3 异常值检测和状态校正

在第三章中，我们采用了一种状态偏差的方法，通过一致性检验和卡方检验有效地检测 FDIA。由于此方法对两种估计器得到的估计向量求范数，所以不能检测到状态估计向量中受到攻击的特定条目。因此，需要进一步采用额外的方法才能定位到 FDIA。此外，在系统中存在负载突变(Sudden Load Changes, SLC)和 FDIA 的情况下，该方法尚未提供校正系统状态的方案。

鉴于此，为进一步改进第三章中的检测方法，本章提出了一种利用状态偏差指数(State Deviation Index, SDI)的异常值检测方法。该方法可以检测到受异常值影响的具体状态向量条目。为了进一步补偿被篡改的量测值和校正被篡改的状态值，提出了一种带有滑动窗口的数据补偿策略来补偿测量值。然后，利用补偿后的测量数据重建系统的状态方程和测量方程。最终，实现对测量值的补偿和系统状态的校正。

4.3.1 基于状态偏差指数的异常值检测

首先，利用 WLS 和 EKF 对 SCADA 系统中采集的测量数据进行状态估计。接着，基于 WLS 估计值执行卡方检验，以检测系统中可能存在的不良数据。如果卡方检验结果超过其设定的阈值，则检测到不良数据的存在并发出警报。然而，需要注意的是，当系统中同时存在 FDIA 和 SLC 时，基于 WLS 的卡方检验可能

无法检测到这些异常的存在。在这种情况下，检测过程会转向基于状态偏差的异常值识别方法。

WLS 方法基于电力系统状态估计的实时测量数据，而不考虑历史状态的演变。与此不同，EKF 方法则基于电力系统的历史和实时数据进行状态估计，综合考虑了系统的时变性和动态行为。然而，在系统同时存在 FDIA 和 SLC 的情况下，使用这两种估计方法得到的估计值会出现偏差。因此，通过比较状态偏差与相应阈值的关系，可以有效地检测此类异常情况[56]。状态偏差指数(State Deviation Index, SDI)表示为

$$\mathrm{SDI}_i = \frac{\left|\hat{x}_i^{\mathrm{WLS}} - \hat{x}_i^{\mathrm{EKF}}\right|}{\sqrt{q_{ii}}} \quad i = 1, 2, \ldots, n \tag{4.10}$$

式中，$\hat{x}_i^{\mathrm{WLS}}$ 表示 WLS 估计的第 i 个状态变量；$\hat{x}_i^{\mathrm{EKF}}$ 表示 EKF 估计的第 i 个状态变量；q_{ii} 是状态估计误差协方差矩阵的第 i 个对角元素。如果 $\max\{\mathrm{SDI}_i\} \geq \tau$，则系统中存在 FDIA 和 SLC。这里，$\tau$ 是检测阈值。

对于检测阈值 τ 的设定，本章采用蒙特卡罗模拟方法进行确定。在系统中存在 FDIA 和 SLC 的情况下，WLS 和 EKF 的估计值会出现偏差。基于这一观察，进行了电力系统在安全条件下的蒙特卡罗仿真实验，并使用最大的 SDI_i 作为检测阈值 τ，以区分安全场景和异常场景。具体而言，计算安全场景下 WLS 和 EKF 的 SDI_i。然后，通过进行 1000 次蒙特卡罗模拟实验，并将最大 SDI_i 设置为检测阈值 τ。这种方法的优势在于它可以根据系统的实际情况和性能要求来确定适当的检测阈值，从而更有效地应对不同的异常场景。

首先，使用 WLS 和 EKF 方法对 SCADA 系统中的测量值进行状态估计。然后，将 WLS 输出的估计值用于卡方检验。如果测量中存在 BD，卡方检验的结果将超过其设定的阈值，并触发警报。然而，如果系统同时存在 FDIA 和 SLC，卡方检验可能无法检测到异常的存在。在这种情况下，检测过程会继续到基于状态偏差的检测阶段。在这个阶段，WLS 和 EKF 获得的状态估计值被用于计算 SDI_i。当 $\max\{\mathrm{SDI}_i\}$ 超过特定的阈值时，将检测到异常情况，否则系统将被认为处于正常状态。

4.3.2 量测补偿和状态校正

在电力系统的正常和稳态运行过程中，测量值和状态的变化非常缓慢，因此电网中的数据在一段时间内变化很小或几乎不变。为了有效降低 FDIA 和 SLC 所造成的错误估计影响，使用最新接收到的与被攻击状态相关的正常测量向量的条目来替换异常量测值。假设在$k-b$时刻之前的测量中没有异常，且攻击者最多连续发起b次攻击。那么攻击范围在$k-b+1$和k之间，最多发起b次攻击。为了记录测量值$\boldsymbol{z}_k,\boldsymbol{z}_{k-1},\ldots,\boldsymbol{z}_{k-b+1},\boldsymbol{z}_{k-b}$，定义了向量$\boldsymbol{l}_k\in\mathbb{R}^{1\times(b+1)}$。这里，$l_k(j)$是向量$\boldsymbol{l}_k$的第$j$个元素，对应于时刻$k-j+1$，$j\in[1,b+1]$时的测量值$\boldsymbol{z}_{k-j+1}$。如果$l_k(j)=0$，则$k-j+1$时刻的测量向量为异常，否则$l_k(j)=1$，则$k-j+1$时刻的测量向量为正常数据。具体判定方法为

$$l_k(j)=\begin{cases}0 & \boldsymbol{z}_{\text{k-j+1}}\text{为异常}\\ 1 & \boldsymbol{z}_{\text{k-j+1}}\text{为正常}\end{cases} \tag{4.11}$$

有了$\boldsymbol{l}_k$，可以确定$\boldsymbol{z}_k,\boldsymbol{z}_{k-1},\ldots,\boldsymbol{z}_{k-b+1},\boldsymbol{z}_{k-b}$是否异常。例如，当$l_k(1)=l_k(3)=0$时，则$\boldsymbol{z}_k$和$\boldsymbol{z}_{k-2}$是异常值。$\boldsymbol{l}_k$中从第一个元素开始连续零的数量可以确定连续量测向量为异常的数量。因此，λ_k用于记录连续异常量测向量的数目，$\lambda_k\in[0,b]$。

为了减少异常对状态估计的影响，该方法采用异常发生前最近时刻的正常量测向量的条目来补偿与异常状态相关的量测值条目。这使得状态估计的校正过程成为可能。因此，定义向量$\boldsymbol{L}_k\in\mathbb{R}^{1\times(b+1)}$来识别可以补偿异常值的最近的正常测量时间。对于向量$\boldsymbol{L}_k$，只有元素$L_k(\lambda_k+1)$设置为 1，其他元素设置为 0。例如，当$\boldsymbol{l}_k=[0\ 0\ 1\ 1]$时，表明$\boldsymbol{z}_k$和$\boldsymbol{z}_{k-1}$为异常数据，而$\boldsymbol{z}_{k-2}$和$\boldsymbol{z}_{k-3}$是正常数据。此时，$\boldsymbol{l}_k$中前两个元素为 0，第三个元素为 1，因此$\lambda_k=2$，$\lambda_k+1=3$，$\boldsymbol{L}_k=[0\ 0\ 1\ 0]$，即$\boldsymbol{z}_k$被$\boldsymbol{z}_{k-2}$补偿。

注意，$\boldsymbol{l}_k$是一个滑动窗口，只考虑$\boldsymbol{z}_k$在时刻k的状态，即$\boldsymbol{z}_{k-1}$在$k-1$时刻已经被$\boldsymbol{z}_{k-3}$补偿。此外，为了最小化异常值对状态的影响并保持状态估计的时效性，本节中补偿的测量值与受攻击状态的测量相关。例如，当 IEEE-14 节点系统中的第 14 节点的电压幅值受到攻击时，则与第 14 节点的电压幅值相关的测量值被补偿，而与其他未受攻击状态相关的测量值继续用于状态估计。

因此，当使用式(4.10)在 k 时刻检测到异常事件时，用于状态估计的测量值可以由式(4.12)更新。

$$\boldsymbol{z}_{i,k}^{c} = \boldsymbol{L}_k[\boldsymbol{z}_{i,k}\ \boldsymbol{z}_{i,k-1}\cdots\boldsymbol{z}_{i,k-d}]^T = \boldsymbol{z}_{i,k-\lambda_k}, i \in \Psi_x \tag{4.12}$$

式中，$\boldsymbol{z}_{i,k}^{c}$ 是在 k 时刻与状态 x 相关的补偿量测值；Ψ_x 是与状态 x 相关测量的索引集合。

为了进一步说明在数据传输过程中存在异常时对量测值进行补偿的过程，假设连续出现异常的最大次数为 $d=3$，测量值出现异常时的补偿如表 4-1 所示。

表 4-1 系统中的量测值传输补偿

k	$l_k(1)$	$l_k(2)$	$l_k(3)$	λ_k	$k-\lambda_k$	$\boldsymbol{z}_{i,k}^{c}$
1	1	0	1	0	1	$\boldsymbol{z}_{i,1}^{c}$
2	1	1	0	0	2	$\boldsymbol{z}_{i,2}^{c}$
3	0	1	1	1	2	$\boldsymbol{z}_{i,2}^{c}$
4	0	0	1	2	2	$\boldsymbol{z}_{i,2}^{c}$
5	0	0	0	3	2	$\boldsymbol{z}_{i,2}^{c}$
6	1	0	0	0	6	$\boldsymbol{z}_{i,6}^{c}$
7	1	1	0	0	7	$\boldsymbol{z}_{i,7}^{c}$
8	0	1	1	1	7	$\boldsymbol{z}_{i,7}^{c}$
9	0	0	1	2	7	$\boldsymbol{z}_{i,7}^{c}$
10	1	0	0	0	10	$\boldsymbol{z}_{i,10}^{c}$
11	0	1	0	1	10	$\boldsymbol{z}_{i,10}^{c}$
12	1	0	1	0	12	$\boldsymbol{z}_{i,12}^{c}$
13	0	1	0	1	12	$\boldsymbol{z}_{i,12}^{c}$
14	1	0	1	0	14	$\boldsymbol{z}_{i,14}^{c}$

表 4-1 中表明，测量值 $z_{i,1}, z_{i,2}, z_{i,6}, z_{i,7}, z_{i,10}, z_{i,12}$ 和 $z_{i,14}$ 是正常的，而测量值 $z_{i,3}, z_{i,4}, z_{i,5}, z_{i,8}, z_{i,9}, z_{i,11}, z_{i,13}$ 和 $z_{i,13}$ 为异常值，其中 $z_{i,3}, z_{i,4}$ 和 $z_{i,5}$ 为连续 3 次异常值。同时，相应的异常通过表 4-1 最后一列中的量测 $z_{i,k}^{c}$ 进行补偿。

当使用式(4.10)检测到异常时，进一步使用式(4.12)补偿量测方程(3.2)中的异常测量值。补偿后的测量结果为

$$\boldsymbol{z}_k^c = \boldsymbol{h}(\boldsymbol{x}_{k-\lambda_k}) + \boldsymbol{v}_{k-\lambda_k} \tag{4.13}$$

在 FDIA 和 SLC 存在的情况下，使用式(4.12)补偿量测结果，重建的状态方程和测量方程分别为

$$\boldsymbol{x}_k = \boldsymbol{f}(\boldsymbol{x}_{k-1}, \boldsymbol{u}_{k-1}) + \boldsymbol{w}_{k-1} \tag{4.14}$$

$$\boldsymbol{z}_k^c = \boldsymbol{h}(\boldsymbol{x}_{k-\lambda_k}) + \boldsymbol{v}_{k-\lambda_k} \tag{4.15}$$

注意，式(4.12)中的 $z_{i,k}^{c}$ 与式(4.15)中的 $\boldsymbol{z}_k^c$ 不同。$z_{i,k}^{c}$ 仅与状态向量中受攻击状态的条目相关联。然而，$\boldsymbol{z}_k^c$ 中的条目不仅包括补偿的测量条目，还包括与正常状态相关的正常测量条目。

当检测到异常值存在时，利用重构的状态方程和测量方程对电力系统进行状态估计。这样就实现了异常事件下的状态校正，从而减少了异常值对状态估计的破坏。同时，仅对量测向量中与污染状态相对应的特定条目进行补偿可以最大限度地保持状态估计的时效性。

因此，异常检测和状态校正方法的具体执行过程如表 4-2 所示。

表 4-2 基于 EKF 和数据补偿的智能电网异常值检测和状态校正策略流程

算法：异常检测和状态估计校正方案
输入：噪声协方差矩阵 $\boldsymbol{Q}$ 和 $\boldsymbol{R}$；初始状态 $\hat{\boldsymbol{x}}_0$ 和估计误差协方差矩阵 $\boldsymbol{P}_0$；检测阈值 τ
输出：检测到的异常值和修正后的状态估计值
1：**for** $k = 1:N$，其中 N 代表时间断面数 **do**
2：　获取测量向量 $\boldsymbol{z}_k$ 并确定雅可比矩阵 $\boldsymbol{H}_k$
3：　利用自适应调节平滑参数算法中的式(4.2)得到 k 时刻的预测状态 $\tilde{\boldsymbol{x}}_k$

续表 4-2 基于 EKF 和数据补偿的智能电网异常值检测和状态校正策略流程

4：	由式(2.7)，计算 k 时刻 WLS 的状态估计向量 $\hat{\boldsymbol{x}}_k^{WLS}$
5：	由式(3.10)，计算 k 时刻 EKF 的状态估计向量 $\hat{\boldsymbol{x}}_k^{EKF}$
6：	**if** $J(\hat{\boldsymbol{x}}) \geq \chi^2_{(m-n),p}$ **then**
7：	系统中存在不良数据
8：	**else**
9：	系统中无不良数据
10：	**end if**
11：	**if** $\max\{\mathrm{SDI}_i\} \geq \tau$ **then**
12：	系统中存在异常值
13：	由式(4.12)补偿的测量值为 $\boldsymbol{z}_{i,k}^c$
14：	重构的状态方程(4.14)和量测方程(4.15)用于状态估计
15：	**else**
16：	系统量测值无异常
17：	**end if**
18：	**end for**

4.4 仿真实验和结果分析

4.4.1 仿真系统

在本章中，所提出的异常检测和状态校正方法分别在 IEEE-14 节点系统和 IEEE-30 节点系统中进行测试。此外，进一步描述了本章提出的量测补偿和状态校正算法的实施效率。讨论了该算法在更复杂的电力系统模型中的可扩展性。SCADA 系统中的测量值包括节点电压幅度、有功和无功功率注入以及支路有功和无功功率。另外，在 SCADA 系统中，测量的采样周期设置为 2 秒，即 k 和 k+1 之间的时间间隔为 2 秒。Matpower 7.1 工具箱用于执行连续最优潮流，以获得系统中状态和测量的真实值。同时，通过在真实量测值中添加平均值为 0、标准差为 0.01 的高斯噪声来获得实时量测值。对于不良数据，相应的测量结果会受到

不属于预定义高斯分布的随机误差的影响。通过根据攻击向量修改相应的量测值，在系统上启动 FDIA[53]。SLC 的建模可以通过在执行最优潮流时减少指定的负载量来实现。

为了评估状态估计校正的性能，本节使用均方根误差(Root Mean Square Error, RMSE)和相对误差(Relative Error, RE)来量化。每个采样时刻的 RMSE，以及 RE 的最大值和平均值分别为

$$\mathrm{RMSE}(k)=\sqrt{\frac{1}{n}\sum_{i=1}^{n}(\hat{x}_{k,i}-x_{k,i}^{\text{pre-attack}})^2},i\in n \tag{4.16}$$

$$\mathrm{MAX}^{\mathrm{RE}}(\boldsymbol{x})=\max\left|\frac{\overline{x}_i-x_i^{\text{pre-attack}}}{x_i^{\text{pre-attack}}}\right|,i\in n \tag{4.17}$$

$$\mathrm{AVG}^{\mathrm{RE}}(\boldsymbol{x})=\frac{1}{n}\sum_{i=1}^{n}\left|\frac{\overline{x}_i-x_i^{\text{pre-attack}}}{x_i^{\text{pre-attack}}}\right|,i\in n \tag{4.18}$$

式中，n 表示状态向量的维数；$\hat{x}_{k,i}$ 表示 k 时刻状态估计向量中的第 i 个条目；$x_{k,i}^{\text{pre-attack}}$ 表示 k 时刻攻击前状态的第 i 个条目；$\overline{x}_i$ 和 $x_i^{\text{pre-attack}}$ 分别表示为校正后和攻击前的第 i 个状态。$\mathrm{MAX}^{\mathrm{RE}}$ 和 $\mathrm{AVG}^{\mathrm{RE}}$ 越小，表明状态校正的性能越好。

4.4.2 仿真数值分析

在本节中，采用 IEEE-14 节点系统的 80 个测量值作为观测值。此外，状态变量是每个节点的电压幅值和相角。由于 1 号节点为平衡节点，因此最终需要估计的状态变量总数为 27 个。卡方分布的自由度可以表示为 $c=m-n=53$。如果将置信度设定为 0.95，则根据卡方检验阈值表，得到卡方检验的阈值为 74.222[1]。为了展示所提出的算法在存在不同异常值类型的情况下检测和校正状态的有效性，本节进行了以下几种情况的分析。

情况 1：在这种情况下，系统中不存在异常值。首先，使用式(2.7)计算 WLS 的状态估计值，然后将这些估计值代入式(2.25)以计算目标函数值 $J(\hat{\boldsymbol{x}})$。通过将每个时间步的 $J(\hat{\boldsymbol{x}})$ 与相应的卡方检验阈值进行比较，以检测系统中是否存在不良数据。图 4-2 展示了 100 个采样时刻的目标函数值 $J(\hat{\boldsymbol{x}})$，其中每个采样时刻的

$J(\hat{\boldsymbol{x}})$均小于卡方检验的阈值 74.222。这是由于传统的不良数据数据检测方法利用统计学原理，例如基于残差的假设检验，来判断测量残差是否符合正态分布或其他已知的分布特性。如果残差符合预期的分布特性，表明不存在不良数据。因此，通过式(2.26)的计算，可以确定该时间段内系统中不存在不良数据。

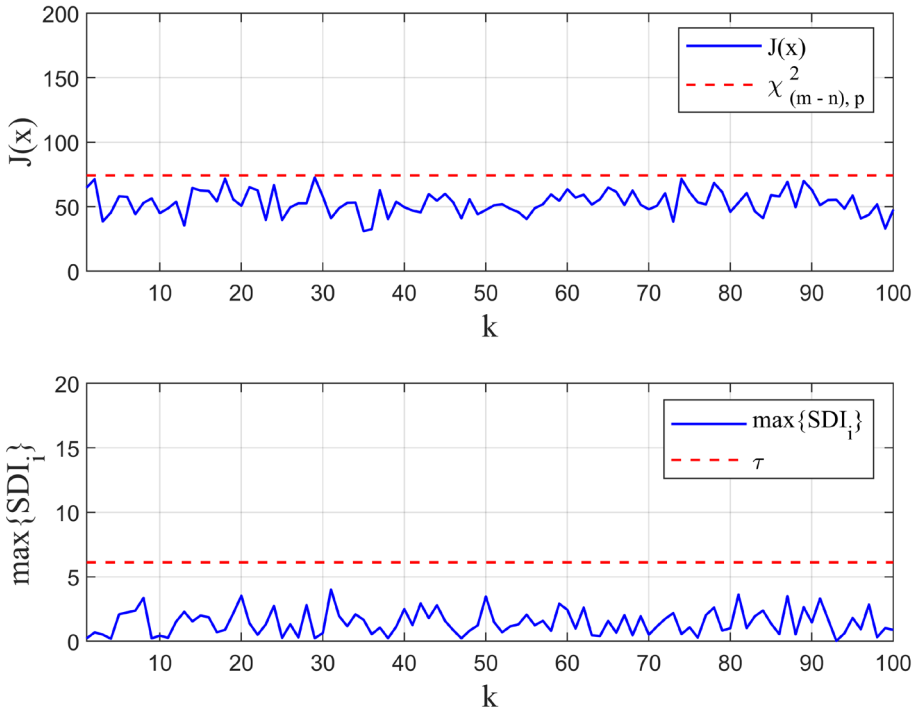


图 4-2 正常系统条件下$J(\hat{\boldsymbol{x}})$和$\max\{\mathrm{SDI}_i\}$的检测指标。

此外，SDI_i是针对没有异常值的情况下计算得到的。首先，分别使用式(2.7)和式(3.10)来计算 WLS 和 EKF 的状态估计值，然后使用方程(4.10)来计算SDI_i。为了确定系统中是否存在异常值，将$\max\{\mathrm{SDI}_i\}$与相应的检测阈值τ进行比较。为了准确设置检测阈值τ，分别在正常场景和异常场景下进行了 1000 次蒙特卡洛模拟。最终，能够准确区分正常场景和异常场景的检测阈值τ被确定为 6.12。在 100 个采样时间段内，系统正常工作时的$\max\{\mathrm{SDI}_i\}$如图 4-2 所示。需要注意的是，每个采样时间段的$\max\{\mathrm{SDI}_i\}$都小于阈值τ。这是因为系统在正常情况下，利用 EKF 与 WLS 进行状态估计得到的估计偏差很小，所以计算出的$\max\{\mathrm{SDI}_i\}$低于相应的检测阈值。

情况 2：系统中存在多种异常值。为了模拟系统中存在的不良数据，本节在 $k=5$ 时在节点 14 的功率注入测量中注入 6%的误差，并且不良数据持续 6 个采样时刻。注入不良数据后系统的卡方检验结果如图 4-3 所示。由图 4-3 可知，注入不良数据后的目标函数值大于阈值 $\chi^2_{(m-n),p}=74.22$。这是因为不良数据会导致实际观测数据和系统正常运行条件下的预期数据之间存在显著偏差。这种偏差体现在 $J(\hat{\boldsymbol{x}})$ 的增加上，因为 $J(\hat{\boldsymbol{x}})$ 是观测值和期望值之间差异的统计测量。因此，传统的不良数据检测方法可以有效地检测系统中的不良数据。然而，该方法无法检测出系统中精心构建的 FDIA 与 SLC。因此，为了进一步检测 FDIA 和 SLC，本章采用了基于状态偏差的检测方法。

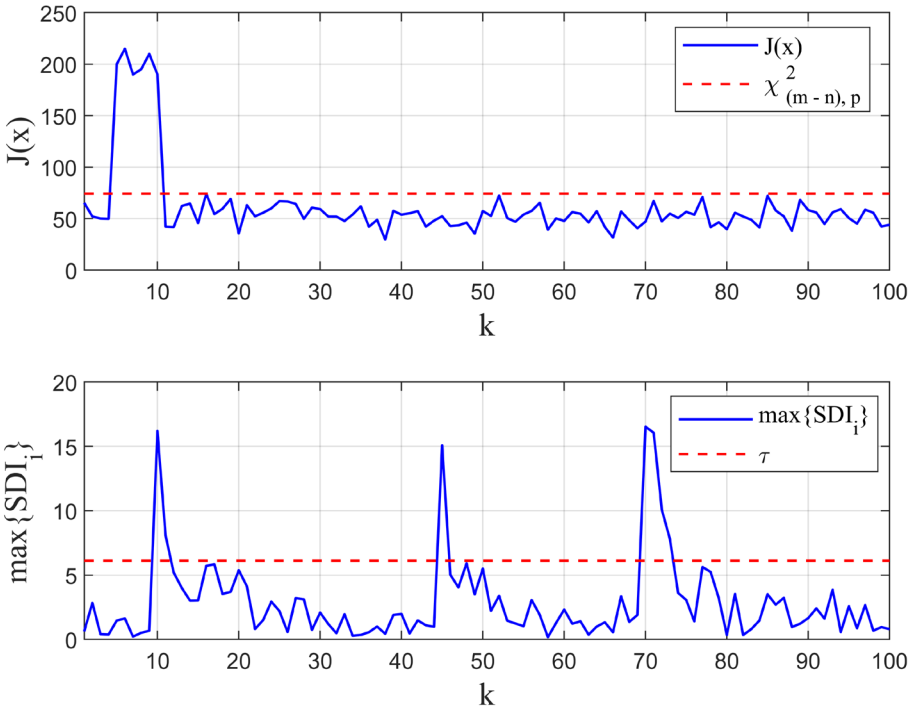


图 4-3 系统存在不良数据和异常情况时 $J(\hat{\boldsymbol{x}})$ 和 $\max\{\mathrm{SDI}_i\}$ 的检测指标。

为了模拟系统中存在的 SLC，本节在 $k=10$ 和 $k=45$ 之间把节点 14 的负载减少了 18%。同时，为了模拟系统中的 FDIA，在时间 $k=70$ 时向系统注入了攻击向量，该攻击向量导致了节点 14 的电压幅度增加 0.06 p.u.。当系统同时受到 FDIA 和 SLC 的影响时，每个采样时刻的 $\max\{\mathrm{SDI}_i\}$ 如图 4-3 所示。在系统存在 FDIA 和 SLC 时，$\max\{\mathrm{SDI}_i\}$ 超过了设定的检测阈值。这里 $k=10$ 和 $k=45$ 分别对

应于 SLC 的出现和消失。显然，利用 $\max\{\mathrm{SDI}_i\}$ 能够有效地检测系统中 FDIA 和 SLC 的存在。值得注意的是，FDIA 和 SLC 可以绕过经典的不良数据检测方法。同时， $\max\{\mathrm{SDI}_i\}$ 也能够检测出高误差的不良数据，尽管卡方检验对于不良数据的检测率已经相对较高。

为了模拟系统中的FDIA，在 $k=70$ 时刻向IEEE-14节点系统注入攻击向量，这使节点 14 的电压幅度增加了 0.06 p.u.。系统受到攻击时的测量值和各节点的电压幅值如图 4-4 所示。系统受到攻击后，14 节点的电压幅值及其相关测量值明显偏离正常值。

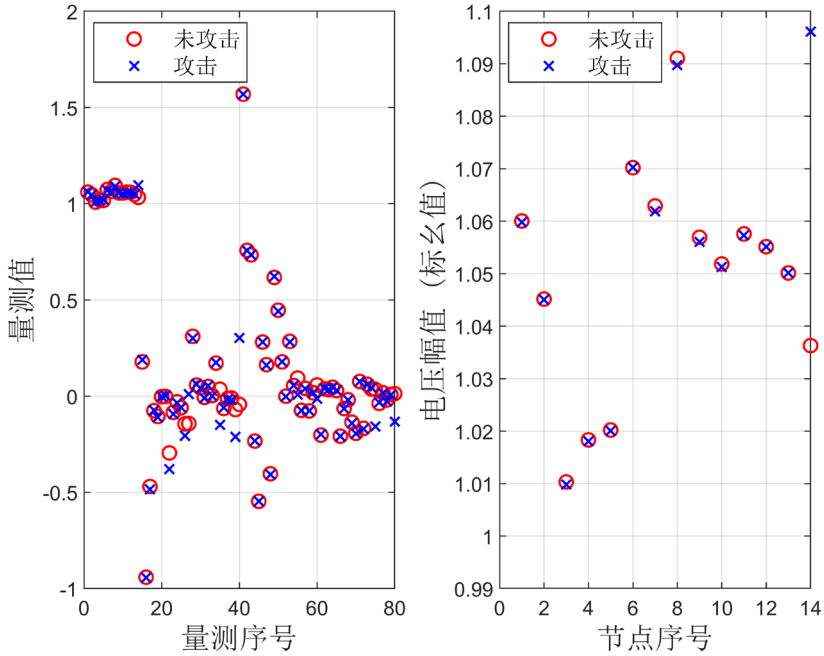


图 4-4 系统受到攻击时的量测值和各节点的电压幅值

尽管卡方检验和状态偏差指数 $\max\{\mathrm{SDI}_i\}$ 可以有效检测系统中是否存在不良数据和异常情况(如 FDIA 和 SLC)，但在异常情况存在时对系统中的状态估计进行修正尤为重要。不良数据或异常值的存在可能会导致状态估计结果偏离正常值。因此，在检测到异常情况后，采用式(4.12)和(4.13)补偿测量值，然后利用补偿后的测量值进行状态估计，最终实现对状态的校正。这一过程对于维护系统状态估计的准确性和可靠性具有重要意义。

情况 3：测量补偿和状态校正后的状态估计性能分析。当使用 SDI 检测到 SLC 和 FDIA 时，系统发出警报并激活测量补偿和状态校正方案以补偿量测值和

校正状态。首先，使用式(4.12)和(4.13)来补偿攻击后的量测值。然后，利用更新后的状态方程和测量方程进行状态估计，最终实现状态校正。通过使用所提出的量测补偿和状态校正方案，补偿后的量测值和校正后的状态值如图 4-5 所示。

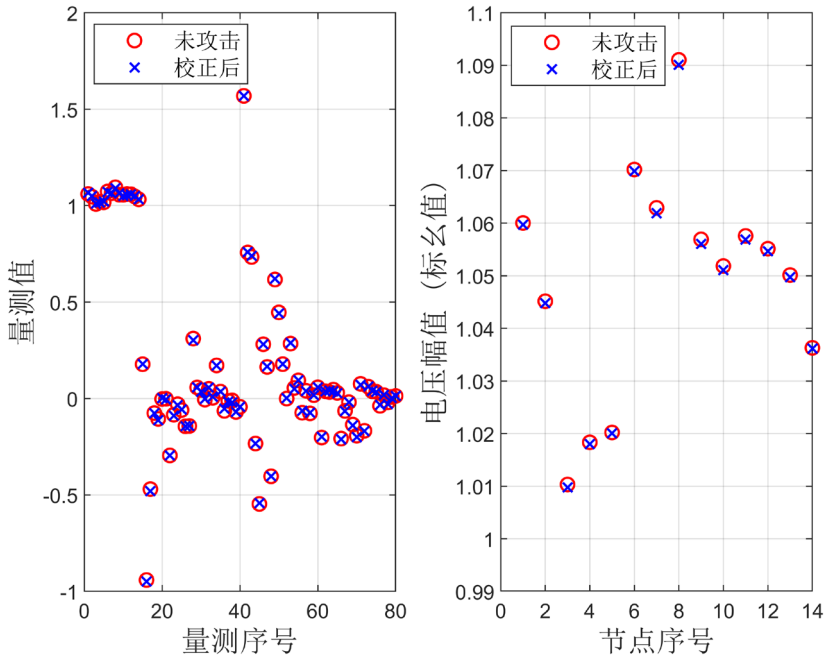


图 4-5 系统校正后的量测值和各节点的电压幅值

图 4-5 中表明，经过补偿后的测量值和状态估计结果与真实值基本一致。同时，详细分析了校正前后的量测值和状态估计值与真实值之间的 RMSE，结果如表 4-3 所示。

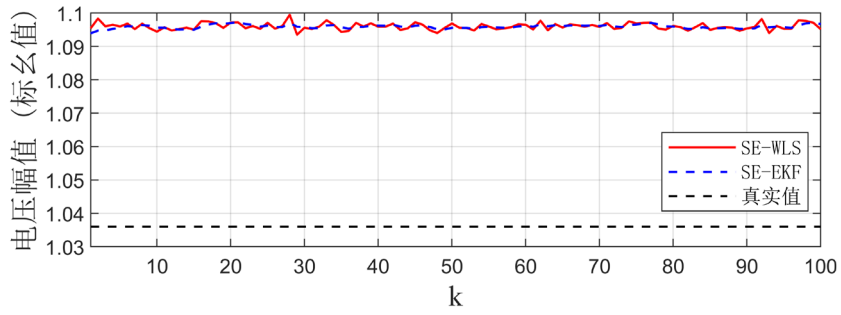
表 4-3 不同场景中量测值和状态估计值的 RMSE

场景	量测值	状态估计值
攻击	0.0621	0.0159
提出的算法	0.0052	0.0017
SLC	0.0077	0.0024
提出的算法	0.0049	0.0015

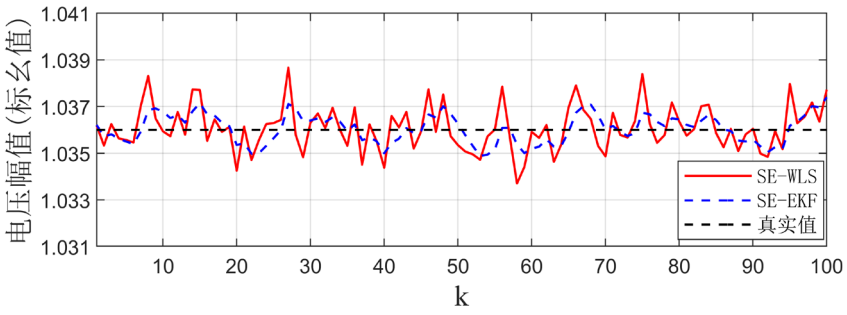
表 4-3 表明了在不同场景下系统的测量值和状态估计值与真实值之间的 RMSE。特别值得注意的是，如果系统中的 FDIA 导致节点 14 的电压幅值增加 0.06 p.u.，则测量值和状态估计值的 RMSE 显著增加。这是因为 0.06 p.u.电压幅值的增加会严重干扰系统运行状态。然而，通过采用本章提出的校正方案，测量和状态估计的 RMSE 几乎降低了十倍。此外，在总线 14 的负载减少 18%后，可

以观察到测量值和状态估计值的 RMSE 略微增加，但并不显著。这是因为 14 号节点的负载减少 18%并未对系统造成明显的干扰。然而，通过采用本章提出的状态校正方案，测量值和状态估计值的 RMSE 显著降低，从而提高了状态估计的准确性。数值实例表明，采用本章提出的方法对测量值和状态估计值进行校正后，测量值和状态估计值与真实值基本一致。

为了进一步证明该方案的有效性，系统在 100 个采样时刻内受到攻击时和校正后的状态如图 4-6 所示。



(a) 攻击时



(b) 校正后

图 4-6 系统受到攻击时以及状态校正后的 14 号节点电压幅值

图 4-6(a)表明系统受到攻击时，14 号节点的电压幅值较真实值出现明显偏差。图 4-6(b)表明，通过本章提出的算法进行校正后，WLS 和 EKF 的状态估计值与真实值一致，使其在正常范围内。这进一步证明了该方法在应对系统异常情况时的可靠性和准确性。

为了进一步验证本章所提算法的有效性，使用 RMSE 来比较不同算法在校正前和校正后的状态估计性能。将本章提出的算法与传统的 EKF 和 WLS 估计的 RMSE 进行了如图 4-7 所示的比较。

图 4-7 表明了状态估计值在校正前和校正后的 RMSE。系统受到攻击时，传统 EKF 和 WLS 状态估计的 RMSE 较大，然而经过状态校正后的 RMSE 显著小

于未校正时的 RMSE。

随着 FDIA 对电力系统攻击强度的增加，状态估计值与正常状态值之间的偏差程度逐渐增大。为了更详细地比较本章提出的状态校正算法与传统 WLS 和 EKF 在不同攻击强度时的状态估计性能，进行了如图 4-8 所示的不同攻击强度的场景模拟。

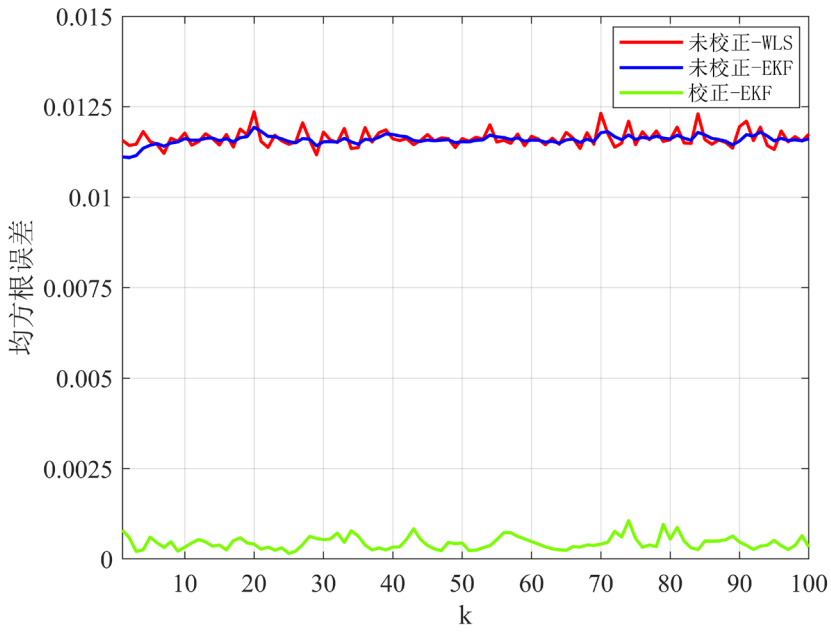


图 4-7 系统受到攻击和状态校正后的 RMSE

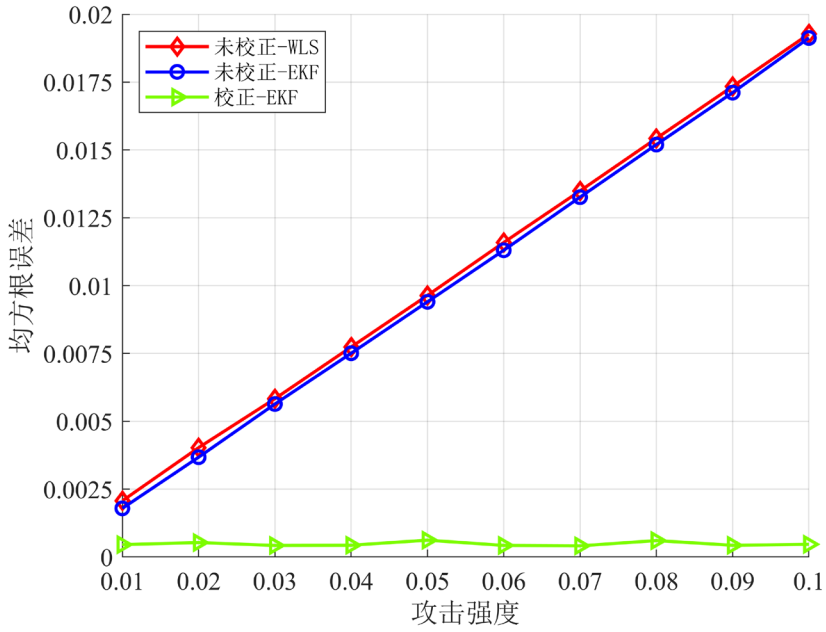


图 4-8 状态估计在不同攻击强度下的 RMSE

图 4-8 表明了不同攻击强度下，状态估计在 100 次采样时刻的 RMSE 平均

值。随着攻击强度的增加，传统 WLS 和 EKF 的估计偏差变得更加显著。然而，本章提出的状态校正方案在不同攻击强度下仍然表现出良好的估计性能，进一步验证了其在不同攻击强度下的有效性。

此外，为了进一步评估所提算法的性能，将其与另外两种状态恢复方案进行了比较[45]。深度学习在状态预测领域具有广泛的应用，尤其在处理时间序列数据和空间数据的预测方面表现出色。本节采用了基于循环神经网络(Recurrent Neural Networks, RNN)的变种，其中包括具有长短期记忆(Recurrent Neural Networks, LSTM)网络和门控循环单元(Gated Recurrent Units, GRU)网络，用于对攻击前的状态进行预测。表 4-4 中展现了在电力系统受到攻击的不同情况下，各种状态恢复方案获得的$\mathrm{MAX}^{\mathrm{RE}}$和$\mathrm{AVG}^{\mathrm{RE}}$指标。值得注意的是，所提出的算法在两个指标上均优于其他方案，这进一步证明了其在状态恢复性能方面的良好表现。

表 4-4 不同场景中的相对误差比较

场景	$\mathrm{MAX}^{\mathrm{RE}}$	$\mathrm{AVG}^{\mathrm{RE}}$
攻击	6.97%	0.3%
LSTM	0.68%	0.064%
GRU	0.41%	0.09%
提出的算法	0.32%	0.045%

为了进一步验证本章所提算法的有效性，将该方法在 IEEE-30 节点系统中进行更深入的测试。在这个测试中，使用了 IEEE-30 节点系统的 93 个测量值作为观测值，其中状态变量包括每个节点的电压幅值和相位角。需要注意的是，1 号节点是平衡节点，最终需要估计的状态变量总数为 59 个。因此，卡方分布的自由度为$c = m - n = 34$。将置信度设定为 0.95，并从相应的卡方表中查询获取的卡方检验阈值为 48.6024[1]。这些测试将有助于进一步验证本章所提算法在不同系统配置下的有效性和适用性。

情况 1：系统中存在不良数据。为了模拟系统中存在的不良数据，本节在$k = 10$时对 30 号节点的有功功率测量注入 6%的误差，并且不良数据持续 10 个采样时刻。然后，利用不良数据检测方法，如卡方检验对模拟的不良数据进行检测。系统注入不良数据后的卡方检验结果如图 4-9 所示。

图 4-9 表明了系统注入不良数据后的目标函数值 $J(\hat{\boldsymbol{x}})$ 大于卡方检测阈值 $\chi^2_{(m-n),p}=48.6024$。由此进一步证明了传统的不良数据检测方法能够有效检测系统中的不良数据。

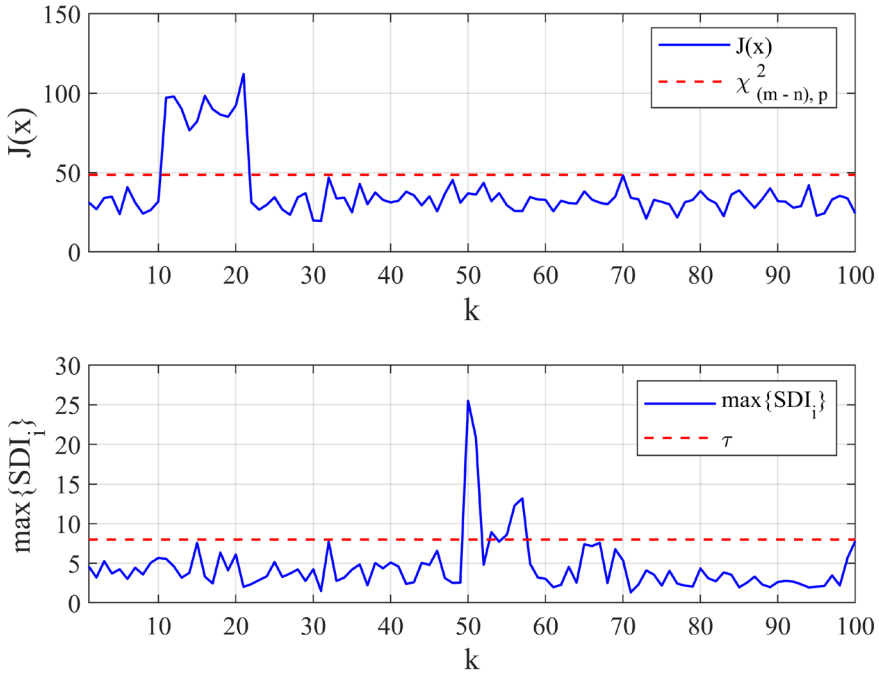


图 4-9 系统存在不良数据和异常情况时 $J(\hat{\boldsymbol{x}})$ 和 $\max\{SDI_i\}$ 的检测指标。

情况 2：系统中存在多种异常情况。为了模拟系统中的 FDIA，在时间 $k=50$ 时注入攻击向量，将节点 30 的电压幅值增加 0.06 p.u。此外，为了模拟系统中可能发生的 SLC，将 30 号节点的负载减少 18%。当系统中存在 FDIA 时，每个时刻的 $\max\{SDI_i\}$ 如图 4-9 所示。

为了准确设置检测阈值 τ，分别在正常场景和异常场景下进行了 1000 次蒙特卡罗模拟。最终，确定了一个能够准确区分正常场景和异常场景的检测阈值 $\tau=8$。因此，当系统中存在 FDIA 时，$\max\{SDI_i\}$ 会超过设定的检测阈值 $\tau=8$，这进一步证明了该算法可以有效地检测 FDIA。

由于 FDIA 的影响，系统的状态和相关测量值发生了偏差。图 4-10 表明了在系统受到攻击时的测量值和各节点的电压幅值。

图 4-10 中表明，系统受到攻击后的测量值和 30 号节点电压幅值与实际值存在显著偏差。

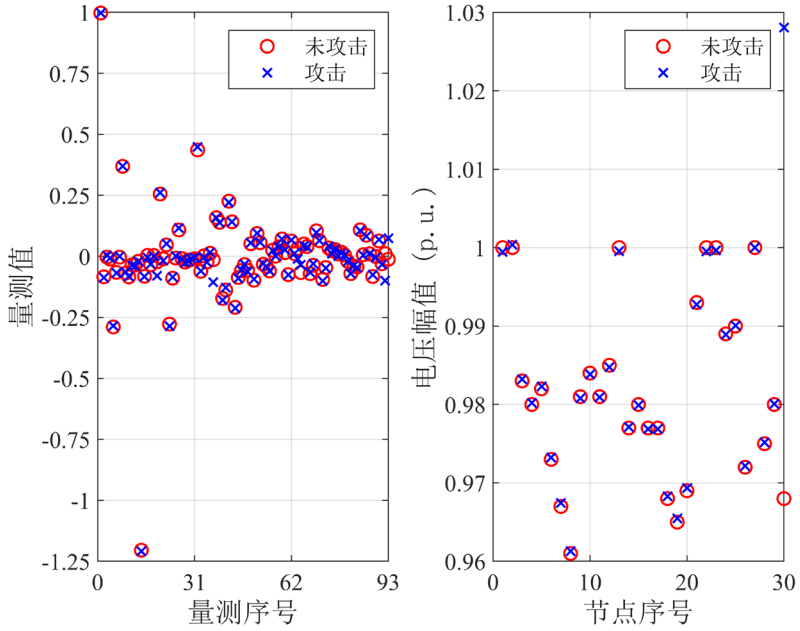


图 4-10 系统受到攻击时的量测值和各节点的电压幅值

情况 3：量测补偿和状态校正后的状态估计性能分析。利用 $\max\{SDI_i\}$ 与阈值比较检测 FDIA 和 SLC 后，分别利用式(4.12)和式(4.13)对污染的测量进行补偿和更新，以减少 FDIA 和 SLC 对电力系统状态估计的影响。然后，利用更新后的状态方程和测量方程进行状态估计，实现状态校正。通过使用本章所提出的量测补偿和状态校正方案，补偿后的测量和校正后的状态如图 4-11 所示。

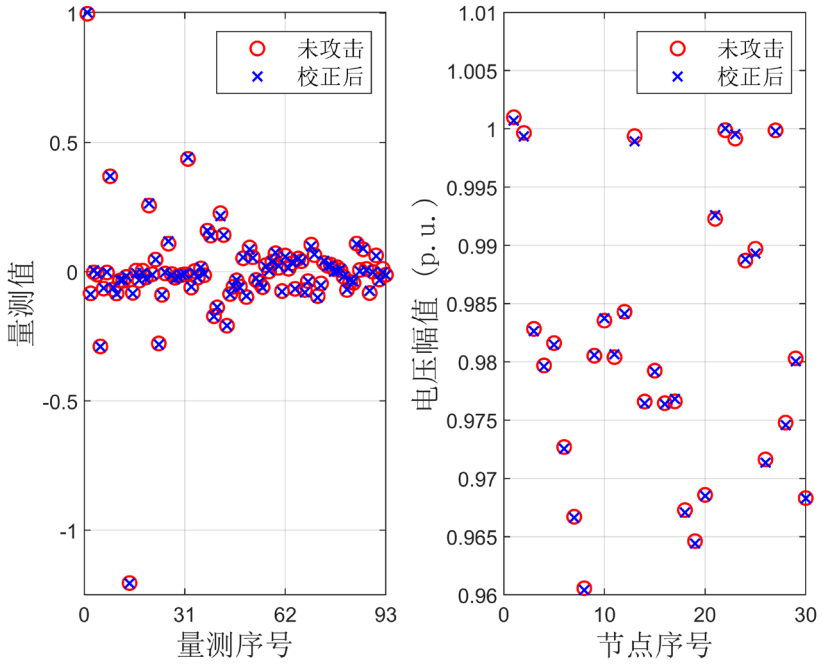


图 4-11 系统校正后的量测值和各节点的电压幅值

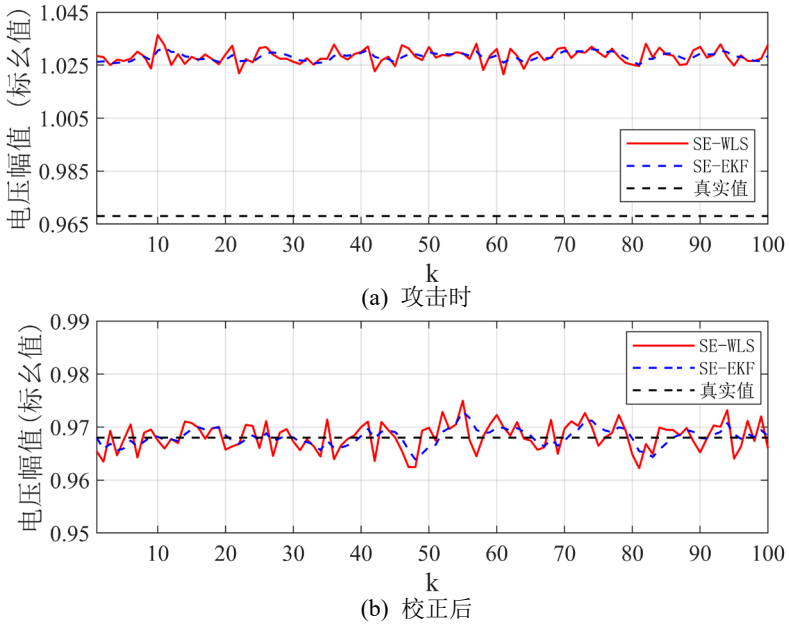
图 4-11 中表明，经过补偿后的测量值和状态估计结果与真实值基本一致。同时，详细分析了校正前后量测和状态估计与真实值之间的 RMSE，结果如表 4-5 所示。

表 4-5 不同场景中量测值和状态估计值的 RMSE

场景	量测值	状态估计值
攻击	0.0218	0.0038
提出的算法	0.0062	0.0021
SLC	0.0119	0.0033
提出的算法	0.0046	0.0028

表 4-5 表明了不同场景下系统的测量值和状态估计值与真实值之间的 RMSE。特别地，当系统中的 FDIA 将节点 30 的电压幅值增加 0.06 p.u. 或者 SLC 使节点 30 上的负载减少 18%时，量测值和估计值与真实值之间的 RMSE 都有不同程度的增加，表明系统的状态估计性能受到干扰。值得注意的是，使用本章提出的算法对这两种不同场景下的量测值和状态估计值进行补偿和校正后，它们的 RMSE 都有不同程度的降低。数值算例表明，采用本章提出的方法对量测值和状态估计进行校正后，校正后的结果与真实值基本一致。

为了进一步证明该方案的有效性，在 100 个采样时刻内系统受到攻击时和校正后节点 30 的电压幅值估计值如图 4-12 所示。



(a) 攻击时

(b) 校正后

图 4-12 系统受到攻击时和状态校正后的 30 号节点电压幅值

图 4-12(a)表明系统受到攻击时，虚假数据导致 30 号节点的电压幅值出现明显偏差。图 4-12(b)表明，通过本章提出的算法进行校正后，WLS 和 EKF 的状态估计值与真实值一致，使其在正常范围内。这进一步证明了该方法在应对系统异常情况时的可靠性和准确性。

为了进一步验证本章所提算法的有效性，使用 RMSE 来比较不同算法在校正前和校正后的状态估计性能。将本章提出的算法与传统 EKF 和 WLS 估计的 RMSE 进行了如图 4-13 的比较。

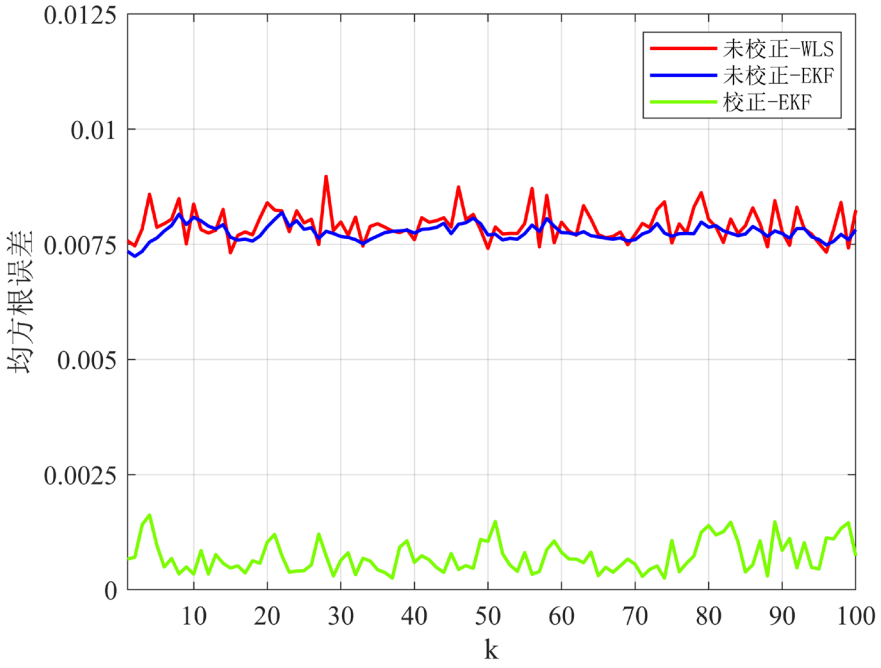


图 4-13 系统受到攻击和状态校正后的 RMSE

图 4-13 表明了校正前和校正后状态估计值的 RMSE。系统存在异常值时，传统 EKF 和 WLS 状态估计的 RMSE 较大，然而经过状态校正后的 RMSE 显著小于未校正的 RMSE。

随着 FDIA 对电力系统的攻击强度增加，状态估计值与正常值之间的偏差程度逐渐增大。本节进一步模拟了 IEEE-30 节点系统在不同攻击强度下的场景。为了更详细地比较本章提出的算法与传统的 WLS 和 EKF 在不同攻击强度下的状态估计性能，进行了如图 4-14 中所示的多种攻击强度场景的模拟。

图 4-14 表明了不同攻击强度下，状态估计在 100 次采样时刻的 RMSE 平均值。随着攻击强度的增加，传统的 WLS 和 EKF 估计的偏差变得更加显著。然而，本章提出的状态校正方案在不同攻击强度下仍然表现出良好的估计性能，进

一步验证了其在不同攻击强度下的有效性。

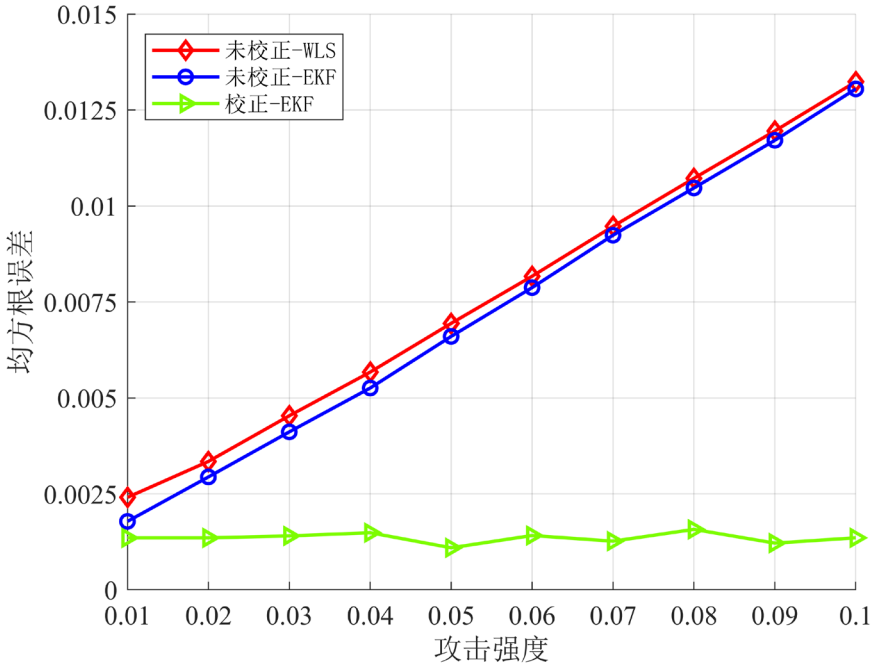


图 4-14 状态估计在不同攻击强度下的 RMSE

此外，为了进一步说明所提出算法的性能，把本章所提方法与其他两种状态恢复方案进行了反复比较[45]。在 IEEE-30 节点系统中，每种场景的状态恢复性能如表 4-6 所示。数值示例表明本文提出的算法比其他两种方法具有更好的状态校正性能。

表 4-6 不同场景中的相对误差比较

场景	MAX^{RE}	AVG^{RE}
攻击	7.79%	0.74%
LSTM	0.78%	0.072%
GRU	0.44%	0.12%
提出的算法	0.36%	0.08%

SCADA 系统的主要任务之一是实时监控电力系统的运行状态，并进行必要的控制。由于 SCADA 系统往往每 2-6 秒采样一次测量数据。因此，实时状态估计对于快速检测和响应系统异常至关重要。当系统出现异常时，本章中的方法可用于快速检测异常，并对测量数据进行补偿，校正被攻击的状态。因此，该方法需要在 SCADA 系统下一次采样之前完成测量补偿和状态校正。

为了证明所提算法的计算效率，将该方法应用于不同规模的电力系统中验证。

在 SCADA 系统中，测量采样周期设定为 2 秒。此外，将本章提出的算法与传统的 EKF 算法进行比较。传统的 EKF 算法在使用状态偏差指数检测到异常值后不对测量进行补偿，也不对状态估计进行修正。本章提出的算法和传统 EKF 算法的平均计算时间如表 4-7 所示。

表 4-7 不同系统中状态估计算法的平均计算时间(秒)

算法	IEEE-14 节点	IEEE-30 节点	IEEE-118 节点
传统 EKF	1.92×10^{-2}	4.55×10^{-2}	1.84×10^{-1}
提出的算法	3.41×10^{-2}	7.71×10^{-2}	3.07×10^{-1}

在 IEEE-14 节点系统和 IEEE-30 节点系统中，传统 EKF 算法和本章提出的算法都具有较高的计算效率。虽然与传统 EKF 算法相比，本章所提算法的平均计算时间有所增加，但其平均计算时间仍远小于 SCADA 系统的采样周期。进一步将提出的算法应用于更大规模的 IEEE-118 节点系统。如表 4-7 所示，本章所提出的算法仍然具有很高的计算效率，其平均计算时间仍然小于 SCADA 系统的采样周期。因此，本章提出的基于滑动窗口的测量补偿和状态校正算法非常适合在不同规模的电力系统中应用。

4.5 本章小结

本章讨论了系统在 FDIA 和 SLC 情况下的异常检测和状态校正问题。为此，本章利用两个估计器的状态偏差指数和相应的阈值比较来检测异常。特别是采用自适应调整参数的指数平滑方法来预测系统状态，提高了状态估计的准确性。同时，为了及时恢复测量和校正状态，本章提出了一种带有滑动窗口的数据补偿策略来补偿量测值。然后，利用补偿后的量测结果重建系统的状态方程和测量方程。通过对 IEEE-14 节点系统和 IEEE-30 节点系统进行仿真，验证了该算法在异常检测和状态校正方面的性能。数值示例表明，本章所提出的方法可以在出现异常时准确地检测和校正状态。

第 5 章 总结与展望

5.1 总结

在网络物理系统中，精确的状态信息是电力系统稳定运行的关键。虚假数据注入攻击可能导致错误的状态估计，从而影响系统的稳定性和安全。CPPS 依赖于准确的数据进行高效的能源管理和分配。FDIA 可以破坏这一过程，导致效率下降。准确检测和定位 FDIA 有助于加强系统的网络安全防御能力，预防未来的攻击。FDIA 可能导致数据损坏，对受异常值影响的状态进行校正可以恢复数据的完整性，保证基于准确信息进行操作。因此，检测和定位虚假数据注入攻击，以及对受异常值影响的状态进行校正具有至关重要的意义。本文详细分析了电力系统状态估计和FDIA原理，着重探讨了如何准确估计电力系统状态并识别FDIA的挑战。接着，文中提出了一种基于动静态联合估计的 FDIA 检测方法，该方法结合了动态估计技术和静态数据分析，以提高检测的准确性和效率。最后，为了应对 FDIA 导致的数据不准确问题，文章介绍了一种基于滑动窗口的量测补偿和状态校正方案，旨在有效校正因攻击而存在偏差的状态数据，保证电力系统运行的安全和稳定。本文主要研究内容如下：

（1）详细阐述了电力系统状态估计的基本理论，包括交流和直流模型的详细讨论。同时，对电力系统中传统的不良数据检测方法及其原理进行了全面分析。接着，文中深入探讨了 FDIA 如何绕过这些传统检测方法，包括 FDIA 在交流和直流模型下的构造方式及其对状态估计系统的潜在影响。

（2）提出了一种基于状态偏差和电网网格划分的 FDIA 检测和定位方法。针对传统的 EKF 在面对 FDIA 时状态估计性能下降的问题，开发了一种改进的鲁棒 EKF 算法。利用改进的 EKF 和 WLS 的状态估计偏差对 FDIA 进行检测。此外，本文还提出了一种对电网进行网格划分的方法，通过在各个子网格中分别进行检测来准确定位 FDIA。最后通过仿真实验验证了方法的有效性。

（3）提出了一种针对 FDIA 的量测补偿和状态校正方案。讨论了滑动窗口方法和基于指数平滑的自适应调节策略。为解决传统 Holt 指数平滑法在预测状态时无法根据系统运行模式自适应调节平滑参数的局限性，本文提出了一种新

型指数平滑法。这种方法能够根据预测误差自适应调整平滑参数，从而提高状态估计的准确性。同时，针对 FDIA 造成的量测数据和状态偏差，本文还引入了一种利用滑动窗口技术的补偿机制。通过这种机制，对受异常值影响的数据进行补偿，并使用补偿后的量测值进行状态估计，以达到状态校正的目的。

5.2 展望

本文针对 CPPS 中的异常值如 FDIA、BD 和 SLC 进行初步研究，开展了异常值检测、定位和对被污染的异常值进行补偿和状态校正方面的初步研究工作。尽管取得了一定的研究成果，但是研究中仍然存在一些不足和可以完善的工作，如：

（1）本文中采用的量测噪声类型是研究中最常用的高斯噪声类型，然而在实际电网中存在的量测噪声可能偏离该假设。WLS 和 EKF 都是基于高斯噪声的假设，当噪声特性偏离该假设时，估计的准确性和鲁棒性可能会受到影响。极值和重尾分布：非高斯噪声，特别是那些具有极值或重尾特征的噪声，可能会在状态估计中引入显着的误差，而这些误差在传统的 WLS 和 EKF 形式中很难有效处理。针对上述问题，可以修改传统的 WLS 以使其对非高斯分布噪声更加鲁棒，并且可以修改 EKF 以使用不同的损失函数或调整滤波算法以使其能够更好地处理非高斯分布噪声。

（2）本文是在 IEEE 标准节点系统中进行的，然而伴随着可再生能源，诸如太阳能和风能的广泛部署，迫切需要深入探究如何更有效地将这些可再生能源资源整合到智能电网中。这一探究不仅有助于进一步验证本研究中关于异常值检测和定位（如虚假数据注入攻击、不良数据和负荷突变）方法的有效性，还涉及对被污染的量测值进行补偿和状态校正的研究。

（3）本文主要是针对虚假数据注入攻击这类威胁进行检测、定位和校正。然而在实际电网中可能受到其他类型的安全威胁。电力系统的通信网络可能会受到网络攻击，如分布式拒绝服务攻击或恶意软件攻击。这些攻击可能导致通信中断，使状态估计数据无法传输，从而影响状态估计的准确性和实时性。因此，开展对其他类型的异常值检测和定位研究对于状态估计的安全性具有重要意义。

参考文献

[1] He R, Xie H, Deng J, et al. Reliability modeling and assessment of cyber space in cyber-physical power systems[J]. IEEE Transactions on Smart Grid, 2020, 11(5): 3763-3773.

[2] Nawaz A, Wang H. Risk-aware distributed optimal power flow in coordinated transmission and distribution system[J]. Journal of Modern Power Systems and Clean Energy, 2021, 9(3): 502-515.

[3] Wang S, Yu D, Yu J, et al. Optimal generation scheduling of interconnected wind-coal intensive power systems[J]. Iet Generation Transmission and Distribution, 2016, 10: 3276-3287.

[4] Gu H, Jie Y, Li Y, et al. Optimal economic dispatch for an industrial park with consideration of an elastic energy cloud model with integrated demand response uncertainty[J]. IEEE Access, 2021, 9: 52485-52508.

[5] Jia Y, Dong Z Y, Sun C, et al. Distributed economic model predictive control for a wind–photovoltaic–battery microgrid power system[J]. IEEE Transactions on Sustainable Energy, 2020, 11(2): 1089-1099.

[6] Miao Z, Guo A, Chen X, et al. Network technology, whole-process performance, and variable-specific decomposition analysis: Solutions for energy-economy-environment nexus[J]. IEEE Transactions on Engineering Management, 2024, 71: 2184-2201.

[7] Ghosh S, Raut R D, Mandal M C, et al. Revisiting the nexus between sustainable supply chain management and the performance of steel manufacturing organizations: A case study from an emerging economy[J]. IEEE Engineering Management Review, 2023, 51(1): 189-213.

[8] 杨鑫, 王启蒙, 陆超杰等. 一种轻量级 SCADA 系统的网络安全设计和实现[J]. 物联网技术, 2023, 13(12): 39-41.

[9] 张家林, 雒毅东. 关键信息基础设施安全检测评估工作机制措施[J]. 网络安全技术与应用, 2023, 12: 163-164.

[10] Liang G, Weller S R, Zhao J, et al. The 2015 Ukraine blackout: Implications for false data injection attacks[J]. IEEE Transactions on Power Systems, 2017, 32(4): 3317-3318.

[11] 唐亚东, 刘寅, 杨维永. 基于等级保护网络安全体系的新型电力系统风险分析与防范[J]. 网络安全技术与应用, 2023(12): 130-133.

[12] 赵学智, 林亮成, 姜帆等. 新形势下电力工业控制系统网络安全防护体系研究[J]. 网络安全技术与应用, 2023(10): 112-118.

[13] Abur A, Expoisito A G. Power system state estimation: Theory and implementation[M]. 1st ed. New York, NY, USA: Marcel Dekker, 2004.

[14] Dutta R, Patel V S, Chakrabarti S, et al. Parameter estimation of distribution lines using SCADA measurements[J]. IEEE Transactions on Instrumentation and Measurement, 2021, 70: 1-11.

[15] Zhao J, Netto M, Huang Z, et al. Roles of dynamic state estimation in power system modeling, monitoring and operation[J]. IEEE Transactions on Power Systems, 2021, 36(3): 2462-2472.

[16] 陈艳波, 陈茜, 马进等. 电力系统线性状态追踪方法[J]. 电网技术, 2015, 39(02): 472-477.

[17] 李钦, 项凤雏, 颜伟等. 基于 SCADA 及 PMU 多时段量测信息的独立线路参数估计方法[J]. 电网技术, 2011, 35(02): 105-109.

[18] 李明, 姜旭, 王春华等. 量测不同步与系统运行快变影响的状态估计精度的分析[J]. 电力系统及其自动化学报, 2020, 32(01): 21-49.

[19] Cui S, Han Z, Kar S, et al. Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions[J]. IEEE Signal Processing Magazine, 2021, 29(5): 106-115.

[20] 田继伟, 王布宏, 李腾耀等. 智能电网虚假数据注入攻击研究进展与展望[J]. 网络空间安全, 2019, 10(09): 73-84.

[21] Guan Y, Ge X. Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks[J]. IEEE Transactions on Signal and Information Processing over Networks, 2019,

4(1): 48-59.

[22] Ashok A, Govindarasu M, Ajjarapu V. Online detection of stealthy false data injection attacks in power system state estimation[J]. IEEE Transactions on Smart Grid, 2018, 9(3): 1636-1646.

[23] 陈艳波, 高瑜珑, 赵俊博等. 综合能源系统状态估计研究综述[J]. 高电压技术, 2021, 47(07): 2281-2292.

[24] 王海涛, 白建伟, 刘文等. 基于改进两阶段鲁棒优化的电力系统状态估计方法[J]. 电网与清洁能源, 2022, 38(09): 55-64.

[25] Gomez-Quiles C, Villa Jaen A, Gomez-Exposito A. A factorized approach to WLS state estimation[J]. IEEE Transactions on Power Systems, 2011, 26(3): 1724-1732.

[26] 肖润龙, 王刚, 郝晓亮等. 静态状态估计中权重矩阵确定的方法研究[J]. 计算机仿真, 2018, 35(09): 391-396.

[27] Kusljevic M D K, Poljak P D. Simultaneous reactive-power and frequency estimations using simple recursive WLS algorithm and adaptive filtering[J]. IEEE Transactions on Instrumentation and Measurement, 2011, 60(12): 3860-3867.

[28] Zhao J, Gómez-Expósito A, Netto M, et al. Power system dynamic state estimation: Motivations, definitions, methodologies, and future work[J]. IEEE Transactions on Power Systems, 2019, 34(4): 3188-3198.

[29] Chughtai A H, Akram U, Tahir M, et al. Dynamic state estimation in the presence of sensor outliers using MAP-based EKF[J]. IEEE Sensors Letters, 2020, 4(4): 1-4.

[30] Huang Z, Schneider K, Nieplocha J. Feasibility studies of applying Kalman filter techniques to power system dynamic state estimation[C]// 2007 International Power Engineering Conference (IPEC), Singapore, 2007: 376–382.

[31] Zhao J, Mili L. Robust unscented Kalman filter for power system dynamic state estimation with unknown noise statistics[J]. IEEE Transactions on Smart Grid, 2019, 10(2): 1215–1224.

[32] Kong X, Zhang X, Zhang X, et al. Adaptive dynamic state estimation of distribution network based on interacting multiple model[J]. IEEE Transactions on

Sustainable Energy, 2022, 13(2): 643-652.

[33] Dang L, Wang W, Chen B. Square root unscented Kalman filter with modified measurement for dynamic state estimation of power systems[J]. IEEE Transactions on Instrumentation and Measurement, 2022, 71: 1-13.

[34] Wang Y, Yang Z, Wang Y, et al. Resilient dynamic state estimation for power system using cauchy-kernel-based maximum correntropy cubature Kalman filter[J]. IEEE Transactions on Instrumentation and Measurement, 2023, 72: 1-11.

[35] Schweppe F C. Power system static-state estimation, part III: Implementation[J]. IEEE Transactions on Power Apparatus and Systems, 1970, 89(1): 130-135.

[36] 魏新迟, 徐琴, 柳劲松等. 基于同步相量测量的配电网状态估计方法[J]. 电力系统及其自动化学报, 2023, 35(09): 30-39.

[37] Dobakhshari A S, Abdolmaleki M, Terzija V, et al. Robust hybrid linear state estimator utilizing SCADA and PMU measurements[J]. IEEE Transactions on Power Systems, 2020, 36(2): 1264-1273.

[38] 俞文帅, 张晓华, 卫志农等. 基于深度神经网络的电力系统快速状态估计[J]. 电网技术, 2021, 45(7): 2551-2561.

[39] 夏添梁, 张玉敏, 杨明等. 联合长短期记忆神经网络和粒子滤波的配电网预测辅助鲁棒状态估计方法[J]. 高电压技术, 2022, 48(4): 1343-1355.

[40] 刘晓莉, 曾祥晖, 黄翊阳等. 联合粒子滤波和卷积神经网络的电力系统状态估计方法[J]. 电网技术, 2020, 44(9): 3361-3367.

[41] Musleh A S, Chen G, Dong Z Y. A survey on the detection algorithms for false data injection attacks in smart grids[J]. IEEE Transaction on Smart Grid, 2020, 11(3): 2218-2234.

[42] Cheng G, Lin Y, Zhao J, et al. A highly discriminative detector against false data injection attacks in AC state estimation[J]. IEEE Transaction on Smart Grid, 2022, 13(3): 2318-2330.

[43] Pei C, Xiao Y, Liang W, et al. A deviation-based detection method against false data injection attacks in smart grid[J]. IEEE Access, 2021, 9: 15499-15509.

[44] Wang Y, Zhang Z, Ma J, et al. KFRNN: An effective false data injection attack

detection in smart grid based on Kalman filter and recurrent neural network[J]. IEEE Internet Things Journal, 2022, 9(9): 6893-6904.

[45] Ruan J, Liang G, Zhao J, et al. An inertia-based data recovery scheme for false data injection attack[J]. IEEE Transactions on Industrial Informatics, 2022, 18(11): 7814-7823.

[46] Wang X, Shi D, Wang J, et al. Online identification and data recovery for PMU data manipulation attack[J]. IEEE Transactions on Smart Grid, 2019, 10(6): 5889-5898.

[47] Li Y, Wang Y, Hu S. Online generative adversary network based measurement recovery in false data injection attacks: A cyber-physical approach[J]. IEEE Transactions on Industrial Informatics, 2020, 16(3): 2031-2043.

[48] Wang H, Wen X, Xu Y, et al. Operating state reconstruction in cyber physical smart grid for automatic attack filtering[J]. IEEE Transactions on Industrial Informatics, 2022, 18(5): 2909-2922.

[49] 于尔铿. 电力系统状态估计[M]. 北京: 水利电力出版社, 1985.

[50] 曲正伟, 董一兵, 王云静等. 用于电力系统动态状态估计的改进鲁棒无迹卡尔曼滤波算法[J]. 电力系统自动化, 2018, 42(10): 87-92.

[51] 魏利胜, 张倩. 基于改进的 UKF 智能电网虚假数据攻击检测[J]. 系统仿真学报, 2023, 35(07): 1508-1516.

[52] Zimmerman R D, Murillo-Sánchez C E, Thomas R J. MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education[J]. IEEE Transactions on Power Systems, 2011, 26(1): 12-19.

[53] Hug G, Giampapa J A. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks[J]. IEEE Transactions on Smart Grid, 2012, 3(3): 1362-1370.

[54] 席梦瑶, 赖俊峰, 张改梅. 含缺失数据 Weibull 分布的参数估计及模拟验证[J]. 统计与决策, 2023, 39(17): 46-51.

[55] Wang Y, Sun Y, Dinavahi V. Robust forecasting-aided state estimation for power system against uncertainties[J]. IEEE Transactions on Power Systems, 2020, 35(1):

691-702.

[56] Zhang R, Zhang Q, Wang Z, et al. Detection of false data injection attack in smart grid based on iterative Kalman filter[C]// 2021 China Automation Congress (CAC), Beijing, China, 2021: 6083-6088.

攻读硕士期间取得的学术成果

[1] Hu P F, Gao W G, Li Y F, et al. Anomaly detection and state correction in smart grid using EKF and data compensation techniques[J]. IEEE Sensors Journal, 2024, 24(8): 12995-13009.

[2] Hu P F, Gao W G, Li Y F, et al. Detection of false data injection attacks in smart grids based on expectation maximization[J]. Sensors, 2023, 23(3): 1683-1704.

[3] Hu P F, Gao W G, Li Y F, et al. Detection of false data injection attacks in smart grid based on joint dynamic and static state estimation[J]. IEEE Access, 2023, 11: 45028-45038.

致谢

时光荏苒，转眼间研究生生涯已接近尾声。回首这段充满挑战与成长的岁月，我深感自己收获颇丰。在此，我要向所有陪伴我、支持我、指导我走过这段旅程的人表达衷心的感谢。

首先，我要特别感谢我的导师高文根教授。您的严谨治学态度、勤奋钻研的精神以及对学生在生活和学习上的无私关怀，都为我树立了榜样。在论文的选题、研究以及撰写过程中，您给予了我悉心的指导和帮助，使我能够顺利完成这篇论文。您不仅为我提供了宝贵的学术建议，还时常鼓励我面对困难时不放弃，坚持到底。您的教诲不仅让我在学术上取得了进步，更在人生道路上指引我前行。

其次，我要感谢李云飞老师对我在论文写作中的耐心指导。您每次都是积极参加组会，并给予我们大有裨益的修改建议。从阅读文献到论文撰写，每一步都离不开您的耐心指导和精准点拨。正是您的悉心教导和无私付出，使我能够顺利完成这篇论文，并在学术研究中取得了长足的进步。

此外，我要感谢实验室的同门和师弟师妹们，他们在学术和生活上给予了我很多启发和帮助。我们共同探讨问题、分享经验，一起度过了许多难忘的时光。你们的陪伴使我的研究生生涯充满了欢笑与温暖、使我在学术研究的道路上不再孤单。

同时，我要特别感谢邵艳宇。在我本科和研究生生涯的每一个阶段，你都给予了我无条件的支持和鼓励。当我遇到困难和挫折时，你总是耐心地倾听我的烦恼，给我勇气和信心去面对。你的理解和包容让我能够更加专注于学术研究，追求自己的梦想。你的陪伴让我感到幸福和温暖，你是我前行路上最坚实的后盾。

当然，我还要特别感谢我的家人。在我上学生涯的每一个阶段，你们总是耐心地倾听我的烦恼，给我勇气和信心去面对。你们为我提供了温暖的港湾，让我能够在学习和生活中勇往直前。

最后，我要感谢参与论文评审的各位老师。感谢您们在繁忙的工作中抽出宝贵的时间对我的论文进行认真细致的评审。您们的专业意见和宝贵建议使我的论文更加完善，也让我对自己的研究有了更深入的认识。

尚德致学 唯实惟新